

Центральноукраїнський національний технічний університет
Центр заочної та дистанційної освіти
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 комп’ютерної
мережі з використанням Fortinet Security Fabric”

Виконав здобувач вищої освіти
IV курсу, групи КБ-22з
ОПП «Кібербезпека»
спеціальності 125 «Кібербезпека»
_____ Кирилов В.О.
«___» _____ 2026 р.

Керівник проекту
доктор технічних наук, професор
_____ Смірнов О.А.
«___» _____ 2026 р.
Рецензент _____

Центральноукраїнський національний технічний університет
Центр Заочної та дистанційної освіти
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

Кириллову Валерію Олексійовичу

(прізвище, ім'я, по батькові)

1. Тема роботи *Програмне забезпечення системи кібербезпеки комп'ютерної мережі з використанням Fortinet Security Fabric*

2. Керівник роботи *Смірнов Олексій Анатолійович, докт. техн. наук, професор*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу № 135-02 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 комп'ютерної мережі з використанням Fortinet Security Fabric*

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

1. Призначення та область використання.

2. Перегляд аналогічних існуючих систем.

3. Опис і обґрунтування проектних рішень.

4. Етапи програмування системи.

5. Впровадження системи кібербезпеки в промислову експлуатацію.

6. Висновки

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

Структурна схема системи кібербезпеки 1 аркуш

Функціональна схема системи кібербезпеки 1 аркуш

Діаграма процесів 1 аркуш

Блок-схема алгоритму роботи додатку 2 аркуша

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

КАЛЕНДАРНИЙ ПЛАН

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

Дата видачі завдання
« 27 » лютого 2026 р.

Підпис керівника

Смірнов О.А.
(прізвище та ініціали)

Завдання прийнято до виконання
« 27 » лютого 2026 р.

Підпис здобувача

Кириллов В.О.
(прізвище та ініціали)

АНОТАЦІЯ

Кириллов В.О. Програмне забезпечення системи кібербезпеки комп'ютерної мережі з використанням Fortinet Security Fabric. 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 комп'ютерної мережі з використанням Fortinet Security Fabric.

Метою розробки є програмне забезпечення системи кібербезпеки комп'ютерної мережі з використанням Fortinet Security Fabric.

Результат роботи – програмна реалізація системи кібербезпеки комп'ютерної мережі з використанням Fortinet Security Fabric.

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, Fortinet Security Fabric

ABSTRACT

Kyryllov V.O. Software for a computer network cybersecurity system using Fortinet Security Fabric. 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 computer network cybersecurity system using Fortinet Security Fabric.

The purpose of the development is software for a computer network cybersecurity system using Fortinet Security Fabric.

The result of the work is a software implementation of a computer network cybersecurity system using Fortinet Security Fabric.

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 PCs with Windows 10/11.

The program is developed in the Python environment.

Keywords: cybersecurity, Fortinet Security Fabric

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	10
2.1 Огляд існуючих систем, технологій, архітектур та програмних рішень за профілем теми випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти.....	10
2.2 Обґрунтування вибору засобів для побудови системи кібербезпеки та мови програмування.....	15
2.3 Розгорнута постановка завдання	16
3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ	17
3.1 Опис функціонування системи	17
3.2 Розробка структурної схеми.....	22
3.3 Розробка функціональної схеми	30
3.4 Розробка діаграми процесів.....	36
4 РЕАЛІЗАЦІЯ РОБОТИ. РОЗРАХУНКИ І ЕКСПЕРИМЕНТАЛЬНІ ДАНІ, ЩО ПІДТВЕРДЖУЮТЬ ВІРНІСТЬ ПРОЕКТНИХ ТА ПРОГРАМНИХ РІШЕНЬ.....	38
4.1 Розробка блок-схем та опис алгоритмів функціонування системи.....	38
4.2 Захист розробленого програмного забезпечення.....	50
5 ВПРОВАДЖЕННЯ СИСТЕМИ КІБЕРБЕЗПЕКИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ	53
6 ОСНОВНІ ВИСНОВКИ.....	59
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	61

					ВКРБ-125.26.0031.00.00.ПЗ			
Вим.	Арк.	№ докум.	Підп.	Дата	<i>Програмне забезпечення системи кібербезпеки комп'ютерної мережі з використанням Fortinet Security Fabric</i>	Лім.	Аркуш	Аркушів
<i>Розроб.</i>	Кирилов В.О.					Б	1	67
<i>Перев.</i>	Смірнов О.А.							
<i>Н.контр.</i>	Коваленко А.С.					ЦНТУ КБ-22з		
<i>Затв.</i>	Смірнов О.А.							

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

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

ВСТУП

Актуальність теми. Існує три сегменти ринку безпеки: безпека критичної інфраструктури, захист гібридних хмар і інтелектуальне виявлення погроз. Так, відповідно до недавнього дослідження Forrester Research понад половину опитаних компаній за рік зштовхнулися з порушеннями безпеки систем SCADA/ICS. Операційні технології/IoT стануть наступним бойовищем.

Для забезпечення безпечної роботи з різними хмарними сервісами розроблений брокер доступу до хмар. Погрози стають усе більше витонченими, відповідно, засоби захисту повинні ставати більш інтелектуальними. Для підвищення оперативності виявлення погроз розроблений Threat Intelligence Service (TIS), де для виявлення погроз використовується аналітика більших даних. Застосування засобів штучного інтелекту в TIS повинне забезпечити проактивний захист від актуальних погроз.

Зараз розробляється інфраструктура Security Fabric, що вважається третім поколінням архітектури мережевої безпеки після брандмауерів з контекстною перевіркою й міжмережевих екранів наступного покоління. Торік Fortinet придбала компанію AccelOps, ведучого виробника SIEM. Відповідний продукт став частиною Security Fabric під назву FortiSIEM. А завдяки партнерській програмі Fabric Ready Partner Program фабрика безпеки може інтегрувати рішення інших постачальників через відкриті API. У цей час до програми приєдналося 60 вендорів, у тому числі Cisco, Brocade, HPE і ін.

Мета й завдання дослідження. Метою роботи є програмне забезпечення системи кібербезпеки комп'ютерної мережі з використанням Fortinet Security Fabric.

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

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		3

- Огляд існуючих систем комп'ютерної мережі з використанням Fortinet Security Fabric.
- Дослідження системи кібербезпеки комп'ютерної мережі з використанням Fortinet Security Fabric.
- Програмна реалізація системи кібербезпеки комп'ютерної мережі з використанням Fortinet Security Fabric.

Практична цінність отриманих результатів полягає в тому, що розроблені алгоритми дозволяють успішно вирішувати задачі комп'ютерної мережі з використанням Fortinet Security Fabric.

Таким чином, виходячи з вищеперерахованого, програмне забезпечення системи кібербезпеки комп'ютерної мережі з використанням Fortinet Security Fabric, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за першим (бакалаврським) рівнем вищої освіти.

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		4

1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ

1.1 Призначення системи

Fortinet Security Fabric охоплює цілий комплекс рішень для забезпечення безпеки – від контролю доступу й міжмережевих екранів до засобів захисту від цільових атак. Фабрика Fortinet реалізує концепцію безперервної сегментації, що дозволяє забезпечити безпеку в умовах розмитого периметра.

Основу Fortinet Security Fabric становлять її міжмережеві екрани FortiGuard. Цього року Fortinet була включена Gartner у квадрат лідерів MCE наступного покоління. Широка лінійка міжмережевих екранів – від пристроїв початкового рівня й віртуальних пристроїв до потужних шасі дозволяє реалізувати сегментацію на всіх рівнях мережі. У рамках фабрики MCE можуть взаємодіяти один з одним, що дозволяє бачити повну картину того, що відбувається в мережі, і вживати погоджені дії для її захисту. Міжмережеві екрани Fortinet повинні стояти в ядрі мережі. Так, потужні MCE серії 7000 здатні забезпечувати інспекцію застосунків на швидкості 100 Гбіт/с.

Компанія Fortinet® (NASDAQ: FTNT), світовий лідер в області високоефективних рішень по забезпеченню інформаційної безпеки, сьогодні оголосила про розвиток адаптивної системи мережевої безпеки Fortinet за рахунок удосконалення функцій автоматизації, відстеження й керування для всіх типів хмарних середовищ, а також збільшення показників продуктивності: від приватних і загальнодоступних хмар моделі «інфраструктура як послуга» (IaaS) до застосунків «програмне забезпечення як послуга» (SaaS).

Компанія Fortinet розширила функціонала віртуалізованого засобу захисту загальнодоступних і приватних хмар FortiGate, і створила економічне рішення, що володіє найвищою продуктивністю.

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		5

Тепер рішення Fortinet доступні «на вимогу» на платформі Microsoft Azure Marketplace. Завдяки цьому організації одержують можливість оплачувати користування службами хмарної безпеки в міру необхідності.

Рішення FortiGate автоматизує процес розгортання загальнодоступної хмари й підтримує поліпшені функції автоматичного масштабування й оркестрації робочих навантажень платформи Amazon Web Services (AWS). Доступні моделі виділення ресурсів на вимогу й використання власної ліцензії (BYOL).

Нова програма ліцензування «as-you-grow» віртуальної машини Fortinet з оплатою в міру використання для постачальників хмарних і керованих послуг, а також сервісів-провайдерів безпеки MSSP підтримує автоматизацію й гнучке призначення цін для кінцевих клієнтів.

FortiCASB – це новий сервіс забезпечення безпеки хмарних застосунків, призначений для відстеження й керування доступом до застосунків SaaS (наприклад, Office 365) і іншим застосункам SaaS як зсередини мережі, так і зовні.

1.2 Область застосування

По даним недавнього опитування компанії ESG Research, 62% фахівців з інформаційної безпеки повідомляють, що їм не вдається реалізувати функцію відстеження хмарних навантажень на тім же рівні, що й у фізичних мережах. 56% фахівців заявляють, що поточний рівень автоматизації й оркестрації процедур і операцій забезпечення безпеки їхніх корпоративних мереж не задовольняє вимогам хмарної безпеки. З метою реалізації таких переваг хмарної технології, як масштабованість, гнучкість і ефективність, необхідно забезпечити інтеграцію, відстеження й обмін даними між всіма елементами системи безпеки у всіх середовищах. Лише після вживання перерахованих заходів можна буде говорити про автоматизацію захисту.

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		6

Компанія Fortinet розширила основні функції архітектури адаптивної системи мережевої безпеки з метою забезпечення безпеки хмарних середовищ і обміну даними про погрози на тім же рівні, що й у фізичних корпоративних мережах. Останні поліпшення входять до складу версії FortiOS 5.6 і забезпечують всебічний гнучкий захист хмарних середовищ організацій і постачальників послуг.

Компанія Fortinet значно вдосконалила віртуалізоване рішення FortiGate з метою забезпечення продуктивності, достатньої для захисту приватних і загальнодоступних хмар. Тепер пропускна здатність віртуальних машин (VM) на ядро в 3 рази перевищує зафіксований раніше показник. Такий результат був досягнутий завдяки підвищенню потужності віртуальних машин, ЦП яких містять 16, 32 і більше ядер. Також однієї з характеристик віртуального засобу FortiGate є найвищий у світі показник продуктивності шестиядерної віртуальної машини – до 132 Гбіт/с. Цього вдалося домогтися за рахунок застосування технології прискорення за допомогою процесорів безпеки (SPU) Fortinet. Крім того, нові економічні рішення сприяють скороченню витрат на 20-30% без зниження продуктивності віртуальних машин.

У міру росту кількості організацій, які здійснили перенос ІТ-інфраструктур у хмару, з'явилися моделі виділення ресурсів на вимогу. Завдяки цим моделям баланс витрат змістився від капітальних до експлуатаційного. Це привело до повернення реінвестованих засобів у бюджети організацій і підвищенню ефективності керування хмарними інфраструктурами. Віртуальні рішення в складі адаптивної системи мережевої безпеки Fortinet, що забезпечують комплексний захист мереж і вмісту, тепер доступні на вимогу на платформі Azure Marketplace. Крім того, тепер рішення Fortinet з підтримкою поліпшених функцій автоматичного масштабування й оркестрації доступні як для AWS на вимогу, так і в рамках моделі використання власної ліцензії (BYOL). Ці рішення підтримують гнучку обробку навантажень і автоматичне масштабування системи безпеки залежно від умов.

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		7

Компанія Fortinet розробила нову віртуальну машину, доступну на вимогу. Рішення являє собою повністю готову до експлуатації платформу віртуальної машини з можливостями ліцензування й виділення ресурсів, призначену для постачальників хмарних і керованих послуг. Платформа підтримує автоматизацію й модель призначення цін для кінцевих клієнтів на вимогу, схожу з моделлю ціноутворення провідних постачальників хмарних послуг. Платформа підтримує оплату в міру використання – як погодинну, так і залежно від обсягу трафіку, – а також сумісна з технологією оркестрації NFV, застосовуваної постачальниками керованих послуг. У сполученні з рішенням FortiHypervisor доступна на вимогу віртуальна машина підтримує використання компаніями, що надають керовані послуги із забезпечення хмарної безпеки, а також послуги SD-WAN, самих різних форм-факторів устаткування, установлюваного в клієнтському приміщенні (CPE): фізичних, віртуальних і гібридних.

Компанія Fortinet представляє нову службу FortiCASB на основі API. Рішення підтримує відстеження IT-фахівцями доступу користувачів до деяким найбільш популярним застосункам SaaS, у тому числі Office 365, як зсередини мережі, так і зовні. Рішення FortiCASB забезпечує захист даних, що зберігаються в розташуваннях SaaS, від хмарних погроз і підтримує інструменти забезпечення відповідності вимогам і аудита, що дозволяють підвищити ефективність керування застосунками SaaS.

У цей час хмарні служби розвиваються набагато швидше, ніж локальні інфраструктури й застосунки, однак директори по IT усе ще б'ються над рішенням питань забезпечення хмарної безпеки. Як і у випадку з будь-яким іншою IT-Ресурсом, для керування й захисту хмарних служб варто використовувати політики, застосунку для моніторингу й інтегровані засоби безпеки. Адаптивна система мережевої безпеки Fortinet, доповнена новітніми хмарними рішеннями, підтримує функції відстеження, автоматизації й керування, за допомогою яких директори з IT зможуть забезпечити захист інформації на всій довжині інфраструктури – від центрів обробки даних до хмарних середовищ.

