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

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

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА
за другим (магістерським) рівнем вищої освіти
на тему
“Дослідження та програмна реалізація системи мережевого антивірусного захисту віртуалізованої інфраструктури дата-центру на базі технологій SDN/NFV”

Виконав здобувач вищої освіти
ІІ курсу, групи КІ-25М
ОПП «Комп’ютерна інженерія»
спеціальності F7 «Комп’ютерна інженерія»
_____ Крутіков О.А.
«____» _____ 2026 р.

Керівник проекту
кандидат технічних наук, доцент
_____ Буравченко К.О.
«____» _____ 2026 р.

Нормоконтроль проекту
_____ Коваленко А.С.
«____» _____ 2026 р.

Рецензент _____
_____

Підписано КЕП
Центральноукраїнський національний технічний університет
Крутіков Олександр Андрійович
Сертифікат: 18DF2C9B93CEA2040400000002B0C75010AC37A06
Дійсний з 24.11.2026 16:21:17 по 24.11.2027 16:21:16

Центральноукраїнський національний технічний університет

Факультет *Механіко-технологічний*

Кафедра *Кібербезпеки та програмного забезпечення*

Рівень вищої освіти *магістр*

Галузь знань _F_____*"*Інформаційні технології*"*_____

Спеціальність F7 *"*Комп'ютерна інженерія*"*

Освітньо-професійна (освітньо-наукова) програма _*"*Комп'ютерна інженерія*"*_

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

ЗАВДАННЯ НА ВИПУСКНУ КВАЛІФІКАЦІЙНУ РОБОТУ ЗА ДРУГИМ (МАГІСТЕРСЬКИМ) РІВНЕМ ВИЩОЇ ОСВІТИ ЗДОБУВАЧА ВИЩОЇ ОСВІТИ

Крутікову Олександру Андрійовичу

(прізвище, ім'я, по батькові)

1. Тема роботи *Дослідження та програмна реалізація системи мережевого антивірусного захисту віртуалізованої інфраструктури дата-центру на базі технологій SDN/NFV*

2. Керівник роботи *Буравченко Костянтин Олегович, кандидат технічних наук, доцент*

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

затверджені наказом вищого навчального закладу № 41-13 від 17.08.2026 року

3. Строк подання студентом роботи до захисту *2.12.2026 р.*

4. Мета та завдання випускної кваліфікаційної роботи*: Метою розробки є дослідження та програмна реалізація системи мережевого антивірусного захисту віртуалізованої інфраструктури дата-центру на базі технологій SDN/NFV*

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

1. Призначення та область використання.	*5. Впровадження системи в промислову експлуатацію*
2. Перегляд аналогічних існуючих систем.	*6. Наукова новизна.*
3. Опис і обґрунтування проектних рішень.	*7. Заходи з охорони праці та техніки безпеки.*
4. Етапи програмування системи.	*8. Висновки.*

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

Наукова новизна	*1 аркуш*
Структурна схема системи	*1 аркуш*
Функціональна схема системи	*1 аркуш*
Діаграма процесів	*1 аркуш*
Блок-схема алгоритму роботи додатку	*2 аркуша*

7. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Марченко К.М., к.т.н., доцент	06.10.2026	16.11.2026

8. Дата видачі завдання « 1 » вересня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти	Строк виконання етапів випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти	Примітка
1.	Аналіз існуючих систем	10.10.2026 р.	
2.	Постановка задачі, оформлення ТЗ	15.10.2026 р.	
3.	Розробка моделі компонента	20.10.2026 р.	
4.	Розробка структур даних	25.10.2026 р.	
5.	Розробка алгоритмів системи	30.10.2026 р.	
6.	Програмування алгоритмів	10.11.2026 р.	
7.	Розрахунки з охорони праці та техніки безпеки	15.11.2026 р.	
8.	Оформлення ПЗ	17.11.2026 р.	
9.	Попередній захист роботи	2.12.2026 р.	

Дата видачі завдання
« 1 » вересня 2026 р.

Підпис керівника

_____ _____
(прізвище та ініціали)

Завдання прийнято до виконання
« 1 » вересня 2026 р.

Підпис здобувача

_____ _____
(прізвище та ініціали)

АНОТАЦІЯ

Крутіков О.А. Дослідження та програмна реалізація системи мережевого антивірусного захисту віртуалізованої інфраструктури дата-центру на базі технологій SDN/NFV. F7 Комп'ютерна інженерія. Центральноукраїнський національний технічний університет. Кропивницький. 2026.

В даній випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти розроблено програмне забезпечення, яке призначено для системи мережевого антивірусного захисту віртуалізованої інфраструктури дата-центру на базі технологій SDN/NFV.

Метою розробки є дослідження та програмна реалізація системи мережевого антивірусного захисту віртуалізованої інфраструктури дата-центру на базі технологій SDN/NFV.

Об'єктом дослідження є процес мережевого антивірусного захисту віртуалізованої інфраструктури дата-центру на базі технологій SDN/NFV.

Предметом дослідження є методи мережевого антивірусного захисту віртуалізованої інфраструктури дата-центру на базі технологій SDN/NFV.

Методи дослідження базуються на методах побудови комп'ютерних мереж, методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Результат роботи – програмна реалізація системи мережевого антивірусного захисту віртуалізованої інфраструктури дата-центру на базі технологій SDN/NFV.

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

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

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

Програму розроблено в середовищі Python.

Ключові слова: комп'ютерна інженерія, комп'ютерна мережа, антивірусний захист, віртуалізована інфраструктура, дата-центр, SDN/NFV

ABSTRACT

Krutikov O.A. Research and Software Implementation of a Network Antivirus Protection System for a Virtualized Data Center Infrastructure Based on SDN/NFV Technologies. F7 Computer Engineering. Central Ukrainian National Technical University. Kropyvnytskyi. 2026.

In this final qualification thesis for the second (master's) level of higher education, software has been developed for a network antivirus protection system designed for the virtualized infrastructure of a data center, based on SDN/NFV technologies.

The objective of this development is the research and software implementation of a network antivirus protection system for a virtualized data center infrastructure based on SDN/NFV technologies.

The object of the research is the process of network antivirus protection for a virtualized data center infrastructure based on SDN/NFV technologies.

The subject of the research consists of methods for network antivirus protection of a virtualized data center infrastructure based on SDN/NFV technologies.

The research methodology is based on approaches to computer network construction, information security, mathematical statistics, and software development.

The result of the work is the software implementation of a network antivirus protection system for a virtualized data center infrastructure based on SDN/NFV technologies.

During the development of the software model, an analysis of existing hardware and software tools was conducted. All components of the developed software are described in full detail. A user-friendly interface has been developed. Instructions for using the software tools are provided.

The program can be used on PCs running the Windows 10/11 operating system.

The program was developed in a Python environment.

Keywords: computer engineering, computer network, antivirus protection, virtualized infrastructure, data center, SDN/NFV

ВІДОМІСТЬ ПРОЕКТУ

		Текстові документи			
1	А4	Пояснювальна записка	95	–	
2	А4	Робоча програма	45	–	Додаток А
		Графічні документи			
3	А4	Наукова новизна	1	–	
4	А4	Структурна схема	1	–	
5	А4	Функціональна схема роботи системи	1	–	
6	А4	Діаграма взаємодії процесів	1	–	
7	А4	Блок-схема основної програми	1	–	
8	А4	Блок-схема роботи підпрограми	1	–	

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ 9
ВСТУП..... 10
1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ 12
1.1 Призначення системи..... 12
1.2 Область застосування 14
2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ 16
2.1 Огляд існуючих систем, технологій, архітектур та програмних рішень за профілем теми випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти..... 16
2.2 Обґрунтування вибору засобів для побудови системи та мови програмування 32
2.3 Розгорнута постановка завдання 34
3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ 36
3.1 Опис функціонування системи 36
3.2 Розробка структурної схеми..... 42
3.3 Розробка функціональної схеми 53
3.4 Розробка діаграми процесів 55
4 РЕАЛІЗАЦІЯ РОБОТИ. РОЗРАХУНКИ І ЕКСПЕРИМЕНТАЛЬНІ ДАНІ, ЩО ПІДТВЕРДЖУЮТЬ ВІРНІСТЬ ПРОЕКТНИХ ТА ПРОГРАМНИХ РІШЕНЬ 57
4.1 Розробка блок-схем та опис алгоритмів функціонування системи 57
5 ВПРОВАДЖЕННЯ СИСТЕМИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ..... 73
6 НАУКОВА НОВИЗНА 76

7 ЗАХОДИ З ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ 77
7.1 Вступ 77
7.2 Шкідливі і небезпечні фактори при роботі з комп’ютером 78
7.3 Аналіз санітарно-гігієнічних умов праці на робочому місці програміста ... 79
7.4 Розробка заходів з умов поліпшення охорони праці 82
7.5 Розрахункова частина 83
8 ОСНОВНІ ВИСНОВКИ 86
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 88

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

КМ	–	комп’ютерна мережа
КСАЗ	–	комплексна система антивірусного захисту
МЕ	–	міжмережний екран
ПЗ	–	програмне забезпечення
ПК	–	персональний комп’ютер
ACL	–	Access Control List
FTP	–	File Transfer Protocol
http	–	HyperText Transfer Protocol
POP3	–	Post Office Protocol Version 3
SMTP	–	Simple Mail Transfer Protocol
VLAN	–	Virtual Local Area Network

ВСТУП

Актуальність теми. Програмно-визначена мережа (SDN) – це новий тип мережевої архітектури, який має переваги над традиційними мережами. Для SDN безпека є базовим питанням. Контролер SDN отримав значну увагу в дослідженнях безпеки SDN. Дослідники зазвичай призначають завдання безпеки контролерам SDN, але це створює важке навантаження на контролер SDN та призводить до зниження стабільності системи. У даній роботі пропонується архітектуру захисту безпеки на основі SDN/NFV. Тим часом, пул віртуальних машин функцій безпеки розроблено на рівні інфраструктури архітектури. Він може автоматично створювати віртуальні машини та керувати їх IP-адресами, що покращує гнучкість та розширюваність архітектури. Крім того, було запроваджено алгоритм композиції функцій на основі Trie (FCT).

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи мережевого антивірусного захисту віртуалізованої інфраструктури дата-центру на базі технологій SDN/NFV.

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

– Огляд існуючих систем мережевого антивірусного захисту віртуалізованої інфраструктури дата-центру на базі технологій SDN/NFV.

– Дослідження системи мережевого антивірусного захисту віртуалізованої інфраструктури дата-центру на базі технологій SDN/NFV.

– Програмна реалізація системи мережевого антивірусного захисту віртуалізованої інфраструктури дата-центру на базі технологій SDN/NFV.

Об’єктом дослідження є процес мережевого антивірусного захисту віртуалізованої інфраструктури дата-центру на базі технологій SDN/NFV.

Предметом дослідження є методи мережевого антивірусного захисту віртуалізованої інфраструктури дата-центру на базі технологій SDN/NFV.

Методи дослідження базуються на методах побудови комп’ютерних мереж, методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Наукова новизна отриманих результатів. У процесі рішення завдань, обумовлених цілями дослідження, отримані наступні результати:

– Удосконалено метод мережевого антивірусного захисту віртуалізованої інфраструктури дата-центру на базі технологій SDN/NFV.

– Розроблено вітчизняний продукт мережевого антивірусного захисту віртуалізованої інфраструктури дата-центру на базі технологій SDN/NFV, який має більш широкі можливості, на відміну від існуючих аналогів.

Практична цінність отриманих результатів полягає в тому, що розроблені алгоритми дозволяють успішно вирішувати задачі мережевого антивірусного захисту віртуалізованої інфраструктури дата-центру на базі технологій SDN/NFV.

Достовірність наукових результатів підтверджена теоретичними викладеннями, даними комп'ютерного моделювання, коректними дослідженнями параметрів на функціонуючій обчислювальній мережі, а також відповідністю отриманих результатів окремим результатам, наведеним у науковій літературі.

Робота апробована на LVIII науково-технічній конференції здобувачів вищої освіти «Наука-виробництву», основні положення випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти надруковані у статті збірника праць молодих науковців ЦНТУ, випуск №17.

Таким чином, виходячи з вищеперерахованого, дослідження та програмна реалізація системи мережевого антивірусного захисту віртуалізованої інфраструктури дата-центру на базі технологій SDN/NFV, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти.

1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ

1.1 Призначення системи

За останні роки ландшафт надання послуг зазнав змін парадигми, зумовленої технологічним прогресом та зміною потреб користувачів. Застарілі мережі, розроблені для простішої ери, погано оснащені для вирішення нових мережевих проблем, пов'язаних з цією трансформацією. Повсюдне впровадження хмарних обчислень, віртуалізації серверів, середовищ BYOD (Bring Your Own Device) та експоненціальне зростання великих даних та штучного інтелекту (ШІ) є прикладами нових парадигм, що вимагають розширених мережевих можливостей [1].

Впровадження будь-яких змін у звичайних мережах, таких як додавання, переміщення або видалення мережевого пристрою, вимагає перегляду всієї конфігурації мережі. Мережі складаються з кількох пристроїв (комутаторів, маршрутизаторів, брандмауерів, балансувальників навантаження тощо), часто від різних постачальників, що призводить до складних конфігурацій, які потребують тривалого часу для впровадження. Потреби бізнесу, що постійно змінюються, вимагають розширених мережевих можливостей, таких як збільшення пропускної здатності, контроль якості обслуговування (QoS) та конвергенція голосового, інформаційного та відеотрафіку. Застарілим мережам бракує динамічної гнучкості, необхідної для ефективного управління цими вимогами [2].

Крім того, масштабованість є основною перешкодою для застарілих мереж. Мережі зазвичай розширюються, щоб задовольнити нових користувачів та їхні потреби в даних, але це зростання часто випереджає потужність застарілих архітектур. Це призводить до того, що мережа стає дедалі перевантаженішою та ненадійнішою. Потреба в новому рівні абстракції є очевидною, який би забезпечував безперешкодне додавання нових пристроїв,

мінімізуючи навантаження на мережевих адміністраторів.

Ще однією значною проблемою є неможливість встановити узгоджені політики в мережі. Підтримка політик безпеки або QoS у застарілих мережах є складним завданням. Кожна зміна мережі вимагає ручного налаштування численних пристроїв, що робить її схильною до помилок та невідповідностей. У середовищах BYOD (використання власних пристроїв), де співробітники використовують особисті мобільні пристрої, забезпечення дотримання політик стає ще складнішим, що збільшує вразливість корпоративної мережі до порушень безпеки. Зростання кількості мобільних пристроїв та користувачів у поєднанні зі складністю традиційних мереж створило ідеальний шторм, який перешкоджає послідовному застосуванню механізмів дотримання політик.

Таким чином, для подолання обмежень застарілої інфраструктури необхідна фундаментальна зміна архітектури мережі. Існує потреба в більш адаптивній, масштабованій та безпечній архітектурі мережі, яка може безперешкодно інтегруватися з мінливим ландшафтом надання послуг [3].

Таким чином, архітектури програмно-визначених мереж (SDN) [4] та віртуалізації мережевих функцій (NFV) [5] приносять численні переваги цій новій обчислювальній парадигмі. Їхня інтеграція в єдину структуру, яка називається програмно-визначеною NFV (SDNFV) [6], є активною сферою досліджень та зосередження промисловості. Ця уніфікована структура використовує контроль, успадкований від SDN, та гнучкість, отриману завдяки віртуалізованим функціям NFV, що дозволяє значно покращити виявлення та усунення проблем безпеки за допомогою SDNFV. Крім того, вони є важливими інструментами для управління безпекою в цій парадигмі [7], оскільки зазвичай є додатковими технологіями. Загалом, мережі на основі SDNFV поєднують управління мережею SDN з віртуалізацією функцій мережевих вузлів NFV, а також спрощують використання ресурсів та послуг у мережі.

1.2 Область застосування

Завдяки інтеграції різноманітних технологій та протоколів в оркестрації мережі, безпека відіграє ключову роль у підвищенні безпеки зв'язку шляхом розгортання інноваційних механізмів. Традиційні заходи безпеки, такі як системи виявлення вторгнень (IDS), брандмауери та інші, традиційно розміщуються на периферії мережі для захисту від зовнішніх загроз. Однак поява нових мережевих архітектур вимагає нових механізмів безпеки для зміцнення служб та мереж, таких як ті, що використовуються в традиційних розгортаннях [8].

Мережева безпека стала важливою темою як для промисловості, так і для академічних кіл, зі сплеском інтересу до її впровадження в архітектурах SDN [8] та NFV [9]. Деякі з цих реалізацій використовують переваги програмованості мережі, застосовуючи рішення на основі машинного навчання для виявлення аномальних потоків [10] або впроваджуючи програмовану систему виявлення вторгнень у мережу SDN [11], або розробляючи функції NFV як брандмауери для розгортання на периферії [12].

Технології SDNFV втілюють нову та складну парадигму вирішення проблем безпеки, пов'язаних з розгортанням нових сервісів. Використовуючи переваги архітектури SDNFV, можна розробити різноманітні програми для управління проблемами безпеки сервісів або програм у мережі.

У цій роботі представлено алгоритм виявлення та зменшення загроз, який використовує переваги мереж на основі SNDFV. Використаний алгоритм використовує інформаційну ентропію, фундаментальну концепцію, запропоновану Шенноном [13], для кількісної оцінки невизначеності в шаблонах мережевого трафіку. Інформаційна ентропія продемонструвала свою ефективність у характеристиці інформаційного вмісту в багатьох областях та застосуваннях, таких як великі дані, нечітка логіка або медицина [14, 15, 16, 17].

Для вимірювання невизначеності в мережі алгоритм обчислює ентропію чотирьох ключових параметрів пакета: IP-адреса джерела, IP-адреса

призначення, порт джерела та порт призначення. Ці значення ентропії згодом служать основою для ініціювання відповідних методів зменшення загроз в мережевій інфраструктурі.

Таким чином, виходячи з вищеперерахованого, дослідження та програмна реалізація системи мережевого антивірусного захисту віртуалізованої інфраструктури дата-центру на базі технологій SDN/NFV, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти.

2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ

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

Більшість людей починають шукати антивірусне програмне забезпечення після того, як щось пішло не так: спливаюче вікно, яке не закривається, текстове повідомлення з «банку», яке виглядало трохи надто реалістично, або ноутбук, який раптово довго не відкриває Chrome. Інші дивляться на повідомлення про поновлення, яке коштує вдвічі дорожче, ніж вони заплатили минулого року, і задаються питанням, чи безкоштовний Microsoft Defender, вбудований у Windows, впорається з цим завданням так само добре. Щоб відповісти на ці запитання, я запустив сканування відомих компаній на власному ПК, засікав час їхнього сканування, надав їм зразки шкідливого програмного забезпечення та фішингові посилання, а також переглянув останні звіти незалежних лабораторій.

У цьому розділі розглядаються п’ять продуктів, які я б рекомендував для домогосподарства у 2026 році (сімейний ноутбук, кілька телефонів, планшет, пароль від якого ніхто не пам’ятає), у чому кожен із них хороший, у чому кожен з них невдачливий і скільки він реально коштуватиме вам після першого року. Також є один відомий антивірус, який я наполегливо не раджу встановлювати з причин, які не мають нічого спільного з тим, наскільки добре він виявляє шкідливе програмне забезпечення.

Norton 360: Найкраще антивірусне програмне забезпечення загалом

Norton – це безпечна відповідь, і я маю на увазі це як комплімент: жоден інший споживчий пакет не проходить стільки незалежних лабораторій так регулярно, і ніщо інше тут не охоплює стільки площі. Це також єдиний, хто повертає вам кошти, якщо його власні техніки не можуть очистити інфекцію, за будь-яким планом, за будь-якою ціною, без жодних умов.

