

Центральноукраїнський національний технічний університет
Механіко-технологічний факультет
Кафедра кібербезпеки та програмного забезпечення

”Допущено до захисту”
Завідувач кафедри кібербезпеки
та програмного забезпечення
д.т.н., професор
_____ Олексій СМІРНОВ
«___» _____ 2026 р.

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА
за першим (бакалаврським) рівнем вищої освіти
на тему
“Програмне забезпечення системи захищеної і адаптованої
мережі SD-WAN”

Виконав здобувач вищої освіти
IV курсу, групи КІ-23-МБ
ОПП «Комп’ютерна інженерія»
спеціальності 123 «Комп’ютерна інженерія»
_____ Царук А.Є.
«___» _____ 2026 р.

Керівник проекту
кандидат технічних наук, доцент
_____ Смірнова Т.В.
«___» _____ 2026 р.
Рецензент _____

Центральноукраїнський національний технічний університет
Факультет Механіко-технологічний
Кафедра Кібербезпеки та програмного забезпечення
Освітній ступінь бакалавр
Галузь знань ._12 _____“Інформаційні технології”
Спеціальність 123 “Комп’ютерна інженерія”
Освітньо-професійна (освітньо-наукова) програма “Комп’ютерна інженерія”

ЗАТВЕРДЖУЮ
Завідувач кафедри
д.т.н., проф.
_____ Олексій СМІРНОВ
« 27 » лютого 2026 року

ЗАВДАННЯ НА ВИПУСКНУ КВАЛІФІКАЦІЙНУ РОБОТУ ЗА ПЕРШИМ (БАКАЛАВРСЬКИМ) РІВНЕМ ВИЩОЇ ОСВІТИ ЗДОБУВАЧА ВИЩОЇ ОСВІТИ

Царуку Артему Євгеновичу

(прізвище, ім’я, по батькові)

1. Тема роботи *Програмне забезпечення системи захищеної і адаптованої мережі SD-WAN*

2. Керівник роботи *Смірнова Тетяна Віталіївна, канд. техн. наук, доцент*

(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу № 126-02 від 27.02.2026 року

3. Строк подання студентом роботи до захисту 23.05.2026 р.

4. Мета та завдання випускної кваліфікаційної роботи: *Метою роботи є розробка програмного забезпечення системи захищеної і адаптованої мережі SD-WAN*

5. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Призначення та область використання.

2. Перегляд аналогічних існуючих систем.

3. Опис і обґрунтування проектних рішень.

4. Етапи програмування системи.

5. Впровадження системи в промислову експлуатацію.

6. Висновки

6. Перелік графічного матеріалу (з точним зазначенням обов’язкових креслень)

Структурна схема системи 1 аркуш

Функціональна схема системи 1 аркуш

Діаграма процесів 1 аркуш

Блок-схема алгоритму роботи додатку 2 аркуша

7. Дата видачі завдання « 27 » лютого 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти	Строк виконання етапів випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти	Примітка
1.	Аналіз існуючих систем	10.03.2026 р.	
2.	Постановка задачі, оформлення ТЗ	15.03.2026 р.	
3.	Розробка моделі компонента	20.03.2026 р.	
4.	Розробка структур даних	25.03.2026 р.	
5.	Розробка алгоритмів зв'язку та відображення	30.03.2026 р.	
6.	Програмування алгоритмів	10.04.2026 р.	
7.	Оформлення ПЗ	17.04.2026 р.	
8.	Попередній захист роботи	23.05.2026 р.	

Дата видачі завдання
« 27 » лютого 2026 р.

Підпис керівника

Смірнова Т.В.
(прізвище та ініціали)

Завдання прийнято до виконання
« 27 » лютого 2026 р.

Підпис здобувача

Царук А.Є.
(прізвище та ініціали)

АНОТАЦІЯ

Царук А.Є. Програмне забезпечення системи захищеної і адаптованої мережі SD-WAN. 123 Комп'ютерна інженерія. Центральноукраїнський національний технічний університет. Кропивницький. 2026.

В даній випускній кваліфікаційній роботі за першим (бакалаврським) рівнем вищої освіти розроблено програмне забезпечення, яке призначено для системи захищеної і адаптованої мережі SD-WAN.

Метою розробки є програмне забезпечення системи захищеної і адаптованої мережі SD-WAN.

Результат роботи – програмна реалізація системи захищеної і адаптованої мережі SD-WAN.

В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

Розроблено зручний інтерфейс користувача. Наведені інструкції по роботі з програмними засобами.

Програма може використовуватися на ПЕОМ з ОС Windows 10/11.

Програму розроблено в середовищі Python.

Ключові слова: комп'ютерна інженерія, SD-WAN

ABSTRACT

Tsaruk A.E. Software for the SD-WAN secure and adapted network system. 123 Computer Engineering. Central Ukrainian National Technical University. Kropyvnytskyi. 2026.

In this final qualification work for the first (bachelor's) level of higher education, software has been developed that is intended for the SD-WAN secure and adapted network system.

The purpose of the development is the software for the SD-WAN secure and adapted network system.

The result of the work is the software implementation of the SD-WAN secure and adapted network system.

In the process of working on the software model, an analysis of existing hardware and software was performed. All components of the developed software are fully described.

A convenient user interface has been developed. Instructions for working with software are provided.

The program can be used on a PC with Windows 10/11 OS.

The program was developed in the Python environment.

Keywords: computer engineering, SD-WAN

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ	2
ВСТУП.....	3
1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ	5
1.1 Призначення системи.....	5
1.2 Область застосування.....	6
2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ	8
2.1 Огляд існуючих систем, технологій, архітектур та програмних рішень за профілем теми випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти.....	8
2.2 Обґрунтування вибору засобів для побудови системи та мови програмування.....	25
2.3 Розгорнута постановка завдання	29
3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ	31
3.1 Опис функціонування системи	31
3.2 Розробка структурної схеми.....	34
3.3 Розробка функціональної схеми	41
3.4 Розробка діаграми процесів.....	43
4 РЕАЛІЗАЦІЯ РОБОТИ. РОЗРАХУНКИ І ЕКСПЕРИМЕНТАЛЬНІ ДАНІ, ЩО ПІДТВЕРДЖУЮТЬ ВІРНІСТЬ ПРОЕКТНИХ ТА ПРОГРАМНИХ РІШЕНЬ.....	45
4.1 Розробка блок-схем та опис алгоритмів функціонування системи.....	45
4.2 Захист розробленого програмного забезпечення.....	75
5 ВПРОВАДЖЕННЯ СИСТЕМИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ	78
6 ОСНОВНІ ВИСНОВКИ.....	84
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	86

					ВКРБ-123.26.0039.00.00.ПЗ			
Вим.	Арк.	№ докум.	Підп.	Дата	Програмне забезпечення системи захищеної і адаптованої мережі SD-WAN	Літ.	Аркуш	Аркушів
Розроб.	Царук А.Є.					Б	1	94
Перев.	Смірнова Т.В.							
Н.контр.	Коваленко А.С.					ЦНТУ КІ-23-МБ		
Затв.	Смірнов О.А.							

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

ЛОМ	—	локальна обчислювальна мережа
MME	—	міжмережні екрани
ATM	—	асинхронний режим передачі
BSD	—	адаптована для Internet реалізація операційної системи UNIX
ICMP	—	міжмережний протокол управляючих повідомлень
IP	—	Internet Protocol – міжмережний протокол
NFS	—	мережна файлова система
PPP	—	протокол передачі від точки до точки
RFC	—	опис набору протоколів Internet
RPC	—	віддалений виклик процедури
SD-WAN	—	програмно-визначаємі територіально розподілені мережі
SLIP	—	міжмережний протокол для послідовного каналу
SMTP	—	Simple Mail Transfer Protocol – простий протокол передачі пошти
TCP	—	Transmission Control Protocol – протокол управління передачею
UDP	—	User Datagram Protocol – протокол користувальницьких датаграм
UNIX	—	багатозадачна операційна система
UTP	—	незахищена вита пара
URL	—	уніфікований показчик інформаційного ресурсу

ВСТУП

Актуальність теми. При реалізації проектів цифрової трансформації багато керівників компаній зіштовхуються з питанням, як об'єднати всі підключені ресурси в єдину зв'язну мережу. У пошуках рішення вони все частіше звертаються до концепції програмно-визначаємих територіально розподілених мереж SD-WAN. Однак критичною проблемою такого підходу є реалізація ефективної стратегії безпеки, яка б охоплювала всю мережу й адаптувалася до змін у ній.

Хмари стають одним з основних місць для розміщення ІТ-ресурсів, застосунків і сервісів, у результаті чого міняється традиційна картина розподілу потоків трафіку. У цьому зв'язку різні організації обертають свою увагу на технологію SD-WAN, що дозволяє реалізувати економічне рішення для підключення безлічі користувачів, пристроїв і площадок. Завдяки використанню недорогих каналів доступу в глобальну мережу Інтернет і програмувальної функціональності, правильно спроектоване рішення SD-WAN спрощує налаштування й підвищує масштабування мережі, забезпечуючи при цьому необхідну продуктивність і надаючи необхідні інструменти контролю з'єднань по значно меншій ціні, ніж традиційні підходи до передачі даних.

У цьому зв'язку цілком очікувано виглядають результати недавнього дослідження аналітичної компанії IHS Market, відповідно до якого три чверті опитаних компаній провели торік власні попередні тестування рішень SD-WAN, а цього року вже планують реалізувати пілотні проекти й потім увести їх у промислову експлуатацію. Готовність компаній до впровадження технологій SD-WAN підкреслює не тільки все більшу залежність бізнесу від надійних з'єднань, але й потенційну уразливість через збільшення загального числа підключень.

Мета й завдання дослідження. Метою роботи є програмне забезпечення системи захищеної і адаптованої мережі SD-WAN.

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		3

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

- Огляд існуючих систем захищеної і адаптованої мережі SD-WAN.
- Дослідження системи захищеної і адаптованої мережі SD-WAN.
- Програмна реалізація системи захищеної і адаптованої мережі SD-WAN.

Практична цінність отриманих результатів полягає в тому, що розроблені алгоритми дозволяють успішно вирішувати задачі захищеної і адаптованої мережі SD-WAN.

Таким чином, виходячи з вищеперерахованого, програмне забезпечення системи захищеної і адаптованої мережі SD-WAN, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за першим (бакалаврським) рівнем вищої освіти.

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		4

1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ

1.1 Призначення системи

SD-WAN (Software-Defined Wide Area Network, програмно обумовлена глобальна комп'ютерна мережа) поступово набирає популярність як зручна альтернатива традиційним технологіям розгортання великомасштабних обчислювальних мереж. Бізнес цінує її як засіб, що дозволяє прискорювати й спрощувати підключення нових сегментів мережі й пристроїв, а також оптимізувати витрати на оренду каналів зв'язку. Типовий її користувач – територіально розподілена й розгалужена організація, що має поряд із центральним офісом деяка безліч регіональних філій, у яких, з одного боку, потрібно забезпечити безперервний інформаційний обмін зі штаб-квартирою й клієнтами, а з іншого боку, досить бажано уніфікувати програмне середовище й використовувати мережні рішення, щоб не витрачати ресурси на компенсацію різнобою. Крім того, географічна далекість підрозділів компанії створює попит на прості в експлуатації продукти, які допускали б розгортання нових обчислювальних ресурсів на місці силами наявного персоналу. SD-WAN – одна зі спроб відповісти на подібні виклики.

Дійсно, програмно керована мережа надає можливості, які важко одержати іншими способами. Зокрема, одне з її ключових достоїнств – інтелектуальне керування трафіком, що дозволяє привласнювати певний пріоритет переданим даним залежно від їхнього типу, а також планувати найбільш підходящі маршрути. Хрестоматійний приклад – проведення відеоконференцій: для об'ємного вмісту, що пред'являє особливі вимоги до якості сигналу, може бути підібраний найбільш пропускний канал з високою швидкістю, у той час як менш критичний трафік буде добиратися до мети по іншим, не настільки «товстим» каналах. Інша корисна властивість SD-WAN – це, скажемо, оперативне централізоване конфігурування мережного встаткування:

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		5

замість того щоб окремо програмувати кожний маршрутизатор, досить розіслати єдиний шаблон налаштування по всіх пристроях відповідного типу.

Втім, вигоди SD-WAN цілком докладно описані, і їх нескладно знайти в статтях, присвячених програмно обумовленим мережам у цілому. Нас цікавить інше: усяка нова технологія, і в першу чергу – яка претендує на популярність, неминуче стає центром притягання для атак зловмисників, і кіберкримінал у таких випадках здатний випередити умовного офіцера безпеки, що ще не успели одержати повне подання про погрози, з якими він може зіштовхнутися. Поговоримо про те, із чого варто виходити при забезпеченні безпеки SD-WAN і на що варто звертати увагу при оцінці ступеня її захищеності.

1.2 Область застосування

Одне з головних переваг SD-WAN – підвищення загального рівня задоволеності користувачів якістю IT-сервісів за рахунок динамічної маршрутизації застосунків по найбільш ефективних з'єднаннях WAN у кожний момент часу. SD-WAN також дозволяє перенести фокус із маршрутизації пакетів на підтримку застосунків, коли ресурси WAN резервуються й виділяються під конкретні бізнес-завдання, що в остаточному підсумку робить мережа більше ефективною й гнучкою.

Для одержання всіх переваг SD-WAN замовники повинні добре уявляти собі ландшафт використовуваних застосунків і те, наскільки вони критичні для бізнесу. Детальний аналіз дозволяє більш ефективно виділяти ресурси й тим самим підвищити продуктивність і знизити витрати.

Таким чином, рішення SD-WAN дозволяють більш ефективно й економічно використовувати всі доступні ресурси традиційних WAN-мереж у рамках територіально розподілених підприємств і оптимізувати бізнес-процеси. У той же час критичною проблемою такої моделі є відсутність ефективної стратегії забезпечення інформаційної безпеки, яка б охоплювала всю мережу й адаптувалася до змін у ній. Саме тому експерти в області SD-WAN і галузеві аналітики думають, що оптимальне рішення для корпоративних мереж SD-WAN

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		6

повинне не тільки задовольняти вимогам замовників до продуктивності і якості WAN-мереж, але й відповідати пріоритетам в області безпеки.

Вплив SD-WAN на безпеку

Зі збільшенням кількості потенційних векторів атаки можливості для злому, крадіжки даних і компрометації інформації розширюються з появою кожного нового пристрою, застосунки й з'єднання, оскільки зловмисникам стає простіше знайти слабку ланку. У той же час підвищення вимог до продуктивності й розподілених мережних ресурсів часто негативно позначається на ефективності багатьох традиційних інструментів кібербезпеки, які й без того із працею справляються з навантаженням внаслідок збільшення швидкостей і пропускну здатності.

Інша проблема, з якою зіштовхуються організації, – зростаюча складність засобів захисту. У результаті проектно-орієнтованого підходу до розширення мереж багато організацій замість цілісних систем безпеки одержали безліч ізольованих «точкових» продуктів. Архітектура безпеки, що вийшла, не тільки погано керована, але й нездатна забезпечити комплексний і інтегрований захист.

Багато рішень SD-WAN уже зараз надають ефективні інструменти для керування розподіленою мережею, але в той же час у них відсутня інтегрована стратегія забезпечення безпеки. Замість цього вони покладаються на зовнішні системи захисту, застосування яких, на жаль, занадто часто погіршує видимість, ускладнює адміністрування й обмежує продуктивність. Згодом проблеми тільки збільшуються, оскільки такі системи нездатні адекватно адаптуватися до постійно, що відбуваються змін, в архітектурі WAN-підключень.

Відповідно, якщо безпека є пріоритетною метою поряд з ефективністю передачі даних, то при виборі рішення SD-WAN необхідно звертати увагу на доступність інструментів безпеки.

Таким чином, виходячи з вищеперерахованого, програмне забезпечення системи захищеної і адаптованої мережі SD-WAN, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за першим (бакалаврським) рівнем вищої освіти.

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		7

2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ

2.1 Огляд існуючих систем, технологій, архітектур, програмних рішень за профілем теми випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти

Інтеграції рішення SD-WAN із продуктами компанії Palo Alto Networks

Сьогодні бізнес як ніколи колись стає усе більш глобальним і орієнтованим на принципи постійної взаємодії й спільної роботи.

Сучасні співробітники працюють у будь-якому місці, у будь-який час і на будь-якому зручному пристрої, а обмін інформацією й ідеями відбувається між системами, не знаючи границь.

Така модель відкриває перед нами нові вершини продуктивності й розвитку інновацій, здатні змінити цілі галузі або навіть створити нові. Але разом з тим вона приносить нові ризики, пов'язані зі збільшенням цифрового периметра, що компаніям необхідно пильно охороняти.

Citrix Systems, Inc. (NASDAQ: CTXS) у своїх продуктах розширює функції захисту мереж, щоб допомогти компаніям вирішити це завдання.

Citrix оголосила про спільну роботу з Palo Alto Networks, світовим лідером в області інформаційної безпеки. Метою нового проекту є забезпечення простого розгортання й керування міжмережевими захисними екранами наступного покоління на платформі Citrix SD-WAN, щоб замовники могли одержати додаткові рівні безпеки для захисту своїх цифрових активів.

Застосунки й робочі навантаження дуже швидко мігрують у хмарні середовища, і системи безпеки не повинні від них відставати. Разом з Palo Alto Networks ми пропонуємо сучасне рішення для забезпечення безпеки на базі SD-

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		8

WAN, що дозволить компаніям захистити своїх користувачів, дані й застосунки в офісах, центрах обробки даних і публічних хмарних середовищах.

Спрощена мережна інфраструктура WAN Edge

Citrix SD-WAN – це рішення WAN Edge наступного покоління, що забезпечує автоматизоване, безпечне мережне підключення, необхідне для оптимізації роботи застосунків і забезпечення високого рівня комфортної роботи користувачів. Завдяки інтеграції віртуальних міжмережевих захисних екранів серії VM Palo Alto Networks і Prisma Access з рішенням Citrix SD-WAN, компанії зможуть поліпшити захист своїх мереж і хмарних середовищ.

Посилений захист

Використовуючи Citrix SD-WAN Orchestrator для уніфікованого керування й контролю, IT-фахівці можуть:

- Створити й підсилити погоджені політики контролю доступу на основі застосунків і користувачів у мережі й хмарних середовищах.
- Автоматизувати надання міжмережевих захисних екранів серії VM Palo Alto Networks (NGFW) на пристроях Citrix 1100 у вигляді віртуальної мережної функції (VNF).
- Автоматизувати підключення до хмарних міжмережевим захисним екранам Palo Alto Networks Prisma Access для погодженої реалізації політик.
- Спростити надання багаторівневих сервісів забезпечення безпеки з Citrix SD-WAN Orchestrator через Citrix Cloud.
- Створити окремі зони безпеки для захисту користувачів, застосунків і даних.

Програмний комплекс Mirobase забезпечення інформаційної безпеки вашого бізнесу

Безперервний аналіз активності користувачів для захисту від інсайдерських погроз.

Сертифікований Державною службою спеціального зв'язку й захисту інформації України.

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		9

Mirobase надійно захищає корпоративну інформацію: бази даних клієнтів, технології, патенти, маркетингові стратегії, персональних даних співробітників, фінансову звітність і багато чого іншого в різних галузях: банки, страхові, ритейлові мережі, промисловість, державний сектор, медицина.

Втрата або витік подібних даних може створити для сучасного бізнесу серйозні проблеми: від фінансових збитків і до втрати репутації. Щоб уникнути подібних негативних інцидентів, необхідно забезпечити надійний захист даних

Які завдання вирішує Mirobase для забезпечення інформаційної безпеки організації

Моніторинг переписки співробітників у месенджерах і в електронній пошті:

- Аналіз по ключових словах.
- Тіньове копіювання файлів, скопійованих на флешку, відправлених на файлообмінники й поштою.
- Відстеження контактів з конкурентами й сторонніми роботодавцями.

Запобігання витоків конфіденційної інформації: фіксація й перехоплення даних:

- Блискавичне виявлення погроз.
- Відстеження спроб порушення безпеки.
- Блокування витоку даних.

Надійний захист від корпоративного шпигунства, підвищення загальної безпеки:

- Керування доступами.
- Розслідування інцидентів.
- Моніторинг робочих програм.

Функціональні можливості Mirobase

Моніторинг активного часу комп'ютера співробітника

Скільки робочого часу співробітник витрачає на активну роботу, а скільки на непродуктивні дії.

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		10

Моніторинг програм

Якими програмами й застосунками співробітник користується в робочий час, і з якими цілями.

Моніторинг відвідуваних сайтів

Контроль використання інтернету співробітниками. Скільки часу співробітник витрачає на використання мережі інтернет у робочих цілях, а скільки – в особисті.

Моніторинг передачі даних

Чи були віддалені або відправлені важливі файли й чи не була важлива база скопійована на змінні носії.

Моніторинг тексту, що вводиться

Яка, а також куди й кому повідомляється або пересилається важлива комерційна інформація.