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		8

Компанії створюють гнучкі й масштабовані інфраструктури за допомогою приватних і загальнодоступних хмар. У цих умовах надто важливо забезпечити надійний і погоджений захист ресурсів. Компанія Fortinet розширює функціонал адаптивної системи мережевої безпеки: тепер у сферу її охопту входять приватні хмари, а також хмари інфраструктур і застосунків (SaaS). До числа вдосконалень ставляться також підвищення масштабованості, нові функції для загальнодоступних хмар і функції відстеження SaaS за допомогою нового рішення CASB. Всі ці міри забезпечують оптимальну продуктивність системи безпеки на рівні хмари.

Таким чином, виходячи з вищеперерахованого, програмне забезпечення системи кібербезпеки комп'ютерної мережі з використанням Fortinet Security Fabric, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за першим (бакалаврським) рівнем вищої освіти.

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		9

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

Брандмауер, він же фаєрвол або міжмережевий екран – важливий елемент безпеки системи. Фаєрвол фільтрує вхідний і вихідний трафік, захищаючи комп'ютер від несанкціонованого доступу. В Windows є присутнім стандартний фаєрвол, але його надійність викликає сумнів у багатьох експертів. Поза залежністю від того, яку версію операційної системи ви використовуєте, рекомендується користуватися окремими спеціалізованими рішеннями. От п'ятірка кращих безкоштовних фаєрволів, доступних на даний момент.

ZoneAlarm Free Firewall

ZoneAlarm Free Firewall забезпечує захист у реальному часі й надає додаткові інструменти для безпеки Wi-Fi. Це – один із самих старих і надійних фаєрволів, що існує вже більше 20 років.

Поточна версія ZoneAlarm уміє приховувати відкриті порти, автоматично визначає підозрілий трафік, відключає шкідливі програми й звіряється з базою погроз DefenseNet. Також програма може захищати комп'ютер у публічних Wi-Fi-Мережах, що досить актуально для ноутбуків.

Зверніть увагу, при установці ZoneAlarm не забувайте відключати непотрібні параметри інакше, інсталятор зробить Yahoo вашою домашньою сторінкою. Також вам доведеться надати ZoneAlarm адреса електронної пошти для активації, хоча компанія не ділиться їм зі сторонніми.

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		10

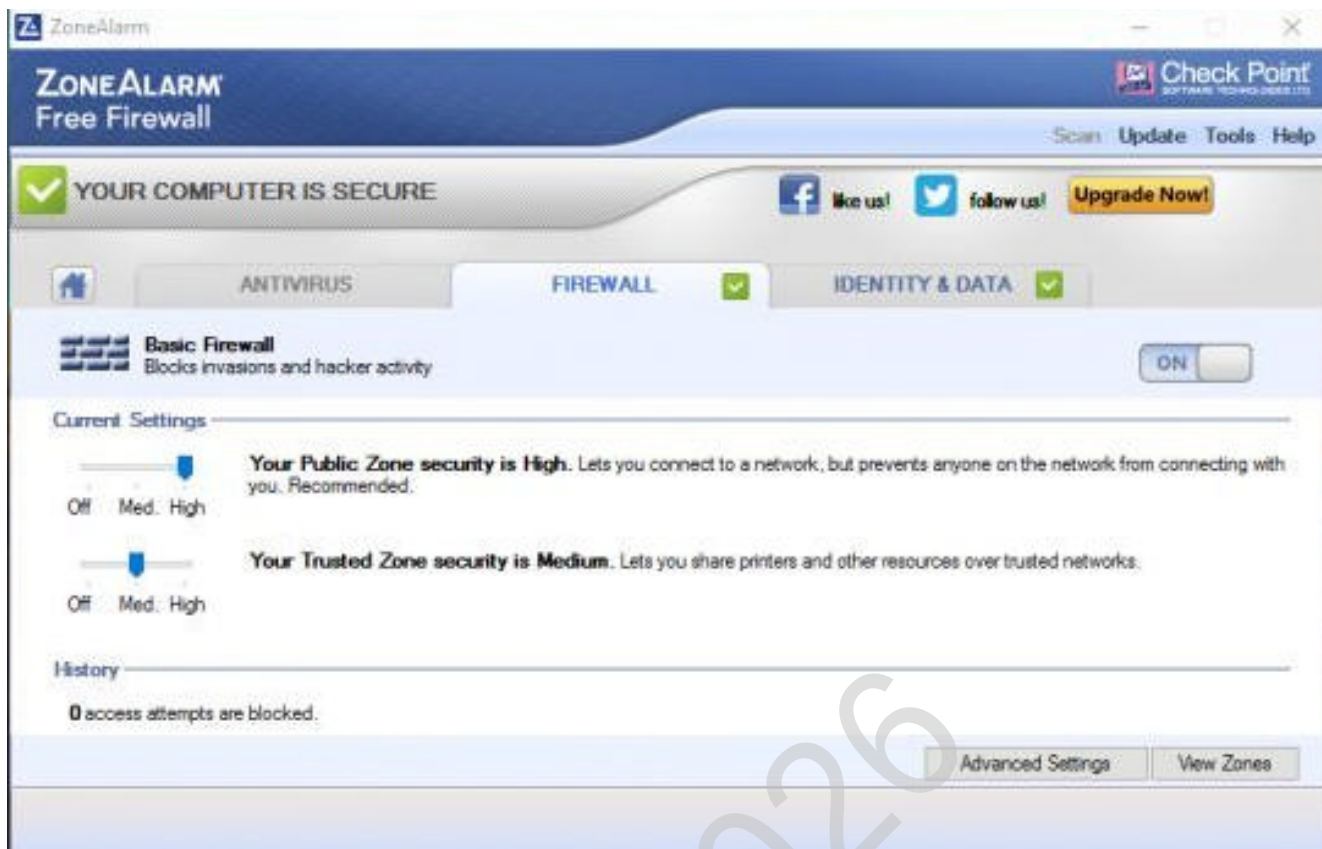


Рисунок 2.1 – Інтерфейс користувача ZoneAlarm

Comodo Free Firewall

Comodo Free Firewall – ще один гарний безкоштовний фаєрвол. Його головна фішка – інструмент “Пісочниця” (Sandbox), що дозволяє запускати будь-які застосунки в окремому віртуальному середовищі. Завдяки цьому навіть явно шкідлива програма не зможе нанести втрати основній системі. Дуже корисна опція, якщо ви любите експериментувати з безкоштовним програмним забезпеченням з неперевіраних джерел. Програма дозволяє легко управляти дозволами для різних мереж і створювати правила для певних програм.

Зверніть увагу, при установці Comodo Free Firewall також важливо дотримувати пильності, інакше інсталятор може замінити вашу домашню сторінку й установити в навантаження браузер Comodo Dragon. Відповідні параметри варто відключити.

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		11

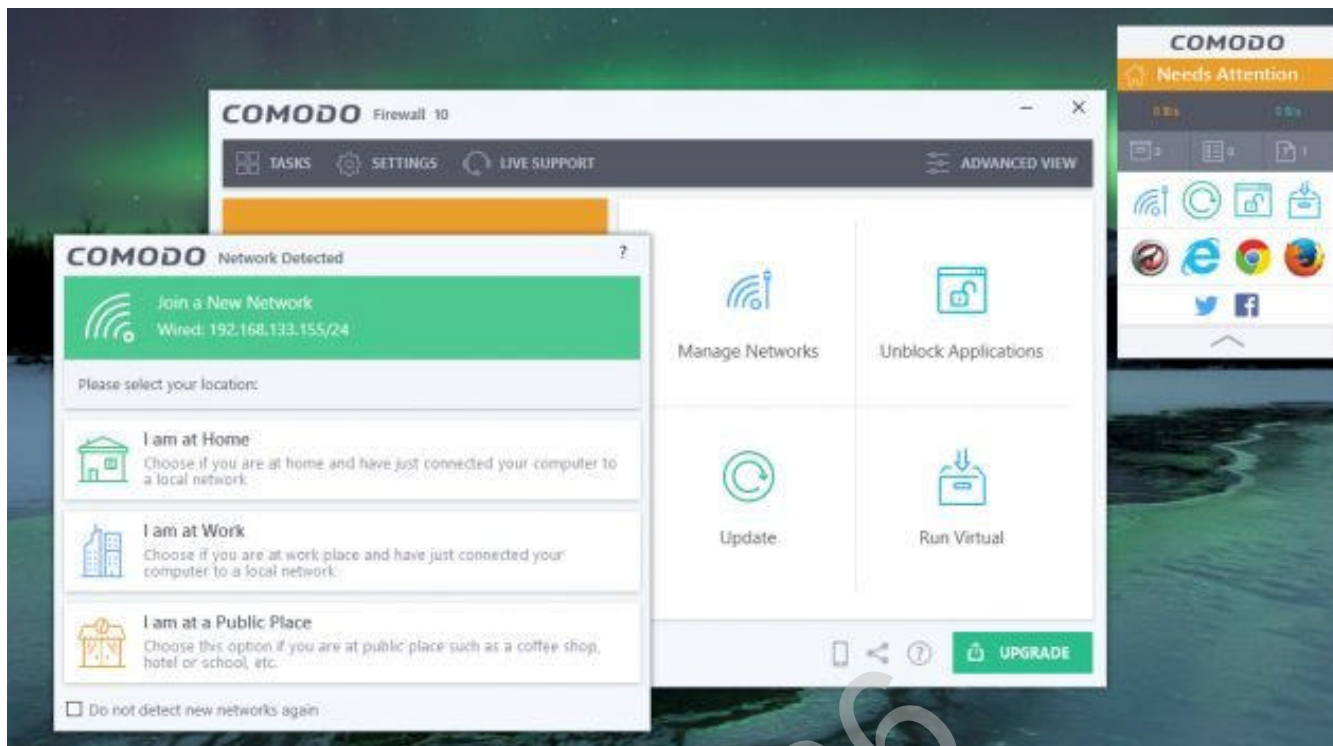


Рисунок 2.2 – Інтерфейс користувача Comodo Free Firewall

GlassWire

GlassWire – добре спроектований брандмауер з упором на інформацію й прозорість. Програма веде докладний облік мережевої активності, так що ви зможете точно довідатися, яке застосунок споживає трафік і в якому обсязі.

Коли який-небудь застосунок або процес намагається вийти в інтернет, користувач миттєво одержує повідомлення й може заблокувати доступ у Мережу одним кліком.

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		12

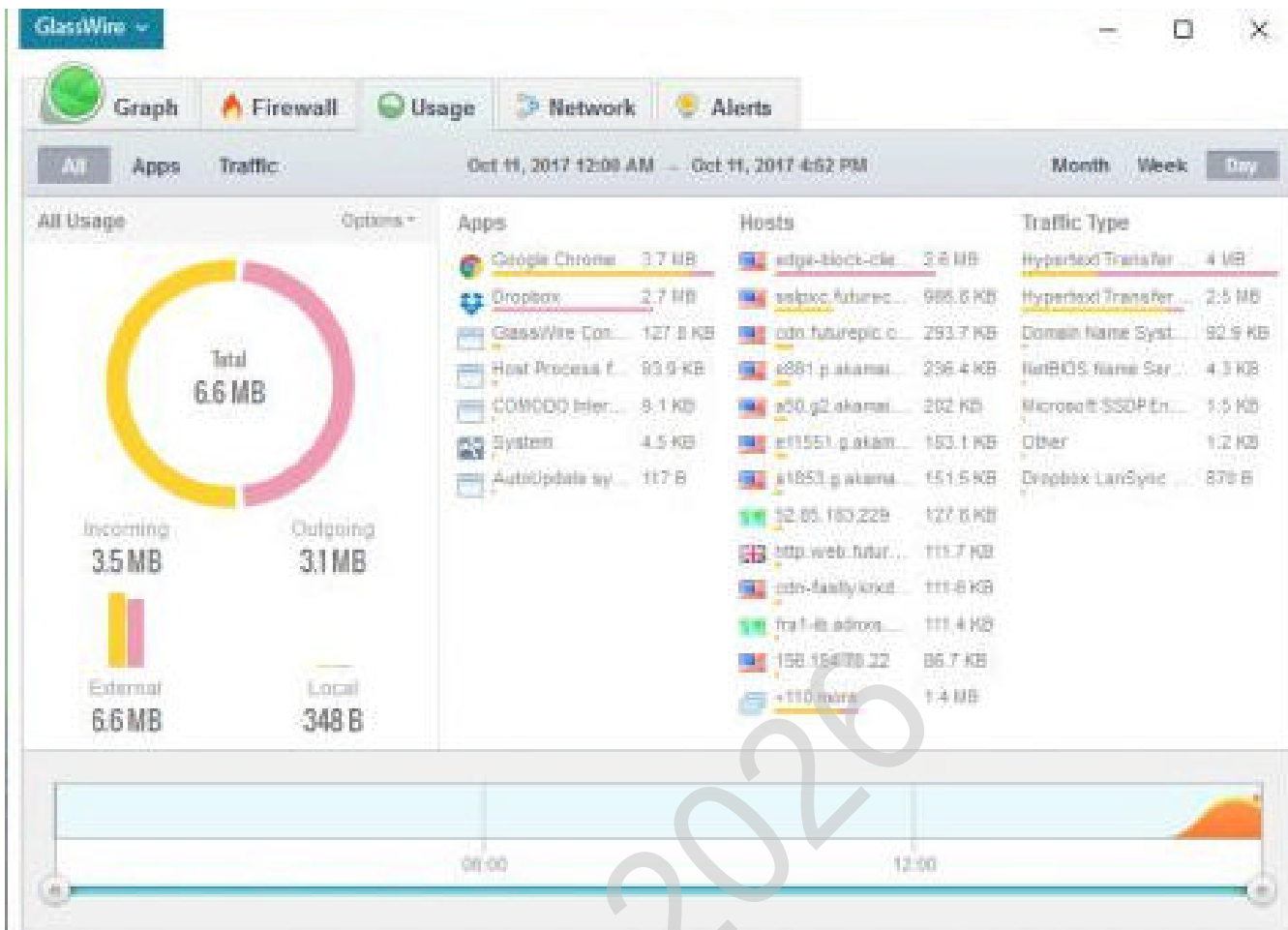


Рисунок 2.3 – Інтерфейс користувача GlassWire

TinyWall

TinyWall – дуже проста й легковага утиліта. Це не стільки самостійний фаєрвол, скільки інструмент для розширеного налаштування й поліпшення убудованого брандмауєра Windows. У роботі TinyWall намагається бути максимально ненав'язливим. Програма не буде тривожити вас повідомленнями, якщо тільки не відбудеться щось по-справжньому важливе.

