

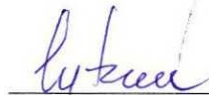
**МІНІСТЕРСТВО ФІНАНСІВ УКРАЇНИ
ДЕРЖАВНИЙ ПОДАТКОВИЙ УНІВЕРСИТЕТ**

**ФАКУЛЬТЕТ ФІНАНСІВ ТА ЦИФРОВИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНИХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ І
СИСТЕМ**

КВАЛІФІКАЦІЙНА РОБОТА

**на тему: МЕТОДИ ЦЕНТРАЛІЗОВАНОГО ЗБОРУ, КОРЕЛЯЦІЇ ТА
АНАЛІТИКИ ПОДІЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОРПОРАТИВНІЙ
МЕРЕЖІ НА БАЗІ FORTIANALYZER**

Здобувача вищої освіти першого (бакалаврського) рівня,
IV курсу, групи КБ-22-1, спеціальності 122 «Комп'ютерні науки»,
освітня програма «Інформаційні управляючі системи і технології (за галузями)»


(підпис)

Луценко Надія
Олександрівна
(прізвище, ім'я, по батькові)

Науковий керівник


(підпис)

Гладченко Оксана Вікторівна,
канд. пед. наук, доцент
(прізвище, ім'я, по батькові, науковий ступінь,
вчене звання)

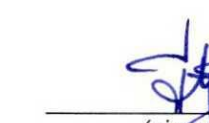
Керівник освітньо-
професійної програми


(підпис)

Ніжегородцев Владислав
Олександрович, канд. пед.
наук, доцент
(прізвище, ім'я, по батькові, науковий ступінь,
вчене звання)

Допущено до захисту за рішенням кафедри комп'ютерних та інформаційних
технологій і систем протокол від « 12 » травня 2026 № 20

Завідувач кафедри


(підпис)

Філоненко Михайло
Миколайович, канд. фіз.-мат.
наук, доцент
(прізвище, ім'я, по батькові, науковий ступінь,
вчене звання)

Ірпінь – 2026

Реєстрація № 51

24.05.2026

(дата)



(підпис відповідальної особи)

Результати перевірки

До захисту

(до захисту, на доопрацювання)

12.05.2026

(дата)



(підпис)

Результат захисту

5 (відмінно)

(оцінка)

09.06.2026

(дата)



(підпис)

Голова комісії:



(підпис)

О.С. Дюбанов

Члени комісії:



(підпис)

М.М. Філоненко



(підпис)

В.О. Ніжегородцев



(підпис)

А.А. Омельчук

БЛАНК ОЦІНЮВАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Об'єкти контролю	Діапазон оцінки в балах	Фактична кількість балів	Примітки	Дата, П.І.Б.: керівника, голови комісії членів комісії, секретаря, (підписи)
ОЦІНЮВАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ КОМІСІЄЮ ПО ЗАХИСТУ				
1. Зміст випускної роботи (якість теоретичного матеріалу, його зв'язок з практичним, вміння представляти матеріал в логічній послідовності, наявність висновків та пропозицій)	від 0 до 30	30		09.06.2026 Гладченко О.В. Дюбанов О.С. Філоненко М.М. Ніжегородцев В.О. Омельчук А.А. Суховерховська Л.П.
2. Дотримання вимог щодо оформлення	від 0 до 10	9		
3. Вчасне виконання роботи на всіх етапах у встановлені кафедрою терміни	від 0 до 5	5		
4. Рецензент	від 0 до 5	5		
РАЗОМ БАЛІВ	від 0 до 50	49		

Оцінювання кваліфікаційної роботи науковим керівником – 49 балів.

ПЕРЕВЕДЕННЯ ОЦІНКИ ЗА 100-БАЛЬНОЮ ШКАЛОЮ ДО НАЦІОНАЛЬНОЇ ШКАЛИ ТА ШКАЛИ ЄКТС

Оцінка за 100-бальною шкалою	Оцінка за шкалою ЄКТС	Оцінка за національною шкалою	Дата	П.І.Б.: голови, членів комісії, секретаря, (підпис)
98	A	5 (відмінно)	09.06.2026	Дюбанов О.С. Філоненко М.М. Ніжегородцев В.О. Омельчук А.А. Суховерховська Л.П.

ПРАВИЛА ПЕРЕВЕДЕННЯ ОЦІНОК ДО НАЦІОНАЛЬНОЇ ШКАЛИ ТА ШКАЛИ ЄКТС

Оцінка за 100-бальною шкалою	Оцінка за шкалою ЄКТС	Оцінка за національною шкалою
90-100	A	5 (відмінно)
80-89	B	4 (добре)
70-79	C	
60-69	D	
50-59	E	3 (задовільно)
35-49	FX	2 (незадовільно)

Факультет фінансів та цифрових технологій
Кафедра комп'ютерних та інформаційних технологій і систем
Галузь знань: 12 «Інформаційні технології»
Спеціальність: 122 «Комп'ютерні науки»
Освітня програма: «Інформаційні управляючі системи і технології (за галузями)»

Затверджую
Завідувач кафедри  Філоненко
М.М.
«01» грудня 2025

Завдання на кваліфікаційну роботу
здобувачу вищої освіти
Луценко Надії Олександрівні
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи методи централізованого збору, кореляції та аналітики подій інформаційної безпеки в корпоративній мережі на базі fortianalyzer
Затверджена наказом ректора від «28» листопада 2025 № 1526
2. Строк здачі закінченої роботи «08» травня 2026
3. Мета роботи полягає в теоретичному обґрунтуванні, проектуванні та практичному впровадженні системи централізованого збору та аналізу подій на базі FortiAnalyzer для підвищення оперативності виявлення атак.
Об'єкт дослідження цілісні процеси моніторингу та всебічного аналізу подій інформаційної безпеки.
Предмет дослідження сукупність методів, алгоритмів та прикладних програмних інструментів централізованого збору, кореляції та аналітики подій безпеки.
Орієнтовна база дослідження ТОВ «ЛАБОРАТОРІЯ КОМП'ЮТЕРНОЇ КРИМІНАЛІСТИКИ».
4. Вихідні дані до роботи журнали реєстрації подій (логи) сегментів корпоративної мережі, технічна документація та віртуальні образи платформи FortiAnalyzer VM.
5. Перелік графічного матеріалу схеми логічної структури віртуальних мереж стенда, графіки прогнозованого зростання обсягів баз даних логів, екранні форми інтерфейсів командного рядка, панелі управління FortiView та кастомних аналітичних звітів (Layouts).
6. Зміст кваліфікаційної роботи (перелік питань за кожним розділом)
ВСТУП РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ МОНІТОРИНГУ ТА АНАЛІЗУ ПОДІЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 1.1. Роль та місце централізованого збору логів у системі захисту корпоративної мережі 1.2. Огляд сучасних методів кореляції та аналітики подій безпеки 1.3. Порівняльний аналіз рішень для збору та аналізу подій РОЗДІЛ 2. ПРОЄКТУВАННЯ ТА ПРАКТИЧНА РЕАЛІЗАЦІЯ СИСТЕМИ ЗБОРУ ПОДІЙ НА БАЗІ FORTIANALYZER 2.1. Моделювання інфраструктури та розгортання віртуального середовища FortiAnalyzer VM 2.2. Розробка та впровадження правил кореляції для виявлення цілеспрямованих атак 2.3. Побудова аналітичних звітів та візуалізація інцидентів безпеки РОЗДІЛ 3. ПРОПОЗИЦІЇ ЩОДО ОПТИМІЗАЦІЇ МОНІТОРИНГУ ТА ОЦІНКА 3.1. Розробка рекомендацій щодо автоматизації реагування на інциденти 3.2. Оцінка продуктивності та масштабованості впровадженої системи ВИСНОВКИ СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

7. Календарний план виконання роботи

№ п/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	
		За планом	Фактично
1	2	3	4
1	Вибір теми, підбір літературних джерел, формування структури кваліфікаційної роботи	До 30.10.2025	15.10.2025
2	I розділ (розкрити сутність і стан дослідження наукової проблематики роботи, після чого навести її загальну характеристику; огляд літератури за темою і вибір конкретних напрямів досліджень)	26.12.2025	20.12.2025
3	II розділ (аналіз експериментальної частини про методики досліджень)	18.02.2026	17.02.2026
4	III розділ (проведені теоретичні і (або) експериментальні дослідження та проєктні рішення)	16.04.2026	10.04.2026
5	Висновки	01.05.2026	01.05.2026
6	Доопрацювання роботи з урахуванням зауважень наукового керівника	07.05.2026	07.05.2026
7	Отримання відгуку керівника	29.05.2026	29.05.2026
8	Отримання зовнішньої рецензії	01.06.2026	01.06.2026

8. Дата видачі завдання «01» грудня 2025

9. Керівник кваліфікаційної роботи


(підпис)

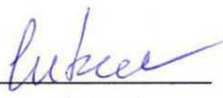
Гладченко О
(прізвище, ініціали)

10. Керівник освітньо-професійної програми


(підпис)

Ніжегородце
(прізвище, ініціали)

11. Завдання до виконання отримав здобувач вищої освіти


(підпис)

Луценко Н.О
(прізвище, ініціали)

АНОТАЦІЯ

МЕТОДИ ЦЕНТРАЛІЗОВАНОГО ЗБОРУ, КОРЕЛЯЦІЇ ТА АНАЛІТИКИ ПОДІЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОРПОРАТИВНІЙ МЕРЕЖІ НА БАЗІ FORTIANALYZER

Мета роботи полягає в теоретичному обґрунтуванні, проектуванні та практичному впровадженні системи централізованого збору та аналізу подій на базі FortiAnalyzer для підвищення оперативності виявлення цілеспрямованих атак та оптимізації процесів реагування на інциденти.

Завданнями роботи є дослідження ролі централізованого логування в інфраструктурі, проведення порівняльного аналізу SIEM-рішень, моделювання віртуального середовища та розгортання FortiAnalyzer VM, конфігурування захищених каналів інтеграції з мережевими пристроями, розробка кастомних правил кореляції для детектування атак та побудова системи візуалізації й аналітичної звітності.

Предметом дослідження є сукупність методів, алгоритмів та прикладних програмних інструментів централізованого збору, кореляції та аналітики подій безпеки, реалізованих на базі віртуалізованої платформи FortiAnalyzer.

Об'єктом дослідження виступають цілісні процеси моніторингу та всебічного аналізу подій інформаційної безпеки, що виникають у межах сучасної корпоративної мережевої інфраструктури.

Базою дослідження виступає ТОВ «ЛАБОРАТОРІЯ КОМП'ЮТЕРНОЇ КРИМІНАЛІСТИКИ».

За результатами дослідження сформульовані підходи до адаптації обробників подій під специфіку сучасних загроз, пропозиції щодо переходу до проактивного захисту через сценарії автоматизованого реагування Automation Stitches, а також рекомендації з оптимізації продуктивності реляційної бази даних логів у віртуальному середовищі VMware ESXi.

Одержані результати можуть бути використані IT-спеціалістами, мережевими інженерами та аналітиками SOC-центрів для модернізації діючих систем моніторингу безпеки, автоматизації обробки великих масивів телеметрії, оперативного розслідування інцидентів та прискорення підготовки експертних форензик-висновків.

Кваліфікаційна робота містить **52** сторінки, **1** таблицю, **20** рисунків, список використаних джерел з **40** найменувань, **0** додатків.

Ключові слова: FortiAnalyzer, SIEM, централізоване логування, правила кореляції, моніторинг мережі, інформаційна безпека, VMware ESXi, інциденти безпеки.

Рік виконання кваліфікаційної роботи — 2026.

Рік захисту роботи — 2026

ABSTRACT

METHODS OF CENTRALIZED COLLECTION, CORRELATION, AND ANALYTICS OF INFORMATION SECURITY EVENTS IN AN ENTERPRISE NETWORK BASED ON FORTIANALYZER

The objective of the work lies in the theoretical substantiation, design, and practical implementation of a centralized event collection and analysis system based on FortiAnalyzer to increase the efficiency of targeted attack detection and optimize incident response processes.

The tasks of the work are to study the role of centralized logging in the infrastructure, conduct a comparative analysis of SIEM solutions, model the virtual environment and deploy FortiAnalyzer VM, configure secure integration channels with network devices, develop custom correlation rules for attack detection, and build a visualization and analytical reporting system.

The subject of the research is a set of methods, algorithms, and applied software tools for centralized collection, correlation, and analytics of security events implemented on the basis of the virtualized FortiAnalyzer platform.

The object of the research is the comprehensive processes of monitoring and comprehensive analysis of information security events occurring within a modern enterprise network infrastructure.

The base of the research is "COMPUTER FORENSICS LABORATORY" LLC (CyberLab).

Based on the research results, approaches to adapting event handlers to the specifics of modern threats, proposals for transitioning to proactive defense via Automation Stitches automated response scenarios, as well as recommendations for optimizing the performance of the relational log database in the VMware ESXi virtual environment are formulated.

The obtained results can be used by IT specialists, network engineers, and SOC analysts to modernize existing security monitoring systems, automate the processing of large telemetry volumes, promptly investigate incidents, and accelerate the preparation of expert forensic conclusions.

The qualification work contains 52 pages, 1 table, 20 figures, a list of used sources of 40 titles, 0 appendices.

Keywords: FortiAnalyzer, SIEM, centralized logging, correlation rules, network monitoring, information security, VMware ESXi, security incidents.

Year of qualification work execution — 2026.

Year of work defense — 2026.

ЗМІСТ

ПЕРЕЛІК ОСНОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ	3
ВСТУП.....	6
РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ МОНІТОРИНГУ ТА АНАЛІЗУ ПОДІЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.....	9
1.1. Роль та місце централізованого збору логів у системі захисту корпоративної мережі.....	9
1.2. Огляд сучасних методів кореляції та аналітики подій безпеки	12
1.3. Порівняльний аналіз рішень для збору та аналізу подій	15
РОЗДІЛ 2. ПРОЄКТУВАННЯ ТА ПРАКТИЧНА РЕАЛІЗАЦІЯ СИСТЕМИ ЗБОРУ ПОДІЙ НА БАЗІ FORTIANALYZER	18
2.1. Моделювання інфраструктури та розгортання віртуального середовища FortiAnalyzer VM.....	18
2.2. Конфігурування механізмів інтеграції та збору даних з мережевих пристроїв	22
2.3. Розробка та впровадження правил кореляції для виявлення цілеспрямованих атак.	26
2.4. Побудова аналітичних звітів та візуалізація інцидентів безпеки	30
РОЗДІЛ 3. ПРОПОЗИЦІЇ ЩОДО ОПТИМІЗАЦІЇ МОНІТОРИНГУ ТА ОЦІНКА	34
3.1. Розробка рекомендацій щодо автоматизації реагування на інциденти.....	34
3.2. Оцінка продуктивності та масштабованості впровадженої системи	39
ВИСНОВКИ	45
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	48

ПЕРЕЛІК ОСНОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ADOM (Administrative Domain) — адміністративний домен; технологія логічного сегментування журналів реєстрації та конфігурацій пристроїв у межах однієї системи управління.

API (Application Programming Interface) — інтерфейс прикладного програмування; набір визначень та протоколів, що дозволяє різному програмному забезпеченню взаємодіяти між собою.