Перегляд всіх працюючих процесів на комп'ютері співробітника

Інформація про всі запущені процеси обраних співробітників, причому, якщо в процесу є своє вікно (відкрите або згорнуте), те це також окремо позначається в інформаційному вікні.

Активна реакція на підозрілі дії (sms/ e-mail)

Можливість миттєвого оповіщення керівника про зроблену підозрілу дію співробітника (запуск шкідливого ПЗ, введення характерного тексту, відвідування небажаних сайтів) за допомогою e-mail або SMS.

Доступ з мобільних пристроїв

Дана можливість дозволяє спостерігати за ефективністю роботи ваших співробітників із планшета або мобільного телефону.

Які оповіщення й звіти керівник компанії побачить в Mirobase:

- Перехоплення пошти, повідомлень у месенджерах і переписки в соціальних мережах.
- Моніторинг відвідуваних сайтів і використовуваних програм.
- Точний час роботи з кожним ресурсом.

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		11

- Оповіщення про підозрілі дії й заборона на їхнє виконання.
- Перехоплення даних, виведених за периметр ПК.
- Запобігання витоків інформації у вигляді таблиць, документів.

Моніторинг і контроль печатки.

- Тайм-трекінг роботи персоналу.

Mirobase генерує регулярні звіти й звіти по запиті

Загальний зведений звіт:

- запізнення, ранні відходи з роботи й прогули;
- характеристики ефективності проведеного їм часу за комп'ютером;
- кількість тексту, що роздруковується;
- наявність підозрілої активності;
- застосунки, яким надається перевага, і сайти

Майстер звітів

Майстер звітів формує звіт по співробітнику або групі співробітників по заданим вами параметрам у будь-яких інформаційних розрізу

Звіт "контакти"

Звіт по взаємодії співробітників один з одним, клієнтами, постачальниками й ін. Дозволяє оперативно визначити коло спілкування співробітника – з ким і як часто спілкується

Експорт звітів в Excel

Дана можливість дозволяє експортувати звіти в Microsoft Excel або OpenOffice Calc (на ваше бажання). Підтримуються формати XLS і CSV

Технічні особливості комплексу Mirobase

Проста установка, зручний контроль, повні звіти:

- Mirobase Smart Control інтегрується з Active Directory і легко вбудовується в будь-яку інфраструктуру.
- Безліч режимів збору даних для груп користувачів. Тонке налаштування рівня контролю для відділів, підрозділів і окремих співробітників.

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		12

- Персоналізація збору й аналізу інформації. Можливість змінювати якість інформації, що зберігається, і місце її зберігання (локально або на сервері).
- Архітектура дозволяє розгорнути й адмініструвати від сотень до тисяч робочих станцій одночасно.
- Установка не займає багато часу й не вимагає особливих знань або навичок. Впровадження не порушує робочі процеси, не має потреби в змінах структури локальної мережі й не веде до простоїв у роботі.
- Низькі системні вимоги дозволяють використовувати програму навіть на слабких «офісних» ПК. Mikrobase не сповільнює роботу комп'ютерів.
- Антивірусні програми не реагують на установку й не заважають роботі.

Огляд засобу захисту SD-WAN FortiGate

У міру поширення хмарних бізнес-застосунків і інструментів розподілені компанії, до складу яких входить велика кількість віддалених офісів, переходять із недостатньо продуктивних глобальних обчислювальних мереж (WAN) на архітектуру програмно-конфігуруємих мереж WAN (SD-WAN). Мережі SD-WAN підтримують керування бізнес-застосунками, знижують витрати й підвищують продуктивність як застосунків «Програмне забезпечення як послуга» (SaaS), так і служб об'єднаних комунікацій. Однак у технології SD-WAN є свої недоліки, особливо при наявності прямого доступу до Інтернету.

Засіб захисту SD-WAN Fortinet FortiGate включає кращий у своєму класі міжмережевий екран наступного покоління (NGFW), функції SD-WAN, розширеній маршрутизації й оптимізації WAN. Це комплексне рішення, що забезпечує безпечну трансформацію периферійної інфраструктури WAN. Компанія Fortinet у другий раз підряд одержала оцінку «Рекомендоване NSS Labs» за результатами групового тесту SD-WAN. Засіб захисту SD-WAN Fortinet показало найнижчий результат за критерієм сукупної вартості володіння (TCO) на Мбіт/с серед рішень всіх восьми постачальників.

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		13

Мережа SD-WAN філії

Філії розподіленої компанії, що переходять на модель цифрового бізнесу, значно впливають на мережу. Оскільки корпоративні користувачі, як віддалені, так і локальні, використовують прямий доступ до Інтернету, працюючи із хмарними застосунками «Безпека як послуга» (SaaS), структура мереж WAN і периферії доступу значно ускладнюється. Більше того, пристрою Інтернету речей (IoT), що підключаються до мережі філії, створюють нові уразливості, які можуть використовувати зловмисники. В умовах цієї нової парадигми критичного значення набуває розгортання стратегій безпеки нового покоління.

Мережа SD-WAN філії від Fortinet дозволяє клієнтам об'єднати систему забезпечення безпеки з керуванням доступом до мережі й поширити переваги Fortinet Security Fabric на розподілені філії організації. Мережа SD-WAN філії складається з міжмережевого екрана наступного покоління FortiGate, рішення для контролю доступу до мережі FortiNAC, FortiSwitch і FortiAP для консолідації служб філії для захисту периферії мережі й граничних пристроїв.

Технологія Fortinet Secure SD-WAN, інтегрована з контролем доступу в мережу, дозволяє забезпечити найвищий у галузі рівень безпеки й керованості для віддалених філій. У відповідь на підривний ріст кількості IoT-пристроїв мережа SD-WAN філії від Fortinet використовує FortiGate як датчик мережі й FortiNAC, щоб адміністратори могли не тільки виявляти й захищати IoT-пристрої, але й виявляти аномалії.

Недавні опитування показали, що користувачі вважають також необхідної інтеграцію рішень WAN і організацію загального керування із внутрішніми мережними рішеннями LAN. При цьому питання безпеки викликають найбільшу стурбованість у всіх респондентів.

Для керування мережею SD-WAN філії від Fortinet використовується наша надійна технологія доступу на базі FortiLink, що поєднує провідні й бездротові служби в інфраструктуру безпеки за допомогою FortiOS. Ключові переваги FortiLink – це загальна платформа керування й інтегрована безпека, що дозволяє

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		14

забезпечити єдиний рівень примусового забезпечення безпеки для комутаторів Ethernet і інтерфейсів WLAN через інтерфейс міжмережевого екрана. Для інтеграції комутаторів FortiLink і бездротових мереж ліцензія не потрібно. Вона включена в можливості FortiOS на кожному міжмережевому екрані FortiGate.

Виділення ресурсів в автоматичному режимі

Процес створення мереж філій і впровадження нових технологій може бути дорогим, складним і часовитратним. Гірше того, безпекою часто зневажають. Мережа SD-WAN філії від Fortinet скорочує час розгортання й зменшує потребу в присутності дорогих висококваліфікованих фахівців на місці, забезпечуючи автоматичну підготовку інфраструктури віддаленої філії. Спрощене керування через єдину панель моніторингу дозволяє адміністраторові розгортати, готувати й захищати мережу філії із середовища NOC/SOC.

Параметри конфігурації мережі SD-WAN і доступу до мережі задаються централізовано в FortiGate. Просто впевніться, що міжмережевий екран FortiGate підключений до Інтернету, щоб централізована платформа керування FortiManager могла переадресувати необхідні налаштування конфігурації для мереж WAN, LAN і елементів системи безпеки віддаленої філії.

Реалізація безпрецедентного підходу

Тільки Fortinet пропонує інтегроване рішення із централізованим керуванням і забезпеченням безпеки, підтримкою провідних і бездротових мереж і SD-WAN на базі однієї платформи. Безпечний доступ Fortinet інтегрований у наш код FortiOS, а значить – прямо убудований у служби безпеки, пропоновані FortiGate.

Fortinet – єдиний постачальник, що пропонує провідні в галузі служби безпеки в з'єднанні із власними рішеннями SD-WAN, LAN, WLAN і AC, дозволяючи консолідувати служби ваших філій у рамках єдиної, простій в управлінні платформи, допомагаючи вам заощадити час і знизити витрати. Fortinet – кращий вибір серед рішень для мереж і безпеки від доступу до мережі з філії до роботи в хмарі.

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		15

Безпека великих підприємств

Забезпечення комплексного захисту інфраструктури без шкоди для продуктивності

Цифрова трансформація (DX) обумовлена необхідністю прискорення адаптації організацій до змін на глобальному рівні й зниження витрат. Цей процес передбачає розгортання нових технологій, які приводять до появи нових напрямків атак. Уразливість мережного периметра для просунутих погроз підвищується. Ці фактори ускладнюють структуру середовищ безпеки. Система Fortinet Security Fabric сегментує всю мережу, починаючи від пристроїв Інтернету речей (IoT) і закінчуючи хмарним середовищем, щоб забезпечити високоефективний захист від витончених погроз

Система Security Fabric для великих підприємств

Система безпеки Fortinet Security Fabric – це єдина інфраструктура, що забезпечує інтеграцію, автоматизацію й широкий охват. Скоротите кількість напрямків атак і управляйте ними за допомогою інтегрованої функції відстеження із широким охоптом, забезпечте захист від просунутих погроз за допомогою засобу запобігання вторгнень на базі технології штучного інтелекту й спростите керування за рахунок автоматизації операцій і оркестрації.

Мережна безпека

Доможіться високої продуктивності підключень і ефективності захисту всіх компонентів корпоративної мережі й мереж філій. Засіб мережної безпеки Fortinet забезпечує комплексне відстеження й автоматизований захист від погроз в усіх напрямках.

Безпека багатохмарної інфраструктури

Захистите застосунки й підключення від центра обробки даних до хмари. Рішення Fortinet для багатохмарних середовищ створюють умови для відстеження й керування хмарними інфраструктурами.

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		16

Безпечний доступ

Кількість підключених до мережі бездротових пристроїв і мобільних застосунків згодом буде тільки рости. Забезпечте захист доступу до застосунків і пристроїв, а також керування ними без шкоди для продуктивності.

Операції безпеки

Використовуйте дані про просунуті погрози для виявлення, запобігання й протидії витонченим атакам. Крім цього, засобу виконання операцій безпеки Fortinet забезпечують відповідність вимогам і підвищують кваліфікацію співробітників у сфері безпеки.

Операції мережі

Запобігайте порушення за допомогою стратегії безпеки, що робить ставку на автоматизацію операцій мережі. Рішення Fortinet являє собою інтегровану архітектуру безпеки, що поєднує раніше ізольовані середовища.

Захист кінцевих точок і пристроїв

Забезпечте безпеку мережі за допомогою функції захисту, що попереджає, кінцевих точок від новітніх погроз. Компанія Fortinet надає засоби безпеки Інтернету речей (IoT) і важливих кінцевих точок, що забезпечують відстеження й керування всіма пристроями в мережі.

Безпека застосунків

Захистите мережні бізнес-застосунки, які часто стають метою кібератак. Рішення захисту веб-застосунків Fortinet Application Security включає набір надійних інтегрованих продуктів, які забезпечують захист застосунків від просунутих погроз.

Коннектори системи безпеки

Коннектори системи безпеки Fortinet – це готове рішення, що забезпечує глибоку інтеграцію з технологіями й платформами партнерів у мультивендорних екосистемах, а також автоматизує безпеку й спрощує керування.

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		17

API-Інтерфейси Security Fabric

Технологічні партнери інтегрують свої рішення із системою безпеки Fortinet Security Fabric за допомогою інтерфейсів програмування застосунків (API) для активного збору й обміну даними про усунення погроз.

Огляд рішення FortiNAC

Швидке поширення пристроїв IoT (Інтернет речей) привело до того, що в організацій виникла необхідність поліпшувати подання про те, що підключено до їхніх мереж. Необхідно знати кожний пристрій і кожного користувача, що одержує доступ до корпоративних мереж. Пристрої IoT роблять можливими проекти по цифровому перетворенню, а також поліпшують ефективність, гнучкість і оптимізацію. Проте, вони по своїй суті ненадійні, тому що при їхній конструктивній розробці перевага забезпеченню досягненню низької вартості, а не безпеки. Рішення FortiNAC надає можливість відстеження мережі для перегляду всього, що до неї підключене, а також можливість керування цими пристроями й користувачами, включаючи динамічне, автоматичне реагування.

Безпечна комутація для локальної мережі Ethernet

У застарілих локальних мережах Ethernet виникає безліч проблем. До їхнього числа ставиться стрімке зростання кількості пристроїв і застосунків у мережі, необхідність підвищення пропускної здатності бездротової мережі LAN, а також складність системи безпеки. Замість того, щоб задаватися питанням, як захистити традиційні локальні мережі Ethernet, Fortinet використовує орієнтований на безпеку підхід, пропонуючи Ethernet як розширення інфраструктури безпеки через засоби FortiSwitch і FortiLink. Рішення FortiSwitch пропонує велику лінійку безпечних, простих і масштабованих рішень Ethernet для безлічі різних середовищ – від настільних систем до центрів обробки даних.

Інтегрована система керування бездротовими мережами від FortiGate – Моделі й характеристики

Ми пропонуємо широкий вибір моделей FortiAP різних цінових категорій і для різних варіантів використання. Конфігурація й керування вашою

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		18

корпоративною бездротовою інфраструктурою здійснюється платформою мережної безпеки FortiGate Fortinet.

Великі організації, компанії з розподіленою мережею філій і підприємства малого бізнесу мають різні потреби в архітектурі WLAN. Саме тому компанія Fortinet надає повний набір точок доступу WLAN як частина рішення для бездротової інфраструктури, розробленого для задоволення унікальних потреб кожної організації.

Fortinet розширює портфоліо Security Fabric і поліпшує свої рішення кібербезпеки третього покоління

Новітній реліз FortiOS містить більше 300 інновацій, представлених у рішеннях Fortinet Security Fabric для захисту всієї мережної інфраструктури, від IoT і периферії до ядра мережі й мультихмарних середовищ.

Компанія Fortinet® (NASDAQ: FTNT), світовий лідер в області масштабних інтегрованих і автоматизованих рішень для інформаційної безпеки, оголосила про випуск новітньої версії своєї флагманської операційної системи FortiOS 6.2 на своїй глобальній конференції для партнерів і замовників Accelerate 19. Новий реліз FortiOS 6.2 продовжує еволюцію рішень Security Fabric і містить більше 300 нових інновацій, що охоплюють всі портфоліо продуктів і рішень Fortinet і мережі, що допомагають організаціям будувати, на основі принципів безпеки, що є необхідною умовою периферійних і мультихмарних оточень, що стали результатом цифрової трансформації.

Продовження цифрової трансформації означає, що для бізнесу стає усе більше важливою вся периферія, а не тільки хмарні оточення. Саме складне завдання полягає в тому, щоб захистити мережу в умовах, коли поверхня атаки росте експонентними темпами через різке збільшення числа периферійних пристроїв. Оскільки успіх бізнесу фактично вимірюється в мікросекундах, організації не можуть поступитися продуктивністю з міркувань захисту. І щоб реалізувати такий захист, організаціям варто скористатися комплексним структурним підходом (fabric-based approach) до забезпечення безпеки, що не

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		19

обмежується окремими пристроями й платформами безпеки, а охоплює одночасно всю мережу, навіть у процесі її змін. Для цього необхідна комплексний, інтегрований і автоматизований захист.

Fortinet допомагає вирішувати важливі завдання, що коштують перед замовниками

Розширена прозорість для всієї поверхні цифрових атак

Fortinet підвищує прозорість і спрощує впровадження й керування в масштабах всіх рішень безпеки Security Fabric за рахунок більше глибокої інтеграції між рішеннями Fortinet і рішеннями більше 70 партнерів Альянсу. FortiGate NGFW, краще у своєму класі рішення FortiGate Secure SD-WAN і велике портфоліо нативних хмарних платформ одержали нову функціональність, у тому числі можливість сегментації залежно від намірів (intent-based segmentation). Замовники можуть тепер повною мірою скористатися всіма перевагами прозорості, реалізованої в FortiOS 6.2, за рахунок пакетів сервісів Fortinet 360 Protection, що включають у себе великий перелік професійних сервісів.

Інтегрований захист і виявлення складних погроз

Fortinet продовжує лідерство в продуктових інноваціях, активно підтримуючи новітні галузеві стандарти, у тому числі забезпечуючи інтегровану підтримку TLS 1.3 для захисту інтернет-трафіку, пропонуючи нові технології на основі маскування (deception-based) для протидії вторгненням, а також можливості сегментації на основі довіри (trust-based segmentation), які тісно інтегровані в усі рішення Security Fabric, від ядра до периферії й у хмарі. Технологія Fortinet FortiDeceptor забезпечує кращу у своєму класі оборону й механізми захисту, при цьому «пастки» автоматично спрацьовують при виявленні шкідливого коду, а також при спробі одержання доступу або звертанні до мережних ресурсів з боку неавторизованих користувачів.

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		20

Автоматизована експлуатація, оркестровані й реагування

Глибока інтеграція й розширені можливості автоматизації в Security Fabric дозволяють замовникам знизити навантаження за рахунок єдиного інтерфейсу контролю й керування (pane-of-glass) у всіх рішеннях, інтегрованих в Security Fabric. Використання автоматизації й функцій машинного навчання для зниження складності, розширення можливостей керування й автоматизації критичних функцій дозволяють реагувати на появу погроз із високою швидкістю. При цьому безперервний потік оновлених даних і аналітики про погрози, що підготовляється фахівцями FortiGuard Labs із застосуванням штучного інтелекту, дозволяє підвищити швидкість і точність виявлення погроз і оптимізувати автоматизацію реагування.

Портфоліо Fortinet Security Fabric являє собою самий повний пакет рішень безпеки в галузі, які представлені в різних форм-факторах і нативно доступні на всіляких платформах. Поліпшення в FortiOS 6.2 розширюють передові можливості рішень Fortinet Security Fabric за рахунок оптимізації наскрізного захисту від просунутих погроз, і в той же час значно знижують складності, що традиційно виникають при проектуванні, впровадженні, керуванні й відновленні більшості архітектур безпеки. Серед основних моментів:

Розширення структури

FortiOS 6.2 містить у собі наступні поліпшення елементів Security Fabric:

- FortiADC – контролер доставки застосунків
- FortiToken – інструмент для автентифікації користувачів і пристроїв
- FortiCWP – брокер безпеки хмарного доступу для публічних хмар
- FortiDDoS – захист від розподілених атак типу «відмова в обслуговуванні»
- FortiNAC – керування мережним доступом
- VDOM – віртуальні домени

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		21

Захист SD-WAN

Реалізовані в Fortinet Security Fabric можливості SD-WAN тепер містять у собі новий набір кращих у своєму класі функцій і сервісів для захисту WAN. Завдяки цим новим функціям замовники можуть підвищувати продуктивність критично важливих застосунків, використовуючи економічно ефективні підключення до філій. Серед переваг:

- Відновлення WAN-лінка за допомогою механізму Forward Error Correction для роботи з нестійкими WAN-з'єднаннями в застосунках уніфікованих комунікацій.
- Вимір пропускної здатності WAN на вимогу.
- Оверлейний контролер (Overlay controller) дозволяє краще управляти складними проблемами підключення.
- Можливість поділу агрегованої пропускної здатності оверлейної мережі між різними з'єднаннями з метою поліпшення продуктивності й мінімізації проблем із затримками.
- Високошвидкісне розпізнавання застосунків для прискорення керування пакетами, що дозволяє кінцевим користувачам одержати максимально якісний досвід і домогтися максимальної продуктивності застосунків у будь-який момент часу.

Багатохмарна безпека

Рішення Fortinet FortiGate NGFW тепер інтегроване з Kubernetes за допомогою FortiOS 6.2 Fabric Connectors, що відкриває нові можливості для захисту контейнерів. Завдяки цьому замовники тепер можуть забезпечити безпеку будь-якого зовнішнього трафіку, що приходить або йде з їхніх контейнерних кластерів, за рахунок логічного визначення політик на основі міток і позначка-даних від контейнерів і хмарних ресурсів:

- FortiMail тепер інтегрований з O365 Exchange, що дозволяє замовникам з легкістю застосовувати саму свіжу аналітику FortiGuard про погрози для більше якісного захисту електронної пошти, що проходить через O365 Exchange.

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		22

Інтеграція не вимагає який-небудь реконфігурації мережі або поштових налаштувань, і безпосередньо підключається до API O365. Це забезпечує організаціям розширений захист від погроз і дозволяє захистити свою електронну пошту.

– Нова віртуальна архітектура SPU FortiGate-VM підтримує роботу з високопродуктивними обчисленнями в хмарі. Віртуальний процесор системи безпеки FortiGate VM (vSPU) підвищує продуктивність як у частці, так і в публічній хмарі, дозволяючи замовникам із упевненістю здійснювати міграцію своїх високопродуктивних застосунків у хмару. Використовуючи цю архітектуру, FortiGate VM як і раніше залишається найшвидшим рішенням на ринку, що забезпечує підтримку технологій віртуалізації високопродуктивних застосунків, наприклад, типів AWS C5n Instance, Intel QAT, Oracle Native Acceleration і інших.

