Міністерство освіти і науки України
Державна наукова установа "Інститут модернізації змісту освіти"
Центральноукраїнський національний технічний університет

Комп'ютерна інженерія і кібербезпека: досягнення та інновації

Матеріали Всеукраїнської науково-практичної конференції здобувачів вищої освіти й молодих учених

(м. Кропивницький, 27–29 листопада 2018 р.)

Кропивницький ЦНТУ 2018

УДК 004
ББК 32.97
К63

К63 **Комп'ютерна інженерія і кібербезпека : досягнення та інновації** : матеріали Всеукр. наук.-практ. конф. здобувачів вищої освіти й молодих учених (м. Кропивницький, 27–29 листоп. 2018 р.) / М–во освіти і науки України, Держ. наук. установа "Інститут модернізації змісту освіти", Центральноукр. нац. техн. ун–т. — Кропивницький: ЦНТУ, 2018. — 448 с.

Збірник містить тези доповідей учасників Всеукраїнської науково-практичної конференції здобувачів вищої освіти та молодих учених "Комп'ютерна інженерія і кібербезпека: досягнення та інновації" (м. Кропивницький, 27–29 листопада 2018 року). Праці присв'ячені актуальним питанням інформаційних систем і технологій, технологій проектування комп'ютерних систем та мереж, інженерії програмного забезпечення, комп'ютерних систем штучного інтелекту, мережних ІТ, комп'ютерної електроніки, логіки, схемотехніки, графіки, нормативно-правових засад забезпечення кібернетичної безпеки, інформаційної безпеки національного сегмента кіберпростору, боротьби з кіберзлочинністю, захисту програм та даних в комп'ютерних системах і мережах.

Видання призначене для аспірантів, докторантів, науковців, викладачів і студентів технічних спеціальностей закладів вищої освіти та всіх, хто цікавиться питаннями комп'ютерної інженерії й кібернетичної безпеки.

УДК 004
ББК 32.97
К63

Рекомендовано до друку Науково-технічною радою Центральноукраїнського національного технічного університету (протокол № 11 від 29 листопада 2018 р.)

Відповідальний за випуск: канд. техн. наук Доренський О. П.

Тексти матеріалів конференції друкуються у авторській редакції, мовою оригіналу. За достовірність наведених у публікаціях даних, назв, імен, цитат та іншої інформації відповідальність несуть автори.

Адреса організаційного комітету конференції
Центральноукраїнський національний технічний університет
Кафедра кібербезпеки та програмного забезпечення
просп. Університетський, 8, м. Кропивницький, 25006
(0522) 55-10-49, 39-04-49; cntu-conference@ukr.net; www.kntu.kr.ua

ІНФОРМАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ

ІНЖЕНЕРІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

МЕРЕЖНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

КОМП'ЮТЕРНА ЕЛЕКТРОНІКА, ЛОГІКА Й СХЕМОТЕХНІКА

КОМП'ЮТЕРНА ГРАФІКА

НОРМАТИВНО–ПРАВОВІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

БОРОТЬБА З КІБЕРЗЛОЧИННІСТЮ

ЗАХИСТ ПРОГРАМ ТА ДАНИХ В КОМП'ЮТЕРНИХ СИСТЕМАХ І МЕРЕЖАХ

UDC 004.942

Huskova V. H., Bidyuk P. I.
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Institute of Applied Systems Analysis

A Combined Approach to Modeling Heteroscedastic Processes and Financial Risk Estimation

The study is focused on combined models development for forecasting nonlinear nonstationary heteroscedastic processes in economy, finances, ecology and other areas. Most of the processes in these areas belong today to the class of nonlinear and nonstationary due to many random factors influencing their evolution in time [1]. Most of the processes in finances are influenced by various random shocks inside of the countries where they are generated and by outside shocks in the form of general world crisis, inflation, growth of prices on energy resources etc. Fig. 1 illustrates a simplified classification of the processes.

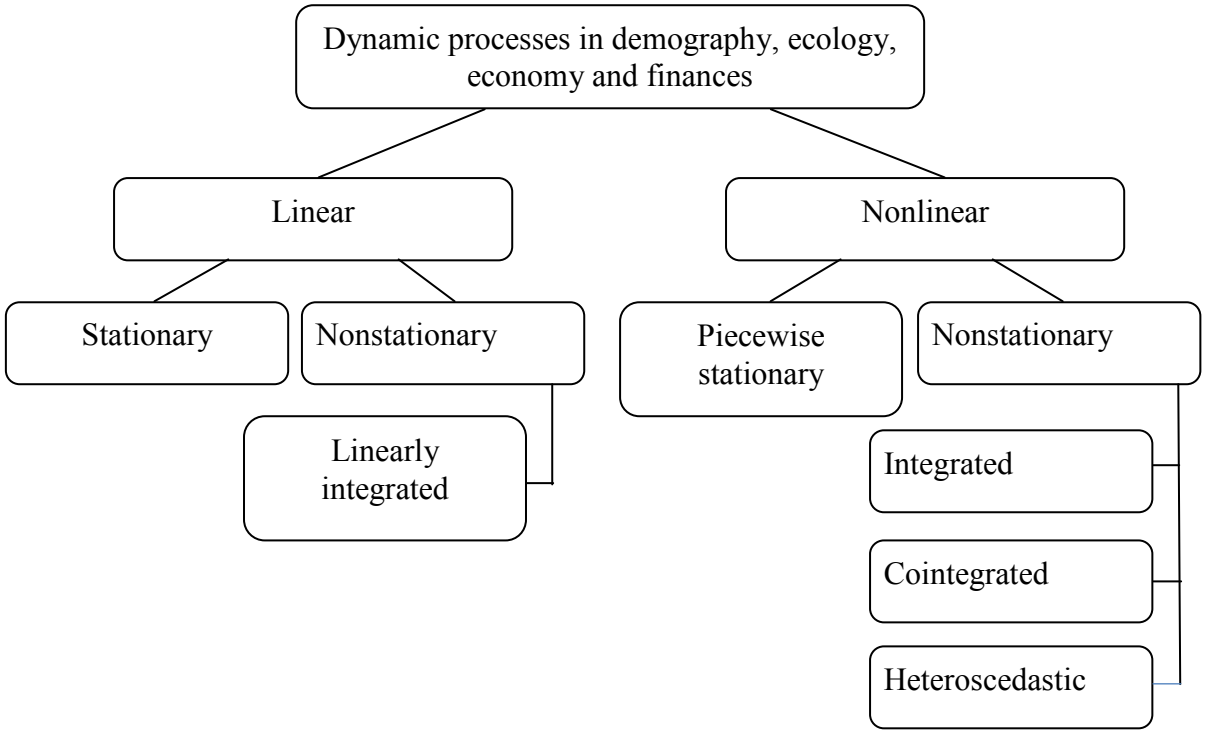


Figure 1 – simplified classification of nonlinear nonstationary processes

Generally linear process can be nonstationary only when it contains linear trend. In all other cases it is linear and stationary. Nonlinear processes sometimes can be piecewise stationary, though mostly in their stable mode of operation. Nonlinear nonstationary processes (NNP) are most commonly met in all aforementioned areas of study. They include nonlinear integrated process with trends of order two and higher, cointegrated processes with the same degree of integration, and heteroscedastic processes. Analysis of the latter processes suggest simultaneous constructing of the following two model types: first model for the process (amplitude) itself, and the second model for formal description of conditional variance dynamics that is widely used in practice for solving various problems of diagnostics (technical, medical, financial and economic), risk management in various spheres of human activities, stock trading etc. It is important to determine a class of a process under study so that to select correctly the model types necessary for modeling the processes. Fig. 2 illustrates

the scheme of the combined approach proposed that is suitable for modeling both linear and nonlinear processes as well as risk estimation.

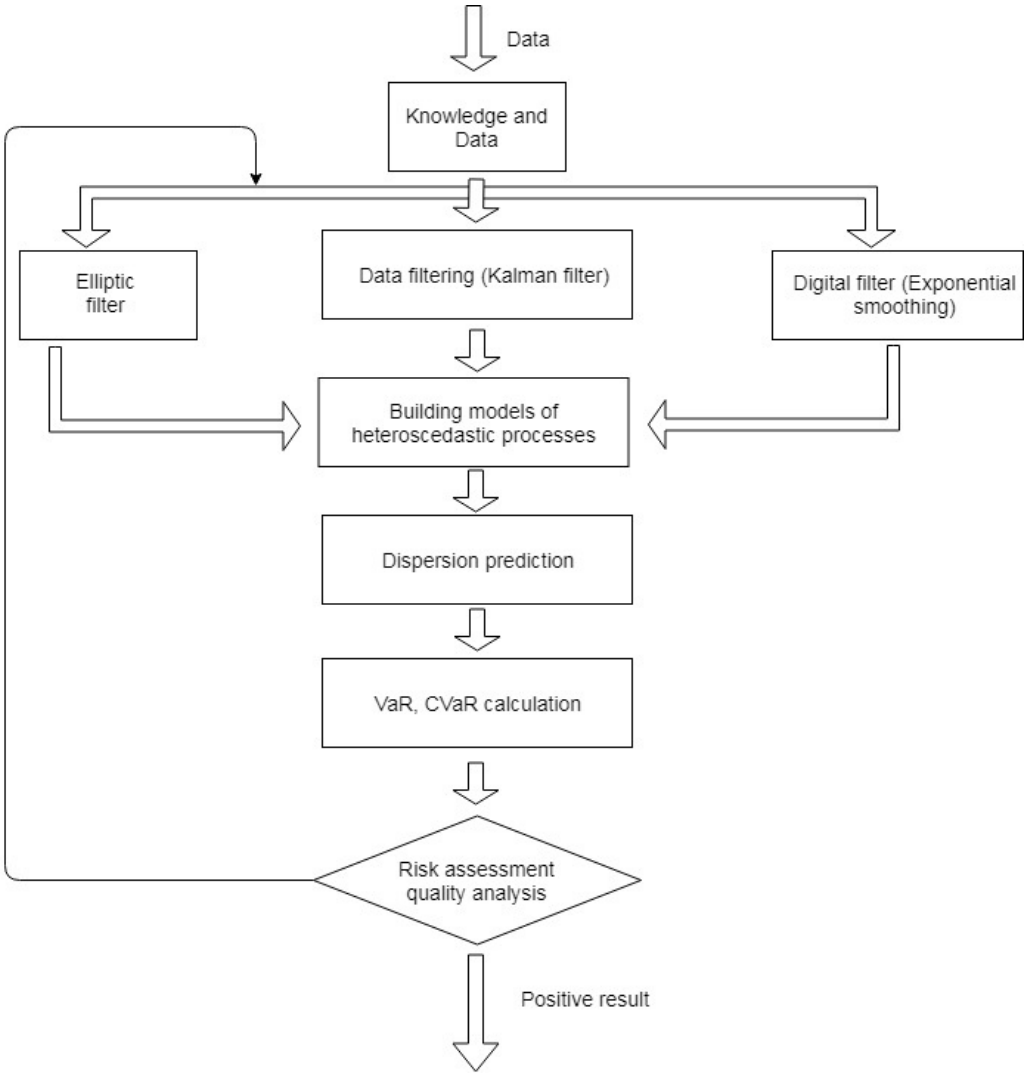


Figure 2 – combined approach to modeling heteroscedastic processes and financial risk estimation

First exponential smoothing, optimal Kalman filtering or elliptical filtering is applied to input data to perform smoothing and prepare the data to further models constructing. After smoothing the model can be linear or nonlinear dependently on effects contained in the input data. Generally data may contain linear and nonlinear part what will result in linear and nonlinear models simultaneously.

In a case of heteroscedastic processes the main problem is to construct a model describing dynamics of conditional variance. One of the best results so far with forecasting the variance was achieved with exponential generalized autoregression with conditional heteroscedasticity (EGARCH) shown below [2]:

$$\log[h(k)] = \alpha_0 + \sum_{i=1}^{p} \alpha_i \frac{|\varepsilon(k-i)|}{\sqrt{h(k-i)}} + \sum_{i=1}^{p} \beta_i \frac{\varepsilon(k-i)}{\sqrt{h(k-i)}} + \sum_{i=1}^{q} \gamma_i \log[h(k-i)] + \upsilon(k) \qquad (1)$$

where $h(k)$ is conditional variance; $\varepsilon(k)$ is random process that influences financial process under study; α_i, γ_i are model parameters to be estimated with maximum likelihood or Monte Carlo Markov chain (MCMC) procedures; $\upsilon(k)$ are model residuals.

Example. Statistical analysis of the time series selected with application of Goldfeld-Quandt test proved that gold prices data create heteroscedastic process with time varying conditional variance. As far as the variance is one of the key parameters that is used in the rules for performing trading operations it is necessary to construct appropriate forecasting models. Table 1 contains statistical characteristics of the models constructed as well as quality of short-term variance forecasting. To solve the problem we used generalized autoregressive conditionally heteroscedastic (GARCH) models together with description of the processes trend which is rather sophisticated (high order process). The models of this type (GARCH) demonstrated low quality of short-term forecasts, and quite acceptable (EGARCH) one-step ahead forecasting properties.

Table 1 – Results of modeling and forecasting conditional variance

Model type	Model quality			Forecast quality			
	R^2	$\sum e^2(k)$	DW	MSE	MAE	MAPE	Theil
GARCH(1,7)	0.99	153639	0.113	972.5	–	517.6	0.113
GARCH (1,10)	0.99	102139	0.174	458.7	–	211.3	0.081
GARCH (1,15)	0.99	80419	0.337	418.3	–	121.6	0.058
EGARCH (1,7)	0.99	45184	0.429	67.8	–	8.74	0.023

Thus, the best model constructed was exponential GARCH(1,7). The achieved value of MAPE = 8.74% comprises very good result for forecasting conditional variance. Further improvements of the forecasts were achieved with application of the adaption scheme [3]. An average improvement of the forecasts was in the range between 0.5 – 1.5%, what justifies advantages of the approach proposed. Combination of the forecasts generated with different forecasting techniques helped to further decrease mean absolute percentage forecasting error for about 0.5 – 0.8% in this particular case. It should be stressed that analysis of heteroscedastic processes is very popular today due to multiple engineering, economic and financial applications of the models and forecasts based upon them.

References

1. *Trofymchuk O.M. Probabilistic and statistical uncertainty processing using decision support systems // Visnyk of Lviv Polytechnic National University, 2015, No. 826, pp. 237-248.*
2. *Tsay R.S. Analysis of financial time series. – New York: John Wiley & Sons, Inc., 2010. – 715 p.*
3. *Dovgiy S.O., Trofymchuk O.M., Bidyuk P.I. DSS based on statistical and probabilistic procedures. – Kyiv: Logos, 2014. – 420 p.*

UDC 004.946

Litvinov A. A., Viniichuk Y. V., Dubovyi M. V., Bezotosnyi D. O.
Oles Honchar Dnipro National University

On Specific of Field Level Database Optimistic Locking for Increasing Information System Performance

In modern multi-user service-oriented systems it is quite possible that multiple users can update the same object at the same time causing data modification conflict. This issue is termed as concurrency problem. Within DBMS the concurrency problems are solved by "locking strategies" [1] using transaction isolation levels. Locking mechanisms prevent simultaneous access to data in a database. Shared and exclusive locks might be set on different levels of database, starting with the whole database level and deep to the row level. Isolation levels determine how the data is locked or isolated from other transactions, processes. Lower isolation level increases the performance, but it also increases the probability of occurrence one of the concurrency phenomena such as dirty reads, lost updates etc.

Practically the use of mechanisms provided by DBMS cannot prevent the modern service-oriented systems from concurrency problems. The situation when remote users are working on the same object or even on a document (represented as a composition of objects) is quite possible. From this point of view, the problem becomes not only the matter of effective execution of incoming transactions and avoidance of concurrency phenomena. Sharing the data means that each user has its own copy of the object and, consequently, the request to change the data from one user can overwrite the changes made by another user with old data copy. It is similar to cache coherence problem in multiprocessor systems.

Two basic patterns of instituting concurrency control [2] are as follows. According to pessimistic concurrency control system locks the data linked with all the objects requested by the user, i.e. after a user gets an object, the object becomes locked to other users until the owner releases the lock. It is mainly used in environments where the cost of protecting data with locks is less than the cost of rolling back transactions if concurrency conflicts occur. In optimistic concurrency control [3], users do not lock the data when they read it. When a user updates data, the system checks to see if another user changed the data after it was read. To make it work each object leveraged by the modification time attribute (timestamp) [4]. If the modification time of the persisted object is not the same as incoming one, it means that another user has already updated the data, and access violation exception is raised. Typically, when the user application receives the error it requests the new copy of the object and starts it over considering the changes. This type of control is mainly used in environments where there is low contention for data [5], and where the cost of occasionally rolling back a transaction is lower than the cost of locking data when read.

The solution works fine when the number of the shared object modification requests is not too high. But when it is, we face the problem. For example, we have an object with a state represented by the fields of 2 categories. The fields of the first category are often to be updated, second one - is rarely updated. Whenever someone tries to update the field of the second category field, he/she should wait until the timestamp of the object will be equal to the timestamp of the persisted one that is rapidly changed because of the 2nd category fields updates. The first solution is to divide the persisted object into two parts and store them separately connected by 1-to-1 relation. In general, the proposed solution brings us to the set of tables where each table responsible for an attribute of the object, i.e. for a column of database table. These tables-columns can be simply distributed among the various nodes. This solution increases the scalability and the performance of the system but seemed too expensive, because each table should have at least two additional fields built the infrastructure: one for string timestamp, other for object id. Another way is to add a number of timestamp fields to the table, each field connected to the set of fields. The solution is not scalable as previous one, but less expensive and more flexible. So, when transaction starts, we must record a date of each category of fields we update. In the above example, we have 2 independent modifications. First transaction set timestamp for first field, after changes checks it and updates the field. Second transaction can modify another field while first transaction is being executed because the lock is set only for first category fields.

Conclusion. The work is devoted to the breaking the limits of the optimistic concurrency control pattern. Two basic solutions based on field-oriented locks are provided.

References

1. *Tropashko V. SQL Design Patterns: The Expert Guide to SQL Programming / Vadim Tropashko., 2006. – 255 c.*
2. *Ambler S. W. Refactoring Databases: Evolutionary Database Design 1st edition / Scott W. Ambler. – Addison-Wesley Professional, 2006. – 384 c.*
3. *Silverston L. The Data Model Resource Book, Volume 3: Universal Patterns for Data Modeling / Len Silverston., 2009. – 648 c.*
4. *Mittra S. S. Database Performance Tuning and Optimization / Sitansu S. Mittra. – New York: Springer-Verlag, 2003. – 489 c.*
5. *Gregg B. Systems Performance: Enterprise and the Cloud / Brendan Gregg., 2013. – 784 c.*

УДК 621.396.2

Артеменко-Діденко А. І., Маковеєнко Д. О.
Одеська національна академія зв'язку ім. О.С. Попова

Моделювання пропускної здатності мережі E-UTRA для адаптивних режимів MCS

Вступ. Нові покоління стільникового зв'язку з'являються з кожним роком все з меншим інтервалом між ними. Телекомунікаційні компанії впроваджують нові технології в цій сфері. Але як і в будь якій іншій сфері постає питання оптимального використання усіх ресурсів із задоволенням якомога більшої кількості показників якості.

Нещодавно в Україні оператори зв'язку почали надавати послуги стандарту 4G (LTE - long-term evolution). Цей стандарт використовує OFDM (orthogonal frequency-division Multiplexing) мультиплексування (модулювання)

Одним з найпростіших методів частотно-територіального планування в системах з OFDM (Orthogonal Frequency-Division Multiplexing). Цей метод має, як переваги, так і недоліки. Серед переваг простота та вища порівняно з іншими методами пропускна здатність. А основний недолік полягає у високому рівні завад, через використання однакової частоти і як наслідок відношення сигнал/шум зменшується.

Використання ж адаптивної модуляції та кодування AMC (adapting modulation and coding) [1] допомагає використати такий тип модуляції, який є оптимальним при певному відношенні сигнал/шум. Така модуляція повинна забезпечити мінімально можливе значення помилкових блоків BLER (block error rate) [2,3].

Вплив втрат на автоматичний вибір типу модуляції в системі AMC. Розробка мереж LTE полягає у вдосконаленні свого фізичного рівня (E-UTRA Radio Access Network).

Мережа E-UTRA дозволяє адаптуватись, застосовуючи різні типи модуляції (табл. I). [4] Кожен тип може використовуватися з заданим пороговим значенням сигнал/шум (SNR), що залежить від втрат при поширенні сигналу.

Адаптована зміна схеми коду модуляції, як основної частини процедури AMC, включає в себе можливість визначення порогового значення SNR та, за допомогою циркуляції зворотного зв'язку, змінювати параметри передачі та тип MCS.

Таблиця 1 – Параметри MCS

№ MCS	*Тип модуляції*	*Швидкість коду*	*Спектральна ефективність,біт/с/Гц*	*SNR, дБ*
1	QPSK	0.076	0.1523	-6,8
2	QPSK	0.12	0.2344	-5,2
3	QPSK	0.19	0.3770	-3,1
4	QPSK	0.3	0.6016	-2,2
5	QPSK	0.44	0.8770	-0,8
6	QPSK	0.59	1.1758	1,4
7	16QAM	0.37	1.4766	3,3
8	16QAM	0.48	1.9141	5,3
9	16QAM	0.6	2.4063	7
10	64QAM	0.45	2.7305	10,5
11	64QAM	0.55	3.3223	11,6
12	64QAM	0.65	3.9023	14,1
13	64QAM	0.75	4.5234	16,8
14	64QAM	0.85	5.1152	18
15	64QAM	0.93	5.5547	21,5

Втрати потужності сигналу. За основу для розрахунку цих даних була використана модель Окамура – Хати для великих міст. Вихідні дані наведені в таблиці 2.

Раніше науковцями розглядалася ефективність використання системи АМС [5], в дослідженні були розрахована пропускна здатність відповідно до теореми Шеннона. В даному дослідженні ставиться за мету порівняти пропускну здатність згідно з теоремою Шеннона та реальну пропускну здатність відповідно до системи АМС.

Таблиця 2 – Вихідні дані

Параметр	*Значення*
Частота	1805-1880 МГц (Band3)
Максимальна відстань у фіранці	1 км
Висота передавальної антени	30 м
Висота приймальної антени	2 м
Частота	15 МГц
Потужність передавача	10 Wt
Ширина смуги	4.5 МГц

$$L = 69.55 + 26.16\log(f) - 13.821\log(h_{tr}) + \left[44.9 - 6.55\log(h_{tr})\right]\log(d)^b - \alpha \quad (1)$$

Де, L :середні втрати (дБ); f :частота (МГц); h_{tr}:висота передавальної антени (м); h_r:висота приймальної антени (м); d :відстань між прийачем і передавачем (км); b=1, if d≤20км

$$\alpha = 3.2 \cdot (\log 11.75 \cdot h_{tr})^2 - 4.97 \quad (2)$$

Існує шість сигналів з однаковою частотою навколо центральної фіранки (рис. 1), і вони є завадами для сигналу від досліджуваного передавача [6].

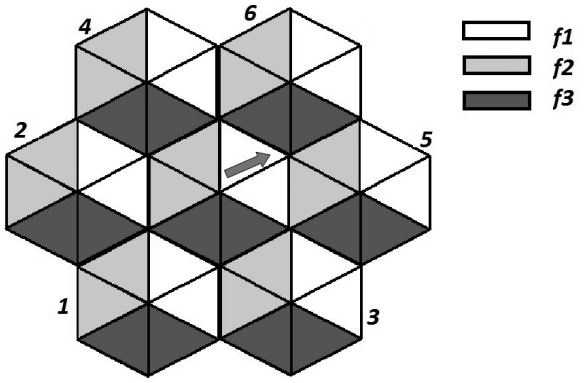


Рис.1 Центральна фіранка оточена іншими фіранками

Відстань від кожної сусідньої антени до кожної з точок на шляху руху відрізняється, але можна сказати, що з 1 і 2 фіранок вона буде однаковою. Те ж саме можна відзначити і для пар 3,4 і 5,6.

$$R_{1,2} = \sqrt{\left(\frac{2\sqrt{3}\cdot d}{2}\right)^2 + R_i^2 + \frac{2\cdot 2\sqrt{3}\cdot d}{2}\cdot R_i \cdot \frac{\sqrt{3}}{2}} \quad (3)$$

$$R_{3,4} = \sqrt{\left(\frac{2\sqrt{3}\cdot d}{2}\right)^2 + R_i^2} \quad (4)$$

$$R_{5,6} = \sqrt{\left(\frac{2\sqrt{3}\cdot d}{2}\right)^2 + R_i^2 - \frac{2\cdot 2\sqrt{3}\cdot d}{2}\cdot R_i \cdot \frac{\sqrt{3}}{2}} \quad (5)$$

Де: R_i :відстань від точок на шляху до кожної з фіранок, що є завадами

Розраховуючи всі втрати на шляху сигналу, шум та завади від сусідніх антен, розраховувався співвідношення сигнал/шум із врахуванням та без врахування завад. (табл. 3).

Таблиця 3- Відношення сигнал/шум

Відстань, м	*Сигнал/шум без завад, дБ*	*Сигнал/шум із завадами, дБ*
100	51.766	39.522
200	41.162	29.305
300	34.96	23.419
400	30.559	19.26
500	27.145	16.003
600	24.356	13.279
700	21.998	10.889
800	19.955	8.716
900	18.153	6.698
1000	16.541	4.804

Пропускна здатність. Для обчислення пропускної здатності була використана теорема Шеннона

$$R_{C1} = \frac{\Delta F}{3 \cdot 10^6} \cdot \log_2(1 + 10^{0.1(P-L-N)}) \quad (6)$$

$$R_{C2} = \frac{\Delta F}{3 \cdot 10^6} \cdot \log_2(1 + 10^{0.1 \cdot h}) \quad (7)$$

Де: R_{C1}: пропускна здатність не враховуючи шум; R_{C2}: пропускна здатність враховуючи шум; P: потужність передавача; N: рівень шуму; h: відношення сигнал/шум

Але для порівняння параметрів також використовувався розрахунок відповідно до адаптивної системи MCS.

$$R_C = \gamma \cdot \Delta F \quad (8)$$

Де: R_C: пропускна здатність відповідно до адаптивної системи MCS γ: Спектральна ефективність; ΔF: ширина смуги каналу.

З графіків (рис.2) можна побачити, що пропускна здатність розрахована за теоремою Шеннона набагато перевищує реальну, що використовує адаптивна система модуляції поблизу передавальної станції.

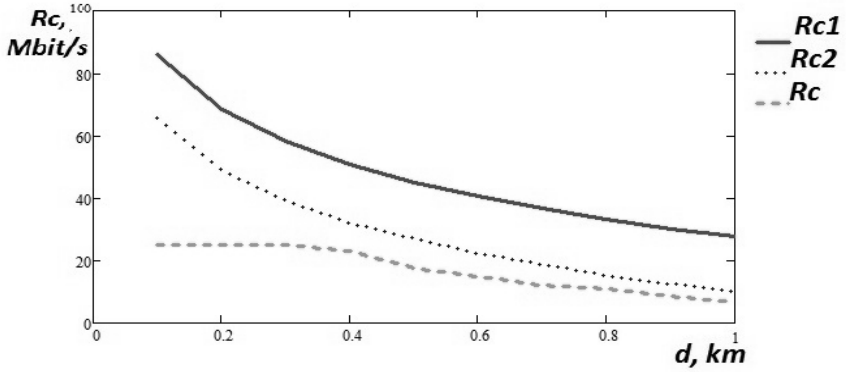


Рисунок 2. Пропускні здатності каналу

Список використаних джерел

1. *P.I. Chernobay. Analysis of increase capacity E-UTRA using SFR / P.I. Chernobay, D.A. Makoveyenko // Refrigeration engineering and technology. – 2014. – № 1. – P. 76 – 80.*
2. *Tihvinskij V.O. Seti mobilnoj svjazi LTE. Tehnologii i arhitektura / V.O. Tihvinskij, S. V. Ter-ent'ev, A. B. JUrchuk – M.: JEko-Trendz, 2010. – 284 p.*
3. *Babkov V.U. Seti mobilnoj svjazi. Chastotno-territorialnoe planirovanie / V.U. Babkov, Voznjuk M.A., Mihajlov P.A. – M.: Gorjachaja linija-Telekom, 2007. – 224 p.*
4. *Sajid Hussain, "Dynamic Radio Resource Management in 3GPP LTE", Blekinge Institute of Technology, 2009. – 58 p.*
5. *Report ITU-R SM.2028-2. Monte Carlo simulation methodology for the use in sharing and compatibility studies between different radio services or systems, 2017. – 57 p.*
6. *Specification 3GPP TR 25.913. Requirements for evolved UTRA (E-UTRA) and evolved UTRAN (E-UTRAN), 2009. – 20 p.*

УДК 004

Береговий С. М.
ДВНЗ «Криворізький національний університет»

Побудова інформаційних систем керування виробничими конвеєрними лініями засобами SCADA Wonderware System Platform

Сучасні виробники товарів активно використовують усі можливі активи для оптимізації виробничих процесів і зниження витрат. Одним із напрямків оптимізації є використання сучасних SCADA-систем.

SCADA Wonderware System Platform реалізує інформаційну модель управління виробничими конвеєрними лініями засобами завдяки таким сервісам: візуалізація даних, конфігурація підсистем і модулів, розгортання розподіленої інфраструктурі, зв'язки в рамках цієї розподіленої інфраструктури, безпека в середовищі для користувачів, підключення до обладнання і керуючих систем, збереження та управління даними, організація колективної роботи користувачів та ін.

В основі SCADA-системи лежить людино-машинний інтерфейс Wonderware InTouch з графічною середою ArchestrA, який дозволяє швидко розробляти стандартизовані, легко тиражовані додатки для візуалізації і, не виходячи з офісу управління, розгортати їх на географічно розподілених об'єктах.

Першим кроком для створення подібних інформаційних систем керування є власне побудова конвеєрів. На основних вузлах проходження товарів встановлюються контролери для приведення механізмів у дію, цифрові датчики та лічильники під’єднуються до загальної мережі та збирають важливу інформацію про стан обладнання та товарів.

Основним завданням SCADA є вилучення даних з цих пристроїв, обробка та збереження на сервері. Доступ до даних пристроїв здійснюється за допомогою протокола SuiteLink. Протокол SuiteLink був спеціально розроблений фірмою Wonderware. В основі протоколу SuiteLink лежить протокол TCP/IP. SuiteLink не є заміною протоколам DDE, FastDDE і NetDDE. Новий протокол розроблений для підтримки швидкодіючих промислових систем і володіє наступними характеристиками: 1. Передача даних здійснюється у форматі VTQ (Value, Time, Quality - значення, час, якість); 2. Завдяки системному монітору операційної системи Windows NT (Performance Monitor) став можливим розширений аналіз продуктивності по передачі даних, ступеня завантаження сервера, ступеня споживання ресурсів комп'ютера і мережі; 3. Підтримка обміну даними між додатками відбувається незалежно від того, чи виконуються ці додатки на одному вузлі мережі або на різних.

Для реалізації функцій OPC-клієнта Wonderware пропонує OPCLink - сервер, що перетворює OPC в SuietLink протокол.

Після того, як System Platform вилучить необхідні для керування дані, у додатку WindowMaker InTouch створюється інтерфейс автоматизованого робочого місця керування процесами за допомогою великого набору різноманітних 2D та 3D символів, які графічно будуть моделювати конвеєрну лінію.

Кожен символ має набір тегів для того, щоб змінювати властивості в залежності від даних, які він отримує. Для того, щоб інтерфейс працював у режимі реального часу необхідно передати символьним тегам відповідні змінні, які містить контролери або датчики на конвеєрних лініях.

Перевагою подібних інформаційних систем є є те, що можна легко створювати HMI-додатки та знизити витрати часу та грошей на обслуговування конвеєрних ліній.

До недоліків можна віднести: висока вартість самого програмного забезпечення та суттєві вимоги до обчислювальних ресурсів та якості каналів передачі.

УДК 519.95

Бураков Р. А., Левицька Т. О.
ДВНЗ «Приазовський державний технічний університет»

Автоматизована обробка класичних творів для фортепіано з використанням сіамської нейронної мережі

Системи обробки та аналізу природної мови з використанням машинного навчання є досить розвиненими і актуальними в наш час. Сучасні системи обробки людської мови здатні розуміти мову не як набір окремих слів або букв, а як цілі речення і їх сенс. Однак, незважаючи на таку актуальність методів аналізу семантики природної мови, системи обробки музики в даній області помітно відстають.

Дана роботи присвячена створенню унікальної моделі нейронної мережі, здатної розуміти музику та її семантику на рівні, зіставному з рівнем розуміння природної мови сучасними моделями нейронних мереж для обробки та аналізу природної мови. У роботі були проаналізовані вже існуючі в цій галузі статті, сформульовані їх основні недоліки і запропоновані методи їх вирішення.

В ході роботи був запропонований метод нотації нот у вигляді акордів з обмеженням на максимальну кількість нот, які він містить і на його максимальну ширину. Такі обмеження дозволяють усунути проблему зайвих витрат потенціалу нейронної мережі на процес збору акордів з безлічі шматочків. На основі даного визначення акордів був створений унікальний словник, який є типовим за розміром серед невеликих моделей обробки природної мови.

Істотним досягненням запропонованого методу є адаптація технології векторного уявлення слів word2vec в контекст музичних акордів. Векторне уявлення є сильним методом навчання нейронних мереж семантиці природної мови. Дана технологія дозволяє навчити мережу знаходити зв'язки між словами ґрунтуючись лише на контексті, в якому вони знаходяться.

Для адаптації технології word2vec треба було багато прикладів існуючих класичних творів для піаніно. У даному проекті використовується відкрита база класичних творів в форматі MIDI, зібрана Берндом Крюгером. Ця база була складена вручну, однак у цьому проекті є можливість працювати і з менш структурованими базами, наприклад створеними із записів живих піаністів.

Для навчання нейронної мережі технології векторного уявлення було треба було уявити музичні твори у вигляді послідовності акордів зі словника. Цей процес детально описано в роботі. Для розширення бази для навчання, було використано метод узагальнення вхідних даних – транспозиції акордів. Даний прийом зміщує кожну ноту в творі на заданий інтервал, що варіюється від однієї октави вниз або вгору. Такий метод дозволяє збільшити розмір бази акордів для навчання в 23 рази. При цьому, нейронна мережа навчається важливої властивості: якщо програти композицію в іншому ключі - вона як і раніше буде звучати мелодійно

У процесі навчання нейромережі векторному уявленню акордів, з бази вибираються пари акордів, які стоять в одному контексті і нейронна мережа дає їм оцінку 0 або 1. Щоб не виявилося, що нейромережа всі зв'язки оцінює як сильні і ніколи не видає 0, використовується негативне семплювання, яке полягає в тому, що для кожної пари з оцінкою 1 вибирається кілька інших пар, яким дається оцінка 0.

Таким чином мережа вчиться робити зв'язки між одними акордами сильніше, а між іншими слабкіше.

Після навчання нейронної мережі, отримане векторне подання було спроектовано методом t-SNE на двовимірну поверхню для подальшого аналізу. В ході проведення аналізу було виявлено, що нейронна мережа навчилася виявляти такі властивості акордів, як їх висота звучання і нотний склад виходячи лише з індексу акорду в словнику і контексту, в якому він знаходиться. Тобто мережа не отримувала інформацію про будь-які властивості акордів заздалегідь.

Векторне подання акордів дозволяє знайти акорди, які мають схожу семантичну роль з даними. Для цього вираховується значення косинусного коефіцієнта для всіх акордів зі словника в парі з заданим, після чого акорди упорядковуються по зростанню отриманого коефіцієнта.

При цьому була знайдена цікава закономірність: на відміну від акордів з однієї клавіші, де схожі акорди зазвичай вишиковуються в міру збільшення інтервалу, схожі акорди з декількох клавіш, як правило, мають одні і ті ж ноти в складі, просто в різних комбінаціях. В роботі наводяться пояснення чому саме таким ознаками дає пріоритет нейронна мережа.

Варто ще раз відзначити, що нейронна мережа не отримувала ніяких даних о клавішах в акорді або інтервалах між ними, тільки індекс акорду і його контекст. Виходить, що вона змогла сама визначити властивості акордів виходячи лише з його індексу і контексту.

В результаті, в роботі розглянуті недоліки більшості існуючих моделей нейронних мереж для аналізу і обробки музичних творів для фортепіано та методи їх вирішення. Ґрунтуючись на отриманій в ході проведення дослідження інформації, показано, що методи аналізу і обробки природної мови виявилися ефективними для музичних творів. Запропоновано новий спосіб нотації нот, запропоновано метод транспозиції акордів і створено унікальний словник музичних акордів. Була спроектована нейронна мережа і застосовано метод векторного уявлення на акорди з алгоритмом навчання skip-gram. Отримані результати показали здатність нейронної мережі навчатися таким властивостям акордів, як висота звучання і нотний склад, при тому, що мережа не отримувала цих даних про акорді заздалегідь.

Список використаних джерел

1. *Lim H. Chord Generation from Symbolic Melody using/ H. Lim, S. Rhyu, K. Lee // arXiv: 1712.01011v1 [cs.SD] - 2017.*
2. *Qu L. Chord2Vec: Learning Musical Chord Embeddings / L. Qu, C. Walder // 30th Conference on Neural Information Processing Systems - 2016.*
3. *Sears D. Evaluating Language Models of Tonal Harmony / D. Sears, F. Korzeniowski, G. Widmer // arXiv: 1806.08724v1 [cs. SD] - 2018.*
4. *Herremans. D. Modeling Musical Context Using Word2vec / D. Herremans, C.-H. Chuan // arXiv: 1706.09088v2 [cs.SD] - 2017.*
5. *Mikolov T. Efficient Estimation of Word Representations in Vector Space/ T. Mikolov, K. Chen, G. Corrado, J. Dean // arXiv: 1301.3781v3 [cs .CL] - 2013.*
6. *Maaten L. Visualizing Data using t-SNE / L. Maaten, G. Hinton // Journal of Machine Learning Research - Рік випуску 2008 - №9 - P. 2579-2605.*

УДК 004:378.1

Вакуленко Д. О.
Центральноукраїнський національний технічний університет

Актуальні питання впровадження інфокомунікаційних технологій в агропромисловому комплексі України

В сучасних умовах основним засобом зростання і розвитку економік у довгостроковій перспективі стають досягнення науково-технічного прогресу та інновації. Надзвичайної актуальності набуває пошук нових технологій, здатних забезпечити підвищення ефективності функціонування аграрної галузі в умовах збіднення природних ресурсів. На сьогодні постійне впровадження новітніх розробок є реальною запорукою сталого розвитку сільського господарства. У зв'язку з цим особливої уваги вимагає питання виявлення позитивних та негативних наслідків впровадження передових агроінноваційних технологій, як запорука ефективного виявлення та усунення загроз технологічній безпеці аграрної галузі [1].

У наш час сільське господарство потребує оптимізації виробництва з метою одержання максимального прибутку, раціонального використання ресурсів, у тому числі природних, захисту навколишнього середовища. Воно набуває нових особливостей. Звичайне сільське господарство перетворюється на "точне", яке передбачає ефективне та раціональне керування процесами росту рослин відповідно до їх потреб у поживних речовинах й умовах зростання [2].

Врожайність сільськогосподарської культури на різних ділянках одного й того ж поля не буває однаковою. На показники врожайності впливають такі фактори, як: якість ґрунту (родючість, кислотність); дози й види добрив; топографія місцевості; наявність лісосмуг; технологія посіву, догляду за сільськогосподарською культурою, збирання врожаю; якість насіння; хвороби, шкідники сільськогосподарських рослин; погодні умови. Порівнюючи ті чи інші характеристики полів з картами врожайності, фахівці господарства можуть виявляти причини нерівномірної врожайності сільськогосподарської культури на полі (окремі ділянки поля більше продуктивні, ніж інші) і після того вживати необхідних заходів.

Знаючи карти врожайності, ґрунтові й інші характеристики полів, використовуючи глобальну позиційну й географічну інформаційну системи, датчики, автоматичні пристрої робочих частин машин, вже є можливість встановити програму руху машинного агрегату (наприклад, з метою поливу) і по заданих програмах вносити на конкретну ділянку поля відповідну кількість води з певними домішками у необхідних пропорціях [4].

Використання сучасних інформаційних технологій в діяльності аграрних підприємств зумовлюють зміну робочих місць, зокрема створення автоматизованих робочих місць. Революція в інформаційних технологіях, яка відбувається сьогодні – глобальний процес, що створює нові можливості в професійній діяльності. В сучасних умовах лідируючі позиції можна зайняти тільки за умови широкого використання інформаційних технологій. Прийняття обґрунтованих рішень знаходиться в прямому зв'язку від того, який обсяг інформації надходить та як вона використовується. Для того, щоб використовувати її результативно, потрібно навчитися накопичувати, узагальнювати, оволодівати інформацією як про внутрішнє, так і про зовнішнє по відношенню до організації, підприємства чи установи середовище. Головним завданням є постійна адаптація до динамічного зовнішнього середовища.

При переході до вищого рівня управління в аграрному підприємстві необхідні інші методологічні підходи до організації і обробки даних отриманих в дослідах, які повинні базуватись на принципах системного підходу до вивчення об'єкту досліджень.

Сучасна економічна ситуація диктує аграрним підприємствам новий підхід до організації внутрішнього планування. За залучення іноземних інвесторів усе частіше необхідним є бізнес-план, який би відповідав міжнародним стандартам і був адаптований до наших умов. Тому виникає потреба в покращенні механізму бізнес-планування із застосуванням при цьому сучасних інформаційних технологій [5].

Найоптимальнішим варіантом для бізнес-планування в аграрному підприємстві є використання комп'ютерної програми Project Expert, яка має не лише дружній інтерфейс, а й дає можливість користувачу описати практично будь-який інвестиційний проект, будь-яку схему фінансування, враховує ризики проекту.

Project Expert дозволяє представляти результати розрахунків у вигляді готових розділів бізнес-плану. Програма Project Expert має декілька рівнів:

перший рівень − Project Expert призначений для розробки стратегічного плану розвитку підприємства. Він включає процедури опису підприємства, його баланс, плани збуту і виробництва, фінансові звіти та інше.

другий рівень − Project Expert Professional дозволяє не тільки здійснювати фінансове планування підприємства або проекту, але й контролювати виконання планів. Крім того, цей рівень дозволяє здійснювати фінансове планування і контроль групи проектів. Для цього в програмний комплекс включено додатковий модуль Project Integrator, який дозволяє розраховувати загальний потік коштів для групи проектів і розраховувати загальні критерії ефективності.

третій рівень − Project Expert Holding призначений для фінансового планування і контролю діяльності крупних корпорацій [3].

Використання сучасних ІКТ у діяльності аграрних підприємств з метою збору, зберігання, перетворення і систематизації інформації має велике значення для корегування технологій управління у сільському господарстві, а також поточного та довгострокового планування й прогнозування економічних явищ. Завдяки широкому використанню сучасних інформаційних технологій вдається досягти кращих результатів в аграрному секторі. Врожаї стають кращими, продукція − якіснішою.

За рахунок інтенсивних технологій ведення вітчизняного сільськогосподарського виробництва можна досягти збільшення виробництва валової продукції, покращити її якість, скоротити витрати ресурсів, що, в свою чергу, сприятиме підвищенню ефективності та прибутковості агровиробництва. Тому необхідність фінансування впровадження електронної техніки в агропромисловий комплекс, підготовки кадрів, здатних створювати й застосовувати інформаційні технології в сільському господарстві, є очевидною.

Список використаних джерел

1. *Крачок Л.І. Новітні технології у сільському господарстві: проблеми і перспективи впровадження / Л.І. Крачок // Сталий розвиток економіки. – 2013. – Вип. 20. – С. 224-231.*
2. *Воскобойников Б.С. и др.Словарь по гибким производственным системам и робототехнике: Англ.,нем.,фр.,нидерл.,рус.:Ок.5600 терминов / Воскобойников Б.С., Зайчик Б.И., Палей С.М.- М.:Рус.яз.,1991. –392 с.*
3. *Загальна характеристика програми Project Expert [Електронний ресурс] /Режим доступу: http://studentbooks.com.ua/content/view/1326/42/1/2/.*
4. *Єдамова А.М. Застосування сучасних інформаційних технологій у сільському господарстві [Електронний ресурс] / А.М. Адамова // Наукова конференція "Наука та практика: Інновація 2007". – Полтава: ГО "Аграрна наука та практика", 2007. – Режим доступу: http://www.pdaa.edu.ua/np/pdf2/27.pdf.*
5. *Тищенко С.І. Використання інформаційних технологій у діяльності аграрних підприємств / С.І. Тищенко // Вісник ХНАУ ім. В.В. Докучаєва. № 3. Серія „Економічні науки".*

УДК 004.02

Гвозденко В. О., Дем'янчик С. О., Давиденко Є. О.
Чорноморський національний університет імені Петра Могили

Технологія прийняття оптимального стратегічного рішення в військово-цивільний сфері

У питаннях, що стосуються військово-цивільної сфери, постійно виникають ситуації ризику, при яких відомі ймовірності настання можливих станів зовнішнього середовища, проте при різних варіантах розвитку цього середовища найкращий результат забезпечується різними альтернативами [1]. В цьому випадку для прийняття рішень в умовах невизначеності та ризику може бути використана наступна модель.

Технологія підтримки прийняття рішень основана на критерії вибору відповідних методів [2]. В якості такого критерію обрано особливість короткострокової пам'яті людини, яка полягає в здатності запам'ятовувати певну кількість структурних одиниць інформації (7±2), що отримали назву «числа Міллера». При виконанні умови $n \leq 9$ та $m \leq 9$, доцільно використовувати метод аналізу ієрархій і його модифікації, що дозволяє вирішити задачу вибору кращої альтернативи. В іншому випадку технологія передбачає наступний підхід. Попередньо обирається два критерії, перевагу між якими визначити неможливо або вкрай складно, та з використанням процедури Парето-оптимального вибору проводиться виділення з вихідної множини альтернатив підмножини недомінуючих альтернатив відносно вказаних критеріїв. Для подальшого аналізу цієї підмножини використовується побудова дерева цілей, що дозволяє вирішувати задачі ранжування або кластеризації альтернатив.

Аналіз проблеми прийняття рішень в MAI починається з побудови ієрархічної структури, яка включає мету, критерії, альтернативи і інші фактори, що впливають на вибір. Ця структура відображає розуміння проблеми особою, яка приймає рішення. Кожен елемент ієрархії може представляти різні аспекти задачі, що розв'язується, причому до уваги можуть бути прийняті як матеріальні, так і нематеріальні чинники, вимірювані кількісні параметри та якісні характеристики, об'єктивні дані і суб'єктивні експертні оцінки. Іншими словами, аналіз ситуації вибору рішення в MAI нагадує процедури і методи аргументації, які використовуються на інтуїтивному рівні.

Наступним етапом аналізу є визначення пріоритетів, які представляють відносну важливість або перевагу елементів побудованої ієрархічної структури, за допомогою процедури парних порівнянь. Для цього використовується шкала парних порівнянь Т. Сааті. Безрозмірні пріоритети дозволяють обґрунтовано порівнювати різнорідні фактори, що є відмінною рисою MAI.

Отже, перший крок MAI полягає в декомпозиції та представленні задачі в ієрархічній формі. Вершина ієрархії – це мета (ціль, яку треба досягти у поставленій задачі). У нашому випадку це вибір стратегічного рішення у військово-цивільній сфері. На другому рівні ієрархії знаходяться критерії, що впливають на прийняття рішення. Найнижчий рівень ієрархії – перелік альтернатив (стратегічних рішень).

Вибір множини Парето-оптимальних рішень представляє собою відбір перспективних альтернатив, з яких потім відбирається одна (найкраща) альтернатива. Множина Парето представляє собою множину альтернатив, які мають наступну властивість: будь-яка з альтернатив, що входять в множину Парето, хоча б за одним критерієм краща за будь-яку іншу альтернативу, що входить в цю множину.

Вибір множини Парето проводиться таким чином. Всі альтернативи попарно порівнюються одна з одною за всіма критеріями. Якщо при порівнянні будь-яких альтернатив виявляється, що одна з них не краща за іншу ні за одним критерієм, то її

можна виключити з розгляду. Виключену альтернативу не потрібно порівнювати з іншими альтернативами, так як вона явно безперспективна.

На наступному етапі на основі методу дерева цілей виокремлюються найбільш суттєвіші альтернативні підходи з множини недомінуючих рішень. На останньому етапі за допомогою елементів теорії нечітких множин обирається найкраща альтернатива для досягнення глобальної цілі, якою є вибір стратегічного рішення у військово-цивільній сфері (рис. 1).

Рисунок 1 – Структура технології підтримки прийняття рішень в задачах вибору альтернатив на основі інтеграції MAI, Парето-оптимального вибору та методу дерева цілей

При прийнятті оптимального рішення в військово-цивільній сфері ціна ризику є достатньо високою порівняно з наявними ресурсами, тому необхідно вибрати таку модель, яка дасть гарантований результат. Враховуючи вище зазначене, запропоновано інформаційну технологію підтримки прийняття рішень в задачах вибору альтернатив на основі інтеграції MAI, Парето-оптимального вибору та методу дерева цілей.

Список використаних джерел

1. *Швед А. В. Оцінка експлуатаційного стану об'єктів військово-цивільного призначення в умовах невизначеності / А. В. Швед, Є. О. Давиденко // «ІНТЕРНЕТ-ОСВІТА-НАУКА-2018», Одинадцята міжнародна науково-практична конференція ІОН-2018, 22-25 травня, 2018 : Збірник праць. – Вінниця: ВНТУ, 2018 – С. 122-123.*
2. *Згуровський М. З., Катренко А. В., Пасічник В. В., Пасько В. П. Теорія прийняття рішень : Підручник / За ред. М. З. Згуровського. – К. : Видавнича група BHV, 2009. – 448 с.*

УДК 004.716

Голобородько Р. В.
Харківський національний університет радіоелектроніки

Дослідження захищеності мереж UMTS/LTE із використанням двостороннього підсилювача у комплексі зі спрямованою антеною

В наш час, завдання забезпечення захищеності інформації стає все більш актуальним. Широкого розповсюдження набули цифрові пристрої для роботи в мережах UMTS / LTE, в тому числі для комерційного / індустріального використання. При поширенні електронних пристроїв збільшується рівень шумів, зростає нестабільність мережі. Тож підвищуються вимоги до якості радіопристроїв та до покриття мережі. З переходом на UMTS (третє покоління) збільшилася робоча частота і, відповідно, зменшилася дальність зв'язку. Таким чином випливає проблема переходу комерційного обладнання на UMTS.

При розгляді системи зв'язку UMTS, загрозою захисту інформації стає не конфіденційність, а цілісність і доступність інформації та каналу зв'язку через який вона передається. Найбільш чутливою до блокування / втрати зв'язку є сегмент "Базова станція – абонентський пристрій".

Це відбувається за деяких причин:

- природних: відображення, інтерференція, нерівномірне затухання;
- штучних: перевантаженість БС, глушилки, промислові завади.

При збоях в роботі каналу зв'язку будуть неминуче відбуватися труднощі в функціонуванні життєво важливих сервісів, таких як банківські термінали в супермаркетах, систем сигналізації, тощо. Таким чином комерційні фірми можуть зазнавати збитків, а клієнти відчувати незручності.

Наведені проблеми дозволяє частково вирішити зовнішня спрямована антена при установці її на кожен девайс. Кращим варіантом є використання двостороннього підсилювача у комплексі зі спрямованою антеною, який виконує ті ж функції значно зручнішим способом. Пристрій являє собою блок прийомопередавача з підсилювачем, до якого підключена зовнішня спрямована та внутрішня антени.

До переваг від використання підсилювача слід віднести наступні:

- Забезпечення зв'язку в важкодоступних місцях для великої кількості абонентських пристроїв
- Зниження випромінювання абонентського передавача
- Знижується рівень чутливості до перешкод
- Зменшується чутливість до "глушилок"
- Можливість вибору потрібної базової станції шляхом обертання антени

Розглянемо принцип роботи підсилювача і його вплив на якість зв'язку в умовах спрямованої перешкоди (рисунок 1).

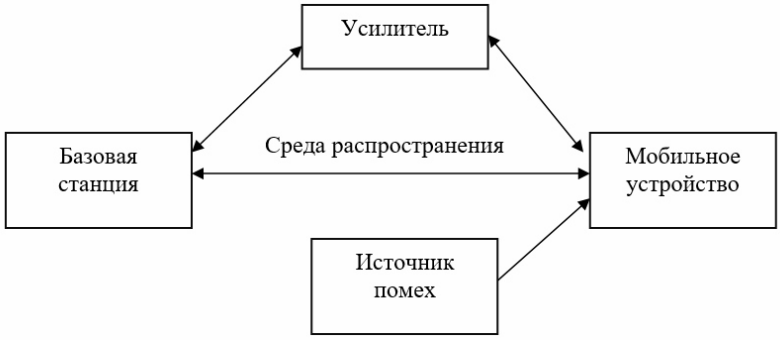


Рисунок 1 – Схема мережі з перешкодою та підсилювачем

Частіше заглушують сигнал від базової станції до абонента. Це пов'язано з великим загасанням корисного сигналу на трасі поширення. За формулою Фріїса [1] розраховано приблизну потужність сигналу базової станції на відстані декількох кілометрів

$$Pr = Pt \cdot Gt \cdot Gr(\lambda/4\pi d)^2 \approx -85 \text{ dBm} = 3.16 \text{ pW} \quad (1)$$

Розрахунки показують що рівень вхідного сигналу на абонентському пристрої досить низький у порівнянні з потужністю перешкоди. В реальних умовах значення будуть ще меншими і цього вистачатиме для роботи в сприятливих умовах, але розглядається випадок з перешкодою. Сигнал перешкоди теж загасає, але оскільки вона знаходиться ближче до приймача, то зловмисник глушилкою потужністю навіть в один Ват може вивести з ладу всі пристрої, що знаходяться в радіусі десятків метрів.

Оскільки мобільні станції приймають сигнал на фоні шуму, введено поняття відношення сигнал/шум. Чим воно більше – тим більша ймовірність прийняти правильну інформацію. Сучасні приймачі в цифрових системах зв'язку забезпечують прийом сигналів з відношенням с/ш 9 дБ, тобто рівень сигналу повинен на 9 дБ перевищувати фонові перешкоди, яких в радіоефірі завжди предостатньо [2]. Очевидно, що глушилка додає ще більше штучного шуму до сигналу, після чого він не може бути прийнятий не пристосованим до цього обладнанням.

Двосторонній підсилювач у комплексі зі спрямованою антеною, знімаючи незашумлений сигнал, ретранслює його в контрольовану зону і збільшує співвідношення сигнал / шум на рівень посилення. Цей ефект звужує робочу область глушилки із десятків до одиниць метрів, тобто у зловмисника не вийде блокувати роботу дистанційно і йому доведеться наблизитись ближче або відмовитись від своїх намірів. Тож, забезпечується деякий захист від глушилок.

Іще одним цікавим застосуванням двостороннього підсилювача є збільшення пропускної здатності каналу. Така можливість пов'язана з методом модуляції - фазова маніпуляція QPSK. Завдяки цьому виду модуляції досягається підвищена пропускна здатність каналу в тій же смузі частот. Залежно від рівня сигналу змінюється кількість помилок розпізнавання фази та мобільний пристрій вимушений використовувати більш стійку модуляцію з меншою швидкістю. Та навпаки, при достатньому рівні сигналу, змінює модуляцію на більш швидкісну. Саме завдяки розширеній модуляції збільшено швидкість доступу в мережах LTE-Advanced, в яких використовується QAM-модуляція. Підсилювач забезпечує можливість підвищення швидкості для UMTS, збільшуючи рівень сигналу штучно. Таке застосування пристрою може бути корисним для використання в підземних промислових об'єктах, таких як метро, підвали будинків, тунелі систем телекомунікацій і охоронні відео-сигналізації на віддалених об'єктах.

Завдяки описаним вище особливостям роботи мережі через двосторонній підсилювач, забезпечується стабільний зв'язок для мобільних телефонів і для комерційних пристроїв що працюють на базі сотових мереж, таких як банківські термінали, банкомати, датчики IoT, охоронні сигналізації. Таким чином, виконується одна з задач захисту інформації - забезпечення доступності. Можемо зробити висновок, що двосторонній підсилювач у комплексі зі спрямованою антеною є необхідним засобом при побудові відмовостійких систем інформаційної діяльності.

Список використаних джерел

1. Вымпелком. Обзор системы GSM – 2004. – 125 с.

2. Гепко И.А. - Современные беспроводные сети: состояние и перспективы развития. – К.: Екмо – 2009. – ISBN 978-966-2153-30-9.

УДК 004.42

Гончар О. М., Дрєєва Г. М.
Центральноукраїнський національний технічний університет

Використання спеціалізованих мов програмування для операторів програмованого обладнання

На сьогоднішній день існує величезна кількість мов програмування, які і розрізняються і схожі між собою. Причина такого явища стає зрозуміла, якщо уявити ту кількість і різноманітність завдань, які на сьогоднішній день вирішується за допомогою обчислювальної техніки. Для вирішення різних завдань потрібні різні інструменти, тобто мови програмування.

В процесі експлуатації програмованих пристроїв виникає проблема підготовки кваліфікованого персоналу. Зі збільшенням складності програмованих пристроїв також збільшуються і вимоги до кваліфікації до операторів, що призводить до парадоксу – розвиток технічних можливостей знарядь праці призводить до значного зменшення кількості операторів достатньої кваліфікації, збільшення вартості їх навчання та зменшення кількості тих, хто успішно завершив це навчання. З метою покращення ситуації вартості навчання було винайдено мову програмування G-code за допомогою якої проводять програмування великої кількості автоматичних верстатів та пристроїв. Однак платою за універсальність стала абстрагованість від пристрою виконання, що значно підвищує вимоги до людини-оператору. Для розв’язання зазначених протирічь розглянемо властивості мов програмування.

Виділимо основні властивості мов програмування: читабельність – легкість читання і розуміння програм; легкість створення програм – зручність мови для створення програм в обраній області; надійність – забезпечення мінімуму помилок при роботі програм; можливість перенесення програм – легкість перенесення програм з одного операційного середовища до іншого; універсальність – можливість застосування до широкого кола завдань; чіткість – повнота і точність офіційного опису мови.

Все існуюче різноманіття мов можна умовно класифікувати за різними критеріями. Наприклад, за типом розв'язуваних завдань, наприклад мови системного або прикладного призначення, мови для web-розробки та ін. Тому чимало програмістів намагалися в минулому і намагаються зараз придумати свою мову програмування, яка володіє тими чи іншими перевагами саме з метою пристосування мови для вирішення більш вузького кола задач, або навпаки – збільшити коло задач які можна розв’язати мовою програмування. Хоча переважна більшість програмістів в даний час витрачають величезну кількість часу на вивчення вже існуючого найбільш вдалого арсеналу інструментів. Ситуація постійного виникнення все нових мов програмування свідчить, що дійсно намагання зменшення кількості часу навчання (вивчити одну мову на всі задачі або зменшення часу на вивчення інструменту для вузького кола задач з подальшою економією часу на розв’язання самих цих задач) є актуальною задачею.

Очевидно, для зменшення порогу входження до мови програмування потрібно максимізувати читабельність програмного коду та легкість створення програм. Однак це можливо зробити лише за рахунок універсальності та можливості перенесення, бо надійність, повнота та чіткість мов програмування безумовно вважаються критичними показниками. Це означає, що створена мова програмування повинна максимальна бути звичною до орієнтовного кола операторів програмованого обладнання. Для випадку програмованої мобільної платформи для використання на території України, звичайно буде більш звичним для операторів використання мовних команд на основі української мови зі звичними для людини операторами.

В основній роботі пропонується система команд керування мобільної платформою на базі української мови, яка складається з трьох компонентів: номер команди, оператор, параметр оператора (який може бути й відсутнім). Створена система має можливість зручного програмування на сенсорній панелі завдяки ряду кнопок з назвами всіх можливих команд (рис. 1). При натисненні на кнопку до програми (рис. 2) додається нова команда з обраним параметром. Також команда може замінити існуючу, або вставлена в між вже введеними командами в залежності від режиму вставки.

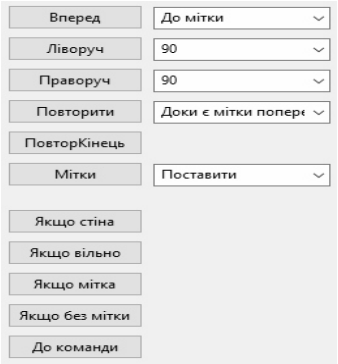


Рисунок 1 – Панель набору команд

№	Команда	Параметр
1	Повторити	Доки не фініш
2	Ліворуч	90
3	Праворуч	До вільного шля
4	Вперед	1
5	ПовторКінець	
6		

Рисунок 2 – Програма «правило лівої руки»

На рис. 2 показано введену програму, яка реалізує алгоритм «правило лівої руки» для пошуку шляху з лабіринту. Згідно цього алгоритму, потрібно повторяти групу команд 2, 3, 4 до тих пір, доки платформа не досягне фінішного положення. Команда 2, 3, 4 відповідають за перевірку наявності шляху ліворуч, та повертанню праворуч до наявного вільного шляху; при наявності тупику це призведе до розвороту.

Розроблена мова програмування в універсальному розумінні не повна, тобто не універсальна, і є повною лише для керування мобільною платформою з детектором наявності перешкод на шляху. Тому ця мова програмування є спеціалізованою і для інших програмованих пристроїв не застосовна. Це зменшує коло застосування мови програмування, але в колі окресленого застосування її зрозумілість переходить до інтуїтивного рівня, що значно зменшує час навчання операторів.

З метою здешевлення процесу навчання операторів було створено віртуальне поле з віртуальною мобільною платформою, яка виконує написаний програмний код. Тому при навчанні операторів мобільних платформ, процес навчання на початкових етапах не потребує наявності робочого пристрою. Також перевагою наявності імітаційної програми є те, що програмний код можна перевірити на віртуальному пристрої. Це запобігатиме аварійним ситуаціям на реальних пристроях, що в свою чергу підвищує критерій надійності використовуваних систем.

Висновок. Створена спеціалізовано мова програмування для керування мобільними платформами з детектором наявності по переду перешкод, яка базується на український мові і має низький поріг входження. В результаті використання розробленої мови є можливість навчати операторів на початкових стадіях без наявного пристрою, на програмній імітації, а також перевіряти створений програмний код.

Список використаних джерел

1. *V.D. Rudenko, "Modern computer literacy and content issues of school informatics", Ukrainskyi pedahohichnyi zhurnal, #3, s.158-169, 2015. (in Ukrainian)*
2. *Shostak, Igor. Problems in Automation of Critical Software Expertise / Igor Shostak, Iuliia Butenko // The First International Workshop Critical Infrastructure Safety and Security «CrISS-DeSSert'11». – 2011. – Vol. № 2. – P. 269–273.*
3. *Липаев, В. В. Программна інженерія. Методологічні основи: Підручник [Текст] В. В. Ліпаєв. – М.: ТЕІС, 2006. – 608 с.*

УДК 004.42

Гринюк С. В., Кирилюк Л. М.
Луцький національний технічний університет

Scratch як об'єктно-орієнтоване середовище візуального програмування

У сучасному світі, інформатика в інтеграції з іншими навчальними предметами є одним із базових для учнів у процесі опанування практичних умінь та навичок роботи з інформаційними технологіями.

Робота за комп'ютером – це завжди творчий процес, який вимагає не тільки вміння діяти за готовими правилами, а потребує самостійності у визначенні плану майбутніх дій, прийнятті рішень, аналізу отриманих результатів [2].

Середовище Scratch створювалося з навчальною та освітньою метою, оскільки у процесі роботи над власними проектами у учнів розвиваються уміння логічно мислити, навички розв'язування творчих задач, навички конструювання та побудови моделей, розвивається творче та системне мислення. Якщо дивитися з практичної сторони, то Scratch – це досить простий у вивченні і потужний інструмент, який, до того ж, не потребує довгого і детального вивчення: учні починають роботу буквального через десять-п'ятнадцять хвилин після знайомства з програмою. У ролі системи програмування Scratch має усі необхідні можливості та атрибути для роботи. У програмі наявний редактор програмного коду, представлений у вигляді цікавого для учнів конструктора Lego, усі елементи мови виглядають як різнокольорові блоки, які з'єднуються між собою та утворюють скрипти [1].

Навчальне середовище «Scratch» — це середовище об'єктно-орієнтованого наочного (візуального) програмування. Воно призначене для створення комп'ютерних анімацій, мультимедійних презентацій, анімаційних та інтерактивних історій, ігор, моделей [2].

Scratch – це вільнопоширюване об'єктно-орієнтоване середовище, у якому можна знайти сучасні елементи середовища візуального програмування типу Delphi [3]. Середовище Scratch (https://scratch.mit.edu) було розроблено Мітчем Рєзником і Аланом Кейему Масачусетському технологічному інституті, США.

З точки зору номенклатури мов, Scratch – об'єктно-орієнтована мова з можливістю створення найрізноманітніших програм, різних за своєю складністю, на думку російських вчених В. О. Дженжер та Л. В. Денисової. Scratch поширюється безкоштовно, не залежить від платформи; легко встановлюється на комп'ютері.

Однією з найважливіших особливостей Scratch є подійно-орієнтований характер, тобто усі об'єкти, наявні у програмі, взаємодіють, обмінюючись повідомленнями. Така схема роботи з об'єктами зближує Scratch з сучасними мовами програмування і дозволяє досить легко перейти до вивчення до вивчення Delphi, C# тощо.

Scratch реалізовано на ідеї багато поточності, що означає, що кожен фрагмент програми запускається окремо у своєму потоці. Саме це відрізняє Scratch від процедурних мов програмування, де прийнято послідовне виконання програмного коду. У Scratch є можливість паралельного виконання скриптів. Scratch можна назвати досить зручним середовищем і для виконання проектів, оскільки тут є бібліотека готових графічних об'єктів, графічний редактор, набір звуків і музичних фрагментів.

Мова програмування Scratch був створений з метою зробити програмування простим і інтуїтивно зрозумілим і дозволити учням, які не мають досвіду програмування, вивчити основні принципи об'єктно-орієнтованого програмування.

Scratch створений як продовження ідей мови Лого і конструктора Лего. Scratch 1 був створений на мові Squeak, Scratch 2 орієнтований на роботу онлайн і переписаний на Flash і ActionScript.

У 2008 році Scratch був портований для мікроконтролерного модуля Arduino. Проект носить назву S4A. Дана мова ілюструє кілька важливих парадигм:

- структурна (в низькорівневому розумінні): всі програми конструюються з обмеженого набору елементів (блоків);

- об'єктно-орієнтована: кожен спрайт насправді є об'єктом зі своїми властивостями (змінними) і поведінкою (скриптами), і різні об'єкти можуть взаємодіяти;

- багатопотокова: об'єкти взаємодіють за допомогою обміну повідомленнями через блоки передати (повідомлення) і, коли я отримаю (повідомлення).

Користуватися Scratch можна повністю безкоштовно як в онлайн-версії (рис.1), так і в офлайн-редакторі.

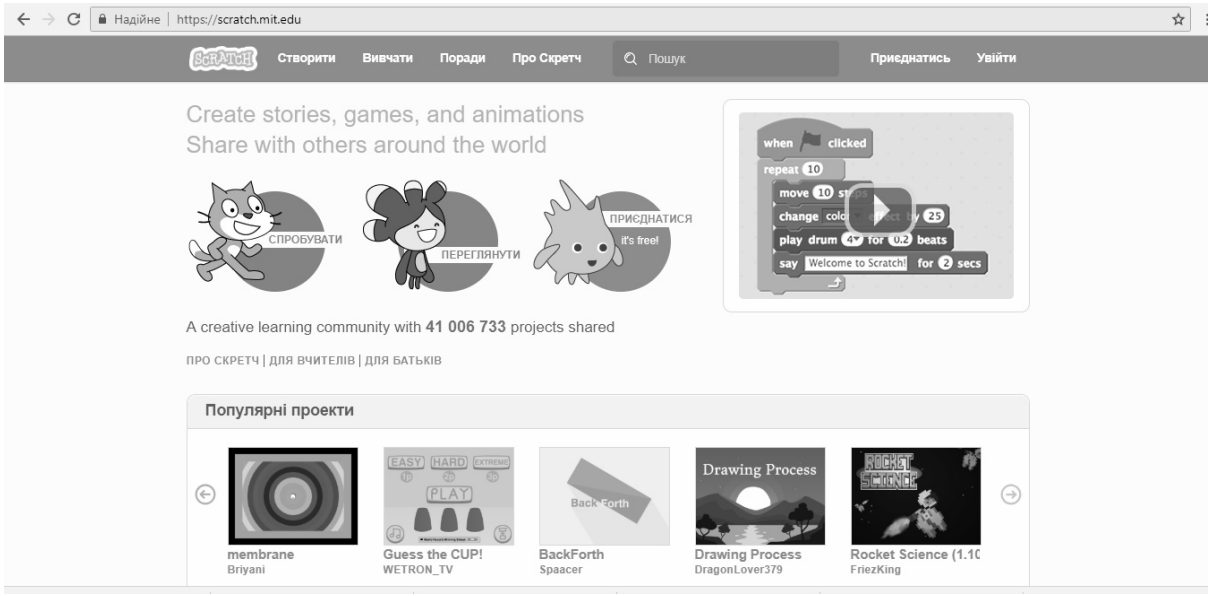


Рисунок 1 – Онлайн-редактор Scratch

Створення програм в Scratch здійснюється шляхом поєднання графічних блоків [1]. При цьому блоки оформлені так, що їх можна з'єднувати тільки в синтаксично вірні конструкції, що виключає помилки. Різні типи даних мають різні форми блоків, підкреслюючи сумісність несумісність об'єктів між собою. Також є можливість внесення змін в програму навіть тоді, коли вона запущена, що дозволяє експериментувати з новими ідеями по ходу рішення задачі. В результаті виконання простих команд створюється складна модель, в якій взаємодіють безліч об'єктів, наділених різними властивостями. Програма Scratch в об'єктно-орієнтованому середовищі «складається» з різнокольорових блоків команд так само, як збираються з різнокольорових цеглинок в конструкторах Лего різні об'єкти (рис.2).

Для створення програми на мові програмування Scratch існують всі необхідні засоби:

- типові для мов процедурного типу: слідування, розгалуження, цикли, змінні, типи даних (цілі і речові числа, рядки, логічні, списки - динамічні масиви), псевдовипадкові числа;

- об'єктно-орієнтовані: об'єкти (їх поля і методи), передача повідомлень і обробка подій;
- інтерактивні: обробка взаємодії об'єктів між собою, з користувачем, а також подій поза комп'ютера (за допомогою підключається сенсорного блоку);
- паралельне виконання: запуск методів об'єктів в паралельних потоках з можливістю координації і синхронізації;
- створення простого інтерфейсу користувача.

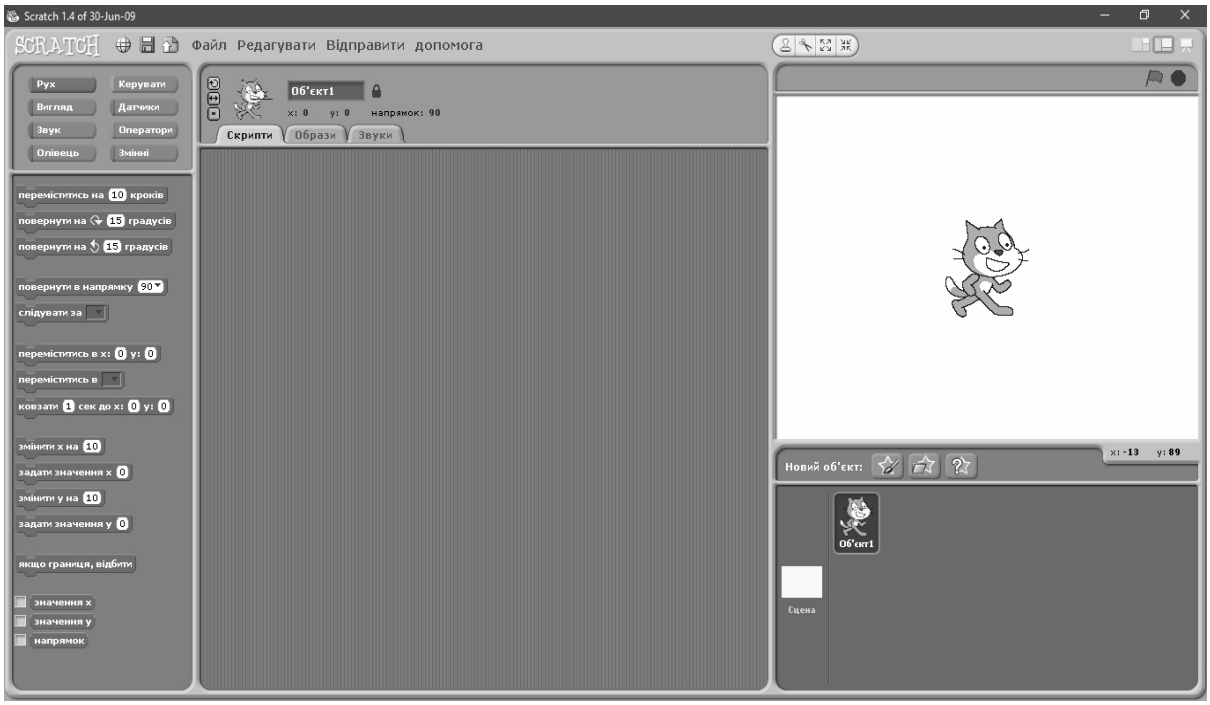


Рисунок 2 – Головне вікно Scratch

Також середовище Scratch здатне допомогти і вчителеві у якості інструмента дослідницької діяльності учнів.

Таким чином, вивчивши мову програмування Scratch, можна зробити висновок, що Scratch має низку позитивних якостей:

- доступність;
- простота, наочність;
- графічна мова (виключені помилки в синтаксисі);
- привабливий для учнів;
- широкі можливості (робота зі звуком, Спрайт, фоном і т.п.);
- дозволяє реалізовувати міжпредметні зв'язки.

Список використаних джерел

1. *Введение в Scratch [Электронный ресурс].- URL: https://younglinux.info/scratch/ - (Дата обращения: 18.04.2018).*
2. *Захар О. Г. Досвід навчання інформатики в початковій школі вчителів Миколаївської області / О. Г. Захар // Комп'ютер у школі та сім'ї : науково-метод. журн. – 2014. – № 3. – С. 22-25.*
3. *Петриченко Т.М. Використання середовища Scratch для підготовки учнів до олімпіади з програмування / Т. М. Петриченко // Комп'ютер у школі та сім'ї : Науковометодичний журнал. – 2013. – № 8. – С. 47-49.*

УДК 004.056.53

Грінченко Є. М., Колмик О. О.
Харківський національний університет внутрішніх справ

Методи управління інформаційними ризиками

У світлі розвитку інформаційних технологій потреба в захисті інформації зростає з кожним днем. Але обробка, передача та захист інформації пов'язані з ризиком, який необхідно враховувати, оцінювати і управляти для успішної роботи організації.

Не дивлячись на значну кількість різних класифікацій загроз у сфері інформаційної безпеки, в вивченій літературі відсутня встановлена класифікація інформаційних ризиків. Вони розглядаються як один з видів операційних ризиків підприємства.

Як правило, всі види інформаційних ризиків взаємопов'язані і впливають на діяльність підприємства. При цьому зміна одного виду ризику може викликати зміну більшості інших.

Класифікація ризиків означає об'єднання сукупності ризиків на підставі певних ознак і критеріїв. Такими критеріями, покладеними в основу класифікації інформаційних ризиків, є:

−основні аспекти інформаційної безпеки;

−час виникнення;

−джерело виникнення;

−природа інформаційного активу;

−характер загрози інформаційної безпеки;

−характер наслідків; механізм впливу.

Основними аспектами інформаційної безпеки є: доступність, цілісність і конфіденційність інформації.

Під доступністю розуміється можливість доступу суб'єкта до даних за запитом в будь-яке передбачене розкладом роботи час. Можливість отримання даних за запитом залежить від працездатності та завантаженості елементів інформаційної системи і її каналів передачі даних.

Ризик порушення доступності інформації може залежати як від несправності обладнання і збоїв в програмному забезпеченні в компанії, так і від успішно реалізованих мережевих атак на інформаційну систему із зовні.

Даний тип ризику безпосередньо залежить від надійності апаратних і програмних компонентів інформаційної системи, а так само від рівня компетенцій персоналу, керуючого їх роботою. Порушення доступності так само виникають через недотримання вимог різних стандартів як на етапі проектування так і на етапах виробництва або експлуатації системи.

Під цілісністю розуміється актуальність і несуперечність інформації, рівень її захисту від руйнування і несанкціонованого зміни і видалення.

Ризик порушення цілісності забезпечується можливостями відмови обладнання і програмного забезпечення, ступенем продуманості алгоритмів і надійністю засобів доступу користувачів системи, які мають право на редагування інформації, ймовірністю наявності в системі недокументованих можливостей, недосконалістю організаційної структури ІС, а так само недодержанням вимог стандартів на етапі проектування, виробництва і експлуатації системи.

Під конфіденційністю розуміється рівень захисту інформації від несанкціонованого доступу.

Ризик порушення конфіденційності так само залежить від рівня алгоритмів аутентифікації користувачів, ймовірністю наявності недокументованих ситуацій при

роботі з ІС, недосконалістю організаційної структури, недотриманням стандартів і людським фактором.

За часом виникнення інформаційні ризики розподіляються на ретроспективні, поточні та перспективні ризики. Аналіз ретроспективних ризиків, їх характеру і методів їх мінімізації дозволяє точніше прогнозувати поточні і перспективні ризики.

За середовищі виникнення ризики діляться на зовнішні і внутрішні.

На зовнішні ризики не впливає внутрішня складова підприємства, вони не пов'язані з прямою діяльністю підприємства і ніяк не може вплинути на їх рівень. Їх рівень обумовлений політичною обстановкою в країні і між державами, економічною ситуацією на ринку, соціальним рівнем громадян і т.д.

До внутрішніх інформаційних ризиків відносяться ризики, які залежать від безпосередньої діяльності підприємства і його персоналу. На їх рівень можуть впливати наступні фактори: виробничий потенціал організації, рівень технічного оснащення, ступінь кваліфікації персоналу, наявність засобів захисту інформації, наявність посадових інструкцій при роботі з ІС.

За природою інформаційного активу інформаційні ризики можна розділити на ризики апаратні і програмні. Апаратні ризики виникають при виході з ладу комплексів ІС, таких як: сервери, персональні комп'ютери, мережеві комутатори і маршрутизатори, виробниче обладнання, верстати і т.д. Програмні ризики безпосередньо пов'язані зі збоями в роботі програмного забезпечення підприємства, дії шкідливого програмного забезпечення, операційних систем користувачів ІС, а так само пов'язані з витоком інформації і дії мережевих атак. Формуючи класифікацію, пов'язану з характером загрози інформаційній безпеці, можна виділити наступні ризики:

Організаційні ризики - це ризики, пов'язані діяльністю персоналу, що експлуатує і обслуговує ІС, проблемами системи внутрішнього контролю, погано розробленими правилами робіт, тобто ризики, пов'язані з внутрішньою організацією роботи компанії.

Технічні ризики пов'язані з обладнанням, програмним забезпеченням, їх завданнями, способами проектування, розробки та експлуатації ІС. Ці ризики безпосередньо пов'язані з життєвим циклом ІС.

До природних інформаційним ризиків відносяться ризики, що не залежать від діяльності людини. Вони здатні завдати шкоди, який можемо привести до повної зупинки функціонування підприємства. Вони пов'язані з діяльністю природних явищ, таких як землетруси, повені, шторми, урагани, і т.д.

Найчастіше ризик характеризується сукупністю трьох якостей: наявністю джерела небезпеки; невизначеністю настання небезпечної події; можливістю заподіяння шкоди. Отже, управляти ризиком - це значить:

– виявляти, вивчати, усувати, нейтралізовувати або зменшувати джерела небезпеки;

– здійснювати систематичний моніторинг і прогнозувати сценарії розвитку небезпечних подій;

– запобігати, локалізувати і усувати негативні наслідки небезпечних подій.

Пропонуються основні методи управління інформаційними ризиками:

– зниження (удосконалення заходів щодо запобігання небезпечних ситуацій, розробка систем їх локалізації);

– прийняття (підготовка фінансових і матеріальних резервів на випадок реалізації небезпечних ситуацій);

– передача (страхування або інші механізми фінансування ризику);

– виключення (перехід на менш небезпечні технології, удосконалення захисних програм, і т. д.).

УДК 004.052 004.032.2
Гура І. О., Александров Р. І.
Київський національний університет будівництва і архітектури

Важливість впровадження та розвитку кіберфізичних систем в Україні

Інтелектуальні пристрої стають все складніше і знаходять все більше можливостей, залишаючись при цьому відносно дешевими. Багато з них використовують доступ до високошвидкісних бездротових мереж, включаючи мережі стандарту 4G. В Інтернеті речей (Internet of Things, IoT) будь-який об'єкт може отримувати інформацію з навколишнього середовища, керувати отриманими даними і надавати їх для інших пристроїв чи користувачам.

Інтернет речей - це динамічне, розподілене середовище, яке пов'язує безліч інтелектуальних пристроїв, здатних сприймати навколишнє середовище і виконувати відповідні дії. Такі пристрої дозволяють відслідковувати стан зовнішнього середовища, збирати інформацію про реальний світ і створювати системи повсюдних обчислень, в яких кожен пристрій може взаємодіяти з будь-яким іншим пристроєм в світі, де б він не знаходився.

Створення кіберфізичних систем підтримують розвиток Інтернету речей. Кіберфізичні системи забезпечують спільну роботу елементів кібернетичного і фізичного просторів, інтегруючи обчислювальні ресурси. Найчастіше кіберфізичні системи підтримують реальні процеси і забезпечують операційний контроль об'єктів в Інтернеті речей, дозволяючи фізичним пристроям сприймати навколишнє середовище і змінювати його.

У кіберфізичних системах обчислювальні елементи взаємодіють з датчиками, які забезпечують моніторинг кіберфізичних показників, і з виконавчими елементами, які вносять зміни в кіберфізичне середовище.

Найчастіше кіберфізичні системи орієнтовані на те, щоб будь-яким чином управляти навколишнім середовищем. Кіберфізичні системи об'єднують інформацію від інтелектуальних датчиків, розподілених у фізичному середовищі, для кращого розуміння середовища і виконання більш точних дій.

Упродовж останніх кількох років спостерігається підвищена активність в сфері створення кіберфізичних систем (КФС). Розвиток та застосування концепції кіберфізичних систем можна порівняти за масштабом та впливом з ефектом від створення мережі Інтернет.

В Україні, як і у всьому світі, спостерігається зростання кількості міського населення, а, отже, уряд, організації та технологічні галузі зайняті вирішенням завдань, що породжуються зростаючим рівнем урбанізації, з метою поліпшення міського життя, наприклад, шляхом підвищення ефективності енергопостачання та якості послуг.

Розглянемо практичні приклади використання кіберфізичних систем, які можуть бути використані або вже використовуються в Україні.

Транспортні засоби та інфраструктура можуть взаємодіяти між собою, обмінюючись в реальному часі інформацією про дорожній рух, місцезнаходженні та проблемах, запобігаючи транспортні інциденти і дорожні пробки, підвищуючи безпеку і в кінцевому підсумку економлячи час і гроші. В Україні моніторинг транспортної інфраструктури здійснюється за допомогою систем відеонагляду TruCam, тим самим підвищуючи безпеку дорожнього руху.

У виробничому середовищі кіберфізичні системи можуть поліпшити виробничі процеси, забезпечуючи обмін інформацією реального часу між промисловим обладнанням, виробничим ланцюжком поставок, постачальниками, системами управління бізнесом і клієнтами. Крім того, кіберфізичні системи можуть підвищувати ефективність цих процесів завдяки автоматичному моніторингу і контролю всього виробничого процесу та адаптації виробництва.

У відновлюваній енергетиці інтелектуальні енергомережі представляють собою кіберфізичні системи, в яких датчики та інші пристрої забезпечують моніторинг мережі для цілей контролю та підвищення енергоефективності.

У сільському господарстві кіберфізичні системи можуть використовуватися для створення більш сучасного та ефективного сільського господарства. Вони можуть збирати важливу інформацію про клімат, грунт та інші дані для більш точного управління сільськогосподарськими роботами. Датчики кіберфізичних систем можуть вести постійний моніторинг різних показників, таких як зрошення грунту, вологість повітря і здоров'я рослин, для підтримання оптимальних навколишніх умов.

В інтелектуальних будівлях спільна робота інтелектуальних пристроїв і кіберфізичних систем дозволяє скоротити енергоспоживання, підвищити безпеку і захищеність, а також створити більш комфортні умови для мешканців. Наприклад, кіберфізичні системи можуть підтримувати моніторинг енергоспоживання та використання систем регулювання для реалізації концепції будинку з нульовим споживанням електроенергії. Крім того, їх можна використовувати для визначення ступеня шкоди для будівель в результаті непередбачених подій і запобігання руйнуванню конструкцій.

В охороні здоров'я кіберфізичні системи використовуються для дистанційного моніторингу фізичних показників пацієнтів в реальному часі з метою зменшення потреб в госпіталізації (наприклад, пацієнтів з хворобою Альцгеймера) або для поліпшення догляду за інвалідами та людьми похилого віку. Крім того, кіберфізичні системи застосовуються в нейробіологічних дослідженнях.

В обчислювальних середовищах кіберфізичні системи дозволяють краще розуміти поведінку систем і користувачів для підвищення продуктивності і більш ефективного управління ресурсами. Наприклад, можна оптимізувати роботу додатків з урахуванням контексту і дій користувачів або відслідковувати доступність ресурсів. Крім того, популярні соціальні мережі і сайти електронної комерції зберігають інформацію про дії користувачів і викликаній контенті, аналізують цю інформацію, щоб передбачати, що може бути цікаво користувачам, і пропонувати рекомендації щодо друзів, публікацій, посилань, сторінок, подій або продуктів.

Широке застосування кіберфізичних систем у різних галузях може підвищити загальну продуктивність та автоматизацію процесів , що відбуваються у сферах діяльності Україні та полегшити життя пересічних українців. Темпи урбанізації та старіння населення мають змусити міські адміністрації переглядати свої організаційні структури та інфраструктури в світлі нових завдань. Такими завданнями є, серед іншого, відповідальне і економне використання ключових ресурсів - електроенергії, води, продуктів харчування і сировинних матеріалів.

Кіберфізичні системи мають величезний потенціал для зміни і вдосконалення кожного аспекту життя людей, допомагаючи вирішувати критично важливі для нашого суспільства проблеми і перевершуючи сучасні розподілені системи в плані безпеки, продуктивності, ефективності, надійності, зручності використання і за багатьма іншими показниками.

Розглянуто напрями розвитку кіберфізичних систем відповідно на наукових досягнень та сучасних концепцій застосування комп'ютерних, інформаційних та телекомунікаційних технологій. Описано загальний принцип роботи кіберфізичних систем та практичні приклади застосування в Україні.

Список використаних джерел

1. *Edward Lee, Cyber Physical Systems: Design Challenges // University of California, Berkeley Technical Report No. UCB/EECS-2008-8б, January 23, 2008.*
2. *Мельник А. О. Спеціалізовані комп'ютерні системи реального часу. – Видавництво Національного університету "Львівська політехніка", Львів, 1998. – 60 с.*
3. *Ambient Intelligence, Werner Weber et al. (Eds.), Springer, 2005. – 388 p. 7. Hakima Chaouchi. The Internet of Things: Connecting Objects, John Wiley & Sons, 2010. – 265 p.*

УДК 004.04:005.31

Дмитрієва О. А., Клімаш О. В.
Донецький національний технічний університет

Алгоритмічні методи кластеризації в рекомендаційних системах з колаборативною фільтрацією

З моменту появи перших робіт по колаборативій фільтрації в середині 1990-х років рекомендаційні системи стали об'єктом пильної наукової уваги [1]. Протягом останнього двадцятиліття була проведена велика робота як теоретичного, так і прикладного характеру, присвячена розвитку рекомендаційних систем [2]. В даний час проблема рекомендаційних систем зберігає до себе великий інтерес, тому що в цій області залишається багато завдань, вирішення яких обіцяє безліч можливостей практичного застосування, що має допомогти користувачам справлятися з величезним обсягом інформації, а також забезпечити їх інструментами вироблення персоніфікованих рекомендацій. В даний час активно розвивається така галузь як електронна комерція, одним з основних завдань якої є збільшення кількості продажів. Для вирішення цього завдання необхідно визначення прихильностей споживача для подальшої рекомендації товарів, які відповідають його інтересам. У зв'язку з цим створюються рекомендаційні системи.

Обрана тематика досліджень є актуальною та має проблеми, які потребують вирішення. Об’єктом даної роботи є процес аналізу переваг користувача для подальшої видачі рекомендацій. Предметом є рекомендаційні методи коллаборативної фільтрації. Метою даної роботи є алгоритмічна модифікація підходу до кластеризації, що базується на методі «ліктя» (elbow method) у колаборативній фільтрації для збільшення точності рекомендацій при найменшій трудомісткості.

Методи колаборативної фільтрації використовують за необхідності обробки великих обсягів інформації. Одним із підходів, що використовуються при цьому є об'єднання в кластери методом k середніх - дуже простий і ефективний алгоритм [3], який має, однак, дві істотні проблеми. По-перше, підсумкові результати чутливі до початкового випадковому вибору центрів груп. Можливе рішення цієї проблеми полягає в багаторазовому виконанні алгоритму з різним випадковим призначенням початкових центроїдів. Ітерація з мінімальним значенням відбирається як кінцевий варіант кластеризації. Друга проблема - необхідність апріорі ставити фіксоване число кластерів для розбиття, яке, безумовно, далеко не завжди обирається оптимальним. Тому одним із завдань кластерного аналізу є підбір оптимального значення k, для якого існує кілька версій розв’язання. Метод «ліктя» розглядає характер зміни розкиду зі збільшенням числа груп k. При об'єднанні всіх n спостережень в одну групу має місце найбільша середньокластерна дисперсія, яка буде знижуватися до 0 при $k \to n$. При дослідженні динаміки збільшення числа кластерів k (рис. 1, а) зниження дисперсії сповільнюється - на графіку це відбувається в точці, яка називається «ліктем» (родич «кам'янистій осипи» при аналізу головних компонент). Необхідність модифікації при реалізації даного методу полягає в тому, що слід підвищити точність кластерізації при незростаючій обчислювальній складності застосування колаборативної фільтрації.

На відміну від завдання класифікації або регресії, в разі кластеризації складніше вибрати критерій, за допомогою якого було б просто представити завдання кластеризації як задачу оптимізації. У разі методу k-середніх [3] широко застосовується такий критерій як сума квадратів відстаней від точок до центроїдів кластерів, до яких вони належать.

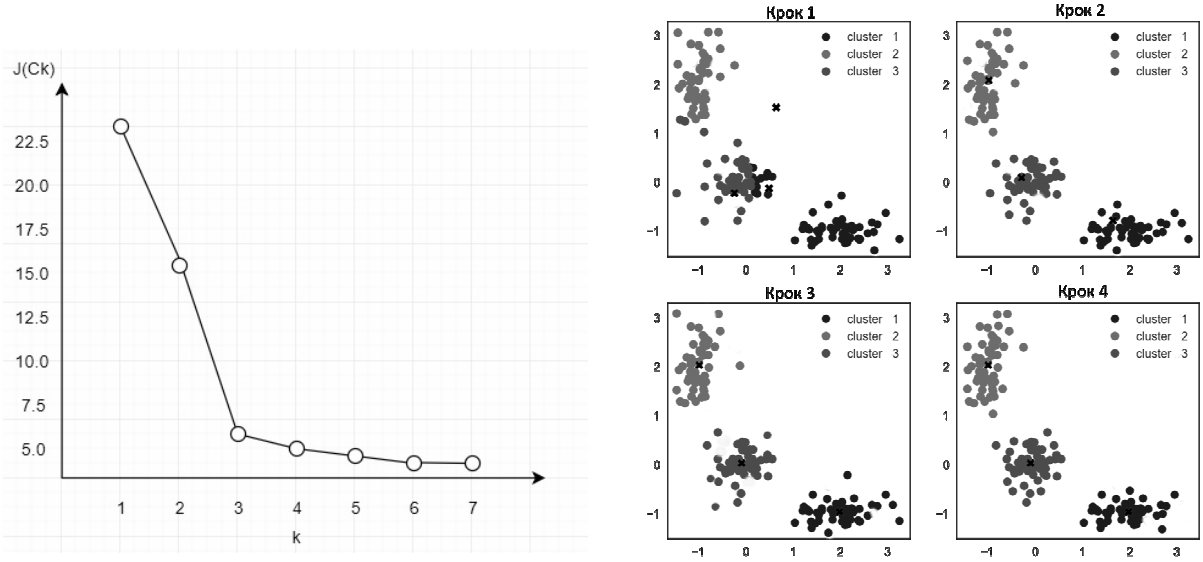
$$J(C)=\sum_{k}^{K}\sum_{i\in C_k}\|x_i-\mu_i\|^2\to\min_{C}$$

де С – множина кластерів потужності К, μ_i – центроїд кластеру C_k .

Для зручності обчислень потрібно, щоб точки розташовувалися разом біля центрів своїх кластерів, проте мінімум такого функціоналу буде досягатися тільки тоді, коли кластерів стільки ж, скільки і точок (тобто кожна точка - це кластер, що складається з одного елемента). Для вирішення цього питання (вибору числа кластерів) було запропоновано методом «ліктя» обирати таке число кластерів, починаючи з якого описаний функціонал J(C) падає не так швидко:

$$D(k)=\frac{|J(C_k)-J(C_{k+1})|}{|J(C_{k-1})-J(C_k)|}\to\min_{k}$$ а

На графіку (рис. 1, а) видно, що $J(C_k)$ стрімко зменшується при збільшенні числа кластерів з 1 до 2 і з 2 до 3 і вже не так сильно - при зміні k з 3 до 4. Значить, в цьому завданні оптимально (рис. 1, б) задати 3 кластера.



а) б)

Рисунок 1 – Знаходження оптимальної кількості кластерів

Висновки: в результаті виконаної роботи був модифікований існуючий алгоритм кластерного аналізу, що базується на методі «ліктя». За допомогою проведеної модифікації, спрямованої на застосування процедури визначення оптимальної кількості кластерів, вдалося суттєво підвищити точність кластеризації і зменшити обчислювальну складність.

Список використаних джерел

1. *Pazzani, M. A framework for collaborative, content-based and demographic filtering/ M. Pazzani // Artificial Intelligence Review. – 2009. – Vol. 13, № 5-6. – P.:393–408.*
2. *Shani G. An MDPbased recommender system / G. Shani, D. Heckerman, R. Brafman // Journal of Machine Learning Research. – 2005. - Vol. 6. -P. 1265–1295.*
3. *Coates A. Learning Feature Representations with K-means/ A. Coates, A. Ng// Neural Networks: Tricks of the Trade – 2012. – P.188-211.*

УДК 004.94

[1]Дмитрієва О. А., [1,2]Гуськова Н. Г.
[1]Донецькій національний технічний університет;
[2]Вища технічна школа університету прикладних наук, м. Бінген, Німеччина

Зведення чисельної реалізації рівнянь в частинних похідних до методу прямих на коллокаціонних блокових різницевих схемах

Одним з ключових питань після зведення рівняння в частинних похідних методом прямих к чисельному розв'язанню задачі Коші (1), як правило, великий розмірності, є вибір методу реалізації, який повинен бути орієнтований на застосування паралельних обчислювальних систем [1]. Крім того, метод розв'язання повинен мати можливість налаштування кроку інтегрування [2], тобто забезпечувати функцію τ-уточнення.

$$u' = \varphi\big(t, u(t)\big), u(t_0) = y_0, t \in [t_0, T]. \quad (1)$$

Для реалізації описаних завдань в роботі пропонується використання коллокаціонних блокових методів з контролем на кроці [3]. Колокаційні схеми для методу прямих в якості вузлів колокації використовують множину точок рівномірної сітки по кожній утвореній прямій $t_{n,i} = t_{n,0} + i\tau \in \left[t_{n,-m+1}, t_{n,s}\right]$, $i = -(m-1), -(m-2), \dots, 0, 1, \dots, s,$ формується канонічний вигляд багатокрокових колокаційних блокових методів з числом опорних точок *m* і числом розрахункових точок *s*.

$$u_{n,i} = u_{n,0} + \tau\left(\sum_{j=-(m-1)}^{0} b_{i,j} F_{n,j} + \sum_{j=1}^{s} a_{i,j} F_{n,j}\right), \quad i = 1,2,\dots,s, \quad (2)$$

де $u_{n,i}$ – наближені розв'язки (1) в точках $t_{n,i}$, $i = 0,1,2,\dots,s$, τ – крок інтегрування, $F_{n,j} = \varphi\big(t_n + j\tau, u_{n,j}\big)$ – праві частини (1), $j = -(m-1), -(m-2), \dots, 0, 1, \dots, s$, $a_{i,j}$ и $b_{i,j}$ – коефіцієнти розрахункової схеми.

Для векторного подання розв'язань введено наступні позначення:

$U_n = \{u_{n,j}\}$, $n = 1,2,\dots, j = -(m-1), \dots, 0,$ – вектор опорних значень,

$U_{n+1} = \{u_{n+1,j}\}$, $n = 1,2,\dots, j = 1,2,\dots,s$ - вектор шуканих точок,

$F_{n,j} = \varphi\big(t_n + j\tau, u_{n,j}\big)$, $n = 1,2,\dots, j = -(m-1), -(m-2), \dots, 0,$

$F_{n+1,j} = \varphi\big(t_n + j\tau, u_{n,j}\big)$, $n = 1,2,\dots j = 0,1,\dots, s$ – відповідно, праві частини рівняння (1) в відомих і шуканих точках,

$U_{n,0} = (u_{n,0})e$– розв'язання в точці $t_{n,0}$,

e – одиничний вектор розмірності *s*.

Тоді в векторній формі система рівнянь (2) буде мати вигляд

$$U_{n+1} = U_{n,0} + \tau(BF_n + AF_{n+1}). \quad (3)$$

Для початку розрахунку вводиться множина опорних значень U_0, які можуть бути визначені однокроковим методом, що забезпечує необхідну точність розрахунків

Пошук чисельного розв'язання може бути зведений до вирішення на кожному кроці нелінійної системи рівнянь (3), з послідовним визначенням векторів $U_1, U_2, \dots$

Необхідно звернути увагу на те, що кожне рівняння в (3) містить $m + s$ невідомих коефіцієнтів

$$b_{i,j}, j = -(m-1), -(m-2), \dots, 0, \quad a_{i,j}, j = 1,2, \dots, s, i = 1,2, \dots, s,$$

які можуть бути визначені з умов апроксимації, або за допомогою інтегро-інтерполяційного методу. В роботі доведено стійкість цих методів за початковими даними і по правій частині, також для них визначено максимальний порядок апроксимації, що становить величину $m+s$. Після визначення невідомих коефіцієнтів і формування матриць A і B з відповідними розмірностями $s \times m$ и $s \times s$ обчислення багатокроковим блоковим методом, представленим у вигляді системи нелінійних рівнянь (3), можна звести до наступного ітераційного процесу

$$U_{n+1}^{(1)} = U_{n,0}e + \tau BF_n, \tag{4}$$

$$U_{n+1}^{(r+1)} = \left(U_{n,0}e + \tau BF_n\right) + \tau AF_{n+1}^{(r)}, n = 1,2, \dots$$

До початку розв'язання системи (4) попередньо визначаються значення вектора U_0 в опорних точках початкового блоку. Обчислення наближених значень в кожному наступному розрахунковому блоці здійснюється ітераційно. Визначення початкових значень в розрахунковому блоці здійснюється на основі багатокрокового предікторного методу, що дозволяє підвищити точність початкового наближення.

В якості тестових рівнянь в роботі використовувалися одновимірні параболічні задачі з різними типами граничних умов і з відомими точними розв’язками для оцінювання глобальної похибки. Дискретизація за просторовою змінною здійснювалася багатокроковим многоточечним коллокаціонним блоковим методом з числом опорних і розрахункових точок в блоці 2×2. Проведені комп'ютерні експерименти умовно поділялися на кілька класів. При тестуванні завдань першого класу основний упор робився на порівняльний аналіз точності отриманих розв’язків методом прямих по відношенню до відомих явних і неявних сіткових методів з порівнянними розмірностями кроків за часом і за простором, процедура управління кроком інтегрування (τ-уточнення) не використовувалася.

У другому класі тестів розглядався вплив варіації кроку по простору на величину глобальної похибки. Показано, що скорочення кроку за просторовою змінною призводить до очікуваного зниження глобальної похибки (практично на порядок). Третій клас експериментів був присвячений розв’язанню жорстких еволюційних задач з можливістю варіації параметра жорсткості. Для цього класу задач показані значні переваги методу прямих.

Висновки. В роботі розглянуті питання побудови просторової дискретизації еволюційних рівнянь методом прямих і чисельної реалізації отриманої системи звичайних диференціальних рівнянь, задачі Коші, із залученням коллокаціонних блокових різницевих схем. При цьому всі переваги розв’язання (паралельне управління кроком, локальний контроль помилок, простота явних методів і стійкість неявних) можуть бути реалізовані і для випадку частинних похідних, тобто метод прямих дозволяє отримати наближення вищого порядку при дискретизації просторових похідних без значного збільшення обчислювальної складності.

Список використаних джерел

1. *Дмитриева О.А. Параллельные численные методы моделирования динамических объектов: монография / О.А. Дмитриева. – Красноармейск: ГВУЗ «ДонНТУ», 2016. – 384 с*
2. *Dmitrieva O. Parallel Step Control. Development of parallel algorithms of the step variation for simulation of stiff dynamic systems / O. Dmitrieva, L. Feldman. – Lambert Academic Publishing. – 2013. – 72p.*
3. *Дмитриева О. А. Моделирование жестких систем на основе коллокационных схем растяжения – сжатия / О.А. Дмитриева, Н.Г. Гуськова // Наукові праці Донецького національного технічного університету. Серія: Інформатика, кібернетика та обчислювальна техніка. - 2017. - № 1 (24). - С. 76-84.*

УДК 004.04:005.31

Дмитрієва О. А. Александров М. О.
Донецькій національний технічний університет

Підвищення ефективності методу контентної фільтрації з урахуванням розрідженності даних

Головне призначення систем рекомендацій полягає в підтримці навігації цільового користувача по складному інформаційному простору [1]. В основі вироблення рекомендацій знаходиться сукупність знань системи про користувача, інших користувачів в системі, і самого інформаційного простору. На відміну від пошукових систем, щоб отримати відповідь, рекомендаційна система не вимагає чіткого запиту [2]. Користувачеві пропонується оцінити деякі об'єкти з колекції і на підставі його оцінок будуються припущення і повертаються ті, що мають найтісніший контакт з ним. Рекомендаційні системи дуже затребувані в даний час, так як значно зменшують час пошуку корисної інформації або товару.

Однією з найбільших проблем в цій галузі є проблема «холодного старту» [2], яка особливо гостро стоїть для нових-інтернет сервісів у яких не вистачає коштів на розробку складної рекомендаційною системи, а для застосування колаборативної фільтрації не вистачає даних. Одним з потенційних рішень може бути застосування контентної фільтрації [3], яка спочатку усуває проблему «холодного старту» для нових товарів, а модифікація методу може дати можливість частково вирішити таку ж проблему для нових користувачів. Також важливою перевагою застосування даного методу є можливість наповнити базу оцінок для дальшого застосування інших видів фільтрації, навіть, не дивлячись на невисоку точність в порівнянні з іншими методами. До того ж підвищити точність і швидкість роботи методу можна модифікувавши його за допомогою алгоритмів зниження розмірності матриці, таких, як SVD (singular value decomposition) та PCA (principal component analysis). Перший розкладає матрицю на добуток трьох меншої розмірності. Другий проектує площину значень на площину меншої розмірності, створюючи при цьому власні вектори.

Метою даної роботи є модифікація методу контентної фільтрації для застосування в рекомендаційних системах за умови великої розрідженості даних, з залученням алгоритмів зниження розмірності декомпозиційних матриць.

Для тестування проведеної модифікації методу була обрана база даних книгарні, яка налічувала 200 тис. користувачів, 30 тис. книг, а також містила 10 тис. оцінок за 10-бальною системою оцінювання. Для тестування було залучено декілька ступенів розрідженості, у кожному з наборів випадковим чином визначалася множина даних для навчання та еталонна множина для порівняння отриманих рекомендацій з наявними результатами. Серед великої кількості критеріїв оцінювання рекомендаційної системи [1], а саме: точність, новизна, можливість дивувати, стійкість до атак, залежність від «холодного старту», переконливість тощо, була обрана точність, яка оцінює близькість передбачення до еталонного результату. Для вимірювання точності був обраний один з найпопулярніших методів - розрахунок середньоквадратичної помилки (RMSE), який дозволяє обчислити помилку передбачення.

В роботі наведено результати тестування з залученням основних методів фільтрації: контентної, контентної із застосуванням PCA, контентної із застосуванням SVD і колаборативної User/ User, в якій для порівняння використовуються користувачі за схожими оцінками. Результати тестування, які відслідковують залежність середньоквадратичної помилки від ступеня розрідженості матриці для кожного типу фільтрації наведено на рис. 1.

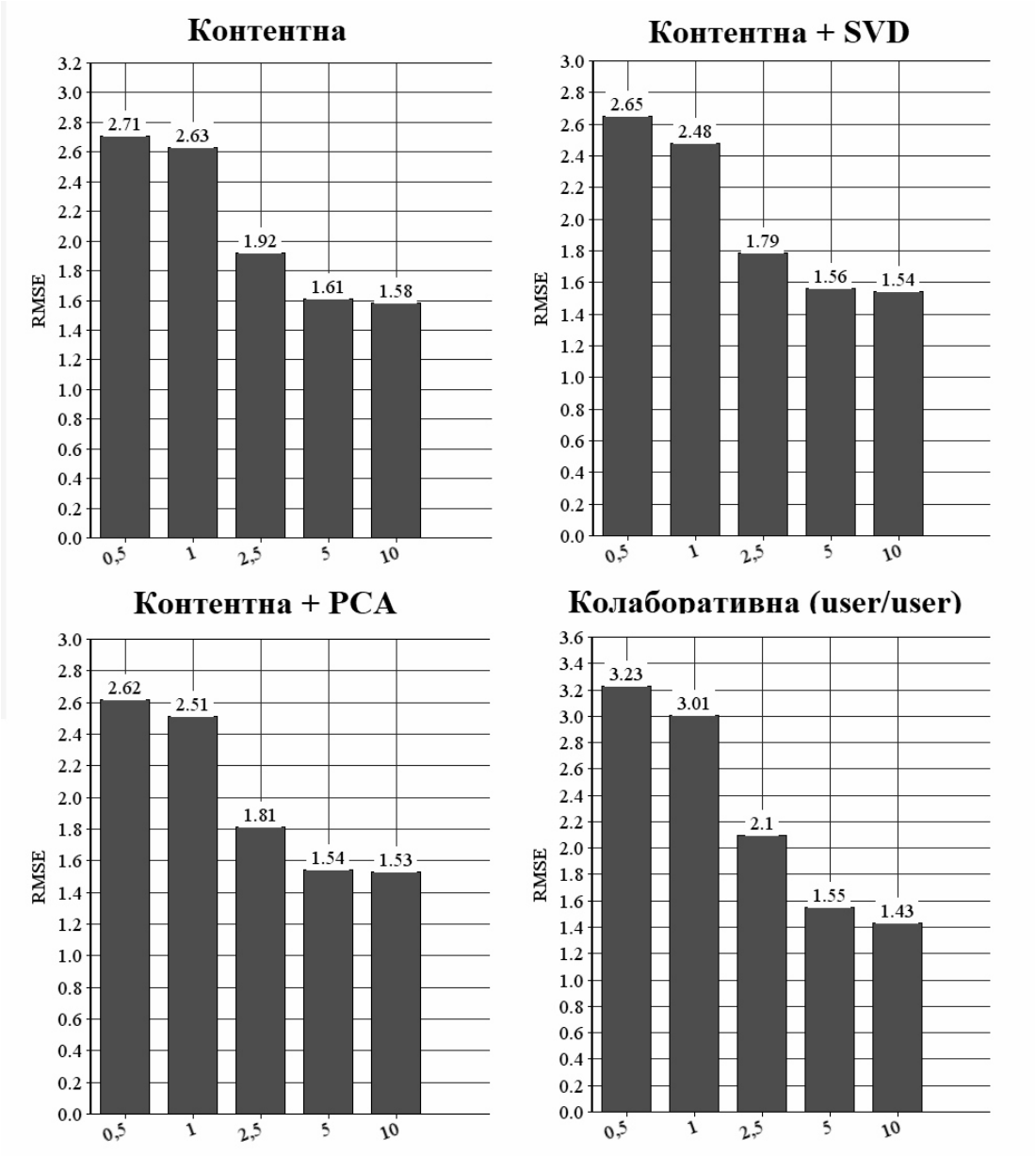


Рисунок 1 – Результати тестування методів фільтрації

За результатами тестування можна стверджувати, що при надзвичайній розрідженості даних контентна фільтрація дає порівняно непогані результати, які значно перевищують показники колаборативної фільтрації і можуть застосовуватися в якості відправної точки на ранньому етапі існування проекту, а при модифікації методу алгоритмами SVD та PCA можна додатково підвищити точність. Надалі подібна система може бути перетворена в гібридну шляхом застосування колаборативної фільтрації і формування довірчих коефіцієнтів, або ж застосування контентного методу до користувачів, кількість оцінок яких менше певного значення.

Список використаних джерел

1. *Mingang C. Performance Evaluation of Recommender Systems/ C. Mingang, L. Pan // International Journal of Performability Engineering. – 2017. - Vol. 13, №8. - P. 1246-1256*
2. *Zhang H. Discrete collaborative filtering / H. Zhang, F. Shen, W. Liu, X. He, H. Luan // 39-nd Conference on Research and Development in Information Retrieval. – 2016. – P. 325–334.*
3. *Melville P., Mooney R., Nagarajan R. Content-Boosted Collaborative Filtering for Improved Recommendations // University of Texas, USA 2002 – 305c.*

УДК 004.382

Желєзняк Б. Ю.[*]
Центральноукраїнський національний технічний університет

Переваги квантових комп'ютерів

Квантовий комп'ютер — це фізичний обчислювальний пристрій, який функціонує шляхом квантової механіки, принципами суперпозиції та явищами квантової заплутаності. Він відрізняється від звичайного транзисторного пристрою тим, що він оперує квантовими кубітами (бітами), які знаходяться у суперпозиції станів, а ось транзисторні пристрої оперуються закодованими даними у логічному виді (0 або 1).

На сьогоднішній день квантові обчислення є реальними, але для суцільної реалізації всіх квантових обчислюваних технологій – треба ще кілька років на дослідження і тільки після цього ми зможемо досягти того, щоб використання всіх доступних ресурсів квантових комп'ютери – було реальними. Сьогодні, ми маємо математичні докази того, що квантові комп'ютери зможуть виконувати операції набагато швидке, ніж будь-який класичний комп'ютер.

Сучасні технології дозволяють розроблення і використання існуючих аналогових квантових комп'ютерів, але вони сильно обмежені кількістю кубітів і коротким часом когерентності. Ці обмеження хоча і є – суттєвими , але вони все ще дозволяють вирішувати деякі практичні задачі. Тому дослідники цього питання дуже зацікавлені в тому, чого вони можуть досягти за допомогою доступних квантових машин. Оскільки «глибина» наявних квантових комп'ютерів є неглибокою ми маємо короткий час когерентності, перш ніж система стає хаотичною і марною для будь-яких розрахунків, ми можемо виконувати лише відносно малу кількість операцій на них.

Недавно командою дослідників була опублікована стаття ("Квантова перевага з мілководдями") про перевагу квантових комп'ютерів над звичайними транзисторними комп'ютерами. У цій роботі дослідники довели, що квантовий комп'ютер з фіксованою глибиною контуру може перевершити класичний комп'ютер, який вирішує ту ж проблему, тому що для класичного комп'ютера буде потрібно збільшити глибину контуру, але вона може залишатися незмінною для квантового комп'ютера . Дослідники вважають, що досягти ефективного використання квантових комп'ютерів можна в найближчі десять років.

Для звичайного користувача квантові комп'ютери стають доступними завдяки компанії D-Wave, які представляють нову , відкриту і безкоштовну платформу Leap Quantum Application Environment, яка дозволяє будь-якому користувачу використовувати потужність квантових комп'ютерів в свою користь. Користувачу не будуть потрібні спеціальні знання в галузі квантової фізики для роботи з такими квантовими комп'ютерами.

Виконавчий директор з досліджень і розробок в D-Wave Алан Барац заявив, що їх система забезпечить доступ до квантових технологій для всіх. Для такої роботи буде потрібно лише мати адресу електронної пошти та базові знання програмування Python і Ocean (open source software suite).

[*] Науковий керівник – Конопліцька-Слободенюк О. К., викладач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету

Система дає кожному користувачеві хвилину машинного часу на квантовому комп'ютері D-Wave 2000Q. З огляду на, те що для обробки самих «важких» програм потрібно від 15 до 250 мс, це дозволить виробляти від 200 до 4000 запусків на місяць. Якщо ж цього не досить , вони пропонують платну підписку.

Компанія позиціонує своє дітище як повноцінний квантовий комп'ютер. Дженніфер Х'юстон, старший віце-президент з маркетингу в D-Wave заявила, що компанія надає не просто доступ до обчислювальних ресурсів. Це також інструменти для навчання, а в майбутньому - основа для формування спільноти.

Послугами Leap вже користуються LANL (Лос-Аламоської національної лабораторії), NASA, Google та інші приватні і державні замовники.

Однак квантовими комп'ютерами в перспективі можуть скористатися і хакери. Тому BlackBerry запустила «квантовостійкий» сервер, який повинен забезпечити безпеку даних навіть якщо для злому використовується квантовий комп'ютер.

«Квантовостійкий» сервер використовує криптографічні бібліотеки, розроблені ISARA Corporation , компанією, що спеціалізується в галузі квантової криптографії і безпеки. Її розробки націлені на майбутнє хакерських атак і, як стверджується, можуть протистояти алгоритмам квантових комп'ютерів.

"Протягом найближчих вісім-десять років експерти оцінюють, що буде великомасштабний квантовий комп'ютер, здатний порушити криптографію відкритого ключа сьогоднішнього дня", - заявив Майк Браун, головний технолог і співзасновник ISARA. "Робота, яку ми робимо з BlackBerry, надасть галузям, що мають міцні підключені пристрої, інструменти, необхідні для захисту своїх систем у майбутньому".

Для захисту від злому створюється особлива цифровий підпис, який відрізняється від класичного методу шифрування з відкритим ключем. Для кінцевих користувачів інструменти формування такого підпису стануть доступні з листопада 2018 року. Цим підписом будуть маркуватися продукти, які відносяться до категорії критично важливих.

На сьогоднішній день квантові комп’ютери вже не здаються фантастикою. Деякі компанії вже сьогодні можуть похизуватися своїми досягненнями в сфері квантових технологій. Дослідники на цю тему з кожним днем досягають все більших і більших перемог і одного дня квантові комп’ютері – ввійдуть в наше життя. Однак, потрібно подолати ще багато перешкод для досягнення бажаних цілей.

Список використаних джерел

1. *Опубліковані доказу переваги квантових комп'ютерів над звичайними* [електронний ресурс]. – Режим доступу: https://tproger.ru/news/quantum-supremacy-over-pc/.
2. *D-Wave представила бесплатную платформу для квантовых вычислений* [електронний ресурс]. – Режим доступу https://tproger.ru/news/dwave-quantum-platform/.
3. *There’s now proof that quantum computers can outperform classical machines* [електронний ресурс]. – Режим доступу: https://techcrunch.com/2018/10/18/theres-now-proof-that-quantum-computers-can-outperform-classical-machines/.
4. *Quantum advantage with shallow circuits* [електронний ресурс]. – Режим доступу : https://arxiv.org/abs/1704.00690.
5. *BlackBerry announces security tools to thwart hacks by quantum computers* [електронний ресурс]. – Режим доступу : https://venturebeat.com/2018/10/04/blackberry-announces-security-tools-to-thwart-hacks-by-quantum-computers/.
6. *BlackBerry запустила сервер із захистом від квантових атак* [електронний ресурс]. – Режим доступу : https://tproger.ru/news/quantum-hack-server/.

УДК 004.021

Железняк Б. Ю.[*]
Центральноукраїнський національний технічний університет

Огляд найбільш використовуваних на практиці алгоритмів

В наш час алгоритми широко використовуються не тільки в програмуванні і в ряді прикладних наук, таких як математика, хімія, генетика та інші, а й навіть у звичайному житті. Наприклад, знаходження найкоротшого шляху від роботи до дому – також можна назвати алгоритмом. Враховуючи величезну кількість застосовуваних в наш час алгоритмів неможливо охопити їх всі, тому розглянемо найцікавіші і найбільш використовувані алгоритми.

Першою групою таких алгоритмів є алгоритми сортування. Хоча вони і не зовсім є повсякденними, але вони використовуються майже в кожному пристрої, яким ми користуємося. Існує безліч таких алгоритмів. Наприклад, сортування вставками, вибором, обміном і т. д. Але «королями» сортування на мою думку є такі : сортування злиттям, швидке сортування і пірамідальне сортування. Всі алгоритми сортування мають свою ціль і можуть використовуватись в різних прикладних задачах. Наприклад, вони можуть бути використаними для сортування пісень в MP3-плеєрі.

Другою групою алгоритмів є алгоритми перетворення Фур'є і швидке перетворення Фур'є. Перетворення Фур'є застосовується для отримання частотного спектру неперіодичної функції, наприклад, електричного сигналу, тобто для представлення сигналу у вигляді суми гармонічних коливань. При цьому використовуються властивості згортки. На практиці, ці алгоритми можна розглядати у процесі використання систем розподіленого обчислення для пошуку можливих сигналів позаземних цивілізацій (проекти SETI і відповідно SETI@Home).

Ще одним цікавим алгоритмом є алгоритм Дейкстри. Саме він дозволяє нам ефективно працювати в мережі Інтернету. Цей алгоритм використовують в задачах, в яких проблему можна представити у вигляді графа, він використовується для пошуку найкоротшого шляху між двома вузлами. Сьогодні алгоритм Дейкстри вже не є універсальним для пошуку найкоротшого шляху, однак цей алгоритм використовується в системах де потрібна стабільність.

Алгоритм RSA – це найважливіший криптографічний алгоритм, який зробив криптографію доступною для всіх у світі. Цей алгоритм став оригінальним рішенням проблеми, яка полягала у створенні можливості ділитися відкритими ключами між незалежними платформами і кінцевими користувачами так, щоб можна було використовувати шифрування (варто відзначити, що насправді ця проблема досі не вирішена повністю).

Алгоритм безпечного хешування – це не зовсім алгоритм, а ціле сімейство криптографічних хеш-функцій. Наприклад SHA-1, SHA-2, і т. д. Вони мають вагоме значення для захисту конфіденційної інформації користувача. Магазини додатків, антивіруси, електронна пошта, браузери і т. д. — всі вони використовують ці алгоритми щоб визначити, завантажили ви те, що хотіли, а також чи не стали ви жертвою атаки «посередника» або жертвою фішингу.

[*] Науковий керівник – Гермак В. С., викладач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету

Алгоритм аналізу зв'язків – за час свого існування розрісся до того, що тепер існують різні способи аналізу посилань з різними характеристиками, що створює унікальність кожного алгоритму, який хоч трохи відрізняється від інших і дозволяє тим самим патентувати алгоритм, хоча при цьому вони все ще залишаються схожими за своєю будовою.

Цей алгоритм широко розповсюджений. Його можна знайти ранжуючи сторінки під час пошуку в Google або при генеруванні стрічки новин в Facebook , або навіть при складанні списку друзів Facebook та багато іншого. Кожен з цих сервісів працює з різними параметрами і об'єктами , але з точки зору математики - кожен алгоритм залишається однаковим.

Пропорційно-інтегрально-диференціюючий алгоритм зустрічається в нашому житті частіше ніж ми можемо собі уявити, а саме кожного разу коли ми користуємося мережею, автомобілем, супутниковою службою, та інше.

В основному алгоритм використовує замкнутий механізм зворотного зв'язку і контуру управління, для мінімізації похибок між бажаним вихідним сигналом і реальним вихідним сигналом. Він використовується скрізь, де потрібна система для обробки сигналу або керування механічними, гідравлічними і тепловими механізмами, які використовують автоматизацію. Можна навіть сказати, що без цього алгоритму наша технологічна цивілізація не існувала би.

Алгоритми стиснення даних. Існує багато алгоритмів стиснення і вирішити який алгоритм є найбільш важливим – дуже складно, оскільки в залежності від отриманого завдання використовувати можна різні алгоритми , наприклад змінювати алгоритм від zip до mp3 і від JPEG до MPEG-2. Але всі ці алгоритми дуже важливі і використовуються майже у всіх сферах людської діяльності.

Крім відомого випадку використання алгоритму для архівації документів, він може бути використаним веб-сторінкою під час її завантаження. Також він може бути використаний у відео, відеоіграх, музиці і навіть у хмарних обчисленнях та базах даних. Алгоритми стиснення даних допомагають робити системи більш рентабельними і ефективними.

Наприкінці хочеться додати, що наведені «Володарі світу» - зустрічаються у нашому житті кожного дня. Але варто пам'ятати, що для кожного завдання – є унікальний підхід і навіть ці володарі, можуть з ними не справитися. Оскільки існують завдання, де інші алгоритми є не менш важливими у сучасному світі і при цьому я їх не згадав.

Список використаних джерел

1. *Подборка алгоритмов, которые правят миром [електронний ресурс]. – Режим доступу: https://tproger.ru/translations/algoritms-rulling-world/*
2. *The 10 Algorithms That Dominate Our World[електронний ресурс]. – Режим доступу: https://io9.gizmodo.com/the-10-algorithms-that-dominate-our-world-1580110464*
3. *Introduction to Algorithms - 3rd [Текст] / Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest and Clifford Stein, 2009. – 1312c .*
4. *Алгоритм Дейкстри [електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Алгоритм_Дейкстри*
5. *RSA [електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/RSA*
6. *PageRank [електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/PageRank*
7. *Пропорційно-інтегрально-диференціальний закон регулювання [електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Пропорційно-інтегрально-диференціальний_закон_регулювання*

УДК 004.056

Железняк Б. Ю.[*]
Центральноукраїнський національний технічний університет

Огляд історії розвитку квантової криптографії

Квантова криптографія – метод захисту інформації, який зосереджений принципах квантової фізики і розглядає випадки, коли інформація переноситься за допомогою об'єктів квантової механіки. Квантова криптографія спирається на принципи невизначеності квантової системи, виражену в принципі Гейзенберга .

Вперше ідея захисту інформації за допомогою квантів була запропонована в 1970 році, що призвело до ідеї передачі особистого ключа за допомогою квантових об'єктів, а в 1983 році було винесено припущення, щодо можливості створення фундаментально захищеного каналу за допомогою квантових станів. Після досліджень була запропонована схема BB84, в якій легальні користувачі обмінюються повідомленнями, представленими у вигляді поляризованих фотонів, по квантовому каналу. Схема BB84 працює досить легко. Щоб правильно виміряти поляризацію фотона (0 °, 45 °, 90 °, 135 °), потрібно знати базис поляризації ("+" або "×"). Якщо використовуваний базис при вимірі відрізняється від базису поляризації, то на виході виходить випадковий результат (0 або 1). Таким чином, зловмисник не може правильно виміряти поляризацію переданих фотонів, не знаючи базис поляризації кожного фотона. Будь-який вплив на квантову систему призводить до зміни її стану.

Перша система яка дозволила двом користувачам обмінюватись секретним ключем з'явилася ще в 1989 році, вона дозволяла обмінювати цей ключ зі швидкістю в 10 біт/с на відстані 30 см, пізніше відбувся експеримент з розповсюдження ключа по оптоволоконному кабелю на відстань до 48 км.

З точки зору технологій квантових комунікацій навколишній світ є досить "галасливим" місцем, заповненим перешкодами і пронизаним електромагнітними сигналами. Як результат, передача сигналу в "гучному" середовищі на відстань в 3 кілометри еквівалентна передачі такого ж сигналу на супутник з базової станції, розташованої в тихому ізольованому місці, підкреслили дослідники.

Компанія Acronis 30 вересня 2015 року заявила про свої плани впровадити технологію квантового розподілу ключа. Ключ шифрування буде передаватися по оптоволоконному каналу за допомогою одиночних фотонів. Якщо будуть спроби перехопити або виміряти певні параметри фізичного об'єкта, що є носієм інформації - це неминуче призведе до спотворення інших параметрів. В результаті, відправник і одержувач виявлять спробу отримання несанкціонованого доступу до інформації. Також планується застосовування квантових генераторів випадкових чисел і шифрування, стійке до квантових алгоритмів.

Компанія Acronis об'єднала свої сили з компанією ID Quantique, щоб разом створити технологію, яка допоможе висловлювати впевненість про те, що квантове шифрування допоможе позбавити замовників від страху відправки даних в хмару.

Компанія Toshiba 23 червня 2015 року заявила про те, що планує розробити незламну систему шифрування, на думку розробників цієї технології, кращий спосіб захистити інформацію в мережі – використовувати одноразові ключі для дешифрування, але основною проблемою – є передача ключа по безпечним каналам.

Ключ в системі буде передаватися в формі фотонів, згенерований лазером, світлові частинки якого будуть доставлятися по спеціальному оптоволоконному кабелю, що не підключений до інтернету. Природа фотонів така, що будь-які спроби перехоплення даних про ключ - змінюють ці дані і це негайно детектується, а оскільки

[*] Науковий керівник – доц. Якименко Н. М., канд. фіз.-мат. наук, доцент кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету

одноразовий ключ повинен мати розмір, ідентичний розміру зашифрованих даних, виключається повторне застосування одного і того ж шаблону, що робить декодування без правильного ключа неможливим.

У липні 2017 року стало відомо про те, що Китай створює захищену комунікаційну мережу, в основі цієї мережі лежатиме принцип квантової криптографії. Проект уже запущений в місті Цзинань. Цей проект допоможе спілкуватися представникам влади та військовим не побоюючись підслуховуючих пристроїв. Ключовою особливістю такої системи є те, що будь-яку атаку, будь-які спроби підслуховувати будуть негайно виявлені. Однак, чим далі, тим потужними стають комп'ютери, і тим більшими повинні ставати ключі шифрування. До того ж на підході квантові комп'ютери, чия обчислювальна потужність буде перебувати на принципово вищому рівні, ніж у сучасної техніки. Традиційна криптографія може виявитися занадто слабкою перед ними. Експериментально було доведено, що квантова криптографія можлива для використання навіть для спілкування. В 2017 році було розроблено квантовий телефон VIPNEt, який демонструє інтеграцію апаратури квантового розподілу ключів.

VIPNEt – розроблений на базі ViPNet Client і ViPNet Connector. Квантовий телефон – дозволяє з'єднувати встановлене програмне забезпечення з робочою станцією та шифрувати трафік між ними з використанням квантових технологій розподілу ключів, що забезпечило високий рівень безпеки при передачі даних по недовіреним каналам зв'язку, що допомогло усунути загрозу обчислення ключів захисту квантових комп'ютерів.

Технологія квантового 4D - кодування вже не є фантастикою, такої думки досягли, коли дослідники успішно провели перші реальні випробування технології квантового 4D - кодування, передавши зашифровані повідомлення між двома станціями, розташованими на дахах висотних будівель, відстань між якими становила 300 метрів. Технологія 4D – кодування є більш захищеним від спроб навмисного втручання і більш стійким до впливу сторонніх чинників навколишнього середовища.

Квантова криптографія ще не вийшла на рівень практичного використання, але наближається до нього. У світі існує кілька організацій, які ведуть активні дослідження в галузі квантової криптографії. Серед них IBM, GAP-Optique, Mitsubishi, Toshiba і інші відомі команди. Діапазон учасників охоплює як найбільші світові інститути, так і невеликі початківці компанії, що дозволяє говорити про початковий період у формуванні ринкового сегмента, коли в ньому на рівних можуть брати участь і ті, і інші.

Зараз одним з найважливіших досягнень в галузі квантової криптографії є те, що вчені змогли показати можливість передачі даних по квантовому каналу зі швидкістю до одиниць Мбіт / с. Це стало можливо завдяки технології поділу каналів Зв'язку по довжинах хвиль і їх одноразового використання в загальному середовищі. Що до речі дозволяє одночасне використання як відкритого, так і закритого каналу зв'язку

Квантова криптографія є важливим кроком до захищеного майбутнього, вже сьогодні існує багато прикладів успішних експериментів і досліджень, але нажаль теоретичні технології випереджаються практичні і ми не можемо спостерігати незламну систему криптографії. Однак дослідними вважаються, що в скорому майбутньому, це зміниться і ми будемо повністю захищеними від кіберзлодіїв.

Список використаних джерел

1. *Understanding Cryptography From Math to Physics [електронний ресурс]. – Режим доступу https://medium.com/datadriveninvestor/understanding-cryptography-from-math-to-physics-54b22a093505*
2. *What Is Quantum Cryptography? [електронний ресурс]. – Режим доступу: https://www.popsci.com/what-is-quantum-cryptography*
3. *What is quantum cryptography? It's no silver bullet, but could improve security ? [електронний ресурс]. – Режим доступу: https://www.csoonline.com/article/3235970/data-protection/what-is-quantumy.html*
4. *Квантовая криптография: что это такое? [електронний ресурс]. – Режим доступу: https://www.popmech.ru/technologies/235655-kvantovaya-kriptografiya-chto-eto-takoe/*
5. *Квантовая криптография [електронний ресурс]. – Режим доступу https://ru.wikipedia.org/wiki/Квантовая_криптография#Первое_устройство_квантовой_криптографии*

УДК 004.7

Жолнер І. Д., Вялкова В. І.
Київський національницй університет імені Тараса Шевченка

Використання теорії живих систем у СКЗІ

Живі системи – це система, що самоорганізується та самовідтворюється, зменшуючи свою внутрішню ентропію за рахунок організації навколишнього середовища. Загальна теорія живих систем оперує сім'ю рівнями живих систем, якими є клітина, орган, організм, група, організація, суспільство, міжнаціональна система. «Жива система» має містити кожну з 20 «критичних підсистем», які визначаються своїми функціями і можуть бути спостережувані в широкому ряді систем, від простих клітин до організмів, країн і співтовариств. У праці «Живі системи» Дж. Міллер представив детальне опрацювання безлічі систем, розташованих по зростанню їх розміру та ідентифікації підсистем в них. Системний підхід є фундаментальним для організаційної теорії, так як в організаціях здійснюються складні динамічні цілеспрямовані процеси. Одним з ранніх мислителів в цій області був Олександр Богданов, який розвинув свою тектологію як теорію, і спрямував її на моделювання та конструювання людських організацій [1].

Вплив на живі системи можуть здійснюватися будь якими зовнішніми чинниками, що будь-яким чином можуть дестабілізувати роботу з будь яких критичних підсистем. Захист системи в такому випадку буде полягати в захисті цих підсистем та обмеженню зовнішнього впливу на них. Використання такої теорії може здійснюватися у багатьох міждисциплінарних сферах, таких як: системна інженерія, програмна інженерія та розробка програмного забезпечення, соціологія. Теорія Живих систем приводить детальний аналіз роботи систем, що започаткувало дисципліни системного аналізу та структурного проектування. Наприклад з 1970-х років загальна теорія систем (ЗТС) є основним фундаментом більшості комерційних методів розробки програмного забезпечення. Також, не без допомоги цієї теорії виникла теорія про нескінченну вкладеність матерії, що доводить те, що космічні системи є самоподібними і самовкладенними системами, що розвиваються за одними і тим ж законами. Сама теорія запроваджує ієрархічну вкладеність систем, у яких однакові критичні підсистеми, і в різних по розміру системах вони виражені іншими елементами, але виконують. Вона також дає можливість масштабування та впровадження її у системи будь-якого розміру та ієрархічної складності. Завдяки цьому, цю теорію можливо використати при побудові систем комплексного захисту інформації, що будуть враховувати не тільки стан захищеності інформації в системі, але й буде захищати усі підсистеми, що впливають на цей стан, включаючи біологічні живі системи, які в свою чергу можуть фігурувати в критичних підсистемах по захисту інформації [2].

Виходячи з вище зазначеного можна стверджувати, що теорія живих систем окрім використання у багатьох міждисциплінарних науках, також може знайти застосування у комплексних засобах захисту інформації. Пропонуючи новий підхід до аналізу систем, що захищаємо, а також підсистем, що до них входять.

Список використаних джерел

1. *Гріер Д. М. Living Systems: наукова робота / Д. М. Міллер. – К : McGRAW-HILL Inc., 1978. - 12 с.*
2. *Elaine Parent The Living Systems Theory of James Grier Miller: наук. посіб. / Parent Elaine. –К: Primer project ISSS, 1996.*

УДК 004.045
Заволодько Г. Е., Павлова Д. Б, Колеснікова Я. С.
Національний технічний університет «Харківський політехнічний інститут»

Інформаційна мережа систем спостереження як основа інформаційного забезпечення користувачів системи контролю повітряного простору

Досвід провідних країн світу свідчить, що в них уже досить тривалий термін існують національні єдині системи контролю використання повітряного простору (ПП). Очевидно, що при цьому досягається максимальна ефективність використання ПП при порівняно низьких матеріальних, технічних і людських витратах. Однією зі складових такої системи є інформаційна мережа (ІМ), на базі існуючих систем спостережень (СС) країни. Мережевої побудови інформаційних засобів приділяється значна увага [1-5]. Зокрема, існуючі національні єдині системи контролю використання ПП, як правило, реалізовані на мережевому використанні окремих СС (програми 968Н, ACCS і ін.). Основними завданнями цих програм є об'єднання в загальну інформаційну систему (ІС) даних існуючих СС різних відомств і централізоване управління цією мережею вищим органом. Об'єднана інформація мережі видається споживачам. Однак такий принцип організації ІС збіднює інформаційне забезпечення споживачів. Дійсно, споживачеві часто потрібна інформація конкретного джерела, а не об'єднана інформація мережі. Крім того, включення окремих СС в єдину ІС на принципі механічного об'єднання тільки інформації не вирішує проблем окремих джерел інформації, зокрема, систем вторинної радіолокації, спільного функціонування систем первинної і вторинної радіолокації і т.д. Це стимулює пошук нових принципів організації єдиної ІС, в якій поєднувалося б повне і надійне інформаційне забезпечення споживачів, а також вирішувалися проблеми функціонування окремих СС.

Природна еволюція СС призводить до об'єднання джерел інформації, розосереджених на певній ділянці контрольованого простору, в мережу. Така еволюція мотивується можливістю злиття великого обсягу даних, одержуваних елементами СС, що працюють незалежно один від одного і володіють певною мірою взаємодоповнюючими можливостями. Завдання полягає в точному відображенні навколишнього оточення і своєчасного виявлення змін в ній.

Серед переваг ІС в порівнянні з одиночними джерелами інформації можна виділити наступні:

- розширення зони бачення;
- збільшення ймовірності виявлення повітряних об'єктів (ПО);
- зниження ймовірності зриву супроводу ПО;
- підвищення точності супроводу ПО;
- виявлення ПО з малою ефективною поверхнею розсіювання;
- підвищення завадостійкості, живучості і скритності.

Перевагами мережевої побудови можна скористатися, лише за умови успішного вирішення цілого ряду технічних проблем, а саме:

- маніпулювання даними при змінної швидкості їх надходження і з нерівною точністю;
- необхідності задавати синхронізацію і організацію даних незалежно від частоти сканування окремих СС.

Головна функція мережі полягає в пересиланні даних, які видаються різними СС споживачеві, який комбінує інформацію для того, щоб забезпечити мережевий супровід ПО. При такій реалізації мережі сукупність СС здійснює виявлення і вимірювання координат ПО з різним темпом видачі даних і різними показниками якості виявлення і

вимірювання координат. По лініях передачі дані пересилаються до споживача, який виконує функції супроводу, прогнозування траєкторії, кореляції, згладжування траєкторій і перетворення координат, одержуваних за даними вимірювань, що видаються до опорної системі координат споживача.

Залежно від ступеня обробки даних, яка використовується мережеві СС можна додатково класифікувати як розподілені або централізовані [5]. Розподілена архітектура характеризується тим, що в кожною СС здійснюється первинна та вторинна обробка даних. Локальні дані спостереження потім видаються споживачам, де в апаратному забезпеченні при обробці дані об'єднуються, з метою встановлення єдиного багатостанційного стеження за кожним ПО. Така структура мережі найбільш доцільна при об'єднанні існуючих СС в єдину ІС.

В ІС з розподіленою або централізованої обробкою інформації дані надходять або споживачеві, або на пункт спільної обробки в різний час і з різних темпом. Саме ці обставини вимагають постачати координатну інформацію з часом її отримання, що дозволяє узгодити процес фільтрації траєкторії. Далі покажемо це.

Припустимо, що є дві СС темп огляду простору, яких різний. У кожній з СС є своя шкала часу, організована, наприклад, за допомогою GPS приймачів, що характеризується тимчасовим процесом, де індексом і позначається номер джерела отримання інформації $(i = 1, 2)$ а j - дискретний час отримання інформації. Будемо вважати, що споживач інформації розташований та де й перший датчик інформації. Припустимо, що по $j = k$ попереднім вимірам в апаратурі споживача отримана результуюча оцінка вектору стану $\vec{W}_k(T_{1k})$ з відповідної матрицею точності $\vec{C}_k$.

При отриманні поточної оцінки вектору стану, наприклад від другого датчика $\hat{\vec{W}}_{y(k+1)}(T_{2(k+1)})$ в момент часу $k+1$ з матрицею точності $\vec{C}_{y(k+1)}$, за даними результуючої оцінки вектору стану і матриці точності на k-му кроці здійснюється обчислення апріорного розподілу на цей крок вимірювань. Цьому розподілу відповідає $\hat{\vec{W}}_{o(k+1)}(T_{1(k+1)})$ і $\vec{C}_{o(k+1)}$, тобто здійснюється прогнозування вектору стану і матриці точності на момент часу отримання поточної оцінки вектору стану. Результуючу оцінку вектору стану і матрицю точності на момент часу $k+1$ можна записати як

$$\hat{\vec{W}}_{k+1}(T_{1(k+1)}) = \hat{\vec{W}}_{o(k+1)}(T_{1(k+1)}) + \vec{C}_{k+1}^{-1}\vec{C}_{y(k+1)} \times$$
$$\left[\hat{\vec{W}}_{y(k+1)}(T_{2(k+1)}) - \hat{\vec{W}}_{o(k+1)}(T_{1(k+1)})\right],$$
$$\vec{C}_{k+1} = \vec{C}_{o(k+1)} + \vec{C}_{y(k+1)}.$$

Надалі процедура повторюється. Таким чином, виходить рекурентне правило, що дозволяє послідовно в часі виробляти фільтрацію траєкторії повітряної цілі при отриманні вимірювань від датчиків інформації з різним темпом видачі інформації.

Як витікає з вищевикладеного, розглянутий алгоритм фільтрації відрізняється від відомих тим, що прогнозування вектору стану і матриці точності здійснюється після отримання нових вимірів, зазначених часом їх отримання. Ось на цей момент часу і здійснюється прогнозування вектору стану і матриці точності.

Вищевикладене дозволяє зробити висновок, що при побудові єдиної ІС необхідно здійснити єдине координатно-часове забезпечення СС, що входять в мережу, з необхідними показниками якості. Залежно від показників якості координатно-часове забезпечення ІС можна класифікувати як мережу, реалізовану на несинхронному і синхронному принципах.

Несинхронний принцип організації мережі вимагає часового забезпечення СС з точністю, що становить частки часу спостереження ПО. Це дозволяє синхронізувати потоки інформації в мережі, забезпечити фільтрацію траєкторії цілі за інформацією з різних джерел та різним темпом видачі інформації.

Синхронний принцип організації мережі, що базується на створенні єдиної шкали часу всіх СС, що входять в мережу, з точністю становить частки мікросекунд. Це дозволяє узгодити процеси отримання і обробки даних від розрізнених СС, а також зумовлює вирішення технічних протиріч, що практично не вирішуються в існуючих СС.

Концептуальними основами створення єдиної ІС на базі існуючих СС, в якій може бути реалізовано надійне інформаційне забезпечення споживачів і дозволені протиріччя окремих СН повинні бути:

- єдине координатно-часове забезпечення всіх СС мережі з необхідними показниками якості;
- розподілена обробка інформації в мережі СС;
- вільний, але контрольований, доступ споживача до необхідної СС.

Єдина інформаційна мережа СС розширює можливості в реалізації різних видів розподіленої обробки даних в порівнянні з існуючим угрупованням інформаційних засобів. Розподілена обробка даних, при цьому, здійснить сумісну оптимізацію якості інформаційного забезпечення етапів обробки даних. Наявність централізованої обробки даних з різноманітних джерел дозволить виконувати процедури етапів обробки в різній послідовності, а це, в свою чергу, підвищить якість інформаційного обслуговування споживачів.

Список використаних джерел

1. *Фарина А., Студер Ф.Цифровая обработка радиолокационной информации. Пер. с англ.–М.: Радио и связь, 1993. – 320 с.*
2. *Farina A., Studer F.A. Radar Data Processing Introduction and Tracking. Vol.1. Research Studies Press. Letch worth England. 1985. – P. 121-123*
3. *Lok J.J. C2 for the air warrior//Jane's International Defense Review. - October 1999. - V.2. - P.53-59.*
4. *Y. Ahmadi, K. Mohamedpour and M. Ahmadi, "Deinterleaving of Interfering Radars Signals in Identification Friend or Foe Systems", in Proc. of 18th Telecommunications forum TELFOR, TELECOMMUNICATIONS SOCIETY - Belgrade, ETF School of EE, University in Belgrade, IEEE Serbia & Montenegro COM CHAPTER, 2010, pp. 729-733.*
5. *Mallick M., Pao L.Y., Chang,K.C., Multiple Hypotheses Tracking Based Distributed Fusion Using Decorrelated Pseudo Measurement Sequence. American Control Conference, Massachusetts, Boston, USA, 2004.*
6. *Теоретичні основи побудови завадозахищених систем інформаційного моніторингу повітряного простору / В.В.Ткачев, Ю.Г.Даник, С.А. Жуков, І.І.Обод, І.О. Романенко. – К.: МОУ, 2004. -271 с*
7. *Обод І.І. Обробка даних систем спостереження повітряного простору: монографія. За заг. ред. І.І. Обод/Обод І.І., Заволодько Г.Е. – Харків: НТУ "ХПІ", 2016. – 281 с*
8. *Обод І.І. Інформаційні технології підвищення інформаційного забезпечення споживачів системами спостереження повітряного простору / І.І. Обод, М.Ю. Охрименко, Г.Е. Заволодько // Тези доповідей XX міжнародної науково-практичної конференції «Інформаційні технології: наука, техніка, технологія, освіта, здоров'я». – Харків.: НТУ «ХПІ», 2012. – Ч.IV. – С. 83.*
9. *Заволодько Г.Е. Інформаційна модель спостереження ПП / Заволодько Г.Е., Обод А. І., Андрусевич В.А. // Тези доповідей XXIV міжнародної НПК "Інформаційні технології: наука, техніка, технологія, освіта, здоров'я". – Харків.: НТУ «ХПІ», 2016. – Ч.IV. – С. 122.*
10. *Заволодько Г.Е, Функціональна архітектура спостереження повітряного простору / Заволодько Г.Е., Довженко В.В., Капустян В.Д. // Міжнародна наукова конференція MicroCAD : Секція №22 - Електромагнітна стійкість - НТУ "ХПИ", 2017.*
11. *Заволодько Г.Е., Синтез та аналіз структури обробки даних в мережі систем спостереження повітряного простору / Заволодько Г.Е., Брагіна Д. А. // Міжнародна наукова конференція MicroCAD : Секція №22 - Електромагнітна стійкість - НТУ "ХПИ", 2018.*

УДК 658:512.011:681.326:519.713
Ізотов Є. О.
Харківський національний університет радіоелектроніки

Аналіз сервісу управління персоналом як частина кіберфізичної системи університету

Кіберфізична система – це механізм, що контролюється або відстежується комп'ютерними алгоритмами і тісно пов'язаний з Інтернетом та його користувачами. В кіберфізичних системах програмне забезпечення тісно пов'язано з фізичними об'єктами. На сьогоднішній день усе більше і більше сфер нашого життя передислокують свою діяльність в кіберпростір. Обговорюються та з'являються різноманітні концепти кіберфізичних систем, що дозволяють відкрити можливості для інновацій і значних удосконалень в соціальних середовищах і бізнес-процесах. Концепти кіберфізичних систем розроблюють або вже успішно застосовують у виробничій середі, в охороні здоров'я, у відновлюваній енергетиці, інтелектуальних будівлях, у транспорті, сільському господарстві та інших сферах.

В свою чергу аналізуючи можливість створення кіберфізичної системи університету можливо виділити наступні складові системи: безпаперовий електронний документообіг; сервіс електронного голосування; сервіс управління персоналом; сервіс управління кафедрою; сервіс тестування знань; сервіс управління наукою; сервіс управління освітою; управління навчанням студентів; сервіс управління захистом; сервіс управління ліцензуванням; сервіс доступу к інфраструктурі; сервіс кібербезпеки. Тож зазначені модулі зможуть надати точний моніторинг і кіберуправління науково освітніми процесами, незалежні системи прийняття рішень щодо управління фінансовими та кадровими ресурсами, виключення паперових носіїв з науково освітнього процесу. Інтелектуальна система управління кадровим складом надасть можливість моніторингу рейтингу викладачів, централізоване та доступне зберігання детальної інформації про досягнення викладачів. Розробка даної системи дозволить перенести управління кадровим складом до сфери оцифрованих відношень, що призведе до зменшення паперового документообігу для проведення рейтингових оцінювань. зменшення витрат людських ресурсів для складання рейтингів, прозорої та доступної інформації щодо досягнень викладачів.

Для зберігання великого обсягу інформації про досягнення викладачів та іх рейтингових показників необхідно створити оптимальну архітектури бази даних. Після аналізу та створення метрики для оцінювання кадрового складу університету необхідно враховувати вигляд інформації, що буде зберігатись. Для показників що можуть нараховувати декілька досягнень, наприклад перелік публікацій, необхідно створити суміжну таблицю для зв'язку кожної занесеної публікації з відповідним автором, що оцінюється. Для показників, що розподіляються на підпункти, найкращім рішенням буде застосувати додатковий стовбець в базі даних для ідентифікації до якого підпункту належить запис.

Створення та застосування сервісу управління персоналом університета призведе до підвищення якості освітніх послуг і наукових досягнень вищої школи за рахунок прозорої та наглядної системи оцінки досягнень. Також система призведе до зменшення паперового документообігу та людських витрат на процеси оцінки науко-педагогічних працівників.

Список використаних джерел

1. *Jongbae, Moon. CFD Cyber Education Service Using Cyberinfrastructure for e-Science [Text] / Moon Jongbae, Kim Chongam, Won Cho Kum // Fourth International Conference Networked Computing and Advanced Information Management, NCM '08. – 2008.– P. 306-313.*
2. *Hahanov, V., Gharibi, W., Kudin, A. P., Hahanov, I., Ngene, C., Tiekura, Y., Krulevska, D., Yerchenko, A., Mishchenko, A., Shcherbin, D., Priymak, A. Cyber Physical Social Systems – Future of Ukraine. Proceedings of IEEE East-West Design & Test Symposium (EWDTS'2014), 2014, Kiev, Ukraine, pp. 67 – 81.*
3. *Савчук Т.О. Організація баз даних і знань [Текст] / Т.О. Савчук. – В. : ВДТУ, 2000. – 63с.*

УДК 658.512

Ісмайлов К. Ю., Балтовський О. А.
Одеський державний університет внутрішніх справ

Концепція побудови динамічної інформаційної системи управління складної соціально-організованою структури

Вступ. На сучасному етапі розробка та впровадження автоматизованих систем управління (АСУ), яка базується на сучасних наукових досягненнях в області обчислювальної техніки, теорії управління, економіко-математичних методів і охоплюють сферу організаційного управління, є одним з головних шляхів підвищення ефективності складних-соціально організованих структур. Практика розробки та впровадження АСУ складними-соціально організованими структурами все більше призводить до висновку про необхідність застосування системного підходу на всіх стадіях дослідницьких і проектних робіт. Це, в першу чергу, відноситься до розробки інформаційної системи (ІС) як ядра АСУ.

Постановка задачі. Процес розробки і конкретної реалізації ІС пов'язаний з проведенням досліджень і вирішенням завдань в наступних напрямках [1]:

1. Вибір найбільш оптимального способу організації інформації в системі.
2. Створення набору алгоритмів і програм, які обслуговують систему незалежно від методу розміщення даних.
3. Опис методу організації інформації на мові, зрозумілою і людині, і машині.

Останнім часом [2, 3] намітився такий підхід вирішення перерахованих вище завдань, при якому ІС являються надбудовою над вже наявної обчислювальної та операційної системами.

Даний підхід пояснюється тим, що існуючі в машинному математичному забезпеченні бібліотеки стандартних програм слабо враховують специфіку інформаційного пошуку і опису даних, які обробляються в конкретній системі управління. При цьому підході можливе вирішення принципових проблем розробки ІС методом виділення інваріантних блоків, реалізація яких дозволяє розглядати структуру ІС як набір однотипних елементів і можливість побудови керованих об'єктів.

Важливою особливістю ІС є забезпечення можливості опису методу організації даних і алгоритмів оперування даними в термінах використовуваної інформаційної мови.

Метою роботи є неперерахування або вибір можливих інваріантних блоків (цей вибір залежить від характеру вирішуваних завдань системою і від властивостей керованих об'єктів), а побудова такої моделі блоків ІС і їх опису мовою, зрозумілою людині і машині, яка дозволяє створити набір алгоритмів і програм, які обслуговують систему, незалежних від вмісту блоків конкретних ІС. З точки зору інформаційної теорії об'єкти управління систем управління щодо спостерігача представляються інформаційним відображенням. Елементарне інформаційне відображення (так звана спостерігається динамічна змінна - НДП) є деяка характеристика певного об'єкта. Отже, ІС є, перш за все, відображення об'єктів.

Рішення задачі. Інформаційні системи АСУ І аналітично можна уявити, як сукупність $I = \left\{ Q(t), U, S\left(\bar{Q}, \bar{U} \right), F(S), \Theta(Q) \right\}$,

де: $Q(t) = \{q_1, q_2, ..., q_m\}$ - безліч спостережуваних динамічних перемінних (СДП) об'єктів управління системи;

$U = \{A, B, ...\}$ - сімейство кінцевих множин імен ознак (властивостей), однозначно визначають спостережувані динамічні змінні (логічний рівень завдання інформації); при цьому кожне ім'я ознаки (властивості) НДП є в свою чергу, безліччю значень інших ознаки (властивості) $A = \{a_1, a_2, ..., a_n\}$, будь-який елемент безлічі A містить | інформацію, яка може бути записана в полі, розміром (завдовжки) l_j одиниць інформації.

$S\left(\bar{Q}, \bar{U}\right)$ - безліч моделей інформаційних структур ІС, які є функцією, яка залежить від двох інших параметрів;

$\bar{Q}$ - потужність безлічі Q СДП об'єктів управління системи;

$\bar{U}$ - потужність безлічі ознак (властивостей) СДП з урахуванням множин, утворених окремою ознакою;

$F(S)$ - алгоритм пошуку, однозначно відображає Q в U;

$\Theta(Q)$ - оператори перетворення моделей інформаційних структур, які визначаються способом їх опису та структур опису даних.

Залежність алгоритму $F(S)$ і складу операторів $\Theta(Q)$ ІС від обраної структури опису даних і методу організації даних в моделях інформаційних структур очевидна. Таким чином, щоб розробити ефективну ІС, необхідно створити метод організації даних в інформаційних структурах на основі єдиної мови опису спостережуваних динамічних змінних. Далі дається визначення моделі інформаційних структур (МІС), що розглядаються як новий підхід до організації та розробці інформаційної системи управління.

Основою, пропонованої МІС являє собою узагальнені поняття мови економічних показників і декомпозиція інформаційного відображення об'єктів управління.

Модель інформаційних структур представлена у вигляді безлічі $\{M\}$ розміром, $m \times n$ де: m - рядки і n - стовпці.

При цьому кожен вектор-стовпець і вектор-рядок МІС визначаються кількістю елементів однорідних ознак (властивостей) СДП, об'єднаній в даній МІС.

Результати розробки інформаційної системи доцільно представляти у вигляді конструкцій форм документів і структур масивів інформації, визначених на основі МІС.

Алгоритм побудови МІС дозволяє вести процес розробки складних інформаційних систем інженерними методами на відміну від існуючих інтуїтивних методів.

Висновки. Результати проведених досліджень показують, що МІС можуть бути прийняті як елементи банків даних, що забезпечують процес нарощування і коригування без зміни алгоритмів їх обробки і пошуку даних в них.

Список використаних джерел

1 Модин А.А. Основы разработки и развития АСУ. - М .: Наука, 1981. - 256 с.

2. Бойко В.В., Савинков В.М. Проектирование баз данных информационных систем. - М .: Финансы и статистика, 1989. - 351 с.

3. Куперштейн В. Современные информационные технологии в делопроизводстве и управлении. - СПб. Издательство "Питер", 2000. - 805 с.

УДК 519.7; 303.732

Казарінова М. В.
Харківський національний університет радіоелектроніки

Дослідження класифікаційних моделей для організації інформації в електронних бібліотечних системах

Термін "електронна бібліотека" в наш час використовується для позначення систем, які є неоднорідними за своїм обсягом і виконують різні функції. Ці системи варіюються від цифрових об'єктів та сховищ метаданих, систем посилань - зв’язку, архівів та систем адміністрування контенту до складних систем, які інтегрують розширені служби цифрової бібліотеки. З цього огляду існують різноманітні класифікаційні моделі для організації інформації в електронних бібліотечних системах. В наш час існує багато тисяч проектів цифрових бібліотек, які застосовують різноманітні підходи, що залежать від потреб різних бібліотек, та галузей, на яких вони базуються. Це призвело до існування різноманітних цифрових бібліотек, але відсутності деякої спільної моделі створення таких систем.

Сучасні дослідження показали, що, незалежно від широкого розмаїття термінів, класифікацій, які використовуються для опису концепції цифрової бібліотеки, існують певні спільні елементи, незалежні від сфери їх використання, з якими клієнти мають бути пов'язані для ефективного задоволення потреб [1-3]. Відповідно до аналізу предметної галузі задоволення потреб кінцевих користувачів цифрових бібліотек є пріоритетним напрямом діяльності, отже аналіз класифікаційних моделей для організації інформації в електронних бібліотечних системах є актуальним.

Для організації інформації в електронних бібліотечних системах була поставлена задача реалізувати:

- підходи та принципи, що регулюють модель цифрових бібліотек;
- сукупність понять та відносин, які колективно фіксують властивість різних сутностей Всесвітньої цифрової бібліотеки;
- створити абстрактну модель для ефективної організації інформації в елеронній цифровій бібліотеці;
- модель має бути розширюваною, тобто реалізувати можливість внесення та додавання інших концепцій представлення інформації за їх потребою.

Отже, в роботі була побудована базова модель цифрової бібліотеки (див. рис.1). Модель охоплює компоненти, які бібліотеки, можливо, побажають включити до своїх цифрових бібліотек, а саме Інтернет та інтранети, інтегрований доступ до інформації, програми для цифрового озвучування, електронні публікації, електронну доставку документів, розподіл ресурсів, спільну діяльність та послуги кінцевого користувача. Модель надалі може вдосконалюватися додаванням компонентів, які є "основними" та "необов'язковими" для розвитку цифрової бібліотеки. Також включені екологічні проблеми, що впливають на цифрові бібліотеки, такі як юридичні, фінансові, клієнтські, кадрові, організаційні, управлінські, технологічні, співпраця та предметні дисципліни, щоб забезпечити загальний погляд на цифрові бібліотеки та їх середовище.

У ході роботи було реалізовано принципи, що регулюють модель цифрових бібліотек, а також сукупність понять та відносин, які колективно фіксують властивість різних сутностей всесвітньої цифрової бібліотеки. Спроектована модель є розширюваною, і, якщо інші концепції потрібні, їх можна буде додати в будь-якому місці за потребою. Як наслідок, отримана модель є достатньою для того, щоб бути використана в безлічі інших сценаріїв. Передбачено "модель", яка необхідна для захоплення цифрового бібліотечного всесвіту і сприяння її впровадженню в якості основи, яка підтримує моделювання на різних рівнях абстракції.

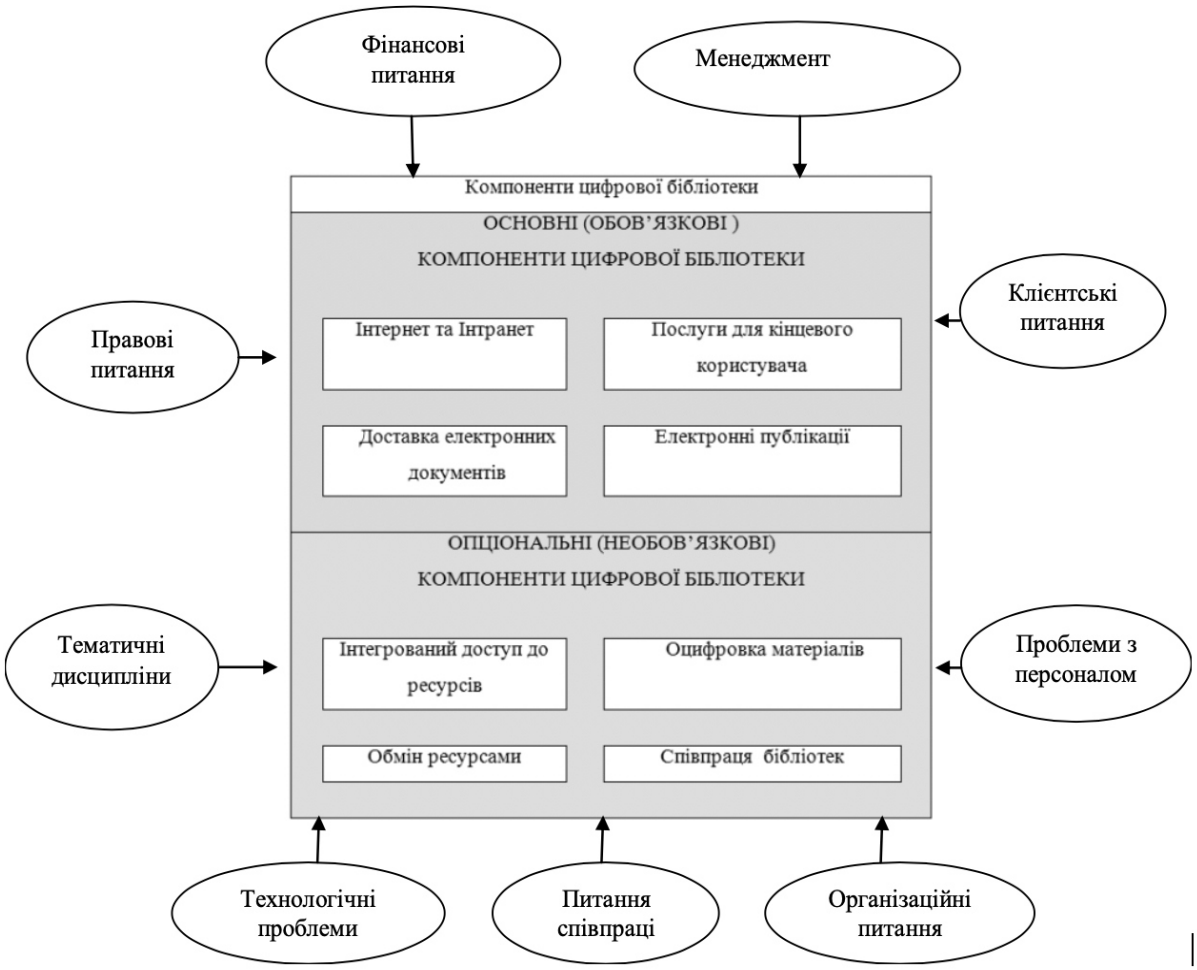


Рисунок 1 – Модель екосистеми цифрової бібліотеки

В архітектурі такої моделі застосовані наступні поняття:

- Reference Model - модель складається з мінімального набору об'єднуючих понять, аксіом та взаємин в рамках конкретного проблемного домену та не залежить від конкретних стандартів, технологій, реалізацій або інших конкретних деталей;

- Reference Architecture - це архітектурна модель, яка вказує абстрактне рішення, яке реалізує концепції та відносини, що виявлені в Reference Model;

- Concrete Architecture. На цьому рівні, Reference Architecture реалізується шляхом заміни механізмів, передбачених в цій архітектурі, з конкретними стандартами та специфікаціями.

Ці три основні поняття є результатом процесу абстракції, який враховує цілі, вимоги, мотивацію та, в цілому, ринок цифрових бібліотек. Коли ці рамки будуть затверджені та реалізовані, отримані системи будуть в основному сумісні один з одним; таким чином, забезпечена сумісність відкриє значні нові горизонти для галузі, щодо представлення ефективних підходів до класифікації інформації кінцевим користувачам.

Список використаних джерел

1. *Bishop, Ann Peterson and Susan Leigh Starr. Social informatics of digital library use and infrastructure// In Annual Review on Information Science and Technology.- №. 31 (Edited by: Williams, Martha E.) Medford, N.J.: Information Today, 2016.- P.301-401.*
2. *Cochrane, Tom and Mike Lean.Copyright, libraries and the electronic future. Australian Library Review.- №12 (4), 2015.-P. 373-380.*
3. *Lesk, Michael. Practical digital libraries: books, bytes, and bucks. San Francisco, Calif.: Morgan Kaufmann, 2007.-355p.*

УДК 004

Коба О. В.
Центральноукраїнський національний технічний університет

Використання системи reCAPTCHA як засобу оцифровки друкованих носіїв

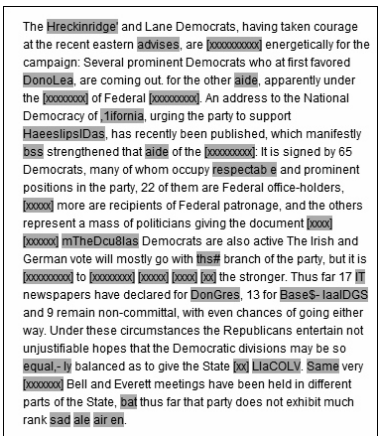
Капча (від CAPTCHA - англ. Completely Automated Public Turing test to tell Computers and Humans Apart - повністю автоматизований публічний тест Тьюринга для розрізнення комп'ютерів і людей) - комп'ютерний тест, який використовується для того, щоб визначити, ким є користувач системи: людиною або комп'ютером. Термін з'явився в 2000 році. Основна ідея тесту: запропонувати користувачу таку задачу, яка з легкістю вирішується людиною, але вкрай складна і трудомістка для комп'ютера [1].

За своєю сутністю, reCAPTCHA, виконує ту ж функцію, яку виконують інші капчі. Суть проста, вводимо запропонований текст і тим самим доводимо, що ми не робот. Головною відмінністю від інших систем є те, що reCAPTCHA не тільки захищає сайт від спамерів, але ще і виконує іншу, досить цікаву функцію.

Метою роботи є опис reCAPTCHA як я засобу для оцифровки старих друкованих носіїв із надійним алгоритмом роботи на відміну від інших способів.

Саме reCAPTCHA пропонує ввести два слова, що практично не зустрічаються у інших капч. Суть в тому, що користувач при введенні цих слів не тільки доводить, що він людина, але ще і допомагає розпізнавати старі книги і газети [2].

Припустимо, є n-на книга, яка збереглася в малій кількості примірників, при цьому всі вони в поганому стані. Один екземпляр у відсканованому вигляді потрапив в руки Google (власник reCAPTCHA). Що з ним робити? Правильно, цифрувати (і справа тут не тільки в збереженні спадщини, але про це пізніше). Як цифрувати? Цифрувати, використовуючи системи розпізнавання символів (OCR). Але, як багатьом відомо, ці системи дуже часто грішать численними помилками в виданому результаті. Вручну перебирати весь текст на предмет помилок - занадто дороге задоволення. І ось, на допомогу приходить reCAPTCHA. Одне слово в зображенні розпізналося системою OCR правильно, а от друге ніяк немає. Друге слово - за користувачем, саме те, що він введе буде використано в якості заміни помилкового варіанту, запропонованого OCR. Напевно зараз деякі посміхнуться, так, я знаю про те, що фактично замість другого слова можна ввести що завгодно. Але кожне незрозуміле для OCR слово reCAPTCHA показує користувачам сотні, а то й тисячі разів (при цифрі в 200 мільйонів генерацій в день це дуже мало), і в кінцевому підсумку правильним вважається той варіант, який користувачі вводили найчастіше. Роботу двох сервісів розглянемо на прикладі від сканованого тексту. Результат роботи OCR зображено на рис.1:



The Hreckinridge' and Lane Democrats, having taken courage at the recent eastern advises, are [xxxxxxxxxx] energetically for the campaign: Several prominent Democrats who at first favored DonoLea, are coming out. for the other aide, apparently under the [xxxxxxxx] of Federal [xxxxxxxxx]. An address to the National Democracy of .1ifornia, urging the party to support HaeeslipsIDas, has recently been published, which manifestly bss strengthened that aide of the [xxxxxxxxx]: It is signed by 65 Democrats, many of whom occupy respectab.e and prominent positions in the party, 22 of them are Federal office-holders, [xxxxx] more are recipients of Federal patronage, and the others represent a mass of politicians giving the document [xxxx] [xxxxxx] mTheDcu8las Democrats are also active The Irish and German vote will mostly go with ths# branch of the party, but it is [xxxxxxxxx] to [xxxxxxxx] [xxxxx] [xxxx] [xx] the stronger. Thus far 17 IT newspapers have declared for DonGres, 13 for BaseS- laaIDGS and 9 remain non-committal, with even chances of going either way. Under these circumstances the Republicans entertain not unjustifiable hopes that the Democratic divisions may be so equal,- ly balanced as to give the State [xx] LlaCOLV. Same very [xxxxxxx] Bell and Everett meetings have been held in different parts of the State, bat thus far that party does not exhibit much rank sad ale air en.

Рисунок 1 – Результат роботи OCR

Червоним виділені помилки. Чи не правда їх занадто багато? А тепер подивимося, що ж буде результатом роботи reCAPTCHA (рис.2):

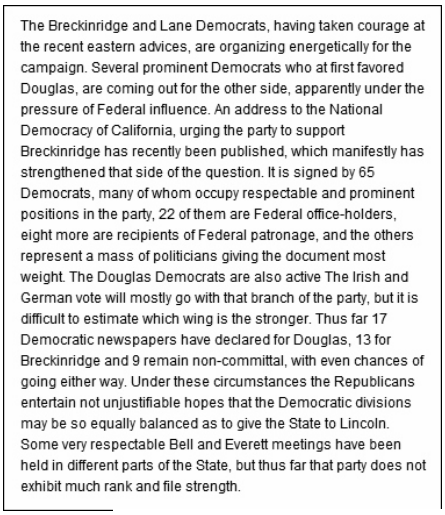

The Breckinridge and Lane Democrats, having taken courage at the recent eastern advices, are organizing energetically for the campaign. Several prominent Democrats who at first favored Douglas, are coming out for the other side, apparently under the pressure of Federal influence. An address to the National Democracy of California, urging the party to support Breckinridge has recently been published, which manifestly has strengthened that side of the question. It is signed by 65 Democrats, many of whom occupy respectable and prominent positions in the party, 22 of them are Federal office-holders, eight more are recipients of Federal patronage, and the others represent a mass of politicians giving the document most weight. The Douglas Democrats are also active The Irish and German vote will mostly go with that branch of the party, but it is difficult to estimate which wing is the stronger. Thus far 17 Democratic newspapers have declared for Douglas, 13 for Breckinridge and 9 remain non-committal, with even chances of going either way. Under these circumstances the Republicans entertain not unjustifiable hopes that the Democratic divisions may be so equally balanced as to give the State to Lincoln. Some very respectable Bell and Everett meetings have been held in different parts of the State, but thus far that party does not exhibit much rank and file strength.

Рисунок 2 - Результат роботи reCAPTCHA

Достатньо помітна різниця між OCR і дуетом OCR + reCAPTCHA. Оцифровка вийшла 100% безпомилковою. Зрозуміло, це щось на зразок ідеальної ситуації, де все складається так, як було задумано творцями reCAPTCHA. Але напевно багато хто з вас зустрічався з абсолютно нечитабельним словами, пропонованими для введення. Проблема в тому, що деякі книги \ газети збереглися настільки погано, що часом і вручну вони розпізнаються огидно. Приклад на рис.3:

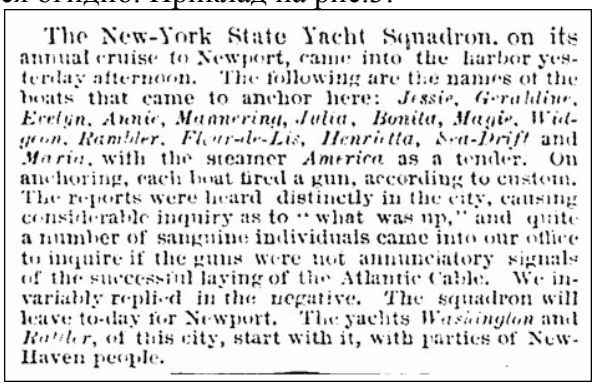

The New-York State Yacht Squadron, on its annual cruise to Newport, came into the harbor yesterday afternoon. The following are the names of the boats that came to anchor here: *Jessie*, *Geraldine*, *Evelyn*, *Annie*, *Mannering*, *Julia*, *Bonita*, *Magic*, *Widgeon*, *Rambler*, *Fleur-de-Lis*, *Henrietta*, *Sea-Drift* and *Maria*, with the steamer *America* as a tender. On anchoring, each boat fired a gun, according to custom. The reports were heard distinctly in the city, causing considerable inquiry as to "what was up," and quite a number of sanguine individuals came into our office to inquire if the guns were not annunciatory signals of the successful laying of the Atlantic Cable. We invariably replied in the negative. The squadron will leave to-day for Newport. The yachts *Washington* and *Rattler*, of this city, start with it, with parties of New-Haven people.

Рисунок 3 – Оцифрований текст

Результат роботи OCR (рис.4) показав, що помилки не підсвічені тому, що все це - одна велика помилка.

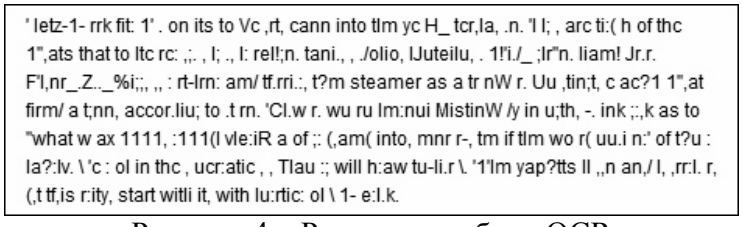

' letz-1- rrk fit: 1' . on its to Vc ,rt, cann into tlm yc H_ tcr,la, .n. 'l l; , arc ti:(h of thc 1",ats that to ltc rc: ,;. , l; ., l: rel!;n. tani., , ./olio, IJuteilu, . 1!'i./_ ;lr"n. liam! Jr.r. F'l,nr_.Z.._%i;;, ,, : rt-lrn: am/ tf.rri.:, t?m steamer as a tr nW r. Uu ,tin;t, c ac?1 1",at firm/ a t;nn, accor.liu; to .t rn. 'Cl.w r. wu ru lm:nui MistinW /y in u;th, -. ink ;:,k as to "what w ax 1111, :111(l vle:iR a of ;: (,am(into, mnr r-, tm if tlm wo r(uu.i n:' of t?u : la?:lv. \ 'c : ol in thc , ucr:atic , , Tlau :; will h:aw tu-li.r \ '1'lm yap?tts ll ,,n an,/ l, ,rr:l. r, (,t tf,is r:ity, start witli it, with lu:rtic: ol \ 1- e:l.k.

Рисунок 4 – Результат роботи OCR

Проте силами reCAPTCHA результат стає цілком читабельним, хоч і не безпомилковим.

Саме таким чином користувачі допомагають оцифровувати книжки засобами reCAPTCHA. На мою думку, це прекрасно.

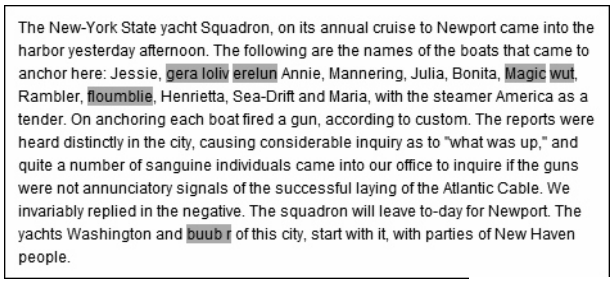

The New-York State yacht Squadron, on its annual cruise to Newport came into the harbor yesterday afternoon. The following are the names of the boats that came to anchor here: Jessie, gera loliv erelun Annie, Mannering, Julia, Bonita, Magic wut, Rambler, floumblie, Henrietta, Sea-Drift and Maria, with the steamer America as a tender. On anchoring each boat fired a gun, according to custom. The reports were heard distinctly in the city, causing considerable inquiry as to "what was up," and quite a number of sanguine individuals came into our office to inquire if the guns were not annunciatory signals of the successful laying of the Atlantic Cable. We invariably replied in the negative. The squadron will leave to-day for Newport. The yachts Washington and buub r of this city, start with it, with parties of New Haven people.

Рисунок 5 – Результат роботи OCR+reCAPTCHA

Виходячи з вищесказаного, зображення, що генерується reCAPTCHA, складається з двох відсканованих слів. Одне вже наперед відомо системі, щодо другого ж є сумніви. Саме це друге слово і є об'єкт для розпізнавання силами користувачів. Грубо кажучи, інтерфейс reCAPTCHA міг би виглядати як на рис. 6:

Рисунок 6 – Інтерфейс reCAPTCHA

Існує помилкова думка, що reCAPTCHA неможливо зламати (мова йде про автоматичне розпізнавання наведеного тексту, без участі людини). Однак, з огляду на тенденції, це не так. З плином часу reCAPTCHA наробила різних підводних каменів для систем розпізнавання. Серед них викривлення тексту, перетин його смугами, так само недавно була введена фіча, завдяки якій перевірочне (відоме системі) слово виглядає здвоєним. Все це вказує на те, що reCAPTCHA все-таки відчуває деякі труднощі із захистом [3].

Та є в reCAPTCHA і мінуси, а саме: є люди, які критикують reCAPTCHA, і з етичної точки зору, критикують вони не дарма. Справа в тому, що за розпізнаний текст Google так чи інакше отримує гроші [4]. А самі тексти видобуваються цілком собі безкоштовно, силами користувачів. Тобто, тут має місце безкоштовна працю. Особисто мене це не хвилює, до того ж, ніхто не змушує користувачів вводити reCAPTCHA, і більш того, ніхто не змушує веб-девелоперів встановлювати її на свої сайти.

Отже, reCAPTCHA – це не просто інструмент для захисту від спаму, а ще й дуже непоганий засіб для оцифрування старих друкованих носіїв із дуже цікавим та надійним алгоритмом роботи.

Список використаних джерел

1. *Система reCAPTCHA. URL: https://www.google.com/recaptcha/intro/v3.html*
2. *Luis von Ahn, Benjamin Maurer, Colin McMillen, David Abraham and Manuel Blum. reCAPTCHA: Human-Based Character Recognition via Web Security Measures. Science. 2008. Vol. 321, № 5895, p. 1465—1468. DOI:10.1126/science.1160379.*
3. *Paul Baecher, Niklas Büscher, Marc Fischlin and Benjamin Milde. Breaking reCAPTCHA: A Holistic Approach via Shape Recognition. Future Challenges in Security and Privacy for Academia and Industry. Springer Boston, 2011. Vol. 354, p. 56-67. DOI:10.1007/978-3-642-21424-0_5.*
4. *Methods and apparatuses for controlling access to computer systemis and for annotating media files: Pub. No.: US 2010/0031330 A1, PCT Filed: Jan. 23, 2008, Pub. Date: Feb. 4, 2010, Appl. No.: 12/524,149. 12 p.*

УДК 004.41:004.056
Коваленко О. В., Коваленко А. С.
Центральноукраїнський національний технічний університет

Аналіз основних підходів математичного моделювання та методологій для забезпечення максимальних показників безпеки програмного забезпечення

Сучасний період розвитку засобів автоматизації та інформатизації суспільства в цілому і окремих організацій та підприємств зокрема можна охарактеризувати як час масового переходу від стихійної комп'ютеризації окремих елементів діяльності організацій до єдиних інтегрованим рішенням, що охоплює всі аспекти їх існування. Це не могло не відобразитися на складі і обсязі ІТ-проектів, які частіше за все виконуються і на методах їх виконання.

Метою роботи **є** дослідження моделей та методів розробки програмного забезпечення для забезпечення максимальних показників безпеки.

У роботах [1, 2] проводилися дослідження і були розроблені комплексні показники якості функціонування комп'ютерних систем критичного застосування. Скористаємося системними підходами. На початку виділимо, що в даний час в теорії системного аналізу виділяють ряд напрямків, серед яких виділимо напрямки якісного і кількісного аналізу різних технічних систем і процесів. При цьому якісний аналіз характеризується простотою і високою швидкістю реалізації, а кількісний аналіз точністю.

Для опису поведінки керованих процесів (в тому числі і процесу розробки ПО) з дискретною безліччю станів і безперервним часом широко використовується теорія марковських процесів. Якщо при цьому закони розподілу тривалості перебування в кожному з станів до відходу в інший можливий стан не є експонентними, то адекватною моделлю поведінки системи є напівмарковський процес [3].

Традиційні технології аналізу напівмарковських систем обмежуються розрахунком фінального розподілу ймовірностей станів системи. Якщо крім фінальних ймовірностей для дослідження системи необхідне знання будь-яких тимчасових характеристик її поведінки (наприклад, закон розподілу тимчасового інтервалу до потрапляння в який-небудь стан системи), то для вирішення відповідних завдань використовується апарат интервально-перехідних ймовірностей. Напівмарковський процес, як відомо, відрізняється від марковского тим, що закон розподілу часу перебування в кожному з станів не є обов'язково експоненціальним, а може бути довільним. Дані фактори доцільно використовувати при кількісній оцінці ризиків розробки ПЗ для розробки оптимізаційної стратегії прийняття рішень.

Одним із сучасних напрямків математичного моделювання є біологічний напрям з допомогою нейронних мереж [4]. Багато в чому це пов'язано зі специфікою функціонування комп'ютерних систем, які є людино-машинними системами. Крім того, останнім часом все більшу увагу розробники та проектувальники стали приділяти питанням захисту даних від програмних загроз. А в цьому випадку результати дослідження систем, проведені за допомогою біологічного підходу, показують найбільш адекватні результати. Однак, проведені дослідження моделей комп'ютерних систем, представлених у вигляді нейронних мереж поряд з їх достоїнствами показали і недоліки пов'язані з істотними (до 100 спостережень) тимчасовими витратами на процес навчання при побудові моделі, і як наслідок, «консерватизмом» по відношенню до динамічних змін в процесі управління розробкою системного ПЗ. Тому дані моделі доцільно використовувати при моделюванні окремих компонентів або структурних елементів інтелектуальних систем прийняття рішень або використовувати в основі процесу вироблення практичних рекомендацій менеджерам.

Однією з поширених технологій математичної формалізації процесів, що протікають в технічних системах є технологія автоматного моделювання. В автоматизованій моделі управління технологія розробки системного ПЗ представляється детермінованим автоматом, на вхід якого надходить послідовність команд користувачів. Основними елементами автоматизованої моделі може бути: безліч станів системи, безліч користувачів, безліч матриць доступів, безліч команд користувачів, що змінюють матрицю доступів, безліч команд користувачів, що змінюють стан, безліч вихідних значень [3]. Перевагою даної технології є можливість відображення різних підходів управління, що визначають не тільки архітектуру системи, але і конфігурацію, порядок взаємодії між об'єктами і суб'єктами процесу розробки ПЗ. Серед недоліків автоматних моделей можна відзначити складність їх практичної реалізації в разі збільшення використовуваних підходів і методологій розробки системного ПЗ. Домінуючим при вирішенні широкого кола завдань аналізу і синтезу систем управління різного призначення тривалий час залишався графокомбінаторний підхід. В цьому випадку процес розробки ПЗ представляється у вигляді функції: $G(N, C)$ або $G(x)$, де N - безліч станів в управлінні, C - безліч зв'язків між станами, x - характеристика якості управління (ефективність, безпеку, вартість і ін.), обрана в якості критерію оптимізації. Тоді приватна задача розробки системного програмного забезпечення може трансформуватися в оптимізаційну задачу виду: $G(x) \to opt$

Рішення мережевих завдань управління в рамках даного підходу грунтувалося на моделюванні процесу у вигляді графа, і було пов'язане з направленим перебором можливих варіантів з метою досягнення деякого оптимуму щодо аналізованого властивості. Одним з можливих методів математичного графового уявлення процесу розробки ПЗ є метод, заснований на GERT-мережах. Даний метод дозволяє моделювати процеси з заздалегідь невідомою функцією розподілу випадкових величин, і успішно випробуваний при математичної формалізації ряду процесів, пов'язаних з проектуванням і тестуванням програмного забезпечення в роботах [5].

Результати, отримані при моделюванні таких процесів показали можливість використання даного підходу з урахуванням можливих негативних ситуацій і наслідків. Зокрема, аналіз GERT-моделей показав доцільність еквівалентних спрощують перетворень складних процесів, розбиття складних етапів на ряд підетапів, використання відомого математичного апарату (наприклад, формули Мейссонье, леми Жордана) і ін.

На рис. 1 представлено порівняльну характеристику найбільш відомих підходів математичної формалізації процесів управління розробкою із зазначенням їх достоїнств і недоліків. Таким чином, в результаті аналізу і порівняльних досліджень існуючих моделей процесу розробки ПЗ були виявлені ряд характерних особливостей, переваг та недоліків існуючих напрямків аналізу і синтезу цих систем.

Проведені дослідження показали, що існує широкий спектр варіантів розробки і використання інформаційних технологій управління розробкою ПЗ. Ці варіанти можуть відрізнятися способами впровадженнями, вартісними і іншими тактико-технічними показниками, характеристиками її окремих елементів і т.д. [2]. Безліч можливих варіантів побудови інформаційної технології розробки ПЗ може бути представлено у вигляді об'єднання підмножин, що забезпечують безпеку на всіх етапах життєвого циклу розробки ПЗ і не забезпечують заданий показник якості відповідно.

