

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 кібербезпеки для
автоматизованого захисту корпоративної мережі”

Виконав здобувач вищої освіти
IV курсу, групи КБ-22-2
ОПП «Кібербезпека»
спеціальності 125 «Кібербезпека»
_____ Врагов А.Б.
«___» _____ 2026 р.

Керівник проекту
кандидат технічних наук, доцент
_____ Смірнов С.А.
«___» _____ 2026 р.
Рецензент _____

Центральноукраїнський національний технічний університет
Факультет Механіко-технологічний
Кафедра Кібербезпеки та програмного забезпечення
Освітній ступінь бакалавр
Галузь знань 12 "Інформаційні технології"
Спеціальність 125 "Кібербезпека"
Освітньо-професійна (освітньо-наукова) програма "Кібербезпека"

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

Врагова Андрія Богдановича

(прізвище, ім'я, по батькові)

1. Тема роботи *Програмне забезпечення системи кібербезпеки для автоматизованого захисту корпоративної мережі*

2. Керівник роботи *Смірнов Сергій Анатолійович, канд. техн. наук, доцент*

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

затверджені наказом вищого навчального закладу № 129-02 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 кібербезпеки для автоматизованого захисту корпоративної мережі*

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 кібербезпеки в промислову експлуатацію.

6. Висновки

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

Структурна схема системи кібербезпеки *1 аркуш*

Функціональна схема системи кібербезпеки *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

Смірнов С.А.
(прізвище та ініціали)

Завдання прийнято до виконання
« 27 » лютого 2026 р.

Підпис здобувача

Врагов А.Б.
(прізвище та ініціали)

АНОТАЦІЯ

Врагов А.Б. Програмне забезпечення системи кібербезпеки для автоматизованого захисту корпоративної мережі. 125 Кібербезпека. Центральноукраїнський національний технічний університет. Кропивницький. 2026.

В даній випускній кваліфікаційній роботі за першим (бакалаврським) рівнем вищої освіти розроблено програмне забезпечення, яке призначено для системи кібербезпеки для автоматизованого захисту корпоративної мережі.

Метою розробки є програмне забезпечення системи кібербезпеки для автоматизованого захисту корпоративної мережі.

Результат роботи – програмна реалізація системи кібербезпеки для автоматизованого захисту корпоративної мережі.

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: кібербезпека, автоматизований захист, корпоративна мережа

ABSTRACT

Vrahov A.B. Cybersecurity system software for automated corporate network protection. 125 Cybersecurity. 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, which is intended for a cybersecurity system for automated corporate network protection.

The purpose of the development is the software of the cybersecurity system for automated corporate network protection.

The result of the work is the software implementation of the cybersecurity system for automated corporate network protection.

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 OS Windows 10/11.

The program was developed in the Python environment.

Keywords: cybersecurity, automated protection, corporate network

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ	2
ВСТУП.....	3
1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ	4
1.1 Призначення системи.....	4
1.2 Область застосування.....	5
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 кібербезпеки та мови програмування.....	18
2.3 Розгорнута постановка завдання	23
3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ	24
3.1 Опис функціонування системи	24
3.2 Розробка структурної схеми.....	33
3.3 Розробка функціональної схеми	40
3.4 Розробка діаграми процесів.....	48
4 РЕАЛІЗАЦІЯ РОБОТИ. РОЗРАХУНКИ І ЕКСПЕРИМЕНТАЛЬНІ ДАНІ, ЩО ПІДТВЕРДЖУЮТЬ ВІРНІСТЬ ПРОЕКТНИХ ТА ПРОГРАМНИХ РІШЕНЬ.....	50
4.1 Розробка блок-схем та опис алгоритмів функціонування системи.....	50
4.2 Захист розробленого програмного забезпечення.....	66
5 ВПРОВАДЖЕННЯ СИСТЕМИ КІБЕРБЕЗПЕКИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ	69
6 ОСНОВНІ ВИСНОВКИ.....	77
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	79

					ВКРБ-125.26.0025.00.00.ПЗ			
Вим.	Арк.	№ докум.	Підп.	Дата	<i>Програмне забезпечення системи кібербезпеки для автоматизованого захисту корпоративної мережі</i>	Літ.	Аркуш	Аркушів
<i>Розроб.</i>	<i>Врагов А.Б.</i>					Б	1	85
<i>Перев.</i>	<i>Смірнов С.А.</i>							
<i>Н.контр.</i>	<i>Коваленко А.С.</i>					ЦНТУ КБ-22-2		
<i>Затв.</i>	<i>Смірнов О.А.</i>							

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

ЗІ	—	захист інформації
ІБ	—	інформаційна безпека
ІТ	—	інформаційна технологія
КІС	—	корпоративні інформаційні системи
ЛОМ	—	локальна обчислювальна мережа
НСД	—	несанкціонований доступ
ОС	—	операційна система
СГ КІС	—	сегмент КІС
СЗІ	—	система захисту інформації
IPS	—	система запобігання вторгнень
NAC	—	Network Admission Control
NIDS	—	система виявлення мережних вторгнень

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		2

ВСТУП

Актуальність теми. Корпоративні мережі постійно зазнають атак хакерів, шкідливого програмного забезпечення та внутрішніх загроз. Щоб забезпечити належний рівень безпеки, компанії повинні вживати ефективних заходів для захисту своїх систем та запобігання несанкціонованому доступу.

Захист корпоративної мережі виходить за рамки простого встановлення брандмауера або антивірусного програмного забезпечення. Він вимагає структурованого підходу, що включає розширені інструменти, постійний моніторинг та сприяння культурі безпеки серед співробітників.

Мета й завдання дослідження. Метою роботи є програмне забезпечення системи кібербезпеки для автоматизованого захисту корпоративної мережі.

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

- Огляд існуючих систем для автоматизованого захисту корпоративної мережі.
- Дослідження системи кібербезпеки для автоматизованого захисту корпоративної мережі.
- Програмна реалізація системи кібербезпеки для автоматизованого захисту корпоративної мережі.

Практична цінність отриманих результатів полягає в тому, що розроблені алгоритми дозволяють успішно вирішувати задачі для автоматизованого захисту корпоративної мережі.

Таким чином, виходячи з вищеперерахованого, програмне забезпечення системи кібербезпеки для автоматизованого захисту корпоративної мережі, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за першим (бакалаврським) рівнем вищої освіти.

1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ

1.1 Призначення системи

Захист ще більше ускладнився з повсюдним впровадженням методологій гнучкої (agile) розробки, для якої характерні часті, численні й невеликі зміни системи, яка захищається, а також заміна докладної документації на додаток з використанням поверхневих «userstories». Кожна зміна породжує поведінкові аномалії, про які система захисту повідомляє як про підозрілу активність. Їх дуже багато, без знання особливостей (документації) системи, яка захищається, упоратися з ними неможливо й залишається тільки нарощувати штат операторів. Дефіцит таких фахівців привів до процвітання аутсорсингу по обробці підозрілих аномалій (це називається «обробка інцидентів», однак реальними інцидентами виявляються менш 5% з них, все інше – помилкові спрацьовування).

Автоматизація бізнес-процесів – відмінний спосіб заощадити, тому банки, роздрібні торговці, телеком-оператори й навіть державні органи намагаються якнайшвидше впровадити такі рішення. Очевидно, що при рості кількості й складності автоматизованих бізнес-систем потреба в операторах з досвідом використання засобів моніторингу активності росте навіть швидше, ніж потреба у властиво «автоматизаторах». Тому ідея автоматизувати працю операторів систем моніторингу не могла не знайти відгуку в душі тих, хто оплачує все це, з боєм спостерігаючи, як росте складність захисту.

Спроби замінити людини в непростій ролі оператора, де доводиться не просто реагувати на аномальну активність, а розбиратися в заплутаних процесах бізнес-додатків і інфраструктури, на якій вони розгорнуті, уживали постійно, але в більшості випадків вдавалося лише зробити більше зручним для оператора процес аналізу аномалій. Доручити машині приймати остаточне рішення, як було з антивірусами в старі добрі часи, ніхто не вирішувався.

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		4

В останні роки відбулося відразу два прориви: виросла обчислювальна потужність і з'явилися алгоритми машинного навчання, – завдяки чому для деяких процесів удалося радикально підвищити точність визначення атак, причому настільки, що досягнута точність перевищила показники людини. Знову стало можливо делегувати прийняття рішень машині. Уже з'явилися автоматизовані системи, здатні працювати в режимі не моніторингу, а саме блокування атак, що дозволяє скоротити навантаження на людей, для чого споконвічно й створювалися обчислювальні системи.

Не варто сьогодні перебільшувати можливості штучного інтелекту, особливо в області систем захисту. Точність його виводів поки недостатня для більшості процесів захисту, однак, наприклад, захист Web-додатку вже можна сміло довіряти машині, що справляється з роботою краще, ніж середньої руки фахівець, і, уже звичайно, більше витривалою й невтомною. У міру нагромадження даних про атаки, удосконалювання алгоритмів навчання й росту обчислювальної потужності будуть автоматизувати й інші системи захисту. Людина стане займатися творчою діяльністю: навчати штучний інтелект, вивчати нові алгоритми атак, вести розслідування й виконувати інші цікаві завдання, де інтелект важливіше швидкості, продуктивності й безпомилковості.

1.2 Область застосування

Областю застосування є корпоративні мережі. Корпоративна інформаційна мережа являє собою систему для автоматизації виробничих процесів і комп'ютерних додатків, з якими працюють співробітники підприємства. Основним завданням мережі є керування господарської діяльності підприємства або корпорації.

Результатом успішного впровадження ефективної корпоративної системи або мережі є:

- підвищення керованості підприємства й ефективності діяльності;

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		5

- поліпшення фінансових показників;
- ріст обсягу продажів;
- поліпшення партнерських відносин з іншими компаніями;
- скорочення часових витрат на виконання замовлень.

Корпоративна інформаційна система мережі підприємств

Корпоративна інформаційна система мережі підприємств використовується для забезпечення ефективності основних бізнес-процесів декількох фірм або компаній. Вона покликана поліпшити електронне діловодство на кожному підприємстві й створити єдиний інформаційний простір для полегшення прийняття важливих управлінських рішень.

Корпоративна інформаційна система мережі підприємств, як правило, є простий і багатофункціональної. Вона також характеризується високим ступенем надійності й масштабованістю інформаційних компонентів. Побудова подібної системи повинне бути засноване на детальному аналізі роботи кожної компанії, що входить у мережу підприємств.

Організація корпоративної мережі підприємства

Для побудови ефективної корпоративної мережі на підприємствах можуть бути використані різні методи. Раніше організація подібних мереж відбувалося по системі Local Area Network (LAN), що містить у собі обмежене число персональних комп'ютерів. Перевагою подібного варіанта є швидкий обмін файлами в системі, а також надійність переданої інформації. Недоліком цього методу є висока вартість впровадження системи, а також неможливість підключення віддалених користувачів.

Альтернативним варіантом є використання віртуальних мереж Virtual Private Network (VPN). Основними перевагами подібних систем є простота їхньої побудови, а також можливість підключення великої кількості абонентів, територіально віддалених друг від друга.

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		6

Організація доступу в інтернет у корпоративних мережах

Користувачі корпоративної інформаційної мережі можуть вийти в інтернет через проксі-сервер або за допомогою маршрутизації. У першому випадку доступ надається по IP-адресі того комп'ютера, на якому працює співробітник. Для цього може бути використаний спеціалізований програмно-апаратний шлюз.

У другому випадку користувачеві необхідно пройти авторизацію у використовуваній системі, увівши логін і пароль. Цей варіант найчастіше реалізується за допомогою проксі-сервера SQUID.

Таким чином, виходячи з вищеперерахованого, програмне забезпечення системи кібербезпеки для автоматизованого захисту корпоративної мережі, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за першим (бакалаврським) рівнем вищої освіти.

					ВКРБ-125.26.0025.00.00.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

Огляд систем пошуку конфіденційних даних у корпоративній мережі (Discovery DLP)

Щоб контролювати доступ до конфіденційних даних, необхідно розуміти, де і яка інформація зберігається. Оперативний пошук і безперервний контроль місць зберігання даних дозволить не тільки точно визначити найбільш важливі інформаційні активи, виявити несанкціоновані копії конфіденційних документів, але уникнути можливих витоків. Підсистема пошуку конфіденційної інформації (Discovery DLP), що входить до складу зрілих DLP як іноземних, так і вітчизняних виробників, допомагає вирішити таке завдання.

У цей час державні й комерційні організації приділяють особливу увагу захисту конфіденційної інформації від витоку по різних каналах зв'язку. Можливість витоку інформації за межі внутрішньої мережі є небезпечною погрозою, тому що крім зниження репутації компанія може понести істотні збитки. Якщо персональні дані, клієнтська база, наукові розробки або інша критична інформація потрапить у руки зловмисників або конкурентів, це загрожуватиме організації серйозними проблемами.

Для рішення проблем витоку даних впроваджуються DLP-системи, здатні забезпечувати активний захист і блокувати відправлення повідомлень із неприпустимими вкладеннями. Однак зловмисником-інсайдером може виявитися не тільки людина, що працює безпосередньо із критичними даними. Може трапитися так, що конфіденційні дані потрапили на комп'ютер співробітника

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		8

помилково або стали поширюватися по компанії внаслідок недбалості, наприклад, неправильно виставлених прав доступу.

Для рішення подібних проблем у системи DLP найчастіше входить додатковий модуль – Crawler (пошуковий робот), або Discovery DLP, що дозволяє сканувати робочі станції співробітників, файлові сервера й мережні сховища даних на присутність у них певних документів і файлів різних форматів.

Ринок Discovery DLP

Попередниками Discovery DLP у сучасному розумінні цього терміна стали пошукові роботи, або програми, які були складовою частиною пошукових систем. Їхньою функцією був перебір веб-сторінок, занесення їх у спеціальну базу пошуку й надання результату при запиті. Поява DLP-систем дозволило організаціям вирішувати проблему витоку конфіденційних даних співробітниками. Крім цього, для співробітників інформаційної безпеки був розроблений окремий компонент, що дозволяє робити пошук файлів необхідного формату на файлових серверах і комп'ютерах користувачів. У даний момент можливості Discovery DLP розширилися. Крім звичайного пошуку з'явилися функції автоматичного видалення документів або їхньої заміни болванками з інформацією про порушення політики безпеки.

Першою компанією, що включила до складу своєї DLP-системи модуль Discovery DLP, була Symantec, що протягом багатьох років займає лідируючу позицію, за версією аналітичного агентства Gartner у дослідженні Content-Aware Data Loss Prevention. Наступною системою, що мала можливості сканування серверів і робочих станцій на наявність конфіденційної інформації, стала DLP-система від компанії Forcepoint (раніше Websense). І тільки через кілька років у складі українських DLP з'явився модуль Discovery DLP.

Discovery DLP звичайно не поставляється як окремий продукт, а йде в складі комплексної DLP-системи. Однак є виключення, наприклад Zecurion Discovery, що буде розглянутий далі. Крім того, Discovery DLP усе ще не ставиться до компонента, за замовчуванням вхідному до складу DLP-систем

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		9

українських виробників. Однією із причин може бути те, що архів, що збирає Discovery DLP, зберігає в собі безліч конфіденційних даних, і у випадку атак зловмисників він може бути скомпрометований. З іншого боку, специфіка використання DLP-систем деяких вендорів не передбачає розслідування інцидентів як найбільш частий сценарій використання системи, а націлена вирішувати іншого завдання.

Можливості Discovery DLP

Можливості Discovery DLP дозволяють співробітникам служби безпеки завжди бути в курсі того, на яких робочих місцях зберігаються файли з конфіденційними даними. Такі відомості необхідні, щоб оцінити ризики інформаційної безпеки й вибудувати адекватний рівень захисту певних робочих станцій або файлових серверів. Знання про розташування критичної інформації дозволять правильно налаштувати систему захисту від витоку, що може полягати в постановці на контроль вузького кола осіб (співробітників, які мають доступ до комп'ютерів і серверів з даними), а також додавання більше твердих політик інформаційної безпеки.

