МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “МЕТОДИ ЗАСТОСУВАННЯ ХМАРНИХ ТЕХНОЛОГІЙ У ЗАХИСТІ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ”

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека та захист інформації
освітньо-професійної програми Управління інформаційною та кібернетичною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Ігор ФОМІН

(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБДМ-61
Ігор ФОМІН
Керівник: Юрій ЩАВІНСЬКИЙ
к.т.н., доцент
Рецензент:
к.т.н., доцент Юрій ПЕПА

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра Управління кібербезпекою та захистом інформації
Ступінь вищої освіти магістр
Спеціальність 125 Кібербезпека та захист інформації
Освітньо-професійна програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедрою УКБЗІ
_____ Світлана ЛЕГОМІНОВА
“____” _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Студенту Фоміну Ігору Олеговичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи: “Методи застосування хмарних технологій у захисті державних інформаційних ресурсів”

керівник кваліфікаційної роботи Юрій ЩАВІНСЬКИЙ, к.т.н., доцент
(Ім’я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “30” жовтня 2025 р. № 467.

2. Строк подання кваліфікаційної роботи “11” грудня 2025 р.
3. Вихідні дані до кваліфікаційної роботи: нормативно-правові та організаційні засади захисту державних інформаційних ресурсів; хмарні моделі та сервіси IaaS, PaaS, SaaS; типові загрози й ризики для державних інформаційних систем у хмарному середовищі; методи та засоби забезпечення інформаційної безпеки; міжнародні стандарти й рекомендації у сфері кібербезпеки; наукові публікації та технічна документація.
4. Перелік питань, які потрібно розробити:
   1. Проаналізувати сучасні хмарні технології та сервіси, що застосовуються для зберігання та обробки державних інформаційних ресурсів.
   2. Вивчити нормативно-правову базу та міжнародні стандарти щодо використання хмарних технологій (ISO/IEC 27017, NIST Cloud Security, законодавство України).
   3. Виявити основні загрози та ризики при застосуванні хмарних технологій у державних системах.
   4. Оцінити ефективність існуючих методів захисту інформації у хмарних середовищах.

5. Розробити модель захисту державних інформаційних ресурсів із застосуванням хмарних технологій.
6. Сформувати практичні рекомендації щодо впровадження методів захисту.
7. Провести апробацію моделі на умовному або реальному кейсі.

5. Перелік ілюстративного матеріалу: *презентація*

6. Дата видачі завдання “02” жовтня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назви етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	10.10.2025	
2.	Збір та аналіз літератури.	23.10.2025	
3.	Аналіз основних характеристик хмарних технологій та їх застосування у захисті державних інформаційних ресурсів.	27.10.2025	
4	Вивчити нормативно-правову базу та міжнародні стандарти щодо використання хмарних технологій (ISO/IEC 27017, NIST Cloud Security, законодавство України) та сервісів IaaS, PaaS, SaaS.	05.10.2025	
5.	Виявити основні загрози та ризики при застосуванні хмарних технологій у державних системах.	10.11.2025	
6	Оцінити ефективність існуючих методів захисту інформації у хмарних середовищах.	13.11.2025	
7.	Розробити модель захисту державних інформаційних ресурсів із застосуванням хмарних технологій.	15.11.2025	
8	Сформувати практичні рекомендації щодо впровадження методів захисту.	19.11.2025	
9.	Формулювання висновків за результатами дослідження.	22.11.2025	
10.	Оформлення роботи.	04.12.2025	
11.	Оформлення презентації.	14.12.2025	
12.	Отримання рецензії на роботу.	18.12.2025	
13.	Захист в ЕК.	20.01.2026	

Здобувач вищої освіти _____ Ігор ФОМІН
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Юрій ЩАВІНСЬКИЙ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Фомін І.О. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека та захист інформації
(код, найменування спеціальності)
Освітньо-професійної програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Методи застосування хмарних технологій у захисті державних інформаційних ресурсів"
Кваліфікаційна робота і рецензія додаються.

Директор ННІКБЗІ _____ Євгенія ІВАНЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач вищої освіти ФОМІН Ігор у кваліфікаційній магістерській роботі на тему «Методи застосування хмарних технологій у захисті державних інформаційних ресурсів» здійснив аналіз теоретичних засад використання хмарних технологій у сфері кібербезпеки, визначив ключові загрози державним інформаційним ресурсам та обґрунтував необхідність системного підходу до їх захисту. У роботі розроблено модель захисту державних інформаційних ресурсів у хмарному середовищі, яка поєднує методи управління ризиками, багаторівневі засоби безпеки та практики централізованого моніторингу і реагування на інциденти. ФОМІН Ігор продемонстрував високий рівень теоретичної підготовки, володіння сучасними методами наукового аналізу та практичними навичками застосування засобів кіберзахисту.

Все це дозволяє оцінити кваліфікаційну роботу здобувача ФОМІНА Ігоря на оцінку «добре» та рекомендувати присвоїти йому кваліфікацію «Магістр з кібербезпеки та захисту інформації» за освітньо-професійною програмою «Управління інформаційною та кібернетичною безпекою».

Керівник кваліфікаційної роботи _____ Юрій ЩАВІНСЬКИЙ
(підпис). *(Ім'я, ПРІЗВИЩЕ)*

"____"_____2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Фомін І.О. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедрою
Управління кібербезпекою та захистом
інформації _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну магістерську роботу

здобувача вищої освіти Фоміна Ігоря Олеговича
на тему “Методи застосування хмарних технологій у захисті державних інформаційних ресурсів ”

Актуальність Швидке зростання обсягів державних інформаційних ресурсів та їх перенесення у хмарні середовища вимагають впровадження нових підходів до забезпечення конфіденційності, цілісності та доступності даних. В умовах зростання кіберзагроз, спрямованих на державні сервіси, особливо актуальним стає дослідження методів безпечного використання хмарних технологій та побудови стійких моделей захисту. Розробка ефективних методів застосування хмарних рішень дозволить підвищити рівень кіберзахищеності державної ІТ-інфраструктури та забезпечити безперервність роботи критично важливих сервісів.

Позитивні сторони

1. Робота має чітку структуру та логічну побудову. Послідовно розкрито теоретичні засади хмарних моделей, ризиків та підходів до їх мінімізації з урахуванням стандартів і практик кібербезпеки.
2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Ключові положення роботи представлено у вигляді рисунків. Автор опрацювала значну джерельну базу: близько 61 публікацій та електронних джерел, в тому числі англомовних.
3. Запропоновано комплексну модель захисту державних інформаційних ресурсів у хмарному середовищі, яка поєднує організаційні та технічні заходи, принципи Zero Trust, моніторинг і реагування.
4. Практична цінність підтверджується апробацією підходів у лабораторному середовищі з використанням інструментів централізованого моніторингу подій та телеметрії, що демонструє реалізовність запропонованих рішень.

Недоліки

1. Доцільним було б більш детально подати кількісне обґрунтування ефективності запропонованої моделі. Зазначене зауваження не знижує загальної позитивної оцінки роботи.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує позитивної оцінки, а здобувач ФОМІН Ігор Олегович заслуговує присвоєння кваліфікації “Магістр кібербезпеки за освітньо-професійною програмою “Управління інформаційною та кібернетичною безпекою”.

Рецензент: доцент кафедри
Технічних систем кіберзахисту

к.т.н, доцент _____ Юрій ПЕПА

підпис

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 78 стор., 30 рис., 6 табл., 61 джерел.

Метою роботи *є* розробка методичних підходи та модель застосування хмарних технологій для ефективного захисту державних інформаційних ресурсів із урахуванням сучасних кіберзагроз.

Об'єктом дослідження процеси захисту державних інформаційних ресурсів України із застосуванням хмарних технологій.

Предмет дослідження **–** методи та моделі застосування хмарних технологій для забезпечення кібербезпеки державних інформаційних ресурсів.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу, порівняння, класифікації, експертної оцінки.

Як результат у роботі проаналізовано особливості застосування хмарних технологій у захисті державних інформаційних ресурсів, визначено актуальні загрози та ризики хмарного середовища. Досліджено основні підходи й архітектурні принципи забезпечення безпеки в хмарі, зокрема управління доступом, захист даних, моніторинг і реагування на інциденти. На основі отриманих результатів розроблено модель захисту державних інформаційних ресурсів у хмарному середовищі та сформовано практичні рекомендації щодо її впровадження.

Короткий зміст роботи. Розроблено модель застосування хмарних технологій для захисту державних інформаційних ресурсів, що інтегрує технічні та організаційні заходи.

Запропоновано практичні рекомендації щодо підвищення ефективності кіберзахисту державних інформаційних ресурсів із використанням хмарних технологій.

Галузь застосування. Розроблені підходи можуть бути використані державними органами, органами місцевого самоврядування,

держпідприємствами. для побудови хмарно-орієнтованої системи кіберзахисту з централізованим моніторингом, телеметрією з кінцевих точок, розширеним логуванням, застосуванням *Zero Trust* та відпрацьованими *playbook* і *runbook* у *SOC*.

Ключові слова: ХМАРНІ ТЕХНОЛОГІЇ, ДЕРЖАВНІ ІНФОРМАЦІЙНІ РЕСУРСИ, ХМАРНА ІНФРАСТРУКТУРА, МОНІТОРИНГ ПОДІЙ.

ABSTRACT

The text part of the qualification work for obtaining the master's degree: 78 pages, 30 figures, 6 tables, 61 references.

The purpose of the study is to develop methodological approaches and a model for applying cloud technologies to effectively protect state information resources, taking into account modern cyber threats.

The object the study is the processes of protecting Ukraine's state information resources using cloud technologies.

The subject of the study is methods and models for applying cloud technologies to ensure the cybersecurity of state information resources.

Research methods. To solve the above scientific problem, the work uses methods of analysis, comparison, classification, and expert assessment.

As a result, the work analyzes the features of applying cloud technologies in the protection of state information resources and identifies current threats and risks of the cloud environment. The main approaches and architectural principles of ensuring security in the cloud, in particular access management, data protection, monitoring, and incident response, are investigated. Based on the results obtained, a model for protecting state information resources in a cloud environment has been developed and practical recommendations for its implementation have been formulated.

Brief summary of the work. A model for the application of cloud technologies for the protection of state information resources has been developed, integrating technical and organizational measures.

Practical recommendations are proposed to improve the effectiveness of cyber protection of state information resources using cloud technologies

Field of application. The developed approaches can be used by state bodies, local self-government bodies, and state-owned enterprises to build a cloud-oriented cyber protection system with centralized monitoring, telemetry from endpoints, extended logging, the use of Zero Trust, and proven playbooks and runbooks in SOC.

Keywords: CLOUD TECHNOLOGIES, STATE INFORMATION

RESOURCES, CLOUD INFRASTRUCTURE, EVENT MONITORING.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ.....…… 13
ВСТУП ……..... 15
РОЗДІЛ 1 ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ ЗАСТОСУВАННЯ ХМАРНИХ ТЕХНОЛОГІЙ У КІБЕРБЕЗПЕЦІ…. 17
1.1 Поняття хмарних технологій та їх роль у захисті інформаційних ресурсів ….…….…….…….…….…….…….…….…….…….…… 18
1.2 Моделі хмарних обчислень: IaaS, PaaS, SaaS, Private Cloud, Hybrid Cloud…… 19
1.3 Основні загрози та ризики при використанні хмарних технологій у державному секторі ……. 23
1.4 Нормативно-правова база та міжнародні стандарти (ISO/IEC 27017, NIST Cloud Security, законодавство України) …… 27
Висновки до розділу 1……. 29
РОЗДІЛ 2 АНАЛІЗ СУЧАСНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ У ХМАРНИХ СЕРЕДОВИЩАХ …… 30
2.1 Технічні методи захисту: шифрування, контроль доступу, багаторівнева автентифікація, резервне копіювання …….……..……..……...……..……..… 31
2.2 Організаційні та адміністративні заходи захисту інформації у хмарних середовищах ……..……..……..……..……..……..……..……...… 38
2.3 Порівняльний аналіз ефективності застосування хмарних технологій для захисту державних ресурсів в Україні та за кордоном …….……..…… 44
Висновки до розділу 2……. 48
РОЗДІЛ 3 РОЗРОБКА МОДЕЛІ ЗАХИСТУ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ ІЗ ЗАСТОСУВАННЯМ ХМАРНИХ ТЕХНОЛОГІЙ ……... 50
3.1 Постановка завдань та принципи системного підходу до захисту державних ресурсів ……..... 51

3.2 Модель захисту державних інформаційних ресурсів у хмарному середовищі …… 55
3.3 Розробка рекомендацій щодо впровадження методів захисту на практиці…… 59
3.4 Апробація моделі на умовному або реальному кейсі…… 63
Висновки до розділу 3…… 76
ВИСНОВКИ …… 78
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ …… 80

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

IaaS	*Infrastructure as a Service* (Інфраструктура як послуга)
PaaS	*Platform as a Service* (Платформа як послуга)
SaaS	*Software as a Service* (Програмне забезпечення як послуга)
KMS	*Key Management Service* (служба управління ключами)
HSM	*Hardware Security Module* (апаратний модуль безпеки)
IAM	*Identity and Access Management* (керування ідентифікацією та доступом)
RBAC	*Role-Based Access Control* (рольове керування доступом)
ABAC	*Attribute-Based Access Control* (атрибутивне керування доступом)
MFA	*Multi-Factor Authentication* (багатофакторна автентифікація)
API	*Application Programming Interface* (інтерфейс прикладного програмування)
QRadar	Система *SIEM*, розроблена *IBM*
RPO	*Recovery Point Objective* (цільова точка відновлення)
RTO	*Recovery Time Objective* (цільовий час відновлення)
NATO CCDCOE	*NATO Cooperative Cyber Defence Centre of Excellence* (Центр передового досвіду НАТО з кооперативної кібероборони)
FedRAMP	*Federal Risk and Authorization Management Program* (Федеральна програма управління ризиками та авторизацією)
GDPR	*General Data Protection Regulation* (Загальний регламент захисту даних)
NCSC UK	*National Cyber Security Centre United Kingdom* (Національний центр кібербезпеки Великої Британії)
ISMS	*Information Security Management System* (Система

	управління інформаційною безпекою)
SOAR	*Security Orchestration, Automation and Response* (оркестрування, автоматизація та реагування у сфері безпеки)
EDR	*Endpoint Detection and Response* (виявлення та реагування на загрози на кінцевих пристроях)
ISCM	*Information Security Continuous Monitoring* (безперервний моніторинг інформаційної безпеки)
DDoS	*Distributed Denial of Service* (розподілена відмова в обслуговуванні)
SLA	*Service Level Agreement* (угода про рівень обслуговування)
SOC	*Security operations center* (Оперативний центр безпеки)

ВСТУП

Актуальність теми. Актуальність теми зумовлена різким зростанням масштабованих і цілеспрямованих кібератак на державні інформаційні ресурси України, які тривають у режимі високої інтенсивності з 2014 року та особливо посилилися після 2022 року. Постійні *DDoS*-атаки, злам реєстрів, спроби компрометації облікових даних і руйнівні кампанії типу *wiper* свідчать про необхідність підвищення стійкості державних ІТС. У таких умовах використання хмарних технологій, що забезпечують масштабованість, резервування, високий рівень ізоляції та сучасні механізми кіберзахисту, стає одним з ключових напрямів модернізації державної цифрової інфраструктури. Дослідження методів безпечного застосування хмарних сервісів є критично важливим для забезпечення безперервності роботи державних сервісів та захисту критичних даних від сучасних загроз.

Мета роботи *є* розробка методичних підходів та моделі застосування хмарних технологій для ефективного захисту державних інформаційних ресурсів із урахуванням сучасних кіберзагроз.

Об'єкт дослідження **–** процеси захисту державних інформаційних ресурсів України із застосуванням хмарних технологій.

Предмет дослідження – методи та моделі застосування хмарних технологій для забезпечення кібербезпеки державних інформаційних ресурсів.

Для досягнення цієї мети в роботі необхідно виконати наступні завдання:

1. Проаналізувати сучасні хмарні технології та сервіси, що застосовуються для зберігання та обробки державних інформаційних ресурсів.
2. Вивчити нормативно-правову базу та міжнародні стандарти щодо використання хмарних технологій (ISO/IEC 27017, NIST Cloud Security, законодавство України).
3. Виявити основні загрози та ризики при застосуванні хмарних технологій у державних системах.

4. Оцінити ефективність існуючих методів захисту інформації у хмарних середовищах.
5. Розробити модель захисту державних інформаційних ресурсів із застосуванням хмарних технологій.
6. Сформувати практичні рекомендації щодо впровадження методів захисту.
7. Провести апробацію моделі на умовному або реальному кейсі.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, експертної оцінки, системного підходу до управління інформаційною безпекою.

Практичне значення одержаних результатів. Застосування напрацювань дасть змогу ефективніше використати наявні ресурси малих та середніх підприємств для виявлення та протидії кіберзагрозам.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 28 лютого 2025 року.

РОЗДІЛ 1 ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ ЗАСТОСУВАННЯ ХМАРНИХ ТЕХНОЛОГІЙ У КІБЕРБЕЗПЕЦІ

Тема використання хмарних технологій у сфері кібербезпеки є надзвичайно актуальною в сучасному світі, адже більшість процесів управління, обробки та зберігання даних здійснюється з опорою на цифрові платформи й мережеву інфраструктуру.

Проте залежність від хмарних технологій водночас породжує і нові виклики. Кіберзлочинці, конкуренти та інші зловмисники активно використовують можливості атак на хмарні середовища, намагаючись отримати несанкціонований доступ до критичних даних або паралізувати роботу організацій. Навіть короткочасний збій у функціонуванні хмарних сервісів може спричинити суттєві фінансові втрати та репутаційні ризики.

Для забезпечення надійного функціонування хмарних технологій необхідно впроваджувати комплексний підхід до кіберзахисту. Це передбачає багаторівневий контроль доступу, застосування сучасних методів шифрування, регулярне оновлення та моніторинг інфраструктури, а також використання систем виявлення й реагування на інциденти.

Оскільки багато користувачів та організацій мають обмежені ресурси, ключовим завданням є раціональне використання доступних інструментів безпеки, вбудованих у хмарні сервіси. Додатково важливим є залучення зовнішніх фахівців, які здатні оптимізувати процеси кіберзахисту та забезпечити відповідність міжнародним стандартам.

Співпраця між компаніями, провайдерами хмарних сервісів та державними інституціями має визначальне значення. Обмін досвідом, впровадження кращих практик та використання спеціалізованих сервісів дозволяють створити більш стійке середовище для функціонування хмарних рішень.

Застосування хмарних технологій у сфері кібербезпеки потребує системного й комплексного підходу. Лише поєднання технічних рішень,

методологічних засад та партнерської взаємодії може гарантувати надійний захист даних та стабільність роботи в умовах зростання кіберзагроз.

1.1 Поняття хмарних технологій та їх роль у захисті інформаційних ресурсів

Хмарні технології є моделлю обчислень, що забезпечує за вимогою доступ до спільного пулу обчислювальних ресурсів. Наприклад до них відносяться сховища даних, сервери, мережеві сервіси, які можна швидко налаштовувати та масштабувати без потреби у їхньому прямих локальному управлінні [1]. Іншими словами, підприємства та користувачі можуть орендувати необхідні потужності та сервіси у провайдерів хмарних платформ замість утримання власної інфраструктури [1]. Такий підхід буде створювати гнучкість і зручність. Хмара дозволяє швидко збільшувати або зменшувати ресурси відповідно до поточних потреб, що значно підвищує швидкість реагування на зміни робочого навантаження. Водночас це зменшує капітальні витрати на обладнання, оскільки компанії платять лише за реально використані ресурси

З точки зору безпеки інформації, хмарні рішення також можуть запропонувати низку переваг. Провайдери хмарних сервісів вкладають значні ресурси в сучасні механізми захисту: від фізичної безпеки дата-центрів до цифрових засобів шифрування та контролю доступу [2]. Зокрема, провайдери автоматично застосовують регулярні оновлення, впроваджують складні схеми автентифікації та шифрування даних, що забезпечує конфіденційність і цілісність інформації. Наприклад, вважається, що криптографічне шифрування – один із ключових методів захисту у хмарі – дозволяє безпечно зберігати й передавати дані, унеможливлюючи їх несанкціоноване використання [2].