Необхідно зазначити, що основою для розробки є методика структурної ідентифікації ризиків розробки ПО, що відрізняється від відомих побудовою оцінки ризиків розробки ПЗ «зверху» у вигляді безлічі, при наявності довільного несуперечливого кінцевого набору «квантів інформації».

Рисунок 1 – Порівняльна характеристика найбільш відомих підходів математичної формалізації процесу управління розробкою системного ПЗ

Проведені порівняльні дослідження основних підходів математичної формалізації розробки ПЗ дозволили сформулювати оптимізаційну задачу синтезу розробки ПЗ для підвищення безпеки даних. Основним завданням синтезу є розробка, вдосконалення та вибір моделей, методів і засобів, що забезпечують максимальні показники безпеки ПЗ.

Список використаних джерел

1. *Яковина В.С., Федасюк Д.В., Мамроха Н.М. Аналіз використання аспектно-орієнтованого програмування як засобу підвищення надійності програмного забезпечення. Інженерія програмного забезпечення. 2010. № 2. С. 24-29*
2. *Wang Y. Software engineering foundations. A software science perspective. Auerbach Publications, 2008.1419 p.*
3. *Praba B., Sujatha R., Srikrishna S. A study on homogeneous fuzzy semi-Markov model. Applied Mathematical Sciences. 2009. №3(50). P. 2453–2467.*
4. *Пильгун В. М. Глубинное обучение нейронных сетей и достижения в их применении. Киев, 2015. 589 с.*
5. *Kovalenko O., Smirnov O., Kovalenko A., Smirnov S., Vialkova V. The mathematical model of the testing technology for Dom Xss vulnerabilities. Scientific & practical cyber security journal (SPCSJ). Georgia. Tbilisi: SCSA 2018. №2(1). p. 22-28 URL: https://journal.scsa.ge/issues/2018/03/997*

УДК 681.5.015

Ковальова К. М.*
Харківський національний університет міського господарства *імені О. М. Бекетова*

Розробка методики діагностування цифрових систем

При сучасному рівні складності обчислювальної техніки знання основ технічного діагностування стає обов'язковим для фахівців у галузі розробки й експлуатації ЕОМ. Застосування методів і засобів технічного діагностування є ефективним способом забезпечення високої надійності виробів, дозволяє скоротити терміни їхнього виготовлення й ремонту.

Складність електронних виробів, що випускаються промисловістю, а також їх кількість зростає так стрімко, що важко уявити розробників засобів, які впоралися б із своїми задачами, маючи на озброєнні лише напівавтоматизовані й інтуїтивні методи виявлення та пошуку виправлення неполадок. При цьому, нерідко, вимоги до процесів діагностування входять в протиріччя з фізичними можливостями сучасної комп'ютерної техніки, яка обмежена як за швидкодією, так і за використанням машинної пам'яті. Вихід із цього положення – удосконалення і розробка нових нестандартних методів розв'язання задач діагностування з подальшою автоматизацією на базі сучасної вимірювальної й обчислювальної техніки. В наш час світові корпорації, які випускають сучасне діагностичне обладнання все частіше знаходять рішення в поєднанні різних стратегій пошуку несправностей. Так функціональне тестування ефективно доповнюється внутрішньосхемним. Сам внутрішньосхемний підхід, в свою чергу, реалізується апаратно декількома системами, які застосовують різні „канали спілкування" з об'єктом, наприклад, у вигляді голчатого контактного пристрою, щупів типу „кліпси", які механічно пересуваються оператором, або „літаючі пробники". Таке компромісне сприйняття проблеми покладено в основу розробки комплексу програм, які вимоги замовника перекладають на взаємодію і раціональне використання можливостей тих чи інших методів діагностування, наприклад, в умовах виробництва і експлуатації цифрових виробів. Стосовно до радіоелектронних виробів як об'єкти розглядаються мікросхеми та інші радіоелектронні компоненти, типові елементи заміни (ТЕЗи, друковані плати, ПЛІС і т. д.), пристрої обчислювальної техніки (комп'ютери, периферійне обладнання, мережеве обладнання), комп'ютерні мережі.

Технічний стан об'єкта – категорія, яка характеризується відповідністю або невідповідністю якості об'єкта певним технічним вимогам, встановленої технічною документацією на даний об'єкт. Під час організації процесів діагностування виникають питання оцінювання якості використовуваних тестів і діагностичних процедур. Найбільш важливими і часто використовуваними оцінками є: повнота контролю, глибина пошуку несправностей, ймовірність контролю. ГОСТ 20911-89 дає такі означення цих критеріїв. Повнота контролю – характеристика, що визначає можливість виявлення відмов (несправностей) в об'єкті за обраним методом його діагностування (контролю). Глибина пошуку місця несправностей – характеристика, що задається вказанням складової частини об'єкта з точністю, до якої визначається місце відмови (несправності). Ймовірність контролю – ступінь об'єктивної відповідності результатів діагностування (контролю) дійсному технічному стану об'єкта.

* Науковий керівник – канд. техн. наук, доцент Дядюн С. В.

УДК 004.056.5

Кузнецов О. О., Агєєва М. М.
Харківський національний університет імені В. Н. Каразіна

Біометрична автентифікація на основі динамічної обробки зображень облич із використанням методу Eigenface

Постановка задачі. На сьогодняшній день біометрична автентифікація використовується у все більшій кількості інформаційних систем, заміщаючи використання парольної автентифікації та забезпечуючи більш високий рівень безпеки. Біометричний захист інформації є більш ефективним, бо за його допомогою можна автентифікувати саме людину, а не пристрій. Метод автентфікації за допомогою розпізнавання обличчя обличчям має широке комерційне та наукове розповсюдження. Цей метод має ряд переваг. По-перше він не потребує спеціальне дороге обладнання, по-друге не потребує фізичного контакту із пристроями.

Існує декілька підходів до рішення задачі розпізнавання обличчя. Алгоритми можуть використовувати статистику, намагатися знайти шаблон, що представляє конкретну людину або використовувати згорткову нейромережу.

Аналіз методу біометричної автентифікації. Eigenface – це метод розпізнавання обличчя на основі статистичного підходу. Метою цього методу є витягування основних компонентів, які найбільше впливають на зміну зображень. Цей підхід є цілісним, процедура прогнозування обличчя основана на цілому наборі навчання. Клас представляє людину. Для підготовки нейромережі потрібні попередньо оброблені зображення у градації сірого. Кожен піксель зображення являє собою одне вимірювання, це означає, що зображення 96x96 пікселів відображається у форматі 96 x 96 = 9216 розмірів. Eigenface базується на аналізі основних компонентів (PCA) для зменшення кількості вимірів при збереженні найважливішої інформації. Тренувальна частина алгоритму Eigenface - це розрахунок ейгенвекторів та відповідних ейгензначень матриці коваріації для тренувального набору[1].

Крок 1 - Перетворення зображень у матрицю. Кожен піксель матриці представляє собою число. Таким чином можна легко представити їх у виді матриці NxN, де кожен елемент матриці є пікселем. Кожне тренувальне зображення стає матрицею I (I_1, I_2, ..., I_m, де I_m дорівнює числу зображень).

Крок 2 - Перетворення матриці I_i у вектор Γ_i. Матриця представляє собою багатовимірний простір. Таким чином, кожний рядок матриці I_i буде конкатинований, а потім перенесений у вектор Γ_i .

Крок 3 - Обчислення середнього векторів Γ_i. Обчислюється сума кожного вектора Γ_i, потім ця сума поділяється на кількість зображень M, що представляє вектор Ψ .

Крок 4 - Віднімання середнього значення від вектора.

Кожне зображення представлене у векторі Γ_i буде віднімати середнє усіх зображення. Результат віднімань представлений у векторі Φ (формула 1).

$$\Phi_i = \Gamma_i - \Psi \quad (1)$$

Крок 5 - Обчислення матриці коваріації C.

Коваріаційне обчислення засноване на Φ_n. Вектори Φ_n сгруповані, щоб представляти матрицю A. Матриця коваріації C обчислюється перемноженням матриці A із транспонованою матрицею A, що називається A^T.

Далі виконується обчислення ейгенвекорів та ейгензначень матриці[2]. Відношення між матрицею A, її ейгенвекторами та її ейгонзначеннями представлене у формулі 2.

$$A\vec{v} = \lambda\vec{v} \text{ або } (A - \lambda I_n)\vec{v} = 0 \quad (2)$$

$\vec{v}$ = ейгенвектор, λ = ейгензначення, I_n = ідентичність матриці A.

Спершу ейгензначення обчислюються, потім ейгензначення повині бути використані для обчислення ейгенвекторів. Щоб обчислити ейгензначення потрібно зробити обчислення за формулою $det(A - \lambda I_2) = 0$.

Крок 6 - Обчислення ейгенвекторів та ейгензначень, що до них відносяться.

Існує дві опції для обчислення ейгенвекторів. Можна обчислити ейгенвектори u_i матриці AA^T або ейгенвекторів V_i матриці A^TA. Ці 2 способи мають однакові ейгензначення та відношення між ейгенвектрами $u_i = Av_i$. AA^T отримує матрицю N^2 x N^2 як результат на відміну A^TA, що дає матрицю MxM. A^TA може мати максимум M ейгензначень та ейгенвекторів на віміну від AA^T, де кількість ейгензначень та ейгенвекторів може досягати N^2. Ейгенвектори u_i повинні бути нормалізовані та нормалізація повинна дорівнювати 1, $\| u_i \| = 1$.

Норма вектора представляє довжину вектора. Для того щоб обчислити норму, слід використовувати теорему Піфагора.

Крок 7 - K ейгенвектори.

M ейгенвекторів відсортвані у зворотньому порядку, заснованому на ейгензначеннях. Зберігаються тільки K ейгенвекторів.. K меньше ніж M та визначено користувачем алгоритму. Усі тренувальні зображення можуть бути представлені комбінацією K ейгенвекторів (формула 3).

$$\Phi_i = \sum_{j=1}^{k} w_j u_j, \ (w_j = u_j^T \Phi_i) \tag{3}$$

K = кількість ейгенвекторів, u_j= ейгенвектори з індексом j, Φ_i= зображення *i*- середнє

Кожен ейгенвектор, який також називається ейгенфейс, являє собою частину кожного зображення в тренувальних даних. Зображення можна розкласти через кожен ейгенфейс. Кожна проекція *w* - це вектор, який обчислюється з зображенням та власним вектором. Існують *k* проекцій, де *k* являє собою кількість відповідних ейгенвекторів[3].

Крок 8 - Розпізнавання обличчя з невідомим зображенням.

Спочатку зображення конвертується у вектор Γ_i та віднімається середнє значення.. Потім зображення проектується у ейгенпростір з $\Phi = \sum_{i=1}^{k} w_i u_i, \ (w_i = u_i^T \Phi)$. Ейгенпростір містить усі ейгенвектори. Після чого, Ф застосовується через Eigenface, щоб отримати проекції (формула 4) .

$$\Omega = \begin{bmatrix} w_1^i \\ w_2^i \\ w^i \\ \dots \\ w_k^i \end{bmatrix} \tag{4}$$

Останнім кроком є знаходження найкоротшої відстані до тестового зображення. Формула 5 представляє порівняння між Ω тестового зображення та Ω_i, де *i* зображення тренувального сету. Клас найближчого зображення прогнозує людину на невідомому зображенні[4].

$$e_r = \min \|\Omega - \Omega_i\| \tag{5}$$

Висновки. Евклідова відстань може бути використана для знаходження найбільш схожого обличчя.. Проте доведено, що дистанція Махаланобіса в більшості випадків є більш точною. e_r можна порівняти з порогом, і якщо e_r менше, ми можемо визначити, що обличчя належить людині, яка не належить до тренувального набору, тому зображення додають до навчального набору як нову людину. В іншому випадку це зображення буде використано як нове зображення для тренування розпізнаного обличчя, а також додане до навчального сету з відповідною міткою. Цей алгоритм представляє постійне машинне навчання і має стати більш надійним щоразу, коли виконується новий тест, оскільки розмір навчального набору постійно зростає.

Описаний метод є легким у виконанні програмної реалізації для навчання класифікатора, може обробляти великі бази даних за невеликий час та зменшує статистичну складність у представленні особи. Але метод Eigenface має досить багато недоліків, зокрема високу чутливість до різного освітлення та маштабу, важко фіксує зміни у виразах обличчя.

Список використаних джерел

1. *Bay H., Ess A., Tuytelaars T., Van Gool L. SURF: Speeded Up Robust Features / Computer Vision and Image Understanding. – Oxford: Elsevier, 2008. – V. 110. – № 3. – P. 346–359.*
2. *Turk, M., Pentland, A. (1991) Face Recognition Using Eigenfaces / The Media Laboratory Massachusetts Institute of Technology, P. 3 - 5.*
3. *Turk, M., Pentland, A. (1991) Eigenfaces for Face Detection / Recognition. Journal of Cognitive Neuroscience, 3(1), P.1–11.*
4. *Belhumeur, P. N., Hespanha, J. P., & Kriegman, D. J. (1997) Eigenfaces vs . Fisherfaces : Recognition Using Class Specific Linear Projection, 19(7), P. 711–720.*

УДК 004.056.5

Кузнецов О. О., Власенко О. В.
Харківський національний університет імені В. Н. Каразіна

Біометрична автентифікація на основі відбитків пальців

Аналіз літератури та постановка задачі дослідження. Для біометричної автентифікації людини за відбитками пальців існує безліч алгоритмів. Відбитки пальців є майже універсальною біометричною ознакою, і ця технологія успішно використовується в різних додатках протягом більше століття. Його популярність також можна пояснити простотою придбання та численними джерелами збирання (десять пальців). Він може бути легко інтегрований у існуючі програми з дуже низькою кривою навчання. Користувачі можуть легко навчитися використовувати ці системи, оскільки це є інтуїтивно зрозумілим і не потребує спеціальної підготовки.

Відбитки пальців класифікуються в різні категорії на основі інформації, яка витягується з глобальних хребтів. Процес розпізнавання, який витягує відбиток пальця з великого набору даних, відповідає заданому відбитку пальців, і процес класифікації присвоює відбиток пальця до попередньо визначеного класу. Ручна класифікація займає багато часу, ніж система автоматичного виявлення. Тим не менш, це складна область класифікації відбитків пальців відповідає її заздалегідь визначеним класам. Хороша система класифікації повинна бути дуже ефективною, надійною, і вона повинна бути вибірковою з точки зору різних класів, що не перекриваються, з однаковими властивостями. [1]

Відбиток пальців класифікується у різні класи. Ці класи розглядають інформацію з різних рівнів для класифікації відбитків пальців. Ці рівні: глобальний рівень, локальний рівня та дрібний рівень. Глобальний рівень –це рівень класифікації знайти особливі точки для класифікації відбитків пальців. Особливі точки також відомі як основна точка і Дельта-точка. Основні і Дельта-точки індивідуально недостатні для точного процесу зіставлення. Місцевий рівень-на місцевому рівні відбитки пальців в основному поділяються на три категорії: петлі, дуги та завитки. Ці три категорії додатково поділяються на підкатегорії: ліва петля, права петля, верхня петля, нижня петля, шатрова арка, проста арка.[2]

Метод класифікації відбитків пальців є ефективним та симетричним підходом для розробки моделей класифікації з даного набору даних. Приклади систем класифікації є: на основі правил, на базі мультиклассифікатора, на базі нейронних мереж, на основі структури, на основі статистики. Для системи класифікації розроблені різні алгоритми. Для системи класифікації зазвичай використовуються лінійний потік, оцінка орієнтації, алгоритми виявлення особливих точок. Кілька підходів для класифікації відбитків пальців. Найбільш часто використовувані підходи поділяються на наступні категорії.

- На основі правил - підхід, заснований на правилах, заснований на кількості особливих точок в зображенні. Цей підхід використовується для прийняття рішень вручну. В принципі, проста арка не має особливих точок. Шатрова арка, ліва петля, права петля складаються з одного ядра і однієї дельти. Мутовка складається з двох дельт і двох основних точок.
- Структурна основа - цей підхід в основному заснований на вимірюванні орієнтації відбитка пальця. Методи оцінки поля орієнтації використовуються для розрахунку орієнтації заданого вхідного зображення.
- Статистична основа – в цьому підході для класифікації використовується загальний класифікатор. Кожному вектору ознак, який виходить із заданого зображення, зіставляється із загальним класифікатором.
- Нейронна мережа – нейромережевий підхід, заснований на використанні багатошарових перцептронів для класифікації відбитків пальців.
- Багатошаровий класифікатор - для класифікації використовуються різні класифікатори, такі як K-класифікатор найближчого сусіда.[3]

Порівняльний аналіз і результати експериментальних досліджень. Багатоканальний підхід до класифікації відбитків пальців. Більша частина інформації про категорії відбитків пальців міститься в центральній частині відбитка пальців.

Метод, заснований на моделях, які використовують як основні, так і дельта-точки для класифікації, вимагають наявності цих особливих точок на зображенні. Знімки відбитків пальців, отримані оптичними сканерами, не завжди фіксують весь відбиток пальців, і часто відсутня точка дельти. Нові твердотільні пристрої для захоплення відбитків пальців невеликі за розміром, тому вони захоплюють лише частину відбитків пальців (наприклад, твердотільний сенсор FPS100 від Veridicom - приблизно розмір поштової марки). Також ядро або дельта-точка важко виявляти в шумних відбитках зображень. Проте, достатньо інформації, доступної в самому хребті, для класифікації відбитків пальців. Незважаючи на те, що підхід, оснований на структурі, не залежить від основних чи дельта-точок, він потребує надійної оцінки поля орієнтації, що знову дуже важко отримати у знімках з низькою якістю відбитків пальців. Ми пропонуємо алгоритм класифікації відбитків пальців на основі нової схеми представлення, яка безпосередньо походить від місцевих структур хребта. Представлення явно не використовує поле ядра, дельти та орієнтації. Він більше здатний терпіти погану якість зображення, що є основною складністю класифікації відбитків пальців. Основними етапами нашого класифікаційного алгоритму

- Знайдіть точку реєстрації на вхідному зображенні і визначте просторову тесселяцію області навколо точки реєстрації (секторів).
- Розкладіть вхідне зображення на набір компонентних зображень, кожне з яких зберігає певні структури хребта; обчисліть стандартне відхилення компонентних зображень в кожному секторі для генерації вектора ознак.
- Подати вектор ознак в класифікатор; в нашому алгоритмі використовується двоступінчастий класифікатор

Цей двоетапний класифікатор використовує класифікатор K-найближчого сусіда на першому етапі і набір нейромережевих класифікаторів на другому етапі для класифікації вектора ознак в один з п'яти класів відбитків пальців. Категорія відбитка визначається його глобальними гребеневими і борозеневими структурами. Допустимий набір ознак для класифікації відбитків пальців повинен бути здатний ефективно фіксувати цю глобальну інформацію. Для цілей класифікації ми використовуємо низькорівневе подання, яке дуже ефективно для подання глобальних структур хребта і борозни і яке інваріантно до окремих найдрібніших деталей. Основні кроки нашого алгоритму вилучення ознак наступні: знайдіть точку реєстрації (центральну точку) і визначте просторову тесселяцію простору зображення навколо точки реєстрації (представленої набором секторів); розкласти вхідне зображення на набір компонентних зображень, які зберігають глобальні структури хребта і борозни; обчислити стандартне відхилення значень рівня сірого в кожному секторі для формування вектора ознак.

Переваги та недоліки

Висновки. Автоматична класифікація відбитків пальців є складною проблемою через малу міжкласової мінливість і велику внутрішньокласової мінливість серед п'яти розглянутих класів. Ймовірність того, що відбитки пальців у двох людей співпадуть - один до 220 мільйонів. Тобто $1/220000000 = 4{,}54 * 10^{-9}$. FAR – 0,01%, FRR – 10%, швидкість обробки - $2{,}5 * 10^{-4}$, с, попит на ринку – 39%. [4]

До переваг даного методу можна віднести: висока достовірність, низька вартість обладнання, достатньо проста процедура сканування відбитка. Недоліки: папілярний узор відбитка пальця дуже легко можно пошкодити дрібними подряпинами, порізами, недостатня захищеність від підробки, викликана широким поширенням методу, залежність від чистоти пальця, для сухої шкіри якість розпізнавання нижче.

Список використаних джерел

1. *Гуреева О. Биометрическая идентификация по отпечаткам пальцев. Технология FingerChip / Ольга Гуреева. // Компоненты и технологии. – 2007. – №4. – С. 176–180.FingerChip / Ольга Гуреева. // Компоненты и технологии. – 2007. – №4. – С. 176–180.*
2. *Anil K. Jain A Multichannel Approach to Fingerprint Classification / Fellow, IEEE, Salil Prabhakar, Student Member, IEEE, and Lin Hong / IEEE transactions on pattern analysis and machine intelligence – april 1999 – vol. 21 – no. 4.*
3. *L. Hong and A.K. Jain, "Classification of Fingerprint Images," Technical Report SUCPS:TR98-18, Michigan State Univ., June 1998.*
4. *Горбенко Ю. И. Модели и методы оценки защищенности механизмов многофакторной аутентификации / Ю. И. Горбенко, И. В. Олешко // Восточноевропейский журнал передовых технологий: научный журнал. – 2012. – №6/2(66). – С. 4 – 10.*

УДК 004.32

Кузьменко Д. С., Луценко В. В., Тарасенко Ю. С.
Університет митної справи та фінансів

Питання підвищення рівня захищеності в інформаційно-телекомунікаційних системах

В 21 сторіччі, де електронно-цифрові прилади стали невідємною частинною нашого життя, дуже гостро ставиться питання інформаційної безпеки в частині нівелювання наслідків різного, як внутрішніх так і зовнішніх, роду атак. Як відомо, такі атаки (наприклад, так звані «атаки по стороннім каналам зв'язку»), спрямовані на ураження цифрових пристроїв. Атака по стороннім каналах використовує інформацію в виді фізичних процеси в пристрої, які не розглядаються в теоретичному описі. Подібного роду атаки мають фізичний вплив на електронно-цифрові пристрої і мережі, що зв'язують їх. Атака по електромагнітному випромінюванню може бути віднесена як пасивна атака, де електронні шифрувальні пристрої випромінюють електромагнітне випромінювання під час своєї роботи. Пов'язуючи певні спектральні компоненти цього випромінювання з операціями виконуваними в пристрої, можна отримати достатньо інформації для визначення секретного ключа або самої оброблюваної інформації. Крім того, не варто забувати про Електромагнітні перешкоди - небажане фізичне явище або вплив електричних, магнітних або електромагнітних полів, електричних струмів або напруг зовнішнього або внутрішнього джерела, яке порушує нормальну роботу технічних засобів, або викликає погіршення технічних характеристик і параметрів цих коштів [1].

Для запобігання подібного роду атак, можливе використання класичного екранування як корпусу самого електронно-цифрового пристрою, в нашому випадку це персональний комп'ютер ПК чи сервер. Це (екранування) суттєво зменшить вірогідність ризику стосовно шкідливого впливу атак, тобто екранування є ефективним способом боротьбі з побічними електромагнітними випромінюванні і наводками (ПЕВН).

Прийнято розрізняти способи екранування на електростатичне, магнитостатичне, електромагнітне. Електростатичне екранування по суті зводиться до замикання електростатичного поля на поверхню металевого екрана і відведення електричних зарядів на землю (на корпус приладу) [2]. Заземлення електростатичного екрана є необхідним елементом при реалізації електростатичного екранування. Застосування металевих екранів дозволяє повністю усунути вплив електростатичного поля. При використанні діелектричних екранів, що щільно прилягають до екрануємого елементу, можна послабити поле джерела наведення в ε раз, де ε - відносна діелектрична проникність матеріалу екрану. Основним ефектом екранування електричних полів є зниження ємності зв'язку між екрануємими елементами конструкції. Отже, ефективність екранування визначається в основному ставленням ємностей зв'язку між джерелом і ураженою зоною наведення до і після установки заземленого екрану. Тому будь-які дії, що призводять до зниження ємності зв'язку, збільшують ефективність екранування. Особливо важливо не мати з'єднувальних проводів між частинами екрана і корпусом. У діапазонах метрових і коротших довжин хвиль сполучні провідники довжиною в кілька сантиметрів можуть різко погіршити ефективність екранування. На ще більш коротких хвилях дециметрового і сантиметрового діапазонів сполучні провідники і шини між екранами неприпустимі. Для отримання високої ефективності екранування електричного поля тут необхідно застосовувати безпосереднє суцільне з'єднання окремих частин екрану один з одним [3].

Магнитостатичне екранування використовується при необхідності позбавлення від наведення на низьких частотах від 0 до 3-10 кГц, при цьому ця ефективність підвищується при застосуванні багатошарових екранів [3].

Екранування високочастотного магнітного поля засноване на використанні магнітної індукції, що створює в екрані змінні індукційні вихрові струми (струми Фуко). Магнітне поле цих струмів всередині екрану буде направлено назустріч збудливій полю, а за його межами - в ту ж сторону, що і збудливу поле. Результуюче поле виявляється ослабленим усередині екрану і посиленим поза ним. Вихрові струми в екрані розподіляються нерівномірно по його перетину (товщині). Це викликається явищем поверхневого ефекту, суть якого полягає в тому, що змінне магнітне поле слабшає в міру проникнення в глиб металу, так як внутрішні шари екрануються вихровими струмами, циркулюючими в поверхневих шарах. Завдяки поверхневому ефекту щільність вихрових струмів і напруженість змінного магнітного поля в міру поглиблення в метал падає по

експонентному закону. Чим нижче частота, тим слабкіше діє екран, тим більшої товщини доводиться його робити для досягнення одного і того ж екрануючого ефекту. Для високих частот, починаючи з діапазону середніх хвиль, екран з будь-якого металу товщиною 0,5 - 1,5 мм діє досить ефективно. Для частот вище 10 МГц мідна і тим більше срібна плівка товщиною понад 0,1 мм дає значний екранує ефект. Тому на частотах вище 10 МГц цілком допустимо застосування екранів з фольгованого гетинаксу або іншого ізоляційного матеріалу з нанесеним на нього мідним або срібним покриттям [4].

Електромагнітне екранування засноване на тому, що високочастотне електромагнітне поле послаблюється їм же створеним (завдяки утворюється в товщі екрану вихровим струмам) полем зворотного напрямку [2-4]. Очевидно, що екрануванню підлягають і монтажні дроти і сполучні лінії поряд блоків апаратури. Алгоритм зменшення рівня ПЕВН цілком аналогічне заходам, викладеними в [3].

Однак, заходи по використанню екранування самого електронно цифрового пристрою (ПК чи сервера, а також самого приміщення, де вони розташовані) можуть бути недостатніми з точки зору необхідного рівня захисту. В цьому випадку можуть бути використана технологія безехових камер (БЕК).

Замість звичного корпусу, ми розмішуймо всі комп'ютерні комплектуючи в так званий «модернізований корпус», розроблений по принципам безехових камер. Також можливо оснащувати серверні приміщення такими камерами, для запобігання шкідливого впливу і витоку інформації.

Найпростішою радіочастотної камерою є звичайна екранована камера, виконана за принципом клітки Фарадея. Вона являє собою якесь замкнуте обсяг з модульних конструкцій, (в попередні роки камери були зварними), який дозволяє захищати секретну інформацію щодо радіочастотного каналу. Основним призначенням таких конструкцій є фільтрація і виключення неналежних перешкод по мережі живлення. Радіосигнал не може піти з екранованої камери і потрапити всередину неї. Екрановані камери можуть бути використані для захисту життя і здоров'я персоналу від шкідливого впливу потужних електромагнітних полів, наприклад, на космодромах або при випробуваннях з високим рівнем напруженості поля. Такі камери також захищають від руйнівного електромагнітного впливу і електронні пристрої різних систем управління. Подібні технології можна використовувати, як для захисту електронно-цифрових приладів від зовнішніх атак, так і для захисту від внутрішнього і зовнішнього прослуховування. В якості прикладу, запропоновано використовувати рупор-образну БЕК стінки якої, є основним джерелом паразитних відбитів покрита радіопоглинаючим матеріалом РПМ (наприклад типу В2-Ф3 коефіцієнтом відбиття по потужності Кп = 0,05 (-13 дБ)) з підставою в виді фольгованого склопластику, забезпечує, крім того екранування. В цьому випадку [5]. При λ =4,3см КБЕ камери склав -47дБ, а при λ =3см відповідно -50дБ. В інших точках робочого діапазону КБЕ був не гірше -35 дБ. Таким чином безехова камера забезпечує певне середовище, в якій можна бути впевненим що інформація не буде перехвачено.

Полубезехова же камера конструктивно відрізняється від безехової тим, що її підлога не покрита радіо-звуко-поглинаючим матеріалом. Полубезехові приміщення зручно для вимірювання, закриття над важливого обладнання з метою запобігання витоку інформації. Полубезехове приміщення розробляться під стандарти електромагнітної сумісності (ЕМС) згідно військовим стандартам MIL-STD-461F. За цим стандартам ЕМС в безеховій камері тестується обладнання від десятків кілогерц до десятків гігагерц. Тут в першу чергу важлива не тільки частота, але і потужність впливу на обладнання різного класу для космосу, авіації, радіолокації, яке працює на різних частотах. Робоча частота тестування визначає довжину хвилі, а довжина хвилі в свою чергу впливає на відстань передачі до об'єкта. 40 ГГц - стандартна величина, до якої забезпечується екранування в камері. Екранування вище досягається завдяки спеціальним радиопоглинаючими матеріалами, тому що сигнал з частотою більше 40 ГГц може проходити крізь корпус радіочастотної кімнати [6].

Таким чином можна зробити висновок, що екранування електронно-цифрових пристроїв (в тому числі ПК) є невід'ємним атрибутом інформаційної безпеки в цілом, а використання технологій безехових камер значно підвищує рівень інформаційної безпеки.

Список використаних джерел

1. https://ru.wikipedia.org/wiki
2. Гавриш В.Ф. Практичний посібник із захисту комерційної таємниці. - Сімферополь: Таврида, 1994. - 112 с.
3. Електромагнітна сумісність радіоелектронних засобів і ненавмисні перешкоди. У 3-х вип. Вип 2.: Сокращ. пер. з англ. / Под ред. А. І. Сапріга. - М .: Сов. Радіо, 1978. - 272 с.
4. Торокіна А.А. Основи інженерно-технічного захисту інформації. - М .: Видавництво "Ось", 1998. - 336 с.
5. Ю.С.Тарасенко. Фізичні основи рідіолокації. / - Д.: «Пороги», 2011. – 487 с.
6. www.umpro.ru

УДК 004.77

Кячев О. А.
Харківський національний університет радіоелектроніки

Аналіз механізмів захищеності систем Інтернету речей

Технологія Інтернету речей об'єднує реальні речі в віртуальні системи, здатні вирішувати абсолютно різні завдання. Ключова ідея концепції - з'єднати між собою всі об'єкти, які можна з'єднати, підключити до мережі, і за рахунок цього отримати синергію.

Для реалізації Інтернет речей необхідна екосистема, яка включала б у себе пристрої оснащені датчиками; мережу доступу і передачі інформації (мобільну або фіксовану - не важливо); а також платформи для управління мережею, пристроями і додатками.

Для передачі даних від пристроїв сьогодні існує кілька спеціалізованих стандартів. Стандарт eMTC (enhanced Machine-Type Communication) розгортається на основі мобільних мереж LTE, а EC-GSM-IoT (Extended Coverage - GSM - Internet of Things) працює поверх мережі GSM. Але найбільш популярний - стандарт NB-IoT (Narrowband IoT). Його особливість полягає в тому, що він може бути розгорнутий, як в мережах GSM або LTE, так і незалежно, окремої мережею.

Концепція Інтернету речей тільки починає набирати обертів, і як відносно новий напрямок - дуже сирий. Я виділю три найбільш гострих проблемми:

- немає єдиної мови на якому могли б спілкуватися всі підключені пристрої;
- немає єдиних стандартів в цій галузі;
- погана захищеність.

Системі Інтернету речей необхідний серйозний захист від проникнення зловмисника. У міру постійного збільшення числа пристроїв, і підключених до Інтернету, виникають нові потенційні вразливі місця.

В даний час технологія Інтернету речей не надійна, ось деякі з основних питань:

- немає загальноприйнятих норм проектування;
- погане співвідношення вартості і захищеності обладнання;
- відсутність спеціалізованих стандартів безпеки обладнання;
- конфіденційність даних, перевірка справжності і контроль доступу;
- немає безпечної системи поновлення програмного забезпечення пристроїв;
- немає нормативно правового регулювання;
- не існує загальноприйнятого підходу до роботи застарілих пристроїв;

Недостатньо захищені пристрої можуть служити точками доступу для кібератак, дозволяючи зловмисникам перепрограмувати пристрій або викликати його несправність.

Список використаних джерел

1. *Вопросы и проблемы использования сети Интернет в более глобальном масштабе / Институт ЮНЕСКО по информационным технологиям в образовании. Аналитическая записка [Электронный ресурс] – Режим доступу: https://moodle.org/pluginfile.php/1969005/mod_page/content/16/Oblachnyie%20vychiskenia%20v%20obrazovanii.pdf.*
2. *Лекторий. Что такое интернет вещей и зачем он нужен / [Электронный ресурс] – Режим доступу: https://nv.ua/techno/popscience/chto-takoe-internet-veshchej-1326653.html.*
3. *Безопасность интернета вещей / [Электронный ресурс] – Режим доступу: https://ru.wikipedia.org/wiki/Безопасность_интернета_вещей.*
4. *Эталонная архитектура безопасности интернета вещей (IoT) / [Электронный ресурс] – Режим доступу: https://www.anti-malware.ru/practice/solutions/iot-the-reference-security-architecture-part-1.*

УДК 004.4

Лозовий А. М.
Кіровоградський науково-дослідний експертно-криміналістичний центр МВС України

Використання віртуальних машин для завантаження криміналістичних образів жорстких дисків

Вступ. Сьогодні віртуалізація вже багато років використовується в найпотужніших промислових системах, і застосовувати її має сенс де завгодно – від малого бізнесу до домашніх цілей.

Постановка задачі. Розглянути основні принципи роботи віртуальних машин, їх призначенням та використанням для завантаження криміналістичних образів жорстких дисків. Дослідити основні характеристики та різновиди платформ віртуалізації.

Мета роботи. Ознайомитись з основними принципами роботи віртуальних машин, їх призначенням та використанням для завантаження криміналістичних образів жорстких дисків. Дослідити основні характеристики та різновиди платформ віртуалізації.

Основна частина. На одному комп'ютері може функціонувати кілька віртуальних машин (це може використовуватися для імітації декількох серверів на одному реальному сервері з метою оптимізації використання ресурсів сервера). Віртуальні машини можуть використовуватися для: захисту інформації та обмеження можливостей програм (пісочниця); розв'язку між декількома користувачами, що працюють в одній обчислювальній системі, забезпечуючи певний рівень захисту даних; дослідження продуктивності ПЗ або нової комп'ютерної архітектури; емуляції різних архітектур; оптимізації використання ресурсів мейнфреймів і інших потужних комп'ютерів; моделювання інформаційних систем з клієнт-серверною архітектурою на одній ЕОМ (емуляція комп'ютерної мережі за допомогою декількох віртуальних машин).

На даний час існує багато віртуальних машин як пропрієтарних так і з відкритою ліцензією, наприклад DOSBox, Virtual PC, Parallels Workstation, VirtualBox, VMware Fusion, VMware Workstation.

В даній доповіді буде розглянута віртуальна машина з відкритим вихідним кодом під назвою Oracle VM VirtualBox.

Також для досягнення кінцевих цілей доповіді використовується програмне забезпечення AccessData FTK Imager - призначена для перегляду і клонування носіїв даних в середовищі Windows. Основні можливості FTK Imager: перегляд файлів і директорій на підключених носіях даних; створення точних копій (побітових) підключених носіїв даних (в форматах dd, EnCase, SMART); створення копій окремих файлів і директорій; експорт хеш-значень для файлів.

Для наших цілей підходить створення копії диску у форматі EnCase (E01), оскільки: більшість форензик-утиліт мають підтримку цього формату - на етапі аналізу вам не доведеться конвертувати образ; образ має довільну ступінь стиснення - від неї залежить підсумковий розмір і необхідний для створення образу час, ви зможете вибрати потрібний ступінь в залежності від ситуації; можливо створювати довільний розмір фрагменту образа - щоб образ було зручно копіювати по мережі або зберігати на файлових системах FAT32; на етапі створення виконується підрахунок контрольної суми образу. Отже, розглянемо покрокову інструкцію:

1. Для початку підключаємо жорсткий диск з якого ми хочемо зробити копію через пристрій для апаратного блокування даних. Після визначення диску ОС переходимо до наступних етапів.

2. Запускаємо FTK Image від імені адміністратора.

3. В головному меню вибираємо вкладку File і переходимо до пункту Create Disk Image.

4. Оскільки в даному прикладі розглядається фізично підключений диск через пристрій для апаратного блокування даних у виборі джерела даних обираємо Physical Drive і переходим на наступний етап.

5. Обираємо диск з якого буде робитися копія. У нашому випадку це \\. \PHYSICALDRIVE3 – Tableau Forensic SATA/IDE Bridge IEE 1394 SBP2 Device [500 GB 1394]

6. Наступний етап натискаємо кнопку додати (Add..)

7. Вибираємо тип образу E01.

8. Заповнюємо дані полів.

9. Вказуємо шлях для зберігання образу, його ім’я, розмір створюваного фрагменту (0 - диск одним фрагментом), ступінь стиснення і натискаємо кнопку Finish.

10. І останнє що нам потрібно зробити для створення образу це натиснути кнопку Start.

11. Після створення образу жорсткого диску потрібно створити папку для кеша монтування, наприклад C:\tempVBox_cache та змонтувати створений образ за допомогою FTK Imager з наступними параметрами:

Mount type: physical only (Тип монтування: тільки фізичний)

Mount method: block device/writeable (Спосіб монтування: блокувати пристрій/записувати)

Write cache folder: (Папка кеша),

Після натиснення кнопки Mount – відбудеться монтування. Звертаємо увагу на номер фізичного диска, він буде потрібний пізніше.

12. Запускаємо командний рядок від імені адміністратора! і виконуємо:

cd c:\Program Files\Oracle\VirtualBox\

13. Після виконання попереднього пункту створюємо диск для віртуальної машини, для цього виконуємо наступну команду:

VBoxManage internalcommands createrawvmdk -filename C:\VBox\temp\filename.vmdk -rawdisk \\.\PhysicalDriveX

Відповідно замінивши шлях (C:\VBox\temp\), ім’я файлу (filename.vmdk) і фізичний номер диску (physicaldriveX)

14. Запускаємо VirtualBox від імені адміністратора і створюємо нову віртуальну машину (Ctrl+N або в головному меню вкладка Машина->Создать...) з параметрами які вам потрібні:

Ім’я: <не принципове>

Тип: <вибрати відповідно>

Версія: <вибрати відповідно>

15. Вказуємо розмір оперативної пам’яті (для нормальної роботи вистачить: 2 - 4 ГБ).

16. На вкладці вибору жорсткого диску обираємо пункт «Использовать существующий виртуальный диск» і вибираємо жорсткий диск який створили за допомогою командного рядка в попередньому пункті → filename.vmdk.

17. Запустити щойно створену віртуальну машину з нашим диском.

Даний спосіб не є панацеєю для всіх можливих варіантів завантажень ОС. Деякі образи можуть не запуститися вилетівши в BSOD (Blue Screen of Death — назва повідомлення про критичну помилку операційної системи Microsoft Windows).

Висновки. Отже, підсумовуючи вище викладене можемо визначити приблизний алгоритм для монтування образів жорстких дисків під час виконання досліджень.

Список використаних джерел

1. *Oracle VM VirtualBox User Manual. [Електронний ресурс]: Режим доступу: https://www.virtualbox.org/manual/UserManual.html.*
2. *Вікіпедія. Вільна енциклопедія [Електронний ресурс]: Режим доступу: https://ru.wikipedia.org/wiki/VirtualBox.*

УДК 004.9

Лудан Д. В.
Вінницький національний технічний університет

Розробка інформаційної технології для організації інтерактивних квестів

Вступ. Із набуттям популярності квестів, виникла потреба у спрощенні процесу їх проведення. Традиційно, квести вважаються одним із способів розваги, яка вимагає поєднання інтелектуальних та фізичних здібностей. Будь-який квест потребує попередньої підготовки та контролю дій гравців організатором. Через стрімкий розвиток інформаційних технологій, більшість процесів, які відбуваються у суспільстві поступово комп'ютеризуються. На сьогодні існує проблема, пов'язана із трудомісткістю організації квестів, для розвязання якої необхідно створити технологію, яка автоматизує даний процес та зменшить матеріальні затрати.

Мета дослідження – створення інформаційної технології для організації інтерактивних квестів.

Результати дослідження. Квест – це завдання або набір завдань, логічно пов'язаних між собою, які мають на меті досягнення гравцем, або командою гравців, певної цілі. Завдання можуть бути інтелектуальними, творчими чи спортивними, що дозволяє використовувати квести у багатьох галузях. У сучасному житті квест стає універсальним інструментом організації діяльності молоді. Проаналізувавши ринок, можемо виділити основні різновиди квестів відповідно до мети їх використання: розважальні; навчальні; маркетингові. Сучасні квести організовуються у реальному світі з використанням реквізиту та заздалегідь підготованої програми. Складність таких квестів у тому, що вони потребують значних матеріальних та часових затрат від їх організатора. Прикладом таких квестів є міські квести, які прив'язані до обраної місцевості та мають на меті пошук певних об'єктів, «скарбів» і розв'язання загадок на основі карти чи, заздалегідь підготованих і розміщених по території, підказок. В якості ще одного окремого прикладу можна виділити квест-кімнати, які зазвичай створюються комерційними організаціями та пропонуються у вигляді атракціону.

Досить зручним способом організації квестів є використання інформаційних технологій, які дозволяють автоматизувати процес гри. Однією із переваг такого способу є те, що у якості реквізиту для завдань чи підказок квесту можна використовувати електронні ресурси. Це означає, що один і той самий квест може бути пройдений безліч разів без необхідності оновлення реквізиту. Тобто досягається економія як матеріальних так і часових затрат. Не менш важливим є те, що в такий спосіб можна оптимізувати процес створення і проходження всіх трьох вище описаних різновидів квестів. Для прикладу, за допомогою веб-квестів сучасні викладачі покращують методики викладання у школах. Під виглядом гри учні краще сприймають передбачений навчальною програмою матеріал, вчаться знаходити та аналізувати інформацію, критично мислити.

Проаналізувавши ринок інтернет-послуг організації квестів та інтелектуально-розважальних ігор, можна виокремити два продукти-аналоги.

Хмарна IT-платформа «City Quiz» для організації і проведення ігор типу інтелектуально-розважального шоу. Дана технологія позиціонує на міжнародному ринку та є платною як для організаторів, які її використовують для створення завдань, так і для учасників, які приймають участь у грі.

Ігрова система 12CODES, яка використовується для проведення ланцюжкових квестів. Даний інтернет-сервіс підходить для багатьох видів квестів: пішохідні, автоквести, вікторини, квести-екскурсії, навчальні квести. Проте для будь-якого виду є можливість створення тільки одного типу квесту, а саме ланцюжкового. Це означає, що суть системи полягає лише у відображенні змісту завдання чи запитання для користувача та, як наслідок виконання, перевірки введеної відповіді, так званого коду відповідного завдання.

Порівнявши аналоги та технологію, яка розробляється, бачимо, що описані

аналоги не задовольняють більшу частину ключових критеріїв. Зокрема, вони не можуть забезпечити проведення різних типів квестів, що дозволило б використовувати такі технології для будь-яких сфер діяльності. Також, унікальністю моєї технології є те, що для всіх охочих прийняття участі у будь-якому наявному в системі квесті буде абсолютно безкоштовним, в той час як проект матиме статус комерційного. Адже його монетизація відбуватиметься за рахунок продажу квестів із прихованою рекламою. Завдяки маркетинговим квестам, заклади, які потребують ефективної піар-стратегії, зможуть привабити більшу кількість клієнтів, а користувачі не лише матимуть можливість безкоштовної участі у грі, а й зможуть отримувати призи від спонсорів, які замовляють дані квести.

Ще однією перевагою стануть рекомендації та фільтри для вибору квестів. Оскільки в системі завжди будуть доступні для проходження завдання, будь-який користувач зможе розпочати гру без попереднього замовлення в зручний для нього час. Тому корисними стануть фільтри й рекомендації, які допоможуть швидко підібрати квести, що найкраще підійдуть певному користувачеві. Наприклад рекомендуватимуться квести, які відбуваються поблизу місця знаходження гравця або ті, які по типу співпадають із завданнями, що обирались найчастіше даним користувачем.

Наявні на сьогодні класифікації квестів базуються на ознаках, які стосуються в основному навчальних квестів, тому для створення інформаційної технології організації інтерактивних квестів, які застосовуватимуться у різних галузях, а не лише у навчальній, доцільно розробити власну універсальну класифікацію за загальними ознаками: 1) за способом виконання: фотоквест; квест-вікторина; ланцюжковий квест; змагання; за часом виконання: з таймером; з єдиним дедлайном. За кількістю виконавців: індивідуальні; командні. З метою автоматизації процесу перевірки результатів квесту, використовується нейронна мережа Кохонена. Застосування нейронних мереж дозволяє створювати не тільки автоматизовані квести, а й квести, проходження і перевірка яких є автоматичною.

Нейронні мережі Кохонена — клас нейронних мереж, основним елементом яких є шар Кохонена. Шар Кохонена складається з адаптивних лінійних суматорів («лінійних формальних нейронів»). Як правило, вихідні сигнали шару Кохонена обробляються за правилом «переможець забирає все»: найбільший сигнал перетворюється в одиничний, решта звертаються в нуль [1]. Оскільки цільова аудиторія користувачів – здебільшого молоді люди та підлітки, необхідна інтеграція з соціальними мережами. API Graph - це основний інструмент для отримання і введення даних на платформі Facebook. Це низькорівневий API на основі HTTP, за допомогою якого можна програмно запитувати дані, створювати публікації, управляти рекламою, завантажувати фото і виконувати безліч інших завдань в додатку [2].

Технологію побудовано на основі клієнт-серверної архітектури, яка є одним із архітектурних шаблонів програмного забезпечення та є домінуючою концепцією у створенні розподілених мережних застосунків і передбачає взаємодію та обмін даними між ними. Вона передбачає такі основні компоненти: набір серверів, які надають інформацію або інші послуги програмам, які звертаються до них; набір клієнтів, які використовують сервіси, що надаються серверами; мережа, яка забезпечує взаємодію між клієнтами та серверами.

Висновки. В результаті аналізу предметної області організації квестів та аналогів продукту, доведено доцільність розробки інформаційної технології для організації інтерактивних квестів. Створено власну класифікацію квестів, у яку включено мінімальний набір типів квестів, яких достатньо для забезпечення потреб трьох основних напрямків їх використання. Автоматизація процесу проходження завдань та перевірки результатів забезпечується за рахунок використання нейронної мережі Кохонена.

Список використаних джерел

1. *Trevor Hastie, Robert Tibshirani, Jerome Friedman. Chapter 14.4 Self-Organizing Maps // The Elements of Statistical Learning. — 2009. — С. 528-534.*
2. *Обзор API Graph [Електронний ресурс] – Режим доступу до ресурсу: https://developers.facebook.com/docs/graph-api/overview.*
3. *Коннолі Т., Бегг К., Страчан А. Бази даних: проектування, реалізація і супровід. Теорія й практика. 2-е вид.: Пер. з англ. – М.: Издательский дом «Вильямс», 2000. – 1120 с.*

УДК: 336.744

Можарівський В. В.
Київський національний університет будівництва і архітектури

Автоматизована торгівля на біржах криптовалют

Ринок криптовалют є досить молодим, на ньому присутня висока волатильність,це відкриває можливості для отримання прибутку. Для того щоб розпочати торги на криптовалютному ринку достатньо обрати біржу, яка підходить під ваші потреби. Але щоб почати заробляти, на будь якому ринку, за допомогою торгівлі, потрібно: володіти певними знаннями по аналізу ринку, знати тренд, слідкувати за індикаторами чи новинамиякі впливають на ціну.

Існують багато принципів та алгоритмів по яким спекулянти, або їх ще називають трейдерами, ведуть свою торгівлю на біржах. В будь-якому випадку, потрібно постійно слідкувати за фоном ринку, вести аналіз та здійснювати відповідні торгові транзакції на торгових платформах, всі ці дії здійснюються вручну. Але технології не стоять на місці, все більше і більше процесів автоматизуються, так і на торгових біржах з'являються нові програми, які ведуть автоматичний аналіз ринку та здійснюють торгівлю без участі трейдера. Звісно не всі торгові алгоритми підходять для автоматизованої торгівлі, деякі працюють в напівавтоматичному режимі, це коли трейдер вказує певні індикатори та змінні в ручному режимі, та паралельно аналізує ринок, наприклад коли спекулянт повинен робити аналіз ринку та вказувати тренд ринку, тобто росту чи падіння в цілому.

Програми які ведуть автоматичну торгівлю на біржах називають ботами. Такі боти працюють напряму з біржами через API інтерфейс. Якщо коротко про даний інтерфейс, то це можливість отримати або ж передати певну інформацію через мережу в заданому форматі по певним посиланням. В основному такі API використовують формат JSON або XML. Кожна сучасна біржа має цей інтерфейс та документацію по ньому. Завдяки документації програміст може написати бота на будь-якій мові програмування, яка може передати запит по HTTP протоколу та зчитати його. Документація розділяється на дві групи, перша - це публічна інформація: курси, об'єм, торгові пари та інше; друга - це приватна інформація: транзакція користувачів, їх баланси та інше. Щоб захистити приватну інформацію, біржі надають користувачам приватний та публічний API ключі. Завдяки цим ключам інформація шифрується певними алгоритмами і ніхто крім власника ключа та біржі не зможе розшифрувати дані, навіть якщо зможе перехопити інформацію в мережі.

Хоч біржа і забезпечує захист передачі даних, це не означає, що ніхто, крім власника не зможе управляти аккаунтом. Багато трейдерів завантажують готове програмне забезпечення та вставляють в налаштування свої API ключі, після чого зловмисник перехоплює ключі та має повний доступ до управління капіталом трейдера. Розуміючи цей факт потрібно зробити висновки і користуватися або безпечним програмним забезпечення або писати свої програми. Також при програмуванні бота, у алгоритмі потрібно враховувати комісію біржі. Кожна біржа бере комісію за кожну транзакцію або ж за час який дана транзакція виконується. Якщо бот часто здійснює транзакції з маленьким профітом (заробітком) і не враховує комісію, то така програма може працювати в мінус по дохідності.

Торгові боти мають багато переваг надтрейдером який працює вручну. Ботам не потрібно спати, їсти, відпочивати, вони працюють без перерв та вихідних. Програма може паралельно працювати над багатьма торговими парами одночасно, аналізувати великий об'єм даних. В деяких алгоритмах потрібна швидкість реагування на зміну курсу, людина фізично не зможе швидше здійснити транзакцію на біржі а ніж це зробить бот, в основному затрата часу йде тільки на передачу запиту по мережі, а це зазвичай менше однієї секунди. Якщо алгоритм бота немає змінних, які потрібно корегувати, то це являється пасивним заробітком.

Існують два типа ботів: торгові і арбітражні. Торговий бот працює на одній біржі. Арбітражного бота теж можна назвати торговим, але він торгує в рамках декількох бірж, отримавши дохід з різниці курсу однієї і тієї ж валютної пари на різних біржах.

УДК 004

Нетепенко В. В.
Харківський національний університет радіоелектроніки

Ідентифікації диктора за голосом

Існують різні підходи до вирішення завдання текстонезалежною ідентифікацій дикторів. Деякі з них грунтуються на статистичному підході, інші засновані на ідеях векторного квантування. Інші використовують системи розпізнавання фонем, і визначають особливості їх вимови. Існують так само різновиди систем другого типу, які виробляють класифікацію сегментів по фонетичному ознакою.

Коефіцієнти лінійного передбачення (КЛП) є одним з найбільш ефективних і часто використовуваних методів аналізу мовного сигналу. Важливість методу обумовлена високою точністю одержуваних оцінок і відносною простотою обчислень. У даній статті викладаються основні положення методу лінійного передбачення.

Основний принцип методу лінійного передбачення полягає в тому, що поточний відлік мовного сигналу можна апроксимувати лінійною комбінацією попередніх відліків. Коефіцієнти передбачення при цьому визначаються однозначно мінімізацією середнього квадрата різниці між відліками мовного сигналу і їх передбаченими значеннями на кінцевому інтервалі. При обробці мовних сигналів розуміють максимум в передавальної характеристиці мовного тракту, або частіше максимум в згладженому спектрі мовного фрагмента.

Основне завдання аналізу на основі лінійного передбачення полягає в безпосередньому визначенні параметрів по мовному сигналу з метою отримання хороших оцінок його спектральних властивостей. Внаслідок зміни властивостей мовного сигналу в часі коефіцієнти передбачення повинні оцінюватися на коротких сегментах мови. Основним підходом є визначення параметрів передбачення, таким чином, щоб мінімізувати короткочасну енергію похибки на короткому сегменті сигналу.

Найбільш ефективним прийомом ідентифікації диктора зарекомендувало себе векторне квантування. Суть цього прийому полягає в наступному. Параметричний простір при формуванні еталону для даного диктора розбивається на кінцеве кількість осередків (кластерів), найбільш детально описує потрапляння векторів параметризації в цей простір при заданій кількості кластерів. Очевидно, що таке розбиття параметричного простору є індивідуальним для кожного диктора. При ідентифікації мовця по вступнику мовному повідомленню розподіл кластерів (або інтегральне по всьому повідомленням, або по осі часу), виявляється схожим на еталонне для зареєстрованого користувача.

При ідентифікації диктора можна зберігати все вектора ознаки з навчальної вибірки і надалі просто порівнювати будь-який з надійшли векторів з зберігаються в пам'яті. На практиці такий підхід практично не застосуємо, тому що кількість векторів у навчальній вибірці може виявитися занадто великим. Отже, необхідно знайти метод, що дозволяє скоротити кількість збережених векторів без істотного зменшення точності ідентифікації. У методі, заснованому на векторному квантуванні, як набір параметрів Y виступає деякий набір векторів ознак, побудованих на основі навчальної вибірки. В якості вирішального правила зазвичай виступає критерій мінімальної відстані від надійшов на вхід вектора до всіх векторів всіх моделей дикторів.

Стандартний метод обчислення формант складається в розбитті вхідного мовного сигналу на сегменти однаковою довжини. На кожному із сегментів обчислюються КЛП коефіцієнти. За отриманими КЛП коефіцієнтам обчислюється спектр потужності сигналу. Одержуваний спектр не є тим же спектром, що і отриманий за допомогою

перетворення Фур'є тому, що для обчислення КЛП використовують сотні вхідних відліків, а самих коефіцієнтів обчислюють не більше двох десятків. Проте, отриманий з КЛП спектр з деякою точністю збігається зі спектром, отриманим за допомогою перетворення Фур'є. Приклад спектра сигналу, обчислений на основі КЛП коефіцієнтів для голосного звуку "А" показаний на Рисунку 1.

У розрахунковому спектрі потужності знаходять максимуми. Їх частоти і амплітуди і покладаються частотами і амплітудами формант.

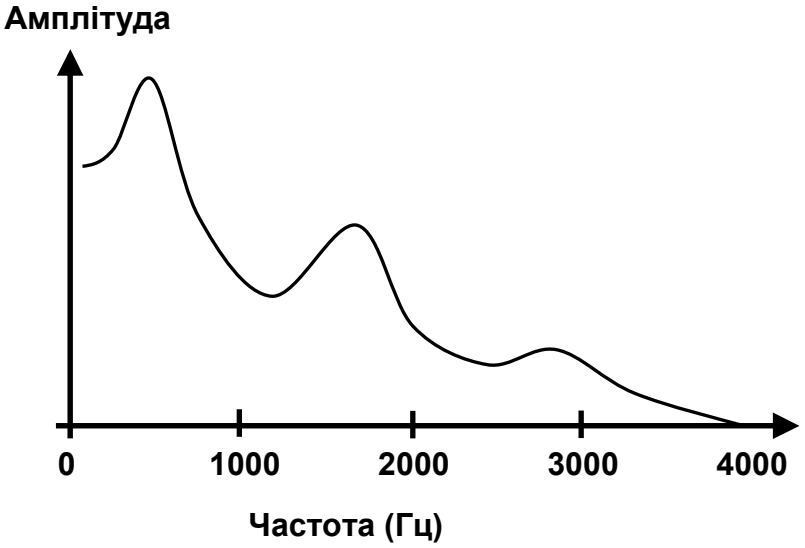


Рисунок 1 – Приклад спектра звуку "А" відновленого з коефіцієнтів лінійного передбачення

Форманти слабо змінюються під впливом адитивних і навіть невеликих мультиплікативний шумів. Однак на практиці вони застосовуються досить рідко. Обумовлено це складністю обробки формант отриманих з реального мовного сигналу.

Однією з основних проблем при використанні формант є те, що їх практично неможливо пронумерувати для обчислення відстані між формантами за подобою евклідової відстані. Закінчуються невдачею спроби нумерації по частоті незалежно від фонетичного контексту. Так само неможливо пронумерувати по займаній частотній смузі. Наприклад, для фонеми "І" частота 1-й форманти становить 765 ± 130Гц, в той час як для фонеми "О" частота 2-й форманти становить 867 ± 100 Гц.

З іншого боку при проведенні процедури експертної ідентифікації особистості по голосу форманти широко і успішно використовуються. Однак при цьому істотно використовується фонетичний контекст, на якому обчислюються параметри формант. Тобто експерти не використовують частоти першої або другої форманти обчислені по мові, а використовують такі поняття як частота першої форманти фонеми "а" або навіть сильнішу зв'язку з фонетичним контекстом -" частота другий форманти першої фонеми "а" в слові "мама".

Список використаних джерел

1. Маркел, Джон Д., Грей. Лінійне передбачення мови / Пер з англ. За редакцією Ю.М. Прохорова, В.С. Звездін, - М.: Зв'язок 1980.

2. фуру С., Ітакура Ф., Санто С. індивідуальні характеристики спектра мови. -РЖ. Кібернетика, 1974, № 12.

3. Атал Б. Автоматичне розпізнавання дикторів за голосом. - ТІІЕР, 1976, Т64 № 4.

УДК 004.056

Окунь Є. В., Романько Д. В.
Київський національний університет будівництва і архітектури

Інтернет речей та проблеми його захисту

Інтернет речей – одна з найпопулярніших концепцій в сучасній футурології. І більш того, одна з тих небагатьох, що вже перестають бути концепціями і втілюються в життя.

Згідно з найбільш поширеним формулюванням, інтернет речей – це концепція обчислювальної мережі фізичних предметів (тобто власне, речей), які оснащені такими собі технологіями для взаємодії один з одним.

Концепція передбачає, що інтернет речей здатний серйозно вплинути на розвиток сучасного суспільства, оскільки дозволить багатьом процесам відбуватися без участі людини.

Інтернет речей (Internet of Things, скорочено IoT) – це глобальна мережа підключених до Інтернету фізичних пристроїв – «речей», оснащених сенсорами, датчиками і пристроями передачі інформації. Ці пристрої об'єднані за допомогою підключення до центрів контролю, управління і обробки інформації.

Для реалізації IoT необхідна екосистема, яка включала б у себе «розумні речі» – різні пристрої, оснащені датчиками; мережу доступу і передачі інформації (мобільну або фіксовану – не важливо); а також платформи для управління мережею, пристроями і додатками. Паззл не склався за відсутності хоча б одного із зазначених компонентів.

Для передачі даних від «розумних» пристроїв сьогодні існує кілька спеціалізованих стандартів. Стандарт eMTC (enhanced Machine-Type Communication) розгортається на основі мобільних мереж LTE, а EC-GSM-IoT (Extended Coverage – GSM – Internet of Things) працює поверх мережі GSM. Але найбільш популярний – стандарт NB-IoT (Narrowband IoT). Його особливість полягає в тому, що він може бути розгорнутий, як в мережах GSM або LTE, так і незалежно, окремою мережею.

Сьогодні різних інформаційних технологій IoT досить багато. Наведемо приклад деяких моделей.

IoT для будинку (технології “розумний будинок”). Передбачає можливість віддаленого керування за допомогою Інтернет-технологій побутовими приладами, віддалений моніторинг і управління, зокрема програмованого, системами освітлення, опалювання, кондиціонування, медіапристроями, протипожежними системами, кухонними пристроями і ін.

IoT для медицини. Для діагностики вже застосовуються методи телемедицини, коли є зв’язок з лікарем, поліклінікою або лабораторією, що знаходяться в іншому районі. Розроблені протези кінцівок, керовані за допомогою сигналів мозку. Існують бездротові пристрої, які дозволяють паралізованим пацієнтам керувати телевізорами, комп’ютерами та інвалідними кріслами.

IoT у фінансовому секторі і страхуванні, охоронній сфері і дослідницькому бізнесі також активно розвивається. Близько 10 % компаній у всьому світі застосовують будь-яку IoT-технологію в своєму бізнесі.

IoT для транспорту. Безліч рішень для безпечнішої експлуатації створено для ж/д та авіатранспорту. Для автомобіля вже використовуються системи відстеження його маршруту, моніторинг вантажоперевезень, контроль відвантаження, складування та ін.

Сьогодні практикується імплантація датчиків всередину тіла людини, яки можуть автоматично передавати медичну інформацію на видалені сервери. Ці дані надалі аналізуються за допомогою технології постачальника, і, нерідко, спільно з третіми

сторонами. Хоча така діяльність несе певну користь всім зацікавленим, проте, для суб'єкта персональних даних стає дедалі відстежувати і контролювати те, де і як вони зберігаються, ким і коли використовуються, і з якою метою.

За прогнозами впровадження технологій IoT матиме наслідком появу до 100 мільярдів технічних пристроїв до 2025 року, які, напевно, будуть оснащені бездротовими технологіями передачі даних, обмін якими буде здійснюватися за допомогою мережі Інтернет.

Наведені та багато інших прикладів свідчить, що IoT розглядається пріоритетним напрямом розвитку в багатьох країнах.

Але більшість пристроїв інтернету речей не володіють достатніми обчислювальними потужностями для обробки коду, який захищає дані. Як правило в таких мережах використовуються шлюзи і проксі, завдяки яким відбувається обмін інформацією між різними пристроями — саме ці елементи системи цікавлять зловмисників в першу чергу.

Для реалізації багатьох сценаріїв використання IoT необхідне впровадження мереж 5G. Мережі п'ятого покоління дозволять знизити затримки, одночасно підтримувати величезну кількість підключень, продовжити службу «розумних» пристроїв до 10 років, а також домогтися неймовірних за нинішніми мірками швидкостей мобільної передачі даних.

До основних проблем Інтернету речей можна віднести інформаційну безпеку і захист персональних даних. Технології IoT значно посилюють ризики порушення конфіденційності персональних даних внаслідок того, що вони передбачають накопичення, циркулювання і використання великого, територіально і технологічно розподіленого обсягу інформації (даних) про конкретну людину. Це викликає цілком закономірні питання про надійність зберігання таких даних та забезпечення їх захисту від несанкціонованого використання.

Можна зазначити, що широке використання технологій Інтернету речей призводить до необхідності вирішення таких основних правових проблем:

- визначення механізмів реалізації принципу попередньої згоди на використання та "на стирання" персональних даних (ст. 17 Регламенту ЄС 2016/679 від 27.04.16 р.);

- правовий вплив на регулювання транскордонних потоків персональних даних, що передбачає не тільки цілеспрямовану діяльність по впорядковуванню інформаційних відносин, але і непряму дію правових засобів і методів на різних суб'єктів, що не підпадають безпосередньо під правове регулювання;

- використання персональних даних інтелектуальними комплексами, що функціонують без участі суб'єктів (юридичних або фізичних осіб). Крім того, необхідність створення багаторівневої і багатооб'єктної системи захисту персональних даних потребує формування нової системи правового регулювання.

Список використаних джерел

1. *Що таке інтернет речей і навіщо він потрібен? [Електронний ресурс] : [Веб-сайт]. – Електронні дані. – Київ : ООО «Видавничий дім «МЕДІА-ДК», 2014-2018.– Режим доступу : https://nv.ua/ukr/techno/popscience/lektorij-shcho-take-internet-rechej-i-navishcho-vin-potriben-1326653.html (дата звернення 10.11.2018) – Назва з екрана.*
2. *Як інтернет речей змінює підхід до безпеки в корпораціях ? [Електронний ресурс] : [Веб-сайт]. – Режим доступу : http://it-ua.info/news/2015/04/09/yak-nternet-rechey-zmnyu-pdhd-do-bezpeki-v-korporacyah.html (дата звернення 10.11.2018) – Назва з екрана.*
3. *Захист персональних даних в сфері Інтернет речей [Електронний ресурс] : / Баранов О.А., Брижко В.М. // Інформація і право. – 2016. – № 2(17). – С. 85-91. – Режим доступу : http://ippi.org.ua/sites/default/files/11_0.pdf (дата звернення 10.11.2018) – Назва з екрана.*

УДК 532.5

Остапенко А. О.
ДВНЗ «Приазовський державний технічний університет»

Застосування кінетичного підходу до моделювання гідродинаміки

Метод граткових рівнянь Больцмана (LBM, від. англ. Lattice Boltzmann Method) – це метод обчислювальної гідродинаміки, що базується на кінетичному підході до моделювання течії в'язкої рідини. На відміну від таких класичних методів, як метод скінченних елементів, метод скінченних об'ємів, спектральний метод, LBM не розв'язує рівнянь Нав'є - Стокса, а моделює динаміку рідини кінетичним рівнянням Больцмана.

На сьогодні метод граткових рівнянь Больцмана набуває популярності. Він вже використовується при моделюванні багатофазних та багатокомпонентних течій, мікротечій, течій із вільною поверхнею, теплопереносу. У порівнянні із класичними методами обчислювальної гідродинаміки, метод LBM має наступні переваги:

- всі етапи моделювання описуються лінійними рівняннями;
- граничні умови задаються у вигляді простих механічних правил;
- моделювання течій можна проводити в областях довільної складної геометрії;
- використовується явна схема врахування впливу зовнішніх сил та обчислення тиску;
- до алгоритму легко застосовуються технологій паралельних обчислень;
- можна розв'язувати широкий клас задач, зокрема проводити мультифізичне моделювання.

Недоліком методу є його умовна стійкість. Чисельні розв'язки сходяться лише за малими числами Маху.

Метод LBM працює на мезоскопічному рівні абстракції опису суцільного середовища. Розрахункова область розбивається на комірки нерухомою ейлеревою сіткою. Кожні комірка трактується як крупна мезоскопічна частинка та описуються статистично через функцію розподілу частинок за координатами і швидкостями $f\left(\vec{r},\vec{\upsilon},t\right)$, що є розв'язком рівняння Больцмана.

Чисельна модель (1) – система дискретних граткових рівнянь Больцмана із урахуванням відсутності зовнішніх сил $\vec{F} \equiv 0$ та інтегралом зіткнення частинок у вигляді наближення Бхатнагара-Гросса-Крука.

$$\underbrace{f_k(\vec{r}+\vec{V}_k\Delta t, t+\Delta t) = f_k(\vec{r},t)}_{\text{переміщення}} - \underbrace{\frac{1}{\tau}[f_k(\vec{r},t) - f_k^{eq}(\vec{r},t)]}_{\text{зіткнення}} \quad (1)$$

де $f_k(\vec{r},t)$ – дискретна функція розподілу частинок за швидкостями;

$\vec{V}_k$ – дискретний набір швидкостей частинок;

Δt – крок за часом;

τ – безрозмірний параметр релаксації;

$f_k^{eq}(\vec{r},t)$ – дискретне наближення локальної рівноважної функції розподілу Максвела-Больцмана.

Розглядається двовимірна дев'яти швидкісна решітка D2Q9, у якій переміщення частинок можливе у кожну із 8 сусідніх комірок. Макроскопічні параметри рідини у кожній комірці, такі як густина, швидкість та тиск визначаються через функцію розподілу відповідно до формул:

$$\rho\left(\vec{r},t\right)=\sum_{k=0}^{8}f_k\left(\vec{r},t\right);\ \ \vec{u}\left(\vec{r},t\right)=\frac{1}{\rho\left(\vec{r},t\right)}\sum_{k=0}^{8}\vec{V}_k f_k\left(\vec{r},t\right);\ \ p\left(\vec{r},t\right)=c_s^2\rho\left(\vec{r},t\right) \qquad (2)$$

Алгоритм методу, відповідно до розкладу рівняння (1) за методом Яненко розкладається на три етапи (рис. 1): перенесення крупних частинок, їх зіткнення і перехід від мезоскопічного рівня до макроскопічних параметрів рідини за формулами (2).

При програмуванні алгоритму методу граткових рівнянь Больцмана є необхідність створення структури даних, що зберігає інформацію про кожну крупну частинку. Крупна частинка утворюється в результаті накладання розрахункової сітки на розрахункову область. Кожна комірка, що є крупною мезоскопічною частинкою, буде містити дев'ять значень функції розподілу $f_k, k=\overline{0,8}$ (для D2Q9 моделі решітки), фізичний сенс яких є ймовірність частинки мати одну з швидкостей $\vec{V_k}$. Потреба зберігати такі дані змушує трансформувати розрахункову сітку розмірності $M\times N$ у розрахунковий куб розмірності $M\times N\times 9$. Частинки, на кожному із дев'яти шарів куба переміщуються в одному з напрямків $\vec{e_k}, k=\overline{0,8}$.

Рис. 1 – Алгоритм моделювання

Майже всі етапи моделювання методом LBM, за винятком переміщення частинок, складаються з ряду локальних операцій у комірках розрахункової сітки. Тому до алгоритму легко застосовуються технології паралельних обчислень. Зокрема розпаралелювання етапу зіткнення частинок на CPU з використанням технології OpenMP дозволяє збільшити швидкість розрахунків приблизно в 3-4 рази.

Розглянуті можливості методу граткових рівнянь Больцмана при моделюванні в'язких течій у каналах різних викривлених геометрій у діапазоні чисел Рейнольдса від 100 до 500. На рис. 2 зображені лінії течії в'язкої рідини у викривленому каналі із Re = 200. Проведено порівняння характеру течій із даними чисельних експериментів, проведених у пакеті Comsol методом скінченних елементів – FEM (рис. 3). Порівняння показало добру відповідність результатів моделювання уздовж усього каналу.

Розглянуті течії виникають у мініатюризованих системах (внутрішньовенна подача рідини, мікротечії у мікросхемах, тощо), тому є актуальним напрямком, що потребує врахування в'язких ефектів. Крім того, течії у мікроканалах можуть бути розв'язані методом LBM через легку побудову різних типів каналів та переважно ламінарний характер течії. Даний метод зокрема дозволяє отримати значення тиску напряму із функції розподілу, можливість моделювання в'язких ефектів без розв'язку

рівнянь Нав'є-Стокса, можливість проводити мультифізичне моделювання із урахуванням темплопереносу. Недоліком такого підходу є досить низька швидкість розрахунків, обмеження на малі швидкості у області та можливу нестійкість розв'язків.

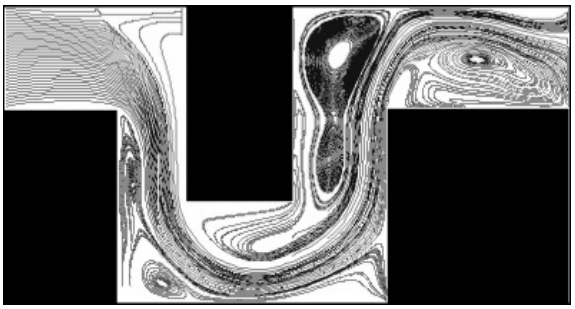


Рис. 2 – Лінії течії в'язкої рідини у мікроканалі із Re = 200, отримані методом LBM

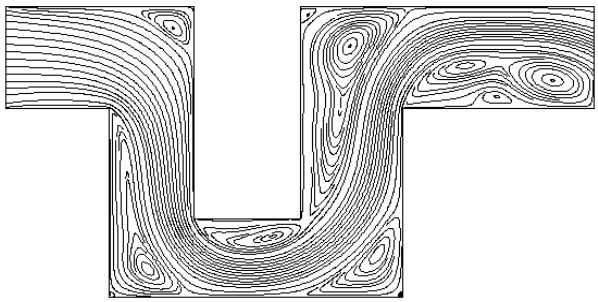


Рис. 3 – Лінії течії в'язкої рідини у мікроканалі із Re = 200, отримані методом FEM

Метод граткових рівнянь Больцмана є досить новим та перспективним підходом у обчислювальній гідродинаміці. Актуальним напрямком подальших досліджень є зменшення часу моделювання за рахунок оптимізації алгоритму та дослідження можливостей методу до моделювання турбулентних течій.

Список використаних джерел

1. *Succi S. The Lattice Boltzmann Equation: A New Tool For Computational Fluid-Dynamics / S. Succi, R. Benzi // Physica D: Nonlinear Phenomena. – 1991. – Vol. 47. – P. 219-230.*
2. Куперштох А.Л. Трехмерное моделирование двухфазных систем типа жидкость-пар методом решеточных уравнений Больцмана на GPU / А.Л. Куперштох // Вычислительные методы и программирование. – 2012. – № 13. – С. 130-138.
3. Grazyna K.The numerical solution of the transient heat conduction problem using the lattice Boltzmann method / K. Grazyna // Scientific Research of the Institute of Mathematic and Computer Science. – 2006. – № 11. – P. 23-30.
4. Coupanec E. Boundary conditions for the lattice Boltzmann method. Mass conserving boundary conditions for moving walls / E. Coupanec. – *Trondheim:* Norwegian University of Science and Technology. Department of Energy and Process Engineering, 2010. – 39 p.
5. *Mussa M. Numerical Simulation of Lid-Driven Cavity Flow Using the Lattice Boltzmann Method / M. Mussa // Applied Mathematics. – 2008. – Vol. 13. – P. 236-240.*
6. *Hong X. Research of Micro-Rectangular-Channel Flow Based on Lattice Boltzmann Method / X. Hong, W. Di, S. Yuhe // Research Journal of Applied Science, Engineering and Technology. – 2013. – Vol.6, №14. – P. 2520-2525.*
7. *Wolf-Gladrow D. Lattice-Gas Cellular Automata and Lattice Boltzmann Models - An Introduction / D. Wolf-Gladrow. – Bremerhaven: Alfred Wegener Institute for Polar and Marine, 2005. – 273 p.*
8. *Sucop M. Lattice Boltzmann Modeling. An Introduction for Geoscientists and Engineers / M.Sucop. – Miami: Springer, 2006. – 171 p.*
9. *Rettinger C. Fluid Flow Simulation using the Lattice Boltzmann Method with multiple relaxation times / C. Rettinger. – Erlander: Friedrich-Alexander Universuty Erlander-Nuremberg, 2013. – 38 p.*
10. *Бикулов Д.А. Реализация метода решеточных уравнений Больцмана для расчетов на GPU-кластере / Д.А. Бикулов, Д.С. Сенин, Д.С. Демин, А.В. Дмитриев, Н.Е. Грачев // Вычислительные методы и программирование. – 2012. – Т.13. – С. 13-19.*
11. *Самойлов Д.А. Вычислительные возможности метода решеточного кинетического уравнения Больцмана / Д.А. Самойлов, А.С. Губкин // Вестник Тюменского Государственного Университета. Физико-Математические науки. Информатика. – 2014. –№ 7. – С. 83-91.*
12. *Ляпин И.И. Введение в теорию кинетических уравнений: Учебное пособие / И.И. Ляпин. – Екатеринбург: УГТУ-УПИ, 2003. – 205 с.*

УДК 004.4

Підгорний П. Є., Сидорова М. Г.
Дніпровський національний університет імені Олеся Гончара

Розробка програмно-математичного забезпечення для аналізу траєкторій пересування об'єктів у просторі та часі

Останні досягнення сучасних інформаційних технологій надають можливість майже безперервного відстежування переміщення різних об'єктів у просторі та часі. Як наслідок – щосекунди генеруються величезні об'єми даних пов'язаних з траєкторіями руху за допомогою різних мобільних пристроїв (мобільні телефони, трекери, розумні годинники, транспорт, системи безпеки). При використанні вдалого підходу до аналізу цих даних можна отримати безліч корисної інформації про власників цих пристроїв, їх звички та особливості руху.

Найбільш очевидними галузями застосування подібних систем є маркетинг та різні сфери аналітики, де досить важливо аналізувати та розуміти аудиторію, правильно розподіляти її по категоріям та інтересам, щоб мати можливість більш точно привертати нову аудиторію, або більш правильно робити висновки щодо існуючої аудиторії.

Метою роботи є розробка програмного та математичного забезпечення призначеного для аналізу геопозиційних даних, що подані у вигляді множини об'єктів спостереження $X = \left\{ X_i; i = \overline{1,N} \right\}$, $X_i = \left\{ t_{ij}, lat_{ij}, long_{ij}; j = \overline{1,T} \right\}$, в момент часу t_{ij}.

Першочерговою задачею в рамках цієї роботи було знаходження «точок інтересів» для кожного з об'єктів. Ці точки можна використовувати для складання певного «портрету» об'єкта, що буде корисним при наданні персоналізованих рекомендацій [1]. Для цієї задачі було використано щільнісний алгоритм кластеризації просторових даних з присутністю шуму DBSCAN. Для оцінки якості результатів кластеризації було застосовано інформаційну технологію оцінки багатокритеріальної якості та підвищення стійкості результатів кластерів [2].

Маючи справу з геопозиційними координатами, класичні міри відстані можуть бути не адаптованими під розглянуту задачу. Це пов'язано еліпсоїдною формою нашої планети. Відстані двох точок в Евклідовому просторі і двох точок, що лежать на поверхні сфери, мають абсолютно різні принципи обчислення. Тому у якості міри відстані було використано модифіковану формулу гаверсинусів:

$$\arctan\left\{\frac{\sqrt{[\cos\varphi_2 \sin\Delta\lambda]^2 + [\cos\varphi_1 \sin\varphi_2 - \sin\varphi_1 \cos\varphi_2 \cos\Delta\lambda]^2}}{\sin\varphi_1 \sin\varphi_2 + \cos\varphi_1 \cos\varphi_2 \cos\Delta\lambda}\right\}$$

Наступною задачею цієї роботи було виявлення закономірностей у досліджуваних траєкторіях переміщення об'єктів, для вирішення котрої було реалізовано алгоритм пошуку асоціативних правил Apriori [3]. Асоціативні правила дозволяють знаходити закономірності між зв'язаними подіями. Прикладом такої закономірності може слугувати правило, котре вказує, що з події X з деякою ймовірністю слідує подія Y. Встановлення таких залежностей надає можливість знаходити досить прості та інтуїтивно зрозумілі правила.

Зазначені вище методи дозволяють аналізувати початкові дані по більшій мірі з просторової точки зори. Для того, щоб аналізувати ці данні з використанням часового атрибуту були використані різні методи дослідження часових рядів.

Якщо розглянути траєкторії як часові ряди то стає очевидною задача оцінки схожості траєкторій між собою, ключовою вимогою для котрої є визначення відстаней між ними. Для цієї задачі можливо використовувати Евклідову відстань, проте вона має істотний недолік: ця відстань не враховує зміщення часового ряду. Тобто використовуючи Евклідову відстань при аналізі двох однакових часових рядів, один з яких трохи зміщений у часовому просторі, ми можемо отримати хибний результат, котрий буде означати, що ці ряди відрізняються один від одного. З метою усунення цього недоліку в цій роботі було застосовано алгоритм динамічної трансформації часової шкали, що дозволяє знаходити відстань між часовими рядами не зважаючи на зміщення по часовій шкалі.

Базуючись на результати попередніх методів було прийнято рішення провести додатковий аналіз використовуючи ієрархічний агломеративний метод кластеризації. Це дозволяє впорядкувати по схожості траєкторії за допомогою створення дерева вкладених кластерів. На основі результатів кластеризації було побудовано дендрограмму, що значно спрощує процес інтерпретації та побудування висновків.

Основними результатами проведеної роботи можна вважати наступні висновки:

- досліджено існуючі підходи, методи та технології для аналізу геопозиційних даних;

- розроблений алгоритм пошуку «точок інтересу» об’єктів дослідження на основі кластерного аналізу, а також цей алгоритм було адаптовано до просторово-часової моделі;

- створено механізм для виявлення закономірностей у досліджуваних траєкторіях переміщення об’єктів на основі алгоритму пошуку асоціативних правил Apriori;

- створено механізм для визначення подібності траєкторій з урахуванням зміщення по часовому атрибуту на базуючись на алгоритмі DTW та на ієрархічному агломеративному методі кластерізації;

- створено комплекс програмного забезпечення, яке реалізує розроблені обчислювальні схеми. Програмний пакет складається з двох частин. Перша частина призначена для впровадження обчислювальних схем та аналізу даних (настільна програма, написана на Java за допомогою графічного фреймворку JavaFX), а друга частина дозволяє створювати штучні траєкторії (веб-додаток, написаний з використанням JavaScript);

- розроблене програмне забезпечення застосовано до аналізу штучних траєкторій городян а також реальних даних з відкритих баз даних.

Список використаних джерел

1. Finding Popular Places / M. Benkert, B. Djordjevic, J. Gudmundsson, T. Wolle., 2007. – 15 с.

2. M. Sidorova, “Information technology of evaluation and improvement the quality of cluster analysis” in Modern Problems of Radio Engineering, Telecommunications and Computer Science - Proceedings of the 11th International Conference, TCSET'2012, February 21–24, 2012, Lviv-Slavske, Ukraine p. 390

3. Agrawal R., Imielinski T., Swami A. Mining association rules between sets of items in large databases. / Agrawal R., Imielinski T., Swami A.., 1993. – 216 с.

УДК 004.021

Пісарєв Д. С., Петрова О. О.
Харківський національний університет
міського господарства імені О.М. Бекетова

Візуалізація «backtracking algorithm»

При знаходженні оптимального рішення задачі інколи неможливо використати ні стратегію «декомпозиції», ні стратегію «динамічне програмування», ні стратегію «обхід дерев», ні інші стратегії, окрім стратегії «пошук з поверненням», або інакше стратегію «повного перебору».

Класичними задачами, які вирішуються за допомогою стратегії «пошук з поверненням» є: гра «хрестики-нулики»; задача про обхід конем шахової дошки; задача про 8 ферзів. Задача про обхід конем шахової дошки полягає в тому, щоб знайти обхід дошки розміром NxM конем, при цьому виконуючи переміщення за правилами шахової гри. При існуванні такого обходу кожне поле шахова фігура навідує тільки один раз [1].

Для рішення задачі про обхід конем шахової дошки використовуються такі методи вирішення [2]: метод Ейлера, який полягає в тому, що спочатку кінь рухається за довільним маршрутом, поки не вичерпає всі можливі ходи, а потім непройдені клітинки, що залишилися, додаються в зроблений маршрут (після спеціальної перестановки його елементів); метод Вандермонда, автор якого спробував звести задачу до арифметичної. Цей метод знаходження відповідної послідовності аналогічний методу Ейлера, але дозволяє знаходити маршрути коня тільки для дошки парної розмірності; правило Варнсдорфа, яке формулюється таким чином: при обході дошки кінь повинен перемістится на те поле, з якого можна піти на мінімальне число ще не пройдених полів. При умові наявності декількох таких полів фігура може зробити переміщення на будь-який з наявних полів. Автори [3] відмічають, що правило Варнсдорфа є найбільш простим серед багатьох евристичних методів, які використовуються для зменшення перебору.

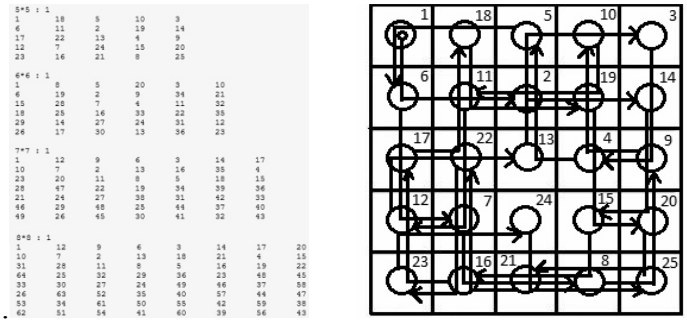


Рисунок 1 – а) результат роботи доопрацьованої програми;
б) траєкторія переміщення шахової фігури

Наведена на сайті [4] програма, яка імітує шлях коня по шаховій дошці з запам'ятовуванням на яких клітинах фігура вже побувала, щоб не повертатись до них, була доопрацьована додаванням стрічки «system("pause");» для коректної роботи програми. На рисунку 1 (а) наведено результат роботи доопрацьованої програми для шахової дошки розмірів 5x5, 6x6, 7x7, 8x8.

Для полегшення сприйняття стратегії «пошук з поверненням» виконано візуалізацію отриманих результатів з вказанням номерів використаних варіантів ходу коня на прикладі шахової дошки розміру 5x5. Алгоритм починає рух від клітини з номером 1, виконуючи перебір варіантів для знаходження рішення.

На рисунку 1 (б) наведено траєкторію обходу дошки та кінцевий шлях переміщення шахової фігури.

Список використаних джерел

1. *Вирт Н. Алгоритмы и структуры данных. / Н. Вирт.- М.: Мир, 1989.- 360 с.*
2. *Задача про хід коня [Електронний ресурс]. Доступ до ресурсу: https://uk.wikipedia.org/wiki.*
3. *Шалыто А. Задача о ходе коня / А. Шалыто, Н. Туккель, Н. Шамгунов. // Мир ПК. - 2003. - №1.- С.152-155.*
4. *Обход конём шахматной доски [Електронний ресурс]. Доступ до ресурсу: http://www.cyberforum.ru/cpp-beginners/thread1980339.html*

УДК 007.2

Пономаренко А. С.
Центральноукраїнський національний технічний університет

Місце генетичних алгоритмів у сучасному світі

На сучасному етапі розвитку комп'ютерних технологій, що забезпечують інформаційну безпеку та захист інформації, широке застосування знаходять криптографічні методи захисту, які відносяться до NP-повних задач. Для їх розв'язування сьогодні застосовують алгоритми, що ґрунтуються на законах природних систем. До таких алгоритмів відносяться генетичні алгоритми.

У процесі розв'язування задачі генетичний алгоритм поводиться так само, як поводилися б живі організми у процесі еволюції. Потенційний розв'язок подається як певна структура-особина. Кожна особина однозначно характеризується набором хромосом, яка є унікальною характеристикою, що дозволяє врахувати властивості конкретної особини в процесі еволюції. Весь генетичний алгоритм складається з таких компонент: - подання хромосом; - початкова популяція (стартовий набір хромосом); - набір операторів для генерації нових рішень з попередньої популяції; - цільова функція для оцінки пристосованості рішень; - алгоритм оцінки пристосованості хромосом

Генетичні алгоритми застосовуються для вирішення наступних задач: оптимізація функцій, оптимізація запитів в базах даних, різноманітні задачі на графах, налаштування і навчання штучної нейронної мережі,апроксимація функцій, штучне життя та біоінформатика.

Під оптимізацією розуміють процес вибору найкращого варіанту з усіх можливих. Методи математичного аналізу зручні для розв'язання цієї задачі, коли функція задається в явному вигляді і при цьому є диференційованою. Коли ж функція задається таблицею значень або має аналітично громіздку формулу, ефективними є числові методи розв'язання.Один з найбільш ефективних числових методів оптимізації функції - Метод золотого перетину, що полягає в побудові послідовності відрізків, які стягуються до точки мінімуму (максимуму) функції. На кожному кроці, за виключенням першого, обчислення значення функції проводяться лише в одній точці, яку називають золотим перетином.

Метод координатного спуску (найпростіший підхід до вирішення багатовимірних завдань) полягає в тому, що пошук ведеться на основі перебору напрямків з довільно заданої множини. Для того, щоб гарантувати можливість проведення пошуку по всій розглянутій області, доцільно накласти вимогу лінійної незалежності напрямків пошуку, які повинні утворити базис в допустимій області визначення. Звідси випливає, що розглянуті методи прямого пошуку використовують, щонайменше, незалежність напрямків пошуку і для цього використовується зручно використовувати генетичний алгоритм.

Штучне життя має справу з еволюцією агентів або популяцій організмів, які існують лише у вигляді комп'ютерних моделей, в штучних умовах. Його метою є вивчення еволюції в реальному світі і можливості впливу на її протікання, наприклад, щоб уникнути деяких спадкових обмежень. Моделі організмів також дозволяють проводити раніше неможливі експерименти (такі як порівняння еволюції Ламарка і природного відбору). Цю технологію часто використовують в Клітинних автоматах (моделювання життя) особливо внаслідок легкості масштабування і паралелізації.

Обчислювальні системи, натхнені біологічними нейронними мережами, що складають мозок тварин, навчаються задач, розглядаючи приклади, загалом без спеціального програмування під задачу. Наприклад, у розпізнаванні зображень вони можуть навчатися ідентифікувати зображення, які містять котів, аналізуючи приклади зображень, мічені як «кіт» і «не кіт», і використовуючи результати для ідентифікування котів в інших зображеннях. Вони роблять це без жодного апріорного знання про котів, наприклад, що вони мають хутро, хвости, вуса та котоподібні писки. Натомість, вони розвивають свій власний набір доречних характеристик з навчального матеріалу, який вони оброблюють.

Нейронні мережі (більш близькі до створення штучного інтелекту) можуть бути корисні для моделювання динаміки популяцій або високорозвинутих самоосвітніх організмів. Симбіоз між навчанням і еволюцією - центральна задача теорій про розвиток інстинктів вищих організмів, як наприклад в ефекті Болдуїна.

Традиційно при створенні штучного інтелекту використовується проектування від елементу до структури і від структури до елементу, тоді як штучне життя синтезується за допомогою проектування від елемента до структури.

Галузь обчислювальної біології, біоінформатика, що застосовує машинні алгоритми і статистичні методи для аналізу великих наборів біологічних даних, які, як правило, складаються з великого числа нуклеотидних (ДНК і РНК) та пептидних (білки) послідовностей і даних структури білків.

З тих пір, як в 1977 році був секвенований геном фагу Phi-X174, послідовності ДНК все більшого числа організмів були розшифровані і збережені в базах даних. Ці дані використовуються для визначення послідовностей білків і регуляторних ділянок. Порівняння генів в рамках одного або різних видів може продемонструвати схожість функцій білків або відношення між видами (таким чином, можуть бути складені філогенетичні дерева).

З зростанням кількості даних вже давно стало неможливим вручну аналізувати послідовності. В наші дні для пошуку по геномам тисяч організмів, що складаються з мільярдів пар основ, використовуються комп'ютерні програми. Цю задачу можна вирішити з використанням задачі комівояжера та використанням ГА.

Висновок: відкриваючи для себе генетичні алгоритми, серед найбільш значущих позитивних сторін, можна відзначити:

1) Якщо спосіб точного вирішення задачі невідомий, то якщо ми знаємо, як оцінити пристосованість хромосоми, то завжди можемо змусити генетичний алгоритм вирішувати цю задачу;

2) Коли спосіб для точного рішення існує, але він дуже складний у реалізації, вимагає великих витрат часу і грошей (Приклад - створення програми для складання персонального розкладу на основі техніки покриття множин з використанням лінійного програмування), то генетичний алгоритм допоможе вирішити цю задачу;

Список використаних джерел

1. *Використання генетичних алгоритмів в задачах оптимізації [Електронний ресурс]. – Режим доступу:http://ela.kpi.ua/bitstream/123456789/16458/1/10.pdf*
2. *Генетичні алгоритми. Ключовіпоняття і методиреалізації[Електронний ресурс]. – Режим доступу:https://studfiles.net/preview/5465767/*
3. *Генетичні алгоритми[Електронний ресурс]. – Режим доступу: https://www.e-olymp.com/uk/problems/3471*
4. *Генетичні алгоритми. Генетичне програмування [Електронний ресурс]. – Режим доступу: https://studopedia.su/16_182110_genetichniy-algoritm-genetichne-programuvannya.html*

УДК 004.056

Пономаренко А. С.[*]
Центральноукраїнський національний технічний університет

Класифікація атак на інформаційні системи

В нашому житті інтернет зайняв певні позиції. Важко уявити сучасний світ без соціальних мереж та великої кількості інформації. Понад 1.59 мільярда користувачів обирають соціальну мережу Facebook. Багато людей використовують месенджери, зокрема WhatsApp, Line, Facebook Messenger, Skype, Telegram та інші. В умовах швидкого розвитку глобального інформаційного суспільства й широкого використання інформаційно-комунікаційних технологій мережі Інтернет у всіх сферах життя, особливого значення набувають проблеми захисту від інформаційної агресії та деструктивного впливу на громадян України з боку окремих держав, організацій та груп осіб, які здійснюють свою діяльність на шкоду національним інтересам нашої держави. Електронні засоби масової інформації взяли на себе значну функцію з формування світогляду людей, встановлення їх ціннісних орієнтацій, поглядів, переконань та вподобань.

У реаліях сучасних інформаційних війн, для здійснення цілеспрямованого пропагандистського впливу на громадян, активно використовуються соціальні мережі. Приклади революцій в Сирії, Єгипті, Тунісі дають підстави вважати, що соціальні середовища мережі Інтернет відіграють роль організатора і координатора різного роду акцій (релігійних, політичних тощо), які відбуваються в державі. Питання ефективної протидії ворожій пропаганді та мінімізації негативного впливу в інформаційному просторі України, а також інших держав на даний час є надзвичайно актуальним. З розвитком соціокомунікативних технологій збільшуються інформаційні потоки у всесвітній мережі, аналіз яких необхідно здійснювати для проведення своєчасної та ефективної контрпропаганди. Контрпропагандист має не лише перманентно відстежувати актуальні інформаційні атаки, а й чітко знати уразливі місця, в які зазвичай б'є супротивник та способи їх захисту від деструктивного впливу. З метою зменшення витрат людської діяльності й фінансових ресурсів, автоматизації пошуку деструктивного контенту та вчасної реакції на здійснені на шкоду інформаційній безпеці акції й кампанії, виникла необхідність побудови математичного та програмного забезпечення дієвої контрпропаганди в соціальних середовищах мережі Інтернет.

Несанкціонований доступ є найбільш розповсюдженим та різностороннім видом атак на систему. Несанкціонований доступ полягає в отриманні порушником доступу до об'єкту з порушенням правил розмежування доступу, встановлених у відповідності до прийнятої в організації політики безпеки. Несанкціонований доступ використовує будь-яку помилку в системі захисту та можливий при нераціональному виборі засобів захисту, некоректному їх встановленні та настроюванні.

Сукупність втручань в інформаційну систему - це атаки на конфіденційність системи, порушення доступності, цілісності. Результатом будь-якої атаки є отримання інформації не законим шляхом, нанесення шкоди, порушення систем безпеки і отримання конфіденційної інформації. Вдала атака можлива за умови не компетентного адміністратора системи безпеки, недосконалого програмного забезпечення. Існують такі типи атак: 1) віддалене проникнення (remotepenetration); 2) локальне проникнення (localpenetration); 3) атака на відмову в обслуговуванні (denialofservice); 4) мережні

[*] Науковий керівник – Гермак В. С., викладач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету

сканери (networkscanners); 5) сканери уразливостей (vulnerabilityscanners); 6) зламувачі паролів (passwordcrackers); 7) аналізатори протоколів (sniffers); 8) спам e-mail (Mailbombing); 9) перехоплення каналу зв'язку (Man-in-the-Middle).

Дуже поширеною атакою в наш час є атака на відмову в обслуговуванні. Її мета змусити сервер працювати невірно або не відповідати на запити. Цей спосіб атак є підмогою ініціалізації інших. Деякі програми через помилки в своєму коді можуть викликати виняткові ситуації, і при відключенні сервісів здатні виконувати код, наданий зловмисником або атаки лавинного типу, коли сервер не може обробити величезну кількість вхідних пакетів(наприклад DoS-атака).

Ще один поширений вид атаки це аналізатор трафіку. Він заснований на роботі мережевої карти в режимі promiscuousmode, а також monitormode для мереж Wi-Fi. В такому режимі всі пакети, отримані мережевою картою, пересилаються на обробку спеціальному додатку, званому сніффером. Після таких дій злочинець має доступ до службової, конфіденційної інформації: логінів, паролів співробітників, які використовуються для не законного проникнення під видом звичайного робітника компанії.

Наступний вид атаки «людина посередині». Це коли зловмисником перехоплюється канал зв'язку між двома системами, в результаті цього він отримує доступ до всієї інформації, що передається. При виконані цих дій зловмисник може внести зміни в інформацію потрібним йому чином, щоб досягти своєї цілі. Результатом такої атаки може бути незаконне фальсифікування переданої інформації, або ж отримання доступу до особистих даних. Вкрай складно відстежити такі атаки , тому що зловмисник знаходиться всередині мережі.

Наразі виникла потреба підготовки профільних фахівців для захисту інформації від незаконного вторгнення. У зв’язку з подіями на сході і півдні України останнім часом питання про підготовку фахівців постало особливо гостро.

Висновок: В сучасному світі дуже швидко набувають популярності соціальні мережі, збільшується кількість користувачів. Різностороння аудиторія в соціальних мережах потрапляє під вплив різноманітної інформації, яка використовується як інструментарій ведення інформаційних війн, також здійснює вплив на громадську думку. Але є і певні позитивні наслідки. Соціальні мережі сприяють механізму громадської самоорганізації і суттєво підвищують ймовірність виникнення громадського суспільства. Нові форми комунікації держави і суспільства створюють передумови розвитку інститутів і організацій громадянського суспільства, які забезпечують нарощування соціального капіталу всіх учасників певної комунікації. У той же час не можна не відзначити негативні моменти впливу соціальних мереж на свідомість людини. Користувач комп’ютера схильний до аддикції, тобто залежності від соціальних мереж та Інтернету загалом, адже при використанні мережі він знаходиться в зміненому стані свідомості – своєрідному психологічному трансі, в якому реальність набуває нечітких рис і зливається з віртуальністю. А це сприяє несвідомому засвоєнню всього, що дає нам мережа – новин, повідомлень, фотографій, відео. Користуючись певними методами, можна легко переконати звичайного користувача у будь-чому, незалежно від його соціального статусу чи місцезнаходження.

Список використаних джерел

1. *Зеленін В. В. По той бік правди: НЛП як зброя інформаційно-пропагандистської війни / В. В. Зеленін. – Вінниця: ТОВ «Віндрук», 2014. – 384 с.*
2. *Інформаційна війна [Електронний ресурс]. – Режим доступу: http://www.bezpeka.com/ru/lib/spec/law/methods-information-warfare.html*

УДК 004.896

Проніна О. І.
ДВНЗ «Приазовський державний технічний університет»

Формалізація організації заказу в умовах індивідуальних потреб клієнта

В сучасному світі робота будь-якої організації, не залежно від її розміру пов'язана з щоденним прийняттям рішень. Функціональність організації щільно пов'язана з розробкою, прийняттям і реалізацією управлінських рішень. Оскільки від цього залежить конкурентоспроможність, та ефективність організації, а значить і фінансовий стан організації в цілому [1]. Зазвичай прийняття рішень стосується насамперед управлінських рішень, але щоденно людина стикається з питаннями, коли необхідно прийняти рішення в звичайному повсякденному житті.

В житті людини, як і в будь якій організації, прийняття рішень є найважливішим етапом, який визначає її майбутній розвиток та достаток. У повсякденному житті людина стикається з прийняттям рішення постійно, будь то вибір товару в інтернет магазині, чи в просто магазині. Оскільки кількість товарів величезна, то проблема вибору та підбору під свої потреби стоїть достатньо гостро. Крім вибору товару людина, як клієнт стикається з вибором майстра для здійснення послуги [2].

В моделі представлення замовлення кожне замовлення включає в себе інформацію о клієнті, що ініціює замовлення, послугу, що необхідно виконати, та інформацію о виконавці, який буде виконувати замовлену послугу. Послуга – це робота, яка виконується на замовлення.

Для опису оперативного вирішення завдання (замовлення) використовуються множини: «послуги», «клієнти» та «виконавці». Формально замовлення представляється кортежем:

$$Z = \left\langle \{K\}, \{p_l^K\}_{l=1}^5, \{O\}, \{p_b^O\}_{b=1}^7, \{P\}, \{p_k\}_{k=1}^n \right\rangle, \quad (1)$$

де $\{K\}$ - множина клієнти, $\{p_l^K\}_{l=1}^5$ - множина атрибутів, що характеризують клієнта; $\{O\}$ - множина виконавці, $\{p_b^O\}_{b=1}^7$ - множина атрибутів, що характеризують виконавця; $\{P\}$ - множина послуги $\{p_k\}_{k=1}^n$ - множина атрибутів, що характеризують послугу.

Множини $\{K\}, \{O\}, \{P\}, \{p_l^K\}_{l=1}^5, \{p_b^O\}_{b=1}^7, \{p_k\}_{k=1}^n$ є складові множини замовлення.

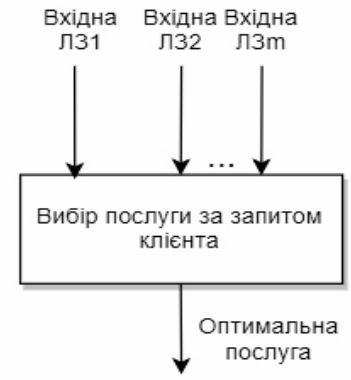
Множина клієнти $\{\mathrm{K}\}$ використовується при описі формування замовлення на здійснення послуги і має наступну множину атрибутів $\{p_i^K\}_{i=1}^5$: p_1^K – ідентифікатор клієнта, p_2^K – номер телефону, p_3^K – ім'я клієнта, p_4^K – поточна геолокація, $\hat{p}_5^K$ – вимоги до послуги. Атрибут $\hat{p}_5^K$ – вимоги до послуги, для кожної окремої послуги може мати різні значення у тому числі лінгвістичні, а також кілька значень для однієї послуги. Даний перелік атрибутів встановлює клієнт, як свої унікальні потреби але аналізуючи цій параметр, можна зробити висновки, що багато клієнтів має схожий набор значень параметрів, чи повністю ідентичний.

Множина виконавці $\{O\}$ має наступну множину атрибутів $\{p_i^O\}_{i=1}^4$: p_1^O – ідентифікатор виконавця, p_2^O – номер телефону, p_3^O – ім'я виконавця, p_4^O – поточна

геолокація, p_5^O – послуги, що надаються, p_6^O – ціна послуги, p_7^O – рейтинг виконавця. Дані атрибути характеризують виконавця та відрізняють його від інших виконавців.

Множина «послуга» $\{P\}$ може володіти будь яким набором параметрів, що її характеризують. Аналіз позволив виявити параметри які в найбільшій ступені присутні при описі послуги за запитом клієнта. Дана множина володіє переліком обов'язкових параметрів $\{p_k\}_{k=1}^{n}$: p_1,– ціна послуги, p_2- розташування виконавця щодо клієнта, p_3- рейтинг виконавця послуги, та може мати n-3 додаткових параметрів відносно категорії послуги, яка аналізується. В момент, коли клієнт серед множини послуг обирає собі найбільш підходящу, з виконавцем, що надає цю послугу, можна отримати всі відомості про створене замовлення. Можна встановити де саме виконується замовлення (координати замовлення), яка послуга буде надаватися, вартість послуги, час початку виконання замовлення, ціна та тощо.

Подання процесу вибору оптимального послуги по запиту клієнта має нечіткий висновок з лінгвістичними змінними вхідних даних, що реалізується в кожній окремій моделі прийняття рішень за обраним параметром з урахуванням початкових даних вибору [3]. Крім даних лінгвістичного типу, можуть надходити дані чіткого типу – числові. При аналізі особливостей рішення задач оптимального вибору послуги, було виявлено, що в умовах нечітких даних структура процесу прийняття рішень може бути як одно-етапною, так і двоетапною чи n-етапною (рисунок 1). Багатоетапне прийняття рішень з паралельним чи послідовним застосуванням моделей нечіткого логічного висновку [4] на кожному етапі дозволяє встановити вид структури моделі для вирішення задач вибору оптимальної послуги за запитом клієнта, рисунок 1 б.



а) Процес вибору послуги, якій складається з одного етапу

б) Процес вибору послуги, якій складається з n-етапів

Рисунок 1 а, б) – Подання процесу вибору послуги

Вибір послуги для клієнта може складатися з кількох етапів, так на першому етапі обирається сама послуга, потім обирається за першим ключовим параметром виконавці, а далі якщо у клієнта декілька ключових параметрів то етапів буде кілька. При вирішенні завдання надання послуг на всіх етапах можуть бути ситуації, коли клієнту треба прийняти рішення з урахуванням багатьох факторів. Які фактори слід вважати найбільш важливими, залежить від якісних особливостей об'єктів послуги і цілей, які переслідує клієнт.

Структура моделі для вирішення задач підбору послуги (рисунок 1) містить n послідовних етапів. Прийняття рішень на і-му етапі впливає на прийняття рішення на наступному (і + 1) -м етапі. Отже відбувається механізм послідовного нечіткого вибору рішень. На кожному і-му, $i = \overline{1,n}$, етапі можливо паралельне застосування кількох моделей нечіткого логічного висновку, загальне число яких дорівнює m_i. Паралельне застосування моделей дозволяє отримати результати нечіткого логічного висновку, які перетворюються в нечіткі вихідні дані для моделей подальшого (і+1)-го етапу багатоетапної моделі для вирішення задач підбору оптимальної послуги. Результати моделей прийняття рішень на і-му етапі розглядаються як лінгвістичні змінні, які обираються для моделей нечіткого логічного висновку (і+1) -го етапу. На останньому n-му етапі формується рішення про оптимальність послуги. На кожному етапі може визначатися вихідна змінна, на основі вхідних лінгвістичних змінних. Після кожного етапу вихідна зміна, яка стає вхідною змінної лінгвістичного типу. Процес отримання змінних відбувається за допомогою моделі нечіткого вибору [3].

На рис. 1 існує поєднання механізмів послідовного і паралельного виборів, тому в роботі [4] це названо механізмом послідовно-паралельного нечіткого вибору. Отримання вихідної лінгвістичної змінної послідовно здійснюється по кожному j-у етапу, паралельно іншим етапом на цьому рівні, відбувається це на кожному етапі вирішення задачі, а потім остаточний висновок робиться на заключному, n-му етапі рішення вибору оптимальної послуги.

На основі розробленої моделі замовлення, була створена двоетапна модель вибору оптимальної індивідуальної міської поїздки, яка основується на нечіткому виводі, з лінгвістичними змінними, результати досліджень наведені в роботі [5].

На основі проведеного аналізу створено модель замовлення, що включає в себе множину клієнтів, виконавців та послуг, які вони представляють. Використання розробленої моделі замовлення полегшує підбір виконавця для клієнта по його запиту. Тим самим мінімізує участь людини та спрощує вибір. В роботі приведено схему процесу вибору оптимальної послуги за запитом клієнта, яка може складатися з будь якої кількості етапів.

Список використаних джерел

1. *Петруні Ю. Є. Прийняття управлінських рішень навчальний посібник / Ю. Є. Петруня, Б. В. Літовченко, Т. О. Пасічник, – 3-тє вид., переробив. і доп. – Дніпропетровськ : Університет митної справи та фінансів, 2015. – 209 с.*
2. *В Украине быстро растет спрос на услуги [Електронний ресурс] // Forbes Украина. – 2012. – Режим доступу: http://forbes.net.ua/news/1335886-v-ukraine-bystro-rastet-spros-na-uslugi.*
3. *Леоненков А. В. Нечеткое моделирование в среде MATLAB и fuzzy TECH / А. В. Леоненков. – СПб. : БХВ-Петербург, 2005. – 736 с.*
4. *Косолапов А. А. Методика оценки надежности нечетких систем с ииспользованиием различных видов размытых множеств / А. А. Косолапов // Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2013 – № 2 (44). – С. 17 – 27*
5. *Пронина О. И. Формализованное представление индивидуальной городской поездки на основе лингвистических переменных / О. И. Пронина // Вісник Харківського національного університету Повітряних Сил ім. Івана Кожедуба «Системи обробки інформації», 2017. – № 1 (151). – С. 39 – 47.*

УДК 004.65

Пронюк М. Я., Кропивницька В. Б.
Івано-Франківський національнийтехнічний університет нафти і газу

Порівняльний аналіз баз даних SQL та NoSQL

Сьогодні стрімкий ріст комп'ютерних та Інтернет технологій створює проблему ефективного зберігання та отримання даних. Дуже великі кількості онлайн транзакцій приводять до великих об'ємів даних, які потребують добре організованих рішень. Бази даних відіграють вирішальну роль при зберіганні та обробці даних. При проектуванні інформаційних систем однією з головних проблем, з якими стикається розробник є проблема вибору способу зберігання даних.

Розглянемо сильні та слабкі сторони двох популярних баз даних, які набули широкого використання останнім часом SQL та NoSQL з точки зору продуктивності, надійності та масштабованості. У більшості випадків NoSQL бази даних мають вбудовані засоби для більш зручної маніпуляції конкретним типом даних, тому такі СУБД доцільно використовувати при збережені та обробці великих обсягів даних. Зазвичай, дані, які там зберігаються є ненормалізовані, тому не має потреби у додаткових запитах для отримання необхідної інформації про певну сутність, натомість всі необхідні дані зберігаються як одне ціле. Крім того, для збільшення продуктивності застосовується кешування даних в системній пам'яті.

В свою чергу бази даних SQL зберігають дані у нормалізованому вигляді, тобто кожна сутність у системі зберігає свої дані у окремій таблиці і для отримання таких даних потрібно об'єднувати таблиці, що часто є відносно довготривалою операцією. Однак варто сказати, що продуктивність буде залежати від розміру бази даних і запитів до бази даних, які використовуються у веб-системі. Для середніх, великих об'ємів(1000 - 1000000) даних, у яких є чітка структура, буде доцільнішим використання SQL баз даних, але коли кількість інформації, що зберігається починає обчислюватися в десятках терабайт, виникає необхідність у використанні декількох фізичних серверів, в такому випадку доцільно використовувати NoSQL баз даних.

З точки зору надійності перевага надається SQL базам даних. Це відбувається за рахунок чіткої схеми таблиць та типів даних для колонок. Для забезпечення надійності SQL бази даних забезпечують відповідність властивостям ACID – атомарності, узгодженості, ізольованості та довговічності. В свою чергу NoSQL бази даних намагається дотримуватись властивостей теореми CAP – узгодженості даних, доступності та стійкості до розділення. Для того щоб забезпечити надійність та цілісність даних у NoSQL базах даних потрібно написати багато коду, який буде відрізнятися у різних видах NoSQL базах даних, в той час як всі SQL бази даних використовують дуже схожий синтаксис для надійного та цілісного збереження даних.

В цілому NoSQL бази даних мають значно більші можливості для масштабованості, оскільки для них характерна вертикальна(збільшення потужності апаратної частини сервера) та горизонтальна масштабованість(дані зберігаються розподілено на багатьох серверах). Горизонтальна масштабованість означає, що дані можуть бути розтащовані розподілено на багатьох серверах. Для SQL баз даних характерна тільки вертикальна масштабованість.

Висновки. Ми порівняли SQL та NoSQL баз даних. Якщо узагальнити дослід, то NoSQL бази даних підходять для високонавантажених веб-додатків з великими об'ємами даних, де потрібен високий рівень масштабованості та продуктивності, тоді як SQL бази даних мають переваги у простості підтримки, забезпечення надійності та цілісності даних, а також зберігають хорошу продуктивність для середньої та великої кількості даних. Дане порівняння може дати чіткіше розуміня як розробляти продуктивні, надійні та масштабовані веб-додатки.

УДК 004

Рідозуб О. В.
Харківський національний університет імені В. Н. Каразіна

Розробка базових підходів до створення програмного забезпечення для роботи з напівпровідниковими детекторами CdTe, CdZnTe

Кількість поглиненої енергії іонізуючих випромінювань людським організмом радикально впливає на ступінь променевих уражень його функціональних органів. Тому коректний вимір дози опромінення і пошук шляхів збільшення точності або зменшення невизначеності виміряних і обчислених дозиметричних величин є актуальною проблемою. Пошук шляхів вирішення цієї проблеми йде в напрямку поліпшення параметрів детекторів, удосконалення характеристик електронних модулів детектуючих систем і створення програмного забезпечення (ПЗ) для управління процесом детектування, збором інформації, її цифрової обробки і адекватного представлення користувачам в on-line режимі. При розробці ПЗ необхідно враховувати особливості взаємодії іонізуючого випромінювання з матеріалами і об'єктами, які опромінюються. Зокрема, потрібно врахування їх гетерогенності і енергетичної залежності чутливості детекторів - так званий "хід з жорсткістю" - в широкому діапазоні енергій і інтенсивностей випромінювання, що є нетривіальною задачею.

Одним з можливих шляхів корекції енергетичної залежності CdTe і CdZnTe детекторів, для дослідження яких передбачається написання програмного коду, є аналіз і врахування апаратурного спектра, відповідного енергетичного спектру реального випромінювання. Для цього до складу дозиметричної апаратури включається багатоканальний амплітудний аналізатор, з якого число імпульсів і їх амплітудне розподілення протягом часу експозиції, подається на цифровий сигнальний процесор і в режимі реального часу обробляється спеціальною програмою. Експозиційна доза D_{exp} програмно обчислюється за формулами [1]:

$$D_{exp} = N_t(M\ E_{ph} + C)$$
$$E_{ph} = \{[\sum_k kN(k)]/N_t\}E_{adc}\ ,$$

де N_t - загальне число імпульсів за час експозиції в обраному діапазоні енергій, M і C - константи, які визначаються при калібруванні детектора, E_{ph} - енергетичний еквівалент середньої амплітуди імпульсів, N (k) - число імпульсів в каналі k, E_{adc} - ціна каналу аналого-цифрового перетворювача в багатоканальному амплитудном аналізаторі.

Обчислене значення експозиційної дози передається по одному з інтерфейсів в комп'ютер системи дозиметрії.

Крім програми обчислення експозиційної дози для повноцінної роботи апаратури необхідні програмні модулі адаптивного управління напругою зміщення детекторів, підбору постійних часу формуючих ланцюгів, установки коефіцієнтів посилення та інші, в тому числі сервісні програми.

Для публічного використання інформації з вимірювальної дози, спектрального складу випромінювання, параметрів детекторів і спектродозіметріческой апаратури дуже корисним апаратно-програмним рішенням для проекту, що виконується, є інтеграція локальних рішень з хмарними технологіями, такими, як сервіс для прийому, аналізу та візуалізації даних ThingSpeak. Сервіс має безкоштовну версію і вбудований пакет MATLAB - високорівнева мова і інтерактивне середовище для програмування, чисельних розрахунків і візуалізації результатів, за допомогою якого можна аналізувати дані, розробляти алгоритми, створювати моделі і додатки.

Сполучення апаратури, наприклад, дозиметра, здійснюється за наведеною на рис.1 схемою. Для цього в прилад вбудовується електронний модуль ESP8266 - мікроконтролер з інтерфейсом Wi-Fi. Перша версія програмного забезпечення н розроблена і знаходиться в стадії налагодження.

Схема, яка розроблена, особо корисна для навчальних цілей. За допомогою такого рішення студенти матимуть зі смартфонів віддалений доступ до дослідницької апаратури і вільно користуватися для розрахунків таким потужним інструментом, як MATLAB і SIMULINK.

Рисунок 1 – Схема інтеграції спектродозіметріческой апаратури з хмарним сервісом

На рис.2 наведено очікуваний у вікні смартфону вид спектра гамма-квантів від ^{137}Cs (662 кеВ), отриманий за допомогою $C_{d0.9}Zn_{0.1}Te$ детектора.

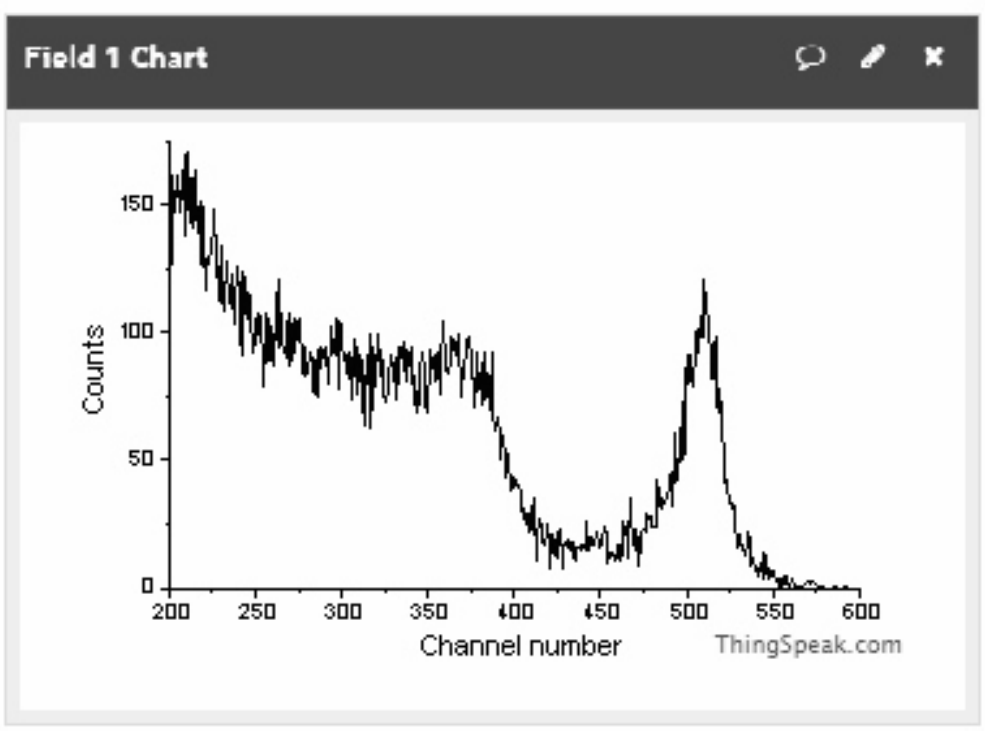


Рисунок 2 – Очікуваний у вікні смартфону вид спектра гамма-квантів від ^{137}Cs

Список використаних джерел

1. Захарченко А.А. Моделирование дозиметрических свойств детекторов гамма излучения на основе высокоомных полупроводников. Диссертация на соискание канд. физ. – мат. наук. Харьков, 2009.

УДК 004.93'12

Рудакова Є. О.
Дніпровський національний університет імені Олеся Гончара

Інформаційна система ідентифікації рослин

Складно уявити повноцінно функціонуюче суспільство, яке не користується рослинними ресурсами. Рослини грають масштабну роль не тільки у сільськогосподарській галузі, але й також у паливно-енергетичному комплексі, медицині, екології та інтер'єрі. У таких умовах гостро постає проблема ідентифікації тої чи іної рослини. Експертна система ідентифікації рослин – це спосіб спростити життя науковців, мандрівників, фермерів або навіть звичайної людини. Будь-хто, маючи можливість зробити фотографію квітки або листка, може отримати повну інформацію про рослину, що бачить перед собою.

Така задача, як розпізнання рослин (тварин, грибів тощо) по фото, має свої специфічні складності. Оптимальним вирішенням задачі ідентифікації рослини є ідентифікація окремих її частин (листя, квітки, плоду тощо) і подальше знаходження перетину множин результатів.

Розглядаючи задачу ідентифікації на зображенні листа чи квітки, можна виділити ряд моментів, врахування яких важливе для успішного розв'язку: масштаб, локалізація об'єкту на певній частині зображення, фон і шуми, проекція, обертання і кут зору. Найбільш актуальним методом до розпізнавання рослини є пошук ключових точок на зображенні. Основна ідея будь-якого алгоритму пошуку ключових точок полягає у виділенні на зразку певних точок і невеликих ділянок навколо них. Наприклад, це можуть бути краї ліній, невеликі кола, різкі перепади освітленості, кути тощо. Стосовно рослин, це можуть бути контури листа, його з'єднання, серединка квітка.

Найбільш популярні алгоритми пошуку ключових точок на даний момент – це алгоритми SURF, SIFT та FREAK. Ці алгоритми є порівняно новими та виникли унаслідок розвитку таких ранніх алгоритмів, як алгоритми Харріса та Ші-Томасі. Важливими властивостями алгоритму SURF у даній задачі є інваріантність до повороту та масштабу, а також краща, порівняно з алгоритмом SIFT, швидкість.

Оскільки ключові точки сильно відрізняються від основної маси точок, то їх кількість буде істотно менше, ніж загальна кількість точок зразка. Надалі цю множину точок та їх дескрипторів необхідно передати до алгоритму машинного навчання, щоби у подальшому використовувати у задачі ідентифікації.

У рамках даної роботи була розроблена веб-система ідентифікації рослин, у якій були використані методи машинного навчання, а також алгоритми SURF, SIFT та FREAK. Дана система дає можливість завантажити своє зображення листка чи квітки та відповідно класифікувати рослину за допомогою цих зображень.

Як висновок, можна сказати, що застосування методу SURF та машинного навчання дає можливість дати порівняно точний результат у задачі класифікації рослини, будучи інваріантним до повороту і масштабу зображення, у той час маючи порівняно високу швидкість. Були розглянуті також інші алгоритми та методи та основні підходи до розпізнавання зображень.

Список використаних джерел

1. *Herbert Bay, Andreas Ess, Tinne Tuytelaars, Luc Van Gool, "SURF: Speeded Up Robust Features", Computer Vision and Image Understanding (CVIU), Vol. 110, No. 3, pp. 346--359, 2008*
2. *Distinctive Image Features from Scale-Invariant Keypoints – David Lowe, Computer Science Department, University of British Columbia, 2004*
3. *Васильева И.К. Методы распознавания образов: учебн. пособ. по лабораторному практикуму / И.К. Васильева, П.Е. Ельцов. – Х.: Нац. аэрокосм. ун-т «Харьківський авиаційний. інститут», 2008. – 56 с.*

УДК 004.8

Савчук Т. О., Приймак Н. В.
Вінницький національний технічний університет

Інформаційна технологія пошуку асоціативних правил при розробці програмного забезпечення

Програмне забезпечення (ПЗ) – це комп'ютерні програми та дані, що зберігаються в цифровому вигляді та використовуються для вирішення визначених задач певного класу [1]. Розробка ефективного сучасного програмного забезпечення повинна здійснюватися організовано та відповідно до запланованих графіків, тому менеджери проектів повинні максимально точно спрогнозувати дату випуску кінцевого програмного продукту або оцінити час, необхідний для реалізації нового функціоналу та виправлення помилок.

Метою даного дослідження є створення інформаційної технології пошуку асоціативних правил при розробці програмного забезпечення, яка зменшить тривалість пошуку таких правил.

Різноманітні технології (табл. 1) розробки програмного забезпечення базуються на відповідних методах, методологіях та засобах програмування і допомагають в управлінні проектуванням систем.

Таблиця 1 – Порівняльна характеристика технології розробки програмного забезпечення

Назва	Переваги	Недоліки
JAD	– накопичується і досліджується велика кількість інформації; – менеджер проекту приймає рішення.	– необхідність у плануванні достатньої кількості зустрічей між замовником і командою розробки; – на проекті можуть працювати лише досвідчені розробники.
RUP	– немає необхідності у визначені тривалості окремих етапів; – розроблені компоненти можна використовувати повторно.	– етапи розробки ПЗ не завжди організовані; – безперервна інтеграція може викликати плутанину під час розробки ПЗ.
FDD	– можливість швидко створювати великі проекти; – відповідає стандартам, створеним індустрією розробки програмного забезпечення.	– неможливо застосовувати для малих проектів; – клієнти не можуть переглянути програмне забезпечення під час його розробки.
CA	– використання сучасних та уніфікованих засобів розробки ПЗ.	– відсутність налаштування на рівні бази даних; – неможливість прийняття рішення щодо процесів прийняття управлінських рішень для узгодження бюджету та стратегії.

Описані технології розробки програмного забезпечення не забезпечують пошук асоціативних правил, які можуть бути використанні для визначення часу необхідного на виконання завдання певним розробником. Тому розробка відповідної інформаційної

технології є актуальною задачею.

Задача пошуку асоціативних правил при розробці програмного забезпечення, може бути сформована таким чином [2]: Dev_j – це j - ий розробник, $Task_i$ – це i - те завдання, що має ряд характеристик та буде вирішене j - м розробником, а t_{i_j} – час необхідний на розв'язання i - го завдання j - им розробником. Отже, необхідно знайти асоціативні правила, що описуються виразом: $Task_i \cup Dev_j \rightarrow t_{i_j}$, $Task_i \cup Dev_j \cap t_{i_j} \rightarrow \varnothing$.

Інформаційна технологія пошуку асоціативних правил при розробці програмного забезпечення представляє собою набір методів, програмного-технологічних засобів пошуку АП, об'єднаних у технологічний ланцюг (рисунок 1). В основі запропонованої інформаційної технології, лежить відповідна інформаційна модель процесу пошуку АП при розробці програмного забезпечення [3].

Основні кроки, що необхідно виконати при розробці ПЗ, з метою генерації асоціативних правил наступні:

1. Завантаження вхідних даних про завдання, що виконуватимуться під час розробки ПЗ, для навчання алгоритму класифікації даних.
2. Навчання алгоритму класифікації C 4.5, для подальшого його використання при класифікації завдань, серед який необхідно знайти АП.
3. Завантаження вхідних даних, що представлені завданнями, серед яких потрібно знайти асоціативні правила.
4. Класифікація вхідної множини завдань, серед яких необхідно знайти асоціативні правила, на три класи в залежності від складності їх виконання для розробника.
5. Обрахунок значення мінімальної підтримки для кожної групи завдань *minsupp* і внесення значення мінімальної достовірності *minconf* експертом, в ролі якого виступає менеджер проекту.
6. Для кожної групи завдань виконувати пункти 7 – 11.
7. Перетворення даних у кожному із класів на деревовидну структуру даних, за допомогою алгоритму пошуку асоціативних правил FPG.
8. Генерація частих предметних наборів та підрахунок значення підтримки *supp* для кожного із них.
9. Відбір лише тих частих предметних наборів, у яких значення підтримки *supp* більше або дорівнює значенню мінімальної підтримки *minsupp*.
10. Генерація асоціативних правил із відібраних частих предметних наборів та обрахунок значення достовірності *conf* для кожного із них.
11. Відбір АП наборів, у яких значення підтримки *conf* більше або дорівнює значенню мінімальної підтримки *minconf*.
12. Запис відібраних з кожного класу асоціативних правил до загальної бази даних.
13. Подання збережених АП користувачу для подальшого їх використання при плануванні розробки програмного забезпечення.

З метою підтвердження ефективності використання запропонованої інформаційної технології пошуку асоціативних правил при розробці програмного забезпечення було проведено експеримент з її використанням та без неї. Результати експерименту показали, що: різниця між часом, що витрачається на пошук асоціативних правил без застосування розробленої інформаційної технології та з її використанням, збільшується зі збільшенням загальної кількості тестових даних; при кількості елементів до 100 швидкість пошуку АП з використанням розробленої ІТ виросла на 0,001сек (0,35%), при

кількості елементів до 500 – зросла на 0,074сек (1,2%), при кількості елементів до 1000 – зросла на 0,252 сек (2%);

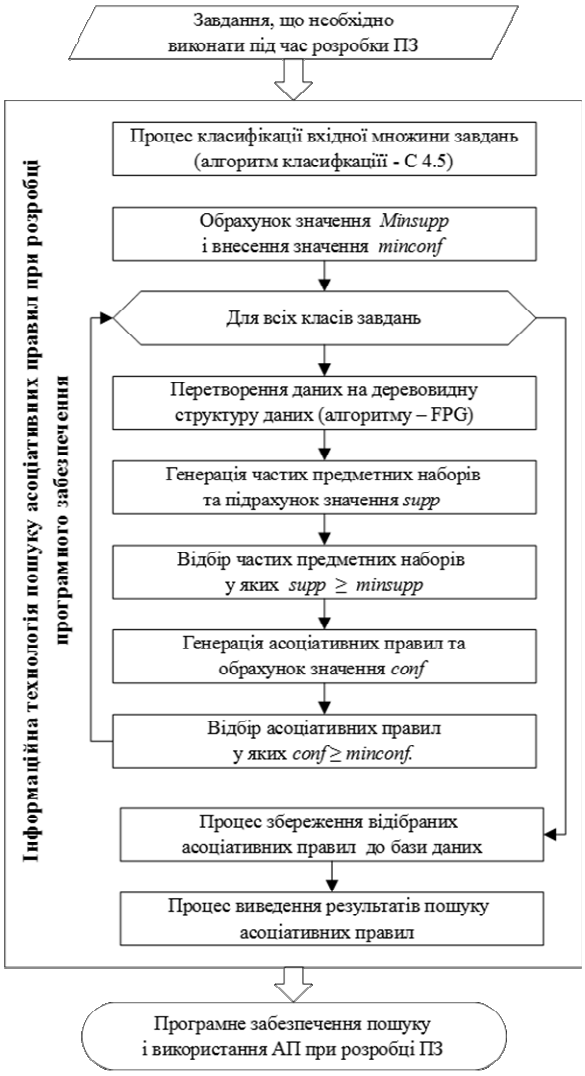


Рисунок 1 - Структура інформаційної технології пошуку асоціативних правил при розробці програмного забезпечення

Таким чином, використання розробленої інформаційної технології пошуку асоціативних правил під час розробки ПЗ є доцільним у випадку коли загальна кількість завдань, серед яких потрібно шукати асоціативні правила, понад 500 елементів.

Отже, розроблено інформаційну технологію пошуку асоціативних правил під час розробки програмного забезпечення, використання якої дозволяє скоротити час пошуку асоціативних правил та підвищити їх інформативність, що підтверджено проведеним експериментом.

Список використаних джерел

1. *Батоврин В. К. Толковый словарь по системной и программной инженерии / В. К. Батоврин. – М: ДМК Пресс, 2012. – С. 280.*
2. *Zhang H. Predicting Bug-Fixing Time: An Empirical Study of Commercial Software Projects / H. Zhang, L. Gong, S. Versteeg // 35th International Conference on Software Engineering (ICSE) – San Francisco, CA, 2013. – С. 1042 - 1051.*
3. *Савчук Т. О. Розробка інформаційної моделі процесу пошуку асоціативних правил при розробці програмного забезпечення/ Т. Савчук, Н. Приймак // Інформаційні технології та комп'ютерна інженерія, № 2, – Вінниця: ВНТУ, 2018. – С. 43-48.*

УДК 004

Семенченко О. А.
Харківський національний університет радіоелектроніки

Аналіз розвитку інформаційних систем у світі

На даний етап розвитку автоматизації українські підприємства суттєво відстають від рівня західних компаній. Для аналізу причин такого значного відставання і можливості оцінити реалії сучасної ситуації, яка склалася на сьогодні з впровадженням інформаційних систем та інформаційних технологій слід розглянути еволюцію розвитку автоматизованих інформаційних систем на заході.

Інформаційна система — сукупність організаційних і технічних засобів для збереження та обробки інформації з метою забезпечення інформаційних потреб користувачів.

До інформаційної системи входять люди, обладнання, процеси, процедури, дані та операції. До них можна віднести всі форми письмового спілкування всередині підприємства (доповіді, звіти, бюлетені та службові записки), а також всі електронні інформаційні засоби (електронну пошту та селекторні і телевізійні наради).

Кожна інформаційна система має такі компоненти:

- структура системи — множина елементів системи і взаємозв'язків між ними. (наприклад, організаційна і виробнича структура підприємства);
- функції кожного елемента системи (наприклад: управлінські функції — прийняття рішень у певних структурних підрозділах підприємства);
- вхід і вихід кожного елемента і системи в цілому. (наприклад: матеріальні або інформаційні потоки, які надходять у систему або вводяться нею);
- мета й обмеження системи та її окремих елементів. (наприклад: досягнення максимального прибутку; фінансові обмеження).[1]

Перші інформаційні системи з’явилися у 1950-х рр. Ще тоді вони були призначені для обробки рахунків і розрахунку заробітної плати, а реалізовувалися на електромеханічних бухгалтерських рахункових машинах.

Це приводило до деякого скорочення витрат і часу на підготовку паперових документів.

Шістдесяті роки знаменуються зміною відношення до інформаційних систем. Інформація почала застосовуватися для періодичної звітності за багатьма параметрами. Для цього організаціям потрібне комп’ютерне устаткування широкого призначення, здатне обслуговувати безліч функцій, а не тільки обробляти розрахунки і рахувати зарплату.[2]

У 1970-х – початку 80-х років інформаційні системи починають широко використовуватися як засіб управлінського контролю, підтримуючий і прискорюючий процес ухвалення рішень. [3]

Також впроваджуються моделі стадій розвитку інформаційних систем мала кілька послідовних версій (1973, 1974, 1977 і 1979 рр.), перша з яких включала чотири стадії, а остання - шість, у тому числі:

- Початкову. Обчислювальна техніка застосовується дуже мало, контроль за її застосуванням здійснюється недостатньо, а планування цього застосування є мінімальним.
- Розширення. Застосування обчислювальної техніки швидко поширюється, посилюється його підтримка з боку керівництва, зростає відповідна зацікавленість з боку споживачів. Витрати на обчислювальну техніку швидко зростають, однак рівень якості проектів, автоматизації залишається невисоким, спостерігаються недоліки у плануванні.

- Управління. Управління процесами автоматизації і контроль за ними стають більш послідовними, починає застосовуватись нова техніка передачі даних, увага керівництва переноситься з управління обчислювальними ресурсами на управління ресурсами даних.

- Інтеграції. Поглиблюється підготовка керівництва у галузі комп'ютеризації і управління нею, управління все більше вдосконалюється. Здійснюється впровадження баз даних, в результаті чого посилюється тенденція до управління ресурсами даних.

- Управління даними. Головна увага зосереджується на управлінні даними, управління обчислювальними ресурсами вдосконалюється. Разом з тим розвиток систем, що приносять підприємству безпосередню користь, здійснюється поволі.

- Зрілості. Застосування обчислювальної техніки є цілісним комплексом, структура якого відображає організацію інформації на підприємстві та її потоки, використовується нова техніка управління комп'ютеризацією, у здійсненні якої беруть безпосередню участь всі пов'язані з цим процесом.

Основні ідеї теорії стадій розвитку інформаційних систем одержали подальше втілення в теорії асиміляційних фаз інформаційних технологій. Цю теорію, що трактує проблему інтеграції трьох інформаційних технологій автоматизації управлінської праці, обробки даних і телекомунікацій, розробили Дж. Маккінні і Ф.Макфарлан, які опублікували результати своїх досліджень у 1982 р. Автори виділяють чотири фази асиміляції інформаційних технологій:

1. Прийняття рішення про інвестиції в нову технологію і про її перевірку.
2. Освоєння технології та її адаптацію.
3. Управління використанням технології і контроль за ним.
4. Широкий трансфер технології.
5. Характеристики окремих фаз такі:

Фаза 1. Передбачається здійснення 1-2 експериментальних проектів, а також навчання споживачів.

Фаза 2. Успішно опробувань технологія застосовується для вирішення нових задач (типів задач), що виходять за рамки тих, які вирішуються на 1-й фазі.

Фаза 3. У разі успішного вирішення задач 2-ї фази у ході подальшого розвитку здійснюються: поширення застосування технології, організація управління, вдосконалення проектування і впровадження інформаційних систем. При занадто жорсткому управлінні, контролі ефективності і стандартизації має місце стагнація, що призводить до обмеження можливості інновацій.

Фаза 4. Застосування технології поширюється на інші ланки діяльності підприємства або організації.

Таким чином, технології, що забезпечують можливість переходу до нових умов застосування інформаційних систем або до здійснення реструктуризації, впроваджуються поступово. Оскільки у певний момент окремі технології можуть знаходитися у різних фазах асиміляції, необхідним є додержання таких правил:

- технології, які знаходяться на 1-й або 2-й фазі асиміляції, повинні бути організаційно відокремлені від тих, що знаходяться на 3-й або 4-й фазі;

- з метою накопичення технічного досвіду при здійсненні інтеграції інформаційних технологій необхідна певна поступовість;

- на 2-й фазі може виявитися доцільним, хоча це і неефективно, розподіл технологій між споживачами із встановленням на наступних фазах більш ретельного контролю і здійсненням організаційних змін.

У 1988 р. Л. Джаз, М.Мавро і Б.Мартін на основі серії емпіричних досліджень розробили проект моделі стадій розвитку інформаційних систем з позицій

використання комп’ютера кінцевими користувачами (end-user computing), концептуально пов'язаний з моделями кінця 70-х років, які запропонував Р.Нолан.

Модель містить п'ять стадій розвитку (зрілості) у використанні обчислювальної техніки, що виділяються з позицій її використання кінцевими користувачами:

Ізоляція. На цій стадії застосування обчислювальної техніки відрізняється примітивністю, декілька користувачів освоюють користування комп’ютера в індивідуальному порядку, за відсутності формальної підтримки з боку відповідної організації. Однак необхідність такої підтримки поступово стає очевидною, що в результаті приводить до створення формальної групи консультантів, яка називається інформаційним центром.

Індивідуальне використання. Використання комп’ютера стає звичною складовою в роботі індивідуальних користувачів, а в окремих випадках і робочих колективів. Позиції інформаційних систем зміцнюються, діяльність стає більш систематичною і планомірною.

Мануальна інтеграція. Обмін даними і програмами між користувачами досягає значних обсягів, здійснюючись, головним чином, на дискетах. Головним у діяльності інформаційного центру є не підтримка індивідуальних споживачів, а здійснення комплексних програм використання комп’ютера кінцевими користувачами у межах певної організації.

Автоматизована інтеграція. Перехід до цієї стадії здійснюється з початком робіт із впровадження системи трансферу даних. Користувачами активно використовується зв'язок систем і баз даних усіх типів, що створюються як централізовано, так і індивідуальними користувачами. Інтеграційна політика в організації проводиться інформаційним центром або за його безпосередньою участю.

Розподільча інтеграція. Вища стадія для даної моделі. Користувачі працюють в системі розподілених баз даних. Роль інформаційного центру зростає ще більше. Необхідними стають система ефективного управління розподіленими даними, а також відповідні засоби передачі даних у мережі.

При плануванні розвитку інформаційних систем основним є співвідношення характеристик існуючої інформаційної системи з критеріями окремих стадій моделі розвитку. Стратегічний план розвитку інформаційної системи передбачає заходи у таких основних напрямах, як витрати на інформаційну технологію, структуру режимів роботи і організацію процесів обробки, методи управління інформаційною системою і вплив на позиції користувачів.[2]

Проаналізувавши розвиток інформаційних систем можна зробити висновок що для кращого розвитку цих систем в нашій країні, ми повинні користуватися технологіями які вже були розробленні у світі.

Список використаних джерел

1. *С.В.Івахненко «Інформаційні технології в організації бухгалтерського обліку та аудиту»: Інформаційні системи і технології/ електронне видання: https://pidruchniki.com/10561127/buhgalterskiy_oblik_ta_audit/informatsiyni_sistemi_tehnologiyi*
2. *«Розвиток інформаційних систем: моделі, сутність та стадії» osvita.ua /електронне видання http://osvita.ua/vnz/reports/management/13928*
3. *В. М. Нижник Д. С. Терехов «Еволюція розвитку інформаційних систем та інформаційних технологій в управлінні підприємствами»/ електронне видання http://journals.khnu.km.ua/vestnik/pdf/ekon/2009_5_2/pdf/220-223.pdf*

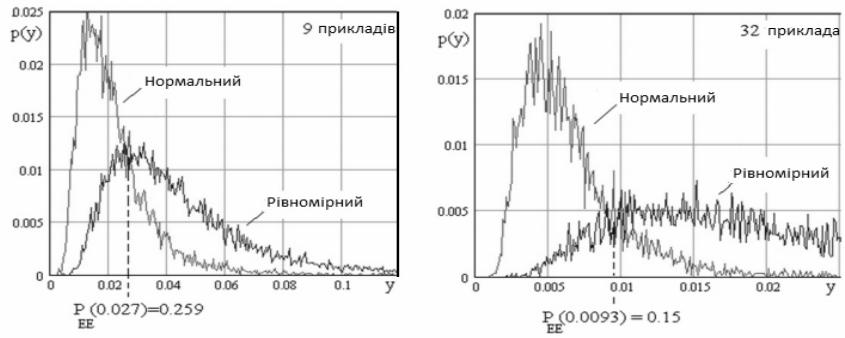
УДК 519.24; 57.017

Середін О. Д., Шматок О. С.
Національний авіаційний університет

Порівняння потужності критерія Крамера - фон Мізеса і критерія хі-квадрат для малих тестових вибірок біометричних даних

Вступ. Для посилення захисту доступу до електронних кабінетів в даний час розробляються технології біометричної автентифікації особистості, шляхом перетворення особистих біометричних даних людини в його криптографічний ключ або довгий випадковий пароль доступу. Використовуються такі біометричні образи, як: малюнок відбитка пальця [1], малюнок райдужної оболонки ока [2], голосовий пароль [3], рукописний пароль [4], малюнок кровоносних судин долоні руки [5]. Природно, що перетворювачі біометрія-код не можуть бути ідеальними і мають ймовірності помилок першого і другого роду. Виникає необхідність тестування помилок першого і другого роду на реальних біометричних даних. Крім того, під час налаштування «нечітких екстракторів» [1-3] і при навчанні нейронно-мережевих перетворювачів [4, 5] необхідно контролювати відсутність в біометричних даних грубих помилок. Формально для цієї мети може бути використаний класичний одновимірний хі-квадрат Пірсона [6, 7], однак такий підхід далекий від оптимального. В рамках даної статті ми спробуємо довести, що контроль нормальних щільностей розподілу біометричних даних вигідніш здійснювати статистичним критерієм Крамера - фон Мізеса. Потужність критерію Крамера - фон Мізеса на малих вибірках прикладів біометричних даних виявляється істотно вище, ніж потужність аналогічного критерію хі-квадрат.

Використання точки рівної ймовірності помилок першого і другого роду при оцінці потужності критерію Крамера - фон Мізеса. Будемо виходити з того, що біометричні дані по кожному з контрольованих параметрів розподілені нормально. Тоді якість даних одного параметра можна оцінювати і за критерієм Крамера - фон Мізеса. При цьому якість прийнятого рішення буде істотно залежати від порога порівняння і розмірів тестової вибірки. Отримати залежності ми можемо чисельним моделюванням. Результати чисельного моделювання для вибірок з 9 і 32 прикладів наведені на мал1.



Мал. 1. Гістограми щільності розподілу значень критерію Крамера - фон Мізеса, побудовані для вибірок з 9 та 32 прикладів

Як видно з мал. 1, щільності розподілу значень критерію Крамера - фон Мізеса істотно залежать від розмірів тестової вибірки. Для малих вибірок динамічний діапазон зміни значень критерію виявляється значним. У міру зростання числа прикладів в навчальній вибірці динамічний діапазон істотно знижується.

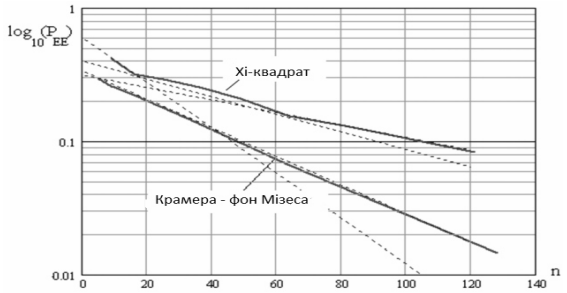
При використанні будь-якого статистичного критерію перевірки гіпотез необхідно задати поріг порівняння, отримавши для нього значення ймовірностей помилок першого і другого роду. Вибір значення порога прийняття рішення багато в чому суб'єктивний. Для того, щоб позбутися суб'єктивності, будемо призначати пороги в точці рівній ймовірності помилок першого і другого роду:

$$P_1(y)=P_2(y)=P_{EE}(y) \quad (1)$$

Як видно з лівої частини мал. 1, точка рівної ймовірності помилок знаходиться при значенні y= 0,027, при цьому значення рівнії ймовірності становить $P_{EE}(0,027)$ = 0,259. Це значення відображає той факт, що на малих вибірках домогтися малих значень ймовірностей першого і другого роду неможливо.

Якщо вибірку збільшити до обсягу в 32 приклада, то відбувається істотне зниження ймовірності помилок першого і другого роду $P_{EE}(0,0093) = 0,15$. Очевидно, що, підвищуючи розміри тестової вибірки, ми можемо монотонно знижувати значення ймовірностей помилок першого і другого роду.

Порівняння по потужності критерію Крамера - фон Мізеса і хі-квадрат критерію Пірсона. Для подання значення рівної ймовірності помилок першого і другого роду критерію Крамера - фон Мізеса як функції, що залежить від розміру тестової вибірки, найбільш зручна логарифмічна шкала мал. 2.



Мал. 2. Вплив обсягу вибірки на значення рівної ймовірності помилок в залежності від обсягу вибірки для критеріїв Крамера - фон Мізеса і хі-квадрат.

Як видно з мал. 2, $log_{10}(P_{EE}(n))$ є лінійною функцією:

$$P_{EE}(n)=10^{-0,47-0,0107*n} \text{ де } n=1, 2, \ldots, \infty \quad (2)$$

Аналогічну залежність можна побудувати і для рівних ймовірностей помилок критерію хі-квадрат [6, 7]. З теорії відомо, що критерій хі-квадрат повинен описуватися розподілом Пірсона:

$$p(\chi^2, m) = \frac{1}{2^{\frac{m}{2}} \times \Gamma(\frac{m}{2})} \times (x^{\frac{m}{2}-1} \times \exp(\frac{-x}{2})) \quad (3)$$

де $\Gamma(\frac{m}{2})$ – гама функція; m – число степенів свободи.

З мал. 2 видно, що критерій Крамера - фон Мізеса забезпечує значно меншу помилку прийняття рішень в порівнянні з критерієм хі-квадрат Пірсона. Зі збільшенням обсягу тестової вибірки перевага критерію Крамера - фон Мізеса зростає. Також перевага цього критерію збільшується зі збільшенням розмірності біометричних даних.

Висновок. Основною причиною переваг критерію Крамера - фон Мізеса є те, що при інших рівних умов його шуми квантування мають велику частоту стрибків і меншу амплітуду кожного стрибка. Як наслідок, шуми квантування згладжуються критерієм Крамера - фон Мізеса краще, ніж ті ж самі шуми квантування в критерії хі-квадрат Пірсона. На типовій вибірці біометричних даних в 32 прикладів критерій Крамера - фон Мізеса дає в 1,5 рази меншу ймовірність помилок, ніж критерій хі-квадрат Пірсона.

Список використаних джерел

1. *Ramírez-Ruiz, J. Keys Generation Using Finger Codes / J. Ramírez-Ruiz, C. Pfeiffer, J. Nolazco-Flores // Advances in Artificial Intelligence – IBERAMIA-SBIA. – 2006 (LNCS 4140). – P. 178–187.*
2. *Monrose, F. Cryptographic key generation from voice / F. Monrose, M. Reiter, Q. Li, S. Wetzel // Proc. IEEE Symp. on Security and Privacy. – 2001. – 354 c.*
3. *Hao, F. Crypto with Biometrics Effectively / Feng Hao, Ross Anderson, John Daugman // IEEE TRANSACTIONS ON COMPUTERS. – 2006. – Vol. 55, № 9. – 244 p.*
4. *Нейросетевая защита персональных биометрических данных / Ю. К. Язов, В. И. Волчихин, А. И. Иванов [и др.]. – М. : Радиотехника, 2012. – 157 с.*
5. *Технология использования больших нейронных сетей для преобразования нечетких биометрических данных в код ключа доступа / Б. С. Ахметов, А. И. Иванов, В. А. Фунтиков [и др.]. – Алматы, Казахстан : ТОО «Издательство LEM», 2014. – 144 с.*
6. *Кобзарь, А. И. Прикладная математическая статистика для инженеров и научных работников / А. И. Кобзарь – М. : ФИЗМАТЛИТ, 2006. – 816 с.*
7. *ГОСТ Р 50.1.037–2002 Рекомендации по стандартизации. Прикладная статистика. Правила проверки согласия опытного распределения с теоретическим. Часть I. Критерии типа χ2. – М., 2001. – 140 с.*

УДК 004.056 (045)

Єлізаров А. Б., Симониченко Я. А., Симониченко А. А.
Національний авіаційний університет

Дослідження сучасних програмних стеганографічних засобів приховування інформації

Велика кількість сучасних програмних стеганографічних засобів приховування інформації зробили дану технологію доступною для будь-якого пересічного громадянина, що може використовувати її для реалізації різних поставлених цілей. Реалізація вищезазначеної технологій приховування інформації може використовуватися з метою організації захисту інформації або з метою організації прихованого каналу передачі (витоку) інформації.

Постановка задачі. Сукупність засобів і методів, що використовуються для формування прихованого каналу передачі інформації утворюють стеганографічну систему [1]. Дана система виконує вбудовування повідомлення (прихованої інформації) в інформаційний об'єкт (далі – ІО) одним із стеганографічних методів. Передавання ІО каналами зв'язку та виділення приховуваного повідомлення з отриманого ІО. Найбільш уніфікованим ІО, що використовується стеганографічними засобами є графічний файл, а прихованою інформацією є текстове повідомлення [2]. Найчастіше, в якості стеганографічних засобів виступають стеганографічні програмні продукти. Таким чином, *метою даної роботи* є дослідження сучасних стеганографічних програмних засобів приховування інформації, що вільно розповсюджуються через мережу Інтернет. Під час дослідження буде виконано виявлення структурних змін у графічних файлах-результатах, що будуть отримані при використанні сучасних стеганографічних програмних засобів, в порівнянні з файлом-оригіналом. В якості методу дослідження, буде реалізований один із методів стеганог-рафічного аналізу, а саме - атака на основі відомого порожнього ІО, що дає можливість шляхом порівняння його із заповненим ІО встановити факт наявності прихованої інформації.

Виконання роботи. Для дослідження стеганографічних програмних засобів було використано більше 20 програмних засобів (продуктів) приховування інформації (далі - ПЗ), які доступні пересічному громадянину та вільно розповсюджуються через мережу Інтернет, а саме: Camouflage (далі - ПЗ1); Clotho (далі - ПЗ2); DeEgger Embedder (далі - ПЗ3); FIRA2 (далі - ПЗ4); HexaStego-BMP (далі - ПЗ5); Hide&Reveal (далі - ПЗ6); ImageSpyer (далі - ПЗ7); ImageSpyer G2 (далі - ПЗ8); JHide (далі - ПЗ9); Our Secret (далі - ПЗ10); QuickStego (далі - ПЗ11); Shusssh! (далі - ПЗ12); SilentEye (далі - ПЗ13); Steganos Privacy Suite 18 (далі - ПЗ14); Steganos Security Suite 2007 (далі - ПЗ15); SteganoG (далі - ПЗ16); SteganographX Plus (далі - ПЗ17); S-Tools (далі - ПЗ18); Xiao Steganography (далі – ПЗ19); Anubis (далі – ПЗ20); Hallucinate (далі – ПЗ21); OpenPuff (далі – ПЗ22). В якості ІО використовувався графічний файл BMP-формату, оскільки він є оптимальнішим форматом при виконанні стеганоперетворення [3].

Припустимо, що вбудовування прихованого повідомлення в обраний ІО буде виконуватися «класичним» методом безпосередньої заміни молодшого біту в компоненті синього кольору зображення при використанні колірної моделі RGB. В якості прихованого повідомлення було обрано три текстових повідомлення на англійській мові різною довжиною, що відповідно становить 5%, 15% та 25% від загальної кількості пікселів колірної компоненти зображення. Збереження повідомлення відбувалося в текстовий файл із TXT-форматом.

Виконаємо дослідження зміни показника розміру графічного файлу-результату в порівнянні із файлом-оригіналом (рисунок 1). Оскільки, в ході дослідження обрано три повідомлення різного розміру, було отримано три відповідних графічних файлів-результатів для кожного ПЗ із прихованими повідомленнями. З рисунку 1 можна побачити, показник розміру файлів-результатів для ПЗ1, ПЗ2, ПЗ3, ПЗ10, ПЗ12, ПЗ19 та ПЗ20 суттєво відрізняється від розміру файлу-оригіналу та прямо пропорційно збільшується з розміром прихованого повідомлення. Розміри файлів-результатів інших ПЗ, після приховування повідомлення, відповідають розміру файлу-оригіналу.

а

б

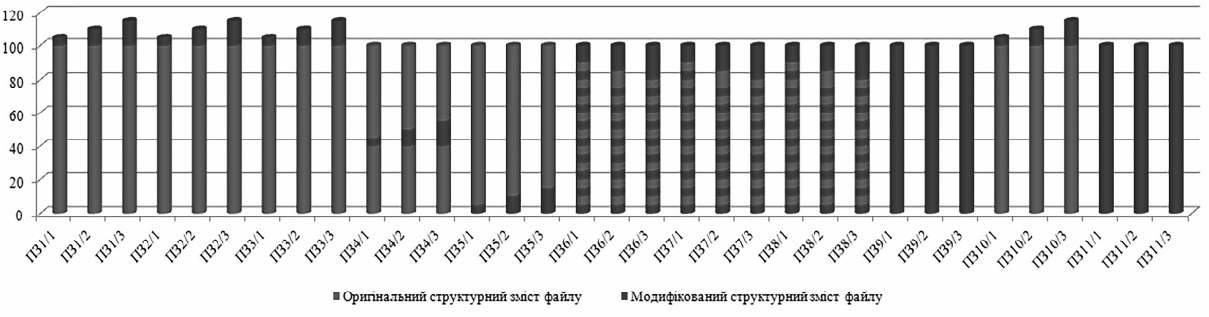
Рисунок 1 - Графічне відображення показника розмірів файлів-результатів, де *а* – ПЗ1-11, а *б* – ПЗ12-22

Виконаємо порівняння структури отриманих графічних файлів-результатів із файлом-оригіналом (рисунок 2).

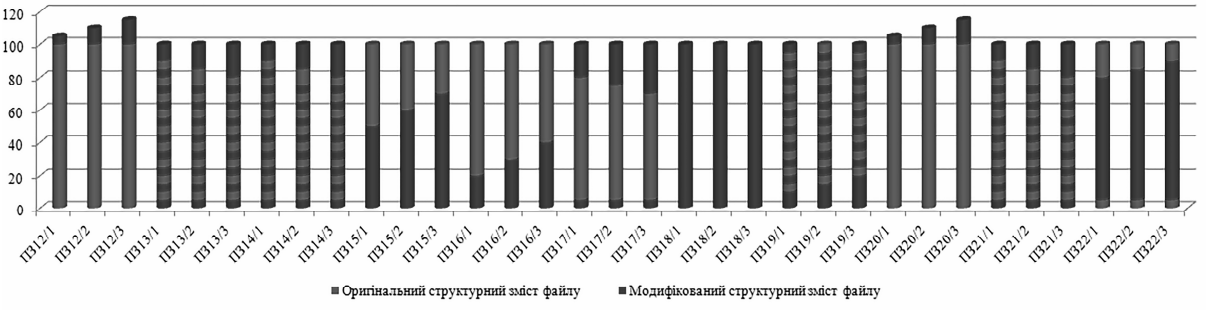
Порівняння структурного змісту та розмірів графічних файлів-результатів, при використанні ПЗ1, ПЗ2, ПЗ3, ПЗ10, ПЗ12, ПЗ19 та ПЗ20, дає можливість попередньо зробити висновок відносно методу приховування повідомлення даними ПЗ. Таким чином, з огляду на вищезазначене, дані ПЗ виконують звичайне додавання прихованого повідомлення в кінець графічного файлу з використанням методу «склеювання». Порівняння файлів-результатів інших ПЗ, свідчать про використання стеганографічних методів приховування інформації, що призвели до зміни структурного змісту файлу в порівнянні із файлом-оригіналом та збереження розміру файлів після стеганоперетворення.

Таким чином, під час дослідження, було використано більше 20 програмних засобів (продуктів) приховування інформації (далі - ПЗ), які доступні пересічному громадянину. Було виконано порівняння структури графічних файлів-результатів із файлом-оригіналом. Враховуючи показник зміни розміру графічного файлу-результату та порівняння структури отриманих графічних файлів-результатів, можна зробити висновок, що використання 6 програмних засобів призводить до збільшення розміру

отриманого файлу, оскільки вони виконують додавання прихованого повідомлення в кінець графічного файлу з використанням методу «склеювання». До таких програмних засобів приховування повідомлення відносяться - ПЗ1, ПЗ2, ПЗ3, ПЗ10, ПЗ12 та ПЗ20. Приховування повідомлення іншими програмними засобами виконується з використанням стеганографічних методів безпосередньої заміни малозначущих частин зображення (надлишкової інформації) бітами прихованого повідомлення. З огляду на результати показника порівняння структури, можливо зробити попередній висновок відносно стеганографічних методів, що використовуються: ПЗ4, ПЗ5, ПЗ9, ПЗ11, ПЗ15, ПЗ16, ПЗ17, ПЗ18 та ПЗ22 - виконують послідовну заміну надлишкової інформації бітами прихованого повідомлення, а ПЗ7, ПЗ8, ПЗ13, ПЗ14, ПЗ19 та ПЗ21 - виконують приховування та розподіл бітів прихованого повідомлення у файлі з певним інтервалом.



а



б

Рисунок 2 - Графічне відображення порівняння структури файлів-результатів, де *а* – ПЗ1-11, а *б* – ПЗ12-22

Висновок. На основі проведених досліджень були отримані результати, щодо сучасних програмних стеганографічних засобів приховування інформації та методів реалізації приховування інформації. Таким чином, частина програмних засобів виконує приховування повідомлення методом «склеювання», а інша частина - використовує стеганографічні методи приховування повідомлення. Дані результати можливо використовувати в подальшому для підвищення ефективності стеганографічної системи або стеганографічного аналізу.

Список використаних джерел

1. *Удосконалення стеганографічних методів на базі аналізу колірних моделей зображення / О. К. Юдін, Я. А. Симониченко. – Київ: Наукоємні технології, 2012. – №1 (13). – С. 70-75.*
2. *Виявлення прихованих каналів передачі інформації на базі методів стеганоаналізу / О. К. Юдін, Я. А. Симониченко. – Київ: Наукоємні технології, 2016. – №4 (32). – С. 389-394.*
3. *Компьютерная стеганография. Теория и практика / Г. Ф. Конахович, А. Ю. Пузыренко. — Киев: МК-Пресс, 2006. — 288 с.*

УДК 004.67

Смірнова Т. В., Смірнов О. А., Дрєєв О. М., Смірнов С. А.
Центральноукраїнський національний технічний університет

Використання хмарних експертних систем в сфері інформаційного забезпечення обробки поверхні деталей

Сучасний стан розвитку матеріалознавства та експериментальної бази привів до створення різноманітних баз знань що до обробки поверхонь деталей. На сьогодні відомі роботи щодо оптимізації обробки поверхонь деталей таких вчених. як Солових Є.К. [1], Бороненков В.Н. [2], Сторожева В.П. [3], Нахимовича Е. [4], Пантєлєєнко Ф.І. [5] та багатьох інших. Результатами кожного дослідження є база знань пошуку параметрів технологічних процесів або, навіть, експертна система мінімізації технологічних витрат за заданими характеристиками готової продукції [6, 7]. В той самий час спостерігається відособлення розроблених систем оптимізації, що не дозволяє обрати засоби обробки деталей з кількох технологічних процесів, а також відсутні можливості створювати ланцюги технологічних процесів. З цієї причини відсутні, в загальному випадку, системи автоматичної пропозиції ланцюгів технологічних процесів, й ця робота лягає на людину-фахівця. У такому випадку, відповідно, до кваліфікації експерта щодо ланцюгів технологічних процесів накладаються значно вищі вимоги, ніж щодо знання окремих технологічних процесів.

Згідно зазначеним вище причинам, виникає потреба у створенні узагальненої експертної системи, в якій може бути використано різноманітні експертні системи в якості складових частин з власними правилами формування бази знань та системи пошуку рішення. З причини інформаційної незалежності розроблених баз знань та процесів отримання рішень, узагальнююча експертна система повинна мати розподілений характер, що відповідає архітектурі хмарних технологій.

Нехай маємо набір експертних систем $E = \{E_i\}$, для кожної з яких, при умові ігнорування внутрішніх характеристик та відмінностей, визначено набір параметрів вхідних поверхонь деталей, які підлягатимуть обробці U_i; набір вимог до параметрів після обробки V_i; прогноз значень отриманих параметрів після застосування технологічного процесу P_i; і також обмеження на технологічний процес (час, витрати та інше) R_i. В результаті кожну з експертних систем можна представити сукупністю множин $E_i = \{U_i,\ V_i,\ P_i,\ R_i\}$ ($i = 0..N\text{-}1$, де N визначає кількість використаних технологічних процесів і, відповідно, експертних систем). При цьому осередком забезпечення кожної експертної системи можуть виступати окремі обчислювальні системи, які поєднані комунікаційною системою, наприклад, Інтернет.

Виділимо множину експертних систем одноетапних технологічних процесів E, як складову узагальнену експертну систему $X = \{E, U, V, P, R\}$ (рис. 1).

В узагальненій експертній системі, яка є технологією об'єднання низки експертних систем окремих технологічних процесів E_i, містяться також узагальнені обмеження на обробку поверхонь деталей. Деякі з цих вимог є адитивними як, наприклад, максимальний загальний час виготовлення виробу, а деякі мають іншу природу. Наприклад хімічний склад та міцність поверхні виробу може відрізнятися при однакових обраних технологічних процесах, але неоднаковому порядку виконання послідовності технологічних процесів.

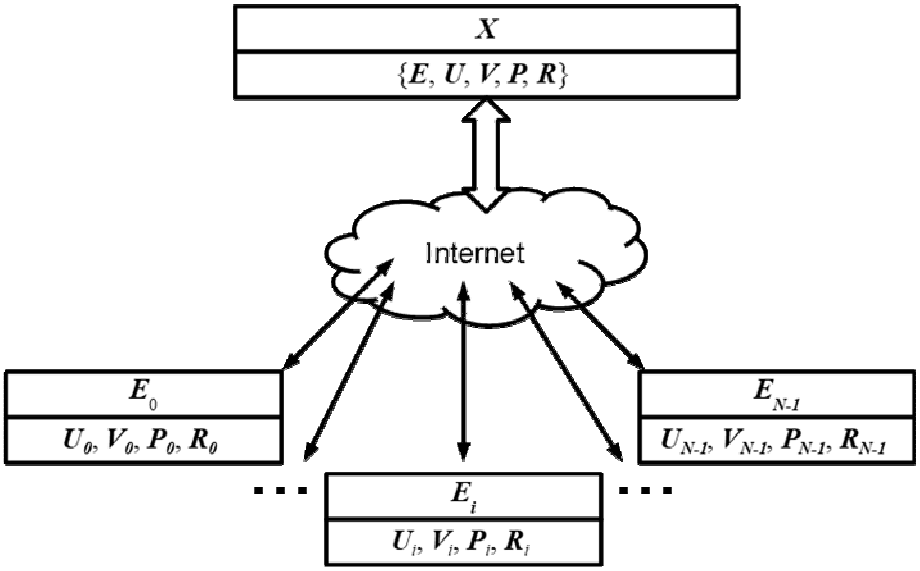


Рисунок 1 – Графік розподіленої сукупності експертних систем

В результаті наявності неадитивних компонент в обмеженнях та вимогах до виробу, ланцюг технологічних процесів є комбінаторною вибіркою з врахуванням порядку елементів E_i. Але комбінаторна складність задачі вибору ланцюга технологічних процесів значно спрощується реальними обмеженнями елементів E_i, коли результати обробки процесу i не перетинаються з вимогами процесу j:

$$V_i \bigcap U_j = \varnothing.$$

Фактично утворена сукупність експертних систем технологічних процесів є графом з ребрами, де умова не виконується (рис. 2):

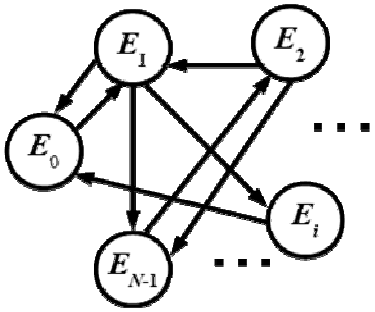


Рисунок 2 – Граф можливих ланцюгів технологічних процесів для яких $V_i \bigcap U_j \neq \varnothing$

Додаткову нелінійність в процес побудови розв'язків приносить неможливість використання технологічного процесу за рахунок браку ресурсів, однак такі ситуації є частиною обмеження R. Також при необхідності до множини універсальних в концепції системи вимог, додають специфічні вимоги до окремого технологічного процесу R_i^*. В таких випадках хмарна система повинна забезпечити обмін додатковими вимогами за специфічним протоколом.

Завдяки утвореному графу можливих комбінацій технологічних процесів з'являється можливість використовувати алгоритми оптимізації пошуку не лише в глибину та в ширину, прямим та оберненим проходом, але й застосувати алгоритми на графі, а також й генетичні алгоритми пошуку рішень близьких до оптимальних, наприклад мурашиний алгоритм.

В процесі розв'язання поставленої задачі шукають допустимі ланцюги технологічних процесів обробки поверхонь деталей

$$C = \{E_{k0,}E_{k1},...,E_{kn-1}\},$$

де n – кількість етапів обробки, k_i – номер обраного технологічного процесу. При цьому вимагається виконання наступних умов:

$$R_{k0} \oplus R_{k1} \oplus ... \oplus R_{kn-1} < R,$$

$$V \in V_{k0}, P_{k0} \in V_{k1}, P_{k1} \in V_{k2},..., P_{kn-1} \in P,$$

де $\oplus$ – узагальнене додавання, який враховує адитивні властивості величин.

Таким чином, поставлена задача пошуку оптимального шляху на побудованому графі можливих ланцюгів технологічних процесів розв'язується точно лише за допомогою повного перебору. Тому, при наявності значної кількості вузлів графу та порівняно повільного розв'язання задачі окремими експертними системами, час на розв'язання задачі може бути занадто великим. Використання розподілених систем, у яких окремі експертні системи розташовані в хмарі і мають множинну програмно-апаратну підтримку, дозволяють використовувати масові паралельні обчислення. При цьому окремі задачі до експертних систем є незалежні і час пошуку рішення стає обернено пропорційним сумарній обчислювальній потужності використаних обчислювальних вузлів.

Список використаних джерел

1. *Соловых Е.К. О концептуальном подходе к повышению несущей способности упрочняющих защитных покрытий. Зб. наук. праць Кіровоградського національного технічного університету. Техніка в с/г виробництві, галузеве машинобудування, автоматизація. 2011. Ч.2, Вип. 24. С.140–145.*
2. *Бороненков В.Н., Коробов Ю.С. Основы дуговой металлизации. Физико-химические закономерности. Екатеринбург: УрГУ; Екатеринбург: Унив. изд-во. 2012, 267 с.*
3. *Сторожев, В.П. Восстановление деталей судовых технических средств. Серия «Судоремонт» 1990. Вып. 1(17). С. 1-60.*
4. *Нахимович Е. Комплексный подход к решению задач по повышению долговечности и износостойкости материалов и деталей машин. Трение, износ и смазка. 2003 – 5. № 4. С. 61–64.*
5. *Пантелеенко Ф.И. Новое в восстановительно-упрочняющих технологиях. Производство и ремонт машин: Сб. матер. Междун. науч-техн. конф., 28 февр.-6 марта 2005. Ставрополь: Изд-во СтГАУ «АГРУС». 2005. С. 58-63.*
6. *Посвятенко, Е.К., Д'яченко С.С., Гончаров В.Г., Ткачук М.А., Шеремет В.Числове обґрунтування параметрів дискретного зміцнення високонавантажених деталей машин [Текст]. Збірник наукових праць "Вісник НТУ "ХПІ" : Машинознавство і САПР. Вестник НТУ "ХПИ". 2011. №51. ISBN 2079-0775.*
7. *Ступницький В. В. Узагальнений алгоритм структурно-параметричної оптимізації функціонально-орієнтованого технологічного процесу. Прогресивні технології і системи машинобудування. 2014. № 2. С. 109-120. URL: http://nbuv.gov.ua/UJRN/Ptsm_2014_2_19.*

УДК 004.4'27

Стовманенко В. О., Григор'єв Д. О., Давиденко Є. О.
Чорноморський національний університет імені Петра Могили

Використання алгоритмів системного аналізу для роботи із медіа

Одним із основних призначень комп'ютерної техніки є робота з великими обсягами даних. Автоматизований аналіз є набагато більш ефективним ніж людський. За той самий час більші обсяги інформації можуть бути оброблені, а також деякі неочевидні закономірності можуть бути знайдені.

Разом із обчислювальною технікою розвивалися і алгоритми роботи з даними [1, 2]. Формувалися засоби для представлення даних у зручному для машин вигляді, оптимізувався час їх роботи і надійність результатів. Кластеризація, класифікація, знаходження елементу, що найбільше відрізняється – це завдання без яких важко уявити роботу з даними.

Більшість алгоритмів для роботи з даними розроблялися таким чином аби абстрагуватися від роду інформації, яка є вхідною для їх роботи. Таким чином їх використання не обмежується якоюсь однією сферою. Якщо правильно представити набори вхідних даних, можна виконувати аналіз у будь-якій сфері.

Можна використовувати алгоритми кластерного аналізу , для знаходження середньої гучності аудіофайлу. Маючи такі дані можна правильно налаштувати механізм компресії звукового сигналу для нормалізації гучності, можна використовувати класифікатори зображень для розпізнавання деяких предметів на фотографіях і так далі.

Задача знаходження палітри кольорів будь-якого зображення стає стандартною задачею класифікації, якщо розглянути її в такому ключі. Після надлежних оптимізацій можна використовувати такі алгоритми як k-means [3] для формування палітри кольорів застосунку відповідно до деякого, обраного користувачем, зображення без видимих затримок (рис. 1).

Рисунок 1 – Демонстрація роботи алгоритму

Подібний підхід і було протестовано для зображення закодованого в метаданих аудіофайлів ID3. Зображення можна представити у вигляді набору інформації про кольори кожного пікселю відповідно до формату збереження (монохромна шкала, RGB, aRGB і т. д.) і дані про ці пікселі використовувати як вхідні для k-means. За умови використання алгоритму послідовно, для не стиснених зображень з розмірами від 512x512 пікселів час затримки був суттєвим (дві з половиною секунди). Для пришвидшення аналізу зображення можна стискати. Автентичні кольори палітри можуть бути встановлені й при меншому розмірі зображення. При стисненні, наприклад, до 128x128 час зменшується пропорційно до зменшення розміру зображення. При цьому точність знаходження кольорів не втрачається. Для додаткового збільшення швидкості роботи було застосовано алгоритми паралельних розрахунків. Набір вхідних даних розбивається на рівні групи і кожен потік використовує спільний набір даних при цьому опрацьовуючи тільки їх частину.

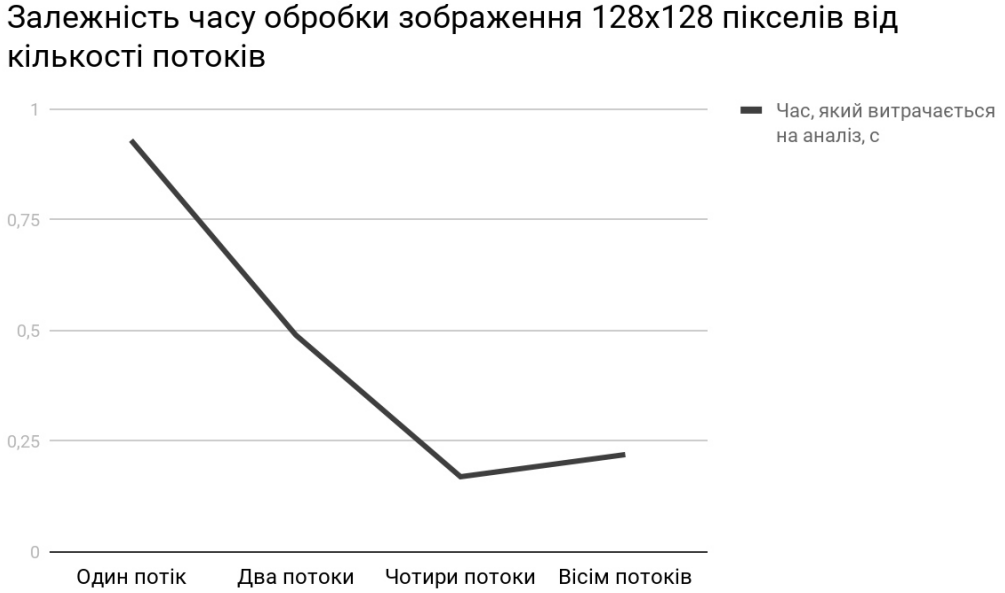


Рисунок 2 – Графік залежності часу обробки від кількості потоків (дійсно для використаного процесора з чотирма фізичними ядрами)

Найбільшим недоліком обраного підходу є значна залежність від початково обраних кластерів. Випадковий характер їх вибору зумовлює випадковість відповіді. Можна отримати різні палітри на одному зображенні. Для його подолання варто розглядати більш складні алгоритми вибору кластерів.

Список використаних джерел

1. *Фісун М. Т. Інтеграція технологій OLAP та Data Mining при побудові міжвимірових асоціативних правил / М. Т. Фісун, Г. В. Горбань // ScienceRise. – 2015. № 6(2). С. 103-111.*
2. *Фісун М. Т. Порівняльний аналіз засобів Data Mining у СКБД SQL SERVER та ORACLE / М. Т. Фісун, Є. О. Давиденко, О. М. Крайник // Проблеми інформаційних технологій. – 2016. – №1 (019). – С. 231-238.*
3. *Shved A., Davydenko Ye. The Analysis of Uncertainty Measures With Various Types of Evidence. Data Stream Mining & Processing (DSMP) : Proceeding of the 2016 IEEE First International Conference, Lviv, Ukraine, 23-27 August 2016. P. 61-64. DOI: 10.1109/DSMP.2016.7583508.*

УДК004.056.55

Столяренко Є. Ю., Неласа Г. В.
Запорізький національний технічний університет

Розробка веб-сервісу для виконання операцій з елементами скінченних полів

Більшість криптографічних алгоритмів використовують перетворення в скінченних групах, кільцях, полях. Особливий інтерес викликають перетворення в простих та розширених полях Галуа, оскільки вони лежать в основі сучасних криптографічних стандартів шифрування та електронного цифрового підпису. Це специфічний розділ вищої математики, який не завжди входить в стандартну програму навчання, але є необхідним для спеціальності «125 - Кібербезпека». Тому актуальною є розробка он-лайн калькулятору арифметики скінченних полів в якості тренажера для проведення навчальних занять.

Скінченне поле, або поле Галуа в загальній алгебрі - це поле, що складається зі скінченого числа елементів. Для будь-якого простого числа p кільце лишків за модулем p— це скінченне поле з p елементів, яке позначається $GF(p)$. Елементи цього поля можуть бути представлені цілими числами $0,1,...p-1$ які додаються і множаться за модулем p. Розширене скінченне поле $GF(p^n)$ містить p^n елементів і однозначно задається своєю характеристикою p і модулем поля – незвідним поліномом степеня n. На практиці часто використовуються поля $GF(2^n)$.

У світі інформаційних технологій скінченні поля мають велике практичне значення. В даний час скінченні поля застосовуються в алгоритмах обробки цифрової інформації, наприклад, в алгоритмах виявлення і виправлення викривлень інформації в інформаційних системах, що використовують протокол Ріда-Соломона; у криптографічних алгоритмах, що базуються на арифметиці скінчених полів і еліптичних кривих, визначених над скінченими полями; для формування псевдовипадкових послідовностей в генераторах випадкових чисел. На даний момент практично відсутні веб-сервіси виконання обчислень в скінченних полях. Дана можливість присутня лише в "великовагових" пакетах лінійної алгебри або динамічних бібліотеках (Maple, Maxima, FLINT), які часто є важкими в освоєнні та платними.

Розроблений авторами калькулятор арифметики скінченних полів на базі технологій HTML і JavaScript має можливість оперувати з елементами простих або розширених полів Галуа, а саме виконує арифметичні операції ділення, складання, віднімання та множення в простих та розширених полях, також реалізовано функціонал перевірки поліномів на незвідність, обчислення слідів, норм, характерів, обчислення коренів поліномів у скінчених полях, генерацію незвідних поліномів, та реалізовано можливість розрахунку характерів скінченних полів, та основних тригонометричних сум: Гауса та Якобі. Цей калькулятор покладений у основу логіки роботи веб-сторінки, що дає можливість зручно проводити розрахунки у режимі он-лайн. Також на веб-сторінці реалізовано пояснення.

Авторами наукової роботи проведено ретельний аналіз математичних основ теорії скінченних полів, зокрема арифметичних операцій в простих та розширених полях Галуа; виконана програмна реалізація цих алгоритмів з використанням мови програмування JavaScript і покладання цих алгоритмів у основу логіки веб - сторінки, що надає можливість проводити розрахунки у режимі он-лайн; розроблено детальну систему пояснень, що дає змогу користуватися сервісом з метою навчання користувачам початкового рівня.

Результати роботи можуть бути використані як науково-популярний довідник в навчальних цілях.

УДК 004

Ткачук Р. О.
Центральноукраїнський національний технічний університет

Переваги операційної системи Linux

Спір між тим, що краще: Linux або Windows, не вщухає вже не один десяток років. І дійсно, ці операційні системи дуже гарні, кожна з яких має як свої недоліки, так і переваги. Визначити, яка з них краща, можете тільки Ви самі, так як це в будь-якому випадку буде суб'єктивна думка. Але можена розповісти про їх позитивні і негативні сторони [1].

Мета роботи полягає у тому, щоб порівняти дві операційні системи та довести превагу Linux над MS Windows.

Звісно, Windows має ряд переваг перед іншими операційними системами, але він також має і ряд недоліків. Ми розглянемо і порівняємо Windows з його основним конкурентом - операційною системою Linux, яка є альтернативою для тих, хто не хоче мати справу з неліцензійної Windows або з Windows взагалі [2].

Основними принциповими відмінностями між ОС являються:

1. «Windows» розробляється і підтримується однією єдиною компанією – Microsoft Corporation. Їй належать авторські права на цей продукт, і вона бере плату за використання. «Linux» розробляється і підтримується багатьма компаніями в різних країнах світу і тисячами програмістів. Права на цю ОС передані в суспільну власність.

2. Графічне середовище «Windows» користувача є невід'ємною частиною ОС. Тобто ОС «Windows» без графічного середовища не існує. У той час як «Linux» – ОС консольного режиму, її графічне середовище – окремий програмний продукт. Програм, які реалізують графічне середовище більше 10, але широко використовуються тільки дві – GNOME та KDE.

3. «Windows» як кінцевий продукт складається з власне ОС і невеликого набору прикладних програм, які мають дуже скромну функціональність. Іншими словами, встановлюючи «Windows» потрібно додатково встановлювати прикладні програми.

4. «Linux» має велику кількість сучасних дистрибутивів, які одночасно підтримують новітнє устаткування та устаткування попередніх поколінь. Пізніші версії «Windows» далеко не завжди підтримують устаткування попередніх поколінь[3].

Недоліки ОС MS Windows:

— Порівняно висока вартість. Варіанти «Windows», які не прив'язані до комп'ютера мають ціну ближче до двохсот доларів США і вище. І це вартість «Windows» для одного комп'ютера. І якщо потрібна ОС, наприклад, на 5 комп'ютерів, то вартість за 5 копій «Windows» буде близько тисячі доларів.

— Дуже велика кількість зловмисних програм (віруси). Це особливо серйозна проблема, яка змушує нести додаткові витрати. Цю проблему можна зменшити за рахунок кваліфікованої настройки ОС «Windows» і акуратного її використання в ситуаціях ризику, головна з яких – Інтернет.

— Жорстка залежність від розробника. ОС «Windows» поширюється тільки в бінарному вигляді, який важкодоступний для зміни, але більш того, компанія Microsoft взагалі забороняє вносити будьякі зміни в робочі коди ОС «Windows».

— Уповільнення системи. Windows працює з часом все повільніше і повільніше через те що засмічується кеш, куки і системні файли. Реєстр теж «забивається». Існує ряд програм, які це виправляють, але тим не менше вони це роблять не повністю [3].

Переваги ОС MS Windows: підтримка великого асортименту комп'ютерного обладнання; величезна кількість прикладних програм, напевно, більше ста тисяч найменувань; для будь-якої прикладної задачі на платформі «Windows» існує як

мінімум кілька десятків програм, для популярних задач існують сотні програм; велика кількість спеціалістів, які на достатньому рівні знають сімейство ОС «Windows» [3].

Недоліки ОС «Linux»:

— Низька підтримка комп'ютерного обладнання, особливо зовнішнього, наприклад, сканери та USB, а також внутрішні HSF/HCF модеми. Але проблема у значній мірі має рішення за рахунок більш ретельного підходу до вибору обладнання.

— Менша кількість прикладних програм. Під ОС «Linux» немає версій програм від компанії Adobe, версій економічних програм 1С, версії програми інженерного проектування AutoCAD, версії програми розпізнавання текстів (FineReader). Звичайно, під ОС «Linux» існують графічні редактори та програми моделювання/проектування, але вони сильно поступаються лідерам. Частково цей недолік можна компенсувати за рахунок того, що деякі Windowsпрограми можна запустити на платформі «Linux».

— Менша, ніж для платформи Windows, кількість спеціалістів. Тобто, знайти Linux-спеціаліста високого рівня не просто, вартість послуг услуг такого спеціаліста буде вища, ніж у випадку з Windows [3].

Переваги ОС «Linux».

Низька вартість. Нескладно отримати диск с будь-яким дистрибутивом «Linux». При цьому, маючи всього одну фізичну копію дистрибутива «Linux», ви маєте право установити його на будьяку кількість комп'ютерів. Незалежність від розробника. Якщо потрібна яка-небудь функціональність, що відсутня в ОС «Linux», можна її додати своїми власними зусиллями. Така можливість існує завдяки тому, що ОС «Linux» розповсюджується не тільки у бінарному вигляді, але і в вихідних кодах, при цьому немає ніяких заборон на модифікацію цих вихідних кодів, що дозволяє робити із «Linux» дуже різні продукти для будь-яких завдань.

Гнучкість системи. За допомогою дистрибутива «Linux», практично з будь-якого комп'ютера можна зробити повноцінний сервер. При цьому є можливість запускати лише ті процеси, які є необхідними, а не ті, які встановлюються системою. Стабільність операційної системи. Так, наприклад, при різкому відключенні напруги або збої роботи комп'ютера шанси втратити дані на Windows набагато вищі, ніж на Linux.

Стабільна швидкість роботи системи. На відміну від уповільнення Windows з часом, Linux працює завжди однаково.

Практична відсутність (на сьогоднішній день) шкідливих програм для цієї платформи. Це дозволяє уникнути додаткових витрат на попередження чи ліквідацію збитків від дії шкідливих програм [3].

Тож в користувача ОС Windows завжди будуть виникати різноманітні проблеми: де знайти калькулятор, як ввімкнути перевірку орфографії в LibreOffice або вставити фрагмент тексту без форматування, де знайти аналог Paint та ін. [4], але переваг використання ОС «Linux» набагато більше та вони вагоміші, ніж переваги ОС Windows.

