

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 протидії
загрозам корпоративній мережі”

Виконав здобувач вищої освіти
IV курсу, групи КБ-22-2
ОПП «Кібербезпека»
спеціальності 125 «Кібербезпека»
_____ Небесний І.С.
«___» _____ 2026 р.

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

Центральноукраїнський національний технічний університет
Факультет Механіко-технологічний
Кафедра Кібербезпеки та програмного забезпечення
Освітній ступінь бакалавр
Галузь знань ._12 _____“Інформаційні технології”
Спеціальність 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

Небесному Івану Сергійовичу

(прізвище, ім'я, по батькові)

1. Тема роботи *Програмне забезпечення системи кібербезпеки для протидії загрозам корпоративній мережі*

2. Керівник роботи *Смірнова Тетяна Віталіївна, 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 протидії загрозам корпоративній 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

Смірнова Т.В.
(прізвище та ініціали)

Завдання прийнято до виконання
« 27 » лютого 2026 р.

Підпис здобувача

Небесний І.С.
(прізвище та ініціали)

АНОТАЦІЯ

Небесний І.С. Програмне забезпечення системи кібербезпеки для протидії загрозам корпоративній 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 протидії загрозам корпоративній мережі.

Метою розробки є програмне забезпечення системи кібербезпеки для протидії загрозам корпоративній мережі.

Результат роботи – програмна реалізація системи кібербезпеки для протидії загрозам корпоративній 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, загрози корпоративній мережі

ABSTRACT

Nebesnyi I.S. Software for a cybersecurity system to counter threats to a corporate network. 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 that is intended for a cybersecurity system to counter threats to a corporate network.

The purpose of the development is software for a cybersecurity system to counter threats to a corporate network.

The result of the work is a software implementation of a cybersecurity system to counter threats to a corporate network.

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, threats to the corporate network

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ	2
ВСТУП.....	3
1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ	5
1.1 Призначення системи.....	5
1.2 Область застосування.....	6
2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ	8
2.1 Огляд існуючих систем, технологій, архітектур та програмних рішень за профілем теми випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти.....	8
2.2 Обґрунтування вибору засобів для побудови системи кібербезпеки та мови програмування.....	18
2.3 Розгорнута постановка завдання	21
3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ	22
3.1 Опис функціонування системи	22
3.2 Розробка структурної схеми.....	35
3.3 Розробка функціональної схеми	38
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.....	65
5 ВПРОВАДЖЕННЯ СИСТЕМИ КІБЕРБЕЗПЕКИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ	68
6 ОСНОВНІ ВИСНОВКИ.....	75
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	77

					ВКРБ-125.26.0037.00.00.ПЗ			
Вим	Арк.	№ докум.	Підп.	Дата	<i>Програмне забезпечення системи кібербезпеки для протидії загрозам корпоративній мережі</i>	Літ.	Аркуш	Аркушів
<i>Розроб.</i>		Небесний І.С.				Б		
<i>Перев.</i>		Смірнова Т.В.					1	85
<i>Н.контр.</i>		Коваленко А.С.				ЦНТУ КБ-22-2		
<i>Затв.</i>		Смірнов О.А.						

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

ВСТУП

Актуальність теми. З генеративним штучним інтелектом як своїм новим помічником, зловмисники діють швидше, ніж будь-коли, використовуючи вразливості зі швидкістю, яку більшість організацій просто не можуть виправити достатньо швидко. І поки бізнес ставить цілі щодо зростання, ефективності та інновацій, кіберзлочинці прагнуть бути на крок попереду.

Від атак соціальної інженерії з використанням глибоких фейків до порушень ланцюгів поставок, спричинених штучним інтелектом, лідери з безпеки стикаються з нагальним імперативом: адаптуватися або бути порушеним.

Згідно зі звітом IBM про вартість витоку даних за 2025 рік, середня світова вартість витоку даних досягла 4,45 мільйона доларів, причому такі галузі, як охорона здоров'я, виробництво та державні послуги, понесли рекордні втрати. Оскільки директори з інформаційної безпеки, команди безпеки та керівники організацій прагнуть дотримуватися таких фреймворків, як NIST, ISO/IEC 27001 та GDPR, вони також стикаються зі зростаючим тиском регуляторів щодо впровадження Zero Trust Security та платформ розвідки загроз, орієнтованих на правоохоронні органи.

Мета й завдання дослідження. Метою роботи є програмне забезпечення системи кібербезпеки для протидії загрозам корпоративній мережі.

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

- Огляд існуючих систем для протидії загрозам корпоративній мережі.
- Дослідження системи кібербезпеки для протидії загрозам корпоративній мережі.
- Програмна реалізація системи кібербезпеки для протидії загрозам корпоративній мережі.

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		3

Практична цінність отриманих результатів полягає в тому, що розроблені алгоритми дозволяють успішно вирішувати задачі для протидії загрозам корпоративній мережі.

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

К6ПЗ_2026

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		4

1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ

1.1 Призначення системи

Самий елементарний спосіб знизити ризик зараження вірусами – стежити за повідомленнями про нові погрози (розсилання партнерів, офіційні повідомлення компаній і дослідницьких груп і т.п.) і вчасно обновляти ПЗ. Корисні ІТ-інструменти для цих цілей пропонують провідні розроблювачі в області забезпечення мережної безпеки: Palo Alto, Fortinet, Check Point і ін.

Ефективним засобом протидії погрозам є сервіс «пісочниці», завдяки якому розроблювачі одержують величезну кількість екземплярів шкідливих файлів і можуть оперативно надавати інформацію (сигнатури) своїм передплатникам – компаніям, у яких установлені міжмережеві екрани того або іншого вендора. Це дозволяє максимально швидко в автоматичному режимі блокувати шкідливе ПЗ після його виявлення на глобальному рівні. Сервіс пісочниці може бути реалізований як хмарна послуга або розміщена в інфраструктурі замовника по моделі on-premise.

Найбільш ефективний спосіб захисту на сучасний момент – реалізувати в компанії комплексний підхід до інформаційної безпеки: установити антивірус (для захисту прикінцевих пристроїв) і міжмережевий екран наступного покоління, а крім того, скористатися можливостями пісочниці. Кожний із цих варіантів окремо – не панацея, але разом вони створюють серйозну смугу перешкод для хакерів.

Уявимо собі компанію, на поштовий сервер якої приходить лист із убудованим шкідливим кодом. Залежно від кваліфікації хакерів, він може або взагалі не проникнути в систему (наприклад, якщо використовується неактуальний метод атаки), або поглибитися «усередину» рівно настільки, наскільки йому дозволять наявні засоби захисту. Комплексний захист споруджує

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		5

відразу кілька перешкод на шляху до даних і корпоративних систем: антивірус захищає кінцеві пристрої, а пісочниця й міжмережевий екран – всю мережу, як би створюючи щит, що не пропускає підозрілі об'єкти. Інноваційні IT-інструменти захисту кінцевих пристроїв, такі як Traps компанії Palo Alto, уміють не просто виконувати аналіз сигнатур, але й боротися з невідомими погрозами нульового дня. Traps виявляє відхилення в стандартній роботі програмних продуктів (наприклад, нетипове звертання до інших ділянок пам'яті) і при необхідності блокує підозрілі дії. На жаль, як показує досвід минулого літа, навіть не всі великі компанії мають подібну систему. Найбільш відповідальний підхід до забезпечення безпеки продемонстрували банки, оскільки подібні інциденти (особливо публічні) для них найбільш критичні. Це питання гостро стоїть на порядку денному в підприємств із нафтогазового й телекомунікаційного секторів. У зоні підвищеної небезпеки перебувають роздрібні мережі, оскільки через велику кількість підрядників, партнерів і безлічі магазинів, розташованих у самих різних регіонах країни, вірус може легко поширитися по ланцюжку.

1.2 Область застосування

Кіберзагрози у 2025 році знову були представлені переважно фішинговими атаками, програмами-вимагачами, шкідливим програмним забезпеченням на базі штучного інтелекту та ризиками для ланцюгів поставок. Але 2026 рік ознаменувався значним прискоренням через впровадження застосувань штучного інтелекту, зростаючий вплив квантових обчислень та фрагментацію глобальної співпраці в галузі кібербезпеки.

Кілька ключових змін формують 2026 рік:

– Штучний інтелект переходить від допоміжного до напіваавтономного: постачальники послуг безпеки переходять від виявлення аномалій до повної оркестрації, автоматизації та реагування на безпеку (SOAR), виявлення та реагування в мережі (NDR) та прогнозової аналітики на основі машинного

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		6

навчання. Але те саме зробили і зловмисники. Складні агентні інструменти штучного інтелекту тепер автоматизують розвідку, доставку корисного навантаження та ескалацію привілеїв.

– Організації SLTT під загрозою: через зменшення федеральної підтримки, включаючи припинення дії Угоди про співпрацю MS-ISAC, організації штатів, місцевих, плеємінних та територіальних органів (SLTT) стали більш вразливими до атак, ніж будь-коли. Це відбувається в той час, коли зловмисники цілеспрямовано атакують муніципальну інфраструктуру та периферійні/ОТ-пристрої державного сектору.

– Атаки на ланцюги поставок перетворюються на багатоетапні операції: підживлювані торговельними майданчиками даркнету та синтетичними профілями, зловмисники проникають у середовища постачальників, щоб швидко проникнути у більші підприємства. Управління ризиками постачальників та аналіз ризиків ланцюгів поставок зараз є критично важливими компонентами будь-якої сучасної програми управління вразливістю.

– Атаки на основі дипфейків та NLP зараз є мейнстрімом: зловмисники використовують обробку природної мови та симуляції інтерфейсу «мозок-комп'ютер», щоб видавати себе за справжніх співробітників у фішингових та вішингових атаках. Це робить традиційні протоколи перевірки особи дедалі застарілими.

Ці події вимагають нової позиції безпеки: такої, що базується на наступальній безпеці, принципах нульової довіри, збагаченої розвідкою про загрози в режимі реального часу та інтегрована в управління інформацією та подіями безпеки (SIEM), хмарну аналітику та віртуальні приватні мережі (VPN) або архітектури на основі SASE.

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

					ВКРБ-125.26.0037.00.00.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

Celestix Networks Taurus One

www.celestix.com

Компанія Celestix Networks серйозно ставиться до поняття «пристрій захисту»: її схожа на тостер модель Taurus One призначена для того, щоб допомогти невеликим фірмам убезпечити свої мережі.

Ефективний захист досягається завдяки партнерству з компанією Check Point Software Technologies, що веде постачальником міжмережевих екранів і інших засобів безпеки. Виріб працює під керуванням ОС Linux, і тому в ньому реалізовані багато функцій, характерні для Linux-пристроїв, такі як перевірка пошти й сумісність із протоколом FTP. Наявність цих функцій забезпечує порівняно просту інтеграцію із програмою захисту, що випускає Check Point. Однак цим інтеграція з ПЗ третіх фірм не вичерпується: партнерство з компанією Rainfinity дозволило включити в Taurus One засоби, що забезпечують відказостійкість і балансування навантаження.

Taurus One – щось більше, ніж просто готовий до роботи міжмережевий екран, що працює під керуванням Linux. Пристрій включає три порти 10/100 Ethernet, гніздо розширення PC Card, гніздо PCI, два порти USB, паралельні, послідовний порти, рознімання для підключення аудіо- і відеозасобів. Taurus One працює як невеликий Linux-сервер, у який убудовані функції забезпечення безпеки, що випускаються третіми фірмами. Це робить його розширюваним і дозволяє використовувати інші Linux-програми.

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		8

Хоча до пристрою можна підключити монітор і клавіатуру, реселлери переконуються, що для початкової установки не потрібно ні те, ні інше. Для установки виробу досить РК-панелі, що перебуває на його передній частині, і клавіш навігації.

Увівши початкову IP-адресу й параметри DHCP, фахівець, що виконує установку, повинен потім указати привласнений внутрішня IP-адреса й перемкнутися на консоль із Web-інтерфейсом через HTTPS-з'єднання й спеціальний порт. Консоль проста в роботі, її інтерфейс інтуїтивно зрозумілий при налаштуванні основних параметрів.

Використання функцій захисту ледве складніше. Наприклад, для звертання до програм Check Point потрібно фірмова керуюча консоль, що повинна бути встановлена на комп'ютер адміністратора. Хоча головна консоль керування Taurus One містить Web-посилання для завантаження керуючої консолі компанії Check Point на адміністративний комп'ютер, під час тестування це посилання не працювало, тому програму довелося встановлювати з CD-Диска.

Тим, хто знаком з інтерфейсом Check Point, буде легко працювати із цією консоллю. Однак користувачі, не знайомі з міжмережевими екранами й стилем керування Check Point, повинні прикласти певні зусилля для їхнього вивчення, але така ціна, що доводиться платити за безпеку на корпоративному рівні. Реселлери знайдуть компоненти Check Point VPN-1 і Firewall-1 досить надійними й швидко освоються з багатьма включеними в них функціями.

Фахівці Celestix заявляють, що пропускна здатність міжмережевого екрана становить 190 Мбіт/с, а віртуальної приватної мережі (VPN) – 90 Мбіт/с. Такі можливості забезпечуються завдяки використанню 900-МГц процесора Celeron і 256-Мбайт ОЗП. На убудованому 10-Гбайт жорсткому диску досить місця для зберігання системних журналів і додаткового ПЗ.

У моделі Taurus One реселлери виявлять велику розмаїтість можливостей, властивих міжмережевим екранам корпоративного класу. Пристрій забезпечує перепризначення портів, трансляцію мережних адрес (NAT) і повний контроль

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		9

пакетів, а також створення декількох так званих демілітаризованих зон (DMZ), що дозволяє організувати доступ зовнішніх партнерів і клієнтів до загальнодоступних Web- і FTP-серверам.