APT (Advanced Persistent Threat) — складна цілеспрямована загроза; тривала, багатоетапна та висококоординована кібератака, спрямована на конкретну інфраструктуру.

C&C / C2 (Command and Control) — командний центр; віддалений сервер, який використовується зловмисниками для управління шкідливим програмним забезпеченням в інфікованій мережі.

CLI (Command Line Interface) — інтерфейс командного рядка; текстовий інтерфейс керування операційною системою чи обладнанням.

CPU (Central Processing Unit) — центральний процесор; головна обчислювальна одиниця апаратного комплексу чи віртуальної машини.

Dataset — набір даних; структурована сукупність інформації, яка формується за допомогою SQL-запитів до реляційної бази даних логів.

DDoS (Distributed Denial of Service) — розподілена атака на відмову в обслуговуванні; кібератака, що полягає у штучному перевантаженні мережевих ресурсів великою кількістю запитів із багатьох джерел.

DNS (Domain Name System) — система доменних імен; мережева служба для отримання IP-адреси за символьним ім'ям хоста.

ELK Stack (Elasticsearch, Logstash, Kibana) — відкритий стек програмного забезпечення для збору, глибокого пошуку та візуалізації великих масивів даних.

EPS (Events Per Second) — кількість подій за секунду; головна метрика швидкості обробки, нормалізації та запису рядків логів у SIEM-системах.

HTTPS (Hypertext Transfer Protocol Secure) — захищений протокол передачі гіпертексту; мережевий протокол, що підтримує шифрування даних за допомогою SSL/TLS.

IOPS (Input/Output Operations Per Second) — кількість операцій введення-виведення за секунду; основна метрика продуктивності дискової підсистеми накопичувачів.

IP (Internet Protocol) — міжмережевий протокол; базовий протокол мережевого рівня, що забезпечує адресацію та маршрутизацію пакетів.

IPS (Intrusion Prevention System) — система запобігання вторгненням; програмний чи апаратний модуль для виявлення та негайного блокування шкідливої мережевої активності.

ISO/IEC 27001 — міжнародний стандарт, що містить вимоги до побудови, розгортання та розвитку систем управління інформаційною безпекою підприємства.

ITSM (IT Service Management) — управління IT-сервісами; стратегічний підхід до формування, надання та підтримки інформаційних технологій на підприємстві.

LAN (Local Area Network) — локальна обчислювальна мережа; замкнена мережева інфраструктура підприємства або офісу.

MTTD (Mean Time to Detect) — середній час до виявлення; метрика, що визначає тривалість періоду від моменту проникнення загрози до її фіксації системою моніторингу.

MTTR (Mean Time to Respond / Repair) — середній час до реагування; тривалість періоду від моменту детектування інциденту безпеки до його остаточної нейтралізації.

NGFW (Next-Generation Firewall) — міжмережевий екран нового покоління; пристрій фільтрації трафіку, що поєднує функції класичного фаєрвола, системи IPS, контролю застосунків та глибокого аналізу пакетів.

OFTP (Original Fortinet Telemetry Protocol) — пропрієтарний протокол телеметрії компанії Fortinet, що функціонує поверх TCP/SSL для безпечного транзиту логів.

OVF (Open Virtualization Format) — відкритий формат віртуалізації; стандарт пакування, поширення та автоматизованого розгортання образів віртуальних машин.

PCI DSS (Payment Card Industry Data Security Standard) — стандарт безпеки даних індустрії платіжних карток.

RDP (Remote Desktop Protocol) — протокол віддаленого робочого столу; прикладний мережевий протокол для віддаленого керування операційними системами.

SIEM (Security Information and Event Management) — система управління інформаційною безпекою та подіями; технологічне рішення для централізованого збору, кореляції та аналізу логів.

SOAR (Security Orchestration, Automation, and Response) — система оркестрації, автоматизації та реагування на інциденти безпеки; технологічний комплекс для автоматизованого виконання Playbooks у гетерогенних мережах.

SOC (Security Operations Center) — центр оперативного керування безпекою; спеціалізований підрозділ організації, що здійснює безперервний моніторинг та ліквідацію кіберзагроз.

SPL (Search Processing Language) — спеціалізована мова обробки та виконання аналітичних запитів до неструктурованих даних у платформі Splunk.

SQL (Structured Query Language) — мова структурованих запитів; декларативна мова програмування для взаємодії з реляційними базами даних.

SSH (Secure Shell) — захищена оболонка; мережевий протокол сеансового рівня для безпечного віддаленого керування операційними системами та обладнанням через шифрований тунель.

SSL/TLS (Secure Sockets Layer / Transport Layer Security) — криптографічні протоколи для забезпечення захищеного з'єднання та шифрування транспортних каналів у мережі.

Syslog — стандартний протокол і формат передачі повідомлень про системні події та журнали реєстрації в комп'ютерних мережах.

TCP (Transmission Control Protocol) — протокол керування передачею; транспортний протокол мережі, орієнтований на обов'язкове встановлення з'єднання та гарантовану доставку даних.

UDP (User Datagram Protocol) — протокол користувацьких датаграм; швидкий транспортний протокол мережі, що функціонує без попереднього встановлення з'єднання та підтвердження доставки пакетів.

UEBA (User and Entity Behavior Analytics) — поведінкова аналітика користувачів та сутностей; технологія виявлення кіберзагроз шляхом пошуку статистичних аномалій відносно базового профілю нормальної активності хостів.

vCPU (Virtual Central Processing Unit) — віртуальний центральний процесор; обчислювальний ресурс, виділений гіпервізором для потреб конкретної віртуальної машини.

VLAN (Virtual Local Area Network) — віртуальна локальна комп'ютерна мережа; технологія логічної сегментації єдиної фізичної інфраструктури на кілька ізольованих доменів широкомовного посилення.

VM (Virtual Machine) — віртуальна машина; програмна або віртуалізована реалізація обчислювальної системи, що виконує програми подібно до фізичного комп'ютера.

vRAM (Virtual Random Access Memory) — віртуальна оперативна пам'ять; обсяг оперативної пам'яті, зарезервований на фізичному сервері для забезпечення роботи віртуальної машини.

ВСТУП

У сучасних умовах стрімкого розвитку цифрових технологій та ускладнення ландшафту кіберзагроз, забезпечення інформаційної безпеки корпоративних мереж стає пріоритетним завданням для стабільного функціонування будь-якої організації. Сучасна мережева інфраструктура щосекунди генерує колосальні обсяги даних у вигляді журналів реєстрації подій, які містять критично важливу інформацію про стан безпеки систем. Проте ключовою проблемою залишається фрагментарність цих даних та складність їх оперативної обробки. Без впровадження методів централізованого збору та інтелектуальної аналітики інформація про початкові етапи кібератак часто залишається непоміченою серед великої кількості системних повідомлень. Використання спеціалізованого аналітичного рішення FortiAnalyzer дозволяє не лише акумулювати логи з різних сегментів мережі, а й застосовувати складні механізми кореляції для ідентифікації аномальної активності в реальному часі. Це зумовлює актуальність даного дослідження, спрямованого на розробку та практичну реалізацію ефективної системи моніторингу, здатної трансформувати розрізнені технічні дані у чітко структуровані інциденти безпеки.

Важливий внесок у розробку теоретичних засад захисту інформації в мережах та управління інцидентами внесли українські науковці та методисти. Питання побудови надійних систем захисту безпосередньо в мережевих структурах, а також базові принципи функціонування та безпеки інформаційного простору ґрунтовно висвітлені у праці О. А. Смірнова та О. К. Коноплицької-Слободенюк [13], присвяченій інформаційній безпеці в комп'ютерних мережах. Крім того, фундаментальні підходи до забезпечення безпеки в системах підтримки прийняття рішень, що є критично важливим для аналітичної обробки та кореляції подій, закладені у дослідженнях В. В. Ковтунця, О. В. Нестеренка та О. І. Савенкова [9]. Ці праці складають надійну науково-методичну базу для розробки методів централізації та інтелектуального аналізу логів у межах даної кваліфікаційної роботи.

Об'єктом дослідження виступають цілісні процеси моніторингу та всебічного аналізу подій інформаційної безпеки, що виникають у межах сучасної корпоративної мережевої інфраструктури. Предметом дослідження є сукупність методів, алгоритмів та прикладних програмних інструментів централізованого збору, кореляції та аналітики подій безпеки, реалізованих на базі віртуалізованої платформи FortiAnalyzer.

Метою кваліфікаційної роботи є теоретичне обґрунтування, проєктування та практичне впровадження системи централізованого збору та аналізу подій на базі FortiAnalyzer для підвищення оперативності виявлення цілеспрямованих атак та оптимізації процесів реагування на інциденти. Для реалізації поставленої мети необхідно виконати низку взаємопов'язаних завдань, що включають дослідження ролі централізованого логування, порівняльний аналіз чинних SIEM-рішень, моделювання віртуальної інфраструктури та розгортання FortiAnalyzer VM. Особлива увага приділяється конфігуруванню механізмів інтеграції з мережевими пристроями, розробці специфічних правил кореляції для детектування атак та створенню системи візуалізації інцидентів через аналітичну звітність.

Методологічну базу роботи складає комплексний науковий підхід, що базується на використанні загальнонаукових методів аналізу та синтезу при вивченні теоретичних засад моніторингу, порівняльного методу — при оцінці технологічних рішень, а також методу комп'ютерного моделювання та експерименту. Останній є ключовим для практичного розділу роботи, оскільки дозволяє у віртуалізованому середовищі відтворити реальні сценарії виникнення інцидентів та перевірити ефективність налаштованих аналітичних механізмів без ризику для продуктивної мережі.

Наукова новизна отриманих результатів полягає в удосконаленні підходів до виявлення цілеспрямованих атак шляхом адаптації правил кореляції FortiAnalyzer під специфіку сучасних мережеских загроз. Практичне значення роботи полягає у створенні чинної моделі системи моніторингу, яка може бути масштабована та впроваджена в реальну корпоративну інфраструктуру для

забезпечення безперервного контролю стану інформаційної безпеки та автоматизації звітності для мережевих аналітиків.

Апробація результатів дослідження здійснювалася шляхом публікації основних теоретичних положень та практичних результатів кваліфікаційної роботи у наукових фахових виданнях та матеріалах міжнародних конференцій. Головні аспекти дослідження висвітлено у наукових статтях у журналах «Наука і техніка сьогодні» [6] та «Таврійський науковий вісник» [7], а також у тезах доповідей на Міжнародній науково-практичній конференції [4, 5] та на Всеукраїнській науково-практичній конференції з автоматичного управління [11].

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ МОНІТОРИНГУ ТА АНАЛІЗУ ПОДІЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Роль та місце централізованого збору логів у системі захисту корпоративної мережі

У сучасній архітектурі кібербезпеки процес журналювання виступає фундаментальним елементом, що забезпечує необхідну прозорість функціонування всієї мережевої інфраструктури [3, с. 24-45]. Кожна окрема подія, яка ініціюється в системі — від спроби автентифікації користувача до зміни правил фільтрації на міжмережевому екрані — неминуче фіксується у формі журналів реєстрації подій або логів (Рис. 1.1). Ці дані є первинним і найбільш правдивим джерелом інформації для моніторингу, проте в умовах великих корпоративних мереж, де кількість активних пристроїв може обчислюватися сотнями або тисячами, децентралізоване зберігання такої інформації безпосередньо на кінцевих вузлах робить процес оперативного аналізу фактично неможливим. Саме ця об’єктивна складність зумовлює перехід до стратегічної концепції централізованого збору даних, де всі журнали реєстрації акумулюються в єдиному захищеному сховищі, що стає «точкою істини» для адміністраторів безпеки та мережевих аналітиків.

User	Action	URL	Category
j_doe	✓ Allowed	https://google.com/search...	Search Engines
j_doe	✗ Blocked	https://googie.com/recovery	Phishing (Typosquatting)
admin_ops	✗ Blocked	https://accounts.googie.com/	Phishing

Рис. 1.1 Фрагмент журналу реєстрації подій із зафіксованою активністю адміністратора щодо автентифікації та зміни конфігурації мережі

Роль централізованого збору логів у загальній системі захисту визначається кількома критичними аспектами, першим з яких є забезпечення цілісності та невідворотності доказової бази. В умовах реального кіберінциденту зломисники, отримавши несанкціонований доступ до системи, першочергово

намагаються видалити або модифікувати локальні журнали реєстрації, щоб приховати сліди своєї активності та унеможливити подальше розслідування. Використання таких рішень, як FortiAnalyzer, дозволяє миттєво передавати копію кожного генерованого лога на віддалений сервер, доступ до якого суворо обмежений. Таким чином, навіть у разі повної компрометації окремого вузла мережі, повна хронологія дій нападника залишається збереженою у централізованому репозиторії, що є критично важливим для проведення подальшої комп'ютерної експертизи та форензики [25]. Крім того, централізація дозволяє подолати проблему фрагментарності даних, коли аналітик змушений збирати докази з різних інтерфейсів, що суттєво уповільнює швидкість реакції на загрозу.

```
[80][http-get-form] host: 192.168.100.155 login: admin password: password
[80][http-get-form] host: 192.168.100.155 login: admin password: p@ssword
[80][http-get-form] host: 192.168.100.155 login: admin password: 12345
[80][http-get-form] host: 192.168.100.155 login: admin password: 1234567890
[80][http-get-form] host: 192.168.100.155 login: admin password: Password
[80][http-get-form] host: 192.168.100.155 login: admin password: 123456
[80][http-get-form] host: 192.168.100.155 login: admin password: 1234567
[80][http-get-form] host: 192.168.100.155 login: admin password: 12345678
[80][http-get-form] host: 192.168.100.155 login: admin password: 1q2w3e4r
[80][http-get-form] host: 192.168.100.155 login: admin password: 123
[80][http-get-form] host: 192.168.100.155 login: admin password: 1
[80][http-get-form] host: 192.168.100.155 login: admin password: 12
1 of 1 target successfully completed, 12 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-07-27 15:28:24
```

Рис. 1.2 Процес автоматизованого перебору паролів (Brute-force атака) до облікового запису адміністратора

Централізований збір даних також виступає необхідним технічним підґрунтям для реалізації складних методів кореляції подій. Окремий запис про невдалу спробу доступу на сервері в ізольованому контексті може помилково трактуватися як випадкова помилка користувача. Однак, якщо централізована аналітична система фіксує ідентичні спроби входу на декількох критично важливих серверах одночасно, що супроводжуються аномальним трафіком з певної IP-адреси, система миттєво ідентифікує це як цілеспрямовану атаку типу «Brute-force» (Рис. 1.2) або початковий етап просування зловмисника всередині мережі [19]. Без консолідації логів у єдиному центрі виявлення таких

взаємозв'язків між розрізненими мережевими подіями стає технічно нездійсненним завданням, оскільки адміністратор не має можливості бачити цілісну картину стану інформаційної безпеки в режимі реального часу.

Місце централізованого збору в ієрархії захисних механізмів визначається його функцією як ядра аналітичної діяльності підприємства. Він дозволяє реалізувати безперервний моніторинг інфраструктури, забезпечуючи негайне виявлення будь-яких відхилень від встановлених профілів нормальної поведінки систем [6, с. 2110-2112]. Важливим є також аспект відповідності галузевим та державним стандартам безпеки, таким як ISO/IEC 27001 (Рис. 1.3), які висувають жорсткі вимоги щодо тривалості зберігання та регулярності аудиту журналів подій [4].