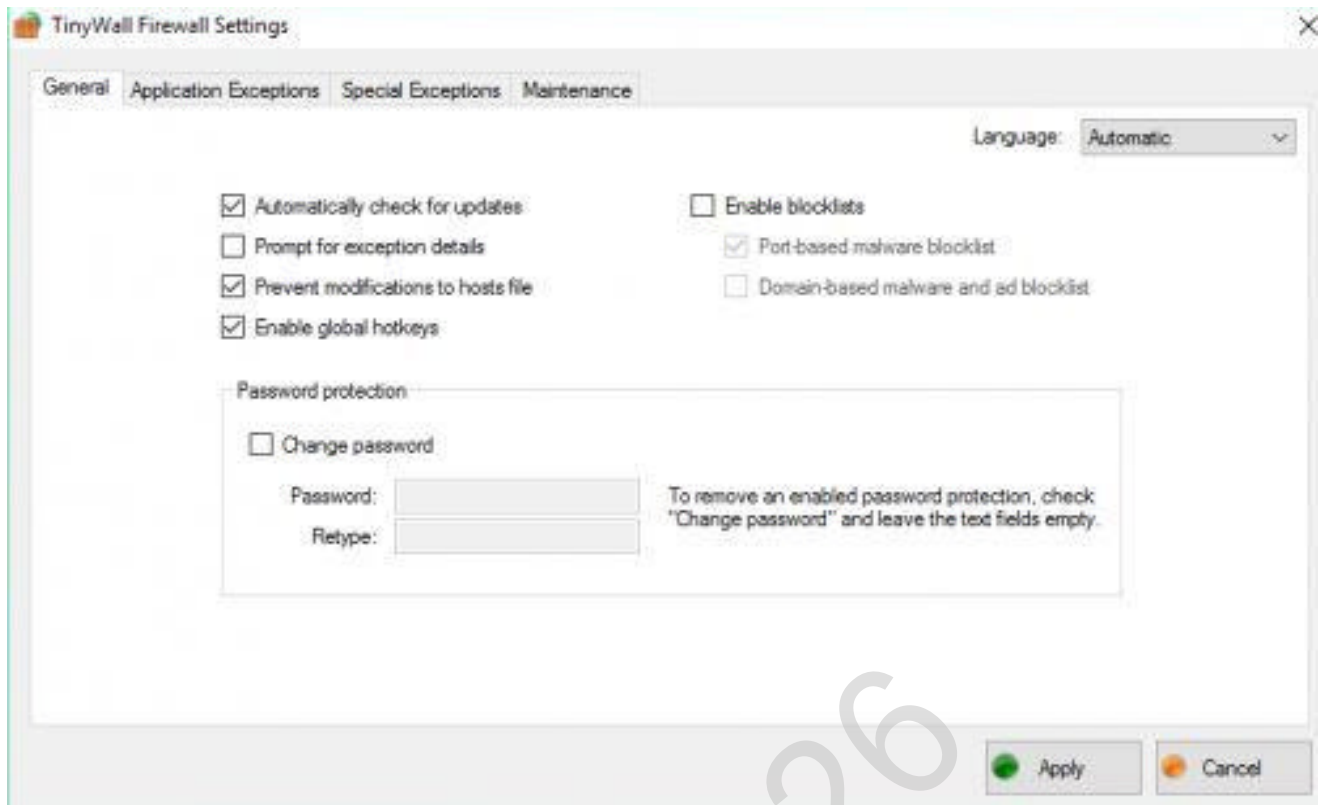


Рисунок 2.4 – Інтерфейс користувача TinyWall

Утиліта повністю відповідає своїй назві – на жорсткому диску вона займає менш 1 МБ і практично ніяк не позначається на продуктивності комп'ютера.

OpenDNS Home

На відміну від варіантів, представлених вище, OpenDNS Home не є що завантажується фаєрволом. Це – набір мережевих налаштувань, які автоматично перенаправляють ваш трафік через сервіс хмарної фільтрації OpenDNS від компанії Cisco. Якщо вказати налаштування в роутері, це захистить всі пристрої, підключені до даної мережі. Фільтри OpenDNS Home автоматично блокують трафік від відомих небезпечних джерел і запобігають спроби фішингу.

Зверніть увагу, сервіс OpenDNS Home вимагає реєстрації. Але це – не примха розроблювачів. В обліковому записі на сайті користувач може вибирати індивідуальні налаштування фільтрації, що може бути корисним для обмеження доступу дітей до певних ресурсів.

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		14

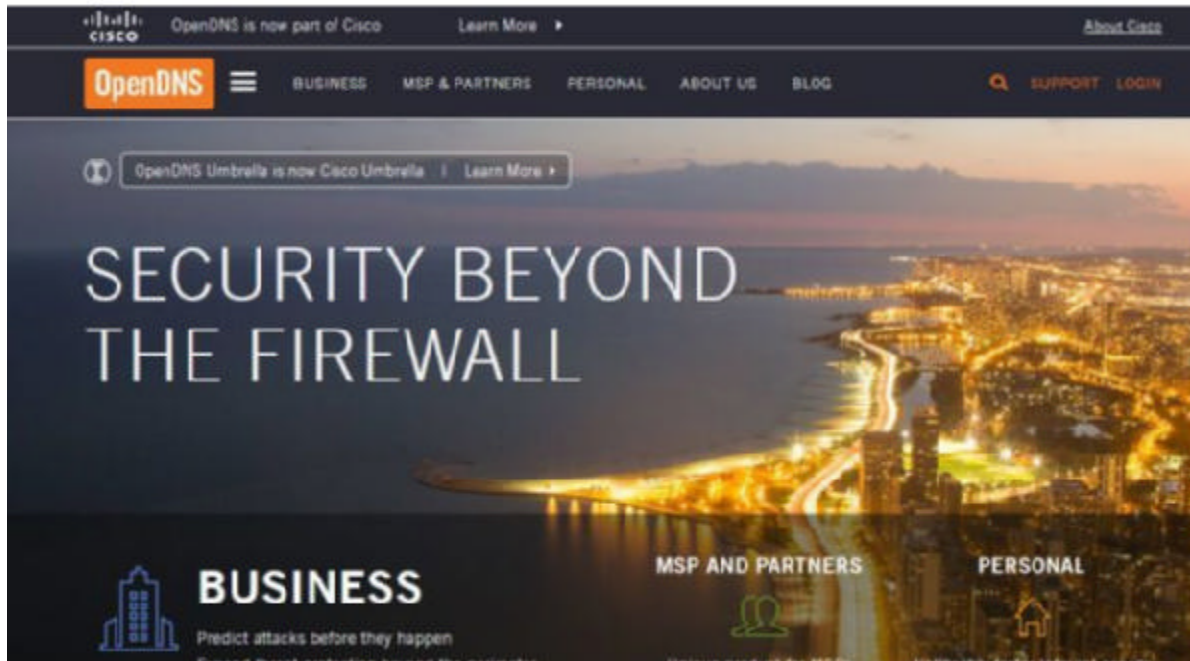


Рисунок 2.5 – Інтерфейс користувача OpenDNS Home

2.2 Обґрунтування вибору засобів для побудови системи кібербезпеки та мови програмування

Python – це потужна мова програмування, яка проста у вивченні. Він має ефективні структури даних високого рівня та простий, але ефективний підхід до об'єктно-орієнтованого програмування. Елегантний синтаксис і динамічна типізація Python разом з його інтерпретованим характером роблять його ідеальною мовою для створення сценаріїв і швидкої розробки додатків у багатьох сферах на більшості платформ. Інтерпретатор Python і обширна стандартна бібліотека доступні у вихідному або двійковому вигляді для всіх основних платформ на веб-сайті Python <https://www.python.org/> і можуть вільно поширюватися. Цей же сайт також містить дистрибутиви та вказівники на багато безкоштовних сторонніх модулів Python, програм і інструментів, а також додаткову документацію. Інтерпретатор Python легко розширюється за допомогою нових функцій і типів даних, реалізованих у C або C++ (або інших мовах, які можна викликати з C). Python також підходить як мова розширення для налаштовуваних програм.

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		15

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 комп'ютерної мережі з використанням Fortinet Security Fabric.

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-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		16

3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ

3.1 Опис функціонування системи

У сучасному інформаційному світі з ростом швидкостей і обсягів передачі даних, використання хмарних технологій і підключення всі нових і нових пристроїв до всесвітньої павутини стає усе більше можливостей для проведення успішних кібератак.

Аналітики прогнозують у найближчому часі збільшення числа атак у сфері інтернету речей (Internet of Things, IoT) і появу нових погроз для гібридних хмар, де розташовується третина від загального числа використовуваних організацією застосунків.

Немаловажним фактором є ріст обсягу шифрованого трафіку – співвідношення між HTTPS і HTTP досягло більше 40%, а використання шифрування шкідливого коду при проведенні кібератаки склало рекордні 50%.

Таким чином, можна зробити вивід, що сучасні погрози стають усе більше витонченими, а засобу захисту повинні ставати більше інтелектуальними.

Для протидії просунутим погрозам безпеки торік компанією Fortinet була представлена стратегічна концепція Fortinet Security Fabric, що у компанії вважають третім поколінням архітектури мережевої безпеки після міжмережевих екранів з інспекційною перевіркою пакетів (Stateful Firewall) і міжмережевих екранів наступного покоління (NGFW).

Платформа Fortinet Security Fabric поєднує критично важливі мережеві технології й технології забезпечення безпеки – від міжмережевих екранів до засобів аналізу контенту й застосунків на кінцевих точках – для забезпечення безперебійної безпеки в розподіленій мережі, будь те локальна або віддалена, фізична або віртуальна, провідна або бездротова, розташована в домені замовника або в хмарі.

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		17

Концепція Fortinet Security Fabric

Платформа Fortinet Security Fabric орієнтована на комплексне застосування всіх продуктів Fortinet у рамках єдиної системи безпеки, а також на їхню спільну роботу з рішеннями інших виробників, дозволяючи динамічно адаптуватися до сучасної IT-інфраструктури.

У своїй концепції вендор робить упор і виділяє три найбільш важливі сегменти ринку: безпека критичної інфраструктури, захист гібридних хмар і інтелектуальне виявлення погроз.

Fortinet Security Fabric сегментує мережу, яка захищається, розділяючи дані й ресурси, забезпечуючи широкий, потужний і автоматичний захист від складних погроз і цілеспрямованих атак.

Платформа дозволяє розподіляти, організовувати й проводити політикові різних доменів, включаючи віддалених співробітників, філії й офіси, географічно розподілені центри обробки даних, приватні й загальнодоступні хмарні мережі.

Платформа побудована по трьох ключових атрибутах:

– Всеосяжність. Fortinet Security Fabric покриває всі поверхні атак. При цьому адміністратори безпеки користуються видимістю всієї інфраструктури, включаючи кінцеві точки, пристрої IoT, точки доступу, мережеві елементи, центри обробки даних, хмари й навіть застосунку й самі дані. Це дозволяє забезпечити захист всіх потенційних точок входу, а також сегментів усередині динамічної мережі. Таке широке розгортання й глибока видимість допомагає контролювати внутрішній трафік і пристрої, запобігає несанкціонованому доступу до обмежених даних і ресурсів і контролює поширення шкідливих програм і дій зловмисників.

– Потужність. Компоненти Fortinet Security Fabric розроблені на основі технології процесорів безпеки Fortinet (Security Processor Unit, SPU). Застосування спеціально розроблених процесорів безпеки значно підвищує продуктивність і масштабованість, запобігаючи впливу безпеки на пропускну здатність мережі й знижуючи навантаження на інфраструктуру.

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		18

– Автоматизація. Fortinet Security Fabric забезпечує швидке й скоординоване реагування на погрози. Платформа дозволяє автоматично визначити й динамічно ізолювати скомпрометовані пристрої, сегменти мережі, правила відновлення, відключити некоректні політики й видалити шкідливі програми. Fortinet Security Fabric також надає рішення для динамічної адаптації до змін мережевих конфігурацій, впровадження нових політик, оскільки зміни в бізнесі тягнуть зміни в ІТ-середовищу. Міри безпеки й контрзаходи автоматично розгортаються в ході розгортання нових пристроїв, робочих навантажень і служб по всій інфраструктурі. Платформа також підтримує відкриті прикладні програмні інтерфейси (API), які дозволяють організаціям інтегрувати наявні засоби захисту й мережеві технології з Fortinet Security Fabric.

Використовуючи пряму взаємодію, Fortinet Security Fabric дозволяє всім елементам системи безпеки швидко обмінюватися інформацією про погрози й координувати відповідні дії.

Кожний сторонній пристрій може брати участь в обміні інформацією залежно від можливостей свого API.

Реалізація системи безпеки на основі Fortinet Security Fabric може виконуватися поетапно, починаючи із захисту самих критичних ресурсів і зниження високих ризиків.

Альянс Fortinet і CarbonBlack поліпшує захист від передових погроз. Так, наприклад, засіб захисту кінцевих точок CarbonBlack може передати підозріле програмне забезпечення мережевій пісочниці FortiSandbox для докладного аналізу в ізольованому середовищі.

Тестування рішень із состава Fortinet Security Fabric здійснюється в рамках програми Fabric-Ready Partner Program, учасниками якої є такі великі корпорації як Cisco, HPE і Nokia.

Склад Fortinet Security Fabric

До складу Fortinet Security Fabric входить цілий комплекс рішень по забезпеченню безпеки.

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		19

Хоча кожний елемент із состава Fortinet Security Fabric може працювати автономно, максимальна ефективність і надійність досягається при їхній взаємній інтеграції.

Фундаментом побудови системи безпеки в контексті Fortinet Security Fabric є корпоративний міжмережевий екран FortiGate під керуванням спеціальної операційної системи FortiOS.

FortiGate дозволяє сегментувати мережеві елементи, забезпечувати контроль трафіку, пристроїв і даних для більше ефективного керування, виконують перевірку SSL-трафіку для запобігання погроз.

Крім того, FortiGate підтримує відправлення всіх файлів для перевірки, протоколи HTTP, FTP, POP3, IMAP, SMTP, MAPI, IM і їхні зашифровані версії на проведення інспекційного аналізу засобами мережевої пісочниці FortiSandbox.

Для віртуальних середовищ Fortinet пропонує віртуальні версії FortiGate, які підтримують всі основні гіпервізори.