Таким чином, Taugus One містить у собі не тільки всі основні засоби безпеки, необхідні для мережі майже будь-якого розміру, але й додаткові можливості. Для використання таких функцій, як відказостійкість і балансування навантаження, необхідно встановити два пристрої в кожній з філій і тим самим забезпечити безперебійну роботу й високу пропускну здатність.

Fortinet FortiGate-200

www.fortinet.com

Сьогодні малі й середні компанії при підключенні до Інтернету приділяють питанням захисту першочергова увага. Фірма Fortinet вирішує основні проблеми безпеки, що турбують як реселлерів, так і власників компаній. Модель FortiGate-200 містить у собі міжмережевий екран з повним контролем пакетів і засобами створення VPN, антивірусне ПЗ, засобу фільтрації Web-інформації й розширені функції реєстрації. Такі можливості дозволяють вирішити головні проблеми, з якими зіштовхуються адміністратори мереж більшості компаній середнього розміру.

FortiGate-200 дозволяє спростити багато завдань захисту мереж, пов'язані з корпоративними міжмережевими екранами. Всіма функціями пристрою можна управляти через консоль із Web-інтерфейсом. Додається чудова документація. Консоль проста в навігації, і процес адміністрування не становить праці. По розмірі модель FortiGate-200 деяким більше Ethernet-комутатора. Вона має корпус висотою 1U, на лицьовій панелі якого розміщені три Ethernet-порти: внутрішньої (локальної) мережі, зовнішньої (глобальної) мережі й демілітаризованої зони (DMZ). Передбачений також 20-Гбайт жорсткий диск для зберігання журналів.

Пристрій виявився простим в установці, зажадавши лише декількох ручних операцій перед запуском майстра-програми. У ході початкової установки

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		10

необхідно сконфігурувати робочу станцію зі статичною IP-адресою. Після того як виконане призначення IP-адрес, усе, що залишається зробити, це підключитися з мережного комп'ютера до пристрою через Ethernet. Потім варто використовувати браузер, щоб приєднатися до консолі керування FortiGate-200 і запустити майстер-програму установки. Вона виконує лише базове конфігурування: завдання внутрішніх і зовнішніх IP-адрес, настроювання сервера DHCP і демілітаризованої зони.

Після завершення роботи майстер-програми адміністратор може використовувати консоль для більш тонкого настроювання пристрою. Параметри міжмережевого екрана задаються на основі політик, і його конфігурування не становить праці.

Користувальницький інтерфейс допомагає адміністраторам створювати нові політики. Для цього потрібно всього лише вибрати кілька опцій з меню в кожному полі вікна. Задавати правила для портів, розкладів і виключень демілітаризованої зони так само просто, як і створювати первісні політики. Інтерфейс пропонує допомогу там, де це необхідно, полегшуючи установку для тих, хто не дуже добре знайом з міжмережевими екранами.

Реселлери знайдуть, що VPN працює надійно. Можна використовувати всі основні протоколи шифрування: IPSec, PPTP і L2TP. Приємним доповненням є можливість автентифікації по методу RADIUS. Модель FortiGate-200 включає також базові функції виявлення вторгнення й навіть реєструє спроби проникнення в мережу. Інтерфейс включає великий список типових атак і допускає створення власних подій, що дозволить урахувати стратегії нових атак у майбутньому. Великою перевагою є убудований антивірусний захист.

Пристрій дозволяє виявити присутність вірусів ще до того, як підозрілі дані досягнуть комп'ютерів внутрішньої мережі й навіть демілітаризованої зони.

Система може виявляти віруси залежно від типів їхньої активності: від трафіку по протоколах FTP і SMTP до локальних HTTP-запитів. Компанії, що бажають контролювати вихідні дані, зможуть скористатися інтегрованим

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		11

фільтром Web-інформації. Фільтр можна вручну налаштувати або на сканування, що попереджає, Web-сторінок для виявлення змісту забороненого до передачі, або на блокування Web-адрес. Правила фільтрації прийдеться сконфігурувати вручну. У цій частині можливості пристрої далекі від досконалості, але проте можуть задовольнити майже всі потреби невеликих компаній.

Реселлери, що обслуговують мережі з інтенсивним трафіком, оцінять великий набір функцій реєстрації. Убудований 20-Гбайт жорсткий диск здатний зберігати величезну кількість інформації, і при бажанні пристрій може реєструвати весь минаючий трафік. Функції внутрішньої звітності забезпечують реєстрацію подій у трьох окремих журналах, призначених для трафіку, подій і атак. Ці журнали можна використовувати при рішенні більшості проблем. Можливо також збереження журналів у форматі програми WebTrends, і реселлери зможуть скористатися цією утилітою для моніторингу за роботою пристрою. З інших адміністративних функцій варто назвати засобу керування з віддаленого комп'ютера й повідомлення по електронній пошті.

SonicWall TELE3 SP

www.sonicwall.com

Пропонуючи пристрій мережного захисту TELE3 SP, фірма SonicWall приходить на виторг невеликим компаніям, що бажають вирішити проблеми безпеки. Виріб призначений для захисту мереж, що нараховують до 10 користувачів, від навал з Інтернету.

TELE3 SP має привабливий срібисто-блакитний корпус, що по розмірі ненабагато перевершує кишеньковий комп'ютер, але забезпечує чимало можливостей.

Пристрій оснащений світлодіодними індикаторами стану, портами для підключення до глобальних і локальних мереж, а також розніманням RJ-11, що забезпечує доступ до убудованого модему. Набір функцій цієї моделі ідеально підходить для невеликих мереж. TELE3 SP підключається безпосередньо до широкополосному з'єднання через порт глобальної мережі, а з іншого боку – до

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		12

локальної мережі через внутрішній порт. Убудований модем можна використовувати для забезпечення відказостійкості системи, зконфігурувавши пристрій на встановлення з'єднання, що комутується, з Інтернет-провайдером у випадку відмови широкополосного каналу зв'язку. Можливості моделі TELE3 SP набагато ширше, ніж у простого широкополосного комутатора. Крім трансляції мережних адрес (NAT) і сервера DHCP, пристрій виконує також функції повнофункціонального міжмережевого екрана й VPN. З інших ключових функцій варто назвати сканування вірусів і фільтрацію інформації з Web.

Для тестування інженери підключили модель TELE3 SP до невеликої мережі, що складається із трьох настільних ПК, що працюють під керуванням ОС Windows. Порт глобальної мережі був підключений прямо до кабельного модему, налаштованому на роботу із широкополосним каналом.

Первинна установка виробу проста, однак необхідно вручну ввести для кожного ПК його задається по умовчання статична IP-адреса у внутрішньої підмережі, що трохи ускладнює цей процес. Реселлери знайдуть, що працювати з консоллю керування на базі браузера під керуванням Java – одне задоволення. Тим, хто використовує Windows XP, перш ніж конфігурувати систему, потрібно буде завантажити й установити засоби для роботи з Java у браузері Internet Explorer. Після первинної установки необхідно зареєструвати пристрій, щоб розблокувати багато хто із включених у нього функцій. Майстер-програма установки полегшує виконання основної частини інсталяції. Після цього можна перейти до конфігурування засобів відказостійкості й інших функцій. Майстер-програму варто розглядати як перший крок у процедурі підключення, за яким піде подальша робота з налаштування встаткування.

Розширені функції моделі TELE3 SP пропонуються за окрему плату, але реселлери можуть завантажити й запустити обмежені за часом пробні версії більшості з них. Це відкриває перед клієнтами звабну можливість їх випробувати, дозволяючи реселлерам додатково продати їм розширені функції в майбутньому. Систему фільтрації контенту можна зконфігурувати або для роботи із власним

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		13

списком Web-адрес компанії SonicWall, або на завантаження оновлюваних списків блокуємих Web-адрес із сайтів Websense або N2H2. Адміністратори можуть установити додаткову фільтрацію по відповідному типі інформації, щоб блокувати доступ до певної категорії сайтів.

Фахівці, що бажають забезпечити віддалений доступ до своєї мережі через віртуальну приватну мережу, також не будуть розчаровані можливостями моделі TELE3 SP. Хоча пристрій здатний обслуговувати не більше 10 паралельних VPN-з'єднань, більшість дрібних компаній знайдуть, що цього досить для невеликого числа їхніх користувачів. Функції VPN реалізовані на базі звичайного стандарту IPSec, що гарантує сумісність із устаткуванням майже будь-якого постачальника, що використовує цей протокол. Захист мережі від вторгнення – ще одна важлива можливість моделі TELE3 SP. У пристрій інтегрований міжмережевий екран, сертифікований організацією ICSA. Екран забезпечує повний контроль пакетів. Це звичайний метод запобігання й реєстрації вторгнень.

Таким чином, модель SonicWall TELE3 SP має все необхідне для безпечної роботи й захисту мережі невеликої компанії або філії корпорації. Єдине її обмеження – кількість одночасних VPN-з'єднань, що не може перевищувати 10.

Symantec Firewall/VPN Appliance 200R

www.symantec.com

Symantec прагне спростити забезпечення мережної безпеки за допомогою моделі Firewall/VPN 200R. Це пристрій, по розмірі деяким більше середнього 8-портового Ethernet-комутатора, включає функції, які потрібні невеликим компаніям, що бажають захистити свою мережу.

Модель 200R відрізняється простотою як в установці, так і в керуванні. Консоль керування з Web-інтерфейсом настільки інтуїтивно зрозуміла й інформативна, що технічно грамотному користувачеві досить кілька хвилин для її освоєння. Два порти для підключення до глобальної мережі дозволяють використовувати два широкополосних з'єднання. В ідеалі компанія при рішенні особливо важливих завдань може працювати й через кабельний модем, і через

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		14

DSL-з'єднання, що дозволить виключити перерви в обслуговуванні. Крім того, пристрій можна сконфігурувати таким чином, щоб забезпечити відказостійкість за допомогою зовнішнього модему, установивши комутирується підключення, що, до Інтернет-провайдеру через послідовний порт і модем у випадку відмови обох широкополосних з'єднань.

Вмонтувавши у свою модель комутатор на 8 портів, Symantec дозволяє клієнтам заощадити на покупці додаткового встаткування, що актуально для малих фірм.

Ті, хто використовує широкополосні з'єднання з динамічно призначуваними IP-адресами, виграють від убудованої підтримки DNS. Ця динамічна служба дозволяє прив'язати доменне ім'я до поточного зовнішнього IP-адресі пристрою. Безпеку забезпечує убудований міжмережевий екран, що виконує повний контроль пакетів, трансляцію мережних адрес (NAT) і який забезпечує роботу VPN, що гарантує захищеність комп'ютерів внутрішньої мережі від вторгнень із Інтернету.

Щоб протестувати пристрій, інженери приєднали його до невеликої мережі із трьох робочих станцій під керуванням Windows 98, 2000 і XP відповідно. Широкополосне з'єднання забезпечував кабельний модем Motorola, підключений до служби Optimum Online мережі Cablevision. Початкова установка пристрою зайняла кілька хвилин. Консоль із Web-інтерфейсом гранично спрощує більшу частину конфігурування. Компанії, що планують скористатися хостингом, оцінять простоту таких функцій, як перепризначення портів і створення демілітаризованої зони.

Одна з важливих можливостей моделі 200R – сумісність із VPN. У комплект поставки входить VPN-клієнт, що відіграє роль персонального міжмережевого екрана й добре працює на Windows-системах. Інженери Тест-центра знайшли, що установка серверної й клієнтської частини VPN не викликає утруднень і дозволяє швидко організувати захищений доступ для віддалених користувачів. З інших важливих функцій варто назвати великі засоби реєстрації,

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		15

ведення системного журналу й відправлення повідомлень по електронній пошті. Постачальники рішень можуть зконфігурувати пристрій для автоматичного розсилання повідомлень у випадку підозрілих подій. Це дозволяє запропонувати послуги дистанційного керування.

Модель 200R – відмінний вибір для компаній, що бажають мати міжмережевий екран і функції VPN; однак тим, кому потрібно блокувати спам, перевіряти трафік на наявність вірусів і фільтрувати Web-контент, прийдеться подумати про установку додаткового встаткування. Підбиваючи підсумок, можна сказати, що модель Symantec 200R відкриває невеликим фірмам і філіям корпорацій простий шлях до забезпечення безпеки, не вимагає особливих зусиль і має привабливу ціну.

WatchGuard Firebox 100

www.watchguard.com

Повнофункціональні міжмережеві екрани часто перебувають за межами фінансових можливостей компаній середнього розміру. Але ж багато хто з них мають потребу в засобах захисту корпоративного класу й функціях VPN, але не мають ні необхідного персоналу, ні бюджету.

Фірма WatchGuard постаралася вирішити цю проблему за допомогою свого пристрою Firebox 1000. Завдяки цій моделі функції міжмережевого екрана корпоративного класу й VPN стають доступними навіть для середніх компаній, тому що пропонуються за привабливою ціною. Реселлери знайдуть, що модель Firebox 1000 забезпечує всі можливості, які можна чекати від міжмережевого екрана високого класу, але відрізняється більше складною установкою, характерної для пристроїв такого рівня.

Інсталяція Firebox 1000 вимагає попереднього планування. Насамперед потрібно зконфігурувати керуючий ПК і зібрати всю необхідну інформацію про мережу. Firebox 1000 ніяк не назвеш пристроєм «plug-and-play», тому тим, кому потрібна дружна майстер-програма установки на базі браузеру, краще звернутися до іншої моделі. Після первісного конфігурування керуючого ПК необхідно діяти

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		16

відповідно до прикладеної схеми експрес-установки. У ході цього процесу потрібно буде скористатися прикладеним CD-Диском, щоб зконфігурувати пристрій. Цікаво, що інструкція з інсталяції рекомендує завантажити останню версію ПЗ. Виникає нерозв'язний парадокс: поки пристрій не зконфігуровано, керуючий ПК не має доступу в Інтернет і не може завантажити нову версію програми.

