experiments were conducted on the program model, the results of which show the adequacy of the model's response to changes in the parameters of individual nodes and network structure.

The article presents the results of experiments: the dependence of the rate of propagation on the density of links, the comparison of selected behavioral strategies, the evaluation of the effectiveness of strategies, depending on the number of nodes-generator links.

software model, information influence, methods of network generation, models of distribution of information in the network, behavioral strategies

Одержано (Received) 07.06.2016

УДК 004.056.5

В.Д. Хох, асп.
Центральноукраїнський національний технічний університет, м. Кропивницький, Україна, E-mail: vd.khokh@gmail.com

Автоматизована система проведення аудиту інформаційної безпеки комп'ютерних систем та мереж

У статті розглядається розроблювана в рамках дисертаційного дослідження система для проведення аудиту інформаційної безпеки комп'ютерних систем та мереж. Пропонується вирішення проблем, що виникли під час розробки системи та розглянуто механізми, що було розроблено та інтегровано у розроблювану систему.

інформаційна безпека, аудит, нечітка логіка, експертні системи, автоматизація

В.Д. Хох, асп.
Центральноукраинский национальный технический университет, г. Кропивницкий, Украина

Автоматизированная система проведения аудита информационной безопасности компьютерных систем и сетей

В статье рассматривается разрабатываемая в рамках диссертационного исследования система для проведения аудита информационной безопасности компьютерных систем и сетей. Предлагается решение проблем, возникших при разработке системы и рассмотрены механизмы, которые были разработаны и интегрированы в разрабатываемую систему.

информационная безопасность, аудит, нечеткая логика, экспертные системы, автоматизация

Постановка проблеми. Ситуація, що склалася в нашій країні з початком агресії Російської Федерації, загострює проблему захисту інформаційних систем, оскільки у РФ є великий досвід у проведені різноманітних операцій із залученням спеціалістів з комп'ютерної та інформаційної безпеки. Наприклад, під час загострення відносин Естонії та РФ у 2007 році на фоні конфлікту, спричиненого переносом пам'ятника «Бронзовий Солдат», було виведено з ладу багато урядових сайтів Естонії, а також деяких банківських установ. Експерти, у тому числі і з ООН відмітили, що це була найбільш організована та добре спланована кібератака [1]. І хоча доказів того, що атака була організована саме РФ, Естонія не змогла надати, згодом, того ж року депутат Державної думи Росії Сергій Марков визнав на прес-конференції, що один з його помічників є організатором цієї атаки [1]. Вже через рік РФ продемонструвала

ефективність координованих кібератак під час військового конфлікту з Грузією 1 серпня 2008 року. Під час цього конфлікту урядові сайти, і не лише, були не тільки виведені з ладу, а й за допомогою них поширювалася спотворена, небезпечна інформація, метою якої була з однієї сторони деморалізація населення, з іншої – консолідація сепаратистів. Воєнні дії, що мали місце під час Російсько-Грузинської війни у кіберпросторі, було названо початком так званої «iWar» [2]. Під час анексії Криму Росією, інформаційна війна також мала своє продовження. Вразливістю, що була використана РФ, є історичні або інші умови, що спричинили глибоке проникнення інформаційного поля однієї країни до іншої. Завдяки цьому у РФ було підконтрольне інформаційне поле, яке було використано. І завдяки дезінформації та пропаганді, було досягнуто збудження сепаратиських настроїв, що дало змогу ввести війська та анексувати півострів. На сході нашої країни проникнення інформаційного простору РФ було не таким сильним, а регіони були не так сильно ізольовані від всієї країни, тому сепаратиські настрої збудити вдалося, але не так ефективно, як на півострові Крим. Але РФ знає та розуміє ефективність та важливість проведення подальшої інформаційної війни проти України, тому поглиблює свій інформаційний вплив на тимчасово окупованих територіях, а також продовжує проводити операції по викраденню особистої інформації деяких громадян України. Прикладом поглиблення контролю за особистою інформацією людей, у тому числі і іноземних громадян, інформаційне поле країн, яких історично перетинається з інформаційним полем РФ, є постанова уряду РФ від 8 квітня 2015 року №327 «Про затвердження правил контролю за діяльністю організаторів розповсюдження інформації в Інтернеті». Ця постанова надає «Роскомнадзору» право доступу до особистої переписки та особистих даних користувача, що є в розпорядженні соціальної мережі або будь-якого дата-центру, що працює на території РФ та за законами РФ. На сьогоднішній день агресія продовжується і основ для того щоб можливо було казати про її завершення – немає. Тому важливо щоб системи управління інформаційною безпекою (СУІБ) були готові адекватно реагувати на можливі атаки з боку агресора. Підтримання актуального стану СУІБ можливо у разі регулярного або поточного аудіювання її систем.