Можливості Discovery DLP також можуть використовуватися при розслідуванні інцидентів інформаційної безпеки. У випадку вже, що відбулася витоку, даних співробітники служби безпеки зможуть визначити всі місця зберігання даних, що витекли, виявити співробітників, які мали можливість працювати із цими даними, тим самим звузивши коло підозрюваних. Отримана в такий спосіб інформація може значно допомогти в розслідуванні інцидентів з витоками.

Під час пошуку Discovery DLP використовують стандартні для DLP технології пошуку інформації (контентний аналіз, OCR, цифрові відбитки й т.п.) і враховують при цьому існуючі політики захисту даних.

Наприклад, підсистема не буде сигналізувати про помилку зберігання файлу, якщо він розміщується на робочій станції довіреного співробітника й диск зашифрований.

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		10

Інакше кажучи, до функцій Discovery DLP можна віднести:

- Сканування робочих станцій і файлових сховищ.
- Пошук конфіденційної інформації шляхом заздалегідь налаштованого списку критеріїв конфіденційних документів.
- Пошук і класифікація даних, що зберігаються у внутрішній мережі організації.
- Виявлення несанкціоновано, що зберігаються файлів, у мережі.
- Моніторинг руху конфіденційних даних і критичних документів.

Щоб одержати подання про роботу Discovery DLP, розглянемо існуючі рішення, які входять до складу закордонних і вітчизняних DLP-Рішень.

DeviceLock DLP

Модуль DeviceLock Discovery є автономним продуктом у складі DLP-системи DeviceLock DLP від компанії Смарт Лайн Інк. Підсистема здатна усувати виявлені порушення інформаційної безпеки шляхом звичайного або гарантованого видалення документів, видалення контейнерів (якщо файл перебуває в архіві або усередині контейнера), установки прав розмежування доступу до файлу й шифрування.

Підсистема може працювати як із застосуванням агентів, установлюваних на робочі станції співробітників і файлові сервера, так і без них, виконуючи віддалене серверне сканування, а також використовуючи обидва способи розгортання продукту.

Особливості DeviceLock Discovery:

- Можливість виконання різних дій зі знайденими файлами з конфіденційною інформацією, у тому числі з тими, що знаходяться в архіві.
- Використання методу цифрових відбитків, що дозволяє класифікувати файли з урахуванням заданого рівня конфіденційності.
- Використання метаданих і розширень властивостей файлів і документів, міток класифікатора Boldon James при пошуку файлів.

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		11

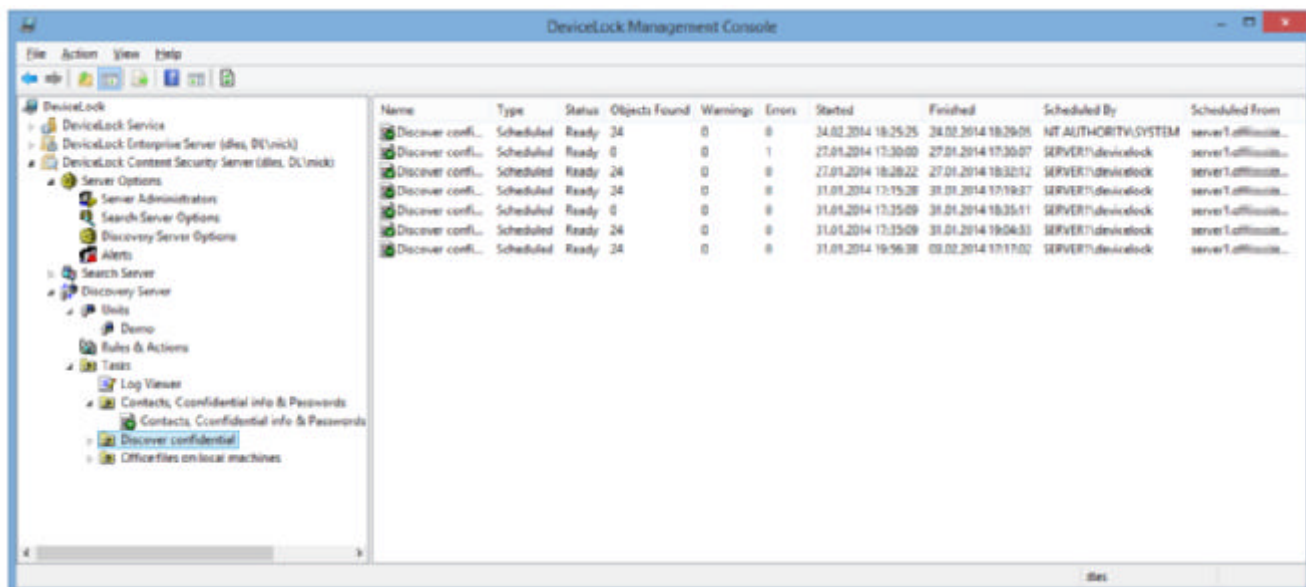


Рисунок 2.1 – Компонентів DeviceLock Discovery можна налаштувати в зручній mms-консолі

Falcongaze SecureTower

До складу DLP-системи Falcongaze SecureTower від компанії Falcongaze також входить модуль, відповідальний за індексування робочих станцій співробітників, – сервіс обробки даних. Він дозволяє робити швидкий пошук по всіх комп'ютерах у локальній мережі організації в автоматичному й ручному режимі. Контроль файлових систем заснований на зіставленні контрольних сум заданих файлів з файлами, що зберігаються на контрольованому комп'ютері. Сервіс обробки даних дозволяє робити пошук за іменем файлів, їхнім розміром і іншим атрибутам.

Особливості Сервісу обробки даних Falcongaze SecureTower:

- Можливості обробки й пошуку даних по планувальнику.
- Мінімальне навантаження на контрольовані робочі станції (ураховуються поточна активність користувача й періоди простою).
- Обробка безпосередньо на контрольованій станції виключає навантаження на локальну мережу.
- Можливість інтеграції з файловими серверами.

Forcepoint DLP

Модуль Data Discovery, що є частиною DLP-системи Forcepoint DLP (раніше відомої як Websense DLP) від групи компаній Forcepoint LLC, встановлюється окремим компонентом. При цьому можлива установка декількох агентських модулів, що дозволяє скоротити час сканування. Така можливість досягається за рахунок того, що система самостійно запускає агентський модуль, що перебуває ближче до досліджуваного комп'ютера.

Особливості Forcepoint DLP Data Discovery:

- Можливість пошуку файлів на серверах IBM Notes, Domino, Microsoft SharePoint, Microsoft Exchange.
- Використання стандартних методів пошуку нарівні з пошуком по цифрових відбитках.
- Можливість сканування даних у хмарних додатках, наприклад Office 365.
- Можливість видалення даних з несанкціонованих місць зберігання.

InfoWatch Traffic Monitor

До складу DLP-системи InfoWatch Traffic Monitor входить модуль Crawler («Краулер»), що дозволяє застосовувати налаштовані політики безпеки до файлів, що зберігається в корпоративній мережі.

Такими файлами можуть бути скани договорів з печатками, фотографії паспортів, вивантаження баз даних, креслення й багато інших типів даних, підтримувані аналітичними інструментами Traffic Monitor.

Розклад завдань Crawler настраюється у веб-консолі DLP Traffic Monitor, де як параметри пошуку можна вибрати мережні вузли, маски оброблюваних файлів, обмеження по розмірі файлів, а також конкретні папки.

Відповідно до налаштованих політиків система формує докладні звіти, а також виконує дії по виявлених інцидентах (відправляє повідомлення адміністраторові безпеки, виділяє кольором проблемний об'єкт).

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		13

InfoWatch Traffic Monitor може проактивно виявляти копіювання конфіденційних даних у загальну мережну папку.

Це дозволяє зафіксувати дію зломисника поза залежністю від того, чи встиг відробити пошук Crawler до того, як файли передані спільникові й віддалені з мережної папки.

Особливості «Crawler» InfoWatch Traffic Monitor:

- Сканування локальних дисків робочих станцій під керуванням операційних систем Microsoft Windows; Server.
- Сканування файлів по протоколі SMB.
- Сканування файлового сховища SharePoint.
- Збереження тінювих копій файлів на сервері, якщо це порушує політики безпеки.

McAfee DLP

Модуль Endpoint Discovery, що входить до складу McAfee DLP від компанії McAfee, Incorporated, являє собою рішення, що встановлюється на комп'ютери користувачів і сервери.

Компонент дозволяє сканувати локальні файли системи й сховища електронних листів (у форматі PST, OST), аналізуючи знайдені файли відповідно до встановлених правил. Залежно від політики безпеки, несанкціоновані файли можуть бути скопійовані, переміщені, зашифровані, переміщені на карантин, відзначені тегами, а також система може змінити права доступу до файлу. У той же час в McAfee є окремий продукт для пошуку конфіденційних даних – McAfee DLP Discover.

Як джерела даних можуть також виступати сервери, мережні ресурси, бази даних і хмарні сховища. При цьому система здатна робити класифікацію даних за критеріями важливості для конкретної організації. А у випадку виявлення порушень політик безпеки система відправить повідомлення адміністраторам.

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		14

Особливості McAfee Endpoint Discovery:

- Можливість налаштування дій, які необхідно виконати зі знайденими файлами.
- Можливість запуску модуля від імені користувача на своїй робочій станції, включаючи налаштування прав для відновлення випадково віддалених документів.
- Гнучке налаштування розкладу перевірок, що дозволяє задати дати не тільки початку сканування, але і його закінчення.
- Можливість припинення сканування у випадку перевищення необхідних ресурсів (процесор і ОЗП) для виконання завдання.

Solar Dozor

Модуль Dozor File Crawler, що входить до складу Solar Dozor, призначений для моніторингу файлових ресурсів у локальній мережі організації з можливістю активної протидії порушенням, для моніторингу хмарних сховищ, сканування корпоративного поштового сервера, а також побудови карти мережі ресурсів організації.

Модуль Dozor File Crawler Solar Dozor входить до складу DLP-системи Solar Dozor і не вимагає окремої установки.

Особливості Dozor File Crawler:

- Сканування вузлів локальної мережі, файлових сховищ, розташованих у локальній мережі організації, а також сканування на хмарних сховищах OneDrive.
- Ретроспективне сканування поштового сервера по протоколі IMAP з метою аналізу архіву електронних листів, а також сканування архівів тіньового копіювання, у тому числі багатотомних архівів.
- Активна протидія порушенням правил зберігання даних, що захищаються.
- У випадку виявлення порушення політики безпеки краулер може виконати одне із заданих дій: замінити файлом-повідомленням, копіювати, перемістити в спеціальне або карантинне сховище.

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		15

- Гнучке налаштування завдань сканування: розклад, періодичність запуску завдань сканування, пошук по різних атрибутах.
- Оповіщення по електронній пошті користувача або адміністратора безпеки про результати виконання завдання, у тому числі про дії, зроблених з файлами.

Symantec DLP

Модуль Network Discover із состава Symantec DLP від компанії Symantec дозволяє виявляти конфіденційні дані, що зберігаються на файлових серверах, веб-сайтах, базах даних, локальних комп'ютерах і платформах спільної роботи.

Особливості Symantec DLP Network Discover:

- Широкий охопит сховищ інформації для пошуку (бази даних SQL, поштові сервера Microsoft Exchange, корпоративні портали Microsoft SharePoint, системи документообігу Lotus Notes, Documentum, Livelink).
- Можливість сканування робочих станцій як під керуванням операційної системи Windows, так і Linux, Solaris, AIX.
- Можливість перевірки політик контролю доступу й шифрування файлів.

Zecurion DLP

Система Zecurion Discovery (Zdiscovery) дозволяє в режимі реального часу виявляти місця зберігання конфіденційної інформації в корпоративній мережі за допомогою спеціальних агентів. Принцип роботи Zecurion Discovery заснований на гібридному аналізі, що складається з більш ніж 10 сучасних технологій детектування. Всі налаштування модуля Zecurion Discovery виробляються в єдиної веб-консолі Zecurion DLP.

Система виконує аналіз даних із всіх пристроїв, які операційна система вважає логічними дисками, пошук виробляється в тому числі й з «схованих дисків». При цьому в процесі роботи визначається інформація, що повинна захищатися в рамках політик безпеки організації.

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		16

Особливості Zecurion Zdiscovery:

- Підтримка операційних систем Microsoft Windows 7/8/10; Server 2008 R2/2012/2012 R2/2016.
- Виконання різних дій зі знайденими файлами, наприклад видалення або переміщення в спеціальні сховища.
- Оповіщення співробітника про те, що на його комп'ютері розташовується критична інформація.
- Використання навчальної технології пошуку SmartID, методу опорних векторів SVM і інших технологій контентного аналізу.

Висновки

Як видно з поточного огляду, підсистеми Discovery для пошуку конфіденційних даних у корпоративній мережі є частиною більшості відомих на ринку DLP-систем. Це можна пояснити тим, що для впровадження системи захисту від витоків конфіденційної інформації в першу чергу необхідно визначитися, що саме буде потрібно захищати, провести категоризацію наявних даних, правильно оцінити ризики й застосувати політики безпеки. У цьому ланцюжку Discovery DLP можуть застосовуватися для пошуку місць зберігання даних, а також як потужний інструмент проведення розслідування інциденту витоку. Коли потрібно з'ясувати, де зберігаються або зберігалися певні файли й хто саме мав до них доступ.

Функції різних підсистем пошуку конфіденційної інформації, як вітчизняних, так і закордонних, не сильно відрізняються друг від друга. Їхній загальний принцип полягає в можливості сканування робочих станцій, мережних або хмарних сховищ відповідно до правил і політиками контентної фільтрації, налаштованими в DLP-системі. Системи можуть розрізнятися по якості аналізу й індексації файлів, кількості підтримуваних платформ зберігання й політикам, застосовуваним відносно несанкціонованих копій файлів.

Проте перед адміністраторами безпеки не стоїть пряма ціль – вибрати кращу підсистему пошуку даних. Як правило, вивчаються комплексні можливості

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		17

DLP-системи в цілому. Проте розроблювачі DLP-систем розвивають підсистеми Discovery DLP, додаючи цікаві функції для адміністраторів безпеки, наприклад складання контентних маршрутів файлів з конфіденційною інформацією, а також побудова «карти ризиків» на базі зібраної інформації, що відбиває критичність ресурсів, що захищаються, і необхідність організувати додатковий захист важливих файлів.

2.2 Обґрунтування вибору засобів для побудови системи кібербезпеки 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 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.

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		19

– 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.

– Неефективна 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,

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		20

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 веброзробки. 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, перетворювати, розділяти, об'єднувати або видаляти файли, перевіряти їх 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.

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		22

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 кібербезпеки для автоматизованого захисту корпоративної мережі.

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

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 кібербезпеки 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 кібербезпеки 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-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		23

3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ

3.1 Опис функціонування системи

2026 рік знаменує собою остаточний вступ глобальної кібербезпеки в еру війни зі швидкістю машин. Ландшафт загроз мережевій безпеці перетворився з серії ізольованих викликів периметральній обороні на багатовимірне, повсюдне поле битви, де автономні агенти – як наступальні, так і оборонні – диктують темп виживання. Оскільки організації інтегрують генеративний штучний інтелект (ШІ), розподілені периферійні обчислення, підключення 6G та Інтернет речей (IoT) у структуру своєї щоденної діяльності, поверхня атаки розширилася за межі традиційного людського моніторингу.

У центрі цієї трансформації знаходиться приголомшлива економічна реальність кіберзлочинності, яка, за прогнозами, коштуватиме світовій економіці 10,5 трильйонів доларів щорічно у 2026 році. Ця фінансова криза зумовлена індустріалізацією програм-вимагачів, ускладненням соціальної інженерії на базі штучного інтелекту та системними вразливостями, властивими гіперпов'язаним глобальним ланцюгам поставок. Для професійних колег, які орієнтуються в цьому середовищі, розуміння нюансів цього ландшафту вже не є просто вимогою ІТ; це фундаментальний стовп організаційної стійкості та стратегічного виживання.