Хмарні платформи відрізняються високою відмовостійкістю та доступністю: ресурси можуть бути георозподіленими між кількома дата-

центрами і дубльованими, що гарантує безперебійну роботу та резервування даних (Рис. 1.1). Згідно з дослідженнями, підприємства, які перейшли на хмарні сервіси, відзначали покращення показників безпеки та відповідності нормативним вимогам, оскільки провайдери забезпечують суворі стандарти і автоматизовані інструменти контролю [2].

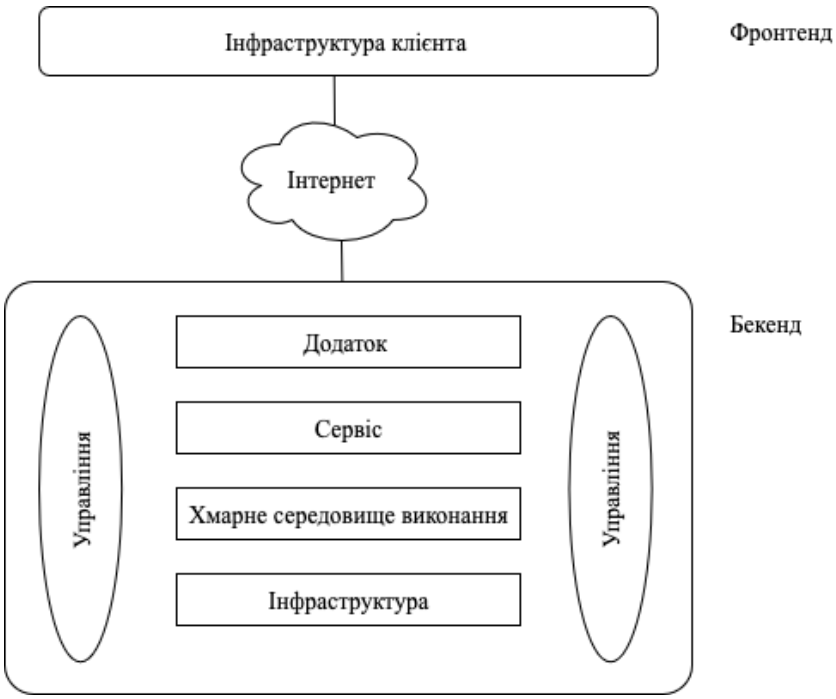


Рис. 1.1. Загальна архітектура хмарних обчислень.

1.2. Моделі хмарних обчислень: *IaaS*, *PaaS*, *SaaS*, *Private Cloud*, *Hybrid Cloud*

У науковій літературі хмарні обчислення класифікуються за моделями надання сервісу до яких відносяться *IaaS*, *PaaS*, *SaaS* та моделями розгортання публічна, приватна, гібридна. Розглянемо моделі надання сервісу: *IaaS* забезпечує інфраструктурні сервіси на вимогу; *PaaS* – готове середовище розробки операційна система, середовища виконання, бази даних; а *SaaS* – готові програмні рішення як хмарний сервіс [3]. Кожна модель має свої особливості: *IaaS* дає змогу гнучко керувати ресурсами, *PaaS* спрощує розробку і розгортання додатків, а *SaaS* звільняє користувачів від операційного

обслуговування ПЗ та інфраструктури.

Модель *IaaS* надає віртуалізовані обчислювальні ресурси: сервери, мережі та сховища через Інтернет за потребою [3]. Прикладами є *Amazon EC2*, *Google Compute Engine* та *Microsoft Azure VM*. Користувачі отримують повний контроль над операційними системами і середовищем, можуть масштабувати ресурси і оплачувати лише фактичне використання. До переваг належать висока гнучкість і відсутність капіталовкладень в IT-інфраструктуру, що виражається у економії коштів, оплаті, що відбувається за моделью *PAYG*. *PAYG* є моделю оплати за спожиті ресурси. Тобто, створюючи наприклад, *SaaS*-продукт, варто розглянути *PAYG*, де клієнт платить за кожен звіт, замість встановлення фіксованої плати за користувача. Серед недоліків *IaaS* є необхідність власного адміністрування, як оновлення ОС, забезпечення безпеки та можливі ризики збереження даних у стороннього провайдера. Тому, *IaaS* зазвичай обирають для інформаційних систем, що потребують значної гнучкості та швидкого виведення в експлуатацію [4]. До готових рішень створених за цією моделлю: *DigitalOcean*, *Linode*, *AWS*, *Cisco Metapod*, *Microsoft Azure*, *Google Compute Engine*.

SaaS відноситься до моделі, при якій клієнт користується готовим програмним забезпеченням, розміщеним і керованим провайдером у хмарі, через інтерфейси веб, *API*. А все інше до чого відноситься інфраструктура, платформа, оновлення, підтримка буде на обслуговувані провайдера. Тобто клієнт лише споживає функціонал і управляє даними, конфігураціями на рівні самого додатку. *SaaS*-модель часто є найбільш економічно ефективною для малого та середнього бізнесу: потрібні мінімальні початкові інвестиції, а оплата зазвичай здійснюється, як і в моделі *laas* за підпискою *PAYG [4]*. До недоліків віднесемо меншу гнучкість конфігурації та питання безпеки й приватності даних, оскільки вся інформація зберігається в хмарі провайдера. До готових рішень створених за цією моделлю: *Google Workspace*, *Salesforce*, *Microsoft Office 365*, *Dropbox*, *Slack*.

PaaS модель надає готову платформу для розробки, запуску і управління

додатками, без потреби управляти інфраструктурою. Тобто провайдер обслуговує: *ОС*, *middleware*, середовище виконання, бази даних, інструменти розгортання. Користувач зосереджується на логіці додатка, коді, даних, а не на базовій інфраструктурі. Однак така модель обмежує контроль над низькорівневими налаштуваннями і може призводити до прив'язки до платформеного стеку провайдера. Виходить, що *PaaS* обирають за можливість доступу до спеціалізованих ресурсів та сервісів без власної побудови складної інфраструктури [4]. До готових рішень створених за цією моделлю: *Google App Engine*, *OpenShift*, *Microsoft Azure*, *Heroku*, *AWS Elastic Beanstalk*.

На рисунку 1.2 наведено модель взаємної відповідальності яка демонструє, як розподіляються зони відповідальності між провайдером хмарних сервісів і користувачем, що були описані у рамках різних моделей.

Рис. 1.2. Модель взаємної відповідальності

Private Cloud є хмарною інфраструктурою, призначеною виключно для однієї організації. Вона може розміщуватися в дата-центрі самої організації, це є *on-premises* типом приватної хмарної інфраструктури або у виділеному

середовищі хмарного провайдера, причому всі обчислювальні ресурси доступні лише цій організації [3]. Приватні хмари надають значний рівень безпеки та відповідності нормативним вимогам, оскільки дані зберігаються в контрольованому оточенні. До основних переваг належать висока захищеність, глибока кастомізація середовища та можливість суворого контролю доступу [3]. Натомість побудова й експлуатація приватної хмари вимагають значних капіталовкладень, таких як витрати на обладнання, кваліфіковану підтримку і часто є менш масштабованими якщо порівнювати з ідентичними за функціоналом публічними хмарними сервісами.

Існує чотири основні типи приватної хмарної інфраструктури:

Локальна приватна хмара *on-premises*, коли ви розгортаєте хмару на власних ресурсах у внутрішньому дата-центрі [5]. Присутня необхідність в самостійній закупівлі обладнання, підтримці, оновленні та забезпеченні безпеки. Управління такою хмарою вимагає великих початкових інвестицій і суттєвих експлуатаційних витрат.

Керована приватна хмара є середовищем для одного клієнта, повністю кероване третьою стороною [5]. Наприклад IT-інфраструктура може бути придбана, встановлена й обслугована стороннім провайдером у його дата-центрі. Постачальник забезпечує обслуговування, оновлення, підтримку й віддалене управління приватною хмарою. Хоча такі рішення часто дорогі, вони зручніші, ніж on-premises варіанти

Віртуальна приватна хмара, *VPC* є приватним середовищем, яке розгортається всередині інфраструктури публічної хмари. Це безпечне, ізольоване середовище, у якому користувачі приватної хмари можуть виконувати код, розміщувати сайти, зберігати дані і виконувати інші задачі, притаманні класичному дата-центру. *VPC* поєднує зручність і масштабованість публічної хмари з додатковим контролем і безпекою.

Приватна хмарна платформа, або *hosted private cloud* інфраструктура, розміщується у дата-центрі стороннього провайдера але при цьому виділена лише одній організації. Тобто провайдер володіє й обслуговує обладнання,

оновлює програмне забезпечення, відповідає за безпеку. Клієнт отримує ізольоване середовище без необхідності його підтримувати.

Hybrid Cloud поєднує публічні й приватні хмарні ресурси, дозволяючи переміщувати дані та робочі навантаження між ними [6]. Така архітектура забезпечує баланс між масштабованістю публічного хмари і безпекою приватного. Наприклад, чутливі дані й критичні сервіси можна тримати в приватній хмарі, а тимчасові пікові навантаження відправляти на обробку в публічну хмару. Це підвищує гнучкість розгортання та оптимізує витрати залучаючи ресурси публічної хмари в міру потреби. Недоліком є більша складність керування інфраструктурою та підвищені вимоги до безпеки, оскільки потрібно одночасно забезпечувати захист у двох різних середовищах [6].

1.3. Основні загрози та ризики при використанні хмарних технологій у державному секторі

Використання хмарних технологій у державному секторі поєднує очевидні вигоди з специфічними для публічної сфери загрозами. Базовою рамкою для їх осмислення є модель спільної відповідальності, за якої частина функцій безпеки та відповідності покладається на провайдера, а частина на споживача сервісу. Розмежування повинно змінюватись залежно від моделі *IaaS*, *PaaS*, *SaaS* та має бути чітко зафіксоване в угодах [7]. На рівні політик і процедур державні установи повинні застосовувати ризик-орієнтований підхід, розширюючи власні політики, процедури на хмарні середовища. Враховувати, що відповідальність за конфіденційність, цілісність та доступність даних не може бути делегована провайдеру повністю. Цю вимогу доповнюють галузеві та національні режими відповідності із стандартизованою оцінкою, авторизацією та безперервним моніторингом безпеки хмарних сервісів, без чого використання хмари органами влади є неприпустимим [7]. Наприклад, у США

діє *FedRAMP* урядова програма, що встановлює стандартизований підхід до оцінювання безпеки, авторизації та безперервного моніторингу хмарних сервісів для федеральних органів [8]. Практичному вимірі це означає застосування контрольних базових наборів, узгоджених із *NIST SP* 800-53. Проходження незалежної оцінки акредитованою організацією з оцінкою третьої сторони та обов'язковий постійний моніторинг після отримання дозволу на експлуатацію, що суттєво знижує операційні ризики для державних установ [8].

Найістотніші технічні та операційні ризики пов'язані з конфіденційністю та цілісністю державних даних. Витоки виникають як через таргетовані атаки, так і через помилки конфігурації відкриті сховища, надмірні привілеї, слабке шифрування, відсутність сегментації та журналювання. Аналітика *ENISA* у 2023–2024 рр. фіксує, що до пріоритетних загроз у хмарі належать атаки на доступність, включно з *DDoS*, програми-вимагачі, загрози даним і складні ланцюгові атаки на постачальників; ці тренди підтверджуються аналізом тисяч інцидентів та розгорнутими рекомендаціями щодо пом'якшення [9].

У 2024 р. *Cloud Security Alliance* назвала 5 пункт *OWASP TOP* 10 «*misconfiguration & inadequate change control*» загрозою №1 для хмарних середовищ (Рис 1.3). Також із слабким управлінням ідентифікацією та доступом, недостатнім моніторингом і збоями у ланцюгах постачання, що безпосередньо корелює з викликами державних організацій [10]. Саме помилки конфігурації та неналежний контроль змін у поєднанні з фішингом і викраденням облікових даних призводять до «*account hijacking*», ескалації привілеїв і несанкціонованого переміщення/шифрування реєстрів та документів [10].

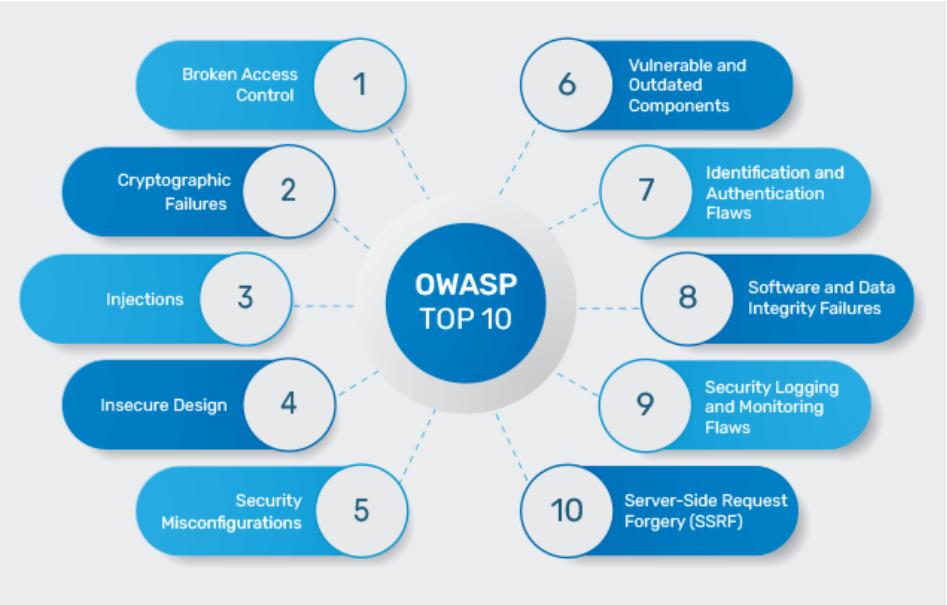


Рис. 1.3. Основні вразливості згідно *OWASP Top* 10

Загрози доступності державних сервісів посилюються як умисними впливами, так і непрямими відмовами, пов'язаними з концентрованою залежністю від провайдера. Збої у великих хмарних екосистемах або у ключових постачальників безпеки можуть одночасно вивести з ладу критичні державні послуги. Рекомендації державних регуляторів вимагають тестованих планів безперервності, запасних каналів зв'язку та процедур виявлення та реагування на інциденти [10].

Окремою групою є юридично-регуляторні ризики: локалізація даних, суверенітет та проблематика зберігання даних регулюються законами кількох держав одночасно. Навіть для публічної хмари фізичне розміщення даних і контроль над ними регулюються правом держави, де розташовані дата-центри; від цього залежать вимоги до передачі, доступу державних органів, інцидент-нотифікації та видалення. *OECP* відзначає швидке зростання обмежень локалізації й те, що особливо чутливі категорії у т.ч. публічний сектор і медичні дані підпадають під найбільш рестриктивні режими; водночас жорстка локалізація може неочікувано підвищувати витрати, зменшувати стійкість і навіть збільшувати кіберризики через гірший обмін інформацією про загрози між юрисдикціями [11]. Для державних систем це означає потребу у прозорих

вимогах до резидентності та суверенітету даних, сценаріях міждержавної передачі, угодах щодо законного доступу та продуманій криптополітиці до якої відносяться: *BYOK/HYOK*, життєвий цикл ключів, контроль над *HSM*, зафіксованих у договорах і технічному контролі їх виконання [11].

Внутрішні та ланцюгові загрози охоплюють персонал провайдера і державної організації, інтеграторів, керовані сервіси, а також програмні залежності [11]. Сучасні доповіді *ENISA* приділяють особливу увагу *supply-chain* атакам. Бо завдяки компрометації однієї компоненти або *SaaS*-постачальника дає зловмисникам доступ до багатьох державних клієнтів. Протидія потребує суворого відбору постачальників, атестації, мінімізації довіри, специфікацію або перелік складових програмного забезпечення *SBOM* та процедур швидкого відкликання вразливих компонент. До цього додаються обмеження прозорості та аналізу даних в хмарі: не всю телеметрію, журнали, метадані і *IoC* надає провайдер за замовчуванням. Це ускладнює реагування на інцидент і доказове забезпечення. Необхідно вимагати потрібні журнали, зберігати їх у холодних сховищах і відпрацьовувати процедури взаємодії команд з провайдером і регуляторами.

Організаційні ризики включатимуть в собі залежність від одного постачальника хмарних послуг, коли перехід до іншого провайдера стає складним і дорогим. Це пов’язано з складністю міграції. До цих складнощів відносяться несумісністю форматів метаданих, різними політиками доступу, а також високою вартістю передачі даних із хмари. Додаткові ризики створює нестача компетенцій адміністрування хмари; а також помилки в розумінні умов *SLA*, зокрема щодо відповідальності за резервне копіювання, тестування відновлення. Водночас рекомендації *NIST*, *NCSC UK* і *FedRAMP* підкреслюють, що ще на етапі планування організації мають чітко визначити вимоги до безпеки й приватності, передбачити незалежну перевірку контролів провайдера, закріпити права на аудит, процедури повідомлення про інциденти, правила видалення чи повернення даних [11]. Також проводити регулярний контроль відповідності протягом усього життєвого циклу хмарного сервісу.

Тобто, якщо підсумувати, то державні органи повинні виходити з того, що ризики хмарної моделі є мультифакторними: від конфігураційних похибок, викрадення облікових даних і ланцюгових атак до правових колізій суверенітету даних, зниження прозорості та залежності від постачальника. Зменшення ризиків потребуватиме створення дотримання архітектурних рішень, процесів, а також договорів і режимів відповідності [11]. В них будуть чітко описана відповідальність сторін, вимоги до журналювання та аналізу, портативності даних, доступності та незалежного аудиту.

1.4. Нормативно-правова база та міжнародні стандарти (ISO/IEC 27017, NIST Cloud Security, законодавство України)

Сучасна нормативно-правова й стандартизаційна екосистема для хмарної безпеки формується з взаємопов’язаних шарів. Міжнародних стандартів, а саме передусім серії *ISO*/*IEC* 27000 та сімейства *ISO*/*IEC* 19086 щодо *SLA*[12]. Методичних рамок *NIST* для управління ризиками й контролями безпеки у хмарі, а також національного законодавства, яке конкретизує вимоги до провайдерів. Ключова ідея цих документів поєднати процесний підхід *Information Security Management System* із моделлю спільної відповідальності, де розмежовано обов’язки провайдера і споживача, закріпивши це у договорах та *SLA* [12]. Саме тому для державних органів критично важливо одночасно: мати сертифікований *ISMS* згідно з *ISO/IEC* 27001:2022. Створити та підтримувати контролі та процеси згідно рекомендацій *NIST SP* 800-144, 800-146, 800-53 та принципів *Zero Trust* та виконувати національні вимоги, зокрема нові регуляції 2025 р. щодо постачальників хмарних і дата-центрових сервісів та законодавство про кібербезпеку й персональні дані.

NIST у сфері безпеки хмарних технологій доповнює стандарт *ISO/IEC* 27017 та надає практичні рекомендації з безпеки та каталоги засобів контролю. Також пропонує набір рекомендацій, які допомагають державним організаціям приймати ризик-орієнтовані рішення щодо використання хмарних сервісів.

NIST SP 800-145 надає канонічне визначення хмарних обчислень: п'ять основних характеристик, три моделі обслуговування та чотири моделі розгортання [13]. На які покладаються багато регуляторних органів та контрагентів; використання цього визначення дозволяє уникнути двозначності при класифікації послуг та розподілі спільних обов'язків

NIST SP 800-144 зосереджується конкретно на безпеці та конфіденційності в публічних хмарних середовищах і виділяє області ризику, які регулярно виникають у державних закупівлях: багатокористувацькість, місцезнаходження даних та їх юрисдикція, підтримка криміналістичної експертизи, прозорість послуг постачальника. Також містить організаційні рекомендації, до яких відносяться умови контракту, технічні заходи щодо зменшення ризиків.

SP 800-144 окреслює виклики безпеки та приватності у публічних хмарах і настанови з міграції даних чи додатків. Також в них наголошується, що відповідальність за захист інформації не може бути повністю делегована провайдеру та вимагає підготовленої програми управління ризиками у замовника [14].

В Українському законодавству забезпечується правовий контекст для обробки даних в інтересах або від імені українських державних органів та організацій. Закон України «Про захист персональних даних» встановлює загальні правила законної обробки, права суб’єктів даних та обов’язки контролерів.Ці вимоги повинні бути відображені в хмарних контрактах та технічних засобах контролю [15]. Закон «Про основні засади забезпечення кібербезпеки України» визначає національне кіберуправління, суб’єктів та механізми координації. Для хмарних технологій у державному секторі це встановлює очікування щодо управління ризиками, координації реагування на інциденти та взаємодії з національними компетентними органами [16]. Закон «Про захист інформації в інформаційно-телекомунікаційних системах» додає жорсткі зобов'язання щодо безпеки для систем, що містять державні інформаційні ресурси. Наприклад, сертифіковані засоби захисту та державні

експертні оцінки, повинні бути відображені в гарантіях *CSP* та в процесах акредитації та прийняття клієнта [17]. На практиці органи влади покладаються на рекомендації *CERT-UA*, *SSSCIP* та опубліковану нормативну базу при визначенні засобів контролю, інтерфейсів звітності та безпеки для хмарних послуг.