Виходячи з вище сказаного, виникає необхідність у розробці систем, що могли б надавати інформацію про поточний стан захищеності системи та надавали рекомендації щодо усунення тих чи інших вразливостей, знайдених у досліджуваній системі або мережі.

Аналіз останніх досліджень і публікацій. Було розглянуто існуючі на сьогоднішній день системи для проведення аудиту інформаційної безпеки, з яких, слід виділити систему SaaAS [3]. Ідея системи SaaAS полягає у наданні аудиту інформаційної безпеки як сервісу, основна відмінність від розроблюваної системи є необхідність встановлення додаткового агенту на стороні системи що підлягає аудиту. Також до увагу було взято систему що описано у роботі [4], дана система також використовує нечітку логіку для вирішення поставлених задач у галузі інформаційної безпеки, але використовує обмежений логічний апарат на відміну від розроблюваної системи.

Розроблювана система використовує парадигму безперервного аудиту, що описано у роботі [5]. Перед тим як використовувати дану парадигму аудиту як, основу для системи було проведено аналіз та порівняння у статті [6].

Процес аудиту СУІБ згідно керівництва по тестуванню та оцінці інформаційної безпеки [7] передбачає проведення ряду заходів по тестуванню, експертизі та інтерв'юванню. Ці методи націлені на збір так званих свідоцтв аудиту – термін, що використовується у міжнародному стандарті ISO 19011:2011 і визначається як

протоколи, факти або інша інформація, що стосується критеріїв аудиту, і найголовніше – може бути перевірена [7].

Постановка завдання. Метою даної роботи є розробка програмної системи тестування СУІБ на основі експертної системи з використанням продукційного представлення знань та методів нечіткої логіки.

Виклад основного матеріалу. Архітектурно система розділяється на три частини. Перша частина – це контрольний центр системи, з яким безпосередньо працює оператор, аудитор. Друга частина – це база знань, яка представлена у системі як SQL-сервер. Третя частина – це пристрій або вузол – провайдер інструментів аудиту, або атакуючий модуль. Розглянемо частини системи окремо.

Контрольний центр є основним і контролює всі інші вузли, з ним безпосередньо працює персонал. Контрольний центр повинен бути з'єднаний з сервером баз даних, на якому знаходиться база знань, а також повинно бути надане з'єднання з модулем – провайдером інструментів. Для з'єднання з SQL-сервером використовується MDAC (Microsoft Data Access Components) компоненти, вони дозволяють отримати уніфіковані засоби доступу до різноманітних реляційних та не реляційних джерел даних, термін MDAC є загальним для усіх розроблених компанією Microsoft технологій пов'язаних з базами даних. З'єднання з модулем – провайдером інструментів відбувається за протоколом SSH. SSH – це мереживий протокол рівня застосунків, що дозволяє проводити віддалене управління комп'ютером і тунелювання TCP-з'єднань, наприклад, для передачі файлів. На відміну від схожих по функціоналу протоколів – Telnet та rlogin, SSH шифрує весь трафік, а відтак і паролі передані за його допомогою, до того ж протокол є алгоритмонезалежним, що дозволяє погодити його використання з політикою безпеки організації або законодавчими нормами в рамках яких функціонує організація.