Визначення ландшафту загроз 2026 року: що це таке?

У сучасній парадигмі «ландшафт загроз» визначається як сукупний набір вразливостей, активних супротивників та потенційних векторів атак, які ставлять під загрозу конфіденційність, цілісність та доступність цифрових та фізичних систем. До 2026 року це визначення вийшло за рамки концепції захисту внутрішніх серверів або робочих станцій. Тепер воно охоплює всю цифрову екосистему, включаючи хмарні робочі навантаження, автономних мобільних

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		24

роботів, медичні пристрої та агентні об'єкти штучного інтелекту, що населяють корпоративні мережі.

Визначальною характеристикою ландшафту 2026 року є «Модель агентної загрози». Ця модель описує зміну, коли актори загроз – від національних держав, таких як групи, що атакують німецькі політичні партії, до децентралізованих синдикатів програм-вимагачів – розгортають автономних агентів штучного інтелекту, які можуть самостійно міркувати, адаптувати свою тактику в режимі реального часу та виконувати цілі цикли атак без втручання людини. Ці агенти здатні виявляти вразливості, використовувати користувацькі експлойти як зброю та орієнтуватися у внутрішніх сегментах мережі з рівнем точності та швидкості, що робить захист на основі сигнатур застарілим.

Концептуальна межа між цифровою та фізичною безпекою фактично розмилася. Кібербезпека тепер нерозривно пов'язана з фізичною безпекою, особливо в промислових та медичних закладах, де порушення мережі може призвести до несправності роботизованих хірургічних рук, турбін електромережі або автономних логістичних парків.

Стратегічне впровадження: як ми використовуємо мережеву безпеку?

У 2026 році застосування мережевої безпеки змістилося від реактивного підходу «блокування та усунення» до проактивної, орієнтованої на ідентифікацію моделі, зосередженої на Zero Trust та Secure Access Service Edge (SASE).

Площина керування, орієнтована на ідентичність

Ідентичність – це новий периметр. Аналіз показує, що 75% порушень зараз пов'язані з використанням скомпрометованих легітимних облікових даних, тобто зловмисники «входять» в систему, а не «зламують». Щоб протидіяти цьому, організації впроваджують децентралізовані системи ідентифікації та безпарольну автентифікацію за допомогою біометрії та апаратних ключів безпеки.

Використання безпеки тепер динамічне, а не статичне. Замість надання користувачеві доступу до всієї мережі після входу в систему, модель

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		25

«Безперервної довіри» оцінює кожен запит на основі оцінки ризиків у режимі реального часу. Наприклад, якщо співробітник намагається отримати доступ до фінансової бази даних з нового пристрою у високоризикованому географічному місці, механізм безпеки може дозволити доступ лише до неконфіденційних папок або вимагати негайної «підвищеної» перевірки за допомогою ключа, сумісного з FIDO2.

SASE та єдині мережеві/безпекові операції

Безпечний доступ до сервісів на межі (SASE) – це основна платформа для захисту сучасного розподіленого підприємства. SASE поєднує програмно-визначені глобальні мережі (SD-WAN) з функціями безпекового сервісу на межі (SSE), включаючи брокери безпеки хмарного доступу (CASB), безпечні веб-шлюзи (SWG) та брандмауер як послугу (FWaaS).

Впровадження SASE дозволяє організаціям застосовувати узгоджені політики в хмарних, периферійних та локальних середовищах. Це критично важливо, оскільки організації все більше покладаються на гібридні робочі сили та багатохмарні архітектури. Завдяки перенесенню безпеки на периферію – точку, найближчу до користувача та даних – затримка зменшується, водночас захист конфіденційної інформації зберігається в середньому в 77 SaaS-додатках та понад 500-1000 API, якими керує типове підприємство.

Рівень розвідки: як ми здійснюємо моніторинг та аналіз?

Моніторинг та аналіз у 2026 році були трансформовані завдяки моделі «AI SOC + Human Ally». Традиційна структура Центру операцій безпеки (SOC), яка спиралася на рівні аналітиків-людей, які вручну досліджували сповіщення, зруйнувалась під вагою величезного обсягу даних. Команди SOC зараз отримують в середньому 2992 сповіщення безпеки на день, причому 63% залишаються без уваги у застарілих системах.

Автономний моніторинг через робочі процеси агентів

Сучасний моніторинг використовує агентні платформи SOC, які обробляють збагачення, кореляцію та початкове сортування на рівні машинної

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		26

швидкості. Ці системи використовують поведінкову аналітику (UEBA) для встановлення базових показників для кожного користувача та сутності, позначаючи незначні відхилення, які статичні правила пропускають, – такі як моделі «неможливих переміщень» або незвичайні обсяги витоку даних. Коли виявляється потенційна загроза, агент штучного інтелекту не просто генерує сповіщення; він ініціює автономне розслідування. Агент запитує SIEM, витягує журнали з відповідних кінцевих точок та хмарних робочих навантажень, збагачує дані глобальною інформацією про загрози та створює структурований звіт про розслідування за лічені секунди. Цей процес, відомий як «Логіка виявлення як код», дозволяє забезпечити час «від сповіщення до сортування» приблизно дві хвилини, порівняно з годинами або днями в традиційних середовищах, керованих людиною.

Складні методи аналізу загроз

Аналіз перейшов від зіставлення сигнатур до «прогнозової оцінки ризиків» та «логіки, що базується на штучному інтелекті». Провідні платформи, такі як Prophet Security або Cortex XSIAM від Palo Alto Networks, використовують багатоагентні системи, які можуть «міркувати» як людина-слідчий, визначаючи першопричину інциденту в розподілених середовищах.

Процес кореляції тепер є цілісним і охоплює всю телеметрію підприємства завдяки розширеному виявленню та реагуванню (XDR). XDR об'єднує видимість між кінцевими точками, мережею, хмарою та ідентифікаторами, дозволяючи аналітикам бачити весь «ланцюжок атаки» в режимі реального часу. Наприклад, якщо зловмисник використовує скомпрометовану ідентифікатор для доступу до сервера, а потім встановлює шкідливий драйвер, XDR співвідносить ці, здавалося б, не пов'язані між собою події в один високоточний інцидент.

Межі розгортання: де використовується мережева безпека?

У 2026 році мережева безпека розгортається у все більш різноманітних середовищах, кожне з яких має унікальні технічні вимоги та профілі ризиків.

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		27

Корпоративна хмара та гібридні екосистеми

Для сучасного підприємства безпека застосовується через політику як код, вбудовану безпосередньо в конвеєр CI/CD. Це гарантує, що нові хмарні екземпляри або програми автоматично успадковують систему безпеки організації, коли запускаються. Ідентифікація тут є основною площиною керування, а SASE об'єднує мережевий та ідентифікаційний контекст для захисту даних на основі їхньої конфіденційності.

Промислові системи керування (ІКС) та ОТ

Безпека операційних технологій (ОТ) захищає виробниче обладнання та фізичні процеси, які забезпечують роботу інфраструктури. «Модель Пердью» залишається фундаментальною структурою, але тепер вона доповнена сегментацією з урахуванням ідентифікації. Оскільки системи ОТ, такі як SCADA та ПЛК, часто мають довгі життєві цикли (15–30+ років) і їх нелегко виправити, безпека застосовується за допомогою мікросегментації мережі та постійного моніторингу «темного» трафіку ОТ.

Охорона здоров'я та медичні технології

Лікарні зараз є екосистемами розумного догляду, що покладаються на підключені медичні пристрої та платформи дистанційного моніторингу. Засоби безпеки розгортаються для захисту як «вітальні», так і лікарняної палати, а допомога лікарняного рівня надається вдома через віртуальні палати. Програми-вимагачі в цьому секторі розглядаються як пріоритет безпеки пацієнтів, що вимагає надійного управління даними та захисту електронних медичних записів (ЕМЗ) від соціальної інженерії на основі штучного інтелекту.

Мережі Edge та 6G

Розгортання 6G приносить архітектуру, налаштовану на штучний інтелект, та інтегровані системи зондування та зв'язку (ISAC). Безпека розгортається безпосередньо на периферії мережі для обробки масивного трафіку з високим навантаженням від фізичного штучного інтелекту (дронів, роботів, транспортних засобів). У цих середовищах швидкість та інтелектуальна обробка в джерелі

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		28

важливіші за пропускну здатність, оскільки рішення, чутливі до затримки, повинні прийматися за мікросекунди, щоб забезпечити безпеку автономних систем.

Ринковий попит: економічний двигун мережевої безпеки

Глобальний попит на мережеву безпеку досяг безпрецедентних висот, зумовлений ескалацією ландшафту загроз та зростанням дефіциту талантів у сфері кібербезпеки.

Тенденції зарплат та професійний попит

«Дефіцит талантів» – це глобальна реальність, оскільки 67% організацій повідомляють про помірний або критичний дефіцит навичок. Це призвело до появи дуже конкурентних компенсаційних пакетів для кваліфікованих фахівців.

Провідними роботодавцями в цій сфері є такі світові гіганти, як TCS, Infosys, Wipro та Accenture, а також спеціалізовані фірми, як QNu Labs та CrowdStrike. Фахівці з такими сертифікатами, як CEH, CISSP та OSCP, можуть отримувати на 20–50% вищу зарплату, ніж їхні колеги без сертифікатів.

Виправлення неполадок мережевої безпеки: підключення та неправильні конфігурації

Підтримка безпеки мережі вимагає систематичного підходу до усунення проблем із підключенням та помилок конфігурації. Неправильні конфігурації, такі як відкриті порти, облікові дані за замовчуванням та неправильний порядок ACL, залишаються легкими точками входу для злоумисників.

Вирішення проблем із неправильними конфігураціями ACL та брандмауера

Центр операцій безпеки повинен забезпечувати явні заборони та підтримувати чисті, добре керовані набори правил, щоб запобігти «накопиченню ACL» – накопиченню застарілих, невикористаних правил, які розширюють поверхню атаки.

Діагностика вузьких місць підключення

Збої з'єднання часто проявляються у вигляді недоступних серверів або

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		29

втрати пакетів. 10-етапний контрольний список допомагає аналітикам швидко визначити першопричину:

1. Визначте проблему: Зберіть повідомлення про помилки та симптоми користувачів.

2. Визначення області застосування: Визначення того, чи проблема локалізована у віртуальній локальній мережі, сайті чи певній групі користувачів.

3. Перевірка фізичного рівня: перевірте кабелі, приймачі та індикатори з'єднання.

4. Стан пристрою: Перевірте використання процесора/пам'яті та температуру на маршрутизаторах і брандмауерах.

5. Конфігурація IP: Перевірка масок підмережі, шлюзів та стану оренди DHCP.

6. Мережевий шлях: Використовуйте ping та traceroute, щоб знайти, куди падають пакети.

7. Розв'язання DNS: Тестування прямого/зворотного пошуку та очищення кешів.

8. Огляд VLAN/сегментів: Перевірка таблиць маршрутизації та налаштувань маршрутизації між VLAN.

9. Аудит ACL/безпеки: Виявлення забороненого трафіку в журналах брандмауера, пов'язаного з інцидентом.

10. Документація: Запишіть діаграми роздільної здатності та оновіть їх, щоб запобігти повторенню.

Використання в технологіях: квантова стійкість та фізичний штучний інтелект

Технології мережевої безпеки у 2026 році відкривають нові горизонти в квантовій стійкості та захисті кіберфізичних систем.

Квантово-безпечна міграція

Квантові обчислення загрожують зробити сучасну асиметричну криптографію (RSA, ECC) небезпечною до 2030 року. У 2026 році організації

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		30

переходять на постквантові криптографічні (PQC) алгоритми. Це передбачає створення криптографічної інвентаризації та узгодження з дорожніми картами, затвердженими NIST. Такі компанії, як QNu Labs, надають квантовий розподіл ключів (QKD) та квантові генератори випадкових чисел (QRNG) для захисту довгоживучих даних від атак типу «Збери зараз, розшифруй пізніше».

Фізичний ШІ та роботизоване управління

Зростання «фізичного штучного інтелекту» – поєднання робототехніки, сенсорів та інтелекту – розширює поверхню атаки у фізичний світ. Технології безпеки тепер повинні керувати автономними агентами, які займаються промисловою точністю, логістикою лікарень та управлінням енергетичною мережею. Це вимагає мереж з урахуванням обчислювальних можливостей, де сама структура зв'язку забезпечує дотримання протоколів конфіденційності даних та безпеки в режимі реального часу, ефективно автоматизуючи довіру до автономних систем.

Стратегічне значення мережевої безпеки

Важливість мережевої безпеки зросла з технічної необхідності до питання національної безпеки, економічної стабільності та людського життя.

Національна безпека та політична цілісність

Атака на німецьку політичну партію Die Linke групою вимагачів Qilin у березні 2026 року підкреслює геополітичний вимір кібербезпеки. Коли політичні структури стають ціллю, ризик пов'язаний не лише з втратою даних, а й з політичним втручанням та розкриттям конфіденційних комунікацій, які можуть вплинути на демократичні процеси.

Відповідальність регуляторних органів та відповідальність ради директорів

У 2026 році кібербезпека є імперативом на рівні ради директорів. Глобальна регуляторна волатильність, включаючи Закон ЄС про кіберстійкість, Директиву NIS2 та різні закони про штучний інтелект на рівні штатів США, означає, що керівники та ради директорів тепер несуть дедалі більшу

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		31

відповідальність за порушення вимог. Бездіяльність може призвести до суттєвих штрафів, втрати бізнесу та незворотної шкоди репутації.

Економічна стійкість та рентабельність інвестицій

Проактивна безпека на основі штучного інтелекту – це вже не просто оборонні витрати, а високодохідна стратегічна інвестиція. Хоча прогнози окремих постачальників вказують на потенційну рентабельність інвестицій у 400% для платформ на основі штучного інтелекту, це значення підтверджується ширшими галузевими дослідженнями.

У звіті IBM «Вартість порушення даних» за 2025 рік зазначається, що організації, які впроваджують штучний інтелект та автоматизацію безпеки, значно заощадили в середньому 2,22 мільйона доларів на витратах на порушення порівняно з тими, хто їх не впроваджував. Крім того, дослідження загального економічного впливу (TEI) Forrester Research послідовно показують, що уніфікована архітектура SASE та Zero Trust забезпечує трирічну рентабельність інвестицій понад 200%, значною мірою завдяки зменшенню «радіуса вибуху» атак та нижчим операційним витратам. Скорочуючи час реагування на порушення на 80 днів та заощаджуючи в середньому 1,9 мільйона доларів на інцидент, організації надають пріоритет створенню основи для сталого цифрового зростання.

Ландшафт загроз 2026 року вимагає фундаментальної зміни підходу фахівців до мережевої безпеки. Ми вийшли за межі епохи реактивного захисту та перейшли до ери, де «превентивна кібербезпека» – використання штучного інтелекту для виявлення та нейтралізації загроз до їх реалізації – є новим стандартом.

Для сучасного технологічного лідера пріоритети чіткі: інвестувати в платформи на основі штучного інтелекту, забезпечити безпеку площини контролю ідентифікації та підготуватися до постквантового майбутнього. Зближення геополітики, автономного штучного інтелекту та зв'язку 6G означає, що кібербезпека – це вже не просто захист даних; це захист самих основ нашого

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		32

цифрового суспільства. Організації, які освоюють цей ландшафт завдяки постійному моніторингу, агентним робочим процесам та відданості кіберстійкості, не лише переживуть «зсув на основі штучного інтелекту», але й очолять перехід до більш безпечного, автономного та надійного майбутнього.

3.2 Розробка структурної схеми

Корпоративні мережі є основою будь-якої організації, що забезпечує спілкування між співробітниками, обмін файлами та доступ до важливих ресурсів. Однак, оскільки вони централізують величезну кількість конфіденційних даних, вони є головними цілями для хакерів та кіберзлочинців.