Висновки до розділу 1

Було розглянуто сутність хмарних технологій та їх роль у забезпеченні інформаційної безпеки, зокрема в контексті захисту державних інформаційних ресурсів. Узагальнено ключові моделі хмарних сервісів з варіантами їх розгортання, а також показано, що рівень контролю та відповідальності за безпеку змінюється залежно від обраної моделі та умов надання послуг.

Окрему увагу приділено типових ризикам хмарного середовища: помилкам конфігурації, компрометації облікових даних, недостатній прозорості, залежності від провайдера, а також питанням доступності та збереження даних. Проаналізовано вимоги стандартів і рекомендацій, які формують основу для побудови системи управління безпекою та вибору відповідних контролів у хмарі. Загалом зроблено висновок, що ефективне використання хмарних технологій у державному секторі можливе лише за умови системного підходу: поєднання технічних механізмів захисту, організаційних процедур, управління ризиками та дотримання вимог стандартів базпеки. Отримані положення створюють теоретичну основу для подальшої розробки та апробації моделі захисту в наступних розділах роботи.

РОЗДІЛ 2 АНАЛІЗ СУЧАСНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ У ХМАРНИХ СЕРЕДОВИЩАХ

В умовах зростання обсягів даних і складності інфраструктури хмарна безпека має будуватися як багаторівнева система, що поєднує архітектурні принципи, технічні контролі та безперервні процеси. Базою є модель спільної відповідальності: провайдер забезпечує безпеку хмарної платформи, а організація - безпеку своїх даних, облікових записів і конфігурацій. Практична мета - зменшення площини атаки, обмеження вибуху інцидентів і гарантована відновлюваність сервісів.

Шифрування має охоплювати дані: транзиті, спокої та у використанні. Для передачі застосовують сучасні версії *TLS*, для зберігання використовують шифрування з керуванням ключами через *KMS/HSM*, з визначеними чіткими політиками створення, ротації та знищення ключів. Коли необхідно обробити дані з чутливим вмістом, використовують *confidential computing*. Це методом, коли виконання відбувається в ізольованих середовищах, що мінімізує ризики доступу з боку гіпервізора чи адміністраторів. Також важливо відокремити життєвий цикл ключів від життєвого циклу даних. Та за потреби застосовувати моделі *BYOK/HYOK*.

Контроль доступу реалізується через централізований *IAM* із принципом найменших привілеїв, сегментацією ролей та умовними політиками доступу. Рольова модель доповнюється атрибутивною для урахування контексту, що міститиме: пристрій, географія, час, ризик. Адміністративні дії відокремлюються у спеціальні облікові записи, з журналюванням кожної операції та тимчасовим підвищенням прав за запитом. Секрети й токени зберігаються у керованих сховищах, доступ до управлінських *API* обмежується за мережевими й ідентифікаційними ознаками.

Багаторівнева автентифікація є обов’язковою до всіх критичних доступів. Насамперед повинна бути стійкою до фішингу, а саме завдяки апаратних ключів та паскії. Це поєднується з політиками сесій в яких повинні бути вказані

час життя токенів, їх повторна перевірка при ризикових операціях з прив'язкою автентифікатора до пристрою й обов'язковим *MFA* для будь-яких змін у конфігурації хмари, керуванні ключами та розгортанні інфраструктури.

Резервне копіювання повинно орієнтуватись на відновлюваність: визначені *RTO/RPO*, міжрегіональна або міжхмарна реплікація. Необхідні також механізми виявлення аномалій у копіях: масові видалення, нетипові зміни. Та повинні бути прописані сценарії швидкого відновлення сервісів, а не лише їх даних.

Мережевий рівень підсилюється мікросегментацією, приватними кінцевими точками, керованими сервісами *WAF* з захистом від *DDoS*.

Безперервний моніторинг і реагування включають: централізацію журналів, кореляцію подій у *SIEM* з їх подальшим аналізом в *SOAR* та моделі поведінкових аномалій, що міститимуть техніки зловмисників згідно їх профілів в *MITRE ATT&CK*.

Безпека ланцюга постачання повинна реалізовуватись через перевірені джерела артефактів, підпис виконуваних образів і контейнерів, ведення *SBOM*, а також регулярні оновлення з тестуванням відкату.

Таким чином, сучасний захист у хмарі - це скоординована сукупність шифрування, керування ідентичністю та доступом, фішингостійкої *MFA*, надійних бекапів і відпрацьованого моніторингу й реагування, що працюють разом і постійно перевіряються на практичну ефективність.

2.1. Технічні методи захисту: шифрування, контроль доступу, багаторівнева автентифікація, резервне копіювання

Технічні засоби безпеки у хмарних середовищах мають реалізовуватися як взаємо доповнювана система контролів, узгоджена з «моделлю спільної відповідальності» та профілем ризиків організації. Базовою засадою є забезпечення конфіденційності, цілісності та доступності даних на всіх етапах їхнього життєвого циклу від створення і передачі до зберігання та відновлення

після інцидентів. У практичному вимірі це означає коректне застосування сучасних криптографічних механізмів, політик керування доступом, стійкої до фішингу багаторівневої автентифікації і перевіреної стратегії резервного копіювання *RTO* і *RPO* [18].

Методи шифрування даних відіграють вирішальну роль у захисті інформації, що передається та зберігається в розподілених хмарних системах. Різні підходи до шифрування забезпечують різні рівні безпеки та продуктивності, що дозволяє вибрати найбільш підходящий метод залежно від вимог системи. Тому у таблиці 2.1 наведено основні методи шифрування даних, їхні переваги та недоліки.

Таблиця 2.1

Характеристики методів шифрування даних

Метод шифрування	**Основні алгоритми**	**Переваги**	**Недоліки**
Симетричне шифрування	*AES*, *DES*, *3DES*	Висока швидкість, ефективність при великих обсягах даних	Проблеми з безпечним управлінням ключами
Асиметричне шифрування	*RSA*, *ECC*	Високий рівень безпеки, зручна передача ключів	Високе обчислювальне навантаження
Гібридне шифрування	*SSL*/*TLS*	Поєднує переваги симетричного та асиметричного шифрування	Складне впровадження, потреби в інфраструктурі

Симетричне шифрування характеризується високою швидкістю роботи, що робить його придатним для оброблення великих обсягів даних, однак воно потребує надійних методів управління ключами. Асиметричне шифрування забезпечує високий рівень безпеки, проте накладає значні обчислювальні навантаження на систему. Гібридне шифрування, представлене такими алгоритмами, як *SSL*/*TLS*, поєднує переваги обох підходів, хоча його реалізація є складнішою і вимагає розвиненої інфраструктури**.**

У сучасних системах розподіленого керування, шифрування даних залишається основним методом забезпечення конфіденційності інформації. Симетричне шифрування, яке використовує один і той самий ключ для процесів шифрування та розшифрування, відзначається високою продуктивністю і часто

застосовується для захисту даних під час зберігання.

Шифрування повинно охоплювати дані, як під час передавання, у зберіганні і під час обробки. Для захисту трафіку в хмарі є обов'язковим використання *TLS* 1.2 з *FIPS*-сумісними наборами шифрів або як мінімум і підтримкою *TLS* 1.3, правильним налаштуванням сертифікатів і відсутністю застарілих алгоритмів; такі вимоги прямо фіксуються у настановах *NIST* щодо *TLS* [19]. Для зберігання даних застосовується симетричне шифрування з перевіреним керуванням ключами: визначаються довжини ключів, періоди ротації, політики розмежування та знищення ключового матеріалу згідно з рекомендаціями з криптографії та менеджменту ключів. Самі криптомодулі повинні відповідати вимогам *FIPS* 140-3, що гарантує належний рівень захисту реалізацій на програмному або апаратному рівні [20]. Для сценаріїв обробки чутливих даних доречно впроваджувати підхід *confidential computing* на базі апаратних довірених середовищ виконання, що ізолюють пам'ять під час виконання й знижують ризики доступу з боку гіпервізора та адміністраторів хмари.

Керування доступом є першою лінією оборони проти ескалації привілеїв і бічного руху зловмисника. У хмарі воно будується на централізованій службі *IAM* з реалізацією принципу найменших привілеїв, чіткого поділу облікових записів користувацькі, сервісні, адміністративні, сегментації ролей і насиченого журналювання дій. Рольову модель *RBAC* доцільно поєднувати з атрибутивною *ABAC*, яка враховує контекст доступу, атрибути суб'єкта та об'єкта, умови середовища. Саме *ABAC* надає гнучкість у мультиорендних хмарних середовищах і спрощує реалізацію політик умовного доступу. Контролі сімейства *AC* у *NIST SP* 800-53 слугують опорним переліком вимог до управління обліковими записами, авторизації операцій, сегментації меж довіри та аудиту; їх застосування забезпечує відтворюваність політик у різних моделях сервісу від *IaaS* до *SaaS* [21]. На практиці це означає: привілейований доступ, лише тимчасово та лише через контрольовані секрети та токени у керованих сховищах. Виклики адміністративних *API* повинні відбуватись із мережевими

та ідентифікаційними обмеженнями.

Багаторівнева автентифікація, *MFA* для адміністративних і всіх інших критичних доступів є обов’язковою. Оновлені Digital Identity Guidelines визначають технічні вимоги для рівнів гарантій автентифікації *AAL* та прямо рекомендують методи, що протидіють атакам з посередником, зокрема *FIDO2*, *WebAuthn*. Практичні настанови з безпеки підтверджують, що *SMS*-коди та звичайні пуш підтвердження можуть бути обійдені сучасними фішинговими інструментами. Натомість криптографічні автентифікатори, прив’язані до пристрою, суттєво знижують ризик компрометації облікових записів [22]. Політика сесій має передбачати контроль часу життя токенів, повторну перевірку під час ризикових операцій і обов’язкову *MFA* для змін у конфігурації хмари, керуванні ключами та розгортанні інфраструктури

Резервне копіювання у хмарі є процесом збереження захищених копій даних і систем у віддаленій інфраструктурі, що управляються постачальником. Та використання цих копій для відновлення роботи після втрати, пошкодження або порушення цілісності. У сучасних хмарних середовищах резервне копіювання тісно пов'язане з відновленням після інцидентів для підтримки безперервності бізнесу [23]. Це дозволяє організаціям відновлювати роботу у визначенні терміни, мінімізуючи капітальні витрати на локальні носії та обладнання.

Дві цілі визначають рішення щодо проектування:

1. *Recovery Point Objective* – це цільова точка відновлення де вказано максимально допустима кількість останніх даних, які можуть бути втрачені.
2. *Recovery Time Objective* – це цільовий час відновлення де вказано максимально допустимий час для відновлення роботи.

Ці показники взаємопов'язані через концепцію *Maximum Tolerable Downtime* [23]:

$$RPO = MTD - Time\ to\ Recover\ Data \qquad (2.1)$$

Наприклад, якщо організація може допустити 4-годинне припинення роботи, а відновлення даних займає 30 хвилин, то *RPO* становитиме 3 години 30 хвилин. Крім того, рівень безпеки хмарного резервного копіювання залежить від застосування криптографічного захисту ключів, що вимагає розмежування життєвих циклів ключів і даних через моделі *BYOK* або *HYOK*, де ротація ключів відбувається незалежно від ротації резервних копій.

Базова формула для оцінювання впливу ризику на вибір *RTO*/*RPO*:

$$Risk = Likelihood \times Impact \qquad (2.2)$$

де *Likelihood* залежить від вразливостей, загроз, експозиції та наявних контролів безпеки.

Це дозволяє державним установам пропорційно розподіляти ресурси: критичні сервіси, реєстри громадян, системи енергопостачання отримують найнижчі значення *RPO*/*RTO*, часто близькі до нуля. Менш критичні системи можуть допускати більші значення за умови вищого рівня захисту даних.

У літературі узагальнено три широко застосовувані моделі, які відрізняються за складністю, вартістю та показниками *RPO* та *RTO*:

1. *Disaster Recovery* – керовані основні та резервні середовища відновлення після збоїв, у яких робоче та резервне середовища повністю адмініструються постачальником послуг.
2. Хмарне резервне копіювання та відновлення – це коли дані зберігаються у хмарних сховищах, а обчислювальні ресурси надаються лише під час відновлення.
3. Реплікація до хмари – це коли забезпечується безперервне віддзеркалення стану системи на хмарні ресурси (Рис.2.1)

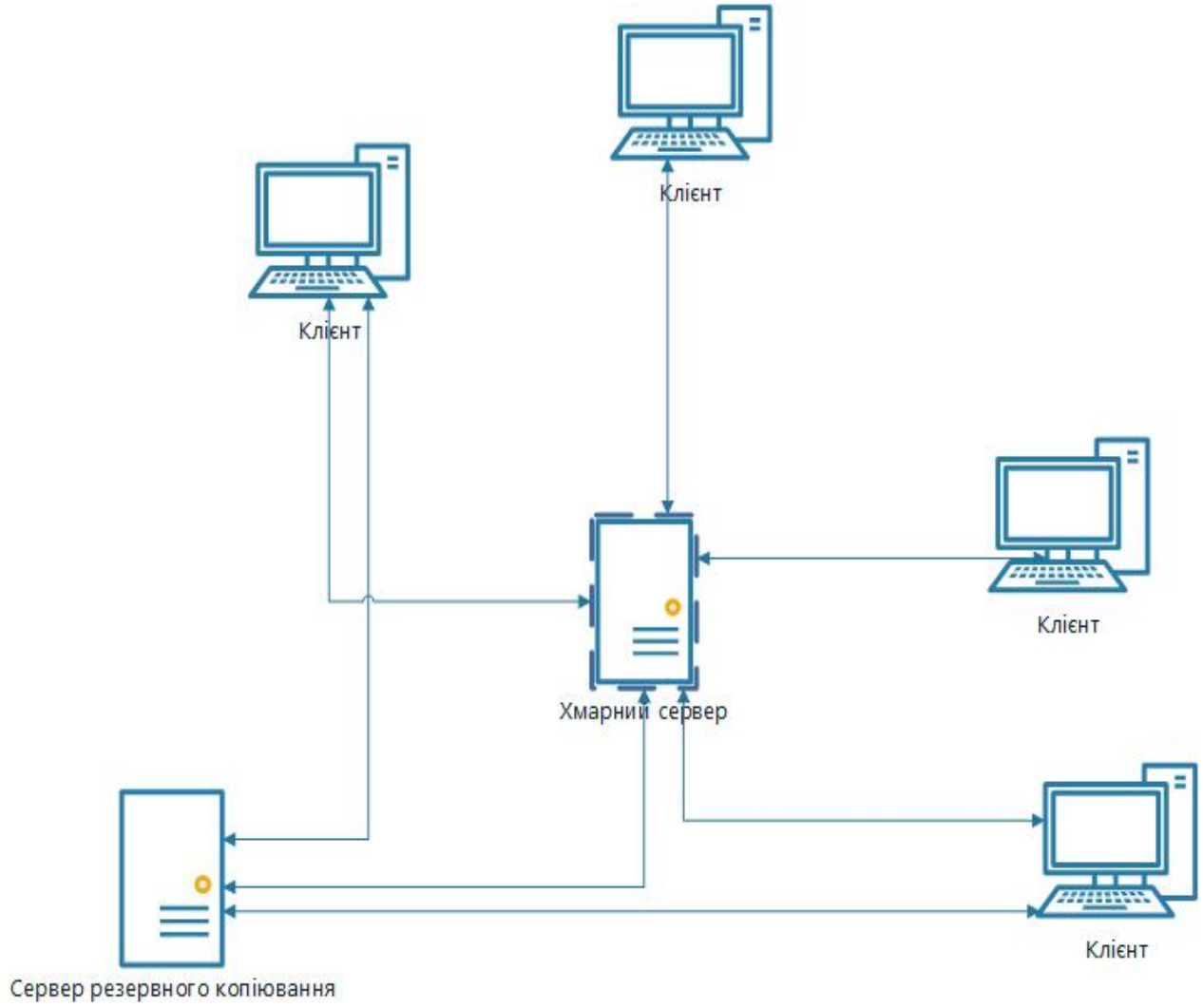


Рис.2.1. Опис архітектури відновлення даних

Кероване *Disaster Recovery* характеризується операційною простотою та оплатою за фактичне використання ресурсів. Підхід резервного копіювання та відновлення зменшує поточні витрати, але потребує більшого часу на відновлення. Реплікація до хмари забезпечує найнижчі значення показників *RPO* і *RTO*, проте супроводжується найвищою операційною складністю. Наприклад, потребою у спеціалізованому програмному забезпеченні для реплікації, мережевих шлюзах та спеціалізованих системах зберігання даних. Можливості резервного копіювання хмарних обчислень наведені в табл. 2.2.

Таблиця 2.2

Підходи до відновлення даних

Фактори	**Керовані основні середовища та середовища відновлення після збоїв**	**Хмарне резервне копіювання та відновлення**	**Реплікація у хмарі**
Середовище	*Salesforce.com*, *CRM*, електронна пошта у хмарі	Реалізується як з локальної інфраструктури у хмару, так і між хмарними середовищами	Може здійснюватися як з локальної інфраструктури у хмару, так і між хмарами.
Показники	Повністю кероване відновлення після збоїв; модель оплати за фактичне використання, найменша операційна складність.	Потребує лише хмарного сховища; Використання віртуальних машин у хмарі є необов'язковим. Зазвичай має меншу складність, ніж реплікація	Забезпечує найкращі показники *RTO* та *RPO*, а також найімовірніше підтримує відновлення з узгодженим станом застосунків.
Застереження	Угоди про рівень надання послуг визначають порядок доступу до робочого та резервного середовищ.	Забезпечує гірші показники *RTO* та *RPO*, порівняно з реплікацією	Відзначається високим рівнем складності
Реалізація	Не передбачено	Використовує спеціалізовані програми та пристрої для резервного копіювання.	Вимагає використання програмного забезпечення для реплікації, хмарних шлюзів та систем зберігання даних, таких як *EMC Atmos* і *Hitachi HCP*.

2.2. Організаційні та адміністративні заходи захисту інформації у хмарних середовищах

На практичному рівні організаційні та адміністративні заходи починаються з побудови системи управління інформаційною безпекою, яка політиками, процедурами та відповідальністю покриває увесь життєвий цикл даних і сервісів у хмарі [24]. Водночас набір формалізованих контролів має бути узгоджений з каталожними вимогами до безпеки та приватності й відображений у внутрішніх регламентах, що забезпечує відтворюваність і перевірюваність рішень на рівні організації [25].

Успіх впровадження організаційних заходів залежить від активної залученості керівництва, яка охоплює визначення пріоритетів безпеки, розподіл необхідних ресурсів, персоніфікацію відповідальності та створення єдиного інформаційного простору для обміну інцидентною інформацією в межах організації. Лідерство в питаннях безпеки хмари передбачає постійний моніторинг стану впровадження контролів та готовність до адаптації підходів у відповідь на зміни загроз .

Для керованого старту важливо одразу зафіксувати «модель спільної відповідальності» в договорах і політиках, уточнивши межі провайдера та замовника, права на аудит, надання телеметрії, строки інцидент-нотифікації та правила видалення/повернення даних після припинення користування [25]. Рамкові принципи безпечного використання хмарних сервісів доцільно брати з державних рекомендацій із захисту хмари, адаптуючи їх до власних вимог і класифікації інформації [26]. При цьому особливої уваги заслуговує гармонізація локальних вимог законодавства та відомчих нормативів із кращими світовими практиками: *ISO*/*IEC* 27017, *NIST*, *FedRAMP*, *Cloud Controls Matrix*. Це надає можливість забезпечити як зовнішню сумісність у разі аудиту, так і внутрішню керованість системи .