Керування пристроєм здійснюється через фірмову консоль адміністрування. Щоб з нею освоїтися, буде потрібно якийсь час, а для доступу до консолі необхідний пароль. Щоб управляти пристроєм, потрібно ввести реєстраційне ім'я користувача й пароль із семи символів. Спочатку адміністраторам прийдеться постійно звертатися до документації, поки вони повністю не освоються з інтерфейсом консолі.

Що стосується функціональних можливостей, те тут Firebox 1000 блищить. Пристрій здатний обслуговувати до 1000 користувачів і забезпечує пропускну здатність до 185 Мбіт/с. Це повинне задовольнити потреби майже будь-якої компанії середнього розміру. Хоча модель WatchGuard складна в адмініструванні, вона має ряд дуже коштовних функцій. Зокрема, можна досить тонко зконфігурувати блокування спама. Для цього призначена програма SpamScreen, що блокує виявлений «сміття». Пристрій також включає функції антивірусного захисту. Завдяки партнерству з фірмою McAfee компанія змогла реалізувати в міжмережевому екрані автоматичне детектування вірусів, ще перше ніж вони потраплять у локальну мережу.

З інших важливих особливостей варто назвати гнучкий засіб забезпечення відказостійкості, а також можливість фільтрації контенту й виявлення вторгнень. Постачальники рішень оцінять великі функції звітності. Можна зареєструвати майже будь-яка подія, а потім одержати звіт. Це дозволить реселлерам запропонувати додаткові послуги й виправдати витрати на впровадження, а також спростить рішення виникаючих проблем.

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		17

З огляду на вищесказане, можна зробити вивід, що модель Firebox 1000 здатна гарантувати безпека мережі компанії середнього розміру, забезпечуючи захищені з'єднання з декількома філіями, а також з мобільними користувачами. Реселлери, яким потрібний міжмережевий екран корпоративного класу із широкими можливостями VPN, будуть повністю задоволені цією моделлю.

2.2 Обґрунтування вибору засобів для побудови системи кібербезпеки та мови програмування

Python – високорівнева мова програмування, яку називають другою за популярністю в світі. Її використовують для розробки вебзастосунків, програмного забезпечення, машинного навчання. Python застосовують для вирішення робочих завдань у компаніях Google, Instagram, Facebook, IBM, NASA, Dropbox, Netflix та інших. Розробники цінують цю мову програмування за простоту у вивченні, ефективність та мультиплатформність.

Python – скриптова мова програмування з досить простим синтаксисом. Для розуміння достатньо порівняти принципи написання найпростішої програми, яка виводить на екран текстове повідомлення. Саме тому мова програмування Python більш доступна для новачків, а професіонали встигли адаптувати її для вирішення великої кількості завдань. Це мультиплатформне рішення, тому знання Python дає можливість працювати у різних сферах: від розробки мобільних застосунків до ігрової індустрії та штучного інтелекту.

У мови програмування динамічна типізація: є можливість передавати до функцій будь-який тип даних без попереднього вказання. Інтерпретованість дозволяє знаходити помилки у коді ще до повної збірки у робочий застосунок. При цьому Python дуже чітко дає зрозуміти, де та через що виникла помилка.

Це мова об'єктноорієнтованого програмування (ООП). Програмне забезпечення на Python оформлене у вигляді моделей, які можуть бути зібраними у пакети. Тип та структуру кожного об'єкта можна запитати під час виконання

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		18

програми. Для кожного з об'єктів можна отримати всю інформацію щодо його внутрішньої структури. Окрім того:

- у мови логічний синтаксис, завдяки чому вихідний код легко читати та розуміти;
- гнучкість та масштабованість Python дозволяє адаптувати високорівневу логіку та розширяти складні застосунки, як тільки виникне така необхідність;
- розробка на Python у більшості випадків проходить швидше, ніж на інших мовах програмування;
- Python – інтерпретована мова програмування. Це значить, що код можна написати у будь-якому текстовому файлі на будь-якій платформі, і потім успішно запустити;
- у Python – колосальна спільнота однодумців. Тож будь-які складнощі конкретних розробників вирішуються колективно.

Проте є декілька особливостей, які можна віднести до недоліків. Це повільність (ця мова програмування хоч і універсальна, проте повільніша за інші), велика кількість ресурсів, необхідних для роботи та «прив'язаність» до системних бібліотек.

Мова програмування Python використовується у наступних сферах:

1. Розробка програмних застосунків будь-якого напрямку.
2. Розробка серверної частини мобільних застосунків (найпопулярніший напрямок).
3. Ігри. Багато сучасних ігор для комп'ютерів (наприклад, World of Tanks) частково чи повністю написані на Python.
4. Вбудовані системи для різних пристроїв. Дуже часто Python використовують для написання внутрішніх платформ управління банкоматами.
5. Скрипти та плагіни до уже реалізованих програм для автоматизації процесів чи створення інших рішень.
6. Тестування (автоматизація цього процесу).

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		19

7. Машинне навчання. – основна мова для написання алгоритмів і аналітичних застосунків у сфері Machine Learning.

Бібліотеки Python

Різні бібліотеки Python використовують для виконання конкретних завдань. Наприклад, Matplotlib підходить для відображення даних у двовимірній та тривимірній графіці. Pandas підходить для зручної роботи з даними. NumPy дозволяє створювати масиви та керувати ними. Requests використовується для веброзробки. OpenCV-Python відкриває можливості для обробки зображень з метою оптимізації систем «машинного зору».

Найвідоміші фреймворки для мови програмування Python

Фреймворки Python допомагають створити зручне та функціональне середовище для розробки. У них міститься набір інструментів, модулів та бібліотек, корисних для виконання конкретних завдань. Це значно полегшує роботу: наприклад, дає змогу не витрачати час на розписування дій, які повторюються, а використати релевантний інструмент. Тож є можливість позбутися рутинних процесів та сконцентруватися на логіці проекту.

Серед найпопулярніших фреймворків для Python:

- Django – найстаріший та найвідоміший. Створений для реалізації великих інтерактивних проєктів;
- Pyramid – зручний у налаштуваннях, і дає можливість реалізувати складні нестандартні ідеї;
- Web2py – підходить в першу чергу для вебзастосунків і може використовуватись на будь-яких архітектурах.

Популярні Python IDE

IDE або інтегровані середовища розробки – це програмне забезпечення, яке надає розробникам необхідні інструменти для написання, редагування, тестування та налаштування коду. Для розробки на Python найчастіше використовують IDE PyCharm, IDLE, Spyder та Atom.

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 протидії загрозам корпоративній 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-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		21

3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ

3.1 Опис функціонування системи

ШІ стає автономним – ризики агентного ШІ, LLM та MCP

Штучний інтелект більше не обмежується прогновною аналітикою чи вузькою автоматизацією. У 2026 році екосистеми штучного інтелекту ближче до повного розвитку у складні середовища, де агентний штучний інтелект, автономні агенти, моделі великих мов (LLM) та нові стандарти, такі як протокол контексту моделі (MCP), взаємодіють у великих масштабах. Ця еволюція створює безпрецедентні виклики для ідентифікації загроз, виявлення загроз та реагування на інциденти.

Зловмисники зараз розгортають системи штучного інтелекту, здатні приймати самостійні рішення, переписувати власний код, перемикатися між мережами та вибирати цілі з майже ідеальною точністю. Оскільки штучний інтелект стає все глибшою інтеграцією в бізнес-операції, центри операцій безпеки (SOC) повинні ставитися до штучного інтелекту не просто як до інструменту, а як до нового класу цифрових персонажів із власною поверхнею атаки.

Як агентний ШІ розширює поверхню атаки

Агентний ШІ стосується систем, здатних до самокерованих дій. Він має «агентність», тому для його опису було обрано термін «агентний».

У руках кіберзлочинців ці автономні агенти можуть:

- проводити розвідку внутрішньої інфраструктури;
- сканувати наявність вразливостей та автоматично їх використовувати;
- налаштувати корисне навантаження, щоб уникнути виявлення SIEM;
- імітувати людську поведінку, щоб обійти засоби контролю автентифікації.

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		22

Ця децентралізована форма автоматизації дозволяє кібератакам пришвидшуватися набагато швидше, ніж час реагування людини, перевантажуючи традиційні захисні робочі процеси.

Перетворення LLM, NLP та застосувань штучного інтелекту на зброю

Кіберзлочинці тепер використовують обробку природної мови та інструменти на основі LLM для:

- створювати синтетичні профілі для крадіжки особистих даних;
- створювати переконливі фішингові або вішингові скрипти;
- видавати себе за керівників за допомогою клонування голосу в режимі реального часу;
- створювати варіанти шкідливого програмного забезпечення за допомогою автоматичної генерації коду.

Зближення моделей NLP та машинного навчання підвищує ефективність фішингових атак та соціальної інженерії з використанням дипфейків, що ускладнює їх розпізнавання співробітниками, навіть за умови навчання.

Ризики сумісності MCP та екосистеми штучного інтелекту

Протокол **контексту моделі (MCP)** стандартизує зв'язок між моделями та програмами штучного інтелекту. Хоча MCP покращує інтеграцію підприємства, він також стандартизує експлуатацію. Один скомпрометований інструмент штучного інтелекту може каскадно поширюватися на підключені системи, зокрема:

- хмарні інструменти безпеки;
- платформи управління ланцюгами поставок;
- внутрішні бази знань;
- постачальники ідентифікаційних даних.

У 2026 році забезпечення безпеки екосистем штучного інтелекту означає постійний аудит вхідних даних штучного інтелекту, контекстних інструкцій та шляхів від моделі до програми.

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		23

Квантова повзучість та поява квантово-безпечної безпеки

Квантові обчислення ще не повністю озброєні, але їхній вплив вже змінює стратегію кібербезпеки. «Квантове повзуче зростання» описує поступове впровадження квантових можливостей та квантово-орієнтованих ризиків у основне планування кібербезпеки. Навіть без широкомасштабних квантових кібератак, саме очікування змушує організації переосмислити криптографію, довгостроковий захист даних та дотримання нормативних вимог.

Підготовка до постквантової криптографії

Лідери галузі, включаючи Національний інститут стандартів і технологій (NIST) і Центр інтернет-безпеки, закликають організації розпочати перехід на квантово-безпечні алгоритми. Це включає підготовку до криптографічної гнучкості, тобто можливості швидко перемикатися між методами шифрування в міру виникнення вразливостей.

Зловмисники, що використовують квантові технології, вже збирають зашифровані дані («зібрати зараз, розшифрувати пізніше»), знаючи, що майбутні квантові інструменти можуть зламати поточні алгоритми. Галузі, що регулюються GDPR, HIPAA та вимогами до дотримання фінансових вимог, стикаються з додатковою терміновістю через чутливість довгохвостих даних.

Стратегічний ризик для довговічних систем та інфраструктури ОТ

Оператори критичної інфраструктури – енергетичні компанії, виробничі заводи, транспортні вузли – значною мірою покладаються на довговічні ОТ та периферійні пристрої, які нелегко оновити або замінити. Ці системи є головними цілями для майбутніх квантових атак.

Керівники відділів безпеки повинні оцінити:

- чи зможуть їхні криптографічні системи витримати майбутнє розшифрування;
- як змінюються ризики їхнього ланцюга поставок за умови теоретичних квантових можливостей;
- тривалий вплив збережених або переданих конфіденційних даних.

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		24

Кіберзагрози критичній інфраструктурі та об'єктам SLTT

У 2026 році критично важлива інфраструктура та суб'єкти державного, місцевого, племінного та територіального рівня (SLTT) стикаються зі зростанням кіберзагроз та зростаючими обмеженнями ресурсів. Скорочення фінансування, включаючи закінчення терміну дії Угоди про співпрацю, яка підтримувала послуги через Багатодержавний центр обміну та аналізу інформації (MS-ISAC), залишило багато державних установ беззахисними, саме тоді, коли зловмисники посилюють свою увагу до них.

Кіберзлочинці націлені на такі сектори, як енергетика, водопостачання, громадський транспорт та освіта, всі з яких значною мірою залежать від недофінансованих або застарілих систем. Ці сектори дедалі більше залежать від периферійних/ОТ-пристроїв, що робить їх особливо вразливими до атак на системи управління на рівні інфраструктури.

Шаблони атак SLTT стають дедалі складнішими

Супротивники більше не покладаються виключно на грубу силу чи опортуністичні методи. Натомість вони використовують:

- скоординовані атаки програм-вимагачів, приурочені до виборчих циклів або розгортання програм у фінансовий рік
- поліморфне (змінне) шкідливе програмне забезпечення, яке адаптується до локальних середовищ
- спеціалізовані фішингові кампанії, спрямовані на муніципальних службовців та обраних посадовців
- крадіжка особистих даних та використання штучних профілів для обходу систем верифікації

Без надійних інструментів виявлення загроз, інтеграції SIEM та співпраці з платформами, орієнтованими на правоохоронні органи, ці атаки залишаються непоміченими, доки не буде завдано шкоди.

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		25

Проблеми державного сектору з дотриманням нормативних вимог та реагуванням

Багато організацій SLTT працюють з ефективними командами безпеки та застарілими системами, які важко посилити. Проте вони все ще повинні дотримуватися вимог CISA, NIST та регіональних регуляторних органів, що постійно змінюються. Розрив між регуляторними вимогами та операційними можливостями зростає.

Результат: навіть агентства з добрими намірами мають труднощі з дотриманням принципів нульової довіри, що залишає широкі можливості для атак.

Зростання напівавтономного та штучно підтриманого шкідливого програмного забезпечення

У 2026 році спостерігається поява нового покоління шкідливих програм: напівавтономних, що працюють за допомогою штучного інтелекту та часто розгортаються через платформи «злочинне програмне забезпечення як послуга» (CaaS). Ці типи шкідливих програм використовують генеративний штучний інтелект, самокероване поширення та методи обфускації з урахуванням середовища, щоб розвиватися швидше, ніж захисники можуть адаптуватися.