Зламана корпоративна мережа може призвести до руйнівних наслідків, включаючи крадіжку даних, збоїв в роботі, фінансові втрати та зниження довіри клієнтів і партнерів. З цієї причини захист корпоративної мережі має бути головним пріоритетом для будь-якого бізнесу, незалежно від його розміру чи галузі.

Поширені загрози для корпоративних мереж

Щоб зрозуміти важливість мережевої безпеки, вкрай важливо розпізнати основні загрози, які можуть поставити під загрозу інфраструктуру компанії.

– Атаки шкідливого програмного забезпечення та програм-вимагачів. Шкідливе програмне забезпечення, включаючи віруси, трояни та шпигунські програми, може заражати корпоративні системи та красти критично важливу інформацію. Зокрема, програми-вимагачі шифрують файли компанії та вимагають викуп за їх розголошення, що потенційно паралізує бізнес-операції.

– Фішинг та соціальна інженерія. Фішингові атаки є одними з найефективніших методів отримання доступу до корпоративних мереж. За допомогою оманливих електронних листів або повідомлень хакери обманом змушують співробітників розкрити облікові дані для входу або завантажити шкідливе програмне забезпечення.

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		33

– DDoS-атаки (розподілена відмова в обслуговуванні). Мета DDoS-атаки – перевантажити корпоративні сервери надмірним інтернет-трафіком, що робить сервіси непридатними для використання. Такі атаки можуть призвести до збоїв у роботі та репутаційної шкоди.

– Несанкціонований доступ та крадіжка облікових даних. Якщо корпоративна мережа недостатньо захищена, хакери або зловмисники можуть отримати доступ, використовуючи викрадені облікові дані або слабкі паролі, що наражає на небезпеку конфіденційну інформацію.

– Використання вразливостей програмного забезпечення. Кожна програмна програма, включаючи операційні системи, може містити недоліки безпеки. Якщо їх не оновлювати регулярно, ці вразливості можуть бути використані хакерами для проникнення в корпоративний мережевий трафік.

Наслідки незахищеної корпоративної мережі

Компанія, яка не інвестує в захист корпоративної мережі, ризикує серйозними наслідками, які можуть поставити під загрозу її довгострокову діяльність.

– Крадіжка та втрата даних. Бізнес-інформацію, від фінансових записів до стратегічних планів, можна викрасти та продати в даркнеті або використати для вимагання та шахрайства. Перебої в роботі. Кібератака може блокувати доступ до критично важливих систем, що призводить до затримок в роботі та значних фінансових втрат.

– Репутаційна шкода. Витік даних може підірвати довіру клієнтів та ділових партнерів, що призведе до втрати авторитету та відтоку клієнтів.

– Високі витрати на відновлення. Після кібератаки компанія повинна нести значні витрати на відновлення даних, відновлення систем та підвищення безпеки мережі для запобігання майбутнім інцидентам.

Як захистити корпоративну мережу від кібератак

Ефективний підхід до захисту корпоративної мережі спирається на поєднання передових технологій, постійного моніторингу та найкращих практик

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		34

управління безпекою. Нижче наведено найкращі стратегії для запобігання атакам та забезпечення високого рівня безпеки.

Підтримуйте системи та програмне забезпечення в актуальному стані

Одним із найпоширеніших методів, що використовуються хакерами для обходу захисту корпоративної мережі, є використання вразливостей у системах і програмах.

Будь-яке програмне забезпечення, включаючи операційну систему, може містити діри в безпеці, які, якщо їх не виправити, стають шлюзами для кіберзлочинців. SSL-сертифікат, що захищає дані та інформацію, захищає кіберщит.

Щоб зменшити цей ризик, компанії повинні:

- Своєчасно встановлюйте оновлення та патчі безпеки;
- Використовуйте інструменти управління вразливостями для виявлення та усунення слабких місць системи;
- Видаліть застаріле програмне забезпечення, яке більше не отримує оновлень безпеки.

Ігнорування оновлень наражає бізнес на такі загрози, як програми-вимагачі, шкідливе програмне забезпечення та атаки нульового дня, які використовують невідомі недоліки безпеки.

Впроваджуйте брандмауери та системи виявлення вторгнень

Брандмауери служать першою лінією захисту від кіберзагроз, фільтруючи вхідний та вихідний мережевий трафік для блокування несанкціонованого доступу.

Крім того, використання систем виявлення та запобігання вторгненням (IDS/IPS) має вирішальне значення для моніторингу мережевого трафіку та виявлення підозрілої активності.

Найкращі практики використання брандмауерів та IDS/IPS включають:

- Налаштування суворих правил доступу для обмеження підключень лише авторизованими користувачами;

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		35

- Моніторинг мережевих журналів для виявлення незвичайної активності;
- Використання брандмауерів наступного покоління (NGFW) з розширеними функціями перевірки трафіку.

Безпечний доступ до мережі з розширеною автентифікацією

Хакери часто намагаються отримати доступ до мереж, використовуючи слабкі або викрадені облікові дані. Щоб протидіяти цьому ризику, компанії повинні впроваджувати безпечну систему автентифікації.

До найефективніших стратегій належать:

- Багатофакторна автентифікація (MFA) вимагає більше одного методу перевірки (пароль + код ОТР, відбиток пальця тощо).
- Суворе керування паролями Використовуйте складні паролі та регулярно їх змінюйте.
- Обмеження прав доступу. Надавайте доступ до даних і системи лише тим, хто дійсно в цьому потребує.

Завдяки надійній системі автентифікації, ймовірність проникнення хакерів або неавторизованих користувачів у корпоративні мережі значно знижується.

Сегментуйте мережу, щоб мінімізувати ризики

Сегментація мережі розділяє інфраструктуру компанії на кілька підмереж, кожна з яких має певний рівень безпеки. Такий підхід обмежує збитки у разі атаки, запобігаючи поширенню шкідливого програмного забезпечення по всій системі.

Приклади сегментації мережі включають:

- Відокремлення адміністративних мереж від мереж співробітників;
- Ізоляція пристроїв Інтернету речей та мобільних пристроїв для запобігання вразливостям;
- Створення VLAN (віртуальних локальних мереж) для відділів з різними потребами безпеки.

Ця стратегія покращує безпеку та управління мережевим трафіком, ускладнюючи для хакерів проникнення в цілу систему.

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		36

Постійно контролювати мережевий трафік

Моніторинг мережевого трафіку є важливим для виявлення підозрілої активності в режимі реального часу. Компанії можуть використовувати інструменти моніторингу мережі та розвідки загроз для аналізу мережевого трафіку та виявлення аномалій.

Найкращі практики для ефективного моніторингу включають:

- Впровадження SIEM-систем (систем управління інформацією та подіями безпеки) для збору та аналізу мережевих журналів;
- Використання технологій поведінкового аналізу для виявлення незвичайних моделей доступу;
- Налаштування автоматичних сповіщень для негайного реагування на потенційні атаки.

Проактивний моніторинг допомагає запобігти кібератакам, перш ніж вони завдадуть значної шкоди.

Безпечні мобільні пристрої та віддалені працівники

Зі зростанням використання мобільних пристроїв та віддаленої роботи компанії повинні забезпечити захист і зовнішніх пристроїв. Смартфони, ноутбуки та планшети, підключені до корпоративної мережі, можуть бути вразливими, якщо ними не керувати належним чином.

Основні заходи безпеки для мобільних пристроїв включають:

- впроваджувати рішення для керування мобільними пристроями (MDM) для контролю використання корпоративних пристроїв;
- вимагати використання віртуальних приватних мереж (VPN) для захисту віддалених з'єднань;
- шифрувати конфіденційні дані для захисту у разі крадіжки або втрати пристрою.

Захист мобільних пристроїв запобігає порушенням безпеки та підтримує високий рівень безпеки корпоративної мережі.

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		37

Навчайте співробітників з питань кібербезпеки

Більшість кібератак використовують людські помилки, такі як натискання на фішингові електронні листи або використання слабких паролів. Навчання співробітників є ключовим компонентом захисту корпоративної мережі.

Компанії повинні:

- Регулярно проводити навчання з кібербезпеки.
- Імітуйте фішингові атаки, щоб навчити співробітників розпізнавати підозрілі електронні листи.
- Встановіть чіткі корпоративні політики щодо обробки даних та використання пристроїв.
- Освічені працівники є одним із найкращих захистів від кіберзагроз.

Як хакери можуть обійти захист корпоративної мережі

Навіть за наявності потужного захисту мережі, кіберзлочинці постійно розробляють дедалі досконаліші методи обходу безпеки корпоративної мережі. Деякі поширені методи включають:

- Фішингові атаки. За допомогою оманливих електронних листів або повідомлень хакери обманом змушують користувачів надати облікові дані для входу.
- Шкідливе програмне забезпечення та програми-вимагачі. Після встановлення в корпоративній системі вони можуть шифрувати дані та блокувати важливі операції.
- Атаки типу «людина посередині». Ці атаки перехоплюють зв'язок між користувачами та серверами з метою викрадення конфіденційної інформації.
- Використання вразливостей програмного забезпечення. Якщо системи не оновлюються, хакери можуть скористатися недоліками безпеки, щоб отримати віддалений контроль над корпоративними пристроями.

З цієї причини хороша стратегія безпеки повинна базуватися на багаторівневому підході, що поєднує рішення захисту для кожної потенційної точки входу.

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		38

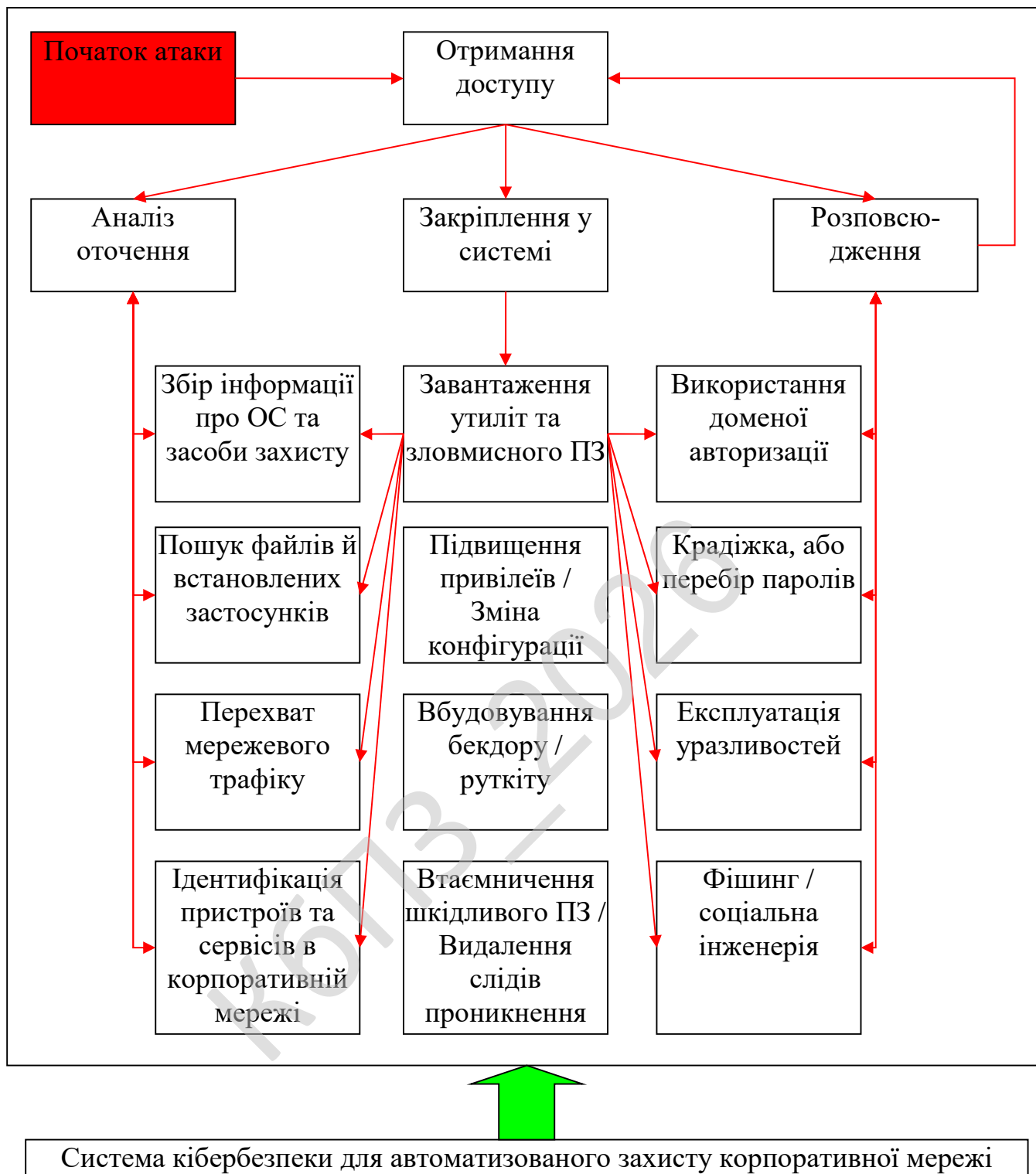


Рисунок 3.1 – Структурна схема системи

Мобільні пристрої та безпека: зростаючий виклик

Використання мобільних пристроїв у компаніях створює проблеми безпеки. Смартфони, планшети та ноутбуки можуть стати слабкими місцями в мережі, якщо вони не захищені належним чином.

Щоб зменшити ризики, компанії повинні:

- Впроваджуйте рішення для керування мобільними пристроями (MDM) для контролю доступу та використання;
- Заборонити несанкціонованим персональним пристроям підключатися до корпоративних мереж ;
- Використовуйте VPN для забезпечення безпечного з'єднання, коли співробітники працюють віддалено;
- Шифруйте дані для захисту у разі крадіжки або втрати пристрою.

Після того, як зловмисник одержав контроль над якою-небудь користувальницькою системою в корпоративній мережі, всі подальші події укладаються в три послідовних етапи: закріплення в системі, аналіз оточення й поширення. Є безліч варіантів реалізації кожного з описаних етапів, що розрізняються технічними методами, стратегією й тактикою. Можливі варіанти дій зловмисника, спрямованих на закріплення, аналіз і поширення в корпоративній мережі, зображені на структурній схемі.

3.3 Розробка функціональної схеми

Для подолання труднощів у слабоформалізованих ситуаціях більше високий якісний рівень оперативного управління припускає забезпечення необхідної й достатньої інтелектуальної підтримки. Запропонована в роботі функціональна схема системи кібербезпеки для автоматизованого захисту корпоративної мережі наведена на рисунку 3.2.

У системі кібербезпеки для автоматизованого захисту корпоративної мережі пропонується використовувати інтелектуальні технології:

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		40

- механізм нечіткого логічного виводу для чисельної оцінки ймовірності атаки;
- організоване впорядкування інформації про події в базі знань;
- моделі протидії погрозам;
- прийняття рішень на вибір раціонального варіанта реагування на події безпеки.