Послідовне управління ризиками починається з інвентаризації активів, загроз і вразливостей, далі відбувається оцінка ризиків із визначенням

критичності сервісів та гранично припустимого залишкового ризику для бізнес-процесів. На підставі класифікації даних формуються правила маркування, доступу, шифрування, терміни зберігання й архівації, а для чутливих категорій проводяться оцінки впливу на приватність і транскордонні передачі з урахуванням юрисдикцій і локалізаційних обмежень. Особливої уваги в державному середовищі заслуговує контроль за транскордонним передаванням даних та відповідність вимогам щодо місцезнаходження інформації, а також інтеграція положень щодо особливих категорій захищених даних. До таких категорій відносяться: державна таємниця, персональні дані.

Захист конфіденційних даних, включаючи персональні ідентифікатори, паролі та фінансову інформацію, потребує застосування криптографічних методів та інтеграції з системами ідентифікації, такими як одноразові коди та біометричні системи. Ці технології забезпечують багаторівневий контроль доступу та з'ясування особи користувача на різних етапах взаємодії з системою, що особливо важливо для захисту державних інформаційних ресурсів від несанкціонованого доступу. У сучасних хмарних інфраструктурах для таких задач застосовується комплексний набір організаційних, технічних і правових заходів, які можна структуровано подати у вигляді таблиці 2.3, як оптимальні методи безпеки.

Таблиця 2.3

Методи забезпечення безпеки у хмарних обчисленнях

Сфера захисту	**Ключові засоби або політики**	**Технологічна реалізація**	**Приклади впровадження або призначення**
Захист даних	Криптографічний захист	*SSL*/*TLS*, *AES*-256, *RSA*	Використання *HTTPS* для всіх ресурсів системи
Резервування інформації	Регламентоване резервне копіювання	*Cloud storage*, диференційоване	Щоденне збереження резервних копій
Географічне резервування	Віддалене резервування	*Incremental backup*	Копії даних у декількох розподілених локаціях

Продовження таблиці 2.3.

Сфера захисту	**Ключові засоби або політики**	**Технологічна реалізація**	**Приклади впровадження або призначення**
Виявлення загроз	Поведінковий та аномалійний аналіз	*SASE*, *DAST*	Постійний аналіз мережевого трафіку
Фільтрація трафіку	*WAF*, *IDS*/*IPS*	*WAF*, *IPS*	Захист від небезпечних запитів
Оперативний моніторинг	Автоматизовані системи моніторингу	*SIEM*	Постійний контроль та фіксація інцидентів
Захист ідентифікаторів	Мультифакторна аутентифікація	*DLP*-системи	Виявлення й блокування підозрілої активності

Організаційна частина керування доступом охоплює процеси «*joiner–mover–leaver*», розділення обов’язків, періодичні рецертифікації доступів і окремі канали для привілейованих операцій з обов’язковим журналюванням. Для зменшення площини атаки доступ надається за принципом найменших привілеїв із контекстною перевіркою ідентичності, пристрою та середовища, що відображає підхід нульової довіри в адміністративних політиках [26]. Підвищення ефективності керування доступом залежить від чіткого розмежування ролей і зон відповідальності: впровадження моделі розподіленого керування доступом *RBAC* та *ABAC*, сегментації адміністрування хмарної інфраструктури та регулярного навчання користувачів і адміністраторів з акцентом на специфічні хмарні ризики

Управління змінами та конфігураціями є стрижнем запобігання помилкам, адже більшість інцидентів у хмарі виникають через відхилення від базових налаштувань і несанкціоновані зміни [27]. Базові конфігурації кодуються як політики та інфраструктура-як-код із обов’язковим погодженням змін, тестовими середовищами, процедурами для екстрених змін та подальшим «post-change» оглядом, а відповідність контрольним наборам відстежується безперервно. Необхідно також забезпечувати періодичні перевірки актуальності базових налаштувань та порівняння з еталонними конфігураціями для

виявлення та усунення відхилень.

Робота з постачальниками закладається в життєвий цикл закупівель: проводяться перевірки безпеки провайдера, аналізуються сертифікації, атестації та документація контролів до визнаних стандартів, а вимоги до журналів, аналізу та часу оповіщення про інциденти вносяться в договірні умови. Державним організаціям доцільно спиратися на стандартизовані підходи до оцінювання, авторизації та безперервного моніторингу хмарних сервісів, що прискорює впровадження і підвищує порівнюваність результатів у секторі [28]. Крім того, потребує контролю механізм затвердження відповідних сертифікацій провайдерів та проведення аудитів на місці чи віддалено, прозорості ланцюгів підрядників та документування вимог до збереження й видалення даних після припинення співпраці .

Безперервний моніторинг оформлюється як програма *ISCM* із визначеними метриками, джерелами телеметрії, періодичністю вимірювань і відповідальними за аналіз відхилень, що забезпечує видимість стану активів і ефективності контролів у часі. На рівні операційного центру безпеки агрегуються журнали, події корелюються в *SIEM*, а процедури реагування формалізуються в *playbook* та *runbook* із чіткими ролями, каналами ескалації та комунікаціями [29]. Програма *ISCM* має включати механізми для збору даних безпеки в режимі реального часу та автоматизовану обробку результатів для своєчасного виявлення відхилень від встановлених норм .

Центральна роль у реагуванні на інциденти відводиться ключовим операційним метрикам, що характеризують готовність та спроможність команди безпеки. *Mean Time To Acknowledge* дозволяє виміряти час від моменту виявлення інциденту до його визнання командою:

$$MTTA = \frac{\sum Time\ Between\ Alert\ and\ Acknowledgement}{Number\ of\ Incidents} \qquad (2.3)$$

Наприклад, три інциденти були визнані за 30 секунд, 10 хвилин та 2

хвилини відповідно, то *MTTA* становитиме (30 + 600 + 120) / 3 = 250 секунд або приблизно 4,17 хвилини. Низьке значення *MTTA* сигналізує про ефективність автоматизованих систем виявлення та ясних процедур ескалації

Mean Time To Resolve - найширше вживана метрика охоплює весь час від виявлення інциденту до повного його розв'язання, включаючи діагностику, виправлення та запровадження довгострокових заходів:

$$MTTR = \frac{Total\ Resolution\ Time}{Number\ of\ Resolved\ Incidents} \quad (2.4)$$

Тобто, якщо система пережила 5 інцидентів загальною тривалістю 12,5 годин розв'язання, то *MTTR* = 12,5 / 5 = 2,5 години. Досягти оптимізацію *MTTR* можливо через:

– впровадження автоматизованого виявлення та оповіщення;

– застосування *SOAR*-платформ для автоматизації першочергових дій реагування;

– регулярне вдосконалення *playbook* та *runbook* на основі аналізу пост-інцидентних звітів.

Mean Time Between Failures вказує на середній інтервал між двома послідовними збоями системи:

$$MTBF = \frac{Total\ Operational\ Time}{Number\ of\ Failures} \quad (2.5)$$

Моніторинг *MTBF* допомагає виявити тенденції та оцінити, чи поточні заходи безпеки ефективно знижують кількість інцидентів. Для державних установ постійний контроль цих метрик через системи *SIEM* та *SOAR* забезпечує чіткість щодо ефективності оперативного реагування та потреб у додаткових інвестиціях у автоматизацію.

Підтримка готовності до інцидентів вимагає регулярних навчань і вправ, включно з сценаріями та перевірками відновлення. Тестується досяжність *RTO*

та *RPO* для критичних сервісів і зазначаються потенційно проблемні місця взаємодії з провайдером і суміжними підрядниками [30]. Паралельно політики й стандарти безпеки періодично переглядаються на відповідність змінам загроз, технологій і вимог регуляторів. Результати аудиту інтегруються у план безперервного вдосконалення *ISMS*. Розбудова культури безпеки охоплює не лише формальні тренінги, а й безперервне підвищення обізнаності щодо нових загроз. Це особливо актуально при використанні хмарних розгортань у держсекторі, та передбачає відпрацювання сценаріїв для різних категорій працівників.

Для системної узгодженості застосовується документування внутрішніх політик на контрольні матриці для хмарних середовищ. Це спрощує перевірки й уніфікує підхід між різними моделями сервісу та розгортання [31]. Додатково принципи безпечної хмари, оприлюднені національними відомствами, інтегруються в локальні стандарти організації, забезпечуючи керованість, підзвітність і прозорість рішень для бізнес IT керівництва. Розбиття на контрольні матриці має полегшити взаємодію з регуляторними органами та дозволити демонструвати відповідність встановленим вимогам .

Послідовне управління життєвим циклом інцидентів і забезпечення безперервності діяльності передбачають формалізацію усіх етапів від моніторингу та виявлення подій до реагування, усунення та постінцидентного аналізу . Для державних органів доцільно формалізувати плани забезпечення безперервності діяльності *BCP* та *DRP*. Їх необхідно обов'язково співвідносити з вимогами законодавства щодо відновлення критичних сервісів у визначені терміни та регулярно тестувати їх через навчання і вправи. Забезпечення безперервного вдосконалення організаційних заходів передбачає обов'язкове врахування результатів аудитів, тестувань та регулярних оглядів політик з метою адаптації до нових ризиків та змін в технологічному ландшафті .

У підсумку організаційні та адміністративні заходи утворюють керівний каркас, у межах якого технічні контролі працюють узгоджено, вимірювано а відповідальність сторін стає чіткою і практично застосовною в щоденних

процесах. Саме така конструкція дозволяє зменшити конфігураційні збої, прискорити реагування на інциденти та підвищити стійкість хмарних сервісів без втрати керованості й відповідності вимогам регуляторів.

2.3. Порівняльний аналіз ефективності застосування хмарних технологій для захисту державних ресурсів в Україні та за кордоном

У порівняльній площині важливо відзначити, що для України ключовим драйвером переходу в хмару стала стійкість державних сервісів під час повномасштабної війни. Коли хмарні провайдери допомогли оперативно переносити критичні реєстри й робочі навантаження, забезпечуючи безперервність надання послуг громадянам. Досвід перших місяців війни продемонстрував критичну важливість попередньо налаштованої інфраструктури відновлення. Це дозволяє зберігати дані про громадян і підприємства навіть за умов руйнування фізичних центрів обробки даних. У цьому контексті значущим прикладом є масштабна підтримка державних органів та критичної інфраструктури у вигляді хмарних ресурсів і кредитів. Дозволило зберегти функціонування цифрових сервісів попри тривалі кібератаки та фізичні руйнування.

Для України конкретно міграція до хмари усунула потребу в підтримці вразливих локальних дата-центрів у зонах конфлікту. Цифрова стійкість українських державних установ також підтримувалася завдяки технологічним можливостям провайдерів щодо швидкого масштабування обчислювальних потужностей і створення географічно розподілених резервних копій [32].

Особливості стратегічних підходів та моделей управління хмарною безпекою в кризових і стабільних умовах можна ясно простежити шляхом порівняння практик України та міжнародних прикладів, як це наведено у таблиці 2.4.

Таблиця 2.4

Стратегічні чинники та управління

Розмір	**Впровадження хмарних технологій в Україні у воєнний час**	**Впровадження хмарних технологій в Великобританії / США / Естонії**
Основний фактор	Швидка безперервність роботи уряду та відновлення після катастроф під час повномасштабної війни; термінова міграція реєстрів та робочих навантажень до гіпермасштабних хмарних середовищ із кредитами провайдерів та практичною підтримкою.	Модернізація на основі політик із стандартизованими, повторюваними засобами контролю для збалансування швидкості, вартості та ризиків. Наприклад, «*Cloud First*» у Великій Британії; централізована федеральна авторизація у США.
Управління та принципи	Прагматичне зміцнення, орієнтоване на операції: багаторегіональні резервні копії, швидке переміщення, послуги безпеки, що управляються постачальником.	Нормативні рекомендації та багаторазове забезпечення: Принципи безпеки хмарних технологій *NCSC* Великобританії; «Стратегія єдиної урядової хмари» Великобританії; базові вимоги *FedRAMP* США та постійний моніторинг.
Авторизація та гарантія	Індивідуальне затвердження в умовах кризи, з використанням підтверджень постачальників та найкращих практик.	Централізовані/стандартизовані схеми зменшують обсяг повторних аудитів: *FedRAMP ATO* та ринкові майданчики; підходи, узгоджені з британською *G-Cloud*.
Суверенітет та безперервність даних	Транскордонні резервні копії та гео-резервування мають пріоритет для забезпечення доступності послуг, незважаючи на фізичні ризики.	Модель «посольства даних»: центри обробки даних з дипломатичним статусом для забезпечення безперервності та суверенітету.

Паралельно із перенесенням даних у хмару ефективність забезпечення доступності підтверджується успішними практиками відбиття *DDoS*-атак. Аналіз хронології кіберінцидентів показує, що після переходу до хмарної моделі державні портали України витримали атаки об'ємом, який раніше міг призвести до багатогодинних збоїв. Такий досвід демонструє, що модель безпеки як сервіс у поєднанні з багато орендною масштабованою інфраструктурою здатні швидко підвищувати стійкість державних систем у кризових умовах [32]. Ключовою відмінністю сучасного підходу є також

інтеграція заходів захисту безпосередньо у провайдера. Він усуває необхідність розгортання і підтримки власних мереж безпеки кожним відомством окремо. Особливості впроваджених механізмів та досягнутих результатів у сфері хмарної безпеки можна узагальнити у вигляді наступної таблиці 2.5.

Таблиця 2.5

Можливості безпеки та спостережувані результати

Спроможність та результат	**Українські державні послуги**	**Міжнародні зразки Великобританія, США, Естонія**
Стійкість до *DDoS*-атак	Використовували глобальних провайдерів «безпеки як послуги» для поглинання сплесків; державні портали залишалися доступними навіть при обсягах, які раніше спричиняли багатогодинні перебої в роботі.	Безперервна глобальна спроможність очищення та автоматизоване пом'якшення наслідків; атаки рекордного масштабу регулярно нейтралізуються без ручного втручання.
Багаторегіональне відновлення після збою та резервне копіювання	Попередньо налаштована інфраструктура відновлення, копії в декількох регіонах, швидке масштабування обчислювальних потужностей під час інцидентів для підтримки послуг для громадян.	Стандартні шаблони: топології з декількома зонами доступності/регіонами, перевірені посібники з відновлення та кодифіковані *RTO*/*RPO* в закупівлях.
Стандартизовані засоби контролю безпеки	Прийняті набори засобів контролю постачальників та найкращі практики в екстрених ситуаціях: посилення *IAM*, ведення журналів.	Формальні базові вимоги: принципи *NCSC*; каталоги контролю *FedRAMP що* забезпечують послідовну, порівнянну гарантію та швидше отримання дозволів.
Аудит та ефективність закупівель	Довіра до доказів постачальника прискорила термінове впровадження; аудити були вдосконалені після міграції.	Повторне використання стандартних оцінок знижує навантаження на аудит та час на виконання операцій у різних установах;.
Безперервність та суверенність даних	Резервні копії, що зберігаються за межами країни	Об'єкти «посольства даних» забезпечують безперервність діяльності та правовий захист у дружніх юрисдикціях на основі міжнародних договорів.

Архітектура нульової довіри *Zero Trust Architecture*, *ZTA* стала ключовим

елементом найкращих практик безпеки хмарних мереж, виходячи з припущення про відсутність автоматичної довіри та постійної верифікації запитів доступу. Дослідження демонструють значні покращення у кількості інцидентів безпеки після впровадження *ZTA*, включаючи пом'якшення бічного переміщення всередині мереж, зменшення ймовірності внутрішніх загроз, покращену мережеву мікросегментацію та вдосконалене управління ідентичністю та доступом. Інтеграція *ZTA* з моделями спільної відповідальності забезпечує глибокий ешелонований захист для урядових хмарних розгортань.

У контексті транскордонного передавання даних та суверенітету ключовим залишається питання юрисдикційного контролю. Міжнародні фреймворки, зокрема *GDPR* Європейського Союзу, встановлюють найбільш комплексний підхід [33]. В ньому описані, як повинна відбуватись локалізація даних та контроль їх обробки. Досвід України з швидким переміщенням критичних державних даних на міжнародні хмарні платформи спочатку створював напруження з принципами суверенітету даних, оскільки інфраструктура знаходилася поза межами української території. Проте нормативні розробки, включаючи запропоновані акти про хмарні сервіси, спрямовані на встановлення балансу між безпековими потребами та питаннями суверенітету.

Модель посольств даних, реалізована Естонією та Люксембургом, пропонує перспективний підхід до забезпечення безперервності та суверенітету даних. Відбувається це через створення дата-центрів із дипломатичним статусом у дружніх юрисдикціях. Така модель забезпечує міжнародно-правовий захист державних даних навіть при їх фізичному розміщенні за кордоном [34]. Це може бути особливо актуальним для України з огляду на потреби географічного резервування критичних реєстрів.

Міжнародна співпраця відіграє критичну роль у посиленні колективних захисних спроможностей. Обмін інформацією про загрози, найкращими практиками та технічною допомогою зміцнює можливості як окремих держав, так і колективної безпеки. Центр передового досвіду *NATO* з кооперативної

кібероборони *CCDCOE* надає спільні фреймворки для держав-членів і партнерів, таких як Україна, визнаючи кіберпростір доменом ведення війни та підкреслюючи автономні агенти кібероборони, захищені мережі та стійкість проти загроз, що еволюціонують[34].

Висновки до розділу 2

Криптографічний захист залишається фундаментальною основою безпеки хмарних інфраструктур. Впровадження симетричних алгоритмів шифрування *AES*, *DES*, *3DES* та асиметричних систем *RSA*, *ECC* забезпечує багаторівневий захист даних як при зберіганні, так і під час передачі. Особливе значення має використання протоколів *SSL/TLS* для захищеного транспортування інформації, при цьому рекомендовано застосування *TLS* 1.3 відповідно до стандартів *NIST* та вимог *FIPS* 140-3. Перспективною технологією є *confidential computing*, що забезпечує захист даних навіть під час обробки.

Системи управління ідентифікацією та доступом *IAM* з використанням моделей *RBAC* та *ABAC* дозволяють реалізувати гранульований контроль доступу до ресурсів відповідно до стандарту *NIST SP 800-53*. Багаторівнева автентифікація *MFA* з використанням стандартів *FIDO2*/*WebAuthn* замінює вразливі *SMS* методи, значно підвищуючи стійкість до фішингових атак.

Стратегії резервного копіювання з чітко визначеними параметрами *RPO Recovery Point Objective* та *RTO Recovery Time Objective* є критичними для забезпечення безперервності бізнес-процесів. Disaster Recovery плани з використанням інкрементального та диференційного копіювання, а також розгортання резервних копій у розподілених геолокаціях гарантують відновлення даних навіть у випадку масштабних інцидентів.

В Україні спостерігається активна трансформація підходів до хмарної безпеки в умовах гібридної війни. Досвід протидії кіберагресії, задокументований *Google Threat Analysis Group*, та співпраця з *NATO CCDCOE* демонструють адаптацію міжнародних стандартів до специфічних загроз.

Однак відсутність власної комплексної програми сертифікації хмарних провайдерів на рівні *FedRAMP* створює виклики для масового впровадження хмарних технологій у державному секторі.

Застосування принципу *Cloud First* у розвинутих країнах супроводжується потужною нормативною базою та технічною підтримкою, тоді як в Україні процес цифровізації державних послуг вимагає прискореної розробки національних стандартів безпеки з урахуванням вимог *GDPR* та специфічних загроз регіону.

Розглянуті методи та міжнародний досвід свідчать про необхідність комплексного підходу, що поєднує технічні, організаційні та нормативні заходи для забезпечення належного рівня захисту інформації у хмарних середовищах.

РОЗДІЛ 3 РОЗРОБКА МОДЕЛІ ЗАХИСТУ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ ІЗ ЗАСТОСУВАННЯМ ХМАРНИХ ТЕХНОЛОГІЙ

За даними *Asian Development* Bank, урядові структури по всьому світу прискорюють цифровізацію публічних послуг, додають нові цифрові інструменти. Розширюється можливість аналізу даних та розробляються плани розвитку цифрової економіки. Багато з цих змін стають можливими саме завдяки хмарним обчислювальним технологіям [35].

У цьому контексті метою даного розділу є розробка комплексної моделі захисту державних інформаційних ресурсів, адаптованої до специфіки хмарних технологій, що поєднує теоретичні принципи системного підходу з практичними механізмами їх реалізації. Інтегрувати передові технології моніторингу та реагування на кіберзагрози. Також бути придатною для практичного впровадження в умовах обмежених ресурсів та високого рівня загроз, характерного для сучасного кіберпростору. Особливого значення набуває питання балансу між безпекою та доступністю: державні сервіси повинні залишатися відкритими для громадян та бізнесу, водночас надійно захищаючи чутливі дані та критичну інфраструктуру.