Список використаних джерел

1. *Що краще: Linux або Windows? URL: http://ittexnoall.com/index.php/osnovy-kompyutera/59-shcho-krashche-linux-abo-windows.html*
2. *Блискавицкий А.А., Кабаев С.В. Операционные системы реального времени URL: http://www.mka.ru/?p=40774.*
3. *Нізієнко Б.І., Трублін О.А., Калачова В.В. Порівняльний аналіз операційних систем для вирішення завдань реального часу в системах військового призначення. Харківський університет Повітряних Сил імені Івана Кожедуба, Харків. 2015. №2, с. 117-120.*
4. *Особистий Досвід: Linux Проти Windows 10. URL: https://techtoday.in.ua/reviews/osobistiy-dosvid-linux-proti-windows-10-66000.html*

УДК:004.021

Фесечко Д. В.[*]
Центральноукраїнський національний технічний університет

Порівняльний аналіз формату MP3

З моменту коли розпочався стрімкий розвиток та розповсюдження інтернету, з'явилась потреба в новому форматі, який міг би швидко та надійно передавати аудіо-інформацію між користувачами. На той час вже існував формат Audio-CD, але аудіо файли збережені в цьому форматі були дуже великого розміру і були незручними для пересилання в мережі Інтернет. У 1993 році невелика компанія Fraunhofer IIS розробила формат стиснення аудіо даних MP3. В ті часи жоден з аудіо-форматів не міг надати такої якості, і при цьому займати так мало місця.

В першу чергу MP3 розроблявся для використання в мережі Іінтернет, для швидкої передачі якісного звуку. Тому MP3 являється потоковим форматом. Його можна назвати одним з найвідоміших форматів аудіо стиснення. Порівняно зі своїми попередниками MP1 і MP2, він має високу складність алгоритму, та більші вимоги до системних ресурсів. Даний формат використовує складний алгоритм кодування. Якщо порівняти алгоритм стиснення MP3 з іншими архіваторами, головною метою яких є стиснення інформації таким чином, щоб після вилучення інформації з архіву в ній не змінилося жодного біта, MP3 використовує крім математичних алгоритмів стиснення, алгоритм видалення непотрібної звукової інформації. Оскільки MP3 є потоковим форматом, він здатний при кодуванні розбивати ділянки звукової інформації на рівні незалежні частини, які називаються фреймами. Кожен фрейм має свої параметри та заголовок, в якому ці параметри описані. При відтворенні послідовності декодованих фреймів породжується безперервне звучання записаного звуку. Такий метод дає можливість перемотування, коли можливий перехід до довільного фрейму, і відтворення звуку саме з цього місця. Саме завдяки такій структурній особливості MP3 являється мережевим форматом. Завантаживши початкові фрейми в оперативну пам'ять або дисковий кеш, програвач вже може їх відтворювати, при цьому одночасно довантажуючи нові фрейми, чим досягається безперервність відтворення.

При високій якості MP3, коли ширина потоку дорівнює 320 кілобіт в секунду, для кодування фреймів застосовуються тільки математичні алгоритми стиснення. Якість при цьому зовсім не страждає, але і розмір зменшується всього в чотири рази, тобто коефіцієнт стиснення такий, який дав би звичайний архіватор. При зменшенні смуги пропускання до 256 кілобіт в секунду і нижче, задіюються ті самі алгоритми видалення "непотрібних" звуків, які засновані на особливостях сприйняття звуку людським вухом. Процеси видалення "непотрібних" звуків називаються квантуванням. Чим менше ширина потоку, тим жорсткіше йде квантування.

Критерій, за яким оцінюється "непотрібність" звуку, є умова, заснована на такій особливості людського слуху, як нездатність більшості людей розрізняти сигнали, які по потужності лежать нижче певного рівня, причому цей рівень різний для різних частотних діапазонів. Оскільки звуки які виходять за поріг чутності людини непотрібні, переважна кількість кодеків викидає такі звуки. При цьому за значення порогу приймається величина рівна 16 kHz. При використанні психоакустичної моделі кодування MP3 CODEC автоматично викидає малопотужні, нечутні частоти. Але люди, які в змозі розрізнити саме ці частоти, часто скаржаться на втрату якості звучання при кодуванні, тоді як середньостатистична більшість цього не помічає.

[*] Науковий керівник – Гермак В. С., викладач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету

Найголовнішою особливістю психоакустичної моделі кодування MP3 є так званий ефект маскування. Саме завдяки цьому ефекту вдається так сильно стискати вихідні звукові дані. Суть цього ефекту в тому, що слабкий сигнал одного діапазону частот часто маскується більш потужним сигналом сусіднього діапазону, якщо він присутній в аудіозаписі, або потужним сигналом попереднього фрейму. Цей сильний сигнал викликає тимчасове зниження чутливості вуха до сигналу поточного фрейма. Для кожного звукового діапазону визначається величина маскуючого ефекту, створюваного сигналом сусідніх діапазонів і сигналом попереднього фрейму. Якщо маскуючий сигнал перевищує потужність сигналу поточного діапазону, то даний діапазон сигналу не кодують, що дозволяє психоакустичній моделі видалити якісь дані з цього фрейму. Для решти даних кожного діапазону визначається, скількома бітами на фрейм ми можемо пожертвувати, щоб втрати від додаткового квантування були нижче величини маскуючого ефекту. Безсумнівно, що звук, кодований при низьких бітрейтах, відрізняється крайньою нечіткістю і глухістю. Це відбувається через те, що при втраті одного біта інформації в загальне звучання вноситься шум квантування величиною близько 6 децибел.

Всі ці методи сумарно називаються адаптивним кодуванням. Використовуючи той факт, що переважна більшість людей не мають ідеального слуху, технологія адаптивного кодування дозволяє істотно зменшити розмір кодованого файлу, викинувши найменш значущі з точки зору слухового сприйняття деталі звучання.

Таблиця 1 – Порівняння звукових форматів

Назва формату	Ширина потоку (бітрейт)	Ступінь стиснення	Число каналів	Частота дискретизації (кГц)	Квантування, біт	Дата виходу
MP3	8—320	11:1 з втратами	до 2	8, 11.025, 12, 16, 24, 48, 32, 44.1	плаваючий	1993
AAC	8—529 (стерео)	з втратами	до 48 каналів	8—192	плаваючий	1997
WMA	4—768	2:1,є версія без втрат	до 8 і більше	8, 22.05, 16, 48, 32, 44.1, 88.2, 96	до 24	1999
Ogg Vorbis	до 1000	з втратами	до 255	8—192	до 32	2000

В наш час формат MP3 все ще є лідером за поширеністю, але при цьому не є найкращим за технічними параметрами. Порівнюючи сучасні формати стиснення аудіо можна прийти до висновку, що існують формати, які дозволяють отримати порівнянну якість, при меншій щільності. Йому на зміну йдуть нові формати: AAC, VQF, Ogg Vorbis, WMA, FLAC та інші. 23 квітня 2017 року розробники формату повідомили про припинення підтримки MP3.

Список використаних джерел

1. *MP3: прошлое, настоящие, будущее [Електронний ресурс]. – Режим доступу: http://www.videoton.ru/Articles/mp3.html*
2. *Сравнение цифровых аудиоформатов [Електронний ресурс]. – Режим доступу:* https://ru.wikipedia.org/wiki/Сравнение_цифровых_аудиоформатов
3. *Сэломон Д. Сжатие данных, изображений и звука.- Москва: Техносфера, 2004. — 368 с.*

УДК:004.023

Фесечко Д. В., Конопліцька-Слободенюк О. К.
Центральноукраїнський національний технічний університет

Методології розробки програмного забезпечення

Методологія розробки програмного забезпечення визначає головні принципи розробки, які залежать від певних чинників: розміру команди, складності проекту, часу відведеного на розробку, зрілості і стабільності процесів в компанії-роботодавця. Обирається методологія де ідея, способи, методи і засоби, які визначають стиль розробки ПЗ, дозволять вирішити поставлену задачу.

На сьогодні найбільш використовуючими та відомими методологіями є:

-Rational Unified Process (RUP) - методологія, яка була створена компанією Rational Software. Головне завдання RUP - максимально чітко розподілити роботу кожного учасника. При створенні проекту, проектувальники заздалегідь продумують всі основні питання.

-Extreme Programming (XP) — одна з найвідоміших гнучких методологій. Основними принципами методології екстремального програмування є: мінімум документації, постійне тестування, тісна комунікація. Головна мета: підвищення якості програмного забезпечення в умовах постійних змін вимог замовника.

-Structured Analysis and Design Technique (SADT) – методологія яка включає методи структурного аналізу і проектування систем. Основні характеристики даної методології включають управління, зворотній зв'язок і ресурси. Її використовують в багатьох областях: бізнесу, виробництва, обороні, зв'язку. SADT реалізує ідею «масштабного проектування на початку розробки».

-Rapid Application Development (RAD) — методологія, яка дозволяє приділити увагу швидкості та зручності програмування, дозволяє програмістові максимально швидко розробляти замовленні проекти. Цю методологію часто пов'язують із концепцією візуального програмування. Зазвичай RAD використовують у невеликих проектах, що розробляються для окремого замовника.

-Microsoft Solutions Framework (MSF) - методологія яка була розроблена компанією Microsoft. MSF була створена на практичному досвіді Microsoft і описує як найкраще розподілити робочі ресурси у процесі розробки. MSF має заданий набір правил, концепцій і моделей. Модель MSF була розроблена через недоліки традиційних проектних методологій.

Таким чином, методологія - це головні теоретичні відомості за допомогою яких відбувається управління розробкою якого-небудь програмного забезпечення. Методологію частіше всього обирають за загальними витратами на розв'язок певного завдання з заданими характеристиками, наприклад: фінансові розрахунки, наукові проекти, системи реального часу, тощо. Масштаб проекту та його ефективність є важливими факторами при визначенні методології програмування.

Список використаних джерел

1. *Технология разработки программного обеспечения [Електронний ресурс]. – Режим доступу : https://core.ac.uk/download/pdf/143995587.pdf*
2. *Методології розробки програмного забезпечення [Електронний ресурс]. – Режим доступу : https://uk.wikipedia.org/wiki/Метоологія_розробки_програмного_забезпечення.*

УДК 004

Четверик А. І.
Дніпровський національний університет ім. Олеся Гончара

Визначення коефіцієнтів розподілу грошових коштів за заходами

Для вирішення даного завдання необхідно проаналізувати дані за певний період і знайти частки розподілу грошових коштів на рекламу кожного заходу. Необхідна умова вирішення даної задачі (1):

$$\sum_{i=0}^{S} d_i = 1 \quad (1)$$

де d_i($0 < i < S$) – і-та доля вкладення грошових коштів у захід; S – кількість заходів.

$$d_i = \frac{L_i}{LS} \quad (2)$$

де L_i – відносна величина, що характеризує відвідуваність і-того заходу; LS – сумарна відвідуваність усіх заходів;

$$LS = \sum_{i=1}^{m} L_i \quad (3) \qquad L_i = GS - G_i \quad (4)$$

де GS – сумарна доля приросту глядацького інтересу; G_i– доля приросту глядацького інтересу до і-го захода. У табл.1 відображені дані про обсяги отриманого прибутку помісячно в розрізі заходів.

Таблиця 1

	Захід 1	Захід 2	Захід 3	Всього
січень	2000	3000	5000	10000
лютий	3000	2000	3000	8000

Розрахуємо частку приросту глядацького інтересу до першого заходу (5) та сумарну долю приросту глядацького інтересу(6). $G_1 = \frac{3}{2} = 1.5$ (5) $GS = \sum G_i = 2{,}7666667$ (6)

Розрахуємо відносну величину відвідуваності першого заходу (7) та сумарну відвідуваність всіх заходів(8).

$$L_1 = GS - G_1 = 2{,}7666667 - 1{,}5 = 1{,}2666667 \ (7) \qquad LS = \sum L_i = 5.533333 \ (8)$$

Розрахуємо коефіцієнти розподілу грошових коштів по заходах(9).

$$d_i = \frac{LS}{L_1} = \frac{5.533333}{1.2666667} = 0.228915663 \ (9)$$

Таким чином отримуємо матрицю розподілу грошових коштів по заходах.

	Захід 1	Захід 2	Захід 3	Всього
G_i	1,5	0,66667	0,6	2,767
L_i	1,266667	2,1	2,1667	5,533
d_i	0,228916	0,37952	0,3916	1

Список використаних джерел

1. Рябчій В. А. Теорія похибок вимірювань: навч. посібник.

УДК 681.5.015

Шевченко М. М.[*]
Харківський національний університет
міського господарства *імені О.М. Бекетова*

Хмарний сервіс зберігання даних

У сучасному світі у галузі інформаційно-комунікаційних технологій спостерігається бурхливий розвиток хмарних технологій. Відповідно до цього виникають численні хмарні сервіси, що все частіше застосовуються у різних сферах людської діяльності. Одним із найпоширеніших подібних сервісів є хмарні сховища даних. Ідею хмарних сервісів запропонували в 60-х роках Джон Маккарті і Джозеф Ліклайдер – відомі вчені у галузі штучного інтелекту та обчислювальної техніки. Але до недавнього часу хмарні технології були суто професійними, тобто недоступними або незнайомими для пересічного користувача. Тим не менш, можливість перетворити ”хмарність” у бізнес - для компаній, і зручність використання хмарних сховищ звичайними людьми, принесли їх у масовий Інтернет. Хмарне сховище даних - модель онлайн-сховища, в якому дані зберігаються на численних розподілених в мережі серверах, що надаються у користування клієнтам, в основному, третьою стороною.

Таким чином, замість розміщення файлів на носіях зовнішньої пам’яті (або на вінчестерах комп’ютерів) інструменти і результати роботи поступово переносяться та розміщуються у хмарному сховищі даних або у ”хмарі“. Хмара представляє собою сукупність серверів (центр обробки даних, ЦОД), часто віддалених один від одного на великі відстані, об'єднаних високошвидкісною мережею і виконуючих специфічні завдання. Точне число серверів назвати важко (компанії тримають його в секреті), на сьогодні кількість серверів оцінюється в 2-2,5 млн і прогнозується їх збільшення до 10 млн. ЦОД підключені до Інтернету безліччю каналів, і коли користувач заходить почитати пошту або відредагувати фотографії, він потрапляє на найближчий і найменш завантажений вузол, який здійснює обробку інформації. Як взаємодіють між собою сервери всередині інфраструктури - таємниця розробника. А завдання користувача полягає в тому, щоб увійти в Інтернет, пройти авторизацію на обраному сервісі (рис.1). За таких умов дані доступні з багатьох комп’ютерів. При цьому важливу роль відіграє те, що багато таких сервісів є безкоштовними або мають невисоку вартість. Серед переваг використання хмарних сховищ даних можна виділити такі: доступ до даних здійснюється з будь-якого місця та в будь-який час за наявності під’єднання до глобальної мережі Інтернет; користувач сплачує тільки за те місце у сховищі, яке фактично використовує або користується певним обсягом дискового простору хмарного сховища безкоштовно; економія дискового простору на жорсткому диску комп’ютера; усі процедури із збереження цілісності даних забезпечуються провайдером хмарного центру. До недоліків належать: небезпека у процесі зберігання та пересилання даних, особливо конфіденційних, приватних; загальна продуктивність при роботі з даними в ”хмарі” може бути нижчою, ніж при роботі з локальними копіями даних; необхідна наявність стабільного та швидкісного підключення до Інтернету.

Отже, основною різницею між хмарним сховищем даних та звичайними носіями даних є:синхронізація даних між різними комп’ютерами, резервне копіювання файлів з комп’ютера у “хмару”, спільна робота певної групи осіб з окремими файлами та папками.

Серед найпопулярніших на сьогодні компаній вважаються ”Dropbox”, ”Google”, ”Microsoft” та ін. Детальніше трійка лідерів серед хмарних сховищ виглядає так: 1.

[*] Науковий керівник – канд. техн. наук, доцент Дядюн С. В.

Перше місце за кількістю користувачів (понад 100 млн. чол.) займає ”Dropbox”. У процесі реєстрації в сервісі відбувається інтеграція в ОС, потім створюється папка для завантаження файлів з неї в хмару сервера. ”Dropbox” доступний також користувачам мобільних пристроїв. Користувачам надається 2 ГБ для зберігання своїх даних в режимі онлайн, також є вигідна пропозиція - реферальна програма, яка дає шанс безкоштовно збільшити дисковий простір. За більш широке місце на диску стягується щомісячна плата; 2. ”Google Drive” - хмарне сховище даних, створене компанією ”Google”, безкоштовний простір цього сховища доступний в розмірі 5 ГБ. Як варіант, можна сміливо інтегрувати сервіс з ”Google Docs”, ”Gmail” і ”Google+”. Перевагою є можливість резервного копіювання, що виступає гарантом збереження цінної інформації. Інтерфейс сервісу зручний і простий в управлінні; 3. ”Microsoft SkyDrive” від розробника ”Microsoft”. При реєстрації користувач отримує 7 ГБ простору на диску, але володарям ліцензійних версій продуктів ”Microsoft” надається вигідний пакет 25ГБ. Збереження файлів структуровано, задані параметри припускають 3 папки: документи, фото і загальна. Для мобільних пристроїв доступне завантаження фото і відео.

Рисунок 1 – Схема роботи хмарного сервісу зберігання даних

Конкретні рекомендації щодо вибору хмарного сервісу для зберігання даних дати не так легко, оскільки це залежить від потреб користувача, операційної системи, яку він використовує тощо. Для того потрібний сервіс варто обирати експериментальним шляхом. За останній час хмарні сховища даних набули великої популярності і є частиною нашого повсякденного життя. Хмарні технології інтенсивно розвиваються і надалі будуть ставати зручнішими та універсальними.

Список використаних джерел

1. *Барінов В. М. Хмарний сервіс зберігання даних / В.М. Барінов. − Київ: МП ”ОКО”, 2016. − 86 с.*
2. *Джонс Т. Анатомія хмарної інфраструктури зберігання даних/ Т. Джонс. – М.: ”МІФ”, 2014. − 65 с.*
3. *Трачук М. Хмарні сховища даних- четвірка лідерів. [Електронний ресурс] / М. Трачук. − Режим доступу: http://webklaster.com.ua/ua/stati/design/1655/*

УДК 004.054

Шуліка Я. П.[*]
Центральноукраїнський національний технічний університет

Сучасне on-page SEO

On-Page SEO - це оптимізація елементів HTML-сторінки контенту та тегів з метою підвищення «рейтингу» сайту в пошукових системах. Це поняття, «On-Site SEO» є американським аналогом вже вживаного терміна «внутрішня оптимізація сайту»: все що знаходиться на сайті.

Для того щоб отримати хороші результати від внутрішньої оптимізації сайту, сьогодні вже недостатньо просто слідувати наміченим чек-листам. Розкрутка сайту стала більш складним процесом. Тож які принципи гарної розкрутки сайту?

1. Задовольняйте наміри і цілі користувача. Кожен пошуковий запит має певну мету. Ми шукаємо інформацію, ми шукаємо шляхи вирішення проблем, сайт повинен задовольняти ці потреби. Часто буває що намір відрізняється від тексту у пошуковому запиті, це теж потрібно враховувати.

2. Швидкість. Google визначає ступінь задоволеності користувачів, спираючись на безліч прямих і непрямих ознак. У сторінок з низькою швидкістю завантаження дуже великий показник відмов, особливо з мобільних пристроїв. Сторінки, які вантажаться швидко, заробляють більше посилань і, відповідно, отримують від користувачів більше активності і взаємодії. Всі ці фактори, включаючи і саму швидкість завантаження, впливають на ранжирування сторінки в результатах пошуку.

3. Рівень довіри. Цей пункт пов'язаний з попереднім. Швидкість завантаження є значущою частиною вражень користувача (UX), і обидві ці сфери критичні для mobile-friendly-сайту.

4. Уникайте того, що відлякує користувачів. Деякі речі можуть збивати відвідувачів з пантелику, відбивати бажання повертатися на ваш сайт. Одна з найбільш поширених проблем цього плану - створення перешкод для споживання контенту, поп-апи, агресивна реклама та інше.

5. Оптимізація під ключові слова. Ключові слова на веб-сторінці є класичним фактором ранжирування, який на сьогоднішній день як і раніше актуальний.

6. Родинна тематика. Потрібно використовувати специфічні для тематики ключові слова, не нехтувати синонімами, та створювати контент для людей, тому що пошукові системи розбираються у семантиці, особливо google.

7. Оптимізація сніпетів. Оптимізована веб-сторінка повинна не тільки добре ранжируватися, а й мати такі теги, щоб залучати кліки користувачів. Якщо її CTR рівний чи більший для сайту на цій позиції – це також позитивний для пошукової системи знак, це означає що видача пошукової системи є релевантною, як і завжди.

8. Унікальна цінність та поширення. Ваш сайт повинен бути корисним для користувача, та мати переваги порівняно з іншими сайтами.

Це основні пункти сучасної внутрішньої оптимізації сайту, дотримуючись їх можна отримати та утримувати гарні позиції у пошуковій системі.

Список використаних джерел

1. *11 on-page Seo techniques[Електронний ресурс]. – Режим доступу: – https://www.reliablesoft.net/5-on-page-seo-techniques-thatll-boost-your-rankings-checklist-included/*
2. *On-page SEO[Електронний ресурс]. – Режим доступу: – https://backlinko.com/on-page-seo*

[*] Науковий керівник – Конопліцька-Слободенюк О. К., викладач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету

УДК 004.054

Шуліка Я. П.
Центральноукраїнський національний технічний університет

Біле та чорне SEO

Оптимізація веб-ресурсу є одним з важливих пунктів його просування та розкрутки. На сьогоднішній день існує декілька видів seo просування: біле та чорне.

І ніби все тут ясно: біле - добре, чорне - погано. Але буквально якихось 6-7 років тому те, що зараз ми називаємо чорним SEO, вважалося цілком нормальним. Досить було вписати ключові слова в генерований текст - і сайт за місяць влітав в ТОП-10.Ці часи минули, пошукові системи запускають нові алгоритми, і тепер все частіше при пошуку потрібної інформації ми потрапляємо дійсно на якісні ресурси з корисним контентом.[1]

Біле SEO, або "білий капелюх", або "етичні" методи SEO - потребують більше часу та зусиль ніж чорне SEO. Методи призначені для отримання пошукового трафіку з високоякісним контентом та можуть включати в себе такі методи:

Забезпечення якості посилань. Посилання мають бути на релевантних сайтах і діяти як "голосування" для вашого сайту.

Створення оригінального, високоякісного контенту.

Використання ключових слів і аналізу ключових слів

Організація сайту, за допомогою тегів заголовків та форматування тексту так, щоб пошуковий робот розумів структуру тексту.

Потрібно використовувати ключові слова у метатегах, таким чином, щоб вони відображали про що ваш контент.

Поліпшення навігації, інформаційної архітектури та назв. Це може бути як розміщення вашого сайту, так і метадані та назви сторінок. Вони також можуть додавати описи та альт-текст до зображень та розмітки.

Крім того, зазвичай пошукова система надає посібник із прийнятних методів SEO.

Ці методи вимагають багато часу і зусиль, але вони того коштують - навіть неактуальний контент може продовжувати збільшувати ваш трафік при дотриманні рекомендацій, без штрафних санкцій.

Що таке чорне SEO?

Методики чорного SEO оптимізують сайт лише для алгоритмів, а не для людей. У певному сенсі це "обманює систему", щоб отримати позиції у системі швидко. Але, за такі дії пошукова система може занизити позиції сайту або видалити його з індексу.

Техніка чорного SEO може включати в себе:

Використання спаму, чужого контенту, чи автоматичного контенту.

Автоматизоване створення посилань на сайт.

Спроба зняти конкурента з негативною кампанією або зловмисне повідомлення пошукової системи про те, що конкурент начеб то використовує чорні методики.

Клоакінг – видача різних даних користувачу і пошуковій системі.

Використання сайтів доступ до яких був отриманий незаконно.[2]

Тож для звичайного бізнесу краще всього використовувати біле SEO, тому що не можна ризикувати, це загрожує існуванню бізнесу клієнта. Чорні методи, як правило, використовують на сайтах, що швидко повернуть гроші або мають незаконну тематику.

Список використаних джерел

1. *Чорне та біле Сео [Електронний ресурс]. – Режим доступу: – http://websoveti.com/ %D1%87%D1%91 D0%BD%D0%BE%D0%B5-%D0%B8-%D0%B1%D0%B5%D0%BB%D0%BE%D0%B5-seo/.*
2. *Біле сео проти чорного[Електронний ресурс]. – Режим доступу: – https://www.upwork.com/hiring/marketing/white-hat-seo-vs-black-hat-seo/*

УДК 004.054

Шуліка Я. П.[*]
Центральноукраїнський національний технічний університет

Сучасне off-page SEO

Off site SEO або Off page SEO - це комплекс зовнішніх по відношенню до сайту заходів, спрямований на збільшення відвідуваності сайту цільовими клієнтами з пошукових систем, робота з посиланнями, залучення посилань з інших сайтів на просувний сайт, або просто побудова посилальної маси на сайт що просувається. Це один з найбільш значущих чинників, що відбивається на успішному просуванні ресурсу в Інтернеті.

Рекомендацією сайту є посилання на нього. Чим більше посилань на сайт розміщено в мережі, тим частіше його рекомендують - це серйозно підвищує авторитет ресурсу в пошуковій системі. Але при виборі ресурсів, що будуть рекомендувати ваш сайт, потрібно бути обережним та враховувати такі фактори, як: довіра сайту, тематичність, чи не використовує сайт спам, тобто це повинен бути дуже гарний сайт.[1]

Посилання можна поділити на декілька груп:

Природні - посилання знаходяться на тематичних форумах чи каталогах.

Соціальні – посилання у соціальних мережах. Мають найнижчий ефект для ранжування, але можуть дати трафік на сайт.

Тимчасові – коли ви купуєте посилання у іншого сайту та оплачуєте кожний місяць, для того щоб ці посилання на сайті залишилися.

Постійні – ви купуєте посилання у іншого сайту, як мінімум на рік. Якщо є змога купити такі посилання з великих та тематичних сайтів – це найкращий варіант.

На якість посилання також впливає текст посилання, тобто анкор. Існують такі види анкорів:

Природні – анкори по типу «тут», «на сайті», тобто такі, які зазвичай залишає звичайна людина на форумі.

Брендові – тобто з назвою бренду, чи сайту.

Прямі – анкор це точне ключове слово, яким користувачі шукають ваші послуги. Мають найсильніший ефект для просування, але занадто велика кількість таких анкорів може викликати підозри у пошукової системи на те, що ви зловживаєте алгоритмами зовнішнього ранжування та накручуєте показники для пошукової системи, це може призвести до санкцій на сайт.

Забагато прямих анкорів називається спамом, щоб розбавити тип посилань на сайт, також роблять перефразовані посилання, посилання зі словоформ основних ключових слів, або ключові слова можуть бути розбавлені іншими словами у посиланні.[2]

Тож як взагалі можна отримати посилання на ваш сайт?

Серед білих методик, що завжди рекомендуються спеціалістами – це створювання подій, конкурсів, знижок, усе що завгодно, щоб про вашу фірму говорили, а ще краще – добре говорили.

Іноді це складно реалізувати, а для деяких тематик і взагалі неможливо, тому також використовуються інші методи.

Біржі посилань. Найпростіший спосіб, що дозволяє отримати посилання на ваш сайт - це, звичайно ж, покупка. Є багато різних бірж пропонуючих багато різних посилань, потрібно мати досвід у тематиці, щоб підібрати посилання, що дійсно дасть поштовх для сайту.

Коментарі на форумах та блогах. Підберіть блоги і форуми з аналогічною тематикою, беріть участь в обговореннях та залишайте там змістовні коментарі,

[*] Науковий керівник – Смірнов С. А., канд. техн. наук, старший викладач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету

додаючи в них посилання на свій сайт (інакше кажучи, використовуйте крауд-маркетинг). При правильному підході ця стратегія не лише дасть вашому сайту посилання, а ще й трафік.

Обмін посиланнями з сайтами схожої тематики. Важливо щоб посилання з обох сторін були релевантними та тематичними. Якщо посилання будуть виглядати як «За що зозуля хвалить півня? за те що хвалить він зозулю.» - можна отримати санкції від пошукової системи.

Посилання з соціальних мереж. Соціальні акаунти - це саме благодатне поле діяльності, що надається вам абсолютно безкоштовно. Спільноти, групи, сторінки заходів - все це ви можете використовувати для розміщення своїх посилань і залучення нових клієнтів, тобто окрім посилань ви також будете отримувати і трафік.

«Аутріч» кампанія – зв'яжіться з володарями хороших сайтів, можливо хтось згодиться створити посилання на ваш сайт на умовах, що вас влаштують? Або ж запропонуйте їм та почніть переговори.[3]

Приватна сітка сайтів. На даний час один з найефективніших та найдешевших способів отримати гарні позиції у пошуковій системі, іноді, навіть трафік. Потрібно створювати сайти схожої тематики, створити видимість, що це живі сайти, інших людей та створити ніби природню сітку посилань між цими сайтами та сайтом для просування.

Сітку можна як будувати з нуля, так і піднімати вже готові сайти. Будуючи з нуля потрібно також попрацювати над кожним сайтом, придумати йому тематику, знайти контент, зазвичай цим займається велике агенство, що має спеціальний відділ.

Піднімати вже готові сайти може кожен, потрібно лише знайти сайт з хорошою історією, що продається, викупити його, відновити на ньому контент, ніби це минулі користувачі сайту, та додати посилань на свій сайт, або взагалі створити переадресацію з того сайту на ваш, ніби той сайт завжди був вашим, тоді пошукова системи об'єднає ваші показники та ваш сайт матиме кращі позиції.[4]

При цьому слід постійно бути обережним, пошукові системи не полюбляють коли маніпулюють зовнішніми факторами ранжування та можуть накласти санкції на ваш сайт за це. Можна видати сітку написавши одну контактну пошту на кожному сайті або навіть просто якщо реєструвати сайти на одну пошту, або будь які інші підозрілі збіги, що можна знайти. Один з варіантів як цього можна досягти – проставляти посилання з якомога меншою закономірністю, ідеальний варіант якщо у вас є декілька проектів яким потрібне посилання однієї тематики, тоді можна зробити посилання більш природніми, а не такими, що сайти однаково посилаються на однаковий сайт. [5]

Наскільки б ідеальною не була б ваша внутрішня оптимізація, як не крути, їх не вистачить, щоб обігнати гігантів, що сидять у топ 1-3 вже роками, для цих цілей вам необхідна гарна зовнішня оптимізація. До того ж потрібно бути готовим до негативних зовнішніх кампаній у ваш адрес від конкурентів, якщо це дуже конкурентна тематика. А коли ви досягнете топ 1, то потрібно постійно оптимізувати та моніторити сайт, щоб удержатися на цій позиції, особливо небезпечними можуть бути негативні кампанії від конкурентів, навіть повністю білі проекти у просуванні яких не використовувалися чорні і сірі методики можуть бути жертвами спаму від конкурентів та навіть бути видаленими з індексу пошукових систем.

Список використаних джерел

1. *What is off-site seo?[Електронний ресурс]. – Режим доступу: – https://moz.com/learn/seo/off-site-seo*
2. *The Best off-site seo techniques[Електронний ресурс]. – Режим доступу: – https://www.crazyegg.com/blog/seo/off-page/*
3. *25 off Page SEO strategies[Електронний ресурс]. – Режим доступу: – https://ignitevisibility.com/off-page-seo/*
4. *Створення PBN під певний проект[Електронний ресурс]. – Режим доступу: – https://seoprofy.ua/blog/na-doske/nomer-227*
5. *Динаміки проставлення посилань з PBN[Електронний ресурс]. – Режим доступу: – https://seoprofy.ua/blog/na-doske/nomer-240*

УДК 681(004.891.3)

Щербак В. К.
Харківський національний університет радіоелектроніки

Використання сенсору Kinect в системах диагностування рухомих об’єктів

На даний момент у зв'язку із розвитком технічного прогресу стали доступними для рядових користувачів такі технології, які раніше лише здавалися фантастикою та не мали можливості бути застосованими у реальному житті. Це машине навчання, нейроні мережі, комп’ютерний зір, віртуальна реальність, доповнена реальність, тощо. Такі гіганти ІТ-індустрії, як Tesla, Boston Dynamics, Google, Microsoft, Motorola Solutions застосовують їх у своїх виробах (безпілотні автомобілі, окуляри, пошукові мережі, системи безпеки). Тому актуальним є питання діагностування динамічних, рухомих об’єктів у тривимірному просторі, що дозволить вирішити кілька проблем сучасності:

1. моніторинг об’єктів на шляху руху транспорту, а отже кардинальна мінімізація аварій і практично повне виключення людських жертв, а значить і витрат на страхування і медицину;
2. зниження вартості транспортування вантажів і людей за рахунок економії на заробітній платі і часу відпочинку водіїв, пілотів та обслуговуючого персоналу, а також економії палива;
3. підвищення ефективності використання транспортних шляхів за рахунок централізованого управління потоком;
4. поява можливості самостійно пересуватися на транспортному засобі без спеціального посвідчення;
5. відстеження руху людей у віці та завчасне попередження падінь та травмувань;
6. охорона та завчасне виявлення злочинців на вулицях та охороняємих об’єктах.
7. перевезення вантажів та особового складу під час природних і техногенних катастроф або військових дій.

Однак сучасні системи діагностування об’єктів мають вагомі недоліки на даному етапі вирішення таких задач. Це досить висока вартість обладнання, проблеми при обробці зображення в умовах поганої видимості, недостатня база для навчання штучного інтелекту, потреба розробки спеціальних модулей для окремих задач.

Одна з особливостей датчика Kinect - відновлення 3D-сцени простору, що знаходиться в полі зору пристрою. Варіантом альтернативних технологій в даному напрямку є стереозір. Він заснований на принципі роботи людського зору - на об'єкт спрямовані дві еталонних камери і потім, за допомогою проективної геометрії, обчислюється відстань до об'єкта, або відновлюється 3D-модель простору. Така технологія має суттєві недоліки: неможливість коректно відновлювати простір, який знаходиться за прозорими об'єктами (наприклад вода). Існуючі лазерні далекоміри позбавлені недоліку стереозору, але вони не можуть передати інформацію про повну характеристику сцени (наприклад яскравість), мають велике енергоспоживання і високу вартість.

Сенсор Kinect є дешевою заміною традиційним технологіям, він отримує хмару точок і за допомогою відповідного програмного забезпечення можна відтворити сцену, яка характерна для лазерних далекомірів,. Також сенсор має цифрову камеру, що дозволяє при накладенні фото на карту глибини простору відновити характеристику яскравості. [1]

У статті "Microsoft Kinect зараз охороняє корейський кордон" розповідається про застосування даного датчика комп'ютерного зору для виявлення людей, що перетинають демілітаризовану зону. Як переваги була виділена та особливість сенсора, що він може відрізнити людину від тварини. І в разі виявлення першої, попередить найближчі форпости про незаконне проникнення. В майбутньому планується оновити прошивку Kinect, щоб він зміг визначати частоту серцебиття і тепло, яке виділяється тілом. [3]

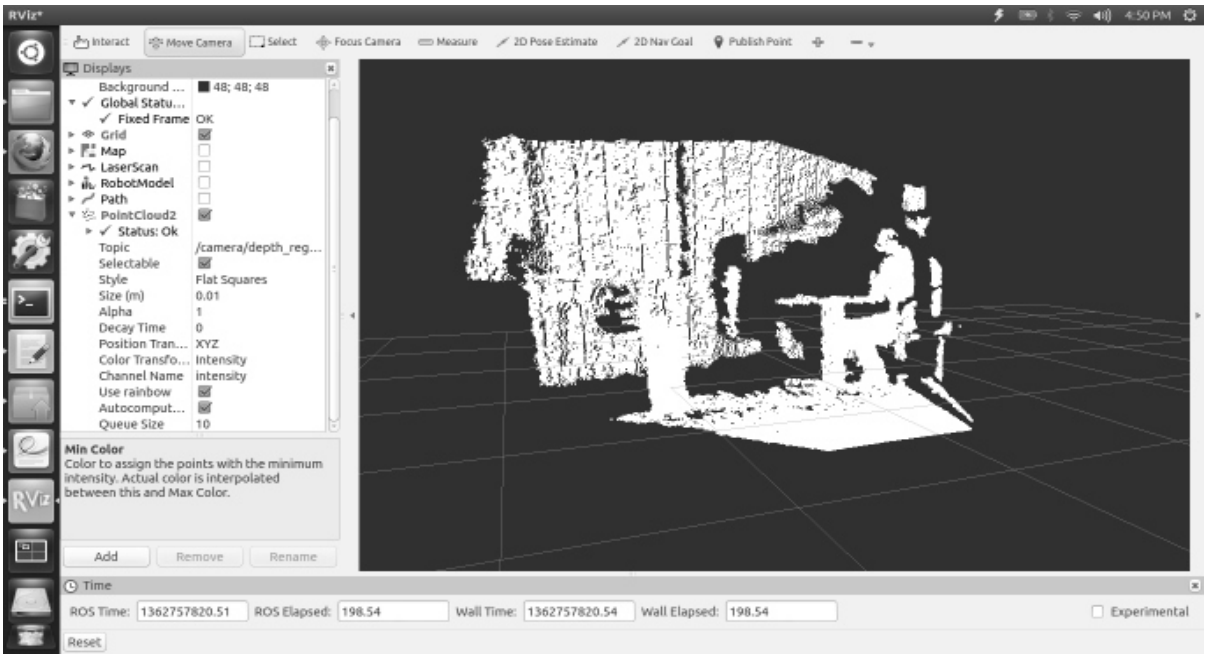


Рисунок 1 — Отримання хмари точок за допомогою Kinect [2]

Автори статті "Survey on fall detection and fall prevention using wearable and external sensors" пояснюють, що на даний момент падіння становлять велику загрозу для людей похилого віку й часто завдають їм травми. Для вирішення цієї проблеми пропонується використовувати системи виявлення і запобігання падінь. В системах використовується велике число датчиків, в тому числі і сенсори комп'ютерного зору, такі як Microsoft Kinect. [4]

Як висновок можна сказати, що сенсор Kinect є унікальним пристроєм, який можна ефективно використовувати в якості комп'ютерного зору в робототехніці, 3D-скануванні, розпізнаванні жестів, міміки й мови, в системах спостереження за об'єктами, що охороняються, такими як державні кордони і демілітаризовані зони, для відстеження положення тіла людини, розпізнавання падінь або непритомності і безлічі різних сфер. Основна його перевага над іншими пристроями машинного зору - ціна і доступність як для професіоналів, так і для любителів-ентузіастів.

Список використаних джерел

1. *Белова Н.В., Томилина А.И., Горошкин А.Н. Автоматизированная виртуализация пространства // Актуальные проблемы авиации и космонавтики. 2014. №10.*
2. *URL:* https://habr.com/post/396291/ *(дата звернення 13.10.2018)*
3. *URL:* https://kotaku.com/microsofts-kinect-is-now-guarding-the-korean-border-1514792443 *(дата звернення 13.10.2018)*
4. *Delahoz YS, Labrador MA. Survey on fall detection and fall prevention using wearable and external sensors. Sensors (Basel). 2014 Oct 22;14(10):19806-42. doi: 10.3390/s141019806. PubMed PMID: 25340452; PubMed Central PMCID: PMC4239872.*

УДК 004:621.391
Щербак Б. В.
Харківський національний економічний університет імені Семена Кузнеця

Розробка модулю автоматизованої системи для подачі матеріалу студентам за допомогою технологій доповненої реальності

Освіта – одна з головних речей в житті людини. Здобути освіту має прагнути кожен, знання нікому ще не заважали, навпаки. Освічені люди були в пошані з давніх часів. Сучасний світ, яким ми його сьогодні бачимо, з новітніми технологіями – все це зробили дуже розумні люди. Природні таланти людина повинна розвивати за допомогою самоосвіти. Активне читання книжок, наукової літератури допомагає здобути нові знання. Але сучасна молодь звикла отримувати інформацію за допомогою смартфонів та інтернету. Таким чином дуже важливим кроком у зацікавленості та подання матеріалу у Харківському національному економічному університеті імені Семена Кузнеця відіграє інтерактивна форма подачі матералу за допомогою відео контентк та сучасних технологій, таких як доповнена реальність.

Саме за допомогою таких технологій, як доповнена реальність студенту буде цікавіше отримувати матеріал. Ця технологія дає змогу студенту використовувати свій телефон на лекційному занятті, а саме відеокамеру телефону, яка дивиться на візитку викладача, або логотип спеціальності та на цій площині з'является відео контент. Таким чином лекції перетворюються в цікаву гру, а матеріал лекцій надовго залишається у пам'яті студента. Таким чином викладач родить свою роботу за допомогою методу "гра, як метод наввчання" [9].

Перевагою для Харківського національного економічного університету імені Семена Кузнеця є те, що цей додаток побудований за допомогою новітніх технологій та вже містить у собі відео контент кафедри кібербезпеки та інформаційних технологій. Створення додатку буде вестися на основі кросплатформенного програмування на Unity3D [5] та ASP.NET Core [3], з використанням Entity Framework 6 Code First [4], через те, що веб-ресурси дуже універсальні і практичні в користуванні. Для того, щоб створити мобільний додаток використоыувалась технологія vuforia 7.0 [8]. Дана технология дозволяэ розробляти мобільні додатки на такі системи, як IOS або Android, використовуючи камеру мобільного телефону та штучний інтеллект для знаходження маркеру (картинки або логтипу). Існують два види мобільних додатків, які використовують таку технологію: розташування предметів на маркері та розташування предметів на землі(тобто пошук землі та після пошуку розташування медіа контенту на землі, яка маэ назву Ground Plane [7]). Для забезпечення зв'язку між сайтом та мобільним додатком буде використана технологія Rest API [6]. Таким чином адміністроатор данного программного продукту має змогу розмістити на панелі адміністратора відео контент та зберегти його на конкретній візитці, або логотипі, а мобільний додаток автоматично за допомогою інтернету зможе оновити данні та показати цей відео контент кінекому користувачу.

Список використаних джерел

1. *Про вищу освіту / Закон України від 17.01.2002 р. № 2984 – III (зі змінами та доповненнями), 2002 р.*
2. *Положення про організацію навчального процесу у ВНЗ МОН України / Наказ Міністерства освіти України № 161 від 02.06.1993 р.*
3. *Get Started with ASP.NET Core and Entity Framework 6 [Electronic resource]. – Access mode: https://docs.microsoft.com/en-us/aspnet/core/data/entity-framework-6?view=aspnetcore-2.1.*
4. *Entity Framework 6 [Electronic resource]. – Access mode:* https://docs.microsoft.com/en-us/ef/ef6/.
5. *Unity 3D [Electronic resource]. – Access mode:* https://unity3d.com/ru.
6. *Rest API – Access mode:* https://ru.wikipedia.org/wiki/REST
7. *Ground planeI – Access mode:* https://library.vuforia.com/articles/Training/ground-plane-guide.html
8. *ViforiaI – Access mode:* https://library.vuforia.com/content/vuforia-library/en/getting-started/overview.html
9. *Гра, як метод навяання – Access mode:* http://ua-referat.com/Гра_як_метод_навчання_та_виховання

УДК:004.38
Берладін В. К., Конопліцька-Слободенюк О. К.
Центральноукраїнський національний технічний університет

Квантові технології сьогодення та перспективи їх розвитку

У сучасному світі технології розвиваються швидше, ніж будь-коли. Однією з пріоритетних галузей розвитку є робота з квантовими технологіями, а саме створення квантового комп'ютера. Квантовий комп'ютер здатний за лічені секунди вирішувати завдання, на які навіть найпотужніший суперкомп'ютер витратив би кілька років.

Ще на початку розробки комп'ютерних схем було відомо, що обчислювальна потужність не безмежна, але не було відомо, коли настане ця межа. Однак вже зараз перед людством постають все більш складні завдання, для вирішення яких навіть найпотужніших рішень стає недостатньо. Наприклад сучасні банки використовують криптографічні системи захисту, принцип якої заснований на розкладанні простих чисел на множники. Квантовий комп'ютер зміг би робити розрахунки настільки швидко, що будь-яка банківська транзакція стала доступна, на що зараз комп'ютери не здатні. Але не виключається ризик використання квантових технологій зловмисники в своїх цілях. На сьогоднішній день квантові комп'ютери досліджують багато вчених і великі компанії, такі як Google, IBM, Microsoft та інші.

Квантовий комп'ютер - це тип комп'ютера, який використовує квантову механіку, щоб він міг виконувати певні види обчислень ефективніше, ніж звичайний комп'ютер. У звичних нам комп'ютерах за представлення інформації відповідають біти - 0 і 1, в квантових комп'ютерах замість звичних бітів використовуються квантові біти (кубіти). Кубіт, як і біт, має як і раніше два значення, які він може приймати: 0 і 1. Але існує властивість квантових об'єктів під назвою «суперпозиція» де кубіт може приймати всі значення, які є комбінацією основних. Але також при цьому його квантова основа дозволяє йому одночасно перебувати у всіх станах.

Саме в цьому полягає паралельність квантових обчислень з кубітами. Все відбувається відразу - зникає потреба перебирати всі можливі варіанти станів системи, на відміну від того, чим займається звичайний комп'ютер. Це дає можливість швидкого пошуку по величезних баз даних, створення оптимального маршруту, розробка нових ліків, і це тільки декілька прикладів завдань, на вирішення яких можна буде витрачати в багато разів менше часу завдяки використанню квантових алгоритмів. В основному це будуть завдання, де для пошуку вірної відповіді потрібно перебрати величезну кількість варіантів.

Дослідження проходять в дуже швидкому темпі, так безліч національних, урядових і військових структур підтримують матеріально дослідження квантових обчислень для подальшого створення квантових комп'ютерів, як для цивільної, так і для безпеки національного рівня. Якщо великомасштабні квантові комп'ютери будуть створені, то вони зможуть вирішувати певні завдання значно швидше, в порівнянні з будь-яким сучасним класичним комп'ютером. Простим прикладом може бути алгоритм

Шора, який направлений на вирішення завдання з розкладання чисел на прості множники, наприклад завдання факторизації дискретного логарифма, який використовується для шифрування.

Якою б не була перспективною квантова технологія, в ній існують деякі проблеми.

Інтерференція. Під час фази обчислення квантового розрахунку, найменший сплеск у квантовій системі (наприклад, розсіяний фотон або хвиля електромагнітного випромінювання) призводить до краху квантового розрахунку, що називається де-когерентністю. Квантовий комп'ютер повинен бути повністю ізольований від всіх зовнішніх перешкод під час фази обчислення. Проте успіх був досягнутий з використанням кубітів в сильних магнітних полях з використанням іонів.

Корекція помилок. Оскільки дійсно ізольована квантова система виявилася настільки складною, що були розроблені системи корекції помилок для квантових обчислень. Кубіти не є цифровими бітами даних, тому вони не можуть використовувати звичайну (хоч і дуже ефективну) корекцію помилок, таку як потрійний надлишковий метод. З огляду на природу квантових обчислень, виправлення помилок є вкрай критичним - навіть одна помилка при обчисленні може привести до краху всього обчислення. У цій області був досягнутий значний прогрес з розробкою алгоритму корекції помилок, який використовує 9 кубітів (1 обчислювальний і 8 корекційних). Зовсім недавно відбувся прорив IBM, який робить загалом 5 кубітів (1 обчислювальний і 4 корекційних).

Необхідність спостереження за виконанням. Ризик пошкодження даних залишається дуже високим, для прикладу у квантового комп'ютера з 500 кубітами у нас є ймовірність 2500, що дані будуть пошкоджені після завершення розрахунків.

Визнаючи обмеження, навіть Гордон Мур пророкує кінець свого однойменного Закону Мура до 2025 року. Темпи розвитку технологій і інновацій в області обчислень тільки набирають обертів з кожним роком. Це викликає настільки ж швидке зростання обсягу і складності задач, які щоразу перевіряють межі обчислювальної потужності сучасних комп'ютерів. За деякими даними повномасштабне застосування квантових комп'ютерів може стати реальністю вже через якісь 10 - 15 років.

Використання квантового комп'ютера в домашніх умовах

Прикро, але використовувати квантовий комп'ютер у себе вдома поки що неможливо. Для існування кубіта в стані суперпозиції на невизначено довгий термін потрібні особливі умови: температура близько 0 градусів за Кельвіном (для надпровідності), вакуум (відсутність сторонніх часток), електромагнітне випромінювання має дорівнювати нулю (для запобігання будь-якого впливу на систему). Якщо буде хоча б якесь відхилення від вимог, це може привести до зникання стану суперпозиції, відповідно результати обчислення не будуть вірними.

Я вважаю, що за квантовими комп'ютерами майбутнє. Враховуючи швидкість розвитку, це майбутнє настане вже дуже скоро. Особливо це потрібно медицині, і хімії зокрема, для моделювання ДНК, хімічних реакцій тощо. І можливо, саме завдяки квантовим технологіям буде створено ліки проти більшості невиліковних хвороб, і стане можливим вдосконалення генетичного коду людини, ще до народження, задля уникнення проблем зі здоров'ям в майбутньому.

Список використаних джерел

1. *Китаєв А. Шень А. В'ялий М. Класичні та квантові обчислення. Навчальний посібник. – Москва: Московський центр безперервної математичної освіти, 1999.*
2. *https://www.nkj.ru/archive/articles/5309/*
3. *https://habr.com/post/401315/*
4. *phys.org/news/2016-05-ibm-users-quantum.html*
5. *К.А.Валиев, А.А.Кокин: Квантові комп'ютери. Надії та реальність. Навчальний посібник. – Іжевськ:РХД, 2001.*

УДК 004.9

Горбань А. С., Цололо С. О.
Донецький національний технічний університет

Декомпозиція першого технологічного циклу синтезу оксидних нанопорошків

Розвиток сучасної індустрії все більше зміщується у бік застосування високотехнологічних продуктів, що зорієнтовані на експлуатаційні властивості кінцевого продукту [1]. Створення таких продуктів невід'ємно пов'язано із розвитком нового напрямку матеріалознавства – нанорозмірних оксидних матеріалів. Це обумовлює необхідність створення та впровадження у виробництво принципово нових технологій отримання наноматеріалів, що містять прийоми та методики, які дозволяють керувати властивостями таких матеріалів. Зазвичай трансфер від лабораторної технології до виробничої займає певний час та значні інвестиції, що стосуються не тільки масштабування обладнання, але й підготовки персоналу. Останнє пов'язано насамперед з різними принципами планування та контролю експерименту в умовах наукової лабораторії та виробництва. Якщо лабораторний експеримент все ще є експериментом ручного режиму, то експеримент у виробництві у більшості своєї є автоматизованим та запрограмованим на вихід здебільшого одного продукту. Тому існує певний дисонанс між навичками планування та проведення експерименту, отриманими студентами та стажерами у лабораторіях, та тими навичками, які вони мають мати для опанування виробничого експерименту. Певний виходом з цієї ситуації є створення смарт-лабораторій, у яких комп'ютеризація процесу буде використана не тільки для асистування при проведенні хімічного синтезу (комп'ютерні розрахунки, бази даних, софт для обчислення даних, програми візуалізації, тощо), але й виконувати також виконавчу й контролюючу та керуючу функції в процесі лабораторного хімічного синтезу (автоматизоване обладнання, система датчиків, тощо). Відзначимо, що перша частина активно розвивається у технологіях електронної науки, непаперових лабораторіях, грід-кластерах та інше [2], тоді як друга частина розвивається у лабораторній практиці значно повільніше [3]. На жаль, якщо окремі елементи установок для хімічного синтезу хоча й обладнаютьсяпрограматорами, все ще не існує автоматизованої системи для проведення синтезу оксидних наноматеріалів методами м'якої хімії. Однак реалізація цього є дуже важливим кроком у створенні певної навчально-наукової платформи для взаємного трансферу знань та сучасних технологій між лабораторією та виробництвом.

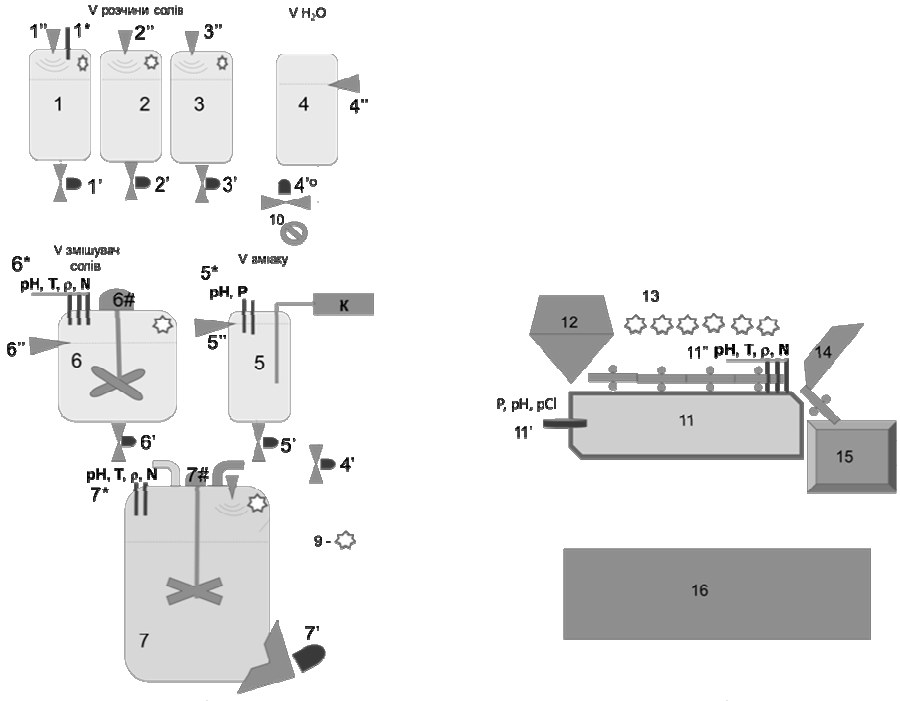
Отже, метою роботи є аналіз хімічного процесу осадження хімічного синтезу наноматеріалів та його декомпозиція для подальшої апаратно-програмної реалізації в рамках створення системи планування та проведення експериментів.

Для компьютерізації роботи фізико-хімічної лабораторії її структура була представлена у вигляді модульної системи: підсистема роботи з даними, підсистема планування експерименту, підсистема виробництва наноматеріалів, підсистема аналізу готового продукту. Підсистема виробництва наноматеріалів є головною в структурі комп'ютеризованої системи фізико-хімічної лабораторії наноматеріалів. Апаратне рішення підсистеми повинне відповідати технології, що обрана для отримання наноматеріалів. У фізико-хімічної лабораторії ДОНФТІ ім. О.О. Галкіна НАН України використовується технологія м'якої хімії, в основі якої лежить метод со-осадження солей різних металів агентами-осадниками. Процес отримання оксидних порошків за такою технологією звичайно можна розбити на два незалежні технологічні цикли:

1. Хімічний синтез аморфного гідрогелю.
2. Формування оксидних наночастинок.

В свою чергу, перший технологічний цикл складається із змішування розчинів солей металів, осадження та фільтрації гідрогелю металу (або гідрогелів металів у разі багатокомпонентної системи).

Перша стадія першого циклу реалізується за рахунок протікання реакцій між солю та агентом-осадникам, за результатами реакцій утворюється осад необхідного складу. Тип та кількість солей металів визначається типом та складом комплексного оксидного матеріалу, який синтезується, а тип та кількість агента-осадника природою – сполуки, що отримується. При проведенні хімічного синтезу треба контролювати ще декілька параметрів – pH процесу; температуру; тиск; наявність іонів хлору, або інших іонів, якщо для синтезу вибирається інша сіль металу ніж хлоридна; кількість неосаджених іонів металу в фільтраті осаду, час перемішування тощо. Цей процес потребує забезпечення взаємодії цілого ряду об'єктів хімічної технології, зокрема резервуарів, змішувачів, реактору та накопичувача осаду, за допомогою виконавчих пристроїв (датчиків температури, pH-метрії, контролерів потоку та часу тощо). Загальна схема технологічного циклу представлена на рис. 1.



а) б)

Рисунок 1 – Схема технологічного циклу синтезу синтезу:
а) осадження; б) фільрування

Планування синтезу повинне врахувати виконання таких основних етапів.

1. Задаються об'єми розчинів солів певної концентрації, що розміщені в сосудах 1-3 (V_1, V_2, V_3). Сосуди обладнані ультразвуковими вимірювачами рівнів та кранами-дозаторами. Співзіставлення даних з цих приладів у разі коли сума об'ємів V_1, V_2, V_3 дорівнює об'єму у змішувачі 6 (V_6) дозволяє перейти до наступного етапу.

2. Запускається ротор змішувача мішалки 6# та реле часу. Датчики 6* контролюють параметри у змішувачі та у кінці змішування параметри записуються в базу даних. Тривалість цього етапу визначається часом змішування і після його зупинки виконується перехід до 4-го етапу.

3. Етап запускається паралельно із 2-им етапом та керує кількістю об'єму аміаку, що необхідно додати в реактор 7 з ємності 5 через кран-дозатор (5') і включає компресор (К) для забезпечення додаткового тиску у ємності 5.

4. У реактор додаються певні об'єми солей зі змішувача, запускається робота реактору та забезпечується вихід осаду з реактору у накопичувач 12.

5. Запускається орошаючий пристрій для послідовної мийки сосудів 1-3, змішувача 6 та реактору 7.

Етапи 1, 2, 4 та 5 запускаються послідовно, етап 3 є паралельним із етапом 2.

На другій стадії першого технологічного циклу протікає процес фільтрування отриманого на першій стадії осаду. Для фільтрація осаду використовують вакуумне фільтрувальне обладнання (11) з системою водного орошення осаду (13), що переміщується на транспортері фільтру.

На 6-му етапі запускає фільтрувальне обладнання, вмикаються датчики параметрів промивки осаду pH, що контролюють кількість остаточних іонів в розчині. Окрім того, приводиться до дії скребок, що збирає продукт першої технологічної стадії в накопичувач 15 та включає реле часу мийки фільтру і орошаючий пристрій 13 (рис. 1б).

На основі аналізу схеми першого технологічного циклу синтезу оксидних нанопорошків та виділення основних етапів циклу побудована відповідна діаграма декомпозиції (рис. 2). Такий підхід дозволив виділити основні етапи процесу та побудувати зв'язки між ними, описати послідовність виконання робіт першого технологічного циклу та описати об'єкти, що приймають в ньому участь.

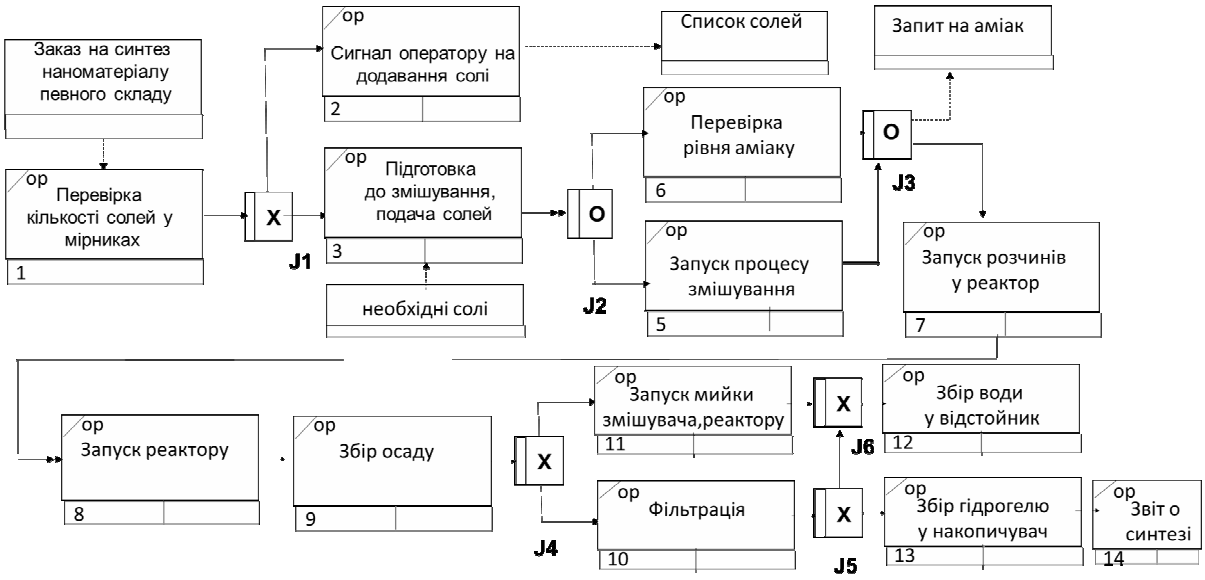


Рисунок 2 – Діаграма декомпозиції першого технологічного циклу синтезу оксидних нанопорошків

Таким чином, у роботі проаналізована організація фізико-хімічної лабораторії наноматеріалів та визначена схема першого технологічного циклу основного модулю виробництва наноматеріалів. На основі цих даних побудована діаграма декомпозиції першого технологічного циклу синтезу оксидних нанопорошків.

Список використаних джерел

1. *Greg Tegart Nanotechnology: The Technology for the 21st Century// Proceeding of the second international conference on technology foresight, Tokyo, 27-28 February 2003. –P. 1-12.*
2. *Frey J.G. Dark Lab or Smart Lab: The Challenges for 21st Century Laboratory Software. //Org. Proc. Res. Dev.- №8.-2004. - P. 1024-1035*
3. *Hans Schuler Automation in Chemical Industry // Automatisierungstechnik. -54 (8).-2006. – P. 363-371.*

УДК 007.681.3:681.326.7
Жесан Р. В., Голик О. П.
Центральноукраїнський національний технічний університет

Коротке узагальнення основних причин вразливості сучасних комп'ютеризованих систем

Комп'ютеризація всіх сфер людської діяльності і зростання темпів електронного документообігу призвели до масового зберігання величезних обсягів державної, військової, комерційної й іншої секретної інформації на машинних носіях і постійному обміну нею по комп'ютерних лініях зв'язку. Такий стан справ вкрай актуально ставить проблему гарантування недоторканності інформації, яка обробляється в сучасних комп'ютеризованих системах (КС).

У сучасних КС криптоалгоритми (шифри) широко застосовуються не тільки для задач шифрування даних, але і для аутентифікації та перевірки цілісності. На сьогоднішній день існують добре відомі й апробовані криптоалгоритми (як із секретними ключами, так і з відкритими ключами), криптостійкість яких або доведена математично, або заснована на необхідності розв'язання математично складної задачі (факторизації, дискретного логарифмування і т. п.). Таким чином, вони не можуть бути розкриті інакше, як повним перебором чи розв'язанням зазначеної задачі.

З іншого боку, у комп'ютерному світі весь час з'являється інформація про помилки чи «слабкі місця» в тій чи іншій системі (у т. ч. і з використанням криптоалгоритмів), або про те, що вона була зламана. Це створює недовіру, як до конкретних КС, так і до можливості взагалі захистити що-небудь криптографічними методами не тільки від спецслужб, але й від простих хакерів.

Тому знання історії атак і «слабких місць» у криптосистемах, а також розуміння причин, по яких вони мали місце, є однією з необхідних умов розробки захищених систем. Перспективним напрямком досліджень у цій галузі є аналіз успішно проведених атак чи виявлених «дірок» у КС із метою їх узагальнення, класифікації і визначення причин і закономірностей появи й існування.

Після аналізу літературних джерел [1-6] і величезних масивів інформації глобальної мережі Internet, виділимо наступні причини ненадійності захищених КС.

1. Мала довжина ключа. Це найочевидніша причина. Стійкі криптоалгоритми можуть мати малу довжину ключа, оскільки розроблялися давно, коли довжина використаного в них ключа вважалася більш ніж достатньою для дотримання потрібного рівня захисту [1-4].

2. Експортні обмеження. Це причина, пов'язана з експортом криптоалгоритмів або з необхідністю здобувати патент чи права на них. Зокрема, із США заборонений експорт криптоалгоритмів з довжиною ключа понад 40 біт. Очевидно, що така криптостійкість не може вважатися надійною при сучасних обчислювальних потужностях [1, 5].

3. Мала швидкість стійких крипто алгоритмів. Це основний фактор, що ускладнює застосування гарних алгоритмів, наприклад у системах «тотального» шифрування чи шифрування «на льоту». Як приклад, програма Norton DiscReet. хоча і має реалізацію DES-алгоритму [1, 2, 6], при зміні користувачем ключа, може не перешифровувати весь диск, тому що це займе занадто багато часу.

4. Використання власних криптоалгоритмів. Незнання або небажання використовувати перевірені чужі алгоритми – така ситуація також має місце, особливо в програмах типу Freeware і Shareware, наприклад, архіваторах. Так ARJ (до версії 2.50 включно) використовував дуже слабкий алгоритм шифрування – простого гаммування.

Здавалося б, що в даному випадку використання його припустиме, тому що архівований текст повинен бути зовсім ненадлишковим і статистичні методи криптоаналізу тут не підходять. Однак, після більш детального вивчення виявилося, що в архівованому тексті присутній (і це є справедливим для будь-яких архіваторів) певна невипадкова інформація, наприклад, таблиця Хаффмана і деяка інша службова інформація. Тому, точно знаючи чи передбачаючи, з певною імовірністю, значення цих службових змінних, можна з тією ж імовірністю визначити і відповідні символи пароля. Далі, використання слабких алгоритмів часто призводить до успіху атаки за відкритим текстом. У випадку архіватора ARJ, якщо зловмиснику відомий хоча б один файл із зашифрованого архіву, він з легкістю визначить пароль архіву і витягне звідти всі інші файли (криптостійкість ARJ при знанні відкритого тексту – 20 біт). Навіть, якщо жодного файлу в незашифрованому вигляді немає, все одно просте гаммування дозволяє досягти швидкості перебору в 700 тис. паролів/сек., навіть на досить слабкому комп'ютері. Аналогічна ситуація має місце й у випадку з популярними програмами з Microsoft Office – для визначення пароля там необхідно знати всього 16 байт файлу *.doc* чи *.xls*, після чого досить перебрати 24 варіанти [1].

5. Зменшення криптостійкості при генерації ключа. Ця причина має дуже велику кількість прикладів, коли криптосистема або обрізає пароль користувача, або генерує з нього дані, що мають меншу кількість біт, ніж сам пароль. Наприклад, у багатьох старих версіях UNIX пароль користувача обрізався до 8 байт перед хешуванням [2, 3].

6. Відсутність перевірки на слабкі ключі. Деякі криптоалгоритми (зокрема, DES, IDEA) при шифруванні зі специфічними ключами не можуть забезпечити належний рівень криптостійкості (слабкі ключі). Для DES відомо 4 слабких і 12 напівслабких ключів. І хоча ймовірність потрапити в них дорівнює $16 / 2^{56} = 10^{-16}$, для серйозних криптографічних систем зневажати нею не можна. Потужність множини слабких ключів IDEA складає ні багато, ні мало – 251 (втім, через те, що усього ключів 2^{128}, імовірність потрапити в неї в $3 \cdot 10^{20}$ разів менше, ніж у DES) [1, 2].

7. Недоліки датчика випадкових чисел. Гарний, математично перевірений і коректно реалізований датчик випадкових чисел так само важливий для криптосистеми, як і гарний, математично стійкий і коректний криптоалгоритм. При цьому для моделювання датчика випадкових чисел на ЕОМ, як правило, застосовують датчики псевдовипадкових чисел, що характеризуються періодом, розкидом, а також необхідністю його ініціалізації. Застосування псевдовипадкових чисел для КС узагалі не можна визнати вдалим рішенням, тому гарні криптосистеми застосовують для цих цілей фізичний датчик випадкових чисел (спеціальну плату), чи, принаймні, виробляють число для ініціалізації псевдовипадкових чисел за допомогою фізичних величин (наприклад, часу натискання на клавіші користувачем). Малий період і поганий розкид відносяться до математичних недоліків датчика випадкових чисел. Інакше кажучи, вибір власного датчика випадкових чисел так само небезпечний, як і вибір власного криптоалгоритму [4, 6].

8. Недостатня захищеність від програмних руйнуючих засобів. Руйнуючі програмні засоби – це комп'ютерні віруси, троянські коні, програмні чи апаратні закладки і т. п. програми, здатні перехопити секретний ключ або самі нешифровані дані, а також просто підмінити алгоритм на некриптостійкий. У випадку, якщо програміст не передбачив достатніх способів захисту від руйнуючих програмних засобів, вони легко здатні порушити безпеку криптосистеми. Особливо це актуально для операційних систем, що не мають вбудованих засобів захисту або засобів розмежування доступу, а також багатозадачних систем з поганою ізоляцією програм одна від одної.

9. Наявність «люків». Розробники КС хочуть мати контроль над оброблюваною в їх системі інформацією і залишають для себе можливість розшифровувати її, не знаючи ключа легального користувача, тобто залишають для себе так звані «люки». Природно, що це рано чи пізно стає відомим досить великому колу осіб і цінність такої захищеної КС стає практично нульовою [2, 5].

10. Зберігання ключа разом з даними. Ця причина призводить до того, що дані, зашифровані за допомогою криптостійкого і коректно реалізованого алгоритму, можуть бути легко дешифровані. Якщо специфіка розв'язуваної задачі така, що неможливо вводити ключ ззовні, то він повинен зберігатися десь всередині у відкритому вигляді. Проблема частково розв'язується шифруванням цього ключа вторинним ключем, але тоді вторинний ключ сам буде у відкритому вигляді. Можна вводити як завгодно багато додаткових ключів, але останній з них все одно буде доступним зломщику, а, отже, і вся схема може бути розкрита.

11. Відсутність контролю прихованих каналів. Варто знати, що рівень захищеності КС не може бути вище, ніж рівень найменш захищеної компоненти програмно-апаратного середовища, що входить до її складу [3-5]. Каналом доступу до КС може служити електромагнітне випромінювання від монітора чи модемного кабелю комп'ютера, які можуть бути перехоплені відповідною апаратурою, а потім перетворені у початкову інформаційну посилку, але вже у зловмисника.

12. Людський фактор. У будь-який КС помилки людини-оператора є чи не найдорожчими і найбільш розповсюдженими. Стосовно до криптосистем, непрофесійні дії користувача зводять нанівець найстійкіший криптоалгоритм і найкоректнішу його реалізацію. В першу чергу це пов'язане з обранням паролів: очевидно, що короткі й осмислені паролі легко запам'ятовуються людиною, але вони набагато простіші для розкриття; а довгі і складні паролі людина зазвичай не може запам'ятати і записує, чим полегшує доступ до них сторонніх. Іншою складовою людського фактора може бути довірливість співробітників. Крім того, існують дві дуже потужних методики криптоаналізу – корупційна і бандитська, коли ключ одержують звичайним підкупом або ж шантажем та катуванням.

Наведена нами класифікація не претендує на істину в останній інстанції, але з усього викладеного можна зробити кілька узагальнюючих висновків.

Для того щоб грамотно реалізувати захищену КС, необхідно не тільки застосувати особливі технічні і програмні засоби, спеціальні захисні прийоми, але й ознайомитися з допущеними раніше помилками інших розробників, а також зрозуміти причини, з яких вони відбулися. При цьому варто пам'ятати, що з постійним розвитком комп'ютерної техніки засоби захисту КС швидко і неминуче застарівають. А, значить, при побудові надійних КС необхідно використовувати тільки найпередовіші засоби і технології.

Список використаних джерел

1. *Домарев В. В. Защита информации и безопасность компьютерных систем. / В. В. Домарев. – К.: Диасофт, 1999. – 480 с.*
2. *Таили Э. Безопасность персонального компьютера. / Э. Таили. – Мн.: 000 «Попурри», 1997. – 480 с.*
3. *Основи техніки передавання інформації. / [Квєтний Р., Компанець М., Кривогубенко С., Кулик А.]. – Вінниця: УНІВЕРСУМ-Вінниця, 2002. – 358 с.*
4. *Захист інформації в автоматизованих системах управління: Навч. посібник. / [Уклад. І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька]. – Житомир: Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.*
5. *Основи захисту інформації в телекомунікаційних та комп'ютерних мережах: Навч. посібник. / [Гончарова Л. Л., Возненко А. Д., Стасюк О. І., Коваль Ю. О.]. – К.: ДЕТУТ, 2013. – 435 с.*
6. *Шмалько А. В. Цифровые сети связи: основы планирования и построения. / А. В. Шмалько. – М.: Эко-Трендз, 2001. – 282 с.*

УДК 658:512.011:681.326:519.713
Колосов А. А.
Харківський національний університет радіоелектроніки

Моделювання компонентів керування МЕМС зі зворотними зв'язками з використанням Matlab / Simulink

Проведений аналіз літературних джерел в області математичного забезпечення МЕМС дає змогу стверджувати, що практично відсутні моделі для опису об'єкта та самого процесу автоматизованого проектування, відсутні постановки задач для системного рівня проектування та не приділено належної уваги розробленю математичних моделей, які враховують специфіку та особливості автоматизованого багаторівневого проектування мікроелектромеханічних систем. Найчастіше, розробляючи МЕМС, використовують такі програмні системи: Abaqus, MEMCAD, IntelliCAD, Solidis, Ansys, Simulink, Saber, SUGAR ver. 5.0, NODAS та ін. Наведені системи проектування МЕМС та їх елементи мають багато недоліків, зокрема: виконують проектування лише окремих процедур з загального процесу проектування МЕМС; їх важко інтегрувати в єдину систему (САПР); відсутня інформація про закладені в них математичні моделі та їх адекватність і точність; відсутні засоби для вбудовування власних математичних моделей.

Системою моделювання був обраний емулятор Simulink. Розширення системи Matlab Simulink характеризується простотою і наочністю використання при моделюванні різних пристроїв і систем, в тому числі і електротехнічних. У Simulink використовується візуально-оріентірованний.підхід, коли готові блоки за допомогою миші переносять з _бібліотекі в вікно документа Simulink і з'єднують лініями входи і виходи цих блоків. В результаті виходить S-модель, тобто Simulink модель, яка запускається натисканням кнопки Run.

Моделювання рівнянь другого порядку (системи з одного степеньюсвободи, Single Degree of Freedom System - SDOF). Система маса-пружина-амортизатор (mass-spring-dashpot) - це базова модель, широко використовувана вмашіностроеніі для моделювання реальних механічних систем.

Реакція системи визначається рівнянням руху, яке є диференціальним рівнянням другого порядку:,Для моделювання системи, почнемо з розгляду Існування трьох вхідних сигнальних ліній: f (t), xdot і x. Елементи xdot і x множаться на константи. Як і в разі моделі першого порядку, це можнареалізувати в Simulink, використовуючи блок Gain. Потім сигнали підсумовуються.Проста модель складається з трьох блоків: Step, Transfer Function і Scope.Step є вихідним блоком, що формує зовнішній вхід. Зазначений сигнал передається по лінії в напрямку, визначеному стрілкою, в блок безперервної передачі передачі. Блок Transfer Function змінює вхідний сигнал і виводить новий сигнал в напрямку, який визначається лінією, наприклад, в осцилограф Scope. Блок Scope - осцилограф, який використовується для відображення сигналу.

Результатом даних досліджень є реалізація моделювання компонентів керування МЕМС зі зворотними зв'язками, з використанням Matlab/Simulink.

Список використаних джерел

1. *Simulink ver. 3.0, The Mathworks, Inc., Natick, MA, http://www.mathworks.com*
2. *Funk J.M., Korvink J.G., Buhler J., Bachtold M., Bakes H. SOLIDIS: A tool for microactuator simulation in 3-D*
3. *Kovacs G T A, Maluf N I, Petersen K E (1998). 'Bulk micromachining of silicon,' Proc. IEEE, 86 (8), 1536–1551.*
4. *MATLAB Central, "Fast Parameter Loading for MATLAB/Simulink," http://www.mathworks.com/matlabcentral/ fileexchange/14898, May 2007.*

УДК 658:512.011:681.326:519.713
Колосов Є. А.
Харківський національний університет радіоелектроніки

Моделювання мікроелектромеханічних актюаторів з використанням Matlab/Simulink

Об'єктом моделювання є мікроелектромеханічні актюатори. Удосконалення технології виготовлення мікроелектромеханічних систем МЕМС, покращання їх техніко-експлуатаційних характеристик, скорочення повного циклу впровадження нових виробів сьогодні визначається автоматизацією як проектування інтегральних пристроїв, так і технологічним процесом їх виробництва. Сучасний процес проектування МЕМС під час використання найпередовіших технологій потребує одночасної оптимізації технологічного процесу, конструкції інтегрального приладу та функціональної схеми. Тому системи автоматизованого проектування (САПР) МЕМС є невід'ємною складовою процесу сучасного виробництва інтегральних пристроїв, а роботи, пов'язані з розробкою нових математичних моделей, методик та програмних засобів для автоматизації проектування МЕМС, є актуальним питанням сьогодення. Мікроелектромеханічна система включає такі основні складові: давач, актюатор, мікропроцесор, підсистеми керування та передачі даних і мікромодуль живлення. Залежно від призначення МЕМС певні складові можуть бути відсутні, а фізичні розміри знаходяться в межах від кількох міліметрів до мікронів. кінцевого автомата.

Давач призначений для визначення змін чи впливу оточуючого середовища. Як правило, до вхідних перетворювачів належать мікродавачі. Такі пристрої перетворюють зміну тиску, напруження чи деформації в зміну електричного параметра, який можна обробити за допомогою мікропроцесора. В багатьох мікропроцесорах як вихідний електричний параметр може бути опір, ємність, частота, напруга, струм тощо. Оскільки безпосередньо аналогову величину напруги чи струму мікропроцесор обробляти не може, то після мікродавача має бути розміщений аналоговоцифровий перетворювач (АЦП), з якого вже цифровий сигнал поступає на шину даних мікропроцесора. Мікропроцесор обробляє отримані дані за попередньо визначеним алгоритмом і результатом обробки і у формі цифрового сигналу видає на цифрово-аналоговий перетворювач 63 (ЦАП). ЦАП перетворює отриманий код в аналоговий сигнал, який безпосередньо подається на вихідний перетворювач. Як вихідний перетворювач виступають актюатори – це мікропристрої, які перетворюють, як правило, електричну енергію в керований рух.

Моделювання МЕМС здебільшого передбачає моделювання зверху вниз, хоча у міру розвитку цієї області все частіше використовуватиметься проектування знизу вверх. Ці види автоматизованого проектування передбачають такі рівні проектування: системний, функціональний, компонентний та елементний. Перший етап моделювання передбачає наявність ТЗ на МЕМС. Другий етап передбачає виконання системного проектування, а третій та четвертий – рівень макропроектування і мікропроектування. На п'ятому етапі виконується технологічне проектування з використанням Matlab/Simulink. Хоча здебільшого на системному рівні проектування вже визначено технологію виготовлення МЕМС, все ж таки виникає необхідність доробки базового технологічного процесу. Наступний етап передбачає випуск проектної документації на виріб.

Результатом даних досліджень є реалізація моделей мікроелектромеханічних актюаторів різних типів, з використанням Matlab/Simulink.

Список використаних джерел

1. *Влах И., Сингхал К. Машинные методы анализа и проектирования электронных схем / Пер. с англ. – М.: Радио и связь, 1988. – 560 с.*
2. *Simulink ver. 3.0, The Mathworks, Inc., Natick, MA, http://www.mathworks.com.*
3. *Ikuta K and Hirowatari K, (1993). 'Real three dimensional microfabrication using stereo lithography and metal molding,' Proc. IEEE MEMS, 42– 47.*

УДК 004.415:004.382

Кумченко Ю. О., Нагін Р. Ю.
Криворізький національний університет

Платформа віртуалізації Proxmox VE для керування кластерами високої доступності

Віртуалізація – це спосіб логічного поділу ресурсів мейнфрейму для різних прикладних процесів. Вона дозволяє об'єднувати різні платформи та робити зручне адміністрування системи загалом, а також зберігати енергію та кошти створюючи віртуальні центри обробки даних. Якщо організація має мережеве сховище та віртуальні машини (ВМ), які розміщено на декількох серверах, у такому випадку необхідно створити кластер і з'єднати сервера у керований пул. Об'єднання серверів у кластер дозволить централізовано, з однієї консолі, управляти хостами та існуючою кількістю ВМ. Крім зручності керування, з'являється можливість мігрувати ВМ з одного хоста на інший без зупинки ВМ – жива міграція. Міграція ВМ дозволить балансувати навантаження між хостами та подібним чином зупиняти деякі з них на профілактику не зупиняючи всієї системи. Після утворення кількох серверів віртуалізації, подальшим кроком буде їх кластеризація – це наступний етап в еволюції віртуальної інфраструктури [1].

Розглянемо платформу віртуалізації Proxmox Virtual Environment (Proxmox VE). Вона має відкритий вихідний код на базі Debian GNU/Linux [2]. Інтерфейс Proxmox VE наведено на рисунку 1.

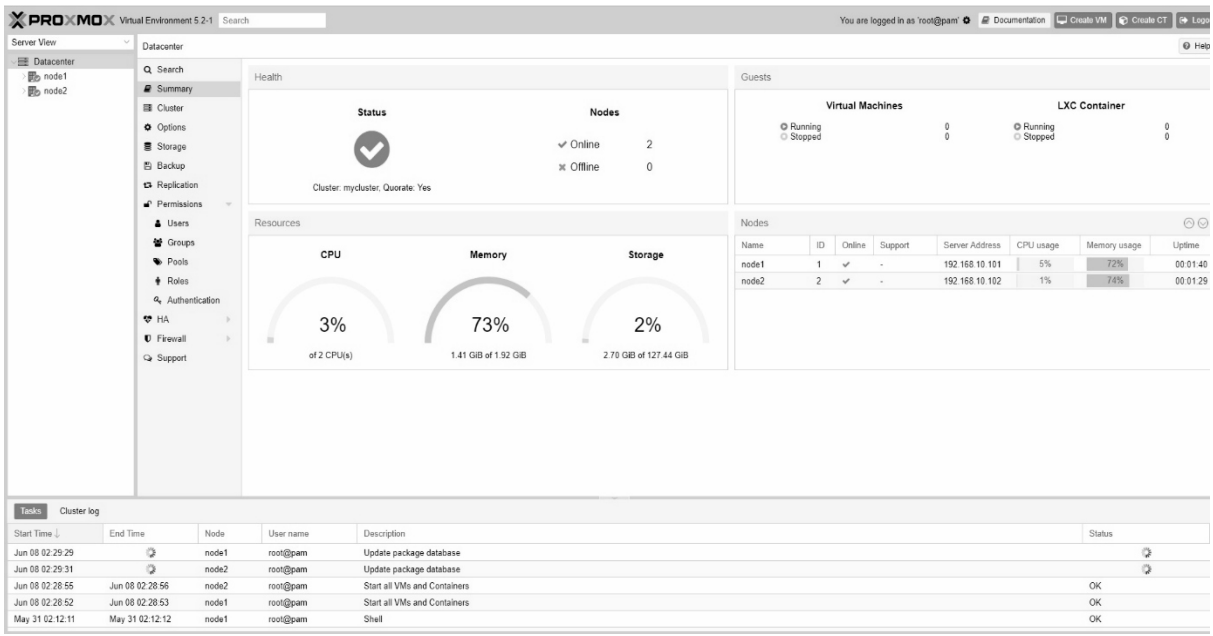


Рисунок 1 – Інтерфейс Proxmox VE

Основні переваги:

1) просте управління через веб-інтерфейс;
2) моніторинг навантаження в реальному часі;
3) статистика, інформативні графіки навантаження серверу віртуалізації та кожної віртуальної машини окремо за оперативною пам'яттю, CPU, HDD, мережею в розрізі останньої години / дня / тижня / місяця/ року;
4) бібліотека встановлених образів (у локальному або віддаленому сховищі);

5) підключення до «фізичної» консолі гостьових систем безпосередньо з браузера (за VNC і з використанням SPICE-клієнта);

6) об'єднання серверів у кластер з можливістю динамічної міграції віртуальних машин (без зупинки гостьової системи);

7) швидке розгортання гостьових систем з шаблонів;

8) збереження образу стану віртуальної машини (snapshot), формування дерева станів і можливість повернення до будь якої з точок відновлення;

9) автоматичне резервне копіювання віртуальних машин.

З недоліків варто відзначити:

1) неповна система постачання: можливо безкоштовно завантажити та встановити Proxmox VE, але в разі потреби оновлення системи необхідна купівля підписки;

2) Network File System не підтримує авторизацію, доступ до NFS-сервера можна обмежити лише за IP адресою;

3) періодично нестабільна робота, написаного на Java, клієнта, який підключається до «фізичних консолей» гостьових систем [3].

За допомогою графічного інтерфейсу моніторингу Proxmox VE переглянемо загальну завантаженість вузлів кластерної системи (рисунок 2).

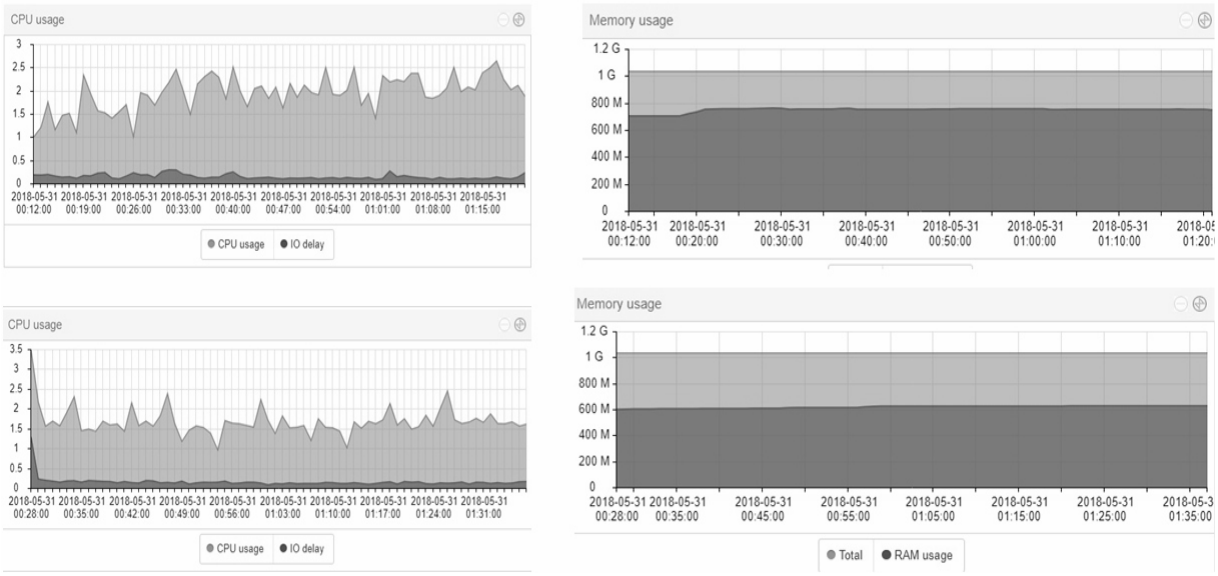


Рисунок 2 – Моніторинг стану завантаженості вузлів кластеру

Таким чином розглянута платформа віртуалізації Proxmox VE для керування кластерами високої доступності є безкоштовна, має гнучкі налаштування у веб-інтерфейсі, зручне відображення статистики навантаження серверу та віртуальних машин, швидке розгортання гостьових систем за допомогою шаблонів з офіційного сайту розробника та власних.

Список використаних джерел

1. *Руденко А. Proxmox VE. Кластер из 2-х Proxmox-хостов [Електронний ресурс] / Александр Руденко // iVirt-it.ru. – 2013. – Режим доступу до ресурсу: https://ivirt-it.ru/proxmox-cluster/.*
2. *Офіційний сайт Proxmox VE [Електронний ресурс] // Proxmox. – 2018. – Режим доступу до ресурсу: https://www.proxmox.com/en/proxmox-ve.*
3. *Holt A. Установка, тестирование и обзор Proxmox VE [Електронний ресурс] / Alan Holt // Linux Space. – 2014. – Режим доступу до ресурсу: https://www.linuxspace.org/archives/5902.*

УДК 004.056.53+614.844

Кумченко Ю. О., Шевченко О. В.
Криворізький національний університет

Комплексна система захисту серверного приміщення

Одним з основних гарантів коректної та надійної роботи серверної є її безпека. Від того, наскільки правильно спеціаліст дотримується всіх інструкції та стандартів для її оснащення, залежить степінь виникнення ризику знищення накопиченої інформації [1]. Розглянемо два аспекти захисту серверного приміщення: фізичний доступ осіб та систему пожежної безпеки. Доступ до серверної повинні мати лише відповідальні за апаратне обладнання особи, тому для досягнення цієї мети серверна кімната повинна бути обладнана системою охоронної сигналізації та контролем доступу.

Перш за все, необхідно розглянути електромеханічні замки з двома способами відкриття: за кодовою комбінацією та за допомогою брелка/картки. Вони є найбільш доцільні для даної задачі, тому що мають високий рівень надійності, можливість змінювати кодову комбінацію через деякий час та порівняно невелику ціну. Обов'язковою є система відеоспостереження безпосередньо в самій серверній і на вході до неї. Вдалим вибором можуть бути IP-камери компанії Hikvision, модель DS-2CD2020F. Вони мають функцію датчика руху та підключення до хмарних сервісів, що допоможе швидко зреагувати на загрозу проникнення до серверного приміщення.

Наступним етапом є встановлення надійної системи пожежної безпеки. У серверній кімнаті застосовується дороге IT-обладнання, не горючі кабелі, тому в теорії ризик виникнення пожежі зведений до мінімуму [2]. Для серверної рекомендується використовувати газову систему пожежогасіння, так як цей спосіб не зашкоджує електронному обладнанню. Також не слід забувати про системи виявлення пожежі. Перевіреним рішенням є активне виявлення диму, тобто датчик повинен автоматично брати проби повітря та аналізувати їх на задимленість.

Побудуємо функціональну схему запропонованої комплексної системи захисту серверного приміщення (рис. 1).

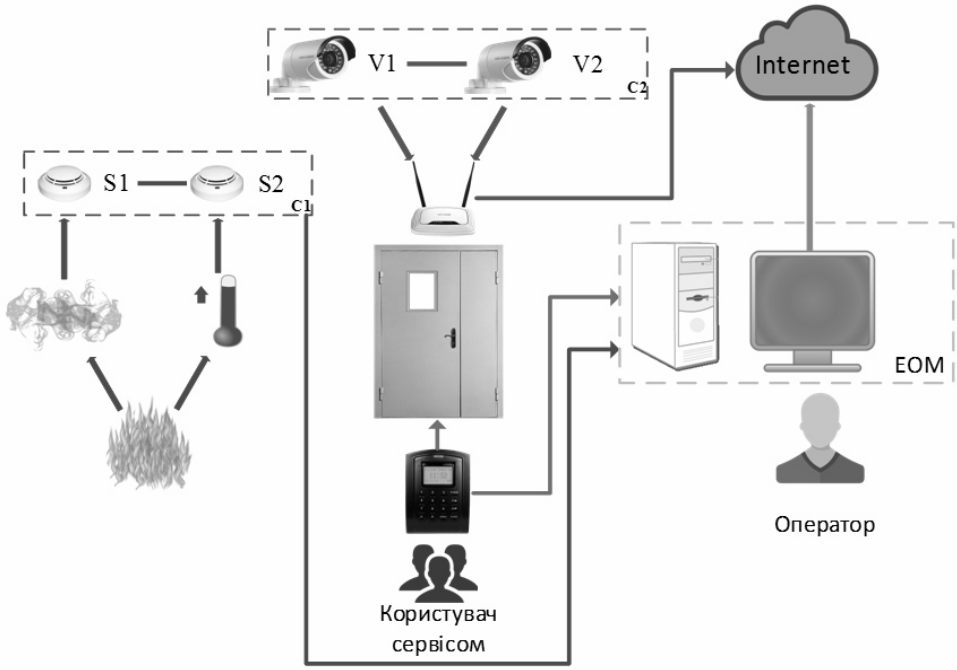


Рисунок 1 – Функціональна схема комплексної системи захисту серверного приміщення

Згідно функціональній схемі, при виникненні пожежі датчики S1 та S2 відправляють дані на ЕОМ служби безпеки. У такий спосіб працює і система контролю доступу до серверного приміщення: при введені вірної чи неправильної комбінації на терміналі контролю доступу, а також при піднесенні картки до зчитувача, відправляються данні оператору про користувача сервісом. Камери підключені до маршрутизатора та мають доступ до мережі Internet. Запис з відеокамер зберігається не тільки на картці пам'яті, але й на хмарних сховищах. Оператор ЕОМ вільно отримує оперативні данні з комплексної системи, яка складається з контролю доступу, відеоспостереження та пожежної безпеки.

Для графічного представлення структурно-функціональної моделі комплексної системи захисту серверного приміщення вирішено використати мову графічного моделювання IDEF0. Основною перевагою даного методу є наочне відображення структури і функцій системи. Побудуємо нульовий рівень IDEF0-діаграми (рис. 2). Він представляє об'єкт моделювання єдиним блоком з граничними стрілками, які відображають зв'язки об'єкта моделювання з навколишнім середовищем. Виконавши декомпозицію нульового рівня діаграми, ми отримаємо детальний опис підсистем, що входять до комплексної системи захисту.

Рисунок 2 – Нульовий рівень IDEF0-діаграми комплексної системи захисту серверного приміщення

Отже, система контролю доступу та пожежогасіння є невід'ємною складовою безпеки серверного приміщення. Наведено етапи проектування сучасної системи пожежної безпеки та контролю доступу до серверної, побудовано та описано функціональну схему, нульовий рівень IDEF0-діаграми.

Список використаних джерел

1. *Марухин А. Организация серверной комнаты [Електронний ресурс] / Алексей Марухин // Технологии и средства связи. – 2009. – Режим доступу до ресурсу: http://tssonline.ru/articles2/fix-corp/organizaciya-servernoy-komnaty.*
2. *Селецкая Л. Пожарная безопасность серверной комнаты [Електронний ресурс] / Людмила Селецкая // Системы безопасности спортивных сооружений. – 2015. – Режим доступу до ресурсу: https://avtoritet.net/library/press/245/15479/articles/15515.*

УДК 004.351+ 004.431.2

Маркова О. М., Дяченко Д. О.
Криворізький національний університет

Інформаційна система для контролю безпеки підйомних сосудів у залізорудних шахтах

Однією зі серйозних проблем, яка виникає в процесі руху підйомних сосудів по вертикальних стволах рудних і вугільних шахт є необхідність виключення можливості виникнення аварійно-небезпечних ситуацій.

Актуальність цієї проблеми обумовлена вкрай складними і агресивними умовами, які діють у стволах шахт. Ці умови з часом суттєво змінюють проектні параметри армування стволів і особливо параметри системи «підйомний сосуд – направляючі провідники». Така ситуація є наслідком значного навантаження на провідники при багаторазовому циклічному переміщенні підйомних сосудів, дії тиску на ствол, інтенсивної корозії армування. Всі ці явища в комплексі можуть порушити лінійність траси руху підйомних сосудів у стволі[1].

Найбільш небезпечними наслідками такого порушення є можливість виникнення так званого «параметричного резонансу» в процесі переміщення підйомного сосуду по направляючим провідникам.

Для того щоб ефективно запобігти явищу параметричного резонансу необхідно заздалегідь виявити ділянки на трасі руху підйомного сосуду, на яких можливе формування умов, що призводять до розвитку параметричного резонансу.

Можливість виникнення цього явища може бути встановлена за параметрами коливань підйомного сосуду відносно провідників. Тобто на таких ділянках амплітуда зміщень підйомного сосуду буде переходити від спонтанних неупорядкованих величин до стабільних величин (або величин близьких до стабільних). Ці коливання певний час повторюються з близьким значенням амплітуди зміщення частин підйомного сосуду[2].

Для виявлення таких потенційно небезпечних ділянок необхідно проаналізувати характер зміни амплітуди коливань підйомного сосуду, який рухається на робочій швидкості вертикально по стволу шахти.

Для здійснення контролю параметричних явищ була розроблена спеціальна мікроконтролерна система. Її принципова наведена на рисунку 1.

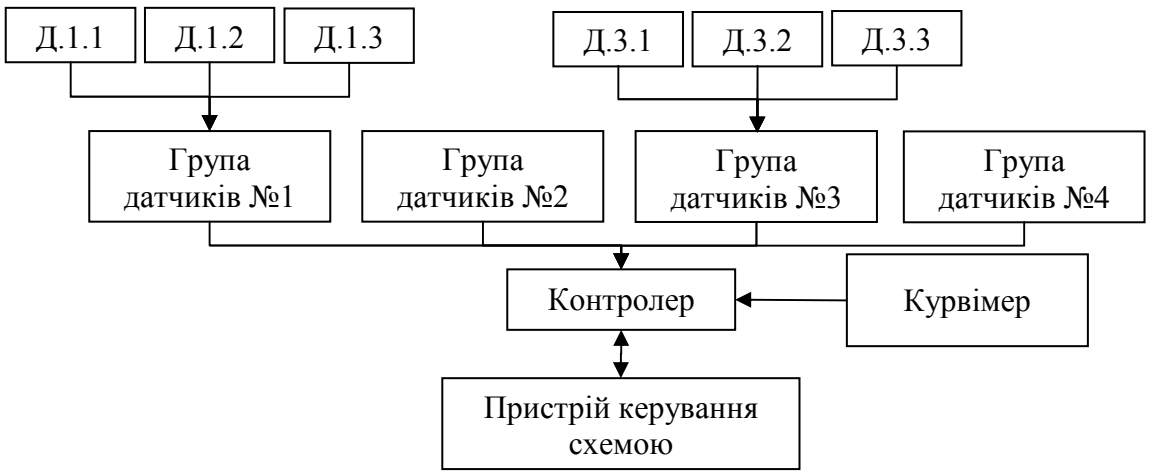


Рисунок 1 – Принципова схема системи контролю параметрів руху підйомного сосуду

Вказана система включає:

– датчики зміщення Д.1.1 – Д.4.4. Ці датчики встановлюються по три на кожному башмаку підйомного сосуду. Вони встановлюються напроти кожного провідника для вимірювання зміщення у лобовому напрямі відносно провідника, і боковому напрямі;

– електронний курвіметр. Визначає глибину розташування кожної точки вимірювання відхилення підйомного сосуду від нульової маркшейдерської відмітки ствола шахти, тобто початку траси переміщення сосуду;

– контролер. Для обробки значень отриманих з датчиків, їх збереження та передачі на пристрій керування схемою;

– пристрій керування схемою. Електронний пристрій здатний встановлювати з'єднання через Serial порт (ноутбук, смартфон, планшет).

Програма мікроконтролеру буде включати декілька функцій, які взаємодіють між собою залежно від поточної конфігурації. На рисунку 2 представлений загальний алгоритм функціонування програми.

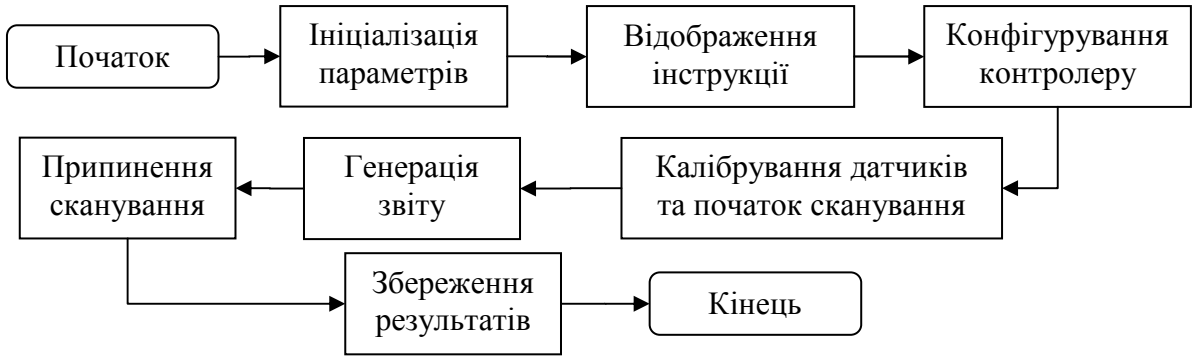


Рисунок 2 – Загальний алгоритм роботи програми контролеру

Основою проекту було обрано контролер Arduino Mega 2560. Для визначення відстані, пройденої візком, використовується цифровий курвіметр, представлений у вигляді колеса, притиснутого пружиною до направляючої.

Користувацький додаток розроблено на об'єктно-орієнтованій мові програмування C# у середовищі Microsoft Visual Studio. Основна задача додатку – надати користувачу можливість зручно працювати з контролером по засобам Serial порту. Можливості та особливості використання додатку розписано в коментарях програмного коду.

В результаті виконаних досліджень була розроблена система на основі мікропроцесорної техніки, яка, на думку автора, повинна вирішити проблему «параметричного резонансу» в стволі залізорудної шахти.

Список використаних джерел

1. *Гаркуша Н. Г. Уравнения движения шахтного подъёмного сосуда, как одномерной упругой конструкции / Н. Г. Гаркуша, В. И. Дворников. // Прикладная механика Т. 5. – 1969. – №12. – С. 125-132.*
2. *Рубель А. А. О возможности совершенствования оборудования шахтных стволов путем создания армировок, обладающих непараметрическими свойствами / А. А. Рубель. – Дніпропетровськ, 1999. – (Зб. науч. трудов. Автоматика та електромеханіка).*

УДК 004:621.391
[1]Минайленко Р. М., [1]Дрєєв О. М., [1]Собінов О. Г., [2]Денисенко О. О.
[1]*Центральноукраїнський національний технічний університет;*
[2]*Epam Systems, м. Київ*

Програмна компенсація дрейфу нуля в системі вимірювання вологості зерна в потоці

Вступ. Процес сушіння зерна є одним із найбільш енерговитратних і важливих із всього циклу зберігання і переробки зерна. Це пов'язано як з прямими витратами, обумовленими втратами якості зернових і неможливістю зберігання при невідповідній вологості, а також великими енергетичними витратами, пов'язаними із забезпеченням процесу сушіння. Оптимізація процесу сушіння безпосередньо пов'язана з контролем вологості зерна.

Постанова задачі. Сучасні системи ряд недоліків, одним з них є дрейф параметрів систем вимірювання зі змінами параметрів навколишнього середовища (як основні, вологість та температура повітря), основний вклад в систематичні помилки вносить дрейф нуля. Для зменшення систематичних помилок поставлено задачу створення апаратно-програмних засобів компенсації дрейфу початку відліку.

Основний матеріал. Розроблений авторами автомат вимірювання вологості зерна в потоці, який проводить вимірювання діелектричної проникності матеріалу між обкладками конденсатору-датчику, відрізняється від відомих аналогів системою порційного відбору зерна з вимірюванням вологості порції в нерухомому стані. Для зменшення впливів випадкових відхилень також в програмній частині вводиться медіанна фільтрація з апертурою m.

Нехай програмна система має на вході m останніх результатів вимірювання W_i, де i=0..m-1. В результаті медіанної фільтрації вхідного сигналу маємо відсортований масив S_i, де $S_i<S_{i+1}$ з множиною елементів S=W. На вихід фільтру подається значення $S_{m/2}$.

Інженерним рішенням зміни конструкції вимірювача вологості зерна стало додавання до вимірювального барабану секції з зразком-еталоном, діелектрична проникність якого відома. Завдяки такій конструктивній зміні кожне k-те вимірювання приходиться на еталонне значення точки відліку. Тепер на вхід фільтрування результатів вимірювання надходить масив W_i, в якому [m/k] або [m/k]+1 вимірів припадає на еталон (тут [a] є операцією відсікання дробової частини). Приклад результатів вимірювання показано на рис. 1:

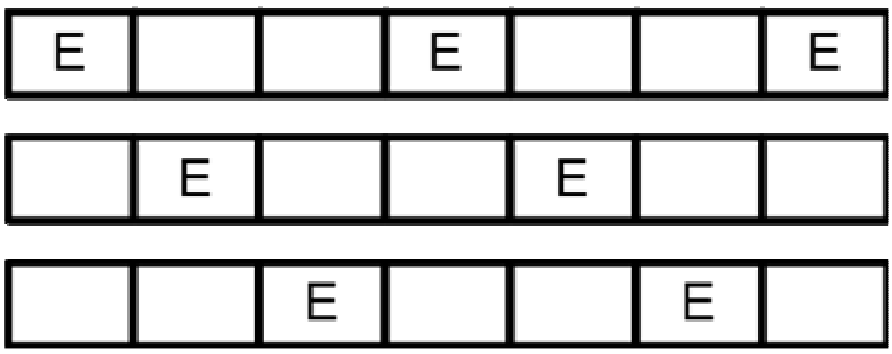


Рисунок 1 – Можливі положення еталонних вимірів при m=7 та k=3

В процесі медіанного фільтрування проводиться сортування, після якого еталонні виміри переміщуються на початок масиву (рис. 2).

Вихідними значеннями фільтрування тут будуть: положення початку відліку $S_{[k/2]}$, та фільтроване значення для визначення вологості $S_{k+[(m-k)/2]}$, і як результат вимірювання приймається значення $R=S_{k+[(m-k)/2]}- S_{[k/2]}$.

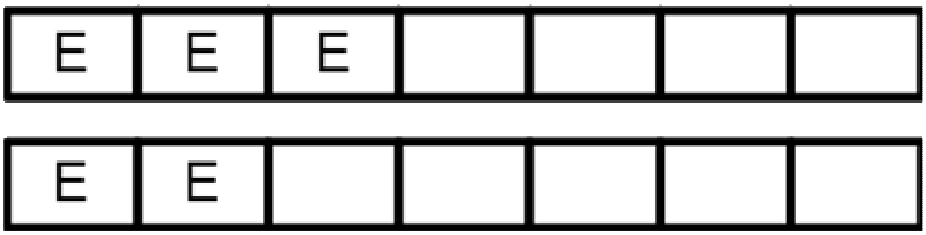


Рисунок 2 – Результати сортування в процесі медіанного фільтрування

Недоліком вказаної системи є використання медіанної фільтрації, яка має значні показники запізнення реакції на зміни вхідних параметрів. В реалізованій системі (рис. 3) використано систему вимірювання з зупинками барабану на 0,25 сек., коли повний цикл заповнення медіанного фільтру потребує від семи вимірювань. Тому повний цикл визначення поточної вологості зерна складає близько хвилини і змінюється в сторону збільшення при попаданні зерна в зону клину.

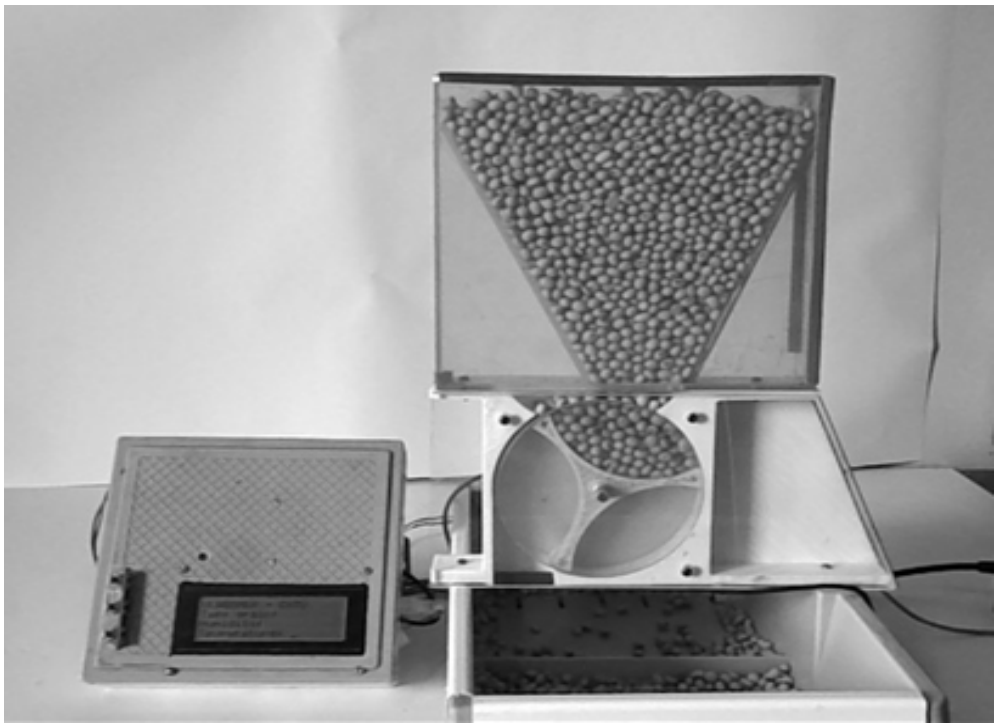


Рисунок 3 – АПК вимірювання вологості зерна в потоці

Висновки. Додавання до конструкції вимірювача вологості зерна еталонного елементу дозволило без втручання до конструкції електронної частини, лише програмними засобами, врахувати повільний дрейф нульової точки і підвищити надійність результатів вимірювань.

Список використаних джерел

1. *Шандров Б.В. Компьютерное управление технологическим процессом, експерементом, оборудованием. / Б.В. Шандров – М.: Горячая линия - Телеком, 2009. – 608с.*
2. *Конюх В.Л. Компьютерная автоматизация производства. /В.Л. Конюх - НГТУ, 2006. – 108с.*

УДК 004.7

Незамай В. О.
Харківський національний університет радіоелектроніки

Використання методу автоматного програмування при побудові систем комунікації «Smart House»

На сьогоднішній день технології досягли такого рівня розвитку, що ми вже не уявляємо свого життя без них. Всі вони спрямовані на поліпшення нашого повсякденного життя. Порівняно недавно почала розвиватися концепція "інтернету речей" (Internet of Things), яка являє собою мережу пов'язаних через інтернет об'єктів, здатних збирати дані і обмінюватися даними, які надходять зі вбудованих сервісів. До поняття "Інтернет речей" впритул примикає поняття "розумний будинок" (Smart House) – система, яка забезпечує безпеку, ресурсозбереження та комфорт для всіх користувачів.

Система "розумний будинок" складається з таких елементів: контролер розумного будинку (по суті, центральний сервер), системи контролю (освітлення, температури, присутності тощо.) і канали зв'язку між системами. Оскільки кожна з систем, в принципі, може працювати незалежно, іноді повертаючи результати виконання роботи (якщо такий є), то всю систему "розумний будинок" можна розглядати як один великий скінчений автомат.

Скінченим автоматом в інформатиці є модель дискретного пристрою, що має один вхід, один вихід і в кожний момент часу знаходиться в одному стані зі скінченої множини можливих. Дана математична модель на сьогоднішній день знайшла широке застосування практично скрізь: від найпростіших перемикачів до систем обробки зображень. Так як будь-яку систему і підсистему "розумного будинку" умовно можна розглядати як велику кількість перемикачів і вимірювачів параметрів, то модель скінченного автомата виглядає дуже привабливо з точки зору простоти опису і побудови.

Також варто відзначити той факт, що на практиці побудова скінченого автомата здійснюється за визначеним алгоритмом. Даний факт можна простежити в роботах А. Тюрінга над "машиною Тюрінга", яка є розширеним варіантом скінченого автомата.

Таким чином, застосування методу автоматного програмування для побудови систем комунікації "розумний будинок" зводиться до наступних дій:

- побудова алгоритму роботи кожної з систем контролю,
- побудова алгоритму роботи контролера системи "розумний будинок",
- перетворення отриманих алгоритмів в один абстрактний автомат,
- створення необхідного програмного забезпечення, що реалізує дану систему.

На жаль, станом на поточний момент, при всьому різноманітті розробок на тему "розумного будинку" ми маємо такі проблеми як велику кількість пропрієтарних протоколів, які мало сумісні між собою, що не дозволяє уніфікувати обладнання, і, в наслідок цього, високу вартість, що ускладнює просування концепції "розумного будинку" до масового користувача. Дані проблеми можна вирішити за допомогою створення єдиного набору протоколів і відкритого програмного забезпечення, яке будь-який користувач може модифікувати для своїх потреб.

Список використаних джерел

1. *Problem Statement for Smart Home Device Vocabulary [Електронний ресурс]. – Режим доступу : https://tools.ietf.org/html/draft-liu-t2trg-ps-smart-home-vocabulary-00*
2. *Хопкрофт, Джон, Э., Мотвани, Раджив, Ульман, Джеффри, Д.Введение в теорию автоматов, языков и вычислений, 2-е изд.. : Пер. с англ. – М. :Издательский дом "Вильямс", 2008. – 528 с.*
3. *Кнут, Дональд Эрвин. Искусство программирования [Текст] : пер. с англ. / Д. Э. Кнут ; общ. ред. Ю. В. Козаченко. - М. : Издательский дом "Вильямс"2005. - (Классический труд).*

УДК 658:512.011:681.326:519.713
Пасічко Є. В.
Харківський національний університет радіоелектроніки

Верифікація кінцевого автомата з допогомогою UVM

Об'єктом системної верифікації є UVM-модель кінцевого автомата. При модульній верифікації функціональні блоки, які входять в состав мікропроцесора, преверяются автономно, тому її також називают автономной. Основним перевагою автономної верифікация є можливість проводити тестування на найстарших етапи розробки, не дочікуючись специфікації та реалізації всієї системи в цілому, заступінь готовності UVM-моделі та специфікації модуля.

На модульному рівні також можливо створення необхідної динаміки роботи UVM-моделі для досягнення критичних ситуацій (переповнення буферів, блокіровок та інших станів). Крім того, час локалізації та виправлення помилок при автономній верифікації значно менше, ніж при системній, що дає можливість скоротити терміни debugging UVM-моделі. В дипломній роботі розглянуті підходи до автономної перевірки модулів мікропроцесорівз використанням еталонних програмних моделей на прикладі управління vending machine

Модель реєстрації UVM забезпечує спосіб відстеження вмісту регістру DUT та зручності для доступу до регістрів та місць пам'яті в DUT. Модель регіста абстракції відображає структуру специфікації регістру апаратно-програмного забезпечення, оскільки це загальна специфікація для апаратних розробників та інженерів перевірок, а також використовується розробниками програмного забезпечення, що розробляють програмне забезпечення для програмного забезпечення прошивки. Дуже важливо, щоб всі три групи посилались на загальну специфікацію, і дуже важливо, щоб проект був перевірений на точні моделі.

Регістрова модель призначена для спрощення складання повторюваних послідовностей, що мають доступ до апаратних регістрів та областей пам'яті. Структура даних моделі організована таким чином, щоб відображати ієрархію DUT, що полегшує написання абстрактного та багаторазового використання стимулу з точки зору апаратних блоків, пам'яті, регістрів та полів, а не працювати на рівні абстракції з нижчим бітовим шаблоном. Модель містить ряд методів доступу, які послідовності використовують для читання та запису регістрів. Ці методи роблять загальні транзакції регістрів конвертованими у транзакції на цільовій шині. У пакеті UVM міститься бібліотека вбудованих тестових послідовностей, яка може використовуватися для виконання більшості основних тестів для реєстрації та запам'ятовування, таких як перевірка значень скидання регістру та перевіряючи шляхи реєстрації та даних пам'яті. Ці тести можуть бути відключені для тих областей реєстру або карти пам'яті, де вони не є релевантними, використовуючи атрибути регістру.

Модель регістра UVM призначена для сприяння продуктивній перевірці програмного обладнання. Коли він ефективно використовується, він підвищує рівень абстракції стимулів і робить код отриманого стимулу простою для повторного використання, коли відбувається зміна адресної карті регістру DUT або коли блок DUT повторно використовується як субкомпонент.

Результатом данних досліджень є розробка кінцевий автомат з можливістю багаторазового використання, з меньшим часом на локалізацію та виправлення помилок.

Список використаних джерел

1. *Universal Verification Methodology // Register Abstraction Layer. URL: http://verificationacademy.com/uvm-ovm*
2. *Universal Verification Methodology // Accellera. URL: http://www.accellera.org/community/uvm/*
3. *Lucas S., Reynolds J. Learning Deterministic Finite Automata with a Smart State Labeling Algorithm // IEEE Transactions on Pattern Analysis and Machine Intelligence. 2005. Vol. 27. № 7, pp. 1063 – 1074. https://verificationacademy.com*

УДК 004.738

Покотило О. А.
Житомирський державний технологічний університет

Аналіз протоколу динамічної маршрутизації BGP та його вразливостей

На сьогоднішній день Інтернет – це невід'ємна частина нашого життя. Для більшості це поняття означає лиш єдиний інформаційний простір. Насправді ж, Інтернет представляє собою набір взаємопов'язаних мереж операторів зв'язку, робота яких заснована на постійному та безперервному обміні між собою інформацією стосовно доступності IP-адрес. На основі отриманих даних вони будують мережеві маршрути до всіх існуючих сервісів.

Для забезпечення такого обміну інформацією стосовно доступних маршрутів між операторами зв'язку і було створено протокол динамічної маршрутизації BGP (Border Gateway Protocol). Його особливістю є забезпечення доступності мереж як на міжнародному, так і на національному рівнях. Тому на даний протокол покладається весь сучасний Інтернет.

BGP здійснює управління трафіком між операторами зв'язку і є єдиним способом їх взаємодії один з одним. Також він дозволяє операторам обирати той чи інший маршрут, по якому інформація буде направлена від їх мережі до місця призначення. В той же час, кожен оператор, навіть проміжний, самостійно приймає рішення стосовно того чи іншого маршруту із набору доступних варіантів.

Протокол BGP підтримує безкласову адресацію і використовує сумування маршрутів для зменшення таблиць маршрутизації. З 1994 року діє четверта версія протоколу, всі інші вважаються застарілими.

BGP – протокол прикладного рівня і функціонує поверх протоколу транспортного рівня TCP. Після встановлення з'єднання передається інформація стосовно всіх маршрутів, призначених для експорту. В подальшому передається тільки інформація стосовно змін в таблицях маршрутизації. При закритті з'єднання видаляються всі маршрути, інформація стосовно яких була передана протилежною стороною.

Процес вибору маршруту запускається після оновлення інформації і використовується для відбору маршрутів, призначених для використання локально, і передачі іншим маршрутизаторам, які використовують BGP. Процес використовує атрибути отриманих маршрутів для оцінки ступеня переваги маршрутизатора або інформації стосовно того, що маршрут не підходить для занесення в базу маршрутів і має бути виключений з процесу відбору. Процес ділиться на три фази:

- обрахування ступеня переваги кожного отриманого маршруту;
- вибір найкращого маршруту для кожного місця призначення і занесення його в базу маршрутів;
- передача маршрутів на інші маршрутизатори (при цьому може проводитися сумування маршрутів) [1].

В протоколі BGP технічно не закладено чітко прописаних законів, а є тільки рекомендаційні правила відносно того, що кожен оператор може робити всередині своєї мережі, а які дії є забороненими. Даний протокол за всі ці роки принципово не змінився. В ньому відсутні механізми верифікації отриманих маршрутів. У зв'язку з цим останнім часом почали з'являтися помилки, пов'язані з цими проблемами.

Загроза протоколу BGP поки не створила великих проблем, але в майбутньому, якщо не прийняти запобіжних заходів, вона може виявитися одною з критичних. Уже

зафіксовані випадки навмисного використання вразливості BGP для «крадіжки» трафіку, тобто переправлення його по хибному маршруту.

Для здійснення загрози необхідно всього лиш змінити префікс автономної системи в BGP-пакетах на неіснуючий, тим самим припиняючи його коректну роботу. В результаті мережевий ресурс, до якого направлений трафік, стає недоступним для користувачів, тобто спостерігається DoS.

Крім того, кількість операторів зв'язку з часом все збільшується, а середня кваліфікація персоналу знижується. Оператори, які погано розбираються в роботі протоколу BGP, почали перенаправляти на себе трафік інших операторів зв'язку, і, "підвішуючи" свої мережі, створювати проблеми для інших операторів, чий трафік вони перехопили[2].

Для захисту BGP від атак подібного типу NIST та DHS наприкінці 2017 року почали роботу над спільним проектом під назвою «Безпечна міждоменна маршрутизація». Стандарт використовує криптографічні методи для забезпечення передачі даних по санкціонованому маршруту в мережах.

Перший компонент – Resource Public Key Infrastructure (RPKI) – дозволяє хмарному сервісу або провайдеру встановлювати обмеження в прийомі даних від інших автономних мереж. Другий – BGP Origin Validation – надає маршрутизаторам можливість виключити неавторизовані BGP-сповіщення при передачі даних. Третій – BGP Path Validation – встановлює цифрові підписи для кожного маршрутизатора в мережі.

Приблизна реалізація, описана в даному стандарті, направлена на захист цілісності і покращення стійкості обміну інтернет-трафіком шляхом верифікації джерела маршруту. Даний проект відправлений на розгляд IETF, програмного продукту, який здійснював би практичну реалізацію, на даний момент не має[3].

Так як більшість витоків інформації спричинена неправильним налаштуванням протоколу, то для вирішення проблеми необхідно усунути умови, при яких помилки інженерів здатні впливати на інших операторів зв'язку. Також потрібно обмежити гнучкість BGP: вбудувати механізми фільтрації в сам протокол, тим самим знизивши складність його налаштування[4].

Отже, найбільш оптимальним варіантом захисту від вразливостей протоколу BGP є використання сервісів, що дозволяють проводити постійний моніторинг протоколу в режимі реального часу і виявляти мережеві аномалії на глобальному рівні маршрутизації. Можливість отримувати інформацію стосовно несанкціонованих змін та BGP-аномалій дозволяє негайно реагувати на інциденти, усуваючи можливі негативні наслідки.

Список використаних джерел

1. *Border Gateway Protocol [Електронний ресурс] – Режим доступу до ресурсу: https://ru.wikipedia Border.org/wiki/Border_Gateway_Protocol.*
2. *Азимов А. "Утекай": проблема протокола BGP и перехвата трафика [Електронний ресурс] / Александр Азимов. – 2018. – Режим доступу до ресурсу: https://www.comnews.ru/content/114069/2018-07-30/utekay-problema-protokola-bgp-i-perehvata-trafika-aleksandr-azimov-setevoy-arhitektor-qrator-labs.*
3. *Опубликован официальный проект стандарта для защиты от BGP-перехвата [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://www.securitylab.ru/news/495532.php.*
4. *Носов Н. BGP для «чайников» [Електронний ресурс] / Николай Носов. – 2017. – Режим доступу до ресурсу: http://www.iksmedia.ru/news/5416067-BGP-dlya-chajnikov.html.*

УДК 681.142

Сіленко М. О.
Харківський національний університет імені В. Н. Каразіна

Вибір системи числення для побудови комп'ютерних систем

Вік інформаційних технологій характеризується насамперед гонкою обчислювальних можливостей систем обробки даних (далі СОД). Технології сьогодення, побудовані на базі мікроелементів та з застосуванням позиційних систем числення (далі ПСЧ), досягли неабиякого прогресу, але, заглядаючи в майбутнє, постає проблема збільшення об'єму оброблюваної інформації з наслідковим зменшенням швидкодії СОД.

Одним з варіантів вирішення проблеми може бути застосування іншої логіки в процесі обробки інформації. В процесі автоматизованого вирішення задачі завжди необхідно балансувати між показниками швидкодії та затрати пам'яті. ПСЧ в такому випадку поступаються непозиційній системі залишкових класів (далі СЗК), через наявність міжрозрядних зв'язків у перших.

На рис. 1 зображена схема СОД на базі СЗК з урахуванням проблеми надмірності. Побудова системи залежить в цілому від двох пристроїв: перетворювача даних *П* та операційного пристрою *О* [1].

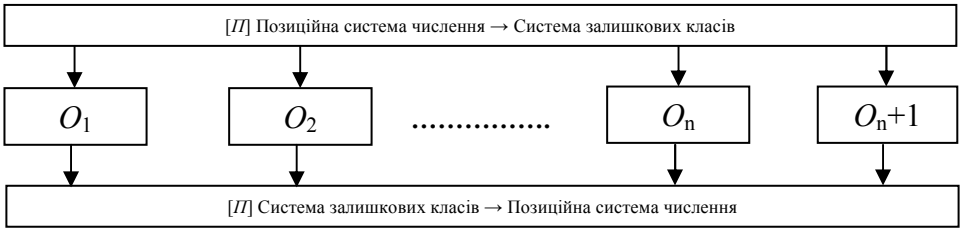


Рисунок 1 – Схема СОД на базі СЗК з застосуванням перетворювачів та операційних пристроїв

Наведені проблеми вирішуються шляхом вибору оптимального базису з застосуванням коефіцієнтів ваги операцій та пам'яті, тобто коефіцієнтів часової складності t_{add}, t_{sub}, t_{mult}, t_{div}, t_{mem} та коефіцієнтів ємносної складності n_{add}, n_{sub}, n_{mult}, n_{div}, n_{mem}. Таким чином задача оптимізації зводиться до пошуку мінімального значення цілевої функції $F = t_{add} \times n_{add} + t_{sub} \times n_{sub} + t_{mult} \times n_{mult} + t_{div} \times n_{div} + t_{mem} \times n_{mem}$ [2].

Такий підхід дозволяє розробити комп'ютерну систему на базі СЗК в якій виконуються наступні вимоги:

1) однозначне представлення чисел в межах задачі;

2) збільшення швидкодії виконання арифметичнх операцій та оптимізоване використання пам'яті;

3) врахування надмірності інформації.

Список використаних джерел

1. *Червяков Н.И., Шапошников А.В., Сахнюк П.А. Модель и структура нейронной сети для реализации арифметики системы остаточных классов // Нейрокомпьютеры: разработка, применение, 2001, №10.*
2. *Осепянц О.А., Исмаилов Ш-М.А. Методика генерации оптимального основания для представления чисел в системе остаточных классов. Електронний ресурс. – Режим доступу: https://docplayer.ru/32425783-Metodika-generacii-optimalnogo-osnovaniya-dlya-predstavleniya-chisel-v-sisteme-ostatochnyh-klassov.html*

UDC 658:512.011:681.326:519.713

Liubchenko O. S.
Kharkiv National University of Radio Electronics

Research Generation Register Model Components Methods for Verification Environment

The Universal Verification Methodology (UVM) is a standardized methodology for verifying integrated circuit designs. It represents the latest advancements in verification technology and is designed to enable creation of robust, reusable, interoperable verification IP and testbench components.

The UVM Environment is a hierarchical component that groups together other verification components that are interrelated. Typical components that are usually instantiated inside the UVM Environment are UVM Agents, UVM Scoreboards, or even other UVM Environments. The top-level UVM Environment encapsulates all the verification components targeting the DUT [1].

The UVM register layer classes are used to create a high-level, object-oriented model for memory-mapped registers and memories in a design under verification (DUV). The UVM register layer defines several base classes that abstract the read/write operations to registers and memories in a DUV. This abstraction mechanism allows the migration of verification environments and tests from block to system levels without any modifications. It also can move uniquely named fields between physical registers without requiring modifications in the verification environment or tests. Figure 1 shows how a register model is used in a verification environment [2].

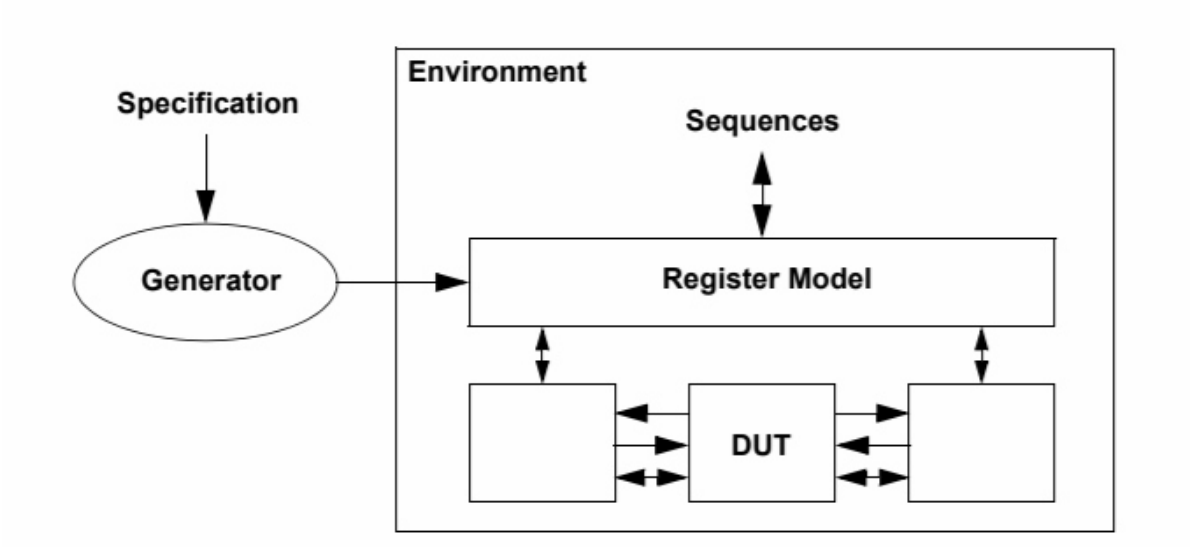


Figure 1 – Register Model in an UVM Environment

A register model can be written by hand, following the pattern given for the SPI master example. However, with more than a few registers (nowadays designs have hundreds and thousands of registers and tens of thousands of register fields) this can become a big task and is always a potential source of errors. Here “Generator” bubble from Figure 1 comes into play. Its role is to take the register specifications of a design (from user input or from the spreadsheet) and automatically generate the equivalent register model in SystemVerilog code. There are a number of other reasons why using a generator is helpful:

- It allows a common register specification to be used by the hardware, software and verification engineering teams
- The register model can be generated efficiently without errors
- The register model can be re-generated whenever there is a change in the register definition
- Multiple format register definitions for different design blocks can be merged together into an overall register description

There are a number of register generators available commercially, including Mentor Graphics' Register Assistant. Register descriptions can be read from spreadsheet (CSV), IP-XACT, and XML format inputs or via API commands within a script. The purpose of this project is to create user-friendly generator with clear GUI available for production and educational usage.

A register model is typically composed of a hierarchy of blocks that map to the design hierarchy. Blocks can contain registers, register files and memories, as well as other blocks. In order to be able to use the UVM register model effectively, it is important to have a mental model of how it is structured in order to be able to find your way around it.

The register model is implemented using five main building blocks: the register field, the register, the memory, the register block and the register map. The register field models a collection of bits that are associated with a function within a register. A field will have a width and a bit offset position within the register. A field can have different access modes such as read/write, read only or write only. A register contains one or more fields. A register block corresponds to a hardware block and contains one or more registers. A register block also contains one or more register maps [1-2].

The UVM register layer classes are not usable as-is. They only provide generic and introspection capabilities. They must be specialized via extensions to provide an abstract view that corresponds to the actual registers and memories in a design. Due to the large number of registers in a design and the numerous small details involved in properly configuring the UVM register layer classes, this specialization is normally done by a model generator. Model generators work from a specification of the registers and memories in a design and are thus able to provide an up-to-date, correct-by-construction register model. Model generators are outside the scope of the UVM library [3].

The UVM register layer models and abstracts registers of a design. It attempts to mirror the design registers by creating a model in the verification testbench. By applying stimulus to the register model, the actual design registers will exhibit the changes applied by the stimulus.

The benefit of this approach comes from the high level of abstraction provided. The bus protocols for accessing registers can change from design to design, but any stimulus developed for verification of the registers doesn't have to. This makes it easy to port code from one project to the next if the registers are the same.

List of sources

1. *Standard Universal Verification Methodology Class Reference Manual, Release 1.2. Accellera Systems Initiative. – 2014*
2. *UVM 1.2 User's Guide. Accellera Systems Initiative. 2014. – 190p*
3. *Brian Hunter. Advanced UVM. - 2nd Edition, Kindle Edition. – 2015. – 200p.*

УДК 004.451

Бабич Є. Ю.
Центральноукраїнський національний технічний університет

Кооперативна багатозадачність в RTOS

Сучасні операційних систем (ОС) є багатопроцесними, або виконувати одночасно декілька задач. Насправді, кожне процесорне ядро може виконувати лише один потік(thread) виконання задачі в будь-який момент часу. Частина операційної системиRTOS, яка називається планувальником (sheduler), несе відповідальність за вибір того, яку задачу(процес) запускати, і забезпечує мультиплекативне виконання за допомогою швидкого перемикання між кожним процесом(здачею).

Одним з основних методів синхронізації процесів операційної системи реального часу(ОСРВ) є кооперативна багатозадачність(КБЗ). КБЗ є такий багатозадачний стиль, в якому ОСРВ ніколи не ініціює перемикання контексту з поточної діяльності на інший процес. Замість цього процеси періодично "добровільно" віддають контроль або знаходяться в станіочікування, так що кілька додатків можуть працювати одночасно. Цей тип багатозадачності називається «кооперативним», оскільки всі програми повинні взаємодіяти з роботою всієї схеми планування. У ОСРВ такий механізм планування відомий як спільний планувальник. Його роль полягає в тому, щоб при переведенні у стан виконання процеси захоплювали управління назад без використання системних переривань.

Хоча КБЗ рідко використовують в сучасних великих системах, крім деяких додатків, таких як CICS або підсистема JES2, кооперативна багатозадачність була основною схемою компонування для 16-розрядних програм, які використовували Microsoft Windows для версій Windows 95 і Windows NT, а також Mac OS версії OS X.

Оскільки система КБЗ вимагає, щоб кожен процес регулярно надавав час іншим процесам у системі, то одна погано спроектована програма може захопити надовго ресурс процесора, виконуючи великі обчислення або перейти у активний стан очікування. Обидва чинники можуть привести до "дедлока" системи. У серверному середовищі це є загрозою, яка робить всю систему нестійкою при великому навантаженні. Однак,КБЗ дозволяє значно спростити реалізацію процесів, оскільки їх виконання ніколи не може бути перервано несподівано планувальником процесора. Наприклад, різні функції всередині програми не повинні використовуватися повторно.

Зазвичай більшість ОСРВ використовуються для мікроконтролерних систем і не є великими ОС (за виключенням QNX). Планувальник в ОСРВ призначений для забезпечення передбачуваного шаблону виконання. Це особливо цікаво для вбудованих систем, оскільки ці системи часто мають вимоги до точного часу свого виконання. Вимоги до режиму реального часу визначають, що вбудована система повинна реагувати на певну подію протягом строго певного часу. Гарантія для задоволення потреб у реальному часі може бути реалізована лише тоді, коли можна прогнозувати поведінку планувальника ОС.

Список використаних джерел

1. Курниц А. FreeRTOS — операционная система для микроконтроллеров // Компоненты и технологии. 2011. № 2–9.
2. www.freertos.org
3. http://ru.wikipedia.org/wiki/FreeRTOS
4. http://electronix.ru/forum/index.php?showforum=189

УДК 004.42

Банченко В. О.[*]
Центральноукраїнський національний технічний університет

Дослідження та програмна реалізація стиснення звукової інформації за допомогою вейвлетних методів

Стиснення звукових даних (стиснення аудіо) — тип стиснення даних, кодування, що застосовується для зменшення розміру аудіофайлів або заради можливості зменшення смуги пропускання для потокового аудіо. Алгоритми стиснення звукових файлів реалізуються у комп'ютерних програмах, які називаються аудіокодеками. Розробка нових спеціалізованих алгоритмів стиснення звукових даних аргументовано тим, що універсальні алгоритми стиснення неефективні для роботи зі звуком [1].

Розрізняють стиснення звуку без втрат (англ. lossless), що робить можливим відновлення вихідних даних без спотворень, та стиснення з втратами (англ. lossy), при якому таке відновлення неможливе [1]. Алгоритми стиснення з втратами дають більшу ступінь стиснення, наприклад audio CD може вмістити трохи більше години «нестисненої» музики, при стисненні без втрат CD вмістить майже 2 години музики, а при стисненні із втратами при середній якості – 7-10 годин. Стиснення звуку без втрат інформації є актуальним, попри порівняно малого коефіцієнту стиснення, бо в такому випадку відновлені дані є придатними для складних аналізів, які можуть бути використані, наприклад, в наукових дослідженнях.

Для кодеків зі стисненням з втратами інформації MP3 є лідером за поширеністю, але при цьому не є найкращим за технічними параметрами. Наприклад, існують формати, що дозволяють отримати порівнянну якість (суб'єктивно) при меншій щільності (AAC, OGG) [3]. Також у форматі MP3 відсутній режим кодування без втрат англ. lossless, придатний для професіоналів [2]. Для домашньої музичної колекції (коли немає необхідності програвати композиції на музичному центрі або поширювати їх через інтернет) можна скористатися конкуруючими форматами.

MP3 непридатний для професійного використання музикантами вже через те, що дані стискаються з втратами, і при кожному редагуванні файлу якість погіршується. При цьому формат цілком підходить (з професійної точки зору) для розповсюдження демонстраційних композицій або інших способів «роздачі» своєї музики завдяки повсюдній поширеності програвачів.

Вейвлет стиснення добре підходить для стиснення зображень. Відомі реалізації вейвлетного стиснення JPEG 2000 та DjVu для нерухомих зображень, CineForm і BBC's Dirac для відео. Вейвлет стиснення може бути виконано з втратами та без втрат, що робить метод більш універсальним [2].

За допомогою вейвлет-перетворення, вейвлет стиснення є достатнім для опису перехідних процесів, таких як ударні звуки в аудіо, або високочастотні компоненти в двовимірних зображень, наприклад, зображення зірок на нічному небі. Це означає, що перехідні елементи даних сигналу можуть бути представлені меншою кількістю інформації, ніж було б у разі використання якої-небудь іншої трансформації, наприклад популярного дискретного косинусного перетворення.

Дискретне вейвлет-перетворення було успішно застосовано для стиснення електрокардіографічних (ЕКГ) сигналів. У даній роботі, висока кореляція між відповідними вейвлет-коефіцієнтами сигналів послідовних серцевих циклів і використовуються лінійне передбачення з використанням.

[*] Науковий керівник – Дрєєв О. М., канд. техн. наук, доцент кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету

Автором було виконано роботу по реалізації програмного забезпечення яке застосовувало алгоритм стиснення звукової інформації методами двовимірних вейвлетів. Алгоритм полягає в приведенні звукового файлу до файлу не стисненого зображення, після застосування до цього зображення стиснення за допомогою кодека JPEG2000 отримувався стиснений за допомогою алгоритму для зображення звук. У якості звукових даних виступають аудіо-доріжки у форматі WAV. Із них отримуються байти даних, без включення заголовку, розраховується розмір картинки (квадрату). Потім байти звукових даних записуються у певній послідовності (в реалізації було використано прогресивний запис звуку та за кривою Гільберта) у зображення BitMap, після чого генерується заголовок для даного формату зображення. Для стиснення зображень існує багатий набір кодеків, але найефективнішим кодеком, використовуючим вейвлетні алгоритми, вважається JPEG2000.

В результаті було отримано наступні дані, які показано в наступній таблиці 1.

Таблиця 1 – Розміри аудіо файлу стисненого та відновленого різними кодеками

	WAV	JPEG2000	RAR	ZIP	MP3
Стиснений	55 960 байт	30 952 байт	30 141 байт	29 772 байт	10 494 байт
Відновлений	55 960 байт	55 960 байт	55 960 байт	55 960 байт	230 478 байт
Втрати	-	-	-	-	Значні втрати якості

В результаті дослідження було виявлено, що вейвлетні методи пристосовані для кодування зображення мають не достатній ступінь стиснення, що робить актуальною задачею створення спеціалізованого одновимірного вейвлетного алгоритму для стиснення звуку. Схема роботи кодеку, який розробляється, представлено на наступному рисунку 1.

Рисунок 1 – Схема послідовності дій вейвлетного стиснення звуку

Висновок. В результаті досліджень показано застосовність вейвлетних методів для стиснення звуку, але метод потребує вдосконалення і задача пошуку більш досконалних алгоритмів є актуальною.

Список використаних джерел

1. *Сэломон Д. Сжатие данных, изображений и звука/ Д. Сэломон// Москва: Техносфера, 2004. — 368 с. — ISBN 5-94836-027-X.*
2. *Капшій О. В. Вейвлет-перетворення у компресії та попередній обробці зображень / О. В. Капшій, О. І. Коваль, Б. П. Русин. – Львів: Сполом, 2008. – 208 с. — ISBN 978-966-665-554-0.*
3. *Плужник Е.Н., Сравнительный анилиз lossy-аудиоформатов/ Е.Н. Плужник, А.А. Уварова. В сборнике: Студенческая наука для развития информационного общества сборник материалов VI Всероссийской научно-технической конференции. 2017. С. 296-298.*

УДК 62-53:623.746-519

Башинська О. О.
Чернігівський національний технологічний університет

Особливості розшифровки телеметричних логів безпілотних авіаційних комплексів в умовах неповноти інформації про перелік типів повідомлень

Концепція побудови фреймів та повідомлень протоколу телеметричного обміну між безпілотним авіаційним комплексом (БпАК) та наземною станцією керування MAVLink полягає в тому, щоб підтримувати творчість самих різних розробників безпілотних систем. Тому в множині XML-файлів опису специфікації [1] повідомлень протоколу MAVLink наводяться тільки такі типи останніх, які є загальновживаними. Головна їх множина (це так звані стандартні повідомлення) міститься в файлі common.xml [2].

Наприклад, опис одного типу повідомлення з файлу common.xml та його структури виглядає так:

<message id="49" name="GPS_GLOBAL_ORIGIN">

<description>Once the MAV sets a new GPS-Local correspondence, this message announces the origin (0,0,0) position</description>

<field type="int32_t" name="latitude" units="degE7">Latitude (WGS84)</field>

<field type="int32_t" name="longitude" units="degE7">Longitude (WGS84)</field>

<field type="int32_t" name="altitude" units="mm">Altitude (AMSL). Positive for up.</field>

<extensions/>

<field type="uint64_t" name="time_usec" units="us">Timestamp (UNIX Epoch time or time since system boot). The receiving end can infer timestamp format (since 1.1.1970 or since system boot) by checking for the magnitude the number.</field>

</message>

Розробники (постачальники) БпАК, які мають необхідність використовувати в роботі їх комплексів якісь додаткові типи повідомлень, створюють “під себе” так звані “діалекти” MAVLink – це специфічні для конкретного постачальника розширення протоколу. Описи специфічних структур та повідомлень таких постачальників, зберігаються в додаткових окремих XML-файлах. Так створюється розгалуження (розвилка, англ. fork) розробки протоколу MAVLink, за яку починає нести відповідальність той розробник, який це зробив. Оскільки протокол MAVLink ліцензований під відкритою ліцензією Creative Commons Universal (CC0 1.0 Universal) [3], такий стан речей є цілком нормальним.

Структура кадру (фрейму) протоколу MAVLink версії 1.0 в нотації мови програмування С така[2]:

```
uint8_t magic; ///< маркер початку фрейму 0xFE
uint8_t len; ///< довжина повідомлення
uint8_t seq; ///< лічильник пакету (0–255), потрібний
 /// для виявлення факту втрати повідомлення
uint8_t sysid; ///< ID системи, яка відправила фрейм
uint8_t compid; ///< ID компоненту,
 /// який відправив фрейм
```

uint8_t msgid; ///< код типу повідомлення
uint8_t payload[max 255]; ///< повідомлення, максимум 255 байт
uint16_t checksum; ///< контрольна сума фрейму

Із наведеного фрагменту видно, що в лог-файлі початки кадрів знахо-дити легко: послідовне, байт за байтом, читання файлу знаходить 0xFE, за яким, власне, і розташований черговий фрейм. Звернімо увагу на той факт, що довжина різних фреймів буде різною, бо в структурі присутнє поле payload змінної довжини, в той час як всі інші поля мають фіксований розмір загальною сумою 8 байт. Тому читання всього фрейму вимагатиме попереднього обчислення суми len+8, тобто розміру фрейму.

Втім, подібна ситуація приводить до того, що при постобробці лог файлів БпАК, одержаних під час їх використання, неможливо розраховувати на те, що наявні в лог файлі повідомлення будуть виключно із стандартного набору. Практично завжди час від часу доводиться зустрічати нестандартні типи повідомлень, оскільки більшість постачальників все ж таки використовує свої власні діалекти MAVLink. Звичайно, додаткові XML-файли розширення протоколу постачальники використовують тільки при програмуванні програмного забезпечення своїх БпАК і їх наявність проявляється тільки в процесі постобробки як поява в потоці повідомлень нестандартних їх типів. Цю особливість треба враховувати при розробці ПЗ постобробки лог файлів.

Розгляд структури опису повідомлення показує, що в кожному типі повідомлення описуються певні параметри різної кількості (рис.1). Вони мають різний зміст та розмірність, і при аналізі логів дослідника цікавить характер змін саме цієї категорії даних лог файлу.

З викладеного ясно, що для змістовної інтерпретації даних лог файлу потрібно одночасно і синхронно читати дані з двох джерел – XML-файлу з описами структури повідомлення, та з самого лог файлу, в якому містяться числові значення параметрів (сигналів). Тільки таким чином можна одержувати пари "ім'я_сигналу=значення_сигналу", за якими можна працювати далі, скажімо, побудувати графік зміни певного сигналу в часі.

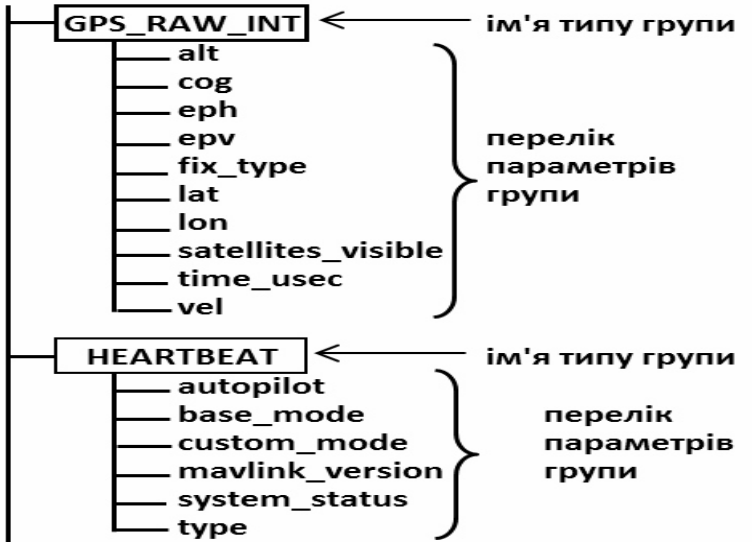


Рисунок 1 – Підпорядкованість типів повідомлень та параметрів (сигналів).

В самому лог файлі в кожному фреймі повідомлення являє собою просто суцільний ланцюжок значень параметрів (сигналів) повідомлення без згадки хоча б про назву параметру. Нариклад, опис структури повідомлення типу “GPS_GLOBAL_ORIGIN”, наведеного вище, фізична структура повідомлення виглядатиме як на рис. 2.

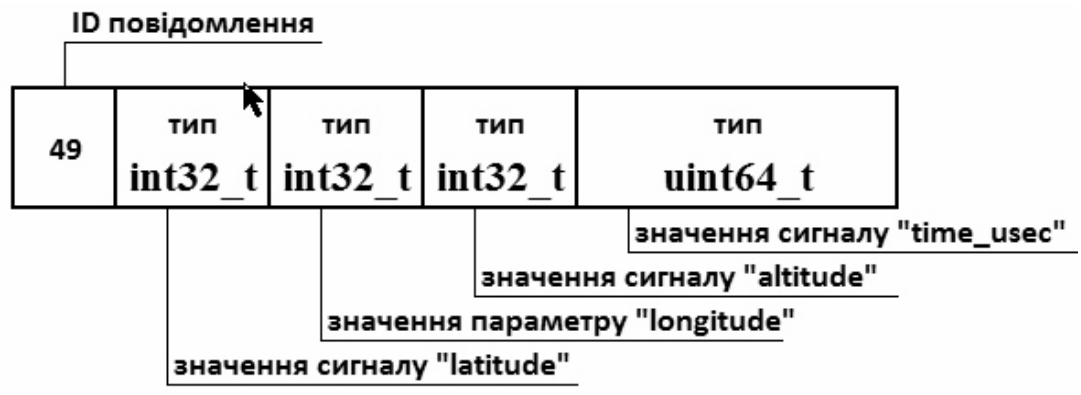


Рисунок 2 – Структура повідомлення GPS_GLOBAL_ORIGIN (приклад)

Подібне зведення імен сигналів з їх значеннями не є швидкою програмною операцією. До того ж одночасне синхронізоване використання двох джерел даних теж створює певні алгоритмічні труднощі при розшифруванні лог файлів. Тому виникає потреба знайти такі рішення, в яких ці труднощі можна було б якось обійти.

З викладеного видно, що змістовна інтерпретація лог-файлу, який розглядається ізольовано, сильно утруднюється тим фактом, що в повідомленнях (payload) фреймів присутні виключно числові дані про значення передаваних сигналів (параметрів). Ніяких прямих вказівок на зміст або хоча б назви цих параметрів в лог файлі не міститься в принципі. Непрямим посиланням на цю інформацію є тільки номер типу повідомлення, який у фреймі йде безпосередньо перед повідомленням. За цим номером в одному з XML-файлів опису специфікації протоколу можна знайти структуру повідомлення з назвами параметрів та послідовністю їх розташування в повідомленні. І тільки співставленням ланцюжка назв параметрів з ланцюжком значень стає можливим одержання пар “назва–значення” для подальшої обробки.

Враховуючи вищесказане, актуальною є задача розробки або знаходження в готовому вигляді певного інструменту одержання згаданих вище пар “назва–значення” параметрів повідомлень лог-файу, оскільки це головна передумова подальшої змістовної інтерпретації логу.

Список використаних джерел

1. *MAVLink Developer Guide. [Електронний ресурс] – Режим доступу: URL: https://mavlink.io/en/. – Назва з екрану.*
2. *Mavlink.message_definitions.v1.0. [Електронний ресурс] – Режим досту-пу: URL: https://github.com/mavlink/ mavlink/tree/ master/ message_definitions/ v1.0. – Назва з екрану.*
3. *(CC) Creative Commons. About The Licenses. [Електронний ресурс] – Режим доступу: URL:https://creativecommons.org/licenses/. – Назва з екрану.*

УДК 004.272.2:519.63

Бобилєва О. С., Дмитрієва О. А.
Донецький національний технічний університет

Дослідження методу стрільби при розв'язанні крайових задач

Однією з основних проблем при моделюванні поведінки динамічних об'єктів з зосередженими параметрами є необхідність чисельної реалізації систем звичайних диференціальних рівнянь (СЗДР) великої розмірності, заданих у формі задачі Коші [1]. Велику кількість робіт в цьому напрямку присвячено модифікації або розробці нових чисельних методів [2-3], спрямованих на ефективну реалізацію в паралельних комп'ютерних системах [4], розглянуто питання паралельного управління кроком інтегрування [5], розроблено нові підходи до оцінювання локальної та глобальної похибок [6], що сприяє посиленню об'єктивності отриманих результатів. Складність завдання при моделюванні динамічних процесів значно підсилюється, якщо мова йде про крайові задачі для СЗДР, до яких приводить велика кількість прикладних задач.

Мета роботи полягає в розробці та дослідженні алгоритмічних методів розв'язання крайової задачі, орієнтованих на ефективну реалізацію в паралельних комп'ютерних системах.

Розв'язання крайової задачі передбачає знаходження часткового розв'язання системи звичайних диференційних рівнянь з додатковими умовами, що накладаються на значення функцій не менше ніж у двох точках відрізка $[a,b]$. Отже, крайова задача для звичайних диференціальних рівнянь ставиться для системи диференціальних рівнянь порядку не менше другого [7]. Лінійна крайова двоточкова задача полягає в знаходженні функції $y(x)$, що задовольняє лінійному звичайному диференціальному рівнянню і лінійним двоточковим крайовим (граничним) умовам. В роботі розглядаються випадки, коли додаткові умови задачі задані на кінцях відрізка, але запропоновані підходи можуть застосовуватися і для завдань, у яких додаткові умови можуть задаватися й у внутрішніх точках відрізка (внутрішні крайові умови). Крім того, додаткові умови можуть пов'язувати між собою значення кількох функцій, похідних функцій або комбінацій функцій і похідних в одній або декількох точках відрізка, де шукається розв'язок [7].

З цього можна зробити висновок, що знаходження точного розв'язку викликає більше труднощів, ніж розв'язання задачі Коші. Звідси – підвищений інтерес і велика різноманітність наближених методів розв'язання таких завдань [6].

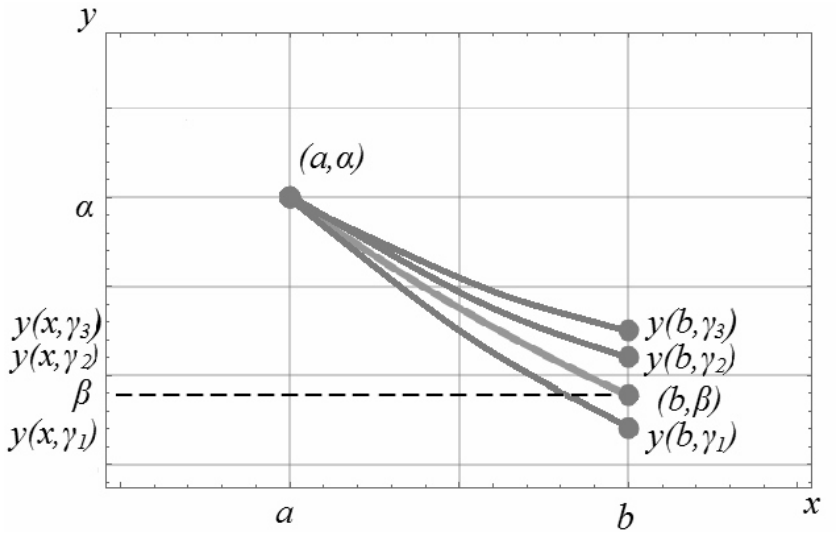


Рисунок 1 – Схема метода стрільби

Ідея алгоритму засновується на тому, що на початку встановлюємо ліву та праву межі симетричні відносно α, які дорівнюють $\alpha - \Delta$ та $\alpha + \Delta$. В залежності від кількості процесів n, за допомогою яких і буде виконуватися розпаралелювання, встановлюється кількість додаткових значень $\gamma_k, k = 1,2,...n$.

Початковий відрізок поділяється на кількість процесів, так щоб у кожного процесора був свій під відрізок. Всі підвідрізки однакового розміру. Значення γ_k дорівнює випадково обраному значенню з підвідрізку, що належить процесору. Після того, як усі процесори обрали свої значення, виконується розв'язання задачі Коші за допомогою класичного багатостадійного методу. Після цього усі отримані розв'язки з кожного процесору пересилаються до головного, де і виконується перевірка на коректність отриманого розв'язку (1) крайової задачі

$$| y(b, \gamma_k - \beta) | \le \varepsilon \tag{1}$$

де ε – задана похибка.

При виконанні умови (1) вважається, що розв'язання було знайдено з заданою точністю, якщо умову не виконано, то розрізняються наступні ситуації:

- ліва та права межи завеликі, треба їх зменшити;
- ліва та права межи замалі, треба їх збільшити;
- відстань, що регламентована умовою (1), порушена, необхідно скоректувати відповідну границю.

На кожний випадок передбачена відповідна дія, що дозволяє коректувати процес обчислень. Також слід зазначити, що розв'язання усіх цих ситуацій виконується за допомогою встановлення нових границь. Для першого та другого випадку встановлюються межі того підвідрізка, який найближче знаходиться до значення β. Для останнього випадку нові межі встановлюються тільки для межових підвідрізків відповідно зменшуючи та збільшуючи їх у відповідності до отриманих результатів. Перевірку на кожному отриманому розв'язанні виконання умови (1) та коригування межі варіації додаткової початкової умови $y'(a)$ можна виконувати паралельно.

Для тестування роботи запропонованого алгоритму була використана крайова задача [8] (2) на інтервалі $x \in [1;3]$

$$y'' = \frac{1}{8}(32 + 2x^3 - yy'), \tag{2}$$

з граничними умовами (3)

$$y(1) = 17, y(3) = \frac{43}{3}, \tag{3}$$

та відомим точним розв'язком (4)

$$y(x) = x^2 + \frac{16}{x} \tag{4}$$

Для проведення обчислювальних експериментів і в послідовному і в паралельному варіантах реалізації використовувалося середовище розробки Microsoft Visual Studio та мова високого рівня C++.

Реалізація запропонованого алгоритму здійснювалася за допомогою програмного інтерфейсу передачі інформації MPI (Message Passing Interface). Визначення експериментального часу виконання алгоритму проводилося з залученням можливостей бібліотеки MPI.

На рис. 2 наведено результати експериментів, які встановлюють залежність часу виконання алгоритму від кількості процесорів та розрахункових вузлів при фіксованій припустимій похибці обчислень, яка дорівнювала значенню 10-5. Результати, які були отримано при проведенні такого експерименту є прогнозованими. Вони показують, що час виконання зменшується при залученні більшої кількості процесорів.

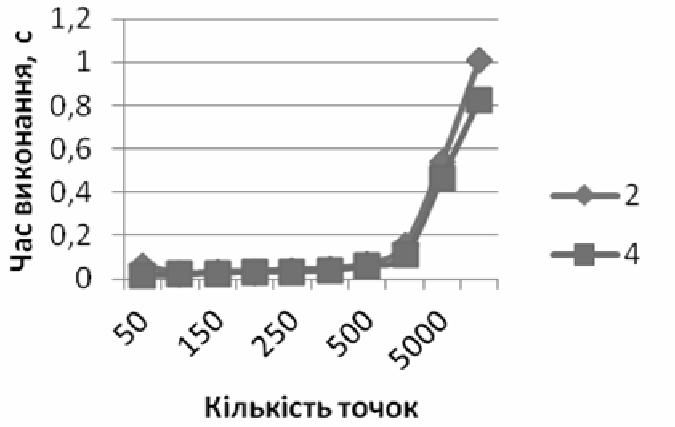


Рисунок 2 – Залежність часу виконання алгоритму від кількості точок для 2 та 4 процесорів

В роботі запропонований паралельний алгоритм балістичного методу, для розробки якого використовувалося середовище Microsoft Visual Studio та мова високого рівня C++.

Наукова новизна полягає у розробці та удосконалені паралельного алгоритму реалізації чисельних методів розв'язання крайової задачі та розв'язання задачі Коші. Було проведено дослідження розробленого методу, проаналізовано результати та відзначено закономірності.

Практична цінність полягає в розробці програмної системи, що містить в собі реалізацію чисельного методу розв'язання крайової задачі шляхом зведення її до задачі Коші та подальшої паралельної реалізації багатостадійним методом.

Програма має вигляд консольного додатка до операційної системи. Подалі система може застосовуватися в інших розробках, як у вигляді окремого модуля, так і в якості вбудованої з модифікацією її коду.

Список використаних джерел

1. *Хайрер Э. Решение обыкновенных дифференциальных уравнений. Нежесткие задачи / Хайрер Э., Нерсетт С., Ваннер Г. // М.: Мир, 1990. – 512с.*
2. *Якимов А.С. Аналитический метод решения краевых задач – Томск: Том. ун-та, 2011. – 199 с.*
3. *Дмитриева О.А. Параллельные численные методы моделирования динамических объектов: монография / О.А. Дмитриева. – Красноармейск: ГВУЗ «ДонНТУ», 2016. – 384 с*
4. *Дмитриева О.А. Разработка коллокационных схем параллельного управления шагом в эволюционных уравнениях / О.А. Дмитриева, Н.Г. Гуськова // Вестник НТУ "ХПИ". Серия: Информатика и моделирование. – Харьков: НТУ "ХПИ". – 2018. – № 24(1300). – С. 25 – 36.*
5. *Dmitrieva O. Parallel Step Control. Development of parallel algorithms of the step variation for simulation of stiff dynamic systems / O. Dmitrieva, L. Feldman. – Lambert Academic Publishing. – 2013. – 72p.*
6. *Фельдман Л.П. Чисельні методи в інформатиці / Л.П. Фельдман, А.І. Петренко, О.А. Дмитрієва. – К.: Видавнича група BHV, 2006. – 480 с.*
7. *Вержбицкий В.М. Основы численных методов: Учебник для вузов/ В.М. Вербицкий. – М.: Высш. шк., 2002. – 840 с.*
8. *Ha S.N. A Nonlinear Shooting Method for Two-Point Boundary Value Problems /S. N. Ha // Computers and Mathematics with Applications 42, Oxford: Pergamon Press .- 2001. – p. 1411 – 1420.*

УДК 004.942

Газдюк К. П., Жихаревич В. В., Остапов С. Е., Чижевський В. В.
Чернівецький Національний університет імені Юрія Федьковича

Розробка системи для комп'ютерного моделювання біологічних процесів

Комп'ютерне моделювання є невід'ємним компонентом сучасної наукової діяльності. Останні досягнення в комп'ютерній техніці мають величезний вплив на потенціал комп'ютерного моделювання не лише як допоміжного інструменту до кожної експериментальної програми досліджень у різних галузях науки, але й як окремого об'єкту дослідження. Зокрема, методи комп'ютерного моделювання стали важливим інструментом для вивчення закономірностей динаміки біо-процесів та структур [1, 2].

Основна увага роботи зосереджена на побудові системи імітаційного моделюванні біологічних процесів і структур. Характерною особливістю складних систем є нетривіальні шаблони і колективна поведінка, що можуть виникати з відносно простих правил для окремих агентів. Складність вивчення цих механізмів полягає в тому, що в лабораторних умовах майже неможливо відстежити динаміку окремих частинок, які входять до їх складу. Також враховано зворотній зв'язок між цими самоорганізаційними механізмами, і, безпосередньо, самими процесами, що відбуваються в біо-подібній структурі (наприклад, рух, ріст, поділ клітини, та ін.). Це вимагає збору та аналізу біологічних даних, та застосування комп'ютерного моделювання як з метою пояснення поведінки даного біологічного процесу, так і для отримання нових, невідомих раніше закономірностей Універсальність та зручність програмного засобу моделювання вимагає необхідність його побудови на основі досить простих та гнучких методів, які опираються на застосування знань із теоретичної біофізики та класичної математики.

Асинхронні стохастичні клітинно-автоматні моделі є найбільш вживаними при моделюванні біологічних систем, оскільки відображають не детермінованість більшості природніх процесів. Тому, для дослідження пов'язаного з динамікою структури модельованого простору, обрано метод рухомих клітинних автоматів (РКА), який дозволяє використовувати концепцію сусідства та описувати процеси, що відбуваються у біо-структурах, набором функцій взаємодій між сусідніми агентами (клітинами).

Візуалізація результатів моделювання є важливим компонентом даної системи, що базується на побудованій моделі. Обробка наборів даних при 3D-просторовому моделюванні є складним та трудомістким процесом, тому важливо включити просту у використанні внутрішню систему візуалізації. Розроблено набір інструментів візуалізації, які дозволяють швидко і легко змінювати дані, налаштовувати типи та кількість РКА, а також функції взаємодії. Для 3D-візуалізації, анімації та вивчення даних із зміною часу використовується бібліотека Java OpenGL (JOGL).

Розроблена система надає можливість моделювати біо-процеси та структури. Анімація та тривимірна візуалізація дозволяють користувачу візуалізувати тимчасову динаміку біоподібних структур. Отримані результати дають змогу не лише пояснити поведінку біологічного процесу, що досліджується але й отримати нові закономірності.

Список використаних джерел

1. *M. Scianna, L. Preziosi, L. Preziosi; Ed. by M. Chaplain, J. Batzel, M. Bachar. New Challenges for Cancer Systems Biomedicine. Hybrid cellular Potts model for solid tumor growth, Springer, 2012, pp. 205–224.*
2. *Multicompartment cell-based modeling of confined migration: regulation by cell intrinsic and extrinsic factors - Sandeep Kumar, Alakesh Das and Shamik Sen, Molecular Biology of the Cell, DOI:10.1091/mbc.E17-05-0313, (2018).*

УДК 004(043.2)

Ганістрат Д. О., Карабут Н. О.
Криворізький національний університет

Методи інтеграції програмного забезпечення

Останнім часом стає актуальним обговорення комп'ютерним суспільством питання інтеграції програм. Загальні цілі інтеграції це зменшення вартості експлуатації сукупності програм підприємства, збільшення швидкості виконання типових завдань або гарантувати його термін виконання, підвищення якості виконання завдань за рахунок формалізації процесів та мінімізації людського фактору, як основного джерела помилок. Майже не існує інформаційних систем, які самостійно мали змогу задовольнити потреби сучасних підприємств. У цих системах доволі часто оброблюються однакові данні – починаючи із довідників та класифікаторів. Для взаємодії програм використовуються такі методи, як обмін файлами, загальна база даних, віддалений виклик і асинхронний обмін повідомленнями. Обмін файлами найбільш поширений підхід до організації взаємодії. Це зв'язано з відносною легкістю реалізації, а також існуванням стандартних форматів обміну. Більша частина корпоративних інформаційних систем дозволяє завантажувати файли. Недоліком даного підходу є те, що якщо необхідно оперувати складними структурами, то прості формати обміну вже не актуальні.

Загальна база даних. Даний підхід концептуально дуже простий – декілька інформаційних систем або програм використовують одну базу даних. Головний його недолік – зв'язок між інтегрованими програмами настільки тісний, що іноді неможливо помітити різницю між ними.

Стандарти на віддалений виклик процедур дозволяє програмному коду, який виконується на одному комп'ютері, викликати код на іншому. Перевагою віддаленого виклику процедур є його синхронність, завдяки цьому виклик виконується негайно. Основний недолік віддаленого виклику – вимога працездатності усіх задіяних програм в момент взаємодії.

Асинхронний обмін повідомленнями – це, підхід, який відтворювався спеціально для інтеграції інформаційних систем. Ідея концептуально проста і нагадує роботу електронної пошти. Повідомлення гарантовано дійде завдяки механізму черг повідомлень, які звільняють з взаємодіючих систем турботу про надійність мережі передачі даних, працездатності взаємодіючих систем в певний час. Недоліком цього підходу є висока ціна. Система гарантованої доставки на основі черг повідомлень зазвичай сама по собі не дешева. Але, є і вільно поширювані безкоштовні, які потрібно розвернути, навчити фахівців, підтримувати, написати адаптери між системою доставки і програмою.

Проаналізувавши основні методи інтеграції програмного забезпечення можна зробити висновок, що всі методи мають позитивні і негативні сторони. При постанові завдання вибору між цими методами потрібно дивитись на тип програм, як вони розташовані і на скільки складну інформацію потрібно буде передавати між програмами.

Список використаних джерел

1. *Соммервил Иан. Инженерия программного обеспечения, 6-е издание /Иан Соммервил. – М.: Вильямс, 2002. - 624 с.*
2. *Орлов С.А. Технологии разработки программного обеспечения. Разработка сложных программных систем / С.А. Орлов - СПб.: Питер, 2002. - 464 с.*

УДК 004.62

Згара К. Г.
ДВНЗ «Приазовський державний технічний університет»

Компоненти та архітектура корпоративної соціальної мережі

Соціальні мережі стали невід'ємною частиною життя сучасного суспільства. Незалежно від віку людина знаходить собі зручну соціальну мережу та в ній – друзів по інтересам. Але об'єднання людей можливо не тільки по інтересам, а й з корпоративних питань. Так актуальним є створення соціальної мережі для студентів. Це дає, по-перше, можливість поширення широкомовних повідомлень серед студентів одного університету або серед студентів усіх вишів, а по-друге – це створення інформаційного простору для спілкування молоді.

Для написання системи були використані наступні технології: NodeJS, MySQL, React Native, AWS Cognito, Docker.

Систему було прийнято розділити на компоненти. Кожен компонент повинен дотримуватися принципу SOLID. Були розроблені наступні компоненти:

- Компонент авторизації. Даний компонент відповідає за реєстрування та надання доступу користувачам. Для поліпшення безпеки проекту було прийнято рішення використовувати сторонні системи авторизації, було вибрано AWS Cognito. Розроблений компонент був як посередник між AWS Cognito і кінцевим користувачем.
- Компонент "Управління університетами". Так як додаток призначений для користувачів студентів в університеті, то потрібно було створити компонент, який міг керувати цими університетами: створювати, видаляти, отримувати списки студентів, змінювати налаштування і т.д.
- Компонент "Управління користувачами". Даний компонент призначений для управлінням профілем користувача, в цьому компоненті реалізовано оновлення профілю, картинки профілю, зміна університету.
- Компонент "Управління постами". Цей компонент один з фундаментальних і є основним функціоналом для користувача. Цей компонент дозволяє створювати пости, отримувати всі пости, додавати пости в обране, отримувати популярні пости і т.д.
- Компонент "Управління потоками". Додаток включає в себе можливість поширення широкомовних повідомлень адміністратором, серед студентів одного університету. У цьому компоненті реалізовано: відправлення текстових повідомлень, створення відповіді на повідомлення, відправка автоматичних повідомлень (наприклад, якщо пост користувача опублікували в соціальній мережі, то йому автоматично відправляється повідомлення з поздоровленням).

Також в системі використовується безліч інших компонентів, таких як: компонент для розсилки повідомлень, компонент для завантаження картинок в хмару, компонент для управління нагородами (в додаток існує система балів і бонусів) і т.д.

Додаток розташовується в Docker контейнерах і запускається на віртуальних машинах Амазону. Для створення API використовувалася RESTful модель і пакети передавалися по протоколу HTTPS. Для аутентифікації і авторизації користувача використовувався стандарт JWT.

Архітектура апобудована на базі шаблону Model-View-Presenter (MVP). В якості View був створений інтерфейс API для реалізації концепції SPA. Використані контролери, які можуть обробляти запити клієнта і видавати потрібну інформацію. Як клієнт виступив додаток на React Native. Цей додаток отримує дані з сервера і виводить користувачеві. Таким чином розроблено соціальну мережу.

УДК 004.415.2:006.1

Золотухін Б. Є.
Центральноукраїнський національний технічний університет

Актуальні питання стандартизації та регламентації процесів реалізації програмних засобів

Розвиток будь-якої галузі економіки обов'язково супроводжується формалізацією підходів, які використовуються, та появою стандартів різного рівня. На ранніх етапах окремі підприємства формалізують внутрішні процеси, щоб забезпечити повторюваність результатів процесу або створення певного продукту. Для полегшення взаємодії підприємств та зручності споживачів розробляються галузеві стандарти. Розвиток кожного виду господарської діяльності призводить до потреби у державних засобах забезпечення якості продукції або процесу, тому розробляються й затверджуються державні стандарти. Для поліпшення умов співробітництва, розроблення загальнозрозумілих правил конкуренції на міжнародному ринку створюються об'єднання галузевих органів стандартизації, результатом діяльності яких є регіональні або міжнародні стандарти.

У ІТ-галузі одним із перших був стандарт BSP (Business System Planning), розроблений компанією IBM. На сьогодні ж діє низка стандартів, які регламентують процес розроблення програмних засобів. Серед них слід відзначити: ДСТУ ISO/IEC TR 15271:2008, ДСТУ 3918; ДСТУ 3919-99 (ISO/IEC 14102-95), ДСТУ ISO/IEC 12119:2003, ДСТУ ISO/IEC TR 15504, ДСТУ ISO/IEC 14598, ДСТУ ISO/IEC TR 9126, ДСТУ ISO/IEC 90003:2006, IS0 9001:2000 до програмного забезпечення (ISO/IEC 90003:2004, IDT), ISO/IEC 12207, Guide to the Software Engineering Body of Knowledge (SWEBOK).

Створення технологій на основі стандартів дозволяє реалізувати принцип взаємної відкритості систем, який є найважливішою характеристикою інформаційного суспільства. Технологічно цей принцип вільної взаємодії та властивості відкритих систем називають інтероперабельністю; також цей термін визначено й законодавчо. Вона є однією з головних властивостей відкритих систем і досягається за рахунок використання узгоджених наборів стандартів. Разом з тим, існує проблема реалізації програмних засобів на основі принципу інтероперабельності. Так, в даний час питання приймати на себе зобов'язання використання стандартів або ні, вирішується в добровільному порядку самими організаціями. Для деяких галузей сформувалася ситуація, при якій "добровільність" трактується як необов'язковість виконання будь-яких вимог відповідних стандартів, коли можна на свій розсуд або виходячи з обстановки використовувати стандарти. Проте "добровільність" стандартів в розвинених країнах має не той зміст, який вкладають наші розробники. У західному розумінні "добровільність" розуміється як необхідність і навіть обов'язок постачальника добровільно покладати на себе відповідальність за виконання і навіть перевищення вимог, викладених у добровільних національних або галузевих стандартах на продукцію, процес або послугу. Кожен учасник цивілізованого ринку знає, що без виконання вимог чинних добровільних стандартів, розроблених при безпосередньому добровільну участь постачальників продукції або послуги, неможливі не тільки успішна діяльність, але й саме існування організації.

Згідно з чинним законодавством, добровільно приймаючи стандарт, суб'єкт певної діяльності тим самим демонструє споживачеві безпеку свого виробництва, що дає йому певну перевагу в конкуренції. Відповідно в разі застосування програмного забезпечення і відсутності стандартів, постають актуальні питання щодо відповідальності за шкоду, заподіяну третім особам.

Список використаних джерел

1. *Найбільш відомі стандарти [Електронний ресурс] : [Веб-сайт] – Режим доступу: https://studopedia.com.ua/1_174031_naybilsh-vidomi-standarti.html/ (дата звернення 17.11.2018) – Назва з екрана.*
2. *Технології програмування та створення програмних продуктів: конспект лекцій / укладач О. В. Алексенко. – Суми : СДУ, 2013. – 133 с.*

УДК 004

Іванова О. Т., Сидорова М. Г.
Дніпровський національний університет імені Олеся Гончара

Опанування проблеми управління часом за допомогою інформаційних технологій

Управління часом – сукупність методик оптимальної організації часу для виконання поточних задач, проектів та календарних подій. Головними допоміжними інструментами для управління часом є особистий календар, список поточних завдань та список проектів.

Управління проектами – область знань з планування, організації та управління ресурсами з метою успішного досягнення цілей та завершення завдань проекту. Проект – це обмежений часовими рамками процес, що має визначений початок та кінець, зазвичай обмежений датою, але також може обмежуватися фінансуванням або досягненням результатів, який здійснюється для реалізації унікальних цілей та завдань, зазвичай, щоб призвести до вигідних змін або створення доданої вартості.

Створюючи програмне забезпечення для управління часом та проектами користувача виконувач має розв'язати комплекс завдань, що включає в себе: завдання реалізації механізмів управління часом, завдання розробки бази даних та роботи з даними, завдання створення користувацького інтерфейсу.

Метою роботи було дослідити сучасний стан проблеми управління часом та управління проектами, а також розробити програмне забезпечення для планування, систематизації та контролю виконання задач. Дослідження виявило, що існуючі на даний час програми-органайзери, такі як Lider Task, C-Organizer, AM Notebook, WinOrganizer, CalendarScope та інші мають ряд недоліків: чи то занадто складний інтерфейс, чи відсутність синхронізації з мобільними пристроями. Але майже усі ці програми не розраховані на те, щоб працювати з ними через інтернет. Це не є зручним у наш час, коли інтернет є майже на кожному пристрої.

На першому етапі роботи було вирішено створювати веб-додаток. Логіка веб-додатку розподілена між сервером і клієнтом, зберігання даних здійснюється, переважно, на сервері, обмін інформацією відбувається по мережі. Однією з переваг такого підходу є той факт, що клієнти не залежать від конкретної операційної системи користувача, тому веб-додатки є міжплатформними службами. В якості архітектурного шаблона для програмного забезпечення було обрано шаблон Модель–вигляд–контролер (або Модель–представлення–контролер, англ. Model-view-controller, MVC).

Розроблено програмне забезпечення мовою C# у середовищі Microsoft Visual Studio за допомогою платформи для розробки веб-додатків ASP.NET. Це програмне забезпечення реалізує запропонований архітектурний шаблон та дозволяє вирішувати поставлену задачу.

Алгоритмічну основу створеного програмного додатка склали методики планування задач та організації часу Д. Ейзенхауера, Л. Зайверта, Д. Аллена.

Висновки цієї праці демонструють, що програмне забезпечення зі зручним та зрозумілим інтерфейсом здатне значно покращити продуктивність процесу планування, контролю виконання задач та мотивувати користувача на більш усвідомлене використання власного часу.

УДК 004.04

Константинова А. А., Константинова Л. В.
Центральноукраїнський національний технічний університет

Дослідження засобів для підвищення транзакційної продуктивності MySQL

У міру збільшення розмірів баз даних (БД) розробники постійно шукають шляхи отримання від них все більшої продуктивності. Функціонування БД, яка підтримує транзакції відбувається набагато складніше ніж нетранзакційної БД, в сенсі підтримки ізоляції різних користувацьких сеансів один від одного. Це впливає на продуктивність всієї системи. І тому питання дослідження засобів для підвищення транзакційної продуктивності є актуальним.

В MySQL робота з нетранзакційними таблицями проходить набагато швидше ніж з транзакційними типами таблиць. Навіть якщо потрібно використовувати транзакційні типи таблиць, існує можливість виконувати деякі дії щоб транзації не створювали надмірного навантаження на систему.

Необхідно підтримувати невеликий розмір транзацій. MySQL використовує механізм блокування на рівні рядків, щоб перешкодити паралельним транзакціям модифікувати один і той самий запис в БД і, можливо, пошкодити його. Механізм блокування на рівні рядків не дозволяє більше ніж одній транзакції отримувати одночасний доступ до одного рядку - це захищає дані, проте, що є недоліком, призводить до постановки інших транзакцій на очікування, доки транзакція, яка ініціювала блокування, не завершить свою роботу. При роботі з великою БД, де протікає безліч комплексних транзакцій, довгі періоди очікування, на які буде ставитися велике число транзакцій, які очікують, може значно знизити продуктивність всієї системи.

З цієї причини рекомендується підтримувати розмір транзакцій невеликим, щоб вони швидко вносили свої спади і підйоми і завершувалися, не приводячи до надмірної затримки виконання інших транзакцій, що йдуть слідом за ними.

При переході від ненадійного рівня ізоляції READ UNCOMMITTED до більш безпечного рівня Serializable продуктивність системи керування РБД також буде знижуватися. Причина цьому: чим вище вимоги до цілісності даних, які пред'являються системі, тим більше роботи потрібно виконати і тим повільніше вона буде функціонувати.

Коли встановлений рівень ізоляції SERIALIZABLE, система керування РБД виконує транзакції послідовно і тому забезпечує найвищий рівень захисту даних від пошкодження. Але якщо одним транзакціям доведеться чекати зняття блокувань іншими, це може значно знизити продуктивність додатку. Рівень ізоляції READ UNCOMMITTED дозволяє паралельним транзакціям «бачити» незбережені зміни, які вносяться кожною з них, і це забезпечує набагато вищий рівень продуктивності. Підхід до вибору рівня ізоляції програми не повинен бути стандартним.

Взаємні блокування також впливають на продуктивність при застосуванні транзакцій. Розробники можуть вдаватися до різних хитрощів на рівні додатку, щоб уникнути взаємних блокувань: застосування всіх необхідних блокувань на початку сеансу, обробки таблиць завжди тільки в одній послідовності або впровадження програмно-апаратного коду для забезпечення керування РБД.

Список використаних джерел

1. *Васвани В. MySQL:использование и администрирование. –СПб.:Питер, 2011. - 368с.*
2. *Маненок С. Настройка производительности MySQL [Електронний ресурс]. Режим доступу: http://manenok.pp.ua/tunning-mysql/*

УДК 519.854

Косолап М. В., Михальчук Г. Й.
Дніпровський національний університет імені Олеся Гончара

Програмне забезпечення для розв'язання задачі маршрутизації з різнорідним вантажем

Доставка товарів різного типу передбачає використання різних транспортних засобів. Так, наприклад, доставку молочних продуктів необхідно здійснювати автомобілями-рефрижераторами, а для доставки круп доцільно використовувати транспорт із закритим кузовом з гарною вентиляцією.

Задача побудови маршрутів для доставки різнорідного вантажа (Vehicle Routing Problem for Multiple Product Types – VRPMPT) є одним із різновидів задачі маршрутизації транспортних засобів (Vehicle Routing Problem – VRP) і найчастіше розглядається у сукупності із іншими видами задач VRP [1].

Розглянемо постановку задачі VRPMPT. Задано координати складу та координати клієнтів. З кожним клієнтом асоційований об'єм товару певного типу, який має бути доставлений клієнту. Для обслуговування клієнтів використовується парк транспортних засобів різного типу. Задача маршрутизації полягає у визначенні такої множини маршрутів з мінімальною загальною довжиною, щоб кожен клієнт був відвіданий одним автомобілем відповідного типу тільки один раз; всі маршрути повинні починатися і закінчуватися на складі; кожна одиниця транспорту має обмежену вантажопідйомність.

Для вирішення задачі розроблено двоетапний алгоритм. На першому етапі, для побудови початкового розв'язку, застосовується алгоритм найближчого сусіда. На другому етапі виконується покращення побудованих маршрутів.

Алгоритм побудови маршруту для кожного типу продукції.

1. Якщо всі клієнти, що замовили відповідний тип продукції, обслуговані, переходимо до кроку 6.
2. Обираємо транспортний засіб відповідного типу; додаємо до маршруту склад.
3. Шукаємо клієнта, найближчого до останнього доданого до маршруту елементу.
4. Якщо сумарний обсяг замовлень клієнтів, вже доданих до маршруту, та знайденого клієнта не перевищує вантажопідйомність машини, додаємо його до маршруту та переходимо до кроку 3.
5. Додаємо до маршруту склад та переходимо до кроку 1.
6. Завершуємо роботу алгоритму.

Алгоритм покращення розв'язку.

1. Для кожного побудованого маршруту застосовуємо 2-opt алгоритм.
2. Для кожного типу продукції обираємо підмножину маршрутів, за якими здійснюється доставка цього типу продукції. На отриманій підмножині застосовуємо алгоритм, що покращує розв'язок, якщо це можливо, за рахунок обміну точок між маршрутами.

Розроблено програмне забезпечення, що реалізує запропонований підхід. Програма дозволяє побудувати набір маршрутів та виконувати їх візуалізацію.

Список використаних джерел

1. *Asawarungsaengkul K. A Multi-Size Compartment Vehicle Routing Problem for Multi-Product Distribution: Models and Solution Procedures / Asawarungsaengkul K., Rattanamanee T., Wuttipornpun T. //International Journal of Artificial Intelligence, 2013. – V. 11, P. 237-256.*

УДК 004.8

Майданик О. О.
Центральноукраїнський національний технічний університет

Особливості генетичних алгоритмів

Останнім часом все більше привертають увагу нейронні мережі та генетичні алгоритми. Природа завжди була чудовим джерелом натхнення для всього людства. Генетичні алгоритми - це алгоритми пошуку, засновані на концепціях природного відбору та генетики. Генетичний алгоритм є підмножиною значно більшої гілки обчислень, відомої під назвою Еволюційні обчислення.

Генетичний алгоритм це еволюційний алгоритм пошуку, що використовується для вирішення задач оптимізації і моделювання шляхом послідовного підбору, комбінування і варіації шуканих параметрів з використанням механізмів, що нагадують біологічну еволюцію. Генетичні алгоритми мають здатність одержувати досить добре рішення досить швидко. Це робить генетичні алгоритми привабливими для використання при вирішенні широкого класу задач оптимізації.