База знань у системі представлена реляційною базою даних SQL, яка знаходиться на сервері Microsoft SQL server 2014. Цей тип бази даних було обрано через поширеність, легкість у використанні, доступність зручних інструментів для використання. Сервер, на якому було розгорнуто базу знань, було обрано через відносні захищеність та стабільність роботи. Сервер підтримує можливість шифрування трафіка за допомогою SSL і підтримує автентифікацію за допомогою протоколу Kerberos.

База знань (база даних) має одну таблицю з шістьма стовпчиками:

– id – унікальний ідентифікатор для кожної продукції, обчислювальний ключовий стовпчик, що забезпечує зручність навігації;

– nameSpace – стовпчик, що визначає область застосування продукції, на кшталт простору імен у Сі-подібних мовах програмування;

– useRule – правило застосування ядра продукції, визначає контекст використання продукції, тобто ті факти, які важливі при використанні продукції, а також дозволяє розрахувати релевантність продукції у поточному стані фактологічної бази;

– logicBlock – логічний блок продукції або її ядро. Являє собою логічний вираз над фактами, які можуть бути включені в фактологічну базу і можуть бути визначені в ній, якщо їх немає в фактологічній базі, або вони не визначенні – такий факт приймає значення false з вагою «1» – максимальна вага;

– prodData – дані пов'язані з продукцією. Це дані, які будуть використанні у разі, якщо ядро продукції задовольнить умови експертної системи. У типовому вигляді дані у стовпчику prodData зберігаються команди терміналу, які будуть надіслані SSH серверу для подальшого виконання на провайдері інструментів аудиту;

– metaData – стовпчик, що не використовується самою експертною системою, але слугує для додавання коментарів від експерта, що працює з базою знань.

Першочергова задача провайдеру інструментів аудиту – прийняти інструкції від контрольного центру, і оскільки, контрольний центр буде намагатися зв'язатися з ним за допомогою SSH-протоколу – провайдер повинен бути здатним розгорнути SSH сервер та прийняти з'єднання. Другою задачею провайдера – є здатність виконати ті інструкції, що були згенеровані та надіслані йому експертною системою, тому наступною вимогою до провайдера є можливість запуску на ньому того програмного забезпечення, з яким готова працювати база знань, а відтак, і експертна система в цілому. Додаткові вимоги до провайдера можуть висувати аудитори, оскільки у контрольному центрі є можливість відкрити термінал і працювати з провайдером напряму, наприклад, для збору додаткових відомостей про ціль аудиту, аудитори можуть висунути свої вимоги до програмного забезпечення встановленого на провайдері.

Вся робота системи поділяється на два великі розділи:

– збір інформації: визначення області інтересів, побудова певного стану фактологічної бази;

– розробка рішення експертною системою: виконання рішення експертної системи.

На першому етапі користувач-аудитор щільно співпрацює з системою, намагаючись якомога чіткіше визначити область своїх інтересів та надати якомога точнішу і найважливішу інформацію для експертної системи.

Другий етап – це розробка рішення експертною системою. Результатом цього етапу роботи є набір інструкцій, які будуть надіслані провайдеру інструментів за допомогою SSH-протоколу. Вхідними даними на цьому етапі є фактологічна база з визначеними фактами.

Загальну функціональну схему системи яка працює з провайдером інструментів на якому для збору інформації використовуються засоби nmap та Metasploit framework, також Metasploit framework використовується для реалізації атак, зображено на рис.1.

Система розробляється таким чином, щоб виробляти рішення, щільно співпрацюючи з користувачем. Система дозволяє охопити кількість фактів, яку або не може охопити людина, або це стає незручно. Система ж не забороняє включати у розрахунок факти, які цікавлять користувача – навпаки, вона їх доповнює, у тому разі, коли включення одного користувацького факту не вплине на роботу системи, оскільки пов'язані з ним дані знаходяться поза межами поточного стану фактологічної бази, або продукції, які активно використовують цей факт, знаходяться за межами «інтересів» експертної системи при тих даних, які в неї зараз є. Ця можливість реалізована за допомогою механізму просторів імен.