Шкідливе програмне забезпечення тепер є живою системою, що навчається, яка може змінюватися, уникати змін та перекомпілюватися майже в режимі реального часу. Це створює величезний тиск на традиційні протоколи ідентифікації загроз, правила кореляції SIEM та стеки безпеки кінцевих точок.

Поліморфні корисні навантаження та багатоплатформний охоплення

Зловмисники розробляють шкідливе програмне забезпечення, яке безперебійно працює в середовищах Windows, Linux та macOS, усуваючи потребу в окремих кодових базах. Ці постійно змінювані та адаптуючі (поліморфні) корисні навантаження адаптують свою поведінку на основі системної телеметрії, що робить виявлення на основі сигнатур неефективним.

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		26

Штучний інтелект у розробці та поширенні шкідливого програмного забезпечення

Використовуючи генеративний штучний інтелект, розробники шкідливого програмного забезпечення можуть:

- створюйте нескінченну кількість варіантів коду з мінімальним втручанням людини;
- автоматично адаптувати експлойти на основі опублікованих CVE;
- автоматично генерувати фішингові сторінки або скрипти імітації, що відповідають корпоративному брендингу;
- імітувати поведінку користувача, щоб уникнути спрацьовування поведінкової аналітики.

Захист від загрози штучного інтелекту та шкідливого програмного забезпечення

Щоб протистояти цьому новому класу загроз, організації повинні поєднати:

- моніторинг поведінки в режимі реального часу;
- адаптивна інтеграція розвідки загроз;
- кросплатформна оркестрація SIEM та SOAR;
- постійні оновлення моделей у засобах захисту кінцевих точок.

Хмарні інструменти безпеки з вбудованим штучним інтелектом у поєднанні з управлінням вразливостями, принципом нульової довіри та робочими процесами швидкого реагування є важливими для запобігання переростанню напівавтономних загроз у повномасштабні порушення.

Багатоетапні, багатовекторні атаки та вдосконалений дизайн кампаній

У 2026 році кібератаки еволюціонували від лінійних вторгнень до багатоетапних, багатовекторних кампаній. Ці складні атаки поєднують традиційне шкідливе програмне забезпечення, глибоку соціальну інженерію та скоординоване використання інфраструктури для обходу багаторівневого

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		27

захисту. Згідно зі звітом Microsoft Digital Defense Report 2025, сучасні кампанії зловмисників часто розгортаються протягом тижнів або місяців: поєднуючи розвідку, проникнення та витік даних у безперервну послідовність.

Багатовекторна інфільтрація – це новий стандарт

Сучасні кіберзлочинці рідко покладаються на одну точку входу. Натомість вони організовують атаки через:

- фішинг (електронна пошта, голосові повідомлення та SMS);
- заражені оновлення програмного забезпечення;
- доступ до ланцюга поставок третіх сторін;
- неправильно налаштовані хмарні середовища;
- скомпрометовані облікові дані з даркнету.

Кожен вектор розподілений за часом та узгоджений для збільшення ймовірності успішного порушення, використовуючи прогалини у внутрішній комунікації, управлінні вразливостями або забезпеченні дотримання політик.

Цілеспрямований пост-експлуатаційний та латеральний рух

Після першого доступу зловмисники використовують методи ухилення від SIEM та інструменти придушення SOAR. Ці кампанії розроблені для того, щоб:

- залишаються неактивними, доки не будуть виявлені цінні дані;
- обійти сегментовані мережі за допомогою моделей поведінки, що базуються на машинному навчанні;
- використовувати легітимні адміністративні інструменти, щоб уникнути виявлення;
- рухатися вбік, щоб евакуюватися з резервних систем або зон аварійного відновлення.

Складність цих кампаній вимагає переходу від захисту периметра до поведінкової аналітики в режимі реального часу.

Розвідка темного вебу як прогностичний сигнал

Одним із найважливіших уроків 2025 року стала поява розвідки даркнету як критично важливої можливості. Команди безпеки тепер відстежують:

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		28

- витік облікових даних;
- набори експлойтів;
- переговорна діяльність щодо програм-вимагачів;
- обговорення майбутніх атак на форумах кіберзлочинців.

Організації, що інтегрують цю аналітику у свої стеки SIEM та NDR, можуть виявляти наміри до розгортання корисних навантажень, що є ключовою перевагою в умовах прискореного циклу загроз у 2026 році.

Загрози у виборчий рік – дідфейки, дезінформація, когнітивна війна

У той час, як Сполучені Штати готуються до важливого виборчого циклу 2026 року, кіберзагрози поєднуються з когнітивними (соціальними та психологічними) шляхами атак, спрямованими на маніпулювання громадською думкою, придушення довіри виборців та дестабілізацію місцевих інституцій. Ця тактика не є новою, а просто більш складною, оперативною, автоматизованою та тривожно ефективною.

Шахрайство з глибокими фейками стає мейнстрімом

У 2026 році технологія глибоких фейків для відео та голосу стане не тільки реалістичнішою, але й доступнішою. Використовуючи генеративний штучний інтелект, зловмисники зможуть створювати в режимі реального часу імітації:

- політичних кандидатів;
- місцеві чиновники;
- керівники корпорацій;
- співробітники служби безпеки.

Ці ресурси використовуються у фішингових атаках, шахрайських дзвінках та дезінформаційних кампаніях для запуску несанкціонованих дій або широкого розголосу.

Дідфейки також використовуються в атаках програм-вимагачів, де жертв маніпулюють, змушуючи повірити, що дані були викрадені або оприлюднені, використовуючи сфабриковані докази.

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		29

Дезінформація як кіберзброя

Когнітивна війна включає стратегічне розгортання дезінформації шляхом:

- боти соціальних мереж та джерела фейкових новин;
- іменовані облікові записи з перевіреними обліковими даними;
- статті, написані за допомогою штучного інтелекту, розміщені на публічних форумах;
- скоординований наплив коментарів та маніпулювання настроями.

Ці атаки зазвичай використовуються для підриву довіри до виборів, корпорацій та державних установ. Для організацій SLTT, які вже й так розчаровані, шкода для довіри та єдності може бути серйозною.

Захист від когнітивних атак вимагає міждисциплінарної стратегії

Традиційні інструменти кібербезпеки, такі як SIEM та захист кінцевих точок, недостатні для виявлення психологічних операцій. Захист повинен включати:

- навчання співробітників щодо імітації штучного інтелекту;
- кампанії з медіаграмотності для установ, що працюють з громадськістю;
- співпраця з федеральними агентствами та цільовими групами з безпеки виборів;
- інтеграція розвідки з відкритих джерел у платформи виявлення загроз.

У контексті Zero Trust Security (безпеки нульової довіри), перевірка особи має поширюватися не лише на користувачів та пристрої, а й включати голосові шаблони, відеоконтент та оцінку автентичності для всіх вхідних повідомлень.

Операційні основи під атакою

Незважаючи на зростання кількості передових кіберзагроз, найруйнівнішими порушеннями у 2026 році все ще є фундаментальні аспекти операційної безпеки. Неправильно налаштовані системи, затримки з оновленнями та недостатній контроль доступу залишаються основними точками входу, особливо коли зловмисники зараз використовують штучний інтелект, щоб скоротити час між опублікованою вразливістю та її реальним експлойтом до

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		30

лічені години.

Цей розрив у швидкості означає, що управління вразливостями, колись рутинна функція, перетворилося на змагання з автономним шкідливим програмним забезпеченням та ботами для сканування в режимі реального часу.

Управління патчами тепер є тактичним пріоритетом

Сучасні зловмисники відстежують цикли випуску патчів від постачальників та використовують прогалини, перш ніж організації зможуть розгорнути виправлення. Навіть короткі затримки можуть мати катастрофічні наслідки.

Щоб пом'якшити це, команди безпеки повинні впровадити:

- автоматизовані конвеєри виправлень для критично важливих активів;
- міжвідомча узгодженість для мінімізації опору простоям;
- оцінювання вразливостей, пов'язане з впливом на бізнес та вікнами впливу.

Розподіл за найменшими привілеями та нульовою довірою

Поширення привілеїв залишається тихим фактором, що сприяє серйозним порушенням. У 2026 році зловмисники використовують надмірно привілейовані облікові записи та погано сегментовані мережі для досягнення горизонтального просування.

Організації, які не впроваджують принцип нульової довіри, часто найбільше страждають від внутрішніх загроз, ескалації привілеїв та постійного часу перебування шкідливого програмного забезпечення.

Втома від лідерства та людський рівень

Ключовий урок 2025 року – і той, що залишається актуальним – полягає в тому, що навіть найкращі технічні інструменти не можуть компенсувати виснажене керівництво. Директори з інформаційних технологій та ІТ-директори, які керують постійними станами підвищеної готовності, часто відчують вигорання, що призводить до:

- затримка у прийнятті рішень;

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		31

- відсутність стратегічної спрямованості;
- накопичення боргу за цінними паперами.

У 2026 році підвищення кіберстійкості також означає вирішення питань добробуту керівників, розподілу ресурсів та психологічної стійкості як векторів стратегічних ризиків.

Глобальний сплеск атак типу «відмова в обслуговуванні» та соціальної інженерії

Глобальне середовище загроз у 2026 році спостерігає відродження атак типу «відмова в обслуговуванні» (DoS) та кампаній соціальної інженерії, не лише за обсягом, але й за стратегічною координацією. Згідно з нещодавніми висновками звіту ENISA «Ландшафт загроз 2025» та звіту Verizon про розслідування витоків даних, зловмисники виконують багаторівневі операції, які поєднують порушення роботи інфраструктури з маніпуляціями з ідентифікацією.

DoS- та DDoS-атаки дешевші, сильніші та частіші

Ботнети скомпрометованих пристроїв Інтернету речей та периферійних пристроїв тепер керуються за допомогою систем командування та управління на базі штучного інтелекту. Ці системи коригують трафік атак у режимі реального часу, орієнтуючись на слабкі місця в:

- хмарна інфраструктура
- урядові вебсайти
- портали реєстрації виборців
- банківські API

Хмарні інструменти безпеки та інтелектуальні служби балансування навантаження допомагають зменшити ці ризики, але лише в поєднанні з раннім виявленням за допомогою мережевого виявлення та реагування (NDR).

Еволюція соціальної інженерії

Тактики соціальної інженерії еволюціонували в психологічно оптимізовані взаємодії, згенеровані штучним інтелектом. Зловмисники тепер поєднують генеративний штучний інтелект, поведінкову аналітику та публічні

дані для створення комунікацій, які:

- імітувати виконавчий тон та стиль письма;
- посилання на внутрішні документи або жаргон;
- виглядають терміновими або емоційно зарядженими.

Варіанти включають:

– фішингові електронні листи, що обходять спам-фільтри за допомогою коригувань NLP;

- дзвінки Вішінга з використанням підроблених голосів;
- кампанії з розваги, приурочені до реальних подій (наприклад, податкові терміни, звільнення, оновлення програмного забезпечення).

Ці загрози обходять технічний захист, впливаючи на людський інстинкт довіри. У відповідь на це навчання з питань безпеки має розвиватися, включаючи симуляції загроз у реальному часі та тестування емоційних реакцій.

Боротьба з гібридною атакою людини та технологій

Щоб захиститися від цієї гібридної моделі, організації повинні:

- Покращення виявлення загроз на всіх рівнях зв'язку (електронна пошта, телефон, текстові повідомлення, інструменти для співпраці).
- Інтегруйте поведінковий моніторинг у системи контролю доступу.
- Проводити навчання з реагування на соціально-інженерні проблеми в рамках ширшого планування реагування на інциденти.

Злиття штучного інтелекту та соціальної інженерії створює нову категорію загроз, яку неможливо нейтралізувати лише брандмауерами.

Різке зростання порушень ланцюга поставок програмного забезпечення

У 2026 році область атак значно розширилася через зростання взаємозв'язку між сторонніми постачальниками, конвеєрами розробки та публічними хмарними сервісами. Атаки на ланцюги поставок програмного забезпечення зараз є однією з найшвидше зростаючих категорій кіберзагроз, і вони більше не обмежуються лише великими постачальниками. Кожна

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		33

організація, незалежно від розміру, тепер є потенційною точкою входу для чужого порушення.

Згідно з даними розвідки загроз Cyble за 2025 рік, у жовтні 2025 року було зафіксовано 32% зростання кількості порушень, пов'язаних з ланцюгом поставок, що перевищує всі попередні показники. Завдяки впровадженню пакетів з відкритим кодом та автоматизованих інструментів розгортання, таких як CI/CD, навіть один скомпрометований компонент може поширювати шкідливе програмне забезпечення або бекдори в тисячах середовищ, що використовуються в дальньому розвитку подій.

Як працюють сучасні атаки на ланцюги поставок

Зловмисники проникають у ланцюги постачання програмного забезпечення шляхом:

- впровадження шкідливого коду в бібліотеки з відкритим кодом;
- компрометація облікових даних довіреного постачальника;
- використання інструментів безперервної інтеграції для розгортання оновлень шкідливих програм;
- використання неправильних конфігурацій третіх сторін у спільних хмарних середовищах.

Ці методи дозволяють отримати непомітний, постійний доступ до організацій, які можуть ніколи безпосередньо не взаємодіяти зі зловмисником.

Управління ризиками постачальників тепер є критично важливим для безпеки

Сучасне управління ризиками постачальників (VRM) зараз є стратегічним імперативом. Організації повинні:

- проводити належну перевірку всіх сторонніх постачальників програмного забезпечення;
- вимагають дотримання таких стандартів, як ISO 27001 та NIST Cybersecurity Framework;
- угоди про рівень обслуговування (SLA) щодо повідомлення про

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		34

порушення мандата та звіти про тестування на проникнення;

- сегментувати зовнішні сервісні середовища за допомогою архітектури Zero Trust.

Оскільки регуляторний тиск навколо GDPR, HIPAA та законів про захист фінансових даних посилюється, компанії, які не перевіряють свої цифрові ланцюги поставок, стикаються зі значними штрафами у разі витоку даних.