Актуальність розробки такої моделі підтверджується світовою практикою. Федеральний уряд США у 2013 році запровадив політику *Cloud First*. Вона зобов'язала державні агентства за замовчуванням розглядати хмарні рішення як пріоритетні та використовувати альтернативи лише за обґрунтованої необхідності. Подальша стратегія *Cloud Smart* у 2019 розвинула цей підхід, пропонуючи практичні настанови щодо безпеки, закупівель та управління персоналом у контексті хмарних середовищ. Європейський Союз не стояв осторонь та почав активно працювати над створенням *Blueprint for Cybersecurity*. *Blueprint for Cybersecurity* є загальноєвропейською архітектурою кіберзахисту, що має забезпечити взаємо сумісність систем безпеки країн-членів, особливо під час кризових ситуацій. Ці ініціативи демонструють усвідомлення того факту, що ефективний захист державних інформаційних

ресурсів у хмарі вимагає не просто технічних рішень, а системної стратегії, що охоплює державні, процеси, технології [36].

3.1. Постановка завдань та принципи системного підходу до захисту державних ресурсів

Державні інформаційні ресурси відіграють критично важливу роль у функціонуванні держави, тому їх захист є пріоритетним завданням національної кібербезпеки. Основними цілями такого захисту є забезпечення конфіденційності, цілісності та доступності інформації, тобто так званої тріади *CIA* [37]. Тобто необхідно не допустити несанкціонованого доступу до чутливих даних, запобігти їх несанкціонованому зміненню чи знищенню та гарантувати своєчасний доступ уповноважених осіб до потрібної інформації. Додатково держава має забезпечити безперервність надання критичних публічних послуг і зберегти довіру громадян, дотримуючись вимог законодавства та міжнародних стандартів у сфері кібербезпеки.

Сучасні кіберзагрози з кожним роком еволюціонують, стають все більш складними та масованими, що створює нові виклики для захисту державних ресурсів [38]. Державні органи стикаються з цілим спектром актуальних загроз: цілеспрямовані атаки *APT*, що спонсоруються ворожими державами, кібершпіонаж і саботаж критичної інфраструктури, масштабні *DDoS*-атаки, операції інформаційного впливу, а також кіберзлочинність. Зростає небезпека ланцюгових атак, коли зловмисники компрометують програмне забезпечення чи хмарні сервіси, якими користуються державні установи. Внутрішні загрози, пов’язані з людським фактором, до яких відносимо навмисні чи випадкові дії співробітників, теж лишаються актуальними.

Усе це означає, що ізольовані заходи безпеки більше не гарантують належного рівня захисту: потрібен системний підхід, здатний проактивно протидіяти сучасним атакам. Логіка системного підходу до кіберзахисту повинна передбачати розгляд усіх

компонентів захищеної системи, як єдиного цілого, де технології, процеси та люди взаємопов'язані і забезпечують один одного. Практика показує, що у багатьох урядових структурах кібербезпека історично будувалася фрагментарно: впроваджувалися окремі засоби захисту або реагування, часто в реактивному режимі, без достатньої координації [38]. Така фрагментація призводить до лазівок між розрізненими рішеннями, якими можуть скористатися зловмисники. Натомість системний підхід покликаний узгодити всі елементи захисту в єдину стратегічно керовану систему. Це означає впровадження єдиної політики безпеки та стандартів для всіх рівнів, створення центральної координації кіберзахисту, а також забезпечення безперервного циклу: від управління ризиками до моніторингу, реагування й вдосконалення заходів безпеки. Важливо, що такий підхід є проактивним: він спирається на оцінку ризиків і прогнозування загроз, а не лише на реагування після факту інциденту.

Щоб реалізувати наведені ідеї на практиці, в захисті державних інформаційних ресурсів застосовуються такі ключові принципи:

1. Комплексність, яка включає в собі всі аспекти інформаційної безпеки. Технічні, що містять мережевий захист, шифрування, резервування даних, організаційні аспекти, до яких відносяться політики доступу, навчання персоналу. Захист має здійснюватися на всіх етапах життєвого циклу інформаційних систем виявлення, реагування, відновлення. Такий комплексний підхід гарантує, що жодна вразливість не залишиться поза увагою. Як зазначає *NIST*, державні установи повинні впроваджувати збалансований набір заходів безпеки. До них відносяться управлінські, операційні і технічні для того щоб покрити весь простір загроз, адже технологій самих по собі недостатньо.

2. Багаторівневість, яку можливо реалізувати за рахунок побудови багатошарової системи оборони, коли безпека забезпечується *на декількох рівнях*. Реалізується це шляхом розгортання кількох незалежних рубежів захисту, наприклад: мережева екранування та *IDS* з *IPS* на периметрі, шифрування і контроль доступу на рівні даних, засоби захисту кінцевих точок.

3. Інтегрованість, відповідає за те, щоб всі компоненти кіберзахисту повинні бути взаємопов’язані та узгоджені між собою в рамках єдиної системи. Це означає, що різні засоби безпеки мають обмінюватися інформацією і працювати скоординовано, а не ізольовано. Наприклад, система моніторингу подій може збирати логи з мережевого обладнання, серверів, хмарних сервісів та робочих станцій, щоб корелювати події і виявляти складні атаки, невидимі при розрізненому аналізі. Центральний операційний центр безпеки, оснащений такими інструментами, буде забезпечувати єдину картину ситуації та швидку реакцію на інциденти. Інтеграція також означає дотримання єдиних стандартів і протоколів. Наприклад, використання централізованих служб каталогів для управління обліковими записами, єдиних систем керування конфігураціями, платформи обміну кіберрозвідкою. Також в США було реалізовано єдиний центр кібербезпеки на базі IBM *QRadar SIEM* для більш ніж 70 державних агентств: усі вони передають події безпеки у спільну систему моніторингу, що аналізує тисячі логів у реальному часі [39]. Це дозволило створити уніфіковану картину загроз і централізовано керувати захистом різних установ. Таким чином, інтеграція забезпечує синергію засобів безпеки та усуває «розриви» між ними.

4. Ризик-орієнтованість базується на постійному управлінні ризиками: ресурси та зусилля розподіляються відповідно до актуальних загроз і вразливостей. Необхідно ідентифікувати критичні активи та сценарії атак, що їм загрожують, і сконцентрувати захист саме там. Такий підхід гарантує ефективне використання ресурсів: насамперед вирішуються найбільш небезпечні проблеми, що загрожують державним функціям, а менш критичні ризики контролюються належним чином і не ігноруються. Ризик-орієнтована стратегія також вимагає постійного перегляду: у міру появи нових загроз або змін у *IT*-ландшафті державних органів. Оцінка ризиків мусить актуалізуватися, а плани захисту адаптуватися.

В рамках концепції *defense in depth SIEM* здійснює моніторинг на всіх рівнях. Починаючи від внутрішньої мережі та серверів до кінцевих точок і

хмарних сервісів тісно взаємодіючи з іншими засобами безпеки, такими як міжмережеві екрани, *EDR*, *XDR* для виявлення та реагування на підозрілу активність.

IBM QRadar SIEM централізує журнали безпеки з усієї IT-інфраструктури та надає засоби аналітики для виявлення загроз у режимі реального часу. *QRadar* збирає, обробляє, агрегує й зберігає мережеві дані та журнали подій, забезпечуючи повну видимість ситуації і генеруючи сповіщення про підозрілі дії. На відміну від традиційного підходу, коли адміністратори окремо переглядають журнали різних систем і реагують постфактум, впровадження SIEM дозволяє автоматизувати кореляцію подій та аналізувати їх у єдиному центрі.

QRadar консолідує логи з мережевих пристроїв, серверів, додатків, кінцевих точок, хмарних сервісів тощо, нормалізує дані та застосовує правила кореляції. Також присутнє використання штучного інтелекту для виявлення складних атак, які неможливо помітити при розрізненому моніторингу. В результаті система відфільтровує шум і подає операторам тільки узгоджені групи подій, що вказують на конкретні інциденти безпеки [40]. Це значно знижує навантаження на аналітиків та прискорює їх реакцію. *SIEM*-рішення на кшталт *QRadar* також надають інструменти для пріоритезації ризиків: наприклад, модуль *QRadar Risk Manager* збирає дані про конфігурації мережі і моделює потенційні вразливості, а *QRadar Vulnerability Manager* інтегрує результати сканування вразливостей. Таким чином, корелюючи загрози з інформацією про найбільш критичні слабкі місця інфраструктури [40]. Додатково *SIEM* підтримує виконання вимог відповідності шляхом централізованого зберігання логів та генерування необхідних звітів, що є важливою складовою системного підходу у державному секторі.

3.2. Модель захисту державних інформаційних ресурсів у хмарному середовищі

Архітектура системи захисту в хмарному середовищі: Нижче наведена схема, яка відображає повну архітектуру рішення для захисту державних інформаційних ресурсів у хмарному середовищі. На ній показано всі ключові компоненти та їх взаємодію – від збору журналів подій на локальних хостах до кореляції інцидентів у хмарній *SIEM* та реагування командою *SOC* за наперед визначеним планом.

Схема архітектури системи захисту державних інформаційних ресурсів у хмарному середовищі. Локальні *Windows*-хости з *Sysmon* генерують журнали подій, які збираються агентом *WinCollect* та передаються в хмарну *SIEM*-платформу *IBM QRadar* для аналізу і кореляції. Паралельно агент *CrowdStrike Falcon EDR* відправляє телеметрію з хостів до власної хмарної платформи. Операційний центр безпеки моніторить корельовані сповіщення в *QRadar та алерти EDR* і, в разі інциденту, діє за наперед підготовленим *playbook* та *runbook* для реагування.

Основні етапи роботи системи та логіка взаємодії компонентів:

1. Моніторинг на хостах: На кожному локальному *Windows*-хості встановлено *Sysmon*. *Sysmon* є службовою програмою, що здійснює детальний моніторинг системних подій. Наприклад створення процесів, мережеві з’єднання з логуванням їх у журнали *Windows*. Це забезпечує глибокий рівень логування, який буде корисний при розслідуваннях та аналізах безпеки.

2. Збирання журналів подій: Спеціалізований *агент WinCollect* запущений на хості або на виділеному сервері збирає журнали подій, згенеровані *Sysmon* та іншими системними компонентами. Він передає ці події у *IBM QRadar*, що розгорнутий у хмарі, для централізованого збору логів. *WinCollect* діє як транспортний агент, який забезпечує надійну доставку даних безпеки з локального середовища до хмарної *SIEM*.

3. Телеметрія *EDR* з кінцевих точок: Одночасно на кожному хості працює агент *CrowdStrike Falcon* є *EDR*-платформою, що дозволяє відстежувати підозрілу активність на кінцевій точці. Наприклад, спроби виконання експлойтів, виконання неперевіреного коду, ознаки виконання кібератак, тактик, технік та вторгнень згідно *MITRE ATT&CK*. Відправляє телеметрію та виявлені індикатори компрометації до хмарної платформи *CrowdStrike*. Таким чином, хмарна платформа *EDR* постійно отримує оновлені дані про стан кожного хоста (Рис. 3.2).

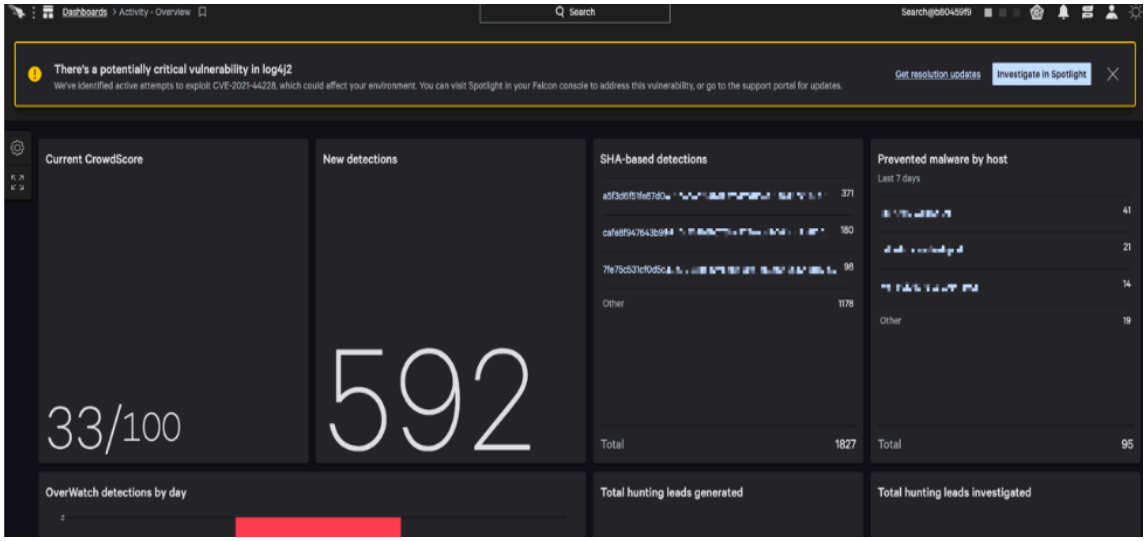


Рис. 3.1. Дашборд телеметрії та виявлень *EDR* у *CrowdStrike Falcon*

4. Кореляція в *SIEM IBM QRadar*: Хмарна *SIEM IBM QRadar* приймає потоки даних подій від *WinCollect*, а також, за наявності інтеграції, може отримувати сповіщення від *CrowdStrike Falcon*. *QRadar* нормалізує отримані журнали і пропускає їх через рушій правил кореляції. На основі правил та моделей поведінки відбувається аналіз: зіставляються події з різних джерел і виявляються ознаки інцидентів. У разі спрацювання кореляційних правил система генерує сповіщення, які вказують на підозрілу активніть (Рис. 3.2).

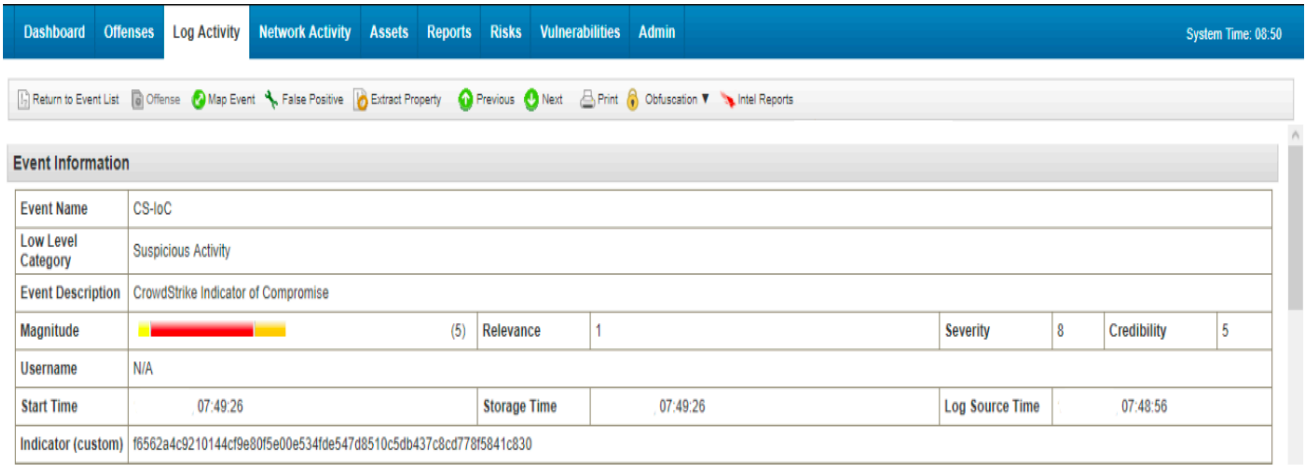


Рис.3.2. Приклад спрацювання кореляційного правила в *IBM QRadar*, отриманого від *CrowdStrike Falcon*, у *QRadar SIEM*

5. Моніторинг та аналіз інцидентів у *SOC*: команда аналітиків, яка цілодобово моніторить панелі інцидентів. Фахівці *SOC* отримують корельовані сповіщення від *QRadar* та події на хостах через *CrowdStrike Falcon*. Аналізуючи ці дані, *SOC* верифікує інциденти, визначає їх пріоритет і масштаб впливу.

6. Запуск процедури реагування використовуючи *Playbook* та *Runbook*. Коли інцидент підтверджено, команда *SOC* діє згідно з наперед визначеним планом реагування – *playbook* та *runbook*. Playbook є деталізованим планом вирішення процесів згідно стратегії команди. *Playbook* чітко регламентує дії для конкретного типу загрози, забезпечуючи скоординоване реагування та мінімізацію шкоди [41]. Runbook є деталізованою покроковою інструкцією для вирішення певної задачі де зазвичай залучається лише один учасник.

7. Реагування та нейтралізація загрози: Відповідно до процедур реагування *SOC* за допомогою доступних засобів здійснює необхідні дії для усунення загрози. Зокрема, команда може використати можливості платформи *CrowdStrike Falcon EDR* для швидкого втручання на кінцевих точках – наприклад, ізолювати скомпрометований хост від мережі зупинити або видалити шкідливі процеси і файли на ньому (Рис.3.3)[42].

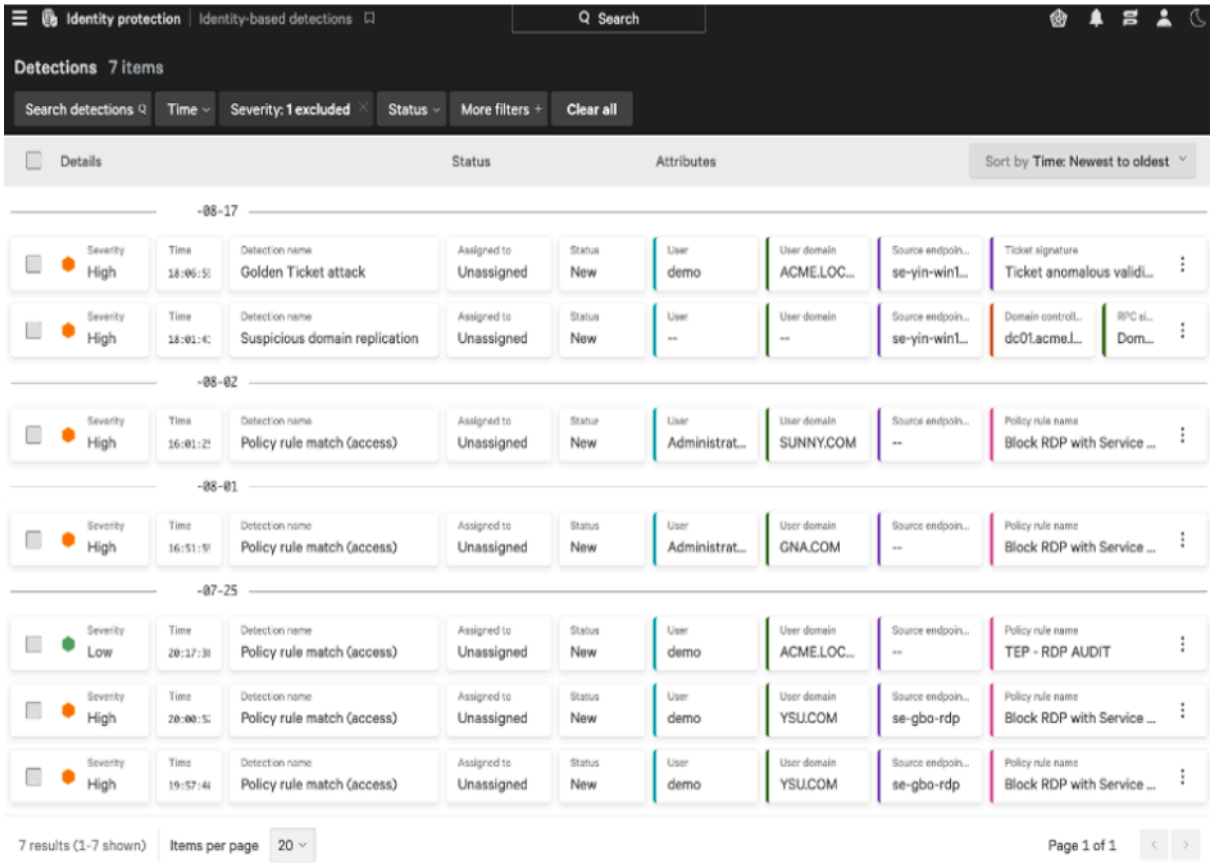


Рис.3.3. Перелік виявлених інцидентів безпеки у *CrowdStrike Falcon*

Завдяки цьому здійснюється оперативне стримування атаки: заражений вузол ізольований від решти системи, що запобігає подальшому поширенню загрози, водночас зберігаючи можливість керувати хостом через хмарну консоль *EDR*. Після локалізації *SOC* переходить до етапів ліквідації наслідків та відновлення системи до штатного режиму роботи.