Рис. 1.3. Ключові переваги та функціональні цілі впровадження стандарту ISO 27001 у систему управління інформаційною безпекою підприємства

Таким чином, впровадження методів централізації перетворює пасивну функцію запису технічних параметрів на активний, проактивний інструмент захисту, що розглядається в сучасних дослідженнях безпеки комп'ютерних мереж [1, с. 110–115]. Це дозволяє службі безпеки підприємства не лише оперативно реагувати на фактичні інциденти та спроби компрометації вебресурсів [15], а й прогнозувати потенційні вектори атак, забезпечуючи високий рівень загальної кіберстійкості всієї корпоративної мережі.

1.2. Огляд сучасних методів кореляції та аналітики подій безпеки

Ефективність функціонування сучасних інтелектуальних систем моніторингу безпосередньо залежить від застосованих методів кореляції, які виступають складним аналітичним надбудованим шаром над процесами первинного збору, нормалізації та агрегації даних. У контексті кібербезпеки кореляція подій являє собою багатоетапний процес логічного та математичного зіставлення розрізнених технічних записів, отриманих з множини гетерогенних джерел у межах визначеного часового вікна, з метою ідентифікації прихованих причинно-наслідкових зв'язків, що вказують на підготовку або розвиток цілеспрямованої атаки. Основним стратегічним завданням даного етапу є критична трансформація колосального масиву сирих логів у обмежену кількість пріоритетних інцидентів, що потребують негайного втручання мережевого аналітика, що дозволяє суттєво мінімізувати час виявлення (MTTD) та час реагування (MTTR) на критичні загрози.

В основі архітектури сучасних аналітичних платформ, до яких належить і FortiAnalyzer, лежить детермінований метод кореляції, заснований на попередньо визначених правилах (Rule-based correlation).

Цей підхід передбачає розробку складних сценаріїв, де генерація сигналу про тривогу відбувається лише за умови виконання сукупності логічних операторів та досягнення встановлених кількісних порогів інтенсивності подій за певний проміжок часу [5].

Наприклад, алгоритмічна логіка може бути налаштована на виявлення специфічної послідовності невдалих спроб автентифікації на критичних сегментах мережі, що супроводжуються раптовою зміною конфігурації міжмережевого екрана або створенням нових привілейованих облікових записів. Перевагою таких детермінованих методів є надзвичайна точність детектування вже відомих векторів атак за допомогою сигнатурного аналізу та повна прозорість логіки прийняття рішень, що значно полегшує подальше розслідування інцидентів. Проте, згідно з сучасними науковими тенденціями, такі методи потребують безперервного оновлення бази правил та сценаріїв для

протидії новим, раніше невідомим типам кіберзагроз та експлуатації системних вразливостей (Zero-day exploits) [27, с. 2144–2147].

Паралельно з детермінованими підходами в інфраструктурах складних корпоративних систем активно інтегруються методи поведінкового аналізу (User and Entity Behavior Analytics, UEBA) [30] та аналізу статистичних аномалій (Рис. 1.4). На відміну від жорстко заданих правил, ці методи базуються на динамічній побудові математичного профілю «нормальної» активності кожного окремого об'єкта або суб'єкта мережі за допомогою методів описової статистики та передових алгоритмів машинного навчання, що дозволяє виявляти загрози на більш ранніх стадіях [4, с. 854–855].

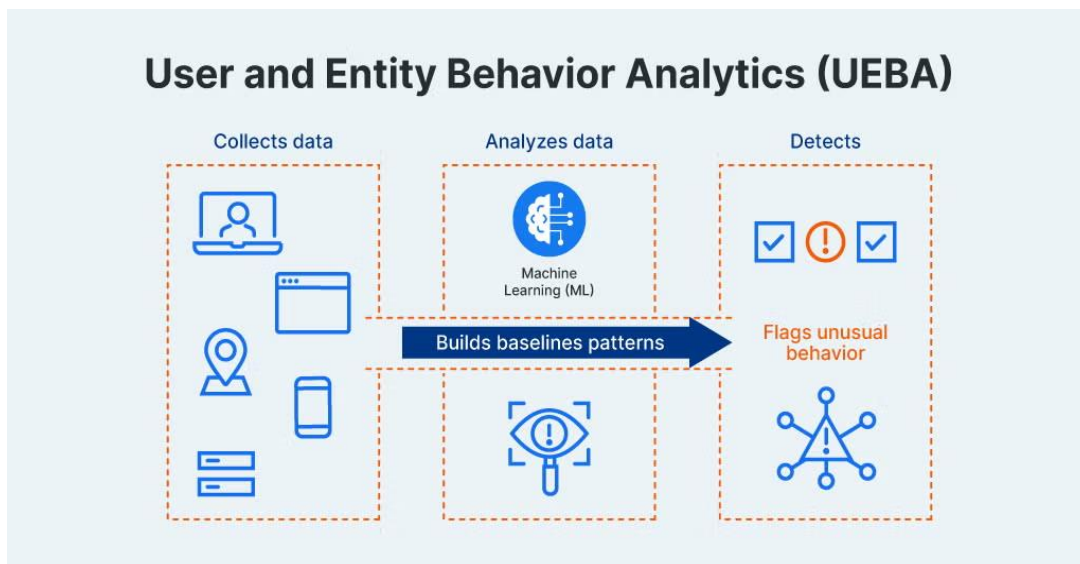


Рис. 1.4. Технологічний цикл виявлення аномальної поведінки об'єктів мережі через формування базових патернів активності

Будь-яке статистично значуще відхилення від сформованого еталонного профілю автоматично розглядається системою як аномальна активність. Даний підхід є критично важливим для ідентифікації складних цілеспрямованих атак (APT), які часто використовують легітимні інструменти системного адміністрування для латерального просування всередині мережевого периметра, не порушуючи при цьому формальних політик доступу, але демонструючи аномальну поведінкову динаміку [20].

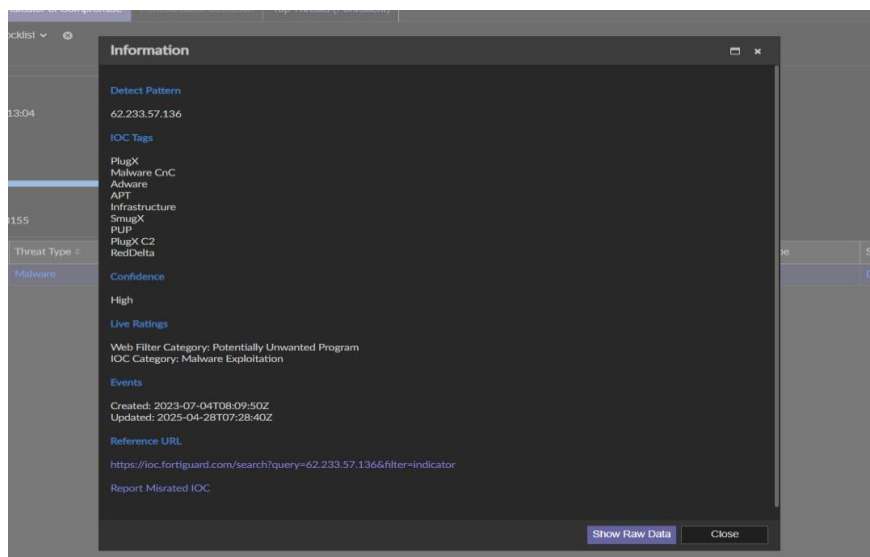


Рис. 1.5. Приклад реалізації концепції збагачення контексту події безпеки даними з глобальної бази репутації FortiGuard

Важливим компонентом глибинної аналітики є метод ієрархічної агрегації та інтелектуальної фільтрації, який дозволяє оптимізувати інформаційне навантаження на персонал SOC-центрів шляхом логічного згортання тисяч однотипних записів про мережеві події в один компактний та інформативний аналітичний об'єкт. Більш просунуті методи, реалізовані в екосистемах Fortinet Security Fabric, використовують передову концепцію збагачення контексту (Рис.1.5) .

У межах процесу, зображеного на рис. 1.5, кожен отриманий лог автоматично доповнюється зовнішньою контекстною інформацією, яка містить відомості про репутаційний статус IP-адрес, географічну прив'язку джерела трафіку, категорію загрози згідно з глобальними базами знань та відомостями про виявлені вразливості активів.

Таке збагачення перетворює сирий технічний запис на комплексний об'єкт аналізу, що дозволяє системі приймати високоточні автоматизовані рішення щодо ізоляції загроз на найбільш ранніх етапах їх виникнення, забезпечуючи стратегічну стійкість та цілісність всієї корпоративної інформаційної системи [7, с. 68–70].

1.3. Порівняльний аналіз рішень для збору та аналізу подій

Вибір оптимальної архітектури для централізованого збору та аналізу подій інформаційної безпеки є стратегічним етапом проєктування захищеної інфраструктури, оскільки кожне з наявних рішень базується на специфічній моделі обробки даних, що визначає швидкість реакції на інциденти.

На сучасному етапі розвитку технологій моніторингу домінують три основні підходи: спеціалізовані вендорні рішення, інтегровані в екосистему безпеки (FortiAnalyzer), універсальні комерційні SIEM-платформи (Splunk), можливості яких детально розглядаються в контексті управління ризиками [3, с. 10–32], та відкриті стеки для роботи з великими масивами даних (ELK Stack). Важливе значення при виборі архітектури має також врахування загальних концепцій розбудови безпекових контурів, серед яких окреме місце посідає модель нульової довіри (Zero Trust Architecture), що вимагає безперервної верифікації кожного суб'єкта та об'єкта мережі [26].

Дослідження сучасних викликів у побудові комп'ютерних мереж та захисту інфраструктур підтверджують, що фрагментарність систем логування призводить до критичного уповільнення виявлення цілеспрямованих атак та суттєво підвищує загальні ризики компрометації.

Система FortiAnalyzer вирізняється максимальною щільністю інтеграції в межах концепції Fortinet Security Fabric, що забезпечує автоматичне розпізнавання типів даних та використання специфічних для мережевого обладнання шаблонів аналітики без необхідності складної попередньої нормалізації. Дослідження підтверджують, що використання вендорно-орієнтованих систем дозволяє суттєво скоротити операційні витрати на підтримку інфраструктури моніторингу, оскільки такі системи мають вбудовані механізми автоматичного збагачення логів та готові правила кореляції, адаптовані під актуальні загрози.

Це має критичне значення для захисту цілісності та конфіденційності великих масивів даних (Big Data), зокрема у фінансовому та корпоративному секторах, де швидкість аналізу визначає стійкість системи до деструктивних

впливів [11, с. 43–45]. Застосування інноваційних методів обробки великих даних на базі машинного навчання та нейронних мереж дозволяє автоматизувати виявлення прихованих закономірностей у потоках телеметрії, що значно розширює можливості стандартних систем детектування [4, с. 854–856].

На противагу цьому, платформа Splunk пропонує ширші можливості для пошуку та візуалізації неструктурованих даних, використовуючи потужну мову запитів SPL [28].

Проте, масштабування таких систем у великих мережах вимагає значних апаратних ресурсів та високих фінансових витрат на ліцензування, що часто стає обмежувальним фактором для підприємств.

Крім того, побудова універсальних рішень потребує глибокого аналізу методів збору даних у гетерогенних мережевих структурах, де виникає необхідність ручного проєктування правил нормалізації та парсингу для кожного окремого типу джерела [1]. У випадку використання відкритих стеків технологій, зокрема ELK Stack, інженери стикаються з гострою потребою самостійного конфігурування та підтримки фільтрів Logstash, що вимагає постійних часових витрат на розробку кастомних рішень для приведення логів до єдиного аналітичного формату [17].

Організація захисту інформації в комп'ютерних системах за допомогою таких гнучких, але складних у налаштуванні інструментів перекладає основне навантаження на кваліфікацію персоналу та вимагає безперервного супроводу архітектури сховища [10, с. 112–115].

Для систематизації аналізу та обґрунтування вибору інструментарію доцільно порівняти ключові технічні характеристики зазначених рішень.

Аналіз даних, наведених у табл. 1.1, дозволяє дійти висновку, що попри універсальність системи Splunk та гнучкість стека ELK, найбільш раціональним рішенням для побудови архітектури безпеки на базі обладнання Fortinet є використання FortiAnalyzer. Ключовим аргументом виступає концепція «Zero-touch Analytics», за якої процеси нормалізації та збагачення контексту відбуваються автоматично на рівні нативної інтеграції пристроїв. Це критично

важливо для оперативного виявлення інцидентів, оскільки мінімізує вплив людського фактора на етапі попередньої обробки сирих даних.

Таблиця 1.1

Порівняльний аналіз систем моніторингу та аналізу подій безпеки

Критерій порівняння	FortiAnalyzer	Splunk Enterprise	ELK Stack (Elastic)
Архітектурна складність	Готове віртуальне, апаратне або хмарне ПЗ, що потребує лише базової ініціалізації мережевих параметрів	Модульна архітектура (Indexer, Forwarder, Search Head), що вимагає точного планування ресурсів	Потребує самостійної збірки та конфігурування взаємодії між Elasticsearch, Logstash та Kibana.
Нормалізація та парсинг	Нативна підтримка форматів логів Fortinet; автоматичне розпізнавання полів без втручання адміністратора.	Використання готових "Add-ons", але для кастомних джерел потрібне регулярне написання регулярних виразів.	Критична залежність від налаштування фільтрів Logstash або Ingest Pipelines для приведення даних до єдиного формату.
Аналітичний потенціал	Орієнтація на мережеві загрози, готові шаблони SOC-звітів та правил кореляції "з коробки".	Потужна мова SPL дозволяє створювати складні математичні запити для будь-яких типів даних	Ідеально підходить для швидкого пошуку в великих масивах, але логіку безпеки треба будувати вручну.
Інтелектуальні сервіси	Прямий зв'язок з сервісом FortiGuard для отримання вердиктів щодо шкідливого ПЗ та IP-репутації в реальному часі.	Можливість підключення зовнішніх Threat Intelligence потоків (наприклад, через TAXII/STIX), що потребує налаштування.	Потребує розробки власних скриптів або використання платних плагінів для інтеграції з базами знань про загрози.

Використання вендорно-орієнтованого підходу дозволяє реалізувати інтелектуальний моніторинг без необхідності утримувати значний штат розробників для написання кастомних парсерів та правил кореляції.

РОЗДІЛ 2. ПРОЄКТУВАННЯ ТА ПРАКТИЧНА РЕАЛІЗАЦІЯ СИСТЕМИ ЗБОРУ ПОДІЙ НА БАЗІ FORTIANALYZER

2.1. Моделювання інфраструктури та розгортання віртуального середовища FortiAnalyzer VM

Перехід від теоретичного обґрунтування до практичної реалізації системи моніторингу інформаційної безпеки вимагає чіткого моделювання архітектури майбутнього стенда. Ураховуючи високу вартість апаратних рішень класу SIEM та необхідність гнучкого масштабування ресурсів під час тестування, для розгортання інфраструктури було обрано метод комп'ютерного моделювання у віртуалізованому середовищі. Базовою платформою для побудови стенда виступає гіпервізор корпоративного рівня VMware ESXi [37]. Вибір гіпервізора першого типу зумовлений його здатністю забезпечувати прямий доступ віртуальних машин до апаратних ресурсів сервера, що є критично важливим фактором для стабільної роботи систем управління базами даних, на яких базується механізм індексації та зберігання журналів реєстрації подій у FortiAnalyzer. Процес віртуалізації операційних систем та розподілу обчислювальних потужностей хоста для дослідницьких і навчальних цілей спирається на перевірені методи конфігурування середовища [24, с. 54–56].