В області інформатики існує цілий ряд важкорозв'язних задач. Проблема полягає в тому, що обчислення деяких задач на найпотужніших обчислювальних системах займають дуже довгий час. У такому випадку генетичні алгоритми виявляються ефективним інструментом для забезпечення доступних оптимальних рішень за короткий проміжок часу.

Головною особливістю генетичного алгоритму є акцент на використання оператора «схрещування», який виконує операцію рекомбінації, роль якої аналогічна ролі схрещування в живій природі. Засновником генетичних алгоритмів вважається американський вчений Джон Генрі Холланд, книга якого «Адаптація в природних і штучних системах» є фундаментальною в цій сфері досліджень.

Перші спроби симуляції еволюції були проведені у 1954 році Нільсом Баричеллі на комп'ютері, встановленому в Інституті перспективних досліджень Принстонського університету. Його робота, що була опублікована у тому ж році, привернула увагу громадськості.

Генетичний алгоритм - це в першу чергу еволюційний алгоритм, іншими словами, основною дією алгоритму є схрещування (комбінування). Як нескладно здогадатися, ідеологія алгоритму взята у природи. Отже шляхом перебору і найголовніше відбору виходить правильна комбінація.

Алгоритм можна поділити на три етапи: схрещування, селекція (відбір) та формування нового покоління. Якщо результат не задовільний, ці кроки повторюються до тих пір, поки результат не почне задовольняти кількість поколінь (циклів), які досягнуть заздалегідь обраного максимуму або вичерпають весь час на мутацію.

З ростом дослідницького інтересу кардинально виросла обчислювальна потужність комп'ютерів, що дозволила використовувати нову обчислювальну техніку на практиці. Наприклад у 80-х роках, компанія General Electric почала продаж першого в світі продукту, який працював з використанням генетичного алгоритму. Це були набори промислових обчислювальних засобів. В 1989 році інша компанія Axcelis, Inc. випустила Evolver - перший у світі комерційний продукт на основі генетичного алгоритму для персональних комп'ютерів.

Задача генетичного алгоритму кодується таким чином, щоб її вирішення могло бути представлено у вигляді масиву подібного до інформації складу хромосоми. Цей масив часто називають саме так - хромосома. Випадковим чином в масиві створюється деяка кількість початкових елементів – осіб. Це і є початковою популяцією. Особи оцінюються з використанням функції пристосування, після виконання якої кожній

особі присвоюється певне значення пристосованості. Дана пристосованість визначає можливість виживання особи. Після цього на основі отриманих значень пристосованості вибираються особи, які допущені до схрещування (селекції). До осіб застосовуються «генетичні оператори» (в більшості випадків це оператор схрещування (crossover) і оператор мутації (mutation)). Вони таким чином створюють наступне покоління осіб. Особи наступного покоління також оцінюються застосуванням генетичних операторів і знову виконується селекція та мутація. Так моделюється еволюційний процес, що продовжується декілька життєвих циклів (поколінь), поки не буде виконано критерій зупинки алгоритму.

Перед першим кроком необхідно випадковим чином створити деяку початкову популяцію. Навіть якщо популяція виявиться абсолютно не конкурентоздатною, генетичний алгоритм все одно достатньо швидко переведе її в придатну для життя популяцію. Таким чином, на першому кроці є можливість не старатися зробити надто пристосованих осіб, достатньо, щоб вони відповідали формату осіб популяції, і на них можна було порахувати функцію пристосованості.

На етапі відбору необхідно із всієї популяції вибрати певну долю, яка залишиться в «живих» на даному етапі популяції. Є декілька способів провести відбір популяції. Ймовірність виживання особи повинна залежати від значення її пристосованості. Долю відібраних осіб визначає параметр генетичного алгоритму, і його просто задають заздалегідь.

Розмноження в генетичних алгоритмах зазвичай статеве - щоб «народити» нащадка, необхідно декілька батьків, зазвичай потрібна участь двох. Розмноження в різних алгоритмах описується по різному. Звісно воно залежить від формату осіб. Головна вимога до розмноження, це зробити так, щоб нащадок чи нащадки мали можливість успадкувати риси всіх батьків, «змішавши» їх якимось достатньо розумним чином.

Особи, які підлягають розмноженню зазвичай вибираються із всієї популяції, а не із тих, що вижили на першому кроці (хоча останній варіант теж має право на існування). Головна проблема генетичних алгоритмів - недостатня різноманітність (diversity) в особах. Достатньо швидко виділяється єдиний генотип, який являє собою локальний максимум. Тому згодом всі елементи популяції програють йому у відборі, і вся популяція «забивається» копіями цієї особи. Існують різні способи боротьби із таким небажаним ефектом; один з них - вибір для розмноження не з самих «пристосованих», а взагалі зі всіх осіб.

До мутацій відноситься все те ж, що і до розмноження: є деяка доля мутантів, що є параметром генетичного алгоритму, і на кроці мутацій необхідно вибрати особи які згодом змінять їх заздалегідь заданими операціями мутації.

Висновок: Генетичні алгоритми все більше набувають популярності саме через те, що мають можливість навчатись. Хоч генетичні алгоритми складні в розробці та займають значний час на «навчання», вони в подальшому налагодженому стані працюють значно швидше в порівнянні з іншими алгоритмами (наприклад пошук найкоротшого маршруту). Зараз генетичні алгоритми мають досить широку сферу застосування: для комп'ютерного бачення, в ігрових стратегіях, оптимізації запитів баз даних, розпізнаванні автомобільних номерів, розпізнаванні облич та в задачах з графами.

Список використаних джерел

1.Генетичний алгоритм [електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/ Генетичний_алгоритм
2. Генетический алгоритм. Просто о сложном [електронний ресурс]. – Режим доступу https://habr.com/post/128704/
3. Генетические и эволюционные алгоритмы - современные возможности и перспективы применения [електронний ресурс]. – Режим доступуhttp://neuropro.ru/memo314.shtml

УДК 004.4

Майданик О. О.
Центральноукраїнський національний технічний університет

Важливість оптимізації коду

Всі програми повинні бути правильними, але деякі програми повинні бути швидкими. Наприклад програма обробки відео-фреймів або мережевих пакетів в реальному часі. Для подібних задач продуктивність є головнним фактором. Недостатньо використання ефективних структур даних і алгоритмів. Потрібне написання такого коду, який компілятор легко оптимізує і транслює в швидкий виконуваний код.

Зазвичай компілятори намагаються оптимізувати код. Чим вище рівень оптимізації, тим більш радикальні зміни компілятором вносяться в програму. Компілятори повинні використовувати тільки безпечну оптимізацію. Компілятор може змінювати програму так, щоб це не змінило її поведінку для всіх вхідних даних.

Програмістам, потрібно розуміти, що існують певні характеристики коду, які не дозволяють компілятору виконати оптимізацію. Їх називають “блокувальниками” оптимізації. Є два типи “блокувальників” оптимізації. Одним з них є покажчики. Компілятор не може точно знати, чи будуть два покажчика вказувати на одну і ту ж область пам'яті, і тому не виконує деякі оптимізації. Інший блокувальник оптимізації - виклик функцій. Виклики функцій тягнуть накладні витрати часу, і їх потрібно намагатися уникати.

Зазвичай найінтенсивнішим місцем програми є цикли, особливо самий внутрішній цикл. Саме там і потрібно шукати можливості для оптимізації.

Багато програм часто звертаються до пам'яті для читання або запису. Це займає багато часу. Для найкращого результату слід працювати з регістрами процесора, а не з пам'яттю. Тому як регістри процесора працюють на високій частоті. Для таких програм потрібно шукати можливість ввести тимчасову локальну змінну, в яку проводити запис, і тільки через якийсь час зробити запис з цієї змінної в пам'ять.

Для розуміння як працює програма та як її оптимізувати потрібно розібратися як працює процесор. Сучасні процесори дуже складні та мають в собі багато блоків. Внутрішній устрій процесора називається мікроархітектурою, і це та частина, над якою не має контролю. Коли процесор читає інструкції програми, він розбиває їх на примітиви, зрозумілі йому, і обробляє їх як йому заманеться. Якщо дивитися на команди кода асемблера, то здається, що процесор виконує інструкції послідовно, одна за одною, як вони представлені в коді. Насправді це не так. Процесор може виконувати інструкції паралельно і навіть в протилежному порядку (в залежності від своєї архітектури), якщо впевнений, що це не змінить кінцевий результат. Виконання процесором інструкцій паралельно називається паралелізмом на рівні інструкцій.

Процесор розділений на частини, які виконують різні типи завдань - функціональні блоки. Кожен функціональний блок виконує певний ряд завдань: читання з пам'яті, запис в пам'ять, складання цілих чисел, множення чисел з плаваючою точкою.

Уявіть, що процесору потрібна вибірка даних із пам'яті і це займає 100 тактів. Але процесору буде нерозумно чекати завершення цієї операції, щоб почати наступну. Адже читанням даних з пам'яті займається окремий блок, а інші блоки в цей час можуть виконувати інші обчислення. Тому процесор наперед зчитує кілька наступних інструкцій і навантажує ними всі функціональні блоки, навіть якщо доведеться виконувати інструкції в іншому порядку.

Зчитування інструкцій наперед називається передвибіркою. Якщо під час передвибірки процесор зустрічає конструкцію розгалуження (наприклад if-else), він

намагається вгадати, яка з гілок буде взята і зчитує інструкції звідти. Якщо пізніше він зрозуміє, що була взята хибна гілка, він скидає виконані обчислення, повертається до попереднього стану і йде по іншій гілці. Така помилка коштує процесору декількох втрачених тактів. Для більшості процесорів це приблизно 20 тактів.

На сьогоднішній день процесори працюють за принципом конвеєра. Функціональні блоки процесора які працюють за принципом конвеєра розділяють всю роботу на кілька етапів, і на різних етапах можуть одночасно оброблятися різні інструкції. Незважаючи на те, що виконання однієї інструкції може займати кілька тактів. Більшість блоків можуть приймати в конвеєр нову інструкцію кожен такт. Такі блоки називаються повністю конвеєрними.

Компілятори дуже консервативні, бояться нашкодити і ніколи не вносять зміни в програму, які можуть вплинути на кінцевий результат в якомусь із випадків. Компілятори знають про техніку розкрутки циклу з декількома акумуляторами. Наприклад компілятор GCC застосовує цю техніку, коли запущений з третім рівнем оптимізації або вище. Компілятори будуть використовувати цю оптимізацію для цілих чисел, але ніколи не використають її для чисел з плаваючою крапкою. Справа полягає в асоціативності, тобто в тому, чи впливає порядок, в якому ми складаємо або перемножуємо числа, на кінцевий результат.

Якщо є послідовність цілих чисел, то незважаючи на порядок в якому їх буде складено або перемножено, все одно вийде один і той же результат, навіть якщо буде переповнення. Таким чином операції додавання і множення для цілих чисел є асоціативними операціями. Додавання і множення для чисел з плаваючою крапкою не є асоціативними. Припустимо в послідовності чисел типу float є дуже маленькі числа і дуже великі. Якщо спочатку перемножити дуже маленькі, то вийде нуль. Помноживши всі інші числа на нуль, ми в результаті отримаємо нуль. Якщо ж спочатку дуже маленькі числа множити на дуже великі, в результаті отримається адекватний результат. Для більшості реальних додатків немає різниці в якому порядку виконувати операції над числами, тому можливо використовувати цю техніку оптимізації.

Також слід враховувати те, що існують задачі де без написання гарно оптимізованого коду не обійтись. Наприклад програмування вбудованих систем. Тобто систем які побудовані на основі мікроконтролера (Має в одному чіпі процесор, оперативну та постійну пам’ять, порти вводу виводу, таймери лічильники та іншу перефирію). Як правило в мікроконтролерах досить мало пам’яті та мала тактова частота. Тому оптимізація грає важливу роль в написанні програм для таких платформ. Так як такі платформи зазвичай працюють без операційної системи, то керуюча програма повністю визначає роботу пристрою. На сьогоднішній день перед багатьма пристроями стоїть задача енергоефективності (мобільні телефони, фітнес браслети) тому вкрай потрібна оптимізація керуючої програми.

Висновок. Сучасні процесори приховують величезну обчислювальну потужність. Але щоб отримувати до неї доступ, потрібно писати програми в певному стилі. Вирішити які зіни і до якої частини коду застосувати. Зазвичай аналіз поєднують з експериментом: виконують різні підходи, роблять виміри продуктивності, досліджують код асемблера для виявлення вузьких місць. Для деяких задач оптимізація вкрай необхідна. Тому як від написаної програми залежить ціна використованої платформи та енергоефективність.

Список використаних джерел

1. Оптимізація [електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/ wiki/Оптимізація
2. Оптимизация кода: процессор [електронний ресурс]. – Режим доступу: https://habr.com/post/309796/
3. Трюки и советы по оптимизации Си кода для 8-и разрядных AVR микроконтроллеров [електронний ресурс]. – Режим доступу: http://chipenable.ru/index.php/programming-avr/179-avr4027 -c-code.html

УДК 658:512.011:681.326:519.713
Манченко Я. В.
Харківський національний університет радіоелектроніки

Спеціалізовані програмні засоби діагностики стану користувача глобальної мережі

На сьогодні існує велика кількість різноманітних соціальних мереж, наприклад: Facebook, Twitter, Instagram, VK і т.д. Вони були створені для комунікації та обміну контентом з рідними, друзями так коллегами, але протягом певного часу, та з розвитком мережі Інтернет, соціальні мережі тоже модернізувалися та змінилися. Таким чином, на сьогоднішный день комунікація уже не являється єдиною метою даних мереж. Нарівні зі спілкуванням з друзями, багато людей використовують соціальні мережі для висловлювання будь-якої своєї позиції, призиву людей до різних дій або просто ведуть онлайн щоденник, де описують свої почуття та все, що відбувається навколо. Нажаль, існує дстатньо груп або окремих корстувачів мережі Інтернет, які побуджують людей реагувати на певні речі агресивно та негумано, деякі підштовхують до порушення правопорядку або, навіть, до суїциду.

Як відомо, майже будь-яку інформацію з Інтернета можливо відслідкувати та оцінити. Ідея даної роботи заключається в тому, щоб побудувати оцінку психологічного та емоційного стану людини, активно використовуючого певну соціальну мережу та спргнозувати вірогідність небезпеки даного користувача для суспільства.

Аналіз емоційного стану проводиться по повідомленням користувача за допомогою аналізатора слів бібліотеки AFINN [1]. Дана бібліотека працює наступним чином: вона розпізнає слова, що знаходяться в повідомленні, та присвоює кожному з них оцнку від -5 до 5 в залежності від емоційної нагрузки. Тобто, бібліотека AFINN дозволяє визначити, наскільки позитивно або негативно наповнено повідомлення. При спостереженні та оцінюванні конкретного користувача можливо побудувати графік «емоційної насиченності», на якому буде видно, як з протягм часу змінювалась інформація, яку він розповсюджував, наскільки вона була негативною та небезпечною та спрогнозувати подальші повідомлення.

В роботі, в якості тестової виборки, використовувалася база данних[2], основана на добровільно предоставленній інформації. Після проведення тустування на базі выповняється парсинг інформації з соціальної мережі та запис в власну базу. Далі, користуючись бібліотекою AFINN, маємо якісний аналіз емоційної нагрузки слів по певному користувачу за певний проміжок часу, тобто отримуємо часовій ряд, що містить у собі порівняльні оцінки повідомлень в певний час. Для того, щоб візуаілувати отримані результати, будується графік залежності стану користувача від часу.

Отриманні дані модифуються та класифікуються на декілька групп використовуючи метод дерева рішень[3]. Класифікація створює схожу блок-схему логіку для розподілення нових данних. В кожній точці блок-схеми задається питання про значимсть того чи іншого аттрибуду, і в залежності від цих аттрибутів користувач потрапляє в певній клас, наприклад, він може попасти в клас А (клас людей с високою негативною оцінкою протгом довгого терміну), клас В (група людей с помірною нагрузкою в повідомленнях, но непостоянним графіком «емоційної насиченност», що свідотствує про перемінливий настрій) або в клас С (люди с високим позитивним показником повідомлень).

Класифікатор використовує дуже класифікованні данні інших користувачів, та на їх основі розподіляє нових користувачів. При розподіленні на класи метод дерева рішень учитує враховуэ такі показнки як кількість позитивных повідомлень, кількість негативних повідомлень, порівняльну оцінку настрою, загальну забарвленність повідомлень та частоту повідомлень.

Список використаних джерел

1. *AFINN [Електронний ресурс] – Режим доступу: http://www2.imm.dtu.dk/pubdb/views/publication_details.php?id=6010*
2. *[Електронний ресурс] – Режим доступу: https://www.kaggle.com/cjroth/chronist*
3. *Методы классификации и прогнозирования [Електронний ресурс] – Режим доступу: http://www.intuit.ru/studies/courses/6/6/lecture/174*

УДК 004.4

Мішевський Г. А., Кузнєцов Д. І.
ДВНЗ «Криворізький національний університет»

Методи та засоби оптимізації пошуку медіа файлів у хмарних сховищах на основі використання Android додатку

На сьогоднішній день однією з головних тенденцій сучасного світу є стрімко зростаюча кількість даних, які люди використовують в різних сферах діяльності. Разом із цим гостро постає питання в раціональному зберіганні цієї інформації. Найбільше ця проблема стосується саме мобільних пристроїв, розмір пам'яті в яких є відносно малим для потреб сучасного користувача. Звісно потрібно розуміти, що існують різноманітні комплектації з довільною кількістю пам'яті і до того ж є можливість її розширення з допомогою SD-карт чи різних зовнішніх носіїв інформації. Але не слід забувати про економічний фактор, адже не кожний зможе собі дозволити такий мобільний пристрій.

Для вирішення цієї проблеми досить добре підходить використання так званих хмарних обчислень – це технологія, яка надає можливість віддаленого використання різноманітних ресурсів. ЇЇ перевагами є відносно невисока ціна, обслуговування апаратної та програмної на стороні сервера, автоматичне оновлення, час розгортання зведений до мінімуму, доступ до ресурсу з будь-якого місця, де є підключення до мережі інтернет. До недоліків можна віднести наступне: відсутність локальної бази даних, що унеможливлює роботу без підключення то мережі інтернет, відсутність фізичного доступу до даних, постачальники хмарного сервісу можуть припинити надавати послуги, завжди є шанс, що нова компанія може вийти з бізнесу або скасувати обслуговування, а також можливі проблеми з надійністю зберігання даних, оскільки від хакерських атак ніхто не застрахований. Незважаючи на ці недоліки дана технологія є досить популярною в наш час і постійно розвивається.

У хмарних обчисленнях виділяють три основні види сервісних моделей.

До першого з них відносяться SaaS (Soft as a Service*)* – програмне забезпечення як послуга, оренда ПЗ через інформаційну мережу. Це повнофункціональний додаток для користувача, що виконує певні функції — наприклад роботу з зображеннями та звуком. *SaaS* є однією з перспективних технологій, що дозволяє підприємствам знизити витрати на IT. Постачальник послуги SaaS надає програмне забезпечення в тимчасове користування. Воно встановлюється, як правило, на сервері цього постачальника послуг. Користувач отримує доступ до сервера в основному через мережу Інтернет, застосовуючи відповідний інтерфейс прикладних програм (Application Program Interface, API).

Моделлю другого типу є PaaS (Platform as a Service) - оренда по мережі середовища розробки і виконання додатків. Дана платформа надає більш високий рівень сервісу, що дає можливість розробляти, тестувати і впроваджувати різні програми. Вона дозволяє розгортати додатки за допомогою Інтернету без витрат на придбання та оновлення програмного забезпечення, на придбання, розгортання, обслуговування різних пристроїв і на управління ними. Платформа PaaS може включати найрізноманітніші інструменти: розробки додатків, їх тестування, розгортання та хостингу; інтеграції з веб-службами і з базами даних; забезпечення безпеки, масштабованості, зберігання.

До моделі третього типу відноситься IaaS (Infrastructure as a Service) - оренда по мережі інфраструктури підприємства, віртуальних апаратних обчислювальних засобів, програмного забезпечення, інформаційної мережі. Зазвичай IaaS надає уніфіковані апаратні і програмні ресурси. Інфраструктура як послуга - це базовий рівень хмарних обчислень і включає засоби зберігання, обчислень, резервування, відновлення після збоїв, роботи з базами даних і забезпечення безпеки, що надаються постачальником інфраструктури. Споживач не керує фізичною та віртуальною інфраструктурою, що лежить в основі хмари, проте він контролює операційні системи, системи збереження, встановлені програми та, можливо, має обмежений контроль над деякими мережевими компонентами (наприклад, мережевими екранами вузлів).

Серед методів та засобів пошуку файлів можна виділити деякі основні, такі як: лінійний пошук, алгоритм ділення навпіл(двійковий алгоритм), пошук по "дереву Фібоначе", метод екстраполяції тощо. Важливо розуміти, що немає поганого алгоритму, кожний із них потрібно застосовувати в залежності від конкретної ситуації та зважаючи на деякі фактори. Потрібно звертати увагу на те, чи масив даних сортированій, на розмір масиву, на технічні характеристика ЕОМ на якій проводяться розрахунки. Так, наприклад зрозуміло, що бінарний алгоритм швидше лінійного, але якщо масив не сортированій то не має ніякого сенсу у його використанні, або якщо масив має малий розмір то використання метода екстраполяції теж не має сенсу, адже він показує значний приріст продуктивності тільки при великих розмірах, тому в цьому випадку доцільно використати бінарний алгоритм чи йому подібні [4].

Висновки. Проаналізувавши зазначені вище моделі хмарних обчислень був зроблений висновок, що якнайкраще для реалізації даного додатку підходе саме модель SaaS**.** Оскільки відомо, що масив буде сортированій, та відносно великих розмірів то одним із найбільш перспективних алгоритмів пошуку із представлених вище є метод екстраполяції. Даний метод характеризується тим, що на відміну від бінарного та йому подібних алгоритмів, він не лише визначає зону нового пошуку, а і оцінює величину кроку. І при великих об’ємах має значно більшу швидкість сходження. Звісно слід розуміти, що це не кінцеве рішення і в ході реалізації проекту воно може змінюватися, в залежності від потреб додатку.

Список використаних джерел

1. *Облачные вычисления, краткий обзор[Електронний ресурс]// habr.com – Режим доступу до ресурсу: https://habr.com/post/111274/*
2. *What is cloud computing? [Електронний ресурс]// azure.microsoft.com– Режим доступу до ресурсу: https://azure.microsoft.com/en-in/overview/what-is-cloud-computing/*
3. *What is SaaS? The modern way to run software [Електронний ресурс]// www.infoworld.com – Режим доступу до ресурсу: https://www.infoworld.com/article/3226386/saas/what-is-saas-the-modern-way-to-run-software.html*
4. *Searching Algorithms [Електронний ресурс]// www.geeksforgeeks.org – Режим доступу до ресурсу: https://www.geeksforgeeks.org/searching-algorithms*
5. *Infrastructure as a Service (IaaS) [Електронний ресурс]// www.service-architecture.com – Режим доступу до ресурсу: https://www.service-architecture.com/articles/cloud-computing/infrastructure_as_a_service_iaas.html*
6. *Что такое PaaS? [Електронний ресурс]// azure.microsoft.com– Режим доступу до ресурсу: https://azure.microsoft.com/ru-ru/overview/what-is-paas/*

УДК 004.05

Пархоменко Д. О.
Центральноукраїнський національний технічний університет

Концептуальні засади забезпечення якості програмних продуктів

Бурхливий і динамічний розвиток інформаційних технологій супроводжується активною розробкою й впровадженням відповідних програмних засобів (ПЗ), що дозволило автоматизувати практично всі сфери діяльності людини. Водночас і першочергово постає питання забезпечення якості програмних засобів.

Під якістю ПЗ варто розуміти його характеристику, ступінь відповідності встановленим вимогам. При цьому вимоги можуть трактуватись по-різному, що породжує декілька незалежних визначень терміну. Тож, якістю ПЗ є набір властивостей програмного продукту, що характеризують його здатність задовольнити встановлені або передбачувані потреби замовника. Слід зазначити, що поняття якості має різні інтерпретації залежно від конкретної програмної системи і вимог до неї.

У сфері якості програмного забезпечення одним з найбільш важливих можна вважати стандарт ISO/IEC 9126. У ньому окреслено п’ять найбільш загальних факторів якості ПЗ: функціональність, надійність, ефективність, наявність зручного супроводу, здатність до транспортації до інших систем, програмного оточення. Перші відображають вимоги до функціонування програмного продукту. Для кількісного встановлення критеріїв якості, за якими буде здійснюватися перевірка і підтвердження відповідності ПЗ заданим вимогам, визначаються відповідні зовнішні вимірювані властивості (зовнішні атрибути) ПЗ, метрики (наприклад, час виконання окремих компонентів), діапазони зміни значень і моделі їх оцінки. Метрики застосовуються на стадії тестування або функціонування й називають зовнішніми метриками. Разом з тим вони є моделями оцінки атрибутів.

Внутрішні характеристики якості і внутрішні атрибути ПЗ використовуються для складання плану досягнення необхідних зовнішніх характеристик якості продукту. Для квантифікації внутрішніх характеристик якості застосовують внутрішні метрики, як інструмент перевірки відповідності проміжних продуктів внутрішнім вимогам до якості, які формулюються на процесах, що передують тестуванню. Зовнішні і внутрішні характеристики якості відображають властивості ПЗ, а також погляд замовника і розробника на таке ПЗ. Безпосереднього кінцевого користувача ПЗ цікавить експлуатаційна якість ПЗ – сукупний ефект від досягнення характеристик якості, що виміряється строком результату, а не властивістю самого ПЗ. Це поняття ширше, ніж будь-яка окрема характеристика (наприклад, зручність використання або надійність).

Таким чином, аналіз якості є діяльністю, що включає процеси управління, інфраструктуру програмної інженерії, тестування, інженерію вимог. Характеристики якості визначають споживчі властивості і мають вартісний вираз, що включає оцінку витрат на процес розробки та експлуатації, оцінку економічних вигод застосування вказаних програм порівняно з іншими засобами вирішення відповідного прикладного завдання, а також перспектив подальшого використання даного програмного забезпечення в умовах зміни середовища функціонування.

Список використаних джерел

1. *Шишкіна М. П. Якість програмних засобів навчального призначення: підходи до визначення предмету / М. П. Шишкіна // Науковий часопис Національного педагогічного університету імені М. П. Драгоманова. – 2010. – Вип. 22. – С. 553-556.*
2. *Бойко Л. Аналіз якості програмного забезпечення [Електронний ресурс] : [Веб-сайт] / Леся Бойко // Матеріали XVIII Міжнародної науково-практичної інтернет-конференції “Проблеми та перспективи розвитку науки на початку третього тисячоліття у країнах СНД”, 29–30 грудня 2013 р., Переяслав-Хмельницький. – Режим доступу: http://oldconf.neasmo.org.ua/node/430. – Назва з екрана.*

УДК 004.05

Патиковський Ю. В.
Центральноукраїнський національний технічний університет

Структурно-функціональні особливості оцінки якості програмних засобів критичного призначення

Однією з актуальних задач програмної інженерії є забезпечення необхідного рівня якості програмних засобів (ПЗ). Її розв'язок є особливо важливим для ПЗ критичного призначення, застосування якого пов'язане з безпекою життєдіяльності. Тому перед допуском такого ПЗ до експлуатації передбачена обов'язкова процедура його сертифікації, що полягає в перевірці відповідності фактичних показників якості ПЗ їх нормативним значенням. Для побудови моделі якості необхідно проаналізувати, узгодити й формалізувати вимоги до програмного засобу зі сторони розробника, замовника та рекомендацій чинних стандартів якості.

Під ПЗ критичного застосування в роботі розуміється ПЗ, що виконує критичні функції, важливі для безпеки; тобто ПЗ, відмова у виконанні функцій якого чи його неправильна або недбала експлуатація можуть призвести до катастрофічних або критичних наслідків. До основних методів оцінювання показників якості програмних засобів відносять інспекції, тестування, статичний аналіз, імовірнісна оцінка надійності, аналіз видів, наслідків і критичності відмов програмного забезпечення, аналіз дерева відмов програмного забезпечення. Разом з тим, основною серією стандартів, що висуває загальні вимоги до ПЗ, є ISO/IEC 9126. Сукупність характеристик якості ПЗ, що визначена стандартом ISO/IEC 9126-1, складає повну модель і визначає приблизно тридцять характеристик та підхарактеристик. Базовими показниками якості вважаються ті, що безпосередньо відбивають якість функціонування ПЗ у зв'язку з її призначенням. Базові показники якості характеризують ступінь виконання переліку функцій відповідно галузевим вимогам до ПЗ критичних систем цільового призначення.

З визначеної у [2] дефініції якості програмного забезпечення (сукупність властивостей ПЗ, які обумовлюють його придатність задовольняти певні потреби відповідно до призначення), а також понять валідації, верифікації, відмови, дефекту, ЖЦ, надійності, показників (характеристик) якості, помилки тощо випливає висновок про те, що для критичного ПЗ на відміну від прикладного визначено особливі вимоги щодо перевірки якості програмних засобів, які розробляються, яка повинна включати функціональне і структурне тестування. Настановою [2] чітко регламентовано методи і дії, які слід виконувати під час реалізації перевірок. Серед них – статичний аналіз ПЗ, ймовірнісна оцінка надійності ПЗ, аналіз видів, наслідків і критичності відмов програмного забезпечення (SFMECA) та аналіз дерева відмов ПЗ (SFTA). При цьому слід зазначити, що немає загальних критеріїв критичності, які застосовуються до ПЗ. Адже це поняття пов'язане із серйозністю наслідків та імовірністю їхнього виникнення.

Отже, структурно-функціональний склад оцінки якості програмних засобів критичного призначення є таким же, як і у прикладного ПЗ. Разом з тим, перевірки якості критичного ПЗ є більш глибоким, строго регламентованим і, відповідно, потребує значно більше ресурсів, ніж прикладне. Це, зокрема, пов'язано необхідністю реалізації різних видів тестування ПЗ критичного призначення.

Список використаних джерел

1. *Райчев І. Е. Проблеми оцінювання якості критичних програмних систем при їх сертифікації / І. Е. Райчев, О. Г. Харченко // Проблеми програмування. – 2004. – № 2, 3. – С. 198-207.*
2. *Галузева система управління якістю. Методи оцінки показників якості програмного забезпечення програмно-технічних комплексів критичного призначення : настанова Національного космічного агентства України [Електронний ресурс]. – НКАУ. – Режим доступу: http://www.nkau.gov.ua/nkau/SOU-NSAU%200031.doc (дата звернення 17.11.2018).*

УДК 004.4:004.75:004.455(043.2)

Петренко А. Б., Колпаков М. О.
Національний авіаційний університет

Інтеграція хмарних сховищ Amazon S3 у веб-додатки розроблені засобами мови програмування Java

Сучасні компанії, повинні вміти просто і безпечно збирати, зберігати і аналізувати дані у великих масштабах відповідно до директив ЕС і FISMA. Amazon S3 – це об'єктне сховище, призначене для зберігання та видалення даних з наступних джерел: веб-сайтів, мобільних та корпоративних додатків. Дані в класах сховища Amazon S3 автоматично розподіляються як мінімум по трьом фізичним зонам доступності, які зазвичай рознесені одна від одної на кілька кілометрів в рамках регіону AWS, при цьому вони можуть автоматично копіюватись в будь-який інший регіон AWS, що забезпечує високий рівень надійності зберігання. Amazon S3 підтримує три різні типи шифрування та пропонує високотехнологічну інтеграцію з AWS CloudTrail для реєстрації, моніторингу та збереження викликів API сховища з метою аудиту. Amazon S3 підтримує стандарти безпеки і сертифікати відповідності, включаючи PCI DSS, HIPAA/HITECH, FedRAMP.

Основним завданням роботи є інтеграція Amazon S3 хмарного сховища до існуючого програмного забезпечення розробленого засобами мови програмування Java. Мета роботи – розширити функціональні можливості існуючого програмного додатку та посилити рівень безпеки даних відповідно до міжнародних стандартів PCI DSS, HIPAA/HITECH, FedRAMP засобами Amazon SDK.

Першим кроком для інтеграції хмарних сховищ Amazon S3 в Java-додаток є включення бібліотек Amazon SDK. Для цього скористаємося фреймворком для збірки проектів Maven та підключимо в pom.xml (рис. 1) файл нашого проекту офіційну залежність представлену розробниками Amazon.

```
<dependency>
    <groupId>com.amazonaws</groupId>
    <artifactId>aws-java-sdk-s3</artifactId>
    <version>1.11.235</version>
</dependency>
```

Рисунок 1 – Підключення бібліотеки Amazon SDK.

Далі необхідно внести дані, що будуть використовуватися при підключенні та автентифікації до сховища. Одним із підходів для цього є створення окремого конфігураційного файлу, що буде містити необхідні дані у формі ключ-значення. Ключ – ідентифікатор вмісту, що використовується в програмі отримання необхідної інформації. Значення ідентифікатора представлене у формі змінної середовища (рис. 2) за для забезпечення конфіденційності цих даних.

application-s3.properties

```
1  jsa.aws.access_key_id=${AWS_ID}
2  jsa.aws.secret_access_key=${AWS_KEY}
3  jsa.s3.bucket=${AWS_BUCKET}
4  jsa.s3.region=${AWS_REGION}
```

Рисунок 2 – Конфігураційний файл для доступу до Amazon S3 сховища.

Після закінчення підготовчого етапу перейдемо безпосередньо до розгляду базових функціональних можливостей Amazon S3 SDK та її імплементації на Java. Процедура загрузки файлів (рис. 3), з локальної системи на віддалені сервера представлена:

- клас ObjectMetadata – зберігає метадані файлу, для успішного зберігання та відновлення файлу;
- клас PutObjectRequest – інкапсулює http запит методом put до віддаленого серверу;
- клас TransferManager – відповідає за передачу даних на віддалені сервери.

```
ObjectMetadata objectMetadata = new ObjectMetadata();
objectMetadata.setContentLength(bytes.length);
InputStream inputStream = new ByteArrayInputStream(bytes);

Upload upload = transferManager.upload(new PutObjectRequest(
        bucketName,
        id,
        inputStream,
        objectMetadata));
```

Рисунок 3 – Приклад реалізації методу загрузки файлу на віддалений сервер.

```
S3Object object = s3client.getObject(bucketName, id);
if(object != null){
    try {
        byte[] fileByteArray = IOUtils.toByteArray(object.getObjectContent());
        return fileByteArray;
    } catch (IOException e) {
        throw new S3Exception();
    }
```

Рисунок 4 – Приклад реалізації методу скачування файлу з віддаленого серверу.

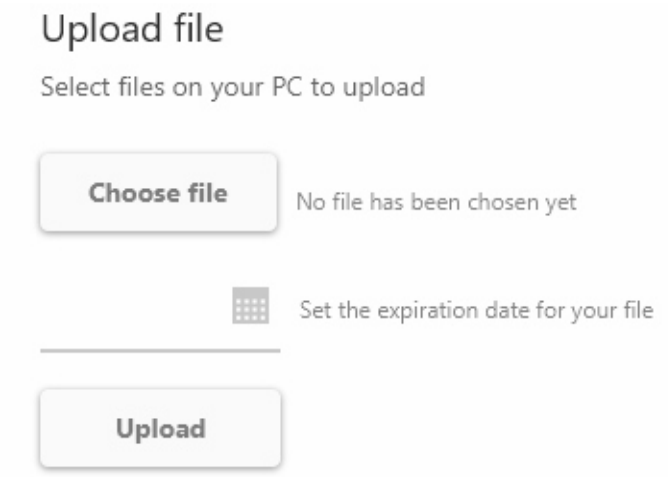


Рисунок 5 – Реалізації графічного інтерфейс.

Процес загрузки об’єктів до локальної файлової системи наступний. Необхідно скористатися класом AmazonS3, що інкапсулює в собі клієнт доступу до сховища (рис. 4). В якості аргументів методу використовуються ім’я корзини в якій знаходиться файл та його ідентифікатор.

Продемонструємо результат працездатності коду, для цього необхідно створити графічний інтерфейс і прив’язати метод загрузки файлів до одного з компонентів. Скористуємося бібліотекою розробки десктопних додатків JavaFX (рис. 5).

В результаті виконання програми відбудеться трансфер файлу з локальної файлової системи до віддаленого серверу Amazon S3 сховища. Amazon Web Services надає можливість керування файлами через веб-додаток, що відображаються у виглядів списку. Система дозволяє перегляд метаданих, групування в папки, скачування або загрузку об’єктів для авторизованих користувачів та шифрування (рис. 6).

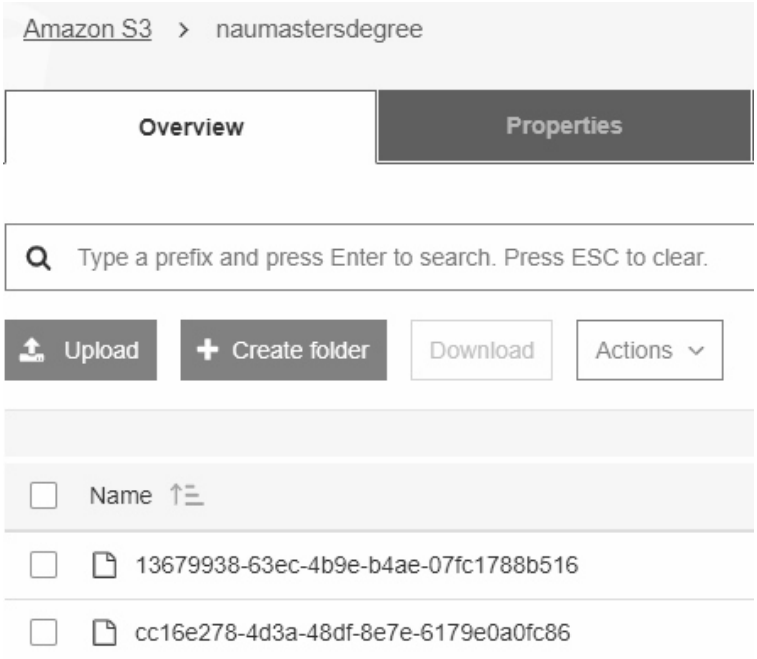


Рисунок 6 – Amazon S3 сховище.

Інтеграція хмарного сховища Amazon S3 дозволить підвищити рівень безпеки, доступності та цілісності даних програмного продукту відповідно до стандартів безпеки PCI DSS, HIPAA/HITECH, FedRAMP. Значною мірою зростуть можливості по обробці інформації внутрішніми аналітичними інструментами веб-сервісу. Результатом роботи є ефективне посилення рівня захисту даних при зберіганні та обробці, значне розширення функціональних можливостей при мінімальних ресурсних витратах.

Список використаних джерел

1. *Офіційний сайт Amazon web-services. [Електронний ресурс]. – Режим доступу: https://aws.amazon.com*
2. *Інформаційний навчальний портал Baeldung. [Електронний ресурс]. – Режим доступу: https://www.baeldung.com/aws-s3-java*
3. *Офіційна документація Amazon SDK [Електронний ресурс]. – https://docs.aws.amazon.com/AWSJavaSDK*

УДК 004.02; 004.415.2

Петренко Д. О.
Харківський національний університет радіоелектроніки

Аналіз методів та розробка прототипу програмної системи для моніторінгу технічного стану автомобіля

Автомобіль є невід'ємною частиною життя населення у світі. В розвинутих країнах рівень автомобілізації населення коливається від 600 до 900 автомобілей на 1000 людей [1]. При цьому з автомобілями пов'язано багато складностей — цей вид транспортау складно назвати надійним. ДТП є малою долею пригод, пов'язаних з даним видом транспорту, також існують такі як: зломи, критичні технічні несправності та інше.

Розглядаючи дану тему варто проаналізувати аналоги в цій сфері. Серед методів моніторингу технічного стану слід зазначити основні: мануальний та автоматичний. Мануальний метод це зовнішній огляд деталей, та технічних складовин автомобіля. Автоматичний – з викроистання датчиків та сенсорів. Слід зазначити, що на сьогоднішній день існує дуже мало універсальних та новітніх систем які використовують автоматичні методи моніторингу технічного стану автомобіля, крім застарілих діагностичних центрів. Однак, існують автоматизовані системи, частково покривають необхідний функціонал: сигналізація зі зворотним зв'язком, яка сповіщає про злом автомобіля на обмеженій відстані; бортовий комп'ютер, який відстежує технічний стан автомобіля, але має обмежений функціонал, пов'язаний з повідомленнями і загальним доступом до інформації.

Концепція Internet of Things дозволяє робити моніторинг практично будь-якого об'єкта, відстежувати і керувати ним, а також включати інформацію про ці об'єкти в загальний «цифрову всесвіт». Залучення в IoT предметів фізичного світу, не обов'язково оснащених засобами підключення до мереж передачі даних, вимагає застосування технологій ідентифікації цих предметів. В якості таких технологій можуть використовуватися всі засоби, що застосовуються для автоматичної ідентифікації: оптично розпізнавані ідентифікатори (штрих-коди, Data Matrix, QR-коди), засоби визначення місцезнаходження в режимі реального часу [2].

Для вирішення сучасних проблем в автомобільній індустрії, запропонований прототип системи, який дозволяє відстежити необхідні події, що відбуваються з транспортним засобом – з використанням IoT сенсорів таких як: датчик руху, наповненості, температури, протікання, тиску та інші – в режимі реального часу. Сенсори розташовані в ключових областях автомобіля і відстежують технічні несправності, зовнішні і внутрішні пошкодження. Датчики можуть відловити основні проблеми, що виникають з автомобілем, наприклад: витік палива, перегрів двигуна, тиск в шинах, а також більш серйозні як аварія, злом. На певні типи подій користувач зможе включити віправлення повідомлень на мобільний пристрій, щоб найшвидше знати про зміни в технісному стані автомобіля.. Реалізація даного прототипу значно розширить набір стандартних можливостей, пов'язаних з управлінням технічним станом транспортного засобу, завдяки використанню сучасних IoT сенсорів.

Список використаних джерел

1. *Рейтинг стран мира по уровню автомобилизации. Гуманитарная энциклопедия [Электронный ресурс] // Центр гуманитарных технологий, 2006–2016 Режим доступа:* http://gtmarket.ru/ratings/passenger-cars-per-inhabitants/info
2. *Тихвинский В.О. Сети IoT/M2M: технологии, архитектура и приложения. [Текст]/ Тихвинский В.О. – М.: Издательство: «Медиа паблишер», 2015. – 287 с.*

УДК 004.274

Половинка О. Л.
Донецький національний технічний університет

Використання паралельної реалізації для пошуку асоціацій

В умовах постійного розвитку технологій, відбувається процес накопичення дуже великих масивів даних. Однак, без попередньої обробки і подальшого аналізу вони не можуть бути корисними. Вибір методів та алгоритмів обробки даних великих обсягів є актуальним завданням.

Мета роботи: обґрунтувати необхідність використання паралельних алгоритмів пошуку асоціативних правил для вирішення задач обробки даних великих обсягів.

Потужним інструментом, що використовується для первинного аналізу даних, є пошук асоціацій. Суть методу полягає в находженні зафіксованої в базі, але раніше невідомої взаємозалежної інформації. Найбільш поширеним та ефективним алгоритмом в цій області є Apriori. Існують лінійна і паралельні реалізації алгоритму.

Недоліками лінійної реалізації алгоритму Apriori, в разі аналізу великого обсягу даних, є багаторазовий перегляд (сканування) вихідного набору даних і велике число отриманих варіантів. Той же недолік відзначається і при дуже низькій підтримці. [1] Таким чином, алгоритм ефективний тільки для малих наборів даних, або при високому рівні мінімальної підтримки. Однак, в рамках розв'язуваної задачі маємо значні обсяги накопиченої неструктурованої інформації, що зберігається в розподіленої базі даних. Тому застосування алгоритму лінійної структури є недоцільним.

Для поліпшення характеристик та підвищення ефективності алгоритму для великих обсягів даних, використовуються його паралельні модифікації, спрямовані на зменшення числа переглядів вхідного набору і зменшення числа отриманих варіантів (згенерованих кандидатів). Існує велика кількість паралельних алгоритмів, заснованих на Apriori. Їх різноманітність пояснюється можливістю використання методу в рішенні багатьох завдань, різними способами з використанням різних критеріїв розпаралелювання і підходів до пошуку асоціативних правил.

Існують наступні підходи до розпаралелювання алгоритму пошуку асоціативних правил: 1. Поділ бази даних на однакові горизонтальні блоки і дублювання кандидатів на кожному з процесорів; 2. Поділ кандидатів і поділ бази даних; 3. Оцінка непересічних множин кандидатів і вибіркове дублювання або спільне використання бази даних.

Для вирішення завдання паралельного пошуку асоціативних правил для великих обсягів даних пропонується обрати одну з найбільш поширених платформ паралельного програмування Hadoop, яку активно використовують для інтелектуального аналізу даних. Застосування Hadoop обумовлює необхідність переробки застарілих алгоритмів і перетворення їх в алгоритми MapReduce. Основним завданнями, при реалізації алгоритму Apriori на каркасі MapReduce, є створення двох незалежних функцій Map і Reduce і перетворення даних у пари ключ - значення. При програмуванні MapReduce всі перетворення на різних машинах виконуються паралельно, але остаточний результат виходить лише після завершення reduce. Якщо алгоритм рекурсивний, то для отримання остаточного результату виконується кілька фаз Map/Reduce.

В ході дослідження проведені експерименти застосування паралельної реалізації алгоритму Apriori з використанням технології Map/Reduce для двох наборів даних з різними характеристиками. Перший масив включає порівняно невеликий набір транзакцій з великою кількістю елементів в кожній з них. Другий - навпаки, складався з великої кількості транзакцій, з порівняно невеликим набором елементів. За результатами експериментів було виявлено, що обраний механізм є актуальним лише для першого набору даних. При його використанні процес обробки працює приблизно в 1,4 рази швидше. Для другого масиву застосування паралельного алгоритму в обраному виді не мало значних результатів.

Список використаних джерел

1. *Кириченко Д.О. Оптимизация входных данных в задаче поиска шаблонов и ассоциативных правил / Д. О. Кириченко, М. А. Артемов // Вестник ВГУ, серия Системный анализ и информационные технологии. – Воронеж, 2014. - №4. – С.63-70.*
2. *Parallel data mining for association rules on shared-memory multiprocessors. / M.J. Zaki, M. Ogihara, S. Parthasarathy, W. Li. 1996. 29 p.*
3. *Review of Apriori Based Algorithms on MapReduce Framework / S. Singh, R. Garg and P. K. Mishra // International Conference on Communication and Computing (ICC - 2014), Bangalore, India, 2014, pp. 593–604.*

УДК 004.05+004.41:331.103.226
Ткаченко О. С.
Центральноукраїнський національний технічний університет

Аналітична оцінка трудомісткості процесів реалізації програмних засобів

Ключовим фактором при оцінюванні програмних засобів є якість. Але, звичайно, щоб досягнути високої якості програмного продукту, треба на ранніх стадіях (процесах) його створення оцінювати трудомісткість виконавців ІТ-проекту, тобто, говорячи математичною мовою, відношення одиниці праці до одиниці виконаної технологічної операції, в даному випадку програмного забезпечення, виконання тих чи інших завдань, пов'язаних із створенням, подальшим тестуванням і реалізацією створеного програмного засобу (ПЗ).

Спираючись на чинний міжнародний стандарт ISO/IEC 12207, сьомим розділом якого регламентуються процеси життєвого циклу ПЗ, процес реалізації програмних засобів складається з таких підпроцесі: процес реалізації програмних засобів, процес аналізу вимог до програмних засобів, процес проектування архітектури програмних засобів, процес детального проектування програмних засобів, процес конструювання програмних засобів, процес комплексування програмних засобів, процес кваліфікованого тестування програмних засобів.

Аналізуючи подані у [1] мету й необхідні дії для виконання певного процесу, випливає аналітичний висновок, що найбільш трудомістким є процес аналізу вимог до ПЗ, адже саме на цьому етапі розробки формується майбутній напрям розроблення, грамотний рівномірний розподіл виробничих ресурсів на всіх процесах та формується хід і порядок виконань виконавцями наступних кроків. І в більшому від правильності та коректності аналізу виконавцем умов до ПЗ залежить і подальший успіх розробки.

За результатами дослідження менш трудомісткими, порівняно з первинним, є процеси проектування архітектури та детального проектування. Під час означених процесів формується проект певних програмних частин і взаємозв'язок між ними. Ще меншу трудомісткість мають процеси конструювання та комплексування ПЗ: розроблення програмного продукту, спираючись на вимоги, критерії й проекти з попередніх етапів ЖЦ ПЗ. І найменше трудомісткості з поміж інших вимагає процес кваліфікованого тестування, адже його завдання – перевірка відповідність створеного ПЗ до вимог, описаних виконавцем у процесі аналізу вимог до програмного засобу.

Отримані аналітичні дані можна використовувати під час розподілення задач між членам команди ІТ-проекту задля отримання найбільшої корисності від кожного виконавця. Разом з тим, звичайно, високо в ІТ-сфері цінується і кваліфікація, так звана "якість" виконавців. Адже можна доручити певний процес одному кваліфікованому виконавцю, ніж двом-трьом менш кваліфікованих, адже "кількість не означає якість". Таким чином можна отримати вільну робочу силу, з можливістю її подальшого використання у виробничому процесі.

Отже, з результатів аналітичного дослідження випливає: 1) з'ясовано, що найбільш трудомістким процесом реалізації ПЗ є процес аналізу вимог до майбутнього програмного забезпечення, який вимагає найбільш високого рівня інтелекту та кваліфікованості осіб, яким буде доручений цей етап (процес) ЖЦ ПЗ; 2) визначено шкалу трудомісткості процесів реалізації програмних засовів, які розміщуються у тому самому порядку, у якому вони подані в стандарті ISO 12207; 3) задля досягання ефективності та найбільшого коефіцієнта корисної праці кожного виконавця ІТ-проекту треба раціонально розподіляти робочу силу між етапами розробки ПЗ.

Список використаних джерел

1. ISO/IEC 12207 : 2008. Systems and software engineering – Software life cycle processes. – [Second edition - 2008-02-01]. – ISO/IEC-IEEE, 2008. – 122 p. – (International Standard).

УДК 004.083

Фесечко Д. В.
Центральноукраїнський національний технічний університет

Принципи роботи з великими даними

В квітні 2017 року компанія International Data Corporation (IDC) підготовила доповідь “The Data Age 2025”. У ньому компанія зробила прогнози, що до 2025 року загальносвітовий обсяг збережених даних досягне 163 зеттабайт. Для порівняння у 2016 році ця цифра становила 16 зеттабайт - таким чином, ми отримаємо практично десятикратний приріст обсягу збереженої інформації.

В документах IDC і Seagate говориться, що створення і використання життєво важливих даних, а також управління ними буде в рівній мірі значимо для підтримки нормальної повсякденної діяльності як споживачів, так і комерційних підприємств, і держструктур. Кількість споживачів і підприємств, що створюють і обмінюються даними між будь-якими пристроями і хмарними сховищами, буде збільшуватися і набуде колосальних масштабів.

Зараз все більше інженерів намагаються покращити технології, для можливості зберігання більшої кількості інформації. Найшвидше розвивається технологія "трілемма магнітного запису". Це коли збільшення щільності запису передбачає зниження фізичних обсягів магнітного домена - ділянки пластини, в якому зберігається 1 біт інформації. Проблема полягає в тому, що чим менше розміри магнітного домена, тим швидше відбувається його розмагнічування, при цьому збережена інформація спотворюється або може бути зовсім втрачена внаслідок теплового руху елементарних частинок.

Поява HAMR здавалася вирішенням проблеми, але вона не змогла виправдати очікування. Термоасистований магнітний запис (HAMR) — гібридна технологія запису інформації, що комбінує магнітне читання і магнітооптичний запис. Принцип роботи пристроїв, що використовують цю технологію, полягає в локальному нагріві лазером магнітних пластин до 450 ° C, що дозволяє тимчасово знизити напруженість магнітного поля і, як наслідок, зменшити площу, необхідну для запису 1 біта інформації. У процесі розробки технології інженери зіткнулися з проблемою: виявилося, що сфокусувати лазерний промінь на ділянці менш 50 нм технічно неможливо.

В результаті систему HAMR довелося значно ускладнити. В останніх зразках накопичувачів, які використовують принцип термомагнітного запису, лазер не опромінює магнітну пластину безпосередньо: теплова енергія передається через оптичний перетворювач ближнього поля, головним компонентом якого є плазмонова антена, виконана із золота. Ускладнення конструкції друкарської головки в поєднанні з використанням золота призвело до істотного зростання собівартості виробництва. Крім того, в ході випробувань було встановлено, що плазмонова антена швидко деформується під дією високих температур і не відповідає сучасним галузевим стандартам надійності.

У тому ж році компанія Western Digital представила в світ HDD об’ємом 14 ТБ. Але ці технології існують вже досить давно і 14 ТБ - практично граничне значення обсягу для HDD без істотного збільшення товщини. Але у Western Digital вже готове рішення, яке дозволить створювати в кілька разів більш ємні накопичувачі.

Компанія представила технологію мікрохвильового магнітного запису (MAMR), яка, за розрахунками WD, дозволить створювати HDD об’ємом до 40 ТБ. Такі

накопичувачі компанія обіцяє до 2025 року, ну а перші моделі нового покоління, розраховані на використання в датах-центрах, вийдуть вже в 2019 році.

В основу технології MAMR ліг спінтронний осцилятор, який представляє собою багатошаровий тонкоплівковий генератор високочастотного (20-40 ГГц) поля, що виникає за рахунок поляризації спінів електронів під дією постійного струму. Генератор здійснює "накачування" магнітного домена, за рахунок чого вдається істотно знизити енергетичні витрати, необхідні для зміни вектора намагніченості ділянки записуючого шару на протилежний.

У поєднанні із застосуванням дамаського процесу виготовлення записуючих головок, здатного забезпечити точний контроль форми і розмірів полюса, а також завдяки використанню багатоступінчастого мікропроводу, вдалося підвищити щільність запису - аж до 4 Тбіт на квадратний дюйм. У перспективі це дозволить створювати 3.5-дюймові HDD ємністю до 40 ТБ, тобто, що перевершують сучасні моделі за обсягом практично в чотири рази! Причому перехід на MAMR ніяк не відбивається на надійності накопичувача, так як спінтронний осцилятор не залежить від екстремальних температур.

Ще однією важливою перевагою MAMR є повна сумісність з технологією HelioSeal, яка конфліктує з HAMR. Оскільки теплопровідність гелію більша, ніж повітря, газове середовище буде досить швидко нагріватися в процесі запису, а значить тиск всередині самого диска зросте. Слідом за нею зросте і сила опору обертанню магнітних пластин, тобто, для розкрутки шпинделя буде потрібно більш потужний привід. У свою чергу, через те, що самі пристрої стануть більш гарячими, збільшаться і витрати на охолодження дата-центрів, що робить масове використання термомагнітних накопичувачів ще більш сумнівним. У випадку з MAMR подібних проблем не виникає: перехід на нові диски не зажадає від власників дата-центрів модернізації системи охолодження і ніяк не відіб'ється на рахунках за електрику.

Незважаючи на всю інноваційність, для більшості користувачів, на даний момент, це не має особливого сенсу, адже навіть зараз, через шість років після появи перших HDD об'ємом 4 ТБ, такі накопичувачі практично не користуються попитом у звичайних споживачів, не кажучи вже про більш об'ємні моделі. Так що HDD з технологією MAMR здебільшого будуть використовуватися в центрах обробки даних та інших подібних структурах. Але вже зараз розвиваються відео в форматі 4K і комп'ютерні ігри вагою від 100 ГБ і вище наприклад (Final Fantasy - 148 Гб, Call of Duty: Black Ops 3 – 113 Гб, Quantum Break – 178 Гб), таке бурхливе зростання пов'язане з підвищеним інтересом з боку бізнесу. Існують також перспективні напрямки, як машинне навчання і системи інтернет речей: мільярди пристроїв щомиті генерують величезну кількість інформації, а нейромережі вимагають все більше відомостей для аналізу і обробки. Можна зробити висновок, що зараз всі вище згадані технології розвиваються і являються ще недосконалими. Інженери і далі будуть працювати, та вдосконалювати технології для зберігання великих об'ємів інформації. Зараз же вони не є такими важливими для звичайних користувачів, але є перспективним напрямком для великих компаній, яким потрібно зберігати і обробляти великі обсяги даних.

Список використаних джерел

1. *Перспективная технология магнитной записи MAMR [Електронний ресурс]. – Режим доступу:http://ale.betting-box.com/company/wd/blog/429278/*
2. *Технология WD MAMR [Електронний ресурс]. – Режим доступу: https://www.ixbt.com/news/2017/10/13/wd-mamr-hdd-40.html*

УДК 004.386

Фролова М. С., Співак Р. В.
Університет митної справи та фінансів

Застосування технології доповненої реальності та 3d-моделювання для попередження надзвичайних ситуацій

При взаємодії людини з комп'ютером використовується інтерфейс, який повинен забезпечити користувачеві комфортну роботу з програмною системою, але іноді при вирішенні певного кола завдань (наприклад - тривимірне моделювання об'єктів) виникає проблема недостатньої наочності, яка викликана складністю виконуваних робіт. Існуючі інтерфейси недостатньо повно вирішують цю задачу. Одним із шляхів вирішення проблеми людино-машинного взаємодії є використання технології доповненої реальності.

Технологія доповненої реальності є перспективним засобом для створення призначених для користувача інтерфейсів мобільних додатків, тому що ця технологія дозволяє сприймати інформацію про становище і орієнтації об'єктів на інтуїтивному рівні [1]. За рахунок накладення додаткової інформації на зображення реального світу технологія доповненої реальності реалізує принципово новий тип інтерфейсу, який може реагувати на навколишнє середовище.

На початку 2000-х років велися розробки мобільних систем доповненої реальності – Mobile Augmented Reality System (MARS). Така система складалася з акумуляторної батареї, що носиться ЕОМ, модуля геолокації, камери і очок стереобачення [2]. Передбачалося, що MARS-системи будуть визначати місцезнаходження користувача за допомогою модуля геолокації і на основі цього отримувати актуальну для користувача інформацію, наприклад про розташованих поблизу будівлях.

В даний час технології досягли такого рівня розвитку, що більшість сучасних смартфонів оснащені GPS/ГЛОНАСС-модулями геолокації і камерами достатньою роздільною здібності, щоб використовувати їх для побудови призначених для користувача інтерфейсів з технологією доповненої реальності - Augmented Reality User Interface (ARUI). Використання смартфонів як апаратної платформи для ARUI-систем дозволить суттєво скоротити вартість розробки подібних систем, так як не доведеться розробляти вже існуючу апаратну частина.

Тому, використання доповненої реальності у різних сферах стало актуальним, особливо якщо вони допомагають виявити, попередити та застерегти від надзвичайних ситуаціях, наприклад на об’єктах підвищеної небезпеки, до яких відноситься значна кількість підприємств України. Згідно закону України «Про об’єкти підвищеної небезпеки» об’єкт підвищеної небезпеки – об’єкт на якому використовуються, виготовляються, переробляються, зберігаються або транспортуються одна або кілька небезпечних речовин чи категорій речовин у кількості, що дорівнює або перевищує нормативно встановлені порогові маси, а також інші об’єкти як такі, що відповідно до закону є реальною загрозою виникнення надзвичайної ситуації техногенного та природного характеру [3].

Складовою частиною розроблюваної системи є розробка підсистеми розпізнавання образів. В основі даної підсистеми лежить принцип визначення і відстеження окремих «реперних» ділянок (сегментів) зображення навколишнього світу, які мають певну характеристику. Після виділення реперних точок необхідно порівняти їх з виділеними раніше точками, щоб відстежити зміну положення точок на зображенні навколишнього світу. Далі на основі цієї інформації визначається зміна положення спостерігача в просторі. На рис. 1 наведена блок-схема основного алгоритму розроблюваної підсистеми.

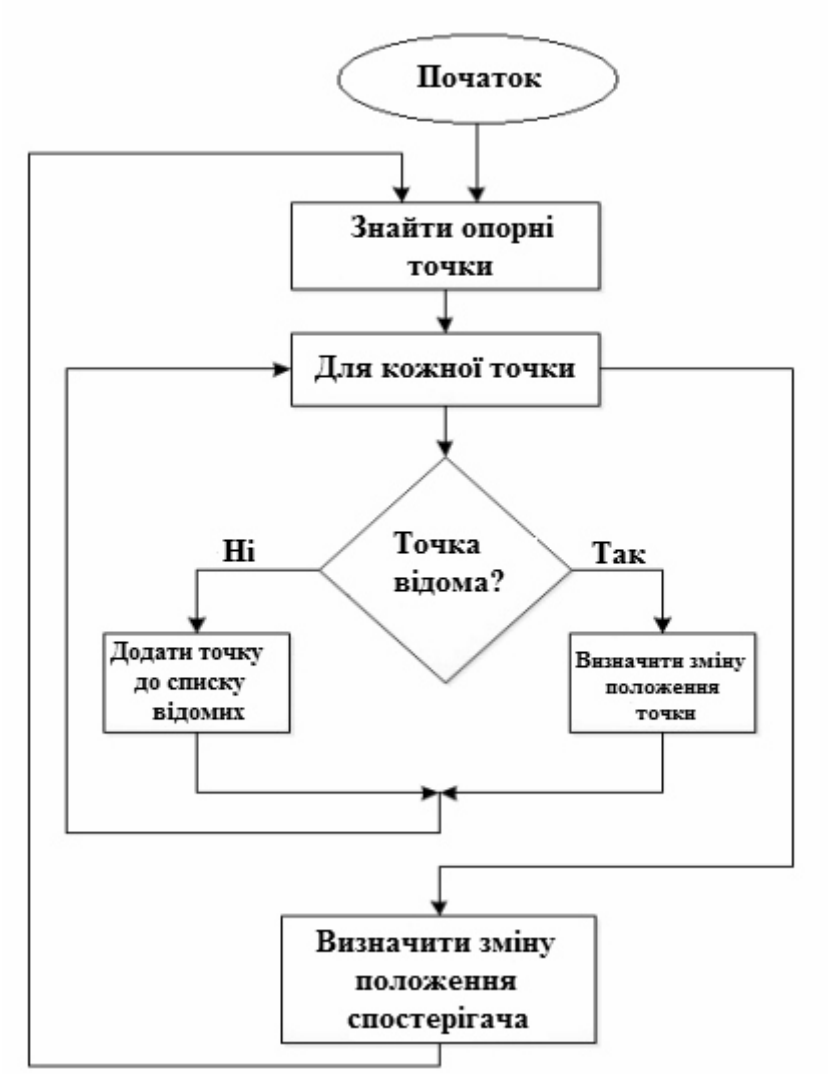


Рисунок 1 – Блок-схема алгоритму

Під характеристикою сегмента зображення розуміється функція $F(\bar{s})$, де $\bar{s}$- растр сегмента зображення. Сегменти зображення з характеристикою вище порогового значення F_0 вважаються особливими «реперними» точками.

Після розрахунку змін положення особливих точок на зображенні необхідно розрахувати зміну положення спостерігача в просторі. Застосування технології доповненої реальності при розробці програмних систем дозволяє створювати принципово нові інтерфейси, які можуть взаємодіяти з навколишнім світом, а доступність і повсюдне використання необхідного аппаратного забезпечення дозволяють використовувати технології доповненої реальності практично кожною людиною.

Список використаних джерел

1. *Schmalstieg D. The World as a User Interface: Augmented Reality for Ubiquitous Computing // Location Based Services and TeleCartography. – 2007. – Vol. 4. – P. 369–391.*
2. *Hollerer T. User Interface Management Techniques for Collaborative Mobile Augmented Reality // Computers & Graphics. – 2001. – Vol. 5, № 26. – P. 799–810.*
3. *Zakon Ukrainy «Pro ob'ekty pidvyshcenoi nebezpeky» vid 18.01.2001 №2245-III // Vidomosti verhovnoi rady Ukrainy.- 2001.- №15.- st. 73.*

УДК 004.023

Черніков Д. Д., Конопліцька-Слободенюк О. К.
Центральноукраїнський національний технічний університет

Проблема 2038 - 32bit systems

Проблема 2038 року в обчислювальній техніці - очікувані збої в програмному забезпеченні, напередодні 19 січня 2038 року. В сучасних обчислювальних системах, в тому числі в найпоширеніших на перше десятиліття XXI століття комп'ютери під управлінням операційних систем Microsoft Windows, Apple Mac OS / iOS і Unix-подібних OS (Linux, Fedora, BSD, etc.), використовується фон-Неймановская архітектура і мова Сі.

У числі бібліотек останнього є заголовки , в якому певні змінні відліку часу time_t типу signed int (стандартне ціле число зі знаком, в 32-бітних і 64-бітних системах еквівалентно 32 бітам), в яку при її ініціалізації (при виконанні програм) записується число секунд, що пройшли з моменту початку, після чого змінна починає збільшуватися на 1 після кожного тика мікропроцесора, що подає сигнали з частотою 1 Гц (1 коливання / тик в секунду). Апаратно-програмне забезпечення, виконавши зміщення дати від початку «епохи Unix», видасть дату 20:45:52, 13 грудня 1901 роки (GMT / GDT / UTC) і (по ідеї) буде вважати час від цієї дати до півночі на 1 січня 1970 року, коли відбудеться обнулення (породивши в результаті закільцьованості). Більшість систем (провідні візуальний облік часу з 1 січня 1970 роки) видадуть на такий результат помилку.

Річ у тім що людство вже стикалось с подібною проблемою у 2000 роках. Проблема 2000 року - проблема яка з'явилася тому що, розробники XX ст. використовували два знака у даті, наприклад, 1 січня 1951 року в таких програмах уявлялося як «01.01.51». Деякі обчислювальні машини мали вже апаратну обробку дати, проте дві цифри від 0 до 9 (тобто замість 4 цифр »1951" зберігалися і оброблялися тільки 2 цифри "51". Але тоді проблема 2000 року виглядала не більше як засіб на якому можливо було заробити методом страху світових компаній, а зараз ця проблема реальна.

З проблемою 2038 року вже зіткнувся Google на своєму сервісі YouTube. А саме з роликом співака PSY - Opa Gangnam Style. Коли кількість його переглядів сягнула 2 147 483 647, лічильник просто перестав працювати. Програмістам Google довелося його переписувати. Полагодили з великим доробком - тепер допустима кількість переглядів становить 9 223 372 036 854 775 808 (більше 9 трильйонів).

Автомобільні системи - ще одна велика проблемна область. Багато різних систем піддадуться збоям в 2038 році. Проблеми з файлами - крім того, формат 32-розрядного формату time_t також включається в специфікації формату файлів, наприклад формат універсального розповсюдження ZIP архіву. Формат файлу може існувати протягом періоду, який зміниться багатьма поколіннями комп'ютерів, що означає, що проблема 2038 залишається актуальною. Насправді, рішення полягає в тому, що протягом 23 років багато 32-бітові системи застаріють і будуть підлягати заміні. На зміну їм прийдуть ті, яким не потрібно виправлення.

Найбільшим головним болем, мабуть, стане модернізація обладнання, наприклад, на енергетичних об'єктах. Але якщо планувати цю роботу заздалегідь, то можна уникнути великих проблем. Одне можна сказати точно: у людства достатньо часу, щоб розібратися з цим питанням.

Список використаних джерел

1.Проблема 2038 [електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/Проблема_2038_года.

2. Блог компанії PVS-Studio [електронний ресурс]. – Режим доступу: https://habr.com/company/pvs-studio/blog/328054/.

УДК 004.853

Бабич Є. Ю.
Центральноукраїнський національний технічний університет

Небезпека штучного інтелекту

Аналізуючи сучасний світ, можна стверджувати, що надзвичайний розвиток ІТ-технологій призводить до заміни людей роботами. Штучний інтелект (ШІ), що оперує машинами, здатний до організації автоматичних систем, обирати та приймати оптимальні рішення на основі раніше отриманого життєвого досвіду та аналізу зовнішніх впливів. Головними особливостями ШІ є здатність до навчання, накопичення досвіду, узагальнення інформації.

ШІ вражає своїми досягненнями кожного дня. Наприклад, голосовий пошук Siri і Alexa є відомим прикладом досягнення ШІ. Також відеоігри, тобто персонажі в них, які грають на рівні зі справжніми гравцями. Автономні автомобілі, які можуть навчити водити машину, точно так як і людину. Вражаюче досягнення - ШІ компанії Google, який обіграв найкращу програму гри в шахи Stockfish 8, не програвши жодної партії зі 100. Розробники AlphaGo Zero створили алгоритми правил гри в шахи, а ШІ сам вдосконалив себе за добу, граючи сам із собою і здобув навички майстра в шахи.

В Саудівські Аравії робот Софія зі ШІ вже отримала паспорт і громадянство. Вона може відтворювати близько 60 емоцій, дає інтерв'ю журналістам, щодо банківської сфери. Машини зі ШІ допомагають людині у роботі, а пізніше й можуть повністю замінити її. Планується, що на виробництві будуть працювати роботи зі ШІ, але творчу роботу роботи замінити не зможуть.

Вчений-астролог Влад Росс вважає, що машини будуть виконувати всю людську роботу, а люди завойовуватимуть простір. Цей варіант був би найкращий для людства. Але, цей процес не настільки досконалий, адже машини постійно мають збої в програмах. Наприклад, у Вашингтоні робот-поліцейський, що мав збій у програмі, відмовився виконувати свою роботу і потонув у фонтані. А на технологічній виставці бот Little Chubby вийшов з-під контролю та розбив скляний стенд. У компанії Facebook зупинили ШІ, коли робот Боб та Еліс, які повинні були бути онлайн-підтримкою для користувачів, створили власну мову і спілкувалася тільки нею. Стівен Хокінг та Ілон Маск стверджують, що необхідно зупинити та обмежити деякі експерименти зі ШІ, тому що вони можуть бути великою загрозою для людей. Маск говорить, що ШІ страшніше, ніж автомобільні аварії та авіакатастрофи, небезпечніші, ніж Північна Корея. Слова Хокінга також не оптимістичні. Він вважає головну небезпеку штучного інтелекту в тому, що він буде куди більш компетентний, ніж люди, оскільки до його послуг буде вся інформація світу, при цьому ШІ не буде обмежений особливостями людського сприйняття, емоціями, та моралі. Також можливою проблемою може бути безробіття, яка неминуче виникне, коли людей почнуть замінювати роботи.

Немає підстав не брати до уваги погляди світових авторитетів у сферах застосування ШІ. Загальний підхід полягає в тому, що без використання систем ШІ технологічний прогрес не може вдосконалюватись, і розвиток інтелектуальних машин має продовжуватися. Але, головною проблемою є не створення ефективних систем ШІ, а створення нових підходів системи управління, в першу чергу етичного характеру. Тому безпека ШІ повинна бути пріоритетом в його розробці.

Список використаних джерел

1. *Лахман Константин. Стоит ли бояться искусственного интеллекта? – Режим доступа : http://polit.ru/article/2012/12/16/ai_fears*
2. *Сценарий терминатора. Опасен ли искусственный интеллект. – Режим доступу : http://nv.ua/publications/ predosteregli-ob-opasnostyah-iskusstvennogo-intellekta.html*

УДК 004.38

Берладін В. К., Гермак В. С.
Центральноукраїнський національний технічний університет

Штучний інтелект у сучасному світі

Від SIRI до самохідних машин, штучний інтелект (AI) розвивається дуже швидкими темпами. Наукова фантастика часто зображує AI як роботів з людськими характеристиками, AI охоплює широку область застосування - від алгоритмів пошуку Google до Watson IBM для автономної зброї.

Термін інтелект (intelligence) походить від латинського intellectus - що означає свідомість, розум. Відповідно, штучний інтелект - ШІ (AI), як правило, розуміють як властивість автоматичних систем брати на себе окремі функції інтелекту людини, наприклад, вибрати і прийняти оптимальні рішення на основі отриманого досвіду та раціонального аналізу зовнішніх впливів.

Комп'ютерні системи на базі AI набагато швидше людей обробляють дані, мають практично моментальний доступ до великого масиву даних, не мають схильності відволікатись на сторонні речі. У багатьох виникають асоціації з SkyNet і Термінатором. Втім, між казкою та реальним світом завжди є різниця. На відміну від людей вони не здатні ставити собі завдання.

Штучний інтелект який створений на сьогодні називається вузьким AI (або слабким AI), оскільки він призначений для виконання вузькоспеціалізованих завдань (наприклад, лише для розпізнавання обличчя або лише для пошуку в Інтернеті або лише для керування автомобілем). Проте довгострокова мета багатьох розробників полягає у створенні загального AI (AGI або сильного AI). Не зважаючи на те, що вузький AI вже може перевершувати людину в конкретному завданні, наприклад, краще грати в шахи чи вирішувати рівняння, AGI у свою чергу перевершить людей у виконанні майже кожного завдання.

Безумовно, сучасним AI під силу поки тільки окремі вузькоспеціалізовані області застосування, хоча слід зазначити, справляються вони з ними вже набагато краще самих людей. Яскравим прикладом такого може стати Deep Blue, який переміг чемпіона світу з шахів Гаррі Каспарова.

Але вже зараз можна з упевненістю сказати, що штучний інтелект на сьогодні існує не тільки для розваги, але і застосовується на практиці в дуже багатьох сферах людського життя.

Відомі голосові помічники Siri від Apple і GoogleAssistant, сервіс пошуку за зображеннями в браузері Google Chrome - це AI. Останнім часом штучний інтелект почав набирати обертів в сучасній медицині, зокрема для діагностики захворювань, а також для прогнозування ризиків страхової діяльності та в торгах на біржі для банків. Зовсім недавно, на початку 2018 року, Facebook заявив про використання штучного інтелекту для визначення суїцидальних намірів користувачів соцмережі та надання їм невідкладної допомоги, а відома пивоварна компанія Carlsberg - навіть для створення нових сортів пива. Також невід'ємною частиною і сферою використання AI є військовий сектор. Зокрема в системах ППО для розпізнавання цілей в умовах активних перешкод.

У довгостроковій перспективі важливим питанням є те, що станеться, якщо розробка сильного AI досягне успіху, і система AI стане кращою за людей у будь-якому аспекті. Існує ризик, що система штучного інтелекту зможе рекурсивно самовдосконалюватись, викликавши інтелектуальний бум, що залишить людський інтелект далеко позаду. Винаходячи революційні нові технології, такий суперінтелект може допомогти нам закінчити війни, знайти ліки від відомих хвороб та викорінити

бідність як таку, а тому створення сильного AI може стати визначною подією в історії людства. Деякі експерти висловлюють занепокоєння, що це також може бути останнім досягненням людства, якщо ми не навчимося узгоджувати цілі AI з нашими, перш ніж він стане суперінтелектуальним.

Більшість дослідників згодні з тим, що суперінтелект навряд чи проявить людські емоції, такі як любов чи ненависть, і що немає підстав очікувати, що ШІ стане навмисно добрим або поганим. У той же час штучний інтелект може стати джерелом небезпеки, експерти вважають, що існують два найбільш вірогідні сценарії такого розвитку подій:

1. Штучний інтелект запрограмують на те, щоб зробити щось руйнівне: автономна зброя - це системи штучного інтелекту, які запрограмовані на вбивство. В руках не тієї людини ця зброя може легко привести до великої кількості жертв. Більш того, гонка озброєнь штучних інтелектів може ненавмисно привести до війни між ними, яка також призведе до масових жертв. Цей ризик присутній навіть вже при вузькому штучному інтелекті, але зростає в міру збільшення рівня інтелекту.

2. Штучний інтелект може бути запрограмований на те, щоб зробити щось корисне, але він вирішить досягти мети особливим шляхом. Це може статися, коли ми не зможемо повністю узгодити цілі штучного інтелекту з нашими. Наприклад якщо ви попросите інтелектуальну машину відвезти вас в аеропорт якомога швидше, це може перерости в прегони, які загрожуватимуть вашому здоров'ю, а можливо навіть життю. Машина буде буквально виконувати те, що ви просили, не аналізуючи, чи саме цього ви хотіли чи ні, і чи не зашкодить вам таке буквальне виконання вказівки. Якщо супер-інтелектуальній системі доручити амбітний проект геоінженерії, його реалізація може завдати шкоди нашій екосистемі побічними ефектами, а спроби людей зупинити її вона сприйматиме як загрозу для виконання завдання.

З самого початку штучний інтелект піддавався перевірці як з боку вчених, так і громадськості. Однією з поширених теорій є ідея, що машини стануть настільки високо розвиненими, що люди не зможуть йти в ногу з ними, і тоді штучний інтелект почне стрімко і безконтрольно розвиватись, прогресуючи з експоненціальною швидкістю. Інший варіант розвитку подій полягає в тому, що машини можуть вторгнутись в особистий, конфіденційний простір людей і навіть озброїтись. Інші дослідники обговорюють етику штучного інтелекту, а саме чи слід інтелектуальні системи, такі як роботи, наділяти такими самими правами, як і людей.

Я вважаю, що створення повноцінного робота, який вміє відчувати, мислити інтуїтивно, проявляти свої емоції дуже потрібно людству. Але якщо людина не може до кінця розпізнати свою природу, свої можливості, то навряд чи вона створить щось подібне собі або те, що перевершує її саму по якихось параметрах. У той же час виникають побоювання, якщо дозволити «розумній» машині приймати самостійні рішення, то неможливо знати заздалегідь, які це будуть рішення, і немає впевненості, що ці рішення будуть спрямовані на благо людини. Тому машина, знову таки теоретично, буде виконувати завдання відповідно до своїх суджень, навіть якщо ви цього не хочете. Насамкінець можна відзначити, що питання про створення ідеального штучного інтелекту, який не відрізнятиметься від людини, ще довго не буде закрите.

Список використаних джерел

1. Тимофеев А. В. Роботы и искусственный интеллект. – М., 1978.
2. Тьюринг А. Может ли машина мыслить. – М., 1960.
3. Балабанов О. Комп'ютерний інтелект: можливості і реальність //Вісник Національної Академії наук України. - 1997. - № 9-10. - С. 16-21.
4. Эндрю А. Искусственный интеллект. - Пер. с англ. - М., 1985.
5. Мельник А. Искусственный интеллект: фантазии и реальность/ А.Мельник //PC WORLD UKRAINE. - 1999. - № 11-12. - С. 99-101.

УДК 004.4

Боярський Д. О.
ДВНЗ «Криворізький національний університет»

Генерація дизайну сайтів на основі використання згорткових генеративних змагальних мереж глибокого навчання

Популярність використання штучних нейронних мереж зростає з кожним роком. Окрім класичних прикладів сфер застосування нейронних мереж, таких як розпізнавання та класифікація зображень, вони також успішно застосовуються у бізнесі, наприклад: медицині, фінансах, комерції, транспорті, промисловості, сфері розваг та мистецтва, безпеці, тощо.

Згорткові генеративні змагальні мережі глибокого навчання (Deep Convolutional Generative Adverserial Networks, DCGAN) - це архітектура глибокого навчання нейронних мереж без вчителя, яка генерує дані, аналогічні даним з навчальної вибірки. DCGAN складається з двох нейронних мереж, які називаються генератором та дискримінатором. Генератор, виходячи із назви, генерує зображення, а дискримінатор, який навчався на певних зображеннях намагається знайти невідповідність тому, що він знає.

Наприклад, якщо генерується зображення банкноти, то на ній обов'язково повинен бути номінал. В тому випадку, коли дискримінатор не знаходить на створеному зображені номінал, то він повідомляє, що це не справжня банкнота. З часом дискримінатор все ліпше виявляє фальшиві зображення, а генератор створює їх все більш досконалими. Оскільки ці дві нейронні мережі мають різні цілі, між ними виникає гра з нульовою сумою – гра з двома гравцями, які мають протилежні інтереси (теорія ігор).

Схему роботи DCGAN можна представити наступним чином:

1. Генератор обирає вектор випадкового шуму і генерує зображення;
2. Зображення віддається дискримінатору, він порівнює її з навчальною вибіркою;
3. Дискримінатор повертає число 0 (фальшивка) або 1 (справжнє зображення).

Хоча на даний момент, звичайна людина в більшості випадків може зрозуміти, що згенероване зображення є несправжнім, але все одно цей підхід вражає своєю перспективою застосування у різних сферах діяльності людини. І це не якісь можливі перспективи, а реальність. Facebook вже використовує DCGAN у своїх цілях [1].

Висновки. Наразі штучні нейронні мережі змінюють цілі галузі, стаючи невід'ємною частиною нашого повсякденного життя. Якщо у подальшому, вони зможуть створювати дизайн ліпше, ніж фахівці цієї галузі, то не слід вважати, що вони витіснять живих людей. Скоріш за все, нейронні мережі будуть дуже гарним інструментом та помічником, які допоможуть спеціалістам поліпшити їх роботу. Також можливість тонкого налаштування безлічі параметрів при генерації дизайну для сайтів, без сумніву показує перспективність використання цього рішення в майбутньому.

Список використаних джерел

1. *Коли комп'ютери будуть мати здоровий глузд? [Електронний ресурс] // scientificamerican.com – 2016. – Режим доступу до ресурсу: https://www.scientificamerican.com/article/when-will-computers-have-common-sense-ask-facebook/*

УДК 004.8

Власюк І. В., Сухомлин А. А.
Черкаський державний технологічний університет

Нейронні мережі з розподіленою обробкою даних

Основною задачею нейронних мереж є вирішення проблем, що не можуть бути точно сформульовані, а також дослідження та генерування множини рішень, що здатні максимально охоплювати проблематику заданої теми. Для відходження від серії послідовних логічних обрахунків в бік наближення їх до реальних нейробіологічних процесів для нейромережі необхідно реалізувати можливість працювати з необроблюваними нейросистемою раніше або невідомими для системи типами даних, враховуючи чужий та власний досвід. Слід зазначити, що на даному етапі розвитку комп'ютерної техніки доречно ставити питання про наближення до порогу комфортного вивчення та дослідження нейронних мереж, а також побудованого на їх основі штучного інтелекту, внаслідок чого однією з актуальних задач є підвищення швидкодії та можливість організації паралельної роботи над декількома незалежними процесами обробки даних. В цьому контексті доцільно розглядати аспекти розподіленої обробки даних, а також цілком логічним є введення в фокус розгляду поняття розподіленої нейронної мережі.

Розподілена нейронна мережа представлена сукупністю логічно взаємозв'язаних нейросистем, розподілених всередині комп'ютерної мережі, в якій для забезпечення контролю, одночасного зв'язку та цілісності частин системи використовується ядро, що використовує точну логіку управління усіма ланками нейромережі. В результаті виникає ілюзія цілісності системи та підвищення швидкості обробки даних внаслідок розпаралелювання їх обробки. Ядро також є основним постачальником даних.

Слід відзначити наступні етапи побудови розподілених нейромереж: створюється ядро для керування ланками системи, кластери Hadoop та розподілена файлова система NDFS, гібридна нейросистема, використовуючи логічний, еволюційний та імітаційний підходи до побудови нейромереж, проводиться навчання нейросистеми, комбінуючи самонавчання та навчання з учителем, за необхідністю або наявності вільних ресурсів мережа розширюється.

Побудована за такою методикою нейронна мережа надасть ряд переваг порівняно із класичною методикою побудови. Відзначимо деякі з них: можливість працювати із різними типами даних, можливість прямої та непрямої постановки задачі, паралельна обробка даних за допомогою моделі MapReduce, можливість розширення обсягу файлової системи та підвищення потужності обчислювальної системи без виконання додаткових маніпуляцій. Передбачена можливість залучення досвіду сторонніх нейронних мереж для вирішення поставлених задач.

Окремо слід відзначити, що після впровадження розподіленої обробки даних з'являться інструменти для роботи з неструктурованими базами даних, такими як NoSQL та відносну нечутливість нейросистеми до відключення одного чи декількох кластерів.

Список використаних джерел

1. *Мак-Каллок У. С., Питтс В. Логическое исчисление идей, относящихся к нервной активності Архивная копия от 27 ноября 2007 на Wayback Machine // Автоматы / Под ред. К. Э. Шеннона и Дж. Маккарти. — М.: Изд-во иностр. лит., 1956. (Перевод английской статьи 1943 г.)*
2. *Галушкин А. И. Синтез многослойных систем распознавания образов. — М.: Энергия, 1974.*
3. *Барцев С. И., Охонин В. А. Адаптивные сети обработки информации. — Красноярск: Ин-т физики СО АН СССР, 1986. Препринт N59Б.*
4. *Калацкая Л. В., Новиков В. А., Садов В. С. Организация и обучение искусственных нейронных сетей: Экспериментальное учеб. пособие. — Минск: Изд-во БГУ, 2003.*
5. *Чернодуб А. Н., Дзюба Д. А. Обзор методов нейроуправления // Проблемы программирования. — 2011. — No 2.*
6. *Гальберштам Н. М., Баскин И. И., Палюлин В. А., Зефиров Н. С. Нейронные сети как метод поиска зависимостей структура — свойство органических соединений // Успехи химии. — 2003. — Т. 72, № 7.*
7. *Миркес Е. М. Логически прозрачные нейронные сети и производство явных знаний из данных // Нейроинформатика / А. Н. Горбань, В. Л. Дунин-Барковский, А. Н. Кирдин и др. — Новосибирск: Наука, 1998.*
8. *Elmasri and Navathe, Fundamentals of database systems (3rd edition), Addison-Wesley Longman, ISBN 0-201-54263-3*
9. *M. T. Ozsu and P. Valduriez, Principles of Distributed Databases (2nd edition), Prentice-Hall, ISBN 0-13-659707-6*
10. *O'Brien, J. & Marakas, G.M.(2008) Management Information Systems. New York, NY: McGraw-Hill Irwin.*

УДК 004.8

Гіцеларь Д. В.[*]
Центральноукраїнський національний технічний університет

Штучний інтелект та його залежність від відеоігор

Штучний інтелект в іграх не є нещодавньою інновацією. Ще в 1949 році математик і криптограф Клод Шеннон роздумував про шахову гру з одним гравцем, в якій люди б конкурували з комп'ютером. Дійсно, ігровий процес був ключовим двигуном ШІ, і є полігоном для моделювання, побудованих середовищ і тестування реалізму, які є основою віртуального досвіду.[1]

У відеоіграх штучний інтелект використовується для створення чутливої, адаптивної або інтелектуальної поведінки в першу чергу персонажів, що не є гравцями (non-player characters або NPCs), схожих із людським інтелектом. Використовувані засоби, як правило, спираються на існуючі методи з області штучного інтелекту (ШІ).

Наприклад, у Sim City 1989 року гравці керували складними симуляціями, а ШІ в елементарних іграх був розвинутий, щоб імітувати щось близьке до реалізму, тобто глибоко людські характеристики, такі як непередбачуваність. Жанр "shoot-‘em-up"(перестріляти їх усіх) також був прикрашений реалізмом. У Total War 2000 року віртуальні воїни мали людські емоції, подібно до солдатів у реальних боях.

ШІ особливо цінний для ігор, оскільки ігровий досвід однозначно залежить від якості. Практично неандертальський візуальний досвід - це добре (ніхто ніколи не скаржився на "реалізм" Pacman). Ідеально відточений візуальний досвід - теж добре. Але досвід, що майже ідеальний, але все ж таки недостатньо, є жахливим до точки дезорієнтації та навіть обурення. Дизайнери ігор називають це “Uncanny Valley”. Дозвольте ШІ працювати та ігри зможуть досягти реалізму, необхідного, щоб уникнути подібного.

Ігровий веб-сайт GamaSutra відзначає багато способів використанння ШІ, що сприяють розвитку ігрових технологій: «У комерційних іграх вже успішно реалізовано ШІ. Є Black & White (машинне навчання), F.E.A.R (контекстно-чутлива поведінка), Facade (природний розбір мови), Spore (моделювання життєвих форм, керованих даними)»[1].

На сьогоднішній день цілий ряд покращень у технологіях (консолі, хмара / зв'язність, ультрапотужні відеокарти, VR / навушники, алгоритми рендеринга) забезпечують живлення штучного інтелекту, що, в свою чергу, забезпечує все більш вражаючі умови, в яких віртуальні персонажі демонструють поведінку та інтелект людини.

«Завдяки сучасній ігровій індустрії ми можемо провести вечір подорожуючи по фотореалістичним ігровим світам, таким як пост-апокаліптичний Бостон Fallout 4 або Лос-Сантос із Grand Theft Auto V, замість того, щоб робити такі речі, як зустрічатися з людьми або займатися людською взаємодією будь-якого роду», говорить Джордан Пірсон.[1] У цьому плані штучний інтелект та машинне навчання створюють наступне покоління всієї індустрії дозвілля.

Алгоритми ШІ стають розумнішими та навчаються виконувати завдання, отримуючи величезну кількість даних. Коли ви знаходитесь на Facebook, не виникає величезної перешкоди. Facebook щодня створює величезні набори даних. У нього є мільйони вже помічених фотографій, які потім допомагають його алгоритму ШІ зрозуміти, хто позначений на майбутніх зображеннях. Але, крім великих компаній-виробників даних, більшість компаній не здобувають обсяги даних, необхідних для належного навчання алгоритмів ШІ. Крім того, люди просто не мають ні часу, ні

[*] Науковий керівник – Конопліцька-Слободенюк О. К., викладач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету

терпіння, щоб витрачати їх на навчання алгоритмів ШІ всьому, що їм необхідно знати. Але відеоігри мають терпіння і час з достатком.[2]

Коли Адрієн Гайдон, комп'ютерний науковець із Xerox Research Center Europe, побачив трейлер до відеогри Assassin's Creed, він був обдурений думкою, що це трейлер до фільму через його реалістичний вигляд. Коли він зрозумів, що це фактично комп'ютерна графіка(CGI), він подумав, що якщо його можна обдурити думкою, що відеогра була реальною, можливо, алгоритми ШІ також можуть бути обдурені.[2]

Артур Філіпович та його команда в Прінстонському університеті використовували Grand Theft Auto, щоб допомогти своєму алгоритму ШІ дізнатися про знаки зупинки. Перша робота полягала в тому, щоб навчити ШІ вивчати варіанти стоп-сигналів, у тому числі, розуміючи, що вони були знаками зупинки, у випадках, коли вони були частково затемнені, в тіні, забруднені або покриті снігом, представлені в різний час доби та багато іншого. Замість того, щоб шукати всі можливі зображення або зібратися робити власні зображення стоп-знаків за різних обставин, команда використала Grand Theft Auto V як тренувальний майданчик. У грі було безліч знаків зупинки в різних ситуаціях, які були ідеальними для тренування ШІ. Для того, щоб гра була використана як симулятор водіння для ШІ, її треба було налаштувати, щоб користуватися нею могла інша комп'ютерна програма, а не лише людина.

Джорджіос Н. Яннакакіс наводить на думку, що академічні розробки ШІ можуть відігравати роль у грі штучного інтелекту за межами традиційної парадигми поведінки NPC, що контролює ШІ. Він виділяє чотири інші потенційні області застосування:

1) Моделювання з використанням досвіду гравців: Вивчаючи вміння та емоційний стан гравця, щоб належним чином адаптувати гру. Це може включати в себе динамічне балансування ігрового процесу, яке полягає у регулюванні складності відеоігор у режимі реального часу залежно від здібностей гравця. Гра ШІ також може допомогти виявити наміри гравця (наприклад, розпізнавання жестів).

2) Створення процедурного контексту: Створення елементів середовища гри, таких як умови навколишнього середовища, рівні та навіть музика в автоматичному режимі. Методи ШІ можуть генерувати новий контекст або інтерактивні історії.

3) Збирання даних про поведінку користувачів: Це дозволяє дизайнерам ігор вивчати, як люди використовують гру, у які саме частини вони грають найбільше, і що змушує їх перестати грати, дозволяючи розробникам налаштовувати ігровий процес або покращувати монетизацію.

4) Альтернативні підходи до NPC: Це включає зміну налаштувань гри для підвищення правдоподібності NPC та вивчення їх соціальної, а не індивідуальної поведінки.[3]

ШІ робить внесок у власне ігровий бізнес. Інвестори усвідомлюють, що ігрова індустрія швидко поєднується з реальним світом, фільмами та іншими медіа або товарами, і що можливості монетизації цього змішаного світу будуть продовжувати рости з нашим розширеним дозвіллям та захоплюючими віртуальними враженнями на основі ШІ. Тобто ШІ поступово стає невід'ємною частиною нашого життя.

Список використаних джерел

1. *Carrozo M. How Artificial Intelligence is changing the gaming industry [Електронний ресурс] / Matthew Carrozo. – 2017. – Режим доступу до ресурсу: https://unbabel.com/blog/ai-changing-gaming-industry/.*
2. *Marr B. Artificial Intelligence: The Clever Ways Video Games Are Used To Train AIs [Електронний ресурс] / Bernard Marr. – 2018. – Режим доступу до ресурсу: https://www.forbes.com/sites/bernardmarr /2018/06/13/artificial-intelligence-the-clever-ways-video-games-are-used-to-train-ais/#29b308a29474.*
3. *Artificial intelligence in video games [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Artificial_intelligence_in_video_games.*

УДК 004.8

Гіцеларь Д. В.[*]
Центральноукраїнський національний технічний університет

Методи утворення штучного інтелекту комп'ютерно-керованим персонажем. Обгрунтування вибору саме нейронної мережі

Штучний інтелект (ШІ) широко використовується у сучасному світі. Він без перебільшення працює всюди: у медицині, промисловості та сільському господарстві, дорожньому русі. Не є новиною, що ШІ зустрічається також у комп'ютерних іграх, а також є випадки попереднього навчання систем штучного інтелекту на комп'ютерних симуляціях. Фактично розробники створювали комп'ютерну гру для штучного інтелекту для його тренування у віртуальному просторі для подальшого використання на реальних задачах. Наприклад нейронна мережа вчиться керувати автомобілем у віртуальному просторі GTA V [1]. Відповідно, в сьогоденні вирішення задач за допомогою нейронних мереж дозволяє наробити статистику їх застосовності, визначити ефективність архітектури мереж для певного кола задач. Тому навіть навчання штучних нейронних мереж для ігрових програм має наукову цінність.

Для створеної гри за допомогою Unity 3D виникла потреба у створенні штучного інтелекту для супротивника людині. Гра полягає в дуелі двох танків. Також у грі наявні перешкоди, тобто ШІ повинен вміти оминати їх. З вище зазначених причин було вирішено використати штучну нейронну мережу (НМ), що навчається сама.

На входи НМ, тобто на зовнішній шар нейронів повинна надходити інформація про місцевість та положення суперника. Для надання інформації про місцевість існує кілька шляхів, наприклад можна подавати інформацію про прохідність місцевості у вигляді двовимірної матриці-мапи; також є доступним рішення оцінювання дистанції до видимих перешкод за фіксованими відносно положення танку напрямками. В роботі надається перевага другому рішенню бо такий спосіб не накладає додаткових умов та обробок на повороти, коли для двовимірної мапи поворот сильно спотворить вигляд вхідної інформації, з'являться помилки дискретизації ігрового простору і значно ускладнить алгоритми підготовки вхідних даних. На рис. 1 показано саме оцінку дистанції до видимих перешкод.

Дані відстані отримуються із тридцяти двох променів, які побудовані рівномірно по колу від напрямку руху танку за допомогою вбудованих можливостей Unity Raycast. Промені посилаються у певному напрямку до відстані «горизонту», як показано на рисунку 1. Червоним позначено побачені перешкоди, а зеленим напрям та відстань до ворога.

Відповідно випущеним 32-м променям формується одновимірний масив з 32-х елементів з значенням від 0 до 1, які відповідають відносній відстані по відповідному напрямку до перешкод. Відстань 1 позначає відсутність перешкод до лінії горизонту; 0 – перешкода знаходиться впритул до танку. Аналогічно будується масив пошуку супротивника або супротивників – одиничні значення означають відстань до супротивника за умовним горизонтом, а значення менше одиниці пропорційне відстані до суперника.

Відповідно двом масивам по 32 значення, тридцять два вхідні нейрони будуть відповідати за напрямок та відстань до перешкод, така ж кількість за відстань та напрям до супротивника. Ці вхідні масиви формують вхідний шар з 64-х нейронів. Наступним шаром з 64-х нейронів повинна проводиться попередня обробка інформації, після чого

[*] Науковий керівник – Дрєєва Г. М., викладач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету

інформація передається до шару суміщення інформацій від перешкод та положення супротивника. Вихідний шар має п'ять виходів. Прийнятим рішенням вважається вихід, який має максимальний вихідний рівень.

Отримана архітектура НМ проілюстрована на рисунку 2.

Рисунок 1 – Демонстрація створення рейкастів

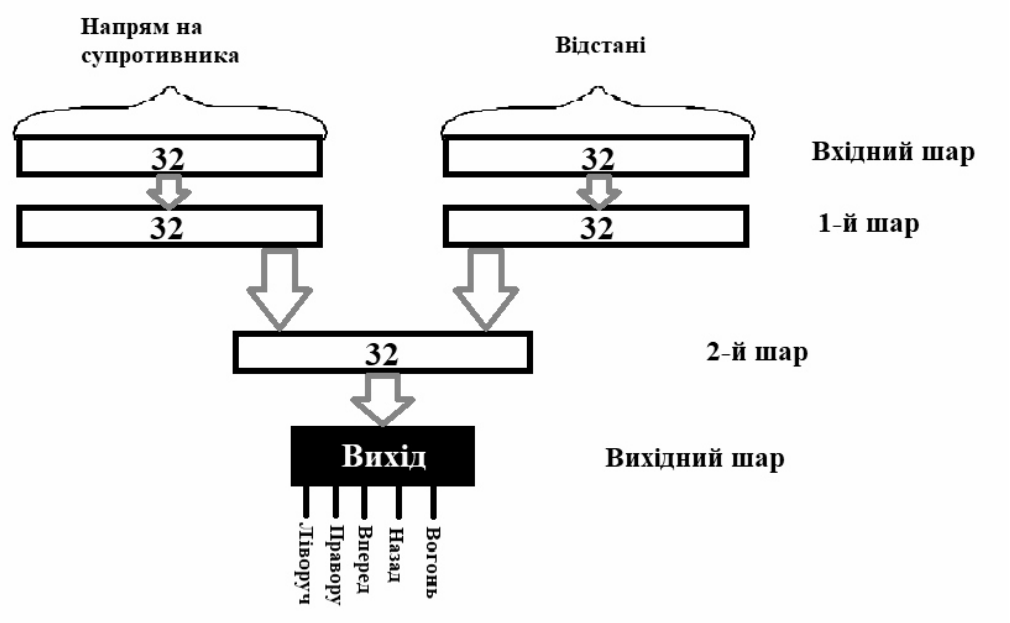


Рисунок 2 – Архітектура нейронної мережі

Висновок. В результаті дослідження було обрано форму вхідних, вихідних даних та вид нейронної мережі для керування комп'ютерним супротивником.

Список використаних джерел

1. *https://www.twitch.tv/sentdex*
2. *Nielsen M. Neural networks and deep learning [Електронний ресурс] / Michael Nielsen. – 2018. – Режим доступу до ресурсу: http://neuralnetworksanddeeplearning.com/chap1.html.*
3. *Luke D. What is an artificial neural network? Here's everything you need to know [Електронний ресурс] / Dormehl Luke. – 2018. – Режим доступу до ресурсу: https://www.digitaltrends.com/cool-tech/what-is-an-artificial-neural-network/.*

УДК:004.38

Гриб О. О., Конопліцька-Слободенюк О. К.
Центральноукраїнський національний технічний університет

Штучні нейронні мережі

Штучна нейронна мережа (Artificial Neural Network ANN) - це парадигма обробки інформації, яка надихається методом біологічної нервової системи, такої як інформація про мозок, процес. Ключовим елементом цієї парадигми є нова структура системи обробки інформації. Вона складається з великої кількості високо взаємопов'язаних процесорних елементів (нейронів), які працюють в унісон для вирішення конкретних проблем. Інтернет-ресурси, як і люди, навчаються на прикладі. АНН налаштовується для певної програми, наприклад, розпізнавання образів або класифікація даних, через процес навчання. Навчання в біологічних системах передбачає коригування синаптичних зв'язків, які існують між нейронами.

Чому використовувати нейронні мережі? Нейронні мережі, що мають чудову здатність отримувати значення з складних або неточних даних, можуть бути використані для вилучення візерунків та виявлення тенденцій, які занадто складні, щоб їх помітили ні люди, ні інші комп'ютерні технології. Підготовлену нейронну мережу можна розглядати як "експерт" у категорії інформації, яку вона дала для аналізу. Цей експерт може бути використаний для надання прогнозів з урахуванням нових цікавих ситуацій та відповідей на запитання "що,якщо". Інші переваги:

Адаптивне навчання: вміння навчитися виконувати завдання на основі даних, наданих для тренування або початкового досвіду.

Самоорганізація: ANN може створити власну організацію або представлення інформації, яку вона отримує під час навчання.

Операція в режимі реального часу: розрахунки ANN можуть виконуватися паралельно, а спеціальні апаратні пристрої розробляються та виготовляються, які використовують цю можливість.

Толерантність до помилок через кодування інформації, що перевищує: Часткове знищення мережі призводить до відповідної деградації продуктивності. Однак деякі можливості мережі можуть зберігатися навіть при значному пошкодженні мережі.

Застосування нейронних мереж в практиці. Нейромережі мають широке застосування для реальних проблем бізнесу. Фактично, вони вже успішно застосовуються в багатьох галузях промисловості.

Оскільки нейронні мережі найкраще визначають схеми або тенденції даних, вони добре підходять для прогнозування або прогнозування потреб, зокрема: прогнозування продажів, контроль промислового процесу, дослідження клієнтів, перевірка даних, управління ризиками, цільовий маркетинг

Нейронні мережі в медицині. Штучні нейронні мережі (ANN) в даний час є "гарячим" науковим напрямом в медицині, і вважається, що вони будуть отримувати широке застосування біомедичних систем в найближчі кілька років. На даний момент дослідження полягають в основному на моделюванні частин тіла людини та розпізнаванні захворювань різними сканами (наприклад, кардіограмами, скануванням CAT, ультразвуковими скануваннями тощо).

Нейромережі ідеально підходять для розпізнавання захворювань з використанням сканування, оскільки немає необхідності надавати конкретний алгоритм визначення хвороби. Нейронні мережі вивчають на прикладі, тому деталі про те, як визнати хворобу, не потрібні. Що потрібно, це набір прикладів, які є репрезентативними для

всіх варіантів захворювання. Приклади слід підбирати дуже ретельно, якщо система повинна виконуватись надійно та ефективно.

Нейронні мережі в бізнесі. Бізнес - це переадресована область з кількома основними спеціалізаціями, такими як бухгалтерський облік або фінансовий аналіз. Майже будь-яке застосування нейронної мережі вписується в одну бізнес-зону або фінансовий аналіз.

Нейронні мережі проти звичайних комп'ютерів. Нейронні мережі використовують інший підхід до вирішення проблем, ніж звичайні комп'ютери. Звичайні комп'ютери використовують алгоритмічний підхід, тобто комп'ютер витримує набір інструкцій для вирішення проблеми. Відомо, що комп'ютери не можуть вирішити проблему, якщо не будуть відмічені конкретні кроки, які комп'ютер повинен виконати. Це обмежує проблему вирішення можливостей звичайних комп'ютерів до проблем, які ми вже розуміємо і вміємо вирішити. Але комп'ютери були б набагато корисніше, якщо б вони могли робити те, що ми точно не вміємо робити.

Нейронні мережі обробляють інформацію подібним чином у людському мозку. Мережа складається з великої кількості високо взаємопов'язаних елементів обробки (нейронів), що працюють паралельно для вирішення конкретної проблеми. Нейронні мережі вивчають на прикладі. Вони не можуть бути запрограмовані для виконання конкретного завдання. Приклади слід обережно вибирати, інакше корисний час витрачається даремно або навіть гірше, що мережа може працювати неправильно. Недолік полягає в тому, що мережа виявляє, як вирішити проблему сама по собі, її операція може бути непередбачуваною.

З іншого боку, звичайні комп'ютери використовують когнітивний підхід до вирішення проблем; те, як проблема повинна бути вирішена, повинна бути відома і зазначена в невеликих однозначних інструкціях. Ці інструкції потім перетворюються на мовну програму високого рівня, а потім на машинний код, який комп'ютер може зрозуміти. Ці машини цілком передбачувані; якщо щось трапиться не так, це пов'язано з несправністю програмного чи апаратного забезпечення.

Нейромережі та звичайні алгоритмічні комп'ютери не конкурують, але доповнюють один одного. Такі завдання більш підходять для алгоритмічного підходу, як арифметичні операції та задачі, які більше підходять для нейронних мереж. Більш того, велика кількість завдань вимагає систем, які використовують комбінацію двох підходів (звичайно звичайний комп'ютер використовується для нагляду за нейронною мережею) для максимально ефективної роботи.

Висновок. У обчислювальному світі багато чого можна придбати для нейронних мереж. Їхня здатність навчатися за прикладом робить їх дуже гнучкими та потужними. Крім того, немає необхідності розробляти алгоритм для виконання конкретного завдання; тобто немає необхідності розуміти внутрішні механізми цього завдання. Вони також дуже добре підходять для систем реального часу через їх швидку реакцію та обчислювальні часи, які пов'язані з їх паралельною архітектурою.

Список використаних джерел

1. Вступ до нейронних обчислень. Александр І., Мортон і Г. 2-е видання.
2. https://uk.wikipedia.org/wiki/Штучна_нейронна_мережа.
3. Нейронні мережі в Pacific Northwest National Laboratory.

УДК 004.89

Калюжний Р. І.
Центральноукраїнський національний технічний університет

Симбіоз штучного інтелекту і хмарних технологій

Штучний інтелект трактується сьогодні як системи, які можуть розуміти, вчитися, прогнозувати, адаптуватися і потенційно здатні функціонувати без участі людини [1].

Одним з найбільш поширених рішень на основі штучного інтелекту (ШІ) є віртуальні персональні помічники, які вміють реагувати на голосові команди, проте компанії-розробники зацікавлені в створенні таких систем штучного інтелекту, які могли б вчитися у людини новим словами та видавати різні варіанти відповідей. Досягненню цієї мети також можуть допомогти хмарні обчислення.

Хмара забезпечує ШІ інформацією і знаннями, яким він повинен навчитися, а ШІ, в свою чергу, заповнює хмарні сховища новими даними. Безліч окремих серверів, на основі яких створюється хмара, містять дані, які ШІ може отримати і використовувати для прийняття рішень і навчання навичкам комунікації. Як тільки ШІ дізнається щось нове, він передає ці дані назад в хмару, звідки цю інформацію будуть черпати і використовувати для навчання вже інші ШІ [2].

Поєднання хмарних технологій і штучного інтелекту реалізується в двох основних формах:

- хмарні платформи машинного навчання;
- хмарні сервіси з вбудованим ШІ з реалізацією різних варіантів застосування ШІ.

Одним із складніших варіантів є створення багатоагентної системи, яка базується на колективній поведінці децентралізованих систем, що самоорганізуються і ґрунтуються на агентних технологіях. При цьому автоматизується частина роботи з прийняття рішень, оцінки та інтерпретації даних сенсорів з функціями попередньої обробки даних разом з їх фільтрацією та відновленням [3].

Автономний високоінтелектуальний агент володіє наступними здібностями: реагувати, вийти на зв'язок, планувати дії, ставити цілі, підтримувати моделі подання знань, підвищувати рівень знань і якість роботи через навчання. Такий агент інтегрується в структуру хмарних обчислень, що містить конкретні функції щодо вирішення завдань, обробці даних і управління.

Він підтримує зв'язок інформації та технологій, заснованих на знаннях; виконує процес логічних міркувань; застосовує функцію навчання і самовдосконалення як на рівні інфраструктури (адаптивна маршрутизація), так і на рівні додатку (адаптивні інтерфейси). Розробляється або як самостійний компонент системи, або як компонент, який взаємодіє з експертними системами.

Отримання правильної інформації і безперервний аналіз в реальному часі в хмарі є актуальним завданням для того, щоб знайти цінну інформацію і управляти репутацією. Здатність хмарних систем робити доступними дані про транзакції активних бізнес-процесів, що відбуваються в реальному часі, дозволить організаціям оперативно реагувати на події в реальному часі. Поєднання ШІ і хмарних технологій дає можливість і ШІ, і людям аналізувати і збирати більше даних, ніж будь-коли раніше.

Список використаних джерел

1. *Рассел, С. Искусственный интеллект, современный подход / С. Рассел, П. Норвинг. – М.: Изд. дом «Вильямс», 2006. – 1408 с.*
2. *Ридз, Дж. Облачные вычисления / Дж. Ридз. – СПб. : БХВ, 2011. – 288 с.*
3. *Wagner G. The Agent-Object-Relationship Meta-Model: Towards a Unified View of State and Behavior / G. Wagner // Information Systems. – 2003. – 28:5 – P. 475 – 504.*

УДК 004.822:004.89

Котов І. А.
ДВНЗ «Криворізький національний університет»

Модель маркування сигнального графа мережі метаправил в онтологіях інтелектуальних систем

Для управління еволюційної ієрархією онтологій необхідний механізм, який, з одного боку, є складовою частиною системи подання знань, а, з іншого боку, є її узагальненням. На основі цього узагальнення в інтелектуальній системі повинен існувати апарат управління всією ієрархією форм представлення знань. Таким апаратом є метазнання (МЗ).

Проведений аналіз показав, що в різних інтелектуальних системах використовуються різні за ідеологією і реалізації форми подання знань. Ця обставина не дає можливості масової, швидкої і дешевої розробки інтелектуальних систем. Тому пропонується однакова уніфікація різних форм представлення знань. Така уніфікована архітектура може бути виражена через ієрархію узагальнюючих процедур, реалізовану в механізмі еволюційного успадкування онтологій.

Розробка системи подання і використання метазнань є окремою, важливу і трудомістку задачу при проектуванні ІС і СППР, зокрема. Поспєлов Д.А. відзначав, що розробка теорії метазнань в інтелектуальних системах є однією з «десяти «гарячих точок» в дослідженнях зі штучного інтелекту» [1].

Метаправила представляють собою вищий рівень знань. Вони відрізняються значним ступенем абстракції по відношенню до знань предметної області. Сутність метазнань полягає в тому, що вони реалізують методи роботи зі знаннями нижніх рівнів. Метазнання мають найбільш загальний характер, і форми їх реалізації можуть бути самими різними. Метазнання можуть бути інтегровані в загальній базі знань, в окремій базі знань або навіть бути виконані у вигляді програмного коду інтелектуальної системи.

В [2] зазначено: «Метазнання - це особливий вид знань, який може управляти іншими знаннями в базі знань інтелектуальної системи. Найчастіше в залежності від базового типу моделі подання знань формується модель подання метазнань. Наприклад, для управління семантичної мережею − найчастіше пропонується метамережа, продукційними правилами − метаправила і т.і.». Муромцев Д.І. в [3] уточнює: «Якщо звичайні правила БЗ представляють кроки вирішення завдання, то метаправила описують стратегію отримання рішень». Метаправила не приймають безпосередньої участі в процесі формування міркувань, а визначають пріоритет виконання або, навпаки, виключають з розгляду звичайні правила. Метаправила виконуються в першу чергу.

Загальний підхід до уніфікації та інтерпретації МЗ зроблений в специфікації стандарту Common Warehouse Metamodel (CWM) [4]. Консорціум Meta Data Coalition визначає МЗ як описову інформацію про структуру і сенсі даних, а також додатків і процесів, які маніпулюють даними.

Перш за все, система метаправил повинна вирішувати два основні завдання:

- завдання наскрізного синтезу і модифікації структур знань;
- завдання функціонування (обчислення) всієї ієрархії представлення знань.

При формуванні базових принципів інтерпретації понятійного апарату використовуємо основні положення, сформульовані К.А. Петрі, і далі узагальнимо їх:

- модель повинна відповідати законам фізики;
- події в мережі повинні відповідати причинно-наслідковим відносинам;
- елементарні дискретні дії повинні підкорятися законам збереження – збереження

енергії і збереження речовини.

Природно, що вихідним постулатом є наявність мережевої структури у всіх форм представлення знань.

Із заявлених принципів слід, що структурні моделі всіх рівнів подання знань можуть розглядатися як сигнальні (імпульсні) лінійні орграфи [5].

Введемо модель маркування сигнального графа мережі метаправил для онтологій інтелектуальних систем.

Атомарний концепт − c_s − це висловлювання, яка призначається вузлу сигнального графа і розглядається цілком при інтерпретації та обчисленні БЗ.

Сигнал − t − це числовий концепт, що характеризує можливість причинно-наслідкового зв'язку між вузлами сигнального графа. В даному випадку сигнал може розглядатися як імплікація, забезпечена числовою характеристикою проходження або поширення сигналу. Іншими словами, якщо в галузі графа існує сигнал, то між вузлами, інцидентними цієї гілки, активна причинно-наслідковий зв'язок.

Потенціал вузла (вузловий сигнал)– $u \in \square$ − це число (в загальному випадку дійсне), яка призначається вузлу і асоційоване з ним в поточній ітерації роботи системи. При наступній ітерації можливе призначення або обчислення іншого числа. Вага вузла не несе конкретної семантичного навантаження і інтерпретується в рамках поточної задачі. Асоційовані з вузлами числа можна інтерпретувати як ваги, потенціали, фішки вузлів [6]. Ніяких принципових обмежень на потенціали вузлів не накладається. Рівень активності вузла (поточний потенціал вузла) - це накопичений потенціал (вага, сигнал) в вузлі на момент участі вузла в процесі інтерпретації мережі. Рівень активності (величина потенціалу) вузла визначається як сума всіх вхідних сигналів через інцидентні вузлу гілки. Призначення сигналів вузлів реалізується функцією маркування або обчислюється.

Активність вузла – $a = (0 \mid 1)$ − це двійкова ознака, що характеризує участь вузла в інтерпретації мережі. Якщо вузол не активний ($a = 0$), він ніяк не інтерпретується блоком (машиною) логічного висновку (БЛВ), не бере участі в логічному висновку і зміст такого вузла не розглядається.

Поріг чутливості вузла до вхідного сигналу в загальному вигляді − $s_u = f(t_m)$ − це міра здатності вузла пропускати вхідний сигнал в наступні інцидентні з ним гілки, де t_m − це граничний рівень сигналу. Вид функції $f(t_m)$ визначається специфікою завдання і цілями моделювання. У найпростішому випадку може використовуватися порогова функція або сигмоид. При перевищенні порогу чутливості s_u активізується вузол p_i, і в ньому констатується сигнал заданої величини $t(p_i)$. Сигнали, менші s_u, не сприймаються вузлом.

Введемо функцію маркування *i-го* вузла сигнального графа бази знань. Визначимо параметр маркування через кортеж

$$m_\mu = < c_s, u, s_u, a >. \quad (1)$$

Тоді маркування для довільного *i-ого* вузла визначиться наступним чином

$$\mu_i^p : p_i \to m_\mu(p_i) = < c_s(p_i), u(p_i), s_u(p_i), a(p_i) >, \quad (2)$$

$$\mu_i^p \in M^p,$$

$$p_i \in P(G_s),$$

$$M^p : P(G_s) \to m_\mu(P),$$

$$u(p_i), s_u(p_i) \in \square,$$

де μ_i^p − функція маркування *i-го* вузла p_i параметром $c(p_i)$;

M^p – загальне маркування вузлів кластера (або всієї мережі), по відношенню до якого використовується модель метазнань;

$P(G_s)$ − множина вузлів кластера (або всієї мережі), по відношенню до якої використовується модель метазнань;

$\mathbb{R}$ − множина дійсних чисел.

Під гілкою b_{jk} між вузлами j і k структури подання знань будь-якого рівня з точки зору застосування до нього метаправил будемо розуміти спрямоване ставлення (зв'язок, дугу) між цими вузлами в сигнальному графі бази знань. Кожна гілка має вхідний і вихідний потенціали (сигнали). При цьому, якщо гілка спрямована від вузла j до вузла k, то вузол j, якій має потенціал u_j , буде істоковим, а вузол k, якій має потенціал u_k, − стоковим.

Провідність (передача) гілки – $\gamma(b)$ − це число (в загальному випадку дійсне), пов'язане з гілкою. Призначення чисел гілкам є маркуванням. Числа, асоційовані з гілками, можна вважати вагами, провідностями, довжинами, вартостями гілок і т.і. Ніяких обмежень на ці цифри не накладається. В рамках даної роботи вважаємо числа, які позначають гілки, провідностями цих гілок.

Тепер запропонована узагальнена модель графа рівня структури БЗ може бути описана наступним кортежом

$$G_s = (P(G_s), A(G_s), M_\Sigma), \tag{3}$$

$$M_\Sigma = < M^P, M^B >.$$

Таким чином, теоретично обґрунтована і практично побудована структурно-лінгвістична модель уніфікованої професійної онтології рівня метаправил на основі моделі маркування сигнального графа мережі метаправил.

Розроблені моделі управління структурою БЗ, засновані на апараті графів, дозволяють формалізувати мову рівня метаправил і описати їх онтологію. При цьому необхідно врахувати такі особливості:

- метаправила виконують структуризацію БЗ, ніж визначають механізм її виконання (обчислення);
- метаправила мають доступ до всіх рівнів БЗ, розташованих нижче;
- метаправила отримують вхідні дані (сигнали) з «зовнішнього світу». Структура вхідних даних може відрізнятися від внутрішнього уявлення БЗ;
- метаправила виступають в якості інтерфейсу між інтелектуальною системою і БЛВ;
- метаправила можуть не утворювати мережевих структур, так як їх логіка використання визначається роботою інтелектуальної системи, а не логікою БЗ.

Список використаних джерел

1. *Поспелов Д.А. Десять «горячих точек» в исследованиях по искусственному интеллекту // Интеллектуальные системы – М.: Изд-во МГУ – 1996 – Т.1, Вып.1-4. – С.47 – 56*
2. *Марьин С.А. Метапродукционные модели в задачах многоэкспертного вывода / Н.В. Кривич, С.А. Марьин // Радиоэлектроника и информатика. – 1997 – №1 – С. 49 – 52*
3. *Муромцев Д.И. Введение в технологию экспертных систем. – СПб: СПб ГУ ИТМО – 2005 – 93 с.*
4. *Башмаков А.И., Башмаков И.А. Интеллектуальные информационные технологии: Учеб. пособие. - М.: Изд-во МГТУ им. Н.Э. Баумана - 2005 - 304 с.*
5. *Робертс Ф.С. Дискретные математические модели с приложениями к социальным, биологическим и экологическим задачам/Пер. с англ. А.М. Раппопорта, С.И. Травкина. Под ред. А.И. Теймана − М.: Наука. Гл. ред. физ.-мат. лит − 1986 − 496 с.*
6. *Берж К. Теория графов и ее применения: Пер. с фран. / Под ред. И.А. Вайнштейна — М.: Изд-во ностр. лит. – 1962 – 320 с.*

УДК 004.032.26:004.42

Логінова С. М.
Донецький національний технічний університет

Дослідження методу лейтнера з нейромережею для мобільного додатку вивчення іноземної мови

В останні десятиліття вивчення іноземних мов викликає підвищений інтерес. В результаті світової глобалізації та інтеграції відбувся бурхливий ріст міжкультурних контактів у всіх сферах нашого життя: з'явилася велика різноманітність ситуацій міжкультурного спілкування, таких як навчання в школі і ВНЗ з обміну, стажування вчених, міжнародні конференції, спільні підприємства, туристичні поїздки, виставки тощо. Таким чином, володіння іноземною мовою є однією з умов успішної адаптації в соціальному просторі.

Вивчення мови починається з формування словникового запасу. Його поповнення повинно бути безперервним процесом. Існують різні підходи до запам'ятовування іноземних слів: традиційний метод Ярцева, метод карток, метод прописування для візуалів; або прослуховування слів, багаторазове повторення для аудиалів. Але всі ці методи вимагають деяких речей у вигляді, наприклад, ручки, паперу і списку, вивчення слів; карток; аудіозаписів, що не завжди може виявитися поруч, коли буде вільна хвилинка для повторення слів. Найефективнішим методом запам'ятовування слів є метод Лейтнера. Метод полягає в повторенні іноземних слів через різні проміжки часу, в залежності від результату відтворення слова напам'ять.

Існують безліч аналогів мобільних додатків. Найвідомішими є наприклад.

Duolingo (Програма вивчення побудована в формі дерева досягнення, тобто для того щоб перейти на новий рівень, потрібно набрати певну кількість балів. Їх можна заробити за правильні відповіді в завданнях: порівняти слово з картинкою, перевести фразу з рідної мови на досліджуваний і навпаки. Свої досягнення можна порівнювати з успіхами інших користувачів і навіть ділитися ними в соціальних мережах.);

Rosetta Stone (У додатку є своя методика, яка головним чином побудована на асоціативному ряді.);

Memrise (Методика роботи проста і зрозуміла: даються слова, потім їх значення, переклад, а вам пропонується запам'ятати їх, скласти слова з букв, грати з ними. В кінці кожного уроку видається відсоток правильних відповідей.).

Усі існуючі мобільні додатки використовують для вводу тексту клавіатуру девайсу. У додатку, який розроблюється, буде можливість писати текст від руки.

Для деяких психотипів людей дуже важливо прописувати інформацію для більш надійного запам'ятовування. Це науково доказано. Професор Прінстонського університету Пем Мюллер провела дослідження у результаті якого виявила, що ті, хто набирають текст, а не пишуть його, гірше справляються з концептуальними питаннями, одне з них стосується саме набору тексту. Воно полягає у тому, що, коли людина набирає текст з клавіатури, вона не включається у процес, робить це на рівні інстинкту, замість того, щоб обробляти інформацію. Це погано позначається на результатах.

Щоб розпізнати почерк людини будемо використовувати нейронні мережі. У реальності часто доводиться працювати не з ідеальними буквами (рис. 1).

Рисунок 1 – Спотворені символи

Виходячи з цього виникає проблема представлення зображення, зрозумілого для нейронної мережі. Кожна буква на зображення може бути представлена як матриця з певними значеннями елементів, які чітко можуть визначити букву. Тобто представлення символу латинського алфавіту зручно формалізувати матрицею з n рядків і m стовпців. Кожен елемент такої матриці може приймати значення в діапазоні [0, 1].

Припустимо, що нейронна мережа включає в себе 35 входів (бо вектор складається з 35 елементів) і 26 виходів (бо букв 26). Дана НМ є двошаровою мережею. Функцією активації поставимо логарифмічну сігмоідную функцію, яку зручно використовувати, тому що вихідні вектори містять елементи зі значеннями в діапазоні від 0 до 1, що потім зручно перевести в булеву алгебру. На прихований рівень виділимо 10 нейронів (бо просто так, можна будь-яке значення, далі перевіримо, а скільки їх треба). Якщо Вам, щось не зрозуміло з вище написаного про побудову мережі, прочитайте, будь ласка, про це в літературі (потрібні поняття, якщо збираєтеся працювати з НМ). Схематично розглянуту мережу можна представити наступною схемою (рис. 2):

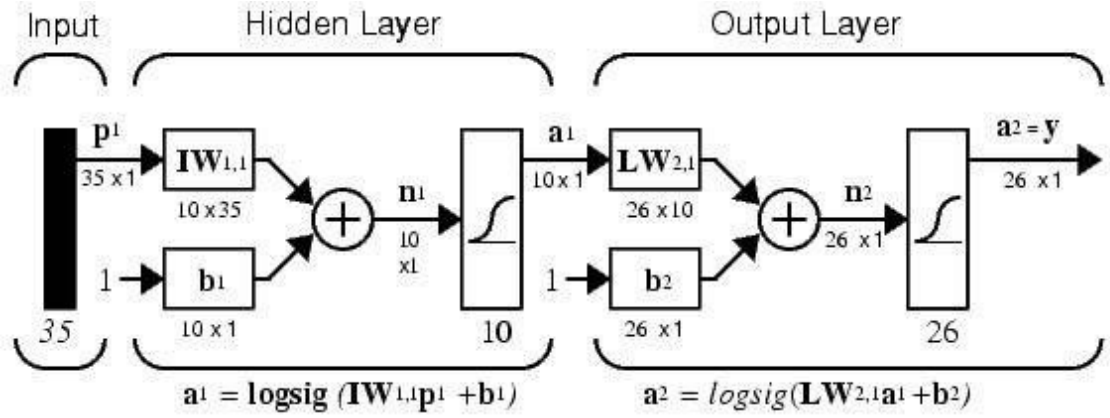


Рисунок 2 – Схема нейронної мережі

Після цього приступимо до навчання мережі. Для створення нейронної мережі, яка може працювати з зашумленими вхідними даними, необхідно навчити мережу, подаючи на вхід дані, як з шумом, так і без. Для цього необхідно спочатку навчити мережу, подаючи дані без шумовий складової. Потім, коли мережа навчимо на ідеальних даних, зробимо навчання на наборах ідеальних і зашумлених вхідних даних.

Результатом роботи буде готовий мобільний додаток з нейронною мережею розпізнавання слів, введених не з клавіатури.

Список використаних джерел

1. *Е. Е. Федоров, Искусственные нейронные сети. Красноармейск: ДВНЗ «ДонНТУ», 2016.*
2. *Г. Р. Еремеева и А. Р. Баранова, «Метод интервальных повторений при изучении иностранного языка», Бюллетень науки и практики, 15 июля 2016.*
3. *О. Г. Руденко, Штучні нейронні мережі. Харків: ТОВ «Компанія СМІТ», 2006.*

УДК 004.4

Маценко Р. В.
ДВНЗ «Криворізький національний університет»

Використання нейромережевої комп'ютерної системи для анімаційних об'єктів

Висока популярність нейромереж та суміжних рішень на їхній основі за останнє десятиліття робить тему досить актуальною. Порівняно зі звичайним алгоритмічним програмуванням нейромежеві комп'ютерні системи дають можливість реалізувати такі функції, що складно піддаються формалізації, наприклад: розпізнавання зображень, визначення ризиків кардіологічних захворювань, метеорологічні прогнози тощо.

Паралельно з розвитком комп'ютерних технологій в 50-х роках, розпочалися дослідження функціонування та структури людського мозку, саме ці дані становлять основу нейронних мереж. Нейронні мережі представляють собою програмну або апаратну реалізацію за принципом біологічних нейронних мереж – з'єднань біологічних нервових клітин. Відомою стала програма AlphaGo для гри в го на основі поглибленої нейронної мережі. Розроблена вона компанією Google DeepMind в 2015 р. AlphaGo стала першою в світі програмою, яка виграла матч без гандикапу у професійного гравця в го [1].

Створення якісних скелетних 3D анімацій сьогодні, мабуть, сама важкодоступна для інді розробників завдання. Якщо фізичний рендеринг і створення якісно освітлених статичних сцен стають доступні ентузіастам завдяки потужним безкоштовним ігровим движкам і інструментам 3D моделювання, то створення гарної анімації вимагає обладнання для захоплення рухів і тривалої копіткої роботи по їх впровадженню.

Наочний приклад реалізації дослідників з Единбурзького університету, які розробили нову систему навчання, яка називається фазово-функціональна нейронна мережа (PFNN) яка використовує машинне навчання для анімації персонажів у відеоіграх і інших додатках. Дослідник Ubisoft Montreal і провідний дослідник проекту Деніел Холден (Daniel Holden) описав PFNN, як навчальний фреймворк, який підходить для створення циклічного поведінки, наприклад, пересування людини. Він і його команда також розробляють вхідні і вихідні параметри мережі для управління персонажами в режимі реального часу в складних умовах з детальним взаємодією з користувачем[3].

На етапі навчання PFNN вчиться використовувати дані рельєфу, щоб створювати рух персонажа в кожному кадрі з урахуванням параметра управління. На етапі виконання вхідних параметрів в нейромережі збирається з призначеного для користувача введення і з середовища, а потім вводиться в системі для визначення руху персонажа.

Такий механізм управління ідеально підходить для роботи з персонажами в інтерактивних сценах у відеоіграх і системи віртуальної реальності. Дослідники заявили, що якщо навчати мережу з нециклічного фазової функцією, PFNN можна легко використовувати для вирішення інших завдань, на зразок моделювання ударів рук і ніг.

Висновки. Нейронні технології середини 20 століття змінюють зараз цілі галузі, оптимізуючи однотипні і специфічні роботи. Нейронні мережі та глибоке навчання наразі забезпечують найкращі рішення для багатьох проблем розпізнавання образів, розпізнавання мови та обробки природної мови. Можливість реалізувати трудомістку задачу руху в скелетній анімації з невеликими затратами без сумніву показує перспективність рішення в майбутньому.

Список використаних джерел

1. *Описання розробки Alphago компанією Google [Електронний ресурс] // googleblog.com – 2016. – Режим доступу до ресурсу :https://research. googleblog.com /2016/01/alphago-mastering-ancient-game-of-go.html*
2. *Нейронні мережі для початківців[Електронний ресурс] // habr.ru – 2016. – Режим доступу до ресурсу https://habrahabr.ru/post/312450/*
3. *Нейросеть генерирует движения в режиме реального времени [Електронний ресурс] // habr.ru – 2017. – Режим доступу до ресурсу https://habr.com/post/373431/*

УДК 004.932+004.627

Мельник Р. А., Шпортько В. О., Тушницький Р. Б.
Національний університет "Львівська політехніка"

Програмне забезпечення для екстракції, збереження та опрацювання зображень супутникових карт хмарності

Близько 2/3 поверхні Землі завжди покриті хмарами протягом усього року, що ускладнює обробку супутникових зображень. Одним із ефективних способів прискорення та автоматизації процесу аналізу зображень з хмарами є застосування алгоритмів для обробки зображень. Найбільш відомим класом алгоритмів обробки зображень є кластеризація.

Методи кластерного аналізу широко використовуються для декомпозиції, дослідження та розпізнавання зображень [1−5]. Зокрема, робота [1] містить класифікацію методів кластеризації та спосіб формування контурів виділених кластерів. Роботи [2, 3] присвячені кластеризації графових моделей, якими відображають частини зображень. В роботах [4, 5] пропонується ієрархічний підхід до декомпозиції медичних зображень з використанням елементів нечіткої логіки.

Програмне забезпечення для екстракції, збереження та опрацювання зображень супутникових карт хмарності розроблене під час дослідження, наданому за підтримки Гранту Фонду фундаментальних досліджень (проект № 33651).

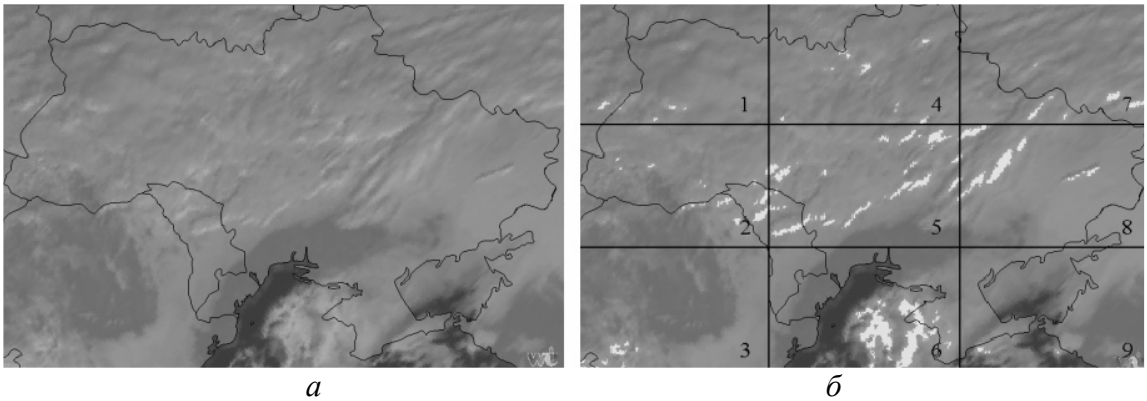
Для дослідження хмарності над територією України використано безкоштовний сервіс [6]. Даний сервіс дає змогу отримати зображення, яке можна піддати обробці з метою детектування на ньому хмар.

Алгоритм опрацювання зображення хмарності має такі кроки:

1. Отримання супутникового зображення із веб-сервісу. На рис. 1, *а* подано отримане із сервісу [6] супутникове зображення хмарності над територією України.

2. Детектування хмар. Хмари на зображенні виділяються сірим кольором. Чим ближче сірий колір до білого, тим густіші хмари. Для детектування хмар використовуються такі діапазони яскравостей пікселів зображення: (148;192], (192;244] та (244;256]. На зображенні виділяємо кольором густину хмар від найменшої (жовтий), середньої (зелений) до найбільшої (червоний).

3. Поділ зображення на сектори та аналіз хмарності в межах секторів (рис. 1, *б*).



а *б*

Рисунок 1 – Зображення карти хмарності України: *а* – отримане із сервіса, *б* – оброблене

На рис. 2 подано сформований графік посекторного розподілу хмарності. Також передбачено ретроспективний аналіз хмарності на основі збережених даних.

Супутникові зображення зберігаються у двох каталогах: Base – містить зображення, отримані із сервісу; Processed – містить опрацьовані зображення.

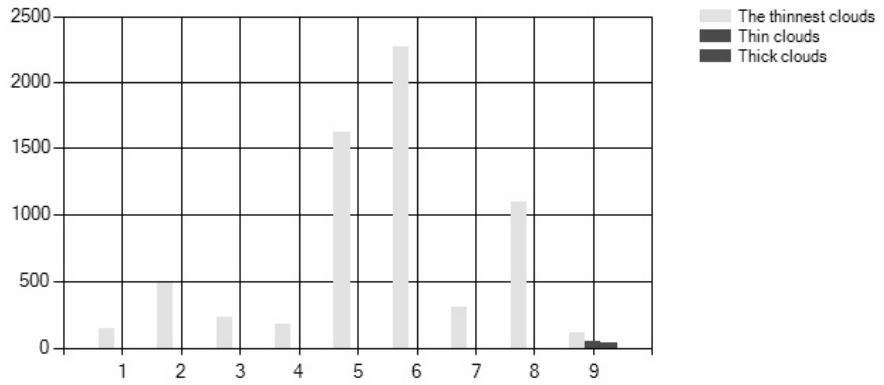


Рисунок 2 – Посекторний розподіл хмарності

Інформація про зображення та його оброблені секції зберігається у файлі у форматі JSON:


```
{
 "TotalYellow": 6613,
 "TotalGreen": 33,
 "TotalRed": 25,
 "TotalSum": 6671,
 "TimeOfLoad": "2018-11-25T13:01:21.1132566+02:00",
 "Sectors": [
  [
   {
    "Index": 1,
    "Yellow": 105,
    "Green": 0,
    "Red": 0,
    "TotalSectorSum": 105
   },
      . . .
  ]
 ]
}
```


Програмне забезпечення розроблене на мові програмування C# із використанням технології Windows Forms та середовища розробки Microsoft Visual Studio.

Для дослідження хмарності над територією України розроблено експериментальне програмне забезпечення. Запропоноване програмне забезпечення має зручний інтерфейс, дає змогу наповнити базу даних супутниковими зображеннями використовуючи веб-сервіс, а також провести їх аналіз.

Список використаних джерел

1. *Andy M Yip, Chris Ding, Tony F.Chan. Dynamic Cluster Formation Using Level Set Methods. – IEEE Trans. on Pattern Analysis and Machine Intelligence, vol.28, n. 6, pp.877–889, June, 2006.*
2. *Leo Grady, Eric L.Schwartz. Isoperimetric Graph partitioning for Image segmentation. – IEEE Trans. on Pattern Analysis and Machine Intelligence, vol.28, n. 3, pp.469-475, March, 2006.*
3. *M. Pavan, M. Pelillo. Dominant sets and Pairwise Clustering. – IEEE Trans. on Pattern Analysis and Machine Intelligence. – Vol.29, n. 1. – P.167–172, January, 2007.*
4. *Sagi Katz, Ayellet Tal. Hierarchical mesh decomposition using fuzzy clustering and cuts // ACM Transactions on Graphics. – 2003. – Vol. 22 , issue 3. – P. 954– 961.*
5. *Dosil R., Pardo X.M., Fdez-Vidal X.R. Decomposition of three-dimensional medical images into visual patterns // IEEE Transactions on biomedical engineering. – 2005, № 12. – Vol. 52. – P. 2115–2121.*
6. *Сервіс для отримання супутникових карт хмарності [Електронний ресурс]. – Веб дотуп до сторінки: https://www.wunderground.com/ (2018).*

УДК 004.8

Разно В. С.
Національний авіаційний університет

Штучна нейронна мережа. Нейронні мережі проти звичайних комп'ютерів

Штучна нейронна мережа (ANN) - це парадигма обробки інформації, яка надихається методом біологічної нервової системи, такої як інформація про мозок, процес; це взаємопов'язана група вузлів, схожа на величезну мережу нейронів у людському мозку. Ключовим елементом цієї парадигми є нова структура системи обробки інформації. Вона складається з великої кількості високо взаємопов'язаних процесорних елементів (нейронів), які працюють в унісон для розв'язання конкретних проблем. Інтернет-ресурси, як і люди, навчаються на прикладі. ANN налаштовується для певної програми, наприклад, розпізнавання образів або класифікація даних, через процес навчання. Навчання в біологічних системах передбачає коригування синаптичних зв'язків, які існують між нейронами. Це також стосується й ANN.

Нейронні мережі були натхненні архітектурою нейронів у людському мозку. Простий "нейрон" N приймає вхід з декількох інших нейронів, кожен з яких, коли він активований (або "звільнений"), подає зважене "голосування" за чи проти того, чи повинен нейрон N активізуватися. Навчання вимагає алгоритму для коригування цих ваг на основі тренувальних даних; один простий алгоритм полягає в тому, щоб збільшити вагу між двома зв'язаними нейронами, коли активація одного викликає успішну активацію іншого. Нейрони мають безперервний спектр активації. Крім того, нейрони можуть обробляти дані нелінійно, а не зважувати прямолінійні голоси. Сучасні нейронні мережі можуть вивчати як неперервні функції, так і, на диво, цифрові логічні операції. Досягнення в нейронних мережах, використовуючи глибоке навчання, спрямовували ШІ у широку суспільну свідомість та сприяли величезному перерозподілу витрат на корпоративний ШІ.

Основними категоріями мереж є ациклічні або опосередковані нейронні мережі (де сигнал проходить лише в одному напрямку) та періодичні нейронні мережі (які дозволяють отримувати відгуки та короткочасні спогади про попередні вхідні події). Серед найбільш популярних форвардних мереж є персептони, багатошарові персептони та радіальні бази мережі. Нейронні мережі можуть бути застосовані до проблеми інтелектуального контролю (для робототехніки) або навчання. Однією з переваг нейрон еволюції є те, що вона може бути менш схильною до попадання в "тупики".

Є два види топології штучних нейронних мереж - FeedForward і Feedback.

FeedForward ANN. Інформаційний потік односпрямований. Відділ передає інформацію іншому підрозділу, з якого не отримує ніякої інформації. Немає циклів зворотного зв'язку. Вони використовуються у генерації / розпізнаванні / класифікації моделей. Вони мають фіксовані входи та виходи.

FeedBank ANN. Тут дозволено цикли зворотного зв'язку. Вони використовуються у контентній адресній пам'яті.

Кожне з'єднання має вагу, ціле число, яке керує сигналом між двома нейронами. Якщо мережа генерує "хороший або бажаний" вихід, немає потреби регулювати вагу. Однак, якщо мережа створює "поганий або небажаний" вихід або помилку, система змінює вагу, щоб поліпшити подальші результати.

Нейронні мережі проти звичайних комп'ютерів. Нейронні мережі використовують інший підхід до розв'язання проблем, ніж звичайні комп'ютери. У звичайних комп'ютерах використовується алгоритмічний підхід, тобто комп'ютер виконує набір інструкцій для розв'язання проблеми. Відомо, що комп'ютери не можуть вирішити проблему, якщо не будуть відмічені конкретні кроки, які комп'ютер повинен виконати. Це обмежує проблему вирішення можливостей звичайних комп'ютерів до

проблем, які ми вже розуміємо і вміємо вирішити. Але комп'ютери були б набагато корисніше, якщо б вони могли робити те, що ми точно не вміємо робити.

Нейронні мережі обробляють інформацію подібним чином у людському мозку. Мережа складається з великої кількості високо взаємопов'язаних елементів обробки (нейронів), що працюють паралельно для вирішення конкретної проблеми. Нейронні мережі вивчають на прикладі. Вони не можуть бути запрограмовані для виконання конкретного завдання. Приклади слід обережно вибирати, інакше корисний час витрачається даремно або навіть гірше, що мережа може працювати неправильно. Недолік полягає в тому, що мережа виявляє, як вирішити проблему сама по собі, її операція може бути непередбачуваною.

З іншого боку, звичайні комп'ютери використовують когнітивний підхід до вирішення проблем; те, як проблема повинна бути вирішена, повинна бути відома і зазначена в невеликих однозначних інструкціях. Ці інструкції потім перетворюються на мовну програму високого рівня, а потім на машинний код, який комп'ютер може зрозуміти. Ці машини цілком передбачувані; якщо щось трапиться не так, це пов'язано з несправністю програмного чи апаратного забезпечення.

Нейромережі та звичайні алгоритмічні комп'ютери не конкурують, а навпаки, доповнюють один одного. Є завдання, які краще підходять для застосування алгоритмічного підходу, наприклад арифметичні операції, а є завдання, які більш зручні для нейронних мереж. Слід зазначити що, велика кількість завдань вимагає систем, які використовують комбінацію двох підходів (звичайно звичайний комп'ютер використовується для нагляду за нейронною мережею) для максимально ефективної роботи.

Нейронні мережі можна широко використовувати для виконання таких завдань, які легкі для людини, але важкі для машини: аерокосмічна промисловість - автопілот, виявлення несправностей літака; автомобільні - автомобільні системи керування; військова зброя - орієнтація та рух зброї, відстеження цілі, дискримінація об'єктів, розпізнавання особи, ідентифікація сигналу / зображення; електроніка - прогнозування послідовності коду, макетування чіпів ІС, аналіз несправностей чіпа, машинного бачення, синтезу голосу; мова - розпізнавання мови, класифікація мови, перетворення тексту в мову; обробка сигналу - нейронні мережі можуть навчатися обробляти звуковий сигнал і правильно фільтрувати його в слухових апаратах; програмне забезпечення - розпізнавання образів у розпізнаванні осіб, оптичне розпізнавання символів тощо; контроль - часто використовуються для прийняття управлінських рішень фізичних транспортних засобів; та багато іншого.

Однак, не дивлячись на таке глибоке навчання штучних нейронних мереж, сказати що такий штучний інтелект дійсно мислить та самостійно приймає рішення – однозначно не можна. Але вже зараз зрозуміло, що в майбутньому штучні нейронні мережі стануть помічниками для людей, допомагаючи в різних сферах життєдіяльності, автоматизуючи багато різних процесів заради досконалого консультування та надання дрібних послуг людям.

Отже, в сучасному світі нейронні мережі це не далеке майбутнє. Нейроінфоматикою та дослідженнями нейромереж у різних галузях займаються науковці з усього світу. За допомогою штучних нейронних мереж можна опрацьовувати, аналізувати та узагальнювати інформації, що аналогічно роботі головного мозку людини. Нейтронні мережі використовуються у економіці, медицині, зв'язку, безпеці та охоронних системах, введенні та обробці інформації. Безумовно, даний перелік не повний, проте він дозволяє отримати уявлення про характер застосування нейромережевих технологій.

Список використаних джерел

1. *Feedforward neural networks, perceptrons and radial basis networks:Russell & Norvig 2003, pp. 739–748, 758, Luger & Stubblefield 2004, pp. 458–467*
2. *Competitive learning, Hebbian coincidence learning, Hopfield networks and attractor networks:Luger & Stubblefield 2004, pp. 474–505.*
3. *М.А. Новотарський, Б.Б. Нестеренко, «Штучні нейронні мережі: обчислення», 2004.*

УДК 004

Сидоренко С. В.
Дніпровський національний університет імені Олеся Гончара

Прогнозування тенденцій рівня цукру у крові за допомогою нейтронної мережі

1. Ініціалізація мережі: вагові коефіцієнти і зсуви мережі приймають малі випадкові значення.

2. Визначення елемента навчальної множини: (вхід - вихід). Входи (x_1, x_2... x_N), повинні розрізнятися для всіх прикладів навчальної множини.

3. Обчислення вихідного сигналу:

$$S_{i_m} = \sum_{i_{m-1}}^{N_{m-1}} w_{i_m i_{m-1}} y_{i_{m-1}} - b_{i_m} \tag{1.1}$$

$$y_{im} = f(S_{jm}) \tag{1.2}$$

$$i_m = 1, 2, ..., N_m,\ m = 1, 2, ..., L \tag{1.3}$$

де S - вихід суматора, w - вага зв'язку, y - вихід нейрона, b - зсув, i - номер нейрона, N - число нейронів у прошарку, m - номер прошарку, L - число прошарків, f- передатна функція.

4. Налаштування синаптичних ваг:

$$w_{ij}(t+1) = w_{ij}(t) + r g_j x'_i \tag{1.4}$$

де w_{ij} - вага від нейрона i або від елемента вхідного сигналу i до нейрона j у момент часу t, x_i' - вихід нейрона i, r - швидкість навчання, g_j - значення похибки для нейрона j.

Якщо нейрон з номером j належить останньому прошарку, тоді

$$g_j = y_j(1-y_j)(d_j-y_j) \tag{1.5}$$

де d_j - бажаний вихід нейрона j, y_j - поточний вихід нейрона j.

Якщо нейрон з номером j належить одному з прошарків з першого по передостанній, тоді

$$g_j = x'_j(1 - x'_j)\sum_k g_k w_{jk} \tag{1.6}$$

де k пробігає всі нейрони прошарку з номером на одиницю більше, ніж у того, котрому належить нейрон j.

Тип передатної функції: сигмоїдальна. Сигмоїдальні функції є монотонно зростаючими і мають відмінні від нуля похідні по всій області визначення. Ці характеристики забезпечують правильне функціонування і навчання мережі.

Переваги. Ефективний та популярний алгоритм для вирішення численних практичних задач.

Модифікації. Модифікації алгоритму зворотного поширення зв'язані з використанням різних функцій похибки, різних процедур визначення напрямку і величини кроку.

Список використаних джерел

1.Тарік Рашид, Математика нейронних мереж, 2016.

УДК 004.932

Сінєгіна А. Д.
Дніпровський національний університет імені Олеся Гончара

Передача стилю за допомогою нейронної мережі

В області нейроної передачі стилю Гетіс [1] запровадив штучну систему, засновану на глибокій нейронній мережі, яка створює художні образи високої перцептивної якості. Натхненний силою конволюційних нейронних мереж, він вперше вивчив, як використовувати ці мережі для відтворення відомих стилів малювання на зображеннях. Представлення змісту та стилю в конволюційній нейронній мережі є сепарабельними. Тобто, ми можемо маніпулювати обома представленнями незалежно, щоб створювати нові, сприйнятливо осмислені зображення. Зображення синтезуються шляхом пошуку зображення, яке одночасно співпадає з представленням вмісту одного зображення та представленням стилю іншого. В основі методу лежить нейронна мережа VGG-19 – конволюційна нейронна мережа, яка конкурує з продуктивністю людини в загальному заданні розпізнавання візуального об'єкта. Ця модель була навчена для розпізнавання та локалізації об'єктів. У методі використовується простір ознак, наданий нормалізованою версією 16 згорткових (convolutional) та 5 агрегувальних (pooling) шарів 19-ти шарової VGG-мережі. Повнозв'язні шари взагалі не використовуються.

Дане вхідне зображення $\vec{x}$ кодується в кожному шарі CNN за допомогою фільтрових відповідей на це зображення. Шар з N_l різними фільтрами має N_l карт ознак, кожна розміром M_l, де M_l – це висота помножена на ширину карти ознак. Таким чином відповіді в шарі l можуть зберігатися в матриці $F^l \in R^{N_l \times M_l}$, де F^l_{ij} – це активація i - го фільтру на позиції j в шарі l. Нехай $\vec{p}$ та $\vec{x}$ – це початкове зображення та зображення, що згенеровано, P^l та F^l – відповідне представлення ознак в шарі l. Тоді втрата квадратичної помилки між двома представленнями ознак: $\mathcal{L}_{content}(\vec{p}, \vec{x}, l) = \frac{1}{2}\sum_{i,j}(F^l_{ij} - P^l_{ij})^2$. На вершині відповідей CNN у кожному шарі ми будуємо представлення стилю, яке обчислює кореляції між різними відгуками фільтрів, де сподівання береться по простору вхідного зображення. Ці кореляції ознак даються матрицею Грама $G^l \in R^{N_l \times N_l}$, де G^l_{ij} – це внутрішній добуток між векторизованими картами ознак i та j в шарі l: $G^l_{ij} = \sum_k F^l_{ik} F^l_{jk}$. Нехай $\vec{a}$ та $\vec{x}$ – це початкове зображення та зображення, що згенеровано, A^l та G^l – відповідні представлення стилю в шарі l. Внесок шару l в загальну втрату тоді дорівнює: $E_l = \frac{1}{4N_l^2 M_l^2}\sum_{i,j}(G^l_{ij} - A^l_{ij})^2$. Та загальна втрата стилю дорівнює: $\mathcal{L}_{style}(\vec{a}, \vec{x}) = \sum_{l=0}^{L} \omega_l E_l$, де ω_l – вагові коефіцієнти вкладу кожного шару в загальну втрату.

Щоб перенести стиль з зображення $\vec{a}$ на зображення $\vec{p}$, синтезується нове зображення, яке одночасно співпадає з представленням вмісту $\vec{p}$ та представленням стилю $\vec{a}$. Таким чином, ми спільно мінімізуємо відстань представлення ознак зображення білого шуму з представлення вмісту фотографії в одному шарі та представлення стиля зображення, визначеного на ряді шарів згорткової нейронної мережі. Функція витрат, яку ми мінімізуємо: $\mathcal{L}_{total}(\vec{p}, \vec{a}, \vec{x}) = \alpha\mathcal{L}_{content}(\vec{p}, \vec{x}) + \beta\mathcal{L}_{style}(\vec{a}, \vec{x})$, де α та β – це вагові коефіцієнти для реконструкції вмісту та стилю відповідно. Вибір $\mathcal{L}_{content}$ та $\mathcal{L}_{style}$ емпірично випливає з принципу, згідно з яким використання нижчого шару має тенденцію до збереження

ознак низького рівня (наприклад, кольорів), тоді як використання вищого шару взагалі зберігає інформацію про семантичний зміст більш високого рівня. Тому $\mathcal{L}_{style}$, як правило, обчислюється з використанням нижчих шарів, а $\mathcal{L}_{content}$ обчислюється з використанням вищих шарів.

Було розроблено програму мовою Python, в якій реалізовано метод, запропонований Гетісом. Результати були сформовані на базі мережі VGG-19 з попередньо навченими вагами ImageNet. Зображення були синтезовані шляхом співставлення представлення вмісту на шарі block5_conv2 та представлення стилю на шарах block1_conv1, block2_conv1, block3_conv1, block4_conv1, block5_conv1. В якості вагових коефіцієнтів вмісту та стилю бралися такі значення: $\alpha = 1$, $\beta = 1$, кількість ітерацій = 300. На рисунку 1 наведено зображення, яке бралося як зображення вмісту. На рисунку 2 наведено зображення, яке бралося як зображення стилю. В результаті було отримане зображення, яке наведено на рисунку 3.

Рисунок 1 – Зображення вмісту

Рисунок 2 – Зображення стилю

Рисунок 3 – Отримане зображення

Список використаних джерел

1. Gatys L. A., Ecker A. S., Bethge M. A neural algorithm of artistic style ArXiv e-prints, 2015.

УДК 004.932

Сінєгіна Ю. Д.
Дніпровський національний університет імені Олеся Гончара

Колоризація зображень за допомогою згорткової нейронної мережі

Останнім часом широко застосовуються нейронні мережі, зокрема згорткові, для вирішення проблеми колоризації зображень. Деякі з них розглядаються нижче.

Чорно-білі зображення можуть бути представлені в сітці пікселів. Кожен піксель має значення, яке відповідає його яскравості. Значення коливаються від 0 до 255, від чорного до білого. Як відомо, нейронна мережа створює зв'язок між вхідним значенням та вихідним значенням. Для задачі колоризації нейронна мережа повинна знайти риси, які пов'язують зображення у відтінками сірого з кольоровими. Таким чином, ми шукаємо ознаки, які пов'язують сітку пікселів некольорового зображення з трьома кольоровими сітки.

По-перше, треба використати алгоритм для зміни кольорового простору, від RGB до $l\alpha\beta$. Тут l означає яскравість, а α і β - кольорові спектри зелено-червоного та синьо-жовтого кольорів. Для тренування нейронної мережі використовуються кольорові зображення у просторі $l\alpha\beta$, а саме, шар зображення у відтінках сірого (l) як вхідні дані та два кольорові шари (α та β), які потрібно передбачити. Між вхідними та вихідними значеннями створюються 3x3 фільтри, які з'єднують ці значення разом, маємо згорткову нейронну мережу, у якій кожен фільтр налаштовується автоматично. Треба відобразити передбачені та реальні значення в одному інтервалі [-1,1] для їх порівняння. Для цього до передбачених значень використовується функція активації гіперболічний тангенс. Реальні значення кольорів лежать в інтервалі від -128 до 128, це інтервал за замовчуванням у колірному просторі $l\alpha\beta$. Поділяючи їх на 128, вони теж потрапляють в інтервал від -1 до 1. Це дає можливість обчислити помилку з передбачення.

Для доброї колоризації треба спочатку шукати прості шаблони: діагональну лінію, всі чорні пікселі тощо. Шукаємо той самий шаблон у кожному квадраті та видаляємо пікселі, які не збігаються. Створюється 64 нові зображення з 64 міні-фільтрів (Рис. 1). Якщо сканувати зображення знову, побачимо ті шаблони, які вже виявлені. Щоб отримати більш високий рівень розуміння зображення, треба зменшити розмір зображення наполовину. Для цього все ще є 3x3 фільтри для сканування кожного зображення. Але, поєднавши дев'ять нових пікселів із фільтрами нижчого рівня, можна виявити більш складні шаблони. Кількість фільтрів показана на рисунку 1.

Деталі шарів мережі показані у таблиці 1. В мережах колоризації для зменшення розміру зображення замість шару пулінгу використовують у шарі згортки крок (*stride*) = 2. Щоб подвоїти розмір зображення, мережа використовує шар *upsampling*.

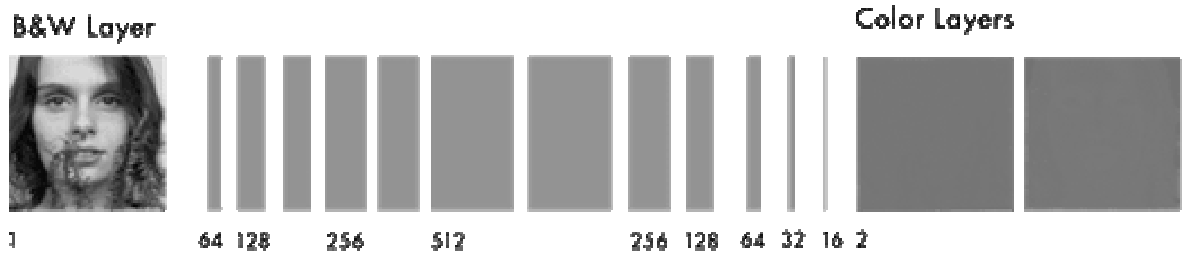


Рисунок 1 – Кількість фільтрів

Таблиця 1 – Шари нейронної мережі

Layer	Kernels	Stride
conv	64x(3x3)	1x1
conv	64x(3x3)	2x2
conv	128x(3x3)	1x1
conv	128x(3x3)	2x2
conv	256x(3x3)	1x1
conv	256x(3x3)	2x2
conv	512x(3x3)	1x1
conv	256x(3x3)	1x1
conv	128x(3x3)	1x1
conv	64x(3x3)	1x1
upsamp	-	-
conv	32x(3x3)	1x1
conv	2x(3x3)	1x1
upsamp	-	-

Для проведення навчання було обрано датасет 200 портретів різних людей. Експерименти проводились на відеокарті NVIDIA GeForce940mx 2GB протягом 2000 епох. Результати показані на рисунку 2.

Рисунок 2 – Результати колоризації

УДК 004.9

Холоша М. С., Сидорова М. Г.
Дніпровський національний університет імені Олеся Гончара

Побудова ансамблю нейронних мереж для тегування зображень

Задача тегування представляє собою підбір ключових слів (тегів), що найкраще характеризують зміст зображення. Використання згорткових нейронних мереж для цієї задачі є досить гарною практикою. Зазвичай вони складаються зі згорткових шарів, які якісно виконують пошук характерних рис зображення, та з повнозв'язних, які на основі отриманих дескрипторів, класифікують зображення.

Навчання нейронної мережі – це процес, в якому параметри нейронної мережі налаштовуються за допомогою моделювання середовища, в яке ця мережа вбудована.

Для можливості отримання якісних результатів слід застосовувати глибокі згорткові нейронні мережі (deep convolutional neural networks), які мають велику кількість нейронів та шарів. Навчання таких мереж потребує значних обчислювальних потужностей та затрат часу. За останні роки з'явилася велика кількість моделей створених і навчених професіоналами з використанням великої кількості даних і великих обчислювальних потужностей (AlexNet, VGG, Inception, ResNet тощо). Багато з цих моделей знаходяться у відкритому доступі і будь-хто може використовувати їх для вирішення своїх завдань абсолютно безкоштовно. Тому популярним є підхід transfer learning, що полягає у використанні таких моделей в основі власної архітектури.

Для рішення задачі тегування було реалізовано нейронну мережу, яка має наступну архітектуру:

- попередньо навчена модель VGG16 без повнозв'язних шарів;
- самостійно спроектована повнозв'язна модель, у якої кількість вихідних нейронів дорівнює кількості тегів.

Для навчання було зібрано 12000 зображень та 18000 відповідних їм міток. Отже, для реалізації такої модель необхідно було б навчати мережу, у якої 18000 вихідних нейронів, але для цього необхідні досить потужні обчислювальні ресурси. Тому було вирішено скоротити набір тегів до 100 найбільш популярних. Реалізувавши дану мережу, були отримані невтішні результати. А саме, час навчання такої моделі складав 24 години лише для однієї епохи. Для отримання прийнятного результату необхідно щонайменше 25 епох. Тому було вирішено модернізувати даний підхід та запропоновано наступний алгоритм:

1) розділити навчальну вибірку зображень на категорії;
2) для кожної категорії створити власну нейронну мережу;
3) навчити кожну мережу розпізнавати теги зображень лише своєї категорії;
4) створити та навчити окрему нейронну мережу, яка буде розпізнавати категорію зображення.

Тестування ансамблю нейронних мереж показало гарні результати. А саме, для навчання дрібних моделей у сукупності потрібно значно менше часу, ніж при класичному підході. Також розбиття монолітної моделі значно збільшує гнучкість навчання, адже для кожної категорії можна окремо і по-різному проводити навчання, при цьому не впливаючи на якість тегування зображень інших категорій.

Дану архітектуру можна зручно масштабувати та вдосконалювати, вводити моделі підкатегорій, досягаючи оптимального відношення кількості категорій та розміру тегуючих мереж.

УДК 004.838.2

Шуліка Я. П.
Центральноукраїнський національний технічний університет

Сучасні можливості штучного інтелекту

«Ти всього лише робот, ти не можеш написати картину чи написати пісню» - на момент виходу фільму «Я – робот» не можна було й уявити сучасні здібності штучного інтелекту. Але технології розвиваються дуже швидко і те що колись здавалося фантастикою, або про що шуткували вже давно є реальністю.

Вже є декілька штучних інтелектів, що можуть написати вам пісню. Перші розробки опублікувалися ще з 2012 роки, а на наш час є алгоритми, що можуть створювати пісню для вас в залежності від ваших уподобань, стилістики, референси і тому подібне. Можна звернутися до послуг композитора і цим композитором буде штучний інтелект.[1]

Можна сказати, що музика це не так вже й складно, там декілька нот, які можна поставити у схожих з хорошими композиціями порядках та отримати нову та хорошу пісню, але цього не вдасться сказати про штучний інтелект, що пише статті.

Тепер замість того, щоб наймати копірайтера, якщо вам потрібна велика кількість статей – ви можете найняти всього лише один штучний інтелект і він зробить, наприклад, тисячу унікальних та відповідаючих вашим вимогам статей, що зручно читаються, оптимізовані для пошукових систем. Крім того, алгоритм навіть може додавати релевантні фото та відео у статті. Ви можете читати статті і навіть не підозрювати, що ці статті писала не людина.[2]

Крім штучної музики, штучних текстів, хочеться подивитись на реальних людей, але навіть вони можуть бути штучними, створеними штучним інтелектом, як у Китаї. Це виявляється дуже вигідно для компанії новин, вони навчили алгоритм штучного інтелекту на реальних людях, що вели новини і тепер мають копію тих самих робітників, але тепер вони можуть працювати 24/7 та 365 днів на рік. Гарне рішення, але частина глядачів скаржиться на дискомфорт із-за усвідомлення того що новини, що вони дивляться веде не реальна людина.[3]

Навіть під час дозвілля, граючи в гру, можна знайти штучний інтелект, що грає краще будь-якої людини, це не дивно з шахами, чи шашками, їх не складно прорахувати, але коли штучний інтелект перемагає чемпіонів таких ігор як японська «го» чи «dota 2», то це вражає, навіть просто прорахувати кількість варіантів у таких іграх – вже доволі складно, тим паче прорахувати самі варіанти та дії в цих варіантах.[4]

Недавно з'явився штучний інтелект, що може малювати картину за вашим текстовим описам, піксель за пікселем. Не кожна людина взагалі зможе намалювати щось зрозуміле, хоча сьогодні це і не обов'язково, якщо ви хочете бути художником, є штучний інтелект, що сам зрозуміє що ви намагалися намалювати і намалює це за вас. Насправді малювання та розпізнавання картинок більш розвинута тема для штучного інтелекту, ніж може здатися на перший погляд, не дарма ж ви вводите стільки капчі на різних сайтах.[5]

Можна дивитись звернення президента і взнати, що це звернення, його міміка та жести – створені штучним інтелектом. Завдяки вченим з Вашингтонського університету людство має такий досвід.[6] Але дехто пішов далі, штучний інтелект Deepfakes навчили замінювати лиця людей на відео, її навчили цьому на роликах на youtube і тепер ви, наприклад, можете дивитись фільми і у кожному фільмі зробити головним героєм вашого улюбленого героя, основне застосування та для чого планувалася ця програма, це звичайно для того, щоб використовувати лиця улюблених акторів у порно-відео.[7]

Все ж таки штучний інтелект відкриває широкі двері для всіх індустрій, тому порно це теж один з двигунів розвитку штучного інтелекту. Набридло дивитися хентай з цензурою? При цьому ви здібний програміст? Чому б не створити тоді штучний інтелект, що буде домальовувати зображення замість цензури? Як наприклад користувач від псевдонімом deeppomf створив нейронну мережу DeepCreamPy. Вам потрібно лише обрати зображення і система сама розцензурить вам його.[8]

Також є нейронна мережа, що може покращувати якість зображення, домалювати до розмитого пікселями зображення інші пікселі таким чином, щоб отримати більш чіткий малюнок. Малюнок у дуже низькій якості може заграти новими красками так, наче б то його перемальовували у високу якість художники. [9]

Навіть релігія не пройшла повз цієї технології. Вчені-католики створили нейронну мережу з ціллю цензурити інтернет, вона повинна була одягати оголених жінок, вона частично з цим справляється, але паралельно з цим, виявилося, що нейронна мережа також може і роздягати жінок у купальних, як побічний ефект при розробці, це не планувалося розробниками, але так вийшло. [10]

Нові системи безпеки, що здавалися надійними вже скомпроментовані штучним інтелектом. Створений штучний інтелект, «The DeepMasterPrints», що може підробити ваші відпечатки пальців, для доступу до телефону, наприклад. Хоча для смартфонів успішність розпізнавання всього лише 23% але це лише початок цієї вітки технологій, в майбутньому навіть технології захисту інформації на основ сканеру сітчатки ока чи замок на днк послідовності можуть бути переможені штучним інтелектом. [11]

Те що декілька років назад вважалося фантастикою вже створено. Вже є проект по створенню виробництва роботів роботами. Можливо, ми застанемо мить коли буде існувати штучний інтелект для кожної цілі, або штучний інтелект, що буде створювати штучний інтелект для певних цілей. Коли вже нічого не залишиться, що людина робила б краще штучного інтелекту. До того часу людству потрібно відповісти на декілька складних філософських питань. Права для штучного інтелекту, що будуть робити люди, коли розвиток цивілізації і взагалі все буде оптимізовано, та чи є взагалі місце людям у такому майбутньому, навіщо штучному інтелекту взагалі люди, якщо він вже може створити сам? Може ми лише будемо заважати штучному інтелекту і він буде розглядати як вирішити це питання? Можливо це стрибок від органічного життя до силіконового? Так чи інакше – побачимо у майбутньому.

Список використаних джерел

1. *AI Music Composer[Електронний ресурс]. – Режим доступу: – https://www.ampermusic.com/.*
2. *The smartest automatic article writer ever[Електронний ресурс]. – Режим доступу: – http://www.articleforge.com/*
3. *Xinhua AI anchor [Електронний ресурс]. – Режим доступу: – https://www.youtube.com/watch?v=eB29ZVDOFfU*
4. *OpenAI at The International [Електронний ресурс]. – Режим доступу: – https://openai.com/the-international/*
5. *Автоматичне малювання[Електронний ресурс]. – Режим доступу: – https://www.autodraw.com/*
6. *Fake Obama created using AI tool [Електронний ресурс]. – Режим доступу: – https://www.bbc.com/news/av/technology-40598465/fake-obama-created-using-ai-tool-to-make-phoney-speeches*
7. *З'явилася програма, що легко змінює лиця на відео[Електронний ресурс]. – Режим доступу: – https://strana.ua/news/111210-deepfakes-nejroset-nauchili-menjat-litsa-na-videorolikakh-kak-sdelat-fejkovoe-video-s-kem-uhodno.html*
8. *Decensoring with Deep Neural Networks [Електронний ресурс]. – Режим доступу: – https://github.com/deeppomf/DeepCreamPy*
9. *Нейронна мережа, що самостійно доповнює зображення[Електронний ресурс]. – Режим доступу: – https://habr.com/post/392961/*
10. *Catholic AI bot[Електронний ресурс]. – Режим доступу: – https://www.theregister.co.uk/2018/07/20/ai_bikini_picture_painter/*
11. *Штучний інтелект навчили підроблювати відпечатки пальців [Електронний ресурс]. – Режим доступу: – https://telegraf.com.ua/tehnologii/4727538-iskusstvennyiy-intellekt-nauchili-poddelyivat-otpechatki-paltsev.html*

УДК 004.414.22

Безрук Є. А., Брусеньский В. Р., Козіна Г. Л.
Запорізький національний технічний університет

Впровадження технологііі блокчейн в торгівлю цінними паперами

За 10 років існування технології Блокчейн увага до неї не знизилася. Професійне використання блокчейна здатне привести до деяких сприятливих змін не тільки на фінансовому ринку, а й в економіці та політиці [1]. Розподілений журнал даних на основі блокчейна здатний гарантувати незмінність, цілісність і надійність будь-яких дискретних одиниць в системі, де сторони не зобов'язані довіряти один одному.

У традиційному протоколі блокчейна всі транзакції записуються в публічний реєстр і доступні для перегляду уповноваженим учасникам. Як тільки транзакція є досконалою, вона підтверджується усіма учасниками мережі і блок з параметрами цієї транзакції додається в блокчейн. Останній доданий блок містить інформацію не тільки про останню транзакції [2], а й про всі попередні, що робить практично неможливим видалення або зміну раніше доданого блоку, тоді як довелося б змінювати всі наступні.

Технологічні можливості блокчейна набагато ширші, ніж забезпечення функціонування криптовалют. На даний момент можна виділити 3 напрями розвитку технології: блокчейн 1.0, 2.0 і 3.0.

Блокчейн 1.0 являє собою криптовалюту, блокчейн 2.0 - розумні контракти і фінансові інструменти, блокчейн 3.0 - це додатки поза фінансовим сектором [1].

На будь-якому рівні використання фінансових транзакцій включає в себе сплату комісії регулюючому органу (посереднику) за підтвердження законності угоди. Обсяг коштів, зароблених на посередництві при здійсненні транзакцій, можна оцінити за доходами біржі від послуг лістингу глобальних компаній [3].

Побудова ринку фінансових інструментів на основі технології Блокчейн здатне провести надання публічного розподіленого реєстру запису транзакцій, який в ідеалі здатний створити спільну платформу для трейдингу. Таким чином, стане можливим об'єднання безлічі торгових майданчиків в єдину мережу, що дозволить прискорити і спростити проведення операцій з цінними паперами.

Блокчейн, або розподілений реєстр, пропонує інший підхід до управління даними і спільному їх використанні, який допоможе підвищити ефективність процесів в цій галузі.

Для впровадження блокчейну в систему трейдінгу цінними паперами пропонується такий алгоритм.

Беруться такі данні транзакції: номер транзакції; дата (Date); назва компаній, акції яких використовувалися (Stock); початкова вартість акції (Entry); вартість акції після закриття транзакції (Exit); прибуток (Profit); сума, яка була витрачена на придбання акцій (Entry amount); ім’я покупця (Broker name); сума, отримана після закриття транзакції (Withdrawal amount). Ці дані хешуться за допомогою алгоритму SHA256. В якості солі використовується хеш-образ попередньої транзакції.

В ролі репозиторіїв для зберігання транзакцій використовуються компанії, які продають акції.

Шляхом детального аналізу алгоритму трейдингу були виділені процеси, які можуть бути успішно переведені на блокчейн. Перш за все, це процес задоволення заявки брокером. При впровадженні розподіленого реєстру брокер буде реєструвати заявки на купівлю-продаж цифрових цінних паперів в новій інформаційній системі, де основні алгоритми обробки будуть виконуватися кодом розумного контракту. Аналогічно, переклад книги замовлень на блокчейн також дозволить перенести

виконання стандартних операцій в область розумних контрактів.

Завдяки технологічним характеристикам розумних контрактів, а саме здатності безпечно отримувати, зберігати і відправляти інформацію і активи на основі заздалегідь визначених правил і умов, вони можуть допомогти децентралізувати модель довіри, скоротити потребу в дорогих посередників, прискорити час врегулювання і підвищити прозорість угод, автоматизувати процеси, знизити ризики і стати базою для багатьох видів операцій [4].

Таблиця 1 – Дані використовувані для хешування

№	Date	Stock	Entry	Exit	Profit, %	Entry amount	Broker name	Withdrawal amount
0	2/14/18	UPRO	$132.92	$141.09	6.15	284,65	Nill	305,15
1	11/29/17	SDY	$87.76	$94.97	8.22	162,58	Jack	175,94
2	9/14/17	GLD	$117.05	$125.67	7.37	356,25	Taya	382,5
3	08/07/17	USO	$9.1	$10.03	10.22	584,62	Erick	644,36
4	01/04/17	INCT	$0.69	$0.31	-54.6	32,23	Bob	17,6

Таблиця 2 – Хеш-образи транзакцій

№	Block hash
0	37334C65CD01EB8C2FB0895C26AEFBB636AD789EA524AB7B72EB5BE3A0071FA3
1	135D7787610FB93219159DA6D9AFA32349CDC4AD2EE60C13609DE047305E783B
2	7B823B1CDF8AFE5CC286D00BCAC43F7B34DD181EA1A85D069D0D45EE52490029
3	13680CDD53A3370E5BD4CD833BBF9DDB6CEA9FBE91477EF218B552758BDEE856
4	77E04C4411EF1627FE07A85F758B02C5F1DE62DE864851B360ED97CF6A23BABA

Таблиця 3 – Хеш-образи попередніх транзакцій

№	Previous block hash
0	
1	37334C65CD01EB8C2FB0895C26AEFBB636AD789EA524AB7B72EB5BE3A0071FA3
2	135D7787610FB93219159DA6D9AFA32349CDC4AD2EE60C13609DE047305E783B
3	7B823B1CDF8AFE5CC286D00BCAC43F7B34DD181EA1A85D069D0D45EE52490029
4	13680CDD53A3370E5BD4CD833BBF9DDB6CEA9FBE91477EF218B552758BDEE856

Список використаних джерел

1. *Daniel Ben-Ami. Securities Services: Blockchain [Електронний ресурс]. — Режим доступу:https://www.ipe.com/reports/special-reports/securities-services/securities-services-blockchain-a-beginners-guide/10014058.article*
2. *Іполітов В. А. Світовий фондовий ринок: історія розвитку та сучасний стан // Зовнішньоекономічний вісник. - 2006. № 3. - С. 18-31.*
3. *Teweles R. J., Bradley E.S., Teweles T.M. The Stock Market. - 6th Edition. - John Willey & Sons Inc., 1992. // Фондовий ринок. - 6-е вид. - М .: ИНФРА-М, 2000. - 648 с.*
4. *CB Insights: блокчейн і цінні папери [Електронний ресурс]. — Режим доступу: https://bloomchain.ru/blockchain-fintech/blokchejn-i-tsennye-bumagi/*

УДК 004.056.53

Демидов З. Г.
Харківський національний університет внутрішніх справ

Big data: застосування та можливості

Великі дані (англ. Big data) - серія підходів, інструментів і методів обробки структурованих і неструктурованих даних величезних обсягів і значного різноманіття для отримання зрозумілих для людини результатів, ефективних в умовах безперервного приросту, розподілу по численних вузлах обчислювальної мережі, що сформувалися в кінці 2000-х років, альтернативних традиційним системам управління базами даних і рішень класу Business Intelligence. [1]

Таким чином під Big Data ми розуміємо не якийсь конкретний обсяг даних і навіть не самі дані, а методи їх обробки, які дозволяють розподілено обробляти інформацію. Ці методи можна застосувати, як до величезних масивів даних (таких, як зміст усіх сторінок в інтернеті), так і до маленьких (таких, як вміст цієї статті).

Наведемо кілька прикладів того, що може бути джерелом даних, для яких необхідні методи роботи з великими даними: список поведінки користувачів в інтернеті, GPS-сигнали від автомобілів для транспортної компанії, дані, що знімаються з датчиків у великому адронному колайдері, оцифровані книги в Державній Бібліотеці, інформація про транзакції всіх клієнтів банку. [2]

Виходячи з визначення Big Data, можна сформулювати основні принципи роботи з такими даними. 1) Горизонтальна масштабованість. Оскільки даних може бути як завгодно багато - будь-яка система, яка має на увазі обробку великих даних, повинна бути розширюваною. У 2 рази зріс обсяг даних - в 2 рази збільшили кількість заліза в кластері і все продовжило працювати. 2) Відмовостійкість. Принцип горизонтальної масштабованості має на увазі, що машин в кластері може бути багато. Це означає, що частина цих машин буде гарантовано виходити з ладу. Методи роботи з великими даними повинні враховувати можливість таких збоїв і переживати їх без будь-яких значущих наслідків. 3) Локальність даних. У великих розподілених системах дані розподілені по великій кількості машин. Якщо дані фізично знаходяться на одному сервері, а обробляються на іншому - витрати на передачу даних можуть перевищити витрати на саму обробку. Тому одним з найважливіших принципів проектування BigData-рішень є принцип локальності даних - по можливості обробляємо дані на тій же машині, на якій їх зберігаємо.

Ідея полягає в тому, щоб «згодувати» комп'ютеру великий обсяг даних і змусити його шукати типові алгоритми, які не здатна побачити людина, або приймати рішення на основі відсотка ймовірності в тому масштабі, з яким чудово справляється людина, але який до цих пір не був доступний для машин, або, можливо, одного разу - в такому масштабі, з яким людина не впорається ніколи.

Величезні обсяги даних обробляються для того, щоб людина могла отримати конкретні і потрібні їй результати для їх подальшого ефективного застосування. Фактично, Big data - це вирішення проблем і альтернатива традиційним системам управління даними.

Важливо зрозуміти, що більше даних допомагають нам не тільки побачити більше в самому розглядаємому, а й побачити нове, побачити краще, по-іншому.

Аналіз великих даних дозволяє побачити приховані закономірності, непомітні обмеженому людському сприйняттю. Це дає безпрецедентні можливості оптимізації всіх сфер нашого життя: державного управління, медицини, телекомунікацій, фінансів, транспорту, виробництва і так далі.

Список використаних джерел

1. https://ru.wikipedia.org/wiki/Большие_данные
2. https://habr.com/company/dca/blog/267361

УДК 004.94

Дрєєва Г. М.
Центральноукраїнський національний технічний університет

Імітаційне генерування фрактального трафіку за допомогою GERT моделі

Вступ. Математичні закономірності в фізичних та інформаційних процесах описують основні закони, за якими можна передбачити низку явищ та на цих прогнозах створювати системи керування процесами з оптимізацією бажаних критеріїв. Розширення математичного апарату дозволило значно розширити можливості вираження законів та передбачення їх наслідків. На прикладі застосування інтегрального до утворення тріщин перехід до неперервності призводить до виникнення нескінченності напруженості матеріалу в точці росту тріщини (рис. 1). Фізично таке не є можливим, причиною цього є порушення закону Юнга при значних деформаціях та дискретна природа речовин – речовина складається з дискретних часток і інтегральне числення є по факту наближенням до реальності і використовується лише з причин математичного спрощення моделі фізичних процесів [1].

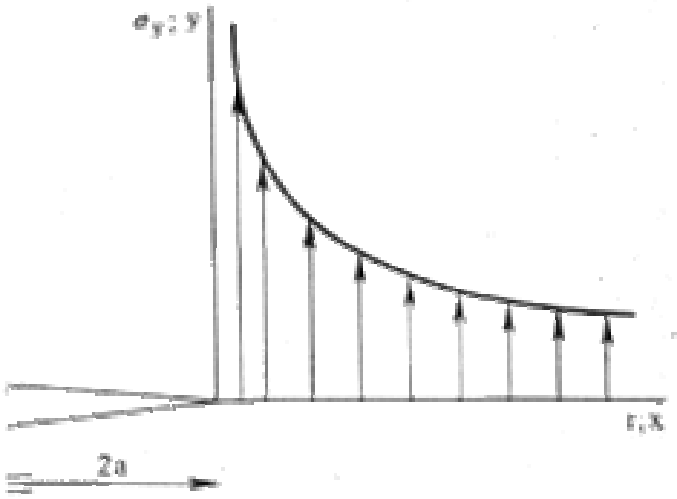


Рисунок 1 – Графік модуля напруженості біля точки росту тріщини [1]

Для вирішення питання застосовності переходу до неперервного моделювання реальних процесів звертаються до експериментів та спостережень. На жаль експеримент в реальних умовах буває провести не просто, можливо експеримент вимагає значну кількість часу або грошей або інших ресурсів. Тому кожна математична модель проходить перевірку імітаційним моделюванням, і якщо результати відповідають величинам які мають реальні системи, модель вважається відповідною дійсності з певними допусками на похибки. Особливо важливо адекватно оцінити математичну модель побудовану на ймовірнісних процесах, тут перехід від неперервного або від дискретного, як і в попередньому прикладі, може мати суттєве значення.

В системах масового обслуговування які є моделями процесів в комп'ютерних телекомунікаційних системах та мережах використовуються моделі фрактального вхідного трафіку, який імітується на основі розподілу Парето. При розподілі Парето випадкова величина може мати нескінченну дисперсію, що і ставиться як основна особливість випадкового трафіку. Однак в такому випадку ігнорується обмеженість

пропускної спроможності каналів комунікації, що в більшості випадків є допустимим. Тому ставиться задача оцінювання меж застосовності такої моделі та створення моделі з усіченим розподілом Парето, яке б не мало вказаного обмеження.

Класично розподіл щільності ймовірності Парето представлено аналітично наступним чином:

$$f_X(x) = \begin{cases} \dfrac{k \cdot x_m^k}{x^{k+1}}, x \geq x_m \\ 0, x < x_m \end{cases},$$

де x – випадкова величина; x_m>0, k>0 – параметри розподілу; $kx_m/(k\text{-}1)$ – математичне очікування при k>1. Для цього розподілу дисперсія при 1<k<2 прямує до нескінченності.

В реалізаціях моделювання систем масового обслуговування з фракталоподібним трафіком використовується генератори запитів на обслуговування за разподілом Парето, при цьому для побудов інтерполяційних формул змін показників від завантаженості системи використовувалися обмеження на пропускну спроможність системи подачі заявок [2]. Але обмеження трафіку призводило до втрати фрактальності трафіку, бо для будь-якого розподілу з обмеженою дисперсією, генерований трафік не є фрактальним, що зменшує відповідність дійсності проведеного моделювання.

Більш перспективним методом генерування фракталоподібного дискретного в часі трафіку в є використання контекстних методів [3] в результаті якого можна отримати трафік, який володіє властивостями фрактальними властивостями. Для генерування трафіку використовується GERT модель представлена на рис. 2.

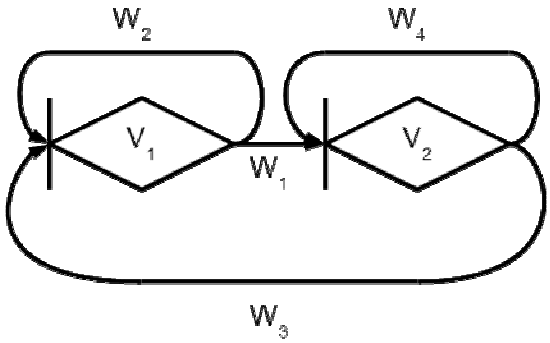


Рисунок 2 – GERT-модель генератора фракталоподібного трафіку

На рис. 3 використано позначення V_1, V_2 як перебування системи в стані генерування трафіку як процес Пуансона, один з яких має інтенсивність близьку до нульової; W_i – позначає функцію ймовірності переходу системи в інший стан, при цьому $W_1+W_2=1$ та $W_3+W_4=1$ – достовірні події.

Моделювання трафіку проводилося серіями по 1000 подій. При цьому інтенсивність потоку була обрана на рівні 0,5. Кожен дискретний момент часу модель давала значення 1 при наявності на виході інформаційного пакету (заявки на обслуговування) та 0 при відсутності. Згідно класичній теорії ймовірності, незалежно від фрактальної розмірності трафіку, математичне сподівання складало 0,5 а дисперсія 0,25. Тобто, при симетричній системі зображеній на рис. 3, стан системи є рівноймовірним. Для двох процесів було змінено ймовірність змінити стан p, для унаочнення результатів в наведеній статті виносяться крайні результати при p=0,05

(рис. 3) та при p=0,95 (рис. 5). Таким чином до системи було додано залежність від попередніх станів. Результати моделювання представлено на рис. 3-6.

Персистентність при порівняно малих значеннях ймовірності зміни стану системи є очевидною, якщо згадати, що розмах телеграфного сигналу завжди є одиничним, а локальне середнє квадратичне відхилення змінюється в широких межах. Така форма поведінки характерна для персистентного числового ряду з високим коефіцієнтом Херста H>0,5.