Відкриті екосистеми

FortiOS 6.2 поліпшує вже наявну в Fortinet панель контролю й керування для всього зростаючого пакета продуктів безпеки Fortinet, сторонніх рішень від співтовариства партнерів Fortinet Fabric-Ready і нативних сторонніх API (connectors). Інтеграція в Security Fabric нових можливостей безпеки й функція автоматизації дозволяє:

- здійснювати автоматичну оцінку погроз і реалізовувати цілісний підхід до реагування;
- забезпечити дотримання регуляторних вимог за рахунок розширеного аналізу ризиків відповідно до галузевих стандартів.

Автоматизація й оркестрація

FortiOS 6.2 значно розширює комплексні можливості автоматизації, оркестрування й реагування у всіх рішеннях Security Fabric з FortiManager і FortiAnalyzer, у тому числі забезпечуючи:

- Єдиний інструмент оркестрування: виділення ресурсів і керування конфігураціями спрощується у всіх рішеннях Fortinet Security Fabric. Серед основних поліпшень – автоматичне виділення ресурсів для FortiGates,

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		23

FortiSwitches, FortiAPs, захищені SD-WAN і Fabric Connectors для більше оптимального оркестрування сервісів і хмари.

– Автоматизація: можливість комплексної автоматизації ручних, ресурсномістких процесів дозволяють зробити операції менш складними. Сюди ставиться сканування історії ІОС для відстеження погроз, а також хронологія інцидентів і панелі SOC для аналізу інцидентів і керування пріоритетами.

– Реагування: використовуються дані про активи й сутності для виявлення й зіставлення просунутих погроз, а також їх швидкого виправлення. Інтеграція з Scripts, Webhooks, ServiceNow і багатьма іншими інструментами дозволяє швидко реагувати на інциденти.

Забезпечення безпеки з використанням штучного інтелекту

FortiGuard Labs розробила систему виявлення й аналізу погроз FortiGuard AI. Лежача в її основі нейронна мережа складається більш ніж з 9 мільярдів взаємозалежних вузлів і здатна не тільки виявляти й класифікувати погрози з безпрецедентною швидкістю, FortiGuard Labs публікує високоточну аналітику про погрози, що активно використовується рішеннями Fortinet:

– Розроблена FortiGuard Labs Система виявлення погроз на базі штучного інтелекту підтримує нові поліпшені технології виявлення витоків і інтегрована в FortiGate NGFW, FortiWeb, FortiMail, FortiClient, FortiSandbox і FortiSIEM, що дозволяє прискорити виявлення погроз і реагування на них.

– Автоматизоване оркестровані використовує аналітику із всіляких джерел, у тому числі із сервісу аналітики погроз FortiGuard Labs, сторонніх джерел і власної аналітики, одержуваної за допомогою рішень Security Fabric. Крім того, ця функція здійснює необхідні дії після виявлення погроз засобами UEBA в FortiSIEM.

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		24

2.2 Обґрунтування вибору засобів для побудови системи та мови програмування

Python – це об'єктно-орієнтована мова програмування високого рівня загального призначення з відкритим кодом. Це визначення може бути важким для новачків, тому розглянемо кожну характеристику окремо, щоб зрозуміти, що вона означає:

- Відкритий вихідний код: це безкоштовно та доступно для подальших покращень, таких як додавання корисних функцій або виправлення помилок.
- Об'єктно-орієнтована: заснована не на функціях, але в об'єктах з певними атрибутами й методами.
- Високий рівень: зручний для людини, а не для комп'ютера.
- Загальне призначення: можна використовувати для створення будь-яких програм.

Ця мова використовується в будь-якому програмному забезпеченні, про яке ви тільки можете подумати. Ви можете використовувати його для створення веб-сайтів, штучного інтелекту, серверів, програмного забезпечення для бізнесу та багато іншого. Також застосовується в науці про дані, аналізі даних, машинному навчанні, інженерії даних, веб-розробці, розробці програмного забезпечення та інших галузях.

Переваги та недоліки Python

Переваги:

- Її легко читати, вчити та писати. Це мова програмування високого рівня з англійським синтаксисом. Це полегшує читання та розуміння коду. Її дійсно легко зрозуміти і вивчити, тому багато людей рекомендують Python новачкам. Вам потрібно менше рядків коду для виконання того ж завдання в порівнянні з іншими основними мовами, такими як C/C++ та Java.
- Підвищує продуктивність. Це дуже продуктивна мова. Завдяки її простоті розробники можуть зосередитися на розв'язанні проблеми. Їм не

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		25

потрібно витрачати багато часу на розуміння синтаксису або поведінку мови програмування. Ви пишете менше коду та виконуєте більше завдань.

- Інтерпретована мова. Python мова, що інтерпретується, а це означає, що вона безпосередньо виконує код по рядку. Якщо сталася помилка, вона зупиняє подальше виконання та повідомляє про її виникнення. Вона показує лише одну помилку, навіть якщо у програмі їх кілька. Це спрощує налагодження.

- Динамічно типізована. Python не визначає тип змінної, доки ми не запустимо код. Вона автоматично надає тип даних, коли відбувається процес виконання. Фахівець може не турбуватися про оголошення змінних та типи даних.

- Безкоштовна та з відкритим вихідним кодом. Ця мова постачається під схваленою OSI ліцензією з відкритим вихідним кодом. Це робить його безкоштовним для використання та розповсюдження. Ви можете завантажити вихідний код, змінити його та навіть розповсюджувати свою версію. Це корисно для організацій, які хочуть використати свою версію для розробки.

- Підтримка великих бібліотек. Стандартна бібліотека Python є величезною, ви можете знайти майже всі функції, необхідні для вашого завдання. Таким чином ви не залежите від зовнішніх бібліотек.

- Портативність. У багатьох мовах, таких як C/C++, потрібно змінити свій код, щоб запустити програму на різних платформах. З Python все інакше. Ви тільки пишете один раз і запускаєте її будь-де.

Недоліки:

- Низька швидкість. Вище ми обговорювали, що це інтерпретована мова з динамічною типізацією. Порядкове виконання коду часто призводить до повільного виконання. Динамічна природа Python також є причиною її низької швидкості, оскільки їй доводиться виконувати додаткову роботу при виконанні коду. Тому вона не підходить для цілей, де швидкість важливий аспект проєкту.

– Неєфективна для пам'яті. Ця мова програмування використовує великий обсяг пам'яті, це може бути недоліком при створенні програм, коли віддають перевагу оптимізації пам'яті.

– Слабка у мобільних обчисленнях. Python зазвичай використовується у серверному програмуванні. Ми не бачимо – її на стороні клієнта або в мобільних програмах з таких причин: вона не заощаджує пам'ять і має повільну обчислювальну потужність у порівнянні з іншими мовами.

– Доступ до бази даних. Програмувати на цій мові легко, але коли ми взаємодіємо з базою даних, її не вистачає. Рівень доступу до бази даних у Python примітивний та недостатньо розвинений у порівнянні з іншими популярними технологіями.

– Помилки виконання. Це мова з динамічною типізацією, тому тип даних змінної може змінюватись у будь-який час. Змінна, що містить ціле число, у майбутньому може містити рядок, що може призвести до помилок виконання.

Застосування Python:

– Для аналізу даних. Дані стали цінним активом у будь-якій сучасній галузі, і більшість компаній зацікавлені у збиранні, обробці та аналізі релевантних даних, щоб витягти з них цінну інформацію для бізнесу. І тут Python виходить за межі будь-якої конкуренції. Python особливо цінна тим, що крім великої стандартної бібліотеки надає величезний набір додаткових модулів, розроблених спеціально для аналітичних цілей. Найвідоміші бібліотеки Python для аналізу даних – це pandas і NumPy . Ці інструменти дозволяють робити з вашими даними майже все, наприклад, очищати і аналізувати їх, вивчати статистику або візуалізувати приховані тенденції у ваших даних.

– Для візуалізації даних. Візуалізація даних – це окрема частина аналізу даних, яка допомагає нам подавати інформацію, необроблену чи очищену, у більш змістовній формі. Тут Python знову входить у гру, пропонуючи широкий спектр інструментів візуалізації даних. Найпопулярніші з них – matplotlib і

заснований на ній seaborn. Використовуючи їх, ми можемо створювати буквально всі види візуалізації: від найпростіших до складніших.

– Для машинного навчання. Машинне навчання (ML) є основою більшості завдань науки даних. Він є областю штучного інтелекту, пов'язаною з використанням алгоритмів, що дозволяють машинам вивчати закономірності та тенденції на основі історичних даних, щоб робити прогнози на основі невідомих даних. – Використовуючи методи ML, ми можемо створювати моделі, які можуть точно передбачити швидкість відтоку клієнтів компанії, оцінити ризик виникнення у людини певного захворювання, визначити оптимальне розташування автомобілів таксі й т.д. За допомогою Python ми можемо побудувати модель ML, використовуючи лише три рядки коду.

– Для розробки програмного забезпечення. Крім свого багатостороннього застосування в галузях науки про дані, Python використовується на кожному етапі розробки програмного забезпечення, включаючи контроль складання, автоматичну безперервну компіляцію, прототипування, відстеження помилок, тестування та обслуговування програмного забезпечення. За допомогою цієї мови можемо створювати аудіо- або відеопрограми на основі методів штучного інтелекту, машинного навчання, API (інтерфейсів прикладного програмування), GUI (графічних інтерфейсів) або будь-якого іншого типу програмного забезпечення.

– Для веброботи. У той час як для створення візуальної частини вебсайту ми переважно будемо використовувати такі мови, як HTML, CSS та JavaScript, для його невидимої частини ми часто вибираємо Python. Серед масштабних вебсайтів та програм, створених за допомогою цієї мови, варто згадати Google, Facebook, Instagram, YouTube, Dropbox та Reddit.

– Для автоматизації задач/скриптингу. Це відмінний інструмент для написання програм для автоматизації різних завдань, що повторюються. Цей процес називається скриптингом. Зокрема, можна робити скрипти для роботи з файлами та папками. Наприклад, можна створювати, перейменовувати,

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		28

перетворювати, розділяти, об'єднувати або видаляти файли, перевіряти їх на наявність помилок. Ви також можете використовувати автоматизацію Python для пошуку та завантаження інформації з Інтернету, заповнення та надсилання онлайн-форм та надсилання регулярних повідомлень або електронних листів.

Яким фахівцям потрібно володіти Python:

- Фахівець з даних.
- Аналітик даних.
- Інженер даних.
- Інженер з машинного навчання.
- Журналіст даних.
- Архітектор даних.
- Повний стек веб-розробника.
- Backend-розробник.
- DevOps-інженер.
- Інженер-програміст.

Можемо зробити висновок, що Python ще довго буде популярною мовою, хоч і має низку недоліків. Цю мову використовують для створення вебсайтів, штучного інтелекту, серверів, програмного забезпечення для бізнесу, аналізу даних, машинного навчання, інженерії даних та для багатьох інших областей. Це перспективна і затребувана навичка, яка необхідна у всіх галузях.

2.3 Розгорнута постановка завдання

Згідно з технічним завданням на випускню кваліфікаційну роботу за першим (бакалаврським) рівнем вищої освіти, реалізації підлягає програмне забезпечення, яке призначено для системи захищеної і адаптованої мережі SD-WAN.

В процесі розробки випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти необхідно виконати наступний обсяг роботи:

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		29

а) провести аналіз існуючих систем-аналогів для виявлення їх позитивних і негативних якостей. Результати аналізу врахувати в подальших розробках;

б) вибрати та обґрунтувати методику побудови системи контролю роботи технологічного обладнання на виробництві в автоматизованому режимі. Розробити функціональну та структурну схеми системи;

в) розробити програмне забезпечення системи, що дозволить реалізувати поставлену технічним завданням задачу. Побудувати блок-схеми алгоритмів програми та підпрограми;

г) організувати інтерфейс користувача з метою формування та виводу на екран ЕОМ повідомлень про некоректні дії користувача та нестандартні ситуації в роботі технологічного обладнання;

д) розробити рекомендації по організаційних та методичних заходах, які забезпечать впровадження системи в промислову експлуатацію та її подальшу успішну експлуатацію;

е) провести розрахунки по визначенню економічної ефективності розробленої системи;

ж) розробити заходи по охороні праці при впровадженні та експлуатації системи, а також розробити заходи з цивільного захисту;

з) сформулювати висновки про виконаний обсяг робіт та одержані результати.

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		30

3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ

3.1 Опис функціонування системи

Рішення SD-WAN часто не мають інтегрованих інструментів безпеки, а тих, що доступно, звичайно недостатньо. У той же час опора на традиційні рішення мережної безпеки для захисту гнучких і адаптуємих мереж представляється проблематичною.

Незважаючи на те що ринок SD-WAN динамічно розвивається, він поки перебуває на ранніх етапах свого становлення. Це виражається, зокрема, у присутності на ринку безлічі гравців і відсутності єдиної думки щодо того, яка реалізація краще. Який шлях у підсумку вибере ринок, поки судити ще занадто рано – його подальший розвиток залежить від цілого ряду факторів. Серед них попит на дані рішення й наявність альтернатив, темпи ринкового проникнення, переваги замовників відносно постачальників і, звичайно, інтегрована безпека, що не тільки захищає дані в процесі їхньої передачі, але й безшовно інтегрується в більше широкий контекст мережної безпеки.

В аналітичній компанії Gartner виділяють чотири основних варіанти побудови архітектури безпеки для технологій SD-WAN:

- SD-WAN з убудованим міжмережним екраном;
- міжмережний екран з інтегрованими засобами SD-WAN;
- SD-WAN і MME наступного покоління від незалежних постачальників;
- SD-WAN із хмарними сервісами безпеки.

Переваги замовника можуть мінятися залежно від його конкретних потреб і ситуації. Однак, по наших досвіді, спостерігається зростаючий попит на так звані захищені рішення SD-WAN (Secure SD-WAN), яким найкраще відповідає варіант 2 з наведеного переліку від компанії Gartner. У цьому сценарії надійна функціональність SD-WAN інтегрується в ключовий елемент сучасної мережної

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		31

архітектури – міжмережевий екран – з метою оптимізації роботи мережних застосунків, перевірки й захисту трафіку при обміні критичними даними між віддаленими площадками.

Чому це важливо? У підтримку того, чому цей підхід, можливо, являє собою найкращий можливий варіант реалізації SD-WAN, можна привести цілий ряд фундаментальні міркування безпеки. І серед них той простий факт, що ефективна й повнофункціональна безпека усе ширше зізнається важливим елементом мережі SD-WAN. У цьому контексті додавання функцій SD-WAN до вже розгорнутого компонента мережі має сенс. Включення цього сервісу в рішення класу NGFW, що вже дозволяє управляти віддаленими з'єднаннями VPN, а також здатно динамічно застосовувати відповідні рівні аналізу й захисту трафіку, має ще більше переваг, тому що воно забезпечує високий рівень контролю за даними й застосунками, що проходять через середовище SD-WAN.

Таким чином, рішення SD-WAN мають потребу в повному наборі інструментів для захисту від погроз, у який входять міжмережевий екран наступного покоління корпоративного класу, антивірус, система запобігання вторгнень і засобу контролю застосунків. Крім того, він повинен включати високопродуктивні інструменти перевірки шифрованого трафіку SSL, фільтрації й контролю Web-трафіку й організації захищених з'єднань VPN на вимогу для захисту трафіку й забезпечення конфіденційності даних, а також можливість інтеграції із просунутими засобами (Advanced Threat Protection, ATP) запобігання погроз нульового дня. Нарешті, ефективність захисту повинна бути підтверджена й сертифікована незалежною третьою стороною, щоб можна було бути впевненим, що надаваний рівень захисту відповідає вимогам мережі.

Функціональні вимоги до SD-WAN

Одні із труднощів, з якими доводиться зіштовхуватися при реалізації SD-WAN, – необхідність у постійній оптимізації. В умовах обмежених ресурсів варто вибирати рішення із простими налаштуваннями, що дозволяє задавати політикові доступу до WAN з урахуванням таких факторів, як критичність застосунків,

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		32

вимоги до продуктивності й прийняті правила безпеки. І звичайно, воно повинне бути максимально автоматизоване – зокрема, автоматично адаптуватися до змін у конфігурації і якості каналів доступу.

У першу чергу варто звертати увагу на наявність таких функцій, як автоматичний інтелектуальний вибір шляхи, при якому враховується інформація про маршрут (затримка, джиттер, відсоток загублених пакетів і т.п.). Це дозволяє вибрати найкращий маршрут для сервісів SaaS, голосових застосунків VoIP і іншого високочитичного трафіку. Якщо характеристики основного маршруту погіршуються до значення нижче заданого порога, то рішення SD-WAN повинне здійснити автоматичне перемикання на найкращий доступний канал без зниження продуктивності застосунки. Визначення порогів для SLA часом виявляється досить трудомістким завданням, відповідно, рекомендується вибирати рішення, які дозволяють легко конфігурувати рівні контролю якості з'єднань SLA.

Аналогічно, будь-яке ефективне рішення SD-WAN повинне бути незалежно від транспорту й типів каналів доступу. Це припускає не тільки підтримку безлічі протоколів і середовищ передачі даних (Ethernet, 3G/4G, VPN і т.п.), але й можливість використання декількох з'єднань одночасно в режимі балансування трафіку між ними.

Централізовані надання, моніторинг і керування

Одне з відмітних переваг SD-WAN – можливість автоматичного віддаленого розгортання й керування. Однак відправлення повністю зконфігурованих і підготовлених до розгортання пристроїв у віддалений офіс сполучені з певними ризиками. І навіть після того, як кінцеві пристрої розгорнуті, для керування функціями оптимізації WAN-з'єднань і функціями захисти необхідні звичайно дві окремі консолі керування. Такий поділ операцій по адмініструванню й захисту мережі не тільки вимагає додаткових зусиль із боку ІТ-персоналу, але й утрудняє можливість зв'язати такі традиційні питання, як продуктивність і функціональність мережі, з результатами аналізу безпеки й

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		33

даних. Але в середовищі SD-WAN такі звичайно розділені функції повинні бути доступні спільно.

І безпека, і SD-WAN припускають моніторинг і аналіз безлічі складних застосунків, тому надзвичайно важлива наявність єдиної панелі керування, що забезпечує високорівневе подання результатів моніторингу поряд з можливістю деталізації інформації з окремих об'єктів і подій.

При оцінці рішень SD-WAN також необхідно брати до уваги такі моменти, як можливість автоматичного розгортання, що полегшує налаштування й моніторинг фізичних і логічних мережних топологій, завантаженості каналів і поведіння мережних пристроїв і застосунків. В адміністратора повинні бути необхідні інструменти, за допомогою яких він міг би без праці оновлювати й поширювати корпоративні правила мережної взаємодії й політик безпеки на всі площадки. Наявність централізованих інструментів керування, конфігурування й моніторингу як для WAN-мереж, так і для безпеки, які вбудовані безпосередньо в середовище SD WAN, дозволить підвищити ефективність і результативність керування й при цьому значно скоротити витрати на впровадження такого рішення й керування їм.

На закінчення необхідно відзначити, що рішення SD-WAN уже довели свою здатність підвищити продуктивність мережі й поліпшити умови роботи користувачів у рамках розподіленої мережі при помірних витратах. Розгортання рішення, що не включає повністю інтегровані засоби безпеки, піддає вашу мережу непотрібному ризику.

3.2 Розробка структурної схеми

Аналітики Gartner виділяють дві ключові проблеми, які можуть піддати ризику інформаційні активи користувачів SD-WAN.

По-перше, точка застосування зусиль по забезпеченню безпеки зміщується із центра до периферії. Традиційні способи побудови глобальної комп'ютерної

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		34

мережі звичайно мають на увазі, що підрозділу організації підключені до центрального сервера (або сукупності декількох серверів), через який іде їхню інформаційну взаємодію із зовнішнім середовищем. На цьому сервері функціонують захисні рішення, і він відіграє роль шлюзу, що відмежовує корпоративну обчислювальну мережу від мереж загального користування. Відповідно, погрозам ззовні піддається в основному цей центральний пристрій, у той час як інші вузли, що перебувають за брандмауером організації, вирішують тільки завдання боротьби з погрозами зсередини.

У випадку з SD-WAN розклад іншої: кожний підрозділ одержує можливість зв'язуватися з інтернетом прямо й самостійно. Це рятує мережа від «вузьких місць» і підвищує продуктивність, але в той же час означає, що умовній філії прийде протистояти всьому спектру зовнішніх погроз індивідуально. Грубо говорячи, якщо у звичайної WAN можна було приділити основна увага захисту декількох точок, то тут прийде обороняти весь периметр. Таким чином, будь-який підрозділ може стати вхідними воротами для порушення режиму безпеки, оскільки вся множина шкідливих факторів – від мережних хробаків до цільових атак – впливає на всі філії одночасно.