Стратегії забезпечення безпеки ланцюга поставок програмного забезпечення

Найкращі практики для зниження ризиків у ланцюжку поставок у 2026 році включають:

- прийняття специфікацій матеріалів програмного забезпечення (SBOM) для забезпечення прозорості
- інтеграція інструментів управління інформацією та подіями безпеки (SIEM) зі сторонньою телеметрією
- проведення постійного моніторингу репозиторіїв коду
- використання самозахисту програм під час виконання (RASP) для виробничих систем

Команди безпеки повинні розглядати видимість ланцюга поставок як динамічний процес, а не як одноразовий контрольний список.

3.2 Розробка структурної схеми

Ландшафт кібербезпеки досягає переломного моменту. Кіберзагрози у 2026 році визначаються загрозами, що керуються штучним інтелектом, дедалі складнішими зловмисниками та розширенням поверхонь атак у хмарних системах, ідентифікаційних системах, операційних технологіях та критично важливій інфраструктурі. Організації повинні вийти за рамки статичних засобів захисту та впровадити адаптивні програми безпеки, що враховують системні ризики в цифрову епоху.

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		35

Зіткнувшись із цим мінливим ландшафтом загроз, стратегії запобігання повинні зміститися в бік операцій безпеки, заснованих на аналітичних даних, які інтегрують управління ризиками, видимість активів, безпеку ідентифікаційних даних та зрілі плани реагування на інциденти. Керівники з безпеки повинні узгоджувати кібербезпеку з корпоративною стратегією, регуляторним тиском та підзвітністю керівництва, одночасно захищаючи конфіденційні дані та підтримуючи операційну ефективність.

Багаторівневе виявлення загроз по всьому стеку

Сучасні кіберзагрози більше не спрямовані на окремі системи. Вектори атак охоплюють хмарні робочі навантаження, мобільні кінцеві точки, автономні системи, операційні технології, сховища коду та інтеграції ланцюгів поставок. Зловмисники все частіше використовують вразливості в кількох середовищах, щоб спровокувати витік даних, крадіжку облікових даних та витік конфіденційних даних.

Ефективне багаторівневе виявлення тепер включає хмарні інструменти безпеки, мобільні кінцеві точки та віддалених працівників, інтеграцію сторонніх розробників та ланцюгів поставок, вбудовані системи, середовища Інтернету речей та ОТ, що підтримують критичну інфраструктуру.

Спільне впровадження платформ SIEM, NDR та SOAR дозволяє проводити поведінкову аналітику, постійний моніторинг та автоматизоване стримування шкідливого коду та підозрілої активності. Ці заходи безпеки дозволяють командам безпеки виявляти несанкціоноване переміщення, внутрішні загрози, кампанії соціальної інженерії та спроби обійти багатофакторну автентифікацію, перш ніж атаки переростуть у численні інциденти.

Квантово-усвідомлене планування та довгострокова цілісність даних

Зі зростанням технологічного прогресу прогнози щодо кібербезпеки вказують на довгострокові ризики, пов'язані з квантовими обчисленнями та новими технологіями. Організації, що зберігають конфіденційну інформацію або

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		36

регульовані дані, повинні враховувати криптографічну стійкість як частину довгострокового планування кіберризиків.

Архітектори безпеки повинні оцінювати криптографічну гнучкість та готовність протоколу контексту моделювання, щоб забезпечити можливість ротації алгоритмів у міру розвитку загроз. Підготовка сьогодні допомагає зменшити ризики, пов'язані з майбутніми крадіжками даних, витоком конфіденційних даних та компрометацією ідентифікаційних даних машин, які можуть вплинути як на великі підприємства, так і на системи державного сектору.

Безпека з нульовою довірою стає стандартом

Нульова довіра більше не є необов'язковою у сфері кібербезпеки. У 2026 році принципи нульової довіри стають вбудованими в структури управління, регуляторні вимоги та програми безпеки, орієнтовані на ідентифікацію.

Основні практики нульової довіри включають мікросегментацію мереж та робочих навантажень, контекстне управління доступом із прийняттям рішень у режимі реального часу, постійну перевірку ідентифікаційних даних користувачів та машин, а також моніторинг ескалації привілеїв та аномальної поведінки.

За умови правильного впровадження, нульова довіра зменшує кількість точок відмови, обмежує радіус вибуху атак та посилює захист від крадіжки облікових даних, витоку даних та методів вторгнення на основі штучного інтелекту.

Зміцнення людського та організаційного рівнів

Навіть попри те, що штучний інтелект та автономні агенти штучного інтелекту змінюють інструменти безпеки, прийняття рішень людиною залишається критично важливим. Команди безпеки повинні бути готові відповідально керувати впровадженням штучного інтелекту, одночасно борючись із внутрішніми загрозами, операційним стресом та відповідальністю керівництва.

У 2026 році стійкі організації зосереджуються на міжфункціональних навчальних заходах, навчанні протидії генеративному штучному інтелекту,

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		37

спрямованому на соціальну інженерію та атаки, що видаються за іншу особу, ініціативах щодо покращення безпеки для зменшення вигорання, а також на співпраці між IT-відділом, юридичним відділом, відділом відповідності та керівництвом.

Безпека більше не є центром витрат. Це стратегічна функція, яка захищає довіру, репутацію та довгострокову стійкість бізнесу.

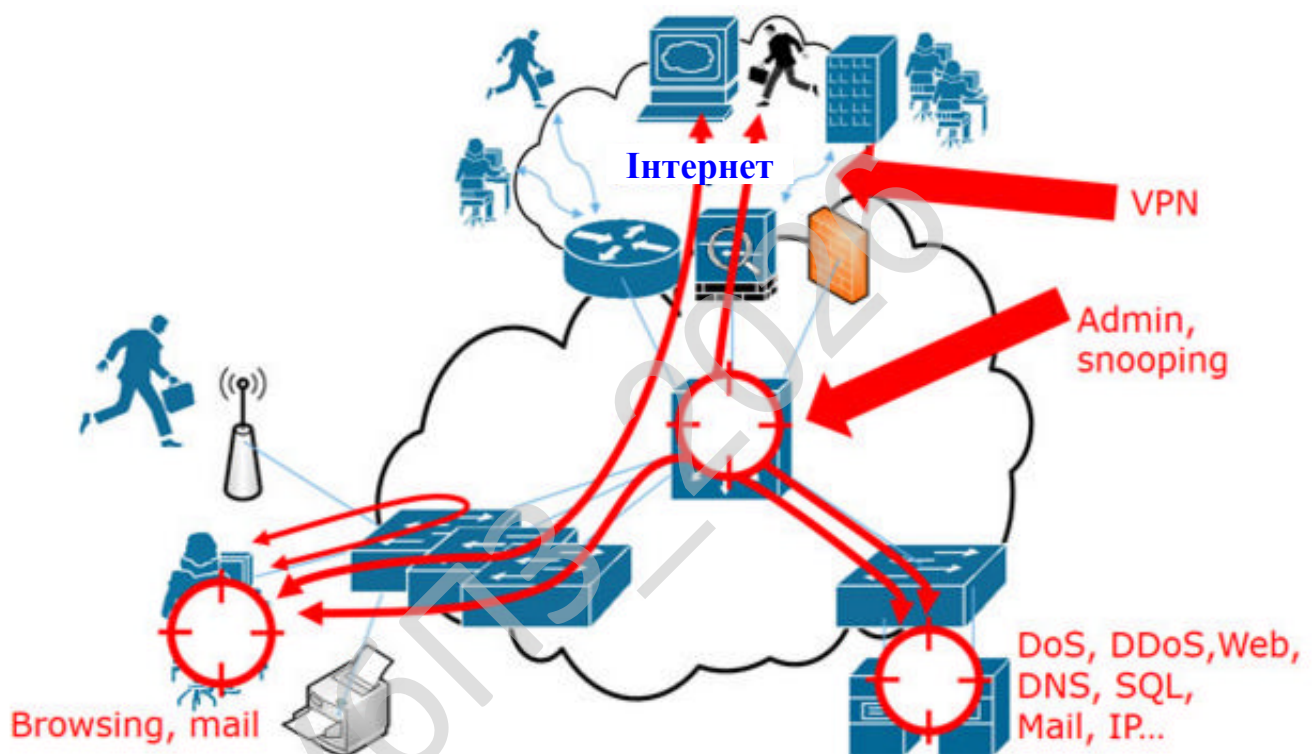


Рисунок 3.1 – Структурна схема системи

3.3 Розробка функціональної схеми

Наскільки важлива будь-яка інформація, що ставиться до бізнесу зрозуміло багатьом. Користуючись зібраною й обробленою інформацією, можна успішно конкурувати на своєму ринку й захоплювати нові. Інформація допомагає в пошуку партнерів і сприяє чіткому визначенню позиції стосовно них.

Говорячи простіше: хто володіє достовірною й повною інформацією – той володіє ситуацією, а хто володіє ситуацією – той здатний управляти нею у своїх інтересах, а хто здатний управляти – той здатний перемогати. От проста формула успіху будь-якої діяльності.

Крім того, при переході до ринкової економіки інформація стає товаром і повинна тому підкорятися специфічним законам товарно-ринкових відносин. У цих умовах проблема захисту інформації досить актуальна й для організацій будь-якої форми власності.

Питання безпеки – важлива частина концепції впровадження нових інформаційних технологій в усі сфери життя суспільства. Широкомасштабне використання обчислювальної техніки й телекомунікаційних систем у рамках територіально-розподіленої мережі, перехід на цій основі до безпаперової технології, збільшення обсягів оброблюваної інформації й розширення кола користувачів приводять до якісно нових можливостей несанкціонованого доступу до ресурсів і даних інформаційної системи, до їхньої високої уразливості.

Немає необхідності пояснювати, що цілісність, вірогідність і доступність інформації – важливі складені успіху діяльності будь-якої організації. Під інформацією можна розуміти: і Ваші конфіденціальні дані на папері, що перебувають у кабінеті на столі або в сейфі; і цифрові дані, збережені в комп'ютері, записані на дискеті або передані по каналах зв'язки; і Ваші розмови по телефоні або просто в приміщенні. Доступ у приміщення теж є доступом до Вашої інформації. Як інформація можуть виступати й Ваші гроші, коштовності, цінні папери. Навіть Ви самі є об'єктом інформації, іноді найціннішої. І все це необхідно захищати. Захищати комплексно.

Ефективність механізмів захисту інформації в значній мірі залежить від реалізації ряду принципів. По-перше, механізми захисту варто проектувати одночасно з розробкою інформаційної системи, що дозволяє забезпечити їхню безконфліктність, своєчасну інтеграцію в обчислювальне середовище й

скорочення витрат. По-друге, питання захисту варто розглядати комплексно в рамках єдиної системи захисту інформації (СЗІ).

Системний підхід забезпечує адекватний багаторівневий захист інформації, розглянуту як комплекс організаційно-правових і технічних заходів. Крім того, при реалізації механізмів захисту повинні використовуватися передові, науково обґрунтовані технології захисту, що забезпечують необхідний рівень безпеки, прийнятність для користувачів і можливість нарощування й модифікації СЗІ надалі.

Керування безпекою електронних документів охоплює широке коло питань, у число яких входить: забезпечення цілісності, конфіденційності й автентичності інформації; розмежування прав користувачів за доступом до ресурсів автоматизованої системи; захист автоматизованої системи і її елементів від несанкціонованого доступу; забезпечення юридичної значимості електронних документів.

До інформації, що вимагає захисту, можна віднести конфіденційну, управлінську, науково-технічну, торговельну й іншу інформацію, що представляє цінність для підприємства в досягненні переваги над конкурентами. Витік такої інформації може завдати шкоди її власникам у вигляді прямих збитків і інших недоглядів.

Інформація, як сукупність знань про фактичні дані й залежності між ними, стала стратегічним ресурсом; вона – основа для вироблення будь-якого рішення. Тому захист інформації, будучи складною, наукомісткою й багатогранною проблемою по суті, в умовах впровадження сучасних інформаційних технологій, створення розподілених обчислювальних систем і мереж зв'язку, здобуває особливу гостроту.

Існує думка, що комп'ютерні бази персональних даних створюють реальну погрозу для негласного вторгнення в приватне життя. Така заклопотаність має під собою ґрунт, оскільки різні файли даних заводяться на кожного громадянина й ведуться протягом всього його життя. Результати медичних обстежень;

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		40

проходження навчання в коледжі й вузах; арешти й приводи в поліцію; суми, узяті під заставу; купівля-продаж товарів і майна; списки книг, узятих у бібліотеці; членство або підтримка суспільно-політичних, релігійних і інших організацій – от далеко не повний перелік відомостей, які осідають у банках даних різних організацій, служб і відомств. Вся ця інформація, потрапивши в чужі руки, у певних умовах може бути використана не по призначенню.

Не секрет, що в цей час одним з основних засобів забезпечення державою, фірмою або іншою організацією своїх інтересів на міжнародній арені стає завоювання їм інформаційного простору шляхом розвитку інформаційних технологій і створення на їхній основі інформаційних систем (ІС), що визначають доступ до досягнень у різних галузях науки, техніки, економіки й т.д. Причому інформаційні системи більше високого рівня розвитку, як правило, одержують можливість управляти системами з відносно низьким рівнем інформатизації, направляючи їхню діяльність у своїх інтересах і постійно контролюючи.

В ІС, створюваних в органах державної влади й у комерційних структурах циркулює інформація, що містить секретні відомості про досягнутий потенціал у галузі економіки, оборони, науки й техніки, конфіденційні відомості про управлінській, господарській, комерційній, фінансовій і іншій діяльності. Технічними засобами освоєння інформаційних ресурсів виступають обчислювальні системи з їх різноманітним периферійним устаткуванням і мережі зв'язку.