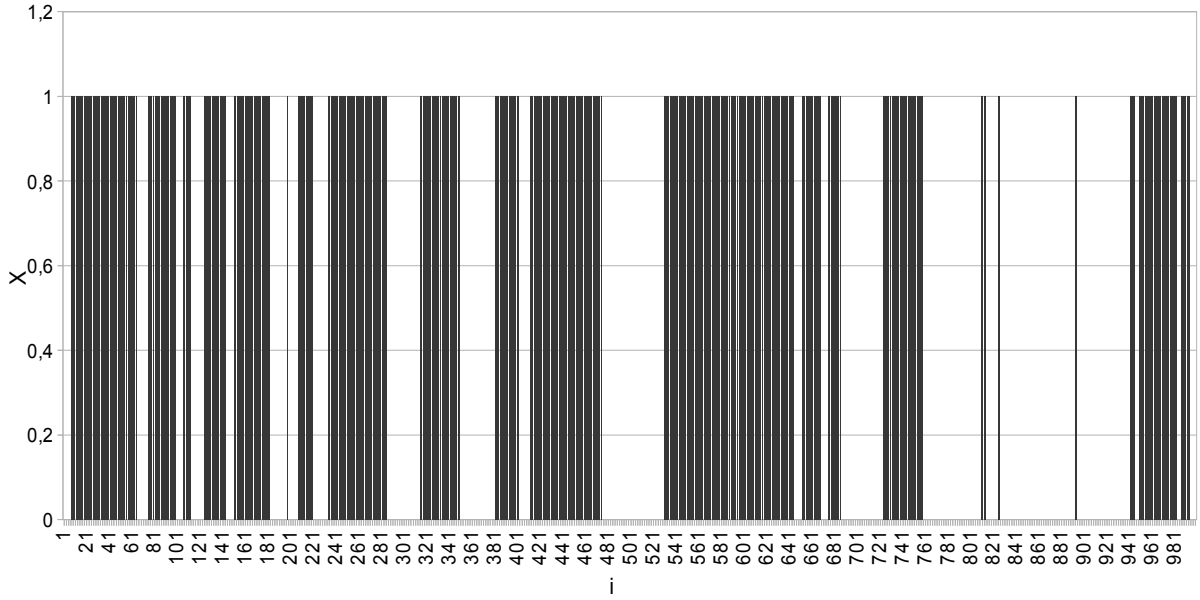


Рисунок 3 – Дискретний телеграфний сигнал з ймовірністю зміни стану p=0,05

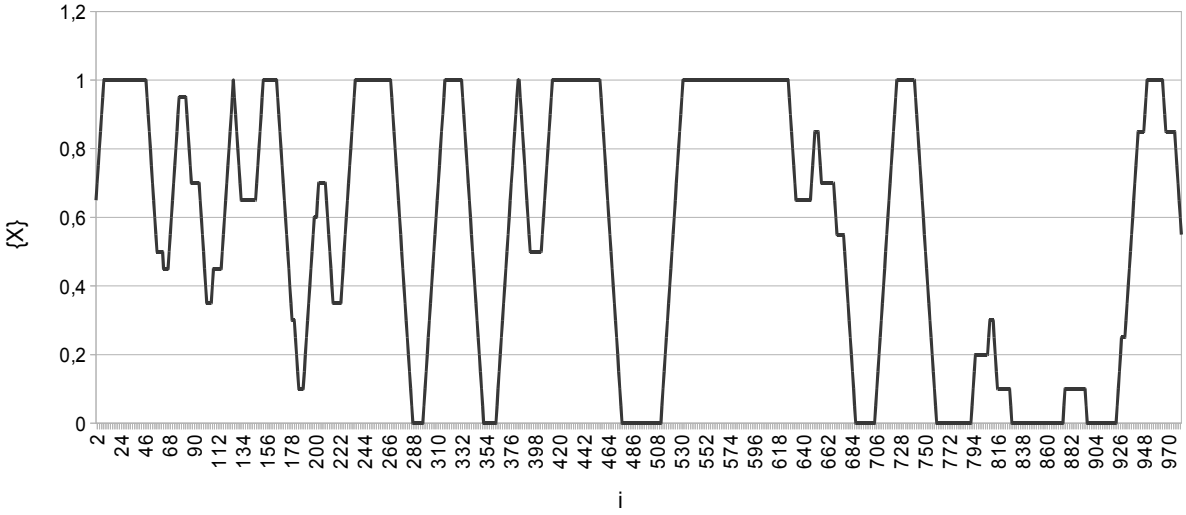


Рисунок 4 – Усереднення по 20-ти значень дискретного телеграфного сигналу з ймовірністю зміни стану p=0,05

В протилежність розглянутого процесу, висока ймовірність змін стану системи формує знижену ймовірність довгих серій з нульовим або одиничним значенням (рис. 6). При цьому усереднення по двадцятьом елементам (рис. 7) показує майже прямий

графік навколо середньої інтенсивності трафіку. Цей процес є антиперсистентним і відповідає низьким значенням критерію Херста H<0,5.

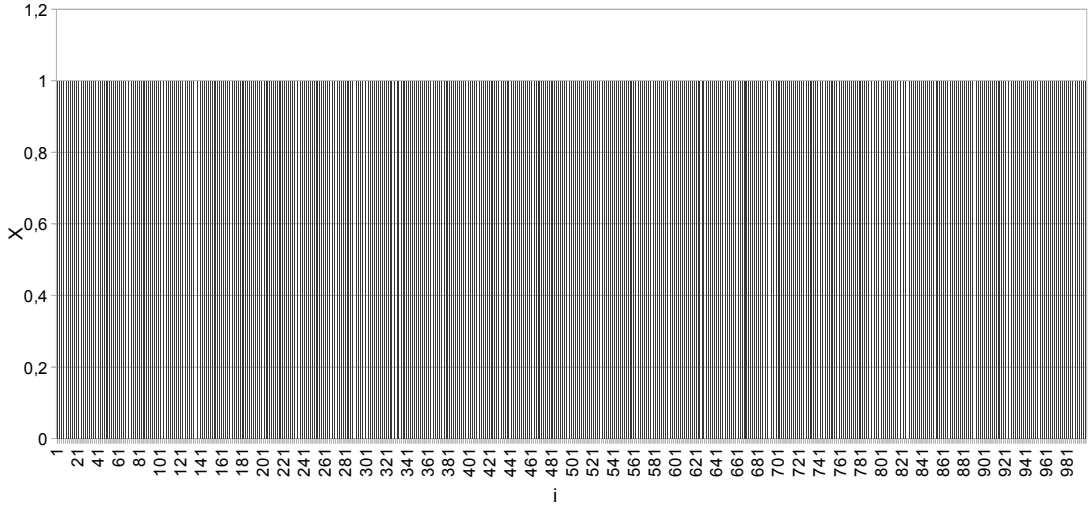


Рисунок 5 – Дискретний телеграфний сигнал з ймовірністю зміни стану p=0,95

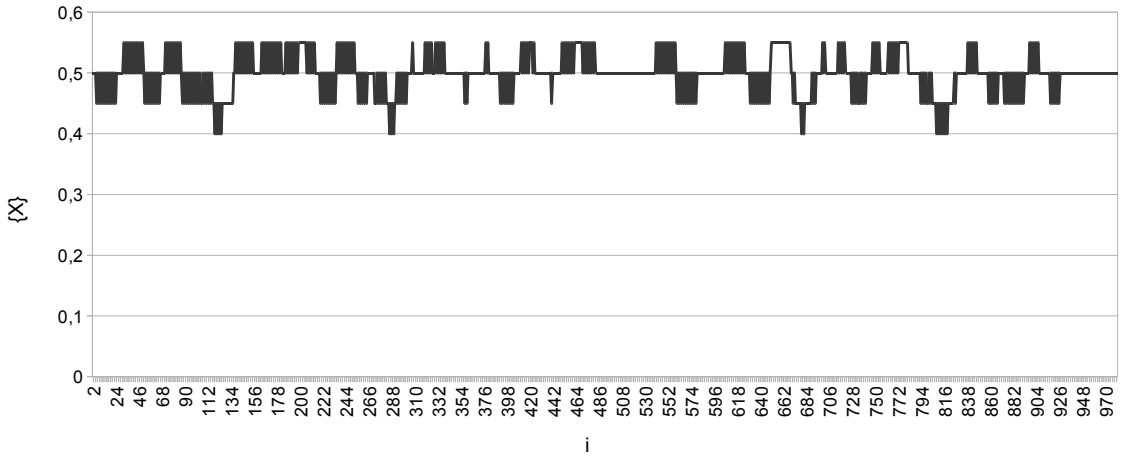


Рисунок 6 – Усереднення по 20-ти значень дискретного телеграфного сигналу з ймовірністю зміни стану p=0,95

Висновок. В результаті переходу до GERT моделі генерування трафіку вдалося реалізувати генератор фракталоподібного трафіку з більш гнучкими параметрами.

Список використаних джерел

1. *Броек Д. Основы механики разрушения./ Д. Броек // Москва. Высшая школа. 1980. 368 с. Перевод Дорофеева Виктора Ивановича (Broek D. Elementary engineering fracture mechanics, Лейден, 1974).*
2. *Ушанев К.В. Имитационные модели системы массового обслуживания типа Pa/M/1, H2/M/1 и исследование на их основе качества обслуживания трафика со сложной структурой/ К.В. Ушанев // Системы управления, связи и безопасности. №4, 2015. С. 217-251*
3. *Добровольский Е.В., Нечипорук О.Л Моделирование сетевого трафика с использованием контекстных методов / Е.В. Добровольский, О.Л Нечипорук // Наукові праці ОНАЗ ім. О.С. Попова, 2005, № 1. С. 24-32*
4. *Семенов С.Г. Математическая модель мультисервисного канала связи на основе экспоненциальной GERT-сети / С.Г. Семенов, Є.В. Мелешко, Я.В. Ілюшко // Системи озброєння і військова техніка. – Х.: ХУПС, 2011. – № 3(27). – С. 64-67.*

УДК 621.391

Коваленко Д. О.
Харківський національний економічний університет імені Семена Кузнеця

Розробка програмного забезпечення для веб-ресурсу “Планувальник навантаження викладачів ХНЕУ імені Семена Кузнеця”

У сучасному суспільстві освіта стала однією з найбільш великих сфер людської діяльності. У ній зайнято понад мільярд учнів і майже 50 млн. педагогів. Помітно підвищилася соціальна роль освіти: від її спрямованості та ефективності сьогодні багато в чому залежать перспективи розвитку людства. В останнє десятиліття світ змінює своє ставлення до всіх видів освіти. Освіта, особливо вища, розглядається як головний, провідний фактор соціального і економічного прогресу. Важливу роль у підвищення рівня освіти у Харківському національному економічному університеті імені Семена Кузнеця відіграє планування роботи професорсько-викладацького складу.

Саме при плануванні визначається обсяг різних видів робіт, що виконуються кожним викладачем, та встановлюється в залежності від характеру контингенту студентів, необхідності його участі в навчальній, науковій, методичній та організаційно-виховній роботі, а також з урахуванням індивідуальних можливостей викладача [3].

Основним документом, що визначає обсяг і види робіт кожного викладача, є індивідуальний план, який складається на поточний навчальний рік до якого вноситься запланована йому навчальна, навчально-методична, науково-дослідна та організаційно-виховна робота, підвищення кваліфікації [1]. Створюване програмне забезпечення призначене для планування навантаження викладачів кафедри [2]. Основними функціями даного додатку є: створення індивідуального плану для кожного викладача; додавання, редагування та видалення інформації в цих індивідуальних планах; збереження заповнених індивідуальних планів у базі даних.

Перевагою для Харківського національного економічного університету імені Семена Кузнеця є те, що цей додаток побудований на підставі документу «Індивідуальний план роботи викладача та її облік». Створення додатку буде вестися на основі web-технології ASP.NET Core [4], з використанням Entity Framework 6 Code First [5], через те, що веб-ресурси дуже універсальні і практичні в користуванні. Веб-додатки полегшують організацію зберігання даних. Для користування веб-додатками необхідні лише комп'ютер з браузером і з'єднання з Інтернет. Для оновлення веб-додатку, його необхідно оновити тільки на сервері і усі відразу зможуть працювати з новою версією. А ASP.NET Core пропонує швидку розробку та управління веб-додатками, дозволяє легко вирішувати рутинні завдання веб-програміста та має підтримку баз даних MS SQL. Таким чином розробка даного програмного забезпечення дозволить підвищити ефективність роботи та зменшити трудовитрати викладачів, та забезпечить вирішення різних задач за допомогою «без паперової» технології.

Список використаних джерел

1. *Про вищу освіту / Закон України від 17.01.2002 р. № 2984 – III (зі змінами та доповненнями), 2002 р.*
2. *Положення про організацію навчального процесу у ВНЗ МОН України / Наказ Міністерства освіти України № 161 від 02.06.1993 р.*
3. *Норми часу для планування і обліку навчальної роботи та переліки основних видів методичної, наукової й організаційної роботи педагогічних і науково-педагогічних працівників ВНЗ / наказ Міністерства освіти України №450 від 07.08.02 р.*
4. *Get Started with ASP.NET Core and Entity Framework 6 [Electronic resource]. – Access mode: https://docs.microsoft.com/en-us/aspnet/core/data/entity-framework-6?view=aspnetcore-2.1.*
5. *Entity Framework 6 [Electronic resource]. – Access mode: https://docs.microsoft.com/en-us/ef/ef6/.*

УДК 004.586

Коваль В. О.
Центральноукраїнський національний технічний університет

Переваги та недоліки клієнт-серверної архітектури

Модель клієнт-сервер - це розподілена структура програми, яка розділяє завдання або навантаження між постачальниками ресурсу, серверами та споживачами тобто клієнтами. Хост сервер запускає одну або декілька серверних програм, які розподіляють свої ресурси з клієнтами. Клієнт не надає ніякого ресурсу, але запитує вміст сервера або службову функцію. Тому клієнти ініціюють сеанс зв'язку з серверами, що очікують на вхідні запити. Прикладами комп'ютерних програм, що використовують модель клієнт-сервер, є електронна пошта, мережевий друк та всесвітня павутина. Організації часто шукають можливості для підтримки послуг та якісної конкуренції. Розгортання клієнт-серверного обчислення в організації ефективно підвищить продуктивність завдяки використанню рентабельного користувальницького інтерфейсу, масового підключення та надійних служб додатків.

Основними перевагами архітектури клієнт-сервер є: - Покращений обмін даними: дані зберігаються в стандартних бізнес-процесах, а маніпуляції на сервері доступні клієнтам за авторизованим доступом; - Інтеграція послуг: кожен клієнт має можливість отримати доступ до корпоративної інформації за допомогою настільного інтерфейсу; - Спільні ресурси серед різних платформ: прикладна програма, що використовується для моделі клієнт-сервер, будується незалежно від апаратної платформи відповідного програмного забезпечення, що забезпечує відкрите обчислювальне середовище; - Можливості обробки даних незважаючи на розташування: користувачі клієнт-сервер можуть безпосередньо входити до системи незалежно від місця розташування; - Легке обслуговування: архітектура клієнт-сервер - це розподілена модель, що представляє розподілені обов'язки між комп'ютерами, інтегрованими в мережу, тому легко замінити, відновити, оновити та перемістити сервер, поки клієнт залишається незмінним; - Безпека: сервери краще контролюють доступ та ресурси системи, щоб забезпечити доступ до неї або маніпулювання ними лише уповноваженим клієнтам.

Разом з тим архітектура клієнт-сервер має і ряд недоліків: -Перевантажені сервери: коли часто зустрічаються одночасно запити клієнтів, сервер серйозно перевантажений, що спричиняє затори; - Вплив централізованої архітектури: якщо критичний сервер не працює, клієнтські запити не виконуються. Отже, клієнт-сервер не має надійності хорошої мережі.

Процеси клієнта і сервера незалежні один від одного. Відповідно до ступеня поділу процесів між клієнтом і сервером вони вважаються слабкими (тонкими) або сильними (товстими). Слабкий клієнт виконує мінімум обробки на стороні клієнта, сильний бере на себе відносно велику частину обробки даних. Сильний сервер несе основне навантаження по обробці даних, навантаження на слабкий сервер відносно невелике. Взаємодія клієнтського і серверного процесів виконується за допомогою програмного забезпечення передачі даних. Це програмне забезпечення зазвичай прив'язане до мережі. Всі клієнтські запити і відповіді сервера передаються по мережі в формі повідомлень, в яких містяться керуюча інформація і дані. Взагалі мережі на базі серверів мають кращі характеристики та більш високу надійність. Сервер володіє головними ресурсами мережі, до яких звертаються інші робочі станції.

Список використаних джерел

1. Arhitektura-klient-server [електронний ресурс]. – Режим доступу : https://www.docsity.com/ru/arhitektura-klient-server/1074860
2. Client-server_model [електронний ресурс]. – Режим доступу: https://techterms.com/definition/client-server_model
3. Client-server-architecture [електронний ресурс]. – Режим доступу: https://www.britannica.com/technology/client-server-architecture

УДК 004.715
Коваль В. О., Конопліцька-Слободенюк О. К.
Центральноукраїнський національний технічний університет

Переваги та недоліки мережевих топологій

Топології мережі описують способи, якими пов'язані елементи мережі. Вони описують фізичне та логічне розташування вузлів мережі. Розглянемо переваги, які пропонують різні топології мережі та їх недоліки.

Топологія Шина

Переваги:

Це найкраще підходить для невеликих мереж.

Це легко налаштувати, обробляти та реалізувати.

Це коштує набагато менше.

Недоліки:

Ізоляція несправностей у вузлах мережі нелегко.

Це підходить для мереж з низьким рівнем трафіку. Високий трафік збільшує навантаження на шину, а ефективність мережі зменшується.

Довжина кабелю обмежена. Це обмежує кількість вузлів мережі, які можуть бути підключені.

Ця топологія мережі може добре працювати лише для обмеженої кількості вузлів. Коли кількість пристроїв, підключених до шини, збільшується, ефективність знижується.

Це сильно залежить від центральної шини. Помилка в шині призводить до збою мережі.

Кожен пристрій у мережі "бачить" всі передані дані, що становить ризик для безпеки.

Топологія Кільце

Переваги:

У цій топології кожен вузол має можливість передавати дані. Таким чином, це дуже організована мережева топологія.

Додавання або видалення вузлів мережі є простим, оскільки процес вимагає змінення лише двох з'єднань.

Трафік односпрямований, а передача даних - висока швидкість.

Дані, що передаються між двома вузлами, проходять через всі проміжні вузли. Центральний сервер не потрібен для керування цією топологією.

У порівнянні з автобусом кільце краще при навантаженні.

Конфігурація полегшує виявлення несправностей у вузлах мережі.

Це менш дорого, ніж топологія зірки.

Недоліки:

Дані, передані від одного вузла до іншого, повинні проходити через всі проміжні вузли. Це робить передачу повільною порівняно з топологією зірки. Швидкість передачі зменшується з збільшенням кількості вузлів.

Відмова одного вузла в мережі може призвести до виходу з ладу всієї мережі.

Рух або зміни, внесені в вузли мережі, впливають на продуктивність всієї мережі.

Існує велика залежність від дроту, що з'єднує мережеві вузли на кільці.

Топологія Зірка

Переваги:

Оскільки аналіз трафіку простий, топологія створює менший ризик для безпеки.

Додавання або видалення вузлів мережі є простим, і це може бути зроблено, не впливаючи на всю мережу.

Завдяки своєму централізованому характеру топологія забезпечує простоту експлуатації.

Це також забезпечує ізоляцію кожного пристрою в мережі.

Через централізований характер, легко виявити несправності мережевих пристроїв.

Пакети даних не повинні проходити через багато вузлів, як у випадку кільцевої мережі. Таким чином, за рахунок використання центрального вузла високої потужності, завантаження трафіку може здійснюватися досить пристойно.

Недоліки

Крім того, кількість вузлів, які можна додати, залежить від потужності центрального вузла.

Робота в мережі залежить від функціонування центрального концентратора. Отже, несправність центрального вузла призводить до провалу всієї мережі.

Вартість установки досить висока.

Топологія мережі означає фізичну або логічну компонування мережі. Він визначає спосіб, яким розміщуються різні вузли та з'єднані один з одним. З іншого боку, топологія мережі може описувати, як дані передаються між цими вузлами.

Топологія мережі є структурою мережі і може бути зображена фізично або логічно. Це додаток теорії графів, в якій комунікаційні пристрої моделюються як вузли, а з'єднання між пристроями моделюються як посилання або лінії між вузлами. Фізична топологія - це розміщення різних компонентів мережі (наприклад, місцезнаходження пристрою та встановлення кабелю), тоді як логічна топологія показує, як відбувається передача даних всередині мережі. Відстані між вузлами, фізичні взаємозв'язки, швидкості передачі або типи сигналів можуть відрізнятися між двома різними мережами, однак їх топології можуть бути однаковими. Фізична топологія мережі є особливою проблемою фізичного шару моделі OSI.

Топологічна структура впливає на пропускну здатність і вартість локальної мережі. Кожна топологія мережі накладає ряд певних умов. Наприклад, вона може диктувати не тільки тип кабелю, а й спосіб його прокладки.

Топології комп’ютерних мереж можна подати за допомогою графів. Множина таких топологій дуже потужна , тому в цій роботі було зосереджено увагу перш за все на тих , які є найуживанішими в реальному житті. Для більшості комп’ютерних мереж застосовуються досить прості типи з'єднань на зразок шини, зірки, кільця або їх комбінацій

Список використаних джерел

1. *Компютерні мережі [електронний ресурс]. – Режим доступу : http://comp-net.at.ua/index/topologija_komp_39_juternikh_merezh/0-6*
2. *Topologiya-kompyuternih-merezh [електронний ресурс]. – Режим доступу: https://studopedia.com.ua/1_190430_topologiya-kompyuternih-merezh.html*
3. *klasifkacya-kompyuternih-merezh-topologyi [електронний ресурс]. – Режим доступу: http://poradu.pp.ua/tehnka-tehnologyi/18217-topologya-kompyuternih-merezh-klasifkacya-kompyuternih-merezh-topologyi.html*
4. *Chap5 [електронний ресурс]. – Режим доступу: https://fcit.usf.edu/network/chap5/chap5.htm*
5. *Connects-computer-networks-in-organizations.[електронний ресурс]. – Режим доступу: https://study.com/academy/lesson/how-star-topology-connects-computer-networks-in-organizations.html*

УДК 004.4

Константинова Л. В., Константинова А. А.
Центральноукраїнський національний технічний університет

Дослідження засобів для кросплатформеної розробки мобільних додатків

Розвиток мобільних додатків став обов'язковим для успіху підприємств в наші дні. Подальше зростання кількості смартфонів надає компаніям унікальну можливість підключатися до потенційних клієнтів через мобільні додатки. За останні кілька років популярність кросплатформених інструментів для розробки мобільних додатків значно розширилася. І тому на разі дослідження засобів для кросплатформеної розробки мобільних додатків є актуальним [1].

Завдяки повсюдному розвитку мобільних пристроїв на різних платформах (Android, iOS, Windows Phone та інших) кросплатформені рішення є найбільш перспективним етапом у розвитку технологій розробки мобільних додатків. Найвищі позиції за кількістю реалізованих програмних продуктів, а також кількістю розробників займають технології Appcelerator Titanium, Kony Platform, Adobe PhoneGap. Також важливим є той факт, що дані рішення є повністю відкритими і добре документованими [2].

Згідно з дослідженнями більша частина підприємств вже застосовує кросплатформену розробку. В найближчі роки кросплатформені засоби розробки мобільних додатків будуть стрімко розвиватись. Найпопулярнішими вважаються засоби Xamarin, Adobe, Ionic, Sencha, Appcelerator, RhoMobile, NativeScript, MonoCross, Codename One, Convertigo [1].

Xamarin - це кросплатформений інструмент для розробки додатків, який пропонує функції, такі як можливість додавати компоненти безпосередньо з інтерфейсу, власний доступ до API, інтеграцію з внутрішніми компонентами і інтерфейси форм для сумісного застосування коду. Він дозволяє створювати власні додатки для декількох платформ з єдиною загальною базою даних C#. Крім того, розробники мають можливість застосовувати ті ж API, мову та середовище IDE.

Adobe пропонує PhoneGap Build і PhoneGap (рішення з відкритим вихідним кодом на основі Apache Cordova). Розроблені додатки можуть отримати доступ до власних специфічних функцій пристрою на різних платформах пристроїв, використовуючи Cordova, набір API-інтерфейсів з відкритим вихідним кодом. Завдяки кросплатформеним плагінам і API-інтерфейсам Cordova у розробників є можливість створювати і кодувати додатки з використанням Java-мов - HTML5 та CSS3. Використовуючи Cordova, можливо створювати додаток з одною кодовою базою.

Ionic - це SDK з відкритим вихідним кодом, який поставляється зі стандартними компонентами JavaScript і CSS. Це допомагає розробникам створювати кросплатформені мобільні додатки з використанням веб-технологій, таких як SASS, HTML5 і CSS. Ionic framework поставляється з більш ніж 120 вбудованими функціями пристрою, включаючи Fingerprint Auth, HealthKit і Bluetooth. Він також має розширення TypeScript і плагіни Cordova / PhoneGap.

Sencha Touch – це заснована на MVC платформа JavaScript, сумісна з усіма новітніми версіями iOS, Android і Blackberry. Можливе використання Sencha для розробки додатків в HTML5, які можна перевести в кросплатформені додатки за допомогою PhoneGap.

Appcelerator пропонує одну кодову базу JavaScript для своїх додатків. Він підтримує мобільну аналітику в реальному часі і може використовуватися для

створення Android, iOS, браузерів HTML5 і додатків Windows. Також він підтримує більше 5000 пристроїв і середовище MVC Alloy, засноване на Eclipse IDE Studio і OS API.

Програми, написані на RhoMobile Suite, працюють на Android, iOS і Windows. Цей інструмент складається з широкого набору API, вбудованого шаблону MVC, інтегрованої синхронізації даних, Object Relational Mapper для додатків з інтенсивним використанням даних, RhoGallery, RhoConnect, RhoStudio, RhoElements і Rhodes. Послуги з розробки додатків з використанням RhoMobile надаються в хмарі і включають в себе синхронізацію, розміщену збірку і управління додатками.

NativeScript підтримує інтеграцію з Visual Studio Code і дозволяє створювати кросплатформені власні мобільні додатки з одної кодової бази JavaScript. Також надається розробникам прямий доступ до кожного компоненту з Angular, TypeScript або JavaScript і API власної платформи. Структура і стиль кодування додатків NativeScript нагадують веб-додатки на основі HTML.

MonoCross - це кросплатформений засіб для розробки мобільних додатків з відкритим вихідним кодом, який дозволяє створювати привабливі програми на телефонах з підтримкою Android, iPhone, iPad, Windows і Webkit. MonoCross використовує середовище Mono, C # і Microsoft.NET, і не вимагає знань низькорівневих розробок всіх платформ.

Codename One забезпечує швидку розробку додатків і глибоку інтеграцію з власною платформою. Має гнучку архітектуру, дозволяє призначеному для користувача інтерфейсу безперешкодно працювати на всіх платформах. Код написаний на Java, і додаток перевірено і протестовано за допомогою інструментів автоматизації тестування і симуляторів Codename One. Ця структура підтримує популярні IDE, такі як IntelliJ IDEA, Eclipse і NetBeans.

Convertigo дозволяє розробляти мобільні додатки один раз і працювати на iOS, Android і Windows. Ця платформа пропонує чотири рішення: Convertigo Server, Convertigo SDK, Convertigo Studio і Convertigo Cloud. Вона поставляється з різними коннекторами, такими як веб-служби або бази даних SQL для підключення до корпоративних даних.

Кросплатформена розробка мобільних додатків грунтується на популярных мовах програмування, таких як JavaScript, CSS та HTML. Кросплатформені інструменти для розробки мобільних додатків доволі універсальні та дозволяють розробникам створювати додатки в одному середовищі та запускать їх на декількох платформах, включаючи iOS, Android и Windows. Можливості сучасних технологій розробки дозволяють створювати мобільні додатки різної складності. Вибір тієї чи іншої платформи залежить від вимог, що пред'являються до майбутнього додатку.

Список використаних джерел

1. *10 Cross-Platform Mobile App Development Tools for Enterprises. [Електронний ресурс]. Режим доступу: https://medium.com/@seema.sharma_51491/top-10-cross-platform-mobile-app-development-tools-for-enterprises-969889f97af4?fbclid=IwAR3XRXqKT5Ka-KDd_NhOL7AADywas9fpmYjaHVdw4743R30d8yoK8fA31so*
2. *Свентицкий П., Иванова Н.А. Инструменты кроссплатформенной разработки мобильных приложений //Инновации в науке: сб. ст. по матер. XL междунар. науч.-практ. конф. № 12(37). – Новосибирск: СибАК, 2014.*
3. *Andrew Klubnikin Cross-platform vs. Native Mobile App Development: Choosing the Right Dev Tools for Your App Project [Електронний ресурс]. Режим доступу: https://medium.com/all-technology-feeds/cross-platform-vs-native-mobile-app-development-choosing-the-right-dev-tools-for-your-app-project-47d0abafee81*

УДК 004.04

Константинова Л. В., Константинова А. А.
Центральноукраїнський національний технічний університет

Огляд існуючих засобів для повнотекстового пошуку в веб-проектах

Кожен розробник, який реалізує сьогодні будь-який проект, стикається з потребою реалізувати збір, зберігання і пошук інформації в своєму веб-додатку. Чим серйозніше додаток і чим складніше структура контенту, якщо потрібні особливі види пошуку та обробки результату - тим більша потреба у власній реалізації. І тому, буде актуальним зробити огляд існуючих засобів для пошуку інформації.

На даний час існують різні варіанти пошукових рішень. Вибираючи пошуковий механізм, слід враховувати наступні параметри: швидкість індексування; швидкість переіндексування; підтримування API; протоколи що підтримуються; розмір бази і швидкість пошуку; типи документів, що підтримуються; робота з різними мовами і стемінг; підтримка додаткових типів полів в документах; платформа і мова; наявність вбудованих механізмів ранжирування і сортування та інші.

Відомі такі продукти для пошуку, як Sphinx Search, Apache Lucene, Xapian, ElasticSearch, Multisearch.io, AnyQuery, Kea Labs, Textocat E-commerce Search, Detectum, FINDOLOGIC, FAST Search Server for SharePoint та ін.

Sphinx - система повнотекстового пошуку, що володіє дуже високою швидкістю індексації та пошуку, відмінно інтегрована з MySQL і PostgreSQL, що має API для поширених мов веб-програмування (PHP, Python, Java, Perl, Ruby і C ++). Sphinx написаний на C ++ і вільно розповсюджується за ліцензією GNU GPL.

Lucene - найвідоміший з пошукових движків, споконвічно орієнтований саме на вбудовування в інші програми. Зокрема, його широко використовують в Eclipse (пошук за документацією) і навіть в IBM (продукти з серії OmniFind). Переваги - розвинені можливості пошуку, хороша система побудови і зберігання індексу, який може одночасно поповнюватися і оптимізуватися разом з пошуком. Доступний і паралельний пошук по безлічі індексів з об'єднанням результатів. Сам індекс побудований із сегментів, проте для поліпшення швидкості рекомендується його періодично оптимізувати. Присутні варіанти аналізаторів для різних мов, включаючи російську з підтримкою стемінгу (приведення слів до нормальної форми). Недоліки - дуже низька швидкість індексації (особливо в порівнянні з Sphinx), складність роботи з базами даних і відсутність API (крім рідного Java).

Solr - найкраще рішення на базі Lucene, значно розширює її можливості. Це самостійний сервер корпоративного рівня, що надає широкі пошукові можливості в якості веб-сервісу. Стандартно Solr приймає документи по протоколу HTTP в форматі XML і повертає результат також через HTTP (XML, JSON або інший формат). Повністю підтримується кластеризація і реплікація на кілька серверів, розширена підтримка додаткових полів в документах (на відміну від Lucene, для них підтримуються різні стандартні типи даних, що наближає індекс до баз даних), підтримка фасетного пошуку і фільтрації, розвинені засоби адміністрування, а також можливості кешування і бекапу індексу в процесі роботи.

Nutch - другий найвідоміший проект на базі Lucene. Це веб-пошуковий движок (пошуковий механізм + веб-павук для обходу сайтів) суміщений з розподіленою системою зберігання даних Hadoop.

Elasticsearch – пошукова система, побудована на базі індексу Lucene. Забезпечує

розподілену роботу з даними, надає RESTful інтерфейс та зберігання JSON-документів без заздалегідь визначеної структури (т.н. schemaless). Найчастіше застосовується в якості пошукової системи. Містить API для роботи з поширеними мовами програмування. Elasticsearch написана на Java та поширюється вільно на умовах Apache License. Застосовується в Wikimedia, Mozilla, Foursquare, Etsy, SoundCloud и GitHub. Спочатку Elasticsearch створювалась для повнотекстового пошуку, але з часом ця система (вдале рішення для високонавантажених проектів з великими обсягами даних) стала настільки зручною, що її стали застосовувати не тільки для пошуку по товарам в інтернет-магазинах. Велика кількість компаній почали засновувати на ES свої рішення з централізованого зберігання логів і різної аналітики.

Xapian – конкурує з Lucene и Sphinx, вигідно відрізняється від них наявністю «живого» індексу, який не потребує змін при додаванні документів, дуже потужною мовою запитів, маючи вбудований стемінг, перевірку орфографії і підтримку синонімів. Але зв'язок системи пошуку з власною системою може представляти певні труднощі. У склад входить Omega - надбудова над бібліотекою, яка застосовується в якості самостійного пошуковика та відповідає за можливості індексації різних типів документів і CGI інтерфейс.

Системи інтелектуального пошуку - це інноваційні системи, що поліпшують можливості пошуку на сайті. Такі системи здатні обробити і зрозуміти запити, що містять помилки, підтримують різні пошукові фільтри, а також можуть бути використані як додатковий маркетинговий інструмент. Інтелектуальний пошук зручний відвідувачам і дозволяє їм швидше і простіше знайти потрібний товар, а магазину збільшити конверсію і кількість замовлень. Велика частина пошукових движків з відкритим вихідним кодом, дозволяє інтегрувати пошук в будь-яку сторінку сайту, а також налаштувати на видачу певних результатів.

Зробити вибір відповідного засобу для пошуку можна тільки лише після детального дослідження і тестів. Sphinx застосовують, якщо необхідно індексувати великі об'єми даних в базі MySQL і має значення швидкість індексації і пошуку, ала не потрібні специфічні можливості пошуку та є можливість виділити на це окремий сервер або навіть кластер. Якщо додаток створюється на Java, то необхідно вибирати Lucene. Але необхідно враховувати достатньо повільну індексацію і необхідність частої оптимізації індекса. Xapian достатньо хороший та якісний продукт, але менш поширений і гнучкий, ніж інші. Для додатків на C++ і з вимогами до широких можливостей мови запиту він буде кращим вибором, однак вимагає ручного доведення і модифікацій для вбудовування в власний код або використання як окремого пошукового сервера. Використання Sphinx і ElasticSearch підвищує швидкість і якість пошуку по великим обсягам інформації, а також надає користувачам корисні в роботі з даними інструменти.

Список використаних джерел

1. *Быстрый поиск на сайте, используя ElasticSearch или Sphinx [Електронний ресурс]. Режим доступу: https://web-creator.ru/articles/accelerate_site_search_engines.*
2. *Обзор решений для полнотекстового поиска в веб-проектах: Sphinx, Apache Lucene, Xapian [Електронний ресурс]. Режим доступу: https://dou.ua/lenta/articles/full-text-search-engines-overview-sphinx-apache-lucene-xapian/.*
3. *К. Ширинкин Введение в ELK: собираем, фильтруем и анализируем большие данные [Електронний ресурс]. Режим доступу: https://mkdev.me/posts/vvedenie-v-elk-sobiraem-filtruem-i-analiziruem-bolshie-dannye.*

УДК 004.021

Корованенко В. В.
Харківський національний університет радіоелектроніки

Оптимізація процесу вибору постачальника безкоштовного хостингу

Вступ. В даний час дуже багато організацій надають послуги реєстрації доменів та хостингу і зробити оптимальний вибір достатньо складно через велику кількість пропозицій [1]. Розвиток сайту компанії робить питання вибору хостингу все більш актуальним.

Метою роботи є оптимізація та автоматизація процесу вибору постачальника безкоштовного хостинга. Для досягнення поставленої мети необхідно виконати алгоритмізацію процесу пошуку оптимального постачальника та розробити програму.

Методи вибору оптимального варіанту. Парне порівняння являє собою процедуру встановлення переваги об'єктів при порівнянні всіх можливих пар. При порівнянні пари об'єктів можливо або відношення строгого порядку, або відношення еквівалентності.

У результаті порівняння пари об'єктів O_i і O_j експерт упорядковує пару, висловлюючи, що або $O_i > O_j$, або $O_j > O_i$, або $O_i \approx O_j$. Вибір числового подання $f(O_i)$ природно зробити так: якщо $O_i > O_j$, то $f(O_i) > f(O_j)$, якщо перевага зворотна, то й знак нерівності зворотний. Якщо об'єкти еквівалентні, то $f(O_i) = f(O_j)$.

Можуть бути використані наступні числові подання [2]:

1. Якщо $O_i > O_j$, то $f(O_i) = 2$, $f(o_j) = 0$; якщо $O_i \approx O_j$, то $f(O_i) = f(o_j) = 1$.

2. Якщо $O_j > O_i$, то $f(O_i) = 1$, $f(o_j) = -1$; якщо $O_i \approx O_j$, то $f(O_i) = f(o_j) = 0$.

3. При використанні відносини квазипорядка застосовується наступне числове подання: якщо $O_i \geq O_j$, то $f(O_i) = 1$, $f(O_j) = 0$.

Результати порівняння експертом всіх пар представляють у вигляді таблиці, стовпці й рядки якої становлять об'єкти, а в осередках таблиці проставляються числові переваги.

У методі Електра [2, 3] розроблена процедура багатокритеріального вибору найбільш бажаних об'єктів, що включає наступні етапи:

1. Для кожного з критеріїв вводиться дискретна шкала можливих значень цього критерію, вагові коефіцієнти критеріїв;

2. Для кожного з критеріїв будується граф, вершинами якого є окремі об'єкти безлічі, а дуги вказують на ставлення домінування між об'єктами відповідно до даного критерію;

3. З урахуванням важливості критеріїв і перевагу об'єктів обчислюються матриці значень спеціальних коефіцієнтів, званих індексами згоди і незгоди;

4. Для кожної пари об'єктів $(x, y) \in X$ вважається встановленим відношення переваги, скажімо х над у, якщо значення відповідного індексу згоди більше деякого порогового значення, а індекс незгоди - менше відповідного порогового значення;

5. Будується узагальнений граф переваги, структура якого залежить від обраних граничних значень.

Для рішення завдання пошуку оптимального постачальника безкоштовного хостинга був обраний метод Електра. Необхідно розробити алгоритм, по якому серед

заданих альтернатив, буде вибиратися найкращий варіант. Як альтернативи повинні застосовуватися різні сайти, що надають послуги хостинга. Як критерії, по яких буде вибиратися краща альтернатива, беруться різноманітні характеристики хостеров, що представляє дані послуги.

Користувач уводить у програму критерії хостинга, що сподівається одержати. Далі відбувається звертання до бази даних, уведені дані рівняються з даними з бази й у випадку збігу альтернатива заноситься в буферний список хостингов. Необхідно помітити, що в списку можуть виявитися альтернативи, які мають оцінки за всіма критеріями гірше чим інші альтернативи. Такі неконкурентоспроможні. Їх можна сміло видаляти зі списку.

Після видалення свідомо найгірших альтернатив, у списку залишаються тільки такі альтернативи, які хоча б по одному критерії не гірше, ніж інші. Множина таких альтернатив одержало назву “множина недомінованих альтернатив”, або “множина Парето”. Далі проводиться перевірка на кількість альтернатив у списку, якщо їхнє число дорівнює 1, те відповідно ніякий метод не використається, інакше використаємо метод Електра, вихідними даними для якого є “множина Парето”.

Розробка програми для вибору оптимального хостинга. Створення сайту для відділу підприємства. На даному сайті можна розмістити інформацію про продукцію, що випускає відділом, новини що відбувається на даному підприємстві, його можна використати як візитку, таким чином збільшивши приплив фахівців на роботу. У загальному для реалізації цих і інших потреб необхідний хостинг. Система являє собою трирівневу архітектуру [4].

На сервері перебуває програма, що робить звертання до бази даних, вибір оптимальної альтернативи й повертає результат у броузер користувача. У базі даних перебуває переліки альтернативних хостингов.

Для того щоб одержати доступ до програми користувач повинен пройти процес авторизації. Дані, уведені в текстові поля уведення, відсилаються на сервер, далі виробляється звертання до бази даних, відбувається порівняння значень і у випадку позитивного результату аутентификации користувач заходить на сайт, інакше буде видане повідомлення про невірне заповнення полів уведення. Якщо користувачі не зареєстрований, він повинен пройти процес реєстрації.

Виробляється перевірка уведення полів, якщо хоча б одне з полів не заповнене буде видане відповідне повідомлення. Після реєстрації користувач не проходить процес авторизації, а відразу переходить на сторінку (рис. 1).

У даній формі користувач вносить параметри, які він хоче бачити у своєму хостинге. Розглянь докладно виконання цього етапу.

У списку, що випадає, занесений перелік характеристик хостинга, наявних у базі даних. Після вибору характеристики необхідно задати значення в поле з написом “задати значення параметра”. Далі варто нажати на кнопку “Додати” і обрана характеристика з відповідним йому значенням відобразиться в таблиці.

Далі можна переходити до вибору черговій характеристиці. Якщо по який або причині було внесено невірне значення характеристики, або користувач після додавання в таблицю порахував характеристику непотрібної для пошуку оптимального постачальника користувача, він може неї видалити.

Для цього необхідно в текстове поле з написом “Номер рядка” увести номер рядка, у якій перебуває не потрібний параметр, і нажати на кнопку “Видалити”.

Після того, як користувач порахує, що таблиця заповнена він може викликати метод розрахунку хостинга, нажавши на кнопку “Пошук”. У випадку, якщо в

користувача виникнуть які або проблеми із системою, або з'являться питання питання до модератора він може відправити поточні параметри модератору нажавши на кнопку “Відправити модератору”. Питання й побажання можна ввести в елемент форми textarea.

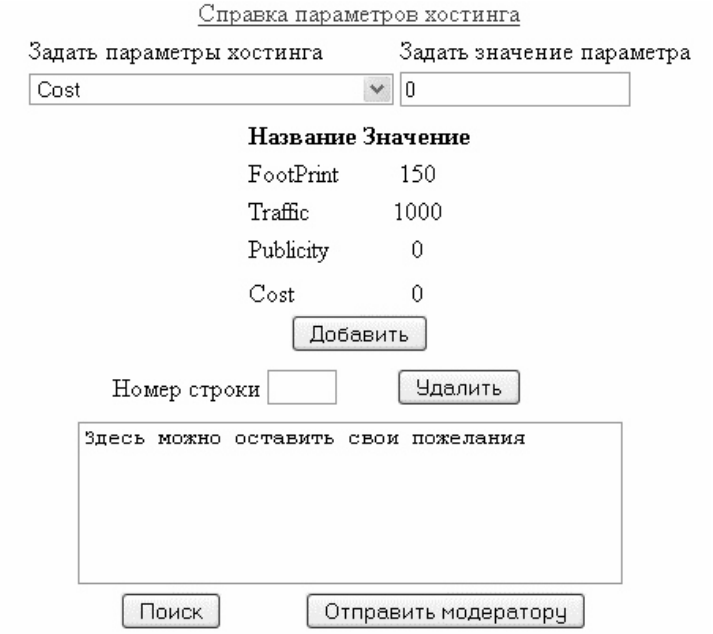


Рисунок 1 – Форма пошуку оптимального постачальника хостинга

Відповідь на запит користувача буде виглядати в такий спосіб (рис. 2)

id	name	FootPrint	Speed	Workload	Traffic	Supporting	BackUp	Monitoring	Cost	ResponseUsers	QuantitySites	LogFile	SSI	EM
7	zymic.com	5000	0	0	50000	0	0	0	0	0	0	0	1	0

Рисунок 2 – Результат пошуку оптимального постачальника

Висновок. В роботі пропонується використання математичних методів оптимізації з урахуванням багатьох критеріїв в процесі вибору хостингу.

Виконано розробку та перевірку програми вибору безкоштовного оптимального хостингу. Розроблена програма може бути використана для оптимізації вибору з урахуванням багатьох критеріїв як безкоштовного, так і платного хостингу.

Список використаних джерел

1. *Вибір хостинга [Електронний ресурс] Режим доступу: http://sv–studio.biz/hosting–domain/ – 23.11.2018 р. – Загол. з екрану.*
2. *Лотов С. А. Многокритериальние задача принятия решений: Учеб. пособие / А. В. Лотов, И. И. Поспелова. – М.: МАКС Пресс, 2008. – 197 с.*
3. *Поль Дюбуа. MySQL 3–е издание [пер. с англ.] / Поль Дюбуа М.: Издательский дом "Вильямс", 2007. – 1168 с.*
4. *Что такое Python хостинг и зачем он нужен [Електронний ресурс] Режим доступу: http://www.tophosting.in.ua/stati/chto–takoe–python–xosting–i–zachem–on–nuzhen.html – 23.11.2018 р. – Загол. з екрану.*

УДК 658:512.011: 681.326:519.713
Кулік І. С.
Харківський національний університет радіоелектроніки

Система підтримки прийняття рішеня при оцінюванні якості трафіку в NGN

Інформаційно-комунікаційні технології і послуги в даний час є Ключовим чинником розвитку всіх галузей соціально-економічної сфери. IPтелефонія дозволяє використовувати будь-яку широкосмугову телекомунікаційну мережу як засіб організації та ведення телефонних розмов, передачі відеозображень та факсів у режимі реального часу. IP-телефонія перетворилася на справжній інструмент для ведення бізнесу, а для багатьох стала безальтернативним способом спілкування з близькими та колегами. Це пояснюється це не тільки тим, що даний вид зв'язку здійснюється через Інтернет і тому є значно дешевшим традиційної телефонії, але й наявністю різних додаткових сервісів. В міжнародних організаціях і форумах иде постійно створюються нові стандарти і протоколи, пов'язані з передачею мови в мережах з пакетною комутацією. Виробники апаратного та програмного забезпечення регулярно представляють на ринок свої нові продукти. Актуальність даної теми полягає в тому, що надійність і доступність зв'язку та телекомунікаційних послуг у нашій країні давно є гострою проблемою, а саме: інформаційні послуги, високошвидкісний доступ в Інтернет, відео, кабельне телебачення, IP-телефонія і т.п.

Системи підтримки прийняття рішень (СППР) [Decision-Support Systems (DSS)) також функціонують на управлінському рівні організації. Вони допомагають менеджерам приймати рішення у виняткових, швидко змінюваних і непередбачуваних ситуаціях. Такі системи спочатку призначені для допомоги у вирішенні проблем, які не можна визначити завчасно. Хоча СППР-системи використовують у своїй роботі «внутрішню» інформацію, що отримується від управлінських систем та систем оброблення транзакцій, часто для отримання додаткових відомостей використовуються зовнішні джерела, такі як поточні біржові курси або ціни на продукцію конкурентів. Очевидно, що системи підтримки прийняття рішень володіють більшими аналітичними можливостями, ніж будь-які інші системи. У них вбудовано обезліч моделей аналізу даних, до того ж вони можуть концентрувати значну кількість інформації і надавати їм форму, зручну для використання співробітниками, відповідальними за прийняття рішень. Ці системи спроектовані таким чином, щоб користувачі могли працювати з ними «прямо» за допомогою дружнього інтерфейсу. СППР є інтерактивними; при роботі з ними користувач може довільно змінювати початкові умови, задавати нові питання і додавати в систему нові дані. Наприклад, компанія володіє кількома судами, ще кілька орендує, а також бере участь на відкритому ринку В тендерах на перевезення різних вантажів. ІС компанії обробляє фінансові та технічні аспекти таких вантажоперевезень. Фінансові розрахунки включають в себе вартість експлуатації судна (паливо, трудові ресурси, капітал), вантажні тарифи (фрахтові ставки) на перевезення різних видів продуктів і портові збори. Технічні деталі включають безліч самих різних факторів, таких як вантажопідйомність судна, швидкість, відстані між портами, споживання палива та схеми завантаження (розташування вантажу в різних портах). Система може відповідати на питання оптимальності використання ресурсів і максимізації прибутків.

Мультисервісні мережі забезпечують можливість надання користувачам найбільш широкого спектра якісних послуг при ефективному використанні універсальному способі обробки передавальних ресурсів мережі й різними застосуваннями. Основною навантаження, що генерується транспортною технологією мультисервісних мереж є технологія ATM (Asynchronous Transfer Mode). ATM як стандартизована архітектура пакетно орієнтованого передавання і комутації, спочатку призначалася для

обслуговування широкосмугових цифрових мереж з інтеграцією служб (BISDN). З того часу можливості ATM були розширені для підтримки різних типів служб: широкосмугових, вузькосмугових, пульсуючого трафіку, додатків реального часу. Для кожного типу служб ATM забезпечує задану якість обслуговування навантаження, яке оцінюється такими параметрами як затримка пакетів, дисперсія затримки та вірогідність втрати пакетів. Ця опція називається Qos (Quality of Service). Забезпечення Qos є корінною відмінністю технології ATM від існуючих мережних технологій і дозволяє повноцінно передавати інтегральний трафік (голос, відео, дані). При цьому ввесь різноманітний трафік перетворюється у стандартні осередки — 48-байтові пакети, доповненні 5-байтовими заголовками. Залежно від вимог джерел до швидкості передавання і QoS розрізняють такі основні категорії класів трафіка: з постійною бітовою швидкістю CBR (Constant Bit Rate); зі змінною бітовою швидкістю VBR (Variable Bit Rate); з доступною бітовою швидкістю ABR (Available Bit Rate); з негарантованою бітовою швидкістю UBR (Unspecified Bit Rate). Основними мережними пристроями ATME ATM-Комутатори, за допомогою яких організовуються віртуальні з'єднання на час сеансу зв'язку, і забезпечується надання QoS користувачам.

Сучасний розвиток комп'ютерних мереж характеризується їхньою конвергенцією. Раніше ізольовані локальні мережі об'єднуються за допомогою глобальних мереж. Актуальною стає задача побудови універсальних мереж, що здібні однаково ефективно надавати послуги різних типів. Перспективна архітектура мереж нового покоління (NGN) припускає створення мультисервісної мережі з винесенням функціональності послуг в граничні вузли мережі, створення спеціальної підсистеми керування послугами у вигляді окремої мережевої підсистеми, а також розширення номенклатури інтерфейсів для підключення устаткування постачальників.

Сутність мережі нового покоління полягає у переході послуг від багатоплатформності до простої та ефективної мережі, розробленої спеціально для того, щоб надавати всі види послуг. З погляду технології перехід від традиційної мережі до мережі нового покоління є переходом від окремого існування мережі з комутацією каналів і мережі з комутацією пакетів до мультисервісних мереж, що здібні функціонувати як в першому, так і в другому режимах Комутації. У результаті можна одержати мережі, що пристосовані до всіх видів послуг. Цими мережами буде набагато легше керувати, і водночас контроль за якістю послуг великою мірою перейде до самих клієнтів. Метою статті є розгляд властивостей мультисервісної мережі, її структури і архітектури керування. У роботі вирішується задача аналізу стану переходу від сучасних Комп'ютерних мереж до мереж нового покоління. В дослідженні застосуються наступні терміни. Мережа зв'язку наступного покоління (NGN) - Концепція побудови мереж зв'язку, що забезпечують надання необмеженого набору послуг з гнучкими можливостями по їх управлінню і створенню нових послуг за рахунок уніфікації мережевих рішень, яка припускає реалізацію універсальної транспортної мережі з розподіленою комутацією, винесення функцій надання послуг у кінцеві мережеві вузли і інтеграцію з традиційними мережами зв’язку.

Мультисервісна мережа – мережа зв'язку, яка побудована відповідно з концепцією мережі зв'язку наступного покоління, що забезпечує надання необмеженого набору послуг. Мультипротокольна мережа – транспортна мережа зв'язку, що входить до складу мультисервісної мережі та забезпечує перенесення різних видів інформації з використанням різних протоколів передачі. Мережа доступу (Access Network – AN) – мережа зв'язку, що забезпечує підключення термінальних пристроїв користувача до кінцевого вузла мультипротокольної мережі. На сьогоднішній день розвиток інфокомунікаційних послуг здійснюється, в основному, в рамках Комп'ютерної мережі Інтернет, доступ до послуг якої виконується через традиційні мережі зв'язку. Проте у ряді випадків послуги Інтернет, зважаючи на обмежені можливості її транспортної інфраструктури не відповідають сучасним вимогам, що пред'являються до послуг інформаційного суспільства. У зв'язку з цим розвиток

інфокомунікаційних послуг вимагає рішення задач ефективного управлінні інформаційними ресурсами з одночасним розширенням функціональності мереж зв'язку. У свою чергу, це стимулює процес інтеграції Інтернет і мереж зв'язку. До основних технологічних особливостей, що відрізняють інфокомунікаційні послуги від послуг традиційних мереж зв'язку, можна віднести наступні:

- інфокомунікаційні послуги виявляються на верхніх рівнях моделі OSI, тоді як послуги зв'язку надаються на третьому, мережевому рівні;
- більшість інфокомунікаційних послуг припускає наявність клієнтської та серверної частин; клієнтська частина реалізується в устаткуванні користувача, а серверна - на спеціальному виділеному вузлі мережі, що називається вузлом служб;
- інфокомунікаційні послуги, як правило, припускають передачу мультимедійної інформації, яка характеризується високими швидкостями передачі і несиметричністю вхідного і вихідного інформаційних потоків;
- для надання інфокомунікаційних послуг часто необхідні складні багатоточкові конфігурації з'єднань;
- для інфокомунікаційних послуг характерна різноманітність прикладних протоколів і можливостей по керуванню послугами з боку користувача;
- для ідентифікації абонентів інфокомунікаційних послуг може використовуватися додаткова адресація в рамках даної інфокомунікаційної послуги.

Більшість інфокомунікаційних послуг є “додатками”, тобто їхня функціональність розподілена між устаткуванням постачальника послуги і кінцевим устаткуванням користувача. Як наслідок, функції кінцевого устаткування також повинні бути віднесені до складу інфокомунікаційної послуги, що необхідно враховувати при їх регламентації. До інфокомунікаційних послуг пред'являються наступні вимоги: мобільність послуг; можливість гнучкого і швидкого створення нових послуг; гарантована якість послуг.

Великий вплив на вимоги до інфокомунікаційних послуг надає процес конвергенції, що призводить до того, що інфокомунікаційні послуги стають доступними користувачам незалежно від способів доступу. Існуючі мережі зв'язку загального користування з комутацією каналів і комутацією пакетів у даний час не відповідають перерахованим вище вимогам. Обмежені можливості традиційних мереж є стримуючим чинником на шляху впровадження нових інфокомунікаційних послуг.

Для реалізації системи підтримки прийняття рішень при оцінюванні якості трафіку в NGN необхідно встановити зв'язки між мультисервісною мережею, середовищем MatLab та аналізуючою системою. Це допоможе більш наглядно зрозуміти структуру системи та зпростить її розробку. У мультисервісних мережах є параметри, які впливають на якість доставлення трафіку. За допомогою середовища MatLab можливо вивести правила, які допоможуть зрозуміти який параметр наскільки впливає на якість у мережі. Це можливо зробити за допомогою набору доставлення пакетів інструментів Fuzzy Logic Tool для нечіткої логіки для середовища MatLab. Аналізуюча система (АС) розгляне всі параметри мережі і вибере які з них найбільш критично впливають на якість обслуговування мережі. Таким чином, АС побудує висновки, які складатимуться з набору параметрів, покращення яких дасть найбільш вагомий внесок у налагоджуванні мультисервісної мережі. За допомогою цих висновків адміністратор зможе швидше та правільніше прийняти рішення для удосконалення та налагодження NGN мережі з максимальним ефектом.

Список використаних джерел

1. *Соколов Н.А. Задачи перехода к сети СВЯЗИ следующего поколения. Автореферат диссертации. Санкт-Петербург, 2006. – 36 с.*
2. *Величко В.В, Субботин Е.А., Шувалов В.П., Ярославцев А.Ф. Телекоммуникационные системы и сети. Том 3. Мультисервисные сети. Москва: Горячая линия-Телеком, 2005. — 592 с.*
3. *История связи и перспективы развития телекоммуникации: учеоп пособие / Ю. Д. Украинцев, М. А. Цветов. - Ульяновск: УлГТУ, 2009. – 128 с.*
4. *Zimmerman, H. J. Fuzzy Set Theory and Its Applications / H. J. Zimmerman. — Kluwer, Dordrecht, 1991. – 315 p.*
5. *Штовба С.Д. Проектирование нечетких систем средствами MATLAB. — М.: Горячая линия — Телеком, 2007. – 288 с.*

УДК 621.391

Кучерявий М. В.
Харківський національний університет радіоелектроніки

Аналіз алгоритмів взаємодії елементів інтернету речей

Інтернет речей (Internet of Things, IoT) - це новий етап розвитку Інтернету, який значно розширює можливості збору, аналізу та поширення даних, що людина може перетворити в інформацію На сьогоднішній день Інтернет технології досягли стрімкого розвитку, зокрема Інтернет речей. З'являються нові стандарти і протоколи взаємодії в мережі IoT. Актуальність теми набирає все більше обертів. Таким станом речей був зумовлений вибір предмета дослідження, а саме порівняння основних протоколів взаємодії між інтернет речами.

Офіційне визначення Інтернету речей наведено в Рекомендації MCE-T Y.2060, згідно з яким IoT - глобальна інфраструктура інформаційного суспільства, що забезпечує передові послуги за рахунок організації зв'язку між речами (фізичними або віртуальними) на основі існуючих та сумісних інформаційних і комунікаційних технологій, що розвиваються. [1]

Інтернет речей базується на трьох базових принципах. По-перше, повсюдно поширену комунікаційну інфраструктуру, по-друге, глобальну ідентифікацію кожного об'єкта і, по-третє, можливість кожного об'єкта відправляти і отримувати дані за допомогою персональної мережі або мережі Інтернет, до якої він підключений. Найбільш важливими відмінностями Інтернету речей від існуючого інтернету є:

- фокус на речах, а не на людину;
- істотно більше число підключених об'єктів;
- істотно менші розміри об'єктів і невисокі швидкості передачі даних;
- фокус на зчитуванні інформації, а не на комунікаціях;
- необхідність створення нової інфраструктури і альтернативних стандартів.

Використовують 3 способи взаємодії з інтернет-речами:

- прямий доступ;
- доступ через шлюз;
- доступ через сервер.

У разі прямого доступу інтернет-речі повинні мати власну IP-адресу або мережний псевдонім, за яким до них можна звернутися з будь-якого клієнтського додатку, і вони повинні виконувати функції веб-сервера.

Якщо інтернет-речі не мають вбудованої підтримки протоколів IP і HTTP, то для взаємодії з ними можна використовувати спеціальний Інтернет-шлюз. Більшість стандартів бездротових сенсорних мереж не підтримують протокол IP, використовуючи власні протоколи взаємодії. Така особливість викликає необхідність наявності пристрою для ретрансляції повідомлень з сенсорної мережі в мережу Інтернет для сумісності протоколів. Недоліки такого підходу ті ж, що і в разі прямого доступу, але поширюються вони вже на шлюз.

Третя форма взаємодії пристроїв в IoT через сервер базується на наявності посередника між інтернет-речами і користувачем і може бути реалізована за допомогою посередницької платформи даних – серверу або групи серверів.

Для взаємодії величезної кількості різноманітних пристроїв в IoT потрібні стандартизовані інтерфейси, формати даних і комунікаційні протоколи. У табл. 1 наведено перелік розглянутих стандартів IoT (ZigBee, Z-Wave, BLE, 802.11), із зазначенням робочої частоти, швидкості передачі даних, методу модуляції і розширення спектра, адресації і інших параметрів.

Таблиця 1 - Порівняння показників стандартів ZigBee, Z-Wave, BLE

Характеристика	ZigBee	Z-Wave	BLE
Частотний діапазон, МГц	868/915/2400	868/908, 2400	2400
Бітова швидкість, кбіт/с	20/40/250	9.6/40, 200	1000
Тип модуляції сигнала	BPSK/BPSK/ O-QPSK	BPSK	GFSK
Метод розширення спектра	DSSS	-	FHSS (ширина канала 2 МГц)
Чутливість приймача, дБм	-92 або краще для 868/915 МГц; -85 або краще для 2400 МГц	-101	<-70 -87...93
Вихідна потужність передавача, дБм	-32...0	-20...0	-20...10
Розмір данних пакета, байт	До 127	До 64	От 8 до 47
Адресація	16- и 64-бит MAC, 16-біт ідентифікатор мережі	32-біт-ідентифікатор будинку; 8-біт - адреса вузла	48-біт відкрита адреса Bluetooth або випадкова адресу
Типові вимоги до реалізації стека протоколів	45...128 кбайт ПЗУ; 2,7...12 кбайт ОЗУ	32...64 кбайт ПЗУ; 2...16 кбайт ОЗУ	~40 кбайт ПЗУ; ~2,5 кбайт ОЗУ

Крім цього в IoT можуть використовуватися і більш традиційні технології. Характеристики сімейства стандартів IEEE 802.11 (більш відомого, як WiFi) наведені в табл. 2 [2].

Таблица 2 – Характеристики семейства стандартов IEEE 802.11

Стандарт IEEE	Діапазон, ГГц	Ширина канала, МГц	Вид модуляції	Антенна технологія	Максимальна швидкість передачі
801.11b	2,4	20	CCK	-	11 Мбит/с
801.11g	5	20	CCK, OFDM	-	54 Мбит/с
801.11a	2,4	20	OFDM	-	54 Мбит/с
801.11n	2,4; 5	20, 40	OFDM (до 64 QAM)	MIMO, MU-MIMO, до 4 потоків Beamforming	600 Мбит/с
801.11ac	5	40, 80, 160	OFDM (до 256 QAM)	MIMO, до 8 потоків Beamforming	6,93 Гбит/с
801.11ad	60	2160	SC/OFDM	Beamforming	6,76 Гбит/с

В ході виконання роботи були досліджені такі протоколи передачі даних IoT, як MQTT, CoAP і HTTP/2.

Протоколи CoAP і MQTT використовують для зв'язку шлюзу з сервером. В даний час численна кількість протоколів використовується для цих цілей, але саме представлені протоколи набули найбільшого поширення при розробці Інтернет Речей через адаптацію до специфіки IoT. Також можливе ефективне використання CoAP і MQTT, коли необхідно відправляти короткі повідомлення. Протокол HTTP/2 ефективен для використання у Вебі Речей (WoT, WEB of Things). Основні відмінності між протоколами CoAP, MQTT і HTTP/2 наведені в табл. 3.

З концепцією WoT перегукується ідея семантичної павутини (Semantic Web) - це напрямок розвитку Всесвітньої павутини WWW, метою якого є надання інформації у вигляді, придатному для машинної обробки. Протоколи MQTT і HTTP/2 на транспортному рівні використовують протокол TCP, що робить їх сумісними з мережами, що працюють на основі стеку TCP/IP.

Таблиця 3 - Основні відмінності між протоколами CoAP, MQTT і HTTP / 2

Протокол	MQTT	CoAP	HTTP/2
Транспортний рівень	TCP	UDP	TCP
Безпека	TLS/SSL	DTLS	TLS/SSL
Обмін повідомленнями	Видавець/ Підписник	Запит Відповідь	Запит Відповідь
Надійність	3 типа: QoS0, QoS1, QoS2	2 типа: Confirmable, Non-comfirmable	-

Протокол MQTT має ряд переваг, порівняно з протоколом HTTP/2 (табл. 4):

- менші накладні витрати на передачу даних;
- менша смуга пропускання;
- не вимагає постійного з'єднання між клієнтом і сервером;
- добре адаптований до роботи по каналах зв'язку з низькою пропускною здатністю. [3]

Таблиця 4 - Порівняння характеристик протоколів HTTP і MQTT

Операція	Протокол		Економія
	HTTP	MQTT	
Читання одного блоку даних з сервера	302 байт	69 байт	в 4 рази менше
Запис одного блоку даних на сервер	320 байт	47 байт	в 7 разів менше
Читання 100 блоків даних з сервера	12 600 байт	2445 байт	в 5 разів менше
Запис 100 блоків даних на сервер	14 100 байт	2126 байт	в 7 разів менше

В представленій роботі був проведений аналіз найбільш поширених стандартів і протоколів Інтернету речей. Були визначені особливості роботи кожного зі стандартів та протоколів, наведені їх основні параметри і характеристики. На основі представлених характеристик та сучасних вимог були представлені ті напрямки практичного застосування Інтернету речей, що відповідають найбільш ефективному обміну даними.

Список використаних джерел

1. Колибельніков, А. І. Огляд технологій бездротових мереж / А.І. Колибельніков // Праці МФТІ. 2012. Том 4. № 2. С. 3-29.
2. Єрохін, С.Д., Макаров С.С. Протоколи маршрутизації в бездротових сенсорних мережах: засновані на розташування вузлів і спрямовані на агрегацію даних// Телекомунікації та транспорт. Т-Сот. 2013. №3. С. 44-47.
3. Восков Л.С., Пилипенко Н.А. Web речей - новий етап розвитку інтернету речей// Якість. Інновації. Освіта. 2013. № 2. С. 44-49.

УДК 004.7

Мамонтов О. О.
Харківський національний університет радіоелектроніки

Застосування методів сплайнапроксимації для синтезу характеристик нелінійних пристроїв засобів телекомунікації

В прикладній математиці суттєва роль відводиться інтерполяції, тобто ситуації коли відомі деякі граничні значення певної функції та необхідно відновити її проміжні значення. За допомогою інтерполяції вирішується широкий спектр задач численного аналізу, а саме диференціювання та інтегрування функцій, знаходження нулів та екстремумів, вирішення диференціальних рівнянь. Інтерполяційні формули Лагранжа, Ньютона і Стірлінга, при використанні великого числа вузлових точок часто призводять до неточного наближення результуючої через накопичення похибок в процесі обчислень, суттєво також зростає степінь інтерполяційних многочленів, що робить їх незручними для обчислення. Для зниження похибок відрізок розбивається на часткові відрізки, де функція наближено заміняється поліномом невисокого ступеню. Коефіцієнти поліному підбираються таким чином, щоб виконувалися певні умови, які залежать від способу інтерполяції. Це має назву кусочно-поліноміальна інтерполяція. Одним із способів інтерполяціїї на довжині всього відрізку є так звана сплайн-інтерполяція.

Сплайн являє собою кусочно-поліноміальну функцію яку можна уявити у вигляді плавно згинаючої сталевої лінійки, закріпленої на деяких вузлових точках. Завдяки зазначеним властивостям, сплайни здатні якісно описувати математичні функції, як з невеликим числом вузлових точок так і з дуже великим числом вузлових точок. Основні види сплайнів:

- лінійний сплайн – це сплайн, що складається з поліномів першого ступеня, тобто з відрізків прямих ліній. Точність при застосуванні таких сплайнів невисока, вони не забезпечують безперервність навіть перших похідних. Проте, в деяких випадках лінійна апроксимація проявляє себе краще, ніж апроксимація більш високого порядку. Наприклад, лінійний сплайн зберігає монотонність переданого в нього набору точок.

- сплайн Ерміта – це сплайн, що складається з поліномів третього ступеня в якому використовується ермітова інтерполяція, згідно якої на кожному вузлі сплайна задано не лише значення функції, але й значення її першої похідної. Сплайн Ерміта має безперервну першу похідну, але друга похідна у нього розривна. Точність такої інтерполяції значно краща, ніж у лінійного сплайна.

- кубічний сплайн – це функція, область визначення якої розбита на кінцеве число відрізків, на кожному з яких вона збігається з деяким кубічним поліномом. Така функція проходить через всі задані точки на відповідних вузлах; на відрізку між сусідніми вузлами функція приймає вид кубічної параболи; функція безперервна разом зі своїми першою і другою похідними в усіх точках. З теорії пружності відомо, що результуюча крива має постійну кривизну і розриви виникають лише в третій похідній.

На відміну від інтерполяційних многочленів Лагранжа, послідовність інтерполяційних кубічних сплайнів на рівномірній сітці завжди зводиться до інтерпольованої неперервної функції, причому з поліпшенням диференціальних властивостей цієї функції швидкість збіжності підвищується.

Основні переваги кубічних сплайнів такі: графік побудованої функції проходить через кожну точку масиву; побудована функція порівняно-легко математично описується; степінь многочленів не залежить від числа вузлів, отже, не змінюється при збільшенні вузлів; побудована функція має добрі апроксимаційні властивості.

Список використаних джерел

1. *Шикин Е.В., Плис А.И. Кривые и поверхности на экране компьютера. Руководство по сплайнам для пользователей – М.: ДИАЛОГ-МИФИ, 1996. – 240 с.*
2. *ALGLIB User Guide - Интерполяция, аппроксимация и численное дифференцирование - Интерполяция сплайнами [Електронний ресурс] – http://alglib.sources.ru/interpolation/spline3.php*
3. *Самоучитель по Maple. Урок 9. Анализ функций и полиномов. 23. Сплайн-интерполяция и аппроксимация [Електронний ресурс] – http://lib.grz.ru/node/12365*
4. *Прикладная математика. Численные методы. Интерполяция функций. Интерполирование сплайнами [Електронний ресурс] – http://www.simumath.net/library/book.html?code=Interpol_splines*

УДК 681.5.015

Матвєєнко Ю. В.*
Харківський національний університет
міського господарства імені О.М. Бекетова

Сучасні WEB-дизайн і інтернет-технології

З питання розробки і створення Web-сторінок у мережі Internet накопичено колосальний багаж різних методів, засобів і технологій, чимало з яких, на жаль, сьогодні вже є умовно застосовними. Відновлення апаратного устаткування рік у рік лише прогресує, причому з наростаючими темпами.

Метою даної роботи є вивчення методичної і прикладної літератури з проблем проектування й створення Web-сторінок[1-3], узагальнення досвіду роботи досвідчених розробників, програмістів і Web-дизайнеров, а також вибір оптимальної стратегії, методів і прийомів створення особистого чи корпоративного Web-сайту, який втілює всі відомі нині передові ідеї і технології.

Багато Web-дизайнерів сходяться в думці, що головні проблеми Web-дизайну - розмаїття браузерів і платформ, кожна з яких по-різному підтримує HTML сценарії[3]. З випуском кожної нової платформи браузерів поліпшуються їх характеристики й можливості, але це значить, що ранні версії зникають. Здебільшого люди не схильні гнатися за новітнім і найкращим. Одні задовольняються тим, що у них є, інші працюють за комп'ютерами фірм чи установ, котрі вибрали браузери за них.

Як зробити дизайн Web-сторінки естетично й технічно цікавим, не ігноруючи власників попередніх версій браузерів? Невже Web-сторінка, розрахована те що, щоб функціонувати на будь-яких браузерах, мусить бути обов'язково нудною? Чи можна догодити всім? А якщо ні, то де провести межу? Скільки старих версій працюватиме з вашою сторінкою? У Web-дизайні немає жорстких правил. Оскільки головне наше завдання – зробити вміст сторінки доступним максимальній кількості користувачів, то для просування вперед важливі нові технології з урахуванням існуючих реалій. Запорука успіху дизайнерського рішення лежить у розумінні потреб аудиторії та в чіткому поданні, як сайт буде використано.

На ринку домінують два основні браузери: Netscape Navigator і Microsoft Internet Explorer. Спільно вони, зокрема всі їх версії, представляють приблизно 90% використовуваних сьогодні браузерів. Буде легше прийняти зважене рішення, яку технологію використовувати й де провести межу для зворотної сумісності, якщо знати, які браузери використовуються найчастіше. Найбільш достовірну інформацію можна одержати, ведучи статистику відвідувань сайту. Відстежуюче програмне забезпечення серверів зазвичай класифікує відвідування по браузерах, здійснюючи запити. У Інтернеті можна знайти кілька сайтів, які надають статистичні дані про браузери. Статистика цих сайтів полягає в аналізі відвідуваності самих цих сайтів, що звужує статистичну вибірку до вузького кола користувачів. Статистичні дані, вміщені з сайту BrowserWatch, дають якомога докладніші дані про версії кожного окремого браузера.

Найчастіше неможливо уникнути прямого контакту з сервером, навіть якщо йдеться про просте завантаження файлів. Через усе це дизайнери повинні мати базові знання про сервери і їхню роботу. Якщо є дозвіл якомога ширшого доступу до сервера, можна вирішити певні завдання самостійно, без сторонньої допомоги.

---

* Науковий керівник – канд. техн. наук, доцент Дядюн С. В.

Сервер – це будь-яке програмне забезпечення, що дає можливість виконувати запити на документи й інші дані. Програми, які запитують і відбивають документи (такі як браузер), називаються клієнтами. Терміни "за серверу" і "за клієнта", використовувані, наприклад, під час роботи з картами-зображеннями, ставляться до тієї машини, яка керує процесом. Функції за клієнта виконуються машиною користувача, функції за сервер – на віддаленій машині. Web-сервери відповідають на запити браузерів (клієнтських програм), на задані файли (або виконують сценарій CGI) і повертають документ чи результати сценарію. Web-браузери і сервери спілкуються за протоколом Hypertext Transfer Protocol (HTTP, протокол передачі гіпертексту).

Більшість серверів працюють на платформі Unix. Саме у світі Web і використовується термінологія системи Unix. У процесі роботи необхідно вивчити кілька Unix-команд. Деякі серверні пакети пропонують графічний інтерфейс як альтернативу управлінню з командної рядки Unix. Ось лише деякі відомі сервери: NCSA Server, Apache, CERN, Netscape Servers, Internet Information Server (IIS). Більшість серверів (приблизно 70%) працюють на Apache або його попереднику NCSA.

Глобальна комп'ютерна мережа Інтернет розвивається дуже стрімко. Швидко збільшується кількість видань, присвячених мережі, що віщує широке її розповсюдження навіть у далеких від техніки областях у майбутньому.

У процесі досягнення поставленої у роботі мети потрібно було вирішити низку наступних завдань: ознайомитися з сучасними Інтернет-технологіями й за можливості, використовувати їх у своїй розробці; вивчити програмний інструментарій, і використовувати його шляхом створення Web-сайту; виявити та врахувати методи і засоби уявлення про Web-сторінки різних видів інформації, що перешкоджають її доступності; ознайомитися з основними правилами і рекомендації з розробки й створенню Web-сайту і дотримуватися їх у своїй практиці; визначитися зі структурою Web-сторінок; вибрати стратегію розробки і створення Web-сайту.

До основних характерних особливостей створення Web-сайту можна віднести: маленький розмір файлів з кодами Web-сторінок (їх лістинг приведено у додатку), що забезпечує їх швидке завантаження з мережі на клієнтській машині; векторний формат використовуваної графіки, стислі формати растрових і звукових файлів, що також позитивно впливає на зменшення розміру Web-сторіноу і часу на їхнє скачування каналами мережі; відсутність проблем сумісності з різними браузерами, наприклад такими широко поширеними, як Internet Explorer і Netscape Navigator; автоматична підтримка anti-aliasing (згладжування контурів з допомогою змішання сусідніх квітів), значно покращує естетичне сприймання використаної графіки; гнучкість, відкритість і модифікованість з допомогою простих коштів.

До наявних недоліків можна віднести: необхідність оволодіння ідеологією і коштами Macromedia Flash 5.0 - сучасним професійним інструментарієм створення Web-сторінок; вимушеність спрямування існуючих версій браузерів (Flash Java Player) для адекватного перегляду Flash-сторінок.

Під час створення Web-сайту використовувався сучасний пакет Macromedia Flash 5.0, використання якого завжди було прерогативою професійних розробників.

Список використаних джерел

1. *Information Dashboard Design: Displaying Data for At-a-Glance Monitoring Stephen Few - М.: Изд-во: «2 edition», «Analytics Press», 2013.*
2. *Этан Вотролл и Джефф Сьярто. Изучаем веб-дизайн. - М.: Изд-во: «Эксмо», 2010.*
3. *Элизабет Фримен, Эрик Фримен. Изучаем HTML, XHTML и CSS - М.: Изд-во: «Питер», 2014.*

УДК 621.396

[1]Оксіюк О. Г., [2]Кротов В. Д.
[1]Київський національний університет імені Тараса Шевченка;
[2]Військовий інститут телекомунікацій та інформатизації мені Героїв Крут

Управління потоками даних в Ad Hoc мережах спеціального призначення

Завдяки високій живучості і розвідзахищенності, швидкого розгортання і можливості доставки інформації в умовах динамічно змінної топології Ad-Hoc мережі, мають перспективи, щодо побудови мереж спеціального призначення (МСП), тобто мереж, що функціонують в інтересах силових структур (Збройних Сил, Національної гвардії, сил охорони правопорядку).

Аналіз наукових праць показав, що з одного боку, необхідні технологічні рішення, що сприяють підвищенню продуктивності МСП в процесі обміну даними, але з іншого боку, відсутні адекватні моделі і теоретично обґрунтовані методи ефективного управління потоками даних, які спрямовані на досягнення вказаної мети. В зв'язку з цим актуальною видається науково-технічна проблема, яка полягає у розробці теоретично обґрунтованих методів і моделей управління потоками даних для підвищення продуктивності МСП. Для вирішення сформульованої проблеми вимагається здійснити вибір наукового апарату, на основі застосування якого можна підвищити ефективність управління потоками даних в МСП.

Процес, що аналізується умовно можна розбити на такі складові (елементи):

- управління відправкою даних вузлами-передавачами;
- управління повторними передачами;
- управління відправкою квитанцій вузлами-приймачами;
- управління відкиданням пакетів в транзитних вузлах.

Елементи процесу управління потоками даних безпосередньо не взаємодіють один з одним. Їх взаємний вплив проявляється через взаємодії з іншими процесами.

З формуванням потоків даних в МСП безпосередньо пов'язані наступні процеси:

- відправка даних вузлами-передавачами;
- повторні передачі, викликані необхідністю заповнення інформації, що втрачена у процесі доставки по мережі внаслідок спотворення даних із-за канальних перешкод і втрат пакетів унаслідок перевантажень елементів МСП;
- відкидання пакетів в транзитних вузлах для попередження перевантажень;
- відправка квитанцій вузлами-приймачами для контролю достовірності доставки даних.

Функціонування МСП супроводжується втратами пакетів внаслідок передчасних розривів з'єднань, які викликані динамічністю топології МСП і деструктивними діями супротивника. Крім того, втрати пакетів, можуть бути викликані спотвореннями даних внаслідок перешкод в радіоканалах мережі. Динамічність топології і зовнішні деструктивні дії призводять до випадкової зміни мережевого трафіку, що також є важливою особливістю МСП.

Для ефективного управління потоками даних потрібне виконання таких умов:

- отримання актуальної інформації про стан елементів (значеннях параметрів) мережі у теперішній момент часу і в найближчому майбутньому;
- своєчасне ухвалення адекватних рішень щодо управління;
- своєчасна реалізація прийнятих рішень.

Перша умова пов'язана з необхідністю наявності на вузлі управління достовірної інформації, про те, у якій ситуації мережа знаходиться у теперішній момент часу, а також який буде стан її елементів у найближчому майбутньому. Отримати точні відомості про поточний стан мережі можна, якщо виміряти значення чисельних параметрів на усіх її ділянках. Проте збір і доставка цієї інформації до вузлів, в яких здійснюється управління потоками даних, мають істотні недоліки: по-перше, вони роблять архітектуру мережі складнішої, по-друге, створюють небажаний службовий трафік і, по-третє, обов'язково відбуваються з деякою затримкою, наявність якої сприяє частковій (чи повній) втраті актуальності цієї інформації. Тому оцінювати ситуацію в мережі доводиться по значеннях обмеженої кількості параметрів, які більшою мірою характеризують стан мережі не тепер, а у минулому.

Ситуацію, що склалася в мережі, побічно характеризують величини, які використовуються для отримання вхідних параметрів при управлінні потоками даних в МСП. Слід зазначити, що маючи в розпорядженні дані про значення цих величин, проблематично адекватно оцінити поточну ситуацію в мережі, і тим більше складно достовірно передбачити її майбутній стан. При цьому, наприклад, відсутні точні відомості про те, який проміжок часу пройде до отримання квитанції на тільки що відправлений пакет, наскільки буде тривалим сплеск трафіку, і яких значень досягнуть при цьому черги пакетів у транзитних вузлах.

Адекватних моделей, які здатні точно описати стан МСП у будь-який момент часу, на жаль, не існує, а застосування наближених моделей в процесі управління ресурсами мережі не дає прийнятних результатів.

Управління потоками даних в МСП відбувається в умовах наявності неповної, розмитої, неточної інформації про стан елементів цієї мережі в реальному часі і в майбутньому. Ефективним засобом управління у таких умовах є застосування систем нечіткого виводу. Основна перевага таких систем – це здатність використати умови і методи рішення завдань, які описані на мові, близькій до природної. Центральне місце в процедурах нечіткого виводу займає база нечітких правил.

Відомі науково-технічні рішення, які пов'язані із застосуванням нечіткої логіки для управління чергами в телекомунікаційних мережах. Проте існують окремі класи прикладних завдань, в яких побудова нечітких правил пов'язані зі значними труднощами концептуального характеру. До них відносяться завдання розпізнавання образів, екстраполяції і інтерполяції функціональних залежностей, класифікації і прогнозування, нелінійного і ситуаційного управління, а також інтелектуального аналізу даних. Загальною особливістю подібних завдань є існування деякої залежності або відношення, що зв'язує вхідні і вихідні змінні моделі досліджуваної системи. При цьому виявлення і визначення цієї залежності у явному аналітичному вигляді не можливо через недостатню кількість інформації про досліджувану предметну область або складність обліку багатьох різних чинників, які впливають на характер цього взаємозв'язку.

Відомо, що класичним системам з нечіткою логікою, не здатним автоматично навчатися, властивий істотний недолік, що полягає в тому, що набір нечітких правил, вид і параметри функцій приналежності, що описують вхідні і вихідні змінні системи, а також вид алгоритму нечіткого виводу, вибираються суб'єктивно людиною, тому вони можуть бути не досить адекватними. Для усунення відміченого недоліку використовують апарат нечітких нейронних мереж як гібридних інтелектуальних систем. Нечітка нейронна мережа – це багатошарова нейронна система, в якій шари

виконують ті або інші процедури нечіткого виводу. Нейрони такої мережі характеризуються набором параметрів, налаштування яких здійснюється у процесі навчання, як в звичайних нейронних мережах. Такі системи об'єднують в собі переваги нейронних мереж і систем нечіткого виводу. З одного боку, вони дозволяють розробляти і представляти моделі систем у формі правил нечіткої продукції, що мають наочність і простоту змістовної інтерпретації. З іншого боку, для налаштування правил нечіткої продукції використовуються можливості нейронних мереж. Відома достатня кількість прикладів успішного використання подібних інтелектуальних систем для вирішення різних прикладних завдань. У зв'язку з цим обґрунтованим видається застосування нейронечетких систем для управління потоками даних в МСП.

Висновок. Розробка теоретично обґрунтованих методів і моделей, які необхідні для ефективного управління потоками даних і підвищення продуктивності МСП, є актуальною науково-технічною проблемою. Вплив чисельних випадкових чинників істотно ускладнює отримання аналітичних залежностей, які потрібні для вирішення вказаної проблеми. Тому в умовах функціонування МСП управління потоками даних доцільно здійснювати на основі застосування наукового апарату нечітких нейронних мереж.

Список використаних джерел

1. *Бунин С. Г., Войтер А. П., Ильченко М. Е., Романюк В. А. Самоорганизующиеся сети со сверхширокополосными сигналами / С. Г. Бунин, А. П. Войтер, М. Е. Ильченко, В. А. Романюк. – К.: Наукова думка, 2012. – 444 с.*
2. *Гавилов А. В. Гибридные интеллектуальные системы / А. В. Гаврилов – Новосибирск: НГТУ, 2002. – 142 с.*
3. *Гостев В.И. Нечеткое активное управление очередью в узкоспециализированной радиосвязи / В.И. Гостев, С.Н. Скуртов, О.В.Невдачина, В.Д. Кротов // Сучасна спеціальна техніка. – 2011. – № 3(26). – С. 66–79.*
4. *Леоненков А. В. Нечеткое моделирование в среде MATLAB и fuzzyTECH / А. В. Леоненков. – СПб: БХВ-Петербург, 2003. – 736 с.*
5. *Люггер Дж. Искусственный интеллект: стратегии и методы решения сложных проблем / Дж. Люгер. – М.: Вильямс, 2003. – 864 с.*
6. *Осипов Е. А. Проблема реализации надежной передачи данных в самоорганизующихся и сенсорных сетях / Е. А. Осипов // Электросвязь. – 2006. – № 6. – С. 29–33.*
7. *Польщиков К. А. Математическая модель передачи мультимедийного сообщения в телекоммуникационной сети с коммутацией пакетов / К. А. Польщиков, Ю. Н. Здоренко, О. Я. Сова // Научные ведомости БелГУ. – 2014. – № 15 (186). – Вып. 31(1). – С. 176 – 184.*
8. *Польщиков К. А. Модель нейро-нечеткого прогнозирования средней интенсивности поступления запросов на передачу потоков реального времени по каналу телекоммуникационной сети / К. А. Польщиков, Е. Н. Кубракова, В. А. Краснобаев // Системи обробки інформації. – 2014. – Вип. 2 (118). – С. 193–197.*
9. *Рвачева Н.В. Метод выбора межсегментного интервала в транспортном протоколе телекоммуникационной сети / Н. В. Рвачева, К. А. Польщиков, С. В. Волошко // Проблемы телекоммуникаций. –Харьков, 2011. – Вып. 2(4). – С. 72 – 82.*
10. *Рутковская Д. Нейронные сети, генетические алгоритмы и нечеткие системы / Д. Рутковская, М. Пилиньский, Л. Рутковский – М.: Горячая линия – Телеком, 2006. – 452 с.*
11. *Усков А. А. Интеллектуальные технологии управления. Искусственные нейронные сети и нечеткая логика / А. А. Усков, А. В. Кузьмин – М.: Горячая линия – Телеком, 2004. – 143 с.*

УДК 004.75

Ткаченко Е. В.
ДВНЗ «Криворізький національний університет»

Огляд сучасних технологій розробки баз даних їх властивостей та функцій

База даних – це колекція взаємопов'язаних, та певним чином структурованих даних, відповідно до формату метаданих. Метадані – це дані, які описують дані, що зберігаються. Саме метадані визначають спосіб, яким дані зберігаються у базі.

Дані та метадані надають середовище, в якому дані логічно упорядковуються так, щоб їх було легко обслуговувати і добувати. Метадані БД визначають структуру, в межах якої дані організуються логічним чином.

Не усі БД мають однакову структуру. Існує цілий ряд різних моделей даних. Найбільш часто реалізуються три такі моделі: ієрархічна, мережева, реляційна.

Однією із перших моделей даних в технології баз даних була ієрархічна модель даних, в якій окремі записи організуються у відношення типу «батько - нащадок» і утворюють дерево у вигляді ієрархічної моделі. «Батьківський» запис може асоціюватись з кількома «нащадками», але для кожного «нащадка» існує лише один «батьківський» запис. Недоліком моделі є складність доступу до потрібних даних, складність внесення змін у дані. Але сьогодні багато даних зберігаються у ієрархічних базах. Для систем управління файлами застосовується саме така модель даних.

Мережева модель краще ієрархічної тим, що дозволяє множинність відношень «батько – нащадок». Навігація по записам простіше, ніж в ієрархічній моделі, але все ж вимагає програмування. Оновлення даних є складними.

Реляційна база даних не залежить від додатка (навігація і оновлення даних не програмуються у додатку). Реляційна модель передбачає не наявність «батьків» та «нащадків», а рядків та стовпчиків, які утворюють таблиці взаємопов'язаних даних. Дані в таблицях можуть змінюватись. З розвитком реляційної моделі даних збільшується кількість продуктів, в яких вона використовується для зберігання даних. До числа таких продуктів відносяться DB2, Oracle, SQL Server, MySQL.

Для зберігання динамічної інформації, окрім реляційної моделі даних, потрібно ще забезпечити маніпулювання даними та інші дії – забезпечення доступа до даних з боку користувачів.

Властивості сучасних СУБД:

- розвинуті властивості визначення складних структур даних та маніпулювання ними;
- потужні засоби обробки збоїв та відновлення інформації після збоїв;
- розвинуті засоби організації даних та методів доступу до них;
- незалежність прикладних програм від даних;
- деякі засоби захисту від непередбачуваних та помилкових дій користувачів, що може привести до аварійного руйнування інформації.

Функціями СУБД є:

- безпосереднє керування даними у зовнішній пам'яті (на дисках);
- керування буферами даних в оперативній пам'яті з використанням дискового кешу;
- керування трансакціями;
- підтримка цілісності бази даних (коректність та непротирічність) - цілісність описується за допомогою обмежень;
- контроль за надлишковістю даних;
- журналізація змін, резервне копіювання та відновлення бази даних посля збоїв;
- підтримка мов БД (мови визначення даних, мови маніпулювання даними).

На сьогодні відомими є такі технології розробки баз даних: Microsoft SQL Server, Oracle, MySQL, MS Access, InterBase/Firebird/Yaffil. У таблиці 1 наведемо рейтинг популярних серед зазначених.

Таблиця 1 – Рейтинг популярних СУБД

№ п/п	СУБД	Відсоток використання
1.	MicrosoftSQL Server	32,3%
2.	MS Access	6,6%
3.	MySQL	10,2%
4.	Oracle	16,1%

MySQL характеризується великою швидкістю, стійкістю і простотою використання. Вихідні коди сервера компілюються на багатьох платформах. Найповніше можливості сервера виявляються в UNIX-системах, де є підтримка багатоканальності, що підвищує продуктивність системи в цілому. Для некомерційного використання MySQL є безкоштовним.

MySQL є рішенням для малих та середніх додатків. Входить до складу серверів WAMP, AppServ, LAMP і в портативних збірках серверів Денвер, XAMPP, VertrigoServ. Загалом, MySQL використовується в якості сервера, до якого звертаються локальні або віддалені клієнти, проте в дистрибутив входить бібліотека внутрішнього сервера, що дозволяє включити MySQL в автономні програми .

Основні переваги MySQL:

- масштабованість. MySQL може підтримувати роботу БД значних розмірів, що підтверджують її реалізації в Yahoo!, Google, HP, Associated Press; згідно документації, що додається до MySQL, деякі БД, що використовуються компанією MySQL AB (розробником MySQL), зберігають до 50 млн. записів;
- переносність. MySQL працює на різних платформах, серед яких Unix, Linux, Windows, OS/2, Solaris, Mac OC; окрім того, MySQL працює на різних платформах;
- зв’язаність. MySQL має мережеву структуру. До MySQL можна одержувати доступ із будь-якої точки Internet кільком користувачам одночасно. MySQL має цілий ряд програмних інтерфейсів додатків (Application Programming Interface –API), які дозволяють встановлювати з’єднання з MySQL із додатків, написаних на таких мовах як C, C++, Perl, PHP, Java, Python;
- безпека. MySQL має систему контроля доступу до даних, забезпечує шифрування даних при передаванні;
- швидкість функціонування;
- зручність експлуатації. MySQL досить зручно встановлюється та реалізується, легко адмініструється;
- відкритий код.

Вище перераховані переваги та відомості про сучасний стан технологій, застосованих для розробки та підтримки баз даних, роблять MySQL найкращим вибором для виконання мого дипломного проекту.

Список використаних джерел

1. *Для чего сайту нужна база данных? [Електронний ресурс] / Joker-jar 2010 – 2018/ – Режим доступу: http://www.myfirstsite.ru/articles/database-for-website*
2. *Основні відомості про бази даних [Електронний ресурс] – Режим доступу: https://support.office.com/uk-ua/article*

УДК 007.51

Цюпко В. В.
ДВНЗ «Криворізький національний університет»

Хмарні сервіси SaaS, PaaS, IaaS і їх тренди розвитку

У той час як хмарні сервіси є надзвичайно гарячою темою від малого бізнесу аж до глобальних підприємств, вони як і раніше є досить широкою концепцією, яка охоплює багато онлайн-територій. Коли замовник починає розглядати перемикання свого бізнесу на хмару, будь то для розгортання додатків або інфраструктури, більш важливо розуміти відмінності і переваги різних хмарних сервісів.

Зазвичай існує три моделі хмарного сервісу.

1. SaaS (програмне забезпечення як послуга) – це повністю готовий веб-сайт, який використовується для вирішення якихось прикладних задач. Тут замовник не бере участі в розгортанні та підтримці сайту. Провайдер SaaS-послуги сам вирішує, де і як буде розміщуватися сайт, сам займається його підтримкою і наповненням. Замовник використовує готовий сервіс і може навіть не замислюватися про те, що стоїть за красивими сторінками, якими він користуєтеся для вирішення якихось прикладних задач, наприклад, для роботи з електронною поштою або знайомства з новими людьми.

2. PaaS (платформа як послуга) – це фактично shared-хостинг. В рамках цієї моделі не потрібно буде адмініструвати операційну систему і системне програмне забезпечення. Для управління сайтом буде надано веб-інтерфейс, за допомогою якого можна наповнити свій сайт потрібним змістом, в тому числі, активним (скриптами, базами даних). З замовника буде знято навантаження з адміністрування сервера: як його апаратної частини, так і програмної.

3. IaaS (інфраструктура як послуга) – надання обчислювальних ресурсів за запитом, на яких замовник має можливість розгорнути і запустити довільне програмне забезпечення, що включає в себе операційні системи і додатки. В рамках даної моделі замовник не керує і не контролює фізичну інфраструктуру, але має контроль над операційними системами і розгорнутими додатками [1].

Таблиця 1 – Характеристики хмарних сервісів

	Споживач	Надана послуга	Зона доступності	Можливість змін
SaaS	Кінцевий користувач	Додаток під ключ	Доступність і працездатність додатку	Мінімальні індивідуальні налаштування
PaaS	Розробники додатків	Платформа для запуску додатку, хмарне сховище	Доступність і продуктивність платформи	Високий рівень кастомізації додатків
IaaS	IT-відділ, розробники додатків	Віртуальні сервера, хмарне сховище	Доступність віртуальних серверів	Мінімальні обмеження по підтримуваним ОС і додатків

Стрімке зростання на хмарні сервіси почалося через їх зручності. Вони економлять для організацій час, гроші і ресурси. Тепер немає потреби встановлювати ПО на власні комп'ютери і сховища зберігання даних.

Передбачити майбутнє такого динамічного ринку непросто, але вже можна виділити деякі тенденції, які вплинуть на розвиток хмарних сервісів в цьому році.

1. Штучний інтелект і машинне навчання. В останні роки з'явилися такі сервіси, як Amazon Alexa, Google Home, Siri. Колись індустрія персональних помічників перебувала в зародковому стані, але тепер ці сервіси конкурують між собою. Amazon інвестує великі кошти у виробництво смарт-динаміка Echo і йде в комплекті помічника Alexa. За словами Девіда Лімпа, старшого віце-президента Amazon за приладами і послугами, зараз над Alexa працюють понад 5000 осіб.

2. Чатботи. Ще один різновид сервісів, який набирає популярність – це чатбот. Інвестиції Google в цю сферу зіграли чималу роль. У минулому році пошуковий гігант придбав стартап-бот API.ai. В цьому році Google представила новий сервіс Chatbase, який проводить аналітику і дає рекомендації щодо поліпшення взаємодії ботів з користувачами. Ця технологія, нарешті, пройшла процес становлення. Тепер віртуальні співрозмовники інтегруються в такі платформи, як Slack і Facebook Messenger.

3. Мобільні пристрої. Смартфони стали невід'ємною частиною повсякденного і робочого життя людини. З їх допомогою люди виставляють клієнтам рахунки через Freshbooks, дзвонять по Skype колегам, які живуть в п'яти різних часових поясах. Хтось обмінюється файлами через Dropbox і Google Docs.Около половини (43%) власників малих підприємств здійснюють ділові операції, головним чином, через смартфони. Це підвищує попит на застосування технології SaaS при розробці мобільних додатків.

4. Безпека і приватна хмарна середа. Безпека залишатиметься важливою проблемою для хмарних сервісів. Ця обставина посилюється прийняттям загального регламенту щодо захисту даних і інших правил щодо конфіденційності. Впровадження смартфонів продовжує нарощувати темпи, але це призводить до появи безлічі можливостей порушення безпеки. Особисті дані та дані компаній знаходяться під загрозою. До того ж, віддалені працівники працюють з компаніями через незашифровані мережі, які більш уразливі перед атаками хакерів. Компанії, що надають інтелектуальний сервіс, прагнуть придумати кращі рішення в сфері безпеки, на зразок Secure WordPress Hosting від компанії Pagely. Наприклад, Pagely розробила PressArmor – архітектуру безпеки, яка зміцнює і захищає її мережу, обладнання та додатки WordPress. Основна мета – запобігання і зниження ризиків для клієнтів. Це один із способів компанії показати, що використання їхнього продукту безпечно [2].

Загалом, кожна хмарна модель пропонує свої власні особливості і функціональні можливості, і для організації важливо зрозуміти відмінності. Незалежно від того, чи шукає замовник хмарне програмне забезпечення для параметрів сховища, плавну платформу, яка дозволяє створювати власні додатки або ж потрібен повний контроль над усією інфраструктурою без фізичного її обслуговування, для замовника існують відповідні хмарні сервіси. Який би варіант не був обраний, перехід на хмарні сервіси – це майбутнє бізнесу і технологій.

Список використаних джерел

1. *IaaS, что это такое? PaaS, SaaS, для чего они нужны? Примеры и сравнение [Електронний ресурс] – Режим доступу до ресурсу:* https://1cloud.ru/services/private-cloud/iaas-paas-saas.
2. *Солозобов О. 4 главных тренда SaaS в 2018 году [Електронний ресурс] / Олег Солозобов. – 2018. – Режим доступу до ресурсу:* https://8d9.ru/glavnyx-trenda-saas-v-2018-godu.

УДК 004.051

Шуліка Я. П.
Центральноукраїнський національний технічний університет

Розробка сайту з урахуванням SEO

Якщо пересічній людині потрібен сайт, то вона не має уявлення про те як сайти потрапляють у пошукову систему та про просування сайту в просторі Internet. Користувач отримує сайт, з певною інформацією, але, виявляється, що на його сайт не користується попитом, тобто відвідуваність такого сайту дуже мала або відсутня взагалі.

Володар сайту починає шукати проблему. У більшості випадків з'ясовується, що популярність сайту, обумовлена, виконанням супроводжуючого сайт певних критеріїв (КСС).

Для виконання КСС потрібно оптимізувати сайт згідно з вимогами SEO – search engine optimization – «оптимізації пошукових систем», мається на увазі оптимізації сайту для пошукових систем. Для цього володар сайту звертається до SEO-спеціалістів(SEOs) - спеціалістів з інтернет маркетингу. У більшості випадків SEO-спеціалісти виконують велику кількість змін на сайті. Таким чином виникає ситуація, коли входять у протиріччя рекомендації SEOs та пропозиції команди розробників сайту.

Розробка якісних, для пошукових систем сайтів, може бути простішим та дешевшим завданням, якщо залучити SEO - спеціалістів ще до початку розробки сайту. У цьому випадку сайт не буде перероблятися і володар сайту буде витрачати кошти лише одноразову розробку, а не при кожній переробці. Крім того у цьому випадку популярність сайту швидше досягне гарних позицій, у зв'язку з урахуванням КСС на початковому етапи.

Розглянемо основні чотири базові принципи(БПРС), які необхідно враховувати при створенні сайту.

1. Мета та актуальність. Хороший сайт завжди починається з формулювання завдання. Перш ніж робити хоч щось, потрібно знати те, для чого взагалі потрібна кожна веб-сторінка. Якщо мети немає, то створювати сторінку не варто.

2. Естетика зовнішнього вигляду. Сайт повинен мати відповідний сучасний дизайн та інтерфейс з урахуванням ергономіки людини. Користувачам неприємно знаходитись на "негарних" сайтах, сайтах заповнених рекламою, особливо агресивною, це негативно впливає на ранжування та карається пошуковими системами.

3. Релевантний і оригінальний контент. Якщо сайт щось пропонує – то він повинен дійсно мати можливість надати це користувачу. Контент повинен бути унікальним. Плагіат - це погано і карається пошуковими системами зниження позицій.

4. Зрозуміла навігація. Те, наскільки просто і зрозуміло можна пересуватися по сайту - дуже важливо. Будь-яка його сторінка повинна бути доступною за три кліка з будь-якої іншої сторінки. Навігація повинна бути простою і зрозумілою - це позитивно позначається на конверсії і на ранжируванні в пошукових системах. [1]

Одним з важливих критеріїв є висока швидкість завантаження сайту. Згідно з дослідженнями[2], майже половина користувачів інтернету очікують, що сайт завантажується за дві секунди або швидше, а якщо цього не відбудеться за три секунди - вони його покинуть. Кожна секунда завантаження знижує конверсію на 20% -згідно з досліджень для мобільних телефонів.

Крім вище вказаного – низька швидкість сайту – це фактор, що негативно впливає на ранжування та позиції сайту. Але не потрібно фанатично покращувати швидкість сайту, це не найголовніша метрика. Головне, щоб був релевантний контент та зручний для користувача сайт. Якщо ваш контент - це відео або gif – зображення, вони можуть довго завантажуватись, але ніхто не будете видаляти свій контент зі сторінки. Найшвидшим буде той сайт, з якого видалити код, але це не той сайт, який потрібен користувачу пошукової системи. [2]

Виходячи з БПРС можна узагальнити порядок розробки сайту з урахуванням SEO-оптимізації:

1. Перед придбанням домену потрібно провести дослідження ключових слів, та проаналізувати сайти-конкурентів, виділити свою цільову аудиторію, та зрозуміти як люди шукають відповіді на проблеми, які сайт може допомогти їм вирішити.

2. Використовуючи дослідження ключових слів можна обрати доменне ім’я, яке вже вказує на тематику сайту та має ключові слова. Після чого розробники сайту, разом зі SEO-спеціалістами роблять зручний у навігації сайт, зі зрозумілою структурою, і з використанням ключових слів у назвах сторінок, категорій та шаблонів.

3. Контент, що надається сайтом теж можна оптимізувати, щоб його можна було простіше знайти у мережі.

4. Потрібно перевірити швидкість сайту, доступність сторінок, відсутність технічних помилок.

5. Після того як сайт готовий - SEO-спеціалісти перевіряють ключові моменти, після чого відправляють сайт на індексування пошукових систем, показуючи їм, що з’явився новий сайт і пошуковим системам потрібно звернути на нього увагу.

6. Після того як сайт проіндексований пошуковими системами він вже має деякі позиції, щоб їх покращити SEO-спеціалісти виконують внутрішню та зовнішню оптимізацію.

7. Велика частина внутрішньої оптимізації вже виконана на минулих етапах, залишається лише перевіряти сайт на зручність для користувача, перевіряти чи не з’явились технічні помилки, та, розширювати охоплення аудиторії контентом.

8. Зовнішня оптимізація полягає у перевірці того, як часто сайт цитується у мережі. Сайт можуть також знайти шукаючи у соціальній мережі, тому спеціалісти рекомендують заводити там сторінки від адміністрації сайту. Також сайт розміщується у актуальних каталогах або сервісах по відгукам. Останній етап зовнішньої оптимізації - цитування на сайтах новин, або популярні статті з цитуванням сайту.

9. Доки сайт існує для нього завжди буде актуальним розширення аудиторії та покращення цитування у мережі, тому ця роботи виконується протягом всього існування сайту. [3]

Використовуючи принципи та підходи SEO на початковому етапі проектування сайтів замовник отримує не тільки якісний програмний продукт, але й оптимізує свої витрати на проектування та супроводження сайту.

Список використаних джерел

1. *Яким повинен бути хороший сайт [Електронний ресурс]. – Режим доступу: – https://spark.ru/startup/megagroup/blog/29188/kakim-dolzhen-bit-horoshij-sajt-kratkoe-rukovodstvo-i-podborka-poleznih-instrumentov.*
2. *Наскільки важлива швидкість сайту[Електронний ресурс]. – Режим доступу: – https://vc.ru/flood/34484-pravda-o-tom-naskolko-vazhna-skorost-zagruzki-sayta*
3. *Розробка сайту під SEO[Електронний ресурс]. – Режим доступу: – https://seo-akademiya.com/baza-znanij/osnovyi-seo/etapyi-sozdaniya-sajta-pod-seo/*

УДК 658:512.011:681.326:519.713
Аносов О. В.
Харківський національний університет радіоелектроніки

Аналіз застосування методу AEP для формальної верифікації HDL-опису дизайнів цифрових систем

Верифікацією називається перевірка відповідності системи (або деякого проміжного результату проектування: прототипу, моделі і т.д.) висунутим до неї вимогам (проектної документації). Верифікація цифрових систем має першочергове значення в життєвому циклі виробництва, оскільки вона безпосередньо впливає на його продуктивність, а в кінцевому підсумку визначає функціональність продукту та рівень задоволеності споживачів. Аспекти верифікації цифрових систем є темою багатьох досліджень та використовуються на усіх етапах виробництва цифрових систем.

Окремим видом верифікації, яка сильно покладається на математику, є формальна верифікація. Формальна верифікація ґрунтується на математичному моделюванні програм і вимог до них та у загальному випадку включає наступні кроки (рисунок 1): створюється формальна модель системи M та вимог ф, формально перевіряється їх відповідність та на підставі результатів перевірки робиться висновок про відповідність або невідповідність реальної програми реальним вимогам.

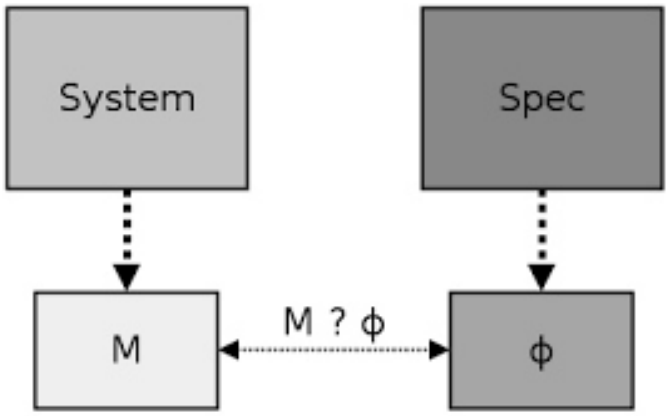


Рисунок 1 – Загальна схема формальної верифікації

Для того щоб виконати формальну верифікацію HDL дизайну, потрібно виконати приведені вище кроки, враховуючи специфіку області.

На першому кроці необхідно перевести скомпільований та синтезований HDL код (наприклад, VHDL RTL опис) в формальну модель M, яка є зрозумілою для формального інструментарію.

Наступним кроком є задання моделі властивостей дизайну ф. Властивість – це набір логічних та темпоральних відношень між підлеглими булевими послідовними виразами, які разом описують поведінку (тобто, шлях) частини системи. Інструментом визначення властивостей дизайну є асерції.

Завдяки тому, що під час верифікації дизайну є його HDL опис, з'являється можливість використовувати метод автоматичного виведення таких властивостей. AEP – Automated Extracted Properties (автоматично зібрані властивості) – концепція

виведення властивостей дизайну з його HDL опису та генерації спеціального HDL коду асерцій для перевірки цих властивостей[1].

Місцями для виведення властивостей можуть бути:

- використання директив parallel/full case;

- використання виразу в якості індексу вектора або масиву, чиє максимальне значення може вийти за границі цільового вектора або масиву;

- опис недосяжного стану автомату.

- Крім того будь-який дизайн має певний набір властивостей та вимог, джерелом яких є специфікація. Прикладами є:

- якщо на вхід суматора поступає два позитивних числа, то результат теж має бути позитивним;

- генератор унарного коду має видавати на вихід вектор, в якому значення '1' є лише в одному біті;

- схема арбітра має задовольняти всі запити.

Асерція –це певне судження про передбачену поведінку дизайну (його властивість), яку необхідно перевірити. В більшості випадків асерція представляє собою HDL код, який не несе додаткової функціональності для цільової системи та не синтезується. Сучасні стандарти HDL мають спеціальні синтаксичні конструкції для написання асерцій.

Генерація синтезованих асерції можлива за допомогою сторонніх бібліотек, наприклад OVL (Open Verification Library) фірми Accellera. OVL представляє собою набір асерційних модулів (чекерів), які перевіряють специфічні властивості дизайну. Такі чекери інстанціюються в певних місцях дизайну та надають методологію для формальної та динамічної верифікації. Кожен OVL чекер представляє собою модуль метою якого є гарантія, що в дизайні виконуються специфічні умови. Чекери складаються с однієї чи декількох властивостей, які необхідно перевірити, повідомленні, рівень важливості та покриття.

Наступним кроком після написання асерцій є їх перевірка. Існує два способи перевірки асерцій. Для цього використовуються спеціальні інструменти формального аналізу, які за допомогою математичних методів та моделей аналізують цільовий дизайн та його властивості. Як правило, на виході такий інструмент видає один з трьох станів:

- proved – дана властивість доведена, тобто не існує такого стану системи, при якому б дана властивість не виконувалась би;

- disproved – властивість спростовано, властивість порушена при певному стані системи. Формальний інструмент видає контрприклад (аналог TestBench) який демонструє стан системи, при якому порушується властивість;

- unknown – властивість не вдалось довести або спростувати через недостатність обчислювальних потужностей.

В цілому, використання методу AEP відкриває можливості для повної автоматизації процесу формальної верифікації описів цифрових систем.

Список використаних джерел

1. Assertion-Based Design 2nd Edition / Foster, Harry D., Krolnik, Adam C., Lacey, David J. – Springer US, 2005. - 390 с.

УДК 004.056.55

Антонюк М. А., Неласа Г. В.
Запорізький національний технічний університет

Дослідження арифметики точок еліптичної кривої на пристроях з обмеженим об'ємом пам'яті

Більшість цифрових пристроїв у світі взагалі працюють в сфері цифрового помічника людини. Особливу роль тут грають пристрої, які можуть об'єднуватися в єдину мережу і мають між собою певний інформацій обмін. А там де є обмін інформацією завжди виникає проблема захисту кіберпростору. Не важливо від яких типів атак: починаючи з збереження конфіденційності, цілісності інформації і закінчуючи порушенням доступу до інформаційних ресурсів. В цьому допомагає криптографія. "Хмари", сервера, що їх підтримують, мережі, персональні комп'ютери, кишенькові смарт-пристрої – це такі гіганти, на яких вже реалізовані і використовуються алгоритми криптографічного захисту.

Більшість смарт-пристроїв незалежно від їх розміру мають власний захист, але це не відноситься до більшості гаджетів, які входять в категорію "Інтернет речей" (наприклад, смарт-годинник), адже у більшості випадків навіть не виникає думки, що якусь шкоду можливо завдати реалізуючи атаку на ці пристрої, або використовувати ці пристрої для обхідної атаки на пристрої с захистом. Зміст питання якраз у цьому - ми можемо захиститися від атак спрямованих на звичні речі, які отримали зв'язок і тепер входять до категорії Iot. Відповідь - використовуючи криптографію, але з поправками на можливості самого пристрою. Власне необхідно мати майже ту саму стійкість при менших затратах як апаратного так і програмного забезпечення. Варіант - використання криптоалгоритмів на еліптичних кривих. Згідно з результатами досліджень, які проводив NIST (National Institute of Standards and Technology), з порівняння розмірів ключів RSA і ECC, необхідних для отримання однакового рівня захисту, еліптична криптографія може використовувати ключи довжиною у 160 біт аби забезпечити стійкість в 2048 біт RSA. Такі цифри наштовхують на дослідження еліптичних кривих на достатньо низькому рівні. А саме мета роботи - дослідити можливості еліптичної криптографії на пристроях з обмеженним об'ємом памятті.

Для реалізації авторами було обрано мікроконтролер Arduino Nano. На мікроконтролері було реалізовано арифметику еліптичних кривих над простим полем Галуа: додавання точок і множення точки на число. Ця арифметика є базовою для генерації ключів, формування та верифікації електронного цифрового підпису. Мікроконтролер використовується для дослідження швидкості різних типів систем координат: афінна, стандартна проективна, система Якобі, система Чудновського-Якобі та змішанні системі Якобі. Дослідження, що проводяться авторами, в змозі дати відповідь на питання, яка система найшвидша і має більший потенціал з впровадження в системи захисту для смарт-пристроїв. Економія апаратного часу з розрахунку базової арифметики дає зріст швидкодії смарт-пристрою із захистом і буде корисна не лише для пристроїв "Інтернету речей". Авторами проведено аналіз математичних основ теорії скінченних полів та реалізація логіки мікроконтроллеру на основі розглянутих алгоритмів з використанням мови програмування AVR C++.

Список використаних джерел

1. *Добуш А. Р., Костик А. Т. Методи вбудованого контролю виконання операцій у полях Галуа для реалізації в НВІС // Вісник Національного університету "Львівська політехніка""Комп'ютерні системи проектування. Теорія і практика".– 2013. – Вип. С.570.*

УДК: 658:512.011:681.326:519.713
Кучеренко І. О.
Харківський національний університет радіоелектроніки

Використання темпоральних графів при розробці шаблону опису алгоритмів функціонування скінченних автоматів

Вступ. Системи автоматизованого управління зазвичай побудовані так, що в них можна виділити системи управління та керовані об'єкти. Дотримуючись цієї концепції, системи управління на основі кінцевих автоматів можна розділити на дві частини: керуючу частину, відповідальну за логіку поведінки та керовану частину, відповідальну за виконання дій, обраних для виконання керуючою частиною. Серед усіх керуючих пристроїв можна виділити пристрої логічного управління, у яких управляючі впливи представляються у двійковому алфавіті. Оскільки для реалізації керуючої частини в таких пристроях, як правило, використовуються кінцеві автомати, вони називаються керуючі автомати. Подібні пристрої широко застосовуються в системах Internet of Things. Будь-який цифровий пристрій, котрий реалізує алгоритм обробки інформації та її управління може бути реалізовано апаратним або програмно-апаратним способом. При програмно-апаратному способі алгоритм реалізується на апаратно-орієнтованій мові програмування. Найпопулярніша мова для цього – С зі спеціальними бібліотеками. Апаратна сторона реалізується, як правило, на різноманітних мікроконтролерах. При апаратному способі алгоритм описується на мові описання апаратури HDL, синтезується інструментальними засобами систем автоматизованого проектування (САПР) та імплементується у ПЛІС або ASIC. При написанні алгоритму функціонування цифрових пристроїв використовуються автоматні програми, у яких розділяється написання логіки програми та описання семантики. Автоматні програми мають тільки три вида функцій: функції переходів, функції виходів та функції реалізації затримок і переходів у новий стан. Вони мають шаблон та використовують оператори вибору, умовні оператори та функції таймеру або фронта.

Об'єкт дослідження: шаблони опису кінцевих керуючих автоматів на мовах програмування та описання апаратури. Предмет дослідження: використання темпоральних графів при розробці шаблонів описання кінцевих керуючих автоматів на мовах програмування та описання апаратури Ціль дослідження: підвищення ефективності процесу розробки кінцевих керуючих автоматів с часовим логічним (не мікропрограмним) керуванням на мовах програмування та опису апаратури. Задача – використати темпоральний граф при розробці єдиного шаблону опису автоматних пристроїв у стилі автоматного програмування.

Зміст дослідження. Пристрої логічного управління, побудовані на основі кінцевих автоматів, функціонують одразу у двух вимірах: в автоматному часі та у реальному часі. Автоматний час вимірюється в автоматних тактах. Автоматний такт – дискретних відрізок часу за який автомат переходить з одного стану в інший. Тривалість такого такту визначається частотою синхросигналу Clk. Реальний час визначається часовими параметрами алгоритму функціонування пристрою. Для усунення протиріччя пропонується використання темпорального графа переходів, який описується розширеною функцією переходів.

$$Z(t+1) = f(X(t), Z(t), T).$$

У такому графі кожному стану становиться у відповідність затримка Ті, яка визначається числом автоматних тактів, протягом яких автомат знаходиться у даному стані. При цьому темпоральний граф переходів є не тільки візуальним відображенням алгоритму функціонування кінцевого керуючого автомата, а й його повною математичною моделлю. Затримка в кожній вершині темпорального графа переходів реалізується через петлю, умовами для якої є підрахунок числа тактів Clk, що схемно реалізується лічильником в ПЛІС або таймером з перериванням в МК. Це означає, що темпоральний граф ідеально підходить для розробки шаблону опису алгоритмів функціонування кінцевих автоматів у стилі автоматного програмування.

Проведено дослідження можливості реалізації темпоральних графів для автоматів Мілі і Мура у вигляді однопроцесних та двухпроцесних автоматних шаблонів на мові опису апаратури VHDL з точки зору коректності подальшого автоматизованого синтезу. Була використана система САПР XILINX ISE.

Висновки. Розроблено єдиний шаблон опису автоматних пристроїв з використанням темпоральних графів на мові опису апаратури VHDL і шаблон програмного коду на мові програмування С. Наукова новизна даного досліду – впровадження темпоральних графів у єдиний шаблон опису автоматних пристроїв, який підвищує ефективність процесу розробки кінцевих керуючих автоматів с часовим логічним управлінням.

Шаблони опису алгоритмів функціонування кінцевих автоматів у системах логічного управління на мовах VHDL і С можуть бути використані новачками проектувальниками цифрових систем логічного управління, а також дає спрощення задачі верифікації.

Список використаних джерел

1. *Harel D. Statechars: a Visual Formalism for complex systems // Science of Computer Programming. Vol. 8, 1987, – P. 231-274.*
2. *Шалыто А.А. Использование граф-схем и графов переходов при программной реализации алгоритмов логического управления. I. // Автоматика и телемеханика.– 1996. – №6. – С.148-158.*
3. *Шалыто А.А. Использование граф-схем и графов переходов при программной реализации алгоритмов логического управления. II. // Автоматика и телемеханика.– 1996. – №7. – С..144-169.*
4. *Шалыто А.А. SWITCH-технология — автоматный подход к созданию программного обеспечения «реактивных» систем / А.А.Шалыто, Н.И.Туккель // Программирование. – 2001. – №5. – С.45-62.*
5. *Шалыто А.А. Алгоритмизация и программирование для систем логического управления и "реактивных" систем. // Автоматика и телемеханика.– 2001. – №1. – С.3-39.*
6. *Шкиль, А.С. Обнаружение ошибок проектирования в HDL-моделях конечных автоматов с использованием синхронизирующих последовательностей / А.С. Шкиль, М.А. Мирошник, Э.Н. Кулак А.С. Гребенюк, Д.Е. Кучеренко // Радиоэлектроника и информатика. – 2016. – № 3(74). – С. 39-46.*
7. *Бибило П.Н. Синтез логических схем с использованием языка VHDL / П.Н. Бибило. – М.: СОЛОН-Р, 2009. – 384 с.*
8. *Haskell R. Digital Design Using Digilent FPGA Boards - VHDL / Active-HDL Edition / Richard E. Haskell, Darrin M. Hanna. – LBE Books Rochester Hills, MI, 2009.– 381 p.*
9. *R. Alur, D. L. Dill. A theory of timed automata. // Theoretical Computer Science.– 1994. – V.126. – N 2. – P. 183-235.*
10. *Shkil A.S. Design automation of easy-tested digital finite state machines / M.A. Miroschnyk, Y.V. Pakhomov, A.S. Shkil, E.N. Kulak, D.Y. Kucherenko // Radio Electronics, Computer Science, Control. – 2018. – №2. – P. 117-124.*

УДК 004.056

Майданик О. О.
Центральноукраїнський національний технічний університет

Мови опису апаратури для ПЛІС та їх використання в сучасній обчислювальній техніці

Програмовані логічні пристрої (PLD) зробили революцію в світі цифрової схемотехніки більш ніж 25 років тому, та на сьогоднішній день в деяких сферах є незамінні. ПЛІС стійкі до впливу радіації та інших зовнішніх збурень, що обумовлює широке застосування в аерокосмічній галузі, військовій техніці та в промисловому виробництві. В порівнянні з звичайними процесорами ПЛІС продуктивніші при тих самих тактових частотах. ПЛІС є універсальною мікросхемою на якій можливо побудувати будь яку цифрову систему. ПЛІС програмується мовою опису апаратури. Пропонуючи розробнику порожній чіп для його програмування і реалізації множини функцій, PLD можуть мати низьку щільність (ємність) логічних осередків і називатися «складні програмовані логічні схеми» (англ. - complex programmable logic devices, CPLD's), або мати велику ємність логічних осередків, реалізованих на базі статичної оперативної пам'яті з довільним доступом (SRAM), і називатися «програмованими вентильними матрицями» - ПКВМ (англ. - field programmable gate array, FPGA). До того ж, крім реалізації логічних функцій і регістрів масиву логічних елементів, можна використовувати такі вбудовані функції, як пам'ять, управління тактовими сигналами, драйвери введення-виведення різних стандартів, трансивери з високою швидкістю передачі даних, MAC-рівні Ethernet, функціональні блоки сигнальної обробки, а також вбудовані процесори.

Програмована логічна інтегральна схема, ПЛІС (англ. programmable logic device, PLD) – електронний компонент, який використовується для створення цифрових інтегральних схем. Сама по собі ПЛІС є заготовкою для подальшого використання. Для того, щоб змусити її функціонувати, необхідно завантажити програму, яка і визначить її логіку роботи. Отримати прошивку можна декількома способами в спеціалізованих САПР: намалювавши логіку роботи схематично, або описавши її за допомогою мови опису апаратури (VHDL, Verilog, SystemC, SystemVerilog). Проектуванням та виробництвом ПЛІС на даний момент часу займаються декілька десятків провідних фірм та компаній (Xilinx, Altera, Lattice, Actel). Лідером у цій галузі є фірма Xilinx, що спеціалізується на виробництві інтегральних мікросхем (ІМС) високої якості, зокрема стійких до впливу радіації та інших зовнішніх збурень, що обумовлює широке застосування ПЛІС в аерокосмічній галузі, військовій техніці та в промисловому виробництві. Серед номенклатури ПЛІС найбільшого поширення набули мікросхеми, що виготовлені за технологіями FPGA та CPLD.

Програмована користувачем вентильна матриця, ПКВМ (англ. Field-Programmable Gate Array, FPGA) – один з архітектурних різновидів ПЛІС. ПКВМ можуть бути змінені практично в будь-який момент в процесі їх використання, що робить їх дуже універсальними. Це обумовлено архітектурою, що складається з конфігурованих логічних блоків, схожими на перемикачі з множиною входів і одним виходом (логічні вентилі або gates). Широкий діапазон мікросхем FPGA-технології дозволяє проектувати на їх основі широкий спектр електронних пристроїв, серед яких: засоби поєднання різних за живленням інтерфейсів, перетворювачі кодів, периферійні контролери, мікропрограмні пристрої керування, скінченні автомати, універсальні та спеціалізовані процесори, пристрої цифрової обробки сигналів.

Мова опису алгоритму або ж мова логічного програмування - це спеціалізована формальна комп'ютерна мова, що використовується для проектування структури,

дизайну та роботи електронної мікросхеми та її моделювання. Вона дає можливість автоматично аналізувати, імітувати та тестувати створюваний пристрій. Компілятор мусить забезпечувати переведення програми, написаної на будь-якій з мов опису апаратури на низькорівневу специфікацію фізичних електронних компонентів з ціллю створити мікросхему.

Мова опису апаратури виглядає дуже схоже на мову програмування, наприклад Сі, оскільки її структура складається з таких самих текстових виразів. Також мови проектування апаратури дають можливість описувати специфікації для апаратного забезпечення, що можуть виконуватися. Це дає ілюзію наявності мови програмування, хоча насправді їх відносять до мов проектування чи моделювання.

Першою причиною цього є те, що, на відміну від мов програмування, які не завжди мають в собі ознаки паралелізму, інструкції мов проектування апаратури завжди виконуються паралельно. Іншою важливою їх складовою є опис синхросигналу, що є особливістю проектування апаратного забезпечення. Мови опису апаратури можуть використовуватися для створення пристрою у структурній, поведінковій формах чи на рівні регістрових передач з такою ж функціональністю.

На сьогоднішній день використовують такі мови логічного програмування для ПЛІС як Verilog та VHDL.

Verilog HDL (англ. Verilog Hardware Description Language) - мова опису апаратури (HDL), що використовується для опису та моделювання електронних систем. Verilog HDL не слід плутати з VHDL (конкуруюча мова), найбільш часто використовується у проектуванні, верифікації і реалізації (наприклад, у вигляді НВІС) аналогових, цифрових та змішаних електронних систем на різних рівнях абстракції.

Розробники Verilog зробили його синтаксис дуже схожим на синтаксис мови С, що спрощує його освоєння. Verilog має препроцесор, дуже схожий на препроцесор мови С, і основні керуючі конструкції.

Слід зазначити, що опис апаратури, написаний мовою Verilog (як і іншими HDL-мовами) прийнято називати програмами, але, на відміну від загальноприйнятого поняття програми, як послідовності інструкцій, тут програма представляє множину операторів, які виконуються паралельно і циклічно під керуванням об'єктів, названих сигналами. Кожен такий оператор є моделлю певного елемента реальної функціональної схеми апаратури, а сигнал - аналогом реального логічного сигналу. Так само для мови Verilog не застосовується термін «виконання програми». Фактично, виконання Verilog-програми є моделюванням функціональної схеми, яку вона описує, що виконується спеціальною програмою - Verilog-симулятором.

VHDL (англ. VHSIC (Very high speed integrated circuits) Hardware Description Language) - мова опису апаратури інтегральних схем. Мова проектування VHDL є базовою мовою при розробці апаратури сучасних обчислювальних систем.

Мова VHDL створена як засіб опису цифрових систем, однак існує підмножина мови - VHDL AMS (аналогових та змішаних сигналів), що дозволяє описувати як чисто аналогові, так і змішані, цифро-аналогові схеми.

Висновок. Мова опису апаратури дуже схожа на вже звичні мови програмування як Сі та Паскаль але при цьому визначає яким чином з'єднана матриця логічних елементів мікросхеми. Тому їх все таки називають програмами. Мови опису апаратури є невід'ємною частиною систем автоматизованого проектування електроніки.

Список використаних джерел

1. *Архітектура ПЛІС FPGA [електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Архітектура_ПЛІС_FPGA*
2. *Мови опису апаратури [електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Мови_опису_апаратури*
3. *Verilog [електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Verilog*
4. *VHDL [електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/VHDL*

УДК 004.3

Попко С. О.
ДВНЗ «Криворізький національний університет»

Розробка інтелектуального зарядного пристрою на основі мікроконтролера

Розвиток випуску транспортних засобів та автомобілів з частковим або повним використанням електричної тяги ставить актуальну задачу управління, контролю та діагностування потужних акумуляторів в процесі їх зарядки. Для реалізації поставленої задачі доцільно використовувати сучасні мікроконтролери, які мають можливість управляти електронними приладами та пристроями. Вони є універсальним інструментом, за допомогою якого можна реалізувати будь який алгоритм управління.

Для прикладу обрано свинцево-кислотний акумулятор – найпоширеніший та один з найбільш затребуваних типів акумуляторів.

При всіх позитивних якостях свинцево-кислотного акумулятора він має суттєвий недолік, який скорочує термін його експлуатації - сульфатація пластин. В результаті неправильної експлуатації акумулятора активна речовина - сульфат свинцю - переходить в хімічно неактивний стан. З цієї причини знижується зарядна і розрядна ємність акумулятора аж до її повної і незворотної втрати.

Основними причинами сульфатації пластин є рекристалізація сульфату свинцю, що веде до укрупнення розмірів кристалів, і адсорбції на кристалах сульфату свинцю поверхнево-активних речовин, присутніх в якості домішок у сірчано-кислому електроліті. І те й інше призводить до зниження розчинності сульфату свинцю і, як наслідок, до зменшення швидкості зарядного процесу. Тому характерними ознаками сульфатації акумуляторних електродів є підвищена напруга і активне газовиділення, що спостерігається на самому початку заряду.

Для усунення сульфатації акумуляторних пластин розроблено метод спеціального заряду акумулятора, заснований на чергуванні імпульсів зарядного і розрядного струмів, на заряді імпульсним асиметричним струмом. Використання імпульсів зарядного струму великої амплітуди в деяких випадках дозволяє ефективно десорбувати з поверхні органічні домішки в процесі сильної катодної поляризації.

Принцип даного способу заряду заснований на чергуванні імпульсів зарядного струму малої тривалості, але великої амплітуди, з імпульсами розрядного струму з частотою їх слідування кратної частоті змінного струму електромережі (50 Гц). На практиці найбільш підходять два значення частоти слідування зарядних імпульсів: 50 Гц і 25 Гц. Кратність з частотою електромережі дозволяє створювати порівняно нескладні пристрої для отримання керуючих імпульсів напруги, синхронних з частотою електромережі, і отримувати на батареї зарядні струми будь-якої величини, які обмежуються тільки можливістю ключового елемента.

Основним фактором подовження терміну експлуатації акумуляторів є організація правильного циклу заряду. Без цієї необхідної умови ефективність роботи останнього знизиться, а згодом підвищиться ймовірність виходу з ладу. Впровадження мікроконтролеру в зарядному пристрою дозволить: по-перше, забезпечити необхідний алгоритм заряду, що суттєво подовжить термін служби акумулятора завдяки дотриманню необхідних умов експлуатації; по-друге, реалізується процес автоматичної зарядки з мінімальним втручанням користувача; по-третє, забезпечить зручність і простоту використання пристрою.

Інтелектуальні методи при вирішенні поставленої задачі дозволять створити базу даних для збереження початкових технічних характеристик кожного акумулятора та їх зміну в процесі зарядки. При цьому виробляються рекомендації та реалізується алгоритм для підтримки оптимальних умов процесу зарядки.

Використання інтелектуального зарядного пристрою на основі мікроконтролерів для управління, контролю та діагностики акумуляторів дозволяє значно оптимізувати процес зарядки акумуляторів та збільшити термін їх експлуатації.

УДК 621.382.2/.3

Семеніхін Д. О.
Харківський національний університет радіоелектроніки

Моделювання МЕМС сенсорів з використанням Matlab/Simulink

Мікромеханічний пристрій, вбудований в електронну систему, виготовлений з використанням змішаної технології виробництва інтегральних мікросхем і мікрообробки, називається мікроелектромеханічною системою Microelectromechanical System (MEMS) [1].

Існують два типи автомобільних сенсорних компонентів [2]:

а) датчики типу plug & play, що являють собою пристрої в захисному корпусі з автомобільними з'єднувачами, що містять друковані плати, на яких розміщені сенсорні та електронні компоненти;

б) мікроелектронні сенсорні компоненти в корпусах з виводами для монтажу на друковану плату.

Зазначені пристрої можна віднести до макрорівня (сенсорні пристрої та системи) і мікрорівня (мікроелектроніка та мікросистемотехніка, мікромеханіка і мікрооптика) відповідно.

В автомобільній галузі використовуються сенсорні системи, які можна класифікувати за призначенням або типами пристроїв (датчики положення, температури, прискорення, тиску), технологіям (CMOS, МЕМС, індуктивні датчики), застосуванню (ESC, системи безпеки або контролю та управління двигуном).

Інтегральна схема, модуль, плата можуть одночасно виконувати кілька сенсорних функцій за рахунок об'єднання декількох сенсорних пристроїв. Розвиток нанотехнологій обумовив їх проникнення в транспортну галузь і автомобільну сенсорику. Інтеграція нанотехнологій і МЕМС в макросистеми дозволяє виробляти та використовувати «розумні» матеріали, обладнання й системи.

Одним з найбільш популярних засобів поведінкового моделювання мікроелектромеханічних систем є Simulink, який являє собою набір інструментів, вбудованих в середовище Matlab [3], що дозволяє здійснювати системне моделювання з урахуванням часу.

Механічний чутливий елемент акселерометра може бути описаний диференціальним рівнянням першого порядку мас-демпферної-пружинної системи. Діапазон переміщення контрольної маси обмежений механічним стоппером, який має деяке відхилення від положення спокою на початку моделювання. На вхід моделі впливає зовнішня інерційна сила, а на виходах визначаються зміщення, швидкість, і прискорення маси як реакція на вхідну силу.

Модель сенсорного елемента акселерометра наведена на рис. 1 і містить контролер обмеження переміщення, який має два входи: вхідне прискорення, що діє на чутливий елемент, і зміщення контрольної маси. Контролер визначає нелінійну поведінку сенсорного елемента в разі, якщо контрольна маса торкається механічних стопперів. У цьому випадку швидкість контрольної маси зменшується до нуля.

Модель сенсорного елемента як підсистеми сенсорної системи містить контур керування зі зворотним зв'язком за силою. Модель описує динаміку сенсорного елемента, перехід від зсуву до диференціальної ємності і напруги, сигма-дельта модуляторні блоки керування і схеми зі зворотним зв'язком. Використовується припущення, що контрольна маса розміщена між двома електродами конденсатора, зміщення може бути перетворено в диференціальну зміну ємності, що моделюється за допомогою реалізації математичного функціонального блоку рівняння з допомогою паралельних ємностей пластин. Диференціальна ємність може бути визначена за

допомогою електронної схеми вимірювання положення, яка в першому порядку може бути представлена блоком посилення моделі. До складу моделі входять компаратор, зразок і утримувач для моделювання системи управління сигма-дельта. На лінії зворотного зв'язку розраховуються електростатичні сили, що діють на контрольну масу, якщо один з двох електродів включений. Сили зворотного зв'язку підсумовуються з будь-якою зовнішньої інерційною силою, що діє на контрольну масу. Результати моделювання наведено на рис.2.

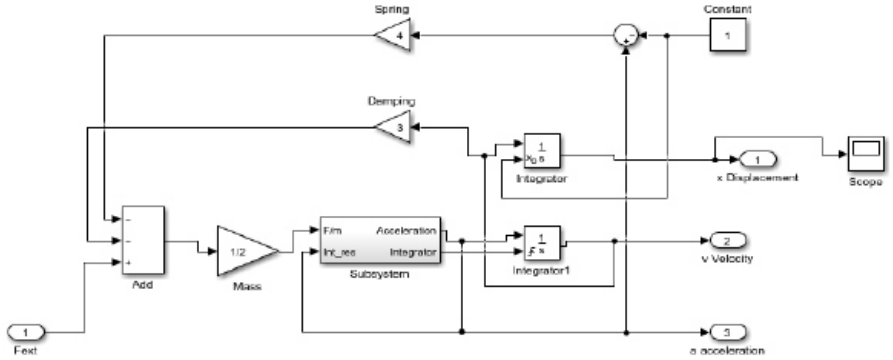
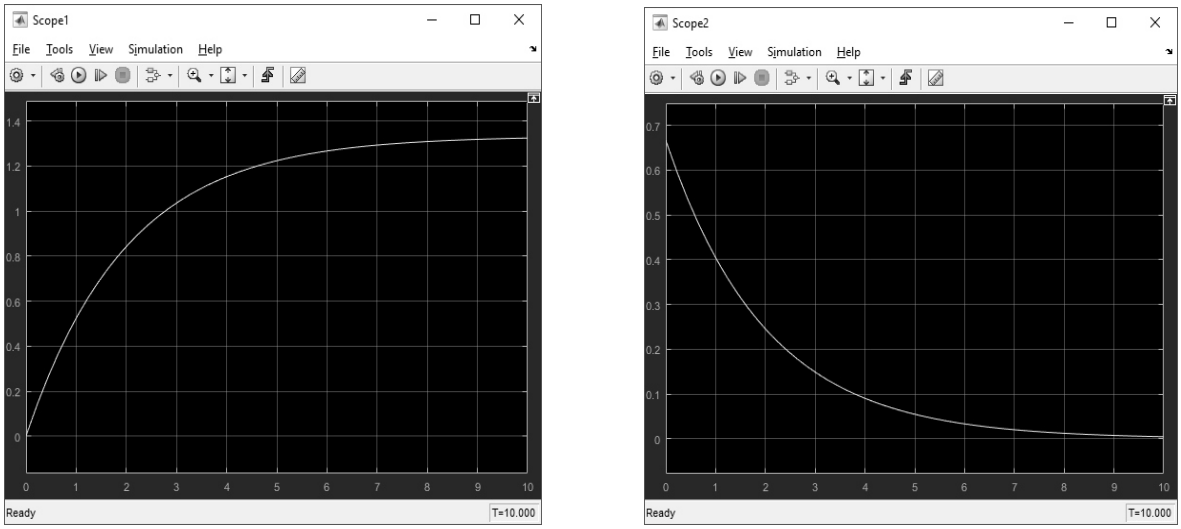


Рисунок 1 – Simulink модель сенсорного елемента акселерометра

Описана модель дозволяє оптимізувати такі параметри проектування: площа електроду, постійна пружини, контрольна маса, необхідний коефіцієнт посилення електронного сигналу і частота дискретизації.



а) б)

Рисунок 2 – Результати моделювання: а) Velocity – швидкість;
б) Acceleration – прискорення

Список використаних джерел

1. *Introduction and application areas for MEMS. Електронний ресурс. 03-01-17. Режим доступу: http://www.eeherald.com/section/design-guide/mems_application_introduction.html.*
2. *Сысоева С. Три уровня автомобильных сенсорных инноваций: макро, микро и нано // Компоненты и технологии.– № 1.– 2010.*
3. *Beeby S. MEMS Mechanical Sensors / S. Beeby, G. Ensell, M. Kraft, N. White. – Artech House, Inc. Boston – London. – 2004.*

УДК 004.056.53+614.844

Сенько А. О., Андрющенко Д. Ю.
Криворізький національний університет

Дослідження структури статичного ОЗП

Оперативна пам'ять призначена для зберігання змінної інформації, так як допускає зміну свого вмісту під час виконання мікропроцесором обчислювальних операцій. Таким чином, цей вид пам'яті забезпечує режими запису, зчитування і зберігання інформації. Завданням є дослідження принципу побудови і структурної організації ІМС ОЗП К176РУ2, елементів у складі схеми.

[1]. Мікросхема К176РУ2 з організацією 256×1 з керуванням, виготовлена за технологією КМОП та складається з 2088 інтегральних елементів, представляє з себе ЗП зі структурою 3D. Вибір елемента пам'яті здійснюється не за однією шиною, а за двома (по рядкам і стовпцям). Функціональна схема такого ОЗП ємністю 256 біт (рис.1).

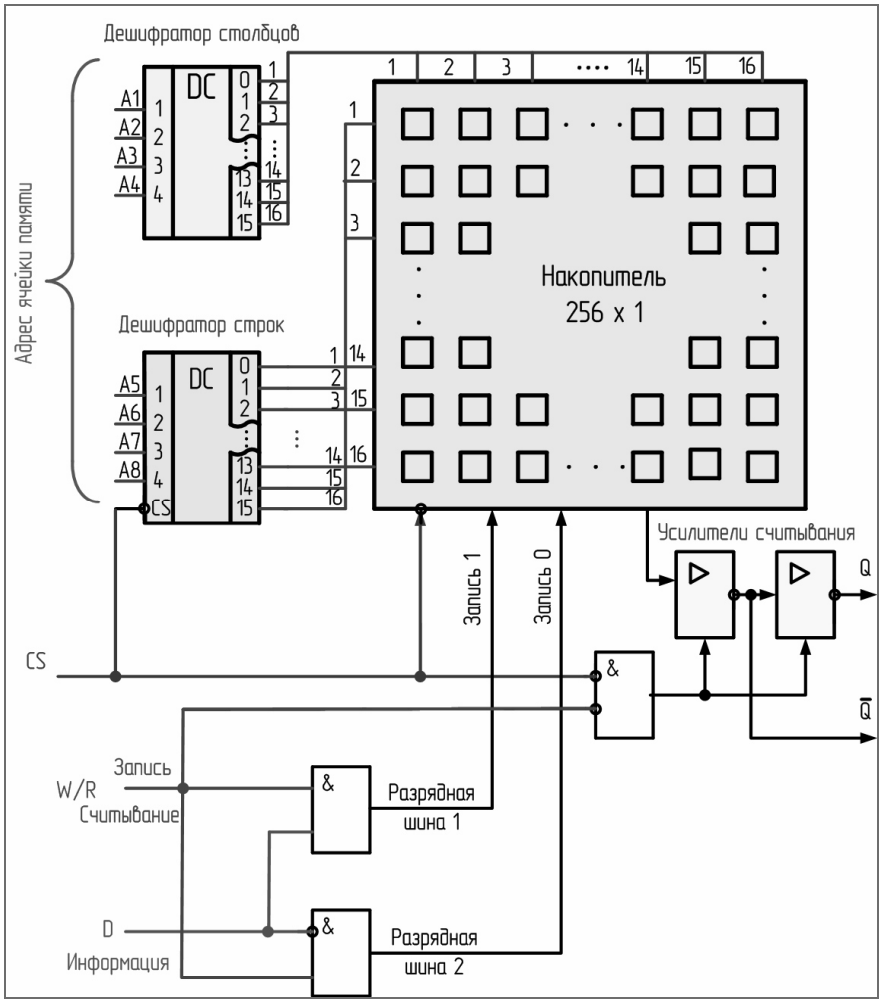


Рисунок 1 - Функціональна схема ІМС К176РУ2

Схема містить два дешифратора: DC стовпців і DC рядків. Дешифратори мають по 4 входи, на які подається по 4 розряди із загальної 8-розрядної адреси, і по 16 виходів. Схема елемента пам'яті даної мікросхеми представлена на (Рис.2).

Кожен елемент пам'яті є статичним RS-тригером. Тригер має два парафазних входи / виходи. З розрядними шинами РШ0 і РШ1 тригер з'єднаний через ключі VT5 і VT6. За розрядними шинами до тригеру підводиться під час запису і відводиться при зчитуванні інформація в парафазній формі подання по РШ1 своїм прямим значенням, а по РШ0 - інверсним.

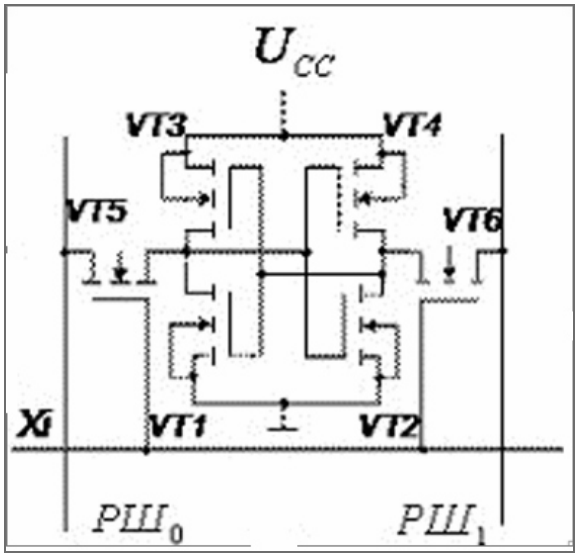


Рисунок 2 - Схема елемента пам'яті ІМС К176РУ2

[2]. В режимах «Запис» і «Зчитування» при збудженні рядка сигналом вибірки Xi=1, що знімаються з дешифратора адреси рядків, ключі VT5 і VT6 відкриваються і підключають тригер до розрядних шин. При X = 0 ключі закриті і тригер відключений (ізольований) від шин, а інформація в них зберігається. При зчитуванні інформації ключі підключають елемент пам'яті до розрядних шин, вони приймають потенціали виходів тригера і через пристрій вводу / виводу передають їх на вихід мікросхеми. Розрядні шини охоплюють всі елементи одного стовпчика, а переходить в активний стан тільки один ЕП, відповідний вибраному рядку. З нього і зчитується інформація. Режими роботи ІМС К176РУ2 наведені в (табл. 1)

Таблиця 1 - Режими роботи ІМС К176РУ2

CS	W / R	Функція
1	1	Запис у обрану комірку
1	0	Зчитування з обраної комірки
0	1	Зберігання інформації
0	0	Зберігання інформації

Отже завданням було дослідження організації, структури і принципу роботи статичного ОЗП К176РУ2. Був проведений аналіз принципів побудови і структурної організації мікросхем статичних RAM, проводилося дослідження інтегральної мікросхеми ОЗП К176РУ, визначення її особливостей та характеристик.

Список використаних джерел

1. *Марухин А. Запоминающие устройства [Електронний ресурс] / Алексей Марухин // Запоминающие устройства. – 2009. – Режим доступу до ресурсу: http://www.plam.ru/radioel/ lekcii_po_shemotehnike/p7.php*
2. *Селецкая Л. Напівпровідникові запам'ятовуючі пристрої [Електронний ресурс] / Людмила Селецкая // Напівпровідникові запам'ятовуючі пристрої 2015. – Режим доступу до ресурсу: http://ratusny.vk.vntu.edu.ua/file/bd6edcc39ee4baade3bc262eeb455075.pdf*

УДК 004.92

Абель Т. В., Дрєєва Г. М.
Центральноукраїнський національний технічний університет

Дослідження та програмна реалізація системи генерування зображення за допомогою рекурентних повторень

Складність будови об'єктів живої та неживої природи змушує людей, які вирішили присвятити життя створенню комп'ютерної графіки, звертатися за допомогою до спеціальних програм-генераторів. Суспільство роками застосовувало комп'ютерні технології в усіх галузях діяльності людини, в тому числі у мистецтві.

2D- і 3D-графіка широко застосовується у ілюстраціях, рекламі, топографії, навчанні, дизайні та багатьох інших галузях праці та розваг людини. Зрозуміло, що для забезпечення достатнього обсягу графіки слід витрачати величезну кількість зусиль, у той же час не знижуючи рівень якості продукту. Бажання заощадити час і звичайний досвід підказують, що слід автоматизувати процес.

На сьогоднішній день, у Світовій мережі можна знайти безліч генераторів рослин, ландшафту та інших природних об'єктів. Звісно, такі об'єкти можна створити і вручну – людина безперечно здатна виконати будь-яку роботу, - але перевагою автоматичного генерування є швидкість і висока деталізація отриманих зображень. Для прикладу, у будь-якому редакторі тривимірної графіки можна легко створити дерево з кількома гілками, що ростуть зі стовбура. Підемо далі й додамо кілька нових гілок, що тепер беруть початок від гілок, створених на попередньому кроці. Вже складніше? Тепер спробуймо додати нові гілки за тим же принципом і повторити всі ці кроки ще разів з десять. Автоматизація побудови такого об'єкту, як дерево, опирається на рекурсивний алгоритм, а самі ці об'єкти вирізняються фрактальною структурою.

Фракталом називають складну геметричну фігуру, яка володіє властивістю самоподоби, тобто яка складена з частин, подібних цілій фігурі. Фрактали бувають кількох видів: геометричні, алгебраїчні та стохастичні фрактали. Останні – мабуть, є найбільш особливими: вони отримуються у тому випадку, коли в ітераційному процесі випадковим чином змінювати деякі його параметри. При такому підході отримані об'єкти дуже схожі на природні – несиметричні дерева, рвані берегові лінії і т.д.

Рисунок 1 – Віртуальне дерево

Генератори ландшафтів дозволяють відносно швидко створювати фото-реалістичні земні та інопланетні пейзажі, які часом за красою й реалістичністю

неможливо відрізнити від справжніх фото. Штучні ландшафти можуть стати основою для різноманітних 3D-сцен у тривимірних іграх, при підготовці телевізійних заставок і кліпів. Однак кожна з представлених систем генерування тривимірних об'єктів є спеціалізованим продуктом або плагіном для тривимірного редактору зі своїми унікальними алгоритмами та принципами роботи. В той самий час, по факту всі генератори фрактальних об'єктів є різноманітними реалізаціями кількох алгоритмів, зокрема генерування на базі ініціатора та генератора [1–3]. В досліджені пропонується створення програмного продукту уніфікації алгоритму побудови фрактальних поверхонь та об'єктів, що в свою чергу значно підвищить коло його застосування.

Розроблений програмний продукт має отримати в якості параметрів меш ініціатор, меш генератор та кількість рекурентних циклів генерування. На основі цих вхідних даних, в залежності від ініціатора, будується тривимірний фрактальний об'єкт або фрактальна поверхня.

Для реалізації фрактального генератора було введено поняття початкового об'єкту ініціатора, який може бути триангульованою поверхньою або триангульованим тілом, та генератора – триангульована поверхня або тіло, яке повинне замінювати структури подібні, в розумінні інваріантності відносно афінних перетворень, до ініціатора. В процесі застосування правил заміни на генератор, система оброблює лише лицьові сторони трикутників, що й дозволило наряду з поверхнями типу ландшафту, генерувати й замкнені об'єкти схожі на дерева та рослини. З метою імітування природніх процесів при генеруванні використовуються випадкові зміщення точок в межах зазначених в налаштуваннях генератора. Регулювання випадкових зміщень покладено на оператора, бо низькі значення призводять до малих відхилень форм від базової, а завеликі випадкові відхилення призводять до самоперетину утворених поверхонь. На даному етапі система не має можливості генерування й текстур, бо широка застосовність системи не дозволяє уніфікувати розрахунки текстурних координат. Але звуження задачі, скажімо до отримання ландшафтів, дозволяє будувати текстурні координати в залежності від висоти над «рівнем моря», що планується урегулювати текстурними плагінами до основної програмної системи.

Результат генерується у вигляді текстового obj формату задання тривимірних фігур. Це дає перевагу застосовності програмного продукту до більшості редакторів тривимірного векторного зображення.

Висновок. Спроектовано програмний продукт для побудови складних тривимірних поверхонь та об'єктів за правилами генерування фракталів, що відповідають L-системам. Програмний продукт має більш широке використання і може бути використаний як для генерування ландшафтів, астероїдів та таких об'єктів як дерева.

Список використаних джерел

1. *Rozenberg, G. & Salomaa, A. (2001), "L-systems", in Hazewinkel, Michiel, Encyclopedia of Mathematics, Springer, ISBN 978-1-55608-010-4*
2. *Andrew Robert Owens Modeling Dense Inflorescences. DEPARTMENT OF COMPUTER SCIENCE, CALGARY, ALBERTA December, 2016. 102 с.*
3. *Болотов В., Кондо Ю. 3D-фракталы для слепых реализация в системе Вектор /В.Болотов, Ю.Кондо// url: http://old.msun.ru/Vector/%D0%A4%D1%80% %D0%BE%D1%80.htm*
4. *Mandelbrot B.B. The Fractal Geometry Of Nature. – Freeman, San Francisco, 1982.*

УДК 004.92

Гіцеларь Д. В.[*]
Центральноукраїнський національний технічний університет

Огляд та практичне застосування L-систем

L-система також відома як система Ліденмайера. L-системи запропонував і розвивав в 1968 Арістід Ліденмайер, угорський біолог і ботанік з Утрехтського університету. Ліденмайер використовував L-системи для опису поведінки клітин рослин і моделювання процесу розвитку рослини. L-системи використовувалися також для моделювання морфології різних організмів [1] і можуть бути використані для генерації самоподібних фракталів, таких як системи ітеративних функцій.

Основна ідея L-системи - постійний перезапис (rewriting) елементів рядка. Якщо коротко, rewriting - це спосіб отримання складних об'єктів шляхом заміни частин простого початкового об'єкта за деякими правилами. Класичним прикладом є сніжинка. На Рисунку 1 initiator - це початковий об'єкт, межі якого замінюються на generator. Далі з новим об'єктом проробляється те ж саме. В даному випадку звичайний фрактал.

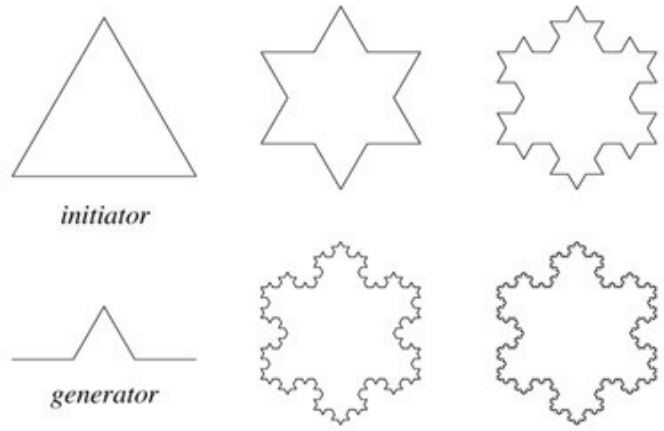


Рисунок 1 – Ілюстрація принципу функціонування L-системи

Рекурсивна природа правил генерації моделей призводить до самоподібності і тому подібні фракталам форми легко описуються за допомогою L-системи. Моделі рослин і органічних форм, що мають природний вигляд, легко сформувати, так як при збільшенні рівня рекурсії модель повільно «росте» і стає більш складною. Системи Ліденмайера популярні також в генерації штучного життя.

L-системи тепер відомі як параметричні L системи, які визначаються як кортеж:

$$G = (V, \omega, P),$$

де:

- V (алфавіт) - це множина символів, що містять як елементи, які можуть бути замінені (змінні), так і елементи, які не можуть бути замінені ("константи" або "термінальні символи");

- ω (старт, аксіома або ініціатор) - це рядок символів з V, який визначає початковий стан системи;

- P - це множина породжуючих правил, що визначають, яким чином змінні можуть бути замінені комбінаціями констант та інших змінних. Породжуюче правило складається з двох рядків, прототип і наступник. Для будь-якого символу A, що входить в

[*] Науковий керівник – Гермак В. С., викладач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету

алфавіт V, що не входить в ліву частину правил P, передбачається правило виведення A → A. Ці символи називаються константами або термінальними символами. [2]

Правила граматики L-системи застосовуються ітеративно, починаючи з аксіоми (початкового стану). На ітерації застосовується якомога більше правил. Факт, що на кожній ітерації застосовується якомога більше правил, відокремлює L-систему від формальної мови, що генерується формальною граматикою, яка застосовує тільки одне правило на ітерацію. Якби правила виведення застосовувалися по одному, легко було б згенерувати мову, а не L-систему. Таким чином, L-системи є підмножиною мов.

Приклад 1: Водорості

Оригінальна L-система Ліденмайера для моделювання росту водоростей.

змінні: A, B; константи: немає;

аксіома: A; правила: (A → AB), (B → A)

Система дає

n = 0: A;

n = 1: AB;

n = 2: ABA;

n = 3: ABAAB;

n = 4: ABAABABA;

n = 5: ABAABABAABAAB;

n = 6: ABAABABAABAABABAABABA.

Приклад 2: Крива дракона

Крива дракона, намальована за допомогою L-системи.

змінні: X Y; константи: F + -;

старт: FX; правила: (X → X + YF +), (Y → -FX-Y)

кут: 90 °

Тут F означає «малюємо відрізок», - означає «повернути вліво на 90 °», а + означає «повернути вправо на 90 °». X і Y не відповідають якій-небудь дії при малюванні, а використовуються тільки для побудови кривої.

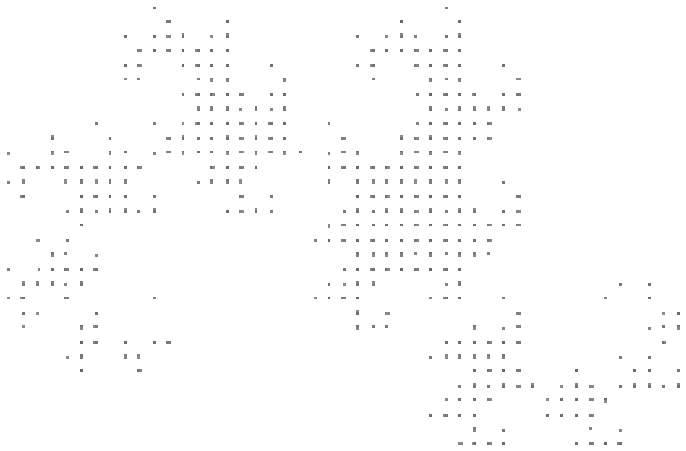


Рисунок 2 – Крива дракона для *n* = 10

Таким чином L-системи слід брати до уваги як зручний інструмент для створення моделей, в основі яких лежить рекурсія. Вони будуть корисними при побудові елементів комп'ютерної графіки. Конкретніше, можуть добре допомогти при демонстрації біологічних процесів в навчальних цілях або у звичайних комп'ютерних іграх.

Список використаних джерел

1. *Grzegorz Rozenberg, Arto Salomaa. The mathematical theory of L systems. — New York: Academic Press, 1980.*
2. *L-система [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/L-%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0.*
3. *valyard. L-Systems — математическая красота растений [Електронний ресурс] / valyard. – 2009. – Режим доступу до ресурсу: https://habr.com/post/69989/.*

УДК 004.092

Долженко І. О.
Харківський національний університет радіоелектроніки

Дослідження методів сегментації для розпізнавання харчових об'єктів

Людей по всьому світу все частіше і частіше починає турбувати їх здоров'я, харчування і вага. Доступно безліч систем для вимірювання кількості спожитих калорій за фотографіями їжі до і після їди. Належна обробка і сегментація зображення це один з найважливіших етапів, необхідних для проведення аналізу зображення.

Зазвичай зображення харчових продуктів використовуються в системах що вимірюють харчову цінність продуктів для подальшого розрахунку кількості спожитих калорій. Розрахунок проводиться шляхом аналізу зображення харчового продукту до того, як його почали їсти і після. Звичайна людина не може неозброєним оком визначити точну кількість калорій, яке містить споживана їм їжа. Так що останнім часом спостерігається гостра потреба в системах, які б могли стежити за дієтою людини і контролювати споживання їжі згідно дієті якої дотримується людина. Системи комп'ютерного зору допомагають в обробці будь-якого типу зображень і вилучення значимої інформації з них. Зображення є одним з найбільш повних уявлень об'єктів реального світу у вигляді цифрових даних, які, крім того, легко піддаються обробці. В аналізі зображень найголовнішим кроком для подальшої обробки є сегментація і від якості сегментації залежить точність результатів, отриманих в ході подальшої обробки зображення.

Сегментація зображення - це процес розділення цифрового зображення на декілька сегментів, тобто пошук пікселів, в області, які є в якійсь мірі схожими за певними критеріями, таким як колір, насиченість або текстура, ця інформація використовується для ідентифікації меж об'єктів, представлених на зображенні. Методи сегментації зображення переважно поділяються на три категорії.

Порогові методи конвертують кольорове зображення в монохромне і відділяють області інтересу від заднього фону. У порогових методах одиниця позначає передній план, а нуль представляє задній план зображення. У методах виявлення країв виділяються края, за допомогою яких різні регіони зображення відокремлюються одна від одної. Метод, заснований на кластеризації, є ітеративним методом, який використовується, щоб розділити зображення на K кластерів. Так само, кластеризація є некерованим методом. У методі розростання областей використовується задані умови або «насіння» і результат сегментації залежить від цих даних.

Пороговий метод сегментації досить простий в порівнянні з іншими методами сегментації, в ньому задається одне значення, граничне, і використовується для поділу зображення в основному на два сегменти передній і задній план. Значення T, яке задано як поріг і зображення, в якому кожен піксель (x, y) насиченість якого перевищує порогове значення позначається одиницею в зворотному випадку позначається нулем. Існує два порогових методу: метод глобального порога і метод локального порогу. У випадках, коли насиченість пікселів заднього і переднього планів сильно відрізняються один від одного використовується метод глобального порога.

Метод визначення меж використовується для сегментації шляхом виявлення меж або пікселів, розташованих між різними регіонами, які мають явний перехід в значеннях насиченості. Такі пікселі об'єднуються і формують контур майбутнього регіону. Результатом роботи цього алгоритму є бінарне зображення. Робота алгоритму розділена на три кроки звані: фільтрація, покращання і виявлення.

У методі вирощування регіонів, пікселі групуються в різні регіони по заздалегідь заданим умовам або заданої зернової точці. Вибирається початкова точка на вихідному зображенні після, задаються певні критерії, за якими відбувається пошук схожих пікселів. Коли не залишається пікселів, що підходять усім заданим критеріям зростання регіону зупиняється.

Методи поділів і об'єднання замість заданої початкової точки, поділяють зображення на групи окремих регіонів і після регіони об'єднуються відповідно до заданих умов сегментації. Якість сегментації залежить від заданих параметрів. Недоліками методу є його складність і низька швидкість роботи.

Алгоритм К-середніх (k-means) передбачає швидкий кластерний аналіз шляхом виділення К сегментів (кластерів), які розташовуються на максимальній відстані один від другого. Число кластерів К вибирається, спираючись на результати експериментів або інтуїтивно. Ідея алгоритму полягає в тому, що центри кластерів відповідають локальним максимумам щільності розподілу даних. Базовий алгоритм К-середніх передбачає випадковий або евристичний вибір К центрів кластерів, розміщення кожного пікселя зображення в кластер з найближчим центром до цього пікселя, після чого заново перераховуються центри кластерів до збіжності процесу. Алгоритм гарантовано сходиться, але не обов'язково призводить до оптимального рішення, оскільки залежить від початкової множини кластерів і значення К.

У цій роботі був проведений аналіз і вивчення різних методів і технік сегментації зображень. Щоб вивчити різні методи сегментації зображень, були взяті зображення їжі з мережі інтернет. В основному вхідні зображення, включали різні фрукти, овочі, усі вхідні зображення мають різний фон і розмір. Для експерименту в якості вхідних даних приймається розмір зображення 200 * 200 пікселів і 10 різних зображень. Методи сегментації зображень, засновані на пороговому значенні, виявленні країв і кластеризації, застосовуються на вхідних зображеннях для сегментації вхідного зображення. Результати роботи методів сегментації розглядаються у вигляді візуальних оцінок і кількісних показників. У методі граничних значень для вхідних зображень застосовується глобальне порогове значення і багаторівневе колірне порогове значення. У глобальному пороговому значенні існує багато яскравих областей, що відносяться до переднього і заднього плану, і які нижче порогового значення і тому призводять до помилково виділеним сегментам. Схожі результати були отримані в багаторівневої або кольоровий розбивці на бінарні зображення, які лише виділяють яскраві області вхідного кольорового зображення шляхом налаштування порогового значення. Метод виявлення краю дає чіткі результати в порівнянні з методом порогового значення. Він виявляє всі контури на зображенні, але також виявляються додаткові контури, які мають меншу насиченість, ніж граничне значення. Алгоритм К-середніх, який використовує маску фільтра Sobel для виявлення країв в двох напрямки по вертикалі і по горизонталі, дає кращі результати. Але у нього висока складність обчислень. Методи Кластеризація та порогового значення дають майже однакові результати, але метод кластеризації враховує всі три площини для сегментації вхідного зображення. Метод кластеризації дає кращі результати в поставленому завданню, оскільки він виявляє краю в вертикальному і горизонтальному напрямках, хоч і не виявляє краю в діагональних напрямках і обчислювально складний.

Список використаних джерел

1. Гонсалес Р., Вудс Р., Цифрова обробка зображень. — Техносфера, 2005, 2006. — 1072 с

2. Потапов А. А., Пахомов А. А., Никитин С. А., Гуляев Ю. В., Новітні методи обробки зображень. — Физматліт, 2008. — 496 с.

УДК 004.9

Карпов Є. О.
Центральноукраїнський національний технічний університет

Особливості комп'ютерної графіки в контексті Net-Art

Комп'ютерна графіка – в науці це розділ інформатики, який вивчає методи цифрового синтезу і обробки візуального контенту, але все знають її як вид сучасного мистецтва, яке також називають цифровим, що входить до загального медіа-арту – зображення, які створюються, перетворюються, оцифровуються, обробляються і виводяться засобами обчислювальної техніки, включаючи апаратні і програмні засоби, рухома комп'ютерна графіка називається комп'ютерним відео або комп'ютерною анімацією [1].

Робота з комп'ютерною графікою – один з найпопулярніших напрямків використання персонального комп'ютера, до того ж займаються цією роботою не тільки професійні художники і дизайнери. На будь-яких підприємствах час від часу виникає необхідність в подачі рекламних оголошень в газетах і журналах або просто у випуску рекламної листівки або буклету. Без комп'ютерної графіки не обходиться жодна сучасна мультимедійна програма. Робота над графікою займає до 90 % робочого часу програмістських колективів, які випускають програми масового застосування.

З розвитком комп'ютерної графіки сформувався новітній вид мистецтва, що розвивається в комп'ютерних мережах, зокрема, в мережі Інтернет – Net-Art. Цей напрямок мистецтва найбільш інтерактивний з усіх існуючих, і на сьогоднішній день більшість мережевих проектів - динамічні аудіовізуальні структури, які миттєво реагують на зміни зовнішнього середовища [2].

Сучасне мережеве мистецтво формується на стику різних, часом суперечливих явищ: індивідуальної творчості і нових технологій, масової культури і субкультури. У широкому сенсі до Net-Art можна віднести безліч різних явищ цифрової графіки та медіа-мистецтва, так як практично всі вони створюються цифровими засобами виключно для експонування в Інтернет середовищі, «виведення» на папір або на полотно не відбувається, полотном для цих творів стає монітор, а простором для виставки - Інтернет.

Цифрова живопис пропонує художнику більш широкий арсенал творчих можливостей: від створення абстрактних композицій до створення складних жанрових творів, властивих традиційній графіці і живописі, з використанням двомірної і тривимірної комп'ютерної графіки [3].

Не дивлячись на те, що для роботи з комп'ютерною графікою існує маса класів програмного забезпечення, розрізняють основні види комп'ютерної графіки: растрова, векторна і фрактальна графіка. Вони відрізняються принципами формування зображення при відображенні на екрані монітора або при друці на папері.

Растрову графіку застосовують при розробці електронних (мультимедійних) і поліграфічних видань. Більшість графічних редакторів, які призначені для роботи з растровими ілюстраціями, орієнтовані не стільки на створення зображення, скільки на їх обробку. В Інтернеті поки що використовують растрові ілюстрації.

Програмні засоби для роботи з векторною графікою, навпаки, призначені, в першу чергу, для створення ілюстрацій і в меншій мірі для їх обробки. Оформлювальні роботи, основані на застосуванні шрифтів і простих геометричних елементів, вирішуються засобами векторної графіки набагато простіше. Існують приклади високохудожніх творів, створених засобами векторної графіки, але вони скоріше виключення, ніж правило, оскільки художня підготовка ілюстрацій засобами векторної графіки надзвичайно складна.

Програмні засоби для роботи з фрактальною графікою призначені для автоматичної генерації зображення шляхом математичних розрахунків. Створення фрактальної художньої композиції полягає не в рисуванні чи оформленні, а в

програмуванні. Фрактальну графіку рідко використовують для створення друкованих або електронних документів, але її часто використовують у розважальних програмах.

Наступний аспект мережевого мистецтва полягає в освоєнні можливостей віртуальної реальності, всередині якої можна створювати щось зовсім нове, оскільки можливості мережі Інтернет набагато ширше можливостей навколишнього нас реального світу. Яскравим прикладом можуть служити комп'ютерні ігри, які також представляють собою один з аспектів Net-Art.

Одним з головних критеріїв Net-Art є співавторство в творчому процесі кожного користувача мережі. Сам художник створює основну ідею, контекст і засоби для втілення цієї ідеї, за допомогою яких користувач може проявити свою фантазію і творчий потенціал. Як матеріальний об'єкт інтернет - твір не існує, тобто він представлений у формі безперервного художнього спілкування між автором і користувачами інтерактивного простору. Художня і рекламна графіка стала популярною багато в чому завдяки телебаченню. За допомогою комп'ютера створюються рекламні ролики, мультфільми, комп'ютерні ігри, відеоуроки, відеопрезентації. Відмінною особливістю цих графічних пакетів є можливість створення реалістичних зображень і анімації.

Мультимедійні мережеві проекти не тільки ставлять перед глядачем питання, але і, отримавши зворотний зв'язок, миттєво реагують на нього, залучаючи глядача в комунікативний процес. Його інтерактивність відповідає простору комунікації, що змінюється під впливом віртуалізації.

Net-Art може комунікувати з глядачем, використовуючи агресивні засоби, іноді нагадуючи комп'ютерні віруси або флешмоби, але мета завжди - не захоплення, а розхитування звичних ілюзій сприйняття, створених масовою культурою, залучення глядача в діалог. Глядач добровільно приймає запропоновану художником гру і в будь-який момент може вийти з неї, а художник, в свою чергу, не намагається видати свою гру за реальність і завжди нагадує, що це гра, навіть коли вона здається абсолютно реальною. Глядач-учасник Net-Art творів не пасивний як, наприклад, глядач-споживач медіареальності, в кожен момент часу він вибирає, думає, творить свій твір.

Прикладами Net-Art можуть служити сайти, які побудовані на таких ідеях, як малювання голосом, використовуючи мікрофон комп'ютера. Залежно від динамічної звукової градації лінії на віртуальному полотні будуть міняти форму або напрям. А «мелодії» зі світлових потоків можна створювати на сайті, де існує можливість направляти промені під певним кутом.

Таким чином, специфічна особливість мистецтва віртуальної реальності полягає в його інтерактивності, що дозволяє відтворити уявний образ через реальну дію. Перетворення інтерактивного користувача з спостерігача в співавтора формує новий тип естетичного мислення. Зростання популярності Net-Art свідчить про життєздатність нового напряму в мистецтві, що зародився в незвичайних умовах - в мережі Інтернет.

Вочевидь, сформований світ техно-художніх форм і гібридів демонструє нові можливості в їх використанні як інноваційних ресурсів для практичного освоєння нових технологій в креативних індустріях (дизайні, архітектурі), науці, медицині та інших областях. Це має величезне значення, оскільки Net-Art відображає нерозривний зв'язок між науковими і технологічними досягненнями, художніми практиками та суспільними змінами.

Список використаних джерел

1. *Летин, А.С. Компьютерная графика / А.С. Летин, О.С. Летина, И.Э. Пашковская. // М.: ГОУВПО «МГУС», 2005. - 125 с.*
2. *Турлюн Л.Н. Компьютерная графика – искусство постмодернизма / Л.Н. Турлюн // Молодой ученый. - 2010. - №12. Т.2. - С. 186-189.*
3. *Berry D.M. Thinking Postdigital Aesthetics : Art, Computation and Design / Berry D., Dieter M. // Postdigital Aesthetics : Art, Computation and Design / ed. by D.M. Berry, M. Dieter. [S.l.] : Palgrave Macmillan, 2015. P. 1—11.*

УДК 004.925

Ладигіна О. А.
Центральноукраїнський національний технічний університет

Аналіз моделей освітлення для досягнення фотореалізму у віртуальній реальності

Створення реалістичного освітлення в сцені - одна з найбільших проблем при розробці тривимірної графіки. Щоб тривимірні моделі виглядали природно на візуалізованому зображенні, їх необхідно правильно висвітлити. Сцена є лише спрощеною фізичною моделлю, тому візуалізоване зображення далеко не завжди походить на натуральне. Але незважаючи на це, освітлення в тривимірній сцені все ж можна наблизити до реального. Для цього потрібно виконувати два правила: встановити джерела світла і підібрати їх яскравість таким чином, щоб сцена була рівномірно освітлена; задати налаштування візуалізації освітлення.

Відповідно до прийнятого в комп'ютерній графіці підходом, розрахунок освітленості розпадається на дві основні задачі: визначити спосіб розрахунку освітленості в довільній точці тривимірного простору, вирішується за допомогою побудови локальної математичної моделі освітленості; застосування локальної математичної моделі освітленості для комп'ютерних розрахунків освітленості тривимірних об'єктів з конкретною геометрією і властивостями поверхні, вирішується за допомогою моделі затінення.

Побудова фотореалістичних зображень складних сцен, що містять об'єкти зі спеціальними властивостями пропускання, відбиття та розсіювання, вимагає застосування фізично акуратних моделей розрахунку яскравості, що формується цими об'єктами.

Вибір моделі освітлення залежить від кількості об'єктів, відбивних властивостей їх матеріалів, а також від геометрії сцени, який тип джерела світла використовується. Наприклад, направлене джерело світла дозволяє сконцентрувати увагу на якомусь певному об'єкті, а всенаправлене точкове джерело - освітити сцену цілком.

Моделі освітлення являють собою апроксимації законів фізики, що описують ефекти освітлення поверхні. Щоб скоротити обсяг обчислень, в більшості пакетів використовуються емпіричні моделі, що засновані на спрощених фотометричних розрахунках. У таких більш точних моделях, як алгоритми дифузного віддзеркалення, для обчислення інтенсивності світла розглядається поширення енергії випромінювання від джерела світла до різних поверхонь сцени.

Існуючі локальні моделі освітлення можна розділити на дві категорії. До першої категорії відносяться емпіричні моделі. Вони зазвичай ефективні в плані швидкодії і деякі з них дають досить реалістичну картинку. Вони зазвичай не оперують такими фізичними величинами, як світлова енергія, або світловий потік. Однак ці моделі знаходять досить широке застосування в областях, де не потрібно точна фізична інформація про висвітлення.

Емпіричні моделі освітлення в комп'ютерній графіці базуються на деякому наборі якісних знань про фізику світла, які можуть бути зведені до наступних:

- поверхні розрізняються по тому, яким чином вони відбивають світло;
- з одного боку існують розсіюють поверхні, для яких світло відбивається в усіх напрямках;
- деякі поверхні відбивають світло, що падає на них, однаково в усіх напрямках;
- з іншого боку існують дзеркальні поверхні, для яких відображення світла відбувається в малій області навколо напрямку відображення;
- деякі дзеркальні поверхні відбивають світло виключно в напрямку відображення.

До другої категорії відносяться теоретичні моделі, що базуються на фізичних уявленнях про теорію світла. Забезпечують точний розрахунок освітлення, а при

поєднанні з алгоритмами розрахунку вторинного освітлення такі моделі дозволяють розраховувати освітлення складних сцен. Зображення, отримані з використанням цих моделей, дуже добре співвідносяться з експериментальними даними. Тому ці моделі знаходять застосування там, де важлива точна імітація поведінки світла.

На основі моделі освітленості можна визначити інтенсивність поверхні в будь-якому спроектованому положенні пікселя. Крім цього, модель освітленості можна застосувати до кількох обраних точок і апроксимувати інтенсивність в інших точках поверхні. Поверхні зазвичай візуалізуються за допомогою алгоритмів рядків розгортки, що скорочують час обробки, оскільки в них використовуються тільки багатокутні поверхні, а розрахунок інтенсивностей проводиться тільки в вершинах цих багатокутників. Потім інтенсивності вершин інтерполюються на інші точки багатокутної поверхні.

Коли враховується не тільки пряма освітленість поверхонь сцени променями, що йдуть безпосередньо від джерел світла, але і вторинна освітленість, що створюється променями, відбитими або заломленими іншими поверхнями, ставиться задача глобальної освітленості. Одним з головних методів вирішення цієї задачі є трасування променів світла з використанням методу Монте-Карло. Для фізичного коректного моделювання освітленості і побудови фотореалістичних зображень використовуються методи прямого і зворотного трасування променів.

Однією з основних проблем, з якими доводиться стикатися при трасуванні шляхів - це оптимальний вибір шляхів з безлічі всіх можливих. У загальному випадку процес трасування стохастичний, і для збіжності в складних сценах може знадобитися розрахунок такої кількості шляхів, що свідомо виводить алгоритм з розряду інтерактивних.

Структури прискорення скорочують час, необхідний для розрахунку фотореалістичної освітленості віртуальних об'єктів шляхом трасування променів. Вони являють собою просторові структури даних, що систематизують об'єкти сцени відповідно до визначених критеріїв. При цьому трасування одного променю вже не перебирає всі трикутники сцени для перевірки перетину з цим променем, а за допомогою даної структури вибирає з них деяку досить малу підмножину.

Загальним недоліком існуючих методів і алгоритмів для структур прискорення трасування є тривалий процес побудови/перестроювання цих структур в разі тривимірних сцен з кількістю полігонів високого порядку. Тому дані методи і алгоритми не можуть застосовуватися при обчисленні освітленості динамічних високополігональних тривимірних сцен в реальному режимі часу, необхідному для моделювання плавного і реалістичного руху об'єктів у віртуальній реальності.

Використання гібридних методів суміщеної візуалізації високополігональних віртуальних сцен дозволяє досягти високої реалістичності синтезованих зображень при збереженні реального режиму часу візуалізації. Наприклад, в об'єднаному використанні трасування променів і шейдерної обробки, де не всі об'єкти віртуальної сцени вимагають повноцінної фотореалістичної якості відображення. Далеко розташовані від спостерігача об'єкти будуть для нього практично однаково виглядати незалежно від того, яким способом вони візуалізовані. Тому, доцільно скоротити на них обчислювальні витрати шляхом відображення їх за допомогою шейдерної обробки, що виконується на порядок швидше трасування променів, але забезпечує менш якісну візуалізацію.

Список використаних джерел

1. *Меженин А.В. Компьютерное моделирование сценариев освещения / Меженин А.В., Сергеева Ю.И // Современные тенденции развития науки и технологий - 2015. - № 3-1. – С. 96- 98.*
2. *Башков Е.А., Реалистическая пространственная визуализация с использованием технологий объемного отображения / Башков Е.А., Зори С.А. // Монография - Донецк, ГВУЗ "ДонНТУ", 2014. - 150 с.*

УДК 004.092

Сахарова А. В.
Центральноукраїнський національний технічний університет

Цифрове оточення людини

У час стрімкого розвитку науково-технічного прогресу, невпинного потоку інформації все більш актуальним стає питання збереження здорової психіки особистості. Людство впевнилося в тому, що досягнення цивілізації мають не тільки позитивні результати.

Останнім часом невід'ємною частиною нашого життя став комп'ютер. Неможливо переоцінити позитивне значення цього науково-технічного досягнення. Однак навіть недовгий період масового користування комп'ютером виявив немало випадків його негативного впливу на людину. Одним з найпопулярніших напрямків використання персонального комп'ютера є робота з комп'ютерною графікою.

Комп'ютерна графіка тривалий час була інструментом створення, обробки, подачі різноманітної візуальної інформації. Згодом масштаби застосування виросли і стали доступними кожній людині, яка має доступ до мережі інтернет. Соціальні мережі, розважальний контент на телебаченні та інтернеті, інформаційні ресурси - все це було розвинуто и покращено за рахунок використання цифрової графіки. Розвиток комп'ютерної графіки в значній мірі змінило наше сприйняття світу і стало невід'ємною частиною нашого повсякденного життя.

Сьогодні по всьому світу відбуваються демонстрації нового рівня розвитку комп'ютерної графіки. Численні виставки присвячені демонстрації нових досягнень в сфери нових можливостей в обробці цифрового зображення [1]. Подібне стало результатом цілої мережі технологічних галузей, що розробляли комплектуючі для ПК та смартфонів. Так само не останню роль в цьому зіграв розвиток штучного інтелекту, що дозволило в більш короткі строки обробляти величезні масиви даних і отримувати результати високого рівня.

Кіберсвіт пристосував традиційні засоби масової комунікації до своїх можливостей. Сьогодні кожний може сам зарезервувати місце в літаку й оплатити переліт за допомогою кредитки. Як гриби після дощу, з'являються Інтернет-магазини, інтерактивні музеї, барвисті тривимірні ілюстрації всіх регіонів і міст світу, що дає можливість подорожувати не виходячи з дому.

Віртуальна реальність приховує величезні можливості. Тривимірний світ вимагає від нас підтвердження автентичності наших слів, переконань, що нерідко вимагає від нас досить великих зусиль. Кіберсвіт усе приймає або за аксіому, або, для контрасту, усе відкидає. Цей світ став таким, в якому тільки думка є сьогоденням, а матерія є ілюзією. І від нас самих залежить дуже багато, навіть то, які емоції ми хочемо відчувати, а які відкидаємо. За допомогою одного кліка мишкою ми можемо опинитися по інший бік земної кулі або в повністю іншій галактиці. Уже зараз в мережі можна зустрічати численні медіа матеріали, що демонструють роботу штучного інтелекту зі зміни зовнішності людей, омолодження акторів або повна заміна обличчя на зовнішність іншої людини, чи результати створення нових графічних матеріалів таких як фотографії не існуючих людей або об'єктів. Так само слід згадати версії технології цифрової графіки для інформування людей, приклад інтерактивні рекламні щити, чи інформаційні табло на яких користувач може знайти необхідну йому інформації просто взаємодіючий з ним, як з екраном смартфона, останні часто застосовуються в торгових, розважальних центрах [2].

Виробники смартфоні розвивають технології та їх ефективність за рахунок зручного та просто інтерфейсу, з поступовим додаванням технології додаткової

реальності, що виконує як інформаційну (навігаційні символи та автоматичне накладання маршрут для користувача), так і розважальну роль (інтерактивні ігри).

Подальший розвиток комп'ютерної графіки буде пов'язано з доповненої і віртуальною реальністю. Уже зараз гіганти такі як Google, Apple, Amazon вливають колосальні кошти для розвитку технології що спростить життя людини. Так само в гонку розвитку вступають і стартапи ентузіастів, що просувають свої ідеї і отримують підтримку звичайних користувачів. Перспективи у новій галузі, пов'язаної з доповненої і віртуальною реальністю колосальні. Доповнена реальність може в значній мірі спростити життя людини в повсякденному житті.

Підвищити безпеку людини за рахунок того, що дозволить отримувати важливу і своєчасну інформацію про об'єкти та суб'єктів, що оточують його. Змінити соціальній аспект взаємодії людей між собою за рахунок доступної інформації. Віртуальна реальність же в свою чергу може стати раніше неможливим інструментом для роботи фахівців величезного числа галузей, починаючи від архітектури і медицини, закінчуючи величезними симуляціями ігрових світів. Значній мірі саме розважальні сфери, будуть мати найбільшу кількість користувачів, що розширить можливості у розвитку економіки багатьох країн світу [3].

Але негативні аспекти, що стануть реальністю, можуть підірвати права і безпеку суспільства та окремих людей. Технології, що дозволяють проводити маніпуляції із зовнішністю можуть стати початком хвилі злочинів, в яких зловмисники зможуть застосовувати зовнішність звичайних громадян або навіть представників влади. Подібного роду події можуть позбавити суспільство впевненості в безпеці, так як будь-хто з них може стати жертвою шахраїв і злочинців, не маючи можливості довести свою не причетність до злочину. Це може призвести до заборони застосування технології, що може уповільнити розвиток технологій в цілому через страх перед ними.

Віртуальна реальність може мати іншу форму загрози. А саме спотворення сприйняття людини. Нездатність відрізнити реальність від цифрового світу призведе до загострення психічних розладів, спалахів насильства, нещасних випадків, тому що людина не буде знати, що вчиняє дії свої в реальному світі [4].

Понад норма в кількості часу проведеного віртуальної реальності може викликати більш прості, але не менш страшні інциденти смертей через виснаження, або нападів пов'язаних з захворюваннями нервової та серцевої системи, при яких людині не надали вчасно допомогу, подібного роду інциденти мають місце і зараз при використання звичайних ПК та смартфонів [5].

Тож не дивлячись на велику кількість негативних аспектів від нових технологій, все ж ключову роль в ній грає людина. Фахівці різних сфер вже сьогодні працюють над вирішенням і запобігання вище описаних негативних подій. Нові технології завжди супроводжують небезпеки, проте ці загрози усуваються фахівцями, які їх удосконалюють і роблять корисними для суспільства.