Простір імен. Механізм простору імен, розроблюваної системи покликаний з одного боку – надати більше простору для творчого пошуку вирішення проблем користувачем, з іншого – збалансувати кількість продукцій, що використовуються у процесі прийняття рішення. Схему роботи механізму простору імен наведено у рис. 2. Як видно зі схеми, у тому разі, якщо продукцією буде задіяно факт, що належить до іншого простору імен, то система це визначить, віднайде факт і включить простір імен до розрахунків. Наприклад, «Продукція 1» на рисунку використовує факти, що належать до різних просторів імен, або «Продукція 3» використовує факти з усіх просторів імен, хоча сама належить до «Простору імен 2». Якщо в фактологічну базу буде додано факт, який належить до ще не включеного простору імен, його буде включено, або якщо продукція буде використовувати факти, що не належать до

включених просторів імен фактологічної бази – його буде включено. Простір імен в системі дозволяє значно зменшити кількість проходжень по базі знань, оскільки факти та продукції у просторі імен семантично з'єднані, наприклад, простір імен для певної операційної системи. Підключивши простір імен існує велика ймовірність того, що перший факт або продукція, яка слугувала приводом підключення – буде не остання.

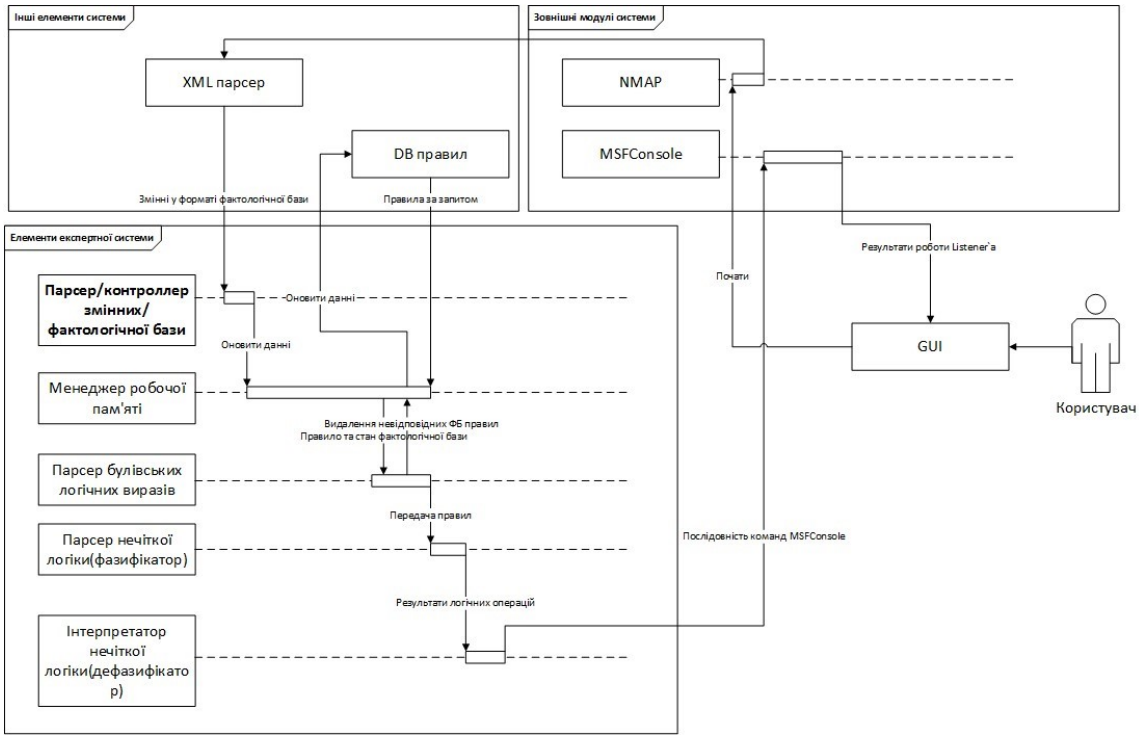

Рисунок 1 – Загальна функціональна схема системи

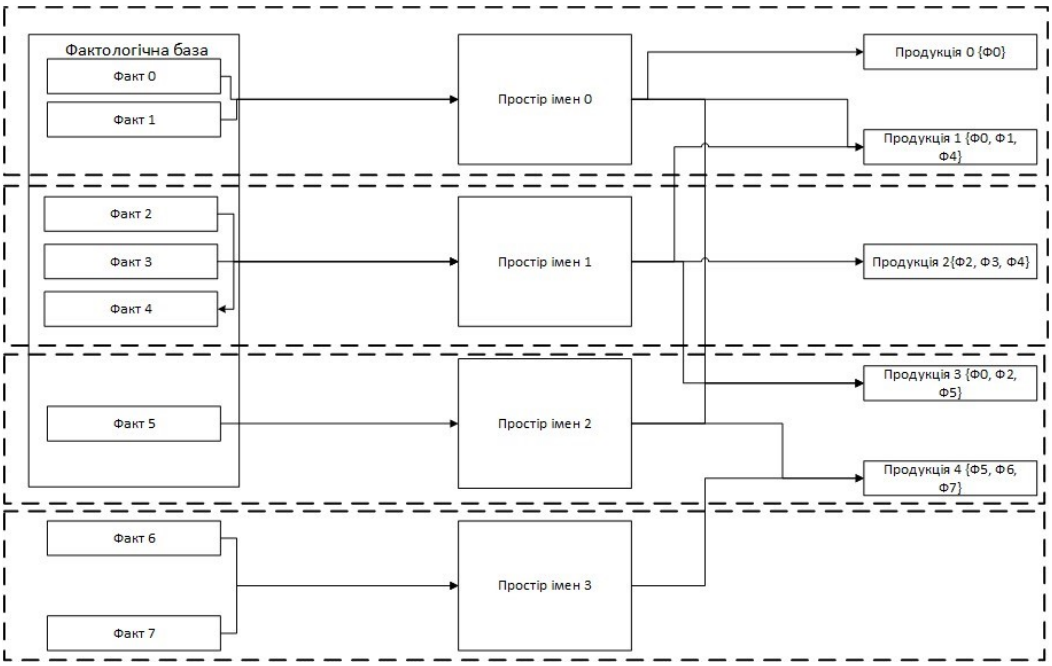

Рисунок 2 – Схема роботи механізму простору імен у системі