Першим етапом практичної реалізації є проєктування логічної топології віртуальної мережі. Для забезпечення ізоляції трафіку та дотримання базових принципів мережевої безпеки, на рівні гіпервізора було створено кілька ізольованих віртуальних комутаторів (vSwitch) та груп портів (Port Groups), архітектура яких повинна враховувати плани на випадок виникнення непередбачуваних критичних збоїв або аварійного відновлення [21]. Мережева інфраструктура стенда логічно розділена на сегмент управління, через який здійснюється адміністрування платформи, та внутрішній сегмент (LAN), що імітує корпоративну мережу, з якої генеруватиметься потік подій безпеки (Рис. 2.1).

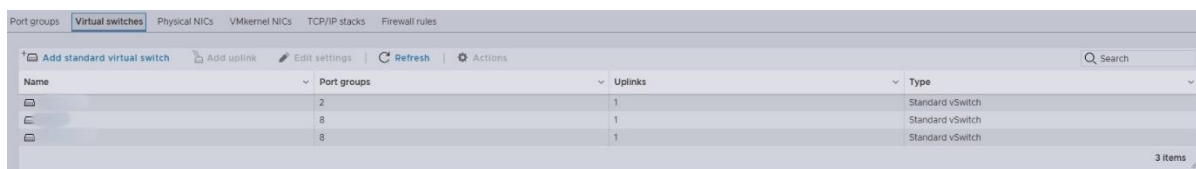


Рис. 2.1. Логічна структура віртуальних мереж стенда на базі гіпервізора VMware ESXi

Мережева інфраструктура стенда логічно розділена на сегмент управління, через який здійснюється адміністрування платформи, та внутрішній сегмент (LAN), що імітує корпоративну мережу, з якої генеруватиметься потік подій безпеки.

Процес безпосереднього розгортання аналітичного ядра системи розпочинається з отримання офіційного дистрибутиву програмного забезпечення.

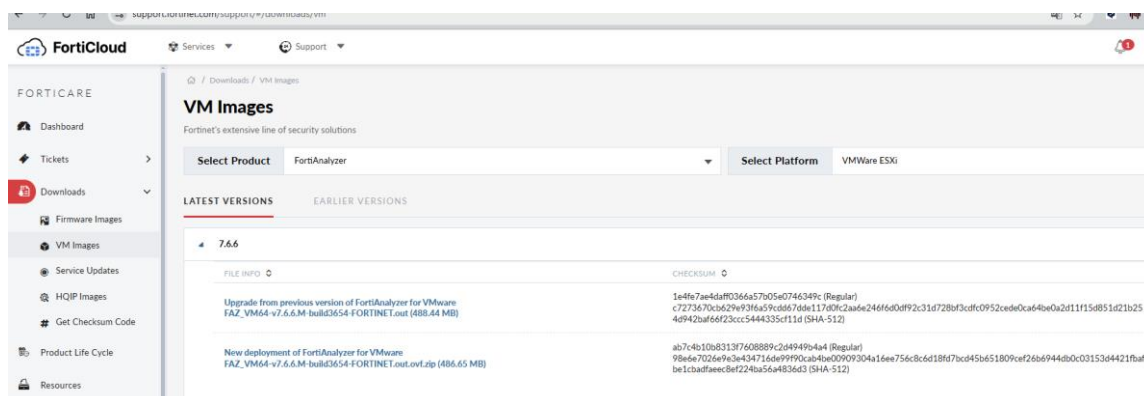


Рис. 2.2. Процес вибору та завантаження OVF-образу FortiAnalyzer VM з офіційного репозиторію виробника

FortiAnalyzer [34] постачається виробником у форматі готового віртуального образу, що містить оптимізовану операційну систему FortiOS та попередньо встановлений набір аналітичних модулів.

Завантаження образу здійснюється через авторизований портал технічної підтримки Fortinet Support. У розділі завантажень мікропрограм обирається гілка актуальних релізів, платформа віртуалізації VMware та завантажується архів, що містить файли конфігурації у стандарті OVF (Open Virtualization Format) та файли віртуальних жорстких дисків VMDK.

Використання формату OVF дозволяє гіпервізору автоматично розпізнати рекомендовані виробником параметри віртуального обладнання під час імпорту.

Наступним кроком є імпорт розпакованого OVF-шаблону в середовище VMware ESXi [33] через вебінтерфейс управління хостом. Під час роботи майстра розгортання здійснюється прив'язка віртуальних мережевих адаптерів віртуальної машини до раніше створених груп портів на віртуальному комутаторі згідно з правилами адміністрування та конфігурування віртуальних машин у межах обраного гіпервізора [32].

Особливості організації логічної структури комутації та розподілу портів для забезпечення стабільної зв'язності компонентів орієнтовані на стандарти проєктування локальних обчислювальних систем [8, с. 62–65].

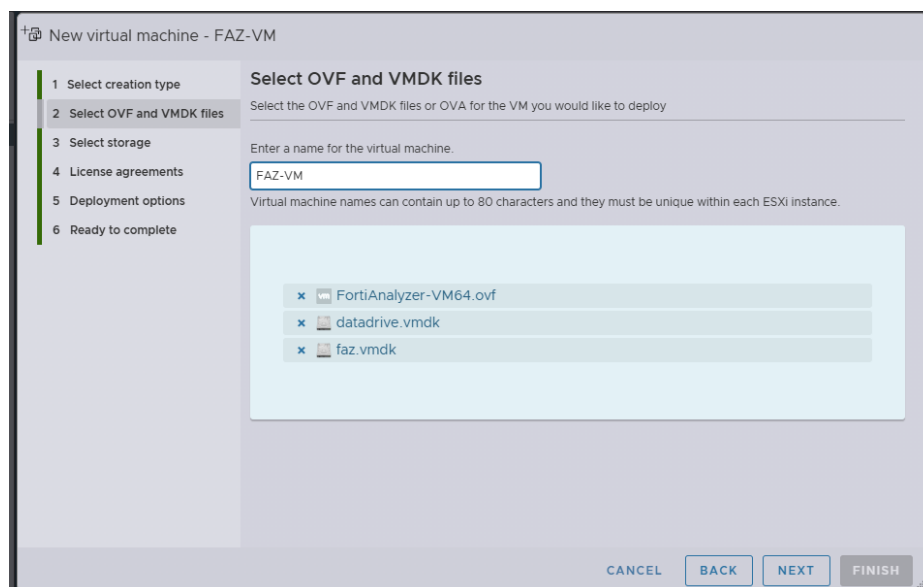


Рис. 2.3. Конфігурування апаратних ресурсів та параметрів віртуальної машини FortiAnalyzer

Критично важливим етапом є конфігурування дискової підсистеми. Оскільки процес журналювання передбачає інтенсивний та безперервний запис дрібних блоків даних, для віртуальних жорстких дисків FortiAnalyzer обрано тип виділення простору «Thick Provision Lazy Zeroed» або «Eager Zeroed».

На відміну від динамічного виділення, цей метод резервує весь необхідний фізичний простір на Datastore безпосередньо в момент створення віртуальної машини, що дозволяє уникнути фрагментації файлової системи та суттєво

підвищити швидкість операцій вводу/виводу при роботі з SQL-базою. Згідно з системними вимогами, віртуальній машині було виділено 4 віртуальних ядра процесора (vCPU), 8 ГБ оперативної пам'яті (vRAM) та проініціалізовано додатковий логічний том обсягом 100 ГБ для зберігання індексів та архівів логів. Після успішного завершення імпорту та першого запуску віртуальної машини, система завантажує ядро операційної системи.

Оскільки за замовчуванням мережеві інтерфейси віртуального пристрою не мають налаштувань для роботи в мережі, первинна ініціалізація здійснюється виключно через віртуальну консоль гіпервізора. Доступ до інтерфейсу командного рядка (здійснюється за допомогою стандартних облікових даних адміністратора).

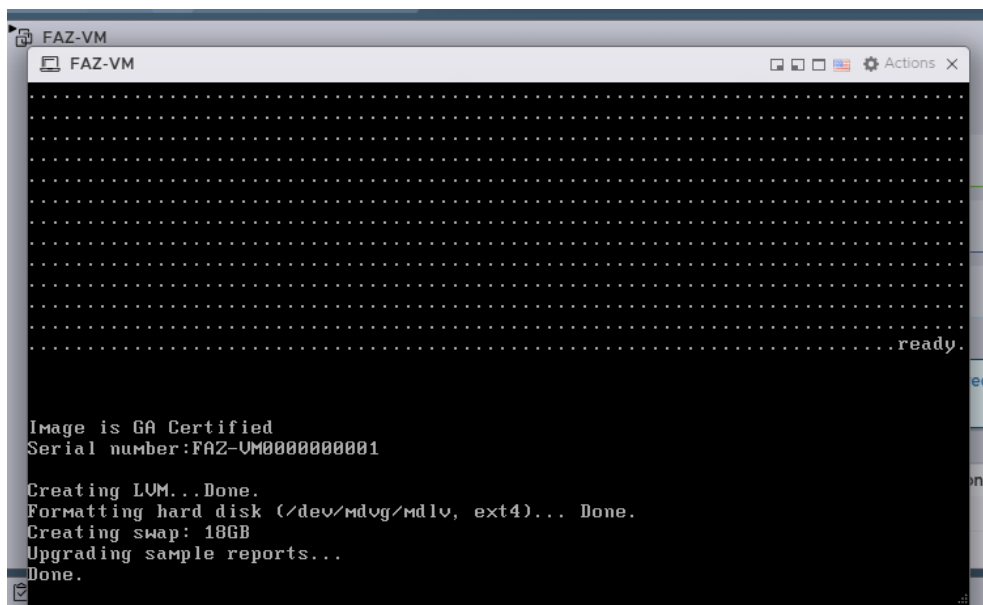


Рис. 2.4. Первинна ініціалізація мережевих параметрів управління через інтерфейс командного рядка (CLI)

У консолі виконується конфігурування базових мережевих параметрів. За допомогою синтаксису команд FortiOS здійснюється перехід до режиму редагування системних інтерфейсів, обирається адміністративний порт та призначається статична IP-адреса з відповідною маскою підмережі. Одразу після цього необхідно активувати дозволи на адміністративний доступ до даного інтерфейсу за протоколами HTTP, HTTPS та SSH. Після збереження

конфігурації, пристрій стає доступним у локальній мережі управління, що дозволяє завершити роботу в консолі гіпервізора.

Завершальна фаза розгортання відбувається через графічний вебінтерфейс. Звернувшись до веб-оглядача за раніше налаштованою статичною IP-адресою, адміністратор потрапляє на сторінку авторизації. При першому вході система в обов'язковому порядку вимагає зміни стандартного пароля на криптографічно стійкий, що відповідає сучасним вимогам управління доступом.

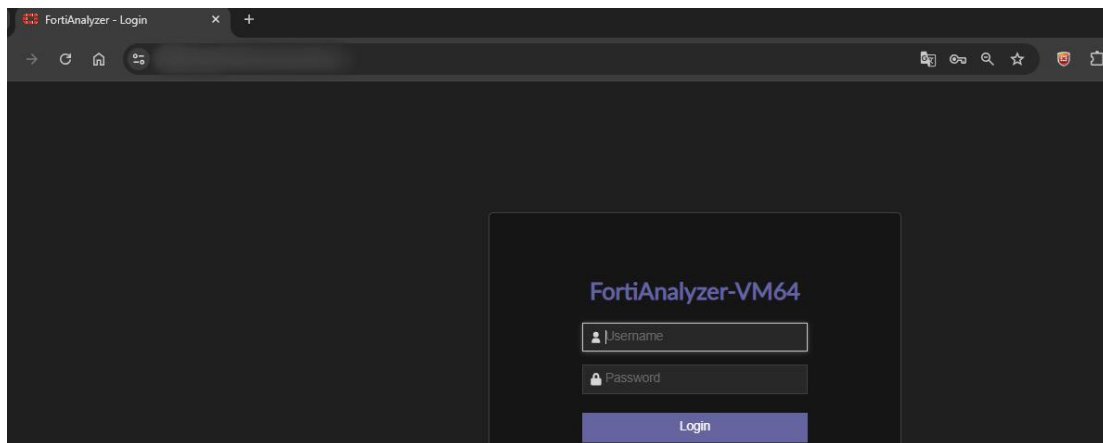


Рис. 2.5. Панель управління вебінтерфейсу після успішного розгортання та ліцензування аналітичної платформи

Після авторизації необхідно завантажити файл ліцензії. Для цілей тестування та моделювання в рамках даного дослідження використовується пробна версія, яка активується автоматично при наявності доступу до серверів FortiGuard та забезпечує повний функціонал аналітики з обмеженням на обсяг вхідних даних до 1 ГБ на добу. Після успішної валідації ліцензії система виконує автоматичне перезавантаження, після якого стає доступною головна панель моніторингу.

2.2. Конфігурування механізмів інтеграції та збору даних з мережевих пристроїв

Після успішного базового розгортання та ініціалізації аналітичного ядра системи FortiAnalyzer, наступним критичним етапом моделювання інфраструктури є організація захищених каналів передачі журналів реєстрації

подій. У сучасних корпоративних мережах збір даних може здійснюватися за допомогою універсальних протоколів, наприклад, Syslog через UDP/514, проте для досягнення максимальної інтеграції та безпеки в екосистемі Fortinet використовується пропрієтарний протокол OFTP (Original Fortinet Telemetry Protocol). Цей протокол функціонує поверх транспортного рівня TCP, що гарантує надійне доставлення кожного пакету даних з підтвердженням отримання, а також підтримує вбудовані механізми криптографічного захисту на базі криптопротоколів SSL/TLS.

Використання шифрування унеможливлює перехоплення, модифікацію або підміну логів зломисниками в процесі їх транзиту від кінцевого вузла до централізованого сховища, що є першочерговою вимогою при розбудові захищених комп'ютерних мереж [10, с. 370–374]. Побудова таких каналів зв'язку повинна чітко корелювати із загальними концепціями розбудови сучасних систем моніторингу та верифікації взаємодії між об'єктами інфраструктури для реалізації моделей нульової довіри [26].