По-друге, усього лише 10% виробників продуктів SD-WAN має яке-небудь відношення до розробки систем захисту. Вони забезпечують базовий рівень безпеки за рахунок використання засобів шифрування, однак більше складні технології боротьби з погрозами прийде шукати в сторонніх постачальників, які займаються цим професійно. Якщо мережа організації не передає критично важливих відомостей, то убудованих можливостей буде досить; однак якщо передбачувані наслідки компрометації даних небезпечні, то покладатися на базовий захист буде проявом надмірного оптимізму.

Втім, сторонні продукти теж можуть забезпечувати захист аж ніяк не на всіх рівнях мережної моделі, що мають значення для безпеки SD-WAN. Якщо вони розроблялися з упором на особливості традиційної глобальної комп'ютерної мережі, те, мабуть, специфіка програмно обумовлених мереж може бути не

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		35

повною мірою врахована їхніми творцями. Наприклад, маршрутизатори звичайно містять убудований брандмауер, однак є ймовірність, що його функціональність виявиться недостатньою (хоча безсумнівно, що зайвої вона не буде, і в оглядових статтях про безпеку SD-WAN радять прибїгати й до таких засобів, якщо немає нічого іншого).

До речі, говорячи про брандмауерів, варто мати на увазі, що традиційні мережні екрани в принципі захищають SD-WAN не дуже успішно. У вважають, що програмно обумовлені мережі мають потребу в брандмауері нового покоління (NGFW, Next Generation Firewall). Можливості такого продукту повинні бути досить широкі, щоб перевіряти зашифрований трафік, блокувати доступ до відомих сайтів зі шкідливим умістом, підтримувати високопродуктивне забезпечення безпеки VPN-з'єднань через архітектуру IPsec і т.д. Відповідно, уже на етапі планування переходу на програмно обумовлену мережу необхідно задуматися про те, яку стратегію нейтралізації погроз варто вибрати й у якому ступені убудовані засоби захисту SD-WAN будуть достатні для потреб організації.

Як вибрати підходяще рішення?

Невеликі підрозділи, які не зіштовхуються з необхідністю обробляти критично важливі інформаційні активи, можуть обійтися варіантами SD-WAN з убудованим брандмауером (на зразок роутерного) або вдатися до допомоги хмарного постачальника, що надає безпеку як послугу (SECaaS). Таке рішення малозатратно економічно й забезпечує прийнятний рівень захисту з обліком того, що інформація, яка обороняється, не представляє великої небезпеки з погляду її можливої компрометації.

Для великих філій, що працюють із конфіденційними даними, підійдуть варіанти підвищеної надійності: брандмауер з убудованою функціональністю SD-WAN або сполучення програмно обумовленої мережі з мережним екраном нового покоління від стороннього постачальника. Таке рішення дорожче, а в деяких

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		36

випадках ще й накладає обмеження на спектр можливостей SD-WAN, однак добратися до переданої через нього інформації сутужніше.

Очевидно, що жодна із цих архітектур не ідеальна. Особливо це стосується другого випадку, коли великої організації де-факто доводиться вибирати між звуженням можливостей SD-WAN і одночасним обслуговуванням декількох різних рішень. З обліком даних Gartner, про які говорилося раніше, складається не занадто зручна ситуація: якщо підприємство бажає одержати всі можливі вигоди від користування SD-WAN і при цьому повинне забезпечити найбільш міцний захист інформації, то воно практично неминуче буде розвертати захисне рішення одного виробника поверх програмно обумовленої мережі іншого виробника: адже, як нам уже відомо, 90% розроблювачів SD-WAN не займається безпекою професійно. У підсумку, навіть якщо не виникне проблем сумісності, працезатрати на обслуговування цієї двоповерхової конструкції однаково помножаться.

Ідеологія полягає в тому, що програмно обумовлена мережа й система її захисти повинні являти собою одне ціле. Саме цей підхід реалізований в апаратних і віртуальних пристроях, які є одночасно мережним устаткуванням і брандмауерами нового покоління. З одного боку, функціональність SD-WAN є не надбудовою або доповненням до мережного екрана, а повноцінним рішенням, що забезпечує доступ до всіх достоїнств цієї технології. З іншого боку, відпадає потреба в багаторівневій підтримці: управляючи SD-WAN, адміністратор одночасно контролює й систему безпеки.

Дійсно, якщо в організації впроваджується програмно обумовлений зв'язок, і передній край боротьби з погрозами виявляється на периферії, те логічно й ефективно буде прагнути до того, щоб кожний маршрутизатор, з'єднаний з мережами загального користування, не тільки забезпечував оптимізацію за рахунок SD-WAN, але й сам же виступав як багатофункціональний засіб захисту, що заздалегідь пристосований до специфіки його роботи й розв'язуваних завдань.

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		37

Наприклад, якщо мережне встаткування вмiє займатися захистом даних (у тому числі на підвищеному рівні), то й кожний такий пристрій де-факто стає джерелом поширення політики безпеки організації – особливо з обліком того, що центр у будь-який момент може розіслати зміни конфігурації по всіх вузлах мережі. Зокрема, це дозволяє не турбуватися із приводу ідеології BYOD («принось свій власний пристрій»), тому що можна довірити системі автоматичну обробку кожного нового користувача й бути впевненим, що його присутність не створить інформаційних ризиків. Будь це клієнт гостьового Wi-Fi або співробітник з певним рівнем допуску, політика безпеки виявиться дотримана. Одночасно із цим організації будуть доступні переваги SD-WAN начебто передачі більших обсягів даних по каналах загального користування – знову ж без нестатку побоюватися за їхню конфіденційність.

Крім спрощення структури й нейтралізації проблем сумісності, цей підхід зручний для аналізу інцидентів і прийняття рішень, оскільки огляд реєструємих кожним пристроєм подій дає можливість узагальнити їх у єдину картину, а не досліджувати кожне з них індивідуально.

Хоча таке рішення особливо зручно в якості здобування індивідуально й що налаштовується, ним можна скористатися й у хмарі на умовах оренди: воно доступно користувачам великих хмарних провайдерів на зразок Amazon.

Захищені мережні контролери SD-WAN

Для того щоб об'єднати мережне встаткування із засобами оптимізації трафіку й системами розширеної безпеки, можна скористатися одним з рішень, які доступні в трьох виконаннях: апаратному, віртуальному й хмарному. У кожному випадку існує можливість вибрати варіант, функціональність якого відповідає бажаним показникам роботи корпоративної мережі

Апаратний продукт забезпечує зв'язок підрозділу з інтернетом, у тому числі за допомогою мобільного трафіку (3G/4G), дозволяє користуватися перевагами SD-WAN і взаємодіє з іншими елементами захисту корпоративної мережі – наприклад, програмним забезпеченням для робочих комп'ютерів або

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		38

точок доступу, – а також дає можливість здійснювати централізоване керування за допомогою інструментів

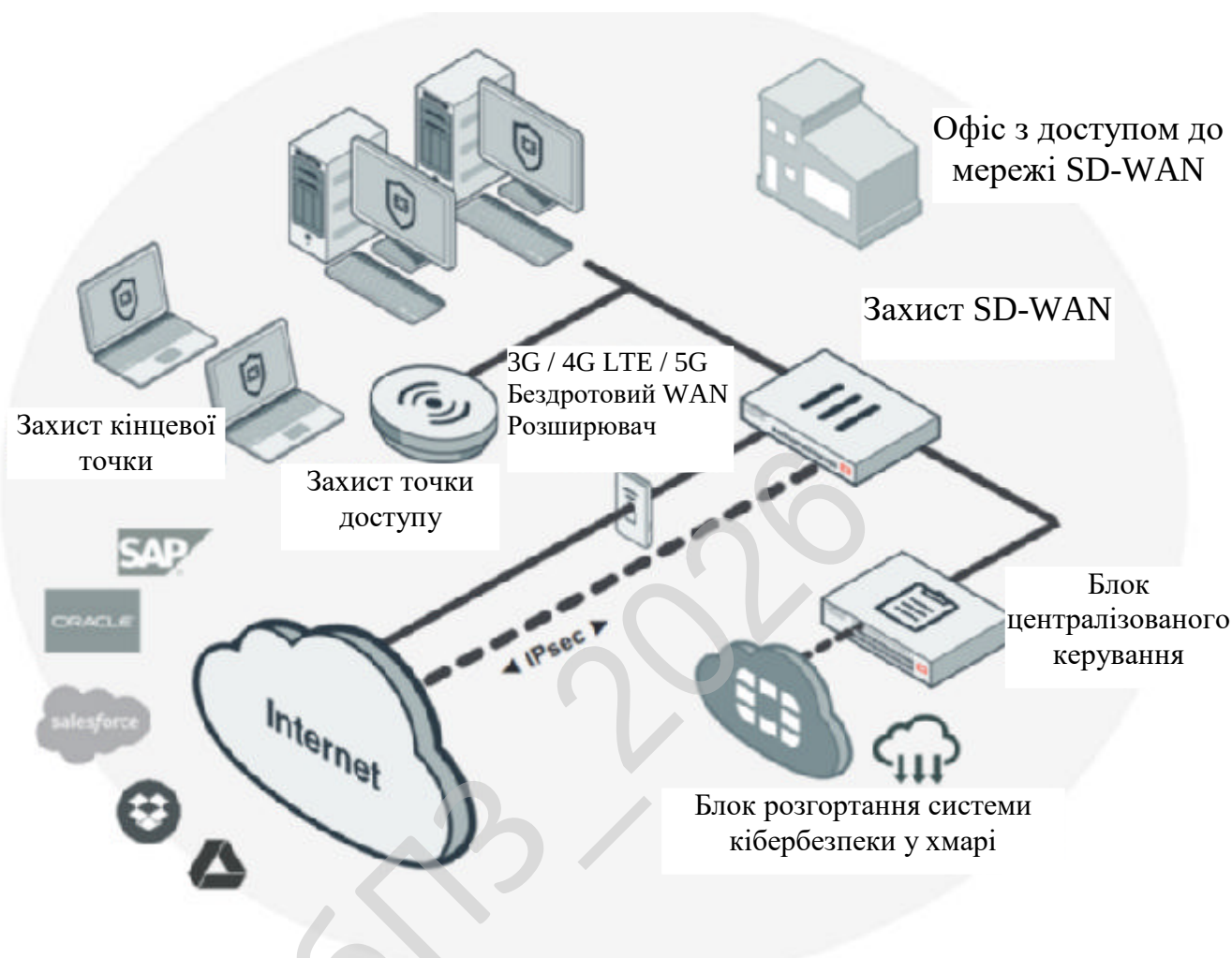


Рисунок 3.1 – Структурна схема системи

У свою чергу, сімейство віртуальних машин забезпечує аналогічні можливості для програмно обумовлених датацентрів. Його представники пристосовані до специфіки віртуалізованих середовищ і враховують типові завдання, які необхідно вирішувати для успішної інтеграції в них – наприклад, підтримують прискорене розгортання.

Всі ці продукти надають доступ до ряду служб безпеки. До їхнього числа ставляться наступні сервіси:

- Контроль застосунків на основі політик дозволу, заборони або обмеження доступу до застосунків і їхніх груп.
- Веб-фільтрація для блокування доступу до відомих шкідливих ресурсів.
- Хмарна пісочниця, що дозволяє визначати ще невідомі шкідливі програми шляхом динамічного аналізу.
- Антивірус.
- Система запобігання вторгнень.

Впроваджуючи SD-WAN з метою оптимізувати фінансові й трудові витрати організації, важливо завчасно вжити заходів для того, щоб перехід на нову технологію не привів до ще більших витрат – або на компенсацію збитку від реалізації інформаційних ризиків, або на обслуговування мережі й охорону її периметра від погроз. Якщо компанія працює з важливими даними, безпека яких критична, то доцільно орієнтуватися на пошук такого рішення, що дозволить скористатися всіма перевагами SD-WAN і одночасно забезпечити належний захист інформації без зайвих складностей у розгортанні й підтримці. Відповідно, логічною буде орієнтація на впровадження таких мережних рішень, які максимально прості конструктивно, але в той же час характеризуються професійним підходом до протидії погрозам. Іншими словами, важливо, щоб програмно обумовлена мережа була інтегрована з багатофункціональною й високопродуктивною системою безпеки, а також щоб ця інтеграція була настільки тісною, наскільки можливо. Тоді організація зможе, з одного боку, одержати всю можливу вигоду від користування SD-WAN, а з іншого боку, урегулювати ризики, сполучені з передачею даних по мережах загального користування й із прямим підключенням кожного підрозділу до інтернету. Мережні контролери SD-WAN, об'єднані із брандмауером нового покоління, є одним із прикладів того, як виробник може перебороти ряд недоліків існуючих архітектур, запропонувавши єдине й цільне рішення. Якщо такий розроблювач

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		40

здатний забезпечити повноту функцій програмно обумовленої мережі й при цьому досить компетентний, щоб створити якісну систему захисту, то його продукт буде економічний, надійний і універсальний – чим, властиво, і обумовлена привабливість подібного підходу для тих організацій, які не схильні шукати компроміси між зниженням витрат і безпекою даних.

3.3 Розробка функціональної схеми

На рисунку 3.2 зображена функціональна схема системи. Вона складається з наступних блоків:

- Головне вікно програмного забезпечення системи захищеної і адаптованої мережі SD-WAN.
- Міжмережевий екран.
- Блок контролю застосунків на основі політик дозволу, заборони або обмеження доступу до застосунків і їхніх груп.
- Блок веб-фільтрації для блокування доступу до відомих шкідливих ресурсів.
- Хмарна пісочниця, що дозволяє визначати ще невідомі шкідливі програми шляхом динамічного аналізу.
- Антивірус.
- Система запобігання вторгнень.

У багатьох пристроях для захищеної і адаптованої мережі SD-WAN, наприклад інтегрованих маршрутизаторах, часто є багатфункціональні програмні міжмережні екрани. Такі міжмережні екрани звичайно реалізують трансляцію мережних адрес (NAT), динамічний аналіз пакетів (SPI), а також фільтрацію по IP-адресах, застосунках і веб-сайтах. Додатково вони підтримують функції DMZ.



Рисунок 3.2 – Функціональна схема системи

Інтегрований маршрутизатор дозволяє налаштувати примітивну DMZ для доступу до внутрішнього сервера з вузлів за межами мережі. Для цього сервер повинен мати статичну IP-адресу, що вказується в конфігурації DMZ. Інтегрований маршрутизатор ізолює трафік, що пересилається на зазначений IP-адрес. Цей трафік пропускається тільки на той порт комутатора, до якого підключений сервер. На всі інші вузли мережі SD-WAN як і раніше поширюється захист міжмережного екрану.

При активації DMZ у найпростішому виді зовнішні вузли одержують доступ до всіх портів сервера мережі SD-WAN, наприклад 80 (HTTP), 21 (FTP) і 110 (POP3 для електронної пошти). Функція переадресації портів дозволяє налаштувати більш строгу конфігурацію DMZ. У цьому випадку вказуються порти, які повинні бути доступні на сервері. Пропускається тільки трафік, спрямований на ці порти. Весь інший трафік виключається. Бездротова точка доступу в складі інтегрованого маршрутизатора часто вважається частиною внутрішньої мережі. Необхідно усвідомлювати, що при роботі точки доступу в незахищеному режимі всі користувачі, що підключилися до неї, одержують доступ до внутрішньої захищеної мережі без проходження міжмережного екрану. Зловмисники можуть у такий спосіб одержати доступ до внутрішньої мережі SD-WAN, минаючи всі засоби захисту. Розглянувши усі блоки функціональної схеми перейдемо до розгляду діаграми взаємодії процесів, які відбуваються у системі.

3.4 Розробка діаграми процесів

Розглянемо розроблену діаграму процесів яка зображена на рисунку 3.3. Основна будова діаграми процесів полягає у графічному представленні складу сукупностей даних, що характеризуються як співвідношення різних частин кожної з сукупностей. Склад статистичної сукупності графічно може бути представлений як за допомогою абсолютних, так і відносних показників. Графічне зображення складу сукупності по абсолютними і відносними показниками сприяє проведенню більш глибокого аналізу і дозволяє проводити аналіз системи. Діаграма взаємодії процесів використовується для візуалізації процесів обробки даних (структурне проектування). Для розробника вважається звичним спочатку креслити діаграму взаємодії процесів даних рівня контексту, завдяки чому буде показано взаємодію системи.

Ця діаграма в подальшому підлягає уточненню шляхом деталізації процесів та потоків даних з метою показати систему що розробляється.

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		43

При детальному її розгляді можна побачити як саме проходить взаємодія у розробленій системі. Використовується модель проектування, графічне представлення «потоків» даних в інформаційній системі.

Діаграми потоків даних містять чотири типи елементів:

- Зовнішні по відношенню до системи сутності.
- Потоки даних між елементами трьох попередніх типів.
- Процеси які являють собою трансформацію даних в рамках описуваної системи.
- Сховища даних (репозиторії).

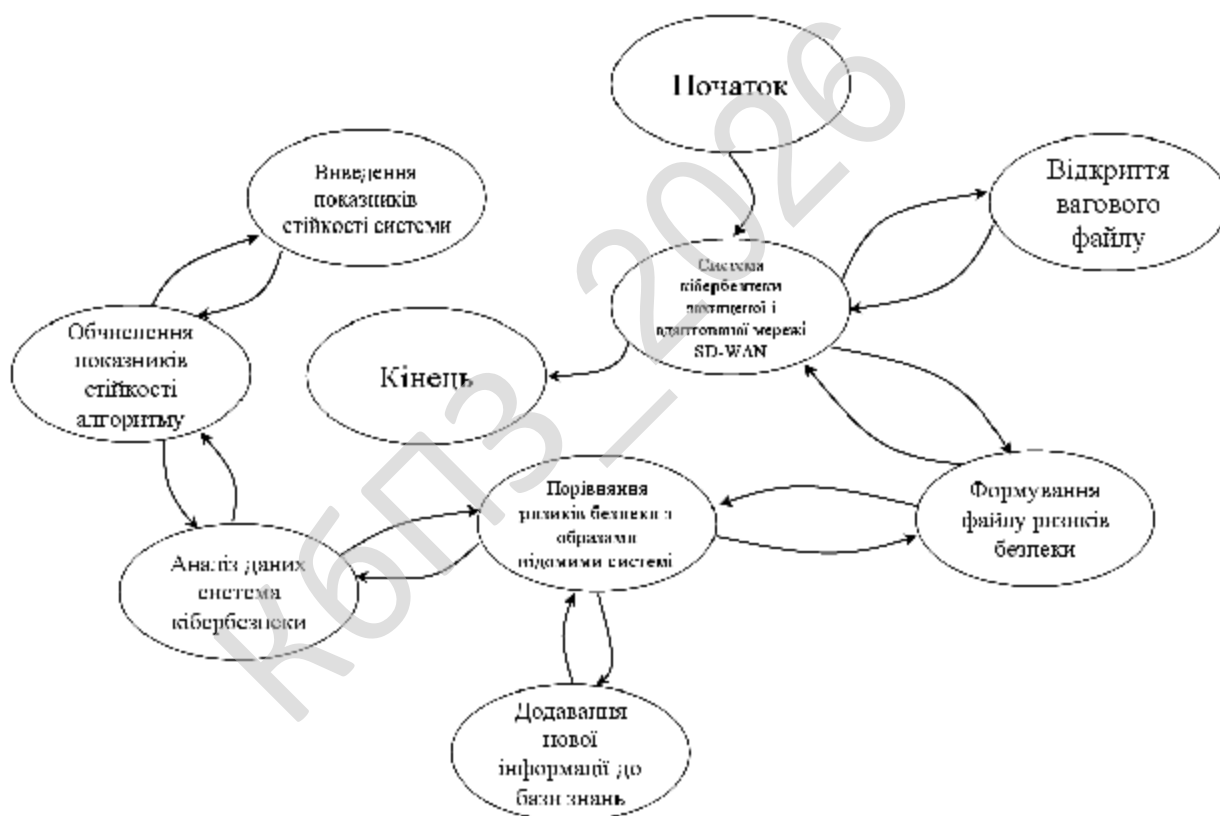


Рисунок 3.3 – Діаграма взаємодії процесів

Таким чином, розглянувши опис системи, структурну, функціональну схеми системи, та діаграму взаємодії процесів перейдемо до опису блок-схем основної програми, та підпрограм, які використовуються, для реалізації системи.

4 РЕАЛІЗАЦІЯ ПРОЕКТУ. РОЗРАХУНКИ І ЕКСПЕРИМЕНТАЛЬНІ ДАНІ, ЩО ПІДТВЕРДЖУЮТЬ ПРАВИЛЬНІСТЬ ПРОЕКТНИХ РІШЕНЬ

4.1 Блок-схеми та опис алгоритмів функціонування системи

Розглянемо реалізацію бакалаврської дипломної роботи. Були проведені розрахунки і підібрані набори тестових даних для перевірки правильності реалізації проектних рішень. Було створено блок-схеми роботи системи.