Один з механізмів, який дає змогу автоматизувати процес керування простором імен і зробити його більш точнішим – це механізм фактів «трігерів». Факт-трігер – це такий факт, значення якого явно вказує на певний простір імен, наприклад, якщо системі доведеться проводити аудит мережі, в якій усі пристрої використовують одну й ту ж саму операційну систему і її версію. Такий механізм значно зменшить кількість проходів по базі знань. До того ж, якщо у поточній версії фактологічної бази немає фактів з певного простору імен, а відтак усі продукції з такого простору імен будуть виключені, все ж їх варто розглянути – користувач може додати такий факт і визначити його значення як назву простору імен, яке його цікавить.

Структура продукції в рамках даної системи відповідає структурі рядку бази знань, яка згадувалась вище, у цій статті. Структурою продукції передбачені два поля з правилом – використання продукції та безпосередньо ядром продукції. Данні у цих двох блоках представляються у вигляді змінних. В рамках системи визначено три типи даних: діапазон цілих чисел, діапазон з плаваючою точкою та строкові множини. Варто зауважити, що, хоча у системі типи даних визначено по різному – для фактологічної бази та для тих, що використовуються у тілі продукції, це необхідно для внутрішніх потреб системи. Розглянемо спільні параметри для типів даних у фактологічній базі та типів даних у тілі продукції:

– NameSpace – параметр вказує на простір імен, якому належить факт;
– Name – ім’я факту у фактологічній базі;
– CurrentValue – поточне значення факту у фактологічній базі;
– Weight – визначає поточну «вагу» змінної. Використовується для зберігання ваги у фактологічній базі, а у тілі продукції використовується для тимчасового зберігання ваги під час обробки даних. Цей параметр буде використано для процесів фазифікації та дефазифікації даних.