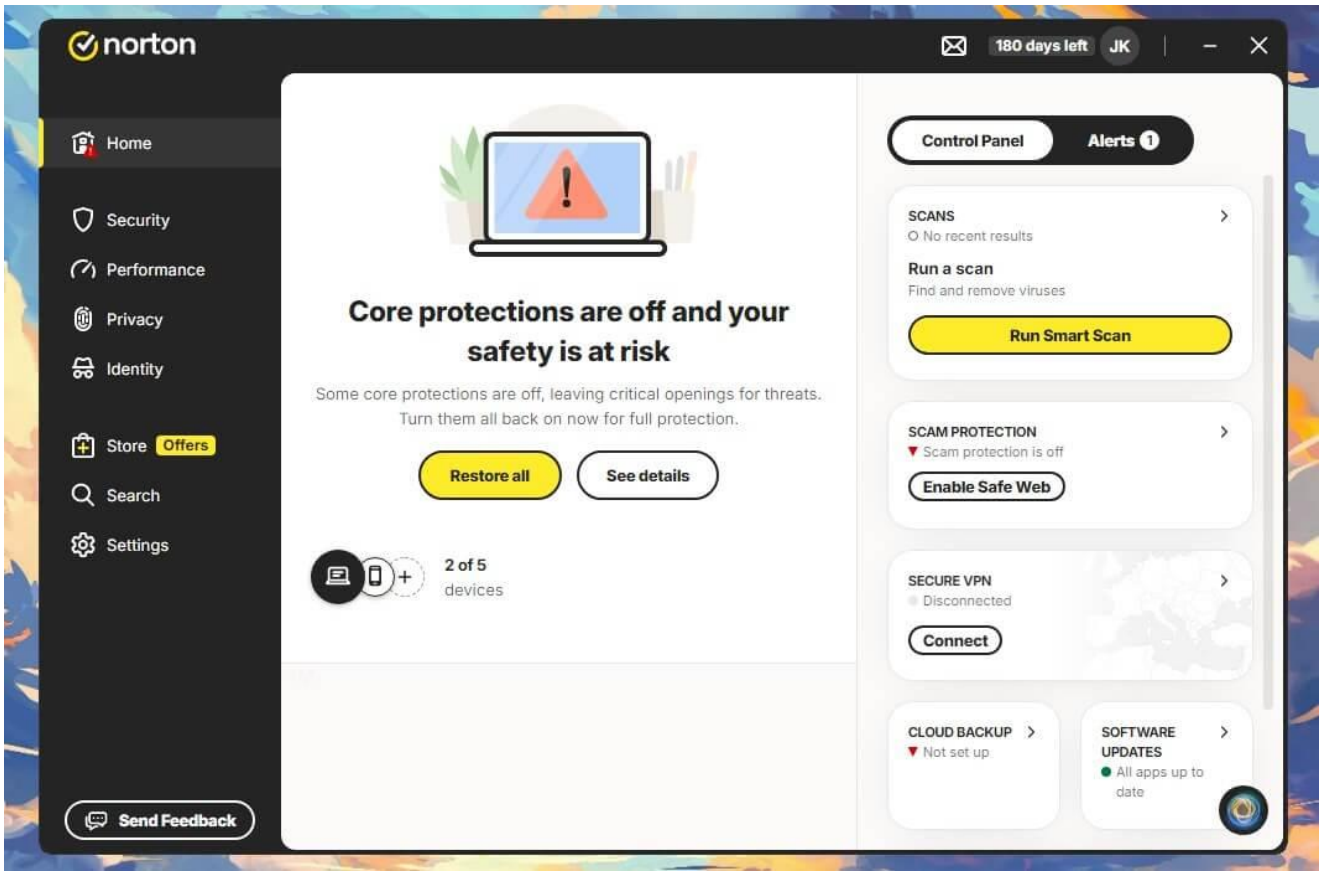


Рисунок 2.1 – Інтерфейс користувача Norton 360

У моєму огляді Norton виявлення склало 99,8% з 3 хибними спрацьовуваннями, два з яких були на цілком звичайних документах, що повільно привчає вас натискати кнопку «дозволити», не читаючи. Тест захисту від шкідливого програмного забезпечення AV-Comparatives у березні 2026 року зафіксував 96,3% виявлення офлайн, 98,7% онлайн, рівень захисту онлайн 99,97% та 9 хибних спрацьовувань, тоді як раунд тестування Windows 11 від AV-TEST у червні 2026 року дав Norton ідеальні 6 з 6 за захист, продуктивність та зручність використання, а також нагороду «Найкращий продукт».

Швидкість сканування Norton та вплив на систему

Швидке сканування Norton тривало 58 секунд, а повне сканування обох моїх дисків – 13 хвилин 22 секунди, що є найшвидшим показником з чотирьох сканерів, які я заміряв. Однак цього вдалося досягти завдяки інтенсивному завантаженню машини: процесор досяг пікового значення 23%, пам'ять – 384

МБ, а пропускна здатність диска досягла 220 МБ/с.

Тест продуктивності AV-Comparatives за квітень 2026 року показує, що Norton має показник 5.3 проти 9.6 у Bitdefender (чим нижче, тим краще), що виглядає суперечливо моїм цифрам, доки ви не зрозумієте, що ми вимірювали різні речі: лабораторні вимірювання відстежують виконання повсякденних завдань, таких як копіювання файлів і відкриття програм, а не пікове навантаження під час сканування. На практиці Norton споживає менше ресурсів під час роботи, а під час сканування – більше ресурсів.

Norton Extras: VPN, брандмауер та інструменти конфіденційності

Три з них варті того, щоб їх мати. Розумний брандмауер – найкращий з п’яти, достатньо детальний, коли ви хочете заглибитися, і достатньо розумний за замовчуванням, щоб більшість людей ніколи його не відкрили. Безпечний VPN не має обмеження даних, що рідкість для VPN, що постачається в пакеті, і Norton нещодавно оновив його для понад 100 серверів (включаючи 25 міст у 18 штатах США), з планами для кількох пристроїв, які тепер охоплюють і смарт-телевізори. Він також використовує Mimic, власний протокол Norton, який приховує той факт, що ви взагалі використовуєте VPN, що стане в нагоді в готельних або офісних мережах, які їх блокують.

Хмарне резервне копіювання (від 2 ГБ до 250 ГБ залежно від плану, лише для Windows) – це найменш цікава функція у списку, і та, якої мені найбільше бракуватиме: якщо програма-вимагач колись зашифрує ваші фотографії, резервна копія, до якої шкідливе програмне забезпечення не зможе дістатися, – це єдине, що може їх повернути, що робить його справжнім захистом від програм-вимагачів тут.

Решта – тонша. Менеджер паролів виконує свою роботу без необхідності зіставляти їх зі спеціалізованим, а моніторинг даркнету корисний, коли він вперше повідомляє про витік електронної пошти, а потім здебільшого повторюється. Norton Family, у версії Deluxe та вище, – це повноцінний пакет батьківського контролю, який починає мати значення з того дня, коли ваші діти отримають власні планшети.

Виявлення дипфейків тепер є в кожному плані, включаючи початковий рівень за 29,99 доларів, і воно перевіряє відео на наявність штучних маніпуляцій. Це звучить як наукова фантастика, поки родич не надішле вам «відео» знаменитості, яка рекламує криптовалютну схему, і переміщення цієї функції з преміум-планів – це найкорисніша зміна, яку Norton зробив цього року.

Select Plus пропонує ще більше можливостей завдяки Scam Protection Pro, яка охоплює електронну пошту, дзвінки, текстові повідомлення та перегляд веб-сторінок, додає Norton Genie (помічник на основі штучного інтелекту, у якого можна запитати: «Це шахрайство?») та відшкодовує до 10 000 доларів, якщо вас все одно обдурять, наприклад, за допомогою текстового повідомлення «ваша посилка зберігається на митниці, сплатіть тут 2 долари». Це покриття відрізняється від захисту від викрадених коштів на суму 25 000 доларів, що додається до функцій LifeLock того ж рівня.

Дві речі, які слід знати, перш ніж платити: 60-денний період повернення коштів вдвічі перевищує той, що пропонують більшість конкурентів, і Norton стягує плату до дати поновлення, а не під час неї, тому оберіть ціну на два роки (124,99 доларів за Deluxe) і не чекайте останнього дня, щоб скасувати підписку.

Bitdefender: Найкраще співвідношення ціни та якості та найменше споживання системних ресурсів

Bitdefender я рекомендую всім, чий комп’ютер старше кількох років , тим ноутбукам, на яких вже й так довго відкривається браузер. Це був найлегший клієнт, який я вимірював, за всіма показниками, і мав найменшу кількість хибних спрацьовувань серед п’яти на AV-Comparatives, тому на другому місці його тримає радше пакет послуг, ніж захист, який є чудовим.

На стенді виявлення склало 99,8% з 5 хибними спрацьовуваннями, що не відповідає лабораторним результатам: AV-Comparatives зафіксував 4 результати для Bitdefender у березні, проти 9 для Norton та Avast, а також 97,6% виявлення та рівень захисту 99,94%. На моєму ПК порядок змінився (Norton 3, Avast 4, Bitdefender 5, а McAfee опинився на останньому місці з 7 в обох), але мій вибірковий набір набагато менший, ніж у лабораторії, тому щодо хибних

спрацьовувань я б довіряв їхньому рейтингу, а не своєму. Раунд тестування AV-TEST у червні 2026 року дав Bitdefender 6 з 6 у всіх трьох категоріях.

Швидкість сканування Bitdefender та вплив на систему

Швидке сканування Bitdefender тривало 1 хвилину 4 секунди, а повне сканування – 14 хвилин 3 секунди, при цьому пікове завантаження процесора становило 11%, обсяг пам'яті – 183 МБ, а пропускна здатність диска – від 40 до 121 МБ/с. Кожен із цих варіантів має найнижчий показник серед чотирьох повних сканерів, головним чином тому, що Bitdefender надсилає значну частину аналізу до власної хмари, тому програмі на вашому комп'ютері менше роботи. Перше повне сканування після встановлення є повільним, оскільки йому доводиться перевіряти весь диск з нуля, а наступні сканування пропускають файли, які не змінилися.

Додаткові функції Bitdefender: VPN, брандмауер та інструменти конфіденційності

Safepay відкриває ваші банківські сесії в ізольованому браузері, який блокує скріншоти та кейлогери без додаткової оплати. Він блокує скріншоти настільки добре, що мені довелося знайти інший спосіб їх запису для цієї сторінки (див. підпис нижче). Автопілот приймає рішення щодо безпеки, не питаючи вас, і це справжня причина, чому нетехнічні люди налаштовують Bitdefender правильно, а ігрові, відео та робочі профілі відкладають сканування, поки відкрито повноекранний додаток, тому ніщо не перериває ваш вечір кіно чи відеодзвінок.

VPN у Total Security обмежений 200 МБ на день на пристрій, чого достатньо для перевірки електронної пошти через готельний Wi-Fi, але не для перегляду жодного епізоду. Раніше я казав, що оновлення до необмеженої версії того не варте, але я змінив свою думку: Premium Security коштує на 20 доларів дорожче, ніж Total Security, тоді як окремий VPN від Bitdefender коштує 34,99 доларів за перший рік, а оновлення також додає Scam Protection Pro, антитрекер та захист електронної пошти на двох адресах.

Захист від шахрайства Bitdefender та чим відрізняється рівень Pro

Це функція, яку Bitdefender найбільше просуває, і вона доступна у двох версіях, які легко переплутати. Стандартна версія, що входить до комплекту Total Security, працює лише на Android та iOS та охоплює текстові повідомлення, чат-додатки, сповіщення, запрошення в календар, блокування дзвінків та веб-захист, а також Scam Radar, який відстежує шахрайські кампанії, що поширюються у вашому регіоні.

Scam Protection Pro, у версії Premium Security та вище, додає Windows та macOS, а також чотири інструменти, яких немає у стандартній версії. Scamio Pro – це помічник на базі штучного інтелекту, в який ви вставляєте повідомлення, посилання, QR-код або знімок екрана, щоб отримати вердикт, Email Protection позначає вхідну пошту Gmail та Outlook як безпечну або небезпечну, а Web Scam Protection блокує фальшиву рекламу та шкідливі сайти. Четверта причина, чому я б за нього заплатив: Remote Access Scam Protection попереджає вас, якщо програмне забезпечення для віддаленого робочого столу працює під час відкритого банківського сеансу. Він одразу реагує на фальшивий дзвінок до служби технічної підтримки, коли хтось, який видає себе за співробітника «Microsoft», телефонує вашим батькам, просить їх встановити програму для віддаленого доступу, а потім просить увійти у свій банк, «щоб обробити повернення коштів», і ніщо інше у цьому списку цього не вловлює.

Avast One: Найкращий безкоштовний антивірус та найкращий для геймерів

Безкоштовний рівень Avast One – найкращий безкоштовний антивірус, який ви можете отримати, і причина проста: він використовує той самий механізм роботи в реальному часі, що й платна версія, тому «безкоштовний» тут означає той самий сканер з меншою кількістю додаткових функцій, а не слабший. У травні 2026 року Avast переробив додаток навколо цієї ідеї, додавши безкоштовну базу та платні модулі, які ви вмикаєте один за одним на одній панелі керування.

У моєму тестуванні рівень виявлення склав 99,78% з 4 хибними

спрацьовуваннями, якщо поєднати результати онлайн та офлайн. AV-Comparatives показує, що Avast має показник 96,3% офлайн, 98,7% онлайн, рівень захисту 99,97% та 9 хибних спрацьовувань у березні 2026 року, а Avast також має нагороду лабораторії «Найкращий продукт» за 2025 рік.

AV-TEST розповідає ту саму історію. У червні 2026 року Avast отримав 6 балів з 6 за захист, продуктивність та зручність використання, отримавши нагороду «Найкращий продукт», і ось що мені подобається: продукт, сертифікований AV-TEST, – це Avast Free Antivirus, який отримав ті ж 18 балів з 18, що й Norton 360 та Bitdefender Total Security.

Швидкість сканування Avast та вплив на систему

Розумне сканування Avast тривало 1 хвилину 12 секунд, а повне сканування – 14 хвилин 38 секунд, при цьому завантаження процесора ніколи не перевищувало 12%, обсяг пам'яті досягав піку близько 200 МБ, а пропускна здатність диска залишалася між 50 і 135 МБ/с. Це ставить його на друге місце після Bitdefender за використанням ресурсів і на третє місце серед чотирьох за швидкістю, що є дуже пристойним результатом для чогось, що нічого не коштує.

Якщо ви граєте в гру, режим «Не турбувати» має більше значення, ніж швидкість сканування: він відкладає заплановані сканування та приховує сповіщення, коли відкрито повноекранний додаток, включаючи власні підказки щодо додаткових товарів Avast, що є саме тим типом спливаючих вікон, які ви не хочете бачити посеред рейтингового матчу.

Додаткові опції Avast: VPN, брандмауер та інструменти для забезпечення конфіденційності

Безкоштовна версія робить набагато більше, ніж зазвичай пропонують безкоштовні рівні. Scam Guardian перевіряє сторінки під час завантаження, щоб виявляти фішингові сайти та фальшиві інтернет-магазини (наприклад, магазин кросівок, який видається занадто гарним, щоб бути правдою, з реклами в Instagram), Avast Assistant – це інструмент штучного інтелекту, який дозволяє запитати, чи безпечне посилання або повідомлення, а Ransomware Shield блокує

вибрані вами папки, щоб ніщо не могло змінити їх без дозволу.

Також є захист агента на базі штучного інтелекту (AI Agent Protection), на який варто звернути увагу, якщо ви почали дозволяти помічнику на базі штучного інтелекту читати ваші файли або надсилати електронні листи. Він стежить за цими помічниками та позначає робочі процеси, які виглядають підробленими, наприклад, коли електронний лист із замахом передає приховані інструкції вашому агенту, і в цьому порівнянні з цим справляється лише Avast. SecureLine VPN – це платний модуль (з 60-денною безкоштовною версією), а інсталятор пропонує Avast Secure Browser, який вже позначений, тому зніміть його, якщо він вам не потрібен.

Антивірус наступного покоління NordVPN: найкращий антивірус та VPN в одному

Антивірус наступного покоління від NordVPN – це не антивірусний пакет, яким його більшість із нас уявляє, з великою кнопкою сканування, яка протягом п’ятнадцяти хвилин сканує ваш диск. Він працює ще раніше: він зупиняє фальшиву сторінку банку ще до того, як ви введете пароль, а заражене завантаження ще до того, як воно потрапить у вашу папку «Завантаження». Дивлячись на фішингові посилання, які я витягнув зі своєї старої поштової скриньки Yahoo для цього тесту, саме там зараз відбувається найбільша частина боротьби.

На практиці він сканує завантаження, блокує шкідливі та фішингові сайти, попереджає вас про шахрайські сторінки, перевіряє посилання у вашій пошті Gmail та Yahoo, а також блокує рекламу та трекери, і все це всередині програми NordVPN , незалежно від того, чи підключено VPN, чи ні (мобільні програми мають менший набір функцій, ніж Windows та macOS). Якщо ви вже платите за VPN , це найкраще поєднання антивіруса та VPN, яке ви можете отримати, оскільки одна підписка покриває обидва. NordVPN ще не анонсував повнодисковий сканер, але враховуючи те, як швидко зріс список функцій цього року, я не здивуюся, якщо побачу його в найближчі місяці.

Ви можете знати його під старою назвою: до травня 2026 року NordVPN

продавав його як Threat Protection Pro, а тепер він відображається в додатках для Windows та macOS як «Захист від шахрайства, фішингу та шкідливого програмного забезпечення» з одним перемикачем замість трьох. Перейменування відбулося з відповідним маркетинговим поштовхом, оскільки в жовтні 2026 року NordVPN підписав контракт з колишньою зіркою НБА Шакілом О'Нілом як глобальним обличчям свого антивіруса наступного покоління. Звісно, знаменитість не покращує програмне забезпечення, але вона показує, куди NordVPN вкладає свої гроші: це вже не додаткова функція, захована в VPN-додатку.

Зі 50 зразків шкідливого програмного забезпечення, завантажених через браузер, антивірус наступного покоління NordVPN заблокував 45 і пропустив 5 на диск, що становить 90% блокування та найнижчий показник шкідливого програмного забезпечення на цій сторінці. Дві речі пояснюють це в контексті: мій набір зразків був набагато меншим, ніж той, який я використовував для повних сканерів, оскільки кожен файл потрібно було завантажувати окремо, а NordVPN перевіряє файли під час їх завантаження, а не після того, як вони знаходяться на вашому диску, що є зовсім іншим видом промаху.

Фішинг – це те, де він сяє. Проти активних фішингових посилань зі старої поштової скриньки Yahoo, він попереджав мене про 95% з них на всю сторінку, яку ви не можете пропустити, а порівняльний аналіз антифішингових технологій AV-Comparatives за перший квартал 2026 року ставить його в той самий діапазон – 92%. Його ще немає в таблиці Windows від AV-TEST, тому лабораторний рекорд все ще слабкий, але одна річ, яку лабораторії не вимірюють, грає на його користь: Nord Security створює свої механізми виявлення власними силами та не використовує сторонні SDK, тоді як кілька брендів середнього рівня ліцензують чужий механізм і розміщують на ньому власний логотип.

Швидкість сканування NordVPN та вплив на систему

З увімкненим антивірусом наступного покоління та відключеним VPN програма використовувала 0,2% процесора та 282 МБ пам'яті, а активність диска

була практично нульовою (0,1 МБ/с), оскільки вона не сканувала ваш диск. Простіше кажучи, ви не відчуєте, що вона працює. 282 МБ – це фіксована плата, і це більше, ніж Bitdefender використовує в найнавантаженіший момент повного сканування (183 МБ), але ця цифра охоплює всю програму, включаючи інтерфейс, і на комп'ютері з 8 ГБ оперативної пам'яті або більше ви цього не помітите.