У рамках єдиної архітектури системи безпеки віртуальні міжмережеві екрани можуть бути розгорнуті через частки, загальнодоступні (IaaS і SaaS) і гібридні хмари для створення мікросегментації трафіку « північ-південь» (взаємодія з/у ЦОД) і «схід-захід» (взаємодія між застосунками й користувачами в ЦОД).

В 2017 році випущена платформа FortiCASB (Cloud Access Security Broker), новий компонент Fortinet Security Fabric, покликаний гарантувати безпека роботи з застосунками, надаваними у вигляді сервісів (SaaS).

Веб-застосунки й програми електронної пошти вже давно є улюбленими об'єктами кіберзлочинців, оскільки вони мають доступ до кошовної інформації і їх відносно легко використовувати в зловмисних цілях.

Успішна атака може привести до безлічі негативних наслідків, включаючи фінансовий збиток, ушкодження репутації компанії й втрату довіри клієнтів.

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		20

Для захисту електронної пошти до складу Fortinet Security Fabric входить продукт FortiMail, що забезпечує захист від спаму, антивірусну захист і інтеграцію з мережевою пісочницею FortiSandbox.

FortiMail відправляє підозрілі вкладення електронної пошти на FortiSandbox для інспекційного контролю.

FortiSandbox повертає назад на FortiMail статистичні дані й результати сканування.

FortiWeb забезпечує захист веб-застосунків, аналізуючи сигнатури й поведіння, захищаючи від DDoS-атак, верифікуючи протоколи й т.д.

Поява великої кількості особистих пристроїв співробітників, що мають доступ до корпоративної інформації організації, а також популярність гібридних хмар привели до розуміння того, що потрібно міняти саму концепцію безпеки.

Міжмережеві екрани не можуть забезпечити гарантований захист на границі із мережею, яка захищається, оскільки постійно росте число точок входу в мережу, а самі границі мереж досить умовні.

Виходячи із цього виникає концепція недовіри жодному вузлу мережі, що поклала початок фабрикам безпеки.

Платформа Fortinet Security Fabric розроблена для забезпечення масштабованої й взаємозалежної безпеки в сполученні з високою поінформованістю про погрози й відкритими стандартами API для захисту навіть самих вимогливих корпоративних середовищ.

Технології безпеки Fortinet зарекомендували себе як ефективні й продуктивні у своїй галузі.

Взаємозалежні рішення Fortinet через Fortinet Security Fabric дозволяють закрити пробіли в захисті, залишені застарілими засобами захисту й платформами безпеки, забезпечуючи широкий охопит, потужну захист без шкоди для продуктивності мережі й автоматичне прийняття інтелектуальних дій.

Крім інтеграції технологій, використовуваних у звичайних платформах безпеки, містить у собі захист кінцевих точок, контроль доступу, сегментацію

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		21

мережі, SIEM і інші інструменти керування, рішення по захисту від складних погроз і механізми безпеки, убудовані безпосередньо в мережеві пристрої.

Ключовим елементом аналізу шкідливих програм є пісочниця FortiSandbox. Fortinet Security Fabric забезпечує інтеграцію всіх компонентів захисту Fortinet з FortiSandbox з метою оптимізації використання обчислювальних ресурсів і збагачення даних про поточні й потенційні погрози з різних джерел в інфраструктурі.

При цьому Fortinet Security Fabric гарантує: широкий охоплення всіх частин організації в міру її росту й зміни; забезпечення потужного захисту без шкоди для продуктивності мережі; автоматичне прийняття інтелектуальних дій по захисту інформації.

3.2 Розробка структурної схеми

Fortinet Security Fabric сегментує всю мережу, починаючи від пристроїв Інтернету речей (IoT) і закінчуючи хмарним середовищем, щоб забезпечити високоефективний захист від витончених погроз:

– Комплексне відстеження й захист від будь-яких цифрових атак. Згідно із прогнозами, до 2020 року більше 25 % всіх атак у корпоративному секторі будуть спрямовані на пристрої IoT. Захист ізольованих застосунків, розташованих у багатохмарних середовищах, є ще більш складним завданням. Fortinet Security Fabric дозволяє відслідковувати всі пристрої й застосунки в режимі реального часу.

– Інтегроване рішення для виявлення й реагування на просунуті погрози. Організації, у яких у середньому налічується більше 30 засобів забезпечення безпеки, зіштовхуються з низьким рівнем прозорості й використанням декількох консолей засобів безпеки, що віднімають масу часу. Fortinet Security Fabric оптимізує зв'язок між різними рішеннями безпеки, скорочуючи кількість вікон виявлення й усунення.

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		22

– Автоматизовані операції й аналітика за допомогою єдиної консолі. Технології витончених кібератак, такі як штучний інтелект (AI) і машинне навчання (ML), скорочують час, необхідний для атаки з моменту вторгнення. У зв'язку із цим виявлення погроз на підприємствах повинне вироблятися більш оперативно. Fortinet Security Fabric дозволяє координувати процес автоматизованого реагування й усунення погроз, виявлених у всій розширеній мережі організації.

FortiGate: Міжмережевий екран наступного покоління

Фахівці з інформаційної безпеки постійно перебувають у пошуку комплексної системи захисту, що здатний виконувати безліч функцій: запобігати вторгнення, виконувати фільтрацію веб-сайтів, блокувати шкідливі програми й застосунки. Однак відсутність інтеграції й погана видимість інфраструктури стають серйозними перешкодами при керуванні цими точковими сервісами. За прогнозами компанії Gartner, до 2019 року підприємства будуть шифрувати 80% свого трафіку, і 50% кібератак будуть сховані саме в зашифрованому трафіку.

Міжмережевий екран наступного покоління FortiGate використовує спеціально розроблені лабораторією FortiGuard процесори й служби безпеки для забезпечення максимального захисту й високої продуктивності, включаючи захист зашифрованого трафіку. Продукція FortiGate має зручний автоматизований огляд мережі, застосунків і користувачів, а також проводить оцінку безпеки для вибору найкращого рішення.

Служби безпеки FortiGuard для FortiGate: Міжмережеві екрани наступного покоління

Міжмережеві екрани FortiGate NGFW одержують постійні відновлення аналітики погроз від служб безпеки FortiGuard Labs. Служби запобігання вторгнень, контролю застосунків, веб-фільтрації, захисту від шкідливих програм і хмарна «пісочниця» захищають підприємства від відомих і невідомих просунутих погроз.

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		23

Application Control

Наше рішення сприяє підвищенню ефективності захисту й забезпечує відповідність вимогам за рахунок реалізації належних політик за допомогою унікальної функції відстеження стану запущених користувачами застосунків у режимі реального часу. Рішення FortiGuard Application Control служить для оперативного створення політик дозволу, обмеження й заборони доступу до застосунків або цілих категорій застосунків.

Web Filtering

Забезпечує захист корпоративної мережі шляхом блокування доступу до зламаних сайтів і сайтів зі шкідливим або неприйнятним умістом.

FortiSandbox Cloud

Служба FortiSandbox Cloud – це рішення для виявлення просунутих погроз, що виконує динамічний аналіз для ідентифікації раніше невідомого шкідливого ПЗ. Актуальні дані, створені «пісочницею» FortiCloud Sandbox, надходять у системи профілактичної перевірки усередині мережі для знешкодження погрози.

Antivirus

Служба FortiGuard AntiVirus забезпечує захист від останніх вірусів, шпигунського ПЗ й інших погроз на рівні вмісту. Ця служба оснащена провідними сучасними модулями виявлення погроз, які запобігають проникненню існуючих і нових погроз у мережу з наступним доступом до коштовного вмісту.

Intrusion Prevention

FortiGuard IPS запобігає вторгненням в мережу за рахунок виявлення й блокування погроз до того, як вони досягнуть мережевих пристроїв.

Virus Outbreak Protection Service

Служба протидії поширенню вірусів FortiGuard Virus Outbreak Protection Service (VOS) забезпечує захист у період між відновленнями антивірусу. Для цього використовується функція аналізу в «пісочниці» FortiCloud Sandbox, що

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		24

виявляє шкідливе ПЗ й блокує його поширення в корпоративній мережі протягом інтервалів між відновленнями підписів. Операційна система в режимі реального часу ініціює пошук у нашій базі даних глобальних погроз.

Content Disarm & Reconstruction

Служба знешкодження й реконструкції вмісту (CDR) у режимі реального часу витягає активний вміст файлів, створюючи неструктуровані очищені файли. Активний вміст розглядається як підозріле й віддаляється. Служба CDR обробляє всі вхідні файли, деконструює їх і видаляє всі елементи, не відповідним політикам міжмережевого екрана.

IP Reputation & Anti-botnet Security

Служба FortiGuard IP Reputation збирає відомості про IP-адреси, що відповідають сумнівним джерелам даних, за допомогою розподіленої мережі датчиків погроз Fortinet, CERT, MITRE, а також одержує необхідну інформацію від готових до співробітництва конкурентів і з інших джерел по усьому світі, що містять актуальні дані про шкідливі ресурси. Відомості надходять від шлюзів розподіленої мережі в режимі, наближеному до реального часу, і в сполученні з даними досліджень, наданими відділом FortiGuard Labs, забезпечують безпека організацій і сприяють блокуванню, що попереджає, атак.

Пакет служб FortiGate Enterprise

У пакет служб Enterprise (ENT) входить:

– Посередницька служба хмарної безпеки (CASB) забезпечує можливість відстеження, відповідність вимогам, захист даних і протидію погрозам для корпоративних хмарних служб.

– Служба Industrial Security Service – SCADA (система диспетчерського керування й збору даних) і ICS (система керування виробничими процесами). Ці сигнатури захищають важливі інфраструктури й галузь промислового виробництва, де спостерігаються часті й витончені кібератаки.

– Служба Security Rating Service виконує перевірки мережі за підтримкою адаптивної системи мережевої безпеки, надає оцінку й рекомендації

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		25

для операційних груп. Отриману систему показників можна використовувати для оцінки відповідності різним внутрішнім і зовнішнім організаційним політикам, стандартам і нормативним вимогам, у тому числі для порівняльного аналізу рейтингу вашої компанії з рейтингом конкурентів. .

Пакет засобів захисту FortiGuard Enterprise (ENT) розроблений з урахуванням сучасної ситуації в області просунутих погроз. Пакет Enterprise надає комплексне рішення, необхідне для забезпечення безпеки й захисту від кібератак в усіх напрямках: від кінцевої точки до хмари. Крім того, у пакеті передбачені технології, необхідні для рішення сучасних складних завдань в області експлуатаційних технологій (ВІД), відповідності вимогам і керування. Пакет Enterprise пропонує найбільш комплексний захист. У пакет служб Enterprise входить:

- Служба керування застосунками (NGFW Application Control).
- IPS.
- Захист від вірусів (Antivirus).
- Захист від ботнетів (Botnet).
- Служба репутації IP-адрес і доменів (IP/Domain Reputation).
- Служба безпеки мобільних пристроїв (Mobile Security).
- Компонент фільтрації веб-вмісту (Web Filtering).
- Захист від небажаної пошти (Antispam).
- Хмарне рішення FortiSandbox Cloud.
- Служба протидії поширенню вірусів (Virus Outbreak Protection).
- Служба знешкодження й реконструкції вмісту (Content Disarm & Reconstruction).
- Брокер безпечного доступу в хмару (CASB).
- Служба оцінки систем безпеки (Security Rating) .
- Служба Industrial Security Service.
- Служба підтримки FortiCare.

Пакет служб FortiGate UTM

Пакет засобів захисту FortiGuard Unified Protection Bundle (UTM) – це традиційний пакет служб уніфікованого керування погрозами Unified Threat Management. Пакет Unified Protection Bundle розширює захист від погроз по всій поверхні цифрових атак, забезпечуючи кращу в галузі захист від витончених атак. Пакет UTM захищає від атак через Інтернет і по електронній пошті. Пакет UTM – краще рішення для уніфікованого захисту від погроз. У пакет служб UTM входить:

- Служба керування застосунками (NGFW Application Control).
- IPS.
- Захист від вірусів (Antivirus).
- Захист від ботнетів (Botnet).
- Служба репутації IP-адрес і доменів (IP/Domain Reputation).
- Служба безпеки мобільних пристроїв (Mobile Security).
- Компонент фільтрації веб-умісту (Web Filtering).
- Захист від небажаної пошти (Antispam).
- Хмарне рішення FortiSandbox Cloud.
- Служба протидії поширенню вірусів (Virus Outbreak Protection).
- Служба знешкодження й реконструкції вмісту (Content Disarm & Reconstruction).
- Служба підтримки FortiCare.

Перевага FortiGuard:

- FortiGuard обробляє більше 69 мільйонів веб-сторінок щогодини, надаючи самі актуальні й точні дані про надійність і категоризацію.
- Запобігання шкідливих завантажень і атак веб-браузера за допомогою функції веб-фільтрації з найвищим рейтингом (VBWeb Verified).
- Підвищення продуктивності електронної пошти завдяки чудовому захисту від спаму, підтвердженої незалежним тестуванням сторонніх виробників (VBSpam + Verified).

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		27

Пакет засобів захисту від просунутих погроз FortiGate

Пакет засобів захисту від просунутих погроз (АТР) FortiGuard забезпечує основний рівень безпеки, необхідний для захисту від відомих і невідомих кіберзагроз. У пакет засобів захисту від просунутих погроз входить:

- Служба керування застосунками (NGFW Application Control).
- IPS.
- Захист від вірусів (Antivirus).
- Захист від ботнетів (Botnet).
- Служба репутації IP-адрес і доменів (IP/Domain Reputation).
- Служба безпеки мобільних пристроїв (Mobile Security).
- Хмарне рішення FortiSandbox Cloud.
- Служба протидії поширенню вірусів (Virus Outbreak Protection).
- Служба знешкодження й реконструкції вмісту (Content Disarm & Reconstruction).
- Служба підтримки FortiCare 24*7.

Fortinet Security Fabric технологія інтеграції мереж, рівня доступу, застосунків, ЦОД і хмари в єдине рішення для забезпечення безпеки використання інформації кінцевими користувачами.

Fortinet Security Fabric – адаптивна система мережевої безпеки. Вона підтримує реалізацію деталізованих політик безпеки на основі таких факторів, як ідентифікація користувачів, застосунків, розташування й типів пристроїв

Інструменти забезпечення захисту доступні за допомогою єдиного інтерфейсу керування.