8. Безперервне вдосконалення захисту: Завершальний етап команда *SOC* проводить аналіз інциденту *post-mortem*, щоб зробити висновки та оновити політики безпеки, правила кореляції й *playbook* у майбутньому. Такий зворотний зв’язок забезпечує підвищення ефективності системи захисту: накопичений досвід використовується для проактивного вдосконалення заходів безпеки в хмарному середовищі.

3.3. Розробка рекомендацій щодо впровадження методів захисту на практиці

Досвід воєнного часу показав ефективність такого підходу: перенесення критичних державних реєстрів у хмару зберегло безперервність сервісів навіть під ударами ракет. В рамках цієї стратегії рекомендується використати хмарну версію *SIEM*-системи *IBM QRadar on Cloud* як центральну платформу моніторингу. Хмарна модель *QRadar* скорочує капітальні витрати: відсутня потреба у власних серверах, а оплата здійснюється як підписка [43].

QRadar збирає журнали подій із різних джерел і здійснює кореляційний аналіз, виявляючи складні атаки. Комерційне рішення *QRadar* потребує ліцензування, проте його вибір обґрунтований: на відміну від безкоштовних *SIEM*, які хоч і привабливі для обмежених бюджетів. Вимагають значних зусиль на підтримку, *QRadar* надає готові засоби аналітики та інтеграцію зі світовими джерелами кіберрозвідки [44]. Зокрема, система групує пов’язані події в інциденти. Що зменшує кількість хибних сповіщень і навантаження на операторів.

Для забезпечення багаторівневого захисту кінцевих точок рекомендується впровадити *EDR*-рішення корпоративного класу, зокрема *CrowdStrike Falcon*. Це хмарний *EDR*, що встановлюється у вигляді агента на робочі станції та сервери і відстежує підозрілу активність у режимі реального часу. *CrowdStrike* вирізняється високою ефективністю виявлення сучасних загроз і надає можливості проактивного моніторингу 24/7 за рахунок керованого сервісу *Falcon Complete*. Крім того він є мультиплатформеним і підтримує *Linux*, *Windows*, *macOS*. Та підримує інтерграцію з хмарними середовищами для захисту хмарних віртуальних машин, контейнерів і сервісів [45].

Альтернативою для установ з обмеженим бюджетом може бути опора на вбудовані засоби захисту *Windows*, такі як *Microsoft Defender for Endpoint*. *Defender* інтегрований в екосистему *Microsoft 365* та *Azure* і не потребує додаткових ліцензійних витрат [45]. Його можливості будуть поступаютися *CrowdStrike* однак він забезпечує базовий рівень *EDR*-функцій і тісно

пов’язаний з іншими службами Microsoft. Практичний підхід може бути поетапним: на першому етапі задіяти *Defender*, паралельно підвищуючи кібергігієну, а з ростом ризиків та можливостей бюджету перейти на *CrowdStrike*. Слід зазначити, що вартість комерційного *EDR* є суттєвою: ліцензія *Falcon* оцінюється близько $8–15 за пристрій на місяць [45]. Таким чином, якщо безпека є пріоритетом і фінансово можлива, використання CrowdStrike надасть розширені можливості включно з експертною підтримкою і розслідуваннями. Але за умов жорсткої економії прийнятним мінімумом може бути *Defender* за умови впровадження належних політик та контролю.

Не менш важливим технічним компонентом моделі є система збору та централізованого аналізу логів з кінцевих хостів**.** Рекомендується розгорнути на всіх *Windows*-системах утиліту *Sysmon.* Ця утиліта дозволяє реєструвати детальні події в системі, такі як: створення процесів, зміни у реєстрі, мережеві з’єднання тощо. У поєднанні з агентом *IBM WinCollect* це дозволить автоматично збирати журнали *Sysmon* і передавати їх до *SIEM* для кореляції. Така зв’язка фактично створює безкоштовний аналог базового моніторингу кінцевих точок: аналітики в *SOC* отримують багату телеметрію з кожного хоста без встановлення дорогого клієнтського ПЗ. Інструменти *Sysmon* і *WinCollect* вже застосовувалися у навчально-практичних проєктах – зокрема, під час інсталяції *QRadar* на базі кафедри в університеті було успішно налаштовано збір логів *Windows* через *WinCollect* з використанням *Sysmon* як джерела даних. Налаштування зводиться до встановлення *Sysmon* на хості та додавання на сервері *QRadar* нового джерела логів *WinCollect* із потрібним *XPath*-запитом. *XPath*-запит містить шлях до журналу *Microsoft-Windows-Sysmon/Operational* [46]. Альтернативою може слугувати рідний механізм *Windows Event Forwarding*, що пересилає стандартні журнали Windows на сервер збору. Проте стандартні логи *Windows* обмежені за глибиною інформації. Без *Sysmon* багато атак можуть залишитися невидимими. У таблиці 3.1 наведено порівняння запропонованих засобів захисту з можливими альтернативами за ключовими характеристиками.

Таблиця 3.1

Порівняльна характеристика засобів кібербезпеки для державних установ

Категорія	**Рішення**	**Переваги**	**Недоліки**
SIEM	*IBM QRadar*	– Хмарна модель розгортання підвищує доступність і масштабованість; – Наявність підтримки від вендора 24/7; – Можливість генерації звітів для відповідності стандартам.	– Висока вартість ліцензії, що залежить від обсягу даних; – Вимагає кваліфікованих спеціалістів для тонкого налаштування; – Оптимальна ефективність досягається при інтеграції з іншими продуктами *IBM*.
SIEM	*Open-Source SIEM*: *Elastic Stack, Wazuh.*	– Нульова вартість ліцензій; – Гнучке налаштування під потреби організації.	– Менше готових аналітичних правил і попередньо налаштованих модулів, ніж у комерційних продуктів; – Відсутня офіційна підтримка .
EDR	*CrowdStrike Falcon*	– Висока ефективність виявлення складних загроз; Наявність модуля *CrowdStrike Falcon Next-Gen SIEM*, яка може замінити класичні *SIEM*; – Хмарна архітектура: централізоване керування, мінімальний вплив на продуктивність хостів;	– Висока вартість: ліцензія починаючи від $60 на рік за один пристрій; – Дані телеметрії з хостів передаються на зовнішні сервери.
EDR	*Microsoft Defender*	– Відсутня додаткова плата за продукт Тісна інтеграція з екосистемою *Microsoft*, єдиний центр керування через *Defender for Endpoint* портал; – Постійно вдосконалюється Microsoft: оновлення сигнатур, додавання функцій на основі хмарного аналізу загроз.	– Поступається найкращим комерційним *EDR* за глибиною аналізу та швидкістю реакції: немає розширених можливостей *AI*-аналізу поведінки, обмежений функціонал без ліцензій E5; – Не пропонує повноцінного 24/7 моніторингу: реагування покладається на внутрішню IT-команду; – Оптимальна робота потребує тонкого налаштування політик: контроль пристроїв, правил реагування; – Менш придатний для гетерогенних середовищ: підтримка *Linux*/*macOS* реалізована лише у платній версії *Defender for Endpoint*.

Продовження таблиці 3.1

Категорія	Рішення	Переваги	Недоліки
Журнали та моніторинг	*Sysmon* та *WinCollect*	– Детальна видимість подій на хостах: процеси, мережа, зміни системних налаштувань. Що покращує результати аналізу інцидентів; Безкоштовність: *Sysmon* розповсюджується вільно, агент *WinCollect* надається *IBM* безкоштовно для клієнтів *QRadar*.	– Вимагає розгортання і підтримки на кожному хості; – Створює значний потік даних, що потребує фільтрації; – Потребує наявності *SIEM* для повноцінного використання.
Журнали та моніторинг	Вбудований *Windows Event Forwarding*	– Стандартний засіб Windows: не потребує встановлення агентів, налаштовується через групові політики; – Мінімальний вплив на систему і мережу завдяки використанню вбудованої в Windows підсистеми логів; – Може передавати події у форматі, сумісному з багатьма *SIEM*.	– Охоплює лише події, що записуються штатними журналами Windows; – Обмежені можливості фільтрації на стороні клієнта можуть призводити до передачі великого обсягу даних, значна частина яких не несуть корисної інформації; – Відсутній механізм надійної буферизації: у разі збою з'єднання частина подій може бути втрачена.

Ефективність технічних засобів значною мірою залежить від правильного регламентування процесів та політик. Тому наступним кроком є впровадження комплексних організаційних заходів кібербезпеки**.** Кожна установа повинна розробити та затвердити внутрішні політики безпеки:

- політику інформаційної безпеки;
- політику реагування на інциденти;
- політику керування обліковими записами;
- політику використання хмарних сервісів.

Ці документи встановлюють правила і відповідальність, забезпечують єдиний підхід до захисту на всіх рівнях [47]. Зокрема, політика реагування на інциденти є критичною бо вона має визначати, що вважається інцидентом, хто і як повинен діяти у разі його виявлення, порядок ескалації та повідомлення керівництва. Наявність такої офіційної політики підвищує готовність

організації до кризових ситуацій і надає командам впевненість у своїх повноваженнях під час реагування.

Далі на основі політики слід розробити детальний план реагування на інциденти та набір конкретних *playbook* для різних типів інцидентів [48]. Він має охоплювати всі фази циклу реагування: підготовка, виявлення та аналіз, стримування, ліквідація, відновлення [49].

Наступна рекомендацією є створення функції моніторингу та реагування**.** В організації має діяти власний операційний центр безпеки або принаймні виділена група реагування на інциденти [51]. З огляду на брак ресурсів у багатьох установ, доцільно розглянути централізовану модель *SOC* на міжвідомчому рівні [50]. Подібний підхід було реалізовано, наприклад, у США: для більш ніж 70 державних агенцій штату побудовано єдиний *SOC* на базі *IBM QRadar*.

Якщо ж централізація з якихось причин неможлива, тоді необхідно визначити в штаті установи відповідальну групу або посадову особу за інформаційну безпеку [52]. Ця група повинна здійснювати моніторинг подій, реагувати на інциденти згідно з планом та підтримувати актуальність налаштувань безпеки. Організаційно варто закріпити процес управління вразливостями до якого будуть входити регулярне сканування та усунення знайдених слабких місць і управління змінами в IT [52]. Для того щоб нові системи або оновлення проходили перевірку на безпеку перед впровадженням.

3.4 Апробація моделі на умовному або реальному кейсі

Для підтвердження практичної реалізовності запропонованих рішень необхідно продемонструвати, що ключові елементи моделі можуть бути відтворені в реальних умовах, забезпечуючи збір, кореляцію та аналіз подій безпеки з різних джерел, а також підтримку процесів реагування на інциденти [53].

В якості експериментального середовища використано інфраструктуру кафедри, де розгорнуто віртуалізовану інсталяцію *IBM QRadar Community Edition* у середовищі *VirtualBox*, що логічно відповідає сценарію використання хмарної *SIEM* у державній установі [54]. На окремих робочих станціях під керуванням *Windows* було налаштовано генерацію детальних системних журналів за допомогою утиліти *Sysmon*, їх передачу до *QRadar* через агент *WinCollect*. *WinCollect*, необхідний для виконання ролі *syslog-forwarder* для надсилання подій Windows у *QRadar* з підтримкою фільтрації та обмеження потоку подій. Додатково для підвищення контекстності аналізу передбачено інтеграцію з CrowdStrike Falcon для отримання і нормалізації даних у форматах, сумісних із SIEM та використання *Threat Intel*/*IoC* для збагачення подій і подальшої їх кореляції (Рис.3.1). Така конфігурація дозволяє відтворити повний ланцюг руху даних безпеки: від кінцевої точки й зовнішнього хмарного сервісу до центральної платформи моніторингу [55].

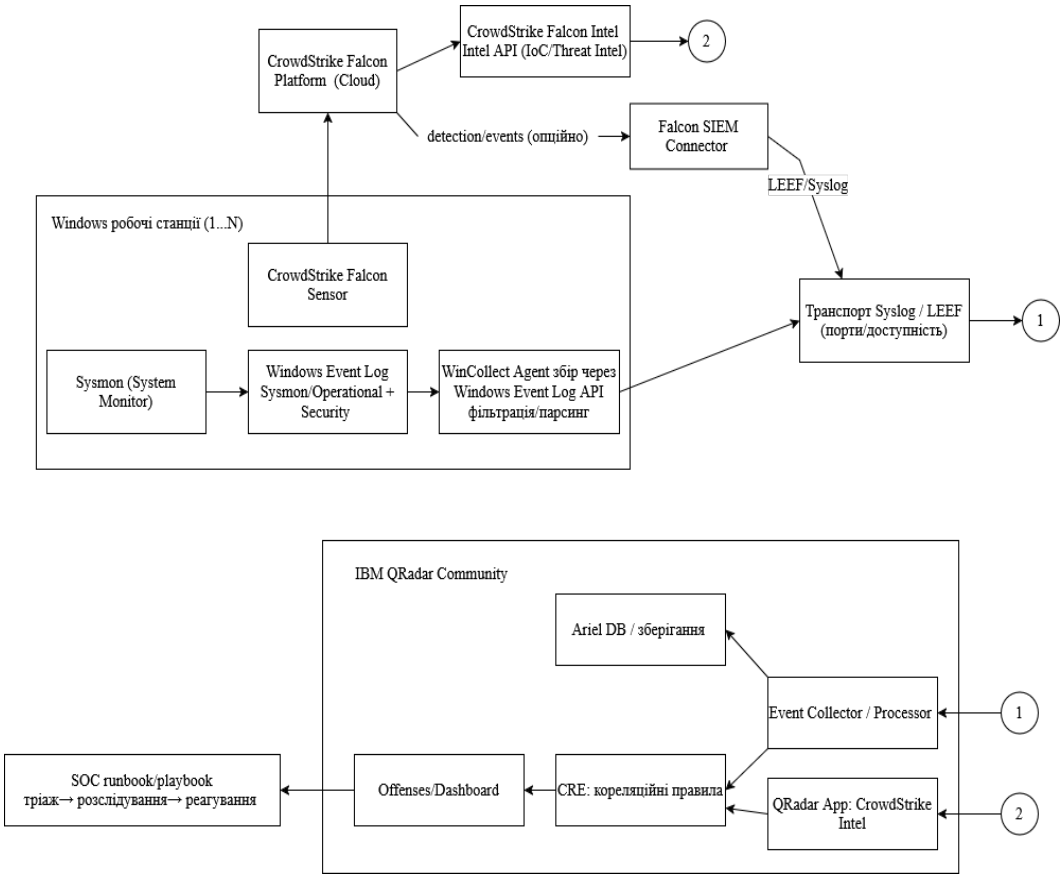


Рис. 3.4. Блок-схема інтеграції телеметрії *Sysmon*/*Windows*

Метою апробації є якісна оцінка працездатності моделі за такими критеріями: коректність інсталяції та базового налаштування *SIEM*-системи; можливість приймання та нормалізації мережевих потоків і журналів подій з операційних систем; здатність системи до інтеграції з зовнішнім джерелом загрозової аналітики *CrowdStrike* та відображення отриманих індикаторів компрометації в консолі *QRadar*; наявність умов для подальшої кореляції подій і підтримки роботи операційного центру безпеки [56]. Отримані результати розглядаються як доказ того, що запропонована модель може бути масштабована й адаптована для використання у виробничих середовищах органів державної влади за умови відповідного ліцензування та розгортання.

У подальшому викладі послідовно наведено: етапи інсталяції та початкового налаштування *IBM QRadar* у віртуальному середовищі; конфігурацію джерел мережевого трафіку *Flow Sources*; організацію збору журналів Windows за допомогою *WinCollect* і *Sysmon*; а також процес підключення до *Qradar* модуля *CrowdStrike Falcon Intel* для отримання *IoC* [57-58]. Це дозволяє простежити, яким чином теоретична модель, розроблена у попередніх підрозділах, реалізується у вигляді конкретного технічного рішення.

Спочатку інсталюємо *Qradar* на *VirtualBox*. Для цього у *VMware* режими мережевого адаптера *Bridged*. Режим *Bridged* дозволяє віртуальній машині безпосередньо отримувати доступ до фізичної мережі, як якщо б вона була окремою фізичною машиною, отримуючи власну *IP*-адресу і поводячись як незалежний пристрій у мережі [59].

Режим *Promiscuous Mode*: *Allow All* дозволяє інтерфейсу захоплювати і обробляти всі мережеві пакети, а не тільки ті, що адресовані йому (Рис.3.5).

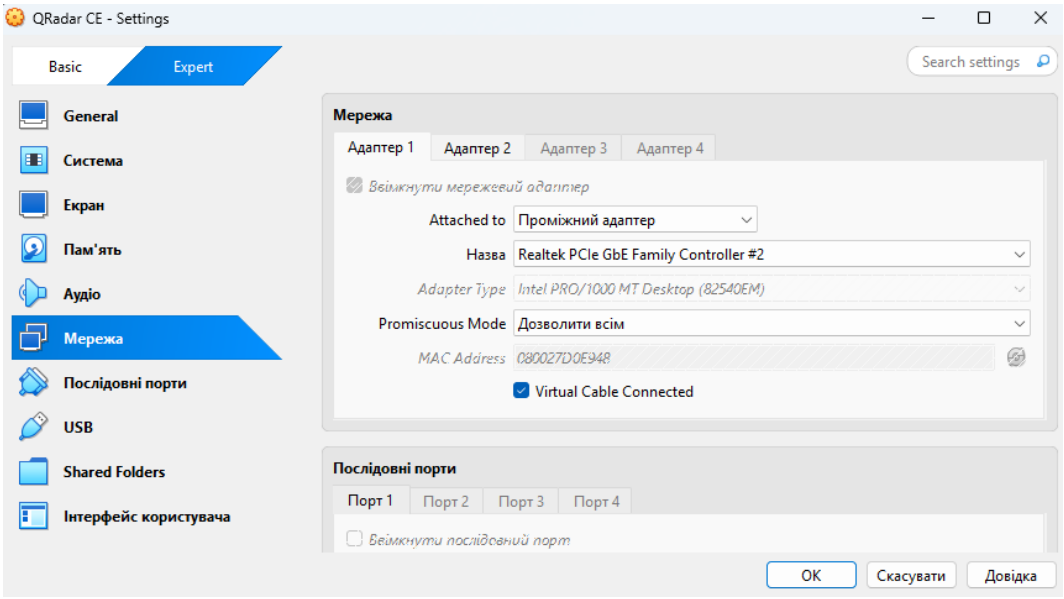


Рис.3.5. Налаштування мережевого адаптеру

В вікні інсталяції обираємо конфігурацію *Qradar*: *All-In-One* (Рис.3.6).

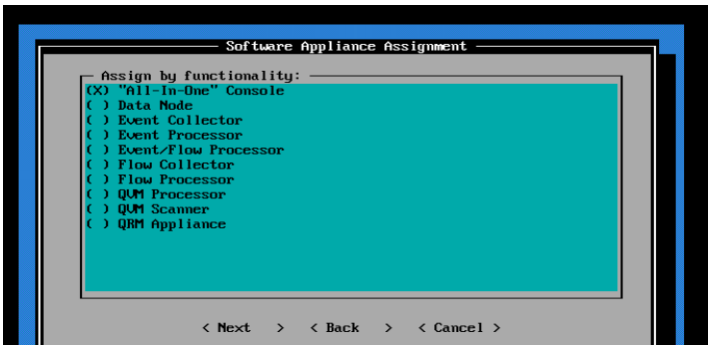


Рис.3.6. Меню вибору ролі вузла *QRadar*

Після інсталяції з'являється запит на введення імені користувача (Рис.3.7). Ім'я користувача за замовчуванням: *root*.