Додаткові можливості NordVPN: VPN, брандмауер та інструменти конфіденційності

Саме тут звичайна логіка пакетів змінюється на протилежне: скрізь у цьому порівнянні VPN є другорядною думкою, прикрученою до пакету безпеки, тоді як тут рівень безпеки постачається з VPN, який варто купувати окремо. Список інструментів навколо нього також стає довшим. Сканер вразливостей виявляє відомі недоліки у встановленому вами програмному забезпеченні, захист електронної пошти перевіряє кожне видиме посилання в Gmail та Yahoo Mail в Інтернеті (тому електронний лист з текстом «ваш обліковий запис буде заблоковано» позначається ще до того, як ви натиснете на нього), а сповіщення про перехоплення сеансу повідомляє вам, чи продаються файли cookie вашого сеансу в даркнеті, тобто так облікові записи захоплюються без знання вашого пароля. Додайте перевірку адреси криптогаманця, засіб очищення URL-адрес та приховування банерів cookie, а також блокування реклами та відстеження, яке набрало 96 балів зі 100 на AdBlock Tester, що дуже близько до спеціалізованого блокувальника.

NordVPN документує три прогалини: блокування реклами не працює на YouTube, оскільки YouTube показує рекламу з тих самих серверів, що й відео, воно перестає працювати, коли активний проксі-сервер, а на macOS файли, завантажені в режимі інкогніто Chrome, не скануються. Також немає брандмауера, батьківського контролю, резервного копіювання в хмару та захисту веб-камери.

Як NordVPN обробляє ваші дані

Антивірусне програмне забезпечення за своєю природою багато бачить, і офіційний документ NordVPN за травень 2026 року про те, як працює його виявлення без профілювання користувачів, є більш конкретним, ніж звичайна сторінка конфіденційності. Файли перевіряються за хешем, а не за вмістом, де це можливо, URL-адреси видаляються з параметрів запиту та фрагментів особистого шляху перед будь-яким пошуком у хмарі, а для файлів cookie для входу ваш пристрій залишають лише перші вісім символів хешу. Згідно з NordVPN, формат даних виявлення взагалі не має поля для ідентифікаторів користувачів, тому конфіденційність вбудована в структуру, а не залежить від політики, якої хтось повинен дотримуватися. Це документ постачальника, але технічні твердження достатньо конкретні, щоб їх можна було перевірити, що більше, ніж пропонує більшість продуктів у цій галузі.

5. McAfee+: найкращий для необмеженої кількості пристроїв та мобільних пристроїв

McAfee відповідає на питання, на яке не можуть відповісти інші чотири: що встановити, коли ніхто вдома насправді не знає, скільки пристроїв? Між двома телефонами на кожного, дитячими планшетами, старим ноутбуком у шухляді та робочим ноутбуком, який призначений «лише для роботи», математика для кожного пристрою вже не наближається до шести чи семи пристроїв. Її мобільні додатки також найкращі тут, і я кажу це не легковажно, тому що більшість постачальників ставляться до Android та iOS як до рутини.

Під час мого тестування McAfee виявив близько 87% зразків офлайн та 99,4% онлайн, що становить загальний показник 99,71%, з 7 хибними спрацьовуваннями, що є найбільшим показником з п'яти на моєму тестовому столі. 87% – це число, на яке варто звернути увагу, оскільки воно майже точно відповідає результату AV-Comparatives у 86,1% офлайн для McAfee у березні, порівняно з 96,3% для Norton та Avast і 97,6% для Bitdefender.

Іншими словами, McAfee відстає від своїх конкурентів приблизно на десять пунктів, коли йому доводиться розпізнавати загрозу, не запитуючи хмару,

що має значення, якщо ваш ноутбук годинами перебуває в автономному режимі в поїздах і літаках, або якщо щось на ньому вже блокує доступ до мережі. В онлайн-режимі рівень захисту 99,97% та 6 з 6 балів у червневому раунді тестування AV-TEST є високими показниками.

Швидкість сканування McAfee та вплив на систему

Швидке сканування McAfee тривало 1 хвилину 26 секунд, а повне сканування – 16 хвилин 47 секунд, при цьому пікове завантаження процесора становило 33%, обсяг пам'яті – 415 МБ, а пропускна здатність диска – від 63 до 220 МБ/с. Це найповільніший і найвитратніший результат з чотирьох, які я виміряв (Norton теж був ненажерливим, але принаймні він був швидким), хоча AV-TEST має рацію, що McAfee залишається осторонь у щоденному використанні та стає вимогливим лише під час повного сканування.

Додаткові функції McAfee: VPN, брандмауер та інструменти для забезпечення конфіденційності

Якщо ви коли-небудь шукали своє ім’я в Google та знаходили свою домашню адресу на сайті пошуку людей, Personal Data Cleanup саме для вас: він знаходить ваші дані на сайтах брокерів даних і, на вищих рівнях, надсилає за вас запити на видалення. Online Account Cleanup знаходить облікові записи, про які ви забули, наприклад, форум, до якого ви приєдналися у 2014 році, кожен з яких має пароль, який чекає, щоб з’явитися під час чиєїсь витоку даних.

Детектор шахрайства перевіряє підозрілі текстові повідомлення, електронні листи та посилання, і це найімовірніше заощадить вам реальні гроші. VPN не має обмежень, але є базовішим, ніж NordVPN, а батьківський контроль продається окремо як McAfee Safe Family, що є значною прогалиною порівняно з Norton за аналогічними цінами.

Відшкодування шахрайства: функція, яка змінила цю категорію у 2026 році

Рік тому головним показником у будь-якому порівнянні антивірусів був рівень виявлення шкідливого програмного забезпечення. Він все ще має значення, але це вже не те, за чим конкурують ці компанії, оскільки кожен

продукт тут виявляє шкідливе програмне забезпечення настільки добре, що відмінності майже не мають значення для домашнього користувача, а чотири з п'яти отримали ідеальні 18 балів з 18 на AV-TEST у червні.

Що змінилося, так це те, що галузь нарешті визнала, що більшість людей, які втрачають гроші в Інтернеті, нічим не заражені: їх вмовляють надіслати їх за допомогою фальшивого рахунку-фактури, телефонного дзвінка на кшталт «ваш обліковий запис заблоковано» або незнайомця в додатку для знайомств, якому раптово потрібна допомога з авіаквитком. Тож постачальники почали повертати людям кошти. Norton вклав до 10 000 доларів у Scam Protection Pro на Select Plus, LifeLock додав відшкодування за шахрайство у серпні (5000 доларів у середньому рівні та 10 000 доларів у верхньому), а Bitdefender побудував свою стратегію 2026 року навколо Scam Protection Pro, хоча вона виявляє та блокує, а не виплачує.

Перш ніж ці цифри вас переконають, пам’ятайте про три речі. Стелі збитків низькі порівняно з реальними збитками, оскільки власне лютневе опитування LifeLock показало середні збитки від крадіжки особистих даних у розмірі 8 401 долара США, причому деякі жертви втратили 75 000 доларів США. Покриття поширюється лише на США, а Нью-Йорк виключений із виплат Norton та LifeLock за шахрайство, що виключає цю функцію для багатьох читачів. Крім того, поліси страхуються HSB Specialty Insurance, а не компанією-розробником програмного забезпечення, тому будь-яка претензія проходить через страховика з власними виключеннями.

Для більшості людей виявлення шахрайства важливіше, ніж виплата: захист від шахрайства віддаленого доступу від Bitdefender, який позначає програмне забезпечення для віддаленого робочого столу під час банківського сеансу, запобіжить більшим втратам, ніж може покрити чек на 10 000 доларів.

Що зараз вважається антивірусом?

Справедливо запитати, що робить NordVPN у списку антивірусів, і компанія опублікувала власну відповідь у офіційному документі за травень 2026 року: галузь завжди визначала антивірус за тим, як він виявляє шкідливі файли,

тоді як більшість атак, які сьогодні досягають людей, взагалі не стосуються файлу. Згідно з визначенням NordVPN, антивірус наступного покоління охоплює захист від шахрайства, захист від фішингу, захист від захоплення особистості та облікового запису, відстеження та блокування реклами, а також захист файлів і пристроїв, і перші чотири є його найсильнішими.

Я вважаю, що цей аргумент виправданий краще, ніж більшість маркетингових перепозицій, і мій результат 95% фішингових атак підтверджує його. Межа досягає ідеї про те, що сканування файлів можна відсунути на задній план, оскільки сканер має найбільше значення саме в тій ситуації, в якій інструмент мережевого рівня не може допомогти: комп’ютер, який був заражений до того, як ви щось встановили, або через USB-носій. Ці два підходи доповнюють один одного, що незручно для рейтингу, але це правда, і якщо ви хочете обидва, безкоштовна версія Avast поруч із підпискою NordVPN не коштує нічого додатково та заповнює прогалину.

Найкращий антивірус для ПК та ноутбуків з Windows 11

Найкращим антивірусом для Windows 11 є Norton 360, і причина цього мало пов'язана з рівнем виявлення: Windows 11 вже добре захищає файлову систему, але погано захищає людину, яка нею користується.

Що вже захищає Windows 11

Windows 11 має Smart App Control, який блокує непідписані та ненадійні програми під час чистої інсталяції, апаратні функції, такі як TPM 2.0 та віртуалізаційна безпека (VBS) з HVCI, які захищають ваші облікові дані та пам'ять ядра, а також список блокування підписаних, але несправних драйверів. Однак він не охоплює те, що відбувається навколо комп'ютера: Windows не перевірятиме скорочене посилання в текстовому повідомленні, не попереджатиме вас, коли ваша електронна пошта з'являється внаслідок порушення безпеки, не захищатиме ваш телефон Android і не відновлюватиме ваші файли після атаки програми-вимагача. Norton охоплює всі чотири аспекти, а Bitdefender – краща покупка, якщо ціна має найбільше значення або ваше обладнання старіє.

Примітка щодо Windows 10: Тепер, коли основна підтримка завершилася, комп’ютер, який все ще працює на Windows 10, потребує захисту від сторонніх розробників більше, ніж будь-коли, і наведені вище варіанти також застосовуються тут.

Чи все ще достатньо Microsoft Defender?

Для багатьох людей – так. У червневому раунді тестування Windows 11, проведеному AV-TEST у червні 2026 року, Defender отримав нагороду «Найкращий продукт» (6 за захист, 5,5 за продуктивність, 6 за зручність використання), а AV-Comparatives зареєстрував лише 3 хибні спрацьовування, тому стара ідея про те, що Windows поміщає ваші легітимні файли в карантин, не витримує. Її обмеження криються в іншому:

– Онлайн-залежність: Виявляє 98,1% загроз онлайн, але лише 89,2% офлайн.

– Обмеження браузера та платформи: Блокування шахрайських сайтів залежить від SmartScreen в Edge, і для вашого телефону чи Mac нічого не передбачено.

– Прогалини: Немає моніторингу даркнету, немає інструментів ідентифікації, а відкат до програм-вимагачів вимкнено за замовчуванням (контрольований доступ до папок залежить від OneDrive).

Висновок: Заплатіть за пакет послуг, якщо вам потрібен батьківський контроль, ви виконуєте банківські операції на цьому комп’ютері, користуєтеся спільним домом з багатьма пристроями або хочете надійний спосіб повернення файлів. Якщо ваш ПК використовується переважно для Netflix, електронної пошти та випадкових онлайн-замовлень, Defender разом із менеджером паролів та здоровою дозою підозри – це розумна конфігурація, краща за платний продукт, який ніхто не налаштовував.

Безкоштовний проти платного захисту від вірусів: де закінчуються безкоштовні рівні

У червневому раунді тестування AV-TEST у 2026 році Avast Free Antivirus отримав ті ж 18 балів з 18, що й Norton 360 та Bitdefender Total Security,

що показує, що безкоштовні та платні версії від однієї компанії зазвичай використовують однаковий механізм виявлення.

Ви платите за все, що побудовано на цьому движку, а те, що залишають безкоштовні версії, практично однаково від однієї компанії до іншої: немає брандмауера, немає відкату програм-вимагачів, VPN, який відсутній або обмежений настільки жорстко, що він стає марним, немає батьківського контролю, немає моніторингу особистості та підтримка через форум спільноти. Покриття також часто обмежується Windows, що залишає кожен телефон у будинку незахищеним, а безкоштовні програми, як правило, показують рекламу платного оновлення (те, що вони насправді продають, хоч це й безглуздо).

Коли безкоштовного достатньо:

– Однокористувацькі налаштування: Ви єдина людина, яка користується одним ПК з Windows.

– Безпечні звички: ви не встановлюєте програмне забезпечення з випадкових сайтів, перевіряєте посилання перед натисканням і зберігаєте резервні копії деінде.

– Найкращий вибір: Avast One Free охоплює основи, не вимагаючи ні копійки.

Коли цього перестає бути достатньо:

– Спільні або змішані пристрої: ваші діти також користуються ПК, або вдома працює поєднання Windows, macOS та Android.

– Завдання з високими ставками: ви займаєтесь банківськими справами, керуєте бізнесом або працюєте за цим комп’ютером.

– Пряма допомога: Ви хочете мати справжню людину, з якою можна поговорити, коли щось піде не так.

– Вартість: Платний захист коштує від 25 до 60 доларів за перший рік, що приблизно дорівнює вартості двох вечерь на винос.

2.2 Обґрунтування вибору засобів для побудови системи та мови програмування

Python є високорівневою об'єктно-орієнтованою мовою програмування загального призначення з відкритим вихідним кодом. У контексті проєктування та реалізації систем мережевого антивірусного захисту віртуалізованих дата-центрів на базі технологій програмно-конфігурованих мереж (SDN) та віртуалізації мережевих функцій (NFV) її ключові характеристики означають наступне:

– Відкритий вихідний код: забезпечує доступність мови для інспекції безпеки, адаптації інтерпретатора та інтеграції з відкритими фреймворками віртуалізації.

– Об’єктно-орієнтована парадигма: базується на моделюванні сутностей за допомогою об'єктів з атрибутами й методами, що спрощує проєктування віртуальних мережевих функцій (VNF) та модулів оркестрації.

– Високорівневість: абстрагує розробника від низькорівневих апаратних деталей, дозволяючи зосередитися на логіці безпеки, правилах маршрутизації трафіку та сигнатурному аналізі.

– Загальне призначення: дає змогу створювати як хмарні керуючі контролери SDN, так і розподілені агенти інспекції шкідливого програмного забезпечення.

Переваги та обмеження для віртуалізованої інфраструктури дата-центрів

Переваги:

– Простота синтаксису та читаність коду: значно скорочує час написання та перевірки складних алгоритмівфільтрації трафіку, вимагаючи меншої кількості рядків коду порівняно з C/C++ чи Java.

– Висока продуктивність розробки: простота мови дозволяє швидко створювати робочі прототипи систем кібербезпеки та інтегрувати їх із хмарними оркестраторами (наприклад, OpenStack, ONOS).

– Інтерпретована природа та налагодження: рядкове виконання коду полегшує локалізацію помилок у правилах обробки мережевих пакетів.

– Динамічна типізація: звільняє розробника від жорсткого оголошення типів даних при маніпуляціях з заголовками пакетів і стрічками сигнатур.

– Екосистема бібліотек: наявність великої стандартної бібліотеки та сторонніх модулів мінімізує залежність від зовнішніх компонентів при створенні інструментів аналізу безпеки.

– Портативність: забезпечує «написання один раз і виконання всюди», що критично для розгортання віртуальних мережевих функцій (VNF) на різних хост-платформах дата-центру.

Недоліки:

– Низька швидкість виконання: інтерпретована природа та динамічна типізація створюють додаткові обчислювальні накладні витрати, що є критичним при обробці гігабітних потоків трафіку в реальному часі без апаратного прискорення.

– Високе споживання пам'яті: може становити обмеження для мікросервісів антивірусного захисту, що працюють у тісних контейнерних середовищах із жорсткими лімітами ресурсів.

– Обмеження у високопродуктивних мережевих інтерфейсах: для глибокого пакетного аналізу (DPI) високого рівня навантаження чистий Python використовується здебільшого для керуючої площини (Control Plane), тоді як дата-площина (Data Plane) потребує оптимізованих модулів на C/C++ чи P4.

Сфери застосування Python у проекті:

1. Оркестрація та керування у середовищах SDN/NFV Використовується для взаємодії з контролерами SDN через REST API, автоматизації конфігурування віртуальних комутаторів (Open vSwitch) та динамічного переспрямування підозрілого трафіку на віртуальні антивірусні шлюзи (VNF).

2. Аналіз даних і логування загроз Застосування потужних бібліотек для роботи з масивами та аналітики дозволяє агрегувати журнали подій безпеки (SIEM), виявляти аномалії в поведінці віртуальних машин та обробляти великі

обсяги телеметрії дата-центру.

3. Розробка серверної частини та API безпеки Побудова централізованих панелей моніторингу, систем сповіщення адміністраторів про виявлені вірусні інциденти та керування політиками ізоляції інфікованих віртуальних середовищ.

4. Автоматизація завдань і скриптинг (DevSecOps) Створення сценаріїв автоматичного розгортання антивірусних сенсорів, оновлення сигнатурних баз на віртуальних нодах, тестування стійкості мережевої інфраструктури та перевірки конфігурацій безпеки.

2.3 Розгорнута постановка завдання

Згідно з технічним завданням на випускну кваліфікаційну роботу за другим (магістерським) рівнем вищої освіти, реалізації підлягає програмне забезпечення, яке призначено для системи мережевого антивірусного захисту віртуалізованої інфраструктури дата-центру на базі технологій SDN/NFV.

В процесі розробки випускної кваліфікаційної роботи за другим (магістерським) 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 контролю роботи технологічного обладнання на виробництві в автоматизованому режимі. Розробити функціональну та структурну схеми системи;

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

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

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

е) провести розрахунки по визначенню економічної ефективності розробленої системи;

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

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

3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ

3.1 Опис функціонування системи

Технологія SDN виникла як нова мережева парадигма, що характеризується відокремленням площини даних від площини керування, що має на меті спростити управління та налаштування традиційних мереж [18]. Цей зсув у контролі, який раніше був тісно інтегрований в окремі мережеві пристрої, дозволяє абстрагувати базову інфраструктуру для додатків та мережевих служб, розглядаючи мережу як логічну або віртуальну сутність:

– Рівень додатків: Ці програмні засоби виконують певні завдання в середовищі SDN, витісняючи та розширюючи функції, традиційно вбудовані в апаратні пристрої звичайної мережі. Приклади додатків SDN включають балансування навантаження, безпеку або управління трафіком.

– Рівень керування: Як ядро інтелектуальної системи SDN-мережі, контролер SDN отримує інструкції та вимоги від прикладного рівня. Він перетворює та передає ці інструкції мережевим пристроям на інфраструктурному рівні. Централізоване управління мережею за допомогою автоматизованих SDN-додатків сприяє розгортанню та модифікації мережевих послуг, роблячи цей процес швидшим та простішим.

– Рівень інфраструктури: Цей рівень складається з пристроїв, які є мережевими компонентами, що реалізують відкриті стандарти (наприклад, OpenFlow), що дозволяє їм контролювати можливості пересилання та обробки даних у мережі.

Площина керування та площина даних – це окремі рівні, що виникають внаслідок розділення функцій керування та пересилання, що надає додаткам більше інформації про стан мережі порівняно з протоколами, що використовуються в традиційних мережах. Таке поширення інформації полегшується наявністю мережевого контролера, запропонованого SDN.