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		28

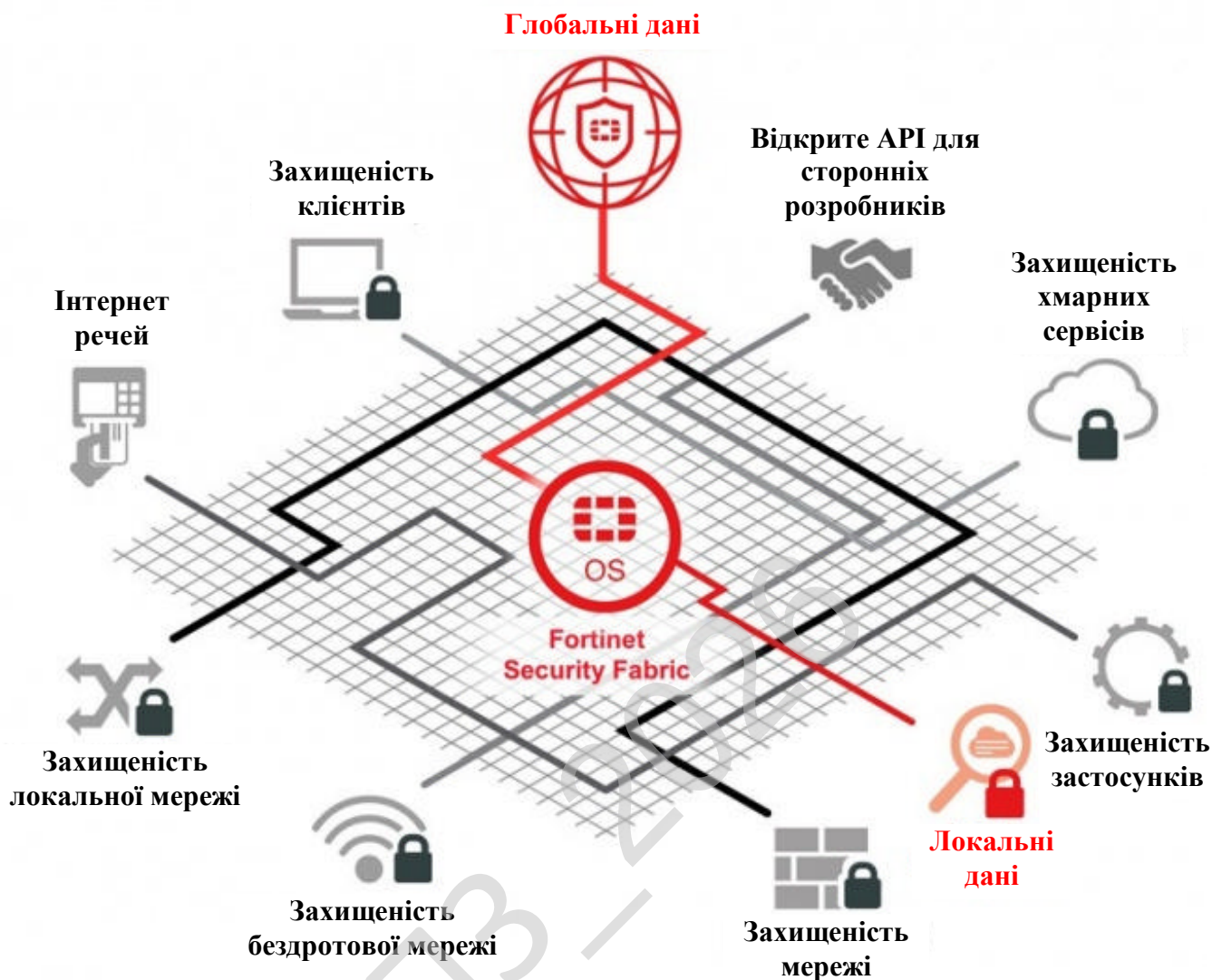


Рисунок 3.1 – Структурна схема системи

Fortinet Security Fabric – об'єднана платформа безпеки, що зводить воедино її засоби захисту мереж у рамках однієї архітектури. Сюди входять засоби захисту:

- інфраструктури;
- дротових і бездротових мереж;
- пристроїв кінцевих користувачів;
- IoT-пристроїв;
- рівнів доступу;

- загальнодоступної й гібридної хмари;
- програмно-конфігуруємої мережі;
- засобів віртуалізації.

3.3 Розробка функціональної схеми

На рисунку 3.2 зображена функціональна схема системи. Нижче розглянемо її більш докладно.

На ринку сьогодні присутній величезна кількість засобів захисту від кібератак, і на цьому тлі вибір міжмережевого екрана нового покоління перестав бути просто порівнянням їхніх технічних характеристик. На перший план сьогодні виходить всебічна підтримка бізнес-процесів, а не їхнє блокування.

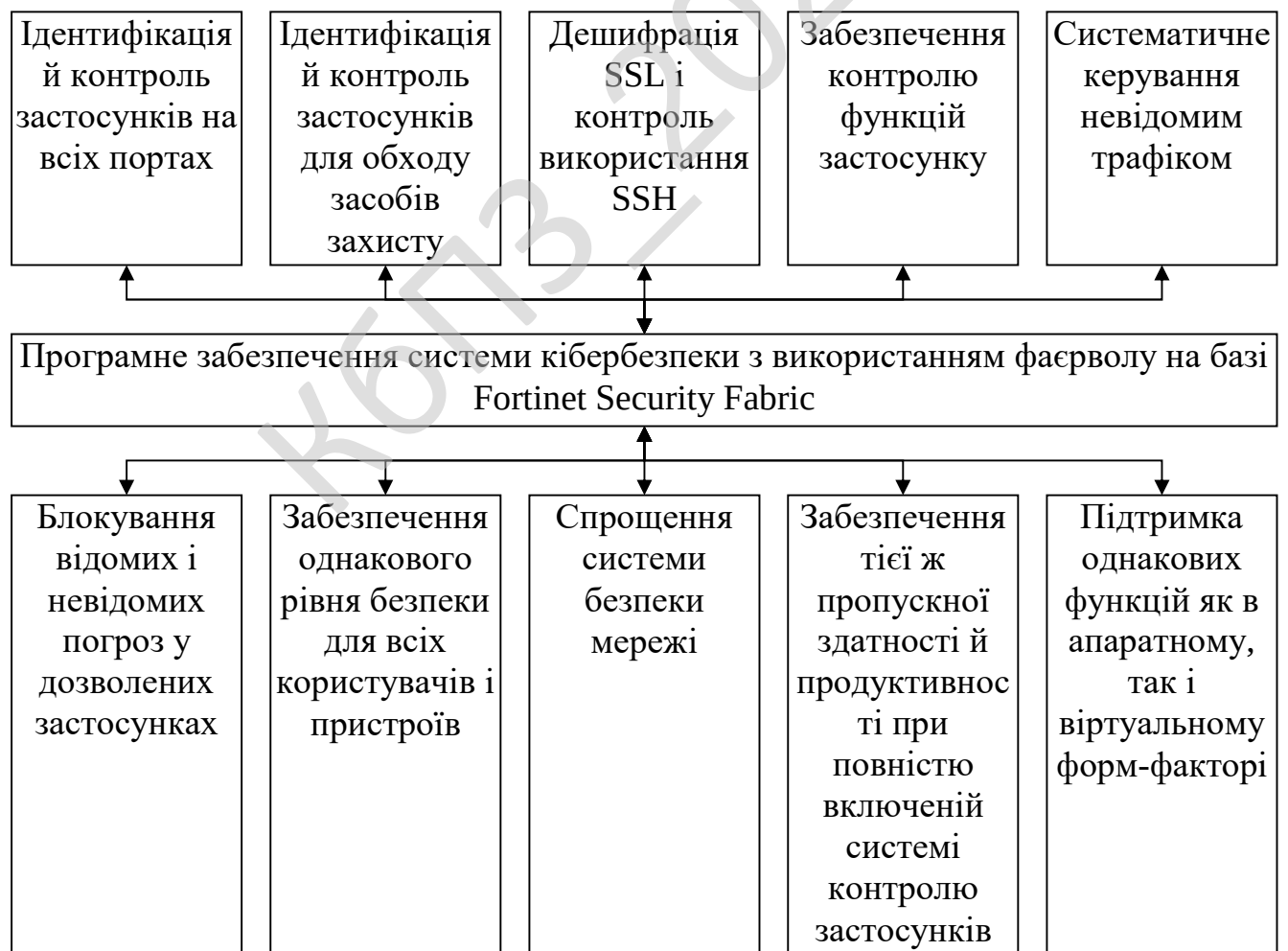


Рисунок 3.2 – Функціональна схема системи

Світ змінився, і компанії більше не можуть захищати свої ресурси за допомогою тих систем захисту від кібератак, які були дуже ефективними, коли в Інтернеті працювали застосунки тільки двох типів – засобу перегляду веб-сторінок і електронна пошта. Сьогодні потрібно набагато більше. У реалізованому в даній роботі фаєрволі на базі Fortinet Security Fabric, виділено 10 функцій.

1. Ідентифікація й контроль застосунків на всіх портах

Розроблювачі застосунків більше не прив'язуються до стандартних портів, протоколам і застосункам. Все більше число застосунків у вашій мережі можуть міняти порти або використовувати нестандартні порти (наприклад, застосунку обміну миттєвими повідомленнями). Крім того, все більше число користувачів уміє направляти роботу застосунків через нестандартні порти (наприклад, RDP, SSH). Щоб перейти до використання політик, орієнтованих на застосунки, а не на порти, необхідний міжмережевий екран, що допускає роботу будь-якого застосунку на кожному з портів.

2. Ідентифікація й контроль застосунків для обходу засобів захисту

Більшість організацій мають свої політики безпеки й застосовує механізми, що забезпечують їхнє дотримання. Для обходу таких засобів захисту, як міжмережеві екрани, використовуються зовнішні проксі, інструменти керування віддаленим сервером/робочим столом і застосунку, що дозволяють туннелювати трафік. Якщо ваша організація не буде мати можливості ідентифікувати й контролювати використання цих інструментів, вона не зможе реалізовувати політики безпеки й буде уразлива для тих самих кібератак, від яких теоретично повинні захищати засоби захисту. Реалізований у даній роботі фаєрвол на базі Fortinet Security Fabric повинен ефективно контролювати використання таких застосунків.

3. Дешифрація SSL і контроль використання SSH

Частка застосунків, широко використовуваних у мережі й використовуюча протокол SSL як засіб шифрування трафіку, у цей час досягає 25%. Усе більше

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		31

часте застосування HTTPS для багатьох затребуваних застосунків з високим ступенем ризику, а також можливість застосування SSL на багатьох веб-сайтах означає, що фахівці служб безпеки втрачають контроль над все більшою частиною мережевого трафіку. А якщо врахувати усе більш часте використання протоколу SSH технічно підкованими співробітниками, то частина непідвласного вам зашифрованого мережевого трафіку виявляється ще більше. Реалізований у даній роботі фаєрвол на базі Fortinet Security Fabric повинен забезпечувати дешифрацію й перевірку трафіку SSL на всіх портах. Він повинен бути досить гнучким у налаштуваннях, щоб не інспектувати весь SSL-трафік, якщо в цьому немає необхідності, і забезпечувати використання SSH тільки по призначенню, як визначено в політиці.

4. Забезпечення контролю функцій застосунку

Багато застосунків оснащені самими різними функціями, які представляють для вашої організації різний ступінь ризику й цінності. Можна привести безліч прикладів, пов'язаних з роботою кінцевих користувачів і цілих підприємств, наприклад WebEx з функцією WebEx Desktop Sharing і Google Mail з функцією Google Talk. Якщо робота вашої організації сильно залежить від схоронності інтелектуальної власності, то можливість доступу до робочих столів ззовні й можливість передачі файлів можуть представляти серйозні ризики з погляду інформаційної безпеки. Реалізований у даній роботі фаєрвол на базі Fortinet Security Fabric повинен безупинно оцінювати трафік, відслідковуючи будь-які зміни. Якщо в ході сеансу виникла нова функція або компонент, міжмережевий екран повинен уловити цю зміну й ініціювати перевірку на базі політики.

5. Систематичне керування невідомим трафіком

У невеликих кількостях, невідомий трафік є присутнім у кожній мережі. Це може бути користувацький застосунок, не ідентифіковане комерційний застосунок або погроза. Невідомий трафік будь-якого походження й типу являє собою серйозний ризик для бізнесу й безпеки. Блокування всього невідомого

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		32

трафіку стане перешкодою для розвитку бізнесу, а повний його дозвіл – дуже високий ризик. Збалансованим підходом стане систематичне застосування класифікації, аналізу й контролю трафіку на базі політик. Такий підхід дозволить зменшити ризик і усуне перешкоду для бізнес-процесів. Реалізований у даній роботі фаєрвол на базі Fortinet Security Fabric повинен виконувати класифікацію всього трафіку, легко визначати характеристики користувальницьких застосунків так, щоб вони переходили в категорію «відомих» застосунків у вашій політиці мережевої безпеки, аналізувати трафік, установлюючи, чи не є він погрозою, і забезпечувати прогнозовану візуалізацію й контроль трафіку, що залишається невідомим.

6. Блокування відомих і невідомих погроз у дозволених застосунках

Організації постійно впроваджують всі нові й нові застосунки, що підвищують ефективність бізнесу, розміщені як усередині локальної мережі, так і за її межами. Будь це SharePoint, Box.net, Google Docs, Microsoft Office365 або інший застосунок, здатне працювати через нестандартні порти, використовувати SSL або надавати спільний доступ до файлів. Такі застосунки підвищують ефективність бізнесу, але являють собою серйозний ризик для бізнесу й безпеки. Реалізований у даній роботі фаєрвол на базі Fortinet Security Fabric повинен забезпечувати безпечний дозвіл застосунків, але при цьому контролювати передачу файлів по їхньому типу, а також сканувати застосунки на наявність погроз, як відомих, так і невідомих, на всіх портах.

7. Забезпечення однакового рівня безпеки для всіх користувачів і пристроїв

Багато хто з користувачів працюють віддалено й вважають саме собою що розуміє, що вони можуть у будь-який момент підключитися до необхідних застосунків через Wi-Fi, 3G або будь-який інший доступний вид зв'язку. Незалежно від місця розташування користувача або типу використовуваного пристрою, вам потрібне забезпечення того самого стандарту контролю застосунків у мережі. Якщо реалізований у даній роботі фаєрвол на базі Fortinet

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		33

Security Fabric забезпечує візуалізацію й контроль застосунків тільки усередині локальної мережі організації, але не за її межами, він у будь-який момент може пропустити трафік, що представляє величезний ризик.