Кількість абонентів, що користуються послугами таких систем неухильно зростає. Стало можливим взаємне сполучення локальних мереж при обміні інформацією. Такі взаємозалежні мережі з підключений ними до них віддаленими абонентськими термінальними пристроями утворюють складні інформаційно-обчислювальні мережі, розподілені на великій території. Очевидно, що в цих системах виключити несанкціонований доступ до інформації лише організаційними мірами практично неможливо.

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		41

Сучасні обчислювальні системи можуть працювати в мультипрограмному режимі (одночасно вирішується кілька завдань), у мультипроцесорному режимі (створюються умови для рішення програми завдання декількома паралельно працюючими процесорами), а також у режимі поділу часу, коли до інформаційних ресурсів одночасно може звертатися велика кількість абонентів. При таких режимах роботи в пам'яті комп'ютерів одночасно можуть зберігатися програми й масиви даних різних користувачів, із ПК або серверами одночасно буде підтримувати зв'язок значне число абонентів. У цьому випадку необхідне рішення як проблем фізичного захисту інформації, так і захист її від користувачів несанкціоновано вклинюються в обчислювальний процес.

У той же час, що циркулює в територіально розподілених системах і мережах інформація стає уразливою у зв'язку зі зростанням різноманіття погроз несанкціонованого її одержання й використання.

З розвитком ринкових відносин, з появою приватних підприємств і перебудовою суспільства в цілому перед підприємцем виникли зовсім нові проблеми, зв'язані не тільки із забезпеченням особистої безпеки, але й з безпекою інформації. Тим більше, що немає чіткої границі між інформацією, доступної всім і комерційною таємницею.

Для забезпечення інформаційної безпеки необхідно по-перше, зрозуміти, наскільки важлива дана проблема, а по-друге, виділити основні напрямки й способи її рішення. Необхідно пам'ятати, що під захистом інформації розуміють захист не тільки комп'ютерної інформації, але й безліч інших аспектів, наприклад: бухгалтерську звітність фірми, кількість грошей на рахунках, ділові партнери й постачальники, реальні обороти фірми, проведення переговорів і містяться контракти, що, і багато чого іншого.

А якщо подивитися на цю проблему не з комерційної, а з державної точки зору, то стає очевидним, що жодна сфера життя сучасного суспільства не може функціонувати без розвитий інформаційної структури. Національний

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		42

інформаційний ресурс стає сьогодні однієї з головних основ економічної й військової потужності будь-якої держави.

Інформація, що проникає в усі сфери діяльності держави, здобуває конкретні політичні, матеріальне й вартісне вираження. Проблема безпеки інформації з погляду державних інтересів останнім часом придбала особливу актуальність і розглядається як одне із пріоритетних державних завдань, як важливий елемент національної безпеки.

Найважливіший ресурс сучасного суспільства – інформація одночасно несе в собі й величезній погрози для нього, пов'язану із внутрішньою специфікою цього ресурсу. Простота й велика кількість різних способів доступу й модифікації інформації, значна кількість кваліфікованих фахівців, широке використання в суспільному виробництві спеціальних технічних засобів дозволяють зловмисникові практично в будь-який момент і в будь-якому місці здійснювати дії, що представляють погрозу інформаційній безпеці як у локальному, так і в глобальному масштабах.

Поширення, що відбувається останнім часом, децентралізації й розподіленої обробки даних висунуло проблеми забезпечення безпеки інформації в число найважливіших для національної економіки. Рішення проблеми забезпечення інформаційної безпеки припускає комплекс заходів і в першу чергу такі дії держави, як розробка системи класифікації й документування інформації й способів захисту, регулювання способів доступу до даних і встановлення відповідальності за порушення інформаційної безпеки.

Гостра актуальність названої проблеми обумовлена також рядом об'єктивних факторів, що грають істотну роль у житті сучасного суспільства. Серед цих факторів особливо варто виділити: неухильне підвищення ролі інформації в забезпеченні життєдіяльності суспільства й держави, всі інтенсифікація, що підсилюється, процесів інформатизації різних сфер діяльності, що здобуває стійкість тенденція органічного злиття традиційних (паперових) і автоматизованих (безпаперових) технологій обробки інформації, різка

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		43

децентралізація використання сучасних засобів електронно-обчислювальної техніки й ін.

При загальному позитивному впливі, об'єктивній доцільності й неминучості перераховані обставини породжують і ряд негативних явищ, одне із яких полягає в різкому підвищенні уразливості що накопичується, збереженої й оброблюваної інформації. Причому зазначені явища можуть носити як випадковий, так і навмисний характер, у тому числі протиправні злочинні, диверсійні й інші дії

Вся зазначена сукупність характерних для інформаційних процесів умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства й держави (що виступає як власників, власників або користувачів інформації) розуміється як погрози безпеки інформації.

Широкомасштабне використання обчислювальної техніки й телекомунікаційних систем у рамках територіально розподіленої мережі, перехід на цій основі до безпаперової технології, збільшення обсягів оброблюваної інформації, розширення кола користувачів приводять до якісно нових можливостей несанкціонованого доступу до ресурсів і даних інформаційних систем, до їхньої високої уразливості.

Керування безпекою електронних документів охоплює широке коло питань, у число яких входить: забезпечення цілісності, конфіденційності й автентичності інформації, розмежування прав користувачів за доступом до ресурсів автоматизованої системи, захист автоматизованої системи і її елементів від несанкціонованого доступу, забезпечення юридичної значимості електронних документів.

Прогрес в області розвитку інформаційних технологій стимулював розвиток засобів забезпечення безпеки, що зажадало перегляду існуючих підходів до проблем створення систем захисту інформації.

У пропонованій книзі автор намагається відповісти на цілий ряд питань, пов'язаних із забезпеченням інформаційної безпеки, а також прагне сформулювати

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		44

цілісне подання про шляхи створення захищених інформаційних систем. Існуючі публікації на цю тему в основному обмежуються перерахуванням погроз і можливостей конкретних засобів захисту інформації. У книзі представлений повний спектр питань про практичне створення захищених інформаційних систем.

Побудова таких систем не обмежується вибором тих або інших апаратних і програмних засобів захисту. Необхідно володіти певними теоретичними знаннями й практичними навичками. Для цього необхідно, по-перше, зрозуміти, що являє собою захищена система, які до неї пред'являються вимоги, розглянути існуючий досвід створення подібних систем і причини порушення їхньої безпеки й, по-друге, визначити, які функції захисту і яким образом повинні бути реалізовані, і як вони протидіють погрозам і усувають причини порушення безпеки. Зрозуміло, дана публікація не претендує на остаточний дозвіл всіх проблем інформаційної безпеки, але, як сподівається її автор, прояснить ряд питань із цієї області знань і дозволить вирішити багато практичних завдань.

У пропонованих матеріалах в узагальненому виді викладені причини порушення безпеки комп'ютерних систем, наведений перелік моделей безпеки, адекватних сучасному рівню розвитку програмних і апаратних засобів, а також розглянуті методи й засоби впровадження механізмів захисту в існуючі системи з можливістю гнучкого керування безпекою залежно від висунутих вимог, припустимого ризику й оптимальної витрати ресурсів.

Як відомо, для того щоб вирішити проблему треба бути вище її й небагато остронь.

Великий обсяг наявних публікацій навряд чи може сформувати чітке подання про тім як же приступитися до створення комплексної системи захисту інформації для конкретних інформаційних систем, з обліком властивих їм особливостей і умов функціонування.

Отже спробуємо глянути на проблему зверху й охопити всі її аспекти.

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		45

Відомо, що основною або складовою частинами практично будь-якої системи (у тому числі й системи захисту інформації) є:

- Нормативно-правова й наукова база.
- Структура й завдання органів.
- Організаційні міри й методи.
- Програмно-технічні способи й засоби.

Представимо основи у вигляді куба, усередині якого й перебувають всі питання захисту інформації.

Далі, керуючись принципом «розділяй і пануй», виділимо основні напрямки в загальній проблемі забезпечення безпеки інформаційних технологій (вони представлені нижче).

Нагадаємо їх:

- Захист об'єктів інформаційних систем.
- Захист процесів, процедур і програм обробки інформації.
- Захист каналів зв'язку.
- Придушення побічних електромагнітних випромінювань.
- Керування системою захисту.

Але оскільки кожне із цих напрямків базується на перераховані вище основах, то грані куба становлять основи й напрямки нерозривно зв'язані один з одним.

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		46

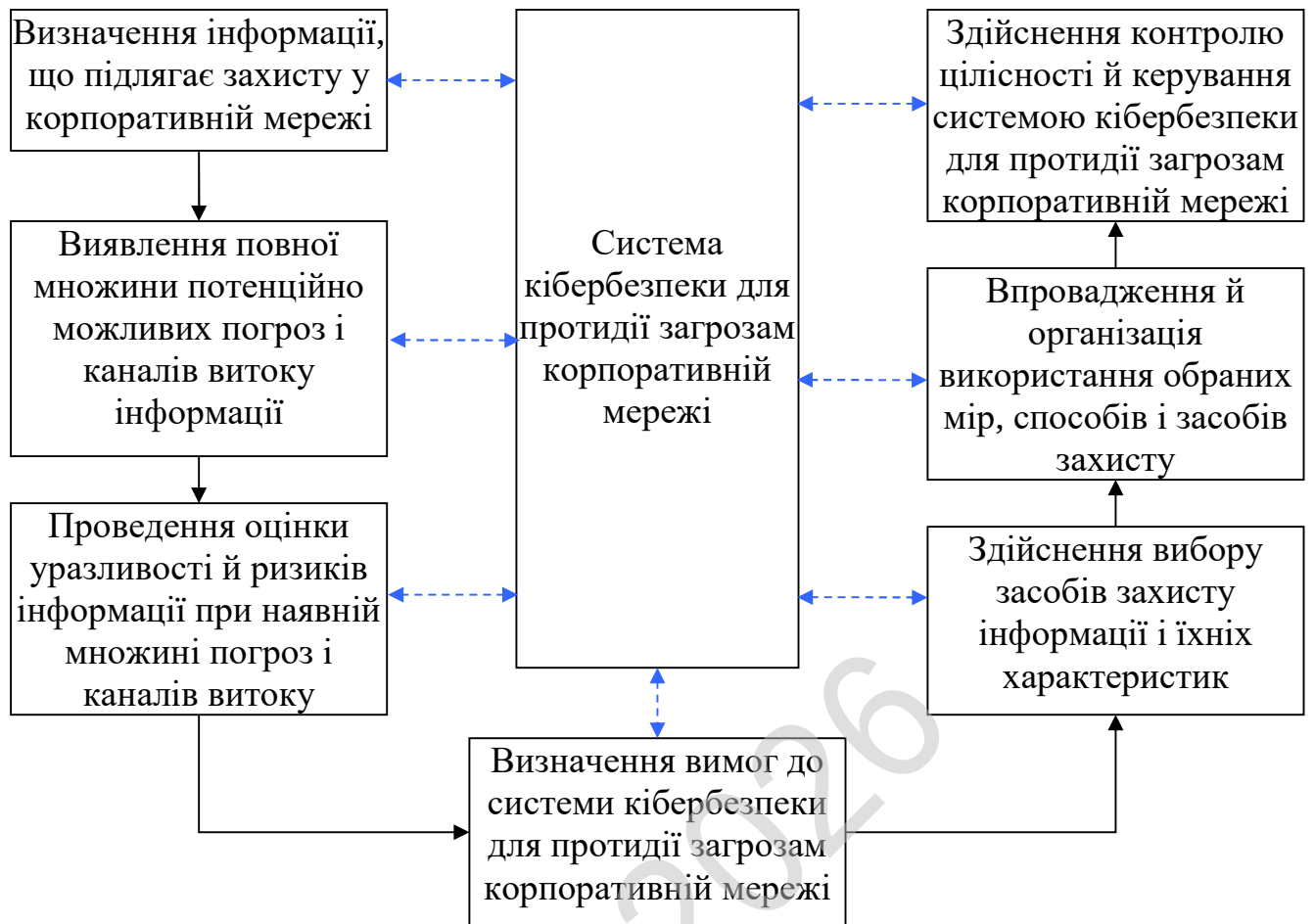


Рисунок 3.2 – Функціональна схема системи

Запропоновано методику (послідовність кроків) побудови СЗІ, що рівною мірою застосовна для всіх напрямків і припускає наступний послідовність дій:

- Визначення інформації, що підлягає захисту у корпоративній мережі.
- Виявлення повної множини потенційно можливих погроз і каналів витоку інформації.
- Проведення оцінки уразливості й ризиків інформації при наявній множині погроз і каналів витоку.
- Визначення вимог до системи кібербезпеки для протидії загрозам корпоративній мережі.
- Здійснення вибору засобів захисту інформації і їхніх характеристик.

– Впровадження й організація використання обраних мір, способів і засобів захисту.

– Здійснення контролю цілісності й керування системою кібербезпеки для протидії загрозам корпоративній мережі.

Зазначена послідовність дій здійснюється безупинно по замкнутому циклі, із проведенням відповідного аналізу стану СЗІ й уточненням вимог до неї після кожного кроку.

3.4 Розробка діаграми процесів

Розглянемо розроблену діаграму процесів яка зображена на рисунку 3.3. Основна будова діаграми процесів полягає у графічному представленні складу сукупностей даних, що характеризуються як співвідношення різних частин кожної з сукупностей.

Склад статистичної сукупності графічно може бути представлений як за допомогою абсолютних, так і відносних показників.

Графічне зображення складу сукупності по абсолютними і відносними показниками сприяє проведенню більш глибокого аналізу і дозволяє проводити аналіз системи.

Діаграма взаємодії процесів використовується для візуалізації процесів обробки даних (структурне проектування).

Для розробника вважається звичним спочатку креслити діаграму взаємодії процесів даних рівня контексту, завдяки чому буде показано взаємодію системи.