Перед їх розглядом необхідно провести роз'яснення який саме тип блок-схем використовується. Блок-схема це представлення задачі для її аналізу або розв'язування за допомогою спеціальних символів (геометричних образів), які позначають такі елементи, як операції, потік, дані тощо.

Блок вхідних та вихідних даних прийнято позначати паралелограмом, блок обчислень (обробки) даних – прямокутником, блок прийняття рішень – ромбом, еліпсом – початок та кінець алгоритму.

У інформаційних технологіях функціональна схема складається з функціональних блоків, які являють собою конструктивно відособлені частини (елементи або пристрої) автоматичних систем, які виконують певні функції. Функціональні блоки на схемі позначають прямокутниками, всередині яких надписують їх найменування відповідно до функцій, що виконуються. Зв'язки між функціональними блоками (внутрішні впливи) позначаються лініями зі стрілками, які вказують напрям впливів.

Функціональні схеми можуть виконуватися в укрупненому і розгорненому вигляді. У першому випадку на схемі зображають найважливіші блоки системи і зв'язки між ними.

У другому варіанті схема відображається більш детально, що полегшує її читання та ілюструє принцип роботи.

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		45

Основні елементи схем алгоритму це термінатор, процес, рішення, зумовлений процес (підпрограма), дані та з'єднувач. Термінатор це елемент відображає вхід із зовнішнього середовища або вихід з неї (найчастіше застосування – початок і кінець програми). Всередині фігури записується відповідна дія.

Процес це виконання однієї або кількох операцій, обробка даних будь-якого виду (зміна значення даних, форми подання, розташування). Всередині фігури записують безпосередньо самі операції. Рішення це показує рішення або функцію перемикального типу з одним входом і двома або більше альтернативними виходами, з яких тільки один може бути обраний після обчислення умов, визначених всередині цього елемента.

Вхід в елемент позначається лінією, що входить зазвичай у верхню вершину елемента. Якщо виходів два чи три то зазвичай кожен вихід позначається лінією, що виходить з решти вершин (бічних і нижній). Якщо виходів більше трьох, то їх слід показувати однією лінією, що виходить з вершини (частіше нижній) елемента, яка потім розгалужується.

Відповідні результати обчислень можуть записуватися поруч з лініями, що відображають ці шляхи. Зумовлений процес (підпрограма) це символ відображає виконання процесу, що складається з однієї або кількох операцій, що визначені в іншому місці програми (у підпрограмі, модулі). Всередині символу записується назва процесу і передані в нього дані.

Дані це перетворення у форму, придатну для обробки (введення) або відображення результатів обробки (виведення). Цей символ не визначає носія даних (для вказівки типу носія даних використовуються специфічні символи). З'єднувач це символ відображає вихід в частину схеми і вхід з іншої частини цієї схеми.

Використовується для обриву лінії та продовження її в іншому місці (приклад: поділ блок-схеми, що не поміщається на листі). Відповідні сполучні символи повинні мати одне (при тому унікальне) позначення.

Блок-схеми показують весь процес роботи системи з підсистемами та частково доказують правильність вибраних проектних рішень. Тому від точності і детальної блок-схеми залежить результат всієї програми.

При виборі початкової точки відліку при побудові схем було враховано, що виходячи з вибору мови програмування і інших технічних засобів, програма буде об'єктно-орієнтована що вимагає високого рівня декомпозиції задач на класи.

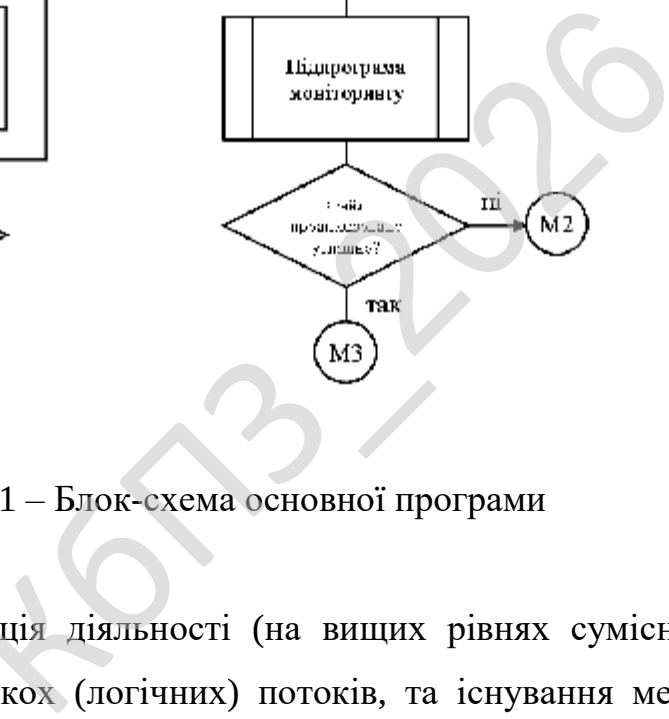
На рисунку 4.1 зображена основна блок-схема програми, на рисунку 4.2 зображено роботу підпрограми.

З яких видно що робота основної програми складається з початкових етапів ініціалізації ПЗ, перевірки наявності ресурсів системи, блоку початку основного циклу з чеканням запиту від користувача в якому відбувається виклик підсистеми та останньої стадії – перевірка поточного стану з завершенням роботи розробленого ПЗ. При роботі підпрограми виконується основний функціонал системи з циклічними послідовностями, перевіркою поточного стану та поверненням в основну програму прапорів стану виконання.

Було використано наступні підходи UML: діаграма діяльності (діаграми поведінки типу); діаграма прецедентів (діаграми поведінки типу).

Діаграма діяльності. Це візуальне представлення графу діяльностей. Граф діяльностей є різновидом графу станів скінченного автомату, вершинами якого є певні дії, а переходи відбуваються по завершенню дій. Дія є фундаментальною одиницею визначення поведінки в специфікації. Дія отримує множину вхідних сигналів, та перетворює їх на множину вихідних сигналів. Одна із цих множин, або обидві водночас, можуть бути порожніми. Виконання дії відповідає виконанню окремої дії. Подібно до цього, виконання діяльності є виконанням окремої діяльності, буквально, включно із виконанням тих дій, що містяться в діяльності. Кожна дія в діяльності може виконуватись один, два, або більше разів під час одного виконання діяльності. Щонайменше, дії мають отримувати дані, перетворювати їх та тестувати, деякі дії можуть вимагати певної послідовності.

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		47



1 – Блок-схема основної програми

Діаграма прецедентів це діаграма, на якій зображено відношення між акторами та прецедентами в системі. Також, перекладається як діаграма варіантів використання.

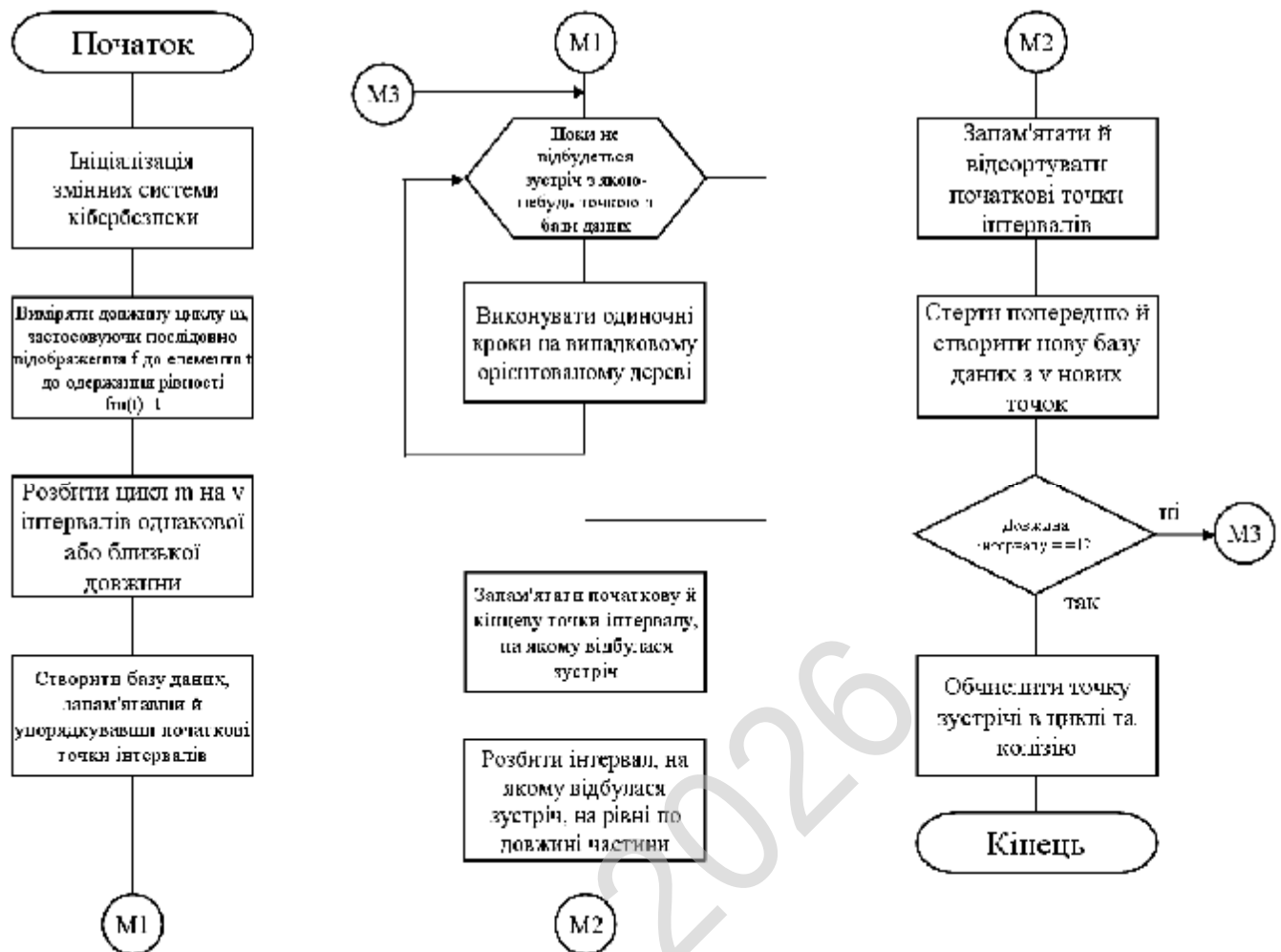


Рисунок 4.2 – Блок-схема роботи підпрограми

Діаграма прецедентів є графом, що складається з множини акторів, прецедентів (варіантів використання) обмежених границею системи (прямокутник), асоціацій між акторами та прецедентами, відношень серед прецедентів, та відношень узагальнення між акторами. Діаграми прецедентів відображають елементи моделі варіантів використання.

Суть даної діаграми полягає в наступному: проєктована система представляється у вигляді безлічі сутностей чи акторів, що взаємодіють із системою за допомогою так званих варіантів використання. Варіант використання (use case) використовують для описання послуг, які система надає актору. Іншими словами, кожен варіант використання визначає деякий набір дій, який виконує система при діалозі з актором.

При цьому нічого не говориться про те, яким чином буде реалізована взаємодія акторів із системою.

У мові UML є кілька стандартних видів відношень між акторами і варіантами використання:

- асоціації (association relationship);
- включення (include relationship);
- розширення (extend relationship);
- узагальнення (generalization relationship).

При цьому загальні властивості варіантів використання можуть бути представлені трьома різними способами, а саме – за допомогою відношень включення, розширення і узагальнення.

Відношення асоціації – одне з фундаментальних понять у мові UML і в тій чи іншій мірі використовується при побудові всіх графічних моделей систем у формі канонічних діаграм.

Включення (include) у мові UML – це різновид відношення залежності між базовим варіантом використання і його спеціальним випадком. При цьому відношенням залежності (dependency) є таке відношення між двома елементами моделі, при якому зміна одного елемента (незалежного) приводить до зміни іншого елемента (залежного).

Відношення розширення (extend) визначає взаємозв'язок базового варіанта використання з іншим варіантом використання, функціональна поведінка якого задіюється базовим не завжди, а тільки при виконанні додаткових умов.

Система керування базами даних (СКБД, Database Management System, DBMS) – набір взаємопов'язаних даних (база даних) і програм для доступу до цих даних. Надає можливості створення, збереження, оновлення та пошуку інформації в базах даних з контролем доступу до даних.

Першим поколінням СКБД прийнято вважати ієрархічні й мережеві системи. Ці системи отримали широке поширення в 1970-х роках, а першою комерційною системою цього типу була система IMS компанії IBM.

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		50

У 1980-х роках ці системи були витіснені системами другого покоління – повсюдно використовуваними і донині реляційними СКБД.

У цих системах використовувалися непроцедурні мови управління даними (SQL) і передбачався значний ступінь незалежності даних. Реляційні системи внесли значні удосконалення в управління даними: графічний користувацький інтерфейс (GUI), клієнт-серверні застосунки, розподілені бази даних, паралельний пошук даних та інтелектуальний аналіз даних.

Але вже до кінця 1980-х років існуюча тоді реляційна модель перестала задовольняти розробників в силу низки обмежень.

Відповіддю на зростаючу складність програм баз даних стали два нових напрямки розвитку СКБД: об'єктно-орієнтовані СКБД і об'єктно-реляційні СКБД.

У 1991 був утворений консорціум ODMG, основною метою якого стало вироблення промислового стандарту об'єктно-орієнтованих баз даних. Між 1993 та 2001 роками ODMG опублікувала п'ять ревізій своїх специфікацій. Остання версія стандарту має індекс 3.0, після чого група розпустилася. До кінця 1990-х існувало близько десяти компаній, що виробляли комерційні продукти, що позиціонуються на ринку як ООСКБД.

Найбільш відомими системами даного класу стали Objectivity, Versant виробництва однойменних компаній, а також СКБД Jasmine, випущена компанією СА. Незважаючи на переваги, що дозволяють ефективніше вирішувати певний ряд завдань, об'єктно-орієнтовані системи так і не змогли завоювати значущу частку ринку СКБД, залишившись «нішевим» продуктом.

Постачальниками традиційних реляційних СКБД також була проведена значна робота з об'єднання об'єктно-орієнтованих і реляційних систем. Розробники постаралися розширити мову SQL, щоб включити в неї концепції об'єктно-орієнтованого підходу, зберігаючи переваги реляційної моделі (об'єктні розширення мови SQL були зафіксовані в стандарті SQL:1999).

Основний принцип – це еволюційний розвиток можливостей СКБД без поломки попередніх підходів та зі збереженням наступності з системами попереднього покоління.

Поняття СКБД третього покоління, якими, власне кажучи, і є об'єктно-реляційні СКБД, з'явилося після опублікування групою відомих фахівців в області баз даних «Маніфесту систем баз даних третього покоління». Основні принципи СКБД третього покоління, позначені в маніфесті:

Крім традиційних послуг з управління даними, СКБД третього покоління повинні забезпечити підтримку розвиненіших структур об'єктів і правил. Розвинутіша структура об'єктів характеризує засоби, необхідні для зберігання і маніпулювання нетрадиційними елементами даних (тексти, просторові дані, мультимедіа).

СКБД третього покоління повинні включити в себе СКБД другого покоління. Системи другого покоління внесли вирішальний вклад у двох областях – непроцедурний доступ за допомогою мови запитів SQL і незалежність даних. Ці досягнення обов'язково повинні враховуватися в системах третього покоління.

СКБД третього покоління повинні бути відкриті для інших підсистем. Це включає оснащення різноманітними інструментами підтримки прийняття рішень, доступом з багатьох мов програмування, інтерфейсами до існуючих популярних систем і бізнес-застосунків, можливістю запуску програм з бази даних на іншій машині і розподілені СКБД. Весь набір інструментів і СКБД має ефективно функціонувати на різноманітних апаратних платформах з різними операційними системами.

Крім того, СКБД, що розраховує на широку сферу застосування, повинна бути оснащена мовою четвертого покоління (4GL).

У середині 1990 років було лише кілька дослідних прототипів СКБД, які поєднали найкращі риси реляційних і об'єктно-орієнтованих СКБД. Першим комерційним продуктом, якому були властиві об'єктно-реляційні риси, став

Universal Server компанії Informix (згодом була поглинена IBM). В даний час більшість цих ідей вже втілено в реальних комерційних рішеннях, в тому числі і в продуктах основних постачальників СКБД (Oracle Database і IBM DB2).

Розвиток індустрії систем керування базами даних базується на значних фундаментальних наукових дослідженнях. Найчастіше, між самими дослідженнями та їхньою конкретною реалізацією в прикладних рішеннях минають роки, а іноді й десятиліття.

Роботу в області управління даними проводять як університетські дослідницькі групи (MIT, Berkeley), так і центри розробок основних постачальників СКБД (Oracle, IBM, Microsoft). Інвестування в управління даними – це довгострокове, і разом з тим, вигідне вкладення коштів. В даний час дослідники мають у своєму розпорядженні засоби, що дозволяють ефективно реалізувати найскладніші запити, що маніпулюють терабайтами й петабайтами різних даних.

Основними тенденціями, які дали привід для проведення різних масштабних досліджень в області баз даних стали:

Експонентний ріст даних. Обсяг даних, у тому числі синтетичних, що генеруються автоматизованими системами, значно зріс. Збільшилося і число прикладних областей, в яких вимагається обробка великих обсягів даних. До таких областей тепер відносяться не тільки традиційні корпоративні програми, пошук у веб, але також і наукові дослідження, обробка природних мов, аналіз соціальних мереж тощо.

Значне ускладнення структур використовуваних даних. Прості види даних у вигляді чисел і символьних рядків стали доповнятися численною мультимедійною інформацією, просторовими, процедурними даними та великою кількістю інших складних форматів.

Широке поширення дешевих високопродуктивних апаратних засобів. Щорічно ми спостерігаємо зростання обчислювальних можливостей

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		53

мікропроцесорів, збільшення ємності і зниження вартості доступних і зручних в експлуатації пристроїв дискової оперативної пам'яті.

Активний розвиток засобів комунікації та «всесвітньої павутини» World Wide Web. WWW стає єдиним інформаційним середовищем, що пронизує весь світ і об'єднує величезне число користувачів та електронних пристроїв.

Поява нових важливих областей застосування СКБД. У першу чергу, це пов'язано з інтелектуальним аналізом даних, сховищами даних, а останнім часом – з паралельними обчисленнями і хмарними технологіями.

Основні характеристики СКБД

1. Контроль за надлишковістю даних.
2. Несуперечливість даних.
3. Підтримка цілісності бази даних (коректність та несуперечливість).
4. Цілісність описується за допомогою обмежень.
5. Незалежність прикладних програм від даних.
6. Спільне використання даних.
7. Підвищений рівень безпеки.

Можливості СКБД

1. Дозволяється створювати БД (здійснюється за допомогою мови визначення даних DDL (Data Definition Language)).

2. Дозволяється додавання, оновлення, видалення та читання інформації з БД (за допомогою мови маніпулювання даними DML, яку часто називають мовою запитів)

3. Можна надавати контрольований доступ до БД за допомогою: Системи забезпечення захисту, яка запобігає несанкціонованому доступу до БД; Системи керування паралельною роботою прикладних програм, яка контролює процеси спільного доступу до БД; Система відновлення – дозволяє відновлювати БД до попереднього несуперечливого стану, що був порушений в результаті збою апаратного або програмного забезпечення.

Основні компоненти середовища СКБД

1. Апаратне забезпечення.
2. Програмне забезпечення.
3. Дані.
4. Процедури – інструкції та правила, які повинні враховуватись при проектуванні та використанні БД.
5. Користувачі: адміністратори даних (керування даними, проектування БД, розробка алгоритмів, процедур) та БД (фізичне проектування, відповідальність за безпеку та цілісність даних); розробники БД; прикладні програмісти; кінцеві користувачі.

Архітектура СКБД

Існує трирівнева система організації СКБД ANSI-SPARC, при якій існує незалежний рівень для ізоляції програми від особливостей представлення даних на нижчому рівні.

Рівні:

1. Зовнішній – представлення БД з точки зору користувача.
2. Концептуальний – узагальнене представлення БД, описує які дані зберігаються в БД і зв'язки між ними. Підтримує зовнішні представлення, підтримується внутрішнім рівнем.
3. Внутрішній – фізичне представлення БД в комп'ютері.

Логічна незалежність – повна захищеність зовнішніх моделей від змін, що вносяться в концептуальну модель.

Фізична незалежність – захищеність концептуальної моделі від змін, які вносяться у внутрішню модель.

PostgreSQL (вимовляється «Пост-грес-К'ю-ель», або «постгрес») об'єктно-реляційна система керування базами даних (СКБД).

Є альтернативою як комерційним СКБД (Oracle Database, Microsoft SQL Server, IBM DB2 та інші), так і СКБД з відкритим кодом (MySQL, Firebird, SQLite).