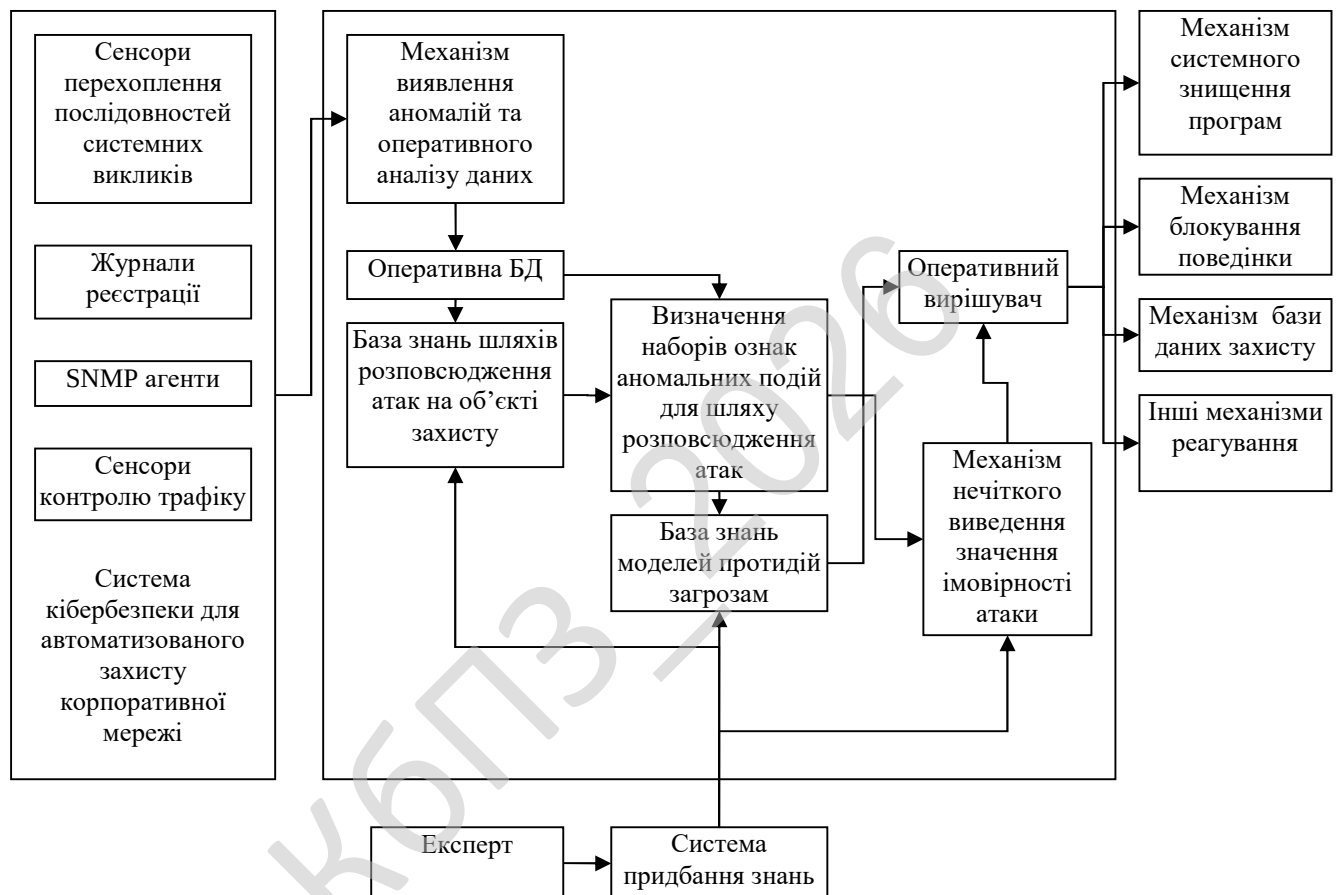


Рисунок 3.2 – Функціональна схема системи

Через необхідність максимальної структуризації розроблюваної системи й рішень, пропонується трирубіжна модель захисту, яка щонайкраще задовольняє всієї сукупності умов її розробки, експлуатації й удосконалення. Трирубіжна модель захисту – неформалізований опис комплексу програмно-апаратних засобів захисту, що є основою для розробки системи захисту:

– перший рубіж – периметр об'єкта захисту – набір функціональних підсистем, що включають засоби захисту від зовнішніх вторгнень зловмисника й потенційно можливих погроз віддаленого користувача;

– другий рубіж – набір засобів захисту мережного сегмента від віддалених і локальних мережних вторгнень;

– третій рубіж містить у собі набір засобів захисту окремого персонального комп'ютера або сервера.

У процесі організаційно-технічного управління, планування ЗІ як функція управління являє собою процес послідовного зняття невизначеності щодо структури й состава засобів захисту в СЗІ. Процес планування $P_{пл}$ раціональних наборів ЗЗ характеризується за допомогою вираження:

$$P_{пл} = \Phi \rightarrow S_r,$$

де Φ – множина функціональних підсистем для рубежу захисту;

S_r – обраний набір засобів захисту.

На першому етапі задається множина функціональних підсистем для рубежів захисту, результатом планування є командна інформація, що містить конкретні дані по розподіляються ресурсам, що, що направляється на досягнення цільового стану СЗІ.

Процес ухвалення рішення про вибір раціонального варіанта набору ЗЗ для рубежу захисту – це функція перетворення змісту інформації про вимоги, запропонованих до засобів захисту, що входить у набір, про характеристики засобів захисту, у підмножину найкращих варіантів набору $S' \subseteq S$. Множина варіантів набору:

$$S = \{S_1, K, S_r, K, S_R\},$$

де R – число варіантів альтернативних наборів, з яких здійснюється вибір.

Для вибору раціонального варіанта набору засобів захисту використовується цільова функція J :

$$S_r = J(S).$$

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		42

Сукупність відомостей, що дозволяють зіставляти варіанти наборів, це характеристики засобів захисту функціональних підсистем для рубежу – множина W , що включає в себе дві підмножини:

$$W_{зщ_l} \subset W_l \text{ і } W_{и_l} \subset W_l,$$

де $W_{зщ_l}$ – показник засобів захисту «захищеність інформації»;

$W_{и_l}$ – показник засобів захисту «витрати» для l -ої функціональної підсистеми.

На основі морфологічного підходу модель прийняття рішень на вибір раціонального варіанта набору може бути представлена у вигляді кортежу:

$$\text{ПР: } \langle \Pi, \Phi, \Pi_s, S, W_l, J, S_r(S') \rangle,$$

де Π – ціль ухвалення рішення;

Φ – вихідні дані для породження варіантів набору засобів захисту:

$$\Phi = \{\Phi_1, \Phi_2, K, \Phi_l, K, \Phi_L\};$$

Π_s – правило породження варіантів набору, що може бути представлене в аналітичному виді як векторний добуток множин:

$$S = \Phi_1 \times \Phi_2 \times K \times \Phi_l \times K \times \Phi_L,$$

де:

Φ_l – множина, що складається із засобів захисту l -ої функціональної підсистеми:

$$\Phi_l = \{A_{l1}, A_{l2}, K, A_{lm}, K, A_{lK_l}\};$$

S – множина породжених варіантів набору;

W_l – дані для вибору раціональних варіантів;

J – цільова функція для вибору раціонального набору засобів захисту(правило вибору);

S_r – раціональний набір засобів захисту.

Відзначається, що в умовах автоматизованого управління й при використанні експертної інформації в процесі ухвалення рішення можна говорити (навіть у випадку формалізованого правила вибору) про раціональне, а

не оптимальне рішення.

Відповідно до трирубіжної моделі захисту, основою планування раціонального модульного состава СЗІ є функціональні вимоги до наборів ЗЗ для кожного рубежу, які формулюються на основі нормативної документації, відповідно до рівня критичності оброблюваної інформації. Альтернативні засоби захисту для кожної функціональної підсистеми набору засобів захисту вибираються з урахуванням цих вимог. Варіантів наборів, сертифікованих по необхідному класі захищеності, може бути багато. Порівняння варіантів наборів засобів захисту пропонується робити по кількісній мері.

Для рішення завдання вибору раціональних варіантів наборів засобів захисту для рубежів захисту розробляється метод обробки знань, що використовує неформалізуємий досвід експерта в області ЗІ, що забезпечує перетворення відомостей про характеристики засобів захисту з бази знань і вивід рішення в аналітичній формі – метод формування раціонального комплексу засобів захисту для СЗІ.

1. Розробляються варіанти набору ЗЗ. Множина можливих варіантів рішення завдання вибору задається морфологічною матрицею. Розробляються морфологічні матриці засобів захисту для три рубежів.

2. Заповнюються допоміжні матриці, у яких відзначаються сумісні один з одним програмно-апаратні засоби. Допоміжна квадратна матриця сумісних рішень заповнюється в такий спосіб: для кожної пари засобів захисту різних функціональних підсистем визначається, чи сумісні вони, і результат заноситься в таблицю. Якщо ЗЗ сумісні, то функція сумісності $s(A_{lm}, A_{pr}) = 1$, у протилежному випадку $s(A_{lm}, A_{pr}) = 0$.

3. Генерується безліч рішень на вибір варіантів набору ЗЗ із униканням цієї множини до підмножини варіантів набору із сумісних між собою програмно-апаратних продуктів.

Множина $S = \{S_1, \dots, S_r, \dots, S_R\}$, що складається із всіх можливих варіантів побудови набору ЗЗ для рубежу, є декартовим добутком множин альтернатив (рядків морфологічної матриці).

Елемент множини:

$$S_r = \{(A_{1i}, A_{2j}, \dots, A_{lm}, \dots, A_{Ln}) : A_{lm} \in \Phi_l, \forall l = \overline{1, L}\},$$

де L – число функціональних підсистем для рубежу;

A_{lm} – засіб захисту для реалізації l -ої функціональної підсистеми.

Генерація множин рішень на вибір варіантів набору, що складаються із сумісних між собою ЗЗ, здійснюється в такий спосіб.

Відбувається ітераційний синтез варіантів набору, що складаються із сумісних ЗЗ: на першому кроці перебираються послідовно варіанти засобів захисту для першої підсистеми, після вибору альтернативи A_{1i} здійснюється перехід до другого кроку. На другому кроці виконується послідовний перебір варіантів засобів захисту другої підсистеми, але вибір здійснюється тільки для таких альтернатив A_{2j} , для яких функція сумісності $s(A_{1i}, A_{2j}) = 1$ і т.д. При виборі альтернатив з l -ої підсистеми вибір здійснюється тільки з таких альтернатив A_{lm} , для яких функції сумісності дорівнюють одиниці: $s(A_{1-1,m}, A_{lm}) = 1$, $s(A_{2j}, A_{lm}) = 1$, $s(A_{1i}, A_{lm}) = 1 \dots$ Таким, образом, вибір ЗЗ із кожного рядка морфологічної матриці (по одній з кожного рядка) для формування варіанта набору здійснюється тільки із сумісних між собою програмно-апаратних продуктів.

4. Подальше усікання множини S виконується методом повного перебору по заданій цільовій функції. Як цільова функція для вибору варіанта набору $S_r = \{A_{1i}, A_{2j}, \dots, A_{lm}, \dots, A_{Ln}\}$, застосовується функція:

$$J = \max_r \frac{W_{K_{3\text{ш}}}^{A_{1i}} + \dots + W_{K_{3\text{ш}}}^{A_{lm}} + \dots + W_{K_{3\text{ш}}}^{A_{Ln}}}{W_{K_{\text{и}}}^{A_{1i}} + \dots + W_{K_{\text{и}}}^{A_{lm}} + \dots + W_{K_{\text{и}}}^{A_{Ln}}},$$

де $W_{K_{зщ}}^{A_{lm}}$ – значення показника «захищеність»;

$W_{K_{и}}^{A_{lm}}$ – значення показника «витрати» засобу захисту A_{lm} .

Для оцінки засобів захисту різних функціональних підсистем наборів розробляються ієрархічні структури узагальнених критеріїв якості засобів захисту: показник «захищеність» і показник «витрати».

Критерії якості засобів захисту по ієрархії «захищеність» діляться на дві групи: показники забезпечення ефективності оперативних методів захисту й показники функціональної придатності. Критерії якості по ієрархії «витрати» діляться також на дві групи: у першу включена вартість відповідного засобу захисту, число користувачів по одній ліцензії й інші можливі економічні витрати; до другої групи витрат ставляться функціональні витрати, такі, наприклад, як падіння продуктивності інформаційної системи при використанні даного засобу захисту.

Оцінка засобів захисту й критеріїв здійснюється попарним порівнянням по методу Т. Сааті, результати приводяться в числовому виді. З використанням ієрархічних структур критеріїв якості ЗЗ обчислюються нормовані значення власних векторів засобів захисту за всіма критеріями до показників «захищеність» $K_{зщ}^1$ і «витрати» $K_{и}^1$ на підставі обробки всіх матриць попарних порівнянь із урахуванням зв'язків критеріїв.

Після вибору раціональних наборів засобів захисту для рубежів захисту отриманий раціональний модульний состав цілісного комплексу засобів захисту об'єкта, що задовольняє вимозі

$$J \rightarrow \max.$$

5. Оцінюється, чи задовольняє сформований комплекс засобів захисту вимозі:

$$C_{\Sigma} \leq C$$

де C_{Σ} – сумарні витрати на реалізацію комплексу ЗЗ;

$C_{\text{доп}}$ – виділені на реалізацію комплексу грошові ресурси.

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		46

При цьому C_{Σ} обчислюється за допомогою наступного вираження:

$$C_{\Sigma} = \sum_s \left(\sum i_s + \sum C_{j_s}^c + \sum C_{k_s}^b + C_{\text{сегм}} \right) + C_{\text{пр}},$$

де S – число мережних сегментів;

$C_{i_s}^b$ – вартість набору засобів захисту хоста, на якому обробляється інформація базового рівня критичності;

$C_{j_s}^c$ – вартість набору засобів захисту хоста, на якому обробляється інформація середнього рівня критичності;

$C_{k_s}^b$ – вартість набору засобів захисту хоста, на якому обробляється інформація високого рівня критичності;

$C_{\text{сегм}_s}$ – вартість набору засобів захисту на границі s -го мережного сегмента;

$C_{\text{пр}}$ – вартість наборів засобів захисту периметра.

Вибір комплексу засобів захисту для СЗІ досягається ітераційно шляхом наближення до раціонального состава, що задовольняє вимогам до припустимих витрат на його реалізацію.

У системі інтелектуальної підтримки раціональні рішення пропонується вибирати на основі використання експертних знань; у ній реалізується механізм придбання знань у процесі заповнення полів знань експертом при взаємодії його з автоматизованою системою, виконується сукупність процедур над проблемною областю з використанням багатокритеріального порівняльного аналізу для виявлення в заданому експертом множини підмножини найкращих за критеріями переваги варіантів наборів, з яких формується раціональний комплекс засобів 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.



Рисунок 3.3 – Діаграма взаємодії процесів

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.

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).

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.

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		50

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

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.

NetBIOS (Network Basic Input/Output System) – протокол для роботи в локальних мережах на персональних ЕОМ типу IBM/PC, розроблений у вигляді інтерфейсу, який не залежить від фірми-виробника. Був розроблений фірмою Sytek Corporation за замовленням IBM в 1983 році. Він включає в себе інтерфейс сеансового рівня (англ. NetBIOS interface), в якості транспортних протоколів використовує TCP і UDP.

Особливістю NetBIOS є можливість його роботи поверх різних протоколів, найпоширенішими/відомими з яких є NetBEUI, IPX і стек протоколів TCP/IP; причому якщо старі версії Windows орієнтувалися на більш легкі в реалізації і менш ресурсомісткі NetBEUI і IPX, то сучасні Windows орієнтуються на TCP/IP.