Для типів даних, які зберігаються у фактологічній базі характерними є параметри:

– CurrentValue – зберігає поточне значення змінної у фактологічній базі, в процесі роботи з системою може бути змінено як системою так і користувачем-аудитором;
– UseAsTrigger – параметр приймає значення true або false. Приймає значення істини у тому разі, якщо значення змінної визначає ім’я простору імен, яке треба додати до фактологічної бази;
– isInLim – параметр приймає значення true або false. Приймає значення істини. Якщо значення факту знаходиться в діапазоні змінної, яка визначена серед продукцій, які відібрано для можливого застосування.

Характерними параметрами для типів даних, що визначаються у тілі продукції є:

Для чисел цілих та з плаваючою точкою:

– Min – визначає мінімальне значення діапазону;
– Max – визначає максимальне значення діапазону.

Для рядкових даних – строкових множин:

– StringSet – масив рядків, що вказують на певне значення факту;
– UseSepWeight – параметр приймає значення true або false. Приймає значення true у разі, якщо користувач-експерт хоче самостійно визначити вагу кожного рядка у множині рядків і відповідно – вказати символ, яким буде розділяти значення ваги та рядок, яка вказує на значення факту;
– SepWeightChar – символ, що буде використано для розділення значення ваги та рядка, який вказує на значення факту.

Висновки. На даний момент були розроблені дві версії системи, обидві можна вважати ранніми альфа-версіями. В першій версії була зосереджена увага на взаємодії вузлів системи та основних механізмах експертної системи. Перша версія системи була ескізним проектом, в якому була зосереджена увага на визначенні способів та алгоритмів взаємозв'язку всіх модулів та механізмів. Ця версія була необхідна для того, щоб можливо було зрозуміти, взагалі можливість функціонування системи у такому форматі. У другій версії структура системи була перероблена таким чином, щоб система стала більш гнучкою до масштабування.

Поточні версії програми демонструють адекватну відповідь на тестові дані. Однак, стала очевидною проблема надмірної гнучкості експертної системи, що робить дуже складним процес заповнення та редагування бази знань.

Список літератури

1. 2007 cyberattacks on Estonia [Електронний ресурс] // en.wikipedia.org. – 2017. – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia..
2. Райан Д. iWar: A new threat, its convenience and our increasing vulnerability [Електронний ресурс] // North atlantic treaty organization : сайт. – Режим доступу: http://www.nato.int/docu/review/2007/issue4/english/analysis2.html.
3. Frank D. Sun Behind Clouds - On Automatic Cloud Security Audits and a Cloud Audit Policy Language / D. Frank, R. Thomas. // International Journal on Advancesin Networks and Services. – 2013. – №6. – С. 1–16.
4. K. Kozhakhmet. Expert System for Security Audit Using Fuzzy Logic [Text] / K. Kozhakhmet, G. Bortsova. // Kazakh-British Technical University, 2012, pp. 146-151.
5. Miklos A. Vasarhelyi. THE CONTINUOUS AUDIT OF ONLINE SYSTEMS / Miklos A. Vasarhelyi, Fern B. Halper. // Submitted to Auditing: A Journal of Practice and Theory. – 1991, 10(1)
6. Хох В. Д. Дослідження методів аудиту систем управління інформаційною безпекою [Текст] / В. Д. Хох, Є. В. Мелешко, О. А. Смірнов. // Системи управління, навігації та зв'язку. – 2017. – №1. – С. 38–42.
7. Technical Guide to Information Security Testing and Assessment [Електронний ресурс] / K.Scarfone, M. Souppaya, A. Cody, A. Orebaugh. // Computer Security Division Information Technology Laboratory National Institute of Standards and Technology. – 2008. – Режим доступу: https://doc.uments.com/h-technical-guide-to-information-security-testing-and-assessment.pdf
8. Information technology — Security techniques — Information security management systems — Requirements (ISO/IEC 27001:2005)(Міжнародний стандарт)