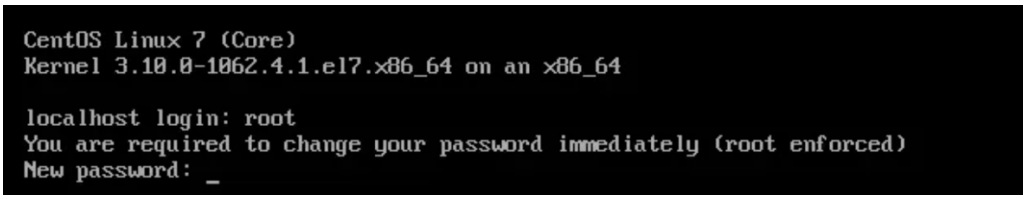


Рис. 3.7. Введіть ім'я користувача та пароль

У консолі вводимо новий пароль та запускаємо команду «./*setup*», де погоджуємось з ліцензійною угодою. Натисніть «q», щоб швидко перейти, а потім «*Y*» для підтвердження початку встановлення (Рис. 3.8).

```
Found /tmp/.accepted_qradar_eula - answer yes to accept eula
About to install QRadar Community Edition 7.3.3 (Build 20191031163225)
Do you wish to continue (Y/[N])? Y_
```

Рис. 3.8. Процес інсталяції ./setup

Відкриваємо браузер і вводимо «*https://qradarIP/console*», де замість *qradarIP* має бути *IP* адреса консолі *QRadar*. Потрапивши на сторінку входу в *QRadar*, вводимо облікові дані (3.9).

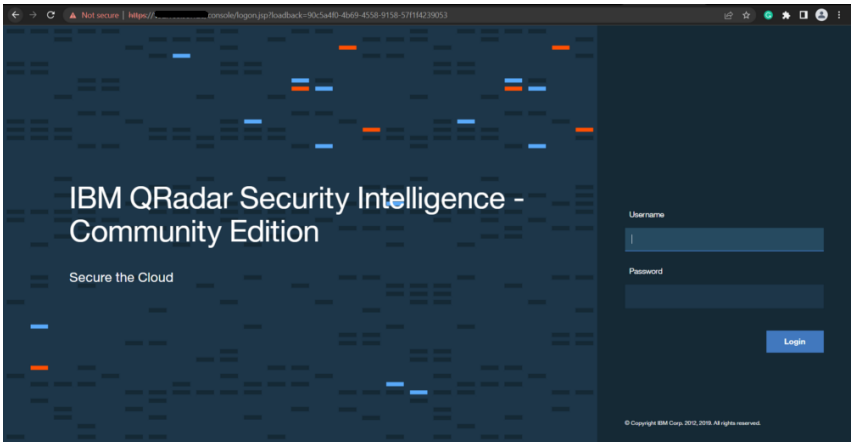


Рис. 3.9. Сторінка входу в *Qradar*

Далі налаштовуємо *Flow Sources* у вкладці *Admin* (3.10)

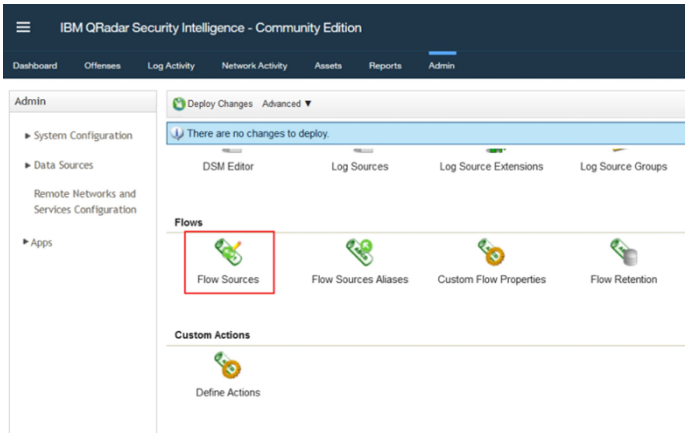


Рис. 3.10. *IBM QRadar*: вкладка *Admin*

Встановлюємо ім'я джерела потоку як *qradar_network*, тип джерела потоку як «*Network Interface*» та зберігаємо конфігурацію (Рис.3.11).

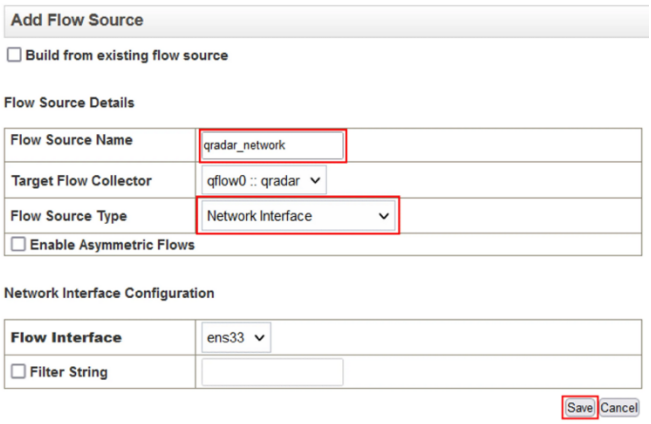


Рис. 3.11. Додавання *Flow Source*

Потім в вкладці *Admin* натискаємо *Deploy Changes* (Рис. 3.12).

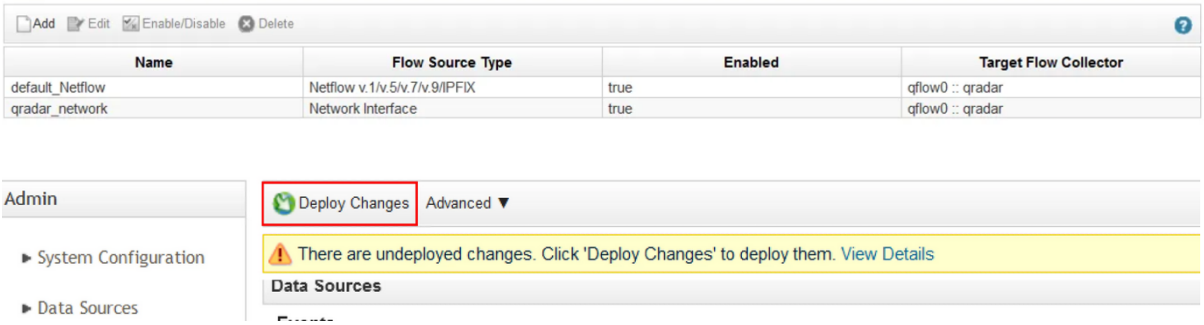
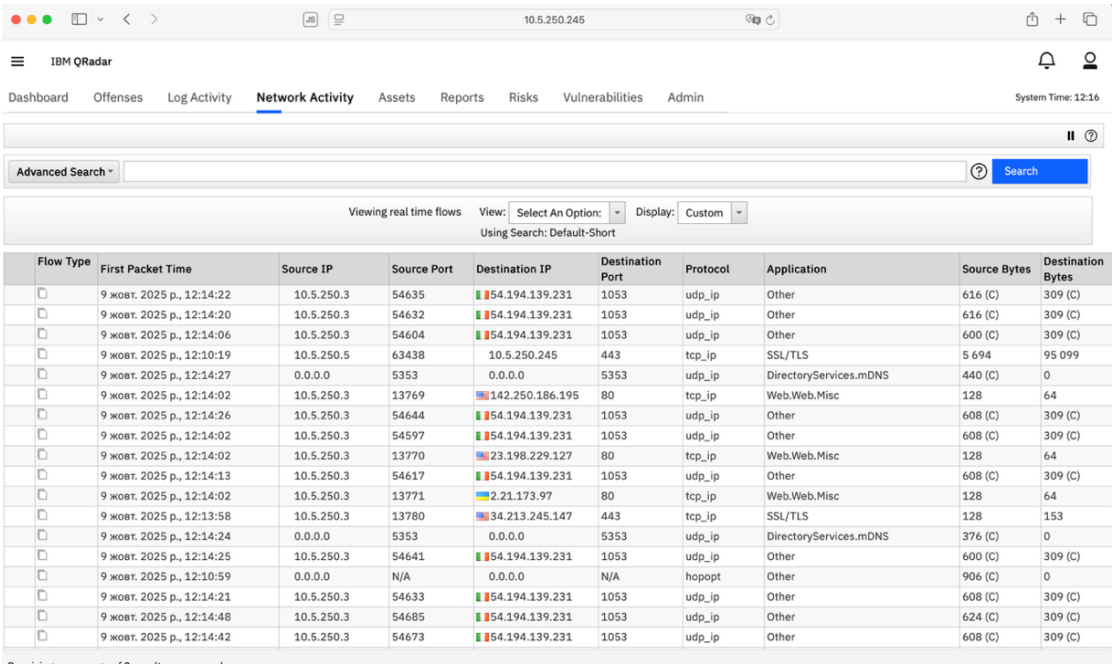


Рис. 3.12. Застосування змін конфігурації джерел потоку в консолі *IBM Qradar*

Після створення джерела мережевого потоку *qradar_network* та застосування змін конфігурації необхідно переконатися, що система коректно отримує та обробляє мережеві дані. Для цього в *IBM QRadar* використовується вкладка *Network Activity* (Рис.3.13).



Flow Type	First Packet Time	Source IP	Source Port	Destination IP	Destination Port	Protocol	Application	Source Bytes	Destination Bytes
	9 жовт. 2025 р., 12:14:22	10.5.250.3	54635	54.194.139.231	1053	udp_ip	Other	616 (C)	309 (C)
	9 жовт. 2025 р., 12:14:20	10.5.250.3	54632	54.194.139.231	1053	udp_ip	Other	616 (C)	309 (C)
	9 жовт. 2025 р., 12:14:06	10.5.250.3	54604	54.194.139.231	1053	udp_ip	Other	600 (C)	309 (C)
	9 жовт. 2025 р., 12:10:19	10.5.250.5	63438	10.5.250.245	443	tcp_ip	SSL/TLS	5 694	95 099
	9 жовт. 2025 р., 12:14:27	0.0.0.0	5353	0.0.0.0	5353	udp_ip	DirectoryServices.mDNS	440 (C)	0
	9 жовт. 2025 р., 12:14:02	10.5.250.3	13769	142.250.186.195	80	tcp_ip	Web.Web.Misc	128	64
	9 жовт. 2025 р., 12:14:26	10.5.250.3	54644	54.194.139.231	1053	udp_ip	Other	608 (C)	309 (C)
	9 жовт. 2025 р., 12:14:02	10.5.250.3	54597	54.194.139.231	1053	udp_ip	Other	608 (C)	309 (C)
	9 жовт. 2025 р., 12:14:02	10.5.250.3	13770	23.198.229.127	80	tcp_ip	Web.Web.Misc	128	64
	9 жовт. 2025 р., 12:14:13	10.5.250.3	54617	54.194.139.231	1053	udp_ip	Other	608 (C)	309 (C)
	9 жовт. 2025 р., 12:14:02	10.5.250.3	13771	2.21.173.97	80	tcp_ip	Web.Web.Misc	128	64
	9 жовт. 2025 р., 12:13:58	10.5.250.3	13780	34.213.245.147	443	tcp_ip	SSL/TLS	128	153
	9 жовт. 2025 р., 12:14:24	0.0.0.0	5353	0.0.0.0	5353	udp_ip	DirectoryServices.mDNS	376 (C)	0
	9 жовт. 2025 р., 12:14:25	10.5.250.3	54641	54.194.139.231	1053	udp_ip	Other	600 (C)	309 (C)
	9 жовт. 2025 р., 12:10:59	0.0.0.0	N/A	0.0.0.0	N/A	hopopt	Other	906 (C)	0
	9 жовт. 2025 р., 12:14:21	10.5.250.3	54633	54.194.139.231	1053	udp_ip	Other	608 (C)	309 (C)
	9 жовт. 2025 р., 12:14:48	10.5.250.3	54685	54.194.139.231	1053	udp_ip	Other	624 (C)	309 (C)
	9 жовт. 2025 р., 12:14:42	10.5.250.3	54673	54.194.139.231	1053	udp_ip	Other	608 (C)	309 (C)

Рис.3.13. Вкладка *Network Activity*

Для подальшого тестування роботи моделі важливо перевірити, чи може система отримувати журнали подій із *Windows*-станцій, адже саме вони містять багато ключової інформації про дії користувачів та можливі загрози. У *QRadar* це реалізується за допомогою агента *WinCollect*, який збирає та передає події до *SIEM*. Його налаштування дозволяє перевірити, як модель працює на практиці та чи забезпечує вона необхідний рівень збору даних для подальшого аналізу.

Завантажуємо *wincollect* з офіційного сайту та запускаємо інсталятор де необхідно ввести *IP*-адресу *QRadar*, куди потрібно пересилати події (3.14).

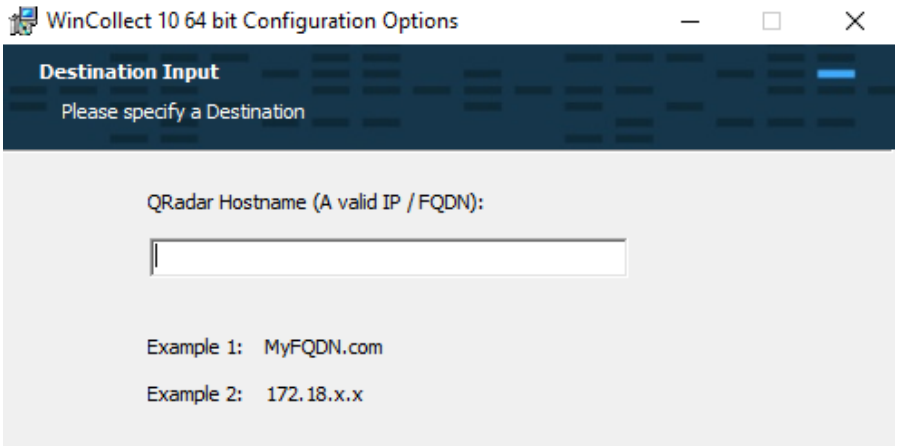


Рис. 3.14. Налаштування підключення *WinCollect* до сервера *QRadar*

Після завершення встановлення відкриваємо *IBM Wincollect*. Де перевіряємо, чи *Wincollect* встановлює з'єднання з *QRadar* перейшовши в *Agent Setting* та натиснувши *Test Setting* (Рис. 3.15).

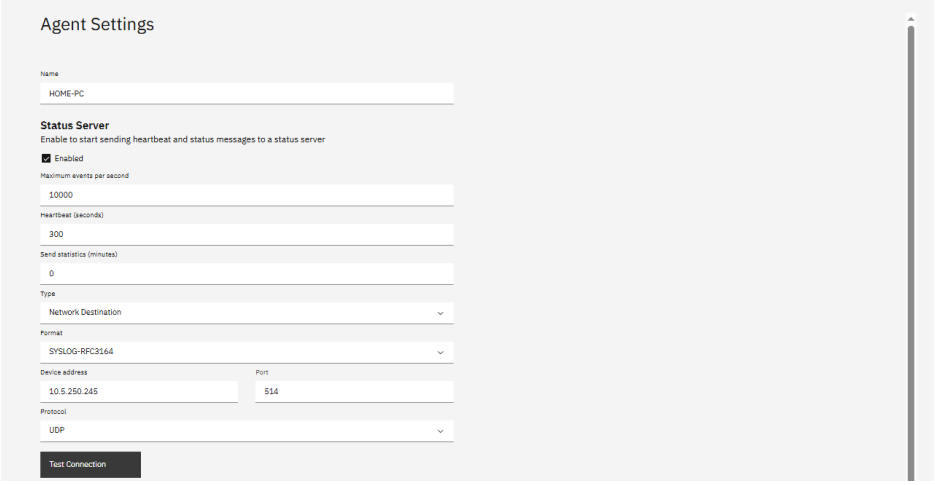


Рис. 3.15. Налаштування *Wincollect Agent*

Тепер додаємо службу *Sysmon* відкриваємо командний рядок як адміністратор та вводимо: *sysmon64.exe –accepteula –i* c:\windows\config.xml. Шлях у кінці команди, це місце де завантажений файл *config.xml*.

Для перевірки чи *Window* надсилає журнали, знаходимо запис sysmon у консолі *IBM Wincollect* на вкладці *Log Viewer* (Рис.3.16).

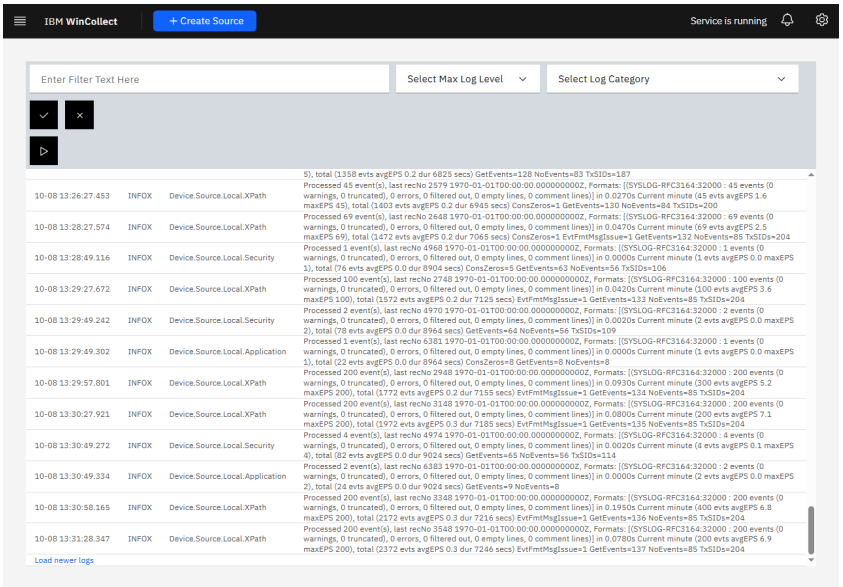


Рис. 3.16. *IBM Wincollect*: *Log Viewer*

Після встановлення агента та надсилання подій у систему необхідно перевірити, чи *QRadar* коректно розпізнає та відображає нові джерела журналів. Для цього у консолі *QRadar* перейдіть до розділу *Admin* і відкрийте меню *Log Sources*, де відображається перелік усіх підключених джерел подій (3.17).

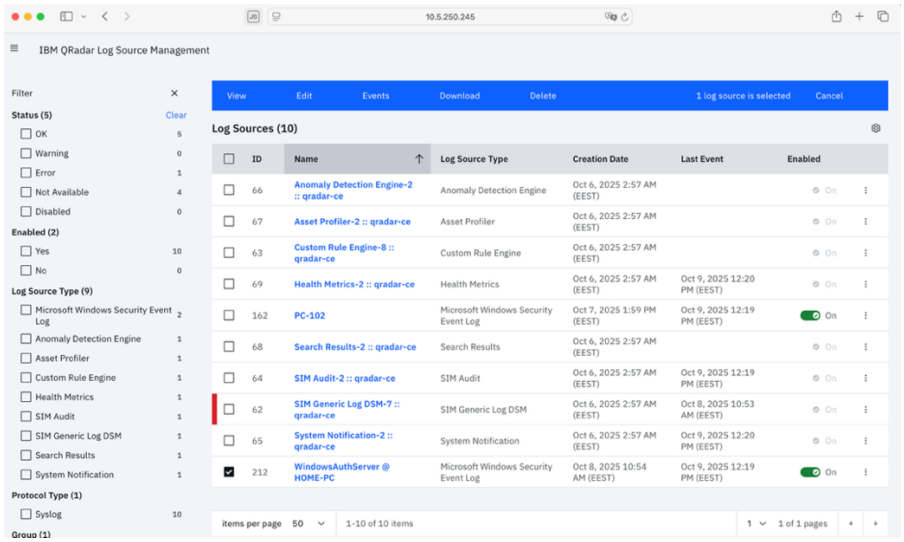


Рис. 3.17. Перегляд підключених джерел подій у розділі *Log Sources* консолі *IBM QRadar*

У консолі *QRadar* можна переглядати всі отримані системою журнали подій. У вкладці *Log Activity* відображаються події різних типів, що надходять у режимі реального часу, що дає змогу оперативно оцінювати стан безпеки та аналізувати активність у мережі (Рис.3.18).

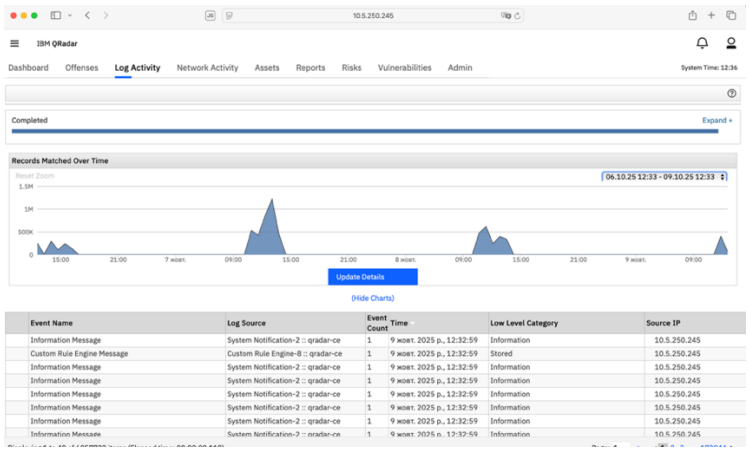


Рис. 3.18. *IBM QRadar*: *Log Activity*

Після підключення джерел подій та налаштування потоків даних основна інформація про стан системи безпеки відображається на панелі моніторингу *QRadar*. У розділі *Dashboard* зібрані ключові показники роботи системи, включно з активністю джерел журналів, кількістю подій, навантаженням процесорів обробки та іншими метриками, що дозволяють оперативно оцінювати загальний стан інфраструктури (Рис.3.19).