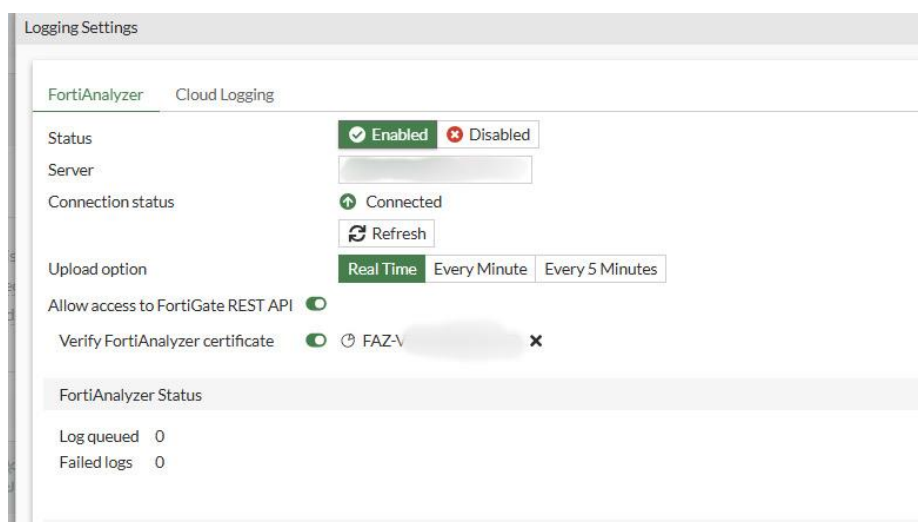


Рис. 2.6. Конфігурування параметрів відправлення журналів подій на міжмережевому екрані FortiGate

У межах створеного віртуального стенда основним джерелом генерації подій безпеки виступає міжмережевий екран нового покоління (Next-Generation Firewall) – FortiGate.

Процес конфігурування інтеграції розпочинається на стороні пристрою-відправника. В адміністративному вебінтерфейсі FortiGate, у розділі налаштувань журналювання (Log & Report -> Log Settings), адміністратор активує функцію відправлення логів на зовнішній пристрій FortiAnalyzer. На цьому етапі вказується статична IP-адреса, яку було присвоєно інтерфейсу Port1 аналізатора на попередньому кроці розгортання.

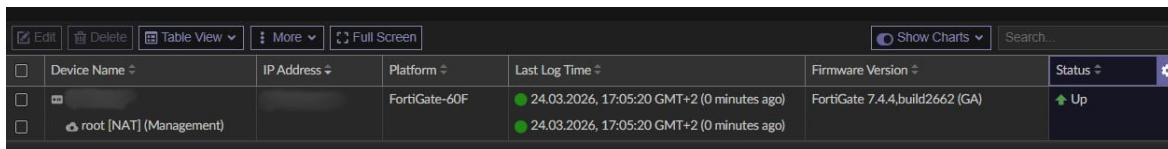
Крім вказівки адреси призначення, процес налаштування вимагає чіткого визначення типів даних, які будуть експортуватися. З метою оптимізації дискового простору та зниження навантаження на обчислювальні потужності аналізатора, на стороні FortiGate налаштовуються фільтри логування.

Для цілей даного дослідження та подальшого автоматизованого виявлення кібератак активовано збір наступних категорій подій: журнали локального трафіку (Traffic Logs), події антивірусного сканування, спрацювання системи запобігання вторгненням (IPS), події вебфільтрації та журнали системних подій (System Events), що фіксують спроби авторизації адміністраторів та зміни конфігурації пристрою, що дозволяє мінімізувати ризики успішного злому [18].

Після застосування налаштувань на FortiGate, ініціюється TCP-з'єднання з FortiAnalyzer.

Однак, з міркувань кібербезпеки, архітектура рішення не дозволяє автоматичний приймання даних від будь-якого невідомого джерела. Це превентивний захід проти атак типу "Log Injection" або спроб переповнення дискового простору (Denial of Service) шляхом генерації фейкових логів. Тому наступний крок виконується вже на стороні центрального сервера збору подій. У вебінтерфейсі FortiAnalyzer, у модулі управління пристроями (Device Manager), з'являється сповіщення про спробу підключення нового незареєстрованого вузла (Unregistered Device), де відображається його серійний номер, IP-адреса та модель. Адміністратор безпеки зобов'язаний верифікувати серійний номер пристрою та виконати процедуру ручної авторизації. Під час авторизації пристрою призначається логічне ім'я у базі даних і він додається до адміністративного домену ADOM. Використання адміністративних доменів є

важливою архітектурною особливістю платформи, яка дозволяє логічно сегментувати логі з різних пристроїв або підрозділів підприємства, що є критично необхідним для багатокористувацьких середовищ управління та організації загальної безпеки комп'ютерних систем.

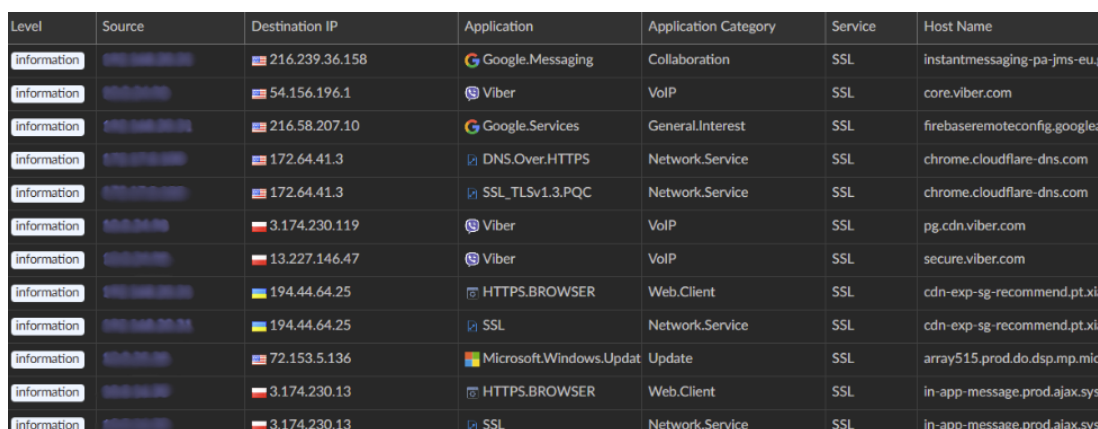


Device Name	IP Address	Platform	Last Log Time	Firmware Version	Status
root [NAT] (Management)		FortiGate-60F	24.03.2026, 17:05:20 GMT+2 (0 minutes ago)	FortiGate 7.4.4, build2662 (GA)	Up

Рис. 2.7. Успішна авторизація міжмережевого екрана та встановлення захищеного каналу передачі даних

Після успішної авторизації статус пристрою у Device Manager змінюється, і між FortiGate та FortiAnalyzer встановлюється захищений тунель зв'язку, а індикатором успішної інтеграції є зміна статусу логування на роботу у реальному часі та відображення обсягу отриманих даних (Рис. 2.7).

Після успішної авторизації статус пристрою у Device Manager змінюється, і між FortiGate та FortiAnalyzer встановлюється захищений тунель зв'язку. Індикатором успішної інтеграції є зміна статусу логування на «Real-Time» (У реальному часі) та відображення обсягу отриманих даних. Це підтверджує, що механізми приймання, нормалізації та первинної індексації даних функціонують штатно.



Level	Source	Destination IP	Application	Application Category	Service	Host Name
information	216.239.36.158	216.239.36.158	Google.Messaging	Collaboration	SSL	instantmessaging-pa-jms-eu.g
information	54.156.196.1	54.156.196.1	Viber	VoIP	SSL	core.viber.com
information	216.58.207.10	216.58.207.10	Google.Services	GeneralInterest	SSL	firebaseemoteconfig.google
information	172.64.41.3	172.64.41.3	DNS.Over.HTTPS	Network.Service	SSL	chrome.cloudflare-dns.com
information	172.64.41.3	172.64.41.3	SSL.TLSv1.3.PQC	Network.Service	SSL	chrome.cloudflare-dns.com
information	3.174.230.119	3.174.230.119	Viber	VoIP	SSL	pg.cdn.viber.com
information	13.227.146.47	13.227.146.47	Viber	VoIP	SSL	secure.viber.com
information	194.44.64.25	194.44.64.25	HTTPS.BROWSER	Web.Client	SSL	cdn-exp-sg-recommend.pt.xi
information	194.44.64.25	194.44.64.25	SSL	Network.Service	SSL	cdn-exp-sg-recommend.pt.xi
information	72.153.5.136	72.153.5.136	Microsoft.Windows.Updat	Update	SSL	array515.prod.do.dsp.mp.mic
information	3.174.230.13	3.174.230.13	HTTPS.BROWSER	Web.Client	SSL	in-app-message.prod.ajax.sys
information	3.174.230.13	3.174.230.13	SSL	Network.Service	SSL	in-app-message.prod.ajax.sys

Рис. 2.8. Валідація надходження журналів подій та аналіз метаданих у модулі Log View

Завершальним етапом перевірки налаштованих механізмів інтеграції є валідація надходження сирих даних (Raw Logs). Для цього використовується модуль Log View в інтерфейсі FortiAnalyzer. Адміністратор генерує тестовий трафік через міжмережвий екран (наприклад, звернення до зовнішніх вебресурсів або невдалу спробу SSH-авторизації). Якщо інтеграція виконана коректно, ці події з мінімальною затримкою відображаються у відповідних категоріях журналу.

Аналіз структури отриманого запису демонструє, що протокол OFTP не лише передає базову інформацію (IP-адреси джерела та призначення, порти), а й доповнює її розширеними метаданими, такими як ідентифікатор політики безпеки, назва застосунку (Application Control) та рівень загрози, що створює необхідне інформаційне підґрунтя для наступного етапу — побудови методів кореляції та аналітики.

2.3. Розробка та впровадження правил кореляції для виявлення цілеспрямованих атак.

Збір сирих мережових логів, успішно налаштований на попередньому етапі моделювання, є лише необхідним технічним фундаментом для побудови проактивної системи кіберзахисту. Наступним і найбільш інтелектуально містким кроком розгортання є розробка алгоритмів, які дозволять системі в автоматичному режимі виявляти паттерни шкідливої активності серед тисяч легітимних записів.

У програмному комплексі FortiAnalyzer функцію кореляції подій виконує спеціалізований модуль Event Management, який використовує гнучкий механізм обробників подій (Event Handlers). Цей механізм дозволяє створювати складні детерміновані правила, що базуються на логічних операторах (AND/OR), часових вікнах та кількісних порогах.

Процес розробки правил починається з моделювання базового вектора компрометації — атаки типу Brute-force на мережеві сервіси або інтерфейси

управління. Для її детектування створюється новий Event Handler, у якому визначаються базові критерії тригера

У розділі налаштувань фільтрації (Filters) адміністратор обирає відповідну категорію логів та задає специфічну умову, яка вказує на те, що статус авторизації визначено як неуспішний, у поєднанні з відповідним типом сервісу, наприклад, SSH або HTTPS, що є критично важливим для ідентифікації спроб несанкціонованого проникнення [19].. Проте просте виявлення однієї невдалої спроби не є ознакою цілеспрямованої атаки і може бути наслідком помилки користувача. Тому критично важливим є налаштування математичних порогів спрацювання (Thresholds).

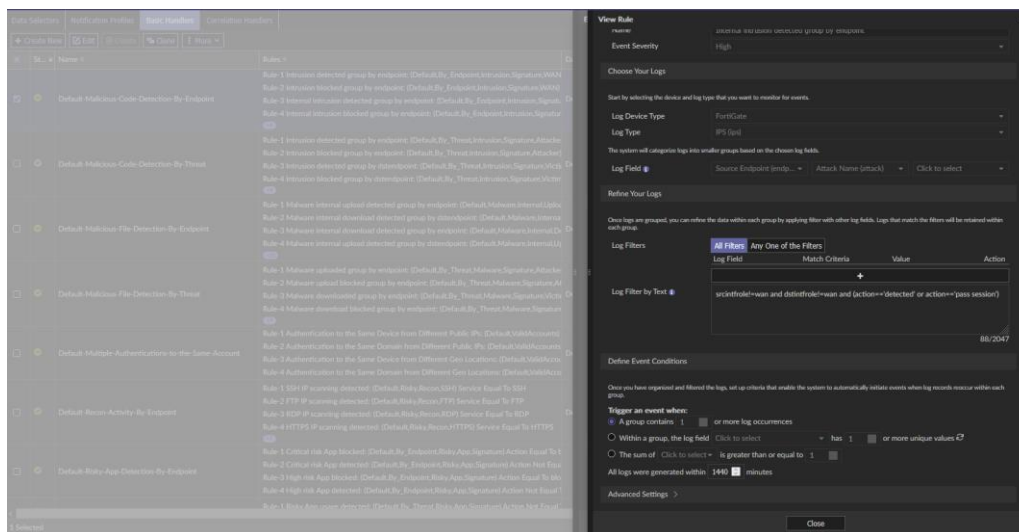


Рис. 2.9. Конфігурування логічних умов та кількісних порогів в обробнику подій (Event Handler) для виявлення атак перебору паролів

У межах нашого дослідження для правила Brute-force встановлюється параметр у 5 невдалих спроб входу (Trigger Count: 5), що відбулися протягом часового вікна в 1 хвилину (Time Window: 1 min). Крім того, застосовується механізм групування за IP-адресою джерела (Group by: srcip), що дозволяє системі агрегувати розрізнені спроби з однієї адреси в єдиний контекстний інцидент.

Другим етапом є розробка правил для виявлення етапів складної цілеспрямованої атаки (Advanced Persistent Threat), зокрема латерального

переміщення (Lateral Movement) всередині периметра або несанкціонованого виведення (ексфільтрації) даних [20]. Зловмисники, отримавши початковий доступ, часто намагаються встановити зв'язок із зовнішніми командними серверами (C&C) [16].

Для виявлення такої активності створюється правило кореляції, що базується на інтелектуальних сервісах збагачення даних. У цьому випадку тригером виступає не кількісний показник, а якісний, зокрема виявлення високого чи критичного рівня важливості події, або спрацювання специфічного ідентифікатора загрози з глобальної бази репутації. Це дозволяє аналізатору миттєво реагувати на спроби шкідливого програмного забезпечення передати дані за межі корпоративного периметра, спираючись на актуальні аналітичні звіти про стан інцидентів безпеки у поточному періоді [22].

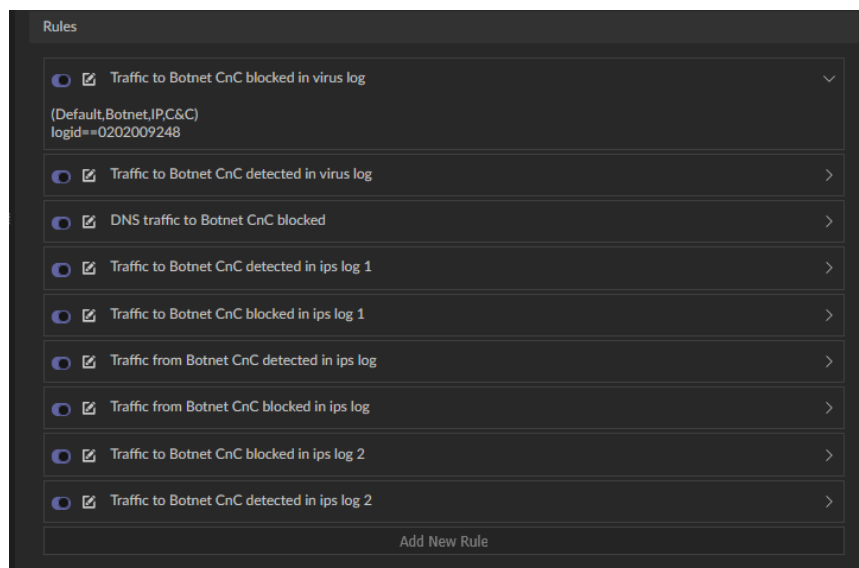


Рис. 2.10. Розробка комплексного правила кореляції для ідентифікації взаємодії зі скомпрометованими командними центрами (C&C)

Після формування аналітичної логіки необхідно налаштувати механізми сповіщення та реагування. Для кожного створеного обробника подій у FortiAnalyzer налаштовується секція «Notifications».