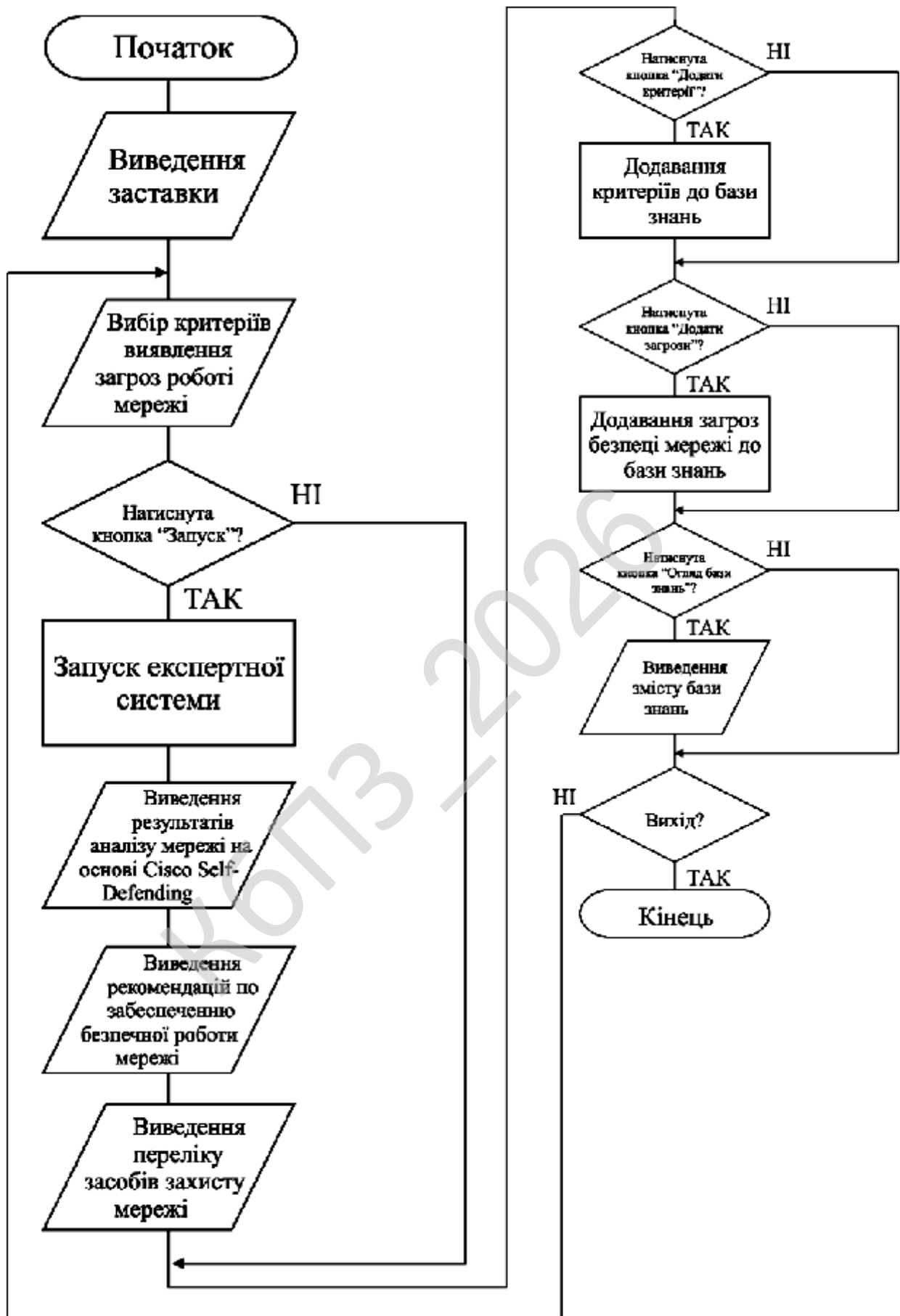


Рисунок 4.1 – Блок-схема основної програми

При використанні NetBEUI і IPX NetBIOS сам забезпечує надійність доставки даних (функціональність SPX не використовувати), а при використанні TCP/IP надійність доставки забезпечує TCP, за що удостоївся окремого імені «NBT».

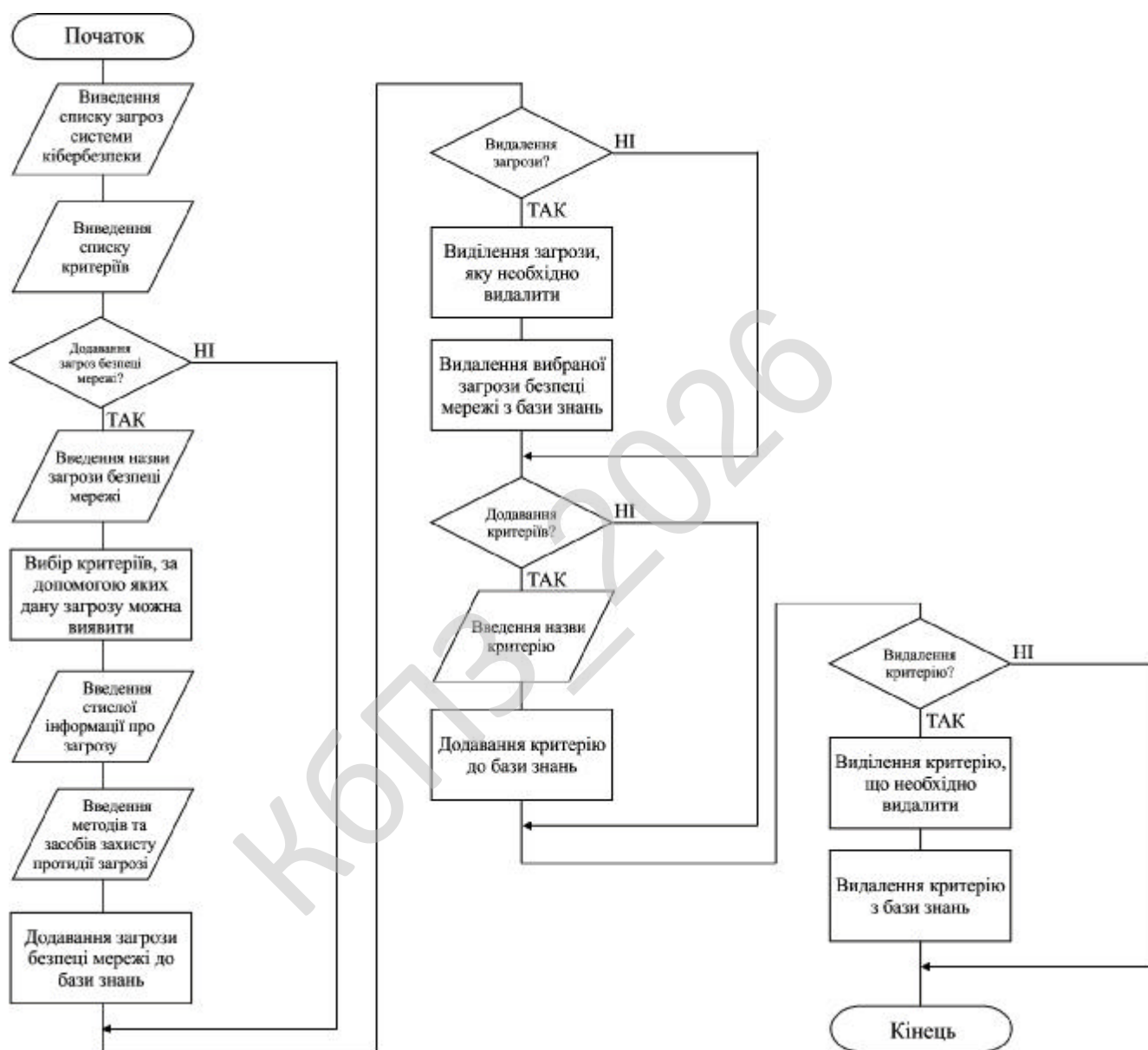


Рисунок 4.2 – Блок-схема роботи підпрограми

Інтерфейс NetBIOS являє собою типовий інтерфейс взаємодії програм (API) для забезпечення мережесих операцій введення–виведення і управління низлежащим транспортним протоколом.

Програми, що використовують NetBIOS API інтерфейс, можуть працювати тільки при наявності протоколу, що допускає використання такого інтерфейсу.

NetBIOS також визначає протокол, що функціонує на сеансовому/транспортному рівнях моделі OSI. Цей протокол використовується протоколами нижчих рівнів, такими як NBFP (NetBEUI) і NetBT для виконання мережесих запитів вводу–виводу і операцій, описаних в стандартному інтерфейсному наборі команд NetBIOS.

Тобто, NetBIOS сам не підтримує виконання файлових операцій. Ця функція покладається на протоколи нижчих рівнів, а сам NetBIOS забезпечує тільки зв'язок з цими протоколами і NetBIOS API–інтерфейс.

Пакет NETBIOS створений для використання групою EOM. Підтримує як режим сесій (робота через з'єднання), так і режим дейтаграм (без встановлення з'єднання). 16–символьні імена об'єктів в NETBIOS розподіляються динамічно.

NETBIOS має власну DNS, яка може взаємодіяти з інтернетівський. Ім'я об'єкта при роботі з NETBIOS не може починатися з символу *.

Додатки можуть знайти через NETBIOS потрібні їм ресурси, встановити зв'язок і послати або отримати інформацію. NETBIOS використовує для служби імен порт 137, для служби дейтаграм – порт 138, а для сесій – порт 139. Будь–яка сесія починається з NETBIOS–запиту, завдання IP–адреси і визначення TCP–порту віддаленого об'єкта, далі йде обмін NETBIOS–повідомленнями, після чого сесія закривається.

Сесія здійснює обмін інформацією між двома NETBIOS – додатками. Довжина повідомлення лежить в межах від 0 до 131 071 байт. Припустимо одночасне встановлення декількох сесій між двома об'єктами.

При організації IP–транспорту через NETBIOS IP–дейтаграма вкладається в NETBIOS–пакет. Інформаційний обмін відбувається в цьому

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		55

випадку без встановлення зв'язку між об'єктами. Імена NETBIOS повинні містити в собі IP-адреси. Так, частина NETBIOS-адреси може мати вигляд IP.XX.XX. XX.XX, де IP вказує на тип операції (IP через Netbios), а XX.XX.XX.XX – IP-адреса.

Система NETBIOS має власну систему команд (call, listen, hang up, send, receive, session status, reset, cancel, adapter status, unlink, remote program load) і примітивів для роботи з дейтаграммами (send datagram, send broadcast datagram, receive datagram, receive broadcast datagram).

Всі кінцеві вузли NETBIOS діляться на три типи:

- широкомовні («b») вузли;
- вузли точка-точка («p»);
- вузли змішаного типу («m»).

IP-адреса може асоціюватися з одним із зазначених типів. В-вузли встановлюють зв'язок зі своїм партнером за допомогою широкомовних запитів. Р- і М-вузли для цієї мети використовують netbios сервер імен (NBNS) і сервер розподілу дейтаграм (NBDD).

NetBIOS забезпечує:

- реєстрацію і перевірку мережеских імен;
- встановлення і розрив з'єднань;
- зв'язок з підтвердженням доставки інформації;
- зв'язок без підтвердження доставки інформації;
- підтримку управління і моніторингу драйвера і мережевої карти.

Було використано наступні підходи UML: діаграма діяльності (діаграми поведінки типу); діаграма прецедентів (діаграми поведінки типу); Діаграма класів; Діаграма компонент; Діаграма об'єктів; Діаграма розгортання.

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.

Специфікація діяльності (на вищих рівнях сумісності) може дозволяти виконання декількох (логічних) потоків, та існування механізмів синхронізації для гарантування виконання дій у правильному порядку.

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

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.

Діаграма класів це статичне представлення структури моделі. Відображає статичні (декларативні) елементи, такі як: класи, типи даних, їх зміст та відношення.

Діаграма класів, також, може містити позначення для пакетів та може містити позначення для вкладених пакетів. Також, діаграма класів може містити позначення деяких елементів поведінки, однак їх динаміка розкривається в інших типах діаграм.

Діаграма класів (class diagram) служить для представлення статичної структури моделі системи в термінології класів об'єктно-орієнтованого програмування. На цій діаграмі показують класи, інтерфейси, об'єкти й кооперації, а також їхні відносини.

В UML існують наступні типи зв'язків які використовуються у діаграмі класів: Асоціації; Агрегація; Композиція.

Асоціації це якщо між двома класами визначена асоціація, то можна переміщатися від об'єктів одного класу до об'єктів іншого. Цілком припустимі випадки, коли обидва кінці асоціації відносяться до одного і того ж класу. Це означає, що з об'єктом деякого класу дозволено зв'язати інші об'єкти з того ж класу. Асоціація, що зв'язує два класи, називається бінарної. Можна, хоча це рідко буває необхідним, створювати асоціації, що зв'язують відразу кілька класів. Графічно асоціація зображується у вигляді лінії, що з'єднує клас сам з собою або з іншими класами.

Асоціації може бути присвоєно ім'я, яке описує природу відносини. Зазвичай ім'я асоціації не вказується, якщо тільки ви не хочете явно задати для неї рольові імена або у вашій моделі настільки багато асоціацій, що виникає необхідність посилатися на них і відрізняти один від одного. Ім'я буде особливо корисним, якщо між одними і тими ж класами існує кілька різних асоціацій.

Клас, що бере участь в асоціації, грає в ній деяку роль. По суті, це "обличчя", яким клас, що знаходиться на одній стороні асоціації, звернений до класу з іншого її боку. Можна явно позначити роль, яку клас грає в асоціації.

Часто при моделюванні буває важливо вказати, скільки об'єктів може бути пов'язано допомогою одного примірника асоціації. Це число називається кратністю (Multiplicity) ролі асоціації та записується або як вираз, значенням якого є діапазон значень, або в явному вигляді.

Вказуючи кратність на одному кінці асоціації, ви тим самим говорите, що на цьому кінці саме стільки об'єктів повинно відповідати кожному об'єкту на протилежному кінці. Кратність можна задати рівною одиниці (1), можна вказати діапазон: "нуль або одиниця" (0..1), "багато" (0 .. *), "одиниця або більше" (1 .. *). Дозволяється також вказувати певне число (наприклад, 3). За допомогою списку можна задати і більш складні кратності, наприклад 0. . 1, 3..4, 6 .. *, що означає "будь-яке число об'єктів, крім 2 і 5".

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		59

Агрегація це проста асоціація між двома класами відображає структурний відношення між рівноправними сутностями, коли обидва класу знаходяться на одному концептуальному рівні і ні один не є більш важливим, ніж інший.

Але іноді доводиться моделювати відношення типу «частина/ціле», в якому один з класів має більш високий ранг (ціле) і складається з декількох менших за рангом (частин).

Ставлення такого типу називають агрегацією; воно зараховане до відносин типу «має» (з урахуванням того, що об'єкт-ціле має кілька об'єктів-частин). Агрегація є окремим випадком асоціації і зображується у вигляді простої асоціації з незафарбованим ромбом з боку «цілого». Графічно агрегація представляється порожнім ромбом на блоці класу, і лінією, яка від цього ромба до міститься класу.

Композиція це більш суворий варіант агрегації. Відома також як агрегація за значенням.

Композиція має жорстку залежність часу існування екземплярів класу контейнера та примірників містяться класів. Якщо контейнер буде знищений, то весь його вміст буде також знищено. Графічно представляється як і агрегація, але з зафарбовани ромбиком.

Діаграма компонент в UML це діаграма, на якій відображаються компоненти, залежності та зв'язки між ними.

Діаграма компонент відображає залежності між компонентами програмного забезпечення, включаючи компоненти вихідних кодів, бінарні компоненти, та компоненти, що можуть виконуватись.

Модуль програмного забезпечення може бути представлено в якості компоненти. Деякі компоненти існують під час компіляції, деякі – під час компонування, а деякі під час роботи програми.

Діаграма компонент відображає лише структурні характеристики, для відображення окремих екземплярів компонент слід використовувати діаграму розгортання.

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		60

Компоненти об'єднуються разом використовуючи структурні зв'язки (assembly connector) щоб об'єднати інтерфейси двох компонент. Це ілюструє зв'язок типу «клієнт-сервер».

Структурна взаємодія – «зв'язок двох компонент, який передбачає, що один з них надає послуги, потрібні іншому компоненту».

При використанні діаграми компонент щоб показати внутрішню структуру компонента, клієнтські та серверні інтерфейси можуть утворювати пряме з'єднання з внутрішніми. Таке з'єднання називається з'єднанням делегації.

Діаграма об'єктів в UML це діаграма, що відображає об'єкти та їх зв'язки в певний момент часу. Діаграма об'єктів може розглядатись як окремий випадок діаграми класів, на якій можуть бути представлені як класи, так і екземпляри (об'єкти) класів. Схожою за змістом є діаграма взаємодії (collaboration diagram).