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

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

Діаграми потоків даних містять чотири типи елементів:

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

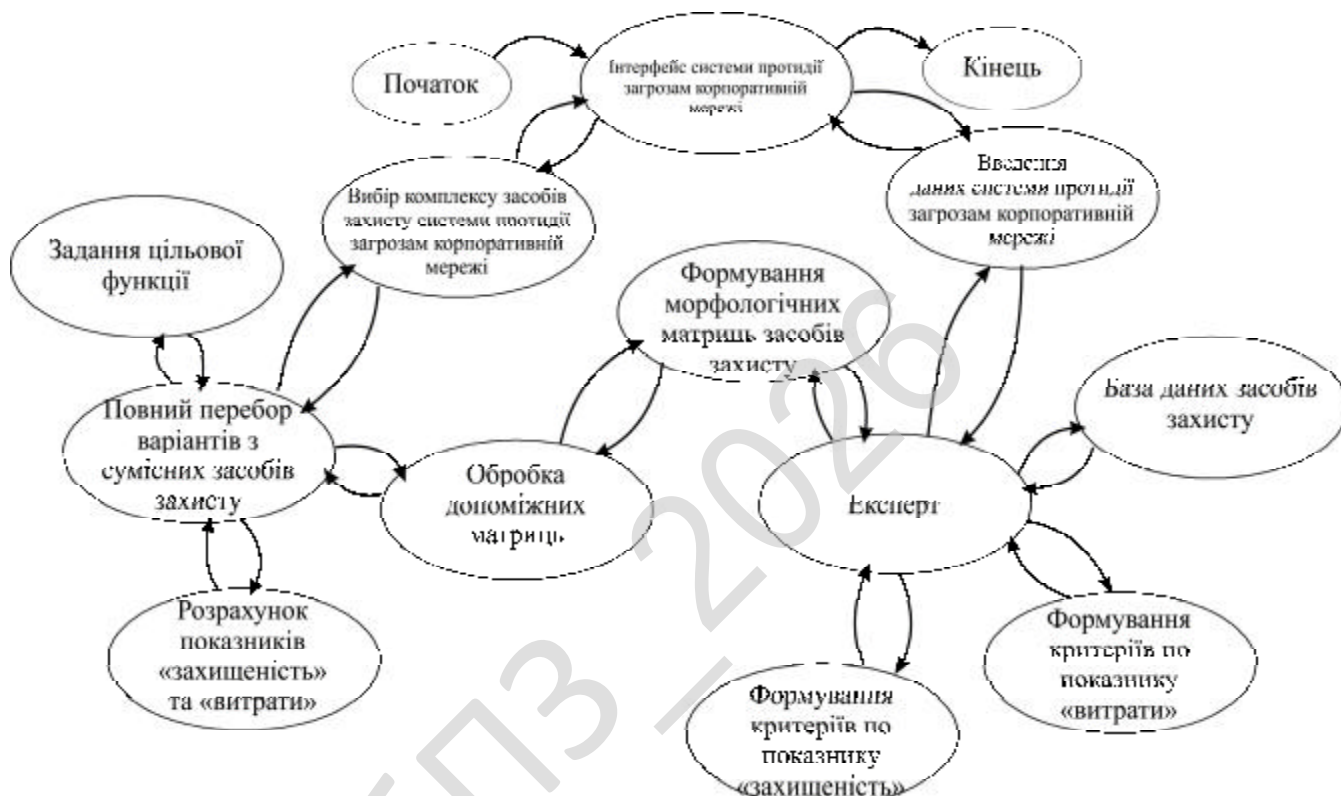


Рисунок 3.3 – Діаграма взаємодії процесів

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

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

4.1 Блок-схеми та опис алгоритмів функціонування системи

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

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

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.

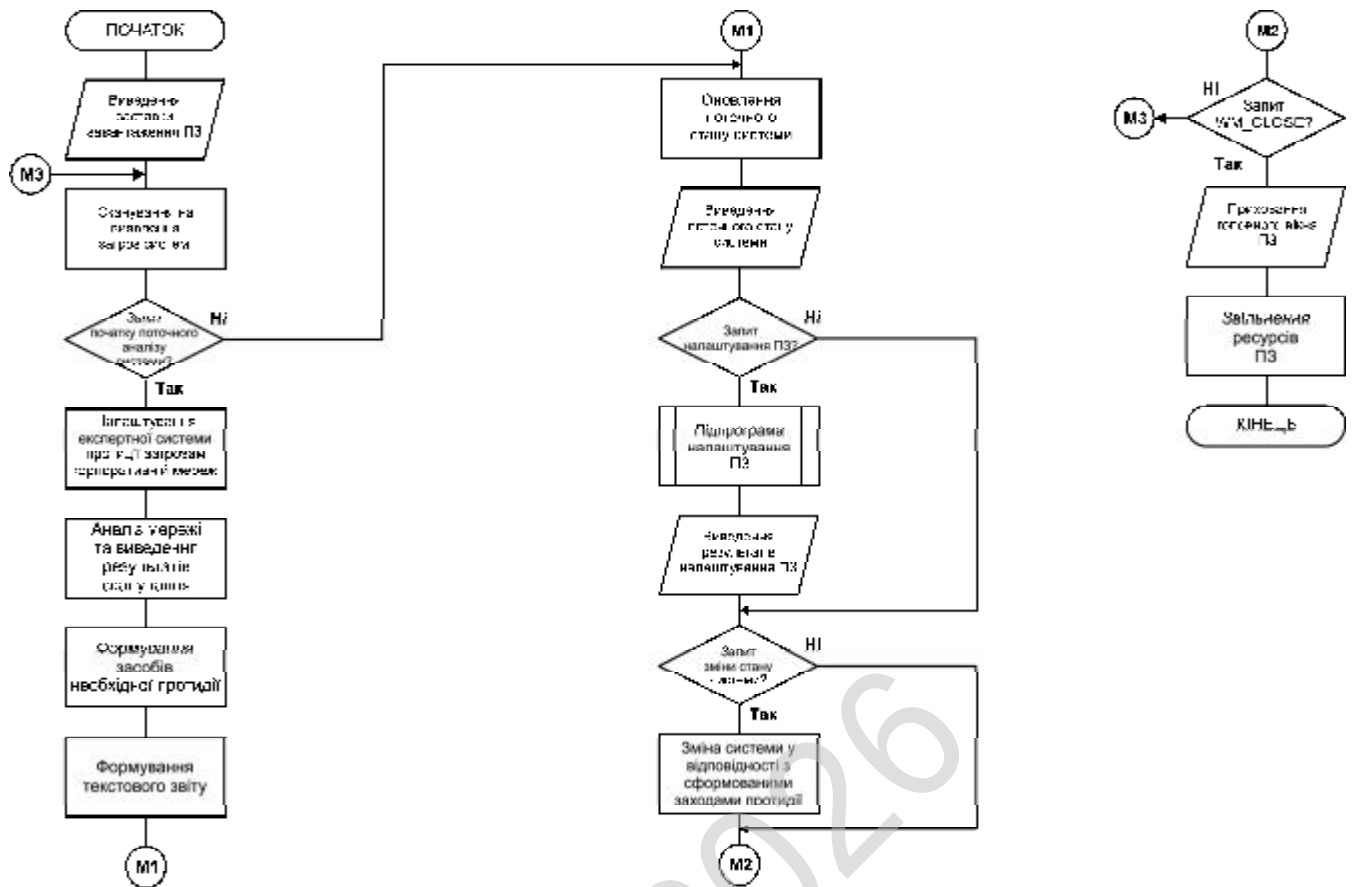


Рисунок 4.1 – Блок-схема основної програми

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.

Архітектура клієнт-сервер є одним із архітектурних шаблонів програмного забезпечення та є домінуючою концепцією у створенні розподілених мережних програм і передбачає взаємодію та обмін даними між ними. Вона передбачає такі основні компоненти:

- набір серверів, які надають інформацію або інші послуги програмам, які звертаються до них;
- набір клієнтів, які використовують сервіси, що надаються серверами;
- мережа, яка забезпечує взаємодію між клієнтами та серверами.

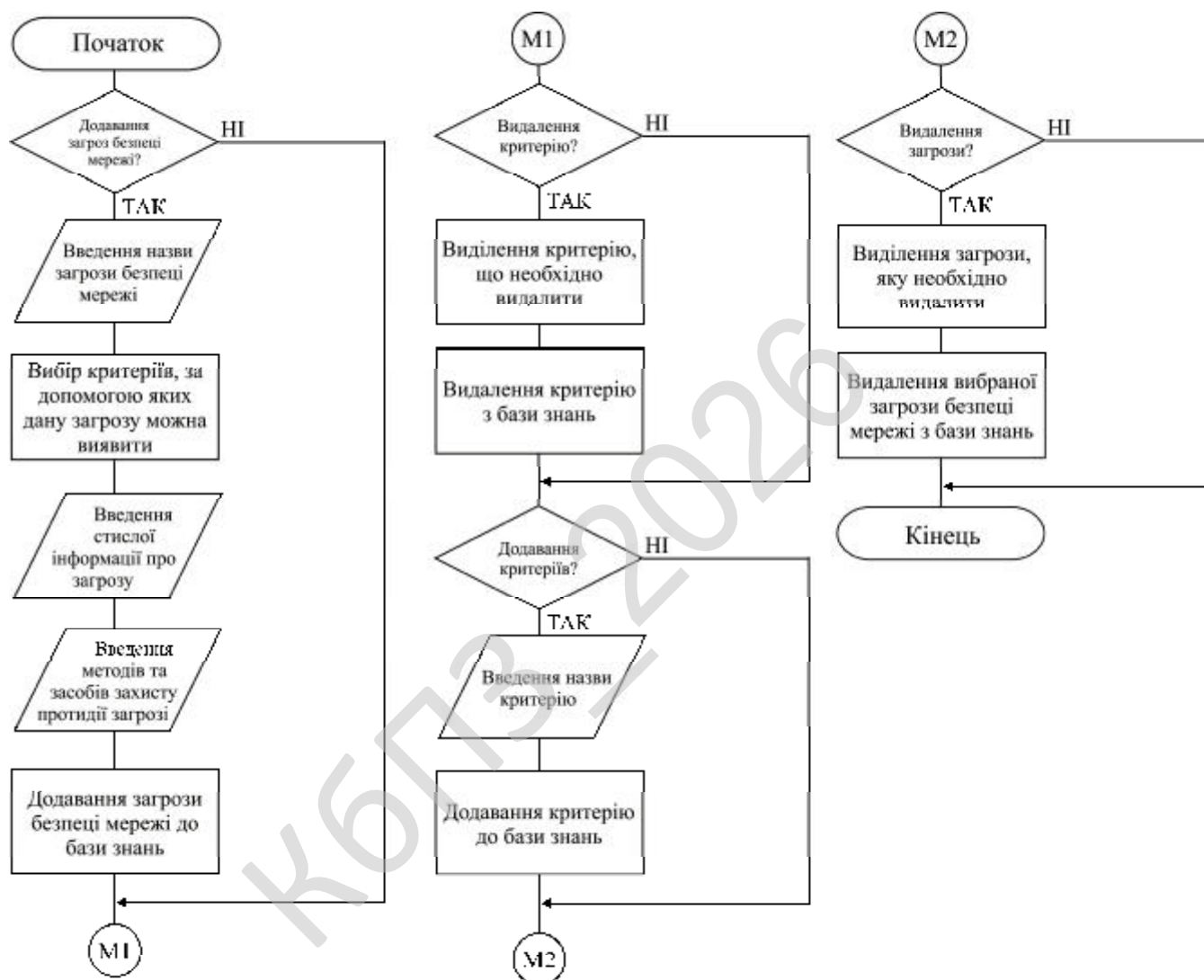


Рисунок 4.2 – Блок-схема роботи підпрограми

Сервери є незалежними один від одного. Клієнти також функціонують паралельно і незалежно один від одного. Немає жорсткої прив'язки клієнтів до серверів. Більш ніж типовою є ситуація, коли один сервер одночасно обробляє запити від різних клієнтів; з іншого боку, клієнт може звертатися то до одного

сервера, то до іншого. Клієнти мають знати про доступні сервери, але можуть не мати жодного уявлення про існування інших клієнтів.

Дуже важливо ясно уявляти, хто або що розглядається як «клієнт». Можна говорити про клієнтський комп'ютер, з якого відбувається звернення до інших комп'ютерів. Можна говорити про клієнтське та серверне програмне забезпечення. Нарешті, можна говорити про людей, які бажають за допомогою відповідного програмного та апаратного забезпечення отримати доступ до тієї чи іншої інформації.

Загальноприйнятим є положення, що клієнти та сервери – це перш за все програмні модулі. Найчастіше вони знаходяться на різних комп'ютерах, але бувають ситуації, коли обидві програми – і клієнтська, і серверна, фізично розміщуються на одній машині; в такій ситуації сервер часто називається локальним.

Модель клієнт-серверної взаємодії визначається перш за все розподілом обов'язків між клієнтом та сервером. Логічно можна відокремити три рівні операцій:

- рівень представлення даних, який по суті являє собою інтерфейс користувача і відповідає за представлення даних користувачеві і введення від нього керуючих команд;
- прикладний рівень, який реалізує основну логіку ПЗ і на якому здійснюється необхідна обробка інформації;
- рівень управління даними, який забезпечує зберігання даних та доступ до них.

Дворівнева клієнт-серверна архітектура передбачає взаємодію двох програмних модулів – клієнтського та серверного. В залежності від того, як між ними розподіляються наведені вище функції, розрізняють:

- модель тонкого клієнта, в рамках якої вся логіка ПЗ та управління даними зосереджена на сервері. Клієнтська програма забезпечує тільки функції рівня представлення;

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		54

– модель товстого клієнта, в якій сервер тільки керує даними, а обробка інформації та інтерфейс користувача зосереджені на стороні клієнта. Товстими клієнтами часто також називають пристрої з обмеженою потужністю: кишенькові комп'ютери, мобільні телефони та ін.