Ця технологія забезпечує гнучкість, дозволяючи динамічне управління потоками та оптимізуючи ресурси для змінних потреб програм, що працюють від користувачів у кластері, які можуть мати різні вимоги щодо функцій та якості обслуговування [19].

Зв'язок та взаємодія між компонентами SDN відбуваються через API (інтерфейси прикладного програмування). API між визначеними SDN-додатками та контролером SDN зазвичай називають північним API. І навпаки, API, визначений між контролером SDN та мережевими пристроями SDN, відомий як південний API.

Технологія SDN надає низку важливих переваг, які описані нижче:

– Покращена автоматизація та управління.
– Швидко та легко надавайте нові мережеві послуги.
– Впроваджуйте широкий спектр мережевих політик.
– Зменшення витрат.
– Підвищена спритність.
– Покращена безпека.

З іншого боку, NFV пропонує значні переваги в наданні послуг у мережах наступного покоління. Основна мета цієї парадигми полягає у відокремленні мережевих функцій від фізичних пристроїв, на яких вони працюють.

Більше того, NFV має потенціал для сприяння та покращення розгортання нових послуг з більшою гнучкістю [20], що дозволяє задовольнити вимоги до низької затримки та високої надійності, необхідні для програм [21]. Як правило, розгортання нових складних мережевих послуг, таких як брандмауер, балансування навантаження, IPS (система запобігання вторгненням), IDS, маршрутизація або оптимізація WAN, вимагає від підприємств придбання спеціалізованих та дорогих апаратних пристроїв. Цей процес також включає встановлення нового обладнання, яке вимагає фізичного простору, збільшує витрати на енергію, вимагає спеціалізованих знань та іноді створює проблеми інтеграції. NFV прагне революціонізувати архітектуру

мережевих операторів, використовуючи стандартні технології віртуалізації. Ця трансформація спрямована на консолідацію різних типів мережевого обладнання на стандартних серверах великої потужності, комутаторах та рішеннях для зберігання даних, поширених у центрах обробки даних, мережевих вузлах та приміщеннях кінцевих користувачів. NFV передбачає реалізацію мережевих функцій у програмному забезпеченні, здатному працювати на різноманітному серверному обладнанні галузевого стандарту. Ці функції можна гнучко переміщувати або створювати екземпляри в різних місцях мережі за потреби, що усуває необхідність встановлення нового обладнання.

Основні характеристики NFV включають наступне:

– Гнучкість: Архітектура NFV сприяє швидкому та простому розгортанню, встановленню та налагодженню нових мережевих послуг, тим самим прискорюючи час виходу на ринок для задоволення потреб бізнесу та користувачів.

– Економічна ефективність: NFV усуває потребу в дорогих апаратних пристроях, дозволяючи емулювати ці пристрої за допомогою віртуалізації на стандартних серверах великої потужності, які є значно економічнішими.

– Масштабованість: NFV дозволяє розгортати нові служби або машини на кількох серверах, усуваючи необхідність додаткового фізичного простору та спрощуючи масштабованість мережі відповідно до бізнес-вимог.

– Безпека: Мережеві оператори можуть адмініструвати та контролювати мережу, дозволяючи своїм клієнтам безпечно керувати власним віртуальним простором та брандмауером у мережі.

– Повсюдність: NFV сприяє розгортанню мережевих послуг по всьому світу за допомогою віртуалізації, забезпечуючи глобальну доступність.

Часто ІТ-експерти поєднують SDN та NFV, оскільки вони мають спільні цілі, як показано на рисунку 2. Основною метою як SDN, так і NFV є логічне керування мережею за допомогою програмного забезпечення, зменшуючи ручну взаємодію з мережевими пристроями. Отже, парадигми SDN та NFV тісно пов'язані [5], і завдяки ефективній інтеграції обох можна досягти значної

економії коштів та більшої гнучкості в наданні послуг. Інтеграція цих парадигм в єдине середовище відома як мережа SDNFV.

Зрештою, хоча обидва рішення доповнюють одне одного, вони не є взаємозалежними та можуть бути реалізовані окремо, що дозволяє розгортати SDN, NFV або їх комбінацію. Згідно з офіційним документом NFV [22], метою віртуалізації мережевих функцій є забезпечення їх використання без застосування механізмів SDN, спираючись на методи, що зараз поширені в більшості центрів обробки даних. Однак підходи, засновані на розділенні площин керування та пересилання, як це пропонує SDN, покращують продуктивність, спрощують сумісність з існуючими розгортаннями та полегшують протоколи управління та обслуговування.

Безпека в NFV та SDN

Інформаційна безпека постійно є критично важливою проблемою в цифрову епоху через першорядну цінність інформації та нагальну потребу в її захисті. Інформаційна безпека охоплює превентивні та реагуючі заходи, що вживаються окремими особами, організаціями та технологічними системами для захисту та збереження конфіденційності, цілісності та доступності інформації, що часто називають тріадою CIA. Ця тріада служить основоположною моделлю, що керує політикою інформаційної безпеки в організаціях, як зазначено в ISO/IEC 27000:2018 [23]:

– Конфіденційність: гарантує, що інформація не буде розголошена неавторизованим особам, організаціям або процесам.

– Цілісність: Забезпечує точність і повноту інформації.

– Доступність: Забезпечує доступність та використання інформації на вимогу уповноваженими особами.

Хоча тріада CIA відображає фундаментальні властивості інформаційної безпеки, додаткові властивості, такі як автентичність, підзвітність, невідмовність відмов та надійність, також можуть бути критично важливими.

Мережі відіграють ключову роль в інформаційних системах, сприяючи обміну інформацією між різними комп'ютерами та розподілу ресурсів. Безпечна

інформаційна система вимагає безпечної мережі. Поява нових мережевих архітектур задовольнила нові бізнес-вимоги; однак, вона одночасно принесла нові загрози та вразливості до тріади CIA, які потребують уваги. З цієї причини важливо аналізувати вразливості та загрози, пов'язані з архітектурами SDN та NFV.

Майбутні мережі на основі NFV та SDN забезпечать простіші процеси безпеки та засоби контролю, ніж ті, що ми маємо сьогодні. Мережі, що використовують ці технології, буде легше оновлювати та виправляти в міру розвитку загроз безпеці. Шифрування буде підтримуватися легше, а інші механізми безпеки – стабільніше, ніж застарілі технології. А моніторинг мережі для управління загрозами буде простішим та економічно ефективнішим.

Відкриті розподілені архітектури надають можливість для більш послідовної реалізації фундаментальних функцій, процесів та протоколів, включаючи легше впровадження нових, безпечніших протоколів. Це, у свою чергу, може спростити впровадження та розгортання процесів і засобів контролю безпеки. Застарілі функції та процеси мережевої інфраструктури значною мірою характеризуються власницькими системами. Навіть реалізація базових списків контролю доступу з IP-інтерфейсів сильно відрізняється не лише інтерфейсами, що використовуються для реалізації списків контролю, але й деталізацією та специфічністю елементів контролю. Деякі області покращилися, але NFV та SDN можуть покращитися ще більше. Наприклад, BGP Flowspec допоміг стандартизувати блокування, обмеження швидкості та перенаправлення трафіку на маршрутизаторах. Однак сьогодні він має суворі обмеження на кількість правил, які практично підтримуються на маршрутизаторах. NFV та SDN можуть забезпечити покращену масштабованість та розширену функціональність. NFV надає можливість вирішити цю складність, надаючи загальні методи впровадження засобів контролю безпеки. SDN пропонує аналогічну можливість, надаючи стандартизовані інтерфейси для впровадження таблиць потоків на пристроях та розгортання конфігурації за допомогою конфігурації на основі моделей (наприклад, за допомогою YANG та

NETCONF).

Стандартизовані функції, процеси та протоколи природним чином призводять до простішого та швидшого розгортання інструментів безпеки та легшого встановлення патчів для програм. NFV дозволяє застосовувати найкращі практики Develop Operations (DevOps) для розробки, розгортання та тестування патчів і оновлень програмного забезпечення. Фізичні та віртуальні маршрутизатори та мережеві пристрої можна аналогічно програмно оновлювати за допомогою SDN. Така гнучка та автоматизована реконфігурація мережі, ймовірно, полегшить вирішення загроз безпеці. Крім того, монітори та датчики безпеки, брандмауери, екземпляри віртуальних приватних мереж тощо можна легко розгортати або оновлювати в міру розвитку загроз безпеці.

Конфіденційність клієнтів можна ще більше підвищити. У минулому шифрування не мало широкого розгортання з низки вагомих економічних та технічних причин. Галузь багато чого навчилася у розгортанні безпечної та зашифрованої інфраструктури для мереж DOCSIS®, а також мереж радіодоступу (RAN). Нові апаратні та програмні можливості, які вже широко використовуються в центрах обробки даних та хмарних рішеннях, можуть бути застосовані до NFV, щоб забезпечити повсюдне шифрування в основних мережах. Отже, розгортання шифрування мережевої інфраструктури тепер може бути набагато практичнішим. Це може значно збільшити складність проведення несанкціонованого моніторингу, атак «людина посередині» та перехоплення маршрутів.

Ключовим викликом для мережевих операторів залишається виявлення шкідливих атак на абонентів. Постачальники послуг використовують різноманітні неінвазивні методи моніторингу для виявлення систем, заражених шкідливим програмним забезпеченням та активних учасників ботнетів. Їм також необхідно швидко виявляти масштабні атаки типу «відмова в обслуговуванні» та намагатися обмежити вплив цих атак на клієнтів. На жаль, таке виявлення було дорогим. NFV обіцяє більш економічно та ширше розподіляти функції моніторингу, що дозволить набагато гнучкіше реагувати на загрози для клієнтів.

Крім того, NFV може використовувати специфічні методи віртуалізації, рекомендовані NIST (такі як інтроспекція гіпервізора), для забезпечення активного моніторингу програм. Крім того, SDN надає можливість швидко обмежувати або блокувати потоки шкідливого трафіку набагато ближче до джерела атак.

Зрештою, NFV обіцяє дати нам можливість зробити крок вперед у сфері безпеки мереж. Більшість основних мережевих технологій, що використовуються сьогодні (маршрутизація, комутація, DNS тощо), були розроблені понад 20 років тому. Галузь, що надає широкосмугові послуги, сьогодні знає набагато більше, ніж коли були вперше розгорнуті перші широкосмугові та корпоративні мережі. Технології NFV та SDN надають можливість значною мірою очистити аркуш та усунути внутрішні вразливості. Інтернет спочатку задумувався як відкрите середовище – доступ до Інтернету був мінімально контрольованим, а автентифікація ніколи не інтегрувалася на рівні протоколу. Це виявилося наївним, і рішення з відкритою розподіленою архітектурою, що реалізуються завдяки NFV та SDN, можуть допомогти забезпечити кращу, більш захищену інфраструктуру. Звичайно, вразливості продовжуватимуть існувати, і будуть виявлені нові, унікальні для рішень NFV та SDN.

3.2 Розробка структурної схеми

Як обговорювалося в попередньому розділі, основною метою архітектури SDN є розділення площин даних та площин керування. Отже, архітектура SDN складається з трьох рівнів: прикладного рівня, рівня керування та рівня інфраструктури, кожен з яких містить певні підкомпоненти:

– Мережеві елементи (ME), розташовані на рівні інфраструктури.
– SDN-контролери, розташовані на рівні керування.
– SDN-сумісні додатки, розташовані на рівні додатків.

Хоча застарілі мережі мають один тип компонентів (мережеві пристрої), архітектура SDN охоплює кілька елементів (NE, контролери SDN, SDN-додатки, а також інтерфейси, що працюють у північному та південному напрямках). Тому існує потреба захищати не лише мережеві пристрої, але й контролери, додатки та їхній зв'язок.

У попередніх роботах [24] було проаналізовано кожен компонент архітектури SDN за допомогою методології Microsoft STRIDE та визначено потенційні загрози, до яких вони вразливі.

Північний інтерфейс (NBI) являє собою значний вектор атаки через множинність API, що використовуються контролерами SDN. Ці API використовують різноманітні технології та мови, такі як Python, Java, C, REST, XML, JSON, FTP, LDAP та інші. Використання вразливостей у будь-якій із цих технологій або мов програмування може надати зловмиснику контроль над мережею SDN через скомпрометований контролер. Наприклад, скомпрометований NBI може дозволити зловмиснику створювати шкідливі політики SDN та маніпулювати мережевим середовищем.

Аналогічно, південний інтерфейс (SBI) являє собою потенційний вектор атаки. Численні API та протоколи сприяють зв'язку між контролером та мережевими елементами. Ці протоколи включають OpenFlow, Simple Network Management Protocol (SNMP), Secure Shell (SSH), NETCONF, OVSDB (Open vSwitch Database Management Protocol), OF-Config (OpenFlow Management and Configuration Protocol) тощо. Хоча кожен протокол використовує свої методи безпеки, їхня відносна новизна та потенційні недоліки реалізації роблять їх вразливими. Зловмисник може скористатися цими вразливостями для зміни або створення шкідливих потоків у таблиці потоків пристрою, що дозволить впроваджувати незаконний трафік або маніпулювати маршрутизацією для шкідливих цілей, таких як атаки типу «людина посередині» (MITM).

Відносна новизна SDN та її програмної інфраструктури створює суттєву проблему з точки зору безпеки. Відсутність історичних даних про інциденти безпеки перешкоджає нашій здатності передбачати та проактивно реагувати на

потенційні вектори атак. Це вимагає проактивного підходу до посилення безпеки мережі, з акцентом на надійних заходах безпеки на всіх інтерфейсах та протоколах в архітектурі SDN.

Для підвищення безпеки мереж SDN можна впровадити кілька заходів. Одна зі стратегій полягає в захисті контролера, який вважається ядром мережі. Отже, якщо цей компонент скомпрометовано, це впливає на загальне функціонування мережі [25]. Іншим заходом є усунення вузького місця в комунікації між контролером і комутаторами, яке можуть використовувати зловмисники [26].

Проблеми безпеки NFV

У реальному мережевому ландшафті розгортання віртуальних мережевих функцій (VNF) має гарантувати збереження надійних функцій безпеки, властивих застарілим мережам. Хоча NFV пропонує численні переваги, вона також створює нові проблеми безпеки, пов'язані із захистом оркестратора та гіпервізора, повсюдними віртуальними пристроями, доступом третіх сторін, спільними віртуальними машинами та сховищами тощо.

VNF, як мережеві функції, що працюють на віртуальних машинах, вразливі до трьох категорій загроз безпеці:

– Загальні загрози віртуалізації: до них належать витік пам'яті, ізоляція переривань та інші вразливості, властиві віртуалізованим середовищам.

– Загрози, характерні для застарілих мережевих функцій: вони охоплюють існуючі загрози, раніше спрямовані на фізичні мережеві функції, такі як атаки перевантаження та вразливості безпеки маршрутизації.

– Нові загрози, що виникають внаслідок поєднання технологій віртуалізації та мережевих технологій: ці загрози є специфічними для середовищ NFV та використовують унікальні характеристики віртуалізованих мережевих функцій.

У заяві про проблему безпеки NFV окреслено ці потенційні загрози, включаючи як нові загрози, так і існуючі загрози, що проявляються по-новому. Для вирішення цих проблем група експертів з безпеки, призначена

Європейським інститутом телекомунікаційних стандартів (ETSI), надала комплексні рекомендації щодо забезпечення безпеки розгортання NFV [27]. Ці рекомендації зосереджені на таких ключових сферах безпеки:

– Перевірка та забезпечення дотримання топології: забезпечення відповідності мережевої топології політикам безпеки та запобігання несанкціонованим змінам.

– Доступність інфраструктури підтримки управління: Гарантування доступності та цілісності критичної інфраструктури, що підтримує управління нетранспортними засобами.

– Безпечне завантаження: впровадження механізмів, які гарантують завантаження лише перевіреного програмного забезпечення під час процесу завантаження.

– Безпечний збій: Захист системної пам'яті та інформації про стан у разі системного збою.

– Ізоляція продуктивності: запобігання нестачі ресурсів та забезпечення справедливого розподілу ресурсів між віртуальними нестачею ресурсів (VNF).

– Автентифікація, авторизація та облік користувачів/орендарів (AAA): впровадження надійних механізмів автентифікації, авторизації та обліку користувачів та орендарів.

– Автентифікована служба часу: забезпечення надійної та захищеної від несанкціонованого доступу служби часу для віртуальних незалежних мереж (VNF).

– Закриті ключі в клонованих образах Iimages: Захист закритих ключів, що використовуються для шифрування та автентифікації в клонованих образах віртуальних машин.

– Бекдори за допомогою віртуалізованих функцій тестування та моніторингу: Запобігання впровадженню несанкціонованих бекдорів за допомогою віртуалізованих функцій тестування та моніторингу.

– Багатоадміністраторська ізоляція: забезпечення ізоляції різних адміністративних доменів для запобігання несанкціонованому доступу та підвищенню привілеїв.

Впроваджуючи ці заходи безпеки та дотримуючись найкращих практик, викладених ETSI, мережеві оператори можуть використовувати переваги NFV, одночасно зменшуючи потенційні ризики безпеки та забезпечуючи безпечне та надійне мережеве середовище.

Впровадження механізмів безпеки в мережі на основі SDN та NFV

Як обговорювалося раніше, хоча SDN та NFV пропонують значні переваги для сучасних мережевих архітектур, вони також створюють проблеми безпеки для мережі та її даних. Інтеграція обох підходів в єдину структуру, відому як мережа на основі SDNFV, пропонує покращені механізми виявлення та зменшення загроз безпеці.

Завдяки комбінованим перевагам контролю та гнучкості, успадкованим від SDN та NFV відповідно, SDNFV став гарячою темою як у дослідженнях, так і в промисловості. З'явилося кілька технологій для реалізації фреймворків SDNFV через притаманну складність його архітектури та взаємозв'язок між цими двома підходами.

Мережа на основі SDNFV визначає складні мережеві сервіси, які можуть працювати на апаратному забезпеченні загального призначення, замінюючи традиційне спеціалізоване обладнання, розроблене для виконання певних функцій [28]. Ця інтеграція між апаратним забезпеченням NFV та SDN частково досягається завдяки розділеній площині керування та площині даних в SDN. Контролер, що керує площиною керування мережі, оркеструє розгортання сервісів, вибираючи оптимальне розташування для кожної віртуалізованої функції.

Хоча основною функцією контролера в чистій SDN-архітектурі залишається керування площиною керування та спрямування мережевих потоків, мережа на основі SDNFV потребує додаткової функціональності для

оркестрації мережевих ресурсів, розгортання віртуалізованих функцій та управління їх життєвим циклом.

З точки зору безпеки, контролер/оркестратор відіграє життєво важливу роль в обробці ключових сервісів для виявлення та пом'якшення атак, розподілі мережевих ресурсів для створення чорних дір та аналізі потоків трафіку, джерел та споживачів.

Обидві парадигми з'єднуються між собою через контролер/оркестратор, розгорнутий у мережі. Архітектура поділена на різні типи взаємопов'язаних вузлів. У запропонованій архітектурі мережі SDNFV існує два типи SDN-комутаторів.

Перший побудовано на CPqD/ofsoftswitch13, що є версією програмного комутатора OpenFlow 1.3, що виконується в просторі користувача та реалізує всі стандартні функції. Цей комутатор був модифікований робочою групою проекту BEhavioural-BAsed forwarding (BEBA) для введення розширеного набору дій та примітивів, призначених для моніторингу мережевого трафіку та підвищення безпеки зв'язку [29]. Підхід BEBA – це реалізація контролера та комутатора OpenState з відкритим кодом, яка доступна за адресою [30]. Другий тип комутатора, що використовується в цій системі, – це Open vSwitch (OVS), який функціонує як модуль ядра, що підтримує OpenFlow, фактично замінюючи реалізацію мосту Linux.