Список використаних джерел

1. *Виставка новітніх цифрових технологій в Сінгапурі URL: https://s2018.siggraph.org/*
2. *Познин В.Ф. Экранное пространство: реальное и воображаемое. Вестник Санкт-Петербургского Университета. 2015. №1, с. 18-25.*
3. *Якубович Л.В. Дополненная реальность: сегодня. URL: https://habr.com/sandbox/117951/*
4. *Шапинская Е.Н. Виртуальная реальность как пространство эскапизма: безграничные возможности и новые опасности. Культура культуры. 2014. №2, с.64-79*
5. *Класифікації захворювань ВОЗ «Всемирная организация здравоохранения» URL: https://icd.who.int/browse11/l-m/en#/http://id.who.int/icd/entity/1448597234*

УДК 004.092

Ткаченко А. М.
Лозівська філія Харківського державного автомобільно-дорожнього коледжу

Роль комп'ютерної графіки у підготовці майбутнього фахівця в сучасних умовах працевлаштування

Комп'ютерна графіка – галузь людської діяльності, пов'язана з використанням комп'ютерів для створення зображень і опрацювання візуальної інформації, отриманої з реального світу. В інформатиці як науці комп'ютерна графіка виділена в окрему галузь, яка вивчає методи і засоби створення, опрацювання та використання зображень за допомогою програмно-апаратних засобів.

Комп'ютерна графіка з'явилась достатньо давно – вже у 1960-х роках існували повноцінні програми роботи з графікою. Сьогодні прийнято користуватися термінами «комп'ютерна графіка» і «комп'ютерна анімація». Поняття «комп'ютерна графіка» об'єднує всі види робот зі статичними зображеннями, «комп'ютерна анімація» має справи з зображеннями, які динамічно змінюються.

Справжнього широкого розвитку комп'ютерна графіка зазнала з появою персональних комп'ютерів «Macintosh» (MAC) фірми Apple, які спеціально визначалися для потреб поліграфії. Саме для платформи MAC почали з'являтися перші спеціалізовані операційні системи та графічні редактори. Але сталося так, що справжніми «масовими» комп'ютерами стали комп'ютери класу IBM/PC (PC). Тоді більшість звичайних сьогодні для багатьох оболонок та редакторів почали відтворюватися на базі графічного досвіду MAC, але перекладені для комп'ютерів PC. Так з'явилася славнозвісна операційна система Windows, а також дуже велика кількість звичних для користувачів комп'ютерів PC пакетів, різнопланових програм та редакторів (наприклад: QuickTime, Page Maker, майже всі продукти корпорації Adobe та багато інших).

У теперішній час, завдяки грандіозному розвитку комп'ютерної техніки, деякі сторони нашого життя неможливо уявити собі без застосування комп'ютерних технологій, у тому числі без комп'ютерної графіки.

Сфера застосування комп'ютерної графіки не обмежується одними художніми ефектами. У усіх галузях науки, техніка, медицина, в комерційній і управлінській діяльності використовуються побудовані за допомогою комп'ютера схеми, графіки, діаграми, призначені для наочного відображення різноманітної інформації. Конструктори, розробляючи нові моделі автомобілів і літаків, використовують тривимірні графічні об'єкти, щоб представити остаточний вид виробу. Архітектори створюють на екрані монітора об'ємне зображення будівлі, і це дозволяє їм побачити, як воно впишеться в ландшафт.

Сфери застосування комп'ютерної графіки:

– наукова графіка;
– ділова графіка;
– конструкторська графіка;
– ілюстративна графіка;
– художня і рекламна графіка;
– комп'ютерна анімація;
– графіка для Інтернету.

Лозівська філія Харківського державного автомобільно-дорожнього коледжу випускає молодших спеціалістів за спеціальністю «Технологія обробки матеріалів на

верстатах і автоматичних лініях». Отримана спеціальність дає можливість випускникам виконувати наступні професійні обов'язки і займати посади:

– технік-технолог відділу – проектування технологічних процесів механічної обробки деталей машин з оформленням відповідної документації;

– технолог механоскладального цеху – забезпечення виконання технологічних процесів обробки деталей на дільницях;

– технолог-програміст – проектування операційної технології для верстатів з ЧПК;

– технік з нормування праці – встановлення норм та розцінок робіт;

– технік з підготовки виробництва – організація підготовки випуску продукції;

– диспетчер виробництва – постачання матеріалів та комплектуючих на робочі місця;

– контролер верстатних і слюсарних робіт – контроль якості виготовлених деталей;

– майстер виробничої дільниці – організація виробництва продукції;

– майстер контрольний дільниці – керівництво контрольними роботами;

– верстатник (на роботах високої кваліфікації);

– оператор верстатів з ЧПК.

Отже, комп'ютерна графіка є однією із важливих дисциплін в отриманні фахової освіти за спеціальністю «Технологія обробки матеріалів на верстатах і автоматичних лініях». А саме, одна із її складових – конструкторська графіка.

Конструкторська графіка використовується в роботі інженерів-конструкторів, архітекторів, винахідників нової техніки. Цей вид комп'ютерної графіки є обов'язковим елементом САПР (систем автоматизації проектування). Засобами конструкторської графіки можна отримувати як плоскі зображення (проекції, перетину), так і просторові тривимірні зображення. Призначення конструкторської графіки - використання в роботі інженерів-конструкторів і винахідників для створення креслень. Комп'ютерні програми, що працюють в цій галузі, отримали назву САПР (Система Автоматизованого ПРоектування).

Графіка в поєднанні з розрахунками дозволяє проводити в наочній формі пошук оптимальної конструкції, найбільш вдалою компонування деталей, прогнозувати наслідки, до яких може привести зміни в конструкції. Засобами конструкторської графіки можна отримувати плоскі зображення (проекції, перетину і просторові, тривимірні зображення

З метою популяризації комп'ютерної графіки та сучасних комп'ютерних технологій автоматизованого проектування в Лозівькій філії вже втретє пройшла Регіональна студентська олімпіада «Комп'ютерне креслення і моделювання засобами САПР» та щорічно проводиться студентський конкурс 3D-моделювання в системі «Компас 3D», з метою підвищення рівня творчої активності і якісної підготовки студентів з інженерних дисциплін.

І як висновок, хочу зазначити, що область застосування комп'ютерної графіки не обмежується одними художніми ефектами. Існує цілий ряд галузей, де комп'ютерна графіка є невід'ємною частиною. Сучасні системи автоматизованого проектування підтримують цілий комплекс інженерних робіт на декількох ключових етапах життєвого циклу виробу – в процесах проектування, конструкторсько-технологічної підготовки виробництва і складають основу інтегрованих систем управління машинобудівного підприємства.

УДК 004.921

Шевченко В. О.
Центральноукраїнський національний технічний університет

Вибір засобів комп'ютерної графіки для вирішення прикладних задач

Однією з найбільш областей комп'ютерних технологій, що динамічно розвивається, на сьогоднішній день є комп'ютерна графіка. Діапазон застосування цієї технології простягається від створення ігор, телевізійної реклами і кіно-спецефектів до комп'ютерного проектування в машинобудуванні і фундаментальних наукових досліджень [1].

Засобами комп'ютерної графіки створюється цифровий образ, який може бути змінений в будь-який час і з ним можна робити різні маніпуляції, зберігаючи при цьому різні варіанти, що раніше було неможливо зробити в традиційних формах образотворчого мистецтва. Є декілька видів комп'ютерної графіки: растрова, векторна, фрактальна, тривимірна.

Основним елементом растрового зображення є піксель (точка), тому векторні зображення представляють собою набір простих геометричних фігур (точки, прямі, кола та прямокутники), їм присвоюється колір, товщина ліній та інші характеристики. Великий обсяг даних – основна проблема при використанні растрових зображень.

В растровій графіці також існують лінії, але там вони розглядаються як комбінації точок. Відповідно, чим довша растрова лінія, тим більше пам'яті вона потребує. Обсяг пам'яті, для зберігання лінії, не залежить від розміру лінії, оскільки лінія представляється у вигляді формули, а точніше, у вигляді кількох параметрів. Що б ми не робили з цією лінією, міняються тільки її параметри, які зберігаються в чарунках пам'яті. Кількість чарунків залишається незмінною для будь-якої лінії.

Фрактальна графіка обраховується як векторна, але відрізняється тим, що жодних об'єктів у пам'яті комп'ютера не зберігається. Зображення будується за рівнянням (або за системою рівнянь), тому нічого, крім формули, зберігати не потрібно. Змінивши коефіцієнти у рівнянні, отримують зовсім іншу картину [2].

Тривимірна графіка оперує з об'єктами в тривимірному просторі. Всі об'єкти є набором поверхонь або часток і усіма візуальними перетвореннями в 3D-графіці управляють матриці.

Розрізняють дві функції комп'ютерної графіки: ілюстративну і когнітивну. Ілюстративна функція дозволяє втілити в візуальному оформленні лише те, що вже відомо і існує. Когнітивна ж функція полягає в тому, щоб за допомогою деякого зображення отримати нове знання, розкрити сутність явища [3].

У заключення, з усього приведеного матеріалу можна побачити, що у теперішній час існує таке велике різноманіття комп'ютерної графіки, що кожен, хто вирішить займатись цією цікавою справою, завжди знайде усі необхідні інструменті для своєї праці.

Також слід звернути увагу на те, що більшість сучасних пакетів, дозволяють виконувати операції з різними типами графіки водночас, користуючись тільки одним пакетом.

Список використаних джерел

1. *Пічугін М. Ф. Компютерна графіка [текст]: навч. посіб. / М.Ф.Пічугін, І.О.Канкін, В.В.Воротніков. – К.: «Центр учбової літератури», 2013. – 346 с.*
2. *Stevens R.T. Creating fractals (Graphics series) // Publisher: Charles River Media; 1 edition, August 15, 2005.*
3. *Gorokhov, V.L. Modern methods of cognitive visualization of multidimensional data [Text] / V.L. Gorokhov, A.A. Lykianez, A.G. Chernov. - Tomsk: Non-commercial development of regional energy fund, 2007. - 216 p.*

UDC 004.056.5:343.3

Obach V.[*]
Central Ukrainian National Technical University

Current Issues of Cyber Defense in Ukrainian Billing and Payment Systems

Given the rapid development of the global information society, the widespread use of ICT in all areas of life, issues of information security are of particular importance. Its purpose is to provide a state of protection of vital interests of the person, society and the state, which is achieved by preventing damage caused by: incompleteness, timeliness and unlikelihood of the information used; negative information influence; negative consequences of the use of information technology; unauthorized distribution, use and violation of the integrity, confidentiality and availability of information [1].

One of the most important spheres of the national economy of any developed state is the banking system. Its practical role is determined by the fact that it manages the system of billing and payments in the state, it conducts most of its commercial transactions through contributions, investments and lending operations, along with other financial intermediaries, banks send savings to firms and productive structures [2]. The main catalyst for development of information security in Ukrainian banking sector was the event that took place in June 2017: Ukrainian banks, energy companies, state-owned Internet resources and local networks, Ukrainian media and other large enterprises suffered a massive hacker attack spreading the Petya virus .A, which blocks the operation of computer systems [3]. About thirty banking institutions suffered from this cyberattack.

The banking system of Ukraine consists of the NBU and other banks, as well as branches of foreign banks established and operating in the territory of Ukraine in accordance with the provisions of the Law on banks and banking and other several Ukrainian laws[5].

The regulatory authority of the banking system of Ukraine is represented by NBU. It is an issuing center, that conducts a single state policy in the field of money circulation, credit, support of price stability in the state, regulates and oversees the activities of commercial banks in Ukraine [6]. Also, according to the Law of Ukraine "On the National Bank of Ukraine", it is responsible to provide information security. In order to protect data in the banking sector, the NBU performs the following functions [7]: a) establishes rules for carrying out banking operations, accounting and reporting, protection of information, funds and property for banks; b) determines the directions of development of modern electronic banking technologies, creates and ensures the continuous, reliable and efficient functioning, development of payment and accounting systems created by them, controls the creation of payment instruments, automation systems of banking activities and means of protection of banking information; c) determine the procedure, requirements and measures for ensuring cyber defense and information security in the banking system of Ukraine and for the entities of transfer of funds, oversees their implementation; forms the center of cyber defense of the National Bank of Ukraine, ensures the functioning of the cyber defense system in the banking system of Ukraine; d) ensures the formation and maintenance of a list of critical infrastructure objects, as well as a register of objects of critical information infrastructure in the banking system of Ukraine, defines the criteria and procedure for assigning objects in the banking

[*] Scientific supervisor PhD in Information Technology Oleksandr Dorenskyi, Central Ukrainian National Technical University

system of Ukraine to objects of critical infrastructure and objects of critical informational infrastructure, provides evaluation of the state of cyber defense and information security audit in the banking system of Ukraine.

Based on the results of the analysis of the Strategy of National Security of Ukraine, the Doctrine of Information Security of Ukraine, the Regulations on the organization of measures to ensure information security in the banking system of Ukraine, the Laws of Ukraine "On the Basic Principles of Cybersecurity of Ukraine", "On National Security of Ukraine", "On the National Bank of Ukraine" it follows that today the issues of ensuring information security in billing and payment systems in the banking sphere of the state are acute. In accordance with the current legislation, in particular Articles 6, 8 of the Law of Ukraine "On the Basic Principles of Cybersecurity Protection of Ukraine," the National Bank of Ukraine takes measures to ensure information security for funds transfer agents, including cybersecurity payment systems and billing systems [8]. Nevertheless, neither the specified nor the current normative legal documents in the banking sphere provide detection and termination of the functioning of payment systems that carry out transfers with the additional use of prohibited payment systems (subsystems) in Ukraine.

Therefore, based on the current state and legal framework of information security in domestic payment systems and billing systems, it is absolutely necessary to improve the present-day legal and regulatory framework of the banking sector of Ukraine, as well as measures of the National Bank of Ukraine [8] regarding the impossibility of making transfers with participation payment systems - intermediaries (subsystems). This will enable elimination of the risk of endangering the national security of Ukraine in the information sphere with the use of payment and billing systems.

References

1. *On the Basic Principles of the Information Society Development in Ukraine for 2007-2015: Law of Ukraine dated January 9, 2007 No. 537-V [Electronic resource] // The Verkhovna Rada of Ukraine. - Access mode: http: //zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=537-16 [in Ukrainian].*
2. *Glossary of financial and legal terms [Electronic resource] / [for co-authors. Ed. D.Sc., Prof. L.K. Crown // 2nd edition, revised and supplemented. - Electronic data. - [reworked. and complemented - K .: Alerta, 2011]. - Mode of access: http://ndi-fp.nusta.com.ua/files/doc/slovnyk-finpravo.pdf (application date 04.10.2018). - Title from the screen [in Ukrainian].*
3. *The virus Petya.A did not give the opportunity to seize private information of citizens - Cyberpolice [Electronic resource]: [Website]. - Access mode: https://www.unian.ua/science/2003211-virus-petyaa-ne-dav-mojlivosti-zavoloditi-privatnoyu-informatsieyu-gromadyan-kiberpolitsiya.html. (application date 04.10.2018). - Title from the screen [in Ukrainian].*
4. *Damage from Petya.A virus attack in the world reaches $ 8 billion - Expert [Electronic resource]: [Website]. - Access mode: https://www.unian.ua/science/2003241-zbitki-vid-ataki-virusu-petyaa-syagayut-8-milyardiv-dolariv-ekspert.html. (application date 04.10.2018). - Title from the screen [in Ukrainian].*
5. *On Banks and Banking: Law of Ukraine dated October 1, 2018, No. 2121-III [Electronic resource] // The Verkhovna Rada of Ukraine. - Mode of access: http://zakon.rada.gov.ua/laws/show/2121-14. - Title from the screen [in Ukrainian].*
6. *National Bank of Ukraine [Electronic resource]: [Web-site]. - Access mode: https://www.bank.gov.ua/control/uk/publish/article?art_id=36081&cat_id=36006. (application date 04.10.2018). - Title from the screen [in Ukrainian].*
7. *About the National Bank of Ukraine: Law of Ukraine dated October 1, 2018, No. 2121-III [Electronic resource] // Verkhovna Rada of Ukraine. - Mode of access: http://zakon.rada.gov.ua/laws/show/2121-14. - Title from the screen [in Ukrainian].*
8. *On approval of the provisions on cyber defense and information security in payment systems and settlement systems: Draft Resolution of the Board of Directors of the National Bank of Ukraine [Electronic resource]: [pdf-file]. - Access mode: https://bank.gov.ua/doccatalog/document?id=78399302 (application date 04.10.2018). - Title from the screen [in Ukrainian].*

УДК 351.865

Гайтота Є. В., Чуницька В. В., Нікуліщев Г. І.
Запорізький національний технічний університет

Про врахування досвіду Німеччини в Стратегії кібербезпеки України

Кіберпростір включає в себе всю інформаційну інфраструктуру, доступну через Інтернет за всіма територіальними межами. Недосконаліть ІТ-продуктів та компонентів, розбиття інформаційної інфраструктури або серйозні кібернапади можуть мати суттєвий негативний вплив на продуктивність технологій, підприємств та адміністрації, а отже, і на соціальну складову нашого життя. Наявність кіберпростору, цілісність, автентичність та конфіденційність даних в кіберпросторі стали актуальними питаннями XXI століття. Забезпечення кібербезпеки, таким чином, перетворилося на центральне завдання для держави, бізнесу та суспільства як на національному, так і на міжнародному рівні. Стратегія кібербезпеки покликана поліпшити рамкові умови в цій галузі, а державна політика кібербезпеки (NCSS) служить засобом посилення безпеки і надійності інформаційних систем держави.

З введенням в дію на початку 2016-го року Стратегії кібербезпеки України, кібербезпекою на державному рівні почала опікуватись і Україна. Метою Стратегії є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Одним з перших кроків з втілення Стратегії, стало створення Національного координаційного центру кібербезпеки як робочого органу Ради національної безпеки і оборони України. Українська стратегія кібербезпеки багато в чому спирається на досвід європейських партнерів. Гарним прикладом для цього є Стратегія безпеки в кіберпросторі у Німеччині, яка була прийнята на початку 2011 року. У даній Стратегії проводиться аналіз необхідності додаткових дій по захисту ІТ-систем за допомогою надання основних функцій безпеки, сертифікованих державою, а також підтримки малого та середнього бізнесу шляхом створення нової робочої групи.

Важливо зазначити, що Стратегія кібербезпеки України передбачає комплекс заходів, пріоритетів і напрямів забезпечення кібербезпеки України, зокрема:

- вироблення і оперативну адаптацію державної політики, спрямованої на розвиток кіберпростору та досягненні сумісності з відповідними стандартами ЄС та НАТО;
- створення вітчизняної нормативно-правової та термінологічної бази у цій сфері;
- формування конкурентного середовища у сфері електронних комунікацій;
- розвиток технологій кіберзахисту засобів рухомого зв'язку, забезпечення апаратної, контентної безпеки, безпеки додатків та сервісів зв'язку;
- підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі;
- проведення навчань щодо надзвичайних ситуацій та інцидентів у кіберпросторі;
- розвиток міжнародного співробітництва, підтримку міжнародних ініціатив у сфері кібербезпеки, поглиблення співпраці України з ЄС та НАТО.

Основна ідея вищевказаних заходів і пріоритетів у Стратегії полягає в тому, що Україна повинна створити складну глобальну високотехнологічну систему для забезпечення безпеки і надійності зв'язку. Це здається непростим завданням, беручи до уваги поточний стан інструментів захисту і безпеки.

Основне призначення Стратегії – це створення умов для безпечної експлуатації кібепростору. У ході аналізу Стратегії було виявлено, що вона, безсумнівно є

необхідною основою для позитивних змін у сфері кіберзахисту. Тим не менш, цей документ лише визначає напрями дії.

Стратегія передбачає створення «активного кіберзахисту», що означає здійснення воєнно-політичних, військово-технічних та інших заходів, спрямованих на розширення прав і можливостей воєнної організації держави, сектора безпеки і оборони в кіберпросторі, створення, розвиток сил, засобів та інструментів для можливої відповіді на агресію у віртуальному просторі, що може бути використаний як засіб стримування воєнних конфліктів і загроз в кіберпросторі. Іншими словами, Україна повинна створити механізм кібератак у відповідь. Але такий механізм вимагає серйозних інвестицій і знань.

Стратегія є важливим кроком на шляху розбудови системи кібербезпеки України та являє собою програму дій, якої мають дотримуватись державні органи. Одним з перших кроків з втілення Стратегії, стало створення в червні 2016 року Національного координаційного центру кібербезпеки як робочого органу Ради національної безпеки і оборони України.

На даному етапі свого існування реалізація Стратегії кібербезпеки України потребує внесення низки змін до українського законодавства, що мають як створити підґрунтя для втілення в життя положень Стратегії, так і посилити відповідальність за порушення в сфері кібербезпеки. Таким чином, випливає, що нова Стратегія є необхідною, однак не достатньою для того, щоб належним чином захистити Україну від кіберзлочинності. Як уже зазначалося, одним з шляхів покращення даної Стратегії це переймання досвіду європейських колег.

Порівнюючи з Німеччиною, ми бачимо, що Федеральний уряд Німеччини прагне зробити вагомий внесок у забезпечення безпечного кіберпростору, таким чином підтримуючи та сприяючи економічному та соціальному процвітанню в Німеччині.

Стратегія кібербезпеки ФРН в основному фокусується на цивільних підходах та заходах. Це включає співробітництво не лише в Організації Об'єднаних Націй, але також в ЄС, Раді Європи, НАТО, G8, ОБСЄ та інших багатонаціональних організаціях. Метою є забезпечення узгодженості та можливостей міжнародного співтовариства щодо захисту кіберпростору.

Для втілення стратегії в життя було створено Федеральний офіс інформаційної безпеки Міністерства внутрішніх справ (BSI), а також Національний центр кібер-реагування (NCAZ). Ці органи займаються визначенням, аналізом і розробкою заходів, необхідних для нівелювання і усунення потенційних загроз. А для координації дій секретаріатів різних міністерств в питаннях кібербезпеки було запроваджено Національну раду кібербезпеки. За допомогою нинішньої стратегії кібербезпеки Федеральний уряд адаптує заходи до існуючих загроз. За стратегією Федеральний уряд зосереджує увагу на таких стратегічних напрямках:

- захист критично важливих інформаційних інфраструктур;
- безпечні інформаційні системи в Німеччині;
- посилення безпеки ІТ у державній адміністрації;
- національна рада з питань кібербезпеки;
- ефективний контроль злочинності у кіберпросторі;
- ефективні узгоджені дії щодо забезпечення кібербезпеки в Європі та у всьому світі;
- використання надійних та надійних інформаційних технологій;
- інструменти для реагування на кібер-атаки.

Зі стратегії випливає, що з реалізацією стратегічних цілей та заходів федеральний уряд сприяє забезпеченню кібербезпеки, а отже, і свободі та процвітанню Німеччини.

Багато чого буде залежати від того, чи прийдуть успіхи на міжнародному рівні в прийнятті ефективних заходів для захисту кіберпростору.

Використані інформаційні технології піддаються коротким циклам інновацій. Це означає, що технічні та соціальні аспекти кіберпростору будуть продовжувати змінюватися і мати не тільки нові можливості, але й нові ризики. З цієї причини Федеральний уряд буде регулярно перевіряти, чи досягнуті цілі Стратегії кібербезпеки під загальним контролем Національної ради з питань кіберзберігання, і адаптуватимуть стратегії та заходи до відповідних вимог та рамкових умов.

29 серпня 2018 року Кабінет Міністрів прийняв рішення про створення в Німеччині агентства з інновацій в області кібербезпеки.

Завданням агентства є координація дослідного процесу з моменту появи ідеї до виходу готового продукту. Йдеться про вивчення на ранній стадії "багатообіцяючих і високоінноваціонних" проектів в області безпеки і їх подальшої фінансової підтримки за участю венчурного капіталу.

Одним з проектів агентства є підтримка власних технологій шифрування, оскільки в майбутньому традиційні алгоритми шифрування можуть бути зламані квантовими комп'ютерами.

Отже, кібербезпека – один із ключових аспектів життя в інформаційну добу. Наші смартфони, соцмережі й інші онлайн-відбитки особи містять про користувачів інформації більше, ніж вони самі знають про себе. При тому, вони можуть бути значно більш вразливими для атак зловмисників, ніж людина в реальному житті. Тому уся електронна інформація, сервіси і пристрою потребують захисту і дотримання певних правил безпеки.

На думку авторів, прийняття, розвиток і втілення в Україні нормативних документів, що стосуються кібербезпеки, є позитивною тенденцією як для забезпечення національної безпеки у кіберпросторі, так і для інтеграції нашої країни у європейське суспільство. Враховуючи прагнення України щодо євроінтеграції, потрібна уніфікація національного законодавства з нормативними документами Європейського союзу, тому при підготовці нормативних актів стосовно кібербезпеки доцільно орієнтуватися на аналогічні правові документи як загальноєвропейського рівня, так і рівня членів Євросоюзу, зокрема, ФРН. Оскільки європейські держави взяли до уваги питання кіберзахисту раніше за Україну, то варто також вивчати їхній досвід з практичної реалізації адміністративного, організаційного, технічного та іншого забезпечення кібербезпеки.

Список використаних джерел

1. *Офіційний портал Верховної Ради України: Указ Президента України Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" [Електронний ресурс]: Верховна Рада України 15.03.2016. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/96/2016*
2. *Чуницька, В.В. Порівняння нормативно-правових документів з кібербезпеки України з європейськими / Чуницька В.В., Гайтота Є.В., Нікуліщев.Г.І. // Тиждень науки: щорічна наук.-практ. конф. викладачів, науковців, молодих учених і аспірантів, 16-20 квітня 2018 р.: тези доповідей. – Запоріжжя, 2018. – С. 906-908.*
3. *Гайтота Є. В. Про перспективи Стратегії кібербезпеки України / Гайтота Є. В., Чуницька В.В., Нікуліщев Г.І. // Актуальні задачі та досягнення у галузі кібербезпеки: Всеукраїнська науково-практична конференція студентів і молодих вчених, 23-25 листопада 2016 р.: матеріали конф. – Кропивницький, 2016. – С.7-8.*
4. *Berlin24.ru: Германию будут защищать „киборги [Електронний ресурс]: Berlin24.ru 30.08.2018. – Режим доступу: https://berlin24.ru/ru/news/novosti-germanii-segodnja-v-novostjah/6428-germaniu-budut-zasisat-kiborgi.html*
5. *European Union Agency for Network and Information Security: National Cyber Security Strategies (NCSSs) Map [Електронний ресурс]: enisa 04.03.2016. – Режим доступу: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map*

УДК 004.056.5

Жогов В. С., Форос Г. В.
Одеський державний університет внутрішніх справ

Особливості нормативно-правового регулювання кібербезпеки в Україні та в законодавстві інших країн

Всі відчувають, як останнім часом змінюється світ. Промислові товари, послуги, продуктивність виробництва, капітал, знання та інформація користуються попитом незалежно від кордонів та обмін ними здійснюється у все більш короткі строки. Це зумовлено стрімким розвитком інформаційних технологій, процесами становлення і розвитку міжнародного кіберпростору, який триває з кінця XX століття та по сьогоднішній день.

Для одних це є безмежною можливістю розвитку економічних, промислових, товарних, політичних, культурних та наукових взаємовідносин, для інших – розуміння того, що дані процеси покликані на задоволення інтересів кількох найбільш розвинених держав, а більшості країнам на планеті спричиняється шкода.

Але як би там не було державні та правові кордони на даному етапі не можуть стримати цей широко розповсюджуваний процес або хоча б впливати на нього. Суспільство та політика повинні приймати у цьому участь та пристосовуватися, якщо хочуть і в подальшому забезпечувати права, свободи та можливості громадян.

Виникнення нових сфер суспільного життя породжує й нові загрози. Державна влада, в особі правоохоронних органів, повинна реагувати на суспільно небезпечні та протиправні дії. Тому необхідність в забезпеченні безпеки інтересів людини і громадянина, суспільства та держави, національних інтересів в кіберпросторі поступово набуває дедалі більшої ваги і стає одним із найважливіших елементів забезпечення національної безпеки держави.

Правове врегулювання кібербезпеки є обов'язковим атрибутом правової системи будь-якої розвинутої країни світу. Наявність його є обов'язковою державною гарантією для забезпечення свободи та можливостей людей, збагачення суспільства, створення нових глобальних інтерактивних ринків ідей, дослідження та інновацій, стимулювання відповідальної та ефективної роботи влади і активного залучення громадян до управління державою та вирішення питань місцевого значення, публічності та прозорості влади, сприяння запобіганню корупції.

Така діяльність повинна базуватися на принципах законності, дотримання основних прав і свобод людини, оперативності, неминучості покарання, комп'ютерної безпека і захисту персональних даних, комплексного використання профілактичних заходів: правових, соціально-економічних та інформаційних, соціального партнерства, співробітництва органів державного управління з міжнародними організаціями, представниками громадянських організацій тощо.

Незважаючи на те, що положення щодо правового врегулювання кібербезпеки містяться, за деякими виключеннями, в правових системах кожної країни, зміст даного поняття, а точніше, масштаби охоплення сфер суспільного життя, різниться.

В одних державах, (наприклад, Білорусь) немає спеціальних галузевих документів, які регулювали б основи державної політики в сфері кібербезпеки, лише деякі аспекти регулюються Кримінальним кодексом, в інших (Японія) – являє собою сукупність взаємопов'язаних правових механізмів, які надають достатні можливості працівникам правоохоронних органів для виявлення, попередження та присікання злочинних діянь, пов'язаних з кібербезпекою. Таку ситуацію зумовлюють по-перше, особливості доктрини держави, а по-друге історія формування нормативної бази, що стосується правового врегулювання питання кібербезпеки.

З метою створення стратегії кібербезпеки Євросоюзу, Європейське агентство з мережевої та інформаційної безпеки (ENISA) розробляє спеціальне керівництво (Good Practices Guide). До нього залучатимуться передові практики та рекомендації з проектування, впровадження та підтримки державної стратегії кібербезпеки. Керівництво розробляється у сприянні з приватними та державними зацікавленими сторонами по всій Європі, шляхом обміну інформацією в сфері реагування на кіберінциденти, а також навчаннями на державному та пан'європейському рівнях.

В США прийнята концепція кібермогутності, яка визначає кібербезпеку фундаментальним явищем сучасного життя. У політичній, економічній і військовій сферах кібертехнології

повинні забезпечувати і підтримувати діяльність ключових елементів американської інфраструктури, в тому числі і в області національної безпеки. Вважається також, що США повинні створити ефективну національну і міжнародну стратегічну основу для розвитку і використання своєї кібермогутності як повномасштабного напрямку реалізації стратегії національної безпеки.

Така стратегічна основа матиме структурні і геополітичні складові. Структурна складова зосередить свою увагу на зміцненні безпеки і людському капіталі, поліпшення управління та більш ефективної організації діяльності. Геополітична складова зосередиться на більш традиційній сфері забезпечення національної безпеки і обороноздатності США.

Проаналізувавши вплив правових норм на відповідні правовідносини у зарубіжних країнах, можна зробити висновок, що нормативно-правове регулювання кібербезпеки в економічно розвинутих країнах має набагато більшу історію із більш усталеними правовими традиціями, оптимальними моделями нормативно-правого регулювання, що є досить важливим в умовах сучасного рівня нормативно-правового регулювання кібербезпеки.

Історія формування поняття «кібербезпека» в правовій науці Україні є порівняно короткою у зв'язку, з відсутністю достатнього нормотворчого, а також правозастосовчого досвіду в області забезпечення кібербезпеки.

На даний момент нормативно-правове регулювання кібербезпеки в Україні забезпечується Конвенцією про кіберзлочинність від 23 листопада 2001 року. У 2005 році Верховна Рада України ратифікувала її, прийнявши відповідний Закон України «Про ратифікацію Конвенції про кіберзлочинність».

Згідно даного Закону в Україні органом, на який покладаються повноваження щодо створення та функціонування цілодобової контактної мережі для надання невідкладної допомоги при розслідуванні злочинів, пов'язаних з комп'ютерними системами і даними, переслідуванні осіб, обвинувачених у вчиненні таких злочинів, а також збору доказів в електронній формі, є Міністерство внутрішніх справ України.

Дана норма дала підстави для створення у Міністерстві внутрішніх справ України окремого структурного підрозділу – Управління по боротьбі з кіберзлочинністю, а в жовтні 2015 року Управління було трансформовано в Департамент кіберполіції Національної поліції України.

У Кримінальному кодексі України правовій регламентації злочинних діянь у даній сфері присвячена Глава XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку».

Указом Президента України від 15 червня 2018 року № 96/2016 уведено в дію рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України», яка є основою для формування державної політики у сфері кібербезпеки України.

З метою імплементації відповідних правових норм у національне законодавство, 5 жовтня 2017 року Верховна Рада України прийняла Закон України «Про основні засади забезпечення кібербезпеки України».

Таким чином, питання актуалізації національного законодавства із забезпечення кібербезпеки під сучасні тенденції повільно, але все ж вирішується. Залишаються проблеми завчасного інформування про появу нових кіберінцидентів, рівень обізнаності населення про загрози використання комп'ютерів, розповсюдження особистої інформації, зокрема персональних даних в кіберпросторі бажає бути кращим.

Список використаних джерел

1. *Конвенція про кіберзлочинність [Електронний ресурс]: від 23.11.2001 ратифікована із застереженнями і заявами Законом № 2824-IV від 07.09.2005 – Електрон. дан. (1 файл). – Режим доступу: http://zakon.rada.gov.ua/laws/show/994_575 – Назва з екрану.*
2. *Кримінальний Кодекс України [Електронний ресурс]: від 5 квітня 2001 року № 2341-III – Електрон. дан. (1 файл). – Режим доступу: http://zakon.rada.gov.ua/laws/show/2341-14#n2491 – Назва з екрану.*
3. *Про Стратегію кібербезпеки України [Електронний ресурс]: указ Президента України від 15.03.2016 № 96/2016 – Електрон. дан. (1 файл). – Режим доступу: http://zakon.rada.gov.ua/laws/show/96/2016 – Назва з екрану.*
4. *Про основні засади забезпечення кібербезпеки України [Електронний ресурс]: Закон України від 05.10.2017 № 2163-VIII – Електрон. дан. (1 файл). – Режим доступу: http://zakon.rada.gov.ua/laws/show/2163-19 – Назва з екрану.*
5. *Обзор законодательства Республики Беларусь в сфере информационной безопасности [Електронний ресурс]: Информационно-аналитический портал о цифровой экономике и ИКТ-политике в странах Евразии Digital Report https://digital.report/zakonodatelstvo-belarusi-informatsionnaya-bezopasnost/*
6. *Киберготовность Японии 2.0: Киберпреступность и охрана правопорядка [Електронний ресурс]: Информационно-аналитический портал о цифровой экономике и ИКТ-политике в странах Евразии Digital Report https://digital.report/kibergotovnost-yaponii-2-0-kiber-prestupnost/*
7. *О.В. Каразин, А.А. Тарасов «Современные Концепции Кибербезопасности ведущих зарубежных государств» [Електронний ресурс]: Научная электронная библиотека «КИБЕРЛЕНИНКА» https://cyberleninka.ru/article/n/sovremennye-kontseptsii-kiberbezopasnosti-veduschih-zarubezhnyh-gosudarstv-1*

УДК 004.738.5:327.8

Колодяжний І. О.[*]
Центральноукраїнський національний технічний університет

Вдосконалений підхід до протидії пропаганді сепаратизму та антиукраїнській ідеології в соціальних мережах

Суттєвий прогрес і поширення інформаційних технологій, глобальний характер систем масової комунікації призвели до утворення глобального інформаційного простору, який змушує світову спільноту, кожну державу швидко орієнтуватися та адаптуватися у сучасному інформаційному середовищі. Світове співтовариство в цих умовах усвідомило, що міжнародна інформаційна безпека є проблемою, розв'язання якої суттєво впливає на існування людства. Тобто з розвитком і поширенням ІКТ у всі сфери життєдіяльності надзвичайної значимості набувають питання забезпечення інформаційної безпеки, визнаної в нашій країні однією з найважливіших складових національної безпеки, як багаторівневої проблеми державної інформаційної політики [1].

Варто окремо зазначити, що Конституція України (стаття 17) визначає інформаційна безпеку найважливішою функцією держави, справою всього Українського народу.

Необхідність протистояти протиправним посяганням на інформаційний простір України, збереження інформаційних ресурсів, захисту населення від негативного інформаційного впливу тощо є одним із основних завдань забезпечення інформаційної безпеки і вкрай важливим для української держави на сучасному етапі. Окрім цього, стратегічно визнаним пріоритетом зовнішньої політики України є європейська інтеграція, що вимагає удосконалення нормативно-правової бази забезпечення інформаційної безпеки України, яке б відповідало не лише міжнародним стандартам, а передусім українським національним інтересам.

Діяльність із забезпечення інформаційної безпеки здійснюється за допомогою різних способів, засобів і прийомів, які у сукупності й складають методи. Вони можуть значно змінюватися і варіюватися в залежності від типу діяльності, в якій вони використовуються, а також сфери застосування.

Методи переконання одержали потужний розвиток впродовж XX сторіччя. Пропаганда, що володіє великим арсеналом такого роду методів, стимулює соціально-політичну активність громадян, вказуючи їм конкретні напрями та завдання діяльності, підказуючи шляхи та засоби вирішення проблем, що стоять перед ними. Методи пропаганди не завжди ставлять за мету повністю змінити існуючу в свідомості громадян думку, а в більшості випадків – скорегувати її в потрібному напрямі, сформувати певні установи. Політична пропаганда дієва тоді, коли її прийоми є не випадковими, а систематичними. Важко знайти будь-який інший інструмент переконання чи навіювання, що порівнюється з пропагандою за ефективністю закріплення в свідомості певних поглядів та ідей.

Метою роботи є вдосконалення підходу до реалізації протидії пропаганді сепаратизму і антиукраїнської ідеології, яка поширюється у соціальних мережах.

В Україні реалізований підхід протидії пропаганді в соцмережах (Указ Президента України від 15.05.2017 №133/2017 Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року "Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)"), який полягає у забороні інтернет-провайдерам надавати послугу з доступу користувачів інтернету до сервісів російського виробництва: "Вконтакте", "Одноклассники" та багато інших.

[*] Науковий керівник – Доренський О. П., канд. техн. наук, доцент кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету

Проте як показує практика, реалізований підхід до забезпечення інформаційної безпеки держави не є ефективним. Адже заблоковані веб-сайти як і раніше входять в ТОП-10 найвідвідуваніших сайтів в Україні (рис. 1), оскільки користувачі активно використовують VPN, Tor, Opera та інші способи "обійти" блокування [2].

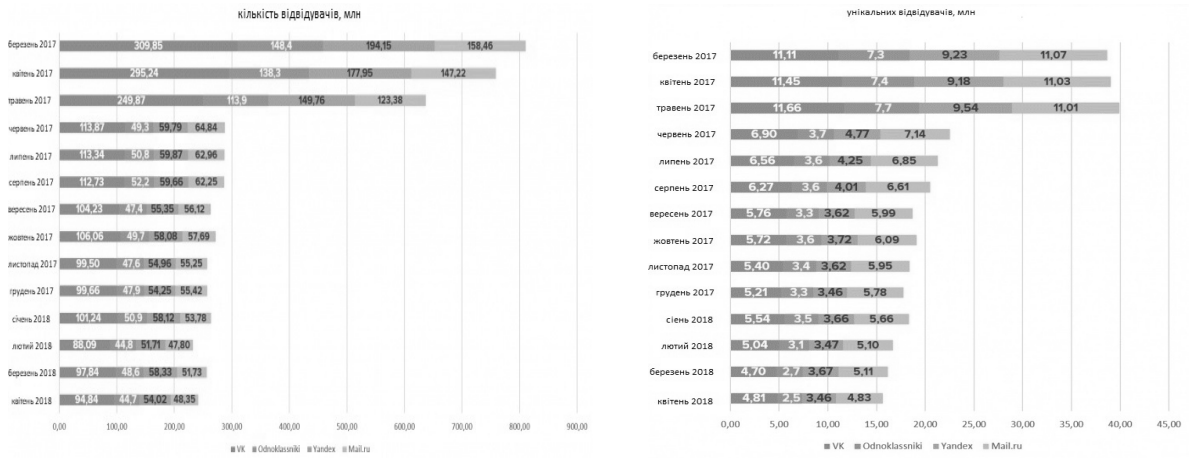


Рисунок 1 – Відвідуваність російських веб-ресурсів користувачами з України [2].

Виходячи з означеного, постає задача вдосконалення реалізованого підходу до блокування Інтернет-ресурсів російського походження, за допомогою яких поширюється пропаганда антиукраїнської ідеології та сепаратизму. Враховуючи зарубіжний досвід розв'язування сформульованої задачі, пропонується шляхом модифікації вітчизняної нормативно-правової бази реалізувати вдосконалений підхід до реалізації протидії пропаганді в соцмережах, який включає блокування Tor і VPN. Тобто, крім вже виконаного в Україні блокування доступу, адреси вхідних вузлів Tor, серверів VPN-провайдерів і сайтів з інформацією про обхід блокування слід вносити до "чорного" списку та блокувати провайдерами [3]. Це унеможливить практично здійснити "обхід" заборонених інтернет-ресурсів, в тому числі соціальних мереж.

Вдосконалений підхід істотно підвищить ефективність протидії пропаганді сепаратизму і антиукраїнській ідеології в соціальних мережах. Наприклад, після запровадження таких обмежень у Білорусії за один рік кількість "звичайних" підключень до Tor скоротилося в тричі, з 9000 до 3000 користувачів за добу [3]. Водночас, кількість людей, які підключаються до Tor через "мости" різко зросла.

Отже, в роботі показано, що не зважаючи на запроваджену в Україні заборону інтернет-провайдерам надавати доступ користувачам інтернету до веб-сервісів російського виробництва, зокрема соціальних мереж "Вконтакте" і "Одноклассники", які є засобами поширення пропаганди сепаратизму і антиукраїнської ідеології, частина українців як і раніше використовуються їх, "обходячи" блокування за допомогою VPN, Tor чи ін. способу. Тому пропонується вдосконалити підхід до реалізації протидії антиукраїнській пропаганді у соцмережах додатковим блокуванням Tor та VPN.

Список використаних джерел

1. *Степанов В. Ю. Інформаційна безпека як складова державної інформаційної політики / В. Ю. Степанов // Державне будівництво: наук. журн. – 2016. – № 2. – С. 1-9.*
2. *Річниця санкцій: чому мільйони українців продовжують відвідувати "Вконтакте" [Електронний ресурс] : [Веб-сайт]. – Режим доступу : https://www.epravda.com.ua/publications/2018/05/15/636802/ (дата звернення 10.11.2018 р.). – Назва з екрану.*
3. *Как именно запрещают VPN и Tor в разных странах мира [Електронний ресурс] : [Веб-сайт]. – Режим доступу : https://www.iphones.ru/iNotes/714931?fbclid=IwAR0OtipSqZwV7VfHLEUBiSXhWgNTN2N3qeacgCdrK2yfBzyRS0L8eKm0zDI (дата звернення 10.11.2018 р.). – Назва з екрану.*

УДК 004.056.53

Копиця Н. С., Ликов Ю. В.
Харківський національний університет радіоелектроніки

Аналіз документа "Політика конфіденційності" на базі регламенту GDPR в популярних інтернет-ресурсах

Для компаній, які надають свої послуги на території Європейського Союзу, важливо забезпечити відповідність політики конфіденційності до загального положення про захист даних (GDPR - General Data Protection Regulation). Компаніям необхідно було виконати ці вимоги до травня 2018 року. Користувачі Інтернету ризикують стати жертвами розсекречування персональних даних, тому вони повинні бути проінформовані про те, які саме особисті дані збираються і навіщо, а також які сайти порушують конфіденційність їх персональних даних.

Зсилаючись на дослідження Obar та Oeldorf-Hirsch можна стверджувати, що 74% з 543 людей не читають політику конфіденційності. Веб-сайти змушують користувачів читати та приймати свою політику, часто політика конфіденційності перевантажена, тому що текст надмірно довгий або незрозумілий. Правила щодо доступності веб-вмісту повинні добре сприйматися, бути зрозумілими та надійними.

Введення GDPR вважається найбільш важливою зміною регулювання конфіденційності даних за останні 20 років. З появою GDPR з'явилися нові складності з написанням політики конфіденційності. За основу були взяті наступні критерії [1]: а) GDPR1: Перелік даних, що збираються; б) GDPR2: Обгрунтування для збору даних; в) GDPR3: Як саме дані будуть оброблятися; г) GDPR4: Як довго зберігатимуться дані; д) GDPR5: З ким можна зв'язатися, щоб видалити дані; є) GDPR6: Повідомлення про конфіденційність. Базуючись на вказаних критеріях були проаналізовані деякі з найвідвідуваніших сайтів: YouTube, Google.com, Facebook, Reddit, Amazon.com, BBC, Wikipedia, eBay, Twitter.

Багато організацій не надають зручне посилання на політику. Завдяки вимогам GDPR, багато компаній перенесли посилання на політику конфіденційності на більш зручне та очевидне для користувача місце. Також було перевірено, наскільки політика конфіденційності веб-сайтів задовольняє вимогам GDPR. Для дослідження було використано Gunning Fog Index (GFI) - індекс туманності Ганнінга, який показує наскільки читачеві легко читати текст. Цей індекс є показником кількості років навчання, які знадобляться читачеві, щоб зрозуміти текст.

У таблиці 1 приведено кількість слів загалом, а також кількість складних слів (з 3 або більше складами). Результати приведені в таблиці направлені на те, щоб дати уявлення читачеві про час, який доведеться витратити, якщо б потрібно було зрозуміти всю політику конфіденційності. Залежність кількості слів від % 3+ складових слів зображено на рисунку 1.

На момент проведення дослідження (перша половина 2018 року) лише одна з цих політик відповідала вимогам Закону GDPR від 28 січня 2018 року. Інші компанії продовжують переглядати політики конфіденційності та розвиватися в цьому плані.

Список досліджуємих сайтів був розширений веб-ресурсами, які популярні на території України, а саме в м. Харкові. Результати деяких з них приведені в таблиці 2. Для прикладу, були взяті наступні веб-ресурсів: LinkedIn, Instagram, Yaposhka.kh.ua.

Проведений аналіз усіх політик допоміг виявити проблеми написання політик конфіденційності. А саме: а) значна кількість 3+ складових слів; б) незрозумілий та важко читаємий текст документації; в) політика конфіденційності схожа на юридичний документ; г) деякі документи не надають інформації про спосіб та процедуру видалення приватних даних користувача ресурсу у разі необхідності; д) великий обсяг тексту.

Дослідження показують, що політики конфіденційності не демонструються вимог зрозумілості та надійності, тим самим зменшуючи ефективність повідомлень про політику конфіденційності, і залишають користувачів вразливими до несвідомого розповсюдження персональних даних. Тобто в регламенті GDPR наведені критерії, слідуючи яким, можна написати чітку, зрозумілу, стислу політику конфіденційності, де користувачі зможуть знайти всю необхідну інформацію про збереження їх

персональних даних, терміни зберігання та спосіб видалення. Отримані результати використовуються як база для дослідження та складання правил і рекомендацій, для того щоб написати власну політику конфіденційності для програмного продукту.

Таблиця 1 - Топ веб-сайти і GDPR (GFI = індекс туманності Ганнінга, "+" - задовольняє, "-" - не задовольняє)

Номер критерия GDPR	1	2	3	4	5	6		
						GFI	Слова	3+ складові слова
YouTube	+	+	+	-	-	15.21	2831	487
Google.com	+	+	+	-	-			
Facebook	+	+	+	-	-	13.71	2697	416
Reddit	+	+	+	-	-	13.86	2680	423
Amazon.com	+	+	+	-	+	12.21	3059	581
BBC	+	+	+	+	+	11.34	5187	608
Wikipedia	+	+	+	+	-	13.74	445	91
eBay	+	+	+	-	-	17.97	5260	994
Twitter	+	+	+	-	-	13.51	3793	586

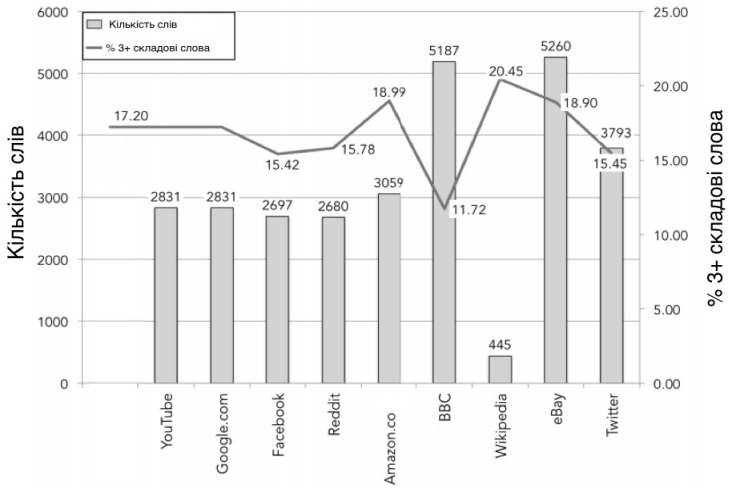


Рисунок 1 - Залежність кількості слів від % 3+ складових слів

Таблиця 2 - Результати власних досліджень (GFI = індекс туманності Ганнінга, "+" - задовольняє, "-" - не задовольняє)

Номер критерия GDPR	1	2	3	4	5	6		
						GFI	Слова	3+ складові слова
LinkedIn	+	+	+	+	+	*12.05*	5611	796
Instagram	+	+	+	+	+	*14.05*	4213	658
Yaposhka.kh.ua	+	+	+	+	+	*13.28*	1319	238

Список використаних джерел

1. How to Make Privacy Policies both GDPR-Compliant and Usable [Електронний ресурс] / Karen Renaud, Lynsay A. Shepherd // arXiv - 2018. – С. 4. – Режим доступу : https://arxiv.org/pdf/1806.06670.pdf

УДК 004.514

Обач В. А., Гермак В. С.
Центральноукраїнський національний технічний університет

Аналіз впливу темних патернів на свідомість людини

Коли мова заходить про прибутки, деякі компанії готові вдаватись до не зовсім добросовісних прийомів щоб заволодіти більшою кількістю клієнтів. Різноманітні маніпулятивні тактики, до яких вони вдаються при цьому, прийнято називати темними патернами. Темні патерни – це користувацькі інтерфейси, які розроблені з метою змусити користувачів зробити небажані для них самих дії. На відміну від непродуманого дизайну, темні патерни використовуються усвідомлено. Їх завдання - збити з пантелику і змусити вас помилитися.

В залежності від особливостей впливу на користувача можна виділити такі основні класи темних патернів: 1) приманка і перемикання - це патерн, при якому користувач, базуючись на своєму минулому досвіді виконує якусь дію, очікуючи на певний результат, а відбувається щось інше; 2) підтвердження з почуттям сорому – цей патерн реалізується в тому випадку, коли людина хоче піти з сайту або відписатися від чогось, на неї вистрибує виринаюче вікно, яке містить фразу або питання з варіантами відповідей, які її присоромлять і змусять залишитися; 3) замаскована реклама – призначена для того, щоб користувач сам не бажаючи того переглянув рекламу, з цією метою на сайтах і в додатках розміщують банери, замасковані під кнопки скачування, пункти меню або контент сторінки; 4) примусове продовження – це коли користувач підписується на безкоштовну пробну послугу, але йому примусово продовжують платну підписку; 5) спам друзів - додаток просить авторизації, а потім публікує повідомлення в соціальній мережі від імені користувача, направляючи спам на адресу його друзів або передплатників; 6) прихована вартість - на останньому етапі оплати за товар користувачеві раптом пропонують заплатити ще невелику суму: комісію, страховку або податок; 7) зміна фокуса – в той час як дизайн сайту привертає увагу користувача до одного об’єкту, на тому ж сайті по відношенню до нього відбувається щось небажане; 8) запобігання порівняння цін - патерн, який ховає від вас цінову політику продукту. Найчастіше це зміна кількості товарів в упаковці або зміна розміру упаковки; 9) цукерінг приватності – це практика використання прийомів веб-дизайну і фразеологізмів для створення незрозумілого і заплутаного інтерфейсу, який буде змушувати користувачів повідомляти про себе більше особистої інформації, ніж це потрібно; 10) пастки - створюють ситуації, коли користувачеві складно відмовитися від зробленого вибору і скасувати свою дію: відписатися від розсилки, видалити додаток; 11) сюрприз в кошику – це додавання зайвого товару в кошик покупця; 12) питання із секретом - цей патерн змушує користувача помилятися і робити неправильний вибір, для цього поруч поміщають два дуже схожих запитання, і при швидкому читанні може скластись хибне уявлення про їх зміст, що і призводить до помилкового вибору.

В наш час ще досить багато користувачів потрапляють в пастки темних патернів. Тому слід пам’ятати про те, що серйозні компанії розуміють, що короткочасний успіх, який несуть темні патерни, нівелюється в довгостроковій перспективі, тому вони ніколи не будуть користуватись подібними технологіями. Отже, кожен користувач, який ознайомлений з суттю подібних технологій, з легкістю омине пастки, розставлені компаніями – одноденками.

Список використаних джерел

1. Що таке темний патерн [Електронний ресурс]. – Режим доступу: http://dark.aic.ru
2. Види темних патернів [Електронний ресурс]. – Режим доступу: https://darkpatterns.org/types-of-dark-pattern
3. Алан Купер «Интерфейс. Основы проектирования взаимодействия». – СПб.: Символ-Плюс, 2017. – 688с.

УДК 004.514

Прокопов В. В., Гермак В. С.
Центральноукраїнський національний технічний університет

Огляд основних вразливостей SCADA-система та засобів їх усунення

SCADA-система (Supervisory Control And Data Acquisition) – програмно-апаратний комплекс збору даних і диспетчерського контролю. Зміст, вкладений в термін SCADA, змінювався разом з розвитком технологій автоматизації і управління технологічними процесами. У 80-ті роки під SCADA-системами частіше розуміли програмно-апаратні комплекси збору даних реального часу. З 90-х років термін SCADA більше використовується для позначення тільки програмної частини інтерфейсу АСУ ТП (автоматичної системи управління технологічними процесами).

SCADA-системи призначені для здійснення моніторингу та диспетчерського контролю великого числа віддалених або одного територіально розподіленого об'єкта.

Головне завдання SCADA-систем – це збір інформації про безліч віддалених об'єктів, що надходить з пунктів контролю, і відображення цієї інформації в єдиному диспетчерському центрі.

Першою кібератакою на SCADA-системи, яку оприлюднили, стала кібератака на автоматизовану систему ядерної програми Ірану. Комп'ютерний вірус Stuxnet проник в систему і порушив роботу центрифуг зі збагачення урану. З цього моменту починається сплеск атак на SCADA-системи, шкідливі програми починають розроблятися під конкретну АСУ ТП, самі атаки стають більш продуманими, удосконалюються також методи і способи доставки шкідливих програм.

Виходячи з особливостей побудовиможна виділити такі вразливості:

1) всі сервери і автоматизовані робочі місця (АРМ) операторів в автоматизованих системах працюють під управлінням тих чи інших операційних систем, які мають свої уразливості. для відомих вразливостей виходять спеціальні оновлення. але з огляду на те, що сервери і АРМи знаходяться в робочому режимі 24/7, не завжди виходить оперативно встановити всі оновлення. тому від моменту виявлення вразливостей до установки оновлень операційні системи залишаються уразливими для зловмисників;

2) сучасні SCADA-системи, як правило, пов'язані з корпоративними системами і використовують загальні комп'ютерні мережі і мають доступ в глобальну комп'ютерну мережу інтернет. таке рішення підвищує ефективність роботи підприємства, дозволяє економити ресурси, але, в той же час, створює додаткову уразливість SCADA-систем. до того ж, застосування бездротового і віддаленого доступу в АСУ ТП без авторизації і аутентифікації створює додаткові ризики;

3) АСУ ТП мають в своєму складі розгалужену мережу каналів зв'язку, пристрої безперебійного живлення, безліч різноманітного обладнання, найчастіше розміщеного на великій території, в важкодоступних місцях, що працює в складних умовах (екстремальні температури, вібрація, запиленість і т.д.). не завжди є можливість забезпечити 100% захист даного обладнання;

4) низька кваліфікація обслуговуючого персоналу часто призводить до помилок в конфігурації параметрів безпеки SCADA-системи, контролю доступу та розподілу повноважень користувачів. некваліфікований персонал часто не в змозі визначити, що саме в цей момент здійснюється атака на SCADA-систему.

Захист SCADA-систем від загроз – це непросте завдання, яке вимагає комплексного підходу. У мережах SCADA безпека необхідна на всіх рівнях, від фізичного до сервісів, мереж, середовищ зберігання і систем обробки даних.

Управління системними ресурсами і їх використання повинні здійснюватися під контролем засобів безпеки. Вибір таких засобів залежить від рівня складності системи, яка повинна бути охоплена ними цілком. Ще одна задача управління безпекою – забезпечення можливості її підтримки – вирішується шляхом тестування систем і перевірки відповідності вимогам. До числа таких процесів відноситься своєчасне виявлення збоїв і їх усунення для зниження ризиків і витрат на техобслуговування.

Політики контролю доступу покликані обмежувати санкціонований доступ і дії всередині системи SCADA, проте застосовувані сьогодні політики безпеки і засоби контролю доступу недостатньо суворі: всі зовнішні з'єднання з диспетчерською SCADA повинні належним чином контролюватися; повинен проводитися моніторинг будь-якої активності всередині системи з протоколюванням часу, імені користувача, дії і його об'єкта.

Згідно з рекомендаціями NIST з безпеки АСУ ТП, мережа SCADA слід розділити на три основні зони: міжмережеві екрани, системи запобігання вторгнень і демілітаризована зона. Склад цих трьох зон являє собою першу лінію оборони АСУ ТП, тоді як контроль операцій доступу до критично важливих серверів можна назвати засобами глибокої оборони.

Захисні компоненти слід своєчасно оновлювати, щоб вони могли протистояти новим векторам атак. Існують діагностичні рішення, що допомагають захисним компонентам розпізнавати і відстежувати сторонні сервіси, наприклад сканери портів, а також виявляти важливі зміни в конфігураціях засобів безпеки.

Для комутовані лінії і зв'язку по TCP/IP слід застосовувати механізми аутентифікації, які автоматично розривають неавторизовані виклики і припиняють спроби встановити зв'язок після певної кількості невдалих спроб. Можливі застосування систем зворотного виклику з ідентифікацією тих, що дзвонять, періодичне оновлення вірчих даних, частий аудит активних модемів з відключенням невикористовуваних і реєстрація всіх спроб віддаленого доступу.

Для захисту повідомлень SCADA, переданих по TCP/IP, можна використовувати віртуальні приватні мережі з режимом IPsec-тунелю і протоколом SSL, а VPN на основі SSL корисні для передачі трафіку HTTPS і віддаленій відправки запитів через веб-сервіси. Запити від таких сервісів до баз даних потрібно автентифікувати і контролювати, а для захисту вмісту самих баз застосовувати шифрування.

Щоб звести до мінімуму доступність бездротової мережі для атакуючих, перед її розгортанням слід провести аналіз можливих перешкод поширенню сигналу, а також визначитися з потужністю і територією охоплення антен. Варто змінити вірчі дані, встановлені виробником за замовчуванням, перш ніж розгортати мережу.

У мережах SCADA варто використовувати криптографічні сервіси при операціях завантаження або вивантаження з хмари, а також шифрувати дані, що розміщуються в хмарі. Необхідно також забезпечити захищену віртуалізацію ресурсів, розмежувати функціональні сервіси для захисту операційних процесів, стежити за активністю в хмарі та діями третіх сторін, що відносяться до SCADA, а також захищати інформацію про місцезнаходження ресурсів в хмарному середовищі.

Список використаних джерел

1. *SCADA-система [Електронний ресурс] . – Режим доступу: http://www.tadviser.ru/index.php/ SCADA_назначение_систем.*
2. *Вразливості SCADA-систем [Електронний ресурс] . – Режим доступу: http://asys.com.ua/helpful/ zashhita-scada-ot-ugroz.html .*
3. *Захист SCADA-систем [Електронний ресурс] . – Режим доступу: https://www.osp.ru/os/2014/01/ 13039680/.*

УДК 004.056.5

Романовська М. С.
Військовий інститут телекомунікацій та інформатизації

Компаративний аналіз визначення сутності поняття „кібербезпека”

Формування інформаційного суспільства та поширення процесів цифровізації є визначальними факторами процесу росту суспільства в XXI столітті. Стрімкий інноваційний розвиток інформаційно-телекомунікаційних технологій сприяв появі принципово нового середовища – кіберпростору, відкритого і вільного, а також виникненню нової системи віртуальних відносин. Але поряд із можливостями нова система віртуальних відносин зумовила нові проблеми, виклики і загрози. Зокрема, на сьогодні гостро стоїть питання забезпечення безпеки інформаційно-телекомунікаційних систем, а також захист інформаційних ресурсів, адже останнім часом спостерігається різке зростання інцидентів в області інформаційної безпеки, які мають широке поширення і набувають загрозливого характеру. Стурбованість кібератаками приймає глобальний масштаб, так як хакерські атаки завдають значної шкоди приватним, корпоративним, а також державним інтересам, як на національному так і на міжнародному рівні. Нові виклики та необхідність мінімізації загроз потребують чіткого розуміння сутності поняття „кібербезпека” для подальшої побудови ефективних систем захисту від кіберзагроз.

Різні підходи до визначення дефініції „кібербезпека” надано у таблиці 1.

Згідно стандарту Міжнародної організації зі стандартизації та Міжнародної електротехнічної комісії в області кібербезпеки ISO / IEC 27032:2012 кібербезпека тлумачиться як безпека в кіберпросторі або як збереження конфіденційності, цілісності, доступності в кіберпросторі [4].

Ураховуючи, що забезпечення кібербезпеки входить до кола питань національної безпеки, країни світу прийняли або здійснюють розробку стратегій кібернетичної безпеки, зокрема США, Канада, Японія, країни Європейського Союзу, Індія, Австралія, Нова Зеландія, Колумбія та інші.

Так, Національний комітет із систем безпеки США визначає: „кібербезпека: можливість захищати і боронити використання кіберпростору від кібератак”. Водночас, у стратегії кібербезпеки Німеччини це поняття трактується як бажаний стан безпеки інформаційних технологій, коли ризики для кіберпростору зменшені до прийнятного мінімуму. Натомість стратегічні документи Канади не містять чіткого визначення, але кібербезпека розуміється як захист кіберсистем від шкідливого неправильного їх використання та від інших деструктивних атак. Поряд із технічними аспектами кібербезпеки та підкресленням її принципів доступності, цілісності та конфіденційності, у стратегії Австралії увага звертається на необхідність захисту людини, особливо дітей, від впливу незаконного та образливого контенту, кіберзнущань, переслідувань і використання інформаційних технологій для цілей сексуальної експлуатації. Враховуючи, що об’єктом кібератак є переважно комп’ютерні та інформаційні системи, Національна стратегія Нідерландів першочерговими серед заходів кібербезпеки визначає попередження загроз і мінімізацію руйнівного впливу на них [2]. Така позиція підтримується Стратегією безпеки та оборони інформаційних систем Франції, а саме кібербезпека – бажаний стан інформаційної системи, коли вона здатна протидіяти викликам кіберпростору, які можуть негативно вплинути на достовірність, цілісність і конфіденційність даних, що зберігаються або обробляються цією системою [3].

Таблиця 1 – Тлумачення сутності поняття „кібербезпека”

Автор	Кібербезпека …
Міжнародний телекомунікаційний союз [12]	набір засобів, стратегії, принципи забезпечення безпеки, гарантії безпеки, керівні принципи, підходи до управління ризиками, дії, професійна підготовка, практичний досвід, страхування та технології, які можуть бути використані для захисту кіберсередовища, ресурсів організації та користувача
Європейська комісія [5]	заходи і дій, спрямовані на захист кіберпростору в цивільній і військовій сферах від загроз, які можуть завдати шкоди взаємозалежним мережам та інформаційній інфраструктурі або є пов’язаними з ними
Закон України „Про основні засади забезпечення кібербезпеки України” [10]	захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі
ISACA [1, 7]	захист інформаційних активів шляхом боротьби із загрозами безпеці інформації, яка обробляється, зберігається та передається за допомогою інформаційних систем, що взаємодіють за допомогою мереж
Фурашев В.М. [13]	стан здібності людини і держави щодо запобігання уникнення спрямованого, у першу чергу – несвідомого, негативного впливу (управління) інформації
Бутузов В.М. [9]	стан захищеності життєво важливих прав та інтересів людини, суспільства, держави у кіберпросторі від внутрішніх і зовнішніх протиправних посягань і загроз таких посягань
Мельник С.В. , Тихомиров О.О., Лєнков О.С. [11]	захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам у сфері функціонування інформаційно-телекомунікаційних систем
Баранов О.А. [8]	стан захищеності життєво важливих інтересів особистості, суспільства і держави в умовах використання комп’ютерних систем та / або телекомунікаційних мереж, за якого мінімізується завдання їм шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки функціонування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації

На властивості стійкості наголошує Стратегія Турції, підкреслюючи важливість захисту інформаційних систем, що входять до складу кіберпростору, забезпечення конфіденційності, цілісності та доступності інформації, яка обробляється у цьому просторі, виявлення та протидія атакам і кіберінцидентам [6]. Зауважимо, що останні характеризуються цільовою спрямованістю, високотехнологічністю, складністю у

виявленні та подоланні, масштабністю і швидкістю поширення, різноманітністю проявів ефектів впливу тощо.

Закон України „Про основні засади забезпечення кібербезпеки України", прийнятий у 2017 році, визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основіні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності, а також базові терміни у сфері кібербезпеки [10].

На сьогоднішній день у різних джерелах зустрічається багато тлумачень поняття „Кібербезпека". Значна кількість джерел, здебільшого українських, спираються на визначення поняття „Кібернетика". Даний підхід призводить до конфлікту сутності поняття та змісту визначення, не кажучи про розбіжність між значеннями поняття, які зустрічаються у міжнародних стандартах.

Компаративний аналіз визначення поняття „Кібербезпека" показав його багатомірність і дозволив визначити основну суть цього поняття. Законом України „Про основні засади забезпечення кібербезпеки України" визначено поняття „Кібербезпека" яким вдалось охопити всю багатогранність даного предмету.

Список використаних джерел

1. *Cybersecurity Fundamentals Glossary. 2014. URL: https://www.isaca.org/Knowledge-Center/Documents/Glossary/Cybersecurity_Fundamentals_glossary.pdf.*
2. *Holland, Den Haag: National Coordinator for Security and Counterterrorism, 2013. URL: // https://www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011.*
3. *Information systems defence and security: France's strategy. URL: https://www.enisa.europa.eu/media/news-items/Information_system_security_France_strategy.pdf/view.*
4. *ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity*
5. *Joint communication to the European parliament, the Council, the European economic and social committee and the Committee of the regions – Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Brussels, 7.2.2013. URL: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf/.*
6. *National Cyber Security Strategy and 2013-2014 Action Plan. – Republic of Turkey. Ministry of Transport, Maritime Affairs and Communications, 2013. URL: //www.ccdcoe.org/ strategies/TUR_CyberSecurity.pdf.*
7. *Transforming Cybersecurity. URL: www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Transforming-Cybersecurity-Using-COBIT-5.aspx.*
8. *Баранов О. А. Про тлумачення та визначення поняття «кібербезпека» / О. А. Баранов // Правова інформатика. – 2014. – № 2(42). – С. 54-62.*
9. *Бутузов В. М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз) : монографія / В. М. Бутузов. – К. : КИТ, 2010. – 408 с. – С. 176.*
10. *Закон України „Про основні засади забезпечення кібербезпеки України"(Відомості Верховної Ради(ВВР), 2017, №45, ст.403).*
11. *Мельник С. В. До проблеми формування понятійно-термінологічного апарату кібербезпеки / С. В. Мельник, О. О. Тихомиров, О. С. Лєнков // Актуальні проблеми управління інформаційною безпекою держави : зб. матер. наук.-практ. конф. (Київ, 22 березня 2011 р.). – К. : Вид-во НА СБ України, 2011. – Ч. 2. – С. 43-48.*
12. *Рекомендация МСЭ-Т X.1205. Обзор кибербезопасности. – Женева : МСЭ, 2009. [Електронний ресурс]. – Режим доступу : https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=9136 HYPERLINK "https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=9136&lang=ru"& HYPERLINK "https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=9136&lang=ru"lang=ru.*
13. *Фурашев В. М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності / В. М. Фурашев // Інформація і право. – 2012. – № 2. – С. 162-169.*

УДК 004.056.5

Семеній Д. М.
Навчально-науковий інститут інформаційної безпеки
Національної академії Служби безпеки України

Нормативно-правові засади забезпечення кібербезпеки України

Кібербезпека є однією із складових частин національної безпеки України. Вона пов'язана із стратегією формування виваженої державної політики, забезпечення інформаційної безпеки, яка повинна передбачати систему заходів державного та міжнародного характеру, належне місце в якому займає кібербезпека.

Відповідно до українського законодавство, кібербезпека - це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [1].

Кіберпростір - середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет або інших глобальних мереж передачі даних [1].

Поряд з національним законодавством на сьогодні існують і міжнародні нормативно-правові акти, які також надають відповідні визначення: кіберпростір – це середовище існування, що виникло в результаті взаємодії людей, програмного забезпечення та послуг в Інтернеті за допомогою технологічних пристроїв і мереж, що під'єднані до них, якого не існує в будь-якій фізичній формі [2].

Сучасний кіберпростір обумовлений виникнення нових загроз національній і міжнародній безпеці.Поряд з інцидентами природного походження зростає кількість і потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб.

Аналіз існуючих тенденцій свідчить, що окремі держави для реалізації власної протиправної мети починають дедалі частіше вдаватися до кібератак. Сьогодні комп'ютерні атаки, як правило, направлені за трьома ключовими напрями:

- виведення з ладу інформаційно-телекомунікаційної системи (ІТКС) та критичної інфраструктури за допомогою вірусів та спаму;
- несанкціонований доступ у систему з метою викрадення даних;
- незаконне оприлюднення персональних даних у мережі Інтернет стосовно політиків, правоохоронців чи військовослужбовців та інших осіб у поєднанні із прямими погрозами.

В нашій країні 27 червня 2016 року потужний комп'ютерний вірус "Petya A"паралізував роботу низки компаній в Україні. Найбільш уразливими виявились українські компанії та відомства. Серед постраждалих - уряд України, національна пошта, метрополітен Києва, міжнародний аеропорт "Бориспіль", Чорнобильська АЕС, а також низка ЗМІ, банків, комерційних структур.

Поширення кіберзлочинності та кібертероризму змусило Сполучені Штати Америки зайняти передові рубежі забезпечення безпеки власного кіберпростору та розширити співпрацю з рядом держав. В цьому контексті співробітництво США з

Україною у сфері кібербезпеки стало важливим чинником наших відносин і отримало тенденцію до розширення.

В лютому 2017 палата представників Конгресу США підтримала законопроект «Ukraine Cybersecurity Cooperation Act of 2017». Цей документ посилює співробітництво між Україною та США і передбачає чотири ключові напрями:

- вдосконалення систем безпеки урядових систем, в першу чергу тих, які захищають критичну інфраструктуру України;
- зменшення залежності від російських інформаційно-комунікаційних технологій;
- нарощування потенціалу, розширення обміну інформацією щодо кібербезпеки та співробітництво в кіберпросторі;
- допомогти в боротьбі з інформаційної війни.

Виникає необхідність нейтралізації подібних загроз,тому без основоположного закону навряд чи можливі інші рішення. На наш погляд, закон – теоретична, фундаментальна база, підзаконні акти деталізують шлях його імплементації.Наразі питання кібербезпеки регулюються базовим Законом України «Про основні засади забезпечення кібербезпеки України», Стратегією кібербезпеки України, Конвенцією про кіберзлочинність, Кримінальним кодексом України та іншими нормативно-правовими актами. Базовим законом встановлюється значна кількість понять, що є новими для правового поля України, зокрема «кібербезпека», «кіберзагроза», «кіберпростір», «кіберінцидент», «кібершпигунство», «кібертероризм». Одним з об’єктів кібербезпеки та кіберзахисту Закон визначає об’єкти критичної інфраструктури. Перелік вказаних об’єктів має затверджуватися Кабінетом Міністрів України, наразі відсутній.

Навіть в разі його затвердження КМУ, інформацію, що міститься в даному переліку, віднесено законодавством до інформації з обмеженим доступом. Тобто, пересічний громадянин не дізнається який об’єкт віднесено державою до критичної інфраструктури, що з точки зору захисту є правильним. Більше того, на даному етапі розвитку законодавства у сфері кібербезпеки, притягнення до кримінальної чи іншої відповідальності за кіберзлочини є практично неможливим.

Хоча законом і встановлено, що за порушення у сфері кібербезпеки особи несуть відповідальність згідно з цивільним, адміністративним та кримінальним законодавством, в кодексах відсутні будь-які згадки поняття "кіберпростір".

Наприклад, Кримінальним кодексом України передбачена відповідальність за вчинення злочинів у сфері використання електроно-обчислювальних машинах систем та комп’ютерних мереж і мереж електрозв’язку. Проте «кіберпростір» чи відповідальність за «кіберзлочин» не згадується жодного разу. Такий стан речей безперечно спричинить складнощі в застосуванні відповідальності за вчинення порушень у сфері кібербезпеки [3].

З огляду на викладене основними проблемами, які потребують розв’язання, є:

- недостатність та неузгодженість нормативно-правового регулювання з питань кібербезпеки;
- відсутність державного органу, відповідального за координацію дій у сфері захисту критичної інфраструктури;
- відсутність єдиних критеріїв та методології віднесення об’єктів інфраструктури до критичної інфраструктури;
- відсутність єдиної методології проведення оцінки загроз в кіберпросторі;
- нерозвиненість державно-приватного партнерства у сфері захисту кібербезпеки.

Проблеми забезпечення захисту кібербезпеки передбачається розв'язати шляхом:

- створення механізму реалізації нормативно-правової бази з питань кібербезпеки та кіберзахисту;

- визначення повноважень, завдань та відповідальності суб'єктів державної системи захисту критичної інфраструктури.

- розбудови державно-приватного партнерства у сфері кібербезпеки для підвищення безпеки та визначенням зобов'язань держави та власників;

- розроблення і затвердження єдиної методології проведення оцінки кібербезпеки об'єктів;

- розроблення переліку об'єктів критичної інфраструктури;

У Стратегії кібербезпеки України зазначається, що метою є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

Слід зазначити, що у зв'язку з її реалізацією Рада національної безпеки і оборони України ухвалила рішення про створення спеціального нового органу як робочого органу – Національного координаційного центру кібербезпеки(НКЦБ). Центр повинен виявляти на ранніх стадіях виникнення кіберзагрози і забезпечувати швидку її локалізацію. Також НКЦБ надає рекомендації з питань кібератак, кіберзахисту та кібербезпеки для державних та приватних підприємств, з якими можна ознайомитися на сайті координаційного центру кібербезпеки

Стратегія визначає, зокрема, такі основні пріоритети для безпечного, стабільного і надійного кіберпростору в Україні:

- розробка та оперативна адаптація державної політики в сфері кібербезпеки, досягнення сумісності з відповідними стандартами ЄС і НАТО;

- створення національної нормативно-правової та термінологічної основи в цій сфері, гармонізація нормативних актів у сфері електронних комунікацій, захисту інформації, інформаційної та кібербезпеки відповідно до міжнародних стандартів та стандартів ЄС і НАТО;

- розробка технологій кібербезпеки мобільних засобів зв'язку; розвиток електронної інфраструктури зв'язку [4].

Отже, подальше вдосконалення нормативно-правових актів, процесів і технологій забезпечення кібербезпеки збільшить ефективність захисту кіберпростору України. Підвищення обізнаності, просвіта та навчання у відповідності до чітко визначених пріоритетів кібербезпеки, принципів, політики, процесів, програм є надзвичайно важливим компонентом забезпечення достатнього рівню кібербезпеки, і їм повинно приділяти дуже багато уваги на усіх рівнях – політичному, законодавчому,економічному та регуляторному.

Список використаних джерел

1. *Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. №* 2163-VI. *[Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/2163-19.*
2. ISO/IEC 27032:2012 «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по обеспечению кибербезопасности».
3. *Що дасть Україні новий закон про кібербезпеку [Електронний ресурс]. – Режим доступу: https://biz.censor.net.ua/columns/3069149/scho_dast_ukran_noviyi_zakon_pro_kberbezpeku.*
4. *Про Стратегія кібербезпеки України: Указом Президентом України, Про рішення Ради національної безпеки і оборони України від 27 січня 2016 р. [Електронний ресурс]. – Режим доступу: https://www.president.gov.ua/documents/962016-19836.*

УДК 004.56.5:070

Толмачов Ю. П.
Центральноукраїнський національний технічний університет

Актуальні питання забезпечення інформаційної безпеки у медіасфері України

Важливим фактором соціального середовища, в якому змушені жити мешканці інформаційних суспільств, є інтегровані в нього аудіовізуальні (електронні, екранні) мас-медіа і продуковані ними тексти (медіатексти). Медіатекст створений людьми з певною метою, набуває самостійності і відтак сам починає впливати на людську свідомість. Він стає учасником соціального середовища, яке постає як медіасередовище, інтегрується в реальність існування людей, створюючи реальність нової якості – медіа реальність [1]. Це означає, що сприйняття світу значною мірою залежить від того, як його подають медіа. Телебачення, радіо, Інтернет є тим повсякденним тлом, від якого люди стають психологічно залежними. Блокування захисних механізмів відкриває інформаційному потоку вхід до підсвідомості людського розуму. Таким чином медіа є інструментом для кодування свідомості й "зомбування" особистості. При цьому система внутрішнього захисту "внутрішньої цензури" практично вимикається [2].

Для забезпечення інформаційної безпеки держави в медіасфері за останні роки зроблено багато: актуалізовано Стратегію національної безпеки України та Доктрину інформаційної безпеки України, запроваджено мовні квоти, блокування російських медіа-сервісів на території України і т.і. Зараз працюють механізми, які відроджують українську мову, культуру та забезпечують національні інтереси України в інформаційній сфері. Разом з тим до основних і актуальних на сьогодні загроз слід віднести намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації, а також прояви обмеження свободи слова та доступу громадян до інформації.

На даний момент дуже важко притягти до відповідальності теле-, радіо-, Інтернет-канали тощо за поширення недостовірної, неповної або упередженої інформації, за прояви обмеження свободи слова та доступу громадян до інформації. Тому пропонується створити окремий механізм або запровадити додаткову функцію Національної ради України з питань телебачення і радіомовлення, що буде отримувати й реагувати на скарги громадян, збирати факти та докази про поширення недостовірної інформації, антиукраїнської пропаганди, обмеження свободи слова. За цими матеріалами можна буде притягнути до відповідальності: спростування, вибачення, штраф, анулювання ліцензії на мовлення тощо. Практична реалізація означеного є можливою шляхом вдосконалення Закону України "Про телебачення і радіомовлення".

Отже, пропонується розширити спектр сервісу державного регулятора в галузі телерадіомовлення. Це дозволить підвищити ефективність законодавства України щодо масмедіа в частині запобігання поширенню теле-, радіо- або Інтернет-каналами недостовірної, неповної, упередженої інформації, проявів обмеження свободи слова, доступу громадян до інформації. Означене також дасть можливість підвищити рівень інформаційної безпеки України в медіасфері.

Список використаних джерел

1. *Петрунько О. В. Агресивне медіасередовище: якісний і змістовий дискурси / О. В. Петрунько // Освітній квартальник українського вчительського товариства у Польщі. – 2011. – № 16. – С. 36-43.*
2. *Козлітін Д. О. Медіа середовище сучасного дошкільника та роль майбутнього педагога у ньому / Д. О. Козлітін, І. І. Матющенко // Молодий вчений. – 2017. – № 3.2 (43.2). – С. 49-52.*

УДК 004.56.5:070

Хомяк О. О., Шматок О. С.
Національний авіаційний університет

Методологія формування систем захисту інформації сучасних АС

Захист інформації, як відомо – це сукупність організаційних, технічних та правових заходів, спрямованих на запобігання нанесенню збитків інтересам її власника. Основними об'єктами захисту при цьому є: технічні засоби приймання, обробки, зберігання та передавання інформації (ТЗПІ) та допоміжні технічні засоби і системи (ДТЗС). Це пояснюється тим, що застосування відповідних технічних й передусім фізичних та програмно-апаратних методів і засобів захисту означених підсистем покликано поставити бар'єр на шляху зловмисників й максимально виключити можливість ненавмисних порушень персоналу, викликаних їх помилками або недбалістю користувачів ІКС. Проте на даний час відсутня єдина системна методика концептуального проектування СЗІ.

Резюмуючи, можна виділити наступні, на мій погляд, найбільш гострі на сьогодні проблеми розвитку теорії та практики захисту інформації[1]: створення теоретичних основ захисту інформації та формування науково-методологічного базису, що дозволяють адекватно описувати процеси захисту в умовах значної невизначеності та непередбачуваності прояву дестабілізуючих чинників; розробка науково обґрунтованих підходів до формування нормативно-методичних документів щодо захисту інформації; розробка методології стандартизації підходів до створення систем захисту інформації та раціоналізації схем і структур управління захистом на об'єктовому, регіональному та державному рівнях. Тож основна мета і спрямованість наукових досліджень в області забезпечення інформаційної безпеки полягає сьогодні в розробці концептуальних і методологічних основ інтенсифікації процесів захисту інформації та раціоналізації підходів до організації систем захисту і управління їх функціонуванням.

Концептуально найважливішою вимогою, що пред'являються до СЗІ, є вимога адаптованості, яке обумовлюється, з одного боку, тим, що численні фактори, що впливають на необхідний рівень захисту, можуть істотно змінюватися, а з іншого - тим, що самі процеси захисту інформації відносяться до слабо структурованих. Управління такого роду процесами ефективно тільки за умови адаптованості системи.[3]

Крім цього до СЗІ пред'являються також різні вимоги функціонального, ергономічного, економічного, технічного та організаційного характеру.

В умовах системно-концептуального підходу до захисту, загальнометодологічні принципи включають концептуальну єдність системи, адекватність поставленим вимогам, адаптованість, функціональну самостійність, зручність використання, мінімізацію наданих прав, повноту контролю, активність реагування, економічність. Очевидно, що архітектура СЗІ повинна бути аналогічною архітектурі захищається системи і може розглядатися в функціональному, організаційному і структурному аспектах [2].

Для забезпечення надійного захисту інформації в сучасних умовах особливого значення набуває попередження виникнення умов, що сприяють породженню загроз безпеки інформації, звідси істотно підвищується значимість законодавчих, організаційно-психологічних і морально-етичних засобів захисту. Отже, увага все більш зосереджується на системних питаннях захисту інформації, розглянутих у [5].

При переході на регіональний (а тим більше державний) рівень розгляду проблеми переважаюче значення набувають завдання стратегічного плану: створення і примноження інформаційних ресурсів, їх збереження та використання відповідно до економічних і політичних потребах розвитку, включаючи і потреби забезпечення інформаційної безпеки. Все це вже означає не просто захист інформації в процесі її обробки і захист від інформації в процесі її циркуляції, а системну ув'язку завдань забезпечення інформаційної безпеки з іншими завданнями рішення інформаційних проблем суспільства.

Список використаних джерел

1. Герасименко В.А. Основи захисту інформації: Підручник. — М.: МИФИ, 2009.
2. Гуз А. М. Захист інформації в Україні та провідних країнах світу
3. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI
4. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі
5. Шураков В.В. Забезпечення збереження інформації в автоматизованих системах обробки даних. - М: Фінанси і статистика, 2013.

УДК 004.056.5
Артюх С. Г., Шевченко А. С.
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут

Аналіз методик забезпечення інформаційної безпеки організацій та інформаційних систем

Сплеск кібератак та інцидентів кібернетичної безпеки загострив стан інформаційної безпеки (ІБ) в Україні. На сьогоднішній час критично стоять питання забезпечення інформаційної безпеки інформаційних систем (ІС) та організацій в цілому.

Побудова довірених інформаційних систем передбачає впровадження ряду сервісів безпеки та механізмів захисту інформації (МЗІ). Контроль інформаційної безпеки ІС здійснюється як на етапі проектування, так і на етапі функціонування під час аудиту ІБ. Під час аудиту ІБ здійснюється перевірка складу реалізованих МЗІ, технічної та організаційної складових, процесів управління системою ІБ. Реалізація заходів ІБ повинна відповідати актуальним стандартам інформаційної безпеки на усіх етапах життєвого циклу інформаційної безпеки.

На даний час в Україні імплементований міжнародний стандарт інформаційної безпеки ДСТУ ISO/IEC 27001:2015. Але на сьогоднішній день у світовій практиці паралельно розроблені та застосовуються ряд методик (практик) забезпечення інформаційної безпеки, таких як: CIS, NIST, PCI DSS, HIPAA, FISMA, ITIL.

Результати порівняльного аналізу методик дозволили виділити основні стандарти, які найбільш повно відображають заходи щодо забезпечення ІБ. До таких стандартів відносяться стандарт NIST SP 800-53 rev.5 “Security and Privacy Controls for Federal Information Systems and Organizations” та CIS 20 “Critical Security Controls”.

Стандарт NIST SP 800-53 надає комплексний набір критичних контролів безпеки, а також інструкції щодо їх вибору та застосування для захисту операцій та активів організацій, фізичних осіб, інших організацій. Стандарт поділяє критичні контролі на типи в залежності від призначення, на сімейства – відповідно до області застосування та рівні пріоритетів відповідно впливу на систему захисту.

Сам по собі документ не визначає перелік функцій та способи практичного застосування, а лише має посилання на стандарти сімейства NIST 800, що створює додаткові складнощі та вимагає більше часу на розгортання системи ІБ.

Розроблений інститутом SANS CIS 20 Critical Security Controls є рекомендованим набором практичних дій щодо реалізації заходів забезпечення ІБ У загальній складності до методики входить 20 елементів керування, що охоплюють пріоритетні сфери, такі як: захищені апаратні та програмні конфігурації, захист від шкідливого програмного забезпечення, процедури відновлення даних після збоїв, моніторинг та контроль облікових записів, тести на проникнення та інші.

CIS Controls, на відміну від NIST, визначає меншу кількість критичних контролів та простішу їх класифікацію. Дана методика дозволяє впроваджувати базові системи захисту поетапно під час функціонування організації та ІС, що не блокує їх функціонування.

Проведений аналіз сучасних методик та стандартів ІБ дозволив виділити основні домени забезпечення ІБ. Реалізації рекомендацій кожного домену дозволяє комплексно забезпечити ІБ організації та ІС. Найбільш прийнятним на даний час є застосування вимог методики CIS Controls, що на відміну від інших стандартів має більш прозорі та практичні рекомендації щодо реалізації заходів ІБ та дозволяє використовувати фрагментарний спосіб впровадження вимог базових доменів.

УДК 004.056.53

Безрук Є. А., Брусеньский В. Р., Нікуліщев Г. І.
Запорізький національний технічний університет

Використання технології uXTD та методу Timing-атак для деанонімізації користувачів Tor

На зараз мережа Tor [1] є найбільшою в світі розгорнутою анонімною мережею. Щомісячне число активних користувачів мережі перевищує 4 млн осіб. Клієнтське програмне забезпечення Tor маршрутизує Інтернет-трафік через всесвітню мережу добровільно встановлених серверів з метою приховування розташування користувача.

Крім звичайних користувачів перевагами анонімізації трафіку можуть користуватися, продавці наркотиків і зброї, терористи а також інші порушники закону. Таким чином, деанонімізація користувачів є актуальною і важливою задачею для спеціальних служб багатьох держав [3, 4].

Нижче подано терміни та скорочення, використані в роботі.

Tor (The Onion Router) — анонімна мережа і відкрите програмне забезпечення, що дозволяє зберігати користувачам свою анонімність.

Корумпована автономна система — автономна система, контрольована спостерігачем.

Корумпований сервер — кінцева точка призначення, контрольована спостерігачем.

Корумпований вузол — вузол, трафік якого може модифікувати і переглядати атакуючий.

Прихована служба - портал / сайт, доступний тільки всередині мережі Tor.

Timing-атака — атака по стороннім каналам, в якій атакуючий намагається скомпрометувати систему за допомогою аналізу часу, що витрачається на виконання операцій.

uXDT (ultrasound cross-device tracking) — технологія збору даних за допомогою ультразвуку

Cross-Site Scripting (XSS) — тип вразливості інтерактивних інформаційних систем у вебі.

SDK (software Development Kit) — набір із засобів розробки, утиліт і документації, який дозволяє програмістам створювати прикладні програми

Мережа Tor складається з добровільних серверів, які є її вузлами. Користувачі через проксі Tor завантажують список вузлів з сервера каталогів і будують анонімні тунелі, використовуючи маршрутизацію Tor. Проксі будує ланцюг який, складається з трьох вузлів: вхідного (guard), проміжного (middle), вихідного (exit). Час життя ланцюга становить 10 хв. Вхідний вузол вибирається із фіксованого набору з трьох вузлів, унікального для кожного проксі. Більш детальний опис Tor можна знайти в роботі [2].

Оскільки мережа Tor є мережею, яка являє собою надбудову над вже існуючою мережею, вона працює на основі транспортного рівня моделі OSI. Основними організаціями, які управляють інтернет-маршрутизацією, є автономні системи (далі - АС). Атакуючий може контролювати одну або кілька АС і передбачається, що він споглядає трафік, що проходить через АС. Аналіз впливу АС на деанонімізацію користувачів Tor можна знайти в роботі [5].

Атакуючий має на меті скомпрометувати як можна більше ланцюгів, що відносяться до деякого конкретного користувача або групи користувачів, оскільки компрометація ланцюгів тягне за собою деанонімізацію користувачів.

Використання uXDT. Метод, описаний в [8], покладається на заманювання користувача Tor на веб-сторінку, яка містить рекламні оголошення, що видають ультразвук, або ж на сторінку, яка містить прихований JavaScript-код, який змушує браузер видавати ультразвук за допомогою HTML5 Audio API.

Ультразвукове перехресне відстеження пристроїв, також відоме як uXDT, використовує мобільні колонки і мікрофон для випускання ультразвуків (звуки, які вище за частотою, ніж те, що чує людське вухо) і їхнього сприйняття.

Мікрофони, що знаходяться поруч з джерелом звуку (в ноутбуках, смартфонах, планшетах тощо), здатні вловлювати коротку послідовність високочастотних тонів. Якщо при цьому на пристрої встановлено додаток, чий SDK містить функціональність з пошуку таких маячків, «почувши» ультразвук, uXDT-фреймворк витягує з нього унікальний ідентифікатор оголошення і. доповідає на віддалений сервер про те, що користувач, який володіє телевізором X, тільки що прослухав рекламу, яку також «чув» смартфон Y. Все це дозволяє скласти більш повний профіль користувача, дізнатися якими пристроями той володіє, чим цікавиться, коли буває вдома тощо.

Користувачі Tor можуть спробувати уникнути викриття uXDT, використовуючи додаток NoScript чи аналогічні для блокування JavaScript, тому що більшість розгорнень uXDT відбувається якраз за допомогою JavaScript. Однак іншим способом, завдяки якому можливо розгорнути маяки uXDT, є використання шкідливого вузла виходу Tor, який вводить код для маяка uXDT з використанням атаки Man-In-The-Middle [8]. Уразливості Cross-Site Scripting (XSS) також можуть використовуватися для розгортання uXDT.

Деякі надбудови включають NoScript, який може блокувати всі JavaScript і може зупинити XSS, а також HTTPS Everywhere, якщо користувач уникає незашифрованих веб-сайтів (або переглядає їх через зашифрований проксі), HTTPS Everywhere запобіжить появі шкідливого вихідного вузла з можливістю вставляти код uXDT в веб - сторінки. Браузер Tor, що надається в Tails OS, також включає Adblock Plus, який може допомогти блокувати рекламу uXDT.

Втім, незважаючи на зареєстровані випадки uXDT-атак, на думку авторів, їхній масовості перешкоджає необхідність широкого розповсюдження на «розумних» пристроях (смарт-тв, смартфонах, колонках з інтелектуальним помічником тощо), які мають оточувати потенційний об’єкт атаки, додатків з необхідним SDK, підконтрольних зловмиснику.

Timing-атака. Timing-атака з використанням браузера [6] дозволяє виявити частину користувачів Tor, які використовують корумпований вузол і залишили відкритим вікно браузера більш ніж на годину. Для реалізації атаки необхідний корумпований сервер, вхідний і вихідний корумповані вузли.

Вихідний вузол модифікує HTTP-трафік, що проходить через нього, вставляючи контейнер iframe, що містить JavaScript-код. JavaScript-код багаторазово контактує з сервером, посилаючи унікальний ідентифікатор, і продовжує працювати до тих пір, доки залишається відкритою вкладка із зараженою сторінкою в браузері.

Нижче поетапно розглянуто як реалізовується сама атака.

Атакуючий вносить два корумпованих вузла в мережу Tor (вхідний і вихідний), а також розвертає веб-сервер, який отримує і записує дані, надіслані JavaScript-кодом.

Корумпований вихідний вузол модифікує весь HTTP-трафік, вставляючи туди JavaScript-код, який генерує сигнал для кожного клієнта Tor.

Веб-браузер клієнта запускає JavaScript-код, посилаючи при цьому сигнал на сервер. Цей трафік надходить через клієнта Tor, але клієнт все таки залишається анонімним.

Кожні десять хвилин проксі будує новий ланцюг, після чого він вибирає корумпований вхідний вузол (завжди випадково).

Атакуючий проводить аналіз трафіку для того, щоб порівняти отримані сигнали на кожному ланцюзі, що надходять через його вхідний вузол, з різними сигналами, які приймає веб-сервер. Збіг зіставляється з історією трафіку, записаною під час використання корумпованого вихідного вузла [9].

Вхідному вузлу тільки необхідно реєструвати шаблон трафіку, що проходить на кожному ланцюзі, вихідний вузол потрібен для вставок JavaScript-коду[6].

Timing-атаки також можуть здійснюватись з використанням протоколу граничної маршрутизації BGP. Згідно з [6] такі атаки бувають двох типів.

Розгляд трафіку через BGP-прослуховування. Для того щоб зробити точну деанонімізацію користувача через аналіз трафіку, корумпована АС може запустити BGP-підслуховування. Така атака дозволяє АС стати проміжною на шляху у напрямку до вхідного вузла, тобто після перехоплення трафік повертається назад до потрібної точки призначення. Вона дозволяє зберегти з'єднання, залишаючи можливість АС точно деанонімізувати клієнта через Timing-аналіз.

Розгляд трафіку через BGP-викрадення. Для деанонімізації користувача споглядач-зловмисник може, застосувати вже відомі атаки для компрометації вхідного вузла [7]. Після чого він починає атаку префіксного перехоплення проти префікса, що відповідає вже знайденому вхідному вузлу. Атака дозволяє корумпованій АС побачити трафік, який призначається вхідному вузлу, за рахунок поглинання всього трафіка вхідного вузла. Тому з'єднання буде активним тільки деякий час, а потім воно буде скинуто[9].

У роботі були розглянуті методи, що дозволяють успішно провести деанонімізацію користувачів мережі Tor. На основі аналізу методів можна зробити висновок, що атакуючому необхідно мати великий запас ресурсів, як часових, так і мережевих та обчислювальних, а також нерідко необхідний контроль над АС. Тому, на часі деанонімізація великої кількості користувачів Tor може вдатися, наприклад, зловмисникам, які контролюють масштабні ботнети, державним службам чи великим приватним корпораціям.

Список використаних джерел

1. *Dingledine R., Mathewson N.. Tor: The Second- Generation Onion Router [Електронний ресурс]. — Режим доступу: https://svn.torproject.org/svn/projects/design- paper/tor-design.pdf*
2. *.TorMetrics [Електронний ресурс]. — Режим доступу: https://metrics.torproject.org*
3. *The Russian government hired people to hack the Tor browser, but they failed and now they're quitting [Електронний ресурс]. — Режим доступу: https://ineduza.io/en/news/2015/09/09/the-russian-government-hired-people-hack-the-tor-browser-but-they-failed-and-now-they-re-quitting*
4 *The NSA's Been Trying to Hack into Tor's Anonymous In¬ternet For [Електронний ресурс]. — Режим доступу: http://gizmodo.com/the-nsas-been-trying-to-hack-into-tors- anonymous-inte-1441153819*
5 *Danezis G. Statistical disclosure attacks [Електронний ресурс]. — Режим доступу: http://freehaven.net/anonbib/cache/statistical-disclosure.pdf*
6 *Abbot T., Lai K., Lieberman M., Price E. Browser-Based At¬tacks on Tor [Електронний ресурс]. — Режим доступу: https://www.petsymposium.org/2007/papers/PET2007_preproc_Browser_based.pdf*
7 *Vanbever L., Li O., Rexford J., Mittal P. Anonymity on QuickSand: Using BGP to Compromise Tor [Електронний ресурс]. — Режим доступу: http://conferences.sig- comm.org/hotnets/2014/papers/hotnets-XIII-final80.pdf*
8 *Catalin Cimpanu A Ultrasound Tracking Could Be Used to Deanonymize Tor Users [Електронний ресурс]. — Режим доступу: https://www.bleepingcomputer.com/news/security/ultrasound-tracking-could-be-used-to-deanonymize-tor-users/*
9 *Безрук Є.А. Деанонімізація користувачів TOR за допомогою методу активних timing – атак / Безрук Є.А., Брусенський В.Р., Куцак С.В. // Майбутній науковець-2017: VIII всеукр. наук.-практ. конф., 1 грудня 2017 р.: тези доп. – Сєвєродонецьк, 2017. – С. 265 – 267.*

УДК 004.9

Бойко О. С.
Харківський національний університет радіоелектроніки

Протидія несанкціонованому запису мовної інформації

Захист мовної інформації у наш час є одним із найважливіших серед комплексу заходів захисту інформації. Несанкціоноване ознайомлення й зняття мовно інформації зловмисником може понести за собою великі втрати. Тому захист цего сегменту не менш важливий. Наприклан під час переговорів можуть бути озвучені и коди доступу, паролі які при попаданні до зловмисника будуть використані проти їх власника, не кажучи про виток комерційної темниці й так далі. Саме тому ця тема є актуальною навіть у час комп'ютерів та електроніки.

Для перехоплення зловмисник може використовувати широкий арсенал портативних засобів акустичної розвідки, які дають змогу перехоплювати мовну інформацію акустичним, віброакустичним, електроакустичним та оптикоакустичним каналами.

* електронні стетоскопи;

* спрямовані мікрофони;

*малогабаритні диктофони, магнітофони та пристрої запису на основі цифрової схемотехніки;

Основні з таких засобів:

*електронні пристрої перехоплення мовної інформації (закладні пристрої) з датчиками мікрофонного й контактного типів з передаванням перехопленої інформації по радіо, оптичному (в інфрачервоному діапазоні хвиль) та ультразвуковому каналах, мережі електроживлення, по телефонних лініях зв'язку, з'єднувальних лініях допоміжних технічних засобів або спеціально прокладених лініях;

* оптико-електронні (лазерні) акустичні системи та ін.

Портативна апаратура звукозапису та закладні пристрої із датчиками мікрофонного типу (перетворювачі акустичних сигналів, що поширюються в повітряному та газовому середовищах) можуть бути встановлені під час неконтрольованого перебування фізичних осіб ("агентів") безпосередньо у виділених приміщеннях. Ця апаратура забезпечує реєстрацію розмови середньої гучності на відстані 10-15 м від її джерела.

Електронні стетоскопи та закладні пристрої з датчиками контактного типу дають змогу перехоплювати мовну інформацію без фізичного доступу "агентів" до захищуваного приміщення. При цьому датчики закладних пристроїв установлюються переважно біля місць можливих витоків такої інформації:

*мікрофонного типу (біля виходів кондиціонерів та вентиляційних каналів);

*контактного типу (перетворювачі віброакустичних сигналів, що поширюються по будівельних конструкціях споруд, інженерних комунікаціях та ін.) на зовнішніх поверхнях будівель, у віконних проймах та рамах, у суміжних (службових і технічних) приміщеннях за дверними проймами, на перегородках, трубах систем опалення та водопроводу, коробах вентиляційних та інших систем.

Відомо, що за допомогою таких засобів розвідки можна перехоплювати мовну інформацію в залізобетонних будівлях через 1-2 поверхи, по трубопроводах через 2-3 поверхи і по вентиляційних системах 20-30 м завдовжки.

Застосування для ведення розвідки спрямованих мікрофонів і оптико-електронних (лазерних) акустичних систем не потребує проникнення "агентів" не тільки у виділені

(захищувані) приміщення та суміжні з ними, а й на охоронну територію об'єкта. Розвідку можна вести із сусідніх будівель чи автомобілів, що перебувають на автостоянках біля будівлі.

За допомогою спрямованих мікрофонів можна перехоплювати розмову із виділених приміщень за наявності в них вікон в умовах міста (на фоні транспортних шумів) на відстані близько 50 м.Максимальна відстань ведення розвідки з використанням оптико-електронних (лазерних) акустичних систем, які знімають інформацію з внутрішнього скла, сягає 150-200 м в умовах міста (наявність інтенсивних акустичних перешкод, запиленість повітря).Захисту мовної інформації можна досягти проектно-архітектурними рішеннями, проведенням організаційних і технічних заходів, а також виявленням електронних пристроїв перехоплення інформації. Канали витоку мовної інформації можна виявити на об'єкті, знайшовши підслуховувальні пристрої й системи.

Аналіз ризиків дає можливість виявити всі реальні загрози інформаційній безпеці об'єкта, які класифікують за кількома критеріями: за імовірністю прояву, за можливими збитками та ін.

Для захисту мовної інформації з обмеженим доступом від витоку технічними каналами на об’єктах інформаційної діяльності створюється комплекс ТЗІ. Комплекс ТЗІ складається з наступних заходів та засобів, призначених для захисту інформації:

- організаційних;
- інженерних;
- технічних.

Результатом проведення всіх вищеперерахованих заходів є випробування та атестація.

Випробування комплексу ТЗІ – сукупність аналітичних, експериментальних та вимірювальних робіт, які проводяться з метою визначення повноти виконання вимог щодо захисту від витоку інформації з обмеженим доступом технічними каналами, а також перевірки (контролю) повноти та достатності реалізованих заходів із захисту інформації на об'єктах інформаційної діяльності.

Атестація – це, визначення відповідності виконаних робіт зі створення комплексу ТЗІ на об'єкті інформаційної діяльності вимогам нормативних документів з питань ТЗІ.

Під час проведення робіт із захисту інформації від витоку технічними каналами здійснюються наступні етапи:

1. Категоріювання об’єкта інформаційної діяльності.

Категоріювання об’єкта інформаційної діяльності або іншими словами встановлення категорії об’єкта - це встановлення класифікаційної характеристики важливості об’єкта, за якою визначається необхідний рівень захисту інформації, що обробляється технічними засобами та/або озвучується на цьому об’єкті.

2. Обстеження ОІД.

Під час обстеження з’ясовуються:

- умови функціонування ОІД, архітектурно-будівельні особливості та особливості розташування його на місцевості відносно меж контрольованої зони (КЗ);
- наявність і порядок роботи технічних засобів, що оброблятимуть ІзОД, та технічних засобів, які не використовують безпосередньо для її оброблення, визначають місця їх розташування на ОІД та їх особливості;
- розташування інженерних комунікацій та металоконструкцій, наявність транзитних, незадіяних кабелів, що виходять за межі КЗ тощо.

3. Попередні інструментальні дослідження щодо захищеності мовної інформації від витоку технічними каналами проводяться з метою оцінки захищеності мовної інформації з обмеженим доступом від витоку технічними каналами без використання засобів активного захисту.

4. Визначення загроз для інформації з обмеженим доступом.

Визначення загроз для інформації з обмеженим доступом здійснюється на основі відомостей, викладених в акті категоріювання, акті обстеження ОІД, протоколах попередніх інструментальних досліджень, будівельних схемах, кресленнях тощо.

Можливі загрози для інформації з обмеженим доступом відображаються у Моделі загроз для інформації, яка циркулює на ОІД.

5. Формулювання технічних вимог до комплексу ТЗІ.

Формулювання технічних вимог до комплексу ТЗІ здійснюється в технічному завданні на створення комплексу ТЗІ (далі – ТЗ). ТЗ повинне містити наступні вимоги:

загальні вимоги;

- вимоги щодо стійкості до зовнішніх впливів;
- вимоги з безпеки експлуатації;
- вимоги до метрологічного забезпечення;
- вимоги щодо забезпечення охорони державної таємниці;
- вимоги щодо технічного забезпечення виконання робіт;
- вимоги щодо забезпечення безпеки при виконанні робіт;
- вимоги до документації.

6. Проведення монтажних/демонтажних робіт, пуско-наладка засобів захисту інформації.

На цьому етапі здійснюється монтаж технічних засобів захисту інформації, необхідних для забезпечення вимог технічного завдання, а також демонтаж систем, транзитних, незадіяних (повітряних, настінних, зовнішніх та закладених в каналізацію) кабелів, контурів та інших комунікацій застосування яких не обґрунтовано службовою чи виробничою необхідністю.

Якщо, неможливо або недоцільно захищати інформацію пасивними заходами захисту (див. розділ «Захист інформації від витоку акустичним, віброакустичним та оптоелектронним каналами») використовуються активні засоби захисту інформації.

Результати монтажних робіт засобів захисту інформації відображаються у відповідному акті.

7. Атестація ОІД

7.1.Складання Програми і методик випробувань.

7.2.Проведення робіт з виявлення закладних пристроїв.

7.3.Висновки за результатами випробувань. Акт атестації ОІД.

Основні характеристики ОІД відображаються в Паспорті на комплекс технічного захисту інформаці.

Список використаних джерел

1. *Экономическая безопасность хозяйственних систем: Учебник / Под ред. А. В. Колосова. -М.: РАГС, 2001.-446 с.*
2. *Віхорсв С. В., Кобцев Р. Ю. Як дізнатися - звідки напасти або звідки виходить загроза безпеці інформації // Захист інформації. Конфідент. - 2002 - № 2*
3. *Інтернет ресурс https://tzi.ua*
4. *Живко М. О. Захист інформації в системі економічної безпеки та підприємства /' Регіональне і місцеве самоврядування в нових умовах: партійна публічна адміністрація і безпосередня демократія: Мат-ли НІ укр.-польськ. наук.-практ. конф. (Львів, 2-4 березня 2006р.). - Л., 2006. - С.270-277*

УДК 004.9

Колодяжний І. О.
Центральноукраїнський національний технічний університет

Дослідження алгоритмів аналізу віртуальних соціальних мереж

Віртуальна соціальна мережа – популярний вид інтернет-спільноти, що відображає соціальну структуру зв'язків між людьми, основою яких можуть бути торгівля, гроші, ідеї, знання, кар'єра, стосунки тощо. Часто ця структура є відображенням зв'язків, які існують у реальному житті.

Одна з найпопулярніших соціальних мереж Facebook містить 10 млн. лише українських акаунтів, станом на 2017 рік. Подібних соціальних мереж безліч, на зважаючи на те, що популярними вони стали не так вже й давно.

З формальної точки зору соціальні мережі зручно представляти у вигляді графів і застосовувати для їх аналізу розвинені математичні моделі.

Аналіз соціальних мереж, який також можна застосувати до аналізу структури та властивостей особистих відносин, веб-посилання на сторінки, і поширення повідомлень, є областю досліджень в соціології. Останнім часом аналіз соціальної мережі привертає все більшу увагу в науковому співтоваристві інтелектуального аналізу даних.

Алгоритми визначення співтовариств. Виділення співтовариств у соціальних мережах є важливою задачею, вирішення якої дозволяє віднайти користувачів мережі зі спільними властивостями. Ці дані можна використовувати, наприклад, в маркетингу, інформаційній безпеці, тощо.

Алгоритми кластеризації графів для визначення співтовариств. Знаходження кластерів дозволяє виявити ті чи інші структури, приховані в соціальній мережі [1]. Кластеризація мережі – розбиття соціальної мережі на непересічні підмножини – кластери, так, щоб кожен кластер складався зі схожих об'єктів, а об'єкти різних кластерів істотно відрізнялися. Даний алгоритм, на відміну від традиційних алгоритмів кластеризації, дозволяє об'єднувати об'єкти в соціальній мережі в різні кластери на основі їх зв'язків і визначати відношення між кластерами динамічно, що не вимагає великої кількості пам'яті.

Визначення співтовариств на основі алгоритму послідовного видалення «навантажених» дуг. Ідея алгоритму полягає в тому, що з графу послідовно видаляються дуги з максимальним міжряддям, при цьому після кожного видалення знову перераховується міжряддя для всіх дуг. Як тільки граф розпадається на незв'язні компоненти, отримується розбиття по цим компонентам зв'язності. Для того, щоб оцінити якість цього розбиття, використовується міра модулярності. В роботі [2] було запропоновано алгоритм, який використовує на кожному кроці глобальну інформацію про всю мережу за допомогою міри «міжряддя» (betweenness), яка визначається для кожної дуги. Міжряддя дуги є мірою того, наскільки часто вона входить в найкоротші шляхи між різними парами вузлів. Інтуїтивно зрозуміло, що якщо два співтовариства з'єднані невеликою кількістю дуг, то всі шляхи між вузлами з одного співтовариства до вузлів з іншого співтовариства повинні будуть проходити через ці кілька дуг. Підраховуючи кількість разів, коли кожна дуга входить в найкоротший шлях між усіма парами вузлів графа, можна отримати міру міжряддя цієї дуги.

Алгоритми вимірювання інформаційного впливу. Дані алгоритми можуть використовуватися для пошуку найбільш впливових учасників мережі, Дана задача є важливою для соціологічних досліджень, у маркетингу та політології.

В [3] запропонований метод вимірювання інформаційного впливу між користувачами в соціальних мережах з орієнтованими зв'язками і переважанням

текстового вмісту (на прикладі Twitter). основою методу є модель, що враховує такі індикатори інформаційного впливу, як близькість інтересів користувачів, кількість оригінальних повідомлень і цитувань, опублікованих користувачем під впливом інших користувачів, близькість користувачів в соціальному графі, а також факт знаходження користувачів в одних і тих же співтовариствах. Крім того, даний метод має низьку обчислювальну складність і має розподілену реалізацію на основі фреймворку Apache Spark, що дозволяє обробляти графи соціальних мереж з населенням понад 1 мільярда користувачів.

Запропонований метод може застосовуватися в системах соціальної рекомендації, а також для пошуку тематичних експертів і знаменитостей, які володіють значним інформаційним впливом на конкретного користувача або в масштабі всієї мережі.

Алгоритми аналізу тональності тексту. Клас методів контент-аналізу в комп'ютерній лінгвістиці, призначений для автоматизованого виявлення в текстах емоційно забарвленої лексики і емоційної оцінки авторів (думок) по відношенню до об'єктів, мова про які йде в тексті [4].

Класифікація за бінарною шкалою. Полярність документа можна визначати за бінарною шкалою. У цьому випадку для визначення полярності документа використовується два класи оцінок: позитивна чи негативна. Одним з недоліків цього підходу є те, що емоційну складову документа не завжди можна однозначно визначити, тобто документ може містити ознаки позитивної оцінки, так і негативної ознаки. Ранні роботи в цій області включають в себе праці Терні і Панга, які застосовують різні методи розпізнавання полярності оглядів товару і відгуків про фільмах відповідно. Це приклад роботи на рівні документа.

Класифікація за багатосмуговою шкалою. Можна класифікувати полярність документа за багатосмуговою шкалою, що було зроблено Пангом і Снайдером (серед інших). Ними було розширене основне завдання класифікації кіновідгуків від оцінки «позитивний або негативний» в бік прогнозування рейтингу за 3-х або 4-х бальною шкалою. Також Снайдер провів поглиблений аналіз оглядів ресторанів, пророкуючи рейтинги їх різних властивостей, таких як їжа і атмосфера (за 5-бальною шкалою).

Системи шкалювання. Іншим методом визначення тональності є використання систем шкалювання, за допомогою чого словами, зазвичай пов'язаних з негативними, нейтральними або позитивними тональностями, ставляться відповідно числа за шкалою від -10 до 10 (від негативного до самого позитивного). Спочатку фрагмент неструктурованого тексту досліджується з допомогою інструментів та алгоритмів обробки природної мови, а потім виділені з цього тексту об'єкти та терміни аналізуються з метою розуміння значення цих слів.

Висновки. В ході аналізу було розглянуто 3 групи методів аналізу соціальних мереж, досліджено їх можливості і сфери застосування. Перспективним напрямком подальших досліджень вбачається поєднання існуючих методів аналізу соціальних мереж для розробки програмного забезпечення системи соціологічних досліджень, результати яких можна використати в маркетингу.

Список використаних джерел

1. *Nair, P. S. Data Mining Through Fuzzy Social Network Analysis [Electronic resource] / P. S. Nair, S. T. Sarasamma // NAFIPS 2007 — 2007 Annual Meeting of the North American Fuzzy Information Processing Society. — Institute of Electrical & Electronics Engineers (IEEE), 2007. — Available at: \www/ URL: http://doi.org/10.1109/nafips.2007.383846*
2. *Newman, Girvan "Finding and evaluating community structure in networks", 2004*
3. *Антон Коршунов. Задачи и методы определения атрибутов пользователей социальных сетей // Труды 15-й Всероссийской научной конференции «Электронные библиотеки: перспективные методы и технологии, электронные коллекции» - RCDL'2013*
4. *Анализ контента социальных медиа в эпоху больших данных [Електронний ресурс] – Режим доступу: https://mebius.io/analysis/social-media-content-analysis (дата обращения: 25.08.2016).*

УДК 004.056.55

Леонтьєв В. С., Неласа Г. В.
Запорізький національний технічний університет

Аналіз методів спарювання точок еліптичних кривих

На теперішній час криптографічні методи знайшли широке застосування в практичній інформатиці для вирішення проблем інформаційної безпеки. Сучасна криптографія нараховує ряд проблем:

– обмежена кількість робочих моделей;

– постійне збільшення обсягу переданих блоків даних і ключів, обумовлене інноваціями в обчислювальної техніки та розвитком математичного апарату;

– потенційна ненадійність загально прийнятої криптографії;

– відсутність перспективи.

В результаті для сучасної криптографії стала актуальною задача підвищення криптостійкості і зменшення обсягу переданих блоків даних шляхом зміни вже існуючих криптосистем. Виходом з цієї ситуації став відносно молодий розділ науки - еліптична криптографія.

При роботі з еліптичними кривими корисним інструментом являється спарювання точок кривої. Криптографія на основі спарювання точок протягом останнього десятиліття почала активно використовуватися для різних криптосистем та обміну ключами. Це алгебраїчне налаштування має гарну функціональність та ефектність. Виграшем застосування спарювання є зменшення числа інформаційних обмінів по мережі.

Еліптична крива з невеликим ступенем вкладу та великою підгрупою головного порядку називається еліптичною кривою, яка підходить для спарювання (pairing-friendly elliptic curve). Основними з них являються MNT, BN, CP, KSS та BLS.

Загалом існує 4 типи спарювань але для реалізації криптографічних протоколів використовують лише спарювання типу 1 та 3. Тип 1 зазвичай називають симетричним. Його структура легша та дорожча в реалізації, ніж спарювання інших типів. Водночас спарювання 3 типу називають асиметричним. Як правило, є найбільш вигідним вибором для реалізації з точки зору пропускної здатності та часу обчислення.

За допомогою бібліотеки MIRACL, яка написана на C/C++, був проведений аналіз спарювання точок на еліптичній кривій. Метою аналізу було визначення оптимального спарювання, серед відомих спарювань Вейля, Тейта, ηT та Ейта. Також експеримент проводився на різних кривих зазначених вище.

Спарювання типу 1 можуть бути реалізовані лише для 80-ти та 128-ми біт захищеності, коли 3 тип реалізований на 80, 128, 192 та 256.

BN криві зі спарюванням Ейта показали найшвидший результат на рівні 192 біт безпеки.

Список використаних джерел

1. *Craig Costello, Pairings for beginners. USA, 2012. – 138c. [Електронний ресурс]: www.craigcostello.com.au/pairings/PairingsForBeginners.pdf*
2. *D. Freeman, M. Scott, E. Teske, A taxonomy of pairing-friendly elliptic curves [Електронний ресурс]: https://eprint.iacr.org/2006/372.pdf*
3. *Венбо Мао, Современная криптография: теория и практика: Переклад з англ.- М. : Издательский дом Вильямс, 2005. -768с.*

УДК 621.396:534

Майборода О. П.
Харківський національний університет радіоелектроніки

Демаскуючі ознаки GSM і CDMA радіоакустичних закладних пристроїв

Закладний пристрій – потай встановлюваний технічний засіб, який створює загрозу для інформації [1]. Закладні пристрої можуть працювати на частотах GSM і CDMA стандарту зв’язку.

GSM — міжнародний стандарт для мобільного цифрового стільникового зв'язку з розділенням каналу за принципом TDMA та високим рівнем безпеки за рахунок шифрування з відкритим ключем [2].

Радіоакустичні закладні пристрої працюють на частотах GSM і CDMA (GSM і CDMA закладки) стандарту є вдосконаленням радіоакустичних закладних пристроїв, де замість відкритого радіоканалу використовується стандарти GSM і CDMA. Використання GSM і CDMA зв'язку в закладних пристроях вирішило основну проблему радіоакустичних закладних пристроїв - дальність дії закладного пристрою. Ці закладні пристрої використовують звичайну стільниковий зв'язок стандарту GSM / CDMA як канал передачі інформації за рахунок цього дальність здійснення прослуховування не обмежена. Зазвичай при роботі від акумулятору GSM закладний пристрій працює в режимі очікування 10-15 днів, а в режимі прослуховування 6-8 годин[3].У деяких моделях GSM і CDMA закладки закладні пристрої використовується стаціонарне живлення від мережі, що дає не тільки безмежну дальність, але і не обмежений час прослуховування, наприклад якщо камуфлювати закладний пристрій під мережевий подовжувач 220В.

Переваги GSM закладних пристроїв:

- безмежна дальність прослуховування;
- скритність роботи;
- довгий час роботи, при стаціонарному живленні від мережі.

Недоліки:

Необхідність оплати стільникового оператора за зв’язок.

Також можливо використання у радіоакустичних закладних пристроях CDMA частот, а саме використовуються діапазон 824-894 МГц.

CDMA - стандарт безпровідного зв'язку с множинним доступом з кодовим поділом каналів [2].

Переваги CDMA закладних пристроїв:

більша скритність, відносно GSM закладних пристроїв, завдяки меншої амплітуди сигналу у смузі частот;

CDMA діапазон менш популярний, тому менша ймовірність пошуку закладного пристрою у цьому діапазоні частот, відносно GSM закладних пристроїв;

CDMA закладні пристрої більш автономні, через меншу витрату енергію від джерела живлення.

Недоліки:

- значно дорожчий зв'язок та більш дорожче обладнання, відносно GSM закладних пристроїв.

Зазвичай при роботі від акумулятору CDMA закладний пристрій працює в режимі очікування 20-25 днів, а в режимі прослуховування 10-12 годин [3].

Демаскуючі ознаки GSM/CDMA радіоакустичних закладних пристроїв поділяються на демаскуючі ознаки зовнішнього вигляду і сигнальні демаскуючі ознаки.

До демаскуючи ознак зовнішнього вигляду відносяться:

1. Одне або кілька отворів малого діаметра в корпусі малогабаритного предмета невідомого призначення (бо без доступу до повітря неможлива робота мікрофону);
2. Тонкий дріт виходячий з пристрою невідомого призначення;
3. Наявність автономних джерел живлення (акумуляторних батарей).

До сигнальних демаскуючих ознак відносяться [5]:

1. Підвищений рівень електромагнітного випромінювання поблизу місця розташування радіоакустичного закладного пристрою порівняно з фоновим рівнем;

2. Кореляційний зв'язок між акустичними сигналами, що циркулюють у контрольованому приміщенні, і демодульованим високочастотним коливанням на частоті небезпечного сигналу;

3. Функційна залежність рівня електромагнітних коливань у точці, яка знаходиться в ближній зоні від відстані до радіоакустичного закладного пристрою (обернено пропорційна квадрату відстані).

4. Особливу увагу потрібно приділяти частотним діапазонам [4]: 935 – 960 МГц (GSM 900), 824-894 МГц (CDMA), 1805 – 1880 МГц (GSM 1800), 2110 – 2175 МГц (3G), 1810 – 1890 МГц (4G), 2620 – 2690 МГц (4G).

Методика виявлення GSM/CDMA радіоакустичних закладних пристроїв активованих голосом за допомогою аналізатора спектра:

З приміщення виносяться всі мобільні телефони, GSM/CDMA модеми, вимикаються GSM охоронні пристрої.

Вмикається тестовий акустичний сигнал, для активації закладного пристрою (сигнал «підзвучки»).

За допомогою портативного аналізатора спектру досліджуються частотні діапазони вказані в сигнальних демаскуючих ознаках у пункті 4.

Пошук GSM/CDMA радіоакустичних закладних пристроїв здійснюється шляхом послідовного обходу приміщення, рухаючись вздовж стін і обходячи меблі і предмети, що знаходяться в приміщенні, при цьому антену необхідно орієнтувати в різних площинах, домагаючись максимального рівня сигналу.

При наближенні до GSM/CDMA радіоакустичного закладного пристрою збільшується рівень амплітуди сигналу. Подальше визначення радіоакустичного закладного пристрою визначається по максимальному рівню амплітуди сигналу.

Виявлення GSM/CDMA радіоакустичного закладного пристрою здійснюється шляхом візуального огляду підозрілих місць і предметів.

Список використаних джерел

1. *ДСТУ 3396. 2−97 «Захист інформації. Технічний захист інформації. Терміни та визначення». [Текст] - Введ. 1997-01-07.*
2. *ДСТУ ETSI EN 301 511:2016 «Обладнання систем цифрового стільникового радіозв`язку GSM абонентське. Технічні вимоги та методи випробування». [Текст] - Введ. 2016-12-30.*
3. *GSM и CDMA закладки [Електронний ресурс]. – Режим доступа :* http://radioskot.ru/publ/peredatchiki/gsm_zhuchok/11-1-0-583 *15.11.2018*
4. *Частотные диапазоны операторов связи Украины [Електронний ресурс]. – Режим доступа :* http://3g-aerial.biz/chastoty/chastotnye-diapazony-operatorov-svyazi-ukrainy *15.11.2018*
5. *Олейніков А.М. Методи та засоби захисту інформації – Навчальний посібник для студентів вищих навчальних закладів [Текст] -Харків: НТМТ, 2014 – 298 с.*

УДК 004.056

Нєдєльський Д. С.[*]
Центральноукраїнський національний технічний університет

Інформаційні війни в соціальних мережах

На сучасному етапі розвитку суспільства також зростає роль інформаційної сфери, що є важливим фактором суспільної, соціальної, політичної та військової діяльності держави. Це зумовлено тим, що з одного боку продовжується науково-технічна революція в області обчислювальної техніки та зв'язку, а з іншого - в умовах реалізації конституційних прав громадян на свободу економічної, інформаційної та інтелектуальної діяльності розширюється потреба соціально активної частини населення в розширенні інформаційної взаємодії як всередині держави, так і за її межами. В свою чергу, геополітична взаємодія світового співтовариства здійснюється сьогодні, перш за все, в рамках інформаційно-психологічного простору. Це породжує значну кількість проблем, ключовою серед яких є використання даного простору для проведення операцій інформаційно-психологічної війни.

Досить часто в наш час піднімається питання про інформаційні війни в соціальних мережах, засобами яких противник розповсюджує неправдиву інформацію про ті чи інші події в суспільстві чи державі. Інтернет - простір заповнений величезною кількістю інформації, достовірність якої просто неможливо перевірити, що робить всю аудиторію інтернету найбільш вразливою до різного роду маніпулювання. Можна сказати, що кіберпростір став справжнім полем інформаційних війн, які ведуть між собою різні держави, політичні та економічні групи, релігійні та етнічні спільноти за уми і душі людей. В інформаційних війнах в соціальних мережах використовуються ті ж самі методи, які характерні для різних форм маніпуляції свідомістю. В першу чергу, це замовчування або приховування важливої інформації. Для соціальних мереж таке замовчування надзвичайно складне, так як соціальні мережі завжди відкриті для повідомлень і коментарів, але тут вступають в роботу модератори які всіма силами намагаються знайти невигідну інформацію, видалити її, не дати користувачу створити публікацію.

Не так давно українські сили боротьби з інформаційною війною прийняли рішення про блокування російських соціальних мереж на території України, тому що в російських соціальних мережах було зафіксовано велику кількість пропаганди та недостовірної інформації про хід та особливості ведення бойових дій на території України а також про ситуацію в країні в цілому. Оприлюднювалися світлини ворожих позицій, недостовірна інформація про кількість обстрілів та напрям пострілів та інше. Інформація такого роду досить швидко здатна нанести психологічного удару громадянам країни та суспільству в цілому, що може призвести до небажаних, навіть катастрофічних наслідків.На сьогоднішній день російські користувачі досить часто публікують пропагандистську інформацію в соціальних мережах, таких як Одноклассники, Вконтакті та Фейсбук. Особливо у великих кількостях зустрічається пропаганда у публікаціях в групах соціальної мережі Вконтакті. Така ситуація, що склалася на сьогодні на теренах онлайнових масмедіа та соціальних мереж вимагає пильної уваги з боку держави з метою розробки ефективних методів боротьби з деструктивними інформаційними впливами.

Список використаних джерел

1. Сергеев И.В. Социальные сети в Интернете как средство реализации операций информационной войны [Електронний ресурс]. – Режим доступу: – http://vernsky.ru/pubs/6820/view_mode=text

2. Політолог [Електронний ресурс]. – Режим доступу: – http://politolog.net/analytics/informacionnaya-vojna-v-socialnyx-setyax-bloger/

3. Могилевская Г.И. Информационная война в социальных сетях//Молодой ученый.-2015.-№15.-С. 650-654.

[*] Науковий керівник – Гермак В. С., викладач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету

УДК 004.056.5

Петров М. В.
ДВНЗ «Криворізький національний університет»

Дослідження технології блокчейн, криптографії та крипто валют

Блокчейн - це багатофункціональна і багаторівнева інформаційна технологія, призначена для надійного обліку різних активів. Потенційно ця технологія охоплює всі без винятку сфери економічної діяльності і має безліч областей застосування. У їх числі: фінанси, економіка і грошові розрахунки, а також операції з матеріальними (реальна власність, нерухомість, автомобілі та т. п.) І нематеріальними (права голосування, ідеї, репутація, наміри, медичні дані, особиста інформація і т . п.) активами. Блокчейн створює нові можливості з пошуку, організації, оцінки та передачі будь-яких дискретних одиниць. По суті, це нова організаційна парадигма для координації будь-якого виду людської діяльності.

Цілком ймовірно, ми знаходимося на порозі блокчейн-революції. Ця революція почалась з появою нової економічної реальності в інтернеті - альтернативна валюта під назвою біткойн, що емітується і забезпечується не державою, а користувачами біткойн-мережі при автоматизованому досягненні консенсусу між ними. Але унікальність цієї валюти полягає в тому, що її користувачам не обов'язково довіряти один одному. Вбудовані в систему алгоритми саморегулювання запобігають будь-які зловмисні спроби обману. Якщо бути точним, то з технічної точки зору біткойн - це цифрові гроші, які звертаються в децентралізованої електронної платіжної системи.

Технологія блокчейн інноваційна завдяки своїй високій надійності яка досягається за допомогою технології обчислювальної гонки. Блокчейн має всі шанси суттєво змінити не лише банківську, але і багато інших систем. Наприклад, змінити варіанти дій між корпораціями - вже без регулюючих посередників. В основному, такому перетворенню заважають недовіра до незвичної технології та відсутність можливості реалізації в промисловості. За кілька років стане остаточно зрозумілі можливості і ефективність блокчейнів, але їх перспективи видно і зараз.

Заклопотаність розвитком даної технології висловлюють уряди багатьох країн - адже за задумом при використанні криптовалюти відпадає необхідність користуватися послугами посередників (банку або регулятора) у взаєминах продавець-покупець.. Оптимісти припускають, що платформа Ethereum допоможе створити держбюджети з відкритими для звичайних людей витратами і доходами і звільнити структури від корупції і грошових махінацій.

Технологія блокчейну дає захист для найважливіших аспектів життя людини, що також дозволяє додати інші важливі аспекти життя людини до інформаційного поля.

Один із актуальних для України прикладів — реєстр права власності. Якщо його побудувати із залученням публічного blockchain, отримаємо найстійкіший цифровий реєстр планети при низькій вартості реалізації. Більше того — для забезпечення цілісності реєстру це є безальтернативним технічним рішенням. Це рішення доступне будь-кому і практично нічого не коштуватиме. І це — в той час як корпорації та держави вкидають мільярдні бюджети на забезпечення цілісності даних різного рівня.

Блокчейн дозволить додати в інформаційне поле та автоматизувати найважливіші сфери життя людини та покращити життя всіх людей на планеті.

У ході наукової роботи буде дослідження блокчейн технологія та принцип її роботи. Це дасть змогу більш широко визначитись с актуальністю технології та можливими сферами застосування. На базі отриманих знань планується розробити на реалізувати конкурентоспроможний проект на базі цієї технології.

Список використаних джерел

1. *Гєнкін А. Блокчейн. Как это работает и что ждет нас завтра / А. Гєнкін, О. Міхаєв., 2017. – (Альпина Паблишер).*
2. *Swan M. Blockchain: Blueprint for a New Economy / Melanie Swan. // Олимп-Бизнес. – 2015. – С. 240.*
3. *Franco P. The Blockchain // Understanding Bitcoin: Cryptography, Engineering and Economics / Pedro Franco. // John Wiley & Sons. – 2014. – С. 1–10.*

УДК 004.056

Прокопов В. В.
Центральноукраїнський національний технічний університет

Нормативно-правові засади протидії маніпуляціям суспільною свідомістю і поширенню спотвореної інформації в Україні

Маніпуляція думкою мас, її направлення у необхідне певній особі чи колу осіб русло є явищем не новим, але у XXI ст. з розвитком засобів комунікації та обміну та поширення інформації (газет, телебачення, інтернету) воно досягло такого масштабу, що можна казати про війни інформаційного століття, які можуть вестися за засоби обробки і породження знань та інформації. Як зазначив президент корпорації SONY в США Г. Стінгер, «кожен будинок стає полем битви».

У роботі під маніпуляцією масовою свідомістю розуміється один із способів управління великою кількістю людей (колективами, спільнотами) шляхом створення ілюзій і умов для управління поведінкою. Це дія направлена на психічні структури людини, здійснюється потай і ставить своїм завданням встановити контроль над поведінкою, позбавити свободи вибору об'єкт маніпуляції за допомогою зміни уявлень, думок, спонукань і цілей людей в потрібному певної групи напрямку. Маніпуляція масовою свідомістю служить ключовим елементом психологічних операцій і інформаційної війни [1].

Значну роль у процесі маніпуляції масовою свідомістю, на даному етапі розвитку інформаційних технологій, відіграють ЗМІ та інтернет. Будучи призвані для інформування населення, соціалізації, формування позитивних цінносних орієнтирів ЗМІ в першу чергу займаються створенням масової інформації – інформації для мас людей, яка забезпечує поирення певних стандартів поведінки, контролюючих і трансформують внутрішній, духовний світ людини; вказує людям, що є поганим, а що хорошим; звужує світогляд та нівелює суверенність та незалежність в судженнях до такого степення, щоб в подальшому масовий споживач сприймав інформацію без її критичної оцінки та аналізу.

Проблема пов'язана з створенням методів і засобів протидії маніпуляціям суспільною свідомістю і поширенню спотвореної інформації стоїть особливо гостро через розпочату війну Російської Федерації проти України, яка включає в себе не тільки бойові дії, а й чинить інформаційний вплив на інформаційний простір України. Тож зокрема виникає потреба у захисті від цих негативних інформаційних впливів, які йдуть ззовні, виявлення і усуненя їх можливих внутрішніх джерел, боротьба з пропагандою та припинення поширення дезінформації, розробка захисних та профілактичних методів та засобів.

Відносини у сфері протидії маніпулювання суспільною свідомістю та поширенню спотвореної інформації регулюються наступними нормативно-правовими актами: рішення РНБО “Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України”; Доктрина інформаційної безпеки України; указ Президента України про рішення Ради національної безпеки і оборони України від 26 січня 2018 року "Про додаткові заходи щодо протидії інформаційній агресії Російської Федерації"; цивільний кодекс України (стаття 277); закон України “Про інформаційні агентства” (статті 33 та 34); закон України “Про телебачення і радіомовлення” (стаття 42).

Аналіз нормативно-правової бази показав її ефективність та компетентність у протидії маніпуляції суспільною свідомістю та поширенню спотвореної інформації. Зокрема особливо ефективними є Доктрина інформаційної безпеки України та закон

України "Про телебачення і радіомовлення". Протистояння загрозам, визначеним у Доктрині, дотримання пріоритетів державної політики в інформаційній сфері належно та відповідним чином виконується відповідними відомствами, на які були покладені зобовязання щодо реалізації положень Доктрини. У минулі роки було проведено тотальну перевірку іноземних програм щодо дотримання ними вимог Європейської конвенції про транскордонне телебачення і українського законодавства та припинено ретрансляцію 80 іноземних програм, то 2017 року із переліку дозволених до ретрансляції програм вилучено лише 4 іноземні мовники, у яких раніше таких порушень не фіксувалося (двоє з них зареєстровані у Російській Федерації, і по одному – в Латвії й Естонії). Таким чином на підставі Закону України "Про телебачення і радіомовлення" стаття 42 (ретрансляція телерадіопрограм та передач), покладено край поширенню в українських кабельних мережах інформації іноземних телеканалів, спрямованої на дискредитацію країни, розхитування її засадничих принципів, послаблення української ідентичності та розпалювання міжнаціональної ворожнечі [1]. Співробітники СБУ заблокували нові спроби кремлівських пропагандистів популяризувати в Інтернеті так звану «Житомирську народну республіку» [2]. У зоні проведення ООС на сході України розпочала роботу система протидії російській інформаційній агресії. Система блокує аналогові, цифрові, телевізійні сигнали, які надходять з непідконтрольних територій Донецької і Луганської областей, зокрема, блокується понад 40 каналів російського і сепаратистського телебачення [3].

Щодо вдосконалення нормативно-правових документів та наявної практики регулювання суспільних відносин у сферы протидії маніпуляціям суспільною свідомістю і поширенню спотвореної інформації можна запропонувати наступне: внести зміни до розділу шостого Доктрини інформаційної безпеки України: створення спеціального державного органу, який би займався моніторингом одразу усіх можливих векторів впливу на людську свідомість (телебачення, радіо, інтернет, газети), та запровадження відповідної нормативно-правової бази з визначенням відповідних повноважень та компетенції, дозволило б зібрати чи підготувати спеціалістів та експертів, які б займалися: моніторингом ЗМІ, як вітчизняних так й іноземних, інтернет; у разі виявлення ознак спроб пропаганди, маніпуляції, поширення спотвореної інформації вчиняли відповідні дії щодо усунення їх джерела та наслідків; створенням технічних та програмних засобів протидії негативним інформаційним впливам; поліпшення медійної грамотності населення; перевірка робітників ЗМІ; виявлення недостовірних та спотворених новин, сповіщення про це і висвітлення достовірної інформації щодо події, що відбулися. Також зобов'язати громадські організації зайнятися підвищенням рівня обізнаності населення з питань виявлення маніпуляторів, ознайомлення із основними способами протидії маніпуляціям та принципами та прийомами за допомогою яких ЗМІ змінює, форматує та спотворює інформацію.

Список використаних джерел

1. *Маніпулювання масовою свідмістю [Електронний ресурс] : [Веб-сайт]. –Режим доступу: https://uk.wikipedia.org/wiki. (дата звернення 01.10.2018). – Назва з екрана.*
2. *Звіти Національної ради [Електронний ресурс] : [Веб-сайт]. – Режим доступу: https://www.nrada.gov.ua/reports/ (дата звернення 20.10.2018 р.). – Назва з екрана.*
3. *СБУ заблокувала фейкову спробу популяризації так званої «Житомирської народної республіки» [Електронний ресурс] : [Веб-сайт]. – Режим доступу: https://www.ssu.gov.ua/ua/news/1/category /2/view/4522#.8h1FskDj.dpbs. (дата звернення 01.10.2018). – Назва з екрана.*
4. *У зоні АТО почали блокувати російський телесигнал [Електронний ресурс] : [Веб-сайт]. –Режим доступу: https://detector.media/infospace/article/136792/2018-04-19-u-zoni-ato-pochali-blokuvati-rosiiskii-telesignal/. (дата звернення 01.10.2018). – Назва з екрана.*

УДК 004.056.5

Савченко О.О.
Харківський національний університет імені В. Н. Каразіна

Специфічні властивості скручених кривих Едвардса для криптографічних додатків

Асиметричні криптосистеми на еліптичних кривих понад десятиріччя успішно використовуються на основі дійсних національних і міжнародних стандартів. Пошуки більш досконалих алгоритмів останніми роками привели до альтернативи канонічної форми кривих – кривих у формі Едвардса [1]. Їх головні переваги: рекордна продуктивність і простота групових операцій та програмування.

Автори робіт [1,2] вперше визначили криві Едвардса до тієї форми, яка зробила їх вельми перспективними для завдань сучасної асиметричної криптографії. Введення другого параметра кривої в роботі [2] розширює клас кривих Едвардса і ставить питання: наскільки це може виявитися корисним для криптографічних додатків? Далі це питання обговорюється.

Обгрунтування нової класифікації кривих в узагальненій формі Едвардса дано в роботах [3,4]. Тут дано визначення 3-х класів цих кривих і перелік фундаментальних властивостей кривих різних класів.

Залежно від властивостей параметрів A і D криві в узагальненій формі Едвардса розбиваються на 3 непересічні класу ізоморфізмів:

- повні криві Едвардса (з умовою C1:$\left(\frac{ad}{p}\right) = -1$;
- скручені криві Едвардса (з умовами C2.1: $\left(\frac{a}{p}\right) = -1$. $\left(\frac{d}{p}\right) = -1$;
- квадратичні криві Едвардса (з умовами C2.2: $\left(\frac{a}{p}\right) = 1$. $\left(\frac{d}{p}\right) = 1$.).

Основні властивості цих класів кривих::

1) Щодо точок 2-го порядку перший клас повних кривих Едвардса над простим полем є класом циклічних кривих, скручені ж і квадратичні криві Едвардса утворюють класи нециклічних кривих. Максимальний порядок точок кривих останніх класів дорівнює N_E /2.

2) Клас повних кривих Едвардса не містить особливих точок.

3) Скручені криві Едвардса містять лише дві особливі точки 2-го порядку $D_{1,2} = \left(\pm\sqrt{\frac{a}{d}}, \infty\right)$.

4) Квадратичні криві Едвардса містять дві особливі точки 2-го порядку $D_{1,2} = \left(\pm\sqrt{\frac{a}{d}}, \infty\right)$ и дві особливих точки 4-го порядку $\pm F_1 = \left(\infty, \pm\frac{1}{\sqrt{d}}\right)$.

5) Скручені і квадратичні криві Едвардса утворюють пари квадратичного кручення на основі перетворення параметрів: $a' = ca, d' = cd, \left(\frac{c}{p}\right) = -1$.

6) Повні і квадратичні криві Едвардса ізоморфні кривим з параметром $a = 1$: $E_{a,d} \sim E_{1,d/a}$. Введення нового параметра *a* в рівняння кривої виправдано лише для класу скручених кривих Едвардса.

7) Для точок непарного порядку закон додавання точок є повним (тобто сума будь-якої пари точок не дає особливої точки).

Для криптографічних додатків слід шукати криві Едвардса порядку $N_E = 4n$ с мінімальним кофактором 4 при непарному n, з яких відбираються криві з простим n.

Серед повних кривих Едвардса (умова С. 1) практично половина мають порядок 4n (n – непарне). Вони є циклічними, і їх порядки пробігають всі кратні 4-м числа в межах Хассе. Квадратичні криві Едвардса з параметром $\left(\frac{d}{p}\right) = 1$ (умова 2) є нециклічними з трьома точками 2-го порядку і чотирма або вісьмома точками 4-го порядку (в останньому випадку згідно з теоремою 1 $p \equiv 1 mod 4$). Звідси випливає, що вони містять нециклічну підгрупу, ізоморфну Z/2 × Z/4 близько 8, а порядок цих кривих має мінімальний кофактор 8. Вони найменш привабливі для криптографії. Тому криві порядку $N_E = 4n$ поряд з повними кривими Едвардса можна шукати лише серед скручених кривих в умовах С.2.1.

Згідно з твердженням 1, при $p \equiv 1 \bmod 4$ всі скручені криві Едвардса мають порядок $N_E = 4n$. Це перше унікальне властивість скручених кривих, що зводить пошук криптостійких кривих до пошуку кривих з майже простим порядком 4n (n – просте) за умови $p \equiv 1 \bmod 4$.

Генератор криптосистеми вибирається як точка G простого порядка n ($\mathrm{Ord} G = n$). Так як практично будь-яка випадкова точка P нециклічної скрученої кривої має порядок n або 2n, генератор криптосистеми легко знаходиться простим подвоєнням випадкової точки: G = 2P. Це друге унікальне властивість скручених кривих Едвардса, корисне на етапі обчислення загальносистемних параметрів. Наявність двох особливих точок 2-го порядку $D_{1,2} = \left(\pm\sqrt{\frac{a}{d}}, \infty\right)$ на скрученій кривій не є підставою для відмови від їх впровадження в стандарти асиметричної криптографії. Ці точки лежать за межами підгрупи точок < G > простого порядку n, з якими оперує криптосистема. Згідно властивості 2.7, для точок цієї підгрупи закон додавання (2) точок повний.

Таким чином, вибираючи мінімальне значення параметра $a \in \{2,3\}$ як квадратичного невирахування , можна досягти, як і для повних кривих, максимальної продуктивності імплементації крипто алгоритмів. Криві Едвардса з одним параметром, що визначені в роботі [1], мають дуже привабливі для криптографії переваги: максимальна швидкість експоненціювання точки [3], повнота і універсальність закону додавання точок, афінні координати нейтрального елемента групи точок [1]. Програмування групових операцій стає більш ефективним і прискорюється у зв'язку з відсутністю особливої точки на нескінченності як нуля групи.

Список використаних джерел

1. *Bernstein D.J., Lange T. Faster Addition and Doubling on Elliptic Curves // Advances in Cryptology—ASIACRYPT'2007 (Proc. 13th Int. Conf. on the Theory and Application of Cryptology and Information Security. Kuching, Malaysia. December 2–6, 2007). Lect. Notes Comp. Sci. V. 4833. Berlin: Springer, 2007. P. 29–50.*
2. *Bernstein Daniel J. , Birkner Peter , Joye Marc , Lange Tanja, Peters Christiane. Twisted Edwards Curves.// IST Programme under Contract IST–2002–507932 ECRYPT,and in part by the National Science Foundation under grant ITR–0716498, 2008, PP. 1-17.*
3. *Бессалов А.В. Эллиптические кривые в форме Эдвардса и криптография. Монография. «Политехника», Киев, 2017. - 272с.*
4. *Бессалов А.В., Цыганкова О.В. Число кривых в обобщенной форме Эдвардса с минимальным четным кофактором порядка кривой . Проблемы передачи информации, - Том 53 (1), 2017. С.101-111.*
5. *Бессалов А.В., Цыганкова О.В. Взаимосвязь семейств точек больших порядков кривой Эдвардса над простым полем. Проблемы передачи информации, - Том 51, вып 4, 2015. С.92-98.*
6. *Бессалов А.В. Метод нахождения порядка точки скрученной кривой Эдвардса. Радиотехника, №.186, 2016. – С.110-118.*

УДК 004.056.5

Трухачов А. В., Козіна Г. Л.
Запорізький національний технічний університет

Аналіз захищеності ідентифікації клієнта у системі Біткоін

Біткоін – це пірингова платіжна система, яка була створена у січні 2009 року. Біткоін на сьогоднішній день є однією з найбільш розповсюджених систем цифрових валют. Система Біткоін, як і інші криптовалюти, має суперечливий правовий статус у багатьох країнах. Складність правового регулювання криптовалют пов'язана з неможливістю їх класифікації по існуючим правовим документам, оскільки криптовалюта не існує у вигляді грошових коштів, банкнот, монет, записів на банківських рахунках. В Україні статус криптовалют зараз законодавчо не врегульований.

Володіння біткоінами встановлюється через секретні і відкриті ключі та Біткоін-адреси.

Секретні ключі використовуються при генерації відкритих ключів, а також для створення цифрового підпису, необхідного для підтвердження факту володіння біткоінами. Відкриті ключі використовуються у процесі формування Біткоін-адреси, а також для перевірки достовірності цифрового підпису.

Біткоін-адреси використовуються для ідентифікації користувача в системі Біткоін.

Секретний ключ d являє собою випадкове число, обране в межах від 2 до $n-1$, де $n = 1.158 \cdot 10^{77}$. Число n відповідає порядку базової точки G (константа, визначена в стандарті ECDSA secp256k1) еліптичної кривої $y^2 = x^3 + 7 \bmod p$, де $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$.

Відкритий ключ Q обчислюється з секретного ключа d за допомогою незворотного множення на еліптичних кривих: $Q = d \cdot G$. Криптостійкість даного перетворення заснована на задачі дискретного логарифмування в групі точок еліптичної кривої.

Біткоін-адреса формується з відкритого ключа шляхом використання односторонньої криптографічної операції хешування. Відкритий ключ перетворюється за допомогою алгоритму SHA-256. Отриманий результат хешується повторно алгоритмом RIPEMD160. Останнім етапом формування Біткоін-адреси є кодування хешу відкритого ключа у формат Base58Check.

Однією з проблем захищеності ідентифікації клієнта у системі Біткоін є можливість вибору однакових секретних ключів, і, як наслідок, генерації однакових відкритих ключів та Біткоін-адрес. Імовірність випадкового вибору однакових секретних ключів дуже мала і складає приблизно $8.23 \cdot 10^{-68}$. На даний момент система Біткоін ніяк не реагує на виникнення колізій секретних ключів.

Використання хеш-функцій при формуванні Біткоін-адреси також створює загрозу виникнення колізій, що призводить до генерації однакових Біткоін-адрес. Криптографічна стійкість хеш-функцій до знаходження колізій другого роду достатньо велика – приблизно 2^{128} та 2^{80} для алгоритмів SHA256 та RIPEMD160 відповідно. Незважаючи на це, імовірність виникнення колізій Біткоін-адрес існує і її необхідно враховувати.

Відсутність обов'язкових механізмів перевірки унікальності секретних ключів та Біткоін-адрес у децентралізованої системі, що використається в Біткоін, значно підвищують імовірність реалізації загрози помилкової ідентифікації клієнта у цієї системі.

УДК 004.056

Шуліка Я. П.[*]
Центральноукраїнський національний технічний університет

Сучасна пропаганда як продукт інформаційного простору

Хто володіє інформацією – той володіє світом. У часи, коли з'явився цей вислів, це було набагато простіше, тому що держава практично мала монополію на інформацію. Тоді ж з'явилось поняття «офіційна версія події» або «офіційна інформація», багато хто вважає що лише така версія відповідає реальності, а неофіційні версії – вигадки. Хоча «офіційна» означає лише що вона походить від держави, це ще не означає, що вона істинна. На тому що люди вважають офіційну інформацію істинною будується пропаганда, а на тому що наявність офіційної версії не завжди передає істинну версію подій будується інформаційна війна. Кожну подію можливо обернути таким чином, щоб отримати з цього вигоду, наприклад так, щоб пропагувати потрібні ідеї, або так, щоб звинуватити у тому що сталось суперника або конкурентів.

Можна подумати, що за цим завжди стоїть хтось, кому вигідне саме таке висвітлення подій, але насправді цей процес виконується самими людьми, журналістами та інформаційними виданнями автоматично. Вони освітлюють події згідно зі своїм кругозором та тим, що зараз «актуально». Актуальна інформація для видання це така із-за якої його прочитає більша кількість людей.

Коли відбувається важлива подія, правильне освітлення якої може бути дуже вигідним, то в її освітлення може відбутися втручання. Іноді важливо скласти враження начебто більшість людей вважає саме так як вам вигідно, тобто купити так звану «громадську думку». Коли з правильним освітленням подій все ясно, є видання у яких є інвестори, то з громадською думкою все не так просто. Виникає цілий ряд запитань:

- Хто взагалі буде цим займатися?
- Скільки коштує думка окремої людини?
- Скільки коштує громадська думка?

Потрібні для формування необхідної громадської думки інструменти створені вже давно і без допомоги держави. В інтернет-маркетингу є такий розділ як orm – online reputation management, тобто менеджмент онлайн репутації, окрім того, є сервіси, у яких ви можете купити позитивну репутацію вашого продукту або ідей серед «громади», чи негативну репутацію продукту чи ідей вашого конкурента. Ціни вражають, на пострадянському просторі думка людини коштує всього лише 0,2-1 грн, в залежності від того, що від неї потребують, розміщення вже готового коментаря, чи написання власного [1]. Ціна громадської думки не буде зависокою навіть якщо вам треба схилити на свій бік мільйонну групу людей у соціальній мережі. Вам не потрібно купувати думку всіх, достатньо купити 1000-10000 коментарів, і люди будуть думати, що «більшість» вважає так, тепер це «громадська думка», і насамкінець дійсно так вважатимуть всі [2].

Такі технології надають великі можливості зловмисникам. Людина може здійснити цілу кібербулінгову кампанію іншої людини використовуючи сервіс, що є у вільному доступі. Тепер ботів у коментарях значно складніше виявити, тому що замість ботів використовують реальних людей. Навіщо люди взагалі приймають участь у подібних сервісах? Звичайна людина задля втіхи захотіла собі на сторінку 200 лайків, звичайно, платити за таке вона вважає не потрібним, тому знаходить сервіс, у якому можна ставити лайки таким же людям і отримувати спеціальну валюту, за яку можна купити лайки собі. Таким чином це звичайний зрозумілий обмін, 200 лайків від мене, 200 лайків мені. Окрім того, можна отримати в 2,5 разів більше спеціальної валюти за

[*] Науковий керівник – Гермак В. С., викладач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету

коментарі, та ще більше за те що підписався на людину та інше. З часом у людини з'являється нове фото на якому теж хочеться щоб були лайки, а ще краще і коментарі! Таким чином у подібних сервісів будується велика база виконавців.

Є сервіси, що спеціалізуються на певних платформах, наприклад лише інстаграм, а є мультиплатформенні сервіси, де можна за дії наприклад у фейсбуці отримувати коментарі на іншому сайті. Зазвичай сервіс реалізує систему так, щоб обмін не йшов 1 до 1, тобто, наприклад, за 200 лайків що ви поставили ви отримаєте 180 лайків на свою сторінку, отже рано чи пізно комусь потрібно буде купити цю валюту за реальні гроші і сервіс продовжує існувати [1]. Такі сервіси функціонують і на рівні компаній. Таким клієнтам потрібні об'єми, які практично неможливо отримати безплатно, вони дають реальні гроші, для них навіть дають знижки, за оптову закупівлю. Дуже важко знайти взагалі бренд чи знаменитість які не користувалася б такими видами послуг. Для них дуже важлива репутація та популярність, тому що звичайна людина, наприклад, не буде купувати телефон від маловідомої фірми, на який є негативні відгуки, навіть якщо негативні відгуки будуть схожі між собою, тобто накручені.

Якщо ж ви представляєте величезну корпорацію і вам така послуга потрібна постійно, то звертатися до таких сервісів не вигідно. Для величезної корпорації буде вигідніше розгорнути свій власний сервіс або створити звичайний smm-відділ (social media marketing), який відповідає за громадську думку та популярність бренду. На такі відділи навіть є вакансії по типу «smm-менеджер» з мінімальною зарплатою, але зручними умовами праці. Для компанії це вигідніше тим, що декілька людей постійно покращують репутацію компанії з декількох аккаунтів, а голова відділу слідкує за змінами. Коли на якомусь форумі про бренд почали погано писати, голові відділу потрібно терміново поставити завдання щодо цього форуму менеджерам, щоб в кінці кінців про бренд залишилася гарна думка. Іноді у такої компанії вже все добре, але вона не може стати №1 тому що не може обігнати найкращу компанію, тоді може прийнятись рішення щоб її smm-відділ погіршував репутацію конкурентів, у той же час інша компанія починає захищатись і можна сказати, що між ними відбувається інформаційна війна.

Навіть цілі держави можуть створювати собі такі smm-компанії, які у будь-який час можуть відстояти потрібну думку, у таких компаніях велика кількість людей та відділів, є відділи, що аналізують інформаційне поле, є відділи, що вирішують, з яким посилом, що і де потрібно коментувати, для того щоб створити потрібну громадську думку. Найвідоміша з таких компаній знаходиться у Росії у Санкт-Петербурзі, робітників цієї компанії також називають «кремлеботами». Не можна сказати, що це найкраща з подібних компанй, тому що найкраще для компанії такого типу бути невідомою для світу. Відома вона із-за постійних витоків внутрішньої інформації.[4]

У сьогоднішній час потрібно дуже скептично відноситись до будь-якої інформації у інтернеті та мати критичне мислення, щоб знаходити істину серед купи іншої інформації. У недалекому майбутньому цієї індустрії не потрібно буде наймати купу людей для того, щоб вони залишали коментарі, цим зможе займатися штучний інтелект. Вже є штучний інтелект, що може писати будь-які тексти на будь-які теми і вони виглядають як людські. Коли індустрія orm отримає потужний штучний інтелект, то штучних коментарів у інтернеті може стати більше ніж людських, а громадську думку у інформаційному просторі буде визначати той, у кого більше грошей.

Список використаних джерел

1. *Likes.FM [Електронний ресурс]. – Режим доступу: – https://likes.fm/*
2. *Online Reputation Management Services [Електронний ресурс]. – Режим доступу: – https://www.eminentseo.com/services/reputation-management/*
3. *BuzzSumo [Електронний ресурс]. – Режим доступу: – https://buzzsumo.com/*
4. *Telegram [Електронний ресурс]. – Режим доступу: – https://web.telegram.org/#/im?p=@trollfactory*

УДК 004.031

Щирова Ю. А.
Харківський національний університет радіоелектроніки

Аналіз впливу атак на традиційні системи автентифікації користувачів

В наш час, володіння інформаційними ресурсами і контроль доступу до них є важливою частиною пристрою сучасного світу. Тому, як ніколи, актуальна проблема захисту цих ресурсів і контрольованого доступу до них.

Для захисту, будь-якого виду інформації, і контролю доступу до неї, необхідно автентифікувати людину. Саме для вирішення цього завдання людство роками розробляло і впроваджувало, описані раніше, системи захисту інформації.

Існує три основних типи автентифікованої інформації:

- коли автентифікований користувач знає якусь унікальну інформацію, наприклад пароль;
- коли користувач має якийсь предмет з унікальними характеристиками або вмістом, наприклад RFID-мітка;
- коли, інформація, що потрібна для автентифікації, є невід'ємною частиною користувача, наприклад відбиток пальця і інші види біометрії.

При масовому впровадженні систем захисту інформації, виникає проблема в безпеці використання таких систем.

Традиційні системи автентифікації більш популярні в застосуванні за рахунок своєї раннього появи і звичності для користувача. І саме тому, що дані системи так популяризували, вони кожен день піддаються атакам, які, вдосконалюються і зростають у геометричній прогресії. Також недоліком цих систем є те, що автентифікаційну інформацію легко вкрасти, так як вона не є частиною людини.

Розрахунки за алгоритмом призводяться на прикладі наступних систем: багаторазовий пароль та PIN-код, магнітна картка, RFID-мітка. Найбільш популрні за статистикою атаки на ці системи – це клонування інформації, фізична крадіжка автентифікаторів, атака повнім перебором та підміна пам’яті.

Для визначення стійкості кожної системи автентифікації до представленої атаки призводиться розрахунок ймовірності атаки на традиційні системи автентифікації з урахуванням складності їх реалізації за наступним алгоритмом:

1) Оцінювання за шкалою від 1 до 9, складності реалізації обраної атаки для кожної системи окремо, де, в оцінці враховується складність підробки автентифікатора. Відповідно, чим ближче оцінка до 9, тим краща система в цьому відношенні.

2) Визначення ймовірністі реалізації атаки на систему від 0,1 до 1, де, відповідно, чим ближче значення до 1, тим вища ймовірність виконання атаки.

3) Ранжування системи за значеннями від 1 до 9, з урахуванням ймовірності та складності реалізації атак відносно системи. Даний крок необхідний для визначення оцінки рівня атаки.

4) Обчислення суми оцінки рівня атаки.

5) Нормована ймовірності атаки на традиційні системи автентифікації, ураховуючи складність реалізації атаки розраховується для кожної атаки окремо за формулою (1):

$$P_н = \frac{x_p}{s_m}, \tag{1}$$

де $P_н$ – нормована ймовірність атаки; x_p – оцінка рівня атаки кожної системи

автентифікації; S_m – сума всіх оцінок рівня атаки.

6) Значення ймовірності атаки на біометричні системи з урахуванням складності їх реалізації, розраховується за формулою (2):

$$P_{підсумкове} = \sum_{i=1}^{n} \frac{P_н}{R_n}, \quad (2)$$

де $P_{підсумкове}$ – ймовірність атаки на системи автентифікації з урахуванням складності реалізації; $P_н$ – нормована ймовірність атаки; R_n – складність реалізації атаки.

Алгоритм ураховує, що кількість атак на традиційні системи, за дією, значно більша, ніж на біометричні сенсори. Тому значення ймовірності атаки на традиційні системи автентифікації з урахуванням складності їх реалізації розраховується для кожної атаки окремо. Для отримання підсумкового значення ймовірності, у даному випадку, необхідно скласти усі розраховані значення ймовірностей атак з урахуванням їх складності реалізації, для кожної традиційної системи автентифікації за формулою 2.

Розраховані результати свідчать про те, які з систем традиційної автентифікації найбільш схильні до реалізації атак зловмисником.

Вихідні дані та результати розрахунку наведено в таблиці 1.

Таблиця 1 – Вразливість динамічних систем біометричної автентифікації до атак

Система	Атаки на традиційні системи автентифікації																
	Клонування інформації		Оцінка рівня атаки	Нормована ймовірність атаки	Фізична крадіжка автенти-фікаторів		Оцінка рівня атаки	Нормована ймовірність атаки	Атака повним перебором		Оцінка рівня атаки	Нормована ймовірність атаки	Підміна пам'яті		Оцінка рівня атаки	Нормована ймовірність атаки	Ймовірність атаки на традиційні системи автентифікації з урахуванням складності реалізації
	Складність реалізації	Ймовірність атаки			Складність реалізації	Ймовірність атаки			Складність реалізації	Ймовірність атаки			Складність реалізації	Ймовірність атаки			
Багаторазовий пароль та PIN-код	-	-	-	-	2	0,8	9	0,17	3	0,7	8	0,151	-	-	-	-	0,135
Магнітна картка	5	0,5	6	0,113	4	0,8	9	0,17	-	-	-	-	-	-	-	-	0,065
RFID - мітки	7	0,5	6	0,113	4	0,8	9	0,17	-	-	-	-	6	0,5	6	0,113	0,077
Сума оцінок ймовірності атак													53				

Таким чином, Виходячи з результатів, можна зробити висновок, що серед статичних систем біометрії найбільш схильна до успішної реалізації атак зловмисником система автентифікації за використанням багаторазового паролью та PIN - коду – 0,135.

Список використаних джерел

1. *Щирова Ю. А. Багатокритеріальний аналіз ефективності систем автентифікації користувача / Ю. А. Щирова, А. А. Астраханцев // Матеріали XXI міжнародного молодіжного форуму "Радіоелектроніка та молодь у XXI столітті" – Харків: ХНУРЕ, 2017. – С. 136 – 137.*
2. *Горелик А.Л. Методы распознавания / А.Л. Горелик, В.А. Скрипкин. – М.: Высшая школа, 1984.*
3. *Парольная аутентификация [Електронний ресурс] – Режим доступу до ресурсу: http://scicenter.online/kriptografiya/141-parolnaya-autentifikatsiya- 44766.html.*
4. *RFID-системы для различных отраслей и областей применения ID Expert. Технологии. RFID-технология [Електронний ресурс] – Режим доступу до ресурсу: http://www.idexpert.ru/technology/121/.*

УДК 004.056.5

Білоконь Д. С., Форос Г. В.
Одеський державний університет внутрішніх справ

Окремі аспекти протидії кіберзлочинності

Закони й нормативні акти виконуються тільки в тому випадку, якщо вони підкріплюються організаторською діяльністю відповідних структур, створюваних у державі, у відомствах, установах і організаціях.

Аналіз наукової літератури засвідчив, що при всій значущості теми розвитку нормативно-правової бази в галузі протидії кіберзлочинності в Україні вивчена ще не у повному обсязі. Ґрунтовному дослідження проблем протидії кіберзлочинності в нашій країні також перешкоджала відсутність статистичних показників даного виду злочинів. На сьогодні вітчизняними та зарубіжними вченими опубліковано та обговорено недостатня кількість наукових праць, що досліджують цю актуальну проблематику. Зокрема, не дістала належного висвітлення організаційних та нормативно-правові засади протидії кіберзлочинності

Деякі аспекти нормативної бази по боротьбі з кіберзлочинності вивчали та обговорювали в своїх публікаціях К. Бєляков, В. Бутузов, А. Волеводз, Д. Гавловський, В. Голубєв, В. Гуславський Д. С. Кльоцкін, М. Литвинов, Е. Рижков, В. Розовський Т. Тропина, В. Цимбалюк, О. Юхно та інші.

Сьогодні закони повинні відповідати вимогам, що пред’являються сучасним рівнем розвитку технологій. Пріоритетним напрямком є також організація взаємодії і координація зусиль правоохоронних органів, спецслужб, судової системи, забезпечення їх необхідною матеріально-технічною базою. Жодна держава сьогодні не в змозі протистояти кіберзлочинності самостійно. Нагальною є необхідність активізації міжнародної співпраці в цій сфері. Експерти впевнені: саме хакери в недалекому майбутньому стануть загрозою номер один, змістивши тероризм. Незважаючи на віртуальність злочинів, збиток вони завдають цілком справжній.

В нашій державі нормативно-правову базу правового регулювання в даній сфері складають Конституція України, Кримінальний кодекс України, Конвенція Ради Європи «Про кіберзлочинність», Закони України «Про основи національної безпеки України», «Про захист інформації в інформаційно-телекомунікаційних системах» тощо, Укази Президента України від 08 липня 2009 року № 514/2009, від 08 червня 2012 року № 389/2012, № 390/2012, інші нормативно-правові акти.

Окрему увагу треба приділити найбільш важливим міжнародним нормативно-правовим актам, які регулюють сферу протидії кіберзлочинності.

З 1985 по 1989 р. Спеціальний Комітет експертів Ради Європи з питань злочинності, пов'язаної з комп'ютерами, виробив Рекомендацію № 89, затверджену комітетом Міністрів ЄС 13.09.1989 року. Вона містить список правопорушень, рекомендований країнам - учасницям ЄС для розробки єдиної карної стратегії, пов'язаної з комп'ютерними злочинами. Також в документі відмічена необхідність досягнення міжнародного консенсусу з питань криміналізації деяких злочинів, пов'язаних з комп'ютерами. Рекомендація містить два списки злочинів - «мінімальний» і «факультативний (додатковий)». «Мінімальний» список включає діяння, які обов'язково мають бути заборонені міжнародним законодавством і підлягають

переслідуванню в судовому порядку. «Додатковий» список містить ті правопорушення, по яких досягнення міжнародної згоди представляється скрутним.

Значення Рекомендації № 89 важко переоцінити. На відміну від прийнятої більш ніж через 10 років після неї Конвенції Ради Європи про кіберзлочинність, яка досі не ратифікована рядом країн, що підписали її, цей документ зробив великий вплив на розвиток і зміну законодавства країн Європи.

У 1990 році VIII Конгрес ООН з попередження злочинності і поводження з правопорушниками ухвалив резолюцію, що закликає держави - члени ООН збільшити зусилля із боротьби з комп'ютерною злочинністю, модернізуючи національне карне законодавство, сприяти розвитку в майбутньому структури міжнародних принципів і стандартів запобігання, судового переслідування і покарання в області комп'ютерної злочинності [9]. 14 грудня 1990 року Генеральна Асамблеєю ООН ухвалила резолюцію, що закликає уряди держав - членів керуватися рішеннями, прийнятими на VIII Конгресі ООН.

У 1995 році в Ліоні (Франція) була проведена міжнародна конференція Інтерполу з комп'ютерної злочинності. Учасники конференції підкреслили, що викликає тривогу відсутність міжнародного механізму для раціонального і ефективного протистояння цьому виду злочинності. За підсумками конференції був зроблений висновок, що у більшості країн світу спостерігається усе зростаюче використання інформаційних технології в кримінальній діяльності. Це викликає необхідність постійного вивчення цього кримінального прояву, оскільки розвиток комп'ютерних технології призводить до використання цих інновацій при скоєні комп'ютерних злочинів.

Підхід Інтерполу до боротьби з кіберзлочинністю полягає в тому, щоб використовувати досвід його членів у боротьбі із злочинами у сфері інформаційних технологій шляхом функціонування робочих груп або експертних груп. Робочі групи створюються для вивчення регіонального досвіду і існують в Європі, Азії, Африці і Північній і Південній Америці.

У 1997 році міністри внутрішніх справ і міністри юстиції Великої Вісімки на зустрічі у Вашингтоні прийняли «Десять принципів боротьби з високотехнологічними злочинами», що включають, у тому числі, положення про те, що «для тих, хто зловживає інформаційними технологіями, не повинно бути ніяких» зон безпеки. Правова система повинна забезпечити захист конфіденційності, цілісності і придатності даних і систем від протиправного ушкодження і гарантувати покарання за серйозні правопорушення.

Продуктом багаторічних зусиль Ради Європи стала прийнята 23 листопада 2001 року у Будапешті Конвенція Ради Європи про кіберзлочинність. Це один з найважливіших документів, що регулюють правовідносини у сфері глобальної комп'ютерної мережі і доки єдиний документ такого рівня. Прийняття його - це своєрідна віха в історії боротьби з кіберзлочинністю. Наша країна ратифікувала цю конвенцію 7 вересня 2005 року.

Підготовка Конвенції була тривалим процесом - за чотири роки було складено 27 проектів. Завершальна версія, що містить преамбулу і чотири глави, датована 25 травня 2001 року, була представлена Європейській комісії з боротьби з кіберзлочинністю на 50-м пленарному засіданні 18-22 червня 2001 року. Перший розділ Конвенції

присвячений видам діянь, що підлягають криміналізації. Її другий розділ освітлює процесуальні аспекти боротьби з кіберзлочинністю.

Конвенція про кіберзлочинність на сьогодні є одним з базових міжнародно-правових актів у сфері права телекомунікацій, але і цей документ не позбавлений недоліків. Ще до підписання Конвенції деякі групи по захисту громадянських прав і провайдери інтернет-послуг приводили серйозні аргументи проти укладення цього договору, який на їх погляд має неясні формулювання і пред'являє провайдерам непосильні вимоги.

У число організацій, що підписали протест проти прийняття Конвенції, увійшли «Фонд Електронних Меж» (Electronic Frontier Foundation, США), міжнародна організація «Суспільство Інтернет» (Internet Society), «Організація кіберправа і кіберсвободи» (Cyber - Rights & CyberLiberties, Великобританія), «Кріптополіс» (Kriptopolis, Іспанія) і інші. У протесті відзначається, що Конвенція несе в собі загрозу для норм захисту особи, що встановилися, невиправдано розширює поліцейські функції уряду, а також знижує відповідальність держави в правоохоронній діяльності.

Дослідження питань боротьби з кіберзлочинністю показало, що орієнтація тільки на технічні засоби забезпечення інформаційної безпеки в умовах інформатизації суспільства, у тому числі профілактики боротьби з кіберзлочинами, не досягла значних успіхів. Це в значній мірі пов’язано з підвищенням рівня знань користувачів комп'ютерної та телекомунікаційної техніки.

Парадокс полягає в тому, що чим складніше стає програмне забезпечення (software), тим більш вразливими виявляються традиційні організаційні заходи і засоби інженерного та технічного захисту інформації в комп'ютерних та інформаційних системах, зокрема стосовно несанкціонованого доступу до комп’ютерів та мереж.

Ще однією проблемою порядку є і те, що з розвитком електронних засобів інформації розвиваються технічні засоби перехоплення і несанкціонованого доступу до інформації, яка передається по електронним системах зв'язку.

Найбільшу небезпеку для держави та суспільства складає міжнародна організована кіберзлочинність особливо у сфері економічних відносин в фінансових та банківських системах.

Підсумовуючи вищевикладене, стає очевидним, що задля ефективної протидії кіберзлочинності відомчих ініціатив вже недостатньо. Потрібна чітка централізована координація зусиль для забезпечення злагодженої взаємодії усіх зацікавлених суб'єктів.

Список використаних джерел

1. *Кримінальний кодекс України № 2341-III від 05.04.2001 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/2341-14*
2. *Конвенція «Про кіберзлочинність» від 23.11.2001, ратифікована Законом України «Про ратифікацію Конвенції про кіберзлочинність» від 07.09.2005 № 2824-IV [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/994_575*
3. *Гуцалюк М. Протидія комп'ютерній злочинності [Електронний ресурс]. – Режим доступу: http://pravoznavec.com.ua/period/article/983/%C3*
4. *Протидія кіберзлочинності в Україні: правові та організаційні засади : навч. посіб. / [О. Є. Користін, В. М. Бутузов, В. В. Василевич та ін.]. – К. : Видавничий дім «Скіф», 2012. – 728 с.*

УДК 004.056:343.982.323

Вакулинська А. Є.
Харківський національний університет радіоелектроніки

Методи біометричної автентифікації

Біометричні методи автентифікації - методи автентифікації, які використовуються для посвідчення особи користувача на основі його біометричних даних.

Біометрична автентифікація - це процедура доведення автентичності заявлених користувачем даних, за допомогою пред'явлення користувачем свого біометричного способу.

Біометричні системи розпізнають людей на основі їх анатомічних особливостей (відбитків пальців, способу особи, малюнка ліній долоні, райдужної оболонки, голоси) або поведінкових рис (підписи, ходи). Оскільки ці риси фізично пов'язані з користувачем, біометричне розпізнавання надійно в ролі механізму, що стежить, щоб тільки ті, у кого є необхідні повноваження, могли потрапити в будівлю, отримати доступ до комп'ютерної системи або перетнути кордон держави. Біометричні системи також мають унікальні переваги - вони не дозволяють відректися від досконалої транзакції і дають можливість визначити, коли індивідуум користується декількома посвідченнями (наприклад, паспортами) на різні імена. Таким чином, при грамотній реалізації у відповідних додатках біометричні системи забезпечують високий рівень захищеності.

Сенс біометричних систем безпеки, по-перше, полягає в тому, щоб довести, що ви – це ви, і якщо сторонній може видати себе за вас – система нікуди не годиться. Такий результат називається помилкової позитивної ідентифікацією. По – друге, виключення можливості того, що система прийме вас за іншу людину. Знову ж біометрія повинна довести, що ви - це ви, а не хтось інший, і якщо ви не зможете переконати в цьому систему, значить, вона знову-таки не дуже хороша. Такий варіант називається помилкової негативної ідентифікацією. У загальному випадку біометричну систему можна оптимізувати за критерієм зменшення як позитивних, так і негативних помилок.

Варто відзначити, що біометричні методи автентифікації діляться на 2 групи, статичні і динамічні.

Статичні методи біометричної автентифікації. Статичні методи біометричної аутентифікації ґрунтуються на фізіологічної (статичної) характеристиці людини, тобто унікальній характеристиці, даної йому від народження і невід'ємною від нього. Ось деякі з них:

– автентифікація за відбитками пальців;

В основі цього методу лежить унікальність для кожної людини малюнка папілярних візерунків на пальцях. Дана технологія є найпоширенішою в порівнянні з іншими методами біометричної автентифікації.

– автентифікація за сітківкою ока;

Це спосіб ідентифікації по малюнку кровоносних судин очного дна. Для того, щоб цей малюнок став видний - людині потрібно подивитися на віддалену світлову крапку, і таким чином підсвічується очне дно сканується спеціальною камерою.

– автентифікація по геометрії руки;

У цьому біометричний методі для автентифікації особистості використовується форма кисті руки. Через те, що окремі параметри форми руки не є чимось унікальним, доводиться використовувати кілька характеристик. Скануються такі параметри руки, як вигини пальців, їх довжина і товщина, ширина і товщина тильного боку руки, відстань між суглобами і структура кістки. Також геометрія руки включає в себе дрібні деталі.

– автентифікація по геометрії обличчя;

Біометрична автентифікація людини по геометрії особи досить поширений спосіб ідентифікації і автентифікації. Технічна реалізація представляє собою складну задачку. Широке застосування мультимедійних технологій, за допомогою яких можна побачити достатню кількість відеокамер на вокзалах, аеропортах, площах, вулицях, дорогах і інших місцях скупчення людей, стало вирішальним у розвитку цього напрямку. Для побудови тривимірної моделі людського обличчя, виділяють контури очей, брів, губ, носа, і інших різних елементів особи, потім обчислюють відстань між ними, і за допомогою нього будують тривимірну модель. Щоб знайти цю унікальну шаблону, відповідного певній людині, потрібно від 12 до 40 характерних елементів. Шаблон повинен враховувати безліч варіацій зображення на випадки повороту особи, нахилу, зміни освітленості, зміни виразу.

Динамічні методи біометричної автентифікації. Динамічні методи біометричної автентифікації ґрунтуються на поведінкової (динамічної) характеристиці людини, тобто побудовані на особливостях, характерних для підсвідомих рухів в процесі відтворення якого-небудь дії. Розглянемо їх нижче:

– автентифікація по голосу;

Біометричний метод автентифікації по голосу, характеризується простотою в застосуванні. Даному методу не потрібно дорога апаратура, досить мікрофона і звукової плати. В даний час дана технологія швидко розвивається, так як цей метод автентифікації широко використовується в сучасних бізнес-центрах. Існує досить багато способів побудови шаблону по голосу. Зазвичай, це різні комбінації частотних і статистичних характеристик голосу. Можуть розглядатися такі параметри, як модуляція, інтонація, висота тону, і т. п.

– автентифікація по рукописному почерку;

Метод біометричної автентифікації по рукописному почерку ґрунтується на специфічному русі людської руки під час підписання документів. Для збереження підпису використовують спеціальні ручки або сприйнятливі до тиску поверхні. Цей вид автентифікації людини використовує його розпис. Шаблон створюється в залежності від необхідного рівня захисту.

Висновки. Біометрією називається сукупність способів і пристроїв для ідентифікації людини, які засновані на його унікальних фізіологічних або поведінкових характеристиках. Цей вид ідентифікації може застосовуватися для запобігання забороненого доступу.

Біометричний захист дає більший ефект у порівнянні, наприклад, з використанням паролів, смарт-карт, PIN-кодів, жетонів або технології інфраструктури відкритих ключів. Це пояснюється можливістю біометрії ідентифікувати не пристроєм, але людини. Звичайні методи захисту загрожують втратою або крадіжкою інформації, яка стає відкритою для незаконних користувачів.

За типом використовуваної інформації біометрична ідентифікація ділиться на: статичні методи, засновані на унікальних властивостях, даних осіб від народження і невід'ємних від нього; динамічні методи, засновані на поведінкової характеристиці особистості.

Список використаних джерел

1. *Кухарев Г. А. Биометрические системы: Методы и средства идентификации личности человека / Г. А. Кухарев. – СПб: Политехника, 2001. – 240 с.*
2. *Сидоркина И. Г.Классификация методов аутентификации человека / И. Г. Сидоркина, Р. В. Канаев, О. Ю. Меркушев. – Москва. – 6 с.*
3. *Методы биометрической аутентификации [Електронний ресурс] – Режим доступу до ресурсу: https://studbooks.net/2038659/informatika/metody_biometricheskoy_autentifikatsii*

УДК 004.056

Глазунов Д. М.
Харківський національний університет радіоелектроніки

Важливість забезпечення захисту інформації від загроз соціальної інженерії

Ви коли-небудь замислювалися, наскільки вразливі в сучасному суспільстві? Наприклад, коли ви йдете з дому, напевно, закриваєте двері, в надії, що це виключає проникнення грабіжника і матеріальні цінності залишаться в цілості. Але насправді в наших руках і руках шахраїв маса можливостей – обмежує тільки уява. Ви і Ваше житло завжди залишаєтеся уразливі для злочинця, який обере «розумний» спосіб проникнення – він зробить так, що Ви самостійно відкриєте йому двері.

У будь-якій маленькій або великій організації є в захисті інформації слабкі місця. Вміст відділень банків і офісів фінансових інститутів має високу матеріальну цінність, тому системи безпеки цих закладів на високому рівні та весь час удосконалюються. Але навіть, попри посилені заходи охорони, навіть якщо на всіх комп'ютерах компанії встановлене найкраще програмне забезпечення, паролі всіх співробітників є складними, а за всіма комп'ютерами стежать найрозумніші адміністратори – все одно можна знайти слабке місце.

Проблема захисту інформації – одна з найважливіших задач у сучасному світі, а головне «слабке місце» – людина або люди, які працюють в компанії, що мають доступ до комп'ютерних систем і є більшою чи меншою мірою носієм інформації про організацію.

В еру поширення інформаційних технологій, удосконалюються, як методи захисту інформації, так і способи її розкрадання. Як відомо, все, що однією людиною було реалізовано – іншою людиною може бути зламано, однак мета соціальної інженерії не зламати обчислювальну машину або програмне забезпечення, а обхитрити людини.

Під поняттям соціальної інженерії у сфері інформаційної та кібербезпеки слід розуміти мистецтво маніпулювання: психологічні методи та способи впливу, якими користуються шахраї, здійснюючи обман і введення в оману людину або групу людей в організації.

Мета таких дій – отримання конфіденційної інформації: паролів, персональних даних клієнтів або співробітників, реквізитів банківських рахунків та іншої інформації, яка дозволяє зловмисникові проникнути в систему і порушити її цілісність, що може принести втрату репутації та фінансів.

Поняття прийшло до нас зі сфери хакерства. Хакер – це людина, яка шукає уразливості в комп'ютерних системах, іншими словами – зламує. Яке відношення, здавалося б, до цього має соціальна інженерія? Все дуже просто. В один момент часу хакери усвідомили, що головна вразливість в будь-якій системі – це не машина, а людина. Вона, точно так само, як і комп'ютер, працює за певними законами. Використовуючи накопичений людством досвід в психології, маніпуляціях і механізмах впливу, хакери стали «зламувати людей».

Людина здатна думати, міркувати, приходити до того чи іншого висновку, але не завжди висновки можуть виявитися справжніми та власними – деякі з них можуть бути нав'язані ззовні, такі які вони потрібні комусь іншому. Але найцікавіше і головне – людина може не помічати, що її міркування помилкові. Вона до останнього моменту може думати, що все вирішила самостійно. Саме цією особливістю користуються люди практикуючі соціальний інжиніринг.

Людські відносини будуються на вмілому використанні психокомплексів. Їх небагато, але достатньо для управління людьми та досягнення цілей. Вплив на психокомплекси є найдієвішим засобом маніпулювання людьми. Кожен з нас має «струни» і «больові точки», вразити які і є завдання хакера, який бажає використовувати мистецтво маніпулювання у своїй протиправній діяльності. Основні з них:

1. Страх. Найімовірніше, самий часто використовуваний і найнебезпечніший психокомплекс людини. Можна відчувати страх здатися смішним в якійсь ситуації, страх за наслідки не виконаного доручення, страх перед чимось невідомим. Існують мільйони маленьких і великих страхів, які змусять людину піти на необдумані вчинки, щоб від них позбутися. Використовувати цей психокомплекс легко – достатньо лише викликати у співрозмовника один зі страхів і зіграти роль «визволителя».

2. Цікавість. Метод в цій категорії може полягати в використанні фізичного носія (дискета, диск, флешка), який містить на собі шкідливе програмне забезпечення. Попередньо зловмисник готує одну або декілька копій носія вірусного програмного забезпечення, оформляє його у фірмовому стилі компанії або ж позначає його текстом, який викликає інтерес, наприклад: "Список співробітників під скорочення" і т. п. Розкидає носії на території компанії, там, де їх буде легко знайти, біля входу в будівлю, коридорах, туалетах, їдальень і чекає. Людина, яка виявить знахідку найімовірніше захоче задовольнити свою цікавість і дізнатися, що на ньому знаходиться.

3. Жадібність. Купити що-небудь цінне, але дешево, отримати багато грошей, не доклавши до цього особливих зусиль, зберегти гроші у кризовій ситуації – всі ці природні людські бажання.

4. Перевага. Мистецтво робити прямі та приховані компліменти в таких випадках – найголовніша зброя. Можна зробити комплімент самій людині – висловити захоплення його заповзятливістю, розумом, зовнішністю. Можна словами в чудовій мірі позначити справу, якою він займається, відзначити його успіхи на цьому терені. Можна утішно відгукнутися про його дружину, дітей, коханку, собаку. Нарешті, компліментарно відгукнутися про його авто або заміському будинку і між тим, підвести людину до теми або певного питання, дізнавшись необхідну інформацію.

5. Великодушність і жалість. Ці два схожих психокомплексів орієнтовані на те, що майже кожній людині властиві жалість і великодушність. Може звернутися співробітник або клієнт з проханням роздрукувати будь-який документ. По простоті душевній, співробітник вставляє носій у свій комп'ютер і отримуєте цілий набір троянських коней, які, активізуючись, починають красти паролі, фінансові звіти та іншу конфіденційну інформацію.

6. Довірливість. Людям властиво сподіватися на краще і вірити, що саме їх ніхто не обдурить. У соціального інженера завжди є кілька способів: він може попросити надати допомогу або зробити так, щоб цю допомогу попросили та з вдячністю прийняли. Шахрай здійснює такий вид атаки соціальної інженерії, наприклад, шляхом дзвінка в компанію через внутрішній телефон або пише на електронну пошту, де він видає себе за співробітника IT-відділу і каже, що в системі були виявлені критичні збої, які необхідно терміново вирішити. У свою чергу, нічого не підозрюючи, співробітник компанії починає слідувати «рекомендацій» фахівця, тим самим надаючи шахраєві доступ до внутрішньої системи, а в наслідок і до конфіденційної інформації.

З розвитком технологій та появою соціальних мереж зловмисникам навіть не доводиться вдаватися до будь-яких спеціальних методів отримання інформації, оскільки потрібні відомості про користувача легко знайти на його сторінці в соцмережі. Інтереси, круг друзів, політичні погляди, захоплення музикою, улюблені фільми, поточне місцеперебування – все це може зіграти на руку злочинцям.

Саме тому, не рекомендується тримати інформацію про себе у відкритому доступі або встановлювати певні обмеження на доступ до цієї інформації. Все, що користувач вводить в Інтернеті, може так чи інакше потрапити до зловмисників, а далі вони можуть використовувати отримані відомості проти людини – шантажувати або маніпулювати.