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		55

Порівняно з іншими проектами з відкритим кодом, такими як Apache, FreeBSD або MySQL, PostgreSQL не контролюється якоюсь однією компанією, її розробка можлива завдяки співпраці багатьох людей та компаній, які хочуть використовувати цю СКБД та впроваджувати у неї найновіші досягнення.

Сервер PostgreSQL написаний на мові C. Зазвичай розповсюджується у вигляді набору текстових файлів із сирцевим кодом. Для інсталяції необхідно відкомпілювати файли на своєму комп'ютері і скопіювати в деякий каталог. Весь процес детально описаний в документації.

PostgreSQL – широко розповсюджена система керування базами даних з відкритим сирцевим кодом. Прототип був розроблений в Каліфорнійському університеті Берклі в 1987 році під назвою POSTGRES, після чого активно розвивався і доповнювався.

В червні 1990 року з'явилась друга версія із переробленою системою правил маніпулювання та роботи з таблицями, у 1991 році – третя версія, із доданою підтримкою одночасної роботи кількох менеджерів збереження, покращеним механізмом запитів і доповненою системою внутрішніх правил. В цей час POSTGRES використовувався для реалізації великих систем, таких як: система аналізу фінансових даних, пакет моніторингу функціональності потоків, база даних відстеження астероїдів, система медичної інформації, кілька географічних систем.

POSTGRES також використовувався як навчальний інструмент в кількох університетах. 1992 року POSTGRES став головною СКБД наукового комп'ютерного проекту Sequoia 2000. 1993 року кількість користувачів подвоїлась. Стало зрозуміло, що для підтримки й подальшого розвитку необхідні великі витрати часу на дослідження баз даних, тому офіційно проект Берклі було зупинено на версії 4.2. 1994 року Andrew Yu і Jolly Chen додали інтерпретатор мови SQL, вдосконалили сирцевий код і виклали в Інтернеті свою реалізацію під назвою Postgres95. 1996 року програмний продукт було перейменовано на PostgreSQL із початковою версією 6.0.

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		56

Подальшою підтримкою й розробкою займається група спеціалістів у галузі баз даних, які добровільно приєднались до цього проекту.

Основні можливості, функції

Функції дозволяють виконувати деякий код безпосередньо сервером бази даних. Ці функції можуть бути написані на SQL, який має деякі примітивні програмні оператори, такі як галуження та цикли. Але гнучкішою буде функція написана на одній із мов програмування, з якими PostgreSQL може працювати. До таких мов належать:

Вбудована мова, яка зветься PL/pgSQL, подібна до процедурної мови PL/SQL компанії Oracle.

Мови розробки сценаріїв: PL/Perl, PL/Python, PL/Tcl, PL/Ruby, PL/sh.

Класичні мови програмування C, C++, Java (за допомогою PL/Java).

Функції можуть виконуватись із привілеями користувача, який її викликав, або із привілеями користувача, який її написав.

Основні можливості, індекси

У PostgreSQL є підтримка індексів наступних типів: B-дерево, хеш, R-дерево, GiST, GIN. При необхідності можна створити нові типи індексів.

Основні можливості, багатоверсійність (MVCC)

PostgreSQL підтримує одночасну модифікацію БД декількома користувачами за допомогою механізму Multiversion Concurrency Control (MVCC). Завдяки цьому виконуються вимоги ACID, і практично відпадає потреба в блокуванні зчитування.

Основні можливості, типи даних

PostgreSQL підтримує великий набір вбудованих типів даних:

1. Числові типи.
2. Цілі.
3. Грошовий тип.
4. Символьні типи довільної довжини.
5. Двійкові типи (включаючи BLOB).

6. Типи «дата/час».
7. Булевий тип.
8. Перерахування.
9. Геометричні примітиви.
10. Мережеві типи.
11. UUID-ідентификатор.
12. XML-дані.
13. JSON-дані.
14. Масиви.
15. OID-типи.

Крім того, користувач може самостійно створювати нові необхідні йому типи та програмувати для них механізми індексування за допомогою GiST.

Основні можливості, об'єкти користувача

PostgreSQL може бути розширено користувачем для власних потреб практично в будь-якому аспекті. Є можливість додавати власні:

1. Перетворення типів.
2. Типи даних.
3. Домени (для користувача типи з самого початку з накладеними обмеженнями).
3. Функції (включаючи агрегатні).
4. Індeksi.
5. Оператори (включаючи перевизначення вже існуючих).

Основні можливості, успадкування

Таблиці можуть успадковувати характеристики та набори полів від інших таблиць (батьківських). При цьому дані, які додаються до породженої таблиці, автоматично будуть брати участь (якщо це не вказано окремо) в запитах до батьківської таблиці. Цей функціонал в поточний час не є повністю завершеним. Однак він достатній для практичного використання.

Основні можливості, тригери

Тригери визначаються як функції, що ініціюються DML-операціями. Наприклад, операція INSERT може запускати тригер, що перевіряє доданий запис на відповідність певним умовам. Тригери можна писати різними мовами програмування. Вони пов'язані з визначеною таблицею. Множинні тригери виконуються в алфавітному порядку.

Інші можливості

1. Дотримання принципів ACID.
2. Відповідність стандартам ANSI SQL-92 і SQL-99.
3. Підтримка запитів з OUTER JOIN, UNION, UNION ALL, EXCEPT і під запитів.
4. Послідовності.
5. Контроль цілісності.
6. Реплікація.
7. Загальні табличні вирази й рекурсивні запити.
8. Аналітичні функції.
9. Підтримка Unicode (UTF-8).
10. Підтримка регулярних виразів у стилі Perl.
11. Вбудована підтримка SSL і Kerberos.
12. Протокол поділюваних блокувань.
13. Завантажувані розширення, підтримують SHA1, MD5, XML і іншу функціональність (API відкритий).
14. Засоби для генерації сумісного з іншими системами SQL-коду та імпорту з інших систем.

Надійність

Згідно з результатами автоматизованого дослідження різного ПЗ на предмет помилок, у вихідному коді PostgreSQL було знайдено 20 проблемних місць на 775 000 рядків вихідного коду (в середньому, одна помилка на 39 000 рядків коду). Для порівняння:

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		59

1. MySQL – 97 проблем, одна помилка на 4 000 рядків коду.
2. FreeBSD – 306 проблем, одна помилка на 4 000 рядків коду.
3. Linux (тільки ядро) – 950 проблем, одна помилка на 10 000 рядків коду.

При розробці ПЗ було використано підходи ризик-менеджменту – це система управління ризиками, яка включає в себе стратегію та тактику управління, направлені на досягнення основних цілей. Ефективний ризик-менеджмент включає:

- систему управління;
- систему ідентифікації і вимірювання;
- систему супроводження (моніторингу та контролю).

Сучасна наука представляє ризик як вірогідну подію, в результаті настання якої можуть відбутися позитивні, нейтральні або негативні наслідки. Якщо ризик припускає наявність як позитивних, так і негативних результатів, він відноситься до спекулятивних ризиків. Якщо ж наслідки негативні, або відсутні взагалі, такий ризик іменується чистим.

Мета ризик-менеджменту – підвищення конкурентоспроможності господарюючих суб'єктів за допомогою захисту від реалізації чистих ризиків.

Теорія ризик-менеджменту ґрунтується на трьох базових поняттях: корисності, регресії і диверсифікації.

У 1738 швейцарський математик Даніель Бернуллі доповнив теорію вірогідності методом корисності або привабливості того або іншого результату подій. Ідея Бернуллі полягала в тому, що в процесі ухвалення рішення люди приділяють більше уваги розміру наслідків різних результатів, ніж їх вірогідність.

В кінці XIX століття англійський дослідник Ф. Гальтон запропонував вважати регресію або повернення до середнього значення універсальною статистичною закономірністю. Суть регресії трактувалася ним як повернення явищ до норми з часом. Згодом було доведено, що правило регресії діє в найрізноманітніших ситуаціях, починаючи з азартних ігор та розрахунку

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		60

вірогідності виникнення нещасних випадків, і закінчуючи прогнозуванням коливань економічних циклів.

У 1952 аспірант Університету Чикаго Гарі Марковіц в статті «Диверсифікація вкладень» («Portfolio Selection») математично обґрунтував стратегію диверсифікації інвестиційного портфеля, зокрема, він показав, як шляхом продуманого розподілу вкладень мінімізувати відхилення прибутковості від очікуваного показника. У 1990 Г. Марковіцу присуджена Нобелівська премія за розробку теорії і практики оптимізації портфеля фондових активів.

Етапи ризик-менеджменту

У ризик-менеджменті прийнято виділяти декілька ключових етапів:

- на першому етапі відбувається виявлення ризику з супутньою оцінкою вірогідності його реалізації і масштабу наслідків;
- на другому етапі здійснюється розробка ризик-стратегії з метою зниження вірогідності реалізації ризику і мінімізації можливих негативних наслідків;
- на третьому етапі вибираються методи і інструменти управління виявленим ризиком;
- на четвертому етапі проводиться безпосереднє управління ризиком;
- на завершальному етапі оцінюються досягнуті результати і коректується ризик-стратегія.

За ключовий етап ризик-менеджменту вважається етап вибору методів і інструментів управління ризиком.

Методи і інструментарій ризик-менеджменту

Базовими методами ризик-менеджменту є відмова від ризиків, зниження, передача і ухвалення.

Ризик-інструментарій значно ширший. Він включає політичні, організаційні, правові, економічні, соціальні інструменти, причому ризик-менеджмент як система допускає можливість одночасного застосування декількох методів і інструментів ризик-управління.

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		61

Найбільш часто вживаним інструментом ризик-менеджменту є страхування. Страхування припускає передачу відповідальності за відшкодування передбачуваного збитку сторонній організації (страхової компанії).

Прикладами інших інструментів можуть бути відмова від надмірно ризикової діяльності (метод відмови), профілактика або диверсифікація (метод зниження), аутсорсинг витратних ризикових функцій (метод передачі), формування резервів або запасів (метод ухвалення).

Jira – була використана комерційна система відслідковування помилок, призначена для організації взаємодії з користувачами, хоча в деяких випадках використовується і для управління проектами. Розроблено компанією Atlassian, є одним з двох її основних продуктів (поряд з вікі-системою Confluence). Має веб-інтерфейс.

Назва системи отримано шляхом усічення слова «Gojira» – Японського імені монстра Годзилла, що, в свою чергу, є відсиланням до назви конкуруючого продукту – Bugzilla; створювалася в якості заміни Bugzilla і багато в чому повторює її архітектуру. Система дозволяє працювати з декількома проектами. Для кожного з проектів створює і веде схеми безпеки і схеми оповіщення.

До версії 3.13.5 (включно) розрізнялися редакції Enterprise, Professional і Standard, після – Залишилася тільки редакція Enterprise (для великих організацій).

Система заснована на Java EE і працює на кількох популярних системах управління базами даних і операційних системах.

Основний елемент обліку в системі – завдання (ticket або issue). Завдання містить назву проекту, тему, тип, пріоритет, компоненти і зміст. Завдання може бути розширена додатковими полями (також і нові призначені для користувача поля можуть бути визначені), додатками (наприклад – Фотографіями, скриншотами) або коментарями. Завдання може редагуватися або просто змінювати статус, наприклад, з «відкритий» в «закритий». Які переходи між станами можливі, визначається через налаштовується потік операцій. Будь-які зміни в задачі записуються в журнал.

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		62

Jira має велику кількість можливостей конфігурації: для кожної програми може бути визначений окремий тип завдання з власним workflow, набором статусів, одним або декількома видами уявлення (screens). Крім того, за допомогою так званих «схем» можна визначити для кожного індивідуального Jira-проекту власні права доступу, поведінку і видимість полів і багато іншого.

Завдяки універсальному підходу можна пристосувати Jira для багатьох непрофільних завдань, наприклад, керування вимогами, керування ризиками, аж до реалізації невеликої системи бронювання, автоматизації процесу рекрутингу.

Для інтеграції з зовнішніми системами підтримує інтерфейси SOAP, XML-RPC і REST. Поставляється із засобами інтеграції з такими системами управління версіями, як Subversion, CVS, Git, Clearcase, Team Foundation Server, Mercurial і Perforce.

Існують доповнення, що дозволяють вбудувати Jira в інтегровані середовища розробки, в тому числі Eclipse і IntelliJ IDEA. Перекладена багатьма мовами, включаючи англійську, японську, німецьку, французьку, іспанську.

Для сторонніх розробників надаються кошти розробки розширень системи – плагінів. Розробники розширень можуть викладати плагіни для продажу на спеціальний розділ сайту Atlassian.

Є комерційним продуктом, який може бути ліцензований для роботи на локальному сервері або доступний в якості віддаленого додатки. Ціноутворення залежить від максимального числа користувачів, при цьому близько \$50 за користувача для локального і \$7 на місяць за користувача для віддаленого доступу є типовими цінами.

Для академічних і комерційних клієнтів доступний повний вихідний код під ліцензією розробника.

Для проектів з відкритим вихідним кодом Atlassian надає спеціальну безкоштовну ліцензію при дотриманні наступних правил:

- проект використовує ліцензії, схвалені Open Source Initiative;
- вихідний код проекту доступний для скачування;

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		63

- у проекту є публічно доступна веб-сайт;
- програмне забезпечення від Atlassian є на веб-сайті проекту.

Розглянемо розробку проекту в контрольованому середовищі (PROjects **I**N **C**ontrolled **E**nvironments – **PRINCE**) – це метод управління проектами. Метод включає в себе управління, контроль і організацію проекту. «PRINCE2» – це другий реліз зазначеного методу, що є зареєстрованим торговим знаком, державної торгово–промислової палати (Office of Government Commerce – OGC), незалежного підрозділу державного казначейства Сполученого Королівства.

PRINCE2 походить від більш раннього методу PROMPT та методу проектного управління PRINCE, який був розроблений у 1989 р. Центральним телекомунікаційним та комп'ютерним агентством (Central Computer and Telecommunications Agency – CCTA), як державний стандарт Великобританії з управління проектами у сфері інформаційних технологій (IT). Незабаром зазначений стандарт почали використовувати за межами IT сфери. У 1996 р. PRINCE2 був визнаний універсальним методом управління проектами. PRINCE2 став надзвичайно популярним і зараз де-факто є стандартом проектного управління в Великобританії.

Остання версія була випущена у 2009 р., як результат проекту оновлення Prince2:2009 державної торгово–промислової палати Великобританії.

PRINCE2:2009 Оновлення: З 2006 р. метод переглядався, а 16 Червня, 2009 р. був опублікований під назвою «Оновлення PRINCE2:2009». Назва «PRINCE2» (замість «PRINCE3» чи схожої) використано задля демонстрації збереження головних принципів методу.

Все ж таки, це найбільш суттєвий перегляд методу з 1996 р. з метою його адаптації до мінливого бізнес середовища, спрощення і «полегшення», а також кращої інтеграції з іншими методами державної торгово–промислової палати Великобританії (ITIL, P3O, P3M3, MSP, etc.). Головна різниця між релізом 2009 р. та більш ранніми релізами полягає в появі двох довідників замість одного. «Управління проектами, використовуючи PRINCE2» (Managing Projects Using

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		64

PRINCE2) – оновлена методика управління, що призначена для менеджерів проектів, для яких управління проектами є щоденною діяльністю. «Стратегічне управління проектами, використовуючи PRINCE2» (Directing Projects Using PRINCE2) – новий документ для Керівника проектів і Ради управління проектами, тобто спонсорів/замовників проектів.

Екзамен як з Теоретичної так і з Практичної частини буде базуватися на новому довіднику «Управління проектами» та не буде включати матеріали з довідника «Стратегічне управління проектами». Прохідний бал для Теоретичного екзамену залишиться не змінним. Прохідний бал для Практичного екзамену збільшиться з 50 % до 55 %. Тривалість екзамену з Практичної частини буде зменшено з 3 годин до 2,5 годин.

PRINCE2 – це структурований підхід до управління проектами, який спрямований на управління проектами в рамках чітко визначеної організаційної структури. PRINCE2 описує процедури координації людей та завдань в проекті, як створювати/планувати проект та що робити, якщо проект потребує внесення змін через невідповідність фактичного стану виконання проекту плану його виконання. Кожний процес зазначено з ключовими вхідними та вихідними даними, а також з специфічними цілями та завданнями, які необхідно виконати, що загалом дає можливість контролю відхилень від плану.

Поділ методу на частини, що підлягають управлінню, забезпечує ефективний контроль ресурсів, завдяки чому можливо здійснювати контрольований та організований моніторинг проекту. PRINCE2 забезпечує єдину термінологію для всіх учасників проекту. Різноманітні ролі управлінців та зони відповідальності повністю описані та можуть бути адаптовані відповідно до складності проекту та компетенцій організації.

Помилки використання

Іноді PRINCE2 вважають не доцільним для дуже маленьких проектів через обсяг роботи, необхідної для створення та оновлення документів, протоколів та

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		65

реєстрів. Досить часто це трапляється через нерозуміння, які частини PRINCE2 використовувати, адже PRINCE2 можливо повністю масштабувати.

Звичайно все це чудово, але сприйняття PRINCE2 погіршене тим, що для кожного ефективного проекту, який використовує методологію PRINCE2 існує певна кількість не ефективних проектів, які використовують, так звану, методологію PINO (PRINCE In Name Only – дослівно, PRINCE лише в назві).

Загальними проблемами є:

- Стадія початку проекту опускається/проштовхується і організація переходить відразу до створення Документу ініціювання проекту (Project initiation document – PID).

- Рада проекту не є ефективною – ескалації уходять в «чорну діру» тощо.

- Відсутній Опис продукту (Product description – PD), без якого управління якістю в PRINCE2 не працює.

- Припустимі відхилення не встановлюються, або встановлюються лише для часу виконання та вартості – чітко не визначено, в якій мірі повноваження передані виконавцям або коли необхідно використовувати ескалацію (піднімати рівень прийняття рішень).

- Проект фактично складається з однієї стадії (або «фази» використовуються, щоб уникнути Огляду виконання стадії завершення (End Stage Review)).

- Документи ініціювання проекту фактично копії-паст (copy-paste – копіювати – вставити) Документу ініціювання проекту з останнього проекту – їм не слідують і вони створюються тому що «потрібно».

- Низький рівень залучення «бізнесу», адже PRINCE2 вважається «технічним» методом – виходи (продукти) проекту можуть не призвести до бажаних результатів.

- Успіхи та невдачі використання PRINCE2 були однією з причин створення Моделі зрілості PRINCE2 (PRINCE2 Maturity Model – P2MM).

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		66

Модель зрілості PRINCE2. Модель зрілості PRINCE2 описує набір Сфер Ключових Процесів (Key Process Areas – KPAs), які необхідні для ефективного впровадження та використання PRINCE2 в організації. Довідник PRINCE2 описує управління проектом і не включає опис процесів впровадження PRINCE2 в організації, в той час як P2MM описує саме процеси впровадження PRINCE2.

P2MM описує ключові практики, які додаються до процесів та складових PRINCE2 з метою забезпечення повторюваного використання методу (Рівень 2 KPAs), а також ключові практики необхідні для впровадження методу (Рівень 3 KPAs), як стандартного бізнес-процесу управління проектами, що включає: призначення власника (3.1), адаптацію методу (3.2), навчання (3.3), інтеграцію з іншими системами управління (3.4), механізм забезпечення якості (3.5).

Огляд методу

Блок-схема процесів PRINCE2. Стрілки означають потоки інформації. PRINCE2 – це процесуальний метод управління проектами на відміну від адаптивних методів, таких як Scrum. PRINCE2 2009 визначає 40 окремих активностей (завдань) і об'єднує їх у сім процесів.

Початок проекту.

На цьому етапі визначаються учасники проектної команди та готується короткий опис проекту (опис цілей проекту та комерційне обґрунтування проекту).

Відповідно до загальних засад методу на цьому ж етапі планується наступний етап проекту. Після завершення зазначених робіт Рада проекту має погодити наступний етап проекту – ініціювання проекту.

Головні завдання включають: призначення керівника проекту та менеджера проекту, визначення та призначення команди управління проектом, створення короткого опису проекту, визначення методу управління проектом, планування наступного етапу проекту (ініціювання).

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		67

Ініціювання проекту

Цей етап базується на результатах виконання завдань етапу початку проекту. Короткий опис проекту розширюється до бізнес плану (Business case). Точки контролю якості проекту узгоджуються з точками контролю стану виконання проекту. Створюється план виконання наступного етапу проекту. Результати етапу виносяться на погодження Ради проекту з метою погодження продовження роботи над проектом.

Головні завдання включають: планування показників якості, створення плану проекту, деталізація бізнес плану та ризиків, визначення точок контролю проекту, створення Документу ініціювання проекту (Project Initiation Document).

Стратегічне управління проектом

Цей процес визначає яким чином Рада проекту (що уособлює роль спонсору проекту) буде загалом контролювати проект. Рада проекту дозволяє/санкціонує етап ініціювання проекту, а також сам проект.

Стратегічне управління також визначає яким чином Рада проекту має погоджувати план етапів, включаючи погодження будь-якого плану етапу, що може змінити існуючий план проекту у зв'язку з будь-якими змінами строків або ключових показників проекту.