8. Спрощення системи безпеки мережі

Співробітники вашої служби мережевої безпеки змушені управляти величезною кількістю інформаційних потоків, безліччю політик безпеки й більшим числом інтерфейсів керування пристроями. Додавання нових компонентів ще більше ускладнить роботу вже перевантажених фахівців. Якщо припустити, що для типових міжмережевих екранів визначені тисячі правил, то з появою міжмережевого екрана нового покоління, що дозволяє ідентифікувати, контролювати, досліджувати й становити звіти по роботі застосунків, користувачів і передачі вмісту по мережі, життя ваших співробітників служби безпеки стане набагато простіше.

9. Забезпечення тієї ж пропускної здатності й продуктивності при повністю включеній системі контролю застосунків

Багато організацій ведуть постійну напружену роботу, намагаючись домогтися оптимального балансу між продуктивністю й безпекою. Нерідко активація функцій мережевої безпеки означає те, що пропускна здатність і продуктивність будуть істотно знижені. Якщо реалізований у даній роботі фаєрвол на базі Fortinet Security Fabric розроблений правильно, вам не буде потрібно боротися за цей баланс. Для виконання ресурсномістких обчислювальних завдань (таких як ідентифікація застосунків) у середовищі високоінтенсивного трафіку, що вимагає мінімізації затримок, реалізований у даній роботі фаєрвол на базі Fortinet Security Fabric повинен бути оснащений виділеними апаратними ресурсами, оптимізованими під відповідного функціонала.

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		34

10. Підтримка однакових функцій як в апаратному, так і віртуальному форм-факторі

Віртуалізація припускає величезні переваги, але, разом з тим, – і величезні проблеми в області безпеки. Традиційні міжмережеві екрани, що управляють портами й протоколами, із працею справляються із завданнями, пов'язаними з автоматизованим розгортанням і видаленням віртуальних машин. Динамічний характер віртуалізованого центра обробки даних припускає, що захист трафіку, що проходить у віртуальному середовищі (трафік «схід-захід»), повинна також здійснюватися динамічно й автоматично. Реалізований у даній роботі фаєрвол на базі Fortinet Security Fabric повинен підтримувати однаковий набір функціональних можливостей як в апаратному, так і віртуальному формі-факторі. Він повинен легко інтегруватися в середовище віртуалізації для забезпечення гарантованого застосування політик на рівні застосунків, з урахуванням постійної появи й видалення віртуальних машин.

Від вибору й роботи застосунків залежать, наскільки ефективно ваші користувачі будуть виконувати свою роботу й наскільки успішно вони будуть конкурувати з іншими в особистому й професійному плані. Ваші користувачі постійно впроваджують нові застосунки й технології, ненавмисно відкриваючи двері перед новими погрозами мережевої безпеки. Дозволити їм користуватися всім, що б вони не побажали, було б нерозумно.

У той же час, заборонивши впровадження нового, ви створите перешкоди для розвитку вашого бізнесу. Саме тому безпечний дозвіл застосунків стає усе більше важливим атрибутом будь-якої політики безпеки. Безпечний дозвіл застосунків буде найбільш ефективним при систематичному й послідовному визначенні завдань і сценаріїв їхнього використання, документальному оформленні необхідної моделі використання й формування відповідної політики, а також при реалізації цієї моделі використання за допомогою обраної технології. Без створення інфраструктури мережевої безпеки, здатної управляти подібним різноманіттям, ви не зможете забезпечити безпечний дозвіл необхідних

застосунків і управляти ризиками, із цими завданнями може успішно впоратися реалізований у даній роботі фаєрвол на базі Fortinet Security Fabric

Розглянувши усі блоки функціональної схеми перейдемо до розгляду діаграми взаємодії процесів, які відбуваються у системі.

3.4 Розробка діаграми процесів

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

Склад статистичної сукупності графічно може бути представлений як за допомогою абсолютних, так і відносних показників. Графічне зображення складу сукупності по абсолютними і відносними показниками сприяє проведенню більш глибокого аналізу і дозволяє проводити аналіз системи.

Діаграма взаємодії процесів використовується для візуалізації процесів обробки даних (структурне проектування). Для розробника вважається звичним спочатку креслити діаграму взаємодії процесів даних рівня контексту, завдяки чому буде показано взаємодію системи. Ця діаграма в подальшому підлягає уточненню шляхом деталізації процесів та потоків даних з метою показати систему що розробляється. При детальному її розгляді можна побачити як саме проходить взаємодія у розробленій системі. Використовується модель проектування, графічне представлення «потоків» даних в інформаційній системі.

Діаграми потоків даних містять чотири типи елементів:

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

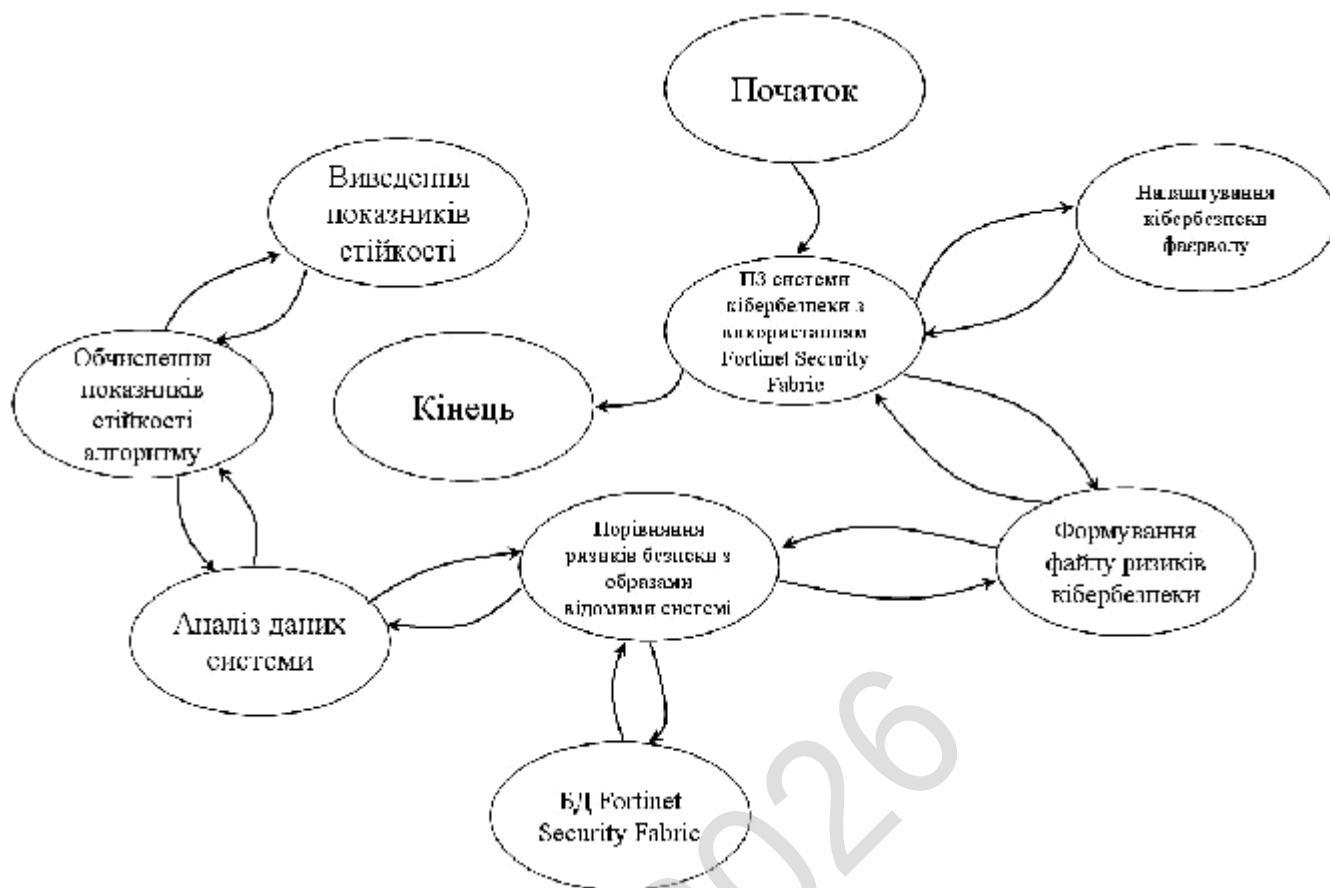


Рисунок 3.3 – Діаграма взаємодії процесів

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

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

4.1 Блок-схеми та опис алгоритмів функціонування системи

Розглянемо реалізацію бакалаврської дипломної роботи. Були проведені розрахунки і підібрані набори тестових даних для перевірки правильності реалізації проектних рішень. Було створено блок-схеми роботи системи. Перед їх розглядом необхідно провести роз'яснення який саме тип блок-схем використовується. Блок-схеми показують весь процес роботи системи з підсистемами та частково доказують правильність вибраних проектних рішень. Тому від точності і детальної блок-схеми залежить результат всієї програми. При виборі початкової точки відліку при побудові схем було враховано, що виходячи з вибору мови програмування і інших технічних засобів, програма буде об'єктно-орієнтована що вимагає високого рівня декомпозиції задач на класи.

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

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

Було використано підходи з використанням UML, це уніфікована мова моделювання, використовується у парадигмі об'єктно-орієнтованого програмування. Є невід'ємною частиною уніфікованого процесу розробки

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		38

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.

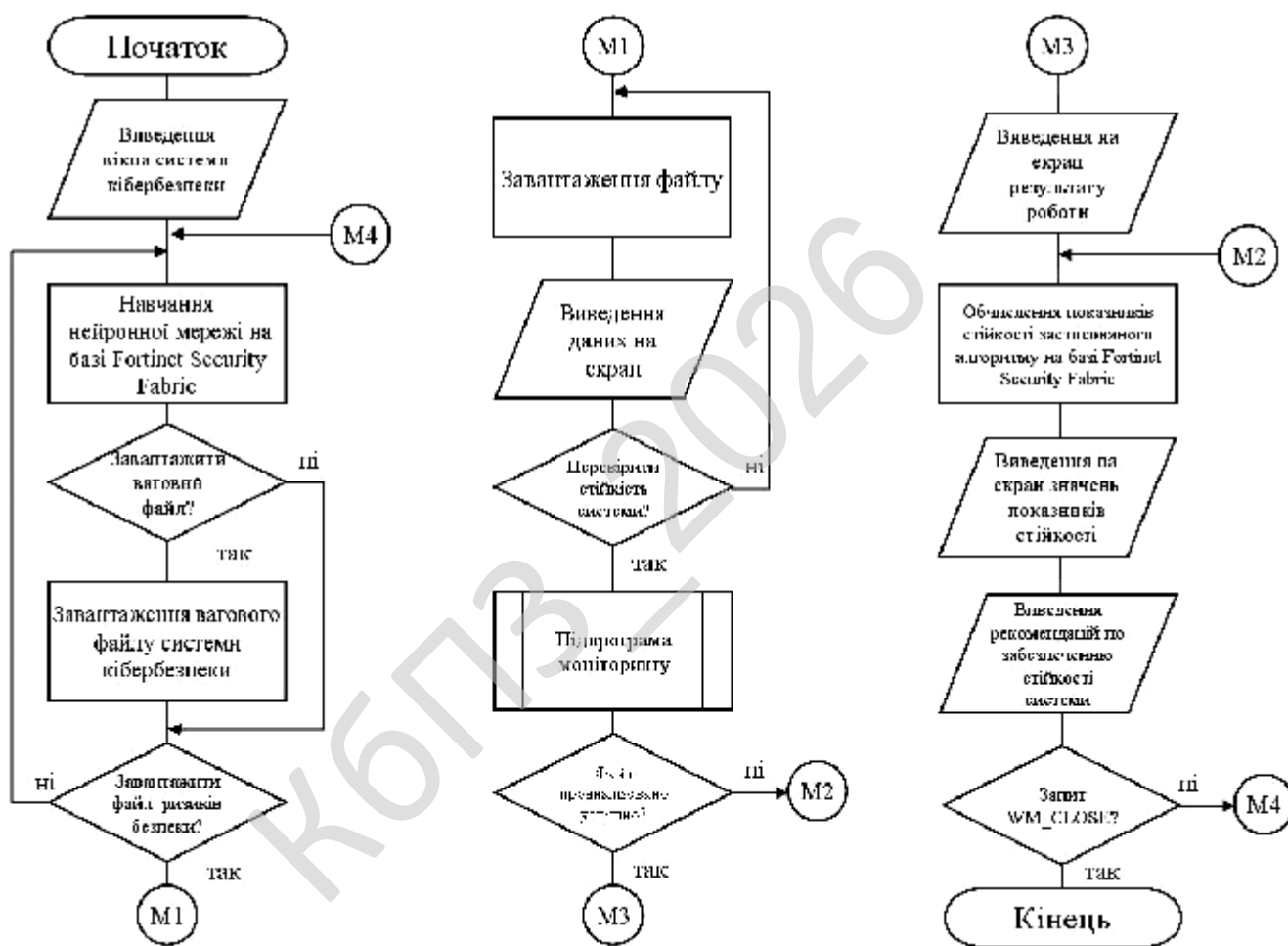


Рисунок 4.1 – Блок-схема основної програми

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.