Діаграми об'єктів не мають власної нотації. Оскільки діаграми класів можуть відображати об'єкти, то діаграма класів, на якій відображено лише об'єкти, та не відображено класи, може вважатись діаграмою об'єктів.

Діаграма об'єктів відображає об'єкти та зв'язки в певний момент роботи програми. Об'єкти можуть містити інформацію про власні значення а не про описання. Для відображення загальних шаблонів об'єктів та зв'язків, що можуть багаторазово створюватись під час роботи програми, слід використовувати діаграму взаємодії, яка може відображати характеристики об'єктів та зв'язків. Екземпляр діаграми взаємодії створює діаграму об'єктів.

Діаграма об'єктів не відображає еволюцію системи під час роботи. Натомість, слід використовувати діаграми взаємодії з повідомленнями, або діаграми послідовності.

Діаграма розгортання (deployment diagram) це діаграма в UML, на якій відображаються обчислювальні вузли під час роботи програми, компоненти, та об'єкти, що виконуються на цих вузлах.

Компоненти відповідають представленню робочих екземплярів одиниць коду. Компоненти, що не мають представлення під час роботи програми на таких

діаграмах не відображаються; натомість, їх можна відобразити на діаграмах компонент.

Діаграма розгортання відображає робочі екземпляри компонент, а діаграма компонент, натомість, відображає зв'язки між типами компонент.

Розглянемо протокол SNMP (Simple Network Management Protocol, простий протокол керування мережею) – це протокол керування мережами зв'язку на основі архітектури TCP/IP.

На основі концепції TMN в 1980–1990 р. різними органами стандартизації був вироблений ряд протоколів керування мережами передачі даних з різним спектром реалізації функцій TMN. До одного з типів таких протоколів керування належить Simple Network Management Protocol (SNMP).

SNMP – це технологія, покликана забезпечити керування й контроль за пристроями й програмами в мережі зв'язку шляхом обміну керуючою інформацією між агентами, що розташовуються на мережних пристроях, і менеджерами, розташованими на станціях керування. SNMP визначає мережу як сукупність мережних керуючих станцій й елементів мережі (головні машини, шлюзи й маршрутизатори, термінальні сервери), які спільно забезпечують адміністративні зв'язки між мережними керуючими станціями й мережними агентами. SNMP різних версій присвячений цілий ряд рекомендацій IETF (RFC).

Зазвичай при використанні SNMP присутні керовані та керуючі системи. До складу керованої системи входить компонент, який називається агентом, який відправляє звіти керуючій системі. По суті SNMP агенти передають управлінську інформацію на керуючі системи як змінні (такі як «вільна пам'ять», «ім'я системи», «кількість працюючих процесів» тощо).

Керуюча система може отримати достовірну інформацію через операції протоколу GET, GETNEXT і GETBULK. Агент може самостійно без запиту надсилати дані, використовуючи операцію протоколу TRAP або INFORM. Управляючі системи можуть також відправляти конфігураційні оновлення або

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		62

контролюючі запити, використовуючи операцію SET для безпосереднього управління системою.

Операції конфігурування та управління використовуються тільки тоді, коли потрібні зміни у мережній інфраструктурі. Операції моніторингу зазвичай виконуються на регулярній основі.

Змінні, доступні через SNMP, організовані в ієрархії. Ці ієрархії та інші метадані (такі як тип і опис змінної) описуються Базами Керуючої Інформації (Management Information Bases (MIBs)).

SNMP не визначає, яку інформацію (які змінні) керована система повинна надавати. Навпаки, SNMP використовує розширювану модель, в якій доступна інформація визначається Базами Керуючої Інформації (MIB – Management Information Base).

Бази Керуючої Інформації описують структуру керуючої інформації пристроїв. Вони використовують ієрархічний адресний простір імен, що містить унікальний ідентифікатор об'єкта (object identifier (OID)).

Грубо кажучи, кожен унікальний ідентифікатор об'єкта ідентифікує змінну, яка може бути прочитана чи встановлена через SNMP. MIB'и використовують нотацію, визначену в ASN.1.

Ієрархія MIB може бути зображена як дерево з безіменним коренем, рівні якого приписані різними організаціями. На найвищому рівні MIB OID'и належать різним організаціям, що займаються стандартизацією, в той час як на нижчих рівнях OID'и виділяються асоційованими організаціями. Ця модель забезпечує управління на всіх шарах мережної моделі OSI, адже MIB'и можуть бути визначені для будь-яких типів даних і операцій.

Керований об'єкт – це одна з будь-якого числа характеристик, специфічних для керованого пристрою. Керований об'єкт включає в себе один або більше екземплярів об'єкта (що ідентифікуються за OID), які насправді є змінними.

Існує два типи керованих об'єктів: Скалярні об'єкти визначають єдиний екземпляр об'єкта; Табличні об'єкти визначають множинні, пов'язані екземпляри об'єктів які групуються в таблицях MIB.

Прикладом керованого об'єкта може бути atInput, який є скалярним об'єктом що містить єдиний екземпляр об'єкта, ціле число, яке показує загальну кількість вхідних пакетів AppleTalk на мережний інтерфейс маршрутизатора.

Ідентифікатор об'єкта (OID) унікально ідентифікує керований об'єкт в ієрархії MIB.

В телекомунікаціях і комп'ютерних мережах, ASN.1 є стандартною гнучкою нотацією для опису структур даних, що служать для кодування, передачі і декодування даних. ASN.1 являє собою набір правил для опису структури об'єктів, незалежних від специфічних для обладнання методик кодування, і формальну нотацію, яка дозволяє уникнути неоднозначностей.

ASN.1 це єдиний ISO та ITU-T стандарт, спочатку визначений у 1984 році як частина стандарту CCITT X.409: 1984. Пізніше, в 1988 році, завдяки його широкому застосуванню, він був виділений в окремий стандарт X.208. Значно переглянута версія 1995року описана в X.680.

Адаптована підмножина ASN.1 Структура Керуючої Інформації (SMI) описана в протоколі SNMP для визначення наборів пов'язаних MIB об'єктів, також званих MIB модулями.

SNMP працює на прикладному рівні TCP/IP (сьомий рівень моделі OSI). Агент SNMP отримує запити по UDP-порту 161. Менеджер може посилати запити з будь-якого доступного порту джерела на порт агента. Відповідь агента буде відправлений назад на порт джерела на менеджері. Менеджер отримує повідомлення (Traps і InformRequests) по порту 162. Агент може генерувати повідомлення з будь-якого доступного порту. При використанні TLS або DTLS запити виходять по порту 10161, а пастки відправляються на порт 10162.

У SNMPv1 зазначено п'ять основних протокольних одиниць обміну (protocol data units - PDU). Ще дві PDU, GetBulkRequest і InformRequest, були введені в SNMPv2 і перенесені в SNMPv3.

Нижче перераховані сім протокольних одиниць обміну SNMP:

1. GetRequest. Запит від менеджера до об'єкту для отримання значення змінної або списку змінних. Необхідні змінні вказуються в полі variable bindings (розділ поля values при цьому не використовується).

Отримання значень зазначеної змінної повинно бути виконано агентом як Атомарна операція. Менеджеру буде повернений Response (відповідь) з поточними значеннями.

2. SetRequest. Запит від менеджера до об'єкту для зміни змінної або списку змінних. Зв'язані змінні вказуються в тілі запиту. Зміни всіх зазначених змінних повинні бути виконані агентом як атомарна операція. Менеджеру буде повернений Response з (поточними) новими значеннями змінних.

3. GetNextRequest. Запит від менеджера до об'єкту для виявлення доступних змінних і їх значень. Менеджеру буде повернений Response зі зв'язаними змінними для змінної, яка є наступною в базі MIB в лексикографічному порядку. Обхід всієї бази MIB агента може бути проведений ітераційним використанням GetNextRequest, починаючи з OID 0. Рядки таблиці можуть бути прочитані, якщо вказати в запиті OID-и колонок в пов'язаних змінних.

4. GetBulkRequest. Покращена версія GetNextRequest. Запит від менеджера до об'єкту для численних ітерацій GetNextRequest. Менеджеру буде повернений Response з декількома пов'язаними змінними, обійденими починаючи зі пов'язаної змінної (змінних) в запиті. Специфічні для PDU поля non-repeaters і max-repetitions використовуються для контролю за поведінкою відповіді. GetBulkRequest був введений в SNMPv2.

5. Response. Повертає зв'язані змінні і значення від агента менеджеру для GetRequest, SetRequest, GetNextRequest, GetBulkRequest і InformRequest. Повідомлення про помилки забезпечуються полями статусу помилки і індексу

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		65

помилки. Ця одиниця використовується як відповідь і на Get-, і на Set-запити, в SNMPv1 називається GetResponse.

6. Trap. Асинхронне повідомлення від агента - менеджера. Включає в себе поточне значення sysUpTime, OID, що визначає тип trap (пастки), і необов'язкові зв'язані змінні. Адресація одержувача для пасток визначається за допомогою змінних trap-конфігурації в базі MIB. Формат trap-повідомлення був змінений в SNMPv2 і PDU перейменували в SNMPv2-Trap.

7. InformRequest. Асинхронне повідомлення від менеджера менеджера або від агента менеджера. Повідомлення від менеджера менеджера були можливі вже в SNMPv1 (за допомогою Trap), але SNMP зазвичай працює на протоколі UDP, в якому доставка повідомлень не гарантована, і не повідомляється про втрачені пакетах. InformRequest виправляє це зворотним відправленням підтвердження про отримання. Одержувач відповідає Response-му, що повторює всю інформацію з InformRequest. Цей PDU був введений в SNMPv2.

4.2 Захист розробленого програмного забезпечення

Дані у системі захищаються за допомогою алгоритму обміну ключа Діффі-Хеллмана.

Ціль алгоритму полягає в тому, щоб два учасники могли безпечно обмінятися ключем, що надалі може використовуватися в якому-небудь алгоритмі симетричного шифрування. Сам алгоритм Діффі-Хеллмана може застосовуватися тільки для обміну ключами.

Алгоритм заснований на труднощі обчислень дискретних логарифмів. Дискретний логарифм визначається в такий спосіб.

Уводиться поняття примітивного кореня простого числа Q як числа, чії ступені створюють всі цілі від 1 до $Q - 1$. Це означає, що якщо A є примітивним коренем простого числа Q , тоді числа:

$$A \bmod Q, A^2 \bmod Q, \dots, A^{Q-1} \bmod Q,$$

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		66

є різними й складаються із цілих від 1 до $Q - 1$ з деякими перестановками. У цьому випадку для будь-якого цілого $Y < Q$ і примітивного кореня A простого числа Q можна знайти єдину експоненту X , таку, що:

$$Y = A^X \bmod Q,$$

де $0 \leq X \leq (Q - 1)$.

Експонента X називається дискретним логарифмом, або індексом Y , по підставі $A \bmod Q$. Це позначається як $\text{ind}_Q(Y)$.

Тепер опишемо алгоритм обміну ключів Діффі-Хеллмана.

Загальновідомі елементи

Q – просте число.

$A - A < Q$ і A є примітивним коренем Q .

Створення пари ключів користувачем I

Вибір випадкового числа X_i (закритий ключ):

$$X_i < Q.$$

Обчислення числа Y_i (відкритий ключ):

$$Y_i = A^{X_i} \bmod Q.$$

Створення відкритого ключа користувачем J

Вибір випадкового числа X_j (закритий ключ):

$$X_j < Q.$$

Обчислення випадкового числа Y_j (відкритий ключ):

$$Y_j = A^{X_j} \bmod Q.$$

Створення загального секретного ключа користувачем I

$$K = (Y_j)^{X_i} \bmod Q.$$

Створення загального секретного ключа користувачем J

$$K = (Y_i)^{X_j} \bmod Q.$$

Передбачається, що існують два відомих усім числа: просте число Q і ціле A , що є примітивним коренем Q .

Тепер припустимо, що користувачі I і J хочуть обмінятися ключем для алгоритму симетричного шифрування.

Користувач І вибирає випадкове число $X_i < Q$ і обчислює:

$$Y_i = A^{X_i} \bmod Q.$$

Аналогічно користувач J незалежно вибирає випадкове ціле число $X_j < Q$ і обчислює:

$$Y_j = A^{X_j} \bmod Q.$$

Кожна сторона тримає значення X у секреті й робить значення Y доступним для іншої сторони.

Тепер користувач І обчислює ключ як $K = (Y_j)^{X_i} \bmod Q$, і користувач J обчислює ключ як $K = (Y_i)^{X_j} \bmod Q$. У результаті обоє одержать те саме значення:

$$K = (Y_j)^{X_i} \bmod Q = (A^{X_j} \bmod Q)^{X_i} \bmod Q = (A^{X_j})^{X_i} \bmod Q =$$

за правилами модульної арифметики

$$= A^{X_j X_i} \bmod Q = (A^{X_j})^{X_i} \bmod Q = (A^{X_i} \bmod Q)^{X_j} \bmod Q = (Y_i)^{X_j} \bmod Q$$

Таким чином, дві сторони обмінялися секретним ключем. Так як X_i і X_j є закритими, супротивник може одержати тільки наступні значення: Q , A , Y_i і Y_j . Для обчислення ключа атакуючий повинен зламати дискретний логарифм, тобто обчислити:

$$X_j = \text{ind}_{a, q}(Y_j).$$

Безпека обміну ключа в алгоритмі Діффі-Хеллмана випливає з того факту, що, хоча відносно легко обчислити експоненти по модулю простого числа, дуже важко обчислити дискретні логарифми. Для великих простих чисел задача вважається нерозв'язною.

Варто помітити, що даний алгоритм уразливий для атак типу "in-the-middle". Якщо супротивник може здійснити активну атаку, тобто має можливість не тільки перехоплювати повідомлення, але й замінити їх іншими, він може перехопити відкриті ключі учасників Y_i і Y_j , створити свою пару відкритого й закритого ключа $(X_{\text{оп}}, Y_{\text{оп}})$ і послати кожному з учасників свій відкритий ключ.

Після цього кожий учасник обчислить ключ, що буде загальним із супротивником, а не з іншим учасником. Якщо немає контролю цілісності, то учасники не зможуть виявити подібну підміну.

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		68

5 МЕТОДИКА ВПРОВАДЖЕННЯ СИСТЕМИ
В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ

На рисунку 5.1 зображено розроблене у бакалаврської дипломної роботі програмне забезпечення системи кібербезпеки для автоматизованого захисту корпоративної мережі. З рисунку можна побачити що інтерфейс головного вікна розподілено на наступні функціональні блоки: Блок авторизації та керування користувачами; Блок головної панелі моніторингу; Блок аналізу стану захисту мережі; Блок виявлення та класифікації загроз; Блок автоматичного блокування атак; Блок сканування пристроїв корпоративної мережі; Блок журналу подій і сповіщень адміністратора; Блок звітів, статистики та налаштування політик безпеки.