Також визначається, яким чином Рада проекту може змінити план проекту, способи закриття проекту.

Головні завдання включають: засоби погодження ініціювання проекту, погодження проекту, погодження етапу або вилучення етапу проекту, підтвердження завершення проекту.

Контроль

PRINCE2 передбачає поділ проекту на етапи, які підлягають контролю. Загалом визначено яким чином пакети завдань призначаються та погоджуються. Також визначається яким чином відслідковується статус виконання завдань і яким чином такий статус доповідається Раді проекту.

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		68

Засоби для відслідковування та оцінювання виконання проекту пропонуються разом з способами застосування коригуючих дій. Також закріплюються методи ескалації визначеного кола проблем Раді проекту.

Головні завдання включають: призначення та погодження пакетів завдань, оцінювання статусу виконання завдань, звітування статусу виконання завдань, застосування коригуючих дій, ескалація проблем проекту, підтвердження завершення пакету завдань.

Управління межами етапів

Контроль виконання етапів проекту – це визначення переліку завдань, які мають бути виконані в межах етапу. Управління межами етапу визначає, що має бути виконано при завершенні етапу. При завершенні етапу необхідно створити план виконання наступного етапу. Загальний план проекту, перелік ризиків проекту та бізнес план за необхідності переглядається та оновлюється. Також визначається перелік дій на випадок, якщо етап не відповідає показникам виконання. Загалом визначається, яким чином звітується про завершення етапу.

Головні завдання включають: планування етапу, оновлення плану проекту, оновлення бізнес плану проекту, оновлення ризиків проекту, звітування про завершення етапу, створення плану дій на випадок не виконання певних завдань проекту.

Завершення проекту

Визначаються завдання, які повинні бути виконані при завершенні проекту. Проект має бути формально завершений (ресурси мають бути вивільнені для виконання інших завдань), результат виконання завдань має бути визначений, а сам проект має отримати формальну оцінку.

Головні завдання включають: завершення проекту, визначення результату виконання завдань, оцінку виконання проекту.

Розглянемо формат що використовується – **JSON** (JavaScript Object Notation, укр. запис об'єктів JavaScript, вимовляється джейсон) – це текстовий формат обміну даними між комп'ютерами.

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		69

JSON базується на тексті, може бути прочитаним людиною. Формат дозволяє описувати об'єкти та інші структури даних. Цей формат головним чином використовується для передачі структурованої інформації через мережу (завдяки процесу, що називають серіалізацією). Розробив і популяризував формат Дуглас Крокфорд.

JSON знайшов своє головне призначення у написанні веб-програм, а саме при використанні технології AJAX. JSON, що використовується в AJAX, виступає як заміна XML (використовується в AJAX) під час асинхронної передачі структурованої інформації між клієнтом та сервером. При цьому перевагою JSON перед XML є те, що він дозволяє складні структури в атрибутах, займає менше місця і прямо інтерпретується за допомогою JavaScript в об'єкти.

JSON з'явився через необхідність обміну даними з сервером у реальному часі без використання плагінів для браузерів, flash-додатків або Java-апплетів, які використовувались скрізь на початку 2000-х років. Дуглас Крокфорд був тим, хто активно просував новий на той час формат. Він з колегами хотів створити технологію, яка використовувала б можливості звичайного браузера давала б веб-розробникам можливість створювати веб-додатки із постійним двостороннім зв'язком із веб-сервером.

JSON вперше був використаний в проєкті в Communities.com для Cartoon Network, він дозволяв обмінюватись повідомленнями і одночасно маніпулювати DHTML-елементами.

Веб-сайт JSON.org було запущено 2002 року. У грудні 2005-го року Yahoo! почав переводити деякі зі своїх веб-сервісів на роботу з JSON. Google взялася до роботи з технологією у своєму веб-протоколі GData у грудні 2006-го року.

Використання

За рахунок своєї лаконічності в порівнянні з XML, формат JSON може бути більш придатним для серіалізації складних структур.

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		70

Якщо говорити про веб-застосунки, в такому ключі він доречний в задачах обміну даними як між браузером і сервером (AJAX), так і між самими серверами (програмні HTTP-інтерфейси).

Формат JSON так само добре підходить для зберігання складних динамічних структур в реляційних базах даних або файловому кеші.

Синтаксис

JSON будується на двох структурах:

1. Набір пар назва/значення. У різних мовах це реалізовано як об'єкт, запис, структура, словник, хеш-таблиця, список з ключем або асоціативним масивом.

2. Впорядкований список значень. У багатьох мовах це реалізовано як масив, вектор, список, або послідовність.

Це універсальні структури даних. Теоретично всі сучасні мови програмування підтримують їх у тій чи іншій формі. Оскільки JSON використовується для обміну даними між різними мовами програмування, то є сенс будувати його на цих структурах.

У JSON використовуються такі їхні форми:

1. Об'єкт – це послідовність пар назва/значення. Об'єкт починається з символу { і закінчується символом }. Кожне значення слідує за : і пари назва/значення відділяються комами.

2. Масив – це послідовність значень. Масив починається символом [і закінчується символом]. Значення відділяються комами.

3. Значення може бути рядком в подвійних лапках, або числом, або логічними true чи false, або null, або об'єктом, або масивом. Ці структури можуть бути вкладені одна в одну.

4. Рядок – це послідовність з нуля або більше символів юнікода, обмежена подвійними лапками, з використанням ескапе-послідовностей, що починаються зі зворотної косої риски \. Символи представляються простим рядком. Тип Рядок (String) дуже схожий на String в мовах C і Java. Число теж дуже схоже на C- або

Java-число, за винятком того, що вісімкові та шістнадцяткові формати не використовуються. Пропуски можуть бути вставлені між будь-якими двома лексемами.

Використання JSON в AJAX

Наступний фрагмент коду JavaScript показує, як клієнт може використати XMLHttpRequest для запиту об'єктів в форматі JSON з серверу. (Серверна частина коду пропущена, вона просто повертає на запит URL рядок у JSON форматі).

Треба відзначити, що тут використання XMLHttpRequest не є кросс-браузерним (за деталями звертайтеся на сторінку XMLHttpRequest), і код зазнаватиме незначних модифікацій в різних версіях оглядачів Internet Explorer, Opera, Safari або Mozilla. Використання запиту XMLHttpRequest обмежено правилом одного джерела (same origin policy): URL, що відповідає на запит, має посилатися на той же сайт, що обслуговує сторінку, що ініціювала запит.

Оглядачі можуть також використовувати тег <iframe> для асинхронного запиту JSON-даних в кросс-браузерному варіанті, або використати просте перенаправлення <form action="url_to_cgi_script" target="name_of_hidden_iframe">. Такий підхід був поширений до приходу популярного нині запиту XMLHttpRequest.

Динамічний тег <script> також можна використати для підвантаження JSON-даних. Ця техніка можлива, щоб обійти надто суворе правило одного джерела, але вона не є безпечною. Запит JSONRequest пропонується, як безпечніша альтернатива.

Питання безпеки

Хоча JSON призначений для передачі даних в серіалізованому вигляді, його синтаксис відповідає синтаксису JavaScript і це створює низку проблем безпеки. Часто для обробки даних, отриманих від зовнішнього джерела у форматі JSON, до них застосовується функція eval() без якої-небудь попередньої перевірки.

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		72

JavaScript eval()

Оскільки JSON представляється синтаксично правильним фрагментом коду JavaScript, природним способом розбору JSON-даних в JavaScript-програмі є використання вбудованої в JavaScript функції eval(), яка призначена для обчислення JavaScript-виразів. При цьому підході відпадає необхідність у використанні додаткових парсерів.

Техніка використання eval() робить систему вразливою, якщо джерело JSON-даних, що використовуються, не відноситься до надійних. Такими даними може виступати шкідливий JavaScript-код для атак за допомогою ін'єкції коду. За допомогою цієї вразливості можливо здійснювати крадіжку даних, підробку автентифікації. Проте, вразливість можна усунути за рахунок використання додаткових засобів перевірки даних на коректність. Наприклад, до виконання eval() отримані від зовнішнього джерела дані можуть перевірятися за допомогою регулярних виразів. У RFC, що визначає JSON пропонується використовувати такий код для перевірки його відповідності формату JSON

```
const my_JSON_object = !(/[^\s,:{}\[\]0-9.\-+Eaeflnr-u \n\r\t]/.test(
text.replace(/\"(\\"|\\.|[^\"\\\\])\"/g, ' '))) &&
eval('(' + testedData + ')');
```

Як безпечніша альтернатива eval() була запропонована нова функція parseJSON(), здатна обробляти тільки JSON-дані.

Вбудований JSON

Останні версії веб-браузерів мають вбудовану підтримку JSON і здатні його обробляти без виклику функції eval(), що призводить до описаної проблеми. Обробка JSON у такому разі зазвичай здійснюється швидше. Так у червні 2009 року вбудовану підтримку JSON мали такі браузери: Mozilla Firefox 3.5+; SeaMonkey 2; Thunderbird 3; Microsoft Internet Explorer 8; Opera 10.5; Браузери, засновані на WebKit (наприклад, Google Chrome, Apple Safari).

Принаймні дві популярні бібліотеки JavaScript використовують вбудований JSON у разі його доступності: jQuery; Dojo.

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		73

Підробка крос-доменного запиту

Непродумане використання JSON робить сайти вразливими до підробки міжсайтових запитів (CSRF або XSRF). Оскільки тег `<script>` допускає використання джерела, що не належить до того ж домену, що і використовуваний ресурс, це дозволяє виконувати код даних, представлених у форматі JSON, в контексті довільної сторінки, що робить можливою компрометацію паролів або іншої конфіденційної інформації користувачів, що пройшли авторизацію на іншому сайті.

Це є проблемою тільки у разі вмісту в JSON-даних конфіденційної інформації, яка може бути компрометована третьою стороною і якщо сервер розраховує на політику одного джерела, блокуючи доступ до даних при виявленні зовнішнього запиту. Це не є проблемою, якщо сервер визначає допустимість запиту, надаючи дані тільки у разі його коректності. HTTP cookie не можна використовувати для визначення цього. Виключне використання HTTP cookie використовується підробкою міжсайтових запитів.

Розширення, JSONP

JSONP або «JSON з підкладкою» є розширенням JSON, коли назва функції зворотного виклику вказується як вхідний аргумент. Спочатку ідея була запропонована в блозі MacPython в 2005 році, і в наш час використовується багатьма Web 2.0 застосунками, такими, як Dojo Toolkit Applications, Google Toolkit Applications і zanox Web Services.

Подальші розширення цього протоколу були запропоновані з урахуванням введення додаткових аргументів, як, наприклад, у разі JSONPP за підтримки S3DB вебсервісів.

Оскільки JSONP використовує скрипт-теги, виклики по суті відкриті світові. З цієї причини JSONP може бути недоречними для зберігання конфіденційних даних.

Включення скриптових тегів від віддалених сайтів дозволяє їм передати будь-який контент на сайті. Якщо віддалений сайт має вразливості, які

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		74

дозволяють виконати ін'єкції JavaScript, то початковий сайт також може бути ними зачеплений.

Розширення, BSON

BSON – це бінарна форма представлення простих структур даних і асоціативних масивів (які називають об'єктами або документами). Назва «BSON» заснована на визначенні JSON і неофіційно означає «Binary JSON» (бінарний JSON).

JSON Reference

Стандарт JSON не описує посилання на інші об'єкти або частини, але існує чернетка стандарту IETF для посилань на об'єкти на основі JSON. Посилання дозволяють здійснювати трансклюзію – вставляти одні документи в інші.

JSON Reference – це JSON-об'єкт з ключем "\$ref" (всі інші ключі ігноруються) і значенням стрічкового типу що містить URI, наприклад:

```
{ "$ref": "http://example.com/example.json#/foo/bar" }
```

Якщо URI містить ідентифікатор фрагмента (в прикладі вище "/foo/bar"), він інтерпретується як JSON Pointer.

Модуль `dojox.json.ref` в Dojo toolkit, забезпечує підтримку декількох форм JSON Reference.

4.2 Захист розробленого програмного забезпечення

Захист розробленого програмного забезпечення буде відбуватися за допомогою Threefish – в криптографії симетричний блоковий криптоалгоритм, розроблений автором Blowfish та Twofish, американським криптографом Брюсом Шнайером 2008 року для використання в геш-функції Skein і як універсальну заміну наявним блоковим шифрам. Основними принципами розробки шифру були: мінімальне використання пам'яті, необхідна для використання в геш-функції стійкість до атак, простота реалізації та оптимізація під 64-розрядні процесори.

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		75

Структура алгоритму

Threefish має дуже просту структуру і може бути використаний для заміни алгоритмів блочного шифрування, будучи швидким і гнучким шифром, що працюють в довільному режимі шифрування. Threefish S-блоки не використовує, заснований на комбінації інструкцій виключаючого або, складання і циклічного зсуву.

Як і AES, шифр реалізований у вигляді підстановочно-перестановочної мережі на оборотних операціях, не будучи шифром мережі Фейстел.

Алгоритм передбачає використання tweak-значення, свого роду вектора ініціалізації, дозволяючи змінювати таким чином значення виходу, без зміни ключа, що має позитивний ефект як для реалізації нових режимів шифрування, так і на криптостійкості алгоритму.

Як результат думки авторів, що кілька складних раундів часто гірше ніж застосування великого числа простих раундів, алгоритм має нетрадиційно велику кількість раундів – 72 або 80 при ключі 1024 біт, проте, за заявою творців, його швидкісні характеристики випереджають AES приблизно вдвічі. Варто зауважити, що через 64-бітної структури шифру, дана заява має місцево лише на 64-розрядної архітектури. Тому, Threefish, як і Skein [1], заснований на ньому, на 32-розрядних процесорах показує значно гірші результати ніж на «рідному» обладнанні.

Ядром шифру є проста функція «MIX», перетворювальна два 64-бітових беззнакових числа, в процесі якої відбувається складання, циклічний зсув (ROL / ROR), і додавання по модулю 2 (XOR) .

Нижче представлений код MIX-функції для Threefish-1024 [2]:

```
<syntaxhighlight lang="C">
// Константи для циклічного зсуву
int R16 [8] [8] = {
    {55, 43, 37, 40, 16, 22, 38, 12},
    {25, 25, 46, 13, 14, 13, 52, 57},
    {33, 8, 18, 57, 21, 12, 32, 54},
    {34, 43, 25, 60, 44, 9, 59, 34},
    {28, 7, 47, 48, 51, 9, 35, 41},
```

```

    {17, 6, 18, 25, 43, 42, 40, 15},
    {58, 7, 32, 45, 19, 18, 2, 56},
    {47, 49, 27, 58, 37, 48, 53, 56},
};
// D - раунд, j - індекс в таблиці циклічного зсуву
void mix (int j, int d) {
    unsigned long long rotl;
    y [0] = x [0] + x [1];
    rotl = R16 [d% 8] [j];
    y [1] = (x [1] << rotl) | (x [1] >> (64 - rotl));
    y [1] ^ = y [0];
}
</Source>

```

Процедура розшифрування обернена процедурі зашифрування і містить зворотну функцію DEMIX.

Кожен з 72 раундів Threefish-256 і Threefish-512 має чотири MIX перетворення, Threefish-1024 – вісім звернень до MIX функції.

Безпека

За заявою авторів, алгоритм має більш високий рівень безпеки, ніж AES. Існує атака на 25 з 72 раундів Threefish, в той час як для AES – на 6 з 10. Threefish має показник фактора безпеки 2.9, в свою чергу, AES всього 1.7 [3]

Для досягнення повної дифузії, шифру Threefish-256 досить 9 раундів, Threefish-512 – 10 раундів і Threefish-1024 – 11 раундів. Виходячи з цього, 72 і 80 раундів відповідно в середньому, забезпечать кращі результати, ніж існуючі шифри. [4]

У той же час, алгоритм має набагато простішу структуру і функцію перетворення, проте виконання 72-80 раундів, на думку дослідників, забезпечує необхідну стійкість. Вживаний розмір ключа від 256 до 1024 біт зводить нанівець можливість повного перебору паролів при так званій атаці грубою силою (brute force attack) на сучасному обладнанні.

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		77

5 МЕТОДИКА ВПРОВАДЖЕННЯ СИСТЕМИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ

На рисунку 5.1 зображено розроблене у бакалаврської дипломної роботі система захищеної і адаптованої мережі SD-WAN. З рисунку можна побачити що інтерфейс головного вікна розподілено на наступні функціональні розділи: Функціональних кнопок ПЗ; Навігаційного меню яке викликається натисканням правої клавіші маніпулятора миші; Верхнього меню; Розділу обрання групи; Розділу виведення результату роботи системи.

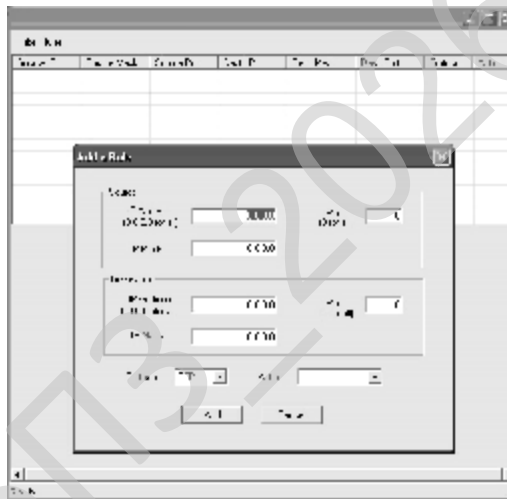


Рисунок 5.1 – Головне вікно ПЗ

Розроблена програма має дуже простий і зрозумілий інтерфейс з користувачем. Кожен, хто в достатньому обсязі володіє операційним середовищем Windows без особливих складностей освоїть і цю програму, оскільки її інтерфейс інтуїтивно зрозумілий. Якщо програма не видала ніяких помилок, і працює, то можна використовувати, інакше слід слідувати інструкціям, які пропонує програма.

На рисунку 5.2 зображено авторські дані розробленого програмного забезпечення.

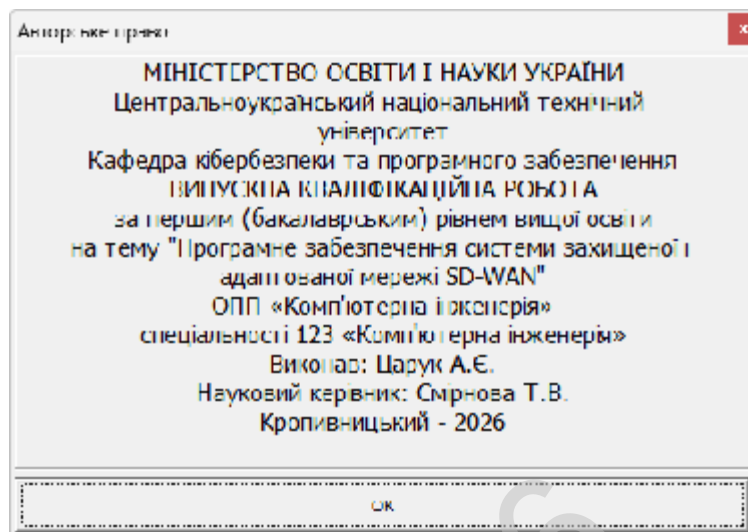


Рисунок 5.2 – Авторське право

Розглянемо процес впровадження програмного забезпечення, це процес налаштування програмного забезпечення під певні умови використання, а також навчання користувачів роботі з програмним продуктом. Впровадження програмного забезпечення це усі дії, що роблять розроблену програмну систему готовою до використання. Даний процес є частинною життєвого циклу програмного забезпечення.

Загалом процес розгортання складається з кількох взаємопов'язаних дій із можливими переходами між ними. Ця активність може відбуватися як з боку виробника так і з боку споживача. Оскільки кожна програмна система є унікальною, то усі процеси та процедури під час розгортання важко передбачити. Тому, "розгортання" можна трактувати як загальний процес відповідно до певних вимог та характеристик. Розгортання може здійснюватись програмістом і в процесі розробки програмного забезпечення.

До діяльностей пов'язаних із розгортанням програмного забезпечення відносять:

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		79

- Випуск.
- Встановлення та активація.
- Деактивація.
- Адаптація.
- Оновлення.
- Вмонтування.
- Відстежування версій.
- Видалення.
- Вилучення з обігу.

При впровадженні програмного забезпечення потрібно урахувати наступні дії:

– Виділення критичних, з точки зору загального результату, процедур в діяльності організації. Коли набір таких процедур визначений, необхідно в першу чергу використовувати ІТ рішення для автоматизації операцій усередині саме цих процедур. Таким чином, розроблене ІТ рішення автоматично стає життєво важливим і затребуваним для організації, а також буде забезпечена публічність процесу впровадження;

– Розширення нормативної бази організації шляхом включення до неї регламентів, що описують порядок виконання процедур автоматизованих процесів. В іншому випадку є небезпека виникнення неузгодженості між автоматизованими процедурами та іншими процесами організації.