Ще одним невід'ємним компонентом є контролер RYU OpenFlow, який керує площиною керування обома типами комутаторів для забезпечення інтелектуальної маршрутизації в мережі SDNFV. Для спрощення цей контролер також виконує роль оркестратора, контролюючи управління ресурсами в інфраструктурі віртуалізації мережевих функцій (NFVI). Ці функції можна розділити на дві сутності в мережі, щоб відокремити функціональність контролера та оркестратора.

У цій архітектурі інфраструктура для розгортання віртуалізованих мережевих функцій використовує інфраструктуру Docker, що працює в кластері Docker. Ці сервери Docker інтегровані в мережу як вузли, доступні через різні

маршрути. Усі віртуалізовані функції розгортаються в межах цих серверів, що вимагає від контролера адаптації маршрутів для включення функцій NFV в мережу та управління взаємодією з мережевими потоками.

Мережа SDN

Як було зазначено в попередньому розділі, мережа SDN включає два різних типи комутаторів. Комутатори OVS, що функціонують як неінтелектуальні комутатори, в основному працюють, дотримуючись правил комутації пакетів, встановлених контролером. Вони також інтегровані в кластер Docker для полегшення розгортання Docker, що реалізують архітектуру NFV.

Комутатори CPqD, розроблені з підтримкою BEBA, втілюють пропозицію, відому як OpenState [31, 32]. OpenState розширює основні функціональні можливості OpenFlow, дозволяючи застосовувати різноманітні правила зіставлення на основі різних станів, виявлених у таблицях потоків SDN комутатора.

Ця розширена функціональність дозволяє комутатору реагувати на події на рівні пакетів, аналізуючи потоки, що комутуються. Якщо аналіз відповідає попередньо визначеним правилам у таблицях потоків, комутатор може діяти відповідно до цих правил.

OpenState працює як розширення OpenFlow, інтегруючи традиційну таблицю потоків зіставлення/дії з додатковою таблицею станів, що містить стани потоків. Комутатори з підтримкою BEBA спочатку зіставляють пакети зі станами з таблиці станів, перш ніж виконати таблицю потоків, щоб визначити подальші дії.

Архітектура NFV

Архітектура NFV реалізована за допомогою використання Dockers у кластері. Для ефективної оркестрації та розгортання віртуалізованих функцій мережевому контролеру потрібна вичерпна інформація про кластер, що включає деталі апаратного забезпечення та IP-адреси серверів для встановлення NFVI. За допомогою цих даних контролер може ефективно розподіляти ресурси та розгортати віртуалізовані функції.

У цій екосистемі мережеві функції інкапсульовані в легкі контейнери Docker. Такий контейнерний підхід забезпечує незалежність розгортання функцій від базової платформи.

NFVI встановлює зв'язок з мережею SDNFV через фізичні мережеві інтерфейси (pNIC). Ці інтерфейси сприяють обміну пакетами між віртуалізованими мережевими функціями та мережею SDN. Кожна інкапсульована віртуальна функція в контейнері оснащена двома віртуальними мережевими інтерфейсами, з'єднаними між собою через міст (що дозволяє динамічну конфігурацію віртуальної мережі між контейнерами за допомогою функцій фізичного комутатора для інфраструктури NFV). Цей фреймворк дозволяє невеликому кластеру розгортати численні екземпляри, налаштовуючи мережеві з'єднання та інтерфейси, одночасно полегшуючи зв'язок між контейнерами. Докери реалізують функціональність контейнера через файл під назвою Dockerfile, який містить інструкції для автоматичного налаштування середовища в образі Docker. Цей образ, коли він створюється в NFVI, виконує функції в мережі SDNFV. Безпечний зв'язок між контролером/оркестратором та NFVI забезпечується шифруванням, що полегшує передачу конфігурацій віртуалізованих функцій, створення Dockerfile та команд розгортання, необхідних для інфраструктури NFV.

Контролер/оркестрація SDNFV

Архітектура включає контролер на базі RYU, який є компонентним SDN-контролером з набором попередньо визначених компонентів, необхідних для його функціональності. Ці компоненти можна налаштувати в програмі контролера, щоб адаптувати його поведінку до конкретних вимог задачі.

Для підтримки фундаментальних функцій BEBA необхідно інтегрувати різні нові повідомлення, дії та поля відповідності. Контролер, що підтримується BEBA, розширює базову реалізацію контролера, дозволяючи розбирати користувацькі програми. Він використовує експериментальні повідомлення для побудови логічної моделі програми та користувацьке навантаження для передачі

важливої інформації для комутації трафіку, рішень щодо потоку або виконання мережевих правил.

Реалізацію BEBA було адаптовано для включення оркестратора NFV. Він отримує інформацію з NFVI (у цьому сценарії, кластера Docker), розгортає віртуалізовані функції та перенаправляє трафік до NFV.

Фреймворк RYU SDN розширено шляхом реалізації BEBA з використанням протоколу OpenFlow 1.3 [33] та зовнішніх бібліотек, інтегрованих в оригінальний фреймворк [34]. Примітно, що мережа SDNFV є гетерогенною, що вимагає від контролера керування комутаторами та реалізації протоколу комутації для маршрутизації потоку. Комутатори OpenFlow з підтримкою BEBA виконують звичайні програми (наприклад, попередньо визначені комутатори L2).

Розроблений застосунок, побудований на цьому фреймворку, використовує реалізацію BEBA для аналізу потоків та виявлення підозрілих. Згодом модуль оркестрації NFV вибирає оптимальний Docker-сервер для розгортання контейнера, що містить функціональність NFV. Він встановлює безпечний канал, виконує команди розгортання для NFV та після успішного розгортання переналаштовує таблиці потоків, щоб перенаправити ідентифікований потік до контейнера NFV, таким чином пом'якшуючи атаку.

Хмарний антивірус

Хмарний антивірус – це сучасне рішення кібербезпеки, яке переносить основні обчислювальні процеси й бази даних на віддалені сервери (у хмару), на відміну від традиційних програм, що залежать від ресурсів локального пристрою.

Принцип його роботи полягає в тому, що під час звернення до файлу його сигнатура та поведінка аналізуються у хмарі за допомогою потужних алгоритмів. Це гарантує миттєве реагування на свіжі загрози та не перевантажує систему користувача.

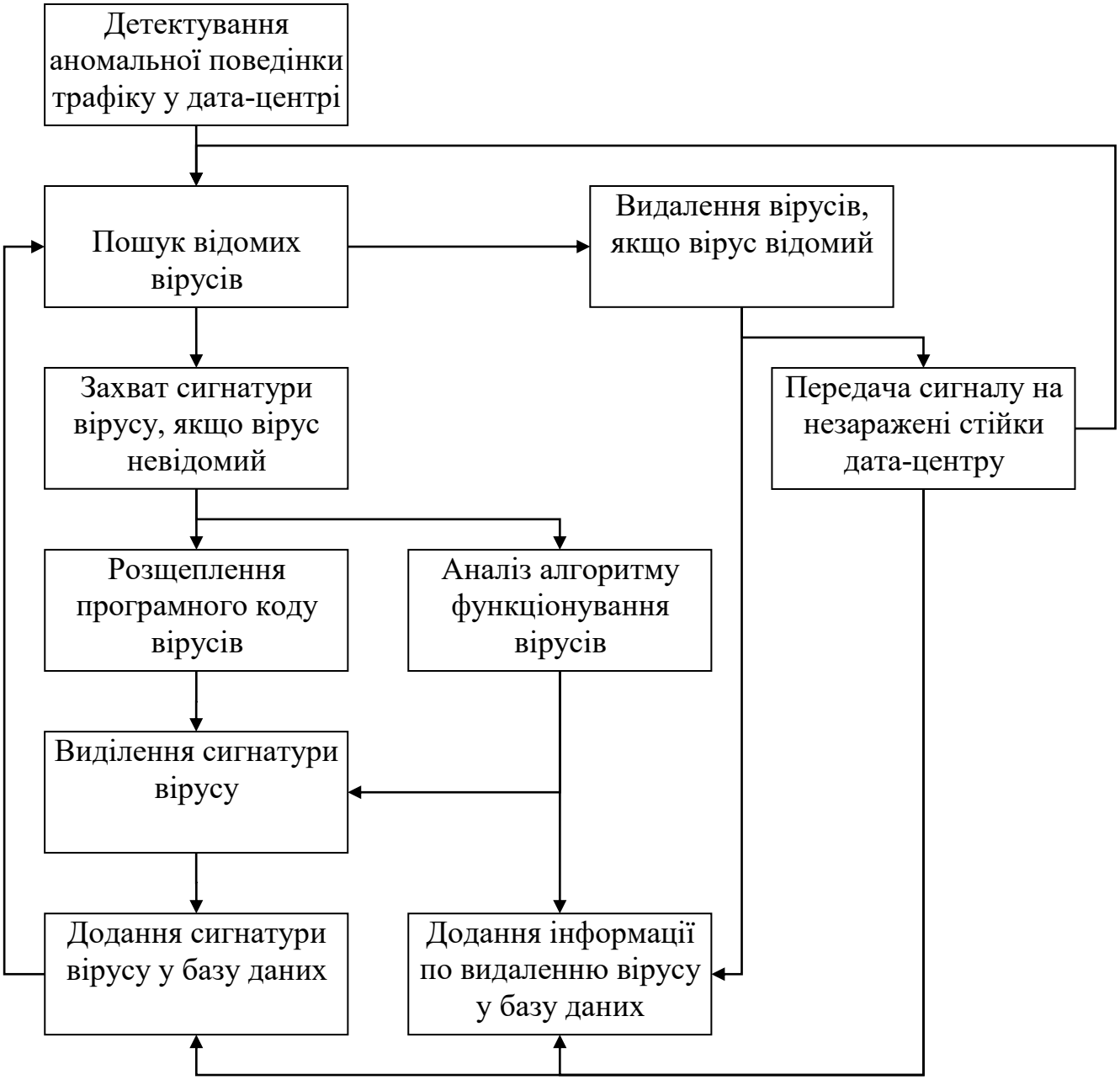


Рисунок 3.1 – Структурна схема системи

Порівняння традиційного та хмарного антивірусу:

– Споживання ресурсів: Класичні антивіруси часто сповільнюють роботу ПК через локальні сканування. Хмарні аналоги обробляють дані на віддалених серверах, мінімізуючи навантаження на пристрій.

– Актуальність захисту: Оновлення бази загроз відбуваються миттєво в режимі реального часу, забезпечуючи імунітет проти атак нульового дня.

– Масштабованість: Хмарне ПЗ легко охоплює та захищає безліч пристроїв у різних локаціях одночасно.

Хмарний антивірус у середовищі хмарних обчислень

Із масовим переходом бізнесу в хмару виникає потреба в спеціалізованому захисті даних, що там зберігаються та обробляються. Хмарні антивіруси забезпечують гнучку безпеку й централізоване управління, що критично важливо для компаній із розподіленою структурою та віддаленими співробітниками.

Завдяки передовим методам аналізу такі рішення здатні виявляти приховані загрози, аномалії та підозрілу поведінку, які часто пропускають стандартні програми.

Переваги для бізнесу:

– Економічність: Зменшення витрат на потужне локальне обладнання та його обслуговування.

– Гнучкість: Можливість швидко масштабувати систему в міру зростання компанії.

– Надійність: Високий рівень захисту конфіденційних даних за допомогою передових хмарних технологій.

Стратегія та етапи впровадження

Кроки для розгортання:

1. Оцінка потреб: Визначте необхідний рівень захисту відповідно до масштабів і ризиків вашої організації.

2. Вибір рішення: Проведіть аналіз ринку та підберіть оптимальний хмарний продукт.

3. Планування: Створіть план розгортання для мінімізації робочих перебоїв.

4. Встановлення та налаштування: Інсталюйте ПЗ і адаптуйте його під корпоративні політики безпеки.

5. Моніторинг: Регулярно аналізуйте звіти та оновлюйте конфігурації.

Найкращі практики експлуатації:

- Підтримуйте всі компоненти системи в актуальному стані.
- Проводьте регулярне навчання та тренінги з кібербезпеки для персоналу.
- Використовуйте багаторівневий захист (брандмауери, резервне копіювання, системи виявлення вторгнень).
- Періодично проводьте аудити безпеки задля виявлення вразливостей.

3.3 Розробка функціональної схеми

На рисунку 3.2 наведено функціональну схему розробленої системи. Створений у межах дипломного проєкту комплекс мережевого антивірусного захисту забезпечує комплексне забезпечення безпеки віртуалізованої інфраструктури дата-центру від кіберзагроз на основі інтеграції з технологіями програмно-конфігурованих мереж (SDN) та віртуалізації мережевих функцій (NFV).

Основні функції та можливості розробленого комплексу:

– Проактивний захист нового покоління – виявлення та блокування невідомих загроз «нульового дня» на основі поведінкового аналізу й евристичного сканування віртуальних машин.

– Сканування уразливостей – автоматична перевірка операційних систем, гіпервізорів та встановленого програмного забезпечення на наявність відомих вразливостей.

– Hardening та оптимізація конфігурацій – налаштування параметрів безпеки операційних середовищ і мережевих служб для мінімізації ризиків несанкціонованого доступу.

– Відновлення працездатності – механізми реверсу змін та відновлення цілісності віртуальних інстансів після деструктивного впливу або вірусних атак.

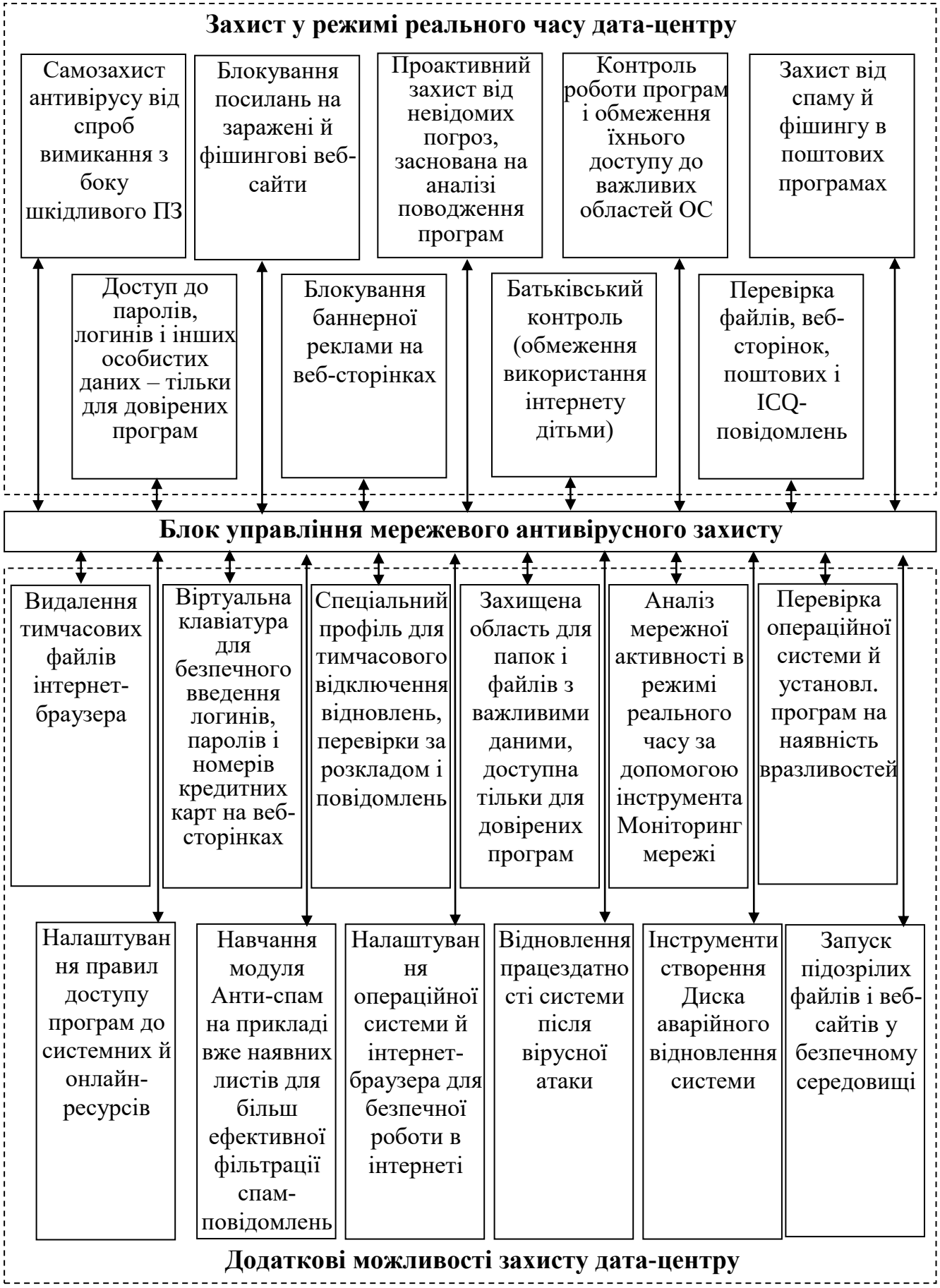


Рисунок 3.2 – Функціональна схема системи

– Захист у реальному часі (Real-Time Protection) – безперервний моніторинг і перевірка файлових потоків, мережевих пакетів, вебсторінок та поштових повідомлень на рівні віртуальних комутаторів.

– Мінімальне навантаження на мережеву інфраструктуру – оптимізація обчислювальних витрат завдяки розподілу антивірусних функцій у середовищі NFV, що виключає надмірне споживання ресурсів хостів дата-центру.

– Інтуїтивно зрозумілий інтерфейс керування – централізована панель моніторингу стану безпеки віртуалізованого середовища.

– Інтеграція з міжмережевими екранами – можливість спільного функціонування з віртуальними фаерволами для реалізації комплексних політик безпеки (Zero Trust Architecture).

– Блокування фішингових і заражених ресурсів – реалізація модуля «Перевірка посилань» для запобігання переходу на шкідливі вебсайти або ресурси перехоплення даних.

– Самозахист антивірусних мікросервісів – захист компонентів комплексу від спроб зупинення, модифікації чи деактивації з боку шкідливого програмного забезпечення.

– Система миттєвого виявлення – екстрене блокування нових сигнатур і шкідливих кодів за допомогою хмарних сервісів аналізу та репутаційних баз даних.

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

3.4 Розробка діаграми процесів

На рисунку 3.3 наведено діаграму потоків даних розробленої системи, детальний розгляд якої дозволяє простежити логіку взаємодії її функціональних компонентів. У процесі проєктування використовується структурний підхід та графічне представлення інформаційних потоків у системі (Data Flow Diagram, DFD), що дає змогу ефективно візуалізувати процеси обробки та передачі даних

між серверами, віртуальними комутаторами і мікросервісами захисту.

Згідно з інженерною методологією, розробка розпочинається з побудови контекстної діаграми (діаграми нульового рівня), яка визначає глобальні межі системи та її зовнішні інтерфейси у віртуалізованому середовищі дата-центру. Надалі ця модель підлягає ітераційній декомпозиції шляхом деталізації базових процесів та потоків трафіку з метою повного відображення архітектури розроблюваного комплексу мережевого антивірусного захисту на базі технологій SDN/NFV.