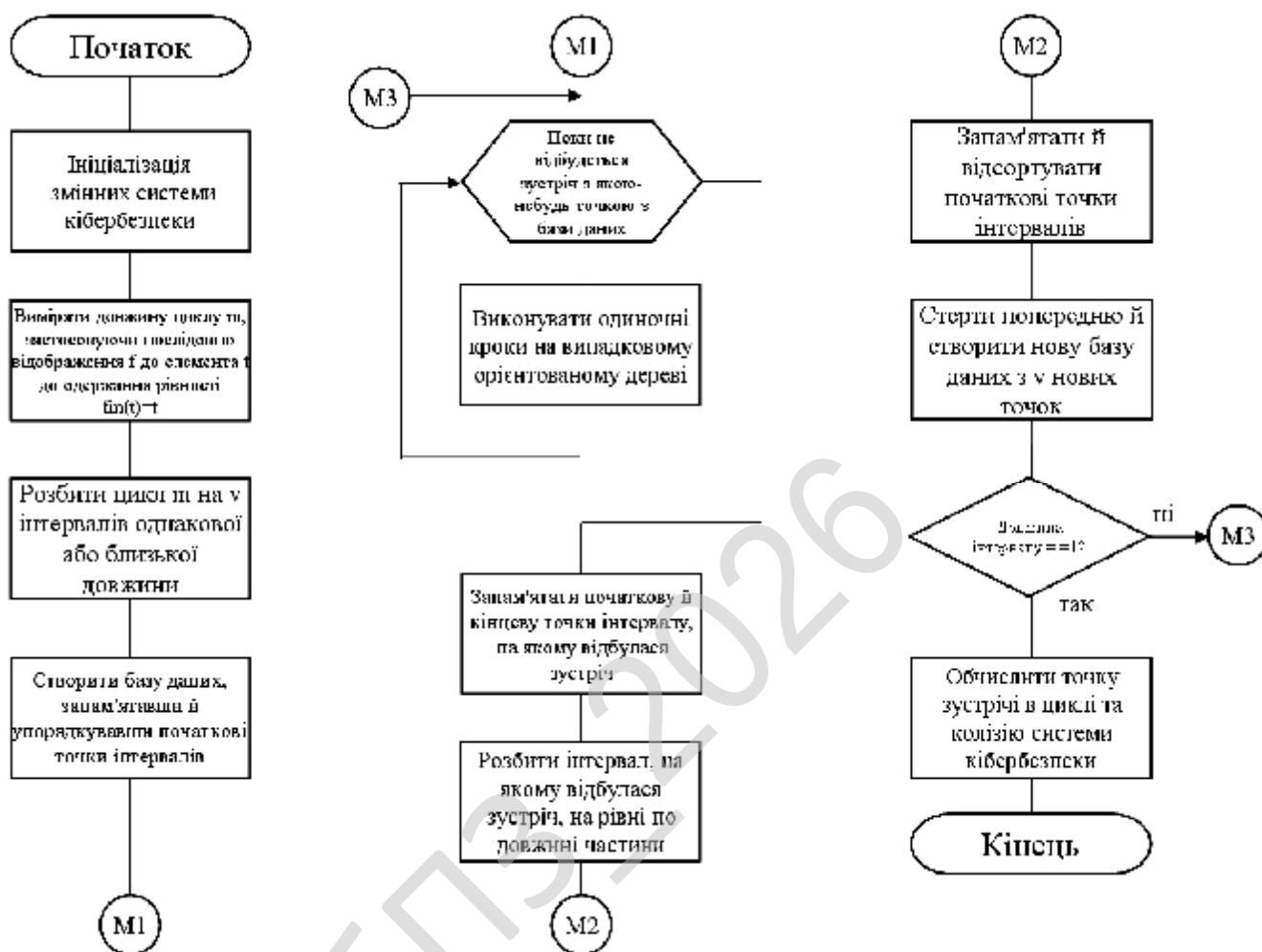


Рисунок 4.2 – Блок-схема роботи підпрограми

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 мережесих операцій введення-виведення і управління низлежащего транспортним протоколом.

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

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

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

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

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

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

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

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		41

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

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

Всі кінцеві вузли NETBIOS діляться на три типи:

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

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

NetBIOS забезпечує:

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

Розглянемо визначення API. Це прикладний програмний інтерфейс (Application Programming Interface, API) – набір визначень підпрограм, протоколів взаємодії та засобів для створення програмного забезпечення.

Спрощено – це набір чітко визначених методів для взаємодії різних компонентів. API надає розробнику засоби для швидкої розробки програмного забезпечення. API може бути для веб-базованих систем, операційних систем, баз даних, апаратного забезпечення, програмних бібліотек.

Одним з найпоширеніших призначень API є надання набору широко використовуваних функцій, наприклад для малювання вікна чи іконок на екрані. API є абстрактним поняттям – програмне забезпечення, що пропонує деякий API, часто називають реалізацією (implementation) даного API. У багатьох випадках API є частиною набору розробки програмного забезпечення, водночас, набір розробки може включати як API, так і інші інструменти/апаратне забезпечення, отже ці два терміни не є взаємозамінювані.

Високорівневі API часто програють у гнучкості. Виконання деяких функцій нижчого рівня стає набагато складнішим, або навіть неможливим.

В об'єктно-орієнтованих мовах, прикладний програмний інтерфейс зазвичай включає в себе опис набору визначень класу, з набором форм поведінки, пов'язаних з цими класами. Це абстрактне поняття пов'язане з реальними функціями, які надані або надаватимуться, класами, які реалізуються в методах класу.

Прикладний програмний інтерфейс в даному випадку можна розглядати як сукупність всіх методів, які публічно доступні в класах (зазвичай званий інтерфейс класу). Це означає, що прикладний програмний інтерфейс вказує методи, за допомогою яких взаємодіє з об'єктами, отриманими з визначень класів і обробляє їх.

У більш загальному плані можна визначити Прикладний Програмний Інтерфейс як сукупність усіх видів об'єктів, які можна вивести з визначення класу, і пов'язаних з ними можливих варіантів поведінки.

Наприклад: клас, що представляє Stack, може просто виставити публічно два методи Push() (для додавання нового елемента в стек) і Pop() (для вилучення останнього пункту, ідеально розташований на вершині стека).

У цьому випадку Прикладний Програмний Інтерфейс може бути інтерпретованим як два методи pop() і push(), або, більш широко, використовується варіант, коли можна використовувати елемент типу Stack, який реалізує поведінку стека, надаючи йому можливість для додавання / видалення

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		43

елементів з вершини. Друга інтерпретація видається більш доречною в дусі об'єктно-орієнтованого підходу.

Якість документації, пов'язаної з Прикладним Програмним Інтерфейсом, є часто ключовим фактором, що визначає його успішність з точки зору простоти використання.

ППІ, як правило, пов'язаний із бібліотеками програмного забезпечення: ППІ описує і вказує очікувану поведінку в той час, як бібліотека є фактичною реалізацією даного набору правил. Один ППІ може мати декілька реалізацій (або жодної, будучи абстрактним) у вигляді різних бібліотек, які мають такий же інтерфейс.

Прикладний програмний інтерфейс також може бути пов'язаним з платформами програмування: платформа може бути заснована на кількох бібліотеках реалізує декілька інтерфейсів ППІ, але на відміну від звичайного використання ППІ, доступ до поведінки вбудований в платформу опосередкований шляхом розширення його змісту новими класами і вставлений в саму платформу. Крім того, загальний потік управління програми може бути під контролем абонента.

Прикладний програмний інтерфейс може бути також реалізацією протоколу.

Коли ППІ реалізує протокол, він може бути заснованим на проксі-методах віддалених викликів, що засновані на протоколі зв'язку. Роль ППІ може заключатися саме в тому, щоб приховати деталі транспортного протоколу. Наприклад: RMI є ППІ, який реалізує протокол або JRMP IIOP як RMI-IIOP.

Протоколи, як правило, розподіляються між різними технологіями і зазвичай дозволяють різним технологіям обмінюватися інформацією, діючи як абстракція між двома світами. ППІ, як правило, є специфічним для конкретної технології: звідси, інтерфейси даної мови не можуть бути використані на інших мовах, якщо виклики функції не будуть перетворені з конкретної адаптації бібліотеки.

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		44

Деякі мови, серед яких такі, що працюють на віртуальних машинах (наприклад: мови, сумісні з NET CLI середовища CLR і JVM сумісних мов у віртуальній машині Java) можуть ділитися програмними інтерфейсами.

У цьому випадку віртуальна машина дозволяє мові взаємодії завдяки спільному знаменнику віртуальної машини, що абстрагується від конкретної мови, використовувати проміжний байт-код і його мову.

При використанні прикладного програмного інтерфейсу в контексті веб-розробки, як правило, ППП визначається набором повідомлень запиту HTTP, також визначається структура повідомлень-відповідей, зазвичай у розширенні мови розмітки XML або в форматі об'єктного запису JavaScript (JSON). У той час як прикладний програмний інтерфейс у Web історично був практично синонімом для веб-служби, останнім часом тенденція змінилась (так званий Web 2.0) на відхід від Simple Object Access Protocol (SOAP) на основі веб-сервісів і сервіс-орієнтованої архітектури (SOA) на більш прямі передачі репрезентативного стану (REST) стилів веб-ресурсів та ресурсів-орієнтованої архітектури (ROA).

Частина цієї тенденції пов'язана з рухом Семантичного веб-ресурсу до Опису Платформ (RDF), Концепції розвитку веб-технологій інженерних онтологій. Прикладні програмні інтерфейси у Web, що дозволяють комбінувати декількома прикладними програмними інтерфейсами в нові додатки називають гібридними.

Хоча я реалізовував програму сам, було використано підходи Scrum для саморозвитку та пришвидшенню розробки, розглянемо цей метод. Scrum – підхід управління проектами для гнучкої розробки програмного забезпечення. Скрам чітко робить акцент на якісному контролі процесу розробки.

Підхід вперше описали Гіротакі Такеучі та Ікуджіро Нонака в статті The New New Product Development Game (Гарвардський Діловий Огляд, січ–лют 1986). Вони відзначили, що проекти, над якими працюють невеликі, крос-функціональні команди, зазвичай систематично продукують кращі результати, і пояснили це, як «підхід регбі». У 1991 році ДеГрейс та Шталь у книжці Злі

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		45

проблеми, справедливі рішення послалися на цей підхід, як на Scrum (штовханина; сутичка навколо м'яча (у регбі)), спортивний термін, згаданий в статті Такеучі і Нонака. Кен Швабер на початку 1990-х використовував підхід який привів Scrum в його компанію.

Вперше метод Scrum було представлено на загальний огляд задокументованим, чітко сформульованим та описаним спільно Сазерлендом та Швабером на OOPSLA'96 в Остіні. Швабер та Сазерленд протягом наступних років працювали разом щоб обробити та описати весь їхній досвід та найкращі практичні зразки для індустрії в одне ціле, в ту методологію, що відома сьогодні як Scrum. Швабер об'єднав зусилля з Майком Бідлом в 2001, щоб детально описати метод в книжці Agile Software Development with SCRUM. Не зважаючи на те, що для Scrum нарікли долю управління проектами з розробки ПЗ, він може також використовуватися в роботі команд обслуговувань програмного забезпечення (software maintenance teams), або як підхід управління розробкою і супроводом програм: Scrum of Scrums.

Scrum – це кістяк процесу, який включає набір методів і попередньо визначених ролей. Головні дійові особи – ScrumMaster, той хто опікується процесами, веде їх і працює як керівник проекту, Власник Продукту, людина, що представляє інтереси кінцевих користувачів та інших зацікавлених в продукті сторін, та Команду, яка включає розробників.

Протягом кожного спринту, 15–30 денного періоду (тривалість визначається командою), працівники створюють функціональний ріст програмного забезпечення.

Набір можливостей, які імплементуються кожного спринту, приходять з етапу, що має назву product backlog (документація запитів на виконання робіт), який має найвищу пріоритетність за рівнем вимог до роботи, що повинна бути виконана.

Запити на виконання робіт (backlog items), що визначені протягом наради з планування спринту (sprint planning meeting), переміщуються в етап спринту.

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		46

Протягом цієї наради Власник Продукту інформує про завдання, які він хоче, аби були виконані. Тоді Команда визначає, скільки з бажаного вони можуть зробити, щоб завершити необхідні частини протягом наступного спринту. Протягом спринту команда виконує визначений фіксований список завдань (т.з. backlog items). Впродовж цього періоду ніхто не має права змінювати перелік запитів на виконання робіт, що слід розуміти, як заморожування вимог (requirements) протягом спринту.

Product backlog – це документ, який має список вимог до функціональності, які упорядковані згідно зі ступенем важливості. Product backlog представляє список того, що повинно бути реалізовано. Елементи цього списку називається «історіями» (user story) або елементами backlog–у (backlog items). Product backlog відкритий для редагування усім учасникам Scrum–процесу.

Обов'язкові поля:

1. ID – унікальний ідентифікатор, порядковий номер, який використовується для ідентифікації історій у разі їх перейменування.

2. Назва (Name) – стислий опис історії. Він повинен бути однозначним, щоб і розробники і product owner могли зрозуміти, про що йдеться і відрізнити одну історію від іншої.

3. Важливість (Importance) – ступінь важливості даної історії на погляд product owner 'а. Зазвичай являє собою натуральне число, іноді для цієї цілі використовуються числа Фібоначчі. Чим більше значення, тим більше пріоритет.

4. Попередня оцінка (initial estimate) – початкова оцінка об'єму робіт, необхідного для реалізації історії порівняно з іншими історіями. Вимірюється у story point'ах. Приблизно відповідає числу «ідеальних людино–днів».

5. Як продемонструвати (how to demo) – стисле пояснення того, як завершена задача буде продемонстрована у кінці спринта. Дане поле може являти собою код автоматизованого приймального тесту.

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		47

Додаткові поля. Іноді, також, використовуються додаткові поля у product backlog, в основному для того, щоб допомогти product owner'у визначитися з його пріоритетами.

Категорія (track). Наприклад, «панель управління» чи «оптимізація». За допомогою цього поля product owner може легко вибрати усі пункти категорії «оптимізація» і задати їм низький пріоритет.

Компоненти (components) – указує, які компоненти (наприклад, база даних, сервер, клієнт) будуть зачеплені при реалізації історії. Дане поле складається з групи checkbox'ів, які відмічаються, якщо відповідні компоненти потребують змін.

Ініціатор запиту (requestor). Product owner може захотіти зберігати інформацію про усіх замовників, зацікавлених у даній задачі. Це потрібно для того, щоб тримати їх у курсі діла про хід виконання робіт.

ID у системі обліку помилок (bug tracking ID) – якщо ви використовуєте окрему систему обліку помилок, тоді у описі історії корисно зберігати посилання на всі дефекти, які до неї відносяться.

Sprint backlog – містить функціональність, обрану Product Owner із Product Backlog. Всі функції розбиті по задачах, кожна з яких оцінюється командою. Кожен день команда оцінює об'єм роботи, який необхідно провести для завершення задачі.

Burndown chart – показує, скільки вже виконано і скільки ще залишається зробити.

Планування спринта (Sprint Planning Meeting)

Проходить на початку нової ітерації Спринта:

– Із Product Backlog обираються задачі, зобов'язання по виконанню яких за спринт приймає на себе команда;

– На основі обраних задач створюється Sprint Backlog. Кожна задача оцінюється у ідеальних людино-годинах;

- Рішення задачі не повинно займати більше 12 годин або одного дня. При необхідності задача розбивається на підзадачі;
- Обговорюється та визначається, яким чином буде реалізовано цей об'єм робіт;
- Тривалість наради обмежена зверху 4–8 годинами в залежності від тривалості ітерації, досвіду команди тощо;
- (перша частина наради) Беруть участь Product Owner + Команда: обирають задачі із Product Backlog;
- (друга частина наради) Бере участь лише команда: обговорюють технічні деталі реалізації, наповнюють Sprint Backlog.