– Виконання робіт з загальної стандартизації існуючої діяльності організації, коли виділяються кращі практики виконання процедур і включаються в ІТ рішення за принципом найбільшої корисності для більшості учасників. Відсоток таких процедур щодо загального обсягу автоматизації може бути невеликий, але це надає процесу побудови рішення вагу в організації за рахунок збільшення його необхідності.

Під час роботи над програмою було проведено тестування програмного забезпечення, тобто технічне дослідження, призначене для виявлення інформації про якість продукту відносно контексту, в якому воно має використовуватись.

Тестування включає як процес пошуку помилок або інших дефектів, так і випробування програмних складових з метою їх оцінки.

Проводилась оцінка:

- відповідності поставленим вимогам;
- правильна відповідь для усіх можливих вхідних даних;
- виконання функцій за прийнятний час;
- практичність;
- сумісність з ОС та стороннім ПЗ.

Оскільки число можливих тестів для програмних компонент практично нескінченне, тому стратегія тестування полягала в тому, щоб провести всі можливі тести з урахуванням наявного часу та ресурсів.

Як результат ПЗ тестувалось стандартним виконанням програми з метою виявлення помилок або інших дефектів.

Проводилось тестування чорної скриньки.

Основне місце програми тестів «чорної скриньки» – інтерфейс ПЗ. Відомі: функції програми. Досліджується: робота кожної функції на всій області визначення.

Ці тести демонструють:

- Як виконуються функції програми.
- Як приймаються вихідні дані.
- Як виробляються результати.
- Як зберігається цілісність зовнішньої інформації.

При тестуванні «чорної скриньки» розглядаються системні характеристики програм, ігнорується їхня внутрішня логічна структура. Вичерпне тестування, як правило, неможливе.

Наприклад, якщо в програмі 10 вхідних величин і кожна приймає по 10 значень, то кількість тестових варіантів становитиме 10^{10} . Тестування «чорної скриньки» не реагує на багато особливостей програмних помилок.

Тестування «чорної скриньки» (функціональне тестування) дозволяє отримати комбінації вхідних даних, які забезпечують повну перевірку всіх функціональних вимог до програми.

Програмний виріб тут розглядається як «чорна скринька», чію поведінку можна визначити тільки дослідженням його входів та відповідних виходів. При такому підході бажано мати:

- Набір, утворений такими вхідними даними, які призводять до аномалій у поведінці програми (назвемо його ІТс).

- Набір, утворений такими вхідними даними, які демонструють дефекти програми (назвемо його ОТ).

Будь-який спосіб тестування «чорної скриньки» повинен:

- Виявити такі вхідні дані, які з високою ймовірністю належать набору ІТс.
- Сформулювати такі очікувані результати, які з високою ймовірністю є елементами набору ОТ.

Принцип «чорної скриньки» не альтернативний принципу «білої скриньки». Скоріше це доповнює підхід, який виявляє інший клас помилок.

Тестування «чорної скриньки» забезпечує пошук наступних категорій помилок:

- Некоректних чи відсутніх функцій.
- Помилки інтерфейсу.
- Помилки у зовнішніх структурах даних або в доступі до зовнішньої бази даних.
- Помилки характеристик (необхідна ємність пам'яті і т.д.).
- Помилки ініціалізації та завершення.

Обрано умови розповсюдження – proprietary software.

Програмне забезпечення, на яке зберігаються як немайнові, так і майнові авторські права. Отримавши або придбавши таке програмне забезпечення, користувач отримує обмежені права користування ним: може бути заборонено або закрито доступ до коду (вивчення), внесення змін, тиражування, розповсюдження та перепродаж. Програмне забезпечення вважається власницьким, якщо наявне хоча б одне з перелічених обмежень.

Найчастіше основним методом захисту майнових прав на власницьке ПЗ, поза ліцензійною угодою, власник обирає закриття сирцевого коду, захищаючи свій продукт від модифікації і вбудовуючи системи обмеження користування через авторизацію. Таке програмне забезпечення називається закритим. Проте, код власницького продукту може бути і відкритим, але власник може обмежити права користувача умовами користувацької ліцензії.

Власницьке програмне забезпечення та комерційне програмне забезпечення не є синонімами – власницьким може бути і безплатне (тобто, некомерційне) програмне забезпечення.

На противагу власницькому ПЗ існує вільне програмне забезпечення, автори і власники якого дозволяють вивчати, модифікувати і поширювати свій продукт.

Саме визначення власницького програмного забезпечення виникло в результаті діяльності громадського руху вільного програмного забезпечення (представленого Фондом вільного програмного забезпечення та іншими організаціями) і осмислення умов свободи користування програмами. Визначенням власницького програмного забезпечення є не невідповідність хоча б одній з базових умов вільного програмного забезпечення.

Сама назва власницьке ПЗ підкреслює визначальне значення власника у способі використання і можливостях розвитку цього програмного забезпечення.

6 ОСНОВНІ ВИСНОВКИ

Програмне забезпечення, створене в результаті виконання випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти, призначено для системи захищеної і адаптованої мережі SD-WAN.

В межах України в недостатній мірі представлені вітчизняні розробки в цій області.

Рішення завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем захищеної і адаптованої мережі SD-WAN.
- Досліджена система захищеної і адаптованої мережі SD-WAN.
- На основі отриманих результатів досліджень створена програмна реалізація системи захищеної і адаптованої мережі SD-WAN.

Розроблені під час виконання випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання захищеної і адаптованої мережі SD-WAN.

Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань.

При створенні програмного забезпечення було використано об'єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем.

Програма реалізована на мові високого рівня Python. Дана мова програмування дозволяє найбільш ефективно обробляти дані призначені для системи захищеної і адаптованої мережі SD-WAN. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		84

програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції.

Програма призначена для виконання під управлінням багатозадачної операційної системи Windows 10/11.

Даються необхідні рекомендації з установки розробленого програмного забезпечення.

Для підвищення рівня безпеки запропоновано застосовувати алгоритм Threefish.

В цілому створене програмне забезпечення підтверджує правильність використаних проектних рішень та повністю відповідає вимогам технічного завдання. Створене програмне забезпечення має потенційну можливість для подальшого вдосконалення і застосування у різних галузях.

К6ПЗ-2026

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		85

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Вінтенко Б.Ю., Смірнов О.А., Коваленко О.В., Смірнов С.А., Коваленко А.С. «Дослідження нормативних документів та галузевих стандартів розробки програмного забезпечення комп'ютерних систем управління АЕС, важливих для безпеки». *Системи управління, навігації та зв'язку*, 2023, вип. 2(72), С. 170-178.
2. Smirnov, O., Neskorodieva, T., Fedorov, E., Rudakov, K., Neskorodieva, A. «Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine» *CEUR Workshop Proceedings*, Volume 3187, 2022,
3. Smirnov O.A., Al-Oraiqat A.M., Ulichev O.S., Meleshko Ye.V., Al-Rawashdeh H.S., Polishchuk L.I. «Modeling strategies for information influence dissemination in social networks». *Journal of Ambient Intelligence and Humanized Computing* Volume 13, Issue 5. Springer, Cham. 2022, pp. 2463-2477.
4. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». *Проблеми інформатизації та управління*, № 2(70). 2022. С. 28-37.
5. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Системи управління, навігації та зв'язку*, 2022, № 3(69). С. 93-98.
6. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Вісник Хмельницького національного університету. Серія: «Технічні науки»*, № 2 (307). С. 46-52. 2022.

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		86

7. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Системи управління, навігації та зв'язку*, 2022, № 1(67). С. 84-89.

8. Smirnov O., Kuznetsov A., Zhora V., Onikiychuk A., Pieshkova O. «Hiding Messages in Audio Files Using Direct Spread Spectrum». *11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2021*, Cracow, Poland, 22-25 September 2021. P. 414-418

9. Smirnov O., Kuznetsov A., Lokotkova I., Kuznetsova T., Florov S., Lebid O. «Using Orthogonal Signals to Hide Information in Images». *4 IEEE International Conference on Advanced Information and Communication Technologies (AICT) - 2021*, Lviv, Ukraine, September 21-25, 2021. P. 255-260.

10. Smirnov O., Kuznetsov A., Girzheva O., Kiian A., Nakisko O., Kuznetsova T. «Advanced Code-Based Electronic Digital Signature Scheme». *2020 IEEE International Conference on Problems of Infocommunications Science and Technology, PIC S and T 2020*, Kharkiv, 6 October 2020-9 October 2020, P. 358-362.

11. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova K. «Data hiding scheme based on spread sequence addressing». *CEUR Workshop Proceedings Volume 2805*, 2020, Pages 44-58.

12. Smirnov, O., Kuznetsov, A., Potii, O., Poluyanenko, N., Stelnyk, I., Mialkovsky, D. «Combining and filtering functions in the framework of nonlinear-feedback shift register». *International Journal of Computing*; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256.

13. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». *CEUR Workshop Proceedings. Volume 2740*, 2020, Pages 102-114.

14. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». *Journal of theoretical and applied information technology* Vol.98. No 21, 2020, P. 3334-3346.
15. Smirnov O., Kuznetsov A., Arischenko A., Chepurko I., Onikiychuk A., Kuznetsova T. «Pseudorandom sequences for spread spectrum image steganography». *CEUR Workshop Proceedings* Volume 2654, 2020, Pages 122-131.
16. Smirnov O., Kuznetsov A., Kovalchuk D., Kuznetsova T. «New technique for data hiding in cover images using adaptively generated pseudorandom sequences». *CEUR Workshop Proceedings* Volume 2654, 2020, Pages 1-14.
17. Smirnov O., Lutsenko M., Kuznetsov A., Kiian A., Kuznetsova T., «Biometric cryptosystems: overview, state-of-the-art and perspective directions». *Lecture Notes in Networks and Systems*, vol 152. Springer, Cham. 2021, pp 66-84.
18. Smirnov O., Kuznetsov A., Onikiychuk A., Makushenko T., Anisimova O., Arischenko A. «Adaptive pseudo-random sequence generation for spread spectrum image steganography». *2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Ukraine, Kyiv, May 14-18. 2020. P. 161-165.
19. Smirnov O., Kuznetsov A., Kiian A., Babenko V., Perevozova I., Chepurko I. «New Approach to the Implementation of Post-Quantum Digital Signature Scheme». *2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Ukraine, Kyiv, May 14-18. 2020. P. 166-171.
20. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». *2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
21. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In:

Radvilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587.

22. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». *CEUR Workshop Proceedings* Volume 2616, 2020, Pages 125-136.

23. Smirnov, O., Shekhanin, K., Kuznetsov, A., Krasnobayev, V. «Detecting Hidden Information in FAT». *International Journal of Computer Network and Information Security (IJCNIS)*. Vol. 12, No. 3, 2020. PP.33-43.

24. Smirnov, O., Kuznetsov, A., Gorbacheva, L., Babenko, V., «Hiding data in images using a pseudo-random sequence», *CEUR Workshop Proceedings* Volume 2608, 2020, Pages 646-660.

25. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». *International Journal of Computing*; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.

26. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». *2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T)*, Kyiv, Ukraine, 8 – 11 October 2019 . P.517-522.

27. Smirnov, O., Ulichev, O., Meleshko, Y., Khokh, V., Goncharenko, I. «Method of Choosing Objects for Informational Influence in Social Networks during Information Campaign Based on the Analytic Hierarchy Process». *CEUR Workshop Proceedings*, Vol 2588, P. 215-227, 2019.

28. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». *CEUR Workshop Proceedings*, Vol 2588, P. 90-106, 2019.

29. Smirnov, O., Kuznetsov, A., Kiian, A., Gorbenko, Y., Cherep, O., Bexhter L. «Code-based Pseudorandom Generator for the Post-Quantum Period», *2019 IEEE International Conference on Advanced Trends in Information Theory (IEEE ATIT 2019)*. 18.12.19-20.12.19 Kyiv Ukraine. P. 204 – 209.

30. Smirnov, O., Kuznetsov, A., Nariezhnii, O., Stelnyk, S., Kokhanovska, T., Kuznetsova T., «Side Channel Attack on a Quantum Random Number Generator», *10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2019*; Metz; France; 18 - 21 September 2019. P.713-718.

31. Smirnov, O., Kuznetsov, A., Kiian, A., Pushkar'ov, A., Mialkovskiy, D., Kuznetsova, T., «Code-Based Schemes for Post-Quantum Digital Signatures», *10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2019*; Metz; France; 18-21 September 2019. P. 707-712.

32. Smirnov, O., Kuznetsov, A., Stefanovych, O., Gorbenko, Y., Krasnobaev, V., Kuznetsova K. «Information Hiding Using 3D-Printing Technology», *10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2019*; Metz; France; 18-21 September 2019. P.701-706.

33. Smirnov, O., Hu, Z., Vasiliu, Y., Sydorenko, V., Polishchuk, Y., «Abstract Model of Eavesdropper and Overview on Attacks in Quantum Cryptography Systems», *10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2019*; Metz; France; 18-21 September 2019. P.399-405.

34. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Averchev, A., Pastukhov, M., Kuznetsova, K., «Formation of Pseudorandom Sequences with Special Correlation Properties», *2019 3rd International Conference on Advanced Information and Communications Technologies, AICT -2019/ Lviv, Ukraine, 2-6 July, 2019*, P. 395-399.

35. Smirnov, O., Kuznetsov, A., Kiian, A., Babenko, B., Zhosan, H., Prokopovych-Tkachenko, D., «Soft Decoding Method for Turbo-Productive Codes», *2019 3rd International Conference on Advanced Information and Communications Technologies, AICT 2019*, Lviv, Ukraine, 2-6 July, 2019, P. 129-134.

36. Smirnov, O., Kuznetsov, A., Kiian, A., Zamula, A., Rudenko, S., Hryhorenko, V., «Variance Analysis of Networks Traffic for Intrusion Detection in Smart Grids», *2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS)*, Kyiv, Ukraine April 17-19, 2019 P. 353-358.

37. Smirnov, O., Kuznetsov, A., Kavun, S., Babenko, B., Nakisko, O., Kuznetsova, K., «Malware Correlation Monitoring in Computer Networks of Promising Smart Grids», *2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS)*, Kyiv, Ukraine April 17-19, 2019 P. 347-352.

38. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Pastukhov, M., Kuznetsova, K., Prokopovych-Tkachenko, D., «Discrete Signals with Special Correlation Properties», *CEUR Workshop Proceedings Volume 2353, CEUR Workshop Proceedings 2019*, Pages 618-629.

39. Smirnov, O., Kuznetsov, A., Kiian, A., Kuznetsova, K., Ivko, T., Prokopovych-Tkachenko, D., «Soft Decoding Based on Ordered Subsets of Verification Equations of Turbo-Productive Codes», *CEUR Workshop Proceedings Volume 2353, CEUR Workshop Proceedings 2019*, Pages 873-884.

40. Smirnov A.A., Kuznetsov A.A., Danilenko D.A., Berezovsky A., «The statistical analysis of a network traffic for the intrusion detection and prevention systems», *Telecommunications and Radio Engineering*. – Volume 74, Issue 1. – Begel House Inc. – 2015. – P. 61-78.

41. Smirnov O., Kuznetsov A., Kovalchuk D., Kuznetsova T. «New Technique for Hiding Data in Cover Images Using Adaptively Generated Pseudorandom Sequences». *CEUR Workshop Proceedings Volume 2732, 2020*, Pages 214-227.

42. Смірнов О.А., Коноплицька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Книшук А.В. «Вступ до кібербезпеки»: навчальний посібник – Кропивницький: ЦНТУ – 2022. – 968 с.

43. Теорія та практика сучасного інформаційно-психологічного протидіювання: навчальний посібник / [В.М. Петрик, С.О. Гнатюк, М.М. Присяжнюк та ін.]; за заг. ред. С.О. Гнатюка, В.М. Петрика та О.А Смірнова. – Полтава, 2022. – 334 с.

44. Smirnov O. Kuznetsov A., Zaichenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». *International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019*; Odessa; Ukraine; 9-13 September 2019. P.22-28.

45. Смірнов О.А., Коноплицька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Поліщук Л.І. Інформаційна безпека в комп'ютерних мережах. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2020. – 294 с.

46. О.А. Смірнов, П.С. Усік, «Дослідження перспектив використання технологічних рішень в мережах 5G» у *Кібербезпека та інформаційні технології: монографія*. – Х. : ТОВ «ДІСА ПЛЮС», 2020.С. 122-135.

47. Смірнов О.А., Коноплицька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В. Поліщук Л.І. Проектування комп'ютерних систем та мереж. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2019. – 264 с.

48. Smirnov, O., Kuznetsov, A., Shekhanin, K., Chepurko, I. Detecting Hidden Information in FAT. Монографія: In.: ISCI'2019: Information Security in Critical Infrastructures. Collective monograph. Edited by Ivan D. Gorbenko and Alexandr A. Kuznetsov, ASC Academic Publishing, USA, 2019, pp. 412-429. – ISBN: 978-0-9989826-8-7 (Hardback), ISBN: 978-0-9989826-9-4 (Ebook)

49. Smirnov, O., Kuznetsov, A., Kuznetsova, K. Synthesis of Discrete Signals with Improved Correlation Properties. Монографія: In.: ISCI'2019:

Information Security in Critical Infrastructures. Collective monograph. Edited by Ivan D. Gorbenko and Alexandr A. Kuznetsov, ASC Academic Publishing, USA, 2019, pp. 281-299. – ISBN: 978-0-9989826-8-7 (Hardback), ISBN: 978-0-9989826-9-4 (Ebook).

50. Смірнов О.А., Гнатюк С.О., Кавун С.В., Терейковський І.А., Жмурко Т.О., Смірнов С.А., Коваленко А.С. Основи безпеки в комп'ютерних мережах. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2018. – 177 с.

51. Смірнов О.А., Стасєв Ю.В., Бараннік В.В. Коваленко О.В., Доренський О.П., Дреєв О.М., Вялкова В.І. Інформаційна безпека держави. Підручник – Кіровоград: РВЛ КНТУ, 2016. – 263 с

52. Смірнов О.А., Кавун С.В., Коваленко О.В., Дреєв О.М. Мережні інформаційні технології. Навчальний посібник – Кіровоград: РВЛ КНТУ, 2016. – 159 с.

53. Смірнов О.А., Кавун С.В., Коваленко О.В., Доренський О.П., Дреєв О.М., Вялкова В.І. Комп'ютерні мережі. Навчальний посібник – Кіровоград: РВЛ КНТУ, 2016. – 233 с.

54. Смірнов О.А., Стасєв Ю.В. Бараннік В.В. Захист інформації в автоматизованих системах управління. Навчальний посібник – Харків: ХУПС, 2015. – 264 с.

55. Смірнов О.А., Коваленко О.В., Кожанова А.С., Лєвошко О.Л., Константинова Л.В. Основи системного програмування. Навчальний посібник для студентів вищих навчальних закладів напрямів підготовки 8.050102 «Комп'ютерна інженерія». За ред. Коваленка О.В. – Кіровоград: КНТУ 2013. – 257с.

56. Смірнов О.А., Кавун С.В., Столбов В.Ф., Мелешко Є.В. Основи інформаційної безпеки. Навчальний посібник для студентів вищих навчальних закладів напрямів підготовки 8.050102 «Комп'ютерна інженерія». За ред. С.В. Кавуна. – Кіровоград: КНТУ 2012. – 442 с.

					ВКРБ-123.26.0039.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		93

57. Смірнов О.А., Кузнецов О.О., Євсєєв С.П., Мелешко Є.В., Король О.Г. Методи та алгоритми симетричної криптографії. Навчальний посібник для студентів вищих навчальних закладів напрямів підготовки 8.050102 «Комп'ютерна інженерія». За ред. О.О. Кузнецова. – Кіровоград: КНТУ 2012. – 315 с.

58. Смірнов О.А., Мелешко Є.В., Семенов С.Г. Методи та засоби обробки сигналів і даних в інформаційних системах. Навчальний посібник для студентів вищих навчальних закладів напрямів підготовки 8.050102 «Комп'ютерна інженерія». За ред. О.А. Смірнова. – Кіровоград: КНТУ 2012. – 250 с.

59. Смірнов О.А., Євсєєв С.П., Жукарев В.Ю., Король О.Г., Сорокін В.Є., Мелешко Є.В. Технології і стандарти комп'ютерних мереж. Навчальний посібник для студентів вищих навчальних закладів напрямів підготовки 8.050102 «Комп'ютерна інженерія» та 8.0925 «Автоматизація й комп'ютерно-інтегровані технології». За ред. О.А. Смірнова. – Кіровоград: КНТУ 2012. – 454 с.

60. Смірнов О.А., Віхрова Л.Г., Осадчий С.І., Ковтун В.Ю., Мелешко Є.В. Основи захисту інформації. Навчальний посібник для студентів вищих навчальних закладів напрямів підготовки 8.050102 «Комп'ютерна інженерія» та 8.050201 «Системна інженерія». За ред. О.А. Смірнова. – Кіровоград: КНТУ 2011. – 322 с.