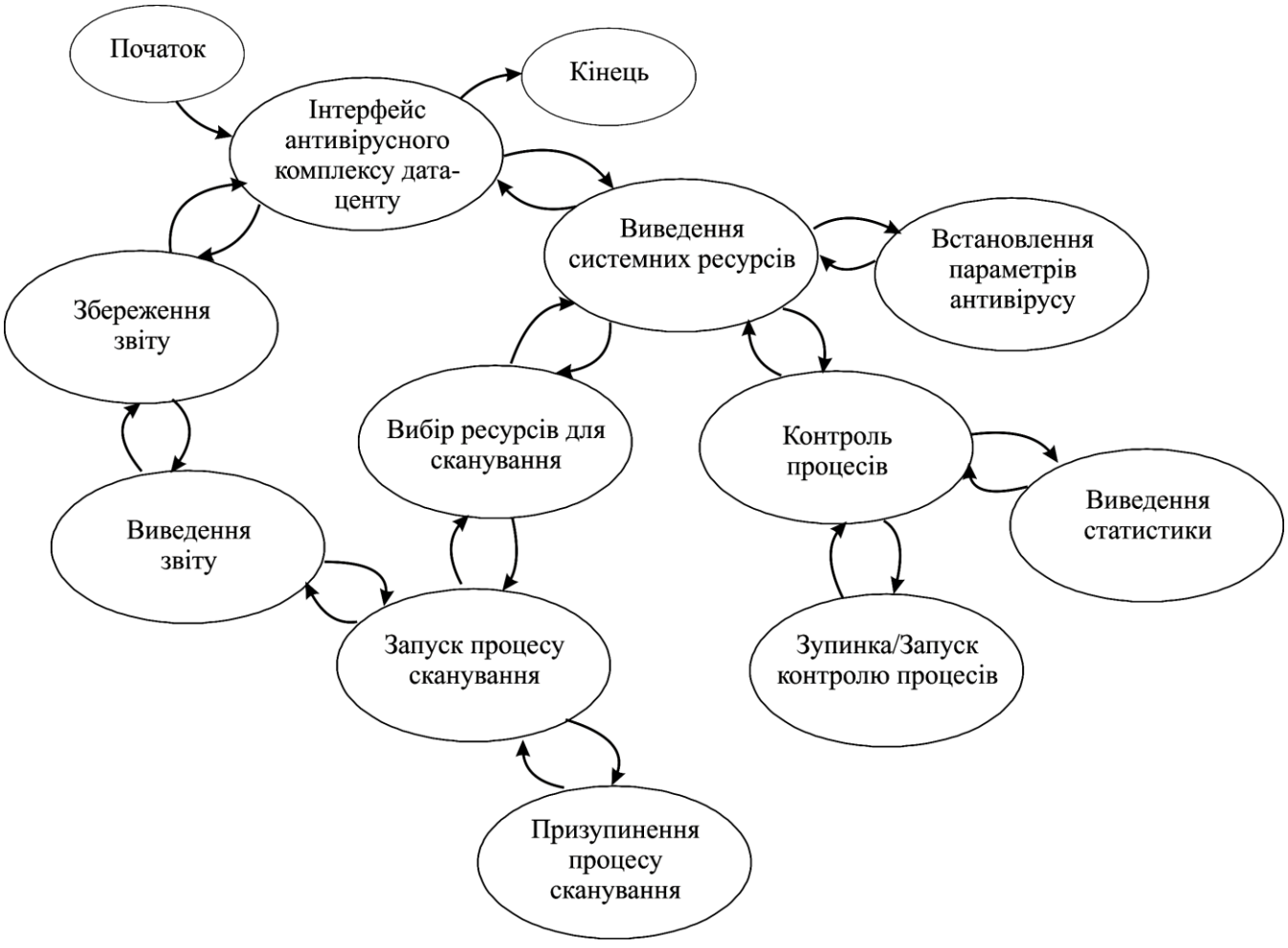


Рисунок 3.3 – Діаграма взаємодії процесів

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

Функціонування системи мережевого антивірусного захисту віртуалізованої інфраструктури дата-центру на базі технологій SDN/NFV передбачає узгоджену роботу механізмів контролю мережевого трафіку, виявлення шкідливого програмного забезпечення та динамічного керування мережевими потоками. Основне завдання алгоритмічного забезпечення полягає в організації перевірки інформаційного обміну між віртуальними машинами, серверами та зовнішніми мережами без необхідності встановлення окремого антивірусного комплексу на кожному мережевому вузлі. Для цього використовується розділення функцій керування мережею та передавання пакетів. Узагальнену послідовність функціонування програмного комплексу відображає блок-схема на рисунку 4.1.

Основою проєктного рішення є використання програмно-визначеної мережі SDN для централізованого керування комутацією та технології NFV для розміщення функцій антивірусної перевірки у віртуалізованому середовищі. Контролер SDN відповідає за визначення маршруту мережевого потоку, застосування правил доступу та перенаправлення трафіку до відповідних засобів перевірки. Віртуалізована мережева функція VNF виконує аналіз доступних для перевірки даних і повертає результат до керуючого компонента. Такий підхід дозволяє логічно відокремити процедури аналізу загроз від фізичної мережевої інфраструктури.

У запропонованій архітектурі доцільно передбачити окрему підпрограму прийняття рішень щодо оброблення мережевих потоків. Вона отримує відомості про з'єднання, результати антивірусного аналізу та чинні правила безпеки. На

їхній основі визначається необхідність продовження передавання даних, додаткової перевірки або ізоляції джерела загрози.

Послідовність функціонування цього модуля представлено на рисунку 4.2. Його робота повинна бути узгоджена зі станом мережевих з'єднань і поточною конфігурацією віртуалізованого середовища.

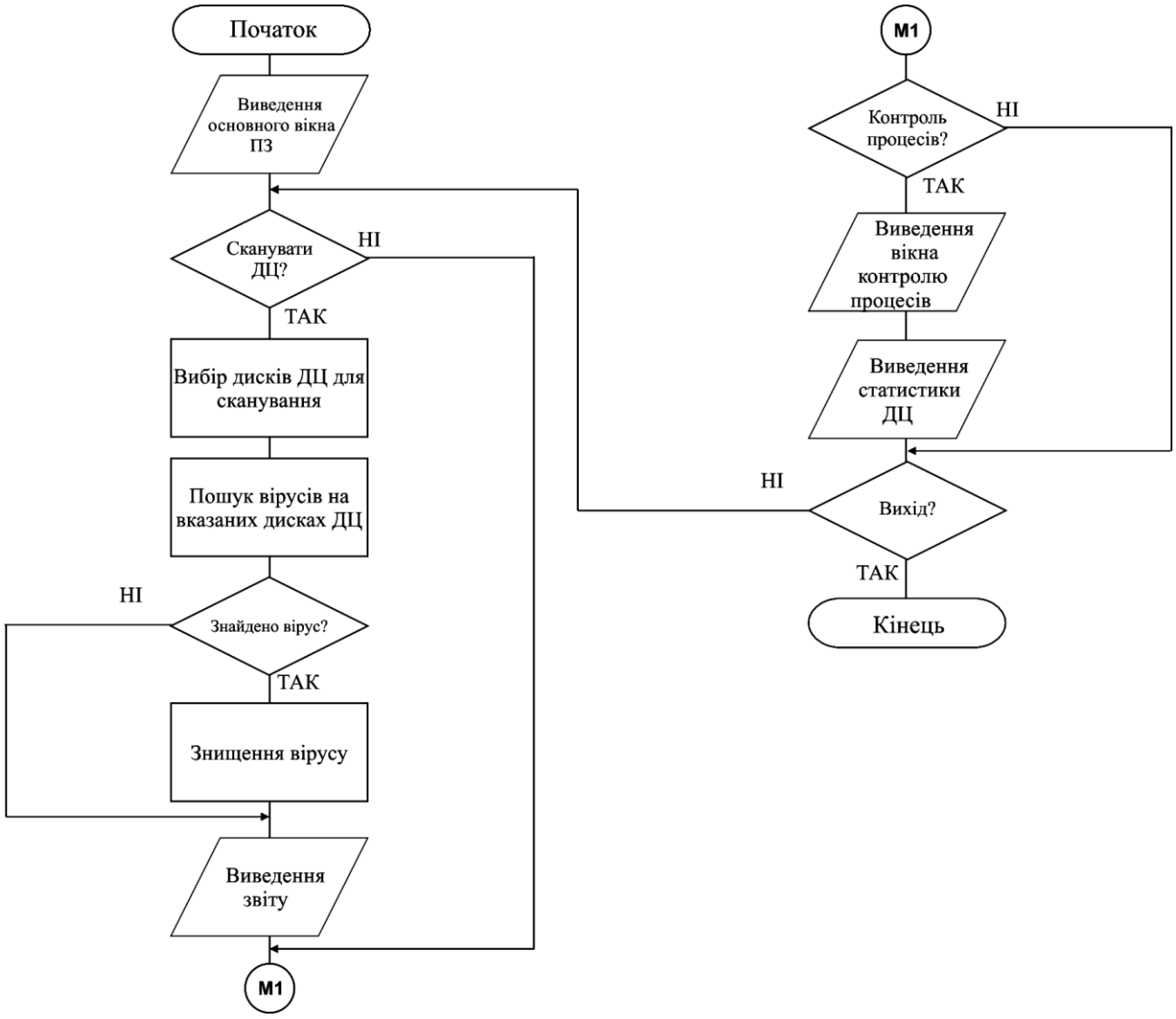


Рисунок 4.1 – Блок-схема основної програми

Особливістю мережевого антивірусного захисту дата-центру є необхідність контролю не лише зовнішніх з'єднань, а й внутрішнього обміну даними між віртуальними машинами. Такий обмін часто здійснюється через

віртуальні комутатори та не проходить через фізичні засоби захисту на периметрі мережі. Тому алгоритми повинні забезпечувати виявлення потоків усередині окремого фізичного сервера, між серверами віртуалізації та між ізольованими мережевими сегментами.

Важливо також розмежовувати аналіз мережевих метаданих і безпосередню антивірусну перевірку вмісту. Для встановлення характеристик потоку достатньо обробити заголовки пакетів, статистику передавання та відомості про з'єднання. Для сигнатурного виявлення шкідливих файлів необхідно отримати відповідний інформаційний об'єкт у придатному для сканування вигляді. Наявність зашифрованого мережевого трафіку не гарантує можливості перевірки його корисного навантаження. Тому система повинна враховувати доступність вмісту та не ототожнювати відсутність виявленої загрози з підтвердженою безпечністю даних.

Формування мережевої моделі та початкових правил захисту

Перед початком аналізу трафіку необхідно визначити склад доступних віртуальних ресурсів і зв'язки між ними. Вхідними даними є інформація про віртуальні комутатори, мережеві інтерфейси, адреси вузлів, належність до VLAN або інших логічних сегментів і стан підключень. Додатково можуть враховуватися ідентифікатори віртуальних машин, отримані через інтерфейс керування інфраструктурою віртуалізації.

На першому етапі контролер встановлює зв'язок із доступними комутаторами та отримує відомості про їхні порти. Після цього формується внутрішня модель мережі. Її доцільно представляти орієнтованим графом (G=(V,E)), де (V) визначає множину вузлів, а (E) характеризує доступні логічні з'єднання. До вузлів можуть належати віртуальні комутатори, мережеві шлюзи та точки підключення віртуальних машин.

Кожному з'єднанню ставиться у відповідність набір характеристик, який містить пропускну здатність, поточну доступність, належність до сегмента та допустимі напрямки передавання даних. Для динамічної інфраструктури важливим є оновлення графа під час створення, видалення або міграції

віртуальних машин. Якщо мережевий інтерфейс переноситься на інший фізичний сервер, контролер повинен переглянути його розташування та правила передавання трафіку.

Наступним етапом є формування початкових політик безпеки. Вони визначають, які типи з'єднань підлягають обов'язковій інспекції, для яких дозволено передавання без додаткового аналізу та які повинні блокуватися незалежно від результатів антивірусної перевірки. Окремо необхідно виділити службовий трафік керування гіпервізорами, контролером SDN та сервісами віртуалізації.

Для збереження працездатності дата-центру політики доцільно групувати за рівнем критичності ресурсів. Наприклад, сегмент керування інфраструктурою повинен мати суворіші обмеження на встановлення нових з'єднань, ніж мережа прикладних сервісів. Водночас політика не повинна автоматично блокувати службові механізми забезпечення доступності, якщо така дія не передбачена конфігурацією.

Результатом початкової обробки є узгоджена множина правил, яка передається контролеру SDN. Перед встановленням кожне правило перевіряється на відповідність доступним мережевим сегментам, коректність адрес і конфлікти пріоритетів. Якщо конфігурація містить суперечливі умови, її застосування необхідно призупинити до встановлення однозначного порядку оброблення.

Оброблення мережевих потоків та визначення необхідності інспекції

Після ініціалізації системи основним об'єктом аналізу стає мережевий потік. Для потоків TCP та UDP його можна ідентифікувати за комбінацією адрес джерела й призначення, транспортного протоколу та номерів портів. У середовищі з кількома ізольованими мережами до цього набору потрібно додавати ідентифікатор мережевого сегмента. Це дозволяє розрізняти з'єднання з однаковими IP-адресами в різних віртуальних мережах.

Під час надходження потоку комутатор перевіряє наявність відповідного запису в таблиці OpenFlow. Якщо запис існує, пакети обробляються згідно з установленими діями. За відсутності правила може використовуватися механізм

звернення до контролера. При цьому для уникнення надмірного навантаження доцільно передавати лише необхідні для прийняття рішення метадані або обмежену кількість початкових пакетів.

Контролер визначає належність потоку до однієї з категорій. Перша категорія охоплює з'єднання, явно дозволені політикою. Друга містить потоки, які потребують додаткової перевірки. Третя категорія включає заборонені з'єднання. Окремий стан необхідно передбачити для випадків, коли аналіз неможливо виконати через технічні обмеження або недоступність відповідного модуля.

Логіку ухвалення рішення можна записати у вигляді функції

$$D(f) = \begin{cases} B, & P(f) = \text{deny}, \\ I, & P(f) = \text{inspect}, \\ A, & P(f) = \text{allow}, \\ U, & P(f) = \text{undefined}, \end{cases}$$

де (f) позначає мережевий потік, (P(f)) є результатом застосування політики безпеки, (B) означає блокування, (I) визначає направлення на інспекцію, (A) відповідає дозволеному передаванню, а (U) характеризує відсутність визначеного рішення.

Для реалізації такого механізму доцільно створити програмний модуль перевірки політик. Його можна побудувати на стандартних засобах Python. Наступний фрагмент ілюструє можливий спосіб програмного представлення рішення. Він показує логіку оброблення, яку необхідно інтегрувати з конкретним SDN-контролером.

```
from dataclasses import dataclass
from enum import Enum

# Можливі результати аналізу мережевого потоку
class Action(Enum):
    ALLOW = "allow"
    INSPECT = "inspect"
    BLOCK = "block"
    UNDEFINED = "undefined"

# Метадані потоку, отримані від мережевого компонента
@dataclass(frozen=True)
```

```
class NetworkFlow:
    source_ip: str
    destination_ip: str
    protocol: str
    destination_port: int
    segment_id: str

# Визначення дії відповідно до заданої політики
def evaluate_policy(flow, policy):
    if not 0 <= flow.destination_port <= 65535:
        return Action.UNDEFINED

    # Явна заборона має найвищий пріоритет
    if policy.is_denied(flow):
        return Action.BLOCK

    # Перевірка необхідності антивірусної інспекції
    if policy.requires_inspection(flow):
        return Action.INSPECT

    # Дозвіл застосовується лише за наявності правила
    if policy.is_allowed(flow):
        return Action.ALLOW

    # Невідомі потоки не вважаються безпечними
    return Action.UNDEFINED
```

Наведений механізм відокремлює перевірку мережевих параметрів від безпосереднього виконання дій комутатором. Об'єкт policy представляє зовнішній компонент зберігання та застосування правил. Його методи повинні враховувати не тільки параметри з'єднання, а й сегментацію інфраструктури, права джерела та пріоритети політик.

Важливо забезпечити однакову обробку повторних пакетів одного з'єднання. Для цього контролер підтримує таблицю активних потоків зі станами прийнятого рішення. Якщо для потоку вже встановлено правило й умови безпеки не змінилися, повторна інспекція кожного пакета не потрібна. Винятком є випадки, коли необхідно перевірити переданий файл або інший окремий інформаційний об'єкт.

Стан потоку може змінюватися протягом його існування. Наприклад, початково дозволене з'єднання може передавати об'єкт, який виявиться шкідливим. У такій ситуації результат перевірки повинен мати пріоритет над раніше встановленим дозволом. Контролер скасовує відповідні правила передавання та застосовує нову політику до конкретного джерела або з'єднання.

Для зниження кількості звернень до контролера використовуються часові параметри існування правил. Значення idle_timeout визначає строк зберігання запису за відсутності активності. Параметр hard_timeout обмежує загальний час його існування незалежно від активності потоку. Такі механізми дозволяють оновлювати політики та запобігати необмеженому накопиченню тимчасових записів.

Організація антивірусної перевірки у віртуалізованій мережевій функції

Після визначення необхідності інспекції система повинна забезпечити передавання відповідних даних до антивірусного сервісу. Для цього може застосовуватися окрема VNF, розміщена у віртуальній машині або контейнері з доступом до виділеної мережі аналізу. Її програмні компоненти не повинні мати необмеженого доступу до керуючої мережі дата-центру.

Вхідними даними для антивірусної перевірки є інформаційний об'єкт і службовий опис його походження. Опис може містити ідентифікатор потоку, джерело передавання, час отримання та контрольну суму. Сам файл повинен передаватися до модуля перевірки лише після виконання обмежень щодо максимального розміру й коректності отримання.

Отримання файлу з мережевого трафіку є окремим завданням. Якщо система працює з HTTP, поштовими вкладеннями або іншими підтримуваними протоколами, модуль інспекції може відновлювати інформаційний об'єкт із прикладного потоку. Для цього необхідно враховувати послідовність TCP-сегментів, повторні передавання, фрагментацію та завершеність прикладного повідомлення. Якщо дані не були зібрані повністю, об'єкт не повинен отримувати статус успішно перевіреного.

У випадку HTTPS та інших захищених протоколів безпосередня перевірка вмісту можлива лише за наявності законного й технічно передбаченого доступу до розшифрованих даних. Для цього може використовуватися перевірка на прикладному шлюзі або інтеграція із сервісом, який отримує файл після завершення захищеного сеансу. Якщо такого механізму немає, система обмежується аналізом доступних метаданих. У цьому випадку результат повинен характеризуватися як відсутність повної інспекції.

Як приклад антивірусного ядра можна використати службу clamd. Вона підтримує сканування об'єктів, переданих клієнтським застосунком через локальний сокет або мережеве з'єднання. Протокол INSTREAM дозволяє послідовно надсилати вміст файлу блоками. Максимальний розмір потоку обмежується параметром StreamMaxLength. Слід також враховувати, що стандартний TCP-інтерфейс clamd не забезпечує власної автентифікації та шифрування.