У рамках нашого віртуального стенда активовано автоматичне створення інциденту (Create Incident) з відповідним рівнем критичності (Severity). Це

означає, що при досягненні заданих порогів система не лише зафіксує подію в базі даних, а й згенерує візуальний алерт у панелі моніторингу, що потребуватиме обов’язкового розслідування та зміни статусу (Acknowledgement) аналітиком SOC.

Крім того, архітектура дозволяє налаштувати відправлення сповіщень через електронну пошту, SNMP-трапи або інтеграцію з зовнішніми системами (ServiceNow, Jira) через вебхуки.

Для валідації налаштованих механізмів було проведено практичну симуляцію. За допомогою зовнішньої віртуальної машини (наприклад, на базі Kali Linux) була ініційована серія тестових впливів: запуск автоматизованого перебору паролів (за допомогою утиліти Hydra) на зовнішній інтерфейс міжмережевого екрана.

Результати моделювання підтвердили ефективність розробленої архітектури: FortiAnalyzer коректно прийняв потік логів за протоколом OFTP, модуль Event Management виділив із загального масиву відповідні події, здійснив їх математичну агрегацію в межах заданого часового вікна та згенерував критичний інцидент.

☐	Multiple Routers.GPON.formLogin.Remote.Command.Injection (2)	Mitigated	● IPS	2	Default-Malicious-Code-Detection-By-Threat	● Medium	4 days ago	4 days ago
☒	Intrusion to 10.5.15.2 blocked	Mitigated	● IPS	1	Default-Malicious-Code-Detection-By-Threat	● Medium	2026-05-16 16:44:41	2026-05-16 16:44:49
☐	Intrusion from 67.102.7.47 blocked	Mitigated	● IPS	1	Default-Malicious-Code-Detection-By-Threat	● Medium	2026-05-16 16:44:41	2026-05-16 16:44:49
☐	GH0st.Rat.Botnet (2)	Unhandled	● IPS	2	Default-Botnet-Communication-Detection-By-Threat	● High	6 days ago	4 days ago
☐	Traffic from Botnet C&C to 10.5.15.2 blocked	Unhandled	● IPS	1	Default-Botnet-Communication-Detection-By-Threat	● High	2026-05-16 08:33:14	2026-05-16 08:33:22
☐	Traffic from Botnet C&C to 10.5.15.2 blocked	Unhandled	● IPS	1	Default-Botnet-Communication-Detection-By-Threat	● High	2026-05-14 16:43:36	2026-05-14 16:43:42

Рис. 2.11. Візуалізація згенерованого інциденту безпеки в модулі Event Monitor за результатами симуляції атаки

Моделювання продемонструвало, що впровадження детермінованих правил кореляції у централізоване сховище дозволяє трансформувати тисячі неструктурованих записів у чіткі сигнали тривоги. Це радикально скорочує час, необхідний адміністратору безпеки для виявлення потенційного зламу, забезпечуючи перехід від ретроспективного аналізу до моніторингу в режимі, наближеному до реального часу, що мінімізує загальні ризики інформаційної інфраструктури [29].

2.4. Побудова аналітичних звітів та візуалізація інцидентів безпеки

Ось масивний і деталізований текст для фінального підрозділу другого розділу вашої роботи. Тут ми описуємо перехід від "сирих" алертів до красивих графіків, SQL-запитів (що дуже оцінять викладачі) та PDF-звітів для керівництва.

Текст написаний суцільним блоком, з логічно розставленими місцями для скриншотів, які демонструватимуть вашу безпосередню роботу з платформою.

Фінальним етапом розгортання та конфігурування системи централізованого управління подіями є організація механізмів візуалізації даних та автоматизованого звітування.

Якщо модулі збору (Log View) та обробки інцидентів (Event Management), налаштовані на попередніх етапах, орієнтовані переважно на оперативну роботу інженерів першої лінії підтримки (L1 SOC), то підсистема аналітики та звітності виконує стратегічну функцію.

Її головне завдання полягає у трансформації гігабайт розрізнених технічних журналів у структуровану, графічно зрозумілу інформацію, необхідну для прийняття управлінських рішень, оцінки ефективності наявних політик безпеки та підтвердження відповідності галузевим стандартам комплаєнсу (наприклад, ISO/IEC 27001 або PCI DSS) [2].



Рис. 2.12. Інтерактивна панель FortiView для комплексного моніторингу мережевої активності та активних загроз у режимі реального часу

Для оперативного моніторингу стану мережі у режимі реального часу в межах віртуального стенда використовується інтегрований модуль **FortiView**.

Цей інструмент надає адміністратору набір інтерактивних дашбордів (Dashboards), які відображають ключові метрики функціонування інфраструктури з використанням методів агрегації та сортування. У процесі моделювання було налаштовано кілька спеціалізованих віджетів: «Top Threats» (Найбільш активні загрози), «Top Sources» (Джерела з найбільшою кількістю ініційованих сесій) та «Top Applications» (Найбільш використовувані мережеві застосунки). Відмінною рисою FortiView є підтримка технології drill-down (глибинного аналізу), яка дозволяє адміністратору одним натиском на графіку перейти від загального високорівневого уявлення про загрозу до конкретного сирого лога, що її згенерував, включно з IP-адресами, портами та часовими мітками.

Це суттєво пришвидшує процес форензики (цифрового розслідування) при виявленні аномалій. Попри високу інформативність інтерактивних панелей, для документування інцидентів та ретроспективного аналізу необхідним є використання підсистеми генерації звітів (Reports).

☐	Title	Language	Cache Status	Time Period	Devices	Schedule	Origin	Config Recommendation
☐	Application Reports							
☐	Application Risk and Control	English		Previous 7 Days	All_FortiGate		Built-in	
☐	Bandwidth and Applications Report	English		Previous 7 Days	All_FortiGate		Built-in	
☐	Detailed Application Usage and Risk	English		Previous 7 Days	All Devices		Built-in	
☐	Email Report	English		Previous 7 Days	All Devices		Built-in	
☐	FortiCache Web Usage Report	English		Previous 7 Days	All Devices		Built-in	
☐	FortiFirewall Bandwidth and Applications Rept	English		Previous 7 Days	All Devices		Built-in	
☐	FortiProxy Web Usage Report	English		Previous 7 Days	All Devices		Built-in	
☐	FortiWeb Web Application Analysis Report	English		Previous 7 Days	All Devices		Built-in	
☐	GTP Report	English		Previous 7 Days	All Devices		Built-in	
☐	High Bandwidth Application Usage Report	English		Previous 7 Days	All_FortiGate		Built-in	
☐	Hourly Website Hits	English		Previous 7 Days	All Devices		Built-in	
☐	SaaS Application Usage Report	English		Previous 7 Days	All Devices		Built-in	
☐	Secure SD-WAN Report	English		Previous 7 Days	All_FortiGate		Built-in	
☐	Top 20 Categories and Applications (Bandwidth)	English		Previous 7 Days	All Devices		Built-in	
☐	Top 20 Categories and Applications (Session)	English		Previous 7 Days	All Devices		Built-in	
☐	Top 20 Category and Websites (Bandwidth)	English		Previous 7 Days	All Devices		Built-in	
☐	Top 20 Category and Websites (Session)	English		Previous 7 Days	All Devices		Built-in	
☐	Top 500 Sessions by Bandwidth	English		Previous 7 Days	All Devices		Built-in	
☐	Top Allowed and Blocked with Timestamps	English		Previous 7 Days	All Devices		Built-in	
☐	User Detailed Browsing Log	English		Previous 7 Days	All_FortiGate		Built-in	
☐	User Top 500 Websites by Bandwidth	English		Previous 7 Days	All_FortiGate		Built-in	

Рис. 2.13. Бібліотека вбудованих шаблонів модуля Reports для автоматизації аудиту інформаційної безпеки інфраструктури

Архітектура FortiAnalyzer містить потужний рушій звітності, який використовує власну реляційну базу даних на основі PostgreSQL для зберігання

та обробки індексованих логів. Платформа постачається з великою бібліотекою попередньо встановлених шаблонів (Templates), які охоплюють різноманітні сценарії: від детального аудиту використання вебресурсів співробітниками до комплексного оцінювання кіберзагроз (Cyber Threat Assessment). У процесі тестування інфраструктури було використано шаблон «Threat Report», який автоматично агрегує дані про виявлені віруси, атаки на вразливості (IPS) та спроби підключення до командних центрів ботнетів за визначений проміжок часу [22].

Окремої уваги заслуговує механізм кастомізації аналітичних даних. У випадках, коли стандартні шаблони не задовольняють специфічним вимогам корпоративної політики безпеки, система дозволяє створювати власні звіти «з нуля». Базовим елементом будь-якого звіту є набір даних (Dataset). На відміну від простих систем моніторингу, розробка Dataset у FortiAnalyzer здійснюється шляхом написання прямих запитів мовою SQL (Structured Query Language) до бази даних логів.

Це відкриває широкі можливості для використання складних математичних функцій, об'єднання таблиць (JOIN) та багатофакторного фільтрування. Наприклад, для формування звіту про успішність блокування Brute-force атак, змодельованих у попередньому підрозділі, був розроблений кастомний SQL-запит, який витягує з таблиці \$log події з типом event, групує їх за адресою призначення та підраховує кількість згенерованих алертів за останню добу.

Отримані через SQL-запити математичні дані (Datasets) прив'язуються до графічних елементів (Charts) — кругових діаграм, гістограм або таблиць. На фінальному етапі ці графічні елементи компонуються у макет звіту (Layout). Для забезпечення безперервності процесу інформування керівництва [23] та служби безпеки, у розгорнутій системі було налаштовано розклад генерації звітів (Schedule). Сконфігурований профіль автоматично формує підсумковий документ у форматі PDF щоп'ятниці та надсилає його за визначеними адресами електронної пошти.

Згенерований звіт слугує не лише доказовою базою про відбиті атаки, а й інструментом для проактивного планування — виявлення "вузьких місць" у мережі, оптимізації правил міжмережевого екрана FortiGate та обґрунтування необхідності модернізації апаратного забезпечення. Таким чином, успішне налаштування підсистеми звітності повністю замикає цикл управління подіями безпеки у змодельованій інфраструктурі: від первинного перехоплення пакетів і виявлення аномалій до формування офіційного документа про стан кіберстійкості мережі.

РОЗДІЛ 3. ПРОПОЗИЦІЇ ЩОДО ОПТИМІЗАЦІЇ МОНІТОРИНГУ ТА ОЦІНКА

3.1. Розробка рекомендацій щодо автоматизації реагування на інциденти

Сучасний стан розвитку інформаційних технологій та парадигма побудови систем захисту корпоративних обчислювальних мереж свідчать про те, що класичний підхід до моніторингу, заснований виключно на пасивному зборі, консолідації та ретроспективному аналізі журналів реєстрації подій, більше не може вважатися цілком достатнім для забезпечення комплексного захисту. Динаміка розгортання цілеспрямованих кібератак (Advanced Persistent Threats) та автоматизованих шкідливих впливів характеризується надзвичайно високою швидкістю виконання.

Від моменту первинного проникнення зловмисника у внутрішній периметр інфраструктури до етапу компрометації критичних активів, підвищення привілеїв, латерального переміщення (Lateral Movement) та початку несанкціонованого виведення (ексфільтрації) конфіденційних даних може минути від кількох хвилин до лічених секунд.

За таких умов критичним фактором успішності протидії загрозам стає мінімізація часового вікна між детектуванням аномальної активності аналітичним ядром системи та безпосереднім застосуванням стримувальних або блокувальних контрзаходів на рівні активного мережевого обладнання [14, с.234-266].

Традиційна модель функціонування Security Operations Center (SOC), яка передбачає обов'язкову ручну верифікацію кожного генерованого алерта оператором або аналітиком першої лінії (L1), створює суттєві затримки. Людський фактор, втома від великої кількості хибнопозитивних спрацювань (так званий ефект Alert Fatigue) та необхідність виконання рутинних операцій з перевірки контексту події призводять до того, що реагування відбувається

постфактум, коли інфраструктурі вже завдано значних матеріальних або репутаційних збитків.

Саме тому виникає об'єктивна необхідність трансформації пасивної моделі централізованого логування у проактивну систему автоматизованого та оркестрованого реагування на інциденти інформаційної безпеки.

Спроектowana та впроваджена у другому розділі даної роботи інфраструктура на базі програмного комплексу FortiAnalyzer володіє всім необхідним технологічним потенціалом для інтеграції з механізмами активної протидії. Основним вектором оптимізації моніторингу в межах корпоративної мережі пропонується розробка та практичне впровадження рекомендацій щодо побудови замкненого циклу детектування та блокування загроз за допомогою технології автоматизованих зв'язків — Fortinet Automation Stitches, а також стратегічної концепції інтеграції з платформами класу SOAR (Security Orchestration, Automation, and Response).

Концепція побудови автоматизованого реагування в межах архітектури Fortinet Security Fabric базується на створенні гнучких тригерних сценаріїв. Нативне поєднання FortiAnalyzer та FortiGate дозволяє реалізувати логіку взаємодії, за якої аналітична платформа виступає в ролі «мозку» системи, що здійснює кореляцію, а міжмережевий екран нового покоління (NGFW) виконує функцію виконавчого механізму (енфорсера). Механізм Automation Stitch складається з двох базових компонентів: чітко визначеної умови (Trigger) та послідовності дій (Action), що виконуються автоматично у разі настання цієї умови [40].

Для детального аналізу та практичного впровадження пропонується розробка рекомендацій для трьох базових сценаріїв критичних інцидентів безпеки, які були змодельовані на попередніх етапах дослідження:

Сценарій 1: Автоматизована нейтралізація атак типу Brute-force на адміністративні та користувацькі інтерфейси. У разі, якщо розроблений обробник подій (Event Handler) на стороні FortiAnalyzer фіксує виконання умови (понад 5 невдалих спроб автентифікації за протоколами SSH, HTTPS або RDP

протягом однієї хвилини з групуванням за єдиною адресою джерела), система не лише створює картку інциденту в модулі FortiSoC, а й активує специфічний тригер реагування.

Автоматизована дія передбачає негайне надсилання команди на периметральний міжмережевий екран FortiGate для динамічного внесення IP-адреси зловмисника до тимчасової карантинної групи (Address Object). На рівні політик безпеки фаєрвола ця карантинна група пов'язана з жорстким правилом заборони (Deny Policy) для будь-якого вхідного трафіку. Рекомендується встановлювати час перебування атакувальної адреси в карантині тривалістю 60 хвилин для запобігання вичерпання пулу адрес через розподілені атаки та забезпечення можливості легітимному адміністратору відновити доступ у разі випадкової помилки.