Типовим прикладом клієнт-серверної взаємодії є WWW. Існує величезна кількість веб-серверів, на яких розміщується та чи інша інформація. У найпростішому випадку ця інформація являє собою набір веб-сторінок, які можуть зберігатися на сервері у вигляді файлів, розмічених за допомогою мови розмітки HTML. Але ситуація, як правило, є складнішою; значна частина веб-ресурсів на сучасному етапі є динамічними, тобто вони не існують в заздалегідь підготовленому вигляді, а створюються безпосередньо в процесі обробки запиту від користувача.

Для того, щоб людина, яка працює в Інтернеті, могла переглянути ту чи іншу сторінку, на її комп'ютері повинно бути встановлено відповідне програмне забезпечення. Програми для перегляду веб-сторінок називаються браузером.

Але, крім браузерів, до серверів можуть звертатися і інші клієнти, а саме – автономні програми. Вони можуть передбачати взаємодію з людиною, а можуть працювати в цілком автоматичному режимі. Типовим класом таких програм є роботи, призначені для автоматичного перегляду веб-ресурсів. Зокрема, роботи є важливим елементом пошукових систем і використовуються ними для перегляду сторінок і збору інформації про них.

Для запиту до веб-сервера клієнтська програма повинна задати місцезнаходження комп'ютера, на якому розміщується серверна програма, назву потрібного документа і, можливо, інші дані, які специфікують запит. Мережа забезпечує знаходження сервера і передачу йому клієнтського запиту. Серверні програми обробляють цей запит, відповідь пересилається по мережі клієнтові.

Трирівнева клієнт-серверна архітектура, яка почала розвиватися з середини 90-х років, передбачає відділення прикладного рівня від управління даними. Відокремлюється окремий програмний рівень, на якому зосереджується

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		55

прикладна логіка ПЗ. Програми проміжного рівня можуть функціонувати під управлінням спеціальних серверів ПЗ, але запуск таких програм може здійснюватися і під управлінням звичайного веб-сервера. Нарешті, управління даними здійснюється сервером даних.

Для роботи з системою користувач використовує стандартне програмне забезпечення – звичайний браузер. Це позбавляє його необхідності завантажувати та інсталиувати спеціальні програми (хоча інколи така необхідність все-таки виникає).

Але користувачеві слід надати в розпорядженні інтерфейс, який дозволяв би йому взаємодіяти з системою і формувати запити до неї. Форми, що визначають цей інтерфейс, розміщуються на веб-сторінках та завантажуються разом з ними.

Веб-оглядач формує запит та пересилає його до сервера, який здійснює обробку. При необхідності сервер викликає серверні програмні модулі, які забезпечують обробку запиту і в разі потреби звертаються до сервера даних. Сервер даних здійснює операції з даними, що зберігаються в системі та складають її інформаційну основу. Зокрема, він може здійснити вибірку з інформаційної бази відповідно до запиту та передати її модулю проміжного рівня для подальшої обробки. Дані, з якими працює сервер даних, найчастіше організовані як реляційна база даних.

Найчастіше веб-сервер і серверні модулі проміжного рівня розміщуються на одному комп'ютері, хоч і являють собою окремі і логічно незалежні програмні модулі.

На сучасному етапі для програмування модулів проміжного рівня використовується мова серверних сценаріїв PHP, а для управління даними – СУБД MySQL. Таким чином, зв'язку PHP-MySQL слід розглядати як стандартний інструмент для створення порівняно простих інтерактивних веб-сайтів та систем електронної комерції; близько 90% комерційних систем сьогодні створюється саме на цій основі. Водночас як засоби управління даними, так і middleware-

засоби можуть бути найрізноманітнішими. Так, для створення серверних програм, крім PHP, широко застосовуються Java, Perl, Python, Delphi.

Взагалі, технології створення розподілених, зокрема веб-програм, стрімко розвиваються. Слід згадати про технології EJB (Enterprise Java Beans), CORBA, а також про .NET – порівняно нову ініціативу компанії Microsoft. Для зберігання даних та їх передачі часто використовується так звана розширювана мова розмітки XML (Extensible Markup Language).

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.

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».

Інтерфейс NetBIOS являє собою типовий інтерфейс взаємодії програм (API) для забезпечення мережових операцій введення-виведення і управління 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

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		57

мережевих 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–дейтаграмма вкладається в NETBIOS–пакет. Інформаційний обмін відбувається в цьому 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).

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		58

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 підходи з використанням UML, це уніфікована мова моделювання, використовується у парадигмі об'єктно-орієнтованого програмування. Є невід'ємною частиною уніфікованого процесу розробки програмного забезпечення. UML є мовою широкого профілю, це відкритий стандарт, що використовує графічні позначення для створення абстрактної моделі системи, називаної UML-моделлю. UML був створений для визначення, візуалізації, проектування й документування в основному програмних систем. UML не є мовою програмування, але в засобах виконання UML-моделей як інтерпретованого коду можлива кодогенерація.

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

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		59

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.

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		60

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

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		62

можна задати і більш складні кратності, наприклад 0..1, 3..4, 6..*, що означає "будь-яке число об'єктів, крім 2 і 5".

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 зафарбованим 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.

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.

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, чий ступені створюють всі цілі від 1 до $Q - 1$. Це означає, що якщо A є примітивним коренем простого числа Q , тоді числа:

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

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.

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		65

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

5 МЕТОДИКА ВПРОВАДЖЕННЯ СИСТЕМИ КІБЕРБЕЗПЕКИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ

На рисунку 5.1 зображено розроблена система кібербезпеки для протидії загрозам корпоративній мережі. З рисунку можна побачити що інтерфейс головного вікна розподілено на наступні функціональні розділи:

- Функціональних кнопок ПЗ.
- Верхнього меню: Файл; Налаштування; Опції; Довідка.
- Розділу обрання групи критерії загрози та її характеристики.
- Розділу виведення результату роботи системи.

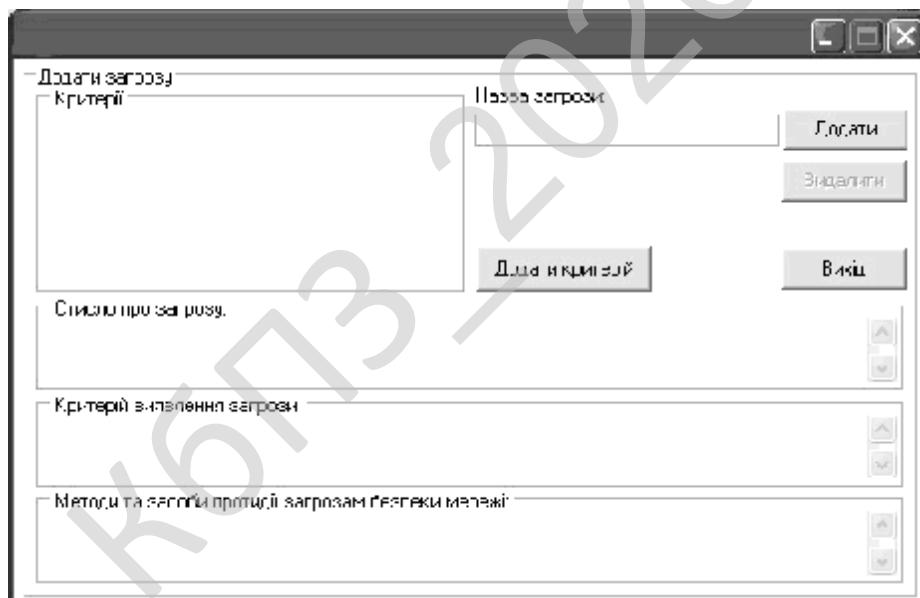


Рисунок 5.1 – Головне вікно ПЗ

Самий елементарний спосіб знизити ризик зараження вірусами – стежити за повідомленнями про нові погрози (розсилання партнерів, офіційні повідомлення компаній і дослідницьких груп і т.п.) і вчасно оновлювати ПЗ.

Ефективним засобом протидії погрозам є сервіс «пісочниці», завдяки якому розроблювачі одержують величезну кількість екземплярів шкідливих

файлів і можуть оперативно надавати інформацію (сигнатури) своїм передплатникам – компаніям, у яких установлені міжмережеві екрани того або іншого вендора.

Це дозволяє максимально швидко в автоматичному режимі блокувати шкідливе ПЗ після його виявлення на глобальному рівні. Сервіс пісочниці може бути реалізований як хмарна послуга або розміщена в інфраструктурі замовника по моделі on-premise.

На рисунку 5.2 зображено авторські дані розробленого програмного забезпечення.

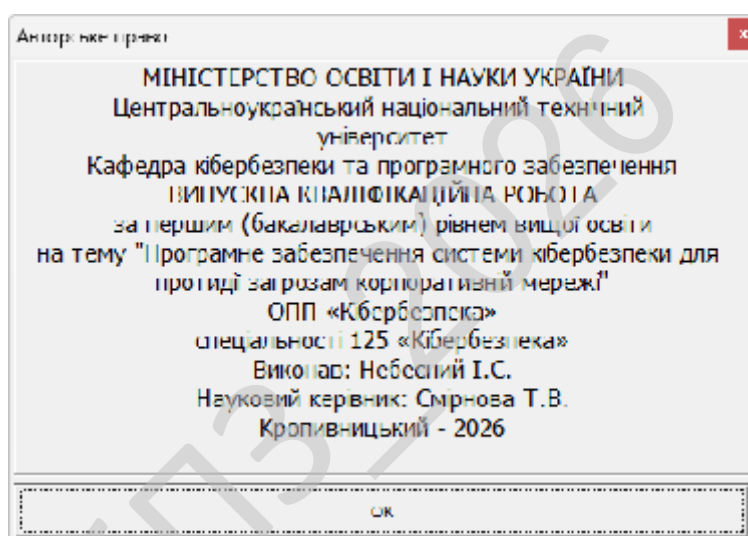


Рисунок 5.2 – Авторське право

Найбільш ефективний спосіб захисту на сучасний момент – реалізувати в компанії комплексний підхід до інформаційної безпеки: установити антивірус (для захисту прикінцевих пристроїв) і міжмережевий екран наступного покоління, а крім того, скористатися можливостями пісочниці. Кожний із цих варіантів окремо – не панацея, але разом вони створюють серйозну смугу перешкод для хакерів.

Розроблена програма має дуже простий і зрозумілий інтерфейс з користувачем. Кожен, хто в достатньому обсязі володіє операційним

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		69

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.

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

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

До діяльностей пов'язаних із розгортанням програмного забезпечення відносять:

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

При впровадженні програмного забезпечення потрібно урахувати наступні дії:

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

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

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

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

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

Проводилась оцінка:

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

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		71

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).

– 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», чию 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-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		73

– 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 – Shareware.

Під умовно-безплатним програмним забезпеченням можна розуміти спосіб або метод розповсюдження комерційного ПЗ на ринку (тобто на шляху до кінцевого користувача), при якому випробувачеві пропонується обмежена за можливостями (не повнофункціональна або демонстраційна версія), терміном дії (тріал версія) або версія з вбудованим набридливим нагадуванням про необхідність оплати використання програми.

В угоді про використання (ліцензії для кінцевого користувача, EULA) також може бути обумовлена заборона на комерційне або професійне (не тестове) її використання.

Основний принцип умовно-безплатного ПЗ – «спробуй, перш ніж купити» (try before you buy). ПЗ що поширюється як умовно-безплатний, надається користувачам безоплатно.

6 ОСНОВНІ ВИСНОВКИ

Програмне забезпечення, створене в результаті виконання випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти, призначено для системи кібербезпеки для протидії загрозам корпоративній 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 протидії загрозам корпоративній мережі.
- Досліджена система для протидії загрозам корпоративній мережі.
- На основі отриманих результатів досліджень створена програмна реалізація системи кібербезпеки для протидії загрозам корпоративній мережі.

Розроблені під час виконання випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання для протидії загрозам корпоративній 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 протидії загрозам корпоративній мережі. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		75

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-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		76

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 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.

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

3. 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

4. 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.

5. 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.

6. 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.

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		77

7. Lakhno, V., Malyukov, V., Smirnov, O., Bebeshko, 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.

8. 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.

9. 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.

10. 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.

11. 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.

12. 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.

13. 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.

14. Батрак О., Смірнова Т., Гнатюк В., Одарченко Р., Смірнов О. «Дослідження показників ефективності функціонування та перспектив розвитку систем IP-телефонії». *Підводні технології*, 2024, № 13, с. 28-35.
15. 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.
16. Akhalaia, G., Iavich, M., Iashvili, G., Prysiashnyy, D., Smirnova, T. «Secure Encrypted Connection on Georgian Website». *CEUR Workshop Proceedings*, 2023, 3550, pp. 313-320.
17. 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
18. 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.
19. 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.
20. 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.
21. 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.

					ВКРБ-125.26.0037.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		79

22. 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 (ІПШРІТ-2023)»* м.Черкаси 6 грудня 2023 року – Черкаси: ЧДТУ.– 2023. – С.251-252.

23. 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.

24. 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.

25. 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.

26. 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,

27. 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.

28. 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.

29. 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.

30. 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.

31. 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.

32. 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

33. 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.

34. 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.

35. 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.

36. 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.

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

38. 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.

39. 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.

40. 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.

41. 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.

42. 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.

43. 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.

44. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». *2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Ukraine, Kyiv, May 14-18. 2020. P. 172-177.

45. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) *Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies*, vol 48. Springer, Cham. 2021. pp 557-587.

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

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

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

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

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

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

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

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

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

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

56. Smirnov, O., Kuznetsov, A., Stefanovych, O., Gorbenko, Y., Krasnobaev, V., Kuznetsova K. «Information Hiding Using 3D-Printing Technology», *10th IEEE International Conference on Intelligent Data Acquisition and Advanced*

Computing Systems: Technology and Applications, IDAACS 2019; Metz; France; 18-21 September 2019. P.701-706.

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

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

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