Програмну взаємодію із сервісом перевірки можна організувати за допомогою Python. Для локального підключення використовується Unix-сокет. Наведений приклад демонструє механізм потокового передавання файлу до clamd та оброблення відповіді.

```
import socket
import struct
from pathlib import Path
from enum import Enum

# Стани результату антивірусної перевірки
class ScanResult(Enum):
    CLEAN = "clean"
    INFECTED = "infected"
    ERROR = "error"
    TOO_LARGE = "too_large"
def scan_file(file_path, socket_path, max_size):
    path = Path(file_path)
    try:
        # Перевірка існування та розміру об'єкта
        if not path.is_file():
            return ScanResult.ERROR
        if path.stat().st_size > max_size:
            return ScanResult.TOO_LARGE
        # Підключення до локального сервісу ClamAV
        with socket.socket(
            socket.AF_UNIX, socket.SOCK_STREAM
        ) as client:
            client.settimeout(15)
            client.connect(socket_path)
```

```
            # Початок потокового сканування
            client.sendall(b"zINSTREAM\0")
            total_size = 0
            with path.open("rb") as file:
                while True:
                    chunk = file.read(8192)
                    if not chunk:
                        break
                    total_size += len(chunk)
                    # Обмеження розміру переданих даних
                    if total_size > max_size:
                        return ScanResult.TOO_LARGE
                    client.sendall(
                        struct.pack("!I", len(chunk))
                    )
                    client.sendall(chunk)

            # Позначення завершення передавання
            client.sendall(struct.pack("!I", 0))
            # Отримання відповіді антивіруса
            response = bytearray()
            while b"\0" not in response:
                data = client.recv(4096)
                if not data:
                    return ScanResult.ERROR
                response.extend(data)

            message = response.split(b"\0", 1)[0].decode(
                "utf-8", errors="replace"
            )
            if message.endswith(" FOUND"):
                return ScanResult.INFECTED

            if message.endswith(" OK"):
                return ScanResult.CLEAN
            return ScanResult.ERROR
    except (OSError, ValueError):
        # Помилка сканування не означає чистий файл
        return ScanResult.ERROR
```

Цей фрагмент демонструє лише клієнтську частину взаємодії з антивірусним ядром. Для застосування в системі необхідно додатково організувати безпечне отримання файлів, керування тимчасовим сховищем та обмеження одночасних перевірок. Значення max_size повинно узгоджуватися з налаштуваннями clamd. Параметр socket_path задається конфігурацією середовища, а не фіксується безпосередньо в програмному коді.

Особливу увагу слід приділити інтерпретації результату. Статус CLEAN означає, що антивірусний механізм завершив перевірку переданого об'єкта та не виявив відомих йому загроз. Він не є абсолютним підтвердженням безпечності файлу. Статус INFECTED вказує на виявлення шкідливого вмісту.

Стан ERROR характеризує невиконану перевірку, а TOO_LARGE свідчить про перевищення встановленого обмеження.

Для запобігання помилковому дозволу на передавання даних стани ERROR і TOO_LARGE повинні оброблятися окремо від CLEAN.

Залежно від політики об'єкт може направлятися на повторну перевірку, утримуватися в контрольованому сховищі або блокуватися. Для критичних сегментів доцільно забороняти передавання інформаційних об'єктів, які не пройшли обов'язкову інспекцію.

Після завершення перевірки формується результат, який пов'язується з вихідним потоком та ідентифікатором конкретного об'єкта.

Це необхідно для коректної роботи з'єднань, що передають кілька файлів протягом одного сеансу. Якщо один файл є шкідливим, система повинна застосувати дію відповідно до політики, не приписуючи автоматично такий самий результат усім іншим об'єктам.

Механізм застосування мережевих рішень та ізоляції загроз

Отриманий результат антивірусної перевірки передається до керуючого модуля. Його завдання полягає в перетворенні логічного рішення на конкретну мережеву дію. Для цього необхідно зіставити результат із поточним станом потоку, конфігурацією комутатора та політикою відповідного сегмента.

Якщо загрозу не виявлено й усі інші умови політики виконано, контролер може дозволити подальше передавання інформаційного об'єкта.

Для цього використовується відповідне правило OpenFlow або команда прикладному шлюзу.

За наявності небезпечного об'єкта встановлюється обмеження, яке запобігає його доставці або подальшому поширенню.

Логіку прийняття остаточного рішення можна подати функцією

$$R(f,s,p) = \begin{cases} B, & s = \text{infected}, \\ A, & s = \text{clean} \wedge p = \text{allow}, \\ H, & s \in \{\text{error}, \text{too_large}\}, \\ B, & p = \text{deny}, \\ I, & \text{в інших випадках}, \end{cases}$$

де f є ідентифікатором потоку, s характеризує результат антивірусної перевірки, (p) визначає чинну політику, (B) означає блокування, (A) відповідає дозволу

передавання, (H) визначає утримання об'єкта до прийняття додаткового рішення, а (I) означає необхідність подальшої інспекції. У реалізації перевірку явних заборон політики потрібно виконувати до надання остаточного дозволу.

Наведена модель описує логіку вибору дії, а не повний набір правил конкретного контролера.

Для блокування небезпечного потоку може використовуватися встановлення запису OpenFlow без дій передавання. Такий запис повинен мати достатній пріоритет для перекриття раніше встановлених дозволів. При цьому умови відповідності необхідно задавати достатньо точно, щоб не заблокувати інші з'єднання того самого віртуального сервера.

Приклад створення тимчасового правила блокування TCP-трафіку на основі синтаксису контролера Ryu наведено нижче. Функція призначена для виклику з компонента, який уже має авторизований доступ до об'єкта datapath. Вона не виконує самостійного пошуку комутатора або встановлення керуючого з'єднання.

```
from ipaddress import IPv4Address

def install_tcp_block(
    datapath,
    source_ip,
    destination_ip,
    destination_port,
    timeout=300
):
    # Перевірка мережевих параметрів
    source_ip = str(IPv4Address(source_ip))
    destination_ip = str(IPv4Address(destination_ip))

    if not 1 <= destination_port <= 65535:
        raise ValueError("Некоректний TCP-порт")

    if not 1 <= timeout <= 3600:
        raise ValueError("Некоректний час дії правила")

    ofproto = datapath.ofproto
    parser = datapath.ofproto_parser

    # Правило застосовується до конкретного
    # напрямку TCP-з'єднання
    match = parser.OFPMatch(
        eth_type=0x0800,
        ip_proto=6,
        ipv4_src=source_ip,
        ipv4_dst=destination_ip,
        tcp_dst=destination_port
    )
```

```
# Відсутність вихідних дій означає скидання
# пакетів, які відповідають умовам
instructions = []

flow_mod = parser.OFPFlowMod(
    datapath=datapath,
    cookie=0xA510,
    table_id=0,
    command=ofproto.OFPFC_ADD,
    priority=35000,
    match=match,
    instructions=instructions,
    idle_timeout=0,
    hard_timeout=timeout,
    flags=ofproto.OFPFF_SEND_FLOW_REM
)

# Надсилання команди на комутатор
datapath.send_msg(flow_mod)
```

У наведеному прикладі правило діє протягом обмеженого часу. Це дозволяє уникнути необмеженого збереження тимчасового блокування. Значення priority визначає порядок порівняння із записами тієї самої таблиці. Водночас ефективність правила залежить від фактичної структури OpenFlow-конвеєра. Для багатотабличної схеми необхідно вибирати таблицю, через яку дійсно проходить контрольований трафік.

Крім надсилання команди, керуючий модуль повинен підтверджувати її застосування. Для цього можна використовувати повідомлення OpenFlow Barrier та перевірку наявності запису в таблиці потоків. Сам факт успішного передавання команди контролером не доводить, що комутатор установив правило без помилки.

При виявленні загрози може виникнути необхідність ізолювати всю віртуальну машину. У такому випадку недостатньо заблокувати лише окреме TCP-з'єднання. Контролер повинен сформувати набір правил, які обмежують небезпечний мережевий обмін, але залишають дозволений адміністративний доступ. Обсяг ізоляції визначається рівнем критичності інциденту та політикою безпеки.

Для уникнення дублювання дій необхідно вести облік уже встановлених блокувань. Якщо від антивірусного модуля повторно надходить повідомлення про ту саму загрозу, контролер повинен зіставити його з попереднім рішенням. За відсутності змін повторне встановлення ідентичного правила не потрібне. Такий

механізм зменшує кількість службових повідомлень і спрощує подальше скасування обмежень.

Скасування ізоляції є окремою процедурою. Воно повинно виконуватися після завершення визначених умов перевірки та відповідного адміністративного рішення. Видалення запису блокування не повинно порушувати правила інших сегментів або автоматично відкривати доступ, який був заборонений початковою політикою.

Розподіл навантаження між віртуалізованими антивірусними сервісами

У віртуалізованому дата-центрі кількість одночасних мережевих з'єднань може змінюватися залежно від навантаження прикладних сервісів. Через це використання одного екземпляра антивірусної VNF створює ризик накопичення черги перевірок. Для забезпечення масштабованості доцільно передбачити можливість розподілення інформаційних об'єктів між кількома екземплярами антивірусного сервісу.

Вхідними параметрами такого алгоритму є кількість активних запитів, завантаженість процесорів, використання оперативної пам'яті та середня тривалість сканування. Додатково необхідно контролювати стан бази сигнатур і доступність кожного екземпляра VNF. Сервіс із застарілою або недоступною базою не повинен автоматично отримувати завдання, для яких потрібна актуальна сигнатурна перевірка.

Для оцінювання рівня завантаження системи можна використовувати коефіцієнт

$$\rho = (\lambda)/(m\mu),$$

де λ означає середню інтенсивність надходження завдань сканування, m визначає кількість активних екземплярів антивірусного сервісу, а μ є середньою інтенсивністю обслуговування одного екземпляра.

Для спрощеної стаціонарної моделі необхідною умовою стійкості черги є $\rho < 1$. Однак реальна продуктивність залежить від розміру та типу файлів, структури архівів, обсягу сигнатурної бази й доступних ресурсів. Тому наведене

співвідношення доцільно використовувати для попереднього оцінювання навантаження, а не як достатню умову гарантованої затримки.

Під час вибору екземпляра VNF алгоритм спочатку виключає недоступні служби. Далі перевіряє ресурсні обмеження й довжину черги. Якщо доступні кілька придатних екземплярів, завдання може передаватися до найменш завантаженого. Для уникнення концентрації навантаження необхідно враховувати не тільки кількість запитів, а й очікуваний обсяг даних.

Розподілення навантаження повинно виконуватися на рівні завершених завдань перевірки або узгоджених мережевих сеансів. Довільне перенаправлення окремих пакетів одного TCP-з'єднання між різними станозалежними сервісами може порушити відновлення даних. Тому алгоритм повинен забезпечувати сталість призначення сервісу протягом оброблення конкретного потоку.

Якщо навантаження перевищує можливості доступних екземплярів, нові завдання розміщуються в обмеженій черзі. За досягнення максимального розміру черги система повинна застосовувати визначену політику перевантаження. Для об'єктів, які потребують обов'язкового контролю, доцільно використовувати утримання або відхилення передавання, а не автоматичний дозвіл без перевірки.

Експериментальна перевірка алгоритмічних рішень

Для підтвердження правильності запропонованих алгоритмів необхідно організувати експериментальне дослідження у віртуалізованому тестовому середовищі. Його структура повинна відтворювати основні властивості дата-центру, зокрема наявність кількох віртуальних машин, програмних комутаторів, SDN-контролера та антивірусної VNF. Експерименти доцільно проводити в ізольованому сегменті, щоб перевірка блокувань не впливала на робочу інфраструктуру.

Перший етап дослідження полягає у перевірці коректності встановлення мережевих політик. Для цього формуються потоки з різними адресами, транспортними протоколами та портами. Система повинна визначити належність кожного потоку до відповідної категорії та застосувати передбачену дію.

Результат перевіряється шляхом порівняння фактичних правил у таблицях комутаторів із заданими політиками.

Наступний етап спрямований на перевірку антивірусної функції. Для нього використовуються безпечні тестові об'єкти та спеціальні файли, призначені для перевірки реакції антивірусних програм. Зокрема, може застосовуватися стандартний тестовий файл EICAR. Його використання дозволяє перевірити проходження сигналу про виявлення загрози без застосування реального шкідливого програмного забезпечення.

Окремо необхідно перевірити оброблення чистих файлів, пошкоджених інформаційних об'єктів, неповних передавань і файлів, які перевищують дозволений розмір. Для кожного випадку фіксуються результат сканування, рішення контролера та фактична мережева дія. Перевірка повинна встановити, чи не отримують неперевірені об'єкти помилковий статус безпечних.

Для оцінювання точності виявлення на наборі об'єктів із відомими еталонними мітками можна використовувати показники повноти та частоти помилкових спрацювань. Повнота виявлення визначається співвідношенням

$$DR = (TP)/(TP + FN),$$

де TP характеризує кількість правильно виявлених шкідливих об'єктів, а FN означає кількість шкідливих об'єктів, які не були виявлені.

Частоту помилкових позитивних рішень можна обчислити як

$$FPR = (FP)/(FP + TN),$$

де FP визначає кількість безпечних об'єктів, помилково класифікованих як шкідливі, а TN відповідає кількості правильно визначених безпечних об'єктів. Обидва показники мають сенс лише за наявності репрезентативного набору перевірених об'єктів. Зразки, для яких сканування не відбулося, необхідно обліковувати окремо.

Для оцінювання впливу системи захисту на продуктивність мережі потрібно порівняти характеристики передавання без антивірусної інспекції та після її увімкнення. Основними параметрами є пропускна здатність, затримка

встановлення з'єднання, час перевірки інформаційного об'єкта та частка втрачених пакетів.

Відносне зниження пропускної здатності можна визначити за формулою

$$\Delta T = (T_0 - T_1)/(T_0) \cdot 100\%,$$

де T_0 характеризує пропускну здатність без залучення антивірусного сервісу, а T_1 визначає пропускну здатність у режимі захисту. Значення показника залежить від інтенсивності трафіку, розмірів об'єктів та апаратних ресурсів, тому його необхідно встановлювати експериментально.

Для вимірювання часу оброблення інформаційного об'єкта доцільно фіксувати момент його надходження до модуля інспекції та момент отримання остаточного результату. Загальна тривалість містить час очікування в черзі, передавання даних до VNF, сканування й повернення рішення. Окреме вимірювання цих складових дозволяє встановити джерело найбільшої затримки.

Масштабованість перевіряється шляхом поступового збільшення кількості одночасних завдань. Спочатку вимірювання виконуються з одним екземпляром VNF. Потім кількість екземплярів збільшується за незмінних характеристик окремого сервісу. Порівнюються сумарна продуктивність, середній час очікування та завантаження обчислювальних ресурсів.

Для оцінювання ефективності горизонтального масштабування можна використовувати коефіцієнт

$$E(m) = \big(X(m)\big)/\big(mX(1)\big),$$

де $X(m)$ означає продуктивність системи за наявності m екземплярів VNF, а $X(1)$ визначає продуктивність одного екземпляра в аналогічних умовах. Зменшення цього показника зі збільшенням кількості екземплярів може свідчити про зростання накладних витрат або появу спільного обмежувального ресурсу.

5 МЕТОДИКА ВПРОВАДЖЕННЯ СИСТЕМИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ

Програмне забезпечення системи мережевого антивірусного захисту віртуалізованої інфраструктури дата-центру призначене для централізованого контролю мережевих з'єднань, перевірки переданих інформаційних об'єктів та автоматизованого застосування захисних правил.

Використання технологій SDN/NFV дозволяє розділити функції керування мережевими потоками та антивірусного аналізу. Робота програмного комплексу передбачає взаємодію керуючого модуля, програмних комутаторів і віртуалізованих сервісів перевірки. Головне вікно програми показано на рисунку 5.1.

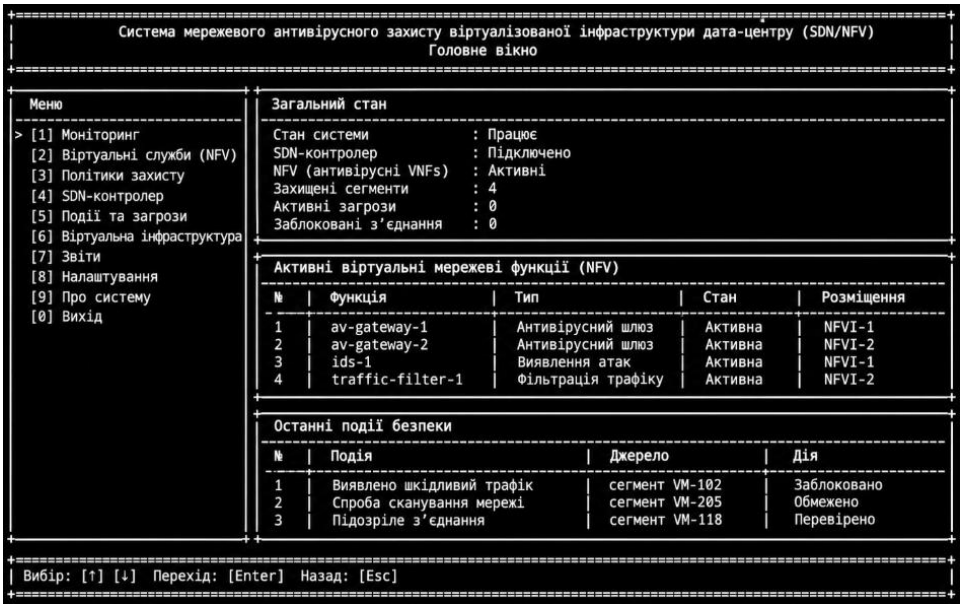


Рисунок 5.1 – Головне вікно ПЗ

Для впровадження системи в експлуатацію необхідно підготувати програмне середовище, яке забезпечує функціонування віртуальних машин, програмно-визначеної мережі та антивірусних компонентів.

Мережеву комутацію можна організувати за допомогою Open vSwitch, а керування потоками реалізувати через SDN-контролер із підтримкою OpenFlow 1.3. Для антивірусної перевірки передбачається використання ClamAV із фоновою службою clamd. Програмні модулі керування та взаємодії між компонентами можуть бути реалізовані мовою Python. Зазначений набір технологій становить рекомендовану конфігурацію відповідно до розглянутого алгоритмічного рішення.

Для ідентифікації програмного продукту необхідно передбачити відображення відомостей про його розробника. Такі відомості дозволяють пов'язати програмну реалізацію з відповідною кваліфікаційною роботою та визначити авторство представленого рішення. Інформацію про автора доцільно розміщувати в окремому інформаційному розділі програмного інтерфейсу без включення конфіденційних відомостей про середовище експлуатації. Авторські дані розробленого програмного забезпечення представлено на рисунку 5.2.

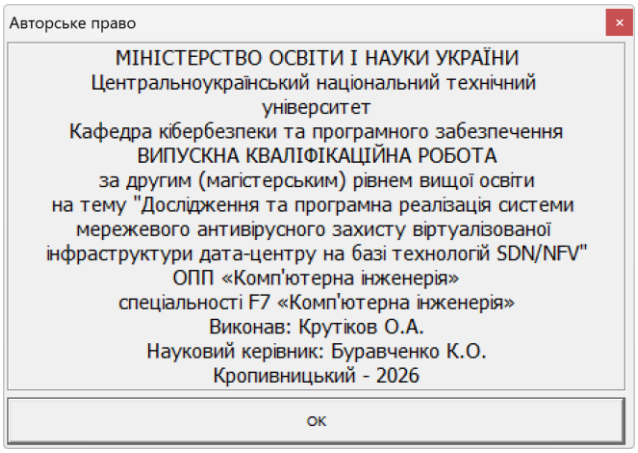


Рисунок 5.2 – Шаблонна форма авторського права

Апаратні вимоги залежать від кількості віртуальних машин, інтенсивності мережевого трафіку та обсягу даних, які підлягають перевірці. Сервер повинен мати процесор із підтримкою апаратної віртуалізації, достатній обсяг

оперативної пам'яті та дисковий простір для розміщення програмних компонентів.

Окремі ресурси необхідно передбачити для антивірусної VNF, оскільки сканування файлів може створювати значне навантаження на процесор і підсистему пам'яті. Для експлуатації важливо забезпечити можливість збільшення кількості екземплярів антивірусного сервісу без зміни основної мережевої архітектури.

Підготовка мережевого середовища розпочинається з визначення логічних сегментів дата-центру. Доцільно відокремити мережу керування, сегмент обміну даними між віртуальними машинами та мережу антивірусної інспекції. Такий розподіл обмежує доступ прикладних вузлів до службових інтерфейсів системи захисту. Для кожного сегмента встановлюються параметри адресації, правила маршрутизації та допустимі напрямки передавання трафіку. Необхідно також перевірити зв'язність між SDN-контролером і керованими комутаторами.