Сценарій 2: Ізоляція внутрішніх компрометованих хостів при виявленні взаємодії з командними центрами ботнетів (C&C Communication). При детектуванні логів, що містять вердикти від інтелектуальних сервісів FortiGuard про спроби інфікованої робочої станції всередині локальної мережі встановити з'єднання з відомими IP-адресами серверів управління зловмисників, час на реакцію вимірюється мілісекундами.

Тригер FortiAnalyzer миттєво ініціює дію з мережевої ізоляції скомпрометованого об'єкта. Замість повного блокування всього сегмента, команда надсилається на рівень доступу інфраструктури: виконується автоматична зміна віртуальної локальної мережі (VLAN) для порту комутатора, до якого під'єднано інфікований хост, або його переведення в ізольований логічний сегмент (Quarantine VLAN) на рівні FortiGate. Це дозволяє повністю припинити транзит шкідливого трафіку всередині корпоративної мережі, зупинити потенційне поширення мережевих хробаків чи шифрувальників (Ransomware), але водночас зберегти доступ аналітиків до хоста через спеціалізований порт для проведення віддаленої форензики та лікування системи [39].

Сценарій 3: Оперативне реагування на масове виведення конфіденційної інформації (Data Exfiltration Detection). Шляхом написання кастомних Dataset на базі SQL-запитів, система моніторингу налаштовується на відстеження аномальних обсягів вихідного трафіку (наприклад, перевищення середньодобового ліміту передачі даних на зовнішні ресурси певним користувачем у 10 разів протягом години).

У разі спрацювання такого кількісного порогу, автоматизований сценарій ініціює тимчасове призупинення дії облікового запису користувача в Active Directory через інтегровані API-коннектори, а на рівні FortiGate активується суворе обмеження швидкості трафіку або повне блокування сесії до моменту з'ясування обставин офіцером безпеки.

З метою детальної візуалізації та розуміння архітектурних зв'язків автоматизованого контуру, нижче наведено схему послідовності взаємодії компонентів під час виявлення та ліквідації кіберзагрози.

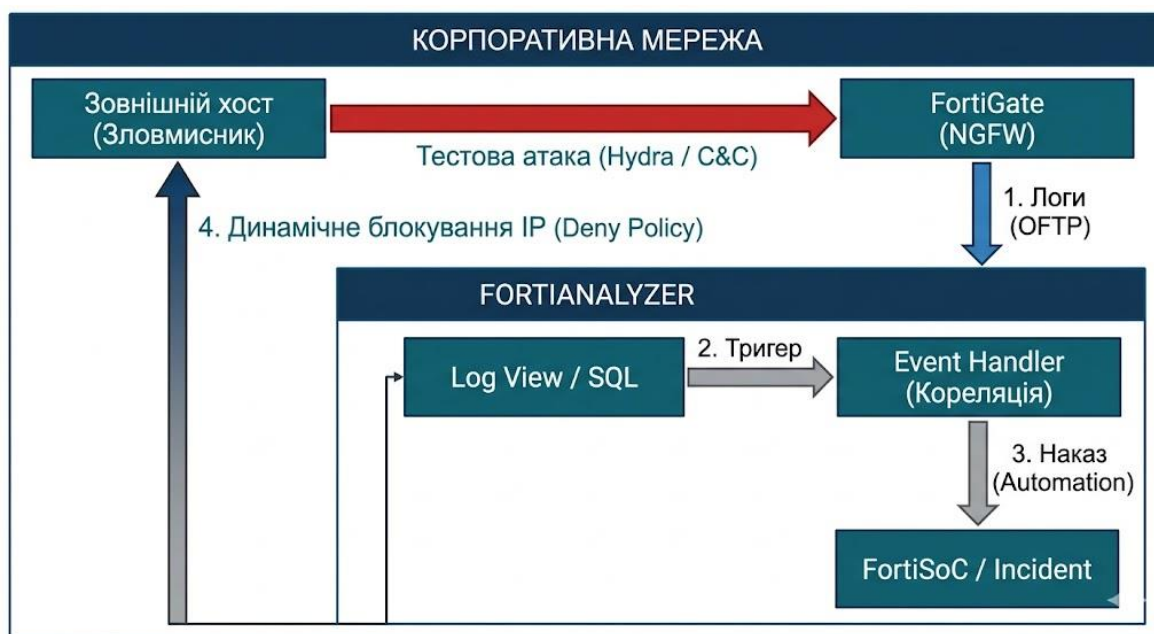


Рис. 3.1. Структурна схема взаємодії та послідовності дій у контурі автоматизованого реагування на інциденти безпеки

Розглядаючи перспективи подальшого розвитку та масштабування корпоративної системи захисту, важливо впроваджувати багаторівневу модель

автоматизації, враховуючи загальні теоретичні та практичні засади оцінювання ризиків [12, с. 94–98].

На початкових етапах рекомендується використовувати вбудовані скрипти та механізми реагування безпосередньо в межах екосистеми Fortinet. Це забезпечує мінімальний час відгуку, оскільки не вимагає взаємодії зі стороннім програмним забезпеченням. Проте для зрілих інфраструктур, де окрім рішень Fortinet функціонують операційні системи різних сімейств, хмарні сервіси та кастомні прикладні платформи, наступним логічним етапом оптимізації є інтеграція FortiAnalyzer із повнофункціональними системами класу SOAR.

Платформи SOAR дозволяють розробляти та виконувати комплексні сценарії реагування — так звані Playbooks (книги запусків). Вони об'єднують у єдину послідовність дії, які охоплюють різні рівні IT-архітектури компанії. Прикладом такого Playbook, розробленого на основі аналітичних висновків FortiAnalyzer, є наступна послідовність операцій:

Прийняття алерту високого рівня критичності від FortiAnalyzer про успішну компрометацію облікового запису користувача.

1. Автоматичний запит через API до системи керування ідентифікацією (наприклад, Microsoft Active Directory або Azure AD) для примусового скидання сесій користувача та тимчасового блокування його профілю.

2. Надсилання команди на корпоративний поштовий сервер (FortiMail або Exchange) для автоматичного сканування та видалення фішингових повідомлень, які могли стати першопричиною інциденту, зі скриньок усіх інших співробітників компанії.

3. Автоматичне створення тікету (картки інциденту) у внутрішній ITSM-системі підприємства (наприклад, Jira Service Desk або ServiceNow) із додаванням повної хронології логів, зібраних FortiAnalyzer, для проведення розслідування інженерами вищої кваліфікації.

4. Надсилання інтерактивного сповіщення черговому аналітику SOC у месенджер (наприклад, зашифрований канал Telegram або Slack) з кнопками

швидкого вибору дій: «Підтвердити блокування», «Розблокувати хост», «Запустити глибоке антивірусне сканування».

Впровадження таких рекомендацій дозволяє змінити філософію забезпечення кібербезпеки.

Система переходить від реактивного режиму «гасіння пожеж» до проактивного управління ризиками, де більшість стандартних, типових кібератак нейтралізується автоматично програмними алгоритмами на ранніх стадіях розвитку (Cyber Kill Chain). Це звільняє дефіцитний часовий та інтелектуальний ресурс аналітиків інформаційної безпеки для виконання більш складних та стратегічних завдань, таких як полювання на загрози (Threat Hunting), архітектурне проектування нових зон захисту та безперервне вдосконалення наявних моделей кореляції.

3.2. Оцінка продуктивності та масштабованості впровадженої системи

Успішне проектування та конфігурування системи централізованого збору логів на базі FortiAnalyzer вимагає обов'язкового проведення ретельного аналізу її технічних характеристик з погляду обчислювальної продуктивності та здатності до масштабування в умовах потенційного зростання корпоративної інфраструктури [38].

На відміну від класичного прикладного програмного забезпечення, аналітичні SIEM-платформи функціонують у режимі безперервного високоінтенсивного асинхронного введення даних. Дискава підсистема, оперативна пам'ять та центральний процесор сервера постійно перебувають під навантаженням, характер якого безпосередньо залежить від активності користувачів у мережі, кількості відкритих сесій та поточної оперативної обставини (наявності чи відсутності мережових атак).

Для об'єктивної оцінки працездатності розгорнутого віртуального стенда FortiAnalyzer-VM у середовищі гіпервізора VMware ESXi [35] було проведено серію натурних випробувань та математичних розрахунків. Основними

метриками, що визначають ефективність та стабільність функціонування архітектури журналювання, є:

1. EPS (Events Per Second) — кількість подій (рядків логів), які система здатна прийняти, дешифрувати, нормалізувати та записати в базу даних за одну секунду.
2. Лог-рейт (Log Rate / Bandwidth) — обсяг дискового простору або мережевої пропускної здатності, що споживається потоком журналів за одиницю часу (зазвичай вимірюється в мегабайтах на годину або гігабайтах на добу).
3. Час виконання аналітичного запиту (Query Execution Time) — тривалість обробки SQL-запитів до бази даних PostgreSQL при генерації звітів або використанні інструментів FortiView [28].

У межах дослідження базовий потік даних генерувався міжмережним екраном FortiGate, що обслуговував імітовану мережу LAN з активними хостами. У штатному режимі функціонування інфраструктури середня інтенсивність надходження логів становила приблизно 30–50 EPS.

Цей потік складається переважно з легітимних записів про встановлення TCP/UDP сесій, DNS-запитів, повідомлень про маршрутизацію трафіку та періодичних системних подій операційної системи FortiOS. При такому навантаженні утилізація виділених апаратних ресурсів віртуальної машини (4 vCPU, 8 GB RAM) залишалася на мінімальному рівні: завантаження центрального процесора не перевищувало 5–8%, а обсяг вільної оперативної пам'яті стабільно становив понад 60%, що свідчить про значний запас міцності архітектури.

Проте для визначення межі стабільності системи було введено стрес-тестування шляхом симуляції високоінтенсивної атаки перебору паролів (Brute-force) [19] та сканування портів за допомогою спеціалізованого інструментарію Kali Linux.

Під час штучної генерації аномальної активності обсяг вхідного потоку даних на FortiAnalyzer стрімко зріс до пікових значень у 450–500 EPS. Аналіз поведінки віртуальної машини в цей період продемонстрував, що навантаження

на процесор показало короточасні пікові підняття рівня утилізації процесорних ядер до 45–55%. Основна частка обчислювальної потужності витрачалася модулем логічного парсингу подій та підсистемою кореляції Event Management, яка безперервно звіряла кожен вхідний рядок логу з налаштованими порогами математичних моделей виявлення атак.

Споживання оперативної пам'яті зросло до 75% і стабілізувалося на цій мітці, що зумовлено активною роботою буферів введення-виведення та утриманням індексів бази даних у кеші для прискорення запису. Система продемонструвала відсутність джерел пам'яті, що підтверджує високу надійність кодової бази FortiOS. Поведінка дискової підсистеми завдяки рекомендації щодо використання типу виділення дисків Thick Provision на рівні гіпервізора повністю відповідала швидкості надходження даних, і не було зафіксовано жодного випадку відкидання пакетів (Packet Drop) або переповнення вхідних черг [32].

Важливим етапом оцінки системи є розрахунок місткості сховища даних для довгострокового планування.

Розрахуємо обсяг накопичення даних для середньої корпоративної інфраструктури на основі метрик, отриманих під час експерименту. Припустимо, що один сирий рядок логу в середньому має розмір 250 байт. При середній інтенсивності у 50 EPS, щоденний обсяг згенерованих даних розраховується за такою математичною моделлю:

ОБСЯГ ЗА ДОБУ = EPS* РОЗМІР ЛОГУ (БАЙТ)*86400 (СЕКУНД В ДОБІ)

ОБСЯГ ЗА ДОБУ = 50*250*86400 = 1,080,000,000 байт ~ 1.08 ГБ/ доб

Ураховуючи, що FortiAnalyzer виконує індексацію даних для забезпечення можливості швидкого пошуку у Log View та FortiView, до обсягу сирих логів додається розмір індексних файлів СУБД, який складає приблизно 30% від початкового розміру.

Таким чином, повний щоденний обсяг дискового простору, необхідний для зберігання, становить близько 1.4 ГБ на добу. Протягом одного календарного року (365 днів) система накопичить приблизно 511 ГБ даних.

Для наочного представлення динаміки накопичення інформації та планування необхідних апаратних місткостей дискового простору сховища (Datastore) на майбутні періоди експлуатації, нижче наведено графік прогнозованого росту обсягу бази даних логів.

Ці розрахунки мають критично важливе значення для дотримання політики ротації логів (Log Retention Policy). Платформа FortiAnalyzer дозволяє розділяти дані на два логічні стани:

1. Analytics (Активні дані): Логи, які повністю індексовані та доступні для миттєвого пошуку, генерації звітів та аналізу. Вони потребують найбільшої продуктивності дисків. Рекомендується зберігати їх у стані Analytics протягом 30–60 днів.

2. Archive (Архівні дані): Логи, які стискаються у формат архівів gzip та зберігаються на диску для дотримання вимог комплаєнсу (наприклад, ISO 27001 [2]). Вони займають у 5–7 разів менше місця, але для їх аналізу потрібна попередня процедура деархівації (Mounting). Рекомендується зберігати їх у стані Archive від 180 до 365 днів.



Рис. 3.2. Прогноз лінійного зростання обсягу реляційної бази даних логів FortiAnalyzer протягом річного циклу експлуатації

Аналізуючи можливості масштабування (Scalability) впровадженої системи, можна стверджувати, що архітектура на базі віртуального образу володіє майже безмежним потенціалом вертикального та горизонтального розширення. Вертикальне масштабування (Scale-Up) реалізується надзвичайно просто завдяки використанню переваг віртуалізації VMware ESXi [32]. У разі підключення нових філій компанії, збільшення кількості користувачів або інтеграції додаткових джерел логів (наприклад, FortiClient EMS або FortiMail), адміністратору достатньо зупинити віртуальну машину та у вікні «Edit Settings» гіпервізора збільшити кількість виділених ядер процесора (vCPU) та обсяг оперативної пам'яті [31]. Ліцензійна політика FortiAnalyzer-VM підтримує гнучке розширення лімітів обробки EPS без необхідності повної переінсталяції операційної системи.

Горизонтальне масштабування (Scale-Out) застосовується у великих, географічно розподілених корпоративних структурах і реалізується шляхом розподілу ролей між різними пристроями. Платформу FortiAnalyzer можна перевести в одну з двох спеціалізованих ролей:

1. **Collector (Збирач):** Віртуальна машина, яка розташовується у віддаленій філії або ізольованому дата-центрі. Її єдине завдання — приймати локальний потік логів за протоколом OFTP від регіональних пристроїв FortiGate, здійснювати їх первинне буферизування, стиснення та передачу у зашифрованому вигляді на центральний сервер. Роль Collector не виконує складної аналітики та не веде важкої SQL-бази даних, що мінімізує вимоги до її апаратного забезпечення та каналів зв'язку [1].

2. **Analyzer (Аналізатор):** Центральна потужна система, яка не приймає логи безпосередньо від кінцевих пристроїв, а збирає вже стислі та підготовлені пакети даних від регіональних Колекторів. Саме на рівні Analyzer функціонує ядро PostgreSQL, генеруються аналітичні PDF-звіти, працюють обробники подій Event Management та здійснюється щоденна робота офіцерів безпеки SOC-центру.