Список літератури

1. 2007 cyberattacks on Estonia. *en.wikipedia.org*. Retrieved from https://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia..
2. Rajan, D. (2007). iWar: A new threat, its convenience and our increasing vulnerability . North atlantic treaty organization. *nato.int.* Retrieved from http://www.nato.int/docu/review/2007/issue4/english/analysis2.html.
3. Frank, D. & Thomas, R. (2013). Sun Behind Clouds - On Automatic Cloud Security Audits and a Cloud Audit Policy Language. *International Journal on Advancesin Networks and Services, 6*, 1–16.
4. Kozhakhmet, K. & Bortsova, G. (2012). *Expert System for Security Audit Using Fuzzy Logic.* Kazakh-British Technical University.
5. Miklos A. Vasarhelyi & Fern B. Halper. (1991). THE CONTINUOUS AUDIT OF ONLINE SYSTEMS. *Submitted to Auditing: A Journal of Practice & Theory*, *10(1),* 110-125.
6. Khokh, V.D., Meleshko, Ye.V. & Smirnov, O.A. (2017). Doslidzhennia metodiv audytu system upravlinnia informatsijnoiu bezpekoiu. *Systemy upravlinnia, navihatsii ta zv'iazku*, *1*, 38–42.
7. Scarfone, K., Souppaya, M., Cody, A. & Orebaugh, A. (2008). Technical Guide to Information Security Testing and Assessment. *Computer Security Division Information Technology Laboratory National Institute of Standards and Technology*. Retrieved from https://doc.uments.com/h-technical-guide-to-information-security-testing-and-assessment.pdf
8. Information technology – Security techniques – Information security management systems – Requirements . (2005). *ISO/IEC 27001:2005.* International Standard)

Vitaliy Khokh, postgraduate
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
Methods of Automated Sentiment Analysis on Social Networks Automated System for Auditing Information Security of Computer Systems and Networks

The article deals with the system for the audit of information security of computer systems and networks developed within the framework of the dissertation research.

The first part of the system is the control center of the system, with which the operator, the auditor works directly. The second part is a knowledge base that is presented as a SQL server in the system. The third part is a device or node, an audit tool provider, or an attack module. The control center is the main and controls all other nodes, with it directly staff. The control center of the system must be connected to the database server, which has a knowledge base, and a connection to the module of the tools provider must be provided. The knowledge base in the system is represented by a relational database of SQL. The primary tasks of the audit tool provider are to accept and execute instructions from the control center, and since the control center will attempt to contact it using the SSH protocol, the provider must be able to deploy the SSH server and accept the connection.

The system is developed in such a way as to make decisions by working closely with the user. The system allows you to capture the number of facts that people may not reach, or it becomes inconvenient. The system does not forbid inclusion in the calculation of facts that interest the user - on the contrary, it complements them, in the event that the inclusion of one custom fact will not affect the operation of the system, because the data associated with it are outside the current state of the factual database, or Products that actively use this fact are beyond the "interests" of the expert system, with the data that it currently has.

At the moment two versions of the system have been developed, both of them can be considered as early alpha versions. In the first version, attention was focused on the interaction of nodes of the system and the main mechanisms of the expert system. In the second version, the structure of the system has been redesigned so that the system becomes more flexible to scaling.
information security, audit, fuzzy logic, expert systems, automation

Одержано (Received) 18.05.2018

УДК 004.9

Д.В. Шингалов, асп., Є.В. Мелешко, доц., канд. техн. наук, Р.М. Минайленко, доц., канд. техн. наук., В.А. Резніченко, викл.
Центральноукраїнський національний технічний університет, м. Кропивницький, Україна, E-mail: elismeleshko@gmail.com, E-mail: dimashingalov@gmail.com

Математична модель рекомендаційної системи з врахуванням емоційного забарвлення коментарів у якості контексту

У статті пропонується математична модель рекомендаційної системи, у якій у якості контексту використовується аналіз емоційного забарвлення коментарів стосовно об’єктів рекомендацій. При відсутності явного зворотного зв’язку аналіз контексту значно підвищує точність рекомендацій та якість прогнозування вподобань користувачів.
рекомендаційні системи, сентимент-аналіз, колаборативна фільтрація, машинне навчання, інтелектуальні системи

Д.В. Шингалов, асп., Е.В. Мелешко, доц., канд. техн. наук, Р.Н. Минайленко, доц., канд. техн. наук, В.А. Резниченко, преп.
Центральноукраинский национальный технический университет, г. Кропивницкий, Украина