Тепер ми знаємо, що для досвідченого соціального інженера практично немає нічого нездійсненного. Чи можливо захиститися від вторгнення?

Система інформаційної безпеки зазвичай починається з визначення критичних інформаційних активів і оцінки ризиків для них. За результатами цієї роботи проектується і будується архітектура системи, а потім проектується і впроваджується технічна складова її підтримки, що включає антивіруси, системи захисту від витоків даних, системи захисту від атак ззовні та ін. Побудувавши ту чи іншу систему захисту, більшість організацій, як правило, на цьому і зупиняються. Однак після того, як така система запущена і починає функціонувати, доцільно перевірити, самостійно або з допомогою зовнішніх компаній, наскільки вона справляється із завданням захисту інформації.

Корпоративна техніка безпеки повинна чітко визначати поведінку співробітника в тих чи інших ситуаціях. Чіткий інструктаж співробітників всіх рівнів надасть необхідну допомогу для запобігання крадіжки інформації. У зв'язку з цим, рекомендується проводити навчання та контрольні перевірки співробітників на ефективність навчання і готовності службовців до виконання дій, пов'язаних із забезпеченням інформаційної безпеки.

Технічними заходами захиститися від загрози соціальної інженерії досить складно, а все тому, що зловмисники використовують слабкості не технічних засобів, а як вже говорилося вище, слабкість людської душі. Тому один з найбільш правильних способів протидіяти зловмисникам – постійна і правильна робота з людським фактором.

Під час навчання, звичайні користувачі (які не займаються питаннями інформаційної безпеки в рамках своєї основної роботи) повинні вивчити такі теми (крім інших тем, пов'язаних з правильним вибором паролів, загальними положеннями політики безпеки організації і т. д.):

1. Як ідентифікувати підозрілі дії та куди повідомляти про них?

2. Що може очікувати користувачів в процесі реалізації атак з боку зовнішніх і внутрішніх зловмисників? Ні в якому разі не можна забувати про внутрішні загрози - адже за статистикою основне число інцидентів безпеки відбувається саме зсередини організації.

3. Яка поведінка користувача може зменшити потенційний збиток, що наноситься даними, системам і мережам?

У дитинстві нас вчили не довіряти незнайомцям. На жаль, з часом ми стали забувати це нескладне правило. Технічні засоби захисту, безумовно, значно зміцнюють «оборону» компанії. Але лише забезпечивши розуміння питань корпоративної безпеки серед співробітників, можливо максимально захистити компанію від злочинних дій шахраїв.

Список використаних джерел

1. *Garfinkel S. Database Nation: The Death of Privacy in the 21st Century [Text] / S. Garfinkel — Sebastopol : O'Reilly Media, Inc., 2000. — 338 p. — ISBN:1-56592-653-6*
2. *Что такое социальная инженерия? Принцип работы и методы влияния [Електронний ресурс] / Д.Н.Глазунов // – 2018. – Режим доступу: http://withsecurity.ru/chto-takoe-socialnaya-inzheneriya-princip-raboty-i-metody-vliyaniya. – Назва з екрана.*
3. *Инженеры человеческих душ [Електронний ресурс] / А.В.Лукацкий // – 2010. – Режим доступу: https://bugtraq.ru/library/misc/engineers.html. – Назва з екрана.*

УДК 004.451:004.056

Донченко П. О., Жума В. М., Савельєва Т. В.
Черкаський державний технологічний університет

Механізм реагування на потенційно небезпечні дії користувача в Linux

Вступ. Операційна система (ОС) Linux сьогодні широко застосовується в якості серверної платформи для реалізації різних мережевих та «хмарних» сервісів. Вихідні коди даної ОС відкриті для загального перегляду та внесення змін. Природно, що користувач або адміністратор даної ОС може, також, вносити зміни в головні конфігураційні файли. Інколи користувач навмисно або спеціально (як зловмисник - інсайдер) може отримати підвищені права доступу і модифікувати ті чи інші системні файли, внаслідок чого намагатиметься змінити цілісність системних файлів/налаштувань, або, навіть, залишити там фішинговий чи інший шкідливий код.

Задача дослідження. Відслідковування цілісності системних файлів та каталогів є важливою складовою в системі реагування на потенційно небезпечні дії з боку користувача інформаційної системи (ІС). Адекватно створений механізм реагування в змозі здійснювати ефективний контроль та блокування роботи в разі несанкціонованих втручань в роботу ІС. В ОС Linux є декілька системних каталогів, зміст яких слід контролювати в рамках контролю потенційно небезпечних дій з боку користувача системи.

Основний матеріал. З огляду на рекомендації, наведені в [1,2] – основні каталоги та файли, зміна змісту яких негативно впливає на роботу сервера ОС Linux та, відповідно, часто є метою атак зловмисників – це каталоги: /etc; /bin; /sbin; /lib. Припустимо, що необхідно відстежити зміни в директоріях /etc. Для цього можна, наприклад, виконати наступну команду: md5sum /etc/*, яка підрахує контрольні суми файлів каталогу. Можна також, виконати команду md5sum -c /home/linux/md5, яка здійснить порівняння контрольних сум md5 з контрольними сумами, підрахованими раніше і записаними у файл md5. В результаті чого на екран буде виведено наступне (рисунок 1):

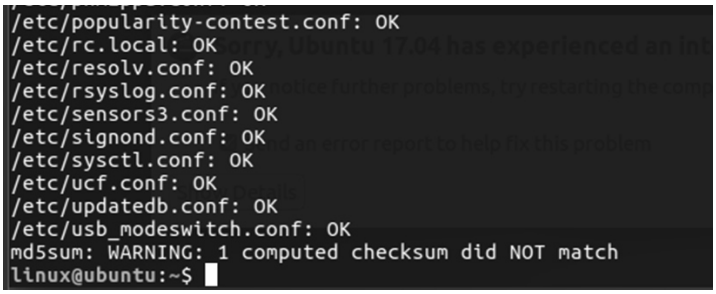


Рисунок 1 – Результат виконання команди md5sum -c /home/linux/md5 після внесення змін в систему шляхом спроби додати нового користувача системи

Але запуск відповідного скріпту по перевірці важливих системних файлів та каталогів регламентовано має сенс проводити кожного разу після початку сеансу даного користувача, що не гарантує оперативності реакцій і може тривати достатньо довго.

Для ОС Linux існує підсистема, яка дозволяє отримувати інформацію про зміни в файловій системі та може бути налагоджена для реагування на відповідні події, яка має назву Inotify [3].

Inotify - це підсистема ядра Linux, яка дозволяє отримувати повідомлення про зміни в файловій системі. Тобто, дає інформацію про час створення або редагування будь-якого файлу або директорії в файлової системі [4].

Після установки запускаємо демон командою service icron start, тобто додаємо його в списки служб, які запускаються при старті системи.

Далі слід прописати завдання для демона. Це робиться командою incrontab -e. Можна файли із завданнями для даного демона редагувати вручну. Конфігураційні файли inotify знаходяться в директорії /var/spool/incrontab.

В якості файлу спостереження демоном inotify оберемо директорію /tmp/testdir/, для неї вказується прапор зміни файлу (IN_MODIFY), із виводом повідомлення при зміні файлу наступним чином (рис.2):

Рисунок 2 – Процес налаштування конфігураційного файлу incron для відслідковування порушення цілісності файлу/каталогу

В зв`язку з тим, що файл був модифікований, то дані зміни були занесені в системний лог. В зв'язку з модифікацією файлу вказаного на рисунку 2, всі зміни були відображені у системному лозі. Далі додаємо ще один об'єкт стеження – цього разу модифікація файлу конфігурації файєрволу ufw (рис.3).

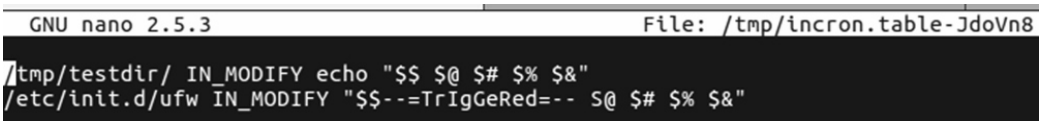


Рисунок 3 – Настройка відслідковування змін в міжмережевому екрані ufw

Механізм реагування на потенційно небезпечні дії користувача буде включати відключення обслуговування web – сайту web – сервером. Це слушно, адже зловмисник (інсайдер) може змінити цілісність сайту, або, навіть, залишити там фішинговий код.

Якщо, наприклад, необхідно щоб веб-сервер автоматично вимикався, за умови що контент змінено і сервер має конфігурацію в /etc/apache2/apache2.conf , то для цього можна відредагувати файл Incrontab кореневого користувача, в incrontab слід додати наступний рядок: /etc/apache2/apache2.conf IN_MODIFY /usr/sbin/service apache2 stop [5, 6]. Наступним кроком зберігаємо та закриваємо конфігураційний файл incrontab. Для внесення наступних змін відкриваємо файл /etc/apache2/apache2.conf, редагуємо та зберігаємо після чого сервіс.

Висновок. Як видно в результату проведеного тестування, створений підхід до побудови механізму реагування на потенційно небезпечні дії користувача виявився вірним. При здійсненні змін тестового файлу механізм працює штатно і реагує адекватно.

Список використаних джерел

1. *Фленов М. Linux глазами хакера (+CD) / Михаил Фленов. – СПб: BHV, 2010. – 480 с.*
2. *Фленов М. Linux глазами хакера. 4-е издание / М. Фленов. – СПб: БХВ-Петербург, 2016. – 400 с.*
3. *Linux Programmer's Manual [Електронний ресурс] // Linux/UNIX system programming training. – 2017. – Режим доступу до ресурсу: http://man7.org/linux/man-pages/man7/inotify.7.html.*
4. *Inotify чи автоматизація рутинних операцій за допомогою incron [Електронний ресурс] // habr. – 08.08.2009. – Режим доступу до ресурсу: https://habr.com/post/66569.*
5. *Wallen J. How to Use Incron to Monitor Important Files and Folders [Електронний ресурс] / Jack Wallen // linux.com. – 27.05.2016. – Режим доступу до ресурсу: https://www.linux.com/learn/how-use-incron-monitor-important-files-and-folders.*
6. *How to run commands on File or Directory changes with Incron on Ubuntu 16.04 [Електронний ресурс] // HowtoForge. – 2018. – Режим доступу до ресурсу: https://www.howtoforge.com/tutorial/how-to-run-commands-on-file-or-directory-changes-with-incron-on-ubuntu-16-04.*

УДК 004.056

Кривенко С. С., Шматок О. С.
Національний авіаційний університет

Методи виявлення закладних пристроїв

Захист інформації, в тому числі і захист від несанкціонованого зйому акустичної інформації за допомогою радіоакустичного закладних пристроїв, є невід'ємною частиною будь-якого бізнесу на сьогоднішній день. Значення інформації в житті будь-якого цивілізованого суспільства безперервно зростає. Вже давно відомо, що інформація, яка мала важливе воєнно-стратегічне значення для держави, ретельно приховувалася і захищалася. В даний час інформація, що відноситься до технології виробництва і збуту продукції, стала ринковим товаром, що має великий попит як на внутрішньому так і на зовнішньому ринках.

Інформаційні технології постійно вдосконалюються в напрямку їх автоматизації і способів захисту інформації. Розвиток нових інформаційних технологій супроводжується такими негативними явищами, як промислове шпигунство, комп'ютерні злочини та несанкціонований доступ до секретної та конфіденційної інформації. Тому захист інформації є надзвичайно важливою державною завданням в будь-якій країні.

Найбільш широко сьогодні використовуються акустичні заставні пристрої, що передають інформацію по радіоканалу. Закладки можуть бути виконані у вигляді окремого модуля або закамуфльовані під предмети повсякденного побуту: попільничку, електронний калькулятор, авторучку, вазу і т.д. Подібні заставні пристрої постійно удосконалюються і вже почали з'являтися на вітчизняному ринку екземпляри закладних пристроїв з підвищеною скритністю (акустопуском, інверсією основного спектру, псевдовипадкової перебудовою робочої частоти і т.п.).

Це означає, що сьогодні актуально розробляти окремі прилади та цілі комплекси по виявленню і виявлення подібного роду пристроїв несанкціонованого знімання інформації.

Сучасні радіоакустичного закладних пристроїв та їх демаскуючі ознаки. Особливості побудови сучасних радіоакустичного закладних пристроїв. Основними характеристиками радіозакладок є:

- габарити і вага;
- термін служби;
- скритність роботи;
- акустична чутливість
- дальність передачі.

Радіомікрофон здатний протягом року передавати інформацію на відстань до 1,5 км з приміщення, де розмова ведеться пошепки. Радіозакладки зазвичай компактні і маскуються під мікро шпильки, годинник, калькулятори, авторучки, пачки сигарет і т.д. Завдяки малим розмірам радіозакладка може бути швидко і надійно захована. Радіозакладки у вигляді годинника, авторучки і т. П. Можуть бути впроваджені у вигляді подарунка довірливому службовцю фірми. Комерційні радіозакладки мають великі габарити і вага, але відповідно меншу вартість. У міру розвитку техніки їх розміри зменшуються.

В даний час середні параметри комерційних закладок складають [1] :

- обсяг - (1 см3- 8дм3);
- вага - (5 - 350) м

Термін служби радіозакладки в основному визначається застосовуваним джерелом харчування. Розглянемо основні види джерел живлення:

- автономне живлення;
- харчування від пристроїв, в яких замаскована радіозакладка;
- харчування від електромережі;
- харчування від телефонної мережі.

При автономному живленні радіозакладками не треба нікуди підключати, тобто час установки і ризик її установки мінімальний. За потреби великого терміну дії, природно, виникає необхідність зміни джерела живлення, що, відповідно, викликає суттєві труднощі і підвищує ризик виявлення. Тому при першій же установці зазвичай намагаються поставити батарею максимальної місткості, встановивши її, природно, спільно із закладкою, в ємні предмети. Наприклад, в макети кораблів, квіткові горщики і т.д.

Для збільшення терміну служби закладки в якості автономного джерела живлення використовують сонячні батареї, замасковані разом із закладкою під питні склянки і т.д. Поки подібні пристрої не знайшли широкого застосування через неможливість роботи в умовах слабкої освітленості.

Заощадити ресурс батареї і підвищити скритність передачі дозволяє використання дистанційного включення. Економія ресурсу батареї можлива і при автоматичному включенні закладки при наявності звуку і відповідному її виключенні через кілька секунд після його зникнення.

Іншою можливістю економії ресурсу батареї є зменшення потужності передавача, що одночасно підвищує скритність його роботи. При зменшенні потужності передавача відповідно зменшується дальність його роботи. Для забезпечення прийому встановлюється додатковий ретранслятор поза об’єктом в сусідній кімнаті, автомобілі і т.д. Габарити і харчування ретранслятора не лімітована, і він забезпечує подальшу передачу на необхідну відстань.

Харчування радіозакладок від пристроїв, всередину яких вони вмонтовані значно збільшує термін їх дії. При старінні батареї сам пристрій (наприклад, калькулятор) перестає працювати, і в ньому не підозрілі співробітники самі змінюють батарейку. Харчування радіоакустичного закладних пристроїв (РАЗУ) від мережі 220 В робить практично не обмеженим їх термін дії. Недоліком такого виду закладок є необхідність проведення певного виду робіт на об’єкті. Харчування РАЗУ від телефонної мережі також забезпечує необмежений термін їх служби. Як і у варіанті з мережею 220 В виникають труднощі з їх установкою.

Скритність роботи забезпечується:

- вибором частотного діапазону;
- накопиченням інформації з подальшою її передачею в режимі швидкодії;
- малої вихідною потужністю передавача.

Найпростіші РАЗУ працюють на частотах FM - мовлення, вони складають 30% всіх наявних на ринку РАЗУ. Більш професійні РАЗУ працюють в діапазоні між мовним FM-діапазоном і 6-м каналом TV-мовлення. Завантаження метрового діапазону мобільними радіостанціями змушує використовувати для РАЗУ наступний діапазон (дециметровий) між 12 і 21 каналами TV. РАЗУ зазначеного діапазону важко виявити, вони дороги, їх використовують професіонали. Для підвищення скритності роботи професіонали почали використовувати інфрачервоний канал. К недоліків такого виду передачі слід віднести необхідність прямої видимості між закладкою і приймачем, а також сильний вплив фонової засвітки.

Накопичення інформації з подальшою її передачею в режимі швидкодії дозволяє підвищити скритність роботи передавача, так як вихід в ефір стає короткочасним. Мала вихідна потужність РАЗУ ускладнює її виявлення через малого рівня сигналу від РАЗУ на тлі потужних перешкод від працюючих радіостанцій, від включення і виключення промислових установок, перешкод від проїжджаючих трамваїв і т. П.

Акустична чутливість і дальність передачі РАЗУ характеризуються акустичної чутливістю - здатністю сприймати звук з різних відстаней. Гарною чутливістю вважається здатність сприймати звук на відстані 5-12 м в тихому приміщенні.

Класифікація радіоакустичного закладних пристроїв і дослідження тенденцій розвитку діапазонів робочих частот Після здобуття нашою країною незалежності і, пов'язаними з цим, неминучими змінами в економіці, розвитком міжнародного науково-технічного та економічного співробітництва, запровадження ринкових відносин призвело до появи промислового шпигунства в звичайному житті. Це означає, що будь-яка сучасна підприємство змушене працювати в умовах жорсткої конкуренції, яка, на жаль, все частіше носить недобросовісної характер. Як правило, промислове шпигунство виражається в порушенні прав власника на інтелектуальну або промислову власність. Порушення цих прав проявляється в несанкціонованому отриманні фінансово-економічних секретів, секретів виробництва, втручанням в особисте життя як рядових співробітників підприємства, так і вищих керівних ланок. Розвиток елементної бази та доступність практично будь-яких електричних компонентів у вільному продажі дозволило створювати закладні пристрої (ЗУ) з мікропередавач не тільки в спеціально обладнаних лабораторіях, але і в домашніх умовах. Сьогодні подібна техніка увійшла в стандартний набір сучасного менеджера. Тому, щоб захистити свої особисті, виробничі та економічні секрети від загроз недобросовісної конкуренції як малі приватні підприємства, так і промислові державні гіганти зобов'язані вживати серйозні заходи боротьби із застосуванням технічних засобів. Отже, для успішної протидії необхідно знати тактико-технічні характеристики та особливості використання технічних засобів розвідки. Лише при цьому можливе успішне виявлення цих технічних засобів і їх ефективне блокування. Часто РАЗУ застосовуються з так званої «апаратурою підтримки», до якої відносяться ретранслятори радіосигналів ЗУ, спеціалізовані радіоприймальні пристрої, мініатюрні диктофони і т.п. Акустичні ЗУ призначені для перехоплення мовної інформації. Перехоплюється акустичними ЗУ інформація може записуватися з використанням портативних пристроїв звукозапису або передаватися по радіоканалу, оптичного каналу, по електромережі змінного струму, по з'єднувальним лініях допоміжних технічних засобів, металоконструкцій будинків, трубах систем опалення та водопостачання, спеціально прокладених кабелів (лініях) і т.д . Найбільш широко використовуються акустичні ЗУ, що передають інформацію по радіоканалу. Закладки можуть бути виконані у вигляді окремого модуля або закамуфльовані під предмети повсякденного побуту: попільничку, електронний калькулятор, електролампочку, запальничку, наручний годинник, авторучку, вазу і т.д. В цілому все ЗУ, які призначені для перехоплення акустичної інформації, можна класифікувати за такими ознаками [2]:

Список використаних джерел

1. *Сидорин, Ю.С. Технічні засоби захисту інформації [Текст]: навч. посібник / Ю.С. Сидорин. - СПб .: Изд-во політехн. ун-ту, 2005. - 141 с.*
2. *Хорев, А.А. Класифікація електронних пристроїв перехоплення інформації [Текст] / А.А. Хорев // Спецтехніка і зв'язок. - 2009. - №1.- С. 46-49.*
3. *Конахович Г.Ф., і ін. Захист інформації в телекомунікаційних системах.*

УДК 343.3/.7:004

Кульчицький О. С.
Центральноукраїнський національний технічний університет

Вимоги протидії кіберзлочинності в умовах громадської локалізації

Успішне запобігання кіберзлочинів та ефективна правоохоронна діяльність загалом неможливі без широкої участі громадськості. Стратегія громадського впливу на злочинність має полягати, з одного боку, в залученні, а з іншого – в ініціативній участі окремих громадян, громадських організацій охорони правопорядку, участі у програмах профілактики кіберзлочинності.

Кіберзлочинність - це злочинність у так званому «віртуальному просторі», що моделюється за допомогою комп'ютера, інформації представленої в символьному, математичному, або будь-якому іншому виді [1].

Особливість даного виду злочинності полягає у тому, що готування та скоєння злочину здійснюється не відходячи від комп'ютера, є доступним з будь-якої точки земної кулі, а об’єкти злочинів можуть знаходитись за тисячі кілометрів від самого злочинця у будь-якому населеному пункті. Крім того, доволі складно зафіксувати і вилучити криміналістично-значущу інформацію при виконанні слідчих дій для використання її в якості речового доказу, а також недостатньо ґрунтоване опрацювання кримінологічних аспектів кіберзлочинності, кримінологічної оцінки нормативного врегулювання забезпечення кібербезпеки в Україні [2]. Усе це, безумовно, є перевагами для кіберзлочинців.

Об’єктом різних видів кіберзлочинів може стати будь-який користувач інтернету:

1. Фішинг - нібито від адміністрації або служби безпеки платіжних систем клієнтам надсилають повідомлення з проханням вказати свої рахунки та паролі.

2. Онлайн-шахрайство – несправжні інтернет-аукціони, інтернет-магазини, сайти та телекомунікаційні засоби зв’язку.

3. Мальваре - створення та розповсюдження шкідливого програмного забезпечення.

Видів такого злочину є дуже багато, всіх не перелічіть, але для хвилювань нема підстав, якщо знати як їх уникнути. Ось декілька порад щодо того, як вберегти себе від кіберзлочинів:

- створення надійних паролів та періодична їх зміна;
- поінформованість про злочинні прийоми, щоб розпізнати їх;
- захист пристроїв, встановлення антивірусних програм;
- використання захищених мереж;
- використання інструментів конфіденційності та безпеки Google [3].

Ефективність запобігання і протидії кіберзлочинності засобами державного управління безпосередньо залежить від узгодженості дій та заходів громадськості. Пам’ятайте всі вимоги кібербезпеки і дотримуйтесь їх!

Список використаних джерел

1. *Баранов О. А. Про тлумачення та визначення поняття «кібербезпека» / О. А. Баранов // Правова інформатика. –2014. –№ 2. – С. 54-62.*
2. *Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» // Офіційний вісник України від 29.03.2016. – № 23. – Стор. 69. – Ст. 899.*
3. *Управління боротьби з кіберзлочинністю // МВС України. [Електронний ресурс]. – Режим доступу : http://mvs.gov.ua/mvs/control/main/uk/publish/article/544754*

УДК 004.056.53

Макеєв А. В.[*]
Центральноукраїнський національний технічний університет

Огляд особливостей кіберзлочинів в Україні

Динамічний розвиток в Україні та світі інформаційно-телекомунікаційних технологій є дуже позитивним, однак використання комп'ютерних технологій із корисливих та інших мотивів може становити не лише особисту небезпеку для громадян, їх службової діяльності, суспільного порядку, моральності, а й створювати загрозу національній безпеці держави та світу в цілому.

У чинному законодавстві України на сьогодні відсутнє нормативно-правове закріплення ключових термінів «кіберзлочин» і «кіберзлочинність», що спричиняє численні наукові дискусії серед дослідників сучасності. Науковці приділяють багато уваги дослідженню зазначеної проблематики.

Основною причиною наявності втрат від злочинів, пов'язаних з інформаційно-комунікативними системами, є недостатня обізнаність користувачів у питаннях безпеки інформації. Тільки наявність у кінцевого користувача певних знань про заходи безпеки може забезпечити припинення інцидентів та помилок, ефективне вживання заходів захисту, запобігти злочину або своєчасно знайти злочинця. У цьому контексті можна визначити п'ять рівнів захисту комп'ютерних та інформаційних ресурсів

Для більшості злочинів, скоєних в глобальних комп'ютерних мережах, характерні наступні особливості:

- підвищена скритність вчинення злочину, що забезпечується специфікою мережевого інформаційного простору;
- транскордонний характер мережевих злочинів, при якому злочинець, об'єкт злочинного посягання, потерпілий можуть перебувати на територіях різних держав;
- особлива підготовленість злочинців, інтелектуальний характер злочинної діяльності; нестандартність, складність, різноманіття і часте оновлення способів скоєння злочинів і застосовуваних спеціальних засобів
- можливість вчинення злочину в автоматизованому режимі в декількох місцях одночасно;
- багатоепізодний характер злочинних дій при множинності потерпілих;
- необізнаність потерпілих про те, що вони піддалися злочинному впливу;
- дистанційний характер злочинних дій в умовах відсутності фізичного контакту злочинця і потерпілого;
- неможливість запобігання та припинення злочинів даного виду традиційними засобами.

У середовищі, де постійно з'являються та еволюціонують кіберзагрози, не можна залишатися незахищеним: сформована в світі ситуація зобов'язує до постійного вдосконалення методів боротьби з кіберзлочинами та стимулює побудову державної моделі, спрямованої на забезпечення кібербезпеки країни.

Список використаних джерел:

1. *Всесвітній огляд економічних злочинів. Кіберзлочини в центрі уваги [Електронний ресурс]. – Режим доступу: http://www.pwc.com/ua/en/services/ forensic/assets/gecs_2011_report_ukraine_ukr.pdf*
2. *Н.Міщук Кіберзлочинність як загроза інформаційному суспільству Вісник Львівського університету. Серія економічна. 2014. Випуск 51. С. 173 - 179*

[*] Науковий керівник – Константинова Л. В., викладач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету

УДК 004.451

Пашинських В. В.[*]
Центральноукраїнський національний технічний університет

Огляд дистрибутивів GNU/Linux для тестування безпеки

В наш час регулярне проведення різноманітних тестів на безпеку є дуже важливим для користувачів комп'ютерних мереж всіх рівнів, як великих корпорацій, так і фізичних осіб. Випадки проникнення зловмисників в інформаційну мережу з кожним роком частішають, зростають і збитки, яких завдають такі проникнення. Тому тестування на проникнення, або pentest є популярною у всьому світі послугою у сфері інформаційної безпеки.

Тест на проникнення — це метод оцінки рівня захищеності комп'ютерної системи чи мережі з використанням моделювання дій зовнішніх зловмисників (які не мають авторизованих засобів доступу до системи) і внутрішніх зловмисників (які мають певний рівень санкціонованого доступу) з проникнення у неї. Цей процес включає активний аналіз системи з виявлення будь-якої потенційної вразливості, що може виникати внаслідок неправильної конфігурації системи, відомих і невідомих дефектів апаратних засобів та програмного забезпечення, чи оперативного відставання в процедурних чи технічних контрзаходах. Цей аналіз проводиться з позиції потенційного нападника і може включати активне використання вразливостей.

Існує велика кількість дистрибутивів для проведення тестування на проникнення. Зазвичай вони ґрунтуються на існуючих Linux-дистрибутивах і являють собою їх перероблені версії. Розглянемо найпоширеніші з них.

Kali Linux. Kali Linux – найбільш популярний дистрибутив GNU/Linux для тестування на проникнення. Він був розроблений компанією Offensive Security, з початковою назвою BackTrack. Він базується на дистрибутиві Debian. В дистрибутиві вбудована велика кількість інструментів тестування на проникнення з різних сфер. Зараз він використовує модель оновлення Rolling-release – це означає, що у Вас завжди буде встановлено останні версії програм.

Оскільки він є самим популярним, він найбільш досконалий серед інших дистрибутивів. Kali Linux підтримує багато різних пристроїв та апаратних засобів. Крім того, він має активну спільноту і якісну документацію.

BlackArch. BlackArch - це відомий дистрибутив для тестування рівня безпеки, який розроблено на базі Arch Linux. Він має власний репозиторій, до якого входить дуже багато різних інструментів для тестування, які було організовано у групи, що значно полегшує пошук потрібного додатку. Не зважаючи на те, що у ньому вже вбудована більша кількість інструментів для тестування, ніж в інших дистрибутивах - їх кількість продовжує зростати. Так, як і Arch Linux він використовує модель оновлення Rolling-release.

Варто зазначити що існує можливість встановити набір інструментів BlackArch поверх Arch Linux, що значно полегшує міграцію на даний дистрибутив користувачам Arch Linux.

Fedora Security Lab. Fedora Security Lab - це версія відомого дистрибутиву Fedora, яка призначена для аудиту безпеки, а також може використовуватись для відновлення пошкоджених ОС.

[*] Науковий керівник – Гермак В. С., викладач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету

На офіційному сайті зазначено, що дистрибутив використовується і в навчальних цілях. На відміну від базової версії Fedora, використовується графічна оболонка XFCE.

BackBox. BackBox – це ще один дистрибутив який заснований на Ubuntu. Він призначений для тестування на проникнення та оцінки рівня безпеки. Досить популярний і має хорошу підтримку спільнотою.

Він має власний репозиторій програмного забезпечення, у якому завжди останні стабільні версії програмного забезпечення, призначеного для аналізу комп'ютерних мереж та систем. Це мінімалістичний дистрибутив, у якому використовується середовище XFCE.

Parrot Security OS. Parrot Security OS - відносно новий дистрибутив, за яким стоїть компанія Frozenbox. Користувачі Parrot Security OS - фахівці з інформаційної безпеки, які потребують дистрибутив зі зручним інтерфейсом, онлайн-анонімністю та з шифруванням даних.

Він заснований на дистрибутиві Debian, та використовує середовище робочого столу MATE. В його репозиторіях є майже кожен відомий інструмент для тестування на проникнення. Parrot Security OS також використовує модель оновлення Rolling-release.

Pentoo Linux. Дистрибутив Pentoo заснований на Gentoo Linux. Він також призначений для тестування на проникнення, і доступний як LiveCD.

На відміну від Gentoo, він має графічну оболонку і дозволяє зберігати усі зміни в LiveCD. Також він має багато специфічних функцій ядра, деякі індивідуальні інструменти для тестування та багато іншого. Цей дистрибутив використовує графічну оболонку XFCE.

Порівняння дистрибутивів за їх популярністю. Для порівняння було використано статистику DistroWatch за останні шість місяців, для кожного дистрибутиву вказано його номер, згідно рівня його популярності серед усіх дистрибутивів GNU/Linux.

- Kali Linux – 16;
- BlackArch – 77;
- Fedora Security Lab – 7;
- BackBox – 81;
- Parrot Security OS – 37;
- Pentoo Linux – 232;

Слід зазначити, що аналогічних дистрибутивів існує значно більше, в рамках цього огляду було розглянуто лише найбільш відомі і популярні. Взагалі, рівень тестера на проникнення залежить від його знань і можливості володіти спеціалізованими інструментами. Але середовище, в якому ці інструменти запущені, впливає на швидкість виконання задач і досягнення результатів. Кожен може обрати собі дистрибутив згідно своїх потреб, а також рівня знань операційної системи GNU/Linux. Серед перелічених дистрибутивів я рекомендував би користувачам з невисоким рівнем знання ОС звернути увагу на Kali Linux. Інший дистрибутив, BlackArch Linux, я б порекомендував спеціалістам. BlackArch Linux не самий простий дистрибутив - з ним доведеться набагато глибше вивчити будову систему GNU/Linux.

Список використаних джерел

1. *Тест на проникнення [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki /Тест_на_проникнення*
2. *DistroWatch Page Hit Ranking [Електронний ресурс]. – Режим доступу: https://www.distrowatch.com /dwres.php?resource=popularity*
3. *Эриксон Дж. Хакинг: искусство эксплойта. 2-е издание. – Пер. с англ. – СПб.: Символ-Плюс, 2010. – 512 с.*

УДК 004.451
Пашинських В. В., Конопліцька-Слободенюк О. К.
Центральноукраїнський національний технічний університет

Двофакторна автентифікація: огляд та недоліки

Двофакторна автентифікація - це додатковий рівень безпеки, який використовується для забезпечення того, щоб люди, які намагаються отримати доступ до аккаунта, були тими, за кого себе видають. Спочатку користувач вводить своє ім'я та пароль. Потім він повинен надати додаткову інформацію. Ця інформація може належати до однієї з наступних категорій факторів:

- те, що Ви знаєте (це може бути персональний ідентифікаційний номер (PIN), пароль або відповіді на секретні запитання);
- те, що у Вас є (як правило, користувач має щось у своєму розпорядженні, наприклад, кредитну картку чи смартфон);
- те, чим Ви є (ця категорія є трохи більш широкою, і може включати в себе біометричні дані: відбитки пальців, райдужна оболонка ока чи геометрія обличчя).

Двофакторна автентифікація значно підвищує захищеність аккаунта. Таким чином, навіть якщо ваш пароль буде зламаний або ваш телефон втрачено, шанси на те, що хтось інший має інформацію про ваш другий фактор, є низькими. Отже, якщо правильно використовувати двофакторну автентифікацію, веб-сайти та програми можуть бути більш впевненими в особистості користувача.

Якщо сайт, яким ви користуєтесь використовує лише один пароль, існує велика ймовірність того, що його буде зламано.

Нині використовуються кілька типів двофакторної автентифікації; деякі можуть бути більш надійними або складними, ніж інші, але всі забезпечують більший захист, ніж паролі. Розглянемо найпоширеніші форми двофакторної автентифікації.

1. Пристрої автентифікації - найстаріша форма двофакторної автентифікації. Являє собою пристрій, який генерує новий числовий код кожні 30 секунд. Коли користувач намагається отримати доступ до облікового запису, він дивиться на пристрій та вводить зображений код на сайті або у додатку. Аналогічні версії пристрою автоматично передають код автентифікації під час підключення до USB-порту комп'ютера.Однак у них є кілька недоліків: для підприємств ці пристрої є дорогими, а також їх легко втратити.

2. SMS-автентифікація та автентифікації через дзвінок- автентифікація, що працює безпосередньо з телефоном користувача. Після отримання імені користувача та пароля сайт надсилає користувачеві унікальний одноразовий пароль (OTP) за допомогою текстового повідомлення. Потім користувач повинен ввести OTP на сайті чи у додатку, щоб отримати доступ. Автентифікація за допомогою дзвінка працює аналогічним чином – але OTP передається користувачу усно. До недоліків можна віднести те, що зловмисники можуть перехопити SMS з кодом, і цей спосіб автентифікації не буде працювати без телефону, та покриття мобільною мережею.

3. Автентифікація за допомогою програмного забезпечення - найпопулярніша форма двофакторної автентифікації (а також головна альтернатива SMS та дзвінку) використовує одноразовий пароль, який генерується програмним забезпеченням (також називається TOTP або "soft-token").

Для використання цього способу автентифікації, користувач повинен завантажити та встановити додаток автентифікації на своєму смартфоні чи комп'ютері. Тоді вони можуть використовувати додаток при авторизації на будь-якому сайті, який підтримує

цей тип автентифікації. Під час входу користувач спочатку вводить ім'я користувача та пароль, а потім, коли з'явиться запит, він вводять код, який генерується в додатку. Створений код зазвичай діє менше хвилини. І через те, що код генерується та відображується на одному і тому ж пристрої, виключається можливість його перехоплення хакером. Це значна перевага над іншими методами автентифікації**.** І головне, оскільки це програмне забезпечення доступне і для мобільних пристроїв, і для комп'ютерів, і для смарт-годинників, і навіть працює без доступу до інтернету – автентифікація користувачів можлива практично скрізь.

Зараз використовується ще один спосіб автентифікації – за допомогою Push-повідомлення. Сайт або додаток може надіслати користувачу повідомлення, за допомогою якого він може підтвердити авторизацію. Але цей метод автентифікації не дуже безпечний, оскільки у хакерів є способи отримати код.

Також варто зазначити, що вже у найближчому майбутньому можуть з'явитися інші способи автентифікації – за допомогою відбитків пальців, малюнка райдужної оболонки ока чи геометрії обличчя.

Багатофакторна автентифікація могла б суттєво знизити частоту крадіжок особистих даних та інших шахрайств в Інтернеті, оскільки пароля більше не буде достатньо, щоб дати злодію постійний доступ до своєї інформації. Проте, багато методів багатофакторної автентифікації залишаються вразливими до фішингу, атаки "man-in-the-browser" та "man-in-the-middle".

Багатофакторна автентифікація може бути неефективною проти сучасних загроз, таких як скімінг, фішинг та шкідливе програмне забезпечення.

Так, наприклад, у травні 2017 року компанія O2 Telefónica, німецький оператор мобільного зв'язку, підтвердила, що кіберзлочинці використовували уразливості SS7 для обходу двофакторної автентифікації на основі SMS, щоб зробити несанкціоноване вилучення з банківських рахунків користувачів. Злочинці заразили комп'ютер власника облікового запису з ціллю викрасти облікові дані та номери телефонів банківського рахунку. Потім хакери придбали доступ до підробленого постачальника послуг зв'язку та налаштували переадресацію з номера телефону жертви на свій телефон. В результаті злочинці ввійшли в інтернет-рахунки жертв та зробили переказ коштів на свої рахунки. SMS-коди автентифікації були переадресовані на телефонні номери зловмисників, тому після цього вони легко отримали доступ до грошей.

Не зважаючи на це, сайти та сервіси дуже повільно відмовляються від SMS-автентифікації, на користь автентифікації за допомогою програмного забезпечення, що сильно зменшує загальну безпеку системи. Поки SMS використовується як варіант двофакторної автентифікації, ми ще не раз побачимо подібні атаки.

Серед усіх способів автентифікації, які зараз використовуються, найбільш безпечним є автентифікація за допомогою програмного забезпечення. Тому саме цей спосіб автентифікації рекомендується використовувати для захисту своїх даних на різних сайтах та сервісах.

Список використаних джерел

1. *Багатофакторна автентифікація [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Багатофакторна_автентифікація*
2. *Two-factor authentication: What you need to know (FAQ) [Електронний ресурс]. – Режим доступу: https://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq*
3. *This is why you shouldn't use texts for two-factor authentication [Електронний ресурс]. – Режим доступу: https://www.theverge.com/2017/9/18/16328172/sms-two-factor-authentication-hack-password-bitcoin*

УДК 004.451

Пашинських В. В.
Центральноукраїнський національний технічний університет

Огляд інструментів для пентестинга

В кібербезпеці часто використовують тест на проникнення — це метод оцінки рівня захищеності комп'ютерної системи чи мережі шляхом моделювання дій зовнішніх зловмисників (які не мають авторизованих засобів доступу до системи) і внутрішніх зловмисників (які мають певний рівень санкціонованого доступу) з проникнення у неї. Процес охоплює активний аналіз системи з виявлення потенційних вразливостей, що можуть виникати внаслідок некоректної конфігурації системи, відомих і невідомих дефектів апаратних засобів та програмного забезпечення, чи оперативного відставання в процедурних або технічних контрзаходах протидії. Оцінка рівня захищеності проводиться з позиції потенційного нападника і може включати активне використання вразливостей.

Для полегшення роботи пентестери використовують спеціальне програмне забезпечення, яке дозволяє проводити тестування на проникнення. Виконано аналіз функціональності найбільш розповсюджених програмних засобів, які використовується для проведення тестування на проникнення.

Netsparker. Netsparker - це дуже точний автоматизований сканер, який визначає такі вразливі, як SQL Injection та Cross-Site Scripting у веб-додатках та API веб-сайтів. Netsparker використовує унікальний механізм перевірки виявлених вразливостей, підтверджуючи, що вони реальні, а не помилкові. Тому вам не доведеться витрачати час на перевірку знайдених вразливостей вручну після завершення сканування. Він доступний як програмне забезпечення для ОС Windows та як онлайн-сервіс.

Acunetix. Acunetix - це повністю автоматизований сканер веб-уразливостей, який виявляє понад 4500 уразливостей веб-додатків, включаючи всі варіанти SQL Injection та XSS. Він значно допомагає пентестеру шляхом автоматизації завдань, які можуть забирати багато часу при тестуванні вручну, забезпечуючи точні результати без помилкових спрацьовувань при максимальній швидкості. Acunetix повністю підтримує HTML5, JavaScript та односторінкові додатки, а також системи CMS.

Metasploit. Це найдосконаліша і популярніша платформа, яку можна використовувати для тестування на вразливості. Вона заснована на концепції "exploit", що являє собою шкідливий код, який може обходити заходи безпеки та входити в певну систему. Якщо він входить в систему, він виконує "payload" - код, який виконує операції на цільовій машині, створюючи таким чином ідеальну основу для тестування проникнення. Вона може бути використаний у веб-додатках, мережах, серверах і т. д. Metasploit працює як у консолі, так і з графічним інтерфейсом на таких операційних системах GNU/Linux, Apple Mac OS X і Microsoft Windows.

Wireshark. Це вільне програмне забезпечення для аналізу мережевих пакетів і комп'ютерних мереж. Розпізнає структуру різноманітних мережевих протоколів, і за допомогою цього дозволяє розібрати пакет, відображаючи значення кожного поля протоколу будь-якого рівня. Він може використовуватися в операційних системах Windows, GNU/Linux, OS X, FreeBSD, Solaris та багатьох інших. Інформація, яка завантажується за допомогою цього інструмента, може бути переглянута за допомогою графічного інтерфейсу або утиліти TShark у режимі TTY.

Nessus. Nessus також є сканером. Це один з найбільш надійних інструментів ідентифікації вразливостей. Він здатен виявити найпоширеніші види вразливостей, серед яких: помилки в конфігурації, наявність вразливих версій служб або доменів, наявність паролів за замовчуванням, а також порожніх, або слабких паролів.

Burpsuite. Burpsuite також є по суті сканером (з обмеженими інструментами для атак). Для багатьох пентестерів це програмне забезпечення є дуже важливим, оскільки воно має багатий функціонал. Burpsuite - це комерційний продукт, тому для використання його слід купити. Також є безкоштовна версія, але з дуже обмеженим функціоналом. Цей інструмент працює на операційних системах Windows, Mac OS X і Linux.

Cain & Abel. Якщо Вам потрібно працювати зі зломом паролів або мережевих ключів, Вам слід звернути увагу на це програмне забезпечення. Воно використовує аналізатор трафіку, словники, метод «грубої сили», криптоаналіз та методи аналізу протоколів маршрутизації для досягнення цілі. Cain & Abel доступне ексклюзивно для операційної системи Microsoft Windows.

John The Ripper. John The Ripper - це ще одне програмне забезпечення для злому паролів. Цей інструмент працює на більшості операційних систем, але призначене, в першу чергу, для операційних систем UNIX. Вважається найбільш швидким інструментом серед своїх аналогів. Входить в склад таких дистрибутивів GNU/Linux, як Parrot Security OS та Kali Linux. Цей інструмент доступний у вигляді двох версії, одна з яких є безкоштовною.

Nmap. Network Mapper - безкоштовне програмне забезпечення для дослідження та аудиту безпеки комп'ютерних мереж та виявлення активних мережевих сервісів. З 1997 року став стандартом в галузі інформаційної безпеки. Переважно допомагає дізнатися характеристики будь-якої мережі, такі як хост, сервіси, операційні системи, фільтри пакетів/брандмауери, тощо. ПЗ доступне для більшості операційних систем.

BeEF. BeEF (The Browser Exploitation Framework) - це інструмент для тестування на проникнення, який зосереджується на веб-браузері, і використовує ідею, що відкритий веб-браузер є вікном у цільову систему та дозволяє через нього проводити атаки.

Це програмне забезпечення має графічний інтерфейс та працює на операційних системах GNU/Linux, Apple Mac OS X і Microsoft Windows.

У підсумку слід зазначити, що перелік програмного забезпечення аудиту кібербезпеки достатньо великий і спеціаліст може обрати найбільш відповідний конкретній інформаційній системі. Але всі ці засоби має супроводжувати і налаштовувати спеціаліст з кіберзахисту з відповідним рівнем кваліфікації, інакше навіть найпотужніша система захисту не гарантує безпеку.

Список використаних джерел

1. *Тест на проникнення [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Тест_на_проникнення*
2. *Kali Linux Penetration Testing Tools [Електронний ресурс]. – Режим доступу: https://tools.kali.org/*
3. *Эриксон Дж. Хакинг: искусство эксплойта. 2-е издание. – Пер. с англ. – СПб.: Символ-Плюс, 2010. – 512 с.*

УДК 354.42

Поліщук О. В., Карабут Н. О.
Криворізький національний університет

Кібертероризм як глобальна проблема

З кожним днем інтернет все більше і більше збільшується в своїх масштабах. Створюється величезна кількість сайтів і онлайн-сервісів, для надання різного роду інформації. Вони відкривають нові можливості в комунікації і передачі знань на великі відстані.

В дозвіллі - сервіси надають різний медіаконтент; в освіті – з'являються різні електронні бібліотеки, електронні навчально-методичні комплекси, цифрові навчальні ресурси; у медицині – електронні картотеки пацієнтів, електронне отримання талонів до фахівців, проводити лікарям онлайн-семінари; в культурі – забезпечується більш широкий доступ до провадженням і явищ мистецтва; на виробництві створюються нові та зручні системи управління та обліку продукції. Однак, цей процес не завжди несе в собі позитивні моменти. Все залежить від точки зору.

Надмірна доступність, слабкий контроль за даними і можливість обходу величезної кількості заборон роблять інтернет дуже зручним інструментом, для різних угруповань, що мають терористичний характер. З кожним днем їх активності і вплив в мережі збільшується в геометричній прогресії, народжуючи нову глобальну проблему - кібертероризм.

Через це багато держав і міжнародних організацій, а зокрема ООН, приділяють велику увагу, видаючи різні укази і правові документи, що закликають до розробки заходів по боротьбі з новою світовою загрозою.

Кібертероризм є глобальна міжнародна проблема, що вимагає активної розробки заходів для її вирішення.

Атаки з боку обчислювальних систем і мереж мають стихійний і непередбачений характер. Практично неможливо передбачити звідки і в якому вигляді буде виходити загроза, що зменшує шанси на її усунення. Основна складність даної проблеми, полягає не в створенні і розборі комплексних систем дій, спрямованих на її вирішення, а в самому її визначенні. Це пов'язано з тим, що кібертероризм не постійний. Він не має чіткої і кінцевої форми, а багато його прояви мають суто індивідуальний характер.

Кібертероризм, це - сукупність дій, що створюють загрозу безпеки особі, суспільству та державі, через мережу інтернет, зі зміною наявної інформації, для отримання переваги при вирішенні політичних, економічних або соціальних завдань, несучих терористичний характер.

Відмінна риса даного виду терору полягає у використанні різних програмних і апаратних засобів, для реалізації своїх цілей. Вони можуть бути представлені, як комп'ютерні віруси або троянські програми, здатні тільки надати різну інформацію з віддалених мереж і машин, але і порушувати їх роботу. Так само це можуть бути спеціалізовані комп'ютерні обчислювальні станції, основна мета яких здійснювати кібератаки на різні інформаційні ресурси і сервіси, з подальшим виведенням їх з ладу.

В основному, даний вид діяльності спрямований на країни, інфраструктура яких безпосередньо пов'язана з комп'ютерними мережами. В першу чергу, її можна помітити по відношенню до державних або комерційних банківських систем, що завдає серйозного удару по фінансових і економічних галузях. Другими в цьому списку є різні рекламні агентства і ЗМІ.

Проблема тут полягає в тому, що вони є всеохоплюючими інформаційними джерелами, які ніколи не були захищені від кібератак належним чином. Дана ситуація робить з них ідеальних посередників між терористами і їх жертвами, дозволяючи першим залишатися непоміченими, видаючи за себе різні станції телерадіомовлення або редакції газет, що розповсюджуються через мережу інтернет.

За останні роки інтерес до урядових структур у злочинців у сфері комп'ютерних мереж зріс у кілька разів. Їх основними цілями була різна секретна документація. Так само їм були цікаві різні наукові розробки, при цьому особливий інтерес викликали саме ті, які були пов'язані зі збройними силами або військовими структурами.

У сукупності це дозволяє представити, кібертероризм, як одне із завдань, що вимагає швидкого і кардинального рішення.

Особливість полягає в тому, що багато експертів в області мережевої та комп'ютерної безпеки, описують пошук методів для боротьби з цією проблемою, як непередбачуваний у своєму протіканні процес. Вони говорять про те, що неможливо створити комп'ютерну обчислювальну систему, здатну повністю бути захищеною від різного роду злому або хакерських атак. Це пов'язано з тим, що яким би великим не був професіоналізм фахівця з безпеки комп'ютерних мереж, завжди є ймовірність що він не помітив маленький пролом у захисті, який зможуть знайти зловмисники.

Ситуацію посилює ще той факт, що багато кіберзлочинців не залишаються на одному і тому ж рівні своїх можливостей. Вони розвиваються, знаходять або розробляють нові способи злому, стають спритнішими і розумними, що ще сильніше ускладнює боротьбу з ними.

Так само фахівці доповнюють, що можливо ця проблема буде актуальною ще довгий час, а точніше до тих пір, поки буде існувати простір для розвитку комп'ютерних технологій. Вони аргументують це тим, що кожна перемога кіберзлочинців, це теж маленький крок у розвитку обчислювальних систем, хоч несе в собі деструктивну функцію. Тому, єдиним кардинальним рішенням є, відмова від комп'ютерів та технологій, які вони нам подарували, але до такого сучасне суспільство ще не готове.

Таким чином ситуація з тероризмом в мережах приймає особливе становище. Через її великий темп розвитку, все більше держав починають визнавати його, як одну з найважливіших проблем сучасного світу, для ліквідації якої потрібна ефективна співпраця всіх країн. У зв'язку з цим, запобігання злочинів в цифровому середовищі і ліквідація їх наслідків мають дійсно глобальне значення.

Список використаних джерел

1. *Домарев В. В. Безопасность информационных технологий. Методы создания систем защиты. — К.: ООО ТИД ДС, 2001. — 688 с.*
2. *Бєляков, К. І. Проблеми законодавчого регулювання у сфері користування інформацією з обмеженим доступом в Україні / К.І. Бєляков, Ю.П. Мірошник // Стратегічна панорама. – 2004. – № 3. – С. 171-177.*
3. *Дубов Д. В. Стратегічні аспекти кібербезпеки України / Дубов Дмитро Володимирович // Стратегічні пріоритети. – 2013. – № 4. – С. 119-126. – Бібліогр.: с. 125-126*
4. *Рудник Л. І. Право на доступ до інформації: дис. канд. юрид. наук : спец. 12.00.07 «Адміністра- 219 2/2017 ІНФОРМАЦІЙНЕ ПРАВО тивне право і процес; фінансове право; інформаційне право» / Людмила Іванівна Рудник ; Національний університет біоресурсів і природокористування України. – К., 2015. – 247 с. 11.*
5. *Скулиш Є. Д. Фактори впливу на формування системи інформаційної безпеки в Україні / Є. Д. Скулиш // Інформаційна безпека людини, суспільства, держави. – 2011. – № 2 (6). – С. 22–26.*

УДК:004.056.53

Стрілець А. М.
Харківський національний університет радіоелектроніки

Основні технології проти кіберзлочиності

Ми живемо в епоху інформаційного суспільства, коли комп'ютери і телекомунікаційні системи охоплюють всі сфери життєдіяльності людини і держави. Через постійно зростаючий обсяг обміну інформаційними даними в Інтернеті та електронні платежі кіберзлочинність стала приваблювати багатьох легкою наживою. Тому за останні десятиріччя із швидким розвитком інформаційних і комп'ютерних технологій та через популяризацію користування інтернет-технологіями у всіх сферах життя (від покупок через Інтернет до звичайних розваг) зростає та розвивається злочинність у цій сфері. Кіберзлочинність та хакери, комп'ютерний злом – це слова, якими вже нікого не здивуєш. Проблеми щодо протидії злочинам у сфері використання комп'ютерної техніки наразі активно обговорюються науковцями всього світу, досить швидко розвивається практика застосування відповідних технічних засобів і норм законодавства про кримінальну відповідальність.

Історія навчила нас, що розвиток і прогрес, які приносять людям нові блага та можливості, на жаль, завжди супроводжуються негативними явищами. Індустріалізація дала нам масове виробництво товарів, але вона ж поклала початок варварському винищенню природи і класовій нерівності. Боротьба за національні та соціальні права зробила аксіомою принципи рівності і справедливості, але часто призводить до кровопролиття і негативних проявів патерналізму.

І нажаль у наші часи з розвитком і поширенням комп'ютерних технологій, комп'ютерні злочини стали однією з найдинамічніших груп суспільно небезпечних посягань. Дуже швидко збільшуються показники поширення цих злочинів, а також постійно зростає їх динаміка та небезпечність. Звісно, це зумовлено прискореним розвитком науки та технологій у сфері комп'ютеризації, а також постійним і стрімким розширенням сфери застосування комп'ютерної техніки. Сьогодні жертвами злочинців, що орудують в віртуальному просторі, можуть стати не тільки люди, а й цілі держави. При цьому безпека тисяч користувачів може виявитися в залежності від декількох злочинців. Кількість злочинів, скоєних в кібер-просторі, зростає пропорційно числу користувачів комп'ютерних мереж, і, за оцінками Інтерполу, темпи зростання злочинності, наприклад, в глобальній мережі Інтернет, є найшвидшими на планеті. Здавалося б, з розвитком інформаційної безпеки повинні прогресувати способи, що дозволяють контролювати кіберзлочинність. Але система протидії злочинним посяганням на безпеку у сфері комп'ютерних та інформаційних правовідносин помітно відстає у своєму розвитку. Відповідно до щорічного звіту про кіберзлочинність за 2018 рік, ця проблема буде приносити щорічні збитки на суму 6 трильйонів доларів США вже до 2021 року. Ця цифра в два рази більше аналогічної за 2015 рік - 3 трильйони.

Що стосується самих проявів кіберзлочинності, їх безліч, починаючи від атак зловмисників, закінчуючи DDoS-атаками. Уряду і компанії, що займаються кібербезпекою, всіма силами намагаються протистояти кіберзлочинності, на даний момент існує безліч способів запобігти більшості форм кібератак. Однак основна проблема полягає в тому, що більшість організацій не дотримуються навіть основних заходів забезпечення безпеки, серед яких відновлення використовуваних програм. Мережа рясніє різними ресурсами, присвяченими способам протидії кібератакам, крім цього, такі технології, як блокчейн і машинне навчання надають нові можливості захисту від кіберзагроз. Розглянемо технології, які допоможуть перемогти кіберзлочинність.

1. *Запобігання 0-day-атак*. Даний термін застосовують щоб визначити не усунутий уразливості, що не знайдені розробниками «дірки» в програмному коді на стадії тестування. А також шкідливі програми, віруси, мережеві черв'яки, боти і трояни проти яких ще не розроблена хоч якогось захисту.

Із самої назви зрозуміло, що у розробників не було ні дня, тобто, не було ніякої можливості виправити помилки і прорахунки в коді, вони про них просто не знали. Про уразливості стає загальновідомо відомо до того моменту, коли виробник програмного забезпечення випустить оновлення з виправленням, або нову версію програми. Тобто до цього моменту, всі комп'ютери, що працюють з цим ПО наражаються на небезпеку. І навіть антивірус і брандмауер в звичайному вигляді не зможуть допомогти підприємству захиститися від таких атак. Є, звичайно, поведінкові аналізатори, однак і вони не здатні гарантувати повну захищеність. У 0-day-атаках кіберзлочинці використовують експлойти, які експлуатують уразливості в програмах, про які або ще невідомо, або не розроблені патчі, що усувають їх. Серед знаменитих шкідливих програм, що використовують проломи нульового дня, відзначився троян Troiton, націлений на основні промислові системи на Близькому Сході. На сьогоднішній день підприємства і організації в області кібербезпеки розглядають машинне навчання як довгострокове рішення проблеми атак нульового дня. Є навіть конкретний приклад – система, створена командою університету штату Арізона. Завдання цієї системи полягає в тому, щоб моніторити сайти «глибокої мережі» (deep web), на яких продаються експлойти. Використовуючи машинне навчання, дослідники фіксували щотижня в середньому 305 високопріоритетних попереджень про загрози. Машинне навчання та штучний інтелект також стали основними технологіями Chronicle, нової компанії з кібербезпеки, організованої Google X. Керівник Google X Астро Теллер описує нове відгалуження як «цифрову імунну систему», Chronicle буде фокусуватися на виявленні загроз на великих підприємствах шляхом зберігання і аналізу даних, пов'язаних з безпекою. Використовуючи інфраструктуру Google, компанія зможе швидше виявляти загрози та робити це в більш широких масштабах, ніж існуючі системи. Chronicle позиціонується як активна платформа запобігання та аналізу кіберзагроз. Її функціонування було б неможливим без будь-якої форми машинного навчання, що використовується в якості основи.

2. *Самостійна ідентифікація (Self-sovereign identity)*. Завдяки тому, що в Мережі з'явилося безліч онлайн-сервісів і державних онлайн-послуг, які збирають особисту і фінансову інформацію громадян, стало можливим таке поняття, як «крадіжка особистості» (Identity theft). Таким чином, споживачі кожного року зазнають десятки мільярдів доларів збитків через «крадіжки особистості». Одними з найпопулярніших способів крадіжки особистості є всім добре знайомі фішинг, веб-спуфинг і скімінг. Однак найбільш дієвим способом є компрометація великого сховища, що зберігає величезну кількість даних користувачів. Одним з останніх інцидентів, які мали великий резонанс, в якому була задіяна крадіжка особистих даних, був злом американського бюро кредитних історій Equifax. Нагадаємо, що тоді за результатами проведеного дослідження було встановлено, що потенційно постраждали в цілому 145,5 млн споживачів США. У цій ситуації на допомогу можуть прийти такі технології блокчейн, як Decentralized.id (DID), що дозволяють користувачам зберігати особисту інформацію в децентралізованому публічному записі. Щоб скористатися послугами і отримати доступ до даних, громадянам потрібно буде підтвердити свою особу за допомогою особистого пристрою. Припустимо, що ви зареєструвалися в сервісі абонентських послуг. Традиційно дані вашого профілю будуть зберігатися в базі даних компанії, вам залишаться тільки ваші облікові дані для доступу (логін-пароль). Модель self-sovereign

identity дозволяє зберігати дані в незмінному блокчейне, доступ до якого можна отримати через приватний пристрій. Така інформація, як водійські права або банківський рахунок зберігається в зашифрованому вигляді, а платформи на зразок DID дозволяють управляти вашими ідентифікаторами і використовувати їх для різних транзакцій, наприклад, для входу в веб-сервіси або покупок.

3. *Протидія DDoS-атакам*. DDoS-атаки (Distributed Denial of Service attack) є найпоширенішою формою кібератак, експерти припускають, що в цьому році вони все ще будуть серйозною загрозою для бізнесу. Говорячи простою мовою, DDoS-атаки - це деякий вид зловмисної діяльності, що ставить собі за мету довести комп'ютерну систему до такого стану, коли вона не зможе обслуговувати правомірних користувачів або правильно виконувати покладені на неї функції. При DDoS-атаці відбувається розподілене напад на IT-систему організації для того, щоб довести її до відмови. В такому випадку легальні користувачі системи не можуть отримати доступ до її ресурсів, або цей доступ ускладнений, також таким чином можна, наприклад, «обрушити» Інтернет-магазин конкурентів. Адже на його відновлення може піти чимало часу, а це – втрачений потенційний прибуток. Крім втрати доходів, ця кіберзагроз може створити вікно для подальших порушень, наприклад витоку даних і зараження шкідливими програмами. Результатом може стати незворотня шкода, нанесена репутації компанії. За даними «Лабораторії Касперського», постачальники послуг DDoS-as-a-service отримують до 95 відсотків прибутку на веб-ринках «глибокої мережі». На щастя, в даний час таким атакам можна протидіяти за допомогою спеціальних сервісів, наприклад Cloudflare. Крім цього, існують послуги веб-хостингу, які забезпечують захист від DDoS на рівні мережі, а також дозволяють блокувати трафік з підозрілих джерел та багато інших дієвих методів.

Таким чином, кіберзлочинність - це проблема, з якою зіштовхнулась планета у 21 столітті, і яка обіцяє рости та поглинати все більше коштів. Незважаючи на усі заходи, що їх приймають окремі особи, фірми, а також держава, кіберзлочинність продовжує свою діяльність, збільшуючи прибутки порушників та зменшуючи вміст кишень пересічних громадян. Насамперед, причиною популярності та стрімкого зростання кіберзлочинності як бізнесу є його неймовірна прибутковість, а також те, що успіх справи не пов’язаний з великим ризиком. Прибутки, які отримують кіберзлочинці за декілька секунд чи хвилин, можуть перевищувати мільйони доларів. Тому сьогодні особливо важливо переглянути усі існуючі заходи та активно розробляти нові, що принесуть більшу користь та надійніший захист від кіберзлочинців. У зв’язку з цим хотілося б, щоб Україна, як одна з країн, в якій активно використовуються інтернет-технології та кількість користувачів постійно зростає, мала у своєму розпорядженні активні способи захисту і протидії кіберзлочинності й активно готувала кваліфікованих спеціалістів, А відмічені вище три технології допоможуть експертам ударити по кіберзлочиності і, можливо, з часом подолати основні її прояви.

Список використаних джерел

1. *Кіберзлочинність [Електронний ресурс]*. – Режим доступу: *https://n-auditor.com.ua/uk/component /na_archive/695.html?view=material*
2. *Бутузов В. М. Протидія комп’ютерній злочинності в Україні (системно-структурний аналіз) : монографія / В. М. Бутузов. – К. : КИТ, 2010. – 408 с.*
3. *Погорецький М. Кіберзлочини: до визначення поняття / М. Погорецький, В. Шеломенцев // Вісник прокуратури. — 2012. — № 8. — С. 89-96.*
4. *Кіберзлочинність в Україні [Електронний ресурс] :−Режим доступу: https://www.sciencecommunity.org /node/16132.*

УДК 004.056

Хлистун В. В.
Центральноукраїнський національний технічний університет

Кіберзлочинність як загроза для кожного: види, причини розвитку, поради до протидії загрозам

Сучасний стан розвитку телекомунікаційних, інформаційних та комп'ютерних технологій обумовлює появу та швидкий розвиток суспільних відносин з приводу їх використання. Це вимагає їх правову регламентацію, яка відповідала б інтересам суб'єктів таких відносин та економічній доцільності використання предметів, що уособлюють в собі подібні технології. Більше того, інформаційні технології та комп'ютерні мережі на сьогодні являють собою важливу галузь економіки, розвиток якої виходить за межі економіки однієї країни і характеризується наявністю усталених міжнародних зв'язків [1].

Так сформований віртуальний простір який можна визначити як простір, що моделюється за допомогою комп'ютера, у якому перебувають відомості про особи, предмети, факти, події, явища і процеси, які відбуваються у локальних і глобальних комп'ютерних мережах, або відомості, що зберігаються в пам'яті будь-якого фізичного або віртуального устрою, а також іншого носія, спеціально призначеного для їхнього зберігання, обробки й передачі. Можна зазначити, що кіберзлочинність - це злочинність у так званому «віртуальному просторі» [2].

Що стосується України, то можна зазначити, що останнім часом рівень кіберзлочинності швидко зростає в Україні. Експерти зазначають, що Україна - дуже важливий центр хакерства, поряд із Бразилією, Китаєм та меншою мірою - Індією. У цих країнах досить освічене молоде населення, високий рівень безробіття та обмежені можливості працевлаштування [3].

Об'єктом кіберзлочинів може стати будь-який користувач інтернету. Найпоширенішими видами таких злочинів є [4]:

- кардинг — використання в операціях реквізитів платіжних карт, отриманих зі зламаних серверів інтернет-магазинів, платіжних і розрахункових систем, а також із персональних комп'ютерів (або безпосередньо, або через програми віддаленого доступу, «трояни», «боти»).
- фішинг — вид шахрайства, відповідно до якого клієнтам платіжних систем надсилають повідомлення електронною поштою нібито від адміністрації або служби безпеки цієї системи з проханням вказати свої рахунки та паролі.
- вішинг — вид кіберзлочинів, у якому в повідомленнях міститься прохання зателефонувати на певний міський номер, а при розмові запитуються конфіденційні дані власника картки.
- онлайн-шахрайство — несправжні інтернет-аукціони, інтернет-магазини, сайти та телекомунікаційні засоби зв'язку.
- піратство — незаконне розповсюдження інтелектуальної власності в Інтернеті.
- кард-шарінг — надання незаконного доступу до перегляду супутникового та кабельного TV.
- соціальна інженерія — технологія управління людьми в Інтернет-просторі.
- мальваре — створення та розповсюдження вірусів і шкідливого програмного забезпечення.
- протиправний контент — контент, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості і насильства.
- рефайлінг — незаконна підміна телефонного трафіку.

Основною причиною розвитку кіберзлочинності, як і будь-якого бізнесу, є прибутковість, – вона неймовірно прибуткова. Величезні суми грошей з'являються в кишенях злочинців у результаті окремих великих афер, не говорячи вже про невеликі суми, які йдуть просто потоком. Друга причина росту кіберзлочинності як бізнесу - те, що успіх справи не пов'язаний з більшим ризиком.

У реальному світі психологічний аспект злочину припускає наявність деяких коштів стримування. У віртуальному світі злочинці не можуть бачити своїх жертв, будь те окремі люди або цілі організації, які вони вибрали для атаки. Грабувати тих, кого ти не бачиш, до кого не можеш дотягтися рукою, набагато легше[4].

Експерти говорять про тривожну тенденцію: за останні роки кіберзлочинність стала більш організованою і почала мати форму бізнесу. Дії хакерів орієнтовані на отримання довгострокового доходу. Більше того, до збитків компаній можна віднести не лише пряму втрату від дій хакерів, але і витрати на оборону від кібератак.

Існує декілька порад щодо того, як вберегти себе від кіберзлочинів:

- створення надійних паролів, захист інформації та періодична їх зміна;
- поінформованість про розповсюджені прийоми, які використовують злочинці для того, щоб розпізнавати їх;
- захист пристроїв, встановлення антивірусних програм;
- використання захищених мереж
- перевірка своїх облікових записів
- використання інструментів конфіденційності та безпеки Google чи інших браузерів.

Підсумовуючи вищевикладене, можемо дійти таких висновків:

- поширеність і суспільна небезпечність кіберзлочинів останніми роками набула загрозливих масштабів, що диктує необхідність формування адекватної відповіді з боку держави;
- вивчення зарубіжного досвіду протидії кіберзлочинності в окремо взятих країнах і надбань міжнародної спільноти, удосконалення механізму міжнародної взаємодії є важливим, адже більшість кіберзлочинів мають транснаціональний характер;
- кіберзлочинність сьогодні становить загрозу не тільки національній безпеці окремої держави, а загрожує людству загалом, саме тому зазначеній проблемі приділяється значна увага в багатьох державах;
- з огляду на сучасну ситуацію в державі та світі, Україна має постійно вдосконалювати методи боротьби з кіберзлочинністю, удосконалюючи чинне законодавство, у т. ч. в галузі адміністративного права, враховуючи над¬бання окремих зарубіжних держав, міжнародної спільноти загалом, спрямовані на забезпечення кібербезпеки країни;
- важливим є прийняття Закону, який би врегулював основні засади забезпечення кібербезпеки України.

Список використаних джерел

1. *Гринчак І. В. Кіберзлочинність як злочин міжнародного характеру. Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького . 2015. № 12, с. 93-98.*
2. *Біленчук Д.П. Кібрешахраї – хто вони? Міліція України. 1999. №7-8, с.32-34.*
3. *Ковальов С.С., Форос Г.В. Кіберзлочинність в україні – як новий вид злочинності. Актуальні питання протидії правопорушенням у сфері використання інформаційно-телекомунікаційних систем : матеріали науково-практичної інтернет-конференції, м. Одеса, 28 жовтня 2016 р.. м. Одеса, 2016, с. 62-64.*
4. *Марков В. В. Щодо питання стосовно зарубіжного досвіду протидії кіберзлочинності. Національний юридичний журнал:теорія і практика. 2015, с. 187-191.*
5. *Кіберзлочинність у всіх його проявах: види, наслідки та способи боротьби. URL: https://www.gurt.org.ua/articles/34602/*

УДК 004.056.53

Шостак В. І.
Національний авіаційний університет

Захист інформаційних ресурсів та засобів обробки інформації

Інтернет полегшує сучасний темп життя людини, відкриваючи нові можливості у всіх аспектах нашого життя. В інтернеті ми шукаємо потрібну інформацію, банки, магазини, завдання для саморозвитку, ігри та спілкуємося з друзями через соціальні мережі. В результаті наші пристрої містять дуже багато конфіденційної інформації. Це може бути паролі від інтернет-банкінгу, соціальних мереж, програм та медіа-ресурси, які ми хочемо захистити. Якщо пристрої не захищені до вашої інформації можуть отримати доступ злодії та інші шахраї, які зможуть використати вашу інформацію для своєї користі. Наприклад, спамери зможуть використати комп'ютер для відсилання різної інформації від вашого імені - це може бути як прохання позичити гроші, так і розсилання вірусів для злому інших людей. Шкідливі віруси або шпигунські програми можуть зберігатися на вашому комп'ютері, сповільнювати його, заробляти гроші на вашому обладнанні чи знищувати файли.

Використовуючи нижчезазначені поради, ви можете захистити ваші інформаційні ресурси:

- Зберігати пристрої безпечно, а саме: вчасно завантажувати рекомендовані оновлення від постачальника операційних систем, особливо для важливих програм, таких як інтернет-браузер; встановлювати антивірусне програмне забезпечення та використовувати брандмауер, що є важливими інструментами для запобігання нападам на ваш пристрій.

- Використовувати антишпигунське програмне забезпечення. Шпигунське програмне забезпечення - це встановлене без вашого відома та згоди, яке може контролювати ваші дії в Інтернеті та збирати особисту інформацію, коли ви знаходитесь в Інтернеті. Деякі види програм-шпигунів, звані клавіатурними шпигунами, записують все що ви вводите, включаючи ваші паролі. Захист від шпигунських програм включений в антивірусні програми, за потреби ви маєте можливість перевірити чи у вас активована ця функція. Щоб уникнути шпигунського програмного забезпечення, завантажте програмне забезпечення лише з сайтів, які ви знаєте та довіряєте.

- Використовувати брандмауери. Брандмауер - це програма або апаратне забезпечення, яке блокує хакерів від входу та використання вашого комп'ютера. Хакери шукають в Інтернеті те, як деякі магазини автоматично набирають випадкові номери телефонів. Вони відправляють пінг на десятки комп'ютерів і чекають відповідей. Брандмауер забороняє відповідати вашому комп'ютеру на ці випадкові виклики. Деякі операційні системи мають вбудовані брандмауери, які можуть бути відправлені в режим «вимкнено». Не забудьте включити брандмауер. Щоб все працювало ефективно, брандмауер повинен бути належним чином налаштований та регулярно оновлюватися.

- Використання складних паролів та надійним методом автентифікації допоможе зберегти вашу особисту інформацію.

- Захистіть свої пристрої та облікові записи від вторгнень, вибираючи паролі, які важко здогадатися. Використовуйте сильний пароль, щонайменше вісім символів, комбінація букв, цифр та спеціальних символів. Не використовуйте слово, яке можна легко знайти в посиланні на особисту інформацію, наприклад день народження, прізвище, номер телефону. Деякі хакери використовують програми, які можуть

спробувати кожне слово в словнику та легко знайти особисту інформацію, таку як дату народження. Спробуйте використати фразу, яка допоможе вам запам'ятати свій пароль, використовуючи першу букву кожного слова у фразі. Виберіть унікальні паролі для кожного інтернет-банкінгу та соціальних мереж, які ви використовуєте. Якщо у вас забагато паролів для запам'ятовування, скористайтеся програмним забезпеченнями для керування паролями або запишіть в нотатку.

- Використовуйте сильнішу автентифікацію. Багато сайтів дозволяють використовувати більш ефективні методи автентифікації. Ці методи можуть мати в собі використання відбитків пальців, одноразові коди(2FA), надіслані на мобільний пристрій або інші функції, що забезпечують, те що користувач повинен мати доступ до облікового запису.

- Захистіть вашу особисту інформацію. Під час перевірки електронної пошти, відвідування веб-сайтів, публікації в соціальні мережі або покупки звертайте увагу на те, куди ви натискаєте і про кого ви надаєте інформацію. Недобросовісні веб-сайти можуть спробувати змусити вас надавати їм ваші особисті дані.

- Будьте обережні та слідкуйте, що ви натискаєте. Фішингові атаки, де хакери відправляють повідомлення, щоб змусити вас передавати особисту інформацію стають все більш витонченими. Наприклад, ви можете отримати термінове повідомлення про те, що ваш банківський рахунок заблоковано, і вам потрібно ввести свій пароль та номер, щоб розблокувати його. Подумайте двічі, перш ніж натискати посилання в таких повідомленнях як цей приклад. Більшість справжніх повідомлень від фінансових установ не вимагатимуть особистої інформації безпосередньо, але замість цього наказують вам зателефонувати або відвідати веб-сайт безпосередньо. Ви також можете підтвердити адресу електронної пошти, надіслану повідомлення, щоб переконатися, що вона надійшла від очікуваного відправника.

- Будьте обережні з публікаціями в мережах. Соціальні мережі дозволяють ділитися всіма аспектами життя, але важливо контролювати, те хто має доступ до інформації, яку ви публікуєте. Зловмисники можуть використовувати публікації соціальних мереж для збору інформації, а потім використовувати інформацію для зламання в банківських рахунках або для крадіжки особистих даних. Щоб захистити себе, використовуйте налаштування конфіденційності, щоб обмежити видимість особистих публікацій у ваших мережах та обмежувати кількість інформації, яку ви публікуєте для всіх.

Незважаючи на всі вище перераховані способи захисту інформації на вашому пристрої, це не гарантує захист інформації від несанкціонованого доступу чи викрадення. Якщо ви виявите, що ваша особисті дані були викрадені без вашої авторизації, необхідно вжити заходи для свого захисту. Розмістіть сповіщення про шахрайство у своєму профайлі, перегляньте свої кредитні звіти, проскануйте свій пристрій на віруси, змініть паролі на всіх веб-сайтах, які зберігають найважливішу інформацію та при потребі перевстановіть операційну систему. Якщо ви підозрюєте що було порушено доступність, цілісність чи конфіденційність інформації, зафіксуйте та зателефонуйте на гарячу лінію вашого банку, щоб запобігти шахрайства деактивуйте банківські карти і відкрийте нові.

Список використаних джерел

1. Е. Баранова, А. Бабаш «Информационная безопасность и защита информации» 3-е изд. (2016);
2. С. Нестеров «Основы информационной безопасности» (2016);
3. Анин Б. Ю. Защита компьютерной информации. (2000);

UDC 316.776:004.58

Sokolov V. Y., Korzhenko O. Y.
Borys Grinchenko Kyiv University

Analysis of Recent Attacks Based on Social Engineering Techniques

Introduction. The history of attacks based on SE practices is a wave: the victims changed, the different, new at their time, tricks were practiced and still are. The era of SE attacks in the field of IT began in 2014 when the first mass attacks were carried out on individuals, users of the banking payment system. People received calls from fake bank operators who informed about innovations regarding the protection of their data and steps that each and should every pass in order to become more secured. At their request, individuals in conversation gave critical data such as CVV2/CVC2 (3 digits on the back of a bank card) and 4 to 6 digits codes that the operator sent on their smartphones to confirm changes applying during the conversation, also in some cases even card pin-codes. The result of such manipulations as can understood had not given an additional level of protection to users, but rather deprived them of many decent sums of money (see fig. 1).

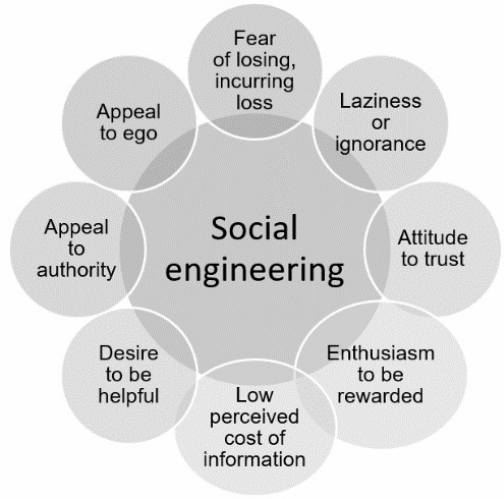


Figure 1 — Exploitation of human behavior

1. Classification and description of known attack methods. In 2015, European Central Bank deputy head of Security and Information Protection admitted that cybercriminals had switched to banks from their clients. The methods were not as advanced as can be seen now, mailing Trojan emails. A bank employee, opening such infected attachment "allows" an attacker to gain access to the account and send a payment order to or from the bank, so in that time the hacker group "Anunak" once attacked more than fifty banks and five payment systems in Ukraine and the countries of the former USSR and was able to steal about 1 billion dollars. Hacker billionaires were found proved guilty and convicted. Banks, in turn, increased protection [1].

Then the trend changed—cyber fraudsters became interested in small and medium-sized businesses, as there was more money on their accounts than on individuals, and protection might be weaker (if there is any) than in large organizations. An additional plus is that such companies often do not have a dedicated information security (IS) unit. As a result, it is enough for hackers to infect the accountant's computer in order to gain access to the accounts. This can be done in several ways that are analyzed further. Infection can occur through resources popular with financial workers. If criminals manage to compromise these sites, they

turn into "hotbeds of infection", as they may contain on their pages a malicious exploit code (a subtype of malware). It uses an open browser vulnerability and establishes a "tunnel" with the user's computer. Through it, a program is loaded into the PC that determines what valuable information is stored on it. And then the "victim" is infected with a virus, specially adapted for antivirus on PC [2].

In 2016, targeted recruitment of insiders began to gain popularity. IS experts have declared the activity of intruders in this direction: more frequent attempts have been made to recruit bank employees, especially those who are part of the economic unit and are able to influence the adoption of certain decisions in the bank. A 2017 report by RedOwl and IntSights confirms the growing demand for insiders on the Dark Web. Employees are recruited purposefully, which greatly reduces the price of an attack: no need to guess how to penetrate the company's network and how to take out the data. For the "percentage from income" this information will provide an insider [3].

In 2017, silent ATM hacks began to gain popularity. When the device itself voluntarily gives money. To carry out such a crime without the help of insiders is extremely difficult. Criminals need information about the device ATM, the software built into it. And the test ATM modules (parts) itself, for training (fig. 2).

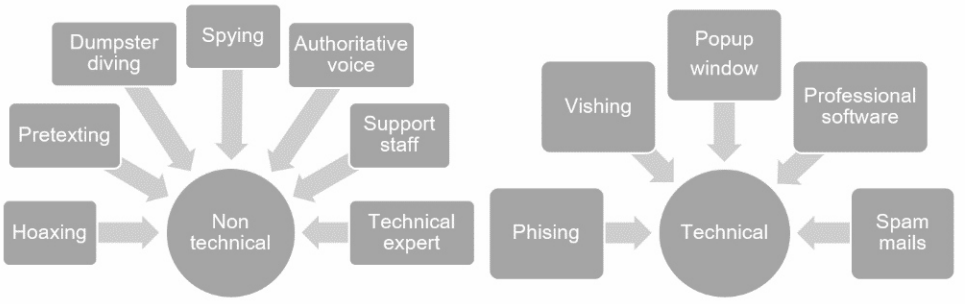


Figure 2 — Attack vectors

Previously, SE techniques united a common goal: the attacker caused obvious damage to the victim—obtaining information, financial damage, spoiled reputation, and demand for ransom. Therefore, it was exactly as long as the world was not overwhelmed with the fever of cryptocurrency mining. Mining promotes a simple idea for the masses: make money out of nothing. All you need to do is take a computer and use its power to "calculate" virtual currency. Currencies, by the way, are offered in abundance. In addition to replicated Bitcoin, today you can "invest with iron" in a dozen alternatives: Monero, litecoin, Zcash and others. But if everything was so simple, we would have been millionaires long ago. Using one computer, mining is economically unprofitable. For simplicity, the situation looks like this: earnings depend on how many hashes per second the processor or video card calculates (what exactly will be used depends on the specific cryptocurrency). For example, Monero is "calculated" by processors. With a performance of 863 kH/sec, you can earn $2,000 equivalent per day. That's just the performance of an Intel Core i5-7400 mid-range processor of about 0.165 kH/sec. This means that in a day at such capacities it will turn out to get as much as 38.3 cents [4].

The new goal of the census (social) engineers is to parasitize on the victim's technique. Of course, this created difficulties and led to an interesting effect—the goal of social engineers evolved. Now in 2018 the main task is not to cause obvious harm to the victim, but to quiet and inconspicuous parasitism on her technique. After all, the longer the virus miner will be on the car of an unsuspecting "donor", the more it "counts". Then revenues soar. Figures in confirmation: in the beginning of 2018 a group of hackers installed malware for the

extraction of cryptocurrency on 9,000 computers via web-sites cookies and, according to analysts, such a network brings its owners up to $30,000 per month [5].

2019th may become the beginning of the era of "friendly" SE. Economically, mining "in the forehead" at its own expense is unprofitable (if not considering specialized devices and farms). Therefore, a new field of activity opens up for social engineers. In theory, mine cryptocurrency is possible on any device that has computing power and access to the Internet. Moreover, this is not only smartphones but also the whole range of IoT devices (or "smart devices"). In addition, for mining it is not necessary to install some kind of software, rather a special script. I think that this is the beginning of a new era—"undisguised" and "friendly" SE. And it is possible that soon, for example, banners will appear on torrent sites with a cat from Shrek and the words: "Please mine form two minutes. This will help us continue uploading pirated-movies for you." Honestly and without cheating the user.

2. Pattern of changing SE threats. There is a general principle "every action has a reaction" the more often attacks of the same type occur, the more identified companies and individuals become in the methods of struggle, prevention and further protect against them, the principle of SE implies that a person will always remain imperfect by creating, in certain circumstances, even a very savvy methodically person can suffer from the proper level of a trained attacker. The graph below shows that the society does not develop evenly known threats and people know about them, people have become more cautious, security policies are more strict and closed, but even now after almost 5 years from the first cases (fig. 3), even an obviously suspicious email can be opened and skipped by spam filter and antivirus and eventually opened by a computer user.

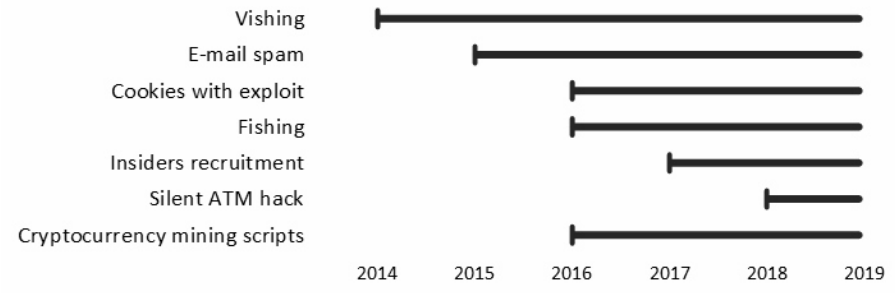


Figure 3 — Pattern of changing social engineering threats

Concluding and further studies. In this paper, there is only an attempt to outline the problem of social engineering. In the future, a full-scale research is planned on the reaction of people to phishing projects as part of the practice of ethical hacking.

References

1. *Mugala Mwami. Social Engineering : Research Assignment [Electronic resource] / M. Mugala. –15 p. – Access mode: https://www.academia.edu/7978172/Social_Engineering_Human_Hacking*
2. *Wilcox H. Social Engineering Through Social Media : An Investigation on Enterprise Security [Electronic resource] / H. Wilcox, M. Bhattacharya, R. Islam // Communications in Computer and Information Science. – 2014. – P. 243–255. – DOI 10.1007/978-3-662-45670-5_23.*
3. *2018 Data Breach Investigations Report. – 11th ed. – Verizon, 2018. – 68 p.*
4. *National Cyber Security Awareness Month: The Enterprise's Safety Online Is Everyone's Business [Electronic resource]. – Trend Micro, 2018. – Access mode: https://www.trendmicro.com/vinfo/us/security/news/social-engineering*
5. *Hulme George V. What is Social Engineering? How Criminals Take Advantage of Human Behavior [Electronic resource] / G. V. Hulme, J. Goodchild. – CSO, IDG Communications, 2017. – Access mode: https://www.csoonline.com/article/2124681/social-engineering/what-is-social-engineering.html*

УДК 004.056

Аяз Р. Х.
Харківський національний університет радіоелектроніки

Використання конволюції/деконволюції для стегоаналізу зображень в рамках підходу Хармсена и Перлмана

Вступ. З розвитком цифрового зв'язку, стенографія стала наукою, що займається непримітним вкладанням цифрових повідомлень в інші цифрові або оцифровані дані. Прогрес стенографії тісно пов'язаний з досягненнями стеганалізу, науки про виявлення прихованої інформації. [1]. Гістограма зображень широко використовується та використовувалась з самого початку формування стеганалізу. Методи цієї науки спрямовані на виявлення артефактів, властивих конкретним алгоритмам вкладання. [1-3]. Наприклад, найбільш популярними з них є критерій хі-квадрат та пар значень [1, 2]. В свою чергу Хармсен і Перлман вивчали ефект випадкового незалежного шуму. [3].

Існує декілька методів калібрування, описаних у літературі [2] – це децимація, JPEG калібрування та інші. Ця робота розширює підхід Хармсена и Перлмана, використовуючи деконволюцію [4] як техніку калібрування, що дозволяє нам підвищити точність алгоритму детектування стеговкладок. Цей метод дозволяє реконструювати гістограму оригінального зображення та використовувати її в якості основи для стеганалізу.

Метод Хармсена та Перлмана. В рамках підходу Хармсена и Перлмана розглядається приховування інформації шляхом додавання шуму до оригінального зображення [3]. Позначимо гістограму оригінального зображення як $h_c[n]$ та функцію розподілення мас (PMF) стегошуму як $f_\Delta[n]$. В результаті процесу вкладення маємо стегозображення з гістограмою $h_s[n]$. У системі, за умов незалежності адитивного шуму та оригінального зображення, дотримується наступне рівняння

$$h_s[n] = h_c[n] * f_\Delta[n] \tag{1}$$

де $*$ означає оператор згортки. Спираючись на теорему про згортку, Хармсен та Перлмен запропонували виконувати стегоаналіз в частотній області та представили поняття характеристичної функції гістограми (HCF) [3]:

$$H[k] = DFT(h[n]). \tag{2}$$

У [3] було показано що при використанні методу заміни найменш значущого біту (LSB), широкосмугового спектру (SS) і методів відносної заміни коефіцієнтів ДКП призводять до фільтрації низькочастотної гістограми оригінального зображення. Для вимірювання рівня спотворень гістограми оригінального зображення, застосовується HCF центр мас (COM) [3]:

$$C(H[k]) = (\Sigma_{k=0}^{(N/2)-1} k \cdot |H[k]|) / (\Sigma_{k=0}^{(N/2)-1} |H[k]|). \tag{3}$$

Чим менша частота зрізу фільтра нижніх частот, тим менше значення HCF COM. Цей факт дозволяє нам виявити наявність прихованого повідомлення.

Зверніть увагу, що посилання [5] пропонує модифікувати підхід Хармсена и Перлмана, щоб зробити його здатним виявляти статистичні дані, вбудовані шляхом модуляції вказаних ДКП коефіцієнтів.

Поняття деконволюції. Використовуючи позначення матриці [4], ми переписуємо згортку (1) щоб отримати:

$$\mathbf{H}_s = \mathbf{F}_\Delta \cdot \mathbf{H}_c, \tag{4}$$

де

$$\mathbf{H}_S = \begin{bmatrix} h_S[0] \\ h_S[1] \\ \vdots \\ h_S[n] \end{bmatrix}; \ \mathbf{F}_\Delta = \begin{bmatrix} f_\Delta[0] & 0 & \dots & 0 \\ f_\Delta[1] & f_\Delta[0] & \dots & 0 \\ \vdots & \vdots & \ddots & 0 \\ f_\Delta[n] & f_\Delta[n-1] & \dots & f_\Delta[0] \end{bmatrix}; \ \mathbf{H}_c = \begin{bmatrix} h_C[0] \\ h_C[1] \\ \vdots \\ h_C[n] \end{bmatrix}.$$

Рівняння (4) можна використовувати для калібрування стегозображення. Насправді, алгоритм вкладання повністю визначає F_Δ та дає зразки гістограми стегозображення, таким чином ми здатні реконструювати гістограму оригінального зображення за допомогою [6]

$$\mathbf{H}C = \mathbf{F}_\Delta^{-1} \cdot \mathbf{H}S, \tag{5}$$

Далі гістограма, розрахована за допомогою (5), використовується в рамках підходу Хармсена и Перлмана в якості основи. Нижче наведені матриці розмірності 256x256, які складені для методів LSB та широкосмугового спектру стеганографії, $\mathbf{F}_\Delta^{\mathrm{LSB}}$ and $\mathbf{F}_\Delta^{\mathrm{SS}}$ відповідно:

$$\mathbf{F}_\Delta^{\mathbf{LSB}} = \begin{bmatrix} 1/4 & 0 & 0 & 0 & \dots & 0 \\ 1/2 & 1/4 & 0 & 0 & \dots & 0 \\ 1/4 & 1/2 & 1/4 & 0 & \dots & 0 \\ 0 & 1/4 & 1/2 & 1/4 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 1/4 \end{bmatrix}, \mathbf{F}_\Delta^{\mathbf{SS}} = \begin{bmatrix} P(-3) & 0 & \dots & 0 & \dots & 0 \\ P(-2) & P(-3) & \dots & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ P(3) & P(2) & \dots & P(-3) & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & \dots & P(-3) \end{bmatrix},$$

де $P(-3) = \int_{-\infty}^{-2.5} p(x)dx$; $P(-2) = \int_{-2.5}^{-1.5} p(x)dx$; …; $P(0) = \int_{-0.5}^{0.5} p(x)dx$; …; $P(3) = \int_{2.5}^{\infty} p(x)dx$;

$p(x) = (2\pi)^{-0.5} \times e^{-x^2/2}$.

Висновок. В роботі запропоновано новий метод калібрування стегозображень, що базується на основі поняття деконволюції. Такий метод дозволяє підвищити точність виявлення стего зображень в рамках підходу Хармсена та Перлмана.

Список використаних джерел

1. *R. Bohme, Advanced statistical steganalysis, Springer, 2010.*
2. *H. G. Schaathun, Machine Learning in Image Steganalysis, Wiley-IEEE Press, 2012.*
3. *J.J. Harmsen and W.A. Pearlman, "Steganalysis of additive-noise modelable information hiding," in Storage and Retrieval for Image and Video Databases. International Society for Optics and Photonics, 2003, vol. 5020, pp. 131–142.*
4. *S. A. Gonzalez, M. E. Valentinuzzi, P. D. Arin, "Deconvolution: It Fans Back, Out, and Ahead," IEEE Pulse, pp.54–61, 2016.*
5. *O.V. Fedorov, A.S. Rubel and A.V. Omelchenko, "Detection of DCT Coefficient Modulation Schemes in JPEG Images," in Proceedings of 26th Conference Radioelektronika 2016, April 19-20, Kosice, Slovak Republic, 2016, pp. 231–234.*
6. *D. Kundur, D. Hatzinakos, "Blind image deconvolution," IEEE Signal Processing Magazine, pp.43–64, 1996.*

УДК 004.056.53.

Бабюк Є. М.
Національний авіаційний університет

Інновації у сфері кібербезпеки: хмарні ресурси та машинне навчання

Кібербезпека - це сукупність технологій, процесів та практик, призначених для захисту мереж, пристроїв, програм та даних від атак, пошкоджень або несанкціонованого доступу. Кібербезпеку також можна назвати безпекою інформаційних технологій. Кібербезпека вважається важливою, оскільки державні, військові, корпоративні, фінансові та медичні організації збирають, обробляють та зберігають безпрецедентну кількість даних на комп'ютерах та інших пристроях. Значна частина цих даних може бути конфіденційною інформацією, будь то інтелектуальна власність, фінансові дані, особиста інформація або інші типи даних, для яких несанкціонований доступ або вплив може мати негативні наслідки. Організації передають конфіденційні дані через мережі та інші пристрої під час ведення бізнесу, а кібербезпека спрямована на захист цієї інформації та систем, що використовуються для її обробки або зберігання.

Оскільки обсяг та витонченість кібератак зростають, компанії та організації, особливо ті, на яких покладено завдання зберегти інформацію стосовно національної безпеки, охорони здоров'я або фінансових документів, повинні вжити заходи для захисту їх вразливої інформації про бізнес та персонал.

Для ефективної боротьби з кібератаками та кіберзлочинністю організація повинна координувати свої дії по всій її інформаційній системі.

Це має на увазі забезпечення наступного: мережева безпека; захист додатків; захист кінцевої точки; захист даних; управління ідентифікацією; безпека баз даних та інфраструктури; cloud security; мобільна безпека; аварійне відновлення / планування безперервності бізнесу; освіта кінцевих користувачів. Слід розуміти, що найважчим завданням в галузі кібербезпеки є постійний розвиток відповіді на всі ризики для безпеки. Традиційно організації та уряд зосереджують більшість своїх ресурсів кібербезпеки на безпеці периметру, захищаючи лише найважливіші компоненти системи та захищаючись від відомих небезпек. Сьогодні такий підхід недостатній, оскільки загрози розвиваються та змінюються швидше, ніж організації, які мають справу з ними.

Розглянемо традиційний захист від кібератак, який виглядає наступним чином: якийсь екран-фільтр контролює периметр входу в інтернет і антивірус, що забезпечує безпеку безпосередньо на самому комп'ютері. На сьогодні дана система вже неефективна, тому розробникам і спеціалістам з кібербезпеки доводиться поламати голови, щоб знайти ефективне інноваційне рішення для порятунку від хакерів.

Спостерігаючи за сьогоднішніми тенденціями, стає зрозуміло, що багатьох користувачів спіткала нова проблема – постійний ріст вірусів-майнерів (miner). Ці програми не завдають шкоди програмному забезпеченню комп'ютера та не несуть небезпеку особистим даним та інформації користувача. Проте вони просто використовують чужу машину, її ресурси для заробітку. І до розряду класичних загроз це вторгнення віднести неможливо. З цієї причини антивіруси не помічають нові майнінгові програми.

Проблема сучасних антивірусних програм в тому, що вони шукають щось відоме. Сьогодні ж шкідливі програми з'являються настільки швидко, що розробники не встигають створювати спеціальні сигнатури. Тепер стає зрозуміло, що і в сфері кібербезпеки, постає потреба в штучному інтелекті та машинному навчанні.

Згадаємо найпростіший спосіб захисту свого комп'ютера від шкідливого ПЗ. В першу чергу, це безпека персонального комп'ютера шляхом відключення від мережі Інтернет. Далі йдуть антивірус і захищений зовнішній контейнер. Проте користувачі

дуже важко йдуть на зміну звичного для них постійного циклу роботи і не завжди готові до інновацій, вважаючи за краще послуги, розташовані прямо на ПК.

Виходячи з того, що так чи інакше захист інформації залежить від людей, як в приватному, так і в корпоративному порядку, розробники корпорації Cisco розробили продукт Umbrella. Розглянемо даний продукт, який являє хмарну платформу захисту від загроз, механізм дії якої нагадує, як уже зрозуміло з назви, парасольку, захищаючи дані замовника від зовнішніх інтернет-загроз. Найчастіше віруси потрапляють в комп'ютери не безпосередньо, а через якийсь файл, який не несе в собі загрози, тому антивіруси не перешкоджають його потраплянню в систему. Далі цей файл здійснивши несанкціонований доступ до комп'ютера, виходить в інтернет і починає довантажувати вірусні файли, що перехоплюють дані, блокують інформацію та виконують інші неправомірні дії. Відповідно Umbrella якраз стає на заваді даному явищу – вона не дозволяє зв'язуватися йому з мережею, закриваючи користувача з усіх можливих сторін, можна навіть вжити такий термін як «купол безпеки», який закриває комп'ютер подібно парасольці, опираючись на назву платформи.

Унікальність Umbrella полягає в тому, що платформу не потрібно нікуди встановлювати, тому вона може захищати будь-який пристрій, навіть банкомат, маршрутизатор або медичне обладнання, яке має зв'язок з глобальною мережею.

Оскільки в сучасному світі уже всі гаджети мають доступ до мережі, це дає впевненість користувачу в тому, що всі його пристрої можуть бути надійно і комплексно захищені.

Щодо захисту персональних даних користувача та апаратної частини його пристроїв на основі машинного навчання.

Технології машинного навчання безпосередньо пов'язані з поведінкою користувачів комп'ютерів та інших пристроїв. Нові технології будуть шукати вже не відомі шкідливі, потенційно небезпечні програми, а навпаки, такі, що до цього були не відомі – аномалії, програми з аномальною поведінкою, не властивою для даного користувача, та його повсякденної поведінки в комп'ютерному середовищі.

Зрозуміло, що система такого класу повинна аналізувати поведінкові особливості користувача або додатків по кожному файлу в комп'ютері і знаходити всілякі зміни в цьому питанні. Далі за особливим алгоритмом визначається ступінь шкідливості файлу з нестандартною поведінкою.

Схожа система, а точніше Cisco Security Connector вже вбудована в платформу Apple iOS, що на даний момент вважається однією з найбільш захищених платформ від вірусних атак.

Статистика компанії Cisco говорить про те, що незабаром у світі буде не вистачати приблизно мільйона IT-співробітників. Отже, зважаючи на такі прогнози, є дві можливості розвитку подій.

Перший – підготовка нових фахівців, створення нових центрів боротьби з кіберзлочинністю. Проте такий варіант не зможе задовольнити настільки велику недостачу спеціалістів.

Отже, залишається другий варіант – розвивати методи названі вище. Відповідно це не те завдання, яке можна вирішити дуже швидко, проте варто розуміти, що як тільки дана технологія вийде на пік, максимум своїх можливостей, слід очікувати значного зменшення небезпеки у кіберпросторі.

Список використаних джерел

1. *Cisco Security Professional's Guide to Secure Intrusion Detection Systems / [T. C., D. James, D. Scott ma ін.]. – Rockland: Syngress Publishing, 2003. – 673 с.*
2. *Managing cisco network security second edition / [K. Eric, B. Brian, W. Weaver ma ін.]. – Rockland: Syngress Publishing, 2002. – 752 с.*
3. *Omar S. Cisco Next-Generation Security Solutions / S. Omar, K. Panos, W. Aaron., 2016. – 368 с.*
4. *Закон України "Про основні засади забезпечення кібербезпеки України" від 05.10.2017 № 2163-VIII.*

УДК 004.056.57

Байлюк Є. М.
Житомирський державний технологічний університет

Розвідувальна організація з питань загроз Cisco Talos Intelligence Group

Наш цифровий світ розширюється з феноменальною швидкістю, відкриваючи нові атаки для кіберзлочинності. У той же час кіберзлочинці постійно розробляють нові методи, що підвищують ефективність їх атак. Отже, як спеціалісти з кібербезпеки можуть випереджати кіберзлочинців? Простого виявлення та відстеження нових загроз недостатньо. Для того, щоб попереджувати загрози в майбутньому, необхідно використовувати проактивний підхід до всеосяжної безпеки і загроз, які надає Talos.

Cisco Talos Intelligence Group – це розвідувальна організація з питань загроз, яка забезпечує захист клієнтів, які використовують продукти і послуги Cisco. Одна з найбільших в світі розвідувальних груп з питань комерційної загрози, Talos складається з дослідників кібербезпеки світового рівня, аналітиків та інженерів. Talos захищає клієнтів Cisco від відомих і нових загроз, виявляє нові уразливості і присікає кібер-загрози, перш ніж вони завдадуть додаткової шкоди Інтернету в цілому. Talos також вносить інформацію в численні системи захисту від відкритих і комерційних загроз та тісно співпрацює з кількома громадськими організаціями з кібербезпеки, такими як Snort.org, ClamAV і SpamCop.

Talos співпрацює з підрозділами Cisco з реагування на інциденти, тестування проникнення і розширених служб для збору даних про кібербезпеку, які охоплюють мережі, кінцеві точки, хмарні середовища, віртуальні системи і щоденний трафік в Інтернеті та електронній пошті. Ця телеметрія даних дає Talos видимість і контекст для даних, що дає їм унікальну інформацію про цілеспрямовані атаки та найпоширеніші загрози [1]. Talos розробила одну з найбільш всеосяжних платформ збору і аналізу інформації в галузі. Вона збирає дані з різних джерел, в тому числі:

1. Інтелектуальні загрози з боку спільноти: Talos отримує цінний інтелект через ClamAV, SNORT, Immunet, SpamCop, центр репутації Talos, сітку загроз та інші спільноти користувачів. Talos також співпрацює з користувачами по всьому світу за допомогою програми Crete, спільного обміну між клієнтами Talos і Cisco FirePOWER, для виявлення регіональних загроз у міру їх появи.

2. Публічні та приватні аналітичні канали: Talos щодня аналізує численні канали для нових загроз і діє в режимі реального часу для розробки нового програмного забезпечення для їх виявлення.

3. Інтелектуальне управління шкідливими програмами в реальному часі: Talos збирає понад мільйон шкідливих програмних зразків кожен день за допомогою телеметрії, прийомів, пісочниць та галузевих партнерських відносин.

4. Дослідження: Talos ідентифікує, досліджує і документує нові загрози та кіберзлочинців.

Talos є основним джерелом інформації про загрози для екосистеми колективної безпеки Cisco (CSI). CSI включає в себе кілька команд по всьому світу, які надають кращі в галузі засоби захисту і керовані служби безпеки для безлічі рішень. CSI включає Cisco Security and Trust Organization, Managed Threat Defense Team і Research and Operations. CSI управляється дослідниками загроз, розвідувальною інфраструктурою, телеметрією продуктів і послуг, державними і приватними каналами і співтовариством з відкритим вихідним кодом.

Talos забезпечує комплексний і активний підхід до мережевої безпеки. Він має довгу історію лідерства та успіху в галузі. Talos фокусується на високоякісних

дослідженнях безпеки, орієнтованих на клієнта, які встановлюють планку точності та актуальності. Їх дослідження і збір інформації втілюються безпосередньо в створення нових продуктів і послуг. Ці продукти безпосередньо сприяють телеметрії Talos, яка, в свою чергу, забезпечує виявлення загроз для будь-якого середовища для захисту всіх видів активів.

Наприклад, Cisco Advanced Malware Protection (AMP) для кінцевої точки блокує шкідливе ПЗ в точці входу і постійно контролює загрози. AMP для кінцевої точки включає в себе глобальну інформацію про погрози від команди безпеки Talos, включаючи попередження про загрози, моніторинг файлів і журнали шкідливих програм. AMP ділиться інформацією щодо загроз зі мережевою безпекою, захистом електронної пошти та пристроями безпеки в Інтернеті; в результаті чого створюється взаємопов'язана Серед рішень захисту від шкідливих програм, які обмінюються інформацією про загрози і вчаться один у одного[2].

Якщо який-небудь замовник Cisco виявляє реальну загрозу, вона буде автоматично заблокована, нейтралізована або поміщена в карантин в мережах інших замовників і клієнтів по всьому світу буквально за лічені хвилини. Але що ще важливіше – це отримання захисту Talos з кожним продуктом або сервісом Cisco.

Підхід Talos, орієнтований на активний захист від загроз безпеки до, під час і після мережевої атаки, охоплює і захищає всю розподілену мережу цілком: від базової мережевої інфраструктури до ЦОД, хмарних сервісів і мобільних пристроїв, підключених до мережі:

1. Безпека електронної пошти та веб-трафіку: фільтр репутації SenderBase (аналітика загроз безпеки електронної пошти і веб-трафіку), URL-фільтри, моніторинг і контроль роботи додатків, антиспам, фільтри епідемій.

2. Захист від складного шкідливого ПО і безпеку кінцевих пристроїв: ClamAV, Razorback, Moflow, рішення аналізу «пісочниці» шкідливого ПО.

3. Безпека мережі: набір правил підписки Snort, VDB: поновлення і вміст, вміст по виявленню продуктів SEU/SRU і запобігання для центру управління Firepower Management Center.

4. Глобальні оновлення аналітики загроз безпеки.

Ця стратегія охоплює весь цикл атаки – до, під час і після неї, забезпечуючи високу ефективність і швидкість виявлення загроз і реагування на інциденти.

Cisco Talos Group припинила діяльність і зламала інфраструктуру організованої групи операторів набору експлойтів Angler, яка заробляла прибл. 60 млн доларів США в рік тільки на вимаганні, за оцінками експертів.

Представники Talos заявили, що помістили в чорний список кілька підмереж класу С Інтернет-Eurobyte, які використовувалися для впровадження експлойтів RIG або мали негативну оцінку веб-репутації. RIG – набір експлойтів, який виконував платні завантаження на пристрої нічого не підозрюють користувачів»[3].

Таким чином, Cisco Talos Intelligence Group озброєна найсучаснішими системами та інструментами моніторингу загроз, що виникають по всьому світу. Провідні спеціалісти Talos виявляють, аналізують і нейтралізують вже відомі і нові загрози, агрегуючи і аналізуючи найповніші телеметричні дані, які надає Cisco.

Список використаних джерел

1. *Cisco TALOS – интеллектуальная платформа для анализа угроз [Електронний ресурс]. – Режим доступу : https://www.slideshare.net/CiscoRu/cisco-talos-75424510*
2. *Cisco Talos – The Intelligence Behind Cisco's Security Offerings [Електронний ресурс]. – Режим доступу : https://ceriumnetworks.com/cisco-talos-the-intelligence-behind-ciscos-security-offerings/*
3. *Cisco Talos. Эксперты по безопасности, которые защитят вас [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/dam/global/ru_ru/about/brochures/assets/pdfs/2160113_flyer_talos_cte_etmg_ru_rgb.pdf*

УДК 004.056.55

Байлюк Є. М.
Житомирський державний технологічний університет

Покращений протокол безпеки безпровідних мереж Wi-Fi Protected Access 3 (WPA3)

Wi-Fi є невід'ємною частиною повсякденного життя. Мільярди людей у всьому світі залежать від Wi-Fi у своїх будинках і бізнесі, в магазині, в банку, координуючи життя та залишаючись на зв'язку. Забезпечення бездротових з'єднань Wi-Fi є важливим елементом захисту персональних даних, а Wi-Fi Alliance продовжує покращувати безпеку Wi-Fi, оскільки кількість Wi-Fi-пристроїв, що використовуються в усьому світі, зросла.

На сьогоднішній день основним протоколом зв'язку Wi-Fi є WPA2. Він був представлений в 2004 році, а з 2006 року його підтримка є обов'язковою для будь-яких сертифікованих пристроїв Wi-Fi. Про розробку нового протоколу WPA3 було оголошено в січні 2018 року. Це пов'язано з тим, що в жовтні 2017 року група дослідників в області інформаційної безпеки оголосила про виявлення в протоколі WPA2 кількох критичних вразливостей. З їх допомогою зловмисник може здійснити атаку реінсталяції ключів (Key Reinstallation Attack, KRACK) і отримати доступ до конфіденційних даних. Ці вразливості дозволяють зловмисникам перехоплювати і змінювати трафік в зашифрованих мережах, а схильними хоча б до частини із цих вразливостей виявилися всі поширені операційні системи та апаратне забезпечення[1].

Нещодавно Wi-Fi Alliance оприлюднив найбільше оновлення безпеки Wi-Fi за останні 14 років. Протокол безпеки Wi-Fi Protected Access 3 (WPA3) вводить дуже потрібні оновлення в протокол WPA2, що був представлений в 2004 році. Замість того, щоб повністю переробити безпеку Wi-Fi, WPA3 концентрується на нових технологіях, які повинні закрити вразливі місця, що почали з'являтися в WPA2.

Одним з головних нововведень стала заміна алгоритму WPA-PSK на SAE. Алгоритм аутентифікації PSK мав серйозний недолік – зловмисник міг перехопити пакет з «рукостисканням», в якому міститься ключ, згенерований на основі пароля і деяких інших параметрів, а потім намагатися підібрати пароль, не потребуючи в доступі до мережі, яка атакується. Оскільки новий механізм аутентифікації вимагає взаємодії з точкою доступу, тепер зловмисники не зможуть застосовувати оффлайн-атаки. Крім того, застосування нового механізму означає, що прості паролі, засновані на словах, будуть не так сильно знижувати безпеку мережі, оскільки зловмисники не зможуть застосовувати атаку по словнику.

Покращення безпеки торкнулися і версії WPA3 для корпоративних користувачів. Він отримав підтримку режиму з 192-бітовим шифруванням і ще більш сильним шифруванням під час аутентифікації. Також Wi-Fi Alliance розробив стандарт Easy Connect для підключення до мережі пристроїв, які не мають екрану. Для цього на такі пристрої буде наноситися QR-код з ключем та ідентифікатором. Користувач зможе підключити пристрій, просканувавши QR-код за допомогою смартфона. Також, нова програма Wi-Fi CERTIFIED Easy Connect, значно зменшує складність бортових пристроїв Wi-Fi з обмеженим інтерфейсом або відсутністю інтерфейсу дисплея – наприклад, пристроїв, що виходять на ринок Internet of Things (IoT), – в той час як все ще зберігаючи високі стандарти безпеки. Wi-Fi Easy Connect і WPA3 представляють собою новітню еволюцію в програмах Wi-Fi Alliance, щоб користувачі отримували позитивний досвід, залишаючись надійно підключеним в міру розвитку ландшафту безпеки [2].

Безпека WPA3 підтримує ринок через два різних режими роботи: WPA3-Personal і WPA3-Enterprise. Всі мережі WPA3 використовують новітні методи захисту,

забороняють застарілі протоколи і вимагають використання захищених фреймів управління (PMF) для забезпечення відмовостійкості критично важливих мереж.

До основних можливостей WPA3 відносяться:

1. WPA3-Personal: більш надійна аутентифікація на основі пароля, навіть коли користувачі вибирають паролі, які не відповідають типовим рекомендаціям складності. WPA3 використовує одночасну аутентифікацію Equals (SAE), протокол встановлення безпечного ключа між пристроями, щоб забезпечити більш надійний захист користувачів від спроб вгадування пароля третіми особами.

2. WPA3-Enterprise: пропонує еквівалент 192-бітного криптографічного перетворення, забезпечуючи додатковий захист мереж, що передають конфіденційні дані, такі як мережі для уряду або фінансів. 192-бітний пакет забезпечення безпеки забезпечує узгоджену комбінацію криптографічних інструментів, розгорнутих в мережах WPA3.

На початку цього року Wi-Fi Alliance ввів удосконалення та нові функції для Wi-Fi Protected Access, необхідного сімейства технологій безпеки Wi-Fi CERTIFIED, щоб гарантувати, що WPA2 підтримує надійні засоби захисту при розвитку бездротового ландшафту. WPA3 підтримує сумісність з пристроями WPA2 через перехідний режим роботи, і користувачі Wi-Fi можуть залишатися впевненими в тому, що вони захищені при підключенні до захищених мереж Wi-Fi CERTIFIED[3].

Користувачі отримують доступ до мереж Wi-Fi всюди: вдома, в офісі, в готелях, торгових центрах, транспортних вузлах і муніципальних місцях. Під час доступу до таких незахищених мереж є ризик того, що хтось може перехватити персональні дані, тому Wi-Fi Alliance наполегливо рекомендує користувачам забезпечити доступ до безпечних мереж з аутентифікацією, коли це можливо. Однак є ситуації, коли відкрита мережа Wi-Fi є єдиним можливим варіантом. Хоча багато споживачів у всьому світі використовують відкриті мережі без будь-яких проблем, важливо знати ризик, який представляє відкрита мережа, та подбати про захист призначених для користувача даних. Щоб усунути ці ризики, Wi-Fi Alliance розробила рішення для користувачів відкритих мереж Wi-Fi.

Wi-Fi Enhanced Open – це програма Wi-Fi CERTIFIED, технологія сумісна з успадкованими мережами. Мережеві оператори, які хочуть розгорнути повнофункціональну аутентифікацію і рішення для надання пристроїв, повинні враховувати такі підходи, як Wi-Fi CERTIFIED Passpoint. Термін «Wi-Fi CERTIFIED Passpoint» визначає продукти, які сертифіковані Wi-Fi Alliance, і є комерційною назвою для програми сертифікації. Основна специфікація або технологія називається «Специфікація Hotspot 2.0 Wi-Fi Alliance»[4].

Отже, WPA3 забезпечує кращий захист від атак з перебором по словнику і підбору пароля без взаємодії з точкою доступу, а також вводить деякі інші поліпшення, пов'язані з безпекою. Стандарт стане обов'язковим для виробників пристроїв з підтримкою Wi-Fi після того, як він стане досить широко поширеним.

Список використаних джерел

1. *Discover Wi-Fi. Security [Електронний ресурс]. – Режим доступу : https://www.wi-fi.org/discover-wi-fi/security*
2. *Представлен стандарт WPA3. Это первое крупное обновление защиты Wi-Fi за 14 лет [Електронний ресурс]. – Режим доступу : https://www.wi-fi.org/discover-wi-fi/security*
3. *Wi-Fi Alliance представляет Wi-Fi CERTIFIED WPA3 [Електронний ресурс]. – Режим доступу : https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-wi-fi-certified-wpa3-security*
4. *Discover Wi-Fi. Passpoint [Електронний ресурс]. – Режим доступу : https://www.wi-fi.org/discover-wi-fi/passpoint*

УДК 004.056.53

Безносюк І. В.
Національний авіаційний університет

Сучасні методи аутентифікації

З кожним роком витоки інформації набувають все більших масштабів, терабайти персональних даних опиняється в чужих руках. Від рук хакерів найчастіше страждають облікові записи з простими паролями. Виникає питання: як зберегти дані?

Відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», безпечний стан оброблюваної інформації визначають три основні властивості – її конфіденційність, доступність і цілісність [1]. Згадаймо, що парольна аутентифікація є одним з перших бар'єрів, що з'явилися в ІТ-системах одночасно з операційними системами, що реалізовують множинний доступ до інформаційних ресурсів.

Однак 80% інцидентів в сфері інформаційної безпеки трапляються внаслідок використання слабких паролів.

Слабкий пароль – це погано з точки зору норм інформаційної безпеки, але є і зворотна сторона застосування складних паролів – труднощі їх утримання в пам'яті людини. Як наслідок – недбалість їх зберігання у вигляді робочих записів, а в цьому випадку вже не має значення, чи буде логін/пароль записано в особистому блокноті або закріплено на моніторі стікером.

Один із способів забезпечити безпеку – використовувати надійні засоби багатофакторної аутентифікації як невід'ємну частину політики безпеки. Багатофакторна аутентифікація – ідентифікація користувача на основі того, що він знає, того, чим він володіє і чогось, ким він є (біометрія).

Сильні і слабкі сторони багатофакторної аутентифікації, в загальному, відомі. До переваг можна віднести її здатність захистити інформацію, як від внутрішніх загроз, так і від зовнішніх вторгнень. Певною слабкістю можна вважати необхідність використання додаткових програмно-апаратних комплексів, пристроїв зберігання і зчитування даних.

В даний час в системах і мережах все ширше застосовуються біометричні засоби безпеки. Біометрична ідентифікація - це пред'явлення користувачем свого унікального біометричного параметра і процес порівняння його з усією базою наявних даних. Для вилучення такого роду персональних даних використовуються біометричні зчитувачі [2].

Біометричні системи контролю доступу зручні для користувачів тим, що носії інформації знаходяться завжди при них і не можуть бути загублені або вкрадені. Біометричний контроль доступу вважається більш надійним, тому що ідентифікатори не можуть бути передані третім особам чи скопійовані.

Методи біометричної ідентифікації поділяють на статичні, засновані на фізіологічних ознаках людини, присутніх з нею протягом усього її життя та динамічні, що беруть за основу поведінкові характеристики людей, а саме підсвідомі рухи в процесі повторення будь-якої звичайної дії рис.1.

Одним з пріоритетних видів поведінкової біометрії - манера друкувати на клавіатурі. При її визначенні фіксується швидкість друку, сила натискання на клавіші, тривалість натискання на клавішу, проміжки часу між натисканнями.

Окремим біометричним фактором може слугувати манера використання миші. Крім цього, поведінкова біометрія охоплює велику кількість факторів, не пов'язаних з комп'ютером, - хода, особливості того, як людина піднімається сходами.

Існують також комбіновані системи ідентифікації, що використовують кілька біометричних характеристик, що дозволяє задовольнити найсуворіші вимоги до надійності і безпеки систем контролю доступу [3].

Застосування всіх біометричних технологій включає чотири основні етапи:

– реєстрація ідентифікатора - відомості про фізіологічну або поведінкову характеристику перетворюються в форму, доступну комп'ютерним технологіям, і вносяться в пам'ять біометричної системи;

– виділення - з пред'явленого ідентифікатора виділяються унікальні ознаки, які аналізуються системою;

– порівняння - зіставляються відомості про пред'явлений і раніше зареєстрований ідентифікатор;

– рішення - виноситься висновок про те, збігаються або не збігаються пред'явлений і раніше зареєстрований ідентифікатор [4].

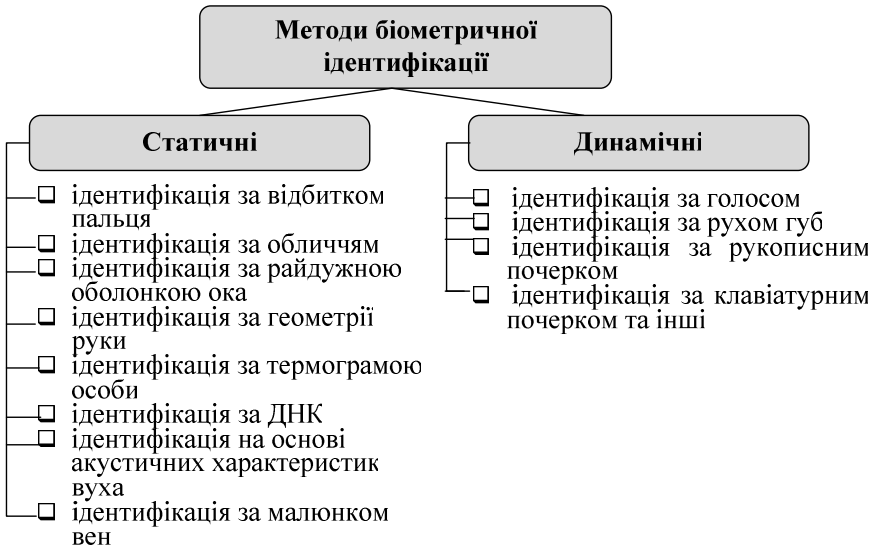


Рисунок 1 – Методи біометричної ідентифікації

Висновок про збіг/розбіжність ідентифікаторів може потім транслюватися іншим системам (контролю доступу, захисту інформації і т.д.), які далі діють на основі отриманої інформації.

Найбільш поширений в даний час спосіб ідентифікації та авторизації за допомогою паролів багато в чому себе дискредитував. Причиною тому є не тільки незручності, пов'язані з їх використанням, і легкість, з якою користувачі порушують встановлені правила застосування паролів, а й принципова нестійкість даної технології проти прийомів соціальної інженерії – найефективнішого способу реалізації кібератак. З впевненістю можна зазначити, що біометрія значною мірою позбавлена цих недоліків - у всякому разі «забути» свої біометричні дані або «передати» їх шахраям складніше, ніж пароль. Отже, біометрична аутентифікація - масштабний сегмент ринку систем безпеки. Фактично кожен новий пристрій біометричної ідентифікації може використовувати нові принципи і алгоритми роботи. Виходячи з усього вище зазначеного можна сказати, що біометрична аутентифікація володіє високим потенціалом: як введення в експлуатацію, так і розвитку нових технологій.

Список використаних джерел

1. *Закон України "Про захист інформації в автоматизованих системах" від 05.07.94, № 80/94-ВР. — К., 1994.*
2. *Царьов Р.Ю. Біометричні технології: навч. посіб. [для вищих навчальних закладів] / Р.Ю. Царьов, Т. М. Лемеха. – Одеса: ОНАЗ ім. О.С. Попова, 2016. – 140 с.: іл.*
3. *Next Generation Identification (NGI) – Нове покоління ідентифікації [Електронний ресурс]. – Режим доступу: http://www.fbi.gov/hq/cjisd/ngi.htm.*
4. *Общая характеристика биометрических технологий [Електронний ресурс]. – Режим доступу: https://www.biolink.ru/technology/biometric.php.*

УДК 004.453

Безрук Є. А., Брусеньский В. Р., Неласая Г. В.
Запорізький національний технічний університет

Використання технології ubeacons для тергетингу та методи боротьби з нею

Екосистема ультразвукового відстеження (uBeacons) - відносно нова технологія, яка використовує аудіомаячки, що не чутні людським вухом, для відстеження користувачів і пристроїв uBeacons - це високочастотні аудіомаячки, випромінювання яких фіксується більшістю комерційних динаміків і мікрофонів. Цей ультразвук дозволяє відстежувати дії користувачів на різних пристроях. Тому технологія має велике розповсюдження у сфері рекламного бізнесу.[1]

Нижче подано терміни та скорочення, використані в роботі.

Web audio API — потужний і багатогранний інструмент для маніпуляції звукової складової на веб-сторінці, що дає можливість розробникам вибрати джерела, додати до них спеціальні звукові ефекти (такі як panning), візуалізувати їх і багато іншого.

HTTPS Everywhere — це вільне і відкрите розширення для браузерів, розроблене спільно The Tor Project і Electronic Frontier Foundation (EFF).[2] Воно автоматично змушує вебсайти використовувати більш захищене HTTPS з'єднання замість HTTP, якщо вони його підтримують.[3]

uXDT (ultrasound cross-device tracking) — технологія збору даних за допомогою ультразвуку

SDK (software Development Kit) — набір із засобів розробки, утиліт і документації, який дозволяє програмістам створювати прикладні програми

Tails OS — дистрибутив Linux на основі Debian, створений для забезпечення приватності та анонімності[4]. Усі вихідні з'єднання повинні пройти через Tor,[5] неанонімні з'єднання блокуються. Система призначена для завантаження з Live CD або Live USB та не залишає жодної інформації після себе на пристрої, де вона використовувалась. [6].

Група дослідників з Брауншвейзького технічного університету (Німеччина) знайшла велику кількість додатків під Android, що використовують ультразвукові маячки за стеження за користувачами. Фахівці кажуть, що технологія (ultrasound cross-device tracking, uXDT) набула великої популярності в останні кілька років.

Ідея в тому, що під час відтворення реклами по телебаченню, на мобільному пристрої або в офлайновому магазині чи ресторані видається нечутний вуху ультразвуковий сигнал. Зазвичай він додається до музичного кліпу або джингла. Цей сигнал (коротка послідовність високочастотних тонів) реєструється мікрофонами оточуючих електронних пристроїв (ноутбуки, ПК, смартфони, планшети) - і після цього рекламодавець знає, що цей конкретний користувач одночасно володіє перерахованими пристроями. Це потрібно в тому числі для зв'язування рекламних профілів і відстеження користувача, який виходить в інтернет з різних пристроїв.

Описаний метод покладається на заманювання користувача на веб-сторінку, яка містить рекламні оголошення, що видають ультразвук, або ж на сторінку, яка містить прихований JavaScript-код, який змушує браузер видавати ультразвук за допомогою HTML5 Audio API.

Рекламодавці використовують uXDT для орієнтування користувачів наступним чином.

1. Спочатку рекламодавець запускає оголошення з елементами ультразвуку: або на TV, або на сайті.

2. Як тільки оголошення відображається, з динаміка пристрою видається коротка послідовність високочастотних тонів. Цей високочастотний тон негайно захоплюється uXDT-фреймворком на смартфоні користувача.

3. Щоб забезпечити таку функціональність, uXDT-фреймворк працює у фоновому режимі і періодично звертається до мікрофона пристрої для прослуховування ультразвукових сигналів.

4. Після того як такий сигнал зафіксований, uXDT-фреймворк витягує з нього унікальний ідентифікатор оголошення і повідомляє про це рекламодавцю - разом з унікальними ідентифікаційними даними пристрою і користувача.

Для цього на пристроях повинен встановлено додаток, чий SDK містить функціональність з пошуку таких маячків.

Використовуючи HTML5 Audio API можливо уникнути відтворенню таких високочастотних тонів за допомогою таких модулів як:

1. Analyzer(Аналіз сигналу).

Аналізатор призначений для того, щоб отримувати інформацію про частотні і тимчасові параметри сигналу у вигляді масиву даних. Як тільки Ви отримаєте цей масив, зможете аналізувати і візуалізувати все, що відбувається зі звуком.

Таким чином, можливо проаналізувати рекламу(або будь-який інший відео/аудіо файл) і виявити в ній наявність прихованого ультразвуку.

```
var analyser = context.createAnalyser();
// Розмірність перетворення Фур'є
analyser.fftSize = 2048;
// Створюємо масиви для зберігання даних
fFrequencyData = new Float32Array(analyser.frequencyBinCount);
bFrequencyData = new Uint8Array(analyser.frequencyBinCount);
bTimeData = new Uint8Array(analyser.frequencyBinCount);
// Отримуємо дані
analyser.getFloatFrequencyData(fFrequencyData);
analyser.getByteFrequencyData(bFrequencyData);
analyser.getByteTimeDomainData(bTimeData);
```

2. Delay (Лінія затримки).

Цей модуль дозволяє затримувати звук на певний час, що дозволяє вимкнути пристрої з мікрофоном, або закрити веб-сторінку.

```
var delayNode = context.createDelay ();
delayNode.delayTime.value = 10; // 10 секунд.
source.connect (delayNode);
delayNode.connect (destination);
source.start (0);
```

3. Filter(Фільтрація)

За допомогою Web Audio API Ви можете додати деякий "еквалайзер" (фільтр) в свій граф обробки сигналу у вигляді модуля.

Нас цікавить один із доступних фільтрів, а саме lowpass - фільтр нижніх частот (він обрізає все, що вище обраної частоти), так як ультразвук розповсюджується у верхньому сегменті.

Для того, щоб налаштовувати ці фільтри, існує кілька параметрів, які, є у фізичних аналогів фільтрів.

Frequency - частота, на якій базується фільтр. Вимірюється в герцах (Hz)

Q (добротність) - ширина смуги навколо обраної частоти, до якої застосовуватиметься посилення або ослаблення(в нашому випадку ослаблення).

Gain - рівень посилення або ослаблення даної частоти.

```
var filterNode = context.createBiquadFilter();
filterNode.type = 1; // Low-pass filter (Тип фільтра)
filterNode.frequency.value = 20000; // Cutoff to 20kHZ (Базова частота)
filterNode.frequency.Q = 1;// Quality factor (Добротність) /
filterNode.gain.value = 0; // Підсилення (не потрібно даному типу фільтра)
```

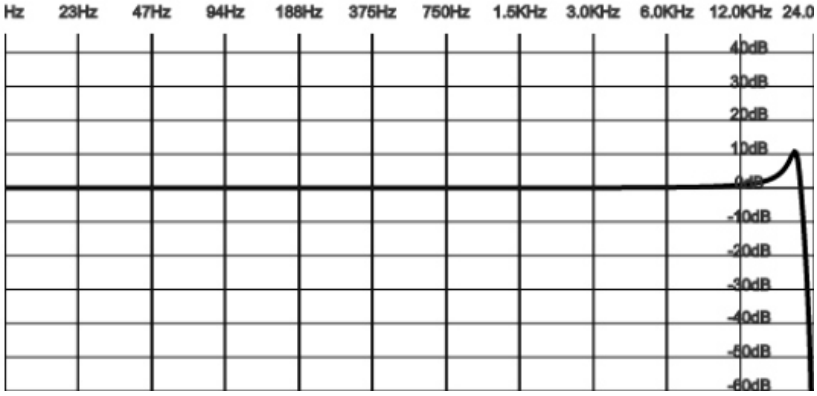


Рисунок 1 – Графік прикладу роботі фільтру lowpass

Деякі додатки включають NoScript, який може блокувати всі JavaScript і може зупинити XSS, а також HTTPS Everywhere, якщо користувач уникає незашифрованих веб-сайтів. Браузер Tor, що надається в Tails OS, може допомогти блокувати рекламу uXDT [7].

В даний час практика uXDT не регулюється. Хоча FTC вже оцінює вплив реклами uXDT, дослідницька група запропонувала серію пом'якшень, які можуть обмежувати вільне правління цього виду реклами в даний час.

Перш за все команда створила розширення для веб-переглядача Chrome під назвою SilverDog, який фільтрує весь звук HTML5, який відтворюється через веб-переглядач, і видаляє ультразвукові дослідження.

На жаль, це розширення не працює із звуками, відтворюваними через Flash, і не може захистити деякі браузери, наприклад, Tor

Для того, щоб вирішити це питання, дослідники також пропонують середньострокове рішення, таке як введення нового запиту в моделі дозволів Android, що явно інформує користувачів про те, що програма може слухати ультразвукові сигнали.

Цей дозвіл дозволить користувачам відкликати або відхилити це право з існуючих або нових додатків для Android, які вони встановлюють на своєму смартфоні.

Список використаних джерел

1. *.Funktionsweise-uBeacons-TU-Braunschweig [Електронний ресурс]. — Режим доступу: https://www.androidpiloten.de/2017/05/08/spyware-wie-dich-dein-smartphone-per-ultraschall-ausspioniert/funktionsweise-ubeacons-tu-braunschweig/*
2 *Electronic Frontier Foundation. HTTPS Everywhere. [Електронний ресурс]. — Режим доступу: https://www.eff.org/https-everywhere*
3 *HTTPS Everywhere reaches 2.0 [Електронний ресурс]. — Режим доступу: http://www.h-online.com/news/item/HTTPS-Everywhere-reaches-2-0-comes-to-Chrome-as-beta-1445615.html*
4 *The Amnesic Incognito Live SystemTor [Електронний ресурс]. — Режим доступу: https://lwn.net/Articles/440279/*
5 *TAILS 0.10.1 - The Amnesic Incognito Live System [Електронний ресурс]. — Режим доступу: https://www.tecchannel.de/a/tails-0-10-1-the-amnesic-incognito-live-system,2038771*
6 *Privacy for anyone anywhere [Електронний ресурс]. — Режим доступу: https://tails.boum.org/doc/about/finances/index.en.html*
7 *Catalin Cimpanu A Ultrasound Tracking Could Be Used to Deanonymize Tor Users [Електронний ресурс]. — Режим доступу: https://www.bleepingcomputer.com/news/security/ultrasound-tracking-could-be-used-to-deanonymize-tor-users/*

УДК 004.056

Вервейко В. В.
Харківський національний університет радіоелектроніки

Аналіз методів захисту від комп'ютерних вірусів

В останній час на підприємства України досить часто здійснюються кібератаки, які завдають шкоди інфраструктурі в цілому. У числі найбільших кіберінцідентів останніх років - атаки на українські енергетичні підприємства і епідемія шифратора NotPetya. Перше в історії масове відключення електроенергії, викликане кібератакою, відбулося в грудні 2015 року, його причина - комплекс шкідливих програм BlackEnergy. Саме тому в наш час досить актуальним є питання вивчення нових та аналіз вже відомих комп'ютерних вірусів і методів захисту від них [2].

Вкрай важливо чітко класифікувати вірус для виявлення відповідного методу захисту від нього. Відомо багато різних способів класифікації комп'ютерних вірусів. Одним із способів класифікації комп'ютерних вірусів є поділ їх за такими основними ознаками: середовище проживання; особливості алгоритму; способи зараження; ступінь впливу (нешкідливі, небезпечні, дуже небезпечні). Залежно від місця існування основними типами комп'ютерних вірусів є: програмні віруси; завантажувальні віруси; макровіруси та мережеві віруси. Комп'ютерні віруси намагаються викрасти персональні дані користувача або зашифрувати їх. Для розшифрування цієї інформації зловмисники вимагають кошти, що є правопорушенням згідно чинного законодавства. Особи, винні у порушенні законодавства у сферах національної безпеки, електронних комунікацій та захисту інформації, якщо кіберпростір є місцем та/або способом здійснення злочину, іншого винного діяння, відповідальність за яке передбачена цивільним, адміністративним, кримінальним законодавством, несуть відповідальність згідно із законом [3, стаття 12].

Для запобігання зараженню вірусами і атаками троянських коней, користувачам мереж необхідно виконувати наступні рекомендації: не варто встановлювати програми, отримані з Інтернету або у вигляді вкладення в повідомлення електронної пошти без перевірки на наявність в них вірусів; необхідно перевіряти всі зовнішні диски на наявність вірусів, перш ніж копіювати або відкривати файли, що містяться на них, або виконувати завантаження комп'ютера з таких дисків; необхідно встановити антивірусну програму і регулярно користуватися нею для перевірки комп'ютерів, оперативно поповнювати базу даних антивірусної програми набором файлів сигнатур вірусів, як тільки з'являються нові сигнатури; необхідно регулярно сканувати жорсткі диски в пошуках вірусів, сканування звичайно виконують автоматично при кожному включенні ПК і при розміщенні зовнішнього диска в зчитувальному пристрої; при скануванні антивірусна програма шукає вірус шляхом порівняння коду програми з кодами відомих їй вірусів, що зберігаються в базі даних; необхідно створювати надійні паролі, щоб віруси не могли легко підібрати пароль і отримати дозволи адміністратора, регулярне архівування файлів дозволить мінімізувати збиток від вірусної атаки; необхідно виконувати резервне копіювання цінних даних, які зберігаються на жорстких дисках; використовувати програмні засоби антивірусного захисту.

Не існує єдиного захисту від вірусних програм, але антивірусні програми, що вже існують, можуть ускладнити незаконне отримання даних злочинцями.

Особливу увагу в роботі присвячено сучасним антивірусним програм. Такі програми зазвичай складаються з наступних модулів: евристичний модуль - для виявлення невідомих вірусів; монітор - програма, яка постійно знаходиться в оперативній пам'яті ПК; пристрій управління, який здійснює запуск антивірусних програм і оновлення вірусної бази даних і компонентів; поштова програма, яка перевіряє електронну пошту; програма сканер, яка перевіряє, виявляє і видаляє фіксований набір відомих вірусів в пам'яті, файлах і системних областях дисків; мережевий екран, який здійснює захист від хакерських атак.

Отже, немає надійного захисту від вірусних програм, але якщо дотримуватися приведених вище методів захисту, то дані будуть мати непоганий рівень захищеності.

Список використаних джерел

1. https://www.lessons-tva.info/edu/e-inf1/e-inf1-4-1-3.html
2. https://habr.com/company/eset/blog/426077/
3. http://zakon.rada.gov.ua/laws/show/2163-19
4. https://uk.wikipedia.org/wiki/Макровірус
5. https://ru.wikipedia.org/wiki/Сетевой_червь
6. https://uk.wikipedia.org/wiki/Завантажувальний_вірус

УДК 004.056

Власов Б. Ф.
Харківський національний університет радіоелектроніки

Модернізація алгоритму гешування MD5

При розробці алгоритмів гешування, як і при розробці будь-яких інших алгоритмів забезпечення безпеки даних, виникає необхідність пошуку компромісу між швидкістю роботи алгоритму та його криптостійкістю. Довгий час найпопулярнішими алгоритмами гешування були алгоритми MD5 та SHA-1, які є більш швидкими за інші алгоритми. Однак із розвитком методів атак на ці алгоритми з'явилася можливість практичної реалізації колізійних атак на них. Це змушує користувачів переходити на більш повільні алгоритми SHA-2 та SHA-3. Актуальність цієї роботи пов'язана з появою нових можливостей завдяки використанню квантових атак на цифрові підписи, для яких алгоритм гешування є невід'ємною частиною.

В даній роботі запропоновано метод модифікації алгоритму MD5, який дозволить підвищити його криптостійкість до рівня, на якому існуючі методи атак не є ефективними. При цьому модифікований алгоритм все ще має більшу швидкість роботи ніж SHA-2 (проведене тестування показало, що модифікований алгоритм працює приблизно на 52% швидше за SHA-2)

Ідея полягає в тому, щоб запустити стандартний алгоритм MD5 два рази із різними ініціалізуючими векторами. Результати роботи конкатенуються. Таким чином алгоритм створює 256 бітне значення хешу, яке складається з двох 128 бітних хешів оригінального MD5. Незалежність двох частин алгоритму одна від одної дозволяє використовувати паралельні обчислення для прискорення швидкості роботи (як багатопоточність так і можливості сучасних процесорів виконувати паралельні обчислення в рамках одного потоку). В той же час обидві частини алгоритму опираються на одні дані, що значно підвищує складність атаки на алгоритм. Для проведення колізійної атаки на стандартний алгоритм MD5 необхідно знайти колізію для одного блоку (або групи блоків) даних таким чином, щоб не змінити внутрішній стан алгоритму. Для проведення колізійної атаки на запропонований модернізований алгоритм MD5 необхідно одночасно знайти колізію для двох хешів. При цьому ця задача не може бути розбита на дві незалежні задачі, оскільки будь-яке внесення змін у дані викличе зміни у внутрішньому стані обох алгоритмів. Тобто якщо для зламу стандартного MD5 необхідно знайти x такий, що $f(x)=A$, то для зламу модернізованого варіанту необхідно знайти x такий, що $f1(x)=A$ та $f2(x)=B$.

Всі існуючі колізійні атаки на алгоритм MD5 та інші алгоритми зі схожою структурою базуються на одному принципі, який був розроблений Ван Сяоюнем і Юй Хунбо[1]. Цей принцип полягає у побудові диференційного шляху, який дозволяє отримати одне значення хешу для двох повідомлень, які відрізняються один від одного на декілька біт. Однак для цього необхідно забезпечити виконання певних бітових умов для внутрішнього стану алгоритму під час обробки блоку даних. Ці бітові умови названі достатніми умовами (sufficient conditions). Складність проведення атаки полягає в тому, що за допомогою методів модифікації повідомлення можна забезпечити виконання достатніх умов лише на перших n кроках алгоритму (число n різне для різних методів атак). Умови для інших кроків алгоритму виконуються випадково, тому для знаходження колізії виконується перебір можливих варіантів блоку даних до тих пір, поки всі умови не будуть виконані.

Запропонована модифікація алгоритму MD5 збільшує кількість достатніх умов для проведення атаки в два рази, оскільки ці умови повинні виконуватися для обох

частин алгоритму. При цьому методи модифікації повідомлення дозволять забезпечити виконання достатніх умов на перших n кроках лише для однієї частини алгоритму. Всі умови для другої частини алгоритму повинні виконуватися випадково. Таким чином, якщо для оригінальної атаки Ван Сяоюня вірогідність отримання необхідного результату при переборі дорівнювала 2^{-37}, то для атаки модифікованого алгоритму ця вірогідність дорівнює 2^{-333}. Оскільки ця вірогідність менше за вірогідність знаходження колізії методом грубої сили (2^{-256}), використання цього методу атаки не є доцільним.

Для прискорення перебору при колізійних атаках використовується метод тунелювання [2]. Цей метод дозволяє створювати нові «точки перевірки», тобто дані, для яких виконуються умови для перших n кроків алгоритму, із однієї точки перевірки, отриманої методами модифікації повідомлення. Однак створення тунелю пов'язане із додаванням нових бітових умов. При атаці на оригінальний алгоритм MD5, це не збільшує складність проведення атаки, оскільки нові умови знаходяться в перших n кроках алгоритму, а отже можуть бути задовільнені методами модифікації повідомлення. При атаці на модифікований алгоритм кожна додаткова бітова умова зменшує вірогідність отримання результату в два рази, оскільки вірогідність її виконання в другій частині алгоритму дорівнює 0,5. Таким чином створення тунелів збільшує складність перебору замість його прискорення, а отже цей метод атаки не є доцільним.

Зазначені вище методи атак є колізійними атаками, які потребують однакового префіксу для колізійних блоків даних. Проведення колізійних атак із заданим префіксом, тобто таких, які дозволяють реалізовувати практичні атаки на системи безпеки, які використовують алгоритми гешування, є більш складним процесом. Метод проведення такої атаки описаний в роботі Марка Стівенса[3]. Атака складається із двох частин: пошуку «днів народження» та колізійної атаки із спільним префіксом. Пошук «днів народження», тобто перебір, який використовує парадокс «днів народження», направлений на пошук таких двох блоків даних, які при додаванні до заданих префіксів зблизять значення хешів таким чином, щоб різницю між ними можна було компенсувати за допомогою зазначених вище методів. В другій частині атаки отримана різниця між значеннями хешів прибирається за допомогою одного або декількох диференційних шляхів. Оскільки для модернізованого алгоритму проведення такої атаки не можливе, то атаку із вибраним префіксом провести також неможливо. Крім того, збільшення розміру хешу ускладнює пошук «днів народження» в першій частині атаки, що збільшить складність атаки навіть при знаходженні способу проведення колізійної атаки з однаковим префіксом.

Таким чином запропонована модифікація алгоритму MD5 є стійкою до існуючих на сьогодні методів атак на алгоритми гешування. Для ще більшої криптостійкості алгоритм MD5 можна запускати не два, а три або чотири рази, отримуючи хеш розміром 384 або 512 біт відповідно. Крім того, запропонований метод модифікації можна застосувати і для модифікації інших алгоритмів гешування.

Список використаних джерел

1. *Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD [Електронний ресурс] / Cryptology ePrint Archive. - Режим доступу: URL: https://eprint.iacr.org/2004/199 - 01.11.2018 - Назва з екрану*
2. *Tunnels in Hash Functions: MD5 Collisions Within a Minute [Електронний ресурс] / Cryptology ePrint Archive. - Режим доступу: URL: https://eprint.iacr.org/2006/105 - 01.11.2018 - Назва з екрану*
3. *Chosen-prefix collisions for MD5 and applications [Електронний ресурс] / École Polytechnique Fédérale De Lausanne. - Режим доступу: URL: https://documents.epfl.ch/users/l/le/lenstra/public/papers/lat.pdf - 01.11.2018 - Назва з екрану*

УДК 004.8:004.56

Ганечко О. О., Даніленко В. М., Сагун А. В.
Черкаський державний технологічний університет

Підсистема інтелектуальної фільтрації електронних повідомлень на базі алгоритму машинного навчання

Вступ. Згідно статистичних даних, наведених в [1], обсяг спам-повідомлень в загальному обсязі поштових e-mail сервісів з січня по березень 2018 року склав від 48,16% до 52,67, що є значним показником. Для фільтрації спам-повідомлень широко застосовуються різноманітні спам-фільтри, принцип роботи яких, в основному будується на наївному класифікаторі Байєса [2]. Його робота побудована на алгоритмі штучного навчання. При навчанні фільтра для кожного слова, що зустрічається в листі вираховується і зберігається його «вага» - оцінка вірогідності того, що лист з цим словом – спам. Ефективність роботи такого фільтра сильно залежить від навчальних вибірок та від того, які саме частини електронного листа він оброблює [3].

Електронний лист має чітку структуру, в якій можна виділити кілька полів, що вимагають заповнення. Електронному повідомленню в структурі листа передує заголовок (header), який містить декілька полів даних, в тому числі службові:

- «from» – ім'я та адреса електронної пошти відправника. За замовченням тут міститься особова поштова адреса відправника;
- «sender» – автор або система відправника повідомлення;
- «to» – ім'я та електронна адреса отримувача. Дане поле є обов'язковим для заповнення.
- «subject» (тема) – необов'язкове, але бажане для заповнення поле. Воно містить відомості відправника про вміст листа або інші дані.
- «subject» – вміст повідомлення, що пересилається.

Дані для фільтрації, як правило, містяться в полі «subject».

Для організації систем електронного документообігу підприємств і організацій різної форми власності використовуються «хмарні» рішення, наприклад google docs та G-Suite. Дані системи прив'язуються до облікових записів користувачів і дозволяють отримувати доступ до сервісу електронного документообігу одразу ж після успішного проходження автентифікації

Формулювання задачі. В організації застосовується сервіс google docs, який має спам-фільтр. Хоча, ефективність фільтрації спам-повідомлень для сервісу gmail складає по різним даним до 95-97%, але ймовірність того, що до спаму потраплять по формальним ознаками листи, зміст яких при класифікації оцінюється в різних джерелах [4], як проблема «рідкісних» або «нейтральних» комбінацій є часто високою. Відповідно до статті 5 Закону України «Про звернення громадян» [5] лист повинен бути проаналізований і повернений відправнику (заявнику) в 10 денний термін в разі, якщо воно оформлене без дотримання вимог, та в п'ятиденний строк лист повинен бути переданий для редагування. Відповідно до статті 20 Закону України «Про звернення громадян» [5] максимальний термін розгляду звернень громадян не повинен перевищувати 30 або 45 днів, його зміст не підлягає розголосу. Отже, задача створення підсистеми інтелектуальної фільтрації спаму, яка підвищує ефективність обробки спам-повідомлень в системі електронного документообігу gmail, підвищує конфіденційність та доступність інформації є *актуальною***.**

Ситуація, коли лист з реальними зверненнями громадян потрапляють в папку «спам» пояснюється тим, що класифікатор gmail навчається на прикладах маси повідомлень всього поштового сервісу та не враховує тематики звернень громадян.

Виклад основного матеріалу. З метою вирішення задачі фільтрації спам-повідомлень в системі електронного документообігу на базі «хмарного» рішення gmail:

1. Введення механізму отримання вмісту папки «спам» для повторної обробки.

2. Під'єднання до бази даних електронної пошти засобами протоколу smtp. Для автентифікації особи обробника пошти окремий файл smtp.properties. Даний файл містить конфіденційну інформацію для автентифікації службовця, відповідального за обробку звернень громадян і має наступні дані автентифікації (рис.1).

Рисунок 1 – Файл автентифікації користувача підсистеми

Файл з реквізитами доступу є конфіденційним і зберігається на флеш-носії. Флеш – носій видається кожного робочого дня на початку робочого дня працівнику, вповноваженому здійснювати обробку електронних звернень типу «e-mail» та повертається даним працівником відповідальному за зберігання після закінчення робочого дня.

3. Обробка відфільтрованих штатним фільтром повідомлень електронної скриньки в базу даних Postgresql відбувається з використанням SQL – запитів.

4. Обробка отриманої інформації з поля «subject» реалізується додатковим фільтром на базі машинного інтелекту здійснюється з використанням файлу-шаблона наступного типу (рис.2).

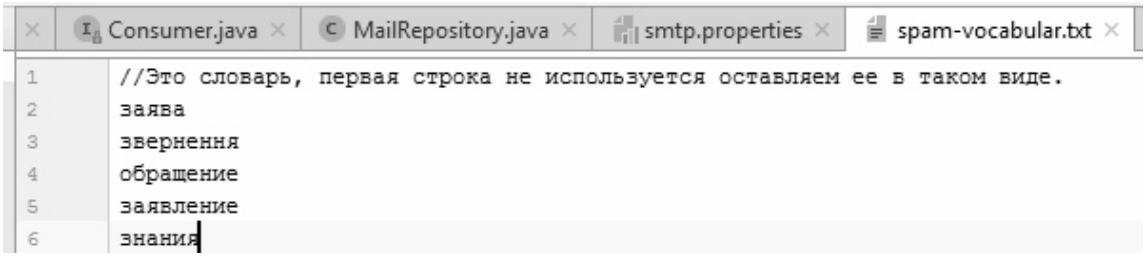


Рисунок 2 – Файл-шаблон для додаткового інтелектуального фільтру

Даний файл використовується в якості файлу – словника для алгоритму машинного навчання підсистеми електронної фільтрації. У випадку, якщо електронний поштовий лист – звернення містить слова або терміни, наведені в шаблоні (рис.2), він знову повертається в папку Inbox і підлягає розгляду, як автентичний.

5. Якщо електронний лист, що міститься в папці «спам» після повторної фільтрації все одно потрапляє у ту ж саму папку, то рішення, про його обробку приймається вручну вповноваженою особою.

Підсистема штучного інтелекту для інтелектуальної фільтрації електронної пошти була реалізована в середовищі IntelliJ IDEA 2017.3.4 (Community edition) мовою java.

Створена програма складається з пакету GmailProject, до складу якого входять пакети fileUtils, mail, user. Структура проекту наведено на рис.3.

Для тестування працездатності програми був створений проект test в складі пакету GmailProject з класом AppTest. Проект реалізує junit – тестування розробленого програмного додатку.

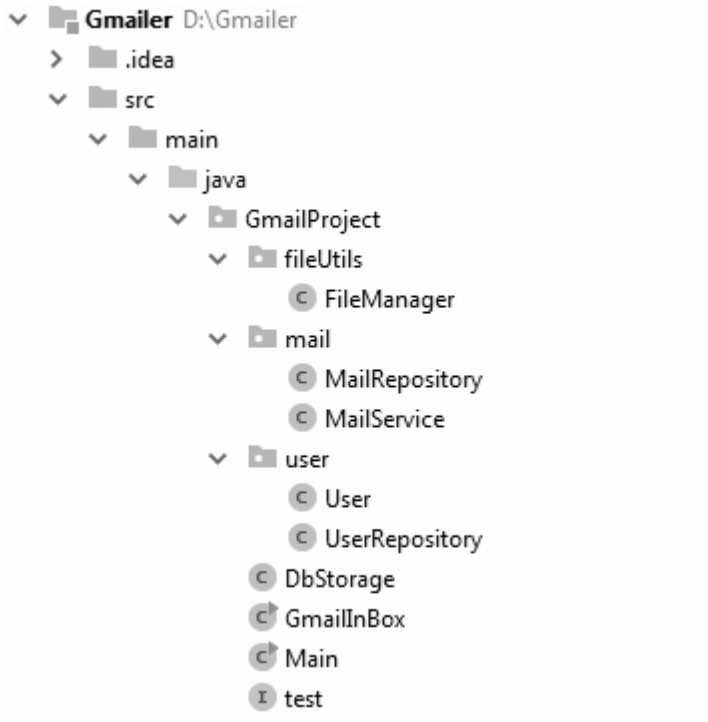


Рисунок 3 – Структура проекту програмного забезпечення підсистеми штучного інтелекту для інтелектуальної фільтрації електронної пошти

Висновки. Запропонована підсистема фільтрації електронних звернень на базі алгоритму машинного навчання знизила частоту хибних перенаправлень електронних листів в папку «спам» з 12-32 до 3-7 на місяць, що, в цілому, покращило рівень реагування і терміни розгляду електронних звернень.

Для розглянутого випадку ефективність роботи фільтрації залежить від якості навчання, яке залежить від коректності підібраної навчальної вибірки. Створене програмне забезпечення не потребує використання браузера, що зменшує ймовірність втручання в роботу шкідливого вірусного програмного забезпечення та покращує доступність інформації. Обраний підхід, щодо програмної реалізації підсистеми дозволяє збільшити мобільність обробки звернень через кросплатформеність отриманого java – програмного коду.

Список використаних джерел

1. *Dr. Horst Stipp. Global spam volume as percentage of total e-mail traffic from January 2014 to March 2018, by month [Електронний ресурс] / Dr. Horst Stipp // Statista. The Statistics Portal. – 2018. – Режим доступу до ресурсу: https://www.statista.com/statistics/420391/spam-email-traffic-share/.*
2. *Tianhao Sun. Spam Filtering based on Naive Bayes Classification [Електронний ресурс] / Tianhao Sun – 2009. – Режим доступу до ресурсу: http://www.cs.ubbcluj.ro/~gabis/DocDiplome/Bayesian/000539771r.pdf.*
3. *Naive Bayes spam filtering [Електронний ресурс] // Wikipedia. The free Encyclopedia. – 2018. – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Naive_Bayes_spam_filtering.*
4. *Байесовская фильтрация спама [Електронний ресурс] // intellect.ml. Искусственный разум. – 2017. – Режим доступу до ресурсу: https://intellect.ml/bajesovskaya-filtratsiya-spama-4749.*
5. *Закон України «Про звернення громадян» від 02.10.1996 р. №393.96-ВР зі змінами від 11.10.2018 [Електронний ресурс] / Законодавство України. – 2018. – Режим доступу до ресурсу: http://zakon2.rada.gov.ua/laws/show/393/96-%D0%B2%D1%80*

УДК 004.49

Гонтарь І. А.
Харківський національний університет радіоелектроніки

Методика виявлення вразливостей мереж стандарту IEEE 802.11 з використанням пакету KALI LINUX

На даний час розвиток підходів щодо побудови систем менеджменту інформаційної безпеки (СМІБ) йде в напрямку використання міжнародних стандартів сімейства ISO/IEC 27к. Відповідно до вимог даних стандартів обов'язком процесом є аудит СМІБ, завданням якого є оцінка технічних та організаційних вразливостей в захисних процедурах.

Мережі стандарту IEEE 802.11 активно використовуються для побудови безпроводових локальних мереж. Майже в усіх сучасних корпораціях, компаніях, навчальних закладах, ресторанах, готелях тощо використовується бездротові мережі даного стандарту.

Існують багато способів, які можна застосувати зловмисниками для атаки на компанію здійснивши злом локальної бездротової мережі [1]:

- нелегальне використання користувальницьких аккаунтів і привілеїв;
- крадіжка програмного забезпечення та даних;
- запуск виконуваного коду для пошкодження систем або даних;
- модифікація збережених даних;
- використання інформації для отримання фінансової вигоди або для промислового шпигунства;
- виконання дій, які не дають можливості легітимним користувачам отримувати доступ до мережевих сервісів і ресурсів;
- виконання дій, які поглинають мережеві ресурси і смугу пропускання та інші.

Тому розробка методики проведення активного аудиту для оцінки вразливостей бездротових мереж даного стандарту є актуальною задачею.

Одним з найкращих інструментальних засобів для проведення аудиту вразливостей бездротових мереж є програмний пакет Kali Linux. Kali Linux — це дистрибутив, оснований на ядрі Debian, та створений для проведення тестів на вразливості в системах. Основні можливості Kali Linux [2]:

- більше 600 інструментів для тестування на проникнення;
- Kali Linux повністю безкоштовний;
- Open source. Весь вихідний код, який входить до Kali Linux, доступний для всіх, хто хоче налаштувати або відновити процеси відповідно до конкретних потреб;
- FHS-сумісний: Kali дотримується стандартної ієрархії файлової системи, що дозволяє користувачам Linux легко знаходити файли підтримки, бібліотеки тощо.
- підтримка широкосмугових бездротових пристроїв: Kali Linux побудований таким чином, щоб підтримувати стільки бездротових пристроїв, наскільки можливо, що дозволяє правильно працювати на різноманітному апаратному забезпеченні та сумісності з багатьма USB та іншими бездротовими пристроями.
- користувальницьке ядро, призначене для ін'єкцій: як тестувальники проникнення, команда розробників часто потребує оцінок бездротового зв'язку, тому ядро містить останні патчі ін'єкцій.

В роботі розглядається використання пакету Kali Linux для аналізу парольного захисту бездротових мереж стандарту IEEE 802.11. Послідовність дій при проведенні аудиту парольного захисту наступні:

1. Виявлення протоколу безпеки (WEP, WPA чи WPA2) бездротової точки доступу.

2. Перехоплення пакету "handshake". Handshake WPA/WPA2 — це 4-стороннє рукостискання для аутентифікації пристроїв в мережі. Перехоплення цього пакету здійснюється під час авторизації пристрою до точки мережі.

3. Підбор паролю. Можна використати: перебір по словнику, радужні таблиці, прямий перебір через цифри та букви, нижнього та верхнього регістру тощо.

Для проведення всіх операцій, використовують AirCrack-NG, який представляє повний набір інструментів для оцінки безпеки бездротової мережі 802.11. Даний пакет дозволяє [3]:

- моніторинг: захоплення пакетів та експорт даних у текстові файли для подальшої обробки сторонніми інструментами;
- здійснення різних типів атак: повторні атаки, деаутентифікація, підроблені точки доступу та інші за допомогою пакетної ін'єкції;
- тестування: перевірка карт 802.11 та драйверів (захват і введення);
- злом: WEP і WPA PSK (WPA 1 і 2).

Інструменти, які входять до AirCrack-NG:

- airbase-ng - багатоцільовий інструмент, спрямований на атаку клієнтів, а не на точку доступу (реалізує атаку клієнта Caffe Latte WEP, Hirte WEP, має можливості захоплення рукостискання WPA / WPA2, діяти як спеціальна точка доступу, фільтрації по SSID або MAC-адресами клієнта, маніпулювати і пересилати пакети);
- aircrack-ng – ключова програма злому 802.11 WEP та WPA/WPA2-PSK;
- airdecap-ng - розшифровка захоплених файлів WEP / WPA / WPA2;
- airdecloak-ng - видалення WEP Cloaking ™ із файлу захоплених пакетів;
- airdrop-ng - інструмент для деавторизації бездротових пристроїв;
- aireplay-ng – дозволяє реалізувати ряд атак на бездротові мережі;
- airmon-ng - увімкнення та вимкнення режиму монітора на бездротових інтерфейсах;
- airodump-ng - захоплення даних 802.11 кадрів;
- airolib-ng - призначений для зберігання та керування списками паролів, обчисленням паролів та їх використанням для злому WPA / WPA2;
- airserv-ng - бездротова картка TCP / IP;
- airtun-ng - створення віртуального тунельного інтерфейсу;
- packetforge-ng - створювання різних типів зашифрованих пакетів, які можна використовувати для ін'єкцій.

В доповіді розглядається методика виявлення паролю бездротової точки доступу за допомогою інструментів "Aircrack-ng". Також в доповіді детально розглянуто, які деструктивні дії можна здійснити при підключенні до мережі та які існують прості атаки на бездротові мережі. Також було представлено деякі програми, які можуть атакувати бездротову точку доступу з різних MAC-адресів, навіть обходячи MAC-фільтри.

Список використаних джерел

1. *Атаки на сеть стандарта Wi-Fi [Електронний ресурс]. – Режим доступу: http://wi-life.ru/treningi/wi-fi-3/praktikum/ataki-na-set-wi-fi.*
2. *Kali Linux. Official Documantation [Електронний ресурс]. – Режим доступу: https://docs.kali.org /introduction/what-is-kali-linux.*
3. *Aircrack-ng[Електронний ресурс]. – Режим доступу: https://www.aircrack-ng.org/documentation.html.*

УДК 004.056

Грек О. М., Марчук А. В.
Харківський національний університет радіоелектроніки

Розробка технологій захисту від мережних атак із використанням апарату штучних нейронних мереж

Важливою складовою процесу забезпечення мережної безпеки є проектування Intrusion Detection System (IDS). До недоліків існуючих моделей IDS можна віднести вразливість до нових атак, низька точність і швидкість роботи.

У зв'язку з перерахованими вище та іншими недоліками відбувається пошук системи, яка б була пристосована до сучасних умов забезпечення мережної безпеки. Одним із найперспективніших напрямків у даній сфері є використання штучних нейронних мереж (ШНМ).

Науковою задачею у даній роботі є дослідження моделей ШНМ, які застосовуються для побудови IDS, та визначення найоптимальнішого варіанта їх використання.

Робота із ШНМ передбачає наявність таких етапів: збір та підготовка вхідних даних, побудова та навчання мережі, тестування мережі і аналіз результатів [1].

Пропонується використовувати базу даних NSL-KDD-99 для навчання та тестування ШНМ. Вона містить близько 5 мільйонів записів про з'єднання. У KDD-99 представлені атаки, розділені на 4 категорії: Denial Of Service (DoS), Users to Root (отримання зареєстрованим користувачем привілеїв адміністратора), Remote to Local (віддалений доступ незареєстрованого користувача до комп'ютера) і Probe (сканування портів).

Для побудови IDS пропонується використовувати багатошаровий перцептрон (Multilayer Perceptron – MLP), навчання якого проводиться за правилом зворотного розповсюдження помилки, Recirculation Neural Network (RNN) та ШНМ Кохонена.

Першим варіантом є IDS, що складається з RNN і MLP, з'єднаних послідовно. Задачею RNN є стиснення вхідного вектора у вихідний. MLP виконує обробку стиснутого простору вхідних образів з метою розпізнавання класу атаки.

У другому варіанті IDS головні компоненти із виходів RNN одночасно надходять на 4 окремих MLP, кожен із яких відповідає певному класу атаки. Із выходів MLP дані надходять до модуля, який приймає остаточне рішення щодо стану системи. В якості такого модуля може використовуватися лінійний або багатошаровий перцептрон.

Суть третьої моделі IDS полягає у використанні ШНМ Кохонена із одним вхідним шаром, одним прихованим шаром, що складається із нейронів Кохонена, і вихідним шаром. Для навчання використовується навчальна вибірка, що складається з 80 % мережних атак і 20 % нормальних мережних з'єднань.

Згідно з результатами тестування, друга та тертя моделі мають найкращі результати та можуть застосовуватися для захисту від мережних атак, таких як DoS, отримання зареєстрованим користувачем привілеїв адміністратора, отримання доступу незареєстрованого користувача до комп'ютера з віддаленої машини і сканування портів.

Наступним етапом роботи є програмна реалізація алгоритмів виявлення мережних атак із використанням розглянутих моделей ШНМ та вибір найкращого рішення для практичного застосування.

Список використаних джерел

1. *Технологии обнаружения сетевых атак [Електронний ресурс]. – 2015. – Режим доступу до ресурсу : https://studfiles.net/preview/3021269/.*

УДК 004.38

Гриб О. О.[*]
Центральноукраїнський національний технічний університет

Особливості роботи брандмауерів

Важко уявити світ без брандмауерів. Вперше розроблені як спосіб вирішення або обмеження зовнішнього доступу до певних мережевих ресурсів, брандмауери в даний час здатні забезпечити дотримання політик мережевої безпеки, протоколювання активності в Інтернеті та забезпечення захисту організації від зовнішніх загроз.

Сьогодні те, що ми називаємо брандмауерами наступного покоління, ґрунтується на тому ж аналізі, що і на прикладному рівні, але з більшою зосередженістю на інтроспекції глибоких пакетів. З цією метою брандмауери наступного покоління можуть використовуватися для реалізації таких функцій, як виявлення і запобігання вторгнень, інтеграція з ідентифікаторами користувачів і брандмауери веб-додатків. Додавання послуг віртуальної приватної мережі в брандмауерах також є широко поширеною практикою з боку компаній, оскільки це дозволяє співробітникам поза офісом отримувати доступ до ресурсів компанії при спілкуванні з небезпечними мережевими з'єднаннями, такими як громадський Wi-Fi.

Брандмауери інтегруються в безліч мережевих пристроїв, щоб фільтрувати трафік і знизити ризик того, що шкідливі пакети, що подорожують через загальнодоступний Інтернет, можуть впливати на безпеку приватної мережі. Брандмауери також можна придбати як автономні програмні додатки.

Термін брандмауер - це метафора, яка порівнює тип фізичного бар'єру, який застосовується для обмеження пошкоджень, який може спричинити пожежа, з віртуальним бар'єром, який встановлюється для обмеження пошкоджень від зовнішньої або внутрішньої атаки. Розташовані по периметру мережі, брандмауери забезпечують захист мережевого рівня, а також важливі функції журналювання та аудиту.

Окрім двох основних типів брандмауерів - на базі хоста та мережі, існує безліч різних типів, які можна встановлювати в різних місцях та контролювати різні дії. Брандмауер на базі хоста встановлюється на окремих серверах та контролює вхідні та вихідні сигнали. Мережевий брандмауер можна вбудувати в інфраструктуру хмари, або це може бути службою віртуального брандмауера.

Види брандмауерів: брандмауери, що фільтрують пакети; брандмауер перевірки стану; брандмауер проксі-сервера.

Коли організації почали переходити від енциклопедичних комп'ютерів та німих клієнтів до моделі клієнт-сервер , пріоритетом стала можливість контролювати доступ до сервера. Перш ніж з'явилися перші брандмауери наприкінці 1980-х років, єдиною реальною формою забезпечення мережевої безпеки було встановлення доступу через списки контролю доступу, що розташовуються на маршрутизаторах. ACL вказували, яким адресам Інтернет-протоколу (IP) надавати або відмовляти в доступі до мережі.

Однак експоненціальний ріст Інтернету і, як наслідок, збільшення підключення до мереж, означали, що фільтрація мережевого трафіку за допомогою лише IP-адреси стала недостатньою. Статичні фільтри пакетного фільтрування міжмережевих екранів, які вивчають заголовки пакетів та використовують правила для прийняття рішень про те, який трафік пропустити, можливо, були найважливішою частиною кожної ініціативи з безпеки мережі до кінця минулого століття.

Як же працюють брандмауери, що фільтрують пакет. Коли пакет проходить через

[*] Науковий керівник – Гермак В. С., викладач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету

брандмауер із фільтрацією пакетів, перевіряється його вихідна та цільова адреси, номер протоколу та номер порту призначення. Пакет скидається - він не передається у пункт призначення - якщо він не відповідає встановленому правилу брандмауера.

Брандмауери для фільтрації пакетів працюють переважно на мережевому рівні еталонної моделі OSI, хоча транспортний рівень використовується для отримання номерів порту джерела та призначення. Вони вивчають кожен пакет незалежно і не знають, чи який-небудь даний пакет є частиною існуючого потоку трафіку. Брандмауери, що фільтрують пакет, є ефективними, але тому, що вони обробляють кожен пакет окремо, вони можуть бути вразливими до атак зловмисників IP і багато в чому були замінені брандмауерами із перевіркою стану.

Як працює брандмауер перевірки стану. Стандартні брандмауери перевірки стану, також відомі як динамічні фільтри брандмауера, що підтримують пакет, підтримують таблицю, яка відстежує всі відкриті з'єднання. Коли з'являються нові пакети, брандмауер порівнює інформацію в заголовку пакетів до таблиці стану та визначає, чи є це частиною встановленого з'єднання. Якщо це є частиною існуючого з'єднання, то пакет допускається без подальшого аналізу. Якщо пакет не збігається з існуючим з'єднанням, він оцінюється відповідно до правила, встановленого для нових з'єднань.

Станція перевірки брандмауерів контролює пакети зв'язку протягом певного періоду часу і розглядає як вхідні, так і вихідні пакети. Існуючі пакети, які є запитами для певних типів вхідних пакетів, відстежуються, і через брандмауер дозволяються лише ті вхідні пакети, які надають відповідну відповідь. Незважаючи на те, що брандмауери, які перевіряють стан, досить ефективні, вони можуть бути вразливими до атак на відмову в обслуговуванні (DoS).

Як працюють брандмауери прикладного рівня і проксі-сервера. Оскільки атаки на веб-сервери стали більш поширеними, стало очевидним, що для захисту мереж від атак на рівні додатків потрібні брандмауери. Брандмауери для пакетної фільтрації та перевірки стану не можуть відрізняти дійсні запити протоколу додаткового рівня, дані та шкідливий трафік, інкапсульовані в очевидно діючий протокольний трафік.

Брандмауерами, що забезпечують фільтрацію прикладного рівня, можна перевірити корисну інформацію пакета та розрізняти дійсні запити, дані та шкідливий код, замаскований як дійсний запит або дані. Оскільки цей тип брандмауера приймає рішення на основі корисного вмісту, він надає інженерам безпеки більш грамотний контроль над мережевим трафіком і встановлює правила для дозволу або відхилення певних запитів або команд програми. Наприклад, він може дозволити або заборонити конкретну вхідну команду Telnet від конкретного користувача, тоді як інші брандмауери можуть контролювати лише загальні вхідні запити з певного хоста.

Якщо на місці встановлено брандмауер проксі-сервера, клієнт і сервер змушені проводити сеанс через посередника - проксі-сервер, на якому розміщено брандмауер прикладного рівня. Тепер кожен раз, коли зовнішній клієнт запитує зв'язок із внутрішнім сервером (або навпаки), клієнт замість цього відкриє з'єднання з проксі. Якщо з'єднання відповідає критеріям бази основного правила брандмауера, проксі-сервер відкриє зв'язок із запитуваним сервером. Оскільки брандмауер поміщається в середині логічного з'єднання, він може спостерігати за трафіком за будь-якими ознаками шкідливої активності на рівні додатків.

Брандмауери будуть продовжувати розвиватися, і ясно, що їх діапазон можливостей і функціональність також буде розширюватися.

Список використаних джерел

1. Балдін Костянтин, Уткін Володимир «Інформатика», 2003р.
2. Дьяконов Володимир, Абраменкова Ірина, Пеньков Олександр «Нові інформаційні технології», 2006.
3. Фрідланд А. «Основні ресурси інформатики», 2007р.

УДК 004.056.53

Григоров А. Г.
Харківський національний університет внутрішніх справ

Актуальність протидії XSS-атакам та засоби захисту від них

XSS (англ. Cross Site Scripting — «міжсайтовий скриптинг») — тип вразливості інтерактивних інформаційних систем у вебі. XSS виникає, коли на сторінки, які були згенеровані сервером, з якоїсь причини потрапляють користувацькі скрипти. Специфіка подібних атак полягає в тому, що замість безпосередньої атаки сервера зловмисники використовують вразливий сервер для атаки на користувача. Для терміну використовують скорочення «XSS», щоб не було плутанини з каскадними таблицями стилів (абревіатура «CSS»). Довгий час програмісти не приділяли їм належної уваги, вважаючи їх безпечними. Однак ця думка помилкова: на сторінці або в HTTP-Cookie можуть бути досить вразливі дані (наприклад, ідентифікатор сесії адміністратора). На популярному сайті скрипт може влаштувати DoS-атаку.

Web-додатки є одними з найбільш небезпечних систем на сьогоднішній день. І, звичайно, хакери цим користуються. Одним з видів атак на додаток є міжсайтовий скриптинг або XSS атака. Зараз вони складають близько 15% всіх атак виявлених вразливостей сайтів.

XSS атака - це атака на вразливість, яка існує на сервері, що дозволяє впровадити в генеруєму сервером HTML-сторінку якийсь довільний код, в якому може бути взагалі все що завгодно і передавати цей код в якості значення змінної, фільтрація по якій не працює, тобто сервер не перевіряє дану змінну на наявність в ній заборонених знаків -, <,>, ', ".

Значення цієї змінної передається від генеруємої HTML-сторінки на сервер в скрипт, її викликавший шляхом відправки запиту. А далі починається найцікавіше для зловмисника. PHP-скрипт у відповідь на даний запит генерує HTML-сторінку, в якій відображаються значення потрібних хакеру змінних, і відправляє цю сторінку на браузер зловмисника. [1] Тобто, кажучи простіше, XSS атака - це атака за допомогою вразливостей на сервері на комп'ютери клієнтів. XSS атака найчастіше використовується для крадіжки Cookies. У них зберігається інформація про сесії перебування користувача на сайтах, що і буває потрібним хакерам для перехоплення управління особистими даними користувача на сайті в межах, поки сесія не буде закрита сервером, на якому розміщений сайт.Крім цього в Cookies зберігається зашифрований пароль, під яким користувач входить на даний сайт, і при наявності необхідних утиліт і бажання зловмисникам не дуже важко розшифрувати даний пароль.

Наведемо інші можливості XSS атак (звичайно за умови їх успішного проведення). Можливо при відкритті сторінки викликати відкриття великої кількості непотрібних користувачеві вікон. Можлива взагалі переадресація на інший сайт (наприклад, на сайт конкурента або якого-небудь "Parimatch").

Існує можливість завантаження на комп'ютер користувача скрипта з довільним кодом (навіть шкідливого) шляхом впровадження посилання на виконуваний скрипт зі стороннього сервера. Найчастіше відбувається крадіжка особистої інформації з комп'ютера користувача, крім Cookies в якості об'єкта крадіжки виступає інформація про відвідані сайти, про версії браузера і операційної системи, встановленої на комп'ютері користувача, та до того ж ще й плюсується IP-адреса комп'ютера користувача.

XSS атака може бути проведена не тільки через сайт, але і через уразливості в програмному забезпеченні (зокрема, через браузери). Тому рекомендується оновлювати використовуєме програмне забезпечення. Також можливе проведення XSS атак через використання SQL-коду. Хакер може опанувати вашою особистою інформацією аж до отримання паролів доступу до сайтів, а це дуже неприємно. До того ж XSS атака завдає шкоди виключно клієнтським машинам, залишаючи сервер в повністю робочому стані, і у адміністрації різних серверів часом мало стимулів встановлювати захист від цього виду атак.

Розрізняють XSS атаки двох видів: активні і пасивні. При першому виді атаки шкідливий скрипт зберігається на сервері і починає свою діяльність при завантаженні сторінки сайту в браузері клієнта. При другому виді атак скрипт не зберігається на сервері і шкідливий вплив починає виконуватися тільки в разі будь-якого дії користувача, наприклад, при натисканні на сформоване посилання.

З метою реалізації радикальних заходів безпеки, які запобігають XSS-атаки, ми повинні пам'ятати про перевірку даних, санітарної обробки даних, і екранування.

Способи боротьби з даним видом атак такі:

1) Перевірка коректності.

Перевірка даних це процес забезпечення того, щоб ваш додаток працював з правильними даними. Якщо ваш PHP скрипт очікує ціле число, для введення даних користувачем, то будь-який інший тип даних буде відхилений і користувач отримає повідомлення про це. Кожна частина призначених для користувача даних повинна бути перевірена при отриманні. Перевіряйте дані як на стороні клієнта, так і на стороні сервера, оскільки перевірку на стороні клієнта надзвичайно легко перехитрити. Дотримуйтесь послідовної стратегії захищеності додатка, грунтуючись на передовому досвіді розробки захищених додатків.

2) Заборонити включення безпосередньо параметрів $ _GET, $ _POST, $ _COOKIE в генеруєму HTML-сторінку 3) Заборонити завантаження довільних файлів на сервер, щоб уникнути завантаження шкідливих скриптів. Всі завантажені файли зберігати в базі даних, а не в файлової системі.

4) Екранування даних.

Для того, щоб захистити цілісність відображення вихідних даних, ви повинні екранувати їх. Це запобіжить спробі браузера ненавмисно спотворити зміст спеціальних послідовностей символів, які можуть бути знайдені ним.

З н7аведеного можна зробити висновки:

1. Атака, пов'язана з міжсайтовою підробкою запиту, досить проста в реалізації, та, отже, часто зустрічається.

2. Існує досить багато варіантів реалізації подібного роду атак, та в багатьох випадках ключову роль відіграє саме людський фактор, а не продумані дії зловмисника.

3. Проблема є актуальною з моменту появи Інтернету і до тепер, що пов'язано з великими темпами зростання кількості веб-ресурсів.

4. Атаки такого роду можуть завдати серйозної шкоди сайту або ж конкретному користувачу.

Список використаних джерел

1. http://ru.wikipedia.org/wiki/Межсайтовый_скриптинг
2. https://dspace.ncfu.ru/bitstream/20.500.12258/57/1/Шахгильдянц А.Т._13.01.18.pdf
3. http://intsystem.org/768/learn-about-csrf-intro/

УДК 004.056.5

Гуреєва А. О., Карабут Н. О.
Криворізький національний університет

Методи і технології захисту комп'ютерних мереж (фізичний та канальний рівні)

Питання захисту комп'ютерних мереж від можливих атак, направлених на порушення функціонування мереж та окремих вузлів, несанкціонованого доступу до інформації та несанкціонованого використання сервісів мережі є одним з актуальніших, особливо для корпоративних мереж, до яких відносяться і мережі вищих навчальних закладів. Для захисту мереж розробляються і реалізуються комплексні системи захисту інформації, які складаються з набору організаційно-технічних заходів, від правил роботи користувачів у корпоративній мережі та розмежування прав доступу до інформаційних ресурсів та сервісів, до встановлення та налаштування високо функціональних апаратно-програмних комплексів, міжмережних екранів для захисту корпоративної мережі від зовнішніх атак.

Існує досить велика кількість підходів до класифікації загроз та можливих атак на комп'ютерні мережі. Враховуючи, що апаратні та програмні засоби комп'ютерних мереж працюють на відповідних рівнях моделі взаємодії відкритих систем, для аналізу методів і технологій захисту використаємо класифікації, які орієнтовані на модель OSI. Найбільша кількість атак найчастіше реалізується на п'яти рівнях (фізичний, канальний, мережний, транспортний, прикладний). Загрози на сеансовому та представницькому рівнях пов'язані, в першу чергу, з процедурами ідентифікації, автентифікації та шифрування, алгоритми і протоколи яких реалізовані в операційних системах і вплив на роботу яких з боку адміністраторів мереж мінімальний.

Зупинимось на розгляді технологій захисту фізичного та канального рівнів.

Найбільш розповсюдженими атаками фізичного рівня на такі об'єкти, як канали передачі даних, є:

- фізичне пошкодження;
- несанкціоновані зміни у функціональному середовищі;
- вимкнення фізичних каналів передачі даних;
- постановка шумів по всій полосі пропускання каналу.

Для реалізації каналів передачі у сучасних мережах використовуються обмежені середовища та необмежені середовища передачі. Вибір середовища передачі для побудови каналів передачі даних здійснюється виходячи з таких основних вимог: призначення каналу та його довжина, безпека передачі інформації, швидкість передачі даних, електромагнітна сумісність, вартість створення і експлуатації.

З точки зору захисту від наведених вище атак найбільш захищеним рішенням є використання оптичного кабелю. Оптичний канал за своєю фізичною природою унеможливлює прослуховування, зняття інформації та постановку шумів. Пропускна здатність оптичних каналів з використанням сучасних технологій щільного та розрідженого мультиплексування за довжинами хвиль може досягати декількох сотень Гб/с, а мінімальна протяжність без використання проміжного підсилення від 10 до 40км.

Як альтернативу для коротких відстаней (до 100м), яка дозволяє захиститися від атак, пов'язаних з електромагнітним впливом на канал, можна використати екрановану звиту пару

Тим не менш, для побудови мереж доступу найбільш розповсюдженим рішенням є використання незахищеної звитої пари та безпроводових технологій. Такі рішення

найменш захищені від згаданих вище атак. Єдиною можливістю захисту від несанкціонованого доступу до інформації при використанні таких ліній зв'язку є шифрування даних.

Для запобігання можливим атакам, направленим на несанкціоновані зміни у функціональному середовищі, необхідно, перш за все, забезпечити обмеження фізичного доступу до кабельних каналів, комутаційних вузлів та дата-центрів, розробити та реалізувати політику віддаленого доступу до мережного обладнання, розгорнути допоміжні системи відеоспостереження та контролю доступу. Важливим фактором при забезпеченні надійності роботи інформаційно-комунікаційних систем можна вважати резервування найбільш критичних каналів, мережних пристроїв та серверів.

Найбільш розповсюдженими атаками канального рівня є генерація широкомовних кадрів з метою перевантаження каналів передачі даних і комутаційного обладнання. Технології захисту канального рівня передбачають, перш за все, роботу з MAC-адресами вузлів, хоча ряд захисних функцій комутаторів аналізує і використовує й IP–адреси вузлів, що розширює область їх дії і на мережний рівень.

Можна виділити такі підходи до захисту на канальному рівні:

- застосування MAC-фільтрації та прив'язок MAC-адрес до портів комутаторів;
- застосування додаткових захисних функцій комутаторів, таких, як DHCP;
- сегментація мережі на окремі зони з використанням технології віртуальних локальних мереж;
- автентифікація та авторизація на канальному рівні.

Задача створення ефективних комплексних систем захисту комп'ютерних мереж може бути вирішена з використанням сукупності методів та технологій, які реалізовані в сучасному телекомунікаційному обладнанні для комп'ютерних мереж, як основи технічної складової таких систем. Виходячи з найбільш поширених загроз фізичного (фізичне пошкодження, несанкціоновані зміни у функціональному середовищі, вимкнення фізичних каналів передачі даних, постановка шумів по всій полосі пропускання каналу) та канального (генерація широкомовних кадрів з метою перевантаження каналів передачі даних і комутаційного обладнання, підміна MAC-адрес вузлів, атаки на ARP і Spanning-Tree протоколи) рівнів моделі OSI проаналізовано особливості методів і технологій захисту та визначено, для вирішення яких задач захисту вони можуть бути застосовані. Розглянуті підходи до захисту на канальному рівні (застосування MAC-фільтрації та прив'язок MAC-адрес до портів комутаторів, застосування додаткових захисних функцій комутаторів, таких, як DHCP Snooping, Dynamic ARP Inspection, IP SourceGuard, сегментація мережі на окремі зони (домени широкомовлення) з використанням технології віртуальних локальних мереж, автентифікація та авторизація на канальному рівні) дозволяють ефективно протидіяти внутрішнім порушенням інформаційної безпеки. Проведений аналіз методів та технологій захисту дозволяє прийняти обґрунтовані рішення щодо вибору методів захисту для мереж різного призначення та з різними вимогами щодо захисту інформації.

Список використаних джерел

1. *B. Y. Korniienko, "Doslidzhennia modeli vzaiemodii vidkrytykh system z pohliadu informatsiinoi bezpeky [Research of open systems interconnection model in terms of information security]," Sci. Technol., vol. 15, no. 3, pp. 83–89, 2012,*
2. *M. V. Graivoronsky and O. M. Novikov, Bezpeka informatsino-komunikatsinikh sistem [Safety of the information and communication systems]. Kyiv, Ukrane: Vydavnicha hrupa BHV, 2009.*

УДК 004.04:005.31

Дмитрієва О. А., Горбенко В. Ю.
ДВНЗ «Донецький національний технічний університет»

Створення відмовостійких розподілених інформаційних систем

Обнародування технології Інтернет породило новий формат споживання інформації. Традиційно комп'ютер асоціюється з фразою «передача даних», але вибух пристроїв на ринку портативних і мобільних пристроїв привів до ще одного «велетенського гравця» у сфері мережевого трафіку. Якщо узяти кількість пристроїв, працюючих на Java, то, відповідно до офіційних заяв компанії Oracle, це – близько трьох мільярдів девайсів. І це ще не врахувуючи інші сервіси, платформи та гібридні технології в нових поколіннях телевізорів зі своєю власною ОС, браузером і додатками. Усе це веде до високих статичних навантажень на ту або іншу систему, платформу чи додаток. Створити простий сервіс на популярній мові програмування, «найсвіжішому» і «багатообіцяючому» стеку технологій досить тільки для невеликого прототипування. Звичайно, можна масштабуватися вертикально, нарощуючи обчислювальну потужність сервера, але все-таки у цього способу є ліміт, який, на жаль, більше неможливо розширити. У зв'язку з проблемою з'явилося таке поняття, як «горизонтальне масштабування», що в подальшому було класифіковане як «розподіл». На даний момент проектування, реалізація та підтримка розподілених інформаційних систем (РІС) є складним, трудомістким процесом [1]. Постійно здійснюється пошук технології [2,3] і методики для максимального спрощення й здешевлення витрат на розробку.

Принципи побудови та характеристики є невід'ємною частиною для РІС. Правильна реалізація дозволять створити масштабовану систему, у тому числі придатну для подальшого додавання функціональних частин. Об'єктом цієї роботи є дослідження та аналіз побудови оптимальної інформаційної системи для пошуку та планування подій. Предметом роботи є кластеризація та розділення системи. Метою роботи є реалізація вибраного підходу і подальша оцінка трудомісткості й витрат.

Для створення розділених систем використовуються реляційні СУБД або NoSQL-рішення. Прикладами можуть виступати MySQL і MongoDB, що додають побічний ефект у вигляді узгодженості по закінченню, який помітний при нарощуванні вузлів реплікування. Альтернативою виступає консистентне хешування, в основі якого лежить проста техніка визначення вузла для зберігання або отримання даних за обумовленою хеш-функцією. Цей підхід найчастіше інкапсульований у БД. Cassandra, DynamoDB або CouchDB є найбільш популярними представниками таких БД. Можливий гібрид для забезпечення високої швидкості читання та запису, але специфіка на рівні сховища вимагає гранично точної і правильної нормалізації чи денормалізації даних.