Функціональність антивірусного компонента доцільно перевіряти за допомогою безпечних тестових файлів, зокрема стандартного тестового об'єкта EICAR. Під час перевірки контролюється проходження запиту до антивірусного ядра, отримання результату та застосування відповідної мережевої дії. Додатково перевіряються ситуації з неповними файлами, перевищенням допустимого розміру та недоступністю служби сканування. Такі об'єкти не повинні автоматично отримувати статус безпечних. Результати перевірок фіксуються в журналі подій для подальшого аналізу.

6 НАУКОВА НОВИЗНА

У випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти розроблено програмне забезпечення, яке призначено для системи мережевого антивірусного захисту віртуалізованої інфраструктури дата-центру на базі технологій SDN/NFV.

Метою розробки є дослідження та програмна реалізація системи мережевого антивірусного захисту віртуалізованої інфраструктури дата-центру на базі технологій SDN/NFV.

Об'єктом дослідження є процес мережевого антивірусного захисту віртуалізованої інфраструктури дата-центру на базі технологій SDN/NFV.

Предметом дослідження є методи мережевого антивірусного захисту віртуалізованої інфраструктури дата-центру на базі технологій SDN/NFV.

Методи дослідження базуються на методах побудови комп'ютерних мереж, методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Наукова новизна отриманих результатів. У процесі рішення завдань, обумовлених цілями дослідження, отримані наступні результати:

– Удосконалено метод мережевого антивірусного захисту віртуалізованої інфраструктури дата-центру на базі технологій SDN/NFV.

– Розроблено вітчизняний продукт мережевого антивірусного захисту віртуалізованої інфраструктури дата-центру на базі технологій SDN/NFV, який має більш широкі можливості, на відміну від існуючих аналогів.

7 ЗАХОДИ З ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ

7.1 Вступ

Законом України “Про охорону праці” [3] регламентуються загальні положення державної політики в галузі охорони праці, а конкретизуються ці положення нормативно-правовими актами про охорону праці, зокрема Наказом Міністерства соціальної політики України 14.02.2018 № 207, який зареєстровано в Міністерстві юстиції України 25 квітня 2018 р. за №508/31960 «Про затвердження Вимог щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями» [5], яким затверджено нормативно-правовий акт з охорони праці НПАОП 0.00-7.15-18, «Правила охорони праці під час експлуатації електронно-обчислювальних машин», та «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» ДСанПіН 3.3.2-007-97.

Програмісти у процесі роботи мають негативний вплив на органи зору, а також мають значну розумову напругою і нервово-емоційне навантаження. Руки (суглоби пальців та м'язи рук) при роботі з клавіатурою мають теж істотне навантаженням. До шкідливих факторів, які впливають на робітників галузі інформаційних технологій (ІТ) спеціалісти відносять високочастотні електромагнітні коливання (випромінювання) роботи апаратної частини ЕОМ та виділення шкідливих газів.

Ці шкідливі фактори можуть привести до професійних захворювань.

Розглянемо шкідливі чинники роботи програмістів керуючись наступними нормативно-правовими актами: «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» ДСанПіН 3.3.2-007-98 [5], та «Вимоги щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями» НПАОП 0.00-7.15-17.

Умови праці програміста включають наступні фактори:

– параметри повітряного середовища в приміщенні;

– вентиляція приміщення;

– освітлення приміщення;

– параметри повітряного середовища в приміщенні, тощо.

Щоб запропонувати заходи щодо зменшення негативного впливу комп'ютера на організм людини визначемо фактори, які можуть викликати професійне захворювання і впливають на працездатність програміста.

7.2 Шкідливі і небезпечні фактори при роботі з комп'ютером

Електронно-обчислювальна машин (ЕОМ) та інше обладнання є джерелами небезпеки ураження електричним струмом. Так як робота програміста характеризується істотним зоровим навантаженням, то вимагає належного освітлення. У приміщенні, в якому працюють програмісти необхідно створити належний мікроклімат, праметри якого регламентуються, Державними санітарними правилами і нормами, зокрема ДСанПіН 3.3.2.007-97.

При роботі з використанням ЕОМ відзначають наступні небезпечні та шкідливі фактори:

– ризик виникнення надзвичайних ситуацій природного або штучного характеру на об'єкті або території.

– ризик виникнення пожежі;

– негативний вплив на органи зору людини;

– ризики ураження електричним струмом;

– недостатня, або надмірна освітленість робочого місця;

– електромагнітні (у тому числі високочастотні) електромагнітні випромінювання (коливання);

– несприятливі мікрокліматичні умови;

– нервово-емоційна напруженість праці;

– інтелектуальні навантаження;

– монотонність праці;

– невідповідність ергономічних показників робочого місця діючим вимогам;

– шум;

– статичні навантаження на кістково-м’язовий аппарат.

7.3 Аналіз санітарно-гігієнічних умов праці на робочому місці програміста

Розглянемо умови праці у приміщенні, в якому працюють програмісти. Геометричні розміри приміщення наведено у таблиці 7.1.

Таблиця 7.1 – Розміри приміщення

Найменування	Значення, м
Ширина	3
Довжина	4,6
Висота	3

Таблиця 7.2 – Площа та обсяг приміщення, на одного працюючого*

Геометрична характеристика	Одиниця виміру	Нормативне значення*	Фактичне значення
Площа, S	$м^2$	не менше 6.0	6,9
Об'єм, V	$м^3$	не менше 20.0	20,7

* Згідно ДСанПіН 3.3.2.007-98 (Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин).

У зазначеному приміщенні працюють двоє людей. За даними, які наведено у табл. 7.1, та табл. 7.2, можна зробити висновок, що площа та об’єм приміщення у розрахунку на одно робоче місце програміста не відповідають

нормативним вимогам ДСанПіН 3.3.2-007-98 «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» [5], але відповідають нормативним вимогам Наказу Міністерства соціальної політики України № 207, від 14.02.2018 «Про затвердження Вимог щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями» [5] та НПАОП 0.00-1.28-10 «Правила охорони праці під час експлуатації електронно-обчислювальних машин»). Таним чином можна зробити висновок, що санітарно-гігієнічні умови праці на робочому місці програміста відповідають вимогам.

Температура повітря в приміщенні визначається впливом температури зовнішнього повітря і тепловою енергією, яка виділяється всередині приміщення. Джерелами виділення теплоти в даному приміщенні є електроустаткування, освітлювальні прилади, а також люди. У світлий час доби джерелом надлишкового тепла є сонячна радіація. Згідно Постанови № 42 від 01.12.1999 Головного державного санітарного лікаря України, робота, виконувана в даному приміщенні, відноситься до категорії Іа. В цьому випадку людина витрачає енергії до 120 ккал у годину. Вологість повітря в приміщенні визначається впливом багатьох факторів, серед яких: вологість атмосферного повітря, виділення вологи людьми (при диханні та випарами з поверхні шкіри).

Мікроклімат повітряного середовища в приміщенні характеризується запиленістю та загазованістю повітря. Мікроклімат приміщення визначається діючим на організм людини поєднанням, вологості, температури, швидкості руху повітря та інтенсивності теплового випромінювання. Аналіз мікроклімату складається з визначення зазначених вище факторів і порівняння результатів із встановленими нормами.

У таблиці 7.3 наведено оптимальні та фактичні значення параметрів мікроклімату як для категорії ваги робіт Іа, так і розглянутого приміщення. У приміщеннях, де встановлено ЕОМ, рекомендується застосування тільки оптимальних значень показників мікроклімату.

Проведений аналіз показує, що показники мікроклімату в приміщенні відповідають установленим нормам. Штучне опалення застосовується у холодний період року.

Таблиця 7.3 – Оптимальні і фактичні значення параметрів мікроклімату

Пора року	Оптимальні для Іа			Фактичні		
	Температура, °С	Волого-гість,%	Швидкість повітря, м/с	Температура, °С	Волого-гість %	Швидкість повітря, м/с
Холодна	22-24	40-60	0,1	22-24	40-55	0,12
Тепла	23-25	50-70	0,1	24-25	50-65	0,9

В літню пору застосовується кондиціонер.

Для боротьби з пилом робляться регулярні провітрювання та вологі прибирання приміщенні.

У приміщенні знаходяться наступні джерела шуму: принтер Xerox WorkCentre 3025BI (3025VBI), електродвигуни вентиляторів ЕОМ.

Одним з найважливіших факторів, які впливають на ефективність трудової діяльності людини та попереджають травматизм і професійні захворювання програмістів є освітлення на робочому місці.

З 2019 року діють Державні будівельні норми України “Природне і штучне освітлення” – ДБН В.2.5-28:2018 [1], у яких прописані вимоги до використання всіх освітлювальних приладів, у тому числі світлодіодних.

Працю працівника, який постійно працює за комп’ютером, згідно ДБН В.2.5-28:2018 [1], можна віднести до роботи з малою точністю (найменший розмір об'єкта розрізнення від 1 до 5 мм) V-го розряду зорової роботи, з великою контрастністю об'єкта розрізнення (символів на екрані дисплея), з темним тлом (під розряд зорової роботи В). Приміщення можна віднести до 1-ої групи приміщень, у яких проводиться розрізнення об'єктів зорової роботи при фіксованому напрямку лінії зору того, що працює на робочу поверхню. Для такого типу приміщень і розряду зорової роботи нормоване значення

коефіцієнта природної освітленості (КПО) робочої поверхні (при поєднаному, спільному освітленні), повинен становити не більше 1,5%, освітленість при штучному висвітленні повинна становити 300 Лк. [1], Крім того, все поле зору повинне бути освітлено достатньо рівномірно – це основна гігієнічна вимога. Оскільки яскраве світло на ділянці периферійного зору значно збільшує напруженість очей і, як наслідок, призводить до їх швидкої стомлюваності, ступінь освітлення приміщення і яскравість екрану комп'ютера повинні бути приблизно однаковими.

7.4 Розробка заходів з умов поліпшення охорони праці

Згідно аналізу умов праці в розглянутому приміщенні, ми одержали наступні результати:

– розмірі приміщення, у розрахунку на одному працюючого, відповідають нормативам;

– мікроклімат відповідає нормативному значенню;

– акустичні умови роботи не перевищують нормативних значень;

Таким чином можна припустити, що основною причиною можливого зниження працездатності програміста є психофізіологічний фактор, тому основна пропозиція буде така: дотримання позитивної психологічної атмосфери в колективі та регламентованого режиму праці та відпочинку, організація робочого місця з урахуванням ергономічних вимог.

Рекомендовані заходи: регулярні періодичні наочні огляди персоналом шляхів для евакуації людей із приміщення, відповідно до плану евакуації (який повинен розташовуватись на видному місці у приміщенні), включення до колективного договору мінімально можливого вмісту аптечок з обов’язковою наявністю масок-клапанів, або іншого спорядження для штучного дихання. Регулярна періодична перевірка параметрів заземлення та занулення (вимірювання опору ланцюга).

Регулярна наочне знайомство персоналу із шляхами для евакуації людей із приміщення відповідно до плану евакуації, забезпечення розподільних щитів спеціальними розетками з заземлюючими контактами; організація заземлення всіх приладів і пристроїв, які працюють при напрузі вище 36 В.

Так як при ураженні електричним струмом у людини може статися фібриляція шлуночків серця, в організації бажано мати дефібрилятор і підготовлений персонал для роботи з ним.

7.5 Розрахункова частина

Проведемо розрахунок штучного освітлення за методом коефіцієнта використання світлового потоку для приміщення ширина якого складає 3 м, довжина – 4,6 м, висота – 3 м.

У зазначеному приміщенні працює 1 особа.

Для того, щоб визначити потрібну кількість світильників, які повинні забезпечити нормований рівень освітленості, визначимо світловий потік, що падає на робочу поверхню за формулою:

$$F = E \cdot S \cdot K \cdot Z / n,$$

де:

F – світловий потік, що розраховується, Лм;

E – нормована мінімальна освітленість, Лк; *E* = 300 Лк;

S – площа освітлюваного приміщення (у нашому випадку *S*=3 х 4,6 = 13,8 м^2);

K – коефіцієнт запасу, що враховує зменшення світлового потоку лампи в результаті забруднення світильників в процесі експлуатації (його значення залежить від типу приміщення і характеру робіт, що проводяться в ньому, в нашому випадку *K* = 1,5);

Z – відношення середньої освітленості до мінімальної (зазвичай, приймається рівним 1.1... 1.2, в нашому випадку *Z* = 1,1);

n – коефіцієнт використання світлового потоку, (відношення світлового потоку, що падає на розрахункову поверхню, до сумарного потоку всіх ламп і обчислюється в долях одиниці; залежить від характеристик світильника, розмірів приміщення, забарвлення стін і стелі, що характеризуються коефіцієнтами відбиття від стін ($\rho_{стін.}$) і стелі ($\rho_{стелі}$), значення коефіцієнтів дорівнюють $\rho_{стін}$ = 50% і $\rho_{стелі}$ = 50%.

Обчислимо індекс приміщення за формулою:

$$i=S/(h(A+B)),$$

де:

S – площа приміщення, S = 13,8 м^2;

h – розрахункова висота підвісу, h = 3 м (співпадає з висотою стелі, оскільки лампи освітлення закріплюються на стелі);

A – ширина приміщення, A = 3 м;

B – довжина приміщення, B = 4,6 м.

Підставимо всі значення у формулу та визначимо індекс приміщення:

$$i=0,43.$$

Знаючи індекс приміщення, за знаходимо n = 0,23 (з табличних даних коефіцієнтів використання світлового потоку (n) світильників з відповідним типом лампам). Підставимо всі значення у формулу, визначимо світловий потік: F=29700 Лм.

Для розрахунку будемо використовувати світлодіодні панелі LED панель 42Вт 6000К SUNLED 000000127, світловий потік яких $F_л$ = 3990 Лм.

Число ламп визначається по формулі:

$$N=F/F_л$$

де:

F – світловий потік,

$F_л$ – світловий потік однієї лампи.

Підставимо всі значення у формулу та визначимо кількість ламп:

$$N= 29700/ 3990=7,4 \text{ шт.}$$

Приймаємо необхідну кількість світлодіодних світильників 8 шт.

Висновки до розділу

Дотримання всіх необхідних умов праці не лише сприяє збереженню здоров’я працівників, а також підвищує ефективність виробництва в цілому.

З цих міркувань було здійснено аналіз умов праці, призначеного для праці програмістів, проведено розгляд небезпечних та шкідливих факторів, що негативно впливають на програмістів під час роботи. Виконано розрахунок штучного освітлення, як одного з ключових факторів впливу на працездатність та здоров’я програміста. Розроблено заходи з охорони праці.

8 ОСНОВНІ ВИСНОВКИ

Програмне забезпечення, створене в результаті виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти, призначено для системи мережевого антивірусного захисту віртуалізованої інфраструктури дата-центру на базі технологій SDN/NFV.

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

У випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти наведені теоретичне узагальнення й рішення наукового завдання дослідження методів мережевого антивірусного захисту віртуалізованої інфраструктури дата-центру на базі технологій SDN/NFV.

Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем мережевого антивірусного захисту віртуалізованої інфраструктури дата-центру на базі технологій SDN/NFV.

– Досліджена система мережевого антивірусного захисту віртуалізованої інфраструктури дата-центру на базі технологій SDN/NFV.

– На основі отриманих результатів досліджень створена програмна реалізація системи мережевого антивірусного захисту віртуалізованої інфраструктури дата-центру на базі технологій SDN/NFV.

Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання мережевого антивірусного захисту віртуалізованої інфраструктури дата-центру на базі технологій SDN/NFV.

Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

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 створені 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. 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 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.

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.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Крутіков О.А. Дослідження та програмна реалізація системи мережевого антивірусного захисту віртуалізованої інфраструктури дата-центру на базі технологій SDN/NFV // Збірник праць молодих науковців ЦНТУ. – Вип. 17. – Кропивницький: ЦНТУ, 2027.

2. Samir Kumar Rakshit. Ethical Hacker's Penetration Testing Guide. BPB Online. 2022. 509 p.

3. Corey J. Ball. Hacking APIs. No Starch Press. 2022. 353 p.

4. Kevin Beaver. Hacking for Dummies. John Wiley & Sons. 2022. 419 p.

5. Mark S. Merkow. Practical Security for Agile and DevOps. CRC Press. 2022. 236 p

6. Derek Fisher. Application Security Program Handbook. Manning Publications. 2021. 155 p.

7. Cameron Wyatt PH.D. Kali Linux Tutorial. Independently published. 2021. 60 p.

8. Богаченко, С., Смірнов, О., Буравченко, К., Смірнова, Т., Конопліцька-Слободенюк, О., Якименко, Н., Смірнов, С. «Обмеження ресурсів мобільних та edge-платформ при розробці програмного забезпечення для реалізації та оптимізації моделей машинного навчання». *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, 2026, т. 2 № 34, С. 677-686.

9. Вінтенко Б.Ю., Смірнова Т.В., Миронець І.В., Смірнов О.А., Буравченко К.О. «Метод оцінки функціональної стійкості комп'ютерно-орієнтованих процедур системи підтримки оперативного персоналу АЕС». *Системи управління, навігації та зв'язку*, 2026, вип. 2(84), С. 62-69.

10. Смірнова Т.В., Усік П.С., Лисенко І.А., Буравченко К.О., Смірнов О.А. «Методологія підтримки технологічних процесів у критичній інфраструктурі з забезпеченням безпеки інформації на основі хмарних технологій». *Безпека інформації.* 2025. Том 31 № 1. С. 49-60.

11. Смірнова Т.В., Буравченко К.О., Добринчук О.А., Смірнов С.А., Якименко Н.М., Смірнов О.А. «Хмарна технологія моніторингу ключових індикаторів ефективності технологічних процесів у критичній інфраструктурі». *Центральноукраїнський науковий вісник. Технічні науки.* 2025. № 12(43), ч. II. С. 36-54.

12. Вінтенко, Б.Ю., Миронець, І.В., Смірнов, О.А., Коваленко, О.В., Усік, П.С., Буравченко, К.О., Лисенко, І.А. «Логіко-структурна модель комп'ютерно-орієнтованої процедури системи підтримки оперативного персоналу АЕС». *Кібербезпека: освіта, наука, техніка*. 2025. Том 2 № 30. С. 413-427.

13. Vintenko, B., Myronets, I., Smirnov, O., Smirnova, T. «Enhancing the Reliability of Input Data for Nuclear Power Plant Operator Support Systems». *International Conference on Sensors, Devices and Systems. SDaS 2025. Lecture Notes in Electrical Engineering,* 2026. vol 1617. pp 3-12/

14. 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.

15. 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.

16. 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.

17. 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.

18. 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

19. 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.

20. 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.

21. 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.

22. 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.

23. 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.

24. 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.

25. 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.

26. 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.

27. Смірнова Т.В., Конопліцька-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.

28. 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.

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

30. 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.

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

32. 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

33. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchev, S. «Simulation of the cloud IoT-based monitoring system for critical

infrastructures». *CEUR Workshop Proceedings,* Volume 3530, 2023, pp. 256-265.

34. 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.

35. Smirnov, O., Lakhno, V., Akhmetov, B., Chubaievskyi, V., Khorolska, K., Bebeshko, B. «Selection of a Rational Composition of İnformation 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.

36. 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.

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

38. 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.

39. 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.

40. 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.

41. 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,

42. 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.

43. 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.

44. 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.

45. 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.

46. 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.

47. 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

48. 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.

49. 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.

50. 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.*

51. 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.

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

53. 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.

54. 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.

55. 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.

56. 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.

57. 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.