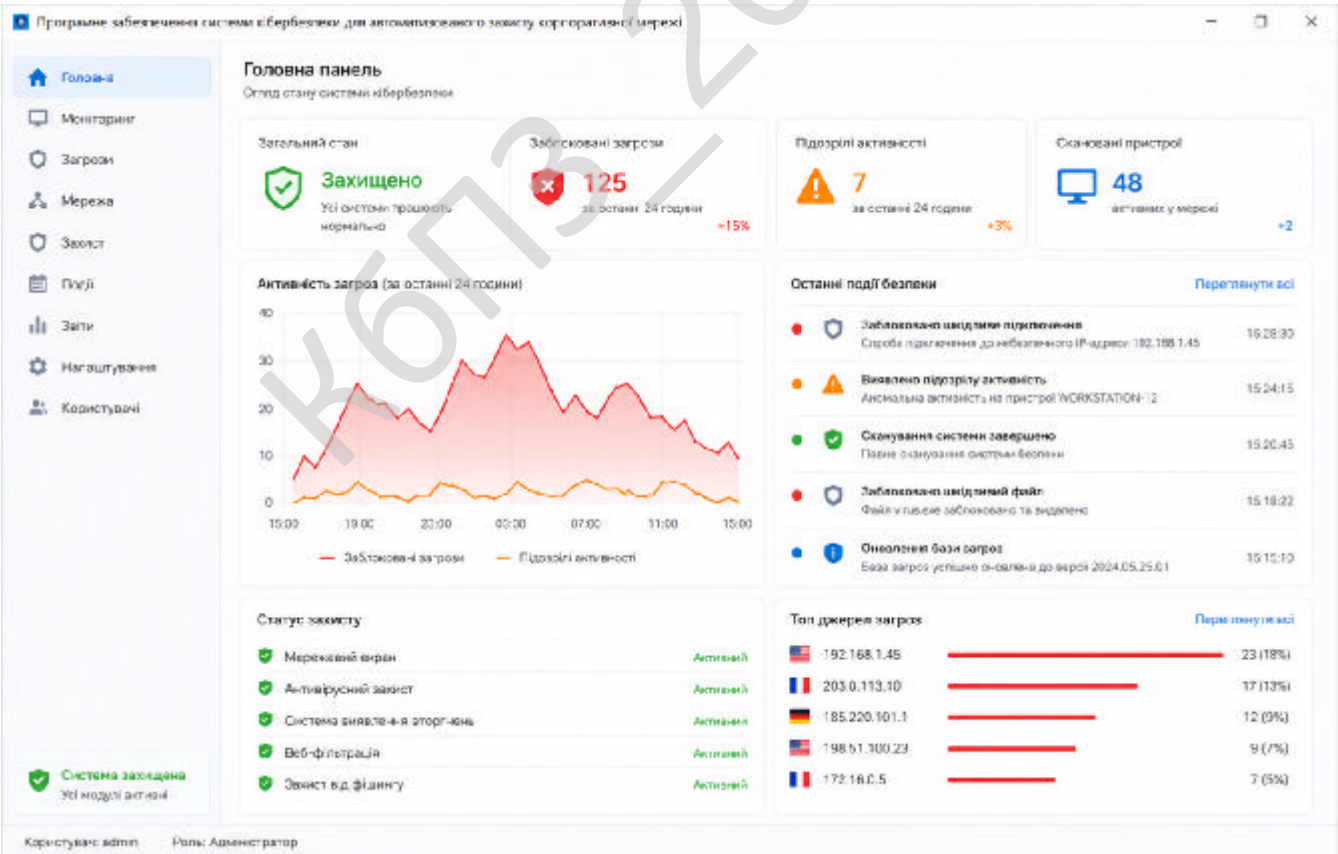


Рисунок 5.1 – Головне вікно ПЗ

Розроблена програма має дуже простий і зрозумілий інтерфейс з користувачем.

Областю застосування є корпоративні мережі. Корпоративна інформаційна мережа являє собою систему для автоматизації виробничих процесів і комп'ютерних додатків, з якими працюють співробітники підприємства. Основним завданням мережі є керування господарської діяльності підприємства або корпорації.

Результатом успішного впровадження ефективної корпоративної системи або мережі є:

- підвищення керованості підприємства й ефективності діяльності;
- поліпшення фінансових показників;
- ріст обсягу продажів;
- поліпшення партнерських відносин з іншими компаніями;
- скорочення часових витрат на виконання замовлень.

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.

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

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		70

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.

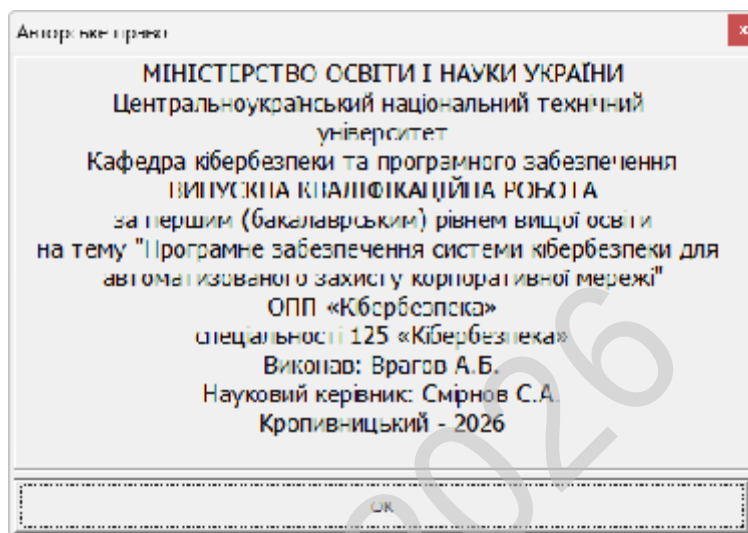


Рисунок 5.2 – Авторське право

До діяльностей пов'язаних із розгортанням програмного забезпечення відносять:

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

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		71

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.

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		72

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 форматом білої скриньки засноване на аналізі керуючої структури програми. Програма вважається повністю перевіреною, якщо проведено вичерпне тестування маршрутів (шляхів) її графа управління.

У цьому випадку формуються тестові варіанти, в яких:

- Гарантується перевірка всіх незалежних маршрутів програми.
- Знаходяться гілки True, False для всіх логічних рішень.
- Виконуються всі цикли (у межах їхніх кордонів та діапазонів).
- Аналізується правильність внутрішніх структур даних.

Недоліки тестування "білої скриньки":

- Кількість незалежних маршрутів може бути дуже велика.
- Повне тестування маршрутів не гарантує відповідності програми вихідним вимогам до неї.
- У програмі можуть бути пропущені деякі маршрути.
- Не можна виявити помилки, поява яких залежить від даних.

Переваги тестування "білої скриньки" пов'язані з тим, що принцип «білої скриньки» дозволяє врахувати особливості програмних помилок:

- Кількість помилок мінімально в «центрі» і максимально на «периферії» програми.
- Попередні припущення про ймовірність потоку керування або даних у програмі часто бувають некоректними. У результаті типовим може стати маршрут, модель обчислень за яким опрацьована слабо.

- При записі алгоритму програмного забезпечення у вигляді тексту на мові програмування можливе внесення типових помилок трансляції (синтаксичних та семантичних).

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		73

– Деякі результати в програмі залежать не від вихідних даних, а від внутрішніх станів програми.

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;

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		74

– Сформулювати такі очікувані результати, які з високою імовірністю 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.

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		75

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.

К6ПЗ-2026

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		76

6 ОСНОВНІ ВИСНОВКИ

Програмне забезпечення, створене в результаті виконання випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти, призначено для системи кібербезпеки для автоматизованого захисту корпоративної мережі.

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

Рішення завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем для автоматизованого захисту корпоративної мережі.
- Досліджена система для автоматизованого захисту корпоративної мережі.
- На основі отриманих результатів досліджень створена програмна реалізація системи кібербезпеки для автоматизованого захисту корпоративної мережі.

Розроблені під час виконання випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання для автоматизованого захисту корпоративної мережі.

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 кібербезпеки для автоматизованого захисту корпоративної мережі. Це

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		77

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 програмне забезпечення, що спеціально розроблене для даної конкретної системи кібербезпеки 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 Діффі-Хеллмана.

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.

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		78

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Awais Rashid, Howard Chivers, George Danezis, Emil Lupu, Andrew Martin. CyBOK The Cyber Security Body of Knowledge. The National Cyber Security Centre. 2019. 854 p.
2. Loren Kohnfelder. Designing Secure Software. No Starch Press. 2022. 332 p.
3. Samir Kumar Rakshit. Ethical Hacker's Penetration Testing Guide. BPB Online. 2022. 509 p.
4. Corey J. Ball. Hacking APIs. No Starch Press. 2022. 353 p.
5. Kevin Beaver. Hacking for Dummies. John Wiley & Sons. 2022. 419 p.
6. Mark S. Merkow. Practical Security for Agile and DevOps. CRC Press. 2022. 236 p.
7. Derek Fisher. Application Security Program Handbook. Manning Publications. 2021. 155 p.
8. Cameron Wyatt PH.D. Kali Linux Tutorial. Independently published. 2021. 60 p.
9. Kuznetsov O., Frontoni E., Arnesano M., Smirnov O., Khruskov B. «Biometric Authentication in TinyML: Opportunities and Challenges». *Tiny Machine Learning: Design Principles and Applications*, 2026, pp. 587-633.
10. Kuznetsov O., Frontoni E., Kuznetsova Y., Chevardin V., Smirnov O. «Architectural foundations for adaptive security in edge computing systems». *Cybersecurity Defensive Walls in Edge Computing*, 2025. pp. 21-61.
11. Chulinda L., Smirnov O., Shapenko L., Ustynova I., Bohatiuk I., Kelyp S. «The role of innovation in ensuring the safety of international civil aviation». *Ceur Workshop Proceedings*, 2025, 4024, pp. 530–542.
12. Петрик В.М., Присяжнюк М.М., Аль-Файюмі Халед та ін. «Системи інформаційної зброї та технології інформаційної війни»: підручник / Петрик В.М., Присяжнюк М.М., Аль-Файюмі Халед, Жарков Я.М., Смірнов О.А,

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		79

Буравченко К.О., Давидюк А.В., Кононович В.Г., Корчинский В.В., Кудирко В.М., Фесенко А.О.; за заг. ред. В.М. Петрика, М.М. Присяжнюка.— К.: Видавничий центр “Кафедра”, 2025.— 320 с.

13. Усік, П.С., Смірнова, Т.В., Буравченко, К.О., Смірнов, О.А., Улічев, О.С., Смірнов, С.А. «Дослідження технологій забезпечення кібербезпеки банківських систем з використанням штучного інтелекту». *Кібербезпека: освіта, наука, техніка*. 2025. Том 1 № 29. С.704–716, 2025

14. Kuznetsov, O., Frontoni, E., Kuznetsova, K., Arnesano, M., Smirnov, O. «A secure biometric authentication architecture for blockchain-driven cyber-physical systems». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 193–224.

15. Kuznetsov, O., Atzeni, G., Arnesano, M., Randieri, C., Smirnov, O. «Secure IoT-based smart wheelchair system: From implementation to security enhancement strategy». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 225–257.

16. Kuznetsov, O., Smirnov, O., Kuznetsova, T., Shaikhanova, A., Svatowsky, I. «Privacy-utility trade-offs in IoT networks: A comparative analysis of differential privacy mechanisms for sensor data aggregation». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 589–622.

17. Lakhno, V., Malyukov, V., Smirnov, O., Bebashko, B., Chubaievskiy, V., Zhumadilova, M., Malyukova, I., Smirnov, S. «Multifactorial Model for Targeted Attacks Counteracting Within the Framework of a Multi-Step Quality Game with Fuzzy Information». *8th International Symposium on Intelligent Informatics, ISI 2023*, 2025. vol 389. pp 377-389. Springer, Singapore.

18. Kuznetsov O., Frontoni E., Kuznetsova Y., Smirnov O., Moskovchenko I. «Trust-Based Security Architecture for Edge Computing: A Simulation Study of Dynamic Trust Evolution and Attack Detection». *CEUR Workshop Proceedings*, 2024, 3909, pp. 227–241.

19. Kuznetsov, O., Frontoni, E., Kryvinska, N., Chevardin, V., Smirnov, O. «Wireless Network Encryption Stream Ciphers, Computational Modeling, and Security Analysis». *Computational Modeling and Simulation of Advanced Wireless Communication Systems*, 2024, pp. 379–402.

20. Kuznetsov, O., Frontoni, E., Kryvinska, N., Smirnov, O., Imoize, G.L. «Computational Modeling of Enhanced Spread Spectrum Codes for Asynchronous Wireless Communication». *Computational Modeling and Simulation of Advanced Wireless Communication Systems*, 2024, pp. 403–447.

21. Ткаченко, О., Ільєнко, А., Улічев, О., Мелешко, Є., Смірнов, О. «Правові засади поширення інформаційних впливів в соціальних мережах». *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2024. № 2(26), С. 170–188.

22. Смірнова Т.В., Коноплицька-Слободенюк О.К., Буравченко К.О., Смірнов С.А., Кравчук О.В., Козірова Н.Л., Смірнов О.А. «Дослідження технологій забезпечення кібербезпеки хмарних сервісів IaaS, PaaS та SaaS». *Кібербезпека: освіта, наука, техніка*. 2024. №4(24), С. 6-27.

23. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». *Кібербезпека: освіта, наука, техніка*. 2024. №3(23), С. 111-131.

24. Батрак О., Смірнова Т., Гнатюк В., Одарченко Р., Смірнов О. «Дослідження показників ефективності функціонування та перспектив розвитку систем ІР-телефонії». *Підводні технології*, 2024, № 13, с. 28-35.

25. Kuznetsov, O., Kryvinska, N., Ilchenko, O., Smirnova, T., Ulianovska, Y. «Comparative Analysis of Cryptocurrency Trading Platforms Using the Analytic Hierarchy Process». *CEUR Workshop Proceedings*, 2023, 3628, pp. 106-115.

26. Akhalaia, G., Iavich, M., Iashvili, G., Prysiashnyy, D., Smirnova, T. «Secure Encrypted Connection on Georgian Website». *CEUR Workshop Proceedings*, 2023, 3550, pp. 313-320.

27. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». *Advanced Information Systems*, 2023, 7(2), pp. 49-56

28. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchев, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». *CEUR Workshop Proceedings*, Volume 3530, 2023, pp. 256-265.

29. Kuznetsov, O., Kandiy, S., Frontoni, E., Smirnov, O. «Trade-offs in Post-Quantum Cryptography: A Comparative Assessment of BIKE, HQC, and Classic McEliece». *CEUR Workshop Proceedings*, Volume 3504, 2023, pp. 1-11.

30. Smirnov, O., Lakhno, V., Akhmetov, B., Chubaievskyi, V., Khorolska, K., Bebesko, B. «Selection of a Rational Composition of Information Protection Means Using a Genetic Algorithm». In: *Rajakumar, G., Du, KL., Vuppapapati, C., Beligiannis, G.N. (eds) Intelligent Communication Technologies and Virtual Mobile Networks. Lecture Notes on Data Engineering and Communications Technologies*, vol 131. 2023. Springer, Singapore. pp. 21-34.

31. Смірнова Т.В., Гнатюк С.О., Бердибаєв Р.Ш., Сидоренко В.М., Жигаревич О.К., «Система корелювання подій та управління інцидентами кібербезпеки на об'єктах критичної інфраструктури». *Кібербезпека: освіта, наука, техніка*, №3(19), 2023, С. 176-196.

32. Смірнов О.А. Козлов Я.О., Смірнова Т.В. «Дослідження застосування SIEM-систем для забезпечення кібербезпеки та захисту інформації». *II Міжнародна науково-практична Інтернет-конференція «Інновації та перспективні шляхи розвитку інформаційних технологій (ІІШРІТ-2023)»* м.Черкаси 6 грудня 2023 року – Черкаси: ЧДТУ.– 2023. – С.251-252.

33. Козлов Я.О., Смірнова Т.В., Смірнов О.А. «Дослідження SIEM-систем для забезпечення кібербезпеки». *VII міжнародна науково-практична конференція “Інформаційна безпека та комп'ютерні технології” до 30-ти річчя*

кафедри кібербезпеки та програмного забезпечення, м. Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 26.

34. Козлов Я.О., Козірова Н.Л., Смірнов О.А. «Дослідження структури та принципу роботи SIEM-системи». VII міжнародна науково-практична конференція “Інформаційна безпека та комп’ютерні технології” до 30-ти річчя кафедри кібербезпеки та програмного забезпечення, м. Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 59.

35. 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.

36. 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,

37. 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.

38. 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.

39. 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.

					ВКРБ-125.26.0025.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		83

40. 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.

41. 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.

42. 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

43. 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.

44. 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.

45. 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.

46. 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.

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

48. 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.

49. 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.

50. 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.

51. 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.

52. 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.

53. 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.