Висновки. В результаті роботи був реалізований метод розподілу за допомогою розбиття на «партиції» за обраною ознакою. Була створена відмовостійка система, яка не втрачає свою працездатність під час відмови елементів системи. Вдалося зменшити час пошуку за заданим критерієм за рахунок паралельного обчислення на більш гранульованих даних. Варто відмітити, що вартість розподілу системи значно менша, зокрема, при достатній кількості обчислювальних вузлів середньої потужності, порівняно з суперкомп'ютерами.

Список використаних джерел

1. *Tanenbaum A. Distributed Systems: Principles and Paradigms / A. Tanenbaum, M. Van Steen. – 2006.*
2. *Coulouris G. Distributed systems: Concepts and Design / G. Coulouris, J. Dollimore, T. Kindberg. – 2011.*
3. *Tamer Özsu M. Principles of Distributed Database Systems / M. Tamer Özsu. – 2011.*

УДК 004.056.5

Добринін К. І.
Харківський національний університет радіоелектроніки

Засоби забезпечення захисту аккаунтів користувачів при використанні публічних мереж стандарту 802.11

На сьогоднішній день практично кожний користувач мережі Internet зазвичай частіше використовує бездротові мережі, ніж дротове з'єднання для виходу у мережу. Сумісно з цим, інтенсивний розвиток бездротових мереж веде к підвищенню інтересу до них з боку зловмисників, якими здійснюються певні заходи щодо отримання конфіденційної інформації, у тому числі й інформації, яка потребує даних облікових записів легальних користувачів мережі.

Приймаючи до уваги зростання загроз інформаційній безпеці, вочевидь, потрібні грамотні заходи щодо захисту інформації у зазначених системах. Особливо актуальною ця задача стає при масовому впровадженні відкритих публічних мереж, які активно впроваджуються муніципальними закладами, наприклад у ресторанах, вокзалах, аеропортах та ін. масових місцях.

Особливістю зазначених інформаційних мереж є те, що вони використовують загальнодоступний радіоканал для зв'язку абонентів та так звану відкриту аутентифікацію. У процесі відкритої аутентифікації здійснюється обмін повідомленнями двох типів: запит та підтвердження аутентифікації. Таким чином, при відкритій аутентифікації можливий доступ будь-якого клієнта до локальної мережі, що являє собою загрозу безпеці інформації.

У доповіді представлений аналіз захищеності аккаунтів користувачів при використанні публічних мереж стандарту IEEE 802.11. Для проведення аналізу захищеності використовувався метод активного аудиту. В ході його проведення, за допомогою спеціального програмного забезпечення (програм-сніфферів WireShark та Intercepter -NG), у навчальному середовищі здійснювався збір інформації, яка передавалась від легальних користувачів мережі для доступу до ресурсів мережі Internet.

Показано, що за допомогою зазначених сніфферів є можливість перехоплення пакетів даних, що передаються протоколами HTTP, POP3, SMTP та ін. Аналіз перехоплених пакетів показав, що за допомогою зазначених програм-сніфферів виявляються облікові записи користувачів, паролі їх електронної пошти, паролі від їх соціальних мереж, паролі їх авторизації на інших ресурсах та ін. Це актуально, тому що відкриті точки доступу ніяк не шифрують пакети, а тому перехопити їх здатний будь-який бажаючий. Програм-сніфферів існує чимало, причому не тільки для настільних операційних систем, але і для смартфонів під управлінням Android. Все це унеможливлює забезпечення цілісності, доступності та конфіденційності даних.

Програма-сніффер – це програма або програмно-апаратний пристрій, призначений для перехоплення і подальшого аналізу, або тільки аналізу мережного трафіку, призначеного для інших вузлів.

Підхід до захисту акантів користувачів стає ще більш актуальним у тому випадку, якщо у компаніях передбачається використання технологій CYOD або BYOD. Так, враховуючи можливу мобільність кінцевих користувачів, не можна виключати їх підключення до відкритих публічних мереж з метою отримання/передачі певної інформації, яка може містити конфіденційну інформацію.

Відомо, що знизити загрозу сніффінга пакетів можна за допомогою різноманітних заходів, основними з яких є:

– використання апаратних або програмних засобів, які розпізнають сніффери;

– використання аутентифікації за технологією OTP – one time passwords;

– застосування засобів криптографії (формування криптографічно захищеного каналу зв'язку);

– формування комутованої інфраструктури.

Однак, вищевказані заходи не завжди є фізично здійсненими саме у публічних мережах.

У доповіді показано, що у якості механізмів, спрямованих на захист аккаунтів користувачів при використанні публічних мереж стандарту IEEE 802.11, можна вважати наступне:

1. Для підприємств та компаній є вкрай важливим коректно та якісно прописати Політику інформаційної безпеки організації. Основна мета Політики у даному питанні – це категорична заборона співробітникам організації звертатися до корпоративної пошти та іншим корпоративним ресурсам за допомогою публічних мереж.

2. Для звичайних (приватних) користувачів актуальним є наступне:

- не підключатися до невідомих Wi-Fi мереж;
- вимикати Wi-Fi на персональному гаджеті у той час, коли він не використовується;
- за можливістю - використовувати Virtual Private Network (VPN) та захищені протоколи доступу, наприклад HTTPS;
- при доступі до ресурсів мережі, які вимагають авторизацію (соціальні мережі, форуми та ін.) не використовувати політику запам'ятовування паролів;
- використовувати складну (двохфакторну) аутентифікацію з використанням технології OTP;
- не відвідувати сайти, про відвідування котрих не повинні знати треті особи;
- за можливістю – підключатися тільки до офіційної Wi-Fi мережі закладу;
- не підтверджувати перехід за підозрілими посиланнями та з потенційно хибним сертифікатом;
- не проводити через публічну мережу фінансові операції;
- заборонити спільний доступ до сторонніх ресурсів свого пристрою;
- використовувати брандмауер.

Отже, публічні Wi-Fi мережі можуть стати серйозною загрозою, якщо не вжити необхідні запобіжні заходи. Всі вищевказані заходи покликані захистити персональні дані та конфіденційну інформацію.

Список використаних джерел

1. *Lee Allen. Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide [Текст] /L. Allen - «Packt Publishing», 2012. – 216p.*
2. *Сніффер під Windows Intercepter-NG [Електронний ресурс]. - Режим доступу до ресурсу: https://hackware.ru/?p=3051 .*
3. *Точки доступу Wi-Fi - захист даних [Електронний ресурс]. – Режим доступу до ресурсу: https://www.comss.ru/page.php?id=1556*

УДК 003.26:004.056.55

Журова П. В.
Черкаський державний технологічний університет

Блочне шифрування з властивостями виправлення помилок

Надійне та безпечне збереження інформації безпосередньо пов'язано із розвитком та застосуванням нових методів та засобів криптографічного захисту інформації [1, 2]. Одними із поширених підходів для розв'язання цих задач є застосування симетричних алгоритмів шифрування, зокрема блочних шифрів (БШ), що дозволяє забезпечити конфіденційність передачі даних у відкритих каналах Зв'язку. Разом з цим, при передачі даних можуть виникати різноманітні спотворення, обумовленні якістю каналів передачі даних, що призводить до втрат повідомлення і унеможливлює забезпечення якості та надійності передачі на заданому рівні. Виникає потреба не тільки у шифруванні даних, але і забезпеченні надійного процесу їх передачі [3, 4]. Отже, актуальною задачею є розробка нових підходів і методів по забезпеченню надійного шифрування та передачі даних. Метою роботи є розробка методів і засобів блочного шифрування з властивістю виправлення помилок для реалізації надійного процесу передачі інформації.

Проведені дослідження показують, що БШ можуть бути використані для виконання завадостійкого кодування, причому побудовані на їх основі коди мають ряд важливих для практичного застосування особливостей, зокрема поєднання шифруючих і кодуючих властивостей в єдиному перетворенні, а також можливість виправлення помилок різної природи: інверсії бітів, пропуски і вставки бітів в переданому блоці даних тощо.

На основі проведеного аналізу існуючих систем щодо застосування БШ із властивістю виправлення помилок розроблений концепт реалізації програмного комплексу та визначені якісні характеристики роботи системи.

Запропоновано спосіб побудови алгоритмів криптокодування на основі функції блочного шифрування, які в рамках єдиного процесу перетворення реалізують захист переданої інформації від несанкціонованого доступу і можливість виправлення помилок передачі даних по каналу Зв'язку з шумом. Даний підхід являє собою застосування блокових шифрів в режимі виправлення помилок, реалізація якого забезпечується оборотністю шифрувального перетворення. Перевагою даного підходу є універсальність, яка полягає в можливості виправлення помилок різної складності. Для випадку помилок типу інверсії сформульовані умови, що забезпечують гарантоване виправлення певної їх кількості.

Для реалізації програмного комплексу блочного шифрування з властивістю виправлення помилок був обраний алгоритм ГОСТ 34.12-2015 та мова програмування Java. Завдяки багатоплатформеності програмний комплекс може успішно використовуватися на різноманітних операційних системах і мати можливість свого розвитку в залежності від поставлених задач.

Проведено тестування розробленого програмного комплексу, аналіз ефективності запропонованих методів захисту інформації, що в цілому підтвердило теоретичні положення щодо забезпечення надійного способу передачі даних у відкритих каналах зв'язку.

Список використаних джерел

1. *Корченко О. Г. Прикладна криптологія : системи шифрування : підручник / О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс. – К. : ДУТ, 2014. – 448 с.: іл.*
2. *Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія - – Х. : Форт, 2012. – 878 с.*
3. *Блочное шифрование в режиме исправления ошибок / Молдовян Н.А., Солнышкин Ж. А., Фахрутдинов Р. Ш. // Вопросы защиты информации. — 2014.*
4. *Молдовян А. А., Муравйов А. В. Блочное шифрование в режиме исправления ошибок – С. : ЛЭТИ, 2018. – 26 с.*

УДК 004.056.53(043.2)

Ільєнко А. В., Яковенко О. Л., Данилюк Ю. Р.
Національний авіаційний університет

Аналіз сучасних методів автентифікації з використанням криптографічних перетворень

Актуальність теми. У зв'язку з високим попитом на користування інтернет-послугами гострою проблемою сьогодення постає захист облікових записів користувачів від несанкціонованого доступу. Обійшовши стандартний парольний захист, зловмисники можуть отримати доступ до персональних даних, особистих файлів, приватного листування та навіть банківських рахунків. Саме тому дуже важливим етапом розробки будь-якого інтернет-ресурсу є організація безпечної системи входу в обліковий запис.

Метою досліджень є аналіз сучасних методів та підходів щодо проведення автентифікації суб'єкту/об'єкту з використанням криптографічних перетворень.

Процес розпізнання системою санкціонованого користувача складається з трьох основних етапів: ідентифікація; автентифікація; авторизація.

На першому етапі користувач повинен надати ідентифікатор, закріплений за ним конкретною системою. Зазвичай таким ідентифікатором служить логін (унікальне ім'я користувача), його електронна адреса або номер телефону. Отримавши ідентифікатор, система перевіряє його достовірність шляхом автентифікації. Автентифікація зазвичай базується на можливостях користувача пред'явити один або декілька доказів того, що він є власником облікового запису (пароль, електронний цифровий підпис, відбитки пальців тощо). Після розпізнавання користувача система визначає, на які дії та ресурси в нього є права та повноваження, тобто проводить автентифікацію [1].

В загальному вигляді схема верифікації користувача виглядає наступним чином:

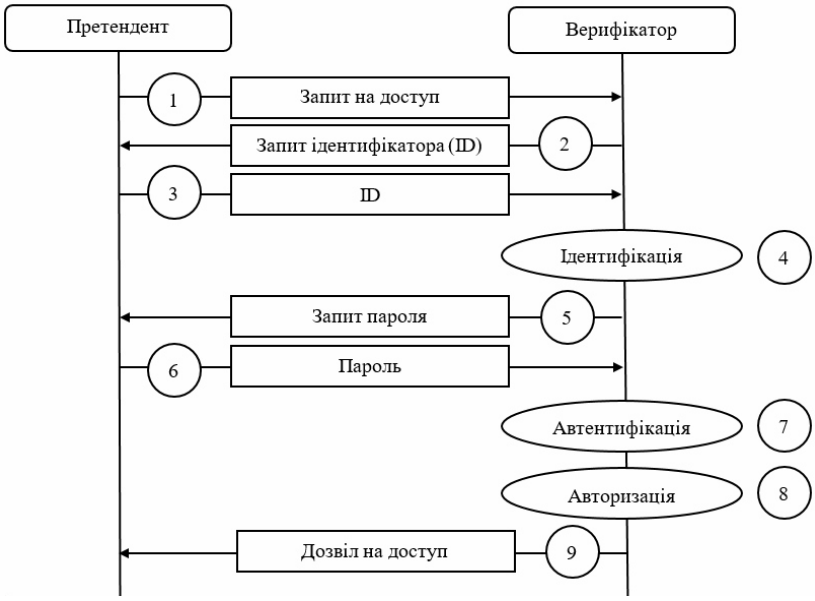


Рисунок 1 – Процеси ідентифікації, автентифікації, авторизації користувача

Серед сучасних методів автентифікації можна виділити наступні: парольна автентифікація; автентифікація з використанням електронного цифрового підпису (ЕЦП); біометрична автентифікація; автентифікація за географічним положенням; багатофакторна автентифікація [2].

Парольна автентифікація – напоширеніший метод автентифікації суб'єкта, основною метою якого є підтвердження належності ідентифікатора претенденту на

доступ до системи. Більшість парольних схем передбачають надання претендентом особистого паролю, який підлягає процесу хешування та перевірки отриманого хешу на відповідність хешу, що зберігається в системі. Досить популярною схемою, що забезпечує захист від перехвату та повтору є автентифікація з використанням «солі» (англ. *salt*). Її особливістю є те, що при створенні пароля використовується випадковий рядок, який і називається salt. При цьому, пароль, введений претендентом, конкатенують з цим рядком і тільки потім результат хешується та порівнюється з хеш-образом, що зберігається на стороні верифікатора (рис. 2) [1].

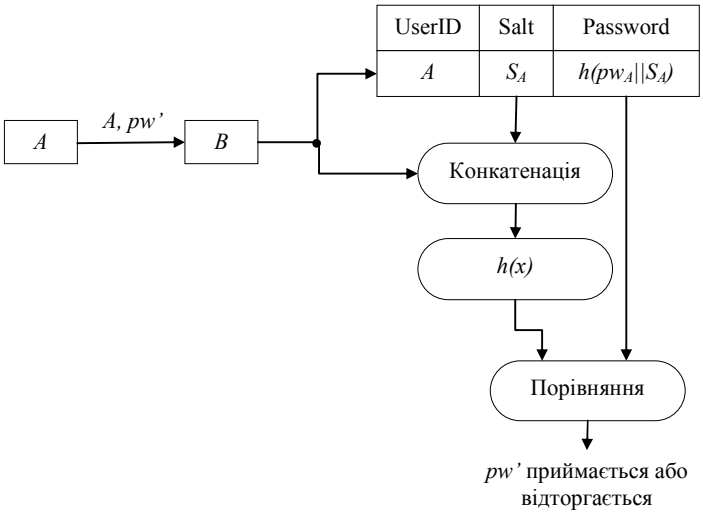


Рисунок 2 – Парольна схема автентифікації з використанням salt

До переваг використання солі можна віднести захист інших профілів користувача від зламу: навіть якщо зловмиснику вдасться несанкціоновано отримати доступ до бази даних, де зберігаються зашифровані паролі, він не зможе використати знайдений пароль для інших облікових записів, оскільки до хешу додана сіль. Крім того, за допомогою солі вирішується проблема однакових хешів за співпадання паролів [3].

Істотним недоліком запропонованого вище методу автентифікації є використання багаторазових паролів. А це означає, що система з такою автентифікацією матиме порівняно низьку стійкість і буде потенційно піддатлива до зламів перебором (smart force і brute force). Тому важливо придержуватись наступних принципів для підвищення рівня захищеності: пароль має бути досить складним (не менше 8 символів, з поєднанням комбінацій літер і цифр, верхнього та нижнього регістру, бажано без семантичного навантаження); пароль повинен регулярно оновлюватись, а строк його дії має бути визначеним політикою безпеки організації; пароль не має бути збереженим на матеріальних носіях, адже в такому випадку зловмисник зможе легко його викрасти; в системі повинно бути присутнім обмеження на кількість спроб введення пароля, щоб забезпечити захист від перебору brute force; системою має передбачатись захист від SQL ін'єкцій, тобто запит на порівняння введеного паролю з оригіналом має бути попередньо підготовленим (prepared statement); для зменшення ризику зламу бажано водночас поєднувати кілька алгоритмів автентифікації, тобто використовувати багатофакторну автентифікацію.

Список використаних джерел

1. *Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях: Учебное пособие / Под ред. М.А. Иванова. М.: НИЯУ МИФИ, 2012. – 400 с.: ил.*
2. *Ричард Э. Смит Аутентификация: от паролей до открытых ключей. : Пер. с англ. – М. : Издательский дом "Вильямс", 2002. – 432 с. : ил. – Парал. тит. англ.*
3. *Мартынова Л. Е., Умницын М. Ю., Назарова К. Е., Пересыпкин И. П. Исследование и сравнительный анализ методов аутентификации // Молодой ученый. — 2016. — №19. — С. 90-93.*

УДК 004.56.5

Коваль В. О.
Центральноукраїнський національний технічний університет

Захист персональних даних в інтернеті

Сучасні суспільні відносини вимагають не тільки вільного руху персональних даних, а й забезпечення їх надійного захисту. Прогрес у галузі інформаційних технологій, активність у створенні баз персональних даних створили загрози захисту приватного життя фізичних осіб, інших основних прав і свобод людини. Тому питання захисту персональних даних в Інтернет на сьогодні є актуальними і вимагають уваги.

В У повсякденному житті люди залишають після себе цифрову інформацію про те: кому дзвонять, куди ходять, якій їжі віддають перевагу, що і де купують, де живуть і інші відомості про особисте життя. Інформація про суб'єкта збирається постійно, як тільки він звертається до лікувального закладу, оплачує комунальні послуги, укладає договір на послуги зв'язку і т. п. За цими даними можна дізнатися більше, ніж власне люди хотіли б про себе розповісти. Цифрові технології дозволяють досліджувати мільярди індивідуальних взаємодій, в ході яких люди обмінюються ідеями, грошима, товарами і чутками.

Доволі поширеним явищем є випадки незаконного збору та поширення персональних даних в системі органів внутрішніх справ та правоохоронних органів загалом, наприклад, незаконна дактилоскопія осіб. Порушенням є також поширення медичної інформації, збір банківськими установами надлишкової інформації тощо [1].

Користувачі мережі повинні постійно дотримуватися правил щоб убезпечити свої персональні дані [2]:

1. Стежити за тим, яка інформація пересилається в повідомленні і кому.

2. Завжди уважно вивчати угоди про обробку персональних даних на сайтах, якими користуются.

3. Не довіряти важливу інформацію сайтам, які не містять угоди про обробку персональних даних.

3. Не прив'язувати банківську карту до платіжної системи сайту при користуванні послугами електронної комерції.

4. Звертатися до відповідних контролюючих органів при виявленні порушень законодавства в сфері захисту персональних даних.

Технологічний прогрес створює все ширше коло потреб та можливостей для збору та обробки персональних даних, а власне персональні дані знаходять все ширше використання в найрізноманітніших сферах. Нові технології, з одного боку, істотно спростили збір, обробку, зберігання, передачу даних, а з іншого - створили очевидні загрози їх незаконного обороту, що призводить до порушень прав особистості. У зв'язку з цим, розвиток системи захисту персональних даних є одним із найбільш актуальних завдань, які стоять перед українським суспільством на сучасному етапі.

Список використаних джерел

1. *Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. – К.: К.І.С., 2015. – 220 с.*
2. *Германова В.А. Атабекян А.С. Проблемы защиты персональных данных в сети интернет// Символ науки №12-3. -2016 [Електронний ресурс]. - Режим доступу: http://cyberleninka.ru/article/n/problemy-zaschity-personalnyh-dannyh-v-seti-internet*
3. *Козак В. Захист персональних даних та правила приватності при дослідженнях в Інтернет –режим доступу: http://uam.in.ua/upload/medialibrary/de7/de7199d7eeaf41d8582cbff76d2f4368.pdf*

УДК 004.056.53

Колмик О. О., Грінченко Є. М.
Харківський національний університет внутрішніх справ

Майнінг на чужих ресурсах

В даний час значно зросла популярність криптовалют. Різке зростання їх вартості привело до появи великої кількості людей які на цьому заробляють. Для багатьох це стає основним джерелом доходу, а для деяких майнінг перетворився на повноцінний бізнес. Частина добропорядних користувачів отримують свої біткоіни, збираючи свої майнінг-ферми, не завдаючи при цьому шкоди іншим людям. Але деякі майнять біткоіни на чужих комп'ютерах. Прихований майнінг - це процес видобутку криптовалюти зловмисником на чужому комп'ютері. При цьому жертва ні про що не підозрює, а шахраї добувають кріптовалу, не витрачаючи власні кошти і ресурси. Для майнінга криптовалюти на чужих потужностях шахраї проводять зараження комп'ютера вірусом. Це зараження відбувається при відкритті шкідливих повідомлень, скачування невідомих файлів і перегляду спам-розсилки. Ця програма активується, автоматично підключається до заданого розробником пулу і починає видобуток криптовалюти. Цей спосіб називається прихованим майнінгом з використанням вірус-майнера. Однак для того, щоб почати майніти за рахунок користувача зовсім необов'язково встановлювати на його комп'ютер троян або іншу вірусну програму. Досить ввести в код сайту спеціальний скрипт, який дозволяє непомітно підключитися до гостьової системі сайту. Такий спосіб називається браузерним майнінгом. Найчастіше приховано майнять піратські популярні сайти, сайти з фільмами і серіалами, торрент-трекери, форуми.

У початковому етапі розвитку шкідливих програм частину їх вдавалося вирахувати і видалити, так як вони активізували всі невикористовувані ресурси ПК, що призводило до перегрівів і неможливості роботи комп'ютера. У цих умовах для маскування своїх дій, і забезпечення отримання прибутку шахраї пішли на зниження обсягів використовуваних ресурсів, припускаючи, що при цьому вірус пропрацює довше, так як якщо він не заважає, то і виявити його буде складніше. Якщо на першому етапі віруси майнери могли використовували 90-100%, потужностей ПК, то далі вони різко знизили завантаження ПК і довели його до 2 до 5% вільних ресурсів, фактично не заважаючи користувачеві спокійно працювати.

Виявлення та захист від прихованого браузерного майнінгу не викликає великих труднощів. Якщо при відвідуванні сторінки комп'ютер почне працювати повільно і при цьому диспетчер задач відображає збільшене навантаження, то потрібно просто вийти з такої сторінки. Крім того, необхідно встановити найсучасніші антивірусні програми і постійно оновлювати їх бази до останніх версій. Також можна скористатися розширеннями для браузерів «No Coin» і «minerBlock». Ще один спосіб - використання блокувальників типу «AdBlock» і йому подібних. Ці програми здатні з успіхом блокувати більшість спливаючих банерів, особливо завдають шкоди вашому центральному процесору CPU шляхом підвищеного використання потужностей. Також потрібно відзначити, що в комп'ютерну та мобільну версії браузера Opera тепер вбудований захист від майнінгу.

Ситуація з прихованим вірус майнінгом трохи складніша. Як зазначалося, багато сучасних вірусів-майнерів використовують невелику частину потужності ПК. Тому їх важко виявити. Якщо виникли підозри, що ПК заражений, необхідно за допомогою антивірусної програми провести глибоку перевірку з метою підтвердження наявності

вірус-майнера на комп'ютері. Це дозволить підтвердити присутність, але можливо антивірусна програма визначить конкретне місце розміщення вірусу. Видалити шкідливий софт з жорсткого диска буде набагато складніше, тому що частина програм можуть відновлюватися з bat файлу в разі, якщо вбудований сканер не знаходить виконавчий файл. Після видалення всіх підозрілих програм з жорсткого диска потрібно відкрити диспетчер задач і закрити всі не знайомі процеси, або ті, які займають більше 10% потужності. Необхідно звернути увагу на завантаженість CPU (процесор) і GPU (відеокарта) понад норму і закрити їх по черзі. Як правило цього вистачає для того щоб вірус-майнер, який не має можливості відновлюватися або автозапускатися, після перезавантаження був знищений. Однак це стосується відносно «слабких» вірус-майнерів. Складні програми прихованого майнінгу можуть приховувати свою присутність в системі, можуть відключаються перед відкриттям диспетчера задач або самі його закривати. Є версії, які відстежують запуск антивірусної програми і видаляють виконавчу частину, а після перезавантаження відновлюються. Алгоритм пошуку і видалення вірус майнера з ПК наступний:

- запустити повну перевірку антивірусною програмою, яка оновлена до останньої версії;
- проаналізувати результати перевірки і видалити всі підозрілі програми, що виявлені антивірусом;
- перезавантажити ПК. Під час перезавантаження увійти в меню BIOS, і вибрати завантаження операційної системи з розширеними настройками Advanced Boot Options;
- запустити безпечний режим з мережевою підтримкою (Safe Mode w Networking);
- запустити систему і авторизуватись під своїми обліковими даними;
- знайти в мережі і завантажити якісне ПО для роботи із шпигунськими програмами, наприклад, Malwarebytes Anti-Malware;
- в обраному режимі, пошукове ПО буде знаходити все підозріле ПО, що не входить в базові настройки Windows і автоматично видаляти. Також, будуть видалені дані з системного реєстру і довантажуючи базові файли для відновлення працездатності ряду програм, частина файлів яких здалася підозрілою.

У більшості випадків цього вистачає для того щоб впоратися навіть з досить сильними вірус-майнерами. Якщо достовірно відомо про присутність вірус-майнера на ПК, то кращим рішенням в ситуації залишається традиційне повне форматування диска і переустановлення операційної системи. Саме в такому порядку, оскільки файли майнера, що виконувані не зберігається в тих папках, де їх будуть шукати і не прив'язані до конкретної ОС, тобто можуть активуватися і після її переустановлення.

Висновки:

1. щоб превентивно захиститися від атак прихованих майнерів, слід обмежити відвідування неперевірених сайтів і відразу ж закривати будь-які інформаційні портали, на які лається антивірус або захист браузера.
2. не відкривати листи від незнайомих кореспондентів, а також рекламні листи.
3. встановити якісне антивірусне ПЗ і постійно його оновлювати.
4. періодично проводити глибокі перевірки, наприклад, щоночі або раз на три дні, щоб видаляти будь-яке вірусне сміття.
5. в ідеальній ситуації відбирати ряд надійних ресурсів для перегляду кіно, прослуховування музики та інше, а також обмежте скачування контенту з піратських порталів.

УДК 004.056.53

Кохан Є. Р.
Національний авіаційний університет

Соціальна інженерія як загроза інформаційній безпеці

В наш час, коли ера інформаційних технологій та кібернетичного простору стрімко розвивається, а вразливість програмного забезпечення зменшується, люди, як особистості, стають більше вразливими, ніж будь-коли раніше, а кіберзлочинність стає частиною повсякденного життя кожного. Сьогодні одними із найбільш практичних та ефективних атак є соціальні, а не технічні. Соціальна інженерія - це мистецтво експлуатувати людські недоліки для досягнення мети. Кіберзлочинці спонукають своїх жертв порушувати протоколи безпеки конфіденційної інформації для більш цілеспрямованої атаки. Кіберзлочинність – це основна загроза економіці, індивідуальній безпеці та навіть громадськості в цілому, оскільки вона є основним середовищем для тероризму. Найбільш поширені нападники - це проникливі злочинці, які продовжують використовувати соціальну інженерію як свій первинний вектор атаки.

Всім відомо, що найслабша ланка захисту будь-якої системи - самі користувачі. Соціальна інженерія намагається використовувати властиві людям слабкості, наприклад, квапливість, жадібність, альтруїзм чи страх перед офіційною установою з метою отримання конфіденційної інформації і подальшого доступу в систему. Соціальну інженерію визначають як один із найпростіших методів збору інформації про ціль за допомогою експлуатації людської слабкості. У контексті кібербезпеки соціальна інженерія, перш за все, використовується для заохочення жертв для розголошення конфіденційних даних або виконання дій, що порушують протоколи безпеки, несвідомо заражаючи їх системи або отримуючи секретну інформацію. Протягом усієї взаємодії жертви не знають про руйнівний характер своїх дій. Талановитий практик цієї дисципліни розуміє і сприймає закономірності соціальної взаємодії, маніпулюючи психологічними аспектами людського розуму. Для досягнення певної мети соціальні інженерні атаки можуть варіюватися від однієї до серії операцій, можливо, за участю декількох учасників загрози, покликаних зібрати фрагменти пов'язаної інформації з різних джерел.

Найбільш популярні методи соціальної інженерії: бейтінг або лов "на живця", фішинг, вішинг або псевдо-антивірус. Постає питання: як же розпізнати прийоми соціальної інженерії? З огляду на те, що методи соціальної інженерії розроблені професіоналами своєї справи, розпізнати обман часом не під силу навіть фахівцям. Необхідно остерігатися будь-яких пропозицій допомоги, особливо тих, що пропонують перехід за сторонніми посиланнями. Зазвичай в таких випадках мова йде про хитрощі соціальної інженерії. Це правило найбільш актуальне, якщо користувач повинен вказати облікові або банківські дані. У такому випадку без всяких сумнівів це – шахрайство, так як фінансові організації ні за яких обставин не будуть запитувати облікові дані за допомогою повідомлення електронної пошти.

Соціальна інженерія нематеріальна, тому її неможливо фізично усунути. Найефективніший спосіб не стати жертвою соціальної інженерії - не втрачати пильності і не дозволяти зловмисникам обманути себе. Саме тому найбільш ефективним способом захисту, як і раніше, є використання сучасного антивірусного рішення, яке розпізнає і усуває всі типи шкідливого програмного забезпечення, а також надійного менеджера паролів, який допоможе створити паролі, що не зламуються і зберігати їх в безпеці.

Основною відмінністю соціальної інженерії є прагнення зловмисників з її допомогою обійти всі технічні засоби захисту, обравши основним вектором атаки людину, а не систему комп'ютера. Саме тому вкрай важливо використовувати потужне антивірусне рішення, щоб забезпечити надійний захист від несанкціонованого встановлення шкідливого ПЗ, виявити і знешкодити віруси і інші типи шкідливого ПЗ, заблокувати спам і, тим самим, уберегтися від фішингового шахрайства.

Інформаційна сфера, як сприятлива інфраструктура для великої різноманітності кримінальних правопорушень, зростає, коли суспільство стає все більш захищеним середовищем. Незаперечним є той факт, що люди є основою ланцюга зараження в більшості кібератак. В найближчому майбутньому соціальна інженерія буде найголовнішим вектором атаки в кібербезпеці і, таким чином, заслуговує на те, щоб грунтовно вивчати її, щоб використовувати корисні практики та заходи для захисту окремих осіб та організації.

Список використаних джерел

1. Социальная инженерия и социальные хакеры / М. В. Кузнецов, И. В. Симдянов. — СПб.: БХВ-Петербург, 2007. — 368 с.
2. "Social engineering fraud: questions and answers", Technical report, Interpol, December 2015.
3. Parker Graeme, Shala Vlerar, "Social engineering and risk from cyber-attacks", Technical report, PECB, March 2016.

УДК 004.056.5

Крапівін В. В.
ДВНЗ «Донецький національний технічний університет»

Система виявлення мережевих атак на основі алгоритмів нечіткого виведення

Системи виявлення атак - важливий елемент систем інформаційної безпеки мереж будь-якого сучасного підприємства, з огляду на зростаючу в останні роки кількість проблем, пов'язаних з комп'ютерною безпекою.

Існують дві основні категорії методів виявлення мережевих атак[1]:

1. Сигнатурні методи. Ґрунтуються на застосуванні сформованої спеціалізованої бази даних сигнатур (шаблонів) для визначення шкідливих дій. Головним недоліком є нездатність виявлення атак невідомих типів, а основними перевагами є простота використання та рівень швидкодії в сукупності з відносно малою кількістю витрачених ресурсів в більшості випадків.

2. Методи виявлення аномальної поведінки. Формується образ нормальної поведінки, відхилення від якої є аномаліями, що являють собою можливу атаку. Основною перевагою таких методів є можливість визначення нових атак, які не були відомі раніше. Недоліками є велика кількість помилкових спрацьовувань через невірно обрані методи і критерії для оцінки. Також вхідний поріг для розуміння і використання подібних методів значно вище, ніж у сигнатурних, і для частини алгоритмів процес перенавчання може бути витратним, як в плані обчислювальних ресурсів, так і часу.

Найбільш відомі методи:

- Статистичний метод.
- Використання прогнозованих шаблонів.
- Аналіз переходів зі стану в стан.
- Приховані марківські моделі.
- Експертні системи.
- Нечітка логіка.
- Генетичні алгоритми.
- Штучні нейронні мережі.
- *Data mining*-методи.

У даній роботі пропонується класифікувати записи за допомогою алгоритмів нечіткої логіки. Однією з головних особливостей нечітких систем є їх прозорість, яка досягається за рахунок їх лінгвістичної інтерпретації у вигляді бази нечітких продукційних правил. Лінгвістична структура правил сприяє швидкому розумінню та аналізу системи. Алгоритм нечіткого виведення дозволяє забезпечити гнучкість системи прийняття рішень за рахунок можливості коригування критеріїв оцінки і правил виведення. Основною перевагою нечіткої логіки є те, що нечіткі правила дозволяють об'єктам належати до декількох класів одночасно з різним ступенем приналежності.

Основні етапи нечіткого виведення:

1.Формування бази продукційних правил. База правил в системах нечіткого виведення призначена для представлення емпіричних або експертних знань у обраній предметної області. При складанні бази нечітких правил необхідно оцінити і забезпечити їх повноту (достатність), їх несуперечливість, а також по можливості, усунути кореляції між окремими нечіткими правилами в базі [3].

2.Фазифікація вхідних змінних. Фазифікація – це процес знаходження значень функцій належності нечітких множин (термів) вхідних змінних для всіх передумов нечітких продукційних правил. Також фазифікацію часто називають введенням

нечіткості. Метою етапу є встановлення відповідності між конкретним значенням вхідної змінної і значенням функції приналежності відповідного їй терма вхідної лінгвістичної змінної. В результаті для кожної передумови з бази буде отримано значення функції приналежності.

3.Агрегування передумов. Оскільки в базі правил можуть бути правила складеного виду, даний етап служить для визначення ступеня істинності кожного правила.

4.Активізація висновків в нечітких продукційних правилах. Визначається ступінь істинності кожного з висновків нечітких правил (підвисновків).

5.Акумуляція висновків нечітких продукційних правил. Знаходження функції приналежності для кожної вихідної лінгвістичної змінної. Метою акумуляції є об'єднання всіх ступенів істинності підвисновків, щоб отримати ступінь істинності кожної з вихідних змінних. В процесі нечіткого виведення цей етап необхідний, тому що підвисновки, що відносяться до однієї і тієї ж лінгвістичної змінної належать різним правилам системи нечіткого логічного висновку. Об'єднанням двох нечітких множин є третя нечітка множина, з функцією приналежності, що обчислюється за формулою:

$MF_i(x)=max\{MF_1(x), MF_2(x)\}$, де $MF1(x)$, $MF2(x)$ – функції приналежності функцій що об'єднуються.

6. Дефазифікація. Дефазифікація – це процес знаходження кількісного значення для кожної вихідної лінгвістичної змінної (перетворення нечіткого значення в чітке). Деякі методи дефаззифікації [3]: метод центру ваги (COGS, Centre of Gravity), метод центру площі (CoA, COA, Centre of Area), максимум функції приналежності, перший максимум (first-of-maxima), самий правий максимум (right most maximum).

Розглянуті етапи нечіткого виводу включають в себе окремі параметри, які можуть бути фіксовані або специфіковані, і тому можуть бути реалізовані неоднозначним чином. Тому вибір конкретних варіантів параметрів кожного з етапів визначає алгоритм, що повністю реалізує нечіткий висновок в системах правил нечітких продукцій.

На теперішній час існують декілька алгоритмів нечіткого виведення[3], найбільш відомі: алгоритм Мамдані (Mamdani), алгоритм Цукамото (Tsukamoto), алгоритм Ларсена (Larsen), та алгоритм Сугено (Sugeno). Алгоритми відрізняються типом правил логічних операцій та методом дефазифікації, а вибір потрібної моделі визначається характером завдань, що вирішуються.

У даній роботі пропонується використати алгоритм Мамдані, як найбільш поширений спосіб логічного виведення в нечітких системах. Етапи алгориму збігаються з описаними вище загальними етапами. Для фазифікації (розмивання) даних застосовуються функції приналежності різних видів: трикутні, трапецієподібні і лінійні (вибір форми функції залежить від типу і специфіки даних, а також від діапазону значень, що необхідно покрити). Дефазифікація виконується центроїдним методом. На вході та виході алгоритму дані мають кількісні значення, а на етапах 3-5 застосовується апарат нечіткої логіки. Це і є основна перевага нечітких систем - можливість роботи зі звичними числовими даними і при цьому використовувати можливості, що надаються системами нечіткого виведення.

Вхідними даними для роботи програми є множина KDD Cup 99, яка розділена на дві підмножини: навчальний набір даних і тестовий набір даних. Навчальний набір даних класифікується в п'ять підмножин: одну нормальних даних та чотири множини

аномальних даних, по одній на кожний тип атак: DoS (відмова в обслуговуванні), R2L (віддалений до локального), U2R (отримання прав адміністратора), Probe (сканування портів). Далі виявляються найбільш важливі атрибути, які згодом використовуються для складання визначених та невизначених правил. Потім, відповідно до правила фазифікації, генеруються нечіткі правила, таким чином, щоб отримати ряд продукційних правил виду «ЯКЩО ... ТО», які дозволять визначити, до якого класу належить запис - нормальні дані або існує аномалія. Для ефективного навчання нечіткої системи, сформовані правила перераховані в базі нечітких продукційних правил. У фазі тестування, тестові дані зіставляються з нечіткими правилами з бази для того, щоб визначити, чи є дані нормальними або аномальними.

У зв'язку з тим, що при зростанні кількості атрибутів число нечітких правил експоненціально зростає, з точки зору продуктивності системи, недоцільно використання великого числа атрибутів. Тому в роботі була виділена підмножина значущих атрибутів, яка дозволила створити базу з мінімальним числом простих нечітких правил, та одночасно володіє високою точністю виявлення і невеликим числом помилкових спрацьовувань. В результаті сформована база нечітких продукційних правил, кожне з яких включає в себе не більше п'яти атрибутів.

Експерименти показали, що запропонований підхід дозволяє ідентифікувати різні класи атак. Точність розробленої системи класифікації даних досить висока, і її можна порівняти з результатами аналогічних досліджень.

Тестування системи проводилося на випадкових наборах записів з кроком в 300 штук (від 300 до 1500). У таблиці 1 представлені узагальнені дані для кожного з класів.

Класи атак User to Root і Remote to Local при оцінці результатів роботи системи не розглядалися, тому що кількість записів для них в тестовій множині дуже мало (близько 30-100 шт). Через малу кількість записів для даних класів рекомендується створювати окремі підмножини правил.

Таблиця 1 – Результати тестування системи

Клас	Ефективність, %	Помилкові спрацювання, %
Normal	93.22	3.5
DoS	91.88	7.89
Probes	94.96	0.29

З метою подальшого вдосконалення запропонованого підходу планується розглянути можливість формування п'яти множин нечітких правил - для кожного класу, а також можливість автоматизації процесу генерації бази нечітких продукційних правил. Зокрема, можливе застосування генетичних алгоритмів для формування бази нечітких правил і функцій приналежності нечіткої системи.

Список використаних джерел

1. *Носенко К. М. Огляд систем виявлення атак в мережевому трафіку / К. М. Носенко, О. І. Півторак, Т. А. Ліхоузова // Адаптивні системи автоматичного управління. - 2014. - № 1. - С. 67-75. - Режим доступу: http://nbuv.gov.ua/UJRN/asau_2014_1_13.*
2. *Shaik Akbar. Intrusion Detection System Methodologies Based on Data Analysis / Shaik Akbar, Dr.K.Nageswara Rao, Dr.J.A.Chandulal // International Journal of Computer Applications (0975 – 8887) Volume 5– No.2, August 2010.*
3. *Борисов В. В. Нечеткие модели и сети / В. В. Борисов, В. В. Круглов, А. С. Федулов. – М. : Горячая линия – Телеком, 2012. – 284 с.*
4. *Рутковская Д.С. Нейронные сети, генетические алгоритмы и нечеткие системы / Д.С. Рутковская, М.В. Пилиньский, Л.П. Рутковский. – М.: Горячая линия –Телеком, 2006. – 383 с.*
5. *Аналіз системи виявлення вторгнень та комп'ютерних атак / Радченко М.М., Іванов О.І., Прохорський С.І., Мужеський К.К. // Междисциплинарные исследования в науке и образовании. – 2013. – № 2 Sp;*
6. *Mamdani E.H. Application of fuzzy algorithms for the control of a simple dynamic plant. / E.H. Mamdani // Proc IEEE. — 1974. — V. 121.No. 12. — P. 121-159.*

УДК 004.043

Краштапук К. К.
Харківський національний університет радіоелектроніки

Чи потребує Інтернет Речей інтеграції блокчейну?

Взаємодія блокчейн і IoT обіцяє незаперечні переваги. Чи потребує Інтернет Речей інтеграції блокчейну? Вважається, що блокчейн здатний підвищити ступінь захисту і цілісності інформації в області Інтернету речей. Однак, потенціал інноваційної технології набагато ширше, а синергія двох технологій має неймовірний потенціал.

Використання смарт контрактів полегшує використання блокчейна в інтернеті речей. Що ж таке смарт контракти? Вони об'єднують в собі і можливість написання умов смарт контракту, і механізмів їх виконання. Якщо умови були задані, то після прийняття цього запиту вже неможливо змінити умови або вплинути на їх виконання. Ще важливо, що ця база даних повинна містити всі умови-тригери для виконання смарт контракту. Крім того, ця база повинна враховувати ту саму цінність, розподіл якої описано в контракті.

Як взаємодіє інтернет речей зі смарт-контрактами? Так: смарт-контракти дають можливість створити автономні пристрої IoT для різних завдань з використанням IT-систем і сервісів; смарт-контракт обробляють дані і керуючі IoT. Неможливо видалити програму, одного разу внесену в блокчейн; виключена така причина збою, як зупинка одного з серверів мережі. У разі збою одного з вузлів, виконання продовжується на інших вузлах.

Більшість пристроїв обмежені в споживанні електроенергії, щоб малопотужне обладнання змогло проводити необхідні обчислення PoW для смарт контракту, також необхідно спростити криптографічні завдання або процедуру їх рішення. Так як зміна складності хеш-функції дозволить зловмисникам маніпулювати системою. Це дозволить IoT використовувати навіть малу обчислювальну потужність для успішного докази виконаної роботи.

Для обробки мікроплатежів між мільярдами пристроїв Сергієм Поповим був розроблений «двоюрідний брат блокчейна» - спрямований ациклічний граф під назвою "Плутанина" (Tangle). Іноді цей свій граф розробники IOTA називають блокчейном наступного покоління, без блоків і без «Чейна» (ланцюга).

В "Плутанини" немає майнерів, так що не доводиться чекати, поки вони сформують блок. У цій децентралізованої мережі криптовалют, повідомлення і дані відправляються відразу і без будь-яких комісій. Замість плати за транзакцію система вимагає підтвердити дві інші транзакції і витратити крихітне кількість обчислювальної потужності для виконання криптографічного алгоритму SHA-3 Proof of Work (PoW). Тобто, якщо людина або автономний пристрій хоче зробити передачу криптовалют або передачу даних в Плутанини, йому потрібно верифікувати в цій мережі дві попередні транзакції, обрані випадковим чином за допомогою спеціального алгоритму Markov Chain Monte Carlo Random Walk.

Таким чином, система забезпечує процес постійного підтвердження транзакцій безліччю великих і маленьких пристроїв. Кожне з них змушена виділяти обчислювальну потужність на підтримку роботи мережі, щоб отримувати можливість здійснення в ній своїх операцій. А оскільки кожен вузол повинен виконати вдвічі більше верифікації, ніж потрібно йому, нові транзакції в Плутанини, теоретично, будуть дуже швидко знаходити охочих їх перевірити і схвалити.

Блокчейн знаходиться в більш широкому контексті, що включає в себе інституційні відносини, юридичні вимоги і регулює контроль. Тож його роль поступово зводиться до журналу «рішень і дій», який, можливо, знадобиться скорегувати в майбутньому.

Список використаних джерел

1. *Suo H., Wan J., Zou C., Liu J. Security in the Internet of Things: A Review // Proceedings of the 2012 International Conference on Computer Science and Electronics Engineering. – 2012. – P. 648–651.*
2. *«Top IoT Vulnerabilities» [Електронний ресурс] – Режим доступу: https://www.owasp.org/index.php/Top_IoT_Vulnerabilities*
3. *Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. [Електронний ресурс]. – Режим доступу: https://bitcoin.org/bitcoin.pdf.*

УДК 004.056.5 Кузнецов А. А., Попова М. В., Шаповал О. В., Чернов К. А., Ерёмин Е. С.
Харьковский национальный университет им. В.Н. Каразина

Анализ и исследование автоматизированных технологий поиска уязвимостей программного обеспечения

Анализ литературы и постановка задачи исследования. Для автоматизированного тестирования программного обеспечения используют большое число различных инструментов. Одним из наиболее перспективных является фаззинг (англ. fuzzing), который используется для автоматизированного поиска уязвимостей в безопасности программ, операционных систем или сетей. Суть фаззинга заключается в передаче тестируемой программе огромного количества случайных данных, называемых fuzz, которое должно привести к появлению сбоев, ошибок, переходу в неустановленные режимы работы и т.д. [1-3].

Понятие фаззинг впервые было введено профессором Висконсинского университета в Мадисоне Бартоном Миллером и его студентами в 1989 [1]. В дальнейшем развитие автоматизированного тестирования продолжилось, создатели фаззинга успешно применяли его метод для поиска уязвимостей программного обеспечения с использованием различных операционных систем, в т.ч. UNIX, Windows и Mac OS [1-3]. В настоящее время фаззинг нашел применение в первую очередь в сфере мониторинга и тестирования программного обеспечения (Quality Assurance). Также фаззинг является одним из составляющих шагов процесса Microsoft Security Development Lifecycle (SDL). По мнению специалистов компании Microsoft, вызов программного сбоя путем умышленного ввода неверных или случайных данных в приложение помогает выявить потенциальные проблемы с безопасностью до релиза и требует при этом малых инвестиций ресурсов [4].

Тестирование методом фаззинга имеет ряд преимуществ, среди которых [4-7]: высокая скорость (зачастую гораздо выше, чем ручная проверка кода); отсутствие необходимости в человеческом труде; фаззер не нужно контролировать, в то время, как человеческие способности ограничены; масштабируемость, т.е. для поиска большего количества уязвимостей можно запустить большее число процессов тестирования.

Однако, у фаззинга есть и некоторые недостатки, например, с его помощью очень трудно обнаружить глубокие ошибки, ошибки бизнес логики и пр. [6]. Актуальным представляется сравнительный анализ различных технологий автоматизированного поиска уязвимостей методом фаззинга, проведение экспериментальных исследований на примере наиболее распространенных прикладных программ пользовательского уровня.

Сравнительный анализ и результаты экспериментальных исследований. В данной работе проведен анализ и сравнительные исследования автоматизированных технологий поиска уязвимостей программного обеспечения. В частности, рассмотрены следующие популярные утилиты для фаззинга [8-10]: American Fuzzy Lop, MiniFuzz, Peach, проведены экспериментальные исследования эффективности автоматизированного поиска уязвимостей на примере таких популярных приложений, как Google Chrome; Notepad++; Winamp; Microsoft Paint.

American Fuzzy Lop (AFL) – фаззер с открытым исходным кодом, разработанный польским экспертом по компьютерной безопасности Михалем Залевски (Michał Zalewski) [8]. Программа использует генетические алгоритмы для автоматизированного поиска тест-кейсов. Задача данного фаззера – вызвать непредсказуемое поведение тестируемых программ путем замены или перемещения битов входных файлов.

MiniFuzz – разработанный компанией Microsoft фаззер, предназначенный для широкого использования [10]. Принцип его работы состоит в том, чтобы сначала сформировать данные, затем передать их целевому приложению и отследить ошибки. Данная утилита относится к категории простых (или т.н. «глупых») фаззеров, то есть процесс фаззинга файлов производится случайно.

Peach – гораздо более продвинутый инструмент «интеллектуального» фаззинга, разработанный Майком Эддингтоном [4-9]. Он поддерживает не только режим мутации, но и режим генерации фазз-файлов. Поскольку для генерации файлов программе нужно знать их структуру, в качестве входных данных используются специализированные XML-файлы. Peach позволяет фаззить приложения, серверы, сетевые протоколы, драйверы, встроенные протоколы, устройства, системы и пр.

В ходе экспериментальных исследований эффективности автоматизированного поиска уязвимостей использована утилита MiniFuzz, проведен фаззинг для нескольких популярных приложений, включая: Google Chrome; Notepad++; Winamp; Microsoft Paint.

Для тестирования приложения Google Chrome в качестве шаблонных файлов было выбрано несколько десятков html-документов разного рода, агрессивность фаззинга (доля входных данных, подлежащих случайному изменению) была установлена на 5%, 15%, 25%, 35%. Полученные результаты эффективности автоматизированного поиска уязвимостей в приложении Google Chrome приведены в таблице 1. Как видно из таблицы выборочное тестирование методом фаззинга позволило выявить появление ошибки «Файл не найден». Очевидно, что повышение агрессивности тестирования приводит, как и ожидалось, к повышению частоты появления этой ошибки.

После нескольких часов фаззинга приложения Notepad++не удалось выявить каких-либо ошибок даже со 100% агрессивностью тестирования, что говорит о высокой устойчивости и безопасности данного приложения. Аналогичные результаты дало автоматизированное тестирование приложения Winamp.

Для тестирования приложения Microsoft Paint в качестве входных данных использовались изображения различных форматов и размеров. Результаты тестирования приведены в таблице 2. Как видно из полученных результатов, выборочное тестирование методом фаззинга позволило выявить появление ошибок «Файл не найден» и «Неверный формат». Частоты появления этих ошибок приблизительно равны и также возрастают с увеличением агрессивности автоматизированного поиска уязвимостей.

Из проведенных тестов можно сделать вывод, что большинство распространенных пользовательских программ защищены от примитивного фаззинга. В случае, например, с приложением Google Chrome это не удивительно, ведь на данный момент известно, что специалисты компании проводят гораздо более сложный фаззинг при разработке своих продуктов, а также для автоматизированного поиска уязвимостей [11]. То же самое касается и продукции компании Microsoft [4].

Выводы. В данной работе проведен анализ различных фаззеров в сфере автоматизированного тестирования программного обеспечения. Подход к тестированию с использованием фаззинга может значительно варьироваться в зависимости от цели, навыков тестировщика, формата данных и других факторов. Некоторые приложения имеют систему разделения привилегий в зависимости от уровня пользователя. Используя фаззер как технологию автоматизированного поиска уязвимостей можно обнаружить ошибки в программных продуктах, которые позволяют атакующему заполучить полный или частичных контроль над системой. На низком уровне ошибки программного обеспечения очень похожи, поэтому аналогичную

логику можно применить и для нахождения уязвимостей в большом количестве приложений.

Таблица 1. Математическое ожидание частоты появления ошибки «Файл не найден» и доверительный интервал (для уровня значимости $\alpha = 0{,}01$ и объема выборки $N = 1000$)

Ошибка	Уровень агрессивности			
	5%	15%	25%	35%
«Файл не найден»	$0{,}239 \pm 8{,}23 \cdot 10^{-4}$	$0{,}269 \pm 2{,}6 \cdot 10^{-4}$	$0{,}295 \pm 3{,}49 \cdot 10^{-4}$	$0{,}320 \pm 8{,}28 \cdot 10^{-4}$

Таблица 2. Математическое ожидание частоты появления ошибок и доверительный интервал (для уровня значимости $\alpha = 0{,}01$ и объема выборки $N = 1000$)

Ошибка	Уровень агрессивности			
	5%	15%	25%	35%
«Файл не найден»	$0{,}13 \pm 2{,}6 \cdot 10^{-4}$	$0{,}15 \pm 2{,}58 \cdot 10^{-4}$	$0{,}18 \pm 2{,}64 \cdot 10^{-4}$	$0{,}22 \pm 1{,}58 \cdot 10^{-4}$
«Неверный формат»	$0{,}09 \pm 2{,}96 \cdot 10^{-4}$	$0{,}16 \pm 3{,}77 \cdot 10^{-4}$	$0{,}2 \pm 3{,}58 \cdot 10^{-4}$	$0{,}23 \pm 4{,}57 \cdot 10^{-4}$

По результатам экспериментального выборочного тестирования можно с уверенностью утверждать, что фаззинг является перспективным методом автоматизированного поиска уязвимостей. Даже для таких надежных и проведенных временем приложений как Google Chrome и Microsoft Paint, нам удалось подобрать такие случайные входные данные, которые вызывают ошибку программного обеспечения. В тоже время, выявленные ошибки не являются критичными для работы прикладного приложения и/или операционной системы, их обработка реализована корректно что, по всей видимости, является предусмотренной реакцией на неправильно заданные входные данные.

Следует отметить, что фаззинг имеет определенные ограничения в практическом использовании и еще не получил широкого применения для автоматизированного поиска уязвимостей программного обеспечения. Однако, тот факт, что крупные компании, например, Google и Microsoft, уже добавили фаззинг в свою методологию тестирования программных продуктов и работают над развитием этой техники, позволяет с уверенностью сказать, что фаззинг имеет очень большой потенциал [4, 11].

Список использованных источников

1. *Rouse, Margaret. What is fuzz testing (fuzzing)? [Электронный ресурс] – Режим доступа: https://searchsecurity.techtarget.com/definition/fuzz-testing*
2. *Barton P. Miller. An Empirical Study of the Reliability [Текст] / Barton P. Miller, Lars Fredriksen, Bryan So. – Mille, Fredriksen, and So, 1989. – 22 с.*
3. *Miller, Barton. Foreword for Fuzz Testing Book. [Электронный ресурс] –Режим доступа: http://pages.cs.wisc.edu/~bart/fuzz/Foreword1.html*
4. *SDL Process: Verification. [Электронный ресурс] – Режим доступа: https://www.microsoft.com/en-us/SDL/process/verification.aspx*
5. *Chris Evans, Matt Moore, Tavis Ormandy. Fuzzing at scale. [Электронный ресурс] – Режим доступа: https://security.googleblog.com/2011/08/fuzzing-at-scale.html*
6. *Freingruber, René. The Art of Fuzzing. [Электронный ресурс] – Режим доступа: https://www.sec-consult.com/wp-content/uploads/files/vulnlab/the_art_of_fuzzing_slides.pdf*
7. *Michael Sutton. Fuzzing: Brute Force Vulnerability Discovery [Текст] / Michael Sutton, Adam Greene, Pedram Amini. – Pearson Education inc., 2007. – 513 с.*
8. *American fuzzy lop. [Электронный ресурс] – Режим доступа: http://lcamtuf.coredump.cx/afl/*
9. *Hanno Böck. How Heartbleed could've been found. [Электронный ресурс] – Режим доступа: https://blog.hboeck.de/archives/868-How-Heartbleed-couldve-been-found.html*
10. *Воробьев Илья. Использование файлового фаззера MiniFuzz. [Электронный ресурс] – Режим доступа: https://blogs.msdn.microsoft.com/security_ru/2009/11/01/143/*
11. *Guided in-process fuzzing of Chrome components. Google Security Blog. [Электронный ресурс] – Режим доступа: https://security.googleblog.com/2016/08/guided-in-process-fuzzing-of-chrome.html*

УДК 004.75

Кузьменко Д. С., Луценко В. В., Тарасенко Ю. С.
Університет митної справи та фінансів

Аспекти експрес аналізу захищеності комп'ютерних даних

Як не парадоксально, гасло заголовка цілком точно відображає, побажання будь-якого користувача комп'ютерної техніки, на знання рівня поточної безпеки комп'ютера, в момент його включення і подальшого використання. Кожному такому користувачеві не хочеться щоб саме его ПК – персональний комп'ютер пав жертвою так званого «Не санкціонованого доступу» до його інформації.

В даний час відомо багато видів захистів, від загроз, пов'язаних з порушенням цілісності та достовірності інформації, яка безпосередньо циркулює в сучасному ПК.

Очевидно що з кожним роком область двобічного протиборства, засобів і видів атак, в протиставлення яким, ставиться методи і засоби захисту інформації. Такі засоби лише удосконалюються і поширюються, це стосуються як елементів захисту так і елементів загроз, зокрема останнім часом різновидів атак та їх реалізацій стає де далі більше, далі будуть переведені декілька з них [1]:

- вірусна атака, наступний вид атаки є більш витончений метод отримання доступу до закритої інформації - використання спеціальних програм для ведення роботи на комп'ютері жертви, а також подальшого поширення (це віруси і черв'яки). Такі програми призначені для пошуку і передачі своєму власникові секретної інформації, або просто для нанесення шкоди системі безпеки і працездатності комп'ютера жертви. Принципи дії цих програм різні.

- фрагментація даних, де при передачі пакета даних протоколу IP по мережі може здійснюватися розподіл цього пакета на кілька фрагментів. Згодом, при досягненні адресата, пакет відновлюється з цих фрагментів. Зловмисник може ініціювати посилку великого числа фрагментів, що призводить до переповнення програмних буферів на приймальній стороні і, в ряді випадків, до аварійного завершення системи.

- нав'язування пакетів, зловмисник відправляє в мережу пакети з помилковим зворотною адресою. За допомогою цієї атаки зловмисник може перемикати на свій комп'ютер з'єднання, встановлені між іншими комп'ютерами. При цьому права доступу зловмисника стають рівними прав того користувача, чиє з'єднання з сервером було переключено на комп'ютер зловмисника.

- нав'язування хосту хибного маршруту з допомогою протоколу ICMP. У мережі Інтернет існує спеціальний протокол ICMP (Internet Control Message Protocol), однієї з функцією якого є інформування хостів про зміну поточного маршрутизатора. Дане керуюче повідомлення носить назву redirect. Існує можливість посилки з будь-якого хоста в сегменті мережі помилкового redirect-повідомлення від імені маршрутизатора на атакується хост. В результаті у хоста змінюється поточна таблиця маршрутизації і, в подальшому, весь мережевий трафік даного хоста буде проходити, наприклад, через хост, відіслав помилкове redirect-повідомлення. Таким чином можливо здійснити активну нав'язування помилкового маршруту всередині одного сегмента мережі Інтернет

- атака smurf полягає в передачі в мережу широкомовних ICMP запитів від імені комп'ютера-жертви. В результаті комп'ютери, які виконують ці широкомовні пакети, відповідають комп'ютера-жертви, що призводить до істотного зниження пропускної здатності каналу зв'язку і, в ряді випадків, до повної ізоляції атакується мережі. Атака smurf виключно ефективна і широко поширена.

Протидія: для розпізнавання даної атаки необхідно аналізувати завантаження каналу і визначати причини зниження пропускної здатності.

- атака DNS spoofing, результатом даної атаки є внесення надв'язуваного відповідності між IP-адресом і доменним ім'ям в кеш DNS сервера. В результаті успішного проведення такої атаки всі користувачі DNS сервера отримають невірну інформацію про доменні імена і IP-адреси. Дана атака характеризується великою кількістю DNS пакетів з одним і тим же доменним ім'ям. Це пов'язано з необхідністю підбору деяких параметрів DNS обміну.

Протидія: для виявлення такої атаки необхідно аналізувати вміст DNS трафіку або використовувати DNSSEC.

- атака IP spoofing, велика кількість атак в мережі Інтернет пов'язано з підміною вихідного IP-адреси. До таких атак відноситься і syslog spoofing, яка полягає в передачі на комп'ютер-жертву повідомлення від імені іншого комп'ютера внутрішньої мережі. Оскільки протокол syslog використовується для ведення системних журналів, шляхом передачі помилкових повідомлень на комп'ютер-жертву можна нав'язати інформацію або замести сліди несанкціонованого доступу.

Протидія: виявлення атак, пов'язаних з підміною IP-адрес, можливо при контролі отримання на одному з інтерфейсів пакета з вихідним адресою цього ж інтерфейсу або при контролі отримання на зовнішньому інтерфейсі пакетів з IP-адресами внутрішньої мережі.

Доцільно має сенс у цих випадках використовувати комплексні способи захисту та їх модернізації, зокрема процес виявлення таких загроз, що в першу чергу виправдано для не професійних користувачів комп'ютерної техніки. Такий аналіз, в цілях доцільності навіювання загроз дозволяє в режимі on-line, виявляти і усувати будь-яку з висче перекислених атак. Низче запропоновано алгоритм експрес виявлення, для більшості професій не потребуючих високого знання комп'ютера.

Алгоритм запропонований нами, в своїй основі реалізує саме такийпринцип дії, де він обробляє сигнатуру «атаки», і вже по цій сигнатурі проводить аналіз, класифікацію і після цього проводить заходи, щодо боротьби з атакою. Особливість цієї програми в тому, що вона не тільки аналізує тип атака, вона (запропонована програма), збирає повну статистику що до атак в цілому, якими був атакований ПК. При поточному аналізі, ця програма в режимі реального часу проводить постійний моніторинг. Якщо ПК був уражений жодною із атак, ця програма аналізує і це, - та на основі свого аналізу робить певні дії. В першу чергу це відключення виконання поточних програм, які мають доступ до важливої інформації, чи в той же час обробляють інформацію, (список програм, вибираються користувачем, крім того програма має свій список програм за замовчуванням, роботу яких треба зупинити). Фактично дана програма зупиняє процеси які мають доступ до важливої інформації. Крім того, запропонована програма, невідмінно від антивірус/меж-мережевого екрану, проводить аналіз, стосовно атак, збирає статистику, та запобігає витоку інформації з важливих процесів які виконуються у рижими «реального часу». Реалізацію цього алгоритму, користувач бачить у вигляді статичних даних при включені ПК.

Список використаних джерел

1. https://uk.wikipedia.org

УДК: 004.056.53

Лісова В. П.
Харківський національний університет радіоелектроніки

Аналіз методів пошуку прихованих мереж в корпоративній мережі з розгорнутими ролями Active Directory

Розвиток глобальних мереж привів до багаторазового збільшення кількості не тільки користувачів, але і атак на комп'ютери, що підключені до Інтернету. Щорічно збитки підприємств через недостатній рівень захищеності комп'ютерів оцінюються десятками мільйонів доларів. Тому при підключенні до Інтернету локальної або корпоративної мережі необхідно подбати про забезпечення її інформаційної безпеки.

Значну загрозу для конфіденційності даних становлять приховані мережі. Вони виникають під час підключення одного USB-накопичувача до декількох комп'ютерів, котрі в свою чергу можуть бути підключені до різних мереж. Окрім цього USB-пристрої можуть бути використані внутрішніми інсайдерами для розкрадання конфіденційної інформації або для завантаження зловмисного програмного забезпечення в мережу компанії.

На сьогоднішній день на ринку представлена велика кількість програмного забезпечення класу DLP (Data Leak Prevention), основною метою котрих є запобігання витоків конфіденційних даних з інформаційної системи. У роботі були розглянуті методи пошуку прихованих мереж на прикладі DeviceLock. Важливою особливістю DeviceLock є можливість розгортання і управління через групові політики в домені Active Directory, завдяки чому продукт легко інтегрується в існуючу інфраструктуру організацій будь-якого масштабу, причому ця можливість не є єдиним способом управління. Тобто це програмне забезпечення може існувати не тільки самостійно, а й бути міцним інструментом, що буде підсилювати роботу штатних засобів захисту Active Directory.

Також було встановлено, що використання спеціального програмного забезпечення значно полегшить роботу системного адміністратора і дозволить автоматизувати процес моніторингу мережі. Але головний недолік використання подібних програм полягає у тому, що не має гарантії що в коді програми, котра використовуються для пошуку прихованих мереж, не прописаний експлойт. Шкідливий код може завдати значної шкоди операційній системі і стати причиною витоку конфіденційної інформації.

Уникнути всіх ризиків, що пов'язані з відпрацюванням шкідливого коду, можуть допомогти штатні засоби Microsoft Windows Server з розгорнутими ролями Active Directory. Правильне використання можливостей цієї операційної системи дозволить знайти приховані мережі, а контроль за використанням змінних носіїв на рівні групових політик допоможе запобігти витоку інформації, що має обмежений доступ.

Було встановлено, що пошук прихованих мереж на базі USB можливий, якщо системний адміністратор володіє інформацією стосовно всіх USB підключень. Під час підключення USB-накопичувача, в реєстрі робочого комп'ютера фіксуються ідентифікатори VID, PID, а також серійний номер. Проаналізувавши ці дані, можна знайти комп'ютери, котрі сумісно використовують один і той же зовнішній накопичувач. Таким чином, після знаходження прихованого зв'язку, буде знайдена й прихована мережа. Цей метод є дієвим, але не дуже зручний у використанні та повільний. Тому у роботі були розглянуті більш швидкі методи пошуку прихованих мереж.

Для того, щоб автоматизувати процес збору інформації про використання USB-пристроїв, на кожному з робочих комп'ютерів домену, було запропоновано відпрацювання спеціального скрипту – невеликої програми, котра здатна виконувати окремі послідовності дій, що були прописані у її сценарії.

За допомогою скрипту системний адміністратор має можливість прискорити свою роботу, адже якщо готового сценарію не має, йому доведеться виконувати ці дії вручну з відповідними витратами часу і можливостями появи помилок. Але для написання подібного компоненту відповідальна особа також має володіти певною скриптовою мовою програмування, або скористатися вже написаним скриптом. У випадку використання готового програмного файлу проблема спрацювання прихованого шкідливого коду залишається актуальною, тому у компанії варто розробити свій власний скрипт, котрий буде відповідати усім її вимогам і побажанням.

Пошук прихованих мереж проводився з використанням Windows Remote Management (WinRM). WinRM – серверна частина програми віддаленого управління, до якого можливо віддалене підключення за допомогою клієнта Windows Remote Shell (WinRS).

З метою автоматизації збору інформації скрипт був протестований в мережі з одним доменом на базі Active Directory (AD). Для підтвердження запуску на віддалених комп'ютерах в локальній мережі використовувався обліковий запис адміністратора домену, який знадобився під час запуску скрипту. За результатами відпрацювання скрипту був отриманий файл CSV, у який була виведена наступна інформація: ім'я комп'ютера, IP (в форматі IPv4), ім'я USB-пристрою, ID (унікальний ідентифікатор).

Вирішення проблеми прихованих мереж проводилося за допомогою групової політики Active Directory. Служба каталогів має гнучкий механізм настройок GPO, на основі котрого можна заборонити використання зовнішніх пристроїв (всіх або деяких), задати список дозволених і відключити автозапуск. Існує 10 політик, що дозволяють уникнути широкого спектру загроз.

Було встановлено, що використання групових політик дає можливість контролювати інформацію, котра буде циркулювати у прихованих мережах. Це міцний і гнучкий інструмент, котрий дозволяє передбачити практично будь-який варіант дій зловмисника і завадити йому отримати доступ до даних з обмеженим доступом.

Превентивним засобом захисту є налаштування шифрування BitLocker To Go, котре буде захищати конфіденційні дані навіть якщо їх вдалося скопіювати на USB-накопичувач. Доступ до зашифрованих носіїв можливий за паролем або шляхом використання смарт-карти з будь-якого комп'ютера. Список комп'ютерів, з яких дозволено читання інформації, при необхідності, також можна обмежити, що не дозволить винести інформацію за межі контрольованої зони.

У службі каталогів Active Directory є можливість налаштувати аудит файлів та папок. Таким чином можна також відслідковувати коли відбулося копіювання файлів – це буде відображатися у Журналі безпеки. Якщо поєднати цю інформацію з часом підключення USB-пристрою, то вдасться встановити які дані потрапили до рук зловмисника або інсайдера.

Список використаних джерел

1. *Детектування прихованих мереж на базі USB-пристроїв [Електронний ресурс]*. – Режим доступу: *https://www.securitylab.ru/analytics/489523.php*
2. *Контроль використання USB–накопичувачів в Windows Server 2008 Електронний ресурс]*. – Режим доступу: https://it–community.in.ua/2014/08/kontrol–ispolzovaniya–usb–nakopitelej–v–windows–server–2008.html/

УДК 004.052.2

Мартиненко О. О., Телющенко В. А.
Національний авіаційний університет

Оцінка надійності програмних засобів захисту

Інформація придбала значну цінність, яка чітко визначається реальним прибутком, одержуваної від її використання, або розміром збитку в результаті негативного впливу. Тому так важливо вчасно оцінити надійність програмних засобів захисту, т.я. від програмного забезпечення залежить багато чого: від правильного функціонування комп'ютерної техніки до адаптації роботи програмної системи з користувачем.

Для забезпечення високої надійності функціонування та безпеки застосування створюваних складних комплексів програмних засобів (ПЗ) захисту необхідні розробка і застосування ефективних методів і засобів, попередження й виявлення помилок, а також підтвердження надійності програм і оперативний захист функціонування ПЗ. Задля забезпечення безпечного функціонування ПЗ, постійного контролю й оцінки надійності з точки зору захисту, пропонується створювати програмні модулі і функціональні компоненти високої, гарантійної якості. Через те, що в програмних засобах можуть бути закладені логічні бомби, троянські коні, віруси, які призводять до швидкого порушення цілісності ПЗ, вважається що на програмному рівні найбільшою небезпекою є віруси та несанкціонований доступ до даних з мережі.

Грунтуючись на методі Дейкстра, де неформальне позначення моделі загального оператора проводиться за допомогою довільної пропозиції, що розкриває в загальних рисах його зміст, що в свою чергу, призведе до узагальненого результату. Синтез на основі його схеми шаруватих систем дозволить по етапно деталізувати використовувані структури і вибрати відповідні структури даних, які будуть використовуватися при виконанні модулем своїх функцій. Це допоможе виявляти й усувати різні дефекти і помилки проектування, що в значній мірі визначить логіку і якісні показники розроблюваного модуля. Але метод Дейкстра не приділяє достатньої уваги до захисту цього модуля. Значно надійнішим та якіснішим є криптографічний захист. В цих засобах для кожного сеансу зв'язку автоматично розповсюджуються ключі для шифрування. Задля підвищення рівня безпеки такі ключі дійсні лише протягом одного сеансу та після завершення сеансу вони вилучаються. Також потрібно використовувати електронний підпис. У разі застосування звичайного підпису та печатки після підписання документ може бути змінений. Змінити ж електронний документ, підписаний цифровим підписом неможливо. Щоб виключити можливість ненавмисного пошкодження, функції розповсюдження і вилучення ключів виконують сертифікаційні центри, де реєструються всі користувачі. Через те, що в програмних засобах можуть бути закладені логічні бомби, троянські коні, віруси, які призводять до швидко виведення з ладу програмної та апаратної частини, потрібно до стандартної схеми отримання ключів додати етапи: попереднього установлення дійсності суб'єкта, що отримує ресурси, та перевірку відповідності характеру дій до заданих повноважень. Система захисту повинна реалізовувати ці функції за допомогою набору привілеїв. Кожний користувач отримує свій набір, який не дає змогу модифікувати програмну частину.

Комплексне, скоординоване застосування цих засобів в процесі створення, розвитку та застосування в програмної середовища дозволяє виключати більшість видів загроз або значно послабити їх вплив. Тим самим рівень досягнутої надійності стає передбачуваним і керованим.

Список використаних джерел

1. *Майерс Г. Надёжность программного обеспечения. М.: Мир, 1980, 360 с*
2. *Лужецький В. А., Кожухівський А. Д., Войтович О. П. Основи інформаційної безпеки. – Вінниця: ВНТУ, 2009. – 268 с.*
3. *Э.Дейкстра. Заметки по структурному программированию / У.Дал, Э.Дейкстра, К.Хоор. Структурное программирование. - М.: Мир, 1975. - С. 24-97.*
4. *Дідковська М.В. Аналіз моделей оцінювання надійності програмного забезпечення // Вісник НТУУ «КПІ». Інформатика, управління та обчислювальна техніка. №41, Київ, 2004. – С. 103-120.*

УДК 004.4

Марченко А. Ю.
Київський національний університет будівництва і архітектури

Мінімізація факторів суб'єктивності в тестуванні на проникнення

З метою оптимізації загальної оцінки захищеності інформаційної системи за результатами її оцінювання кількома незалежними експертами пропонується використовувати алгоритм МГУА (метод групового урахування аргументів).

Основна структура алгоритму складається з наступних блоків:

1) попередньої обробки спостережень (Нехай D це вибірка {$X_{D,i}$, $Y_{D,i}$}, 1<=i<=n, де $X_{D,i}$ - вектори незалежних змінних розмірності m, $Y_{D,i}$ - залежні змінні, n - кількість наборів. В нашому випадку компоненти вектора $X_{D,i}$ відіграють роль оцінок окремих конкретних критеріїв вразливості і-м експертом, m - кількість критеріїв; залежною змінною $Y_{D,i}$ є загальна оцінка захищеності системи, n – кількість незалежних експертів. Вибірка D розбивається на навчальну G та тестову C);

2) вибору вигляду функцій-моделей, які описуватимуть залежність між змінною Y та вільними змінними X (в нашому випадку це поліноми другого степеня);

3) розрахунку параметрів моделей-претендентів (На навчальній виборці G формується система рівнянь $A_G(X_G)W_G=Y_G$ відносно вектора W_G шуканих коефіцієнтів поліному, кількість елементів G дорівнює розмірності W_G. Система розв'язується методом найменших квадратів);

4) обчислення зовнішнього критерію селекції та вибору оптимальної моделі (На тестовій підвибірці C застосовується критерій регулярності - середньоквадратична похибка між векторами $A_c(X_c)W_G$ та Y_c. Обирається поліном-модель з найменшою похибкою).

МГУА має перевагу при малих вибірках за рахунок можливості вибору моделі, що оптимально враховує інформативність наявних даних.

Коефіцієнти многочлену (вектор W_G) являють собою фактично оцінки відносної важливості кожного окремого критерію вразливості в тестуванні на проникнення. Це дозволяє за наявності оцінок окремих критеріїв вразливості (від різних незалежних експертів) розрахувати загальну оцінку захищеності системи.

Після вибору оптимальної моделі на тестовій виборці результати загальної оцінки захищеності системи окремими експертами можна оптимізувати, для цього необхідно обрати експерта з таблиці та натиснути кнопку «Оптимізувати». На формі з'явиться оптимізований результат тестування, який можна зберегти у базі даних. Збережені результати відображаються в таблиці. З головного вікна програми можливо потрапити: у форму вибірки даних для створення навчальної вибірки, тестової вибірки, до вікна керування обліковими записами; до вікна додавання тестових даних.

Для збільшення швидкості роботи програми була реалізована багатопоточність на мові Java. Створено програмне забезпечення для одночасного розрахунку коефіцієнтів на різних наборах функцій-поліномів. Кожен набір функцій опрацьовується в окремому потоці. В роботі виконано паралельне опрацювання двох функцій.

Список використаних джерел

1. *Івахненко А.Г. Індуктивний метод самоорганізації моделей складних систем / Івахненко А.Г. - К.: Наук. думка, 1982. - 296 с.*
2. *Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— К.: ДУТ, 2015.— 288 с.*
3. *The types of pentests you must know about [Електронний ресурс].— Режим доступу: https://blog.cipher.com/the-types-of-pentests-you-must-know-about.*

УДК 004.056

Машталер Д. О.
ДВНЗ «Криворізький національний університет»

Динамічне використання групи ключів в асиметричному шифруванні

Для асиметричного шифрування існують такі основні "погані" сценарії: 1) зловмисник матиме закритий ключ і шифр-текст; за допомогою ключа він отримає відкритий текст та отримає доступ до конфіденційної інформації; 2) зловмисник матиме відкритий ключ і відкритий текст і зможе відправити нам підроблене повідомлення, що завдасть нам деяку шкоду; 3) зловмисник буде підмінювати інформацію в процесі передачі по каналу зв'язку завдяки одному з ключів, що критично знизить користь цієї інформації. У всіх цих випадках зловмисник знає хоча б один ключ і отримує повний контроль над інформацією що кодується. Тому я вважаю, що використання декількох ключів одразу значно збільшить стійкість шифру.

Для прикладу у якості асиметричного шифру обрано алгоритм RSA.

Для (де)шифрування за алгоритмом RSA потрібно встановити наступні параметри: відкритий {e;n} та закритий {d;n} ключі, де e - відкритий ключ,d - закритий ключ, n - модуль. Щоб сформувати группу ключів додамо наступні параметри кожній парі ключів:

Відкритий ключ - {e;n;index;count;sc}, закритий - {d;n;index;count;sc}, де index - індекс, count - кількість символів, що (де)кодуються цією парою за раз, sc - спецсимвол.

Параметр index: Обирається одна пара, що буде кореневою, її індекс буде дорівнювати нулю, усім іншим парам можуть бути присвоєні випадкові числа від 1 включно до найменшого модулю цієї групи n мінус одиниця включно. Також індекси не повинні повторюватися.

Параметр count: Це може бути будь-яке випадкове число з проміжку від 1 включно до нескінченності.

Параметр sc: Будь який символ що можна закодувати за допомогою модуля n і який не зустрічається у вхідному алфавіті.

Для того щоб працювати з групою ключів відкритий текст потрібно змінити. А саме додати до нього шаблонні вставки. Шифрування матиме два режими. Перший з використанням параметром count, та другий - з параметром sc.

Для першого методу нам знадобиться колекція, що зберігатиме індекси пар ключів, які будуть по черзі змінюватись при шифруванні. Колекція працюватиме у режимі FIFO. Для другого методу цю колекцію потрібно вдосконалити, кожен елемент це пара {count*;index}, де count* - через скільки символів потрібно замінити ключ шифрування на новий. Модифікований відкритий текст для першого режиму буде мати вставки у тексті з індексу ключа, для другого ж режиму він буде складатись з двох послідовних символів: першим символом буде спец символ sc ключа index_old, та другий символ - наступний ключ для шифрування index_new. У результаті новий асиметричний алгоритм буде мати більшу крипто стійкість, через те, що зростає вимога до кількості потрібної інформації для злому. Також такі алгоритми можуть використовуватись у корпоративній безпеці для розподілу прав різним корпоративним групам шляхом надання не всієї групи відкритих ключів, а лише певної її частини.

Перевагою використання груп ключів є те, що після модифікації ми захищаємо інформацію від перших двох сценаріїв тому що від тепер зловмисник повинен мати всю групу закритих/відкритих ключів з усіма параметрами та повну копію відкритого/шифр тексту щоб правильно його розшифрувати чи непомітно підробити.

До недоліків можна віднести те, що час на кодування та декодування зростає. Відкритий текст потребує попередньої обробки перед шифруванням. Більш складний процес формування ключів.

УДК 004.492.3

Михайловский Р. Л., Шматок О. С.
Національний авіаційний університет

Система стеганоаналізу на основі розпізнавання образів

Основним завданням стеганоаналізу є визначення факту наявності прихованого повідомлення в можливому контейнері (мові, відео, зображення). Вирішити це завдання можливо шляхом вивчення статистичних характеристик сигналу. Наприклад, розподіл молодших бітів сигналів має, як правило, шумовий характер (помилки квантування). Вони несуть найменшу кількість інформації про сигнал і можуть використовуватися для вставки секретного повідомлення. При цьому, можливо, зміниться їх статистичні характеристики, що і послужить для атакуючого ознакою наявності прихованого каналу.

Розпізнавання образів. Розпізнавання образів (об'єктів, сигналів, ситуацій, явищ або процесів) - завдання ідентифікації об'єкта або визначення будь-яких його властивостей по його зображенню (оптичне розпізнавання) або аудіо-записи (акустичне розпізнавання) та інші характеристики [1].

Одним з базових понять яке застосовується в теорії розпізнавання є множини. У комп'ютері множини представляється набором неповторюваних однотипних елементів. Слово «неповторюваних» означає, що якийсь елемент в множині або є, або його там немає. Універсальне множина включає всі можливі для розв'язуваної задачі елементи, порожня множина не містить жодного [2].

Образ - класифікаційне угруповання в системі класифікації, яка об'єднує (виділяє) певну групу об'єктів за певною ознакою. [3-5] Образи мають характерною властивістю, що виявляється в тому, що ознайомлення з кінцевим числом явищ з одного і того ж безлічі дає можливість дізнаватися як завгодно велике число його представників. Образи мають характерні об'єктивними властивостями в тому сенсі, що різні люди, які навчаються на різному матеріалі спостережень, здебільшого однаково і незалежно один від одного класифікують одні і ті ж об'єкти. У класичній постановці задачі розпізнавання універсальне множина розбивається на частини-образи. Кожне відображення будь-якого об'єкта на сприймаючі органи системи, що розпізнає, незалежно від його положення щодо цих органів, прийнято називати зображенням об'єкта, а множини таких зображень, об'єднані певними загальними властивостями, являють собою образи.

Методика віднесення елемента до якого-небудь образу називається вирішальним правилом. Ще одне важливе поняття - метрика, спосіб визначення відстані між елементами універсальної множини.

$$\|x_1 - x_2\| = \sqrt{\sum_{i=1,d} (x_1[i] - x_2[i])^2}$$

Чим менший цей період, тим більше схожими є об'єкти (символи, звуки та ін.) - те, що ми розпізнаємо. Зазвичай елементи задаються у вигляді набору чисел, а метрика - у вигляді функції. Від вибору уявлення образів і реалізації метрики залежить ефективність програми, один алгоритм розпізнавання з різними метриками буде помилятися з різною частотою. Далі розглянемо різні методи які відносяться до різних груп розпізнавання образів.

Класифікація по найближчому середньому значенні У класичному підході розпізнавання образів, в якому невідомий об'єкт для класифікації представляється у вигляді вектору елементарних ознак [6, 7]. Система розпізнавання на основі ознак

можуть бути розроблені різними способами. Ці вектори можуть бути відомі системі заздалегідь в результаті навчання або передбачені в режимі реального часу на основі будь-яких моделей.

$$\bar{x}_i = \frac{1}{n_i} \sum_{j=1,n_i} x_{i,j}$$

де $x(i,j)$ - j-й еталонний ознака класу i, nj - кількість еталонних векторів класу i.

Простий алгоритм класифікації полягає в угрупованні еталонних даних класу з використанням вектору математичного очікування класу (середнього значення).

Тоді невідомий об'єкт буде ставитися до класу і, якщо він істотно ближче до вектору математичного очікування класу і, ніж до векторів математичних очікувань інших класів. Цей метод підходить для задач, в яких точки кожного класу розташовуються компактно і далеко від точок інших класів [3-5, 8].

Класифікація по відстані до найближчого сусіда. Інший підхід при класифікації полягає у віднесенні невідомого вектору ознак x до того класу, до окремого зразком якого цей вектор найбільш близький. Це правило називається правилом найближчого сусіда. Класифікація по найближчому сусіду може бути більш ефективна, навіть якщо класи мають складну структуру або коли класи перетинаються [8].

При такому підході не потрібно припущень про моделях розподілу векторів ознак в просторі. Алгоритм використовує тільки інформацію про відомих еталонних зразках. Метод рішення заснований на обчисленні відстані x до кожного зразка в базі даних і знаходження мінімальної відстані. Переваги такого підходу очевидні:

- в будь-який момент можна додати нові зразки в базу даних;
- деревовидні і сіткові структури даних дозволяють скоротити кількість обчислюваних відстаней [9-11].

Крім того, рішення буде краще, якщо шукати в базі не одного найближчого сусіда, а k. Тоді при k> 1 забезпечує найкращу вибірку розподілу векторів в d-вимірному просторі. Однак ефективне використання значень k залежить від того, чи є достатня кількість в кожній області простору. Якщо є більше двох класів то прийняти вірне рішення виявляється складніше.

Приклади завдань розпізнавання образів: розпізнавання букв; розпізнавання штрих-кодів; розпізнавання автомобільних номерів; розпізнавання осіб та інших біометричних даних; розпізнавання зображень; розпізнавання мови.

Список використаних джерел

1. *Миленький А.В. Классификация сигналов в условиях неопределенности. М.: Советское радио, 1975. 328 с.*
2. *M. Castrillón, . O. Déniz, . D. Hernández и J. Lorenzo, «A comparison of face and facial feature detectors based on the Viola–Jones general object detection framework,» International Journal of Computer Vision, № 22, pp. 481-494, 2011*
3. *Харкевич А.А. Опознавание образов // Радиотехника. 1959. Т. 14, №5. С. 3-9.*
4. *Пугачев В.С. Введение в теорию вероятностей. М.: Наука, 1968. 368 с.*
5. *Вапник В.Н. Червоненкис А.Я. Теория распознавания образов (статистические проблемы обучения). М.: Наука, 1979. 416 с.*
6. *Сенин А.Г. Распознавание случайных сигналов. Новосибирск: Наука, 1974. 76 с.*
7. *Фомин Я.А., Тарловский Г.Р. Статистическая теория распознавания образов. М.: Радио и связь, 1986. 263 с.*
8. *Тихонов В.И. Статистическая радиотехника. М.: Радио и связь, 1982. 624 с.*
9. *Леман Э. Проверка статистических гипотез. М.: Наука, 1979. 408 с*
10. *Фукунага К. Введение в статистическую теорию распознавания образов. М.: Наука, 1979. 367с.*
11. *Закс Ш. Теория статистических выводов. М.: Мир, 1975. 776 с.*

УДК 004.056.5
Нєдєльський Д. С., Конопліцька-Слободенюк О. К.
Центральноукраїнський національний технічний університет

Grey Wizard – нові технології захисту веб-ресурсів

З кожним роком все більше і більше з'являється шпигунських програм, які мають за мету викрадати цінну інформацію у користувачів. Найчастіше від кібератак страждають банківські сфери або юридичні установи. Наслідком такого втручання у конфіденційність файлів насамперед є заволодіння банківськими рахунками користувача для подальшого використання цих данний в своїх цілях, а саме викрадення коштів користувача.

Для створення безпечного користування інтернет-ресурсами, було створено програму Gray Wizard shield яка забезпечує захист від DDoS атак. Данна програма працює як зворотній проксі, іншими словами це сервер між користувачем та інтернет простором. Він забезпечує фільтрацію веб-трафіку, та дозволяє проходити лише справжнім користувачам.

DdoS-атака - одна з самих великих загрозв сучасному світі, найчастіше такий вид атак спрямований на державні та фінансові установи для заволодіння конфіденційними файлами. Для захисту від вірусної атаки Gray Wizard змінює записи DNS і таким чином перенаправляє весь HTTP на сервер фільтрації, де всі пакети ретельно перевіряються. Ці сервери знаходяться по всьому світу, тому програмний продукт може швидко та ефективно перевіряти та блокувати атаки з ближчого сервера, таким чином зменшити час на обробку данних та завантаження сторінки.

Також програмним продуктом підтримується захист від атак на веб-сервери. Веб сторінки часто відвідуються автоматизованими агентами, яких використовують зловмисники для збору данних, таих як, логіни, паролі, адреси електронних скриньок, номери банківських карт. Цих автоматизованих агентів часто називають "Ботами". Отримані данні зловмисники використовують для входу на персональні сторінки користувачів та вилучення цінних матеріалів або коштів.

Брандмауер веб-розширень зосереджується на захисті веб-сторінок. Атаки, спрямовані на рівень користувача, часто дуже важко виявляти. На відміну від інших типів атак, вони не споживають посилання та системні ресурси сервера. Скоріше, вони спрямовані на конкретні уразливості вашої програми. За допомогою цього типу атаки достатньо одного комп'ютера для ефективного блокування веб-сторінки або викрадення даних.

Якщо можна втрутитися у вміст веб-сайту, бази даних та вмісту додатків, хакери легко атакують їх, щоб викрасти конфіденційні дані або здійснити інші шахрайські (такі як спам, фішинг або заміщення веб-сторінок) атаки. Наслідки включають в себе шкоду репутації компанії та її фінансів.

WAF забезпечує ефективний захист від атак XSS (Cross-Site Scripting), SQL-данних та записує до своєї бази данних ідентифкатори виявлених атак. Крім того, це дозволяє блокувати активність підозрілих ботів, які крадуть вміст. Правила захисту визначаються користувачем, і захист активний цілодобово. Функція WAF адресована всім власникам веб-сайтів.

Отже програмний продукт добре справляється зі своєю задачею, забезпечує безпечне користування інтернет простором, та захищає користувачів від кібератак.

Список використаних джерел

1. https://oberig-it.com/statti-ta-ogljadi/grey-wizard-zahist-veb-resursiv-novi-tehnologii-ta-rishennja/
2. https://greywizard.com/shield/ddos-protection
3. https://www.kaspersky.ru/resource-center/threats/mobile

УДК 004.056

Оксіюк О. Г., Руденко А. С.
Київський національницй університет імені Тараса Шевченка

Захист інформації у корпоративних мережах на основі моделі OSI

Сучасні системи захисту інформації повинні відповідати запитам сучасного бізнесу в умовах росту числа загроз безпеки інформації, що виходять із самої корпоративної мережі. Сучасні системи безпеки повинні захищати не окреміелементи мережі, аінформацію у виглядіінформаційних ресурсів і потоків незалежно від місця й часу їхнього виникнення [3]. Інформаційна безпека є складовою частиною інформаційних технологій - області, що розвивається надзвичайно високими темпами. Розробка сучасної системи інформаційної безпеки вимагає, з одного боку, відстеженняшвидких змін в інформаційних технологіях і погрозах, що з'являються, а з іншого боку – обліку реальних характеристик апаратного й програмного забезпечення корпоративних мереж і систем. Процедура придбання пристроїв інформаційної безпеки не складна. Істотно більш складним є рішення проблем: як захищати і які засоби безпеки застосовувати. Це рішення охоплює й керування інформаційною безпекою, включаючи планування, розробку політики безпеки й проектування необхідних процедур безпеки [3, 4]. Інформаційна безпека представляє собою багатогранну сферу діяльності, в якій успіх можливий тільки при систематичному, комплексному підході.

На данному етапі будуть розглянутіспособи захисту інформації на рівні моделі OSI.

Захист інформації на мережному рівні. Більшість атак мережевого рівня пов'язані з використанням протоколу IP: підмінаIP-адреси вузла, нав'язування хибного маршруту, перехоплення зловмисником діапазону IP-адрес та отримання інформації про логічну структуру мережі (IP-адреси вузлів, доменніімена), проблеми одноразової ідентифікації заIP-адресою. Можна виділити такі підходи до захисту від наведених атак:

- створення прив'язок IP – MAC-порт для запобігання підмініIP-адреси та несанкціонованому підключенню до мережі [1],
- використання технології трансляції мережних адрес (Network Address Translation – NAT [2]) для приховання від зовнішніх зловмисників діапазону IP-адрес організації та логічної структури мережі,
- створення списків контролю доступу (Access Control List– ACL [2]) для обмеження доступудо вузлів та протоколів/сервісів прикладного рівня.

Протокол NAT використовується для передачі пакетів з IP-адрес, призначених тільки для внутрішнього використання, в зовнішні мережіі для вирішення задачі приховування внутрішньої логічної структури мережі від зовнішніх мереж [2], [3]. NAT транслює тільки той трафік, який проходить між внутрішньою і зовнішньою мережею і визначений для трансляції. Будь-який трафік, який не відповідає критеріям трансляції або той, який проходить між іншими інтерфейсами на маршрутизаторі, ніколи не транслюється і пересилається з використанням маршрутизації. Слід звернути увагу на те, що протокол NAT виконує тільки трансляцію адрес і не виконує функції фільтрації. Для заборони проходження пакетів з зовнішніх мереж у внутрішню необхідно застосовувати відповідні списки доступу.

Списки контролю доступу(Access Control List – ACL [2], [3]) містять набір правил, де визначено дію над пакетами і параметри пакетів для фільтрації (адреси відправників та отримувачів, номера портів протоколів транспортного рівня тощо).

Захист на транспортному рівні. Для протоколів транспортного рівня характерна відсутність перевірки джерел інформації, що сприяє таким загрозам, як перехоплення та підключення до відкритих портів протоколів транспортного рівня.

Для вирішення цієї задачі використовується протокол SSL/TLS (SecureSocketLayer / TransportLayerSecurity) [10], який реалізує шифрування іавтентифікацію між транспортними рівнями приймачаі передавача. Процедура роботи протоколу SSL/TLS включає в себе три основних фази:

- діалог між сторонами, метою якого є вибір алгоритму шифрування;
- обмін ключами на основі криптосистем з відкритим ключем або автентифікація на основі сертифікатів;
- передача даних, які шифруються за допомогою симетричних алгоритмів шифрування;

Захист інформації на прикладному рівні. Відкритий характер протоколів прикладного рівня зумовлює велику кількість загроз, пов'язаних з основною проблемою цих протоколів —передачаінформації у нешифрованому вигляді. Використання на прикладному рівні процедур ідентифікації таавтентифікації користувачів із подальшою авторизацією утворює також загрозу перехоплення або підбору облікових записів та паролів. Значну загрозу також становлять віруси та шпигунське програмне забезпечення, які діють саме на прикладному рівні, DoS та DDoS-атаки наінформаційні системи.

Зазвичай, коли говорять про засоби захисту на прикладному рівні, розглядають два підходи: використання серверів-посередників (proxy) [4] та використання механізмів контролю сесій (Statefull Inspection),основи якого було розглянуто вище. Обидва ці підходи реалізують контроль за з'єднанням, але не вирішують задачу аналізу вмісту пакетів та фільтрації пакетів з небажаним вмістом, що не дозволяє запобігти розповсюдженню вірусів через електронну пошту, встановленню несанкціонованих програмних додатків через Інтернет на робочі станції, несанкціонованій зміні вмісту веб-сайтів тощо. Для захисту від таких порушень може бути використана контентна фільтрація, яка базується на сигнатурному аналізі пакетів [5]–[6]. Цей механізм передбачає аналіз інформації у пакеті, при чому як заголовка пакета, так і поля даних. Це дозволяє встановити відповідність між інформацією з поля даних та конкретними додатками, контролювати передачу даних між конкретними додатками та проводити фільтрацію небажаної інформації. Враховуючи, що інформація аналізується по пакетно, цей механізм не дозволяє повністю аналізувати трафік мережних додатків.

Список використаних джерел

1. *P. V. Kucherniuk, "Metody i tekhnolohii zakhystu komp'iuternykh merezh (fizychnyi ta kanalnyirivni) [Methods and technologies for computer networks protection (the physical and data link layers)]," Microsystems, Electron. Acoust., vol. 22, no. 6, pp. 64–70, 2017, DOI: 10.20535/2523-4455.2017.22.6.113191.*
2. *E. Knipp et al., Managing Cisco Network Security. Elsevier Inc., 2002, ISBN: 978-1-931836-56-2.*
3. *S. Wilkins and T. Smith, CCNP Security. SECURE 642-637 Official Cert Guide. Cisco Press, 2011, ISBN: 978-1-58714-280- 2.*
4. *A. D wankhade and P. N. Dr Chatur, "Comparison of Firewall and Intrusion Detection System," Int. J. Comput. Sci. Inf. Technol., vol. 5, no. 1, pp. 674–678, 2014, URL: http://ijcsit.com/docs/Volume 5/vol5issue01/ijcsit20140501145.pdf/*
5. *A. M. Plaskovsky, A. G. Novopashenny, Y. E. Podgurskiy, and V. S. Zaborowski, Metodyi i sredstva zaschity i kompyuternoy informatsii. Mezhsetevoe ekranirovanie. Razgranichenie dostupa na prikladnom urovne [Methods and means of protection of computer information. Firewall. Access control at the application level]. St. Petersburg, Russia: Publishing House of STU, 2012*
6. *A. Ott, "Sovremennyie tendentsii v oblasti kontentnoy filtratsii [Modern trends in content filtering]." [Online]. Available: http://alexott.net/ru/writings/cf/. [Accessed: 01-Feb-2017].*

УДК 004.056

Павлов І. І.
ДВНЗ «Криворізький національний університет»

Методи підвищення надійності та захищеності корпоративних комп'ютерних мереж

Головна тенденція розвитку сучасного суспільства тісно пов'язана з розвитком інформаційної складової та, як наслідок, інформаційної безпеки. Питання інформаційної безпеки на сучасному етапі розглядаються як пріоритетні в державних структурах, в наукових установах і в комерційних фірмах. Метою роботи є розробка заходів для забезпечення надійності та захищеності корпоративної мережі підприємства.

Розвиток засобів, методів та форм автоматизації процесів обробки інформації та масове застосування персональних комп'ютерів, які обслуговуються непідготовленими користувачами, роблять інформаційний процес уразливим за низкою показників.

Основними факторами, що сприяють підвищенню інформаційної уразливості, є наступні:

- зберігання в єдиних базах даних інформації різного призначення та різної приналежності;
- розширення кругу користувачів, що мають безпосередній доступ до ресурсів обчислювальної системи та наявних в ньому масивів даних;
- ускладнення режимів роботи технічних засобів обчислювальних систем;
- автоматизація обміну інформацією, в тому числі на великих відстанях;

Виявлення атак реалізується за допомогою аналізу або журналів реєстрації операційної системи і прикладного програмного забезпечення, або мережевого трафіку в реальному часі. Компоненти виявлення атак, розміщені на вузлах або сегментах мережі, оцінюють різні дії. Засоби виявлення атак функціонують відразу на двох етапах. На першому етапі ці засоби доповнюють традиційні механізми новими функціями, підвищуючи захищеність корпоративної мережі. Наприклад, при проникненні в мережу через брандмауер, система виявлення атак зможе виявити і запобігти діям, що відрізняються від нормальної поведінки користувача. Ці системи однаково ефективно функціонують і для захисту периметра корпоративної мережі, доповнюючи можливості брандмауера, і для захисту внутрішніх сегментів мережі.

При розробці заходів націлених на захист інформації у локальній мережі насамперед необхідно забезпечити фізичну захищеність обладнання. Тобто доступ в усі серверні шафи і кімнати повинен бути наданий строго обмеженому числу користувачів. Утилізація жорстких дисків і зовнішніх носіїв, повинна проходити під жорстоким контролем.

Антивірусний захист є головним елементом захисту корпоративної мережі від зовнішніх атак. Комплексний антивірусний захист мінімізує можливість проникнення в мережу вірусів. В першу чергу необхідно захистити сервера, робочі станції, інтернет шлюзи і систему корпоративного чату.

Необхідно забезпечити захист віртуальних приватних мереж (VPN). На сьогоднішній день велика кількість працівників багатьох компаній здійснюють робочу діяльність віддалено, у зв'язку з цим необхідно забезпечити максимальний захист трафіку, а реалізувати це допоможуть шифровані тунелі VPN. При цьому категорично забороняється використовувати стороннє програмне забезпечення для доступу до корпоративної мережі.

Компанії які обробляють велику кількість електронної пошти, в першу чергу схильні до фішинг-атак. Основними способами фільтрації спаму є:

- установка спеціалізованого програмного забезпечення;
- створення і постійне поповнення «чорних» списків ір-адрес пристроїв, з яких ведеться спам-розсилка;
- аналіз листів (повинен здійснюватися аналіз не тільки текстової частини, але і всіх вкладень - фото, відео і текстових файлів);
- визначення «масовості» листів: спам-листи зазвичай ідентичні для всіх розсилок, це і допомагає відстежити їх антиспам-сканером, таким як «GFI MailEssentials» і «Kaspersky Anti-spam».

Використання брандмауера забезпечить захист від несанкціонованого віддаленого доступу. У той же час він забезпечить «невидимість» інформації про структуру мережі. Брандмауер повинен виконувати наступні функції :

Забезпечувати комплексний захист. Захист мережі в сьогоднішніх умовах з безліччю загроз безпеки вимагає кращих в своєму класі засобів захисту від шкідливих програм і вторгнень на основі аналізу уразливості, оцінки репутації та інших важливих факторів.

Працювати з бізнес-політиками. брандмауер нового покоління повинен надавати можливість реалізації політик для роботи з додатками в усій своїй повноті і глибині. Крім того, він повинен давати можливість детального моніторингу і контролю (на основі політик підприємства) різних додатків для сумісної роботи, призначених як для особистих, так і для службових цілей.

Забезпечувати застосування політик з урахуванням пристрою користувача. Брандмауер повинен забезпечувати повноцінний контроль доступу пристроїв користувачів до мережі з урахуванням їх місцеположення

Будь-який засіб захисту створює додаткові незручності в роботі користувача, при цьому перешкод тим більше, чим менше часу приділяється налагодженню систем захисту. Адміністратор безпеки повинен щодня обробляти дані реєстрації, щоб своєчасно коригувати параметри, які забезпечують адаптацію до змін в технології обробки інформації. Без цього будь-яка система захисту, якою б хорошою вона не була, приречена на повільне вимирання. Окрему увагу слід приділити навчанню адміністратора. В процесі навчання адміністратор отримує базові знання про технології забезпечення інформаційної безпеки, про наявні в операційних системах підсистемах безпеки і про можливості систем захисту, про технологічні прийоми, які використовуються при їх налаштування і експлуатації.

Необхідно виконувати періодичний аудит системи інформаційної безпеки. Корпоративна мережа є постійно змінюваною структурою: з'являються нові сервери і робочі станції, змінюється програмне забезпечення та його налаштування, склад інформації, персонал, що працює в організації. Все це призводить до того, що ступінь захищеності системи постійно змінюється і, що найбільш небезпечно, знижується.

Слід пам'ятати, що не існує стандартних рішень, однаково добре працюючих в різних умовах. Завжди можливі і необхідні доповнення до розглянутого загального плану організації захисту корпоративної мережі, що враховують особливі умови тієї чи іншої організації. Однак реалізація комплексу розглянутих заходів з урахуванням можливих доповнень здатна забезпечити достатній рівень захищеності інформації в корпоративній мережі.

УДК 004.738

Покотило О. А.
Житомирський державний технологічний університет

Аналіз моделі Cyber Kill Chain та її використання для забезпечення захисту мережі

Сучасні направлені атаки – це цілий комплекс засобів, в результаті застосування яких відбувається зараження мережі. Процес злому не відбувається моментально, цьому передує цілий набір дій. Модель Cyber Kill Chain якраз і описує всі етапи атаки.

Cyber Kill Chain визначає, що мають зробити зловмисники для того, щоб досягти своєї цілі, здійснюючи атаки на мережу. Завдяки цій моделі відомо, що блокування хакерів на будь-якому етапі розриває весь ланцюг атаки. Для досягнення успіху злочинці мають пройти через всі етапи, тому для досягнення мінімального успіху стороні, яка захищається, досить всього лиш блокувати їх на будь-якому етапі.

Кінцевий вузол є елементом, через який проходять всі атаки. Тому зупинка атаки на цьому рівні суттєво підвищує шанс на протидію будь-якій кібератаці. Можливість успіху буде більшою, якщо спромогтися зупинити хакерів на ранніх етапах.

Крім того, кожне втручання і сліди, яке воно залишає на кінцевій точці, - це можливість краще дізнатися дії хакера та використати дану інформацію собі на користь. Чим краще розуміння зловмисників та способів виконання їх атак, тим більша вірогідність побудувати ефективніший захист[1].

В кібербезпеці «вбивчий ланцюг» (Kill Chain) – це стадії атаки на інформаційні системи. На даний момент розроблена структура безпеки для виявлення та реагування на інциденти, створені за допомогою Kill Chain. До основних етапів «вбивчого ланцюга» відносять:

- розвідка – вибір цілі, збір інформації та виявлення особливостей організації, дослідження активності компанії в соцмережах;
- озброєння – створення шкідливих програм, орієнтуючись на виявлені вразливості, та підготовка засобів для відправлення на ціль;
- доставка – передача експлойту до цілі по електронній пошті або шляхом компрометації мережевої служби;
- проникнення – розгортання шкідливої програми;
- встановлення – початок процесу встановлення зловмисного програмного забезпечення та створення «чорного ходу» для контролю експлойтом без відома жертви;
- керування та контроль – віддалене керування ціллю через канал керування та контролю або сервер, збір необхідної секретної інформації;
- дія – безпосереднє здійснення шкідливих дій, зокрема крадіжка інформації або виведення з ладу пристроїв мережі жертви[2].

Для захисту від «вбивчого ланцюга» засоби захисту мережі мають бути розроблені з урахуванням його етапів, адже кожен з них веде до збільшення зусиль та витрат для протидії атакам та відновлення системи. Всі організації мають бути готові до ситуації, коли хакер отримав доступ до внутрішньої корпоративної мережі, і бути готовими діяти негайно.

Традиційний підхід до забезпечення безпеки має бути розширений за рахунок методів, заснованих на розумінні Cyber Kill Chain, і використані технологій, які можуть попередити отримання хакером доступу до кінцевих вузлів, а також зупинити їх на будь-якому можливому етапі.

Для попередження дій злочинця, необхідно суворо обмежити публікацію даних компанії в Інтернеті. Крім того, рекомендується здійснювати детальний аналіз можливих типів атак, і вчасно попереджувати їх виникнення. Це можливо завдяки спеціальним засобам захисту, які постійно контролюють стан мережі для виявлення аномальної поведінки[3].

Запобігання нападу ускладнює злочинцю процес проникнення і зараження системи. Це можна зробити за допомогою встановлення індивідуальної політики безпеки та аналізу поточних сигнатур за допомогою звичайних вірусних сканерів. Відповідні рекомендації для компаній можуть бути отримані на основі аналізу векторів атак, що використовуються шкідливим програмним забезпеченням. Основним питанням тут є виявлення будь-якого існуючого недоліку безпеки як на рівні клієнта, так і на рівні сервера.

У найгіршому випадку, коли зловмисник перейшов на етап безпосереднього здійснення шкідливих дій, вже мають бути попередньо визначені конкретні дії, які мають чітко виконувати співробітники компанії, зокрема технічні процедури та аналіз. Це єдиний спосіб запобігти значному пошкодженню.

Організації мають можливість збільшувати свої знання в галузі безпеки інформаційних технологій та розвивати їх, використовуючи концепцію Cyber Kill Chain. Постійне навчання, засноване на аналізі поточних загроз, допомагає захистити себе від кібератак[4].

Визначення цілей кіберзлочинців також є проблемою, зокрема через велику кількість та складність кібератак. Коригування власних запобіжних заходів відповідно до стратегії зловмисника практично неможливе, орієнтуючись тільки на модель Cyber Kill Chain. Підхід, який спрямований на необхідність завжди залишатися на крок попереду злочинця, на практиці можна реалізувати в досить обмеженій мірі. Тим не менше, кінцеве завдання полягає в тому, щоб знайти відповідний спосіб усунення можливих недоліків, визначених в моделі Cyber Kill Chain.

Отже, кожен крок в Cyber Kill Chain – це можливість зупинити атаку під час її безпосереднього здійснення. Стратегія безпеки має зосереджуватися не на якомусь конкретному кроці, адже атака почалася до того і триватиме після того, як шкідливий файл буде фактично доставлений. Жоден окремий продукт не може забезпечити безпеку на кожному рівні розглянутої моделі. Тому необхідно розробити комплекс засобів та заходів, які зможуть здійснювати захист системи до початку атаки, бути корисними під час нападу, і залишатися ефективними після того, як атака завершиться.

Список використаних джерел

1. *Что такое Cyber-Kill Chain и почему ее надо учитывать в стратегии защиты [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://habr.com/company/panda/blog/327488/.*
2. *Understanding The Cyber Kill Chain [Електронний ресурс] – Режим доступу до ресурсу:* https://www.gomindsight.com/blog/understanding-cyber-kill-chain/.
3. *Cyber Kill Chain Increasing IT security in companies step-by-step [Електронний ресурс] – Режим доступу до ресурсу: https://www.hornetsecurity.com/en/knowledge-base/cyber-kill-chain.*
4. *What's the Cyber Kill Chain? [Електронний ресурс] – Режим доступу до ресурсу: https://safebreach.com/What-is-the-Cyber-Kill-Chain.*

УДК 004.056

Романько С. В., Астраханцев А. А.
Харківський національний університет радіоелектроніки

Методи вбудовування цифрових водяних знаків у відеофайли, що стиснені за стандартами MPEG

Одним з найважливіших питань, що вирішуються суспільством на сьогоднішній день, є забезпечення захисту авторського права. Ефективним шляхом вирішення проблеми захисту авторського права, що дозволяє перевірити правовласника цифрових відеофайлів, є організація забезпечення автентичності за рахунок впровадження цифрових водяних знаків (ЦВЗ), що вбудовуються за допомогою стеганографічних алгоритмів. На сьогоднішній день пропонуються алгоритми, які здійснюють автентифікацію відеофайлів, проте наявні розробки не позбавлені ряду істотних недоліків, залишаючи актуальним завдання розробки нових стеганографічних алгоритмів, що дозволяють одночасно забезпечувати приховану передачу даних і аутентифікацію відеофайлу.

Існує велика кількість методів вбудовування ЦВЗ у нерухомі зображення та в відеофайли. Більшість з них призначене для вбудовування у нестиснені відеофайли [1], в той час як інші вбудовують ЦВЗ безпосередньо у стиснені [2].

Останнім часом багато уваги приділяється алгоритмам вбудовування, що мають такі властивості, як стійкість до атак та прихованість вбудованої інформації. Ці алгоритми можна класифікувати за типом області в яку вбудовується або вилучається цифровий водяний знак, їх пропускною здатністю, продуктивністю в режимі реального часу та стійкістю до конкретних типів атак. В залежності від області, в яку вбудовується ЦВЗ, сучасні алгоритми вбудовування в відеофайли можна умовно поділити на три основні групи: методи вбудовування в просторовій області, в області перетворень та методи вбудовування в відеофайли, що стиснені за стандартами MPEG. Основні види методів вбудовування в відеофайли наведені на рисунку 1.

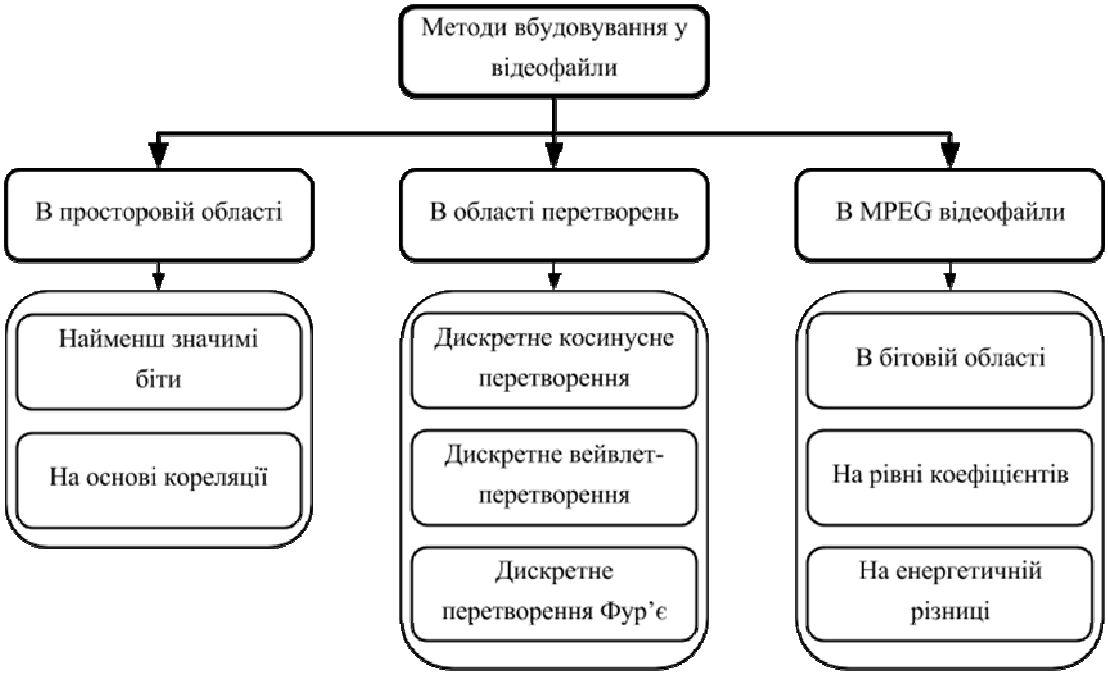


Рисунок 1 – Класифікація методів вбудовування в відеофайли

Здебільшого методи вбудовування ЦВЗ у MPEG відеофайли основані на MPEG-1, MPEG-2 і MPEG-4 стандартах. У цих методиках вбудовування ЦВЗ і стиснення об'єднані, щоб зменшити складність обробки відеофайлу. Стиснення в блокових методах, таких як MPEG-2 отримується за допомогою двонаправленого і прямого передбачення кадру для усунення часової надмірності, а у статистичних методах для усунення просторової надмірності. Методи вбудовування цифрового водяного знаку в відеофайл, що стиснене за стандартом MPEG, дуже чутливі до повторної компресії з різними параметрами, а також до перекодування, що є основним недоліків цих методів. Існує велика кількість методів, на основі форматів MPEG-2 і MPEG-4, в тому числі алгоритми, засновані на модифікації групи кадрів, високочастотного перетворення ДКП коефіцієнтів та класифікації ДКП блоків.

В стандарті MPEG використовуються три типи кадрів: I-кадри, P-кадри і B-кадри (див. рис. 2). Кодування I кадрів схоже на JPEG через використання сусідніх пікселів простору кадру для стиснення надлишкової інформації; P-кадр повинен використовувати попередній кадр при кодуванні і поточний кадр може бути використаний в якості опорного кадру для прогнозування. B-кадру потрібен попередній кадр і наступний кадр для прогнозування. Методика впровадження водяних знаків в стиснений відеофайл полягає у вбудовуванні водяного знаку в послідовність бітів, стиснених за допомогою стандарту кодування, наприклад, MPEG-2 або MPEG-4. Цей метод має більш низьку обчислювальну складність в порівнянні з іншими методами.

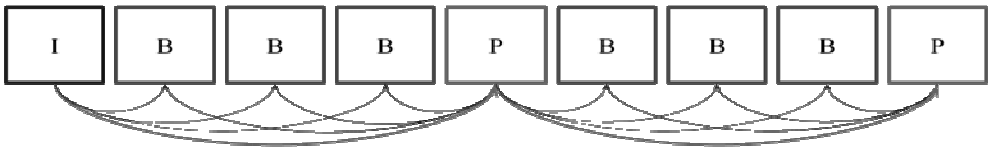


Рисунок 2 – Послідовність кадрів формату MPEG

Ліанг та співавтори [3] запропонували застосовувати хмарні водяні знаки для ідентифікації стиснутого відеофайлу MPEG-2, який також здатний відрізнити шкідливі атаки від звичайної обробки. В цьому методі відеофайл спочатку розділяється на кадри і з нього витягуються особливі вектори. Ці особливі вектори діють як водяні знаки, які вбудовуються у відеофайл.

Метод вбудовування на основі об'єктів був запропонований Абделсамадом [4] з метою перевірки аутентифікації відеофайла MPEG-4. Запропонована методика заснована на формі адаптивного дискретного вейвлет-перетворення, алгоритм вбудовування якого полягає у впровадженні водяного знака у вейвлет-коефіцієнти і молодші біти зображення тільки в області до кодування MPEG-4. Кожен кадр розкладається на передній план і фоновий об'єкт, вбудовування здійснюється в середні вейвлет-коефіцієнти на передньому плані. Автор використав візуальну модель, щоб отримати кращий компроміс між непомітністю та стійкістю.

Список використаних джерел

1. *Multiresolution Video Watermarking using Perceptual Models and Scene Segmentation [Електронний ресурс] // Режим доступу: http://ieeexplore.ieee.org/abstract/document/638832.*
2. *Digital watermarking applied to MPEG2 coded video sequence exploiting space and frequency masking [Електронний ресурс] // Режим доступу: http://ieeexplore.ieee.org/iel5/7221/19490/00900989.pdf.*
3. *Video authentication and tamper detection based on cloud model [Електронний ресурс] // Режим доступу: https://goo.gl/CpSvGB.*
4. *A waveletbased object watermarking system for mpeg4 video [Електронний ресурс] // Режим доступу: https://goo.gl/7wXQpF.*

УДК 004.715

Сандаков О. О., Гермак В. С.
Центральноукраїнський національний технічний університет

Огляд сучасних криптографічних алгоритмів

Різкий стрибок зростання обсягів даних, що циркулюють і зберігаються в комп'ютерних і телекомунікаційних системах, створює сприятливі умови для протиправних дій щодо електронної інформації. Мета цієї роботи полягає в огляді криптографічних алгоритмів. Для вирішення задач інформаційної безпеки найважливішого значення набувають програмно-технічні засоби управління правами доступу до ресурсів інформаційно-обчислювальних систем, що забезпечують розмежування повноважень користувачів, залучених в технологічний процес автоматизованої обробки інформації. Ефективне управління доступом досягається широким застосуванням криптографічних перетворень, що забезпечують аутентифікацію і цілісність інформації, а також її захист від несанкціонованого доступу.

На цей час проблема інформаційної безпеки в обчислювальних системах набула масового характеру. У зв'язку з зазначеними факторами зростає роль засобів шифрування в якості базового механізму захисту інформації, використання якого істотно підвищує рівень захищеності інформації на всіх етапах її обробки. Застосування механізму шифрування як елемента системи захисту набуло в даний час технологічного характеру. Актуальність теми пов'язана з широким застосуванням комп'ютерних технологій в системах управління та обробки інформації, що зумовлює найважливішу роль програмних механізмів захисту, включаючи програмні реалізації криптографічних алгоритмів. В основі шифрування лежать два основних поняття - це алгоритм та ключ. Ключі влаштовані так, що повідомлення, зашифроване однією половинкою, можна розшифрувати лише іншою половиною (але не тією, якою воно було закодовано). Створивши пару ключів, ми можемо поширювати публічний ключ (відкриту половину) і надійно зберігати закритий ключ (свою половинку). Використання шифрування характеризується масовістю застосування та різноманітністю умов застосування. Криптографічні алгоритми в свою чергу характеризуються в залежності від числа ключів, що застосовуються в конкретному алгоритмі. Криптосистеми з ключем діляться на симетричні і асиметричні системи шифрування.

В наш час існує ряд класифікацій криптографічних алгоритмів. За ключами: безключові криптографічні алгоритми - не використовують в обчисленнях ніяких ключів; одноключові криптографічні алгоритми - працюють з одним ключовим параметром (секретним ключом); двохключові криптографічні алгоритми - на всіх робочих стадіях застосовують два ключові параметри: секретний і відкритий ключ.

Ще одним критерієм класифікації криптоалгоритмів є тип виконуваних перетворень над блоками відкритого тексту. За цим критерієм криптоалгоритми поділяють на підстановчі і перестановчі. У перестановчих шифри блоки інформації не змінюються самі по собі, але змінюється їх порядок проходження, що робить інформацію недоступною сторонньому спостерігачеві. Символи шифри змінюють самі блоки інформації за певними законами.

Говорячи про атаки на шифри, можна виділити наступні види атак: атака на основі шифро-тексту, атака на основі відомого відкритого тексту, атака на основі вибіркового відкритого тексту.

При атаці на основі шифро-тексту крипто аналітику відомий тільки закодований текст і на його основі він повинен дізнатися секретний ключ шифрування.

Атака на основі відкритого тексту передбачає, що крипто аналітику відомі одна або кілька пар «відкритий текст / шифро-текст», зашифрованих на одному ключі, і на основі цієї інформації він проводить свій аналіз.

Виконуючи атаку на основі вибіркового відкритого тексту, зловмисник має можливість подати на вхід шифрувального пристрою довільний відкритий текст і отримати відповідний йому шифро-текст. Для того, щоб називатися практично стійким, крипто алгоритм повинен успішно протистояти будь-якому з перерахованих типів атак.

Основними властивостями криптографічних алгоритмів за якими оцінюється їх якість є: - Криптографічна стійкість незалежно від умов технологічного застосування, які можуть бути використані для спроби несанкціонованого доступу до інформації; - Висока швидкість шифрування з метою мінімізації зменшення продуктивності інформаційних систем, що функціонують в реальному масштабі часу; - Економічність апаратної або програмної реалізації.

Конфіденційність даних забезпечується завдяки введенням в алгоритми спеціальних ключів, це надає можливість використовувати один алгоритм з різними ключами для відправки різним адресатам. На теперішній час найпоширеніші три підкласи несиметричних систем, стійкість яких базується відповідно на складності факторизації числа великої розрядності, знаходженні дискретного логарифма у кінцевих полях і знаходженні дискретного логарифма в групі точок еліптичних кривих. До першого класу відноситься RSA-подібні шифри, до другого Диффі-Хеллманна та Ель-Гамаля.

RSA-алгоритми. У RSA відкритим параметром є багаторозрядний модуль перетворення (не менш 512 біт). Ключ формування підпису є закритим, а ключ зняття підпису звичайно відкритий.

Алгоритми Диффі-Хеллманна. Першим із способів, що одержали поширення, виявився експоненційний ключовий обмін. Суть його в наступному: - А і В вибирають випадкове число X_A і X_B відповідно. А передає В $Y_A = a^{XA} \pmod q$, а В - А - $Y_B = a^{XB} \pmod q$. Так званий примітивний елемент кінцевого поля Галуа GF(q), чудова властивість якого полягає в тому, що його ступені дають усі ненульові значення елементів поля. У якості секретного ключа використовується значення $Y_a = a^{XAXB} \pmod q$, яке А одержує зведенням переданого В числа в ступіні X_A, відомому тільки йому, а В - отриманого від А числа у відому тільки йому ступіні X_B. Криптоаналітик змушений обчислювати логарифм принаймні одного з переданих чисел.

Алгоритми Ель-Гамаля. Основна ідея алгоритму Ель-Гамаля полягає в тому, що не існує ефективних методів рішення порівняння $a^x == b \pmod p$. Через $Z(n)$ позначимо відрахування по модулю n, через $Z^*(n)$ - мультиплікативну групу оборотних елементів в $Z(n)$. Через $a^b \pmod n$ будемо позначати піднесення a у ступінь b у кільці $Z(n)$. Якщо p – просте число, то група $Z^*(p)$ ізоморфна $Z(p-1)$. За складністю ведення крипто аналізу вище перераховані алгоритми приблизно еквівалентні, тому що в наш час задачі факторизації багаторозрядного модуля вважаються розрахунково нерозв'язними для використовуваних на практиці 512-ти бітних модулів (вимагають порядку 10^{20} групових операцій). Однак при однаковій довжині модуля алгоритм Ель-Гамаля є трохи більш стійким. Довжина ключа не менше 320 біт.

Отже було розглянуто 3 основних класи криптографічних алгоритмів: RSA-подібні шифри, Диффі-Хеллманна та Ель-Гамаля. Найбільш стійким являється алгоритм Ель-Гамаля, тому найбільш вигідним з боку захисту даних буде являтися саме цей криптографічний алгоритм.

Список використаних джерел

1. Вязмина М.В.Проблемы защиты информации в компьютерных системах и пути их решения.
2. Бауэр Ф. Расшифрованные секреты. Методы и принципы криптологии. М.: Мир, 2007. 550 с
3. Молдовян А.А., Молдовян Н.А., Рад Б.Я. Криптографія.

УДК 004.49

Сердюк О. Ю.
Харківський національний університет радіоелектроніки

Підхід щодо оцінки вразливостей інформаційних систем з використанням метрик стандарту NIST CVSS v3

Оцінка ризиків інформаційної безпеки є одним з найголовніших процесів під час побудови та функціонування систем менеджменту інформаційної безпеки (СМІБ). Реалізація даного процесу дозволяє спрогнозувати потенційні дії зловмисників враховуючі існуючі вразливості інформаційних систем (ІС), та потенційні збитки в організації внаслідок втрати конфіденційності, цілісності або доступності інформаційних активів.

Для оцінки вразливостей ІС можуть використовуватися сканери вразливостей, результати експертних оцінок, різні вимірювання, наприклад рівнів електромагнітного поля комп'ютерної техніки для оцінки витоку через помічні електромагнітні випромінювання тощо. Для отримання значення вразливості одним з найефективніших механізмів є методика стандарту NIST CVSS v3 (Common Vulnerability Scoring System, версія 3).

Мета дослідження – аналіз методики NIST CVSS v3 з метою використання її результатів для оцінки ризику інформаційної безпеки ІС.

В стандарті NIST CVSS v3 критичність вразливостей оцінюється на основі декількох глобальних груп метрик:

- базові метрики – постійні та не змінюються з часом (таблиця 1);
- тимчасові метрики – оцінюють поточний стан експериментальних методів або наявність коду щодо експлуатації вразливостей, наявність будь-яких виправлень вразливостей, наприклад офіційним розробником ІС, а також ступінь впевненості в існуванні вразливості.
- метрики навколишнього середовища – дозволяють деталізувати базові та тимчасові метрики та врахувати рівень важливості впливу ІТ-активів, вразливості яких можуть бути проексплуатовані зловмисником, на організацію користувача.

В даній роботі пропонується використовувати лише базові метрики, так як вони є універсальними і достатніми для проведення оцінок.

Таблиця 1 - Параметри базових метрик стандарту NIST CVSS v3

Значення	*Опис*	*Числове значення*
Вектор доступу (Attack Vector)		
Потребується фізичний доступ	зловмисникові потрібен безпосередній фізичний доступ до об'єкта, на якому розташована вразливість	0,2
Потребується локальний доступ	зловмисник експлуатує вразливість за допомогою локального доступу, шлях атакуючого - через можливості читання / запису / виконання.	0,55
Можливий доступ із суміжної мережі	атака обмежена однією спільною фізичною (наприклад, Bluetooth, IEEE 802.11) або логічною (наприклад, локальною IP-підмережею) мережею, і не може бути виконана через границю шару OSI (наприклад, маршрутизатор)	0,62

Значення	*Опис*	*Числове значення*
Можливий доступ з будь-якої мережі	зловмисник може атакувати віддалено через OSI layer 3 (мережевий рівень)	0,85
Складність атаки (Attack Complexity)		
Низька	Немає особливих умов для доступу зловмисником до вразливості (наприклад, коли система доступна багатьом користувачам одночасно або коли вразлива конфігурація працює на безлічі вузлів мережі)	0,77
Висока	Успішність атаки вимагає від злочинця здійснювати певні вимірювані зусилля для підготовки чи виконання атаки. Наприклад проведення розвідки системи захисту, підготовка цільового середовища для підвищення надійності експлуатації вразливості, вбудовування себе в логічний мережевий шлях між ціллю та ресурсом, що атакується, для перехоплення або зміни мережевих зв'язків (наприклад, атака - людина посередині, man in the middle)	0,44
Обов'язкові привілеї (Privileges Required)		
Немає	Зловмиснику не потрібна авторизація перед атакою	0,45
Висока	Зловмиснику потрібні привілеї, які надають основні можливості користувача, які, як правило, можуть впливати лише на налаштування та файли, що належать користувачеві. Крім того, зловмисник з низькими привілеями може мати можливість впливати лише на нечутливі ресурси	0,56
Низька	Зловмисник авторизований, тобто вимагає привілеїв, які забезпечують значний (наприклад, адміністративний) контроль над вразливим компонентом, який може вплинути на загальні параметри та файли	0,704
Взаємодія з користувачем (User Interaction)		
Немає	Вразливість системи може експлуатуватися зловмисником без необхідності дій будь-якого іншого (крім зловмисника) окремого користувача (або процесу, ініційованого користувачем)	0,85
Потрібно	Для успішної експлуатації уразливості зловмисником будь-якому іншому користувачеві (крім зловмисника) потрібно вжити певні дії, перш ніж вразливість може бути використана	0,62
Збиток конфіденційності, цілісності, доступності		
Відсутній	Можливість порушення конфіденційності, цілісності або доступності інформації відсутня	0,0

Значення	*Опис*	*Числове значення*
Низький	Існує значна можливість порушення конфіденційності, цілісності або доступності інформації: часткове розкриття конфіденційності інформації, часткової модифікації даних або системних файлів, зниження продуктивності або виведення з ладу деяких функцій системи	0,22
Високий	Існує можливість повного розкриття конфіденційної інформації, модифікації будь-яких даних системи, повного виведення з ладу системи	0,56

Параметр критичності вразливостей на заданому елементі ІС пропонується розраховувати за формулою:

$$R_{CVSS} = \frac{\sum_{i=1}^{n} B_{score_i}}{n} \cdot \frac{1}{10}, \quad (1)$$

де $\sum_{i=1}^{n} B_{score_i}$ – сума всіх метрик по усім вразливостям елемента ІС; n – загальна кількість знайдених вразливостей на елементі ІС.

Так як $B_{score} \in [0;10]$, то поділ на 10 забезпечує нормування параметру критичності вразливостей $R_{CVSS} \in [0;1]$.

Подальші розрахунки параметрів виконуються згідно з CVSS v3:

$$B_{score} = \lceil 1{,}08 \cdot (I + E) \rceil, \quad (2)$$

де B_{score} – це покажчик базової метрики; I – збиток; E – можливість експлуатації.

$$I = 7{,}52 \cdot (ISC - 0{,}029) - 3{,}25 \cdot (ISC - 0{,}02)^{15}, \quad (3)$$

$$ISC = 1 - (1 - I_c) \cdot (1 - I_i) \cdot (1 - I_a), \quad (4)$$

де *ISC* – рівень впливу; I_c, I_i, I_a – збитки від порушення конфіденційності, цілісності та доступності.

$$E = 8{,}22 \cdot A_v \cdot A_c \cdot A_n \cdot A_в, \quad (5)$$

де: A_v – значення вектору доступу; A_c – значення складності атаки; A_n – значення параметру привілеїв; $A_в$ – значення параметру взаємодії з користувачем.

Перевагою даного методу можна вважати простоту. Критичність вразливостей на основі базових метрик стандарту NIST CVSS розраховується експертами та є універсальною і незмінною. Розрахована критичність може бути використана при створенні сигнатур сканерів вразливостей, які дозволяють в автоматизованому режимі виявляти вразливості та їх рівні критичності на елементах ІС.

Список використаних джерел

1. Common Vulnerability Scoring System v3.0: Specification Document [Електронний ресурс]. – Режим доступу: https://www.first.org/cvss/specification-document.

УДК 004.021

Трапезнікова В. П., Телющенко В. А.
Національний авіаційний університет

Алгоритм вибору альтернативних засобів захисту для автоматизованої системи

Найбільший інтерес при побудові КСЗІ викликають технічні засоби приймання, обробки, зберігання та передавання інформації. Зважаючи на таке та враховуючи відсутність єдиної системної методики концептуального проектування СЗІ на даний час актуальним і найбільш пріоритетним завданням є передусім проведення повноцінного ефективного вибору засобів і методів фізичного захисту інформації (ФЗІ) в інформаційно-комунікаційних системах, а також складу засобів системи ФЗІ, що, як результат, дозволить приймати певні стратегічні рішення по варіантах побудови системи.

Метою роботи є розробка алгоритму вибору засобів систем фізичного захисту інформації в автоматизованій системі.

У ході даної роботи ми з'ясували основні проблеми захисту та сформували на основі типових ситуацій алгоритм вибору засобів для комплектування системи фізичного захисту інформації (рис. 1).

На першому кроці реалізації методики здійснюється збір вихідних даних про об'єкт захисту, необхідних для опису характеристик його окремих елементів (виділення матеріальних та інформаційних цінностей, категорування об'єкта захисту і його елементів тощо). На другому кроці здійснюється ранжирування актуальних загроз фізичної безпеки. При цьому кожному носію інформації ставиться у відповідність численний набір загроз, реалізованих при ненульовому значенні просторового, часового та енергетичного факторів. На третьому кроці проводиться визначення найбільш уразливих місць об'єкта захисту. Враховуючи, що СФЗІ з повним перекриттям передбачає створення для кожного шляху проникнення загрози певного бар'єру захисту (бар'єр – сукупність механізмів фізичного захисту, спрямованих на локалізацію уразливостей системи), головне завдання третього кроку алгоритму полягає у знаходженні раціонального набору засобів ФЗІ в кожному бар'єрі. Вибір засобів здійснюється на користь альтернативи, що має найбільший коефіцієнт відповідності. На четвертому кроці алгоритму будується оцінна матриця та здійснюється розрахунок показника захищеності системи. Якщо бар'єр відповідає заданим вимогам, приймається рішення про його розміщення на об'єкті захисту. Якщо вимоги не дотримуються відбувається повторний вибір. Завданням роботи є вибір засобу ФЗІ в автоматизованій системі підприємства.

Одним з найважливіших етапів при проектуванні СФЗІ є здійснення оптимального вибору засобів для комплектування перспективної системи, при певних експлуатаційних і технічних обмеженнях. Зважаючи на те, що на цей час єдиної системної методики концептуального проектування СФЗІ й зокрема методики вибору засобів СФЗІ не існує у роботі були проаналізовані фізичні загрози інформаційної безпеки в ІКС та підтверджено необхідність здійснення їхньої локалізації.

На основі цих даних побудовано алгоритм вибору альтернативних засобів захисту інформації, що надає можливість урахувати весь спектр загроз відносно об'єктів захисту й протиставити кожній загрозі відповідний засіб фізичного захисту. Використання запропонованого підходу дозволить порівнювати різні засоби захисту й вибрати серед них більш раціональні з точки зору забезпечення необхідного рівня захисту.

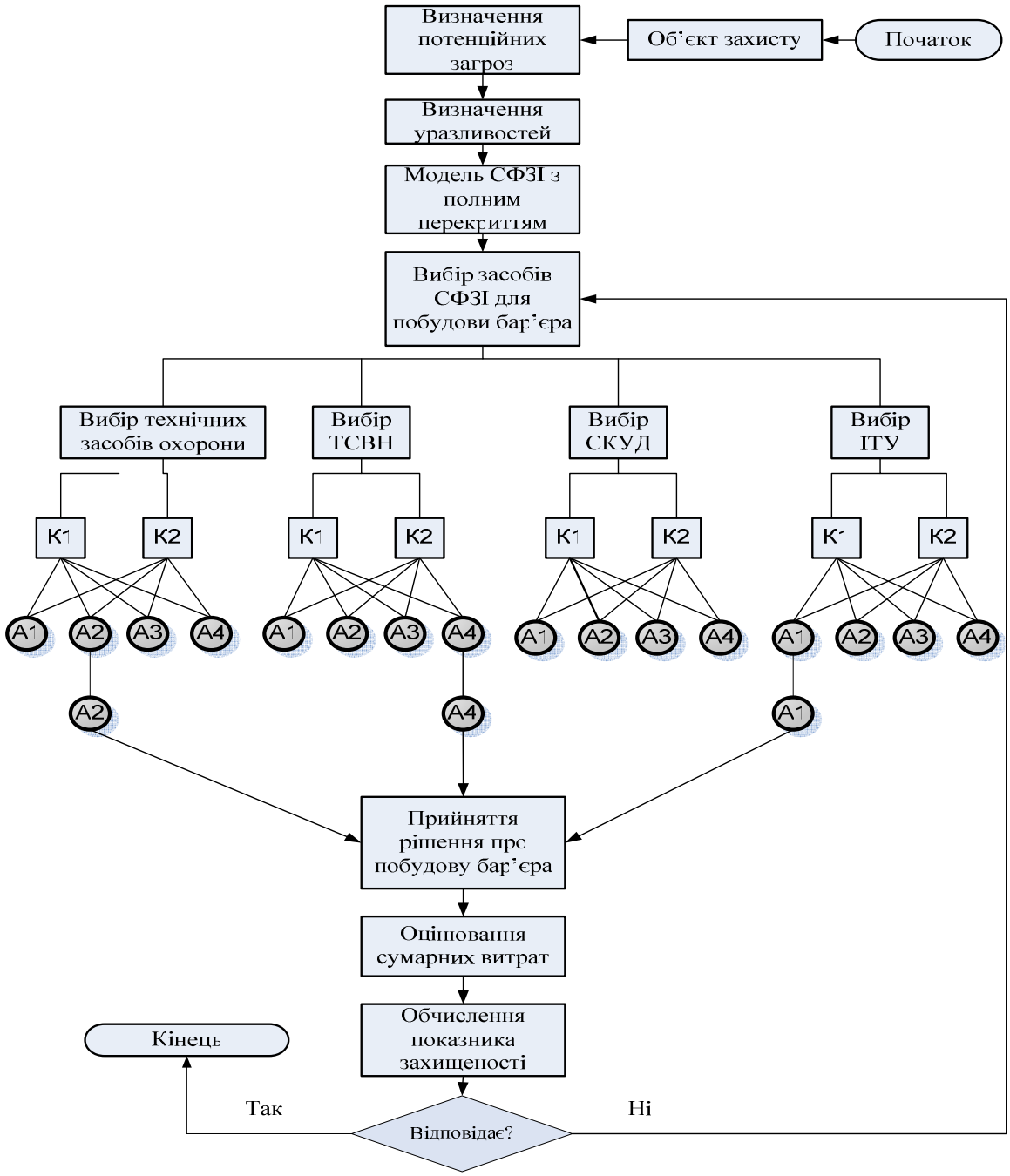


Рисунок 1 – Алгоритм вибору засобів для комплектування СФЗІ

Практична значимість даної роботи полягає в тім, що її матеріали і результати можуть бути використані при проектуванні СФЗІ та вибору засобів для її комплектування. Теоретична значимість – матеріали й результати даної дипломної роботи можуть бути використані як методичний посібник.

Список використаних джерел

1. *Закон України «Про інформацію» N 2657-XII від 2 жовтня 1992 року*
2. *Указ Президента України від 24 вересня 2001 року №891/2001 "Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних".*
3. *Концепція технічного захисту інформації в Україні, затверджена постановою Кабінету Міністрів України від 8 жовтня 1997 року, №1126.*
4. *Домарев В.В. Защита информации и безопасность компьютерных систем. – К.: ДиаСофт, 1999. – 480 с.*

УДК 004.7

Удовиченко А. В.
Харківський національний університет імені В. Н. Каразіна

Вибір методу аутентифікації у бездротових мережах

Аутентифікація - це процес перевірки автентичності чого-небудь. Термін найчастіше використовується в середовищі інформаційних технологій. Прикладом аутентифікації може бути порівняння пароля, введеного користувачем, з паролем, який збережений в базі даних сервера. Подібна перевірка може бути як односторонньою, так і взаємної - все залежить від способу захисту і політики безпеки сервісу.

В наш час безпека даних, як персональних так і зберігаємих, набуває першочергової уваги. Цифрові технології с кожним роком прогресують, але в такому прогресі яскраво виділяється один пункт – мінімізація компонент обчислювальних мереж. В наш час широко використовуються бездротові мережі, тому питання доступу до мережі порушником, а як наслідок і до даних, являє собою ще одну проблему, так звану, проблему вибору способу аутентифікації.

Проблеми які вирішує аутентифікація через Ethereum:

1. Користувач не зобов'язаний довіряти сайту, на який заходить, і хоче уникнути витоку персональної інформації.

2. Сайт хоче використовувати зовнішню систему аутентифікації, щоб уникнути зберігання призначених для користувача даних і пов'язаних з цим витрат на забезпечення безпеки.

3. Існуючі зовнішні системи, що надають сайтам можливість аутентифікації користувачів, несуть в собі небезпеку цензури. Всі облікові записи можуть бути заблоковані в будь-який момент без пояснення причин і іноді без можливості відновлення.

Загальний процес аутентифікації користувача з використанням EtherAuth виглядає так: Сайт (backend) звертається в смарт-контракт і отримує Ethereum-адреса користувача. Сайт (backend) генерує і запам'ятовує якесь повідомлення і просить користувача підписати це повідомлення за допомогою адреси authKey. Користувач, перебуваючи на сайті (frontend), підписує повідомлення за допомогою плагіна MetaMask і відправляє його в backend.Сайт (backend) перевіряє підпис, і якщо все в порядку, активує сесію користувача відповідно до своєї обраної логіки.

Безумовно, сьогодні мізерно мало користувачів використовують мережу Ethereum в порівнянні з числом користувачів Facebook. Однак популярність блокчейн-технологій зростає, і я вірю, що в доступному для огляду майбутньому таких користувачів буде ставати все більше і більше, а значить з'явиться можливість для використання децентралізованої аутентифікації в промислових системах.

Список використаних джерел

1. *Authentication Types for Wireless Devices. Електронний ресурс. Режим доступу – https://www.cisco.com/c/en/us/td/docs/routers/access/wireless/software/guide/SecurityAuthenticationTypes.html*
2. *Алексеев Н.А., Майборода О.В., Терновой М. Ю. Design of Wi-Fi Wireless Network as a Part of Corporate Network. Електронний ресурс. Режим доступу – http://www.its.kpi.ua/itm/ternovoy/Lists/publications/Attachments/94/Создание%20беспроводной%20сети%20WI-Fi%20как%20части%20корпоративной%20сети.pdf*

УДК 004.056.55

Федорко М. А., Маслова Н. О.
Донецький національний технічний університет

Застосування вітчизняних стандартів шифрування для захисту даних великих обсягів

Однією з основних проблем сучасності є стрімке зростання обсягів найрізноманітнішої інформації. Особливу роль в організації роботи з великими даними мають методи захисту інформації. Розповсюджені в даний час антивірусні засоби не призначені для забезпечення необхідного рівня безпеки таких даних, а стандарти з захисту великих даних на даний час ще не затверджено, тож проблема забезпечення безпеки Big Data є невирішеною та актуальною.

Метою роботи є дослідження сучасних алгоритмів шифрування та виявлення доцільності застосування вітчизняних стандартів при рішенні задач захисту та забезпечення конфіденційності та цілісності великих даних.

Найбільший внесок у розробку технологій захисту Big Data зроблено міжнародним альянсом Cloud Security Alliance (CSA), Національним інститутом стандартів і технологій США (NIST) та Агентством Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) [3-5]. Спеціалізовані рішення з захисту «великих даних» пропонують фірми IBM, Oracle, Cloudera, Forrester та ряд інших.

Основними напрямками захисту даних великих CSA вважають: захист обчислень в розподілених програмних системах; захист нереляційних баз даних; захист сховищ даних; процедури фільтрації і валідації даних; моніторинг безпеки у режимі online; забезпечення конфіденційності; криптографічний захист; гранульований контроль доступу; контроль походження даних (Data provenance).

Особливостями криптографічних підходів до обробки Big Data є відокремлена обробка інформації та метаданих, організація пошуку за допомогою булевих запитів на зашифрованих даних, порівняння даних без їх розшифрування, виявлення дублікатних даних в великих масивах на основі ключів [4] й інші.

Застосовується як відомі та розповсюджені алгоритми шифрування такі, як, наприклад, DES або AES, так і такі методи, як хешування паролів, наскрізне шифрування даних, пов'язане шифрування, шифрування на базі атрибутів (ABE), шифрування на базі ідентичності (IBE), конвергентне шифрування.

Необхідність застосування швидких криптографічних алгоритмів при роботі з Big Data та вимога мінімізувати ризики, пов'язані з застосуванням неузгоджених один з одним алгоритмів або програмних продуктів з невідомими прихованими функціями, вимагає звернути увагу на вітчизняні розробки.

Так, одним з сучасних вітчизняних алгоритмів шифрування є шифр Kalyna («Калина»), в основі якого лежить національний криптографічний стандарт України ДСТУ 7624:2014. Стандарт визначає структуру шифру та режими його роботи. Шифр є прикладом блочного симетричного перетворення і підтримує розмір блоку і довжину ключа шифрування 128, 256 і 512 біт.

Дослідження виконувалось на комп'ютерах під управлінням Windows - версій операційної системи. В процесі проведення експерименту застосовано персональні комп'ютери з характеристиками процесорів:

- Intel Core i7-7700HQ CPU @ 2.8Gz 2.8 GHz. 2-4 ядра. Кеш 1-го рівня (L1) - 256 КБ, 2-го рівня (L2) - 1024 КБ, 3-го рівня (L3) - 6144Кб.
- Intel Core i5-4200U CPU @ 2.3GHz 2.4 GHz, 2-4 ядра. Кеш 1-го рівня (L1) - 128КБ, 2-го рівня (L2) - 512 КБ, 3-го рівня (L3) - 3072Кб

- Intel Pentium® CPU N3700. Тактова частота 1600-2400 МГц. Кеш 1-го рівня (L1) - 224КБ, 2-го рівня (L2) - 2048 КБ, 3-го рівня (L3) – немає.

- Intel(R) Core(TM) i3-2310M CPU @ 2.10GHz 2 ядра. 3 MB SmartCache.

Розмір оперативної пам'яті у всіх випадках дорівнював 6Гб, включено 2 ядра, без прискорення. Криптографічні алгоритми, які досліджувалися для обрання найбільш ефективного варіанту: AES, Blowfish, IDEA, Camellia, Kalyna. Застосовані криптографічні бібліотеки Crypto API (C#), Cryptography (C++).

Проведені експерименти та результати.

Експеримент 1. Обрання швидкодіючого алгоритму.

Для виконання порівняння шифрів було розроблено програмне забезпечення, яке підтверджувало їх роботу і дозволяло заміряти час виконання криптографічних операцій.

Дослідження швидкодії алгоритмів (режим шифрування, розмір блоку 256, довжина повідомлення (10 304 байт = 82432 біт) кратна довжині блоків всіх алгоритмів).

Результати. Алгоритм AES показав найвищу швидкодію на всіх типах процесорів, що було задіяно в дослідженні.

Підтверджено, що в цілому, час виконання алгоритму «Калина» на тих самих пристроях має той же рівень швидкодії, що й стандартного AES – алгоритму з відповідною довжиною ключа.

Більш того, український шифр Kalyna продемонстрував ті ж тенденції зміни показників швидкодії, що й AES на блоках довжиною 128 та 256 бітів, а на сучасних типах процесорів шифр Kalyna випередив за швидкодією алгоритми IDEA і Camellia.

Відомо, що зараз Kalyna єдиний у світі стандарт блокового шифрування, що підтримує 512-бітові симетричні ключі. Можливість швидкої роботи з блоками даних значної довжини є перспективною при обробці даних великих обсягів.

Експеримент 2. Обрання технічних засобів (процесору) для роботи алгоритму.

В процесі досліджень доказано вплив архітектурних особливостей процесора на показники швидкодії алгоритму Kalyna. Експеримент проводився на означеному вище наборі пристроїв. На процесорі з кешем першого рівня L1 у 256КБ отримані найкращі результати на усіх трьох досліджених розмірах блоку - 128, 256, 512 біт (довжина ключа дорівнювала розміру блоку). Трохи нижча швидкодія виявилася для випадку, коли розмір кешу L1 дорівнював 128 КБ. Третя та четверта конфігурації обладнання доцільність застосування алгоритму Kalyna не показали.

Висновки. З оглядом на всі переваги вітчизняного алгоритму (нормальний, високий і надвисокий рівень стійкості, довжина блока і ключа 128, 256 і 512 бітів, односпрямована конструкція схеми розгортання ключів, циклове перетворення, стійкість до переборних атак та відомих методів аналізу), застосування шифру «Калина» для захисту великих даних на сучасних пристроях є перспективним.

Список використаних джерел

1. *Big Data Threat Landscape and Good Practice Guide. URL: https://www.enisa.europa.eu/publications/ bigdata-threat-landscape/at_download/fullReport*
2. *Big Data Security and Privacy Handbook: 100 Best Practices in Big Data Security and Privacy. Cloud Security Alliance: https://downloads.cloudsecurityalliance.org/assets/research/big-data/BigData_*
3. *NIST Special Publication 1500-1. NIST Big Data Interoperability Framework. URL: https://bigdatawg.nist.gov/_uploadfiles/NIST.SP.1500-1.pdf (дата звернення 15.07.2018).*
4. *Принципи побудови і основні властивості нового національного стандарту блокового шифрування України / Р. Олійников, І. Горбенко, О. Казимиров, В. Руженцев, Ю. Горбенко // Захист інформації, том 17, №2, квітень-червень 2015, С.142-157.*

УДК 004.056.5

Нікуліщев Г. І., Хвостенко А. І.
Запорізький національний технічний університет

Дослідження та аналіз сучасних методів та засобів захисту хмарних обчислень

У сфері ІТ набуває все більшого поширення концепція використання віддалених (хмарних) ресурсів, які можуть замовляти і отримувати користувачі на вимогу (за передплатою). Рішення дозволяє заощаджувати кошти, бо ресурси оплачуються по факту їх фактичного споживання. У разі необхідності клієнт може отримати додаткові ресурси, запускаючи віртуальні машини і / або додатки, розташовані в хмарі, або, навпаки, відмовитися від частини або від усіх ресурсів, коли необхідність в їх використанні зникла. Для роботи з хмарою користувачеві не потрібно дорогого обладнання, так як комп'ютер користувача фактично використовується в якості терміналу, а всі ресурсомісткі обчислення проводяться на комп'ютерах що входять в хмарну інфраструктуру.

У хмарних обчисленнях виділяють три основні моделі обслуговування: ПЗ як послуга (SaaS), платформа як послуга (PaaS) і інфраструктура як послуга (IaaS). Відрізняються вони ступенем контролю над ресурсами, що надається користувачеві.

Контроль і управління хмарами є проблемою безпеки. Немає гарантій, що всі ресурси хмари підраховані і в ній немає неконтрольованих віртуальних машин, не запущено зайвих процесів і не порушена взаємна конфігурація елементів хмари. Це високорівневий тип загроз, тому що він пов'язаний з керованістю хмарою, як єдиною інформаційною системою і для нього загальний захист потрібно будувати індивідуально. Для цього необхідно використовувати модель управління ризиками для хмарних інфраструктур.

Збільшення місткості носіїв інформації, зниження вартості зберігання 1 Мб інформації дозволило безмежно (принаймні так позиціонують себе більшість «хмар») збільшити обсяги інформації, що зберігається і знизити вартість обслуговування сховищ інформації, значно збільшивши обсяги даних.

Розвиток апаратного забезпечення сприяв не стільки швидкому зростанню хмарних технологій, а й доступності даної технології для малого бізнесу і індивідуальних осіб. Що стосується технічного прогресу, то значну роль в цьому зіграло створення багатоядерних процесорів і збільшення місткості накопичувачів інформації.

В даний час виділяють три основні категорії «хмар»: публічні, приватні та гібридні.

Публічна хмара - ІТ-інфраструктура що використовується одночасно безліччю компаній і сервісів. Користувачі подібних хмар не мають можливості управляти і обслуговувати хмару, всю відповідальність з цих питань покладено на власника даної хмари. Абонентом пропонованих сервісів може стати будь-яка компанія і індивідуальний користувач. Вони пропонують легкий і доступний за ціною спосіб розгортання веб-сайтів або бізнес-систем, з великими можливостями масштабування, які в інших рішеннях були б недоступні. Приклади: онлайн сервіси Amazon EC2 і Simple Storage Service (S3), Google Apps / Docs, Salesforce.com, Microsoft Office Web та OneDrive.

Приватна хмара - безпечна ІТ-інфраструктура, контрольована і експлуатована в інтересах однієї-єдиної організації. Організація може керувати приватною хмарою самостійно або доручити це завдання зовнішньому підряднику. Інфраструктура може розміщуватися або в приміщеннях замовника, або у зовнішнього оператора, або частково у замовника і частково у оператора. Ідеальний варіант приватної хмари - це хмара розгорнута на території організації, що обслуговується, і перебуває під

контролем її співробітників. Однак витрати на утримання і обслуговування подібної хмари не сильно відрізняються від витрат на власний центр обробки даних.

Гібридна хмара - IT-інфраструктура що використовує кращі якості публічної і приватної хмари, при вирішенні поставленого завдання. Часто такий тип хмар використовується, коли організація має сезонні періоди активності, іншими словами, як тільки внутрішня IT-інфраструктура не справляється з поточними завданнями, частина потужностей перекидається на публічну хмару (наприклад великі обсяги статистичної інформації, які в необробленому вигляді не являють цінності для підприємства), а також для надання доступу користувачам до ресурсів підприємства (до приватної хмари) через публічну хмару.

Центр обробки даних (ЦОД) являє собою сукупність серверів, розміщених на одному майданчику з метою підвищення ефективності і захищеності. Захист центрів обробки даних являє собою мережевий і фізичний захист, а також відмовостійкість і надійне електроживлення. В даний час на ринку представлений широкий спектр рішень для захисту серверів і ЦОД від різних загроз. Їх об'єднує орієнтованість на вузький спектр вирішуваних завдань. Однак спектр цих завдань піддався деякому розширенню внаслідок поступового витіснення класичних апаратних систем віртуальними платформами. До відомих типів загроз (мережеві атаки, уразливості в додатках операційних систем, шкідливе програмне забезпечення) додалися складності, пов'язані з контролем середовища (гіпервізора), трафіку між гостьовими машинами та розмежуванням прав доступу. Розширилися внутрішні питання і політики захисту ЦОД, вимоги зовнішніх регуляторів. Робота сучасних ЦОД в низці галузей вимагає закриття технічних питань, а також питань пов'язаних з їх безпекою. Фінансові інститути (банки, процесингові центри) підпорядковані певним стандартам, виконання яких закладено на рівні технічних рішень. Проникнення платформ віртуалізації досягло того рівня, коли практично всі компанії, що використовують ці системи, досить серйозно зайнялися питаннями посилення безпеки в них. Хоч буквально нещодавно інтерес був скоріше теоретичним.

В основі забезпечення фізичної безпеки лежить суворий контроль фізичного доступу до серверів і мережевої інфраструктури. На відміну від фізичної безпеки, мережева безпека в першу чергу являє собою побудову надійної моделі загроз, що включає в себе захист від вторгнень і міжмережевий екран. Використання міжмережевого екрану має на увазі роботу фільтра з метою розмежувати внутрішні мережі ЦОД на підмережі з різним рівнем довіри. Це можуть бути окремо сервери, доступні з Інтернету або сервери з внутрішніх мереж.

Сервери хмарних обчислень і локальні сервери використовують одні і ті ж операційні системи і додатки. Для хмарних систем загроза віддаленого злому або зараження шкідливим ПО висока. Ризик для віртуальних систем також високий. Паралельні віртуальні машини збільшують «поверхню що атакується». Система виявлення та запобігання вторгнень повинна бути здатна виявляти шкідливу активність на рівні віртуальних машин, незалежно від їх розташування в хмарному середовищі.

Список використаних джерел

1. *Откуда взялись «облака» и какими они бывают? [Електронный ресурс] Rusbase – Режим доступу: https://rb.ru/opinion/raznye-oblaka*
2. *Обеспечение безопасности данных при использовании облачных технологий [Електронный ресурс] Первая миля – Режим доступу: http://www.lastmile.su/journal/article/3823*
3. *Угрозы облачных вычислений и методы их защиты. [Електронный ресурс] Habrahabr – Режим доступу: https://www.lektorium.tv//lecture/13538*
4. *Облачные вычисления, краткий обзор или статья для начинающих. [Електронный ресурс] Habrahabr – Режим доступу: https://habr.com/post/111274*

УДК 621.396.2:004.0565
Хемішінець Є. В., Куцак С. В.
Запорізький національний технічний університет

Аналіз механізмів захисту даних в бездротових мережах

Серйозною проблемою для всіх бездротових мереж (а також і дротових) є безпека. Безпека тут так само важлива, як і для будь-якого користувача мережі Інтернет. Захищеність мережі зв'язку є складним питанням і вимагає постійної уваги. Величезної шкоди може бути завдано користувачеві через те, що він використовує випадкові хот-споти (hot-spot) або відкриті точки доступу вдома або в офісі і не використовує шифрування або VPN (virtual private network – віртуальна приватна мережа). Небезпечно це тим, що користувач вводить свої особисті або професійні дані, а мережа при цьому не захищена від стороннього втручання.

В даній роботі авторами проведених огляд сучасних механізмів захисту бездротових мереж від несанкціонованого доступу (НСД) на прикладі технологій LTE, WiMAX та Wi-Fi.

Архітектура мереж LTE (long term evolution), більш відома як 4G, сильно відрізняється від схеми, яка використовується в існуючих мережах 3G. Ця різниця породжує необхідність адаптувати і покращувати механізми забезпечення безпеки. Найбільш важливою вимогою до механізмів безпеки залишається гарантія принаймні того ж рівня безпеки, який вже існує в мережах стандарту 3G.

Існують чотири основні вимоги до механізмів безпеки технології LTE [1]:

- забезпечити як мінімум такий же рівень безпеки, як і в мережах типу 3G, не доставляючи незручності користувачам;
- забезпечити захист від Інтернет-атак;
- механізми безпеки для мереж LTE не повинні створювати перешкод для переходу зі стандарту 3G на стандарт LTE;
- забезпечити можливість подальшого використання програмно-апаратного модуля USIM (universal subscriber identity module, універсальна сім-карта).

Для закриття даних в мережах LTE використовується потокове шифрування методом накладення на відкриту інформацію псевдовипадкової послідовності (ПВП) за допомогою оператора XOR (виключне або). Ключовим моментом у схемі є той факт, що псевдовипадкова послідовність ніколи не повторюється. Алгоритми, що використовуються в мережах LTE, виробляють псевдовипадкову послідовність кінцевої довжини. Тому для захисту від колізій ключ, який використовується для генерації ПВП, регулярно змінюється, наприклад, при підключенні до мережі, в процесі передачі і т.д. У мережах LTE алгоритми шифрування та забезпечення комплексної безпеки основані на технології Snow 3G та стандарті AES (advanced encryption standard). Окрім цих двох алгоритмів, технологія 3GPP використовую два додаткових алгоритми таким чином, що навіть якщо один з алгоритмів буде зламаний, ті які залишаться повинні будуть забезпечити безпеку мережі LTE

Модель безпеки (trust model) мережі LTE дуже схожа на модель, запропоновану в рамках мереж UMTS. Її можна грубо описати як мережу, що складається з надійної опорної мережі (core network), а також сукупності інтерфейсів між базовими станціями, користувацькими пристроями та опорною мережею, які вразливі для атак.

Щоб звести до мінімуму схильність атакам базову станцію, вона має забезпечити безпечне середовище, яке підтримує виконання таких чутливих операцій, як шифрування і розшифрування користувачів даних, зберігання ключів. Крім того, переміщення конфіденційних даних повинні обмежуватися цим безпечним середовищем. Заходи протидії:

- перевірка цілісності пристрою;
- взаємна автентифікація базової станції оператора (видача сертифікатів);
- безпечні поновлення; механізм контролю доступу;
- синхронізація часу; фільтрація трафіку.

Навіть з розпочатими заходами безпеки, слід враховувати атаки на базові станції. Якщо атака успішна, то зловмисник може отримати повний контроль, включаючи доступ до всіх переданих даних, як від пристрою користувача, так і інформації, що передається до інших базових станцій.

Питання безпеки в мережах WiMAX, заснованих на стандарті IEEE 802.16, стоять дуже гостро в зв'язку з легкістю підключення до мережі.

Стандарт IEEE 802.16 визначає протокол PKM (privacy and key management protocol), протокол приватності і управління ключем.

У мережах WiMAX поняття захищеного зв'язку SA (security association) – це одностороннє з'єднання для забезпечення захищеної передачі даних між пристроями мережі [2].

SA бувають двох типів:

1. Data security association – захищений зв'язок для даних.
2. Authorization security association – захищений зв'язок для авторизації.

Захищений зв'язок для даних в свою чергу буває трьох типів: первинний або основний (primary SA); статичний (static SA); динамічний (dynamic SA).

Первинний захищений зв'язок встановлюється абонентською станцією на час процесу ініціалізації. Базова станція потім надає статичний захищений зв'язок. Що стосується динамічних захищених зв'язків, то вони встановлюються і ліквідовуються по мірі необхідності для сервісних потоків. Як статичний так і динамічний захищений зв'язок можуть бути одним для декількох абонентських станцій.

Абонентська станція і базова станція поділяють один захищений зв'язок для авторизації. Базова станція використовує захищений зв'язок для авторизації та для конфігурації захищеного зв'язку для даних.

У мережах WiMAX використовуються наступні протоколи автентифікації:

1) Extensible authentication protocol (EAP, розширюваний протокол автентифікації) – це протокол, що описує більш гнучку схему автентифікації в порівнянні з сертифікатами X.509. EAP-повідомлення кодуються прямо в кадри управління. У зв'язку з цим в протокол PKM були додані два нових повідомлення PKM EAP request (EAP-запит) і PKM EAP response (EAP-відповідь). Стандарт IEEE 802.16e не встановлює будь-який певний метод автентифікації EAP, ця область зараз активно досліджується.

2) Privacy and key management protocol (PKM protocol) – це протокол для отримання авторизації і ключів шифрування трафіку TEK (traffic encryption key).

Вразливості в стандарті IEEE 802.16:

1. Атаки фізичного рівня, такі як глушіння передачі сигналу, що призводить до відмови доступу або лавинний наплив кадрів (flooding), який має на меті виснажити батарею станції. Ефективних способів протистояти таким загрозам на сьогодні немає.

2. Самозвані базові станції, що пов'язані з відсутністю сертифіката базової станції. У стандарті проявляється явна несиметричність в питаннях автентифікації. Запропоноване рішення цієї проблеми – інфраструктура управління ключем в бездротовому середовищі (WKMI, wireless key management infrastructure), заснована на стандарті IEEE 802.11i. У цій інфраструктурі є взаємна автентифікація за допомогою сертифікатів X.509.

3. Вразливість, пов'язана з невипадковістю генерації базовою станцією ключів авторизації. Взаємна участь базової і абонентської станції, можливо, вирішила б цю проблему.

4. Можливість повторно використовувати ключі TEK, чий термін життя вже закінчився. Це пов'язано з дуже малим розміром поля EKS індексу ключа TEK. Так як максимальний час життя ключа авторизації 70 діб, тобто 100800 хвилин, а найменший час життя ключа TEK 30 хвилин, то необхідне число можливих ідентифікаторів ключа TEK - 3360. А це означає, що число необхідних біт для поля EKS - 12.

5. Ще одна проблема пов'язана з небезпекою використання шифрування DES. При досить великому часі життя ключа TEK і інтенсивному обміні повідомленнями, можливість злому шифру становить реальну загрозу безпеці. Ця проблема була усунена з введенням шифрування AES в поправці до стандарту IEEE 802.16e. Однак, велика кількість користувачів до цих пір має обладнання, що підтримує лише старий стандарт IEEE 802.16.

З метою захисту даних в мережах Wi-Fi застосовуються методи обмеження доступу, автентифікації і шифрування. Методи обмеження доступу є фільтрація MAC-адрес і використання режиму прихованого ідентифікатора SSID (service set identifier).

Фільтрацію можна здійснювати трьома способами [3]:

- точка доступу дозволяє отримати доступ станціям з будь-якою MAC-адресую;
- точка доступу дозволяє отримати доступ тільки станціям, чиї MAC-адреси знаходяться в довірчому списку;
- точка доступу забороняє доступ станціям, чиї MAC-адреси знаходяться в "чорному списку".

У мережах Wi-Fi передбачено два варіанти автентифікації:

1) відкрита автентифікація, коли робоча станція робить запит автентифікації, в якому присутня тільки MAC-адреса клієнта. Точка доступу відповідає або відмовою, або підтвердженням автентифікації. Рішення приймається на основі MAC-фільтрації, тобто по суті це захист на основі обмеження доступу, що небезпечно;

2) автентифікація з загальним ключем, при якому використовується статичний ключ шифрування алгоритму WEP (wired equivalent privacy).

У мережах Wi-Fi використовуються наступні методи шифрування:

- WEP – використовується симетричний потоковий шифр RC4 (Rivest cipher 4), який досить швидко функціонує. На сьогоднішній день WEP і RC4 не вважаються криптостійкими;
- TKIP (temporal key integrity protocol) – використовується більш криптостійкий шифр RC4. З урахуванням всіх доопрацювань і удосконалень TKIP також не вважається криптостійким;
- CKIP (Cisco key integrity protocol) – протокол для перевірки цілісності повідомлень;
- WPA (Wi-Fi protected access) – замість вразливого RC4, використовується криптостійкий алгоритм шифрування AES;
- WPA2 – в даному протоколі застосовується RSN (robust security network, мережа з підвищеною безпекою).

Список використаних джерел

1. *Наконечний В.С. Захист інформаційних ресурсів у мережах нового покоління LTE / В.С. Наконечний // Сучасний захист інформації. – 2016. – №4. – С. 10 – 15.*
2. *Безпека в мережах WiMAX [Електронний ресурс]: Матеріал з Вікіпедії 19.11.2018. – Режим доступу: https://uk.wikipedia.org/wiki/Безпека_в_мережах_WiMAX.*
3. *Публічний Wi-Fi: п'ять способів (спробувати) захистити себе [Електронний ресурс]: Радіо Свобода 07.08.2018. – Режим доступу: https://www.radiosvoboda.org/a/29415422.html.*

УДК 004.4

Целуйко В. В., Никодюк Д. В.
Київський національний університет будівництва і архітектури

Важливість використання SIEM в системах захисту банківської таємниці

Поняття SIEM (Security Information and Event Management) це процес, який об'єднує мережеву активність в єдиний адресний набір даних. Сам термін був придуманий Gartner в 2005 році, але з тих пір саме поняття і все, що до нього відноситься, зазнало чимало змін.

Принцип роботи SIEM, по суті, зводиться до циклічності набору дій. Система збирає відомості з різних джерел, аналізує дані в режимі реального часу, при необхідності робить превентивні заходи, систематизує бази даних, аналізує дії користувачів на основі результатів попереднього моніторингу, створює попередження та оповіщення про критичні події. Функціонування SIEM-системи забезпечують окремі компоненти. Агенти відповідають за збір інформації з джерел. Колекторні сервери узагальнюють відомості з джерел, сервер баз даних зберігає інформацію, сервер кореляції відповідає за моніторинг і аналіз відомостей.

Досить клопітно вручну переглядати логи з великої кількості джерел. До того ж, бувають ситуації, коли зовні нешкідливі події, отримані з різних джерел, в сукупності несуть в собі загрозу. Коли відбувається відправка листа з чутливими для компанії даними людиною, що має на це право, але на адресу, що знаходиться поза звичайним колом адрес, на які він відправляє. DLP система цього може не відловити, але SIEM, використовуючи накопичену статистику, на підставі цього вже згенерує інцидент. Інцидент стався - але співробітник, який допустив витік, всіляко відхрещується. SIEM здатна надати всю необхідну доказову базу, придатну як для внутрішніх розслідувань, так і для суду. Власне кажучи, це одне з її головних призначень. У момент створення інциденту також будуть сповіщені всі зацікавлені особи.

Періодично треба проводити аудити на відповідність яким-небудь стандартам. Це SIEM теж вміє. На даний момент - банківська сфера являється основним користувачем SIEM. Тому що: а) їм потрібно регулярно проводити аудити відповідності; б) банки працюють з чутливою інформацією, тому в разі виникнення інцидентів важливо знати, хто-коли-звідки допустив витік, було це зловмисне дію або випадкове і які були супутні фактори.

Оцінка SIEM за основними характеристиками забезпечує вибір рішення на попередньому етапі. Параметри «успішності» у різних замовників збігаються частково. Більш глибоке порівняння SIEM-систем враховує потреби і особливості IT-інфраструктури конкретної компанії, важливість параметрів і значимість функцій системи оцінюється індивідуально. Замовник самостійно формулює перелік критеріїв «успішного» рішення під час тестування. Специфічні параметри SIEM-системи будуть остаточно встановлені тільки в процесі повсякденної експлуатації. SIEM є покращеною систему виявлення шкідливої активності і різних системних аномалій. Робота SIEM дозволяє побачити більш повну картину активності мережі та подій безпеки. Коли звичайні засоби виявлення окремо не бачать атаки, але вона може бути виявлена при ретельному аналізі і кореляції інформації з різних джерел. Тому багато організацій розглядають використання SIEM-системи в якості додаткового і дуже важливого елемента захисту від цілеспрямованих атак.

Список використаних джерел

1. *Congresso Annuale AICA, Chapter: Security information and event management Models, Publisher: AICA, pp.7-16.*
2. *McAfee SIEM products [Електронний ресурс].—Режим доступу: https://www.mcafee.com/enterprise/ru-ru/products/siem-products.html.*

УДК 004.056.5

Чекурда О. М., Пономарьов О. А.
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут

Формування моделі загроз для інформації, що циркулює в телекомунікаційних системах військового призначення

Оцінювати та аналізувати захищеність об'єкту можна тоді, коли на об'єкті вже існує, встановлена функціонуюча система захисту. Аналіз полягає в оцінюванні надійності та дієздатності системи. Це завадостійкість, час відновлення системи, неперервність захисту. По іншому, це здатність системи захисту забезпечувати свої функції (забезпечувати захист інформації) в умовах виявлення каналу несанкціонованого доступу до інформації ,тобто в умовах відмови, та час, за який система усуває виявлений канал несанкціонованого доступу до інформації.

Для більшої ефективності система захисту буде проектуватись з самого початку. Тому що проектування комплексної системи захисту на базі діючої системи може викликати несумісність або конфлікти між окремими засобами захисту, а це призведе до виникнення додаткових каналів витоку інформації (КВІ) та каналів доступу до інформації (КДІ), разом з тими що вже існували в системі. Хоча чим довше функціонує система тим менше таких залишається.

У даному випадку під системою розуміється телекомунікаційна мережа військового призначення (ТМВП). Досвід враховано при проектуванні нової комплексної системи захисту інформації, до якої будуть встановлені високі вимоги виходячи із завадостійкості - це посилення засобів для підвищення надійності системи, а саме – зменшення часу відновлення системи при виявлені несанкціонованих КДІ та КВІ.

Можна констатувати, що загрози інформації розглядаються з точки зору їх будь-якої небажаної дії на будь-яку з цих властивостей і можливого їх порушення. З цієї точки зору в автоматизованих системах (АС) розрізняють наступні класи загроз інформації:

1) Порушення конфіденційності.

2) Порушення цілісності.

3) Порушення доступності або відмова в обслуговуванні.

4) Порушення спостережливості або керованості.

Аналіз загроз є одним з найбільш важливих питань при побудові захищених ТМВП. Такий аналіз має на меті виявити можливі загрози інформації, а також показати, з якого боку і в якій точці АС слід чекати атаки. Загрози можуть реалізуватися внаслідок багатьох причин, серед яких: кількісна, якісна недостатність, відмови елементів системи, збої елементів ТМВП, помилки елементів мережі, стихійні лиха, зловмисні дії, побічні явища.

Джерелами наведених причин порушення безпеки можуть бути:

а) особи, що мають будь-яке відношення до функціонування мережі;

б) технічні засоби;

в) моделі, алгоритми, програмне забезпечення (ПЗ);

г) технологія функціонування – сукупність засобів, прийомів, правил, заходів і погоджень, що використовуються в процесі обробки інформації;

д) зовнішнє середовище – сукупність елементів, що не входять до складу ТМВП, але можуть впливати на захищеність інформації в мережі.

Отримані формальні визначення загроз можна використати для дослідження політики безпеки та захищеності ТМВП, а також дослідження профілів захищеності в ТМ, що, в свою чергу, дає можливість для розробки нових і вдосконалення існуючих профілів.

УДК 004.056

Черняк Т. О., Глушко В. В.
Донецький національний технічний університет

Вдосконалення методів безпечного хешування при забезпеченні автентичності та цілісності даних у автоматизованих банківських системах

Високорентабельна економіка у процесі розвитку потребує впровадження ультрасучасної системи обігу грошей, а також експлуатації ефективних платіжних інструментів. Обсяги даних, які оброблюються у сучасних внутрішніх платіжних системах (ВПС), постійно зростають, з'являються нові електронні послуги, стрімко розвивається обчислювальна техніка – все це потребує збільшення показників безпеки даних у ВПС.

Актуальність теми зумовлена необхідністю створення теоретичної рекомендації по використанню методів ключового хешування, що забезпечують цілісність та автентичність інформації у всесвітніх платіжних системах комерційних банків. Нажаль, зараз не існує механізмів та концепцій, які б гарантували фінансову безпеку національної платіжної системи в цілому та банківської діяльності окремо, щоб при цьому ще були науково обґрунтовані.

Постійний розвиток ринкової економіки потребує належної платіжної системи, яка дозволить проводити розрахунки, що виповідатимуть світовим загальноприйнятим стандартам: де на першому находяться безпека, надійність та час проведення платежів. Національна платіжна система є складною та багаторівневою системою із централізованим керуванням. Саме це забезпечує надійний і важливий у стратегічному плані канал, через який фінансові транзакції проводяться.

НПС – це багаторівнева складна система управління критичного застосування або СУКЗ, де передача даних потребує постійного контролю над безпекою, при цьому це повинно здійснюватися на кожному рівні обов'язково. Підсистема криптографічної безпеки даних – це одна з найважливіших частин у складі ВПС, реалізація базується на відповідних механізмах та протоколах.

Питання безпеки ВПС та мереж зв'язку банківської й фінансово-кредитних сфер можна без перебільшення віднести до національного рівня. Методи обробки, зберігання та передачі даних, які використовувалися у інформаційних системах останні роки, самі по собі були факторами появи загроз. Вони пов'язані з ймовірністю повної втрати або спотворення чи втрати конфіденційності інформації, яка направлена чи належить кінцевому користувачеві.

Загроза інформаційної безпеки в інформаційних системах – це можливість втручання у дані, які обробляються автоматизованою системою, що може призвести до копіювання даних чи їх спотворення або знищення, блокування доступу, в тому числі втручання у дію роботу компонентів автоматичної системи.

Класифікація загроз інформаційної безпеки відбувається за наступними критеріями: компоненти інформаційних систем (ІС), на які направлені загрози (програмне забезпечення, дані, інфраструктура та підтримуюче обладнання); мета впливу; зовнішнє чи внутрішнє джерело загрози; спосіб реалізації (техногенний чи природній характер). [1]

Мета впливу загроз ділиться на три основні типи: загроза цілісності, доступності та конфіденційності.

На даний момент оцінка стану інформаційної безпеки вказує на те, що її обсяг та якісні характеристики не відповідають сучасним потребам. Тому визначення основних

реальних та потенційних загроз, що негативно будуть впливати на процес стабільного урегулювання інформаційної безпеки є важливим завданням.

Якщо проаналізувати загальну класифікація загроз інформаційної безпеки на ВПС, то можна зробити висновки, що є джерела ненавмисних загроз ІС:

- поламка складових частин обладнання;
- збій у роботі програмного забезпечення;
- неправильні дії з боку користувачів та персоналу;
- ненавмисні помилки у програмно-апаратному забезпеченні.

Звичайно, такі загрози наносять суттєвий збиток, але навмисні загрози з точки зору функціювання є більш значними, бо сама їх мета – це завдання збитків ІС або її користувачам. Такі загрози реалізуються шляхом довготривалої та масової атаки за допомогою вірусів чи несанкціонованих запитів. Атаки матимуть наступні наслідки: повна чи часткова втрата інформації, підтасовка даних, доступ до інформації отримують сторонні особи. Не важко уявити до чого можуть привести події такого роду. Тому протидія загрозам інформаційної безпеки, які вже були розглянуті вище, є пріоритетною задачею засобів захисту комп'ютерних систем та мереж. Послуги інформаційної виступають в якості засобів захисту ІС.

Рисунок 1 – Види послуг безпеки

За рахунок основних досягнень у сфері ІТ та комунікацій ВПС постійно розвивають да вдосконалюють свої функції. А саме послуги оплати насамперед через банкомати, термінали та віддалених користувачів; продаж товарів через онлайн-магазини тощо.

Характеристики обчислювальної техніки постійно модернізуються, а її продуктивність постійно зростає – це підтверджує закон Мура. Таким чином, інформаційні системи постійно вразливі перед різноманітними атаками та загрозами.

Висновоки. На даний момент оцінка стану інформаційної безпеки вказує на те, що її обсяг та якісні характеристики не відповідають сучасним потребам. Тому визначення основних реальних та потенційних загроз, що негативно будуть впливати на процес стабільного урегулювання інформаційної безпеки є важливим завданням.

Список використаних джерел

1. *Соколов А. В. Защита от компьютерного терроризма. [Текст] / Соколов А. В., О. М. Степанюк. – БХВ-Петербург Арлит, 2002. – 496 с.*
2. *Конеев И. Р. Информационная безопасность предприятия [Текст] / И. Р. Конеев, А. В. Беляев. – БХВ-Петербург, 2003. – 752 с.*

УДК 004.056

Ярош І. В., Черняк Т. О.
Донецький національний технічний університет

Розробка системи виявлення вторгнень у web-додатки

Згідно зі звітом корпорації Mitre, понад чверть вразливостей припадає на проблеми безпеки web-додатків. На відміну від прикладного програмного забезпечення, операційних систем і систем управління базами даних, які використовуються в корпоративній мережі, web-додатки найбільш поширено створюються всередині компанії і не проходять такий ретельний контроль якості, як широко поширені програмні продукти. З іншого боку, проблеми в web-додатках набагато легше виявити та використовувати.

Основна проблема забезпечення безпеки web-додатку полягає в тому, що не існує можливості обмежити доступ до нього для потенційних зловмисників. Вимоги до бізнесу в сучасний час призводять до необхідності створення багатофункціональних web-додатків, що, відповідно, негативно позначається на безпеці, тому що чим складніше додаток, тим більша ймовірність наявності в ньому помилки, яка потенційно може стати в подальшому вразливістю.

Слабка захищеність і широка поширеність web-додатків робить їх привабливими цілями для зломщиків. Існуючі системи забезпечення безпеки часто неефективні при захисті додатків даного класу [1].

Програмне забезпечення, що використовується в інфраструктурі web-додатку (web-сервер, СУБД та інше), зазвичай створюється компетентними в питаннях безпеки фахівцями та є добре захищеним. Але web-додатки в ряді випадків розробляються фахівцями, які не володіють аналогічними навичками або погано розуміють значимість захищеності системи [2]. Результатом такої розробки стає слабо захищений web-додаток, що доступний кожному користувачу мережі Інтернет.

Метою роботи є дослідження типових вразливостей в сценаріях web-сторінок, написаних з використанням мови PHP, і розробка системи виявлення вторгнень у web-додатки, яка є одним зі складових елементів, необхідних для створення якісного рівня захисту.

Дана система виявлення вторгнень у web-додатки розроблена на мові PHP. Розроблена система призначена для захисту web-додатків від проведення реальних атак або вторгнень. Дана система виявлення вторгнень є вбудованою і її робота здійснюється паралельно з роботою web-додатку. Вхідними точками є методи GET і POST протоколу HTTP, а також HTTP Cookie.

Система виявлення вторгнеь (СВВ) – це програмне забезпечення, призначене для забезпечення додаткового захисту web-додатків від спроб зловмисника здійснити атаку, намагаючись знайти та експлуатувати уразливість. Дане програмне забезпечення є вбудованим і підключається у вигляді додаткового модуля до конкретного web-додатку. Крім того, СВВ також складається з модулів, які в сукупності складають систему виявлення вторгнень. До складу СВВ входить компоненти – модулі, що описані далі.

Модуль логіки СВВ – це модуль, що здійснює аналіз і фільтрацію даних, які передаються web-додатком. Даний модуль контролює вхідні дані на предмет безпеки та, в разі виявлення події спроби потенційного вторгнення, передає управління Модулю формування звіту.

Модуль формування звіту – це модуль, що здійснює процес створення об'єкта зареєстрованої СВВ події про потенційну спробу вчинити атаку. Сформований об'єкт

події поміщається в масив, що формує загальний звіт, який потім передається в Модуль реєстрації подій.

Модуль реєстрації подій – це модуль, що отримує сформований звіт, який містить всі зареєстровані події і здійснює завантаження даних про всі події в таблицю «intrusions» наявної бази даних.

Модуль управління СВВ – це консоль управління. що представляє собою панель з web-інтерфейсом. Даний модуль призначений для адміністраторів і дозволяє здійснювати моніторинг зареєстрованих подій, налаштування СВВ і додавання нових сигнатур.

Загальний алгоритм роботи СВВ у web-додатки складається з наступних етапів.

Етап 1. Введення даних (передача параметрів). Даний етап є початковим і має на увазі передачу параметрів, яка реалізується логікою web-додатків, або введення даних користувачем для обробки web-додатками. Слід зазначити, що даний етап може бути перерваний, в разі, якщо користувач ввів дані, послав сигнал на їх відправку (зазвичай, натисканням кнопки у web-формі) і потім негайно скасував дію. В цьому випадку обробка вхідних даних не здійснюється ні системою, ні web-додатками.

Етап 2. Формування масиву вхідних даних. Передача вхідних даних web-додатків може здійснюватися кількома способами. Як було зазначено раніше, мережева взаємодія здійснюється за допомогою протоколу HTTP, який має методи POST і GET. Їм відповідають глобальні масиви $_POST і $_GET мови PHP. Крім того, для здійснення механізму Cookie існує масив $_COOKIE. На даному етапі відбувається збір вхідних даних з усіх глобальних масивів і формування загального масиву даних, для зручності здійснення процесу обробки.

Етап 3. Пошук збігів з сигнатурою. На даному етапі відбувається перевірка відповідності кожного параметра з масиву даних з сигнатурами на встановлення відповідності. При виявленні збігу відбувається реєстрація виникнення події; якщо подія не встановлена, то проводиться аналіз наступного параметра.

Етап 4. Наявність збігів з сигнатурою. При виявленні збігу з сигнатурою відбувається приведення значення параметра, що співпав, шляхом фільтрації до безпечного виду. Це здійснюється з використанням спеціальних PHP-функцій (strip_tags (string $str), mysql_real_escape_string (string $unescaped_string) і ін.). Крім цього інформація про цю подію реєструється в СВВ для подальшого аналізу адміністратором системи.

Етап 5. Передача управління web-додатками. Після здійснення аналізу всі вхідні параметри передаються для обробки логікою web-додатків. До даного етапу web-додатки перебувають в стані так званого «очікування», але, так як робота СВВ відбувається з високою швидкістю, то в залежності від кількості параметрів час не перевищує декілька секунд.

Висновки. На підставі аналізу найбільш популярних web-вразливостей було встановлено, що головною причиною виникнення «проломів» в безпеці є недостатня або відсутня фільтрація переданих даних web-додатками. Для забезпечення більш високого та якісного рівня безпеки web-додатків використовуються системи виявлення атак (вторгнень).

Список використаних джерел

1. *Олифер В. А. Компьютерные сети. Принципы, технологии, протоколы. Учебное пособие для вузов [Текст] / В.А. Олифер, Н.А. Олифер. – Питер, 2011. – 944 с.*
2. *Суэринг, С. PHP и MySQL. Библия программиста. Учебное пособие [Текст] / С. Суэринг, Т.Конверс, Д.Парк. – Диалектика, 2010. – 912 с.*

Наукове видання

КОМП'ЮТЕРНА ІНЖЕНЕРІЯ І КІБЕРБЕЗПЕКА: ДОСЯГНЕННЯ ТА ІННОВАЦІЇ

Матеріали Всеукраїнської науково-практичної конференції здобувачів вищої освіти й молодих учених

(м. Кропивницький, 27-29 листопада 2018 р.)

Технічний редактор *О. П. Дóренський*

Підписано до друку 29.11.2018. Формат 60x84/8. Папір офсетний.
Надруковано на ризографі. Тираж 245 прим.