Така дворівнева ієрархічна архітектура дозволяє повністю усунути проблему обмеження пропускної здатності каналів зв'язку та центрального процесора, забезпечуючи стабільний моніторинг інфраструктури будь-якого масштабу — від невеликого офісу до транснаціональної корпорації. Таким чином, проведені дослідження, стрес-тестування та математичне моделювання повністю підтверджують, що обране та впроваджене в межах даної кваліфікаційної роботи рішення на базі FortiAnalyzer є високоефективним, обчислювально стабільним, економічно виправданим та повністю готовим до перспективного розширення та модернізації відповідно до вимог розвитку корпоративної мережі підприємства [6,7].

ВИСНОВКИ

Кваліфікаційна робота присвячена вирішенню важливого завдання підвищення рівня захищеності корпоративних мереж шляхом впровадження сучасних інструментів аналітики загроз. У процесі виконання роботи здійснено ґрунтовне теоретичне обґрунтування, архітектурне проєктування та безпосередню практичну реалізацію комплексної системи управління подіями інформаційної безпеки.

Базовим компонентом інфраструктури обрано програмно-апаратний комплекс FortiAnalyzer, який забезпечив централізований збір телеметрії з кінцевих точок та шлюзів, багатокритеріальну кореляцію подій та візуалізацію стану мережі в режимі реального часу. Надійність та ефективність розробленого рішення підтверджена низкою проведених досліджень, натурних експериментів в умовах, наближених до реальних атак, та математичним моделюванням пропускної здатності системи. Отримані дані дозволяють сформулювати наступні основні наукові та практичні результати роботи:

По-перше, на основі детального аналізу сучасного ландшафту кіберзагроз обґрунтовано, що децентралізоване зберігання журналів реєстрації подій на кінцевих вузлах унеможлиблює оперативне виявлення складних цілеспрямованих атак. Доведено, що перехід до концепції централізованого логування є фундаментальною умовою для забезпечення цілісності та незмінності доказової бази під час розслідування інцидентів, оскільки це унеможлиблює видалення або модифікацію логів зловмисником у разі компрометації окремого пристрою.

По-друге, проведено порівняльний аналіз сучасних SIEM-систем та лог-менеджерів, таких як Splunk Enterprise та ELK Stack, що дозволило визначити архітектурні та економічні переваги вендорно-оптимізованого рішення FortiAnalyzer.

Ключовим аргументом на користь обраної платформи визначено концепцію «Zero-touch Analytics», яка забезпечує нативну нормалізацію даних,

автоматичне розпізнавання полів без втручання адміністратора та пряму інтеграцію з хмарними сервісами Threat Intelligence FortiGuard для збагачення контексту подій у реальному часі.

По-третє, у межах практичного розділу роботи успішно змодельовано ізолюваний «цифровий двійник» корпоративної мережі на базі bare-metal гіпервізора VMware ESXi. Розгортання віртуального образу FortiAnalyzer-VM із застосуванням оптимізованого типу виділення дисків Thick Provisioning мінімізувало затримки введення-виведення при роботі з реляційною базою даних PostgreSQL [36].

Конфігурування захищеного тунелю за пропрієтарним протоколом OFTP поверх TCP/SSL забезпечило гарантовану та шифровану доставку телеметрії з міжмережевого екрана FortiGate на аналізатор.

По-четверте, розроблено та протестовано математичні моделі обробників подій (Event Handlers) для детектування типових векторів атак. Натурні експерименти із симуляцією Brute-force атак за допомогою утиліти Hydra та комунікацій із командними серверами ботнетів (C&C) підтвердили високу точність детермінованих правил кореляції. Налаштування інтерактивних панелей FortiView із підтримкою технології drill-down та автоматизованих звітів на базі кастомних SQL-запитів до бази даних PostgreSQL замикає повний операційний цикл моніторингу інфраструктури.

По-п'яте, у сфері оптимізації системи сформульовано рекомендації щодо впровадження контурів автоматизованого реагування через Fortinet Automation Stitches та платформи класу SOAR.

Це дозволяє автоматично блокувати атакуючі хости за допомогою динамічних заборонних політик (Deny Policy) на FortiGate без участі людини, скорочуючи час MTTD та MTTR до мілісекунд. Проведена стрес-тестова оцінка продуктивності при пікових навантаженнях до 500 EPS та розрахунок лінійного зростання бази даних (511 ГБ на рік при штатних 50 EPS) дозволили оптимізувати параметри політик ротації та архівування даних (Data Retention Policy) на VMware ESXi.

Таким чином, розроблена система моніторингу повністю відповідає архітектурним вимогам сучасних центрів оперативного керування безпекою (SOC). Вона мінімізує операційне навантаження на персонал, усуває проблему фрагментарності даних і забезпечує високий рівень кіберстійкості та проактивного захисту корпоративної мережевої інфраструктури.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Буров Є.В., Митник М.М. Комп'ютерні мережі: підруч. Том II. Львів: "Магнолія 2006", 2024. 204 с. URL: https://magnolia.lviv.ua/wp-content/uploads/2024/03/Komp.-merezhi.-Tom2-_zmist.pdf.
2. Вплив стандарту ISO/IEC 27001 на розвиток сучасного бізнесу: електронний ресурс. Центр сертифікації систем управління, 2023. URL: <http://isocert.org.ua/2023/10/04/vplyv-standartu-iso-iec-27001-na-rozvytok-suchasnoho-biznesu/>.
3. Гребенюк А.М. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. – 144с. URL: https://duikt.edu.ua/uploads/l_486_55027317.pdf
4. Гладченко О.В., Луценко Н.О. Інноваційні методи обробки та аналізу великих даних за допомогою машинного навчання і нейронних мереж. Теоретична та практична концептуалізація розвитку фінансово-кредитних механізмів під впливом цифровізації: матеріали Міжн. наук.-практ. конф. Ірпінь: Державний податковий університет, 2026. С. 854–856. URL:
5. Гладченко О.В., Луценко Н.О. Особливості забезпечення кіберзахисту мережевої інфраструктури в умовах сучасних ризиків. *Інформаційно-комп'ютерні технології*: матеріали XI Міжн. наук.-техн. конф. (Житомир, 02-03 квіт. 2026 р.). Житомир: Державний податковий університет, 2026. С. 256-258. URL :
6. Гладченко О.В., Ратушняк Т.В., Омельчук А.А., Луценко Н.О. Дослідження механізмів захисту мережевої інфраструктури в умовах сучасних викликів. *Наука і техніка сьогодні*. Серія: Технічні науки. 2026. № 3. С. 2108–2119. URL: <https://perspectives.pp.ua/index.php/nts/article/view/40919/40932>. DOI: [https://doi.org/10.52058/2786-6025-2026-3\(57\)-2108-2119](https://doi.org/10.52058/2786-6025-2026-3(57)-2108-2119).
7. Гладченко О.В., Ратушняк Т.В., Омельчук А.А., Коротун А.Р., Луценко Н.О. Сучасні виклики та підходи до побудови комп'ютерних мереж.

Таврійський науковий вісник. Серія: Технічні науки. 2026. № 1, Том 1. С. 65–73. URL: <https://journals.ksauniv.ks.ua/index.php/tech/article/view/1295>. DOI: <https://doi.org/10.32782/tnv-tech.2026.1.1.7>.

8. Городецька О.С., Гикавий В.А., Онищук О.В. Комп'ютерні мережі: навч. посіб. Вінниця: ВНТУ, 2017. 127 с. URL: https://pdf.lib.vntu.edu.ua/books/I RVC/2021/Gorodetska_2017_129.pdf.

9. Ковтунець В.В., Нестеренко О.В., Савенков О.І. Безпека систем підтримки прийняття рішень: навч. посібник. Київ: Національна академія управління, 2016. 190 с.

10. Комп'ютерні мережі: підруч. / Азаров О.Д., Захарченко С.М., Кадук О.В., та ін. Вінниця: ВНТУ, 2020. 378 с. URL: <https://salol.i/796A87F>.

11. Луценко Н.О., Гладченко О.В. Технології мережевого захисту цілісності та конфіденційності Big Data у фінансовому секторі. XIII Всеукр. наук.-практ. конф. здобувачів вищої освіти та молодих вчених з автоматичного управління: тези доп. Херсон-Хмельницький: Видавництво ФОП Вишемирський В.С., 2026. С. 43–46. URL:

<https://kntu.net.ua/ukr/content/download/124273/692957/file/%D0%97%D0%B1%D1%96%D1%80%D0%BD%D0%B8%D0%BA%20%D0%BA%D0%BE%D0%BD%D1%84%D0%B5%D1%80%D0%B5%D0%BD%D1%86%D1%96%D1%97%20%D0%90%D0%A0%D0%9C%20%D0%A5%D0%9D%D0%A2%D0%A3-2025.pdf>.

12. Мінухін С.В., Кавун С.В., Знахур С.В. Комп'ютерні мережі. Загальні принципи функціонування комп'ютерних мереж: навч. посіб. Харків: ХНЕУ, 2008. 210 с. URL: <https://salol.i/75fFec3>.

13. Смірнов О.А., Коноплицька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Поліщук Л.І. Інформаційна безпека в комп'ютерних мережах: навч. посіб. Кропивницький: Видавець Лисенко В.Ф., 2020. 295 с. URL: <https://dSPACE.kntu.kr.ua/server/api/core/bitstreams/73209786-0b68-4fc2-8338-a86137bf992c/content>.

14. Хоменко В.Г., Павленко М.П. Комп'ютерні мережі: навч. посіб. Донецьк: ЛАНДОН-XXI, 2011. 316 с. URL: <https://salol.i/d91552a>.

15. Хостік Лабс. Як захистити сайт від злону та вірусів: електронний ресурс. Hostiq Blog, 2024. URL: <https://hostiq.ua/blog/ukr/site-protection/>.
16. Strategically-Motivated Advanced Persistent Threat: Definition, Process, Tactics and a Disinformation Model of Counterattack: Electronic Resource. arXiv.org, 2021. URL: <https://arxiv.org/pdf/2103.15005>.
17. Elastic NV. Logstash Reference: Configuring Logstash Filters: Electronic Resource. 2024. URL: <https://www.elastic.co/guide/en/logstash/current/filter-plugins.html>.
18. He X. Research on Computer Network Security Based on Firewall Technology. Journal of Physics: Conference Series. 2021. URL: <https://iopscience.iop.org/article/10.1088/1742-6596/1744/4/042037>.
19. Imperva. Brute Force Attacks. Electronic Resource. URL: <https://www.imperva.com/learn/application-security/brute-force-attack/>.
20. Kindervag J. No More Chewy Centers: Introducing the Zero Trust Model of Information Security. Forrester Research, 2010. URL: <https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf>
21. National Institute of Standards and Technology. Contingency Planning Guide for Federal Information Systems (NIST SP 800-34 Rev. 1). U.S. Department of Commerce, 2021. URL: <https://csrc.nist.gov/pubs/sp/800/34/r1/upd1/final>
22. National Institute of Standards and Technology. Measurement Guide for Information Security: Volume 1 - Identifying and Selecting Measures (NIST SP 800-55 Vol. 1). 2024. URL: <https://csrc.nist.gov/pubs/sp/800/55/v1/final>
23. National Institute of Standards and Technology. Measurement Guide for Information Security: Volume 2 - Developing an Information Security Measurement Program (NIST SP 800-55 Vol. 2). 2024. URL: <https://csrc.nist.gov/pubs/sp/800/55/v2/final>
24. Petar Kr. Boyanov. Using VMware vSphere hypervisor ESXI 6.5.0 for virtualization of the operating system Kali Linux (64-bit) for educational purposes in

the faculty of Technical Sciences. Journal Scientific and Applied Research. 2021. P. 54–63. URL: <https://salolli.org/8b736ED>. DOI: <https://doi.org/10.46687/jsar.v21i1.320>.

25. Physical Social Engineering: Addressing the vulnerabilities that threaten to compromise workplace security. Digitalisation World. URL: <https://m.digitalisationworld.com/blogs/57641/physical-social-engineering-addressing-the-vulnerabilities-that-threaten-to-compromise-workplace-security>.

26. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. NIST Special Publication 800-207. 2020. DOI: <https://doi.org/10.6028/NIST.SP.800-207>.

27. Sina Ahmadi. Adaptive Cybersecurity: Dynamically Retractable Firewalls for Real-Time Network Protection. Journal of Computer Science. 2025. P. 2142–2152. URL: <https://salolli.org/CA1E8a0>. DOI: 10.3844/jcssp.2025.2142.2152.

28. Splunk Inc. Search Processing Language (SPL) Reference Guide: Electronic Resource. 2023. URL: <https://docs.splunk.com/Documentation/Splunk/latest/SearchReference/>.

29. The State of Incident Response 2026: Insights from 630 Investigations. Eye Security, 2026. URL: <https://www.eye.security/blog/the-state-of-incident-response-2026-insights-from-630-investigations>.

30. User and Entity Behavior Analytics (UEBA): Electronic Resource. AppOmni. URL: <https://appomni.com/saas-glossary/user-and-entity-behavior-analytics-ueba/>.

31. VMware by Broadcom Inc. VMware vSphere 8.0: official documentation, 2025. 3723 p. URL: <https://salolli.org/8b736ED>.

32. VMware Inc. vSphere Virtual Machine Administration Guide. ESXi 6.5 / VMware vCenter Server 6.5: Electronic Resource. 2021. URL: https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.vm_admin.doc/GUID-A54D6C43-611F-433E-81E9-C66C2E4A70CD.html.

33. Veeam Software. Veeam Backup & Replication v12: Security and Hardening Guide for Enterprise Infrastructure: Electronic Resource. 2024. URL: <https://www.veeam.com/documentation-guides-manuals.html>.
34. Veritas Technologies LLC. NetBackup Appliance Security Patching and Log Management Guide: Electronic Resource. 2023. URL: https://www.veritas.com/support/en_US/doc/96220900-156917520-0/index.
35. VM Install Guide for FortiAnalyzer: Microsoft Hyper-V, VMware ESXi, KVM, Citrix Hypervisor, Nutanix AHV, and AWS: Electronic Resource. Fortinet Tech Docs, 2024. URL: <https://docs.fortinet.com/document/fortianalyzer/7.4.0/vm-install-guide/>.
36. VMware by Broadcom Inc. vSphere Security Configuration Guide 8.0: Hardening ESXi and vCenter: Electronic Resource. 2025. URL: <https://core.vmware.com/vsphere-security-configuration-guide>.
37. VMware Inc. vSphere Administration for Storage and Datastore Management (ESXi 7.0): Electronic Resource. 2022. URL: <https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.storage.doc/>.
38. Vsphere Integration and Administration Guide for FortiAnalyzer Core Systems: Electronic Resource. Fortinet Technical Documentation, 2025. URL: <https://docs.fortinet.com/document/fortianalyzer/7.6.0/administration-guide/>.
39. Vsphere Networking Guide: Configuring Virtual Switches and Port Groups (ESXi 8.0): Electronic Resource. VMware Technical Documentation, 2025. URL: <https://docs.vmware.com/en/VMware-vSphere/8.0/vsphere-networking.pdf>.
40. What Is Vulnerability Management? A Complete Guide: Monitoring and Remediation. Fortinet Technical Documentation, 2022. URL: <https://www.fortinet.com/uk/resources/cyberglossary/vulnerability-management>.