Щоденна нарада (Daily Scrum Meeting)

Відбувається кожен день протягом спринта. Є «пульсом» ходу спринта. Нараді властиві наступні обмеження:

- починається точно вчасно;
 - всі можуть спостерігати, але говорять тільки обрані;
 - триває не більш ніж 15 хвилин;
 - проводиться в одному і тому ж місці протягом одного спринта.
- Протягом наради кожен член команди відповідає на 3 запитання:
- Що зроблено з моменту попередньої щоденної наради?
 - Що буде зроблено з моменту поточної наради до наступної?
 - Які проблеми заважають досягненню цілей спринта? (Над рішенням цих проблем працює ScrumMaster. Зазвичай це рішення проходить за рамками щоденної наради і у складі осіб, що безпосередньо займаються даною перешкодою.)

Демонстрація (Sprint Review Meeting):

- Проходить у кінці ітерації (спринта).
- Команда демонструє внесок функціональності до продукту всім зацікавленим особам.
- Залучається максимальна кількість глядачів.

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		49

- Усі члени команди беруть участь у демонстрації (одна людина на демонстрацію або кожен показує, що зробив за спринт).
- Обмежена 4-ма годинами в залежності від тривалості ітерації і змін у продукті.

Ретроспектива (Sprint Retrospective):

- Члени команди висловлюють свою думку про минулий спринт.
- Відповідають на два основних запитання: Що було зроблено добре у минулому спринті?; Що потрібно покращити в наступному?.
- Виконують покращення процесу розробки (вирішують питання та фіксують вдалі рішення).
- Обмежена 1–3ма годинами.

4.2 Захист розробленого програмного забезпечення

Для захисту розробленого програмного забезпечення запропоновано використовувати алгоритм Blowfish, який є симетричним алгоритмом шифрування, тобто таким, у якому ключ шифрування дорівнює ключу дешифрування. Він є мережею Фейштеля, у якій кількість ітерацій дорівнює 16. Довжина блоку дорівнює 64 бітам, ключ може мати будь-яку довжину в межах 448 біт. Хоча перед початком будь-якого шифрування виконується складна фаза ініціалізації, саме шифрування даних виконується досить швидко.

Алгоритм призначений в основному для застосунків, у яких ключ міняється нечасто, до того ж існує фаза початкового рукостискання, під час якої відбувається автентифікація сторін і узгодження загальних параметрів і секретів. При реалізації на 32-бітних мікропроцесорах з більшим кешем даних Blowfish значно швидше DES.

Алгоритм складається із двох частин: розширення ключа й шифрування даних. Розширення ключа перетворює ключ довжиною, принаймні, 448 біт у кілька масивів підключів загальною довжиною 4168 байт.

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		50

В основі алгоритму лежить мережа Фейштеля з 16 ітераціями. Кожна ітерація складається з перестановки, що залежить від ключа, і підстановки, що залежить від ключа й даних. Операціями є XOR і додавання 32-бітних слів.

Blowfish використовує велику кількість підключів. Ці ключі повинні бути обчислені заздалегідь, до початку будь-якого шифрування або дешифрування даних. Елементи алгоритму:

1. P – масив, що складається з вісімнадцяти 32-бітних підключів: $P_1, P_2, \dots, P_{18}$.

2. Чотири 32-бітних S-boxes с 256 входами кожний. Перший індекс означає номер S-бокс, другий індекс – номер входу.

3. $S_{1,0}, S_{1,1}, \dots S_{1,255}$;

4. $S_{2,0}, S_{2,1}, \dots S_{2,255}$;

5. $S_{3,0}, S_{3,1}, \dots S_{3,255}$;

6. $S_{4,0}, S_{4,1}, \dots S_{4,255}$;

Шифрування

Входом є 64-бітний елемент даних X , що ділиться на дві 32-бітні половини, X_l і X_r .

$$X_l = X_l \text{ XOR } P_i$$

$$X_r = F(X_l) \text{ XOR } X_r$$

Swap X_l and X_r

Функція F

Розділити X_l на чотири 8-бітних елементи A, B, C, D .

$$F(X_l) = ((S_{1,A} + S_{2,B} \bmod 2^{32}) \text{ XOR } S_{3,C}) + S_{4,D} \bmod 2^{32}$$

Дешифрування відрізняється від шифрування тим, що P_i використовуються у зворотному порядку.

Генерація підключів

Підключи обчислюються з використанням самого алгоритму Blowfish.

1. Ініціалізувати перший P -масив і чотири S-boxes фіксовані рядки.

2. Виконати операцію XOR P_1 з першими 32 бітами ключа, операцію XOR P_2 із другими 32 бітами ключа й т.д. Повторювати цикл доти, поки весь P -масив не буде побітово складний з усіма бітами ключа. Для коротких ключів виконується конкатенація ключа із самим собою.

3. Зашифрувати нульовий рядок алгоритмом Blowfish, використовуючи підключи, описані в пунктах (1) і (2).

4. Замінити P_1 і P_2 виходом, отриманим на кроці (3).

5. Зашифрувати вихід кроку (3), використовуючи алгоритм Blowfish з модифікованими підключами.

6. Замінити P_3 і P_4 виходом, отриманим на кроці (5).

7. Продовжити процес, замінюючи всі елементи P -масиву, а потім всі чотири S -boxes, виходами відповідним чином модифікованого алгоритму Blowfish.

Для створення всіх підключів потрібна 521 ітерація.

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		52

5 МЕТОДИКА ВПРОВАДЖЕННЯ СИСТЕМИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ

На рисунку 5.1 зображено розроблене у бакалаврської дипломної роботі ПЗ системи кібербезпеки з використанням фаєрволу на базі Fortinet Security Fabric. З рисунку можна побачити що інтерфейс головного вікна розподілено на наступні функціональні розділи:

- Функціональних кнопок ПЗ.
- Навігаційного меню яке викликається натисканням правої клавіші маніпулятора миші.
- Верхнього меню: Файл; Налаштування; Дані Fortinet Security Fabric; Довідка.
- Розділу обрання групи.
- Розділу виведення результату роботи системи.

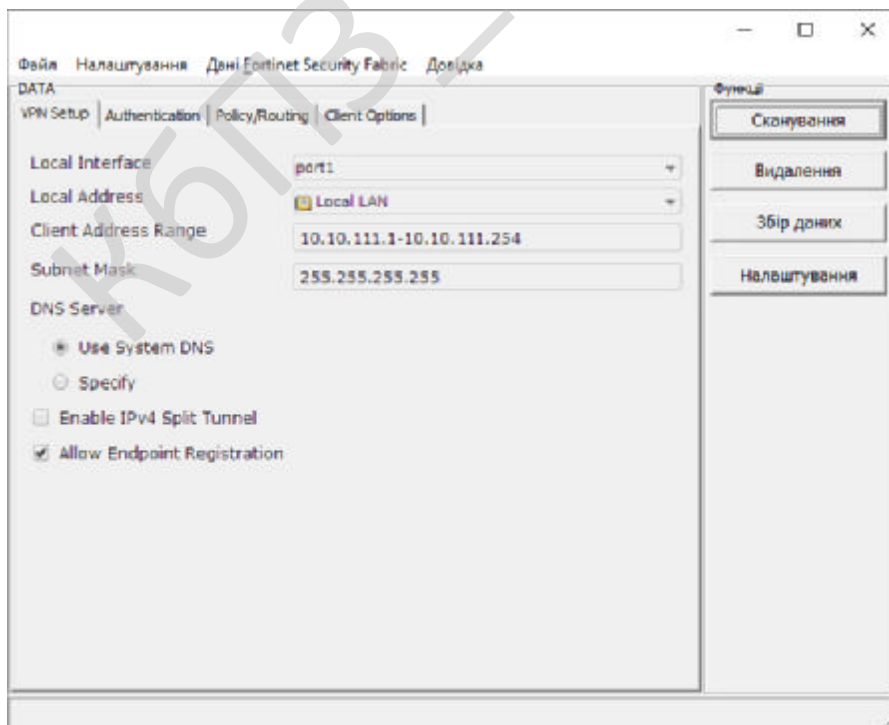


Рисунок 5.1 – Головне вікно ПЗ

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

На рисунку 5.2 зображено авторські дані розробленого програмного забезпечення.

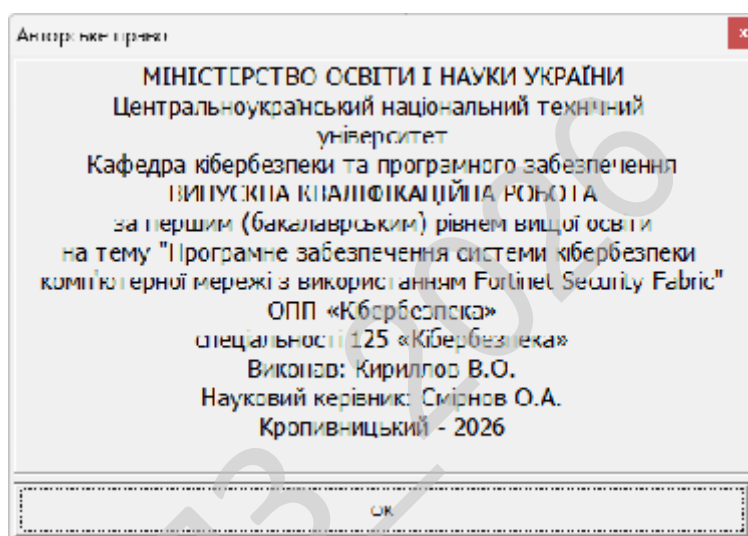


Рисунок 5.2 – Авторське право

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

Загалом процес розгортання складається з кількох взаємопов'язаних дій із можливими переходами між ними. Ця активність може відбуватися як з боку виробника так і з боку споживача. Оскільки кожна програмна система є

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		54

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

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		55

в ІТ рішення за принципом найбільшої корисності для більшості учасників. Відсоток таких процедур щодо загального обсягу автоматизації може бути невеликий, але це надає процесу побудови рішення вагу в організації за рахунок збільшення його необхідності.

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

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

Проводилась оцінка:

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

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

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

Проводилось тестування 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.

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

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		57

користувачам безоплатно. Звичайно користувач платить тільки за час завантаження файлів через Інтернет або за носій (CD диск, флешку, ключ). Протягом певного терміну, що становить зазвичай тридцять днів, він може користуватися програмою, тестувати її, освоювати її можливості.

Якщо після закінчення цього терміну користувач вирішить продовжити використання ПЗ, він зобов'язаний купити його (zareestruvatisya), zaplativshi avtorovi певну суму.

В іншому випадку користувач повинен припинити використання ПЗ та видалити його зі свого комп'ютера.

К6ПЗ_2026

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		58

6 ОСНОВНІ ВИСНОВКИ

Програмне забезпечення, створене в результаті виконання випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти, призначено для системи кібербезпеки комп'ютерної мережі з використанням Fortinet Security Fabric.

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

Рішення завдання полягало у вирішенні наступних задач:

- Був проведений огляд існуючих систем комп'ютерної мережі з використанням Fortinet Security Fabric.
- Досліджена система комп'ютерної мережі з використанням Fortinet Security Fabric.
- На основі отриманих результатів досліджень створена програмна реалізація системи кібербезпеки комп'ютерної мережі з використанням Fortinet Security Fabric.

Розроблені під час виконання випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання комп'ютерної мережі з використанням Fortinet Security Fabric.

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 комп'ютерної мережі з використанням Fortinet Security

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		59

Fabric. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне 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 Blowfish.

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-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		60

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Josh Armitage. Cloud Native Security Cookbook. O'Reilly Media. 2022. 516 p.
2. Massimo Bertaccini. Cryptography Algorithms. Packt Publishing. 2022. 358 p.
3. Alyssa Miller. Cybersecurity Career Guide. Manning Publications. 2022. 368 p.
4. Awais Rashid, Howard Chivers, George Danezis, Emil Lupu, Andrew Martin. CyBOK The Cyber Security Body of Knowledge. The National Cyber Security Centre. 2019. 854 p.
5. Loren Kohnfelder. Designing Secure Software. No Starch Press. 2022. 332 p.
6. Samir Kumar Rakshit. Ethical Hacker's Penetration Testing Guide. BPB Online. 2022. 509 p.
7. Corey J. Ball. Hacking APIs. No Starch Press. 2022. 353 p.
8. Kevin Beaver. Hacking for Dummies. John Wiley & Sons. 2022. 419 p.
9. Mark S. Merkow. Practical Security for Agile and DevOps. CRC Press. 2022. 236 p.
10. Derek Fisher. Application Security Program Handbook. Manning Publications. 2021. 155 p.
11. Cameron Wyatt PH.D. Kali Linux Tutorial. Independently published. 2021. 60 p.
12. Kuznetsov O., Frontoni E., Arnesano M., Smirnov O., Khruskov B. «Biometric Authentication in TinyML: Opportunities and Challenges». *Tiny Machine Learning: Design Principles and Applications*, 2026, pp. 587-633.
13. 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.
14. Chulinda L., Smirnov O., Shapenko L., Ustynova I., Bohatiuk I., Kelyp S. «The role of innovation in ensuring the safety of international civil aviation». *Ceur Workshop Proceedings*, 2025, 4024, pp. 530–542.

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		61

15. 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., Корчинский В.В., Кудирко В.М., Фесенко А.О.; за заг. ред. В.М. Петрика, М.М. Присяжнюка.– К.: Видавничий центр “Кафедра”, 2025.– 320 с.

16. 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

17. 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.

18. 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.

19. 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.

20. 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.

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		62

21. 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.

22. 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.

23. 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.

24. 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.

25. 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.

26. 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.

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

28. 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.

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

30. 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

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

32. 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.

33. 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., Vuppalapati, 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.

34. 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.

35. 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.

36. 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.

37. 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.

38. 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.

39. 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,

40. 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.

41. 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.

					ВКРБ-125.26.0031.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		65

42. 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.

43. 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.

44. 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.

45. 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

46. 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.

47. 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.

48. 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.

49. 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.

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

51. 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.

52. 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.

53. 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.

54. 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.

55. 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.