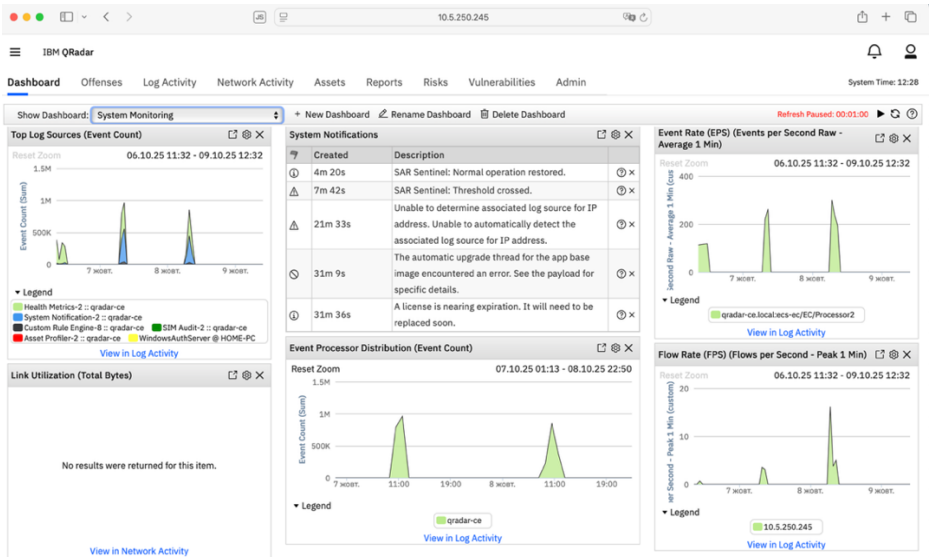


Рис. 3.19. *IBM QRadar*: *Dashboard*

Додаємо додаткове джерело у вигляді логів з *CrowdStrike Falcon* в *Qradar*. Відкриваємо панель адміністратора та переходимо в *Extension Management* (Рис. 3.20). Перевіряємо, що є шість властивостей користувацьких подій і одне джерело журналу, та встановлюємо.

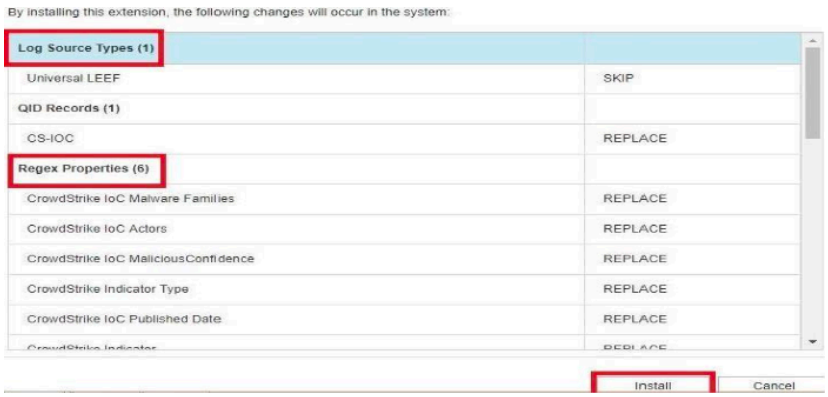


Рис. 3.20. Інсталяція розширень *CrowdStrike* в *Qradar*

Після завершення інсталяції в вкладці «Адміністратор» відкриваємо «Налаштувати інтеграцію *CrowdStrike Falcon Intel*» та вводимо ідентифікатор клієнта *Intel API* та ключі (Рис.3.21).

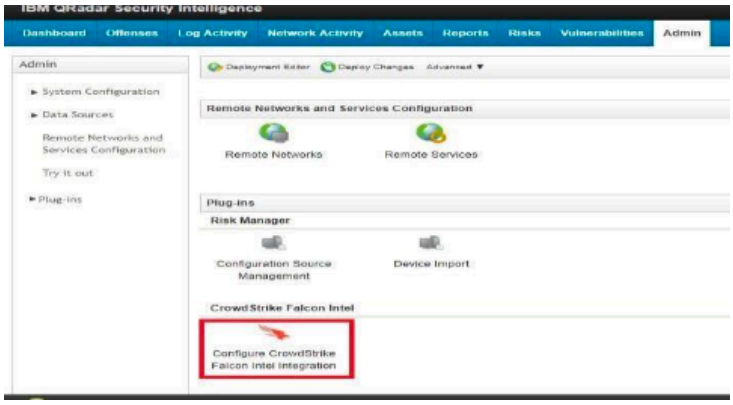


Рис. 3.21. Налаштування інтеграції *CrowdStrike Falcon Intel*

У вікні, що з’являється надаємо наступну інформацію (Рис.3.22):

1. *URL*-адреса хосту *Intel API* – https://intelapi.crowdstrike.com.
2. Ідентифікатор клієнта – ідентифікатор *Intel API*, наданий службою підтримки *CrowdStrike*.
3. Ключ клієнта – ключ *Intel API*, наданий службою підтримки *CrowdStrike*.

Рис.3.22. Додавання індентифікаторів та ключів клієнта в конфігурацію *CrowdStrike Falcon Intel*

Після збереження налаштувань додаток автоматично розпочинає періодичне опитування сервісу *CrowdStrike* з метою отримання подій типу *IoC*.

Усі отримані індикатори надходять у середовище *IBM QRadar* як стандартні журнали подій, що забезпечує можливість їх подальшої кореляції, аналізу та використання в механізмах виявлення загроз. Далі для перегляду отриманих даних необхідно перейти до розділу *Log Activity* та застосувати фільтр за джерелом логів *CrowdStrike IoC* (Рис.3.23).

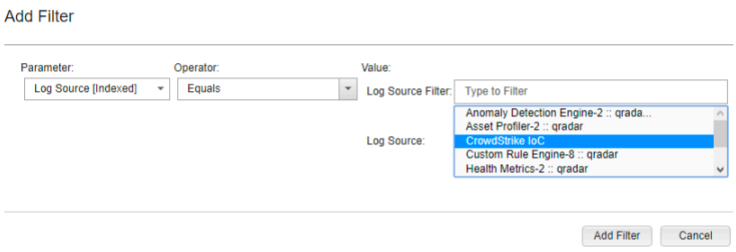


Рис.3.23. Відфільтровуємо події обравши лог-джерело *CrowdStrike Falcon*

Після застосування фільтру отримуємо можливість переглянути отримані від *CrowdStrike Falcon* індикатори компрометації [60]. Зокрема такі параметри, як назва події, час її фіксації, категорія загрози, IP-адреси джерела та призначення (Рис. 3.24).

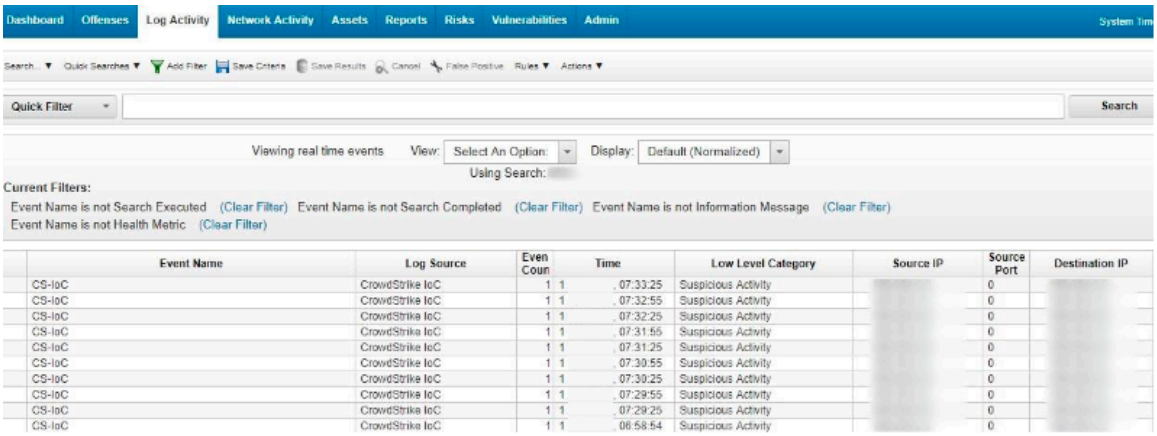


Рис.3.24. Отримані індикатори компрометації від *CrowdStrike Falcon*

Таким чином, інтеграція *CrowdStrike IoC* з *IBM QRadar* забезпечує автоматизований обмін загрозовою аналітикою, розширює можливості кореляції подій [61]. Це все підвищує загальну ефективність процесів виявлення та реагування на кіберзагрози (Рис.3.25).

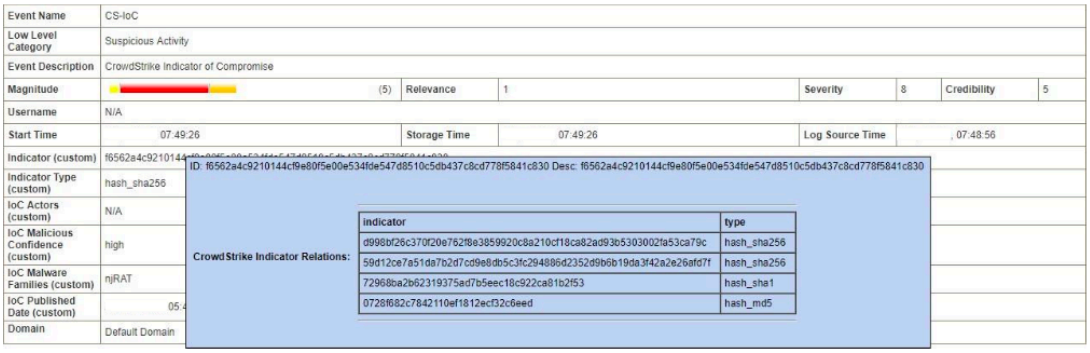


Рис.3.25. Перегляд детальної інформації про подію у *QRadar* після інтеграції з *CrowdStrike*

Для кількісної ілюстрації ефективності запропонованої моделі наведено умовне порівняння середнього часу обробки типового інциденту підозріла автентифікація і фішинг в лабораторному стенді. До впровадження моделі аналіз виконувався переважно вручну. Після впровадження за рахунок централізованої кореляції в *QRadar*, збагачення телеметрією *EDR* та застосування стандартизованих *runbook*/*playbook*. Сумарний час скоротився з 285 до 85 хв (Рис.3.26). Економія становить близько близько 70% часу.

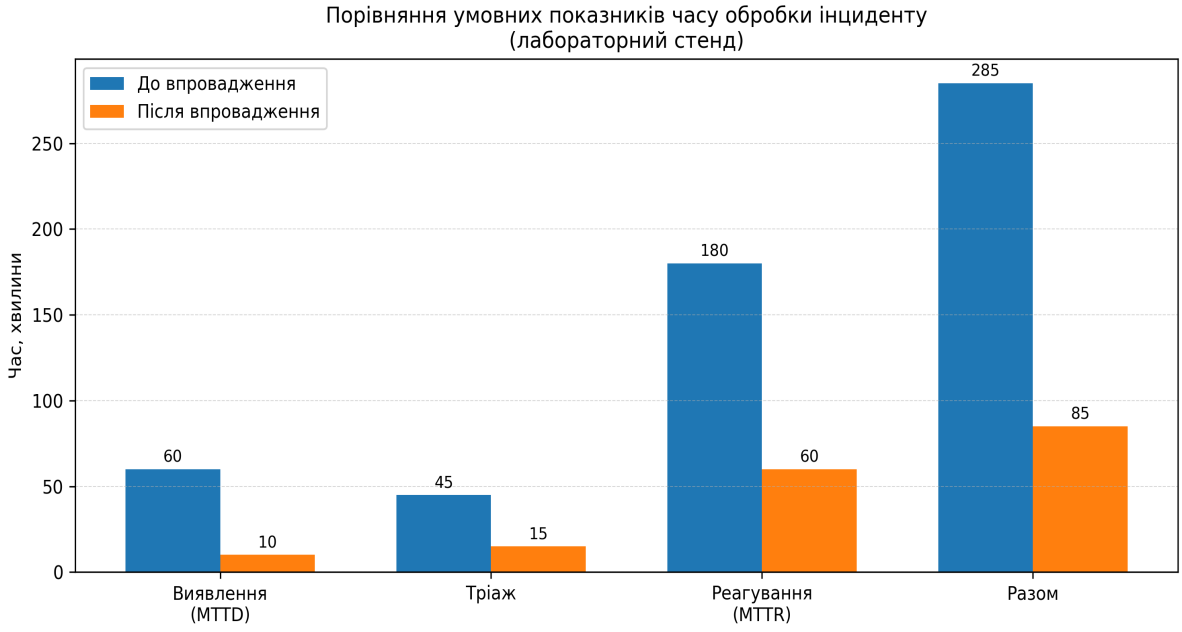


Рис. 3.26. Порівняння умовних показників часу обробки інциденту до та після впровадження моделі

Висновки до розділу 3

У третьому розділі дипломної роботи було розроблено та обґрунтовано модель захисту державних інформаційних ресурсів у хмарному середовищі. На основі системного підходу сформульовано завдання захисту та побудовано багаторівневу архітектуру із залученням сучасних інструментів: *IBM QRadar*, *CrowdStrike Falcon*, *Sysmon* та *WinCollect*.

Особливу увагу приділено практичному кейсу інсталяції та налаштування системи в умовах університету, що підтвердило життєздатність запропонованого рішення в реальному середовищі.

Надано практичні рекомендації щодо впровадження обраної моделі в українських державних установах, з урахуванням бюджетних обмежень, технічних вимог і кадрових можливостей. Загалом розроблена модель є адаптивною, масштабованою і може бути впроваджена поетапно відповідно до потреб конкретної установи.

ВИСНОВКИ

Під час роботи над дипломним проектом було виконано поставлені завдання:

1. Проаналізовано сучасні хмарні моделі й сервіси: *IaaS*, *PaaS*, *SaaS*, гібридні та мультихмарні підходи. Що застосовуються для зберігання та обробки державних інформаційних ресурсів, і узагальнено їх сильні та слабкі сторони з позицій безпеки та керованості.

2. Вивчено нормативно-правову базу та міжнародні стандарти *ISO*/*IEC* 27001/27017/27018, *NIST CSF*/800-53/800-207, а також вимоги законодавства України й узагальнено вимоги до організації хмарної безпеки у держсекторі.

3. Виявлено основні загрози та ризики застосування хмари в державних системах конфігураційні помилки, компрометація облікових записів, уразливі *API*, витік даних, ланцюгові атаки постачальників. Запропоновано підходи до їх мінімізації через *Zero Trust*, шифрування та централізований моніторинг.

4. Проаналізовано ключові методи захисту у хмарних середовищах *IAM*/*MFA*, *KMS*/*BYOK*, *CASB*, *EDR*/*XDR*, *SIEM*/*SOAR*, резервування та відновлення. Обґрунтовано доцільність їх поєднання в єдиній системній моделі, що підтверджено практичною апробацією.

5. Розроблено модель захисту державних інформаційних ресурсів із застосуванням хмарних технологій, що інтегрує *Zero Trust*, розподілену відповідальність і багаторівневий моніторинг; центральним елементом визначено *SIEM IBM QRadar* з надходженням телеметрії з *Sysmon* і *WinCollect*, хмарних сервісів та *EDR CrowdStrike*.

6. Сформовано практичні рекомендації щодо впровадження для державних установ України з урахуванням бюджетних обмежень: поетапне розгортання від базового логування та політик до *SIEM* і *EDR*, варіанти централізованого *SOC*, типові *playbook* та *runbook*, підготовка персоналу.

Наведено порівняльні таблиці рішень і обґрунтовано вибір *QRadar*, *CrowdStrike* та *Sysmon* з *WinCollect*.

7. Проведено апробацію моделі на умовному кейсі: інсталяція *QRadar All-in-one* у лабораторному середовищі університету з підключенням Windows-хостів через *Sysmon* і *WinCollect* з інтеграцією *EDR*; отримано офенси, перевірено роботу плейбуків і підтверджено придатність моделі до практичного застосування.

Завдяки запропонованій архітектурі *QRadar, Sysmon і WinCollect* та *CrowdStrike* та чітким процедурам *SOC*, рішення може бути впроваджене у державних установах різного рівня зрілості: від невеликих органів влади до центральних відомств із гібридною інфраструктурою.

Мету проекту було досягнуто. Сформована та апробована модель підвищує рівень кіберзахисту державних інформаційних ресурсів за рахунок поєднання хмарних технологій, централізованого моніторингу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. R. Islam, V. Patamsetti, A. Gadhi, R. M. Gondu, C. Bandaru, S. Kesani, O. Abiona, ‘‘The Future of Cloud Computing: Benefits and Challenges,’’ (in English) *Int. J. Commun. Network Syst. Sci.*, vol. 16, no. 4, pp. 53–65, Apr. 2023. DOI: https://doi.org/10.4236/ijcns.2023.164004 (дата звернення: 29.09.2025).

2. M. Mehrtak et al., ‘‘Security challenges and solutions using healthcare cloud computing,’’ (in English) *J. Med. Life*, vol. 14, no. 4, pp. 448–461, Jul–Aug 2021. DOI: 10.25122/jml-2021-0100 (дата звернення: 29.09.2025).

3. M. Kothapalli, ‘‘Cloud Computing Architectures: Comparing Service Models (IaaS, PaaS, SaaS) and Deployment Models (Public, Private, Hybrid, Community) – Uses and Trade-offs,’’ (in English) *Journal of Scientific and Engineering Research*, vol. 5, no. 10, pp. 334–341, Oct. 2018. DOI: http://dx.doi.org/10.5281/zenodo.12798259 (дата звернення: 30.09.2025).

4. F. Wulf, T. Lindner, S. Strahringer, M. Westner, ‘‘IaaS, PaaS, or SaaS? The Why of Cloud Computing Delivery Model Selection – Vignettes on the Post-Adoption of Cloud Computing,’’ (in English) Proceedings of the 54th Hawaii International Conference on System Sciences (HICSS), pp. 6285, Jan. 2021. DOI: http://dx.doi.org/10.24251/HICSS.2021.758 (дата звернення: 30.09.2025).

5. What is a Private Cloud URL: https://aws.amazon.com/what-is/private-cloud (дата звернення: 30.09.2024).

6. What’s the Difference Between Public Cloud and Private Cloud? URL: https://aws.amazon.com/compare/the-difference-between-public-cloud-and-private-cloud (дата звернення: 30.09.2024).

7. W. Jansen, T. Grance, ‘‘Guidelines on Security and Privacy in Public Cloud Computing,’’ (in English) NIST Special Publication 800-144, Dec. 2011. DOI: https://doi.org/10.6028/NIST.SP.800-144

8. FedRAMP Program Management Office, ‘‘FedRAMP: A standardized approach to security assessment, authorization, and continuous monitoring for cloud

services,'' (in English) U.S. GSA Official Guidance, 2025. DOI: — (дата звернення: 01.10.2025).

9. European Union Agency for Cybersecurity (ENISA), ''ENISA Threat Landscape 2024,'' (in English) ENISA Report, Sep. 2024. DOI: https://doi.org/10.2824/0710888

10. Cloud Security Alliance, ''Top Threats to Cloud Computing 2024,'' (in English) CSA Report, Aug. 2024. URL: https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2024 (дата звернення: 01.10.2025).

11. C. Del Giovane, J. Ferencz, J. López-González, ''The Nature, Evolution and Potential Implications of Data Localisation Measures,'' (in English) OECD Trade Policy Paper No. 278, Nov. 2023. DOI: https://doi.org/10.1787/179f718a-en (дата звернення: 01.10.2025).

12. ISO/IEC 27017:2015, "Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services," ISO, 2015 (in English). DOI: https://www.iso.org/standard/43757.html

13. . Mell, T. Grance, «The NIST Definition of Cloud Computing (SP 800-145)» NIST, Sept. 2011. DOI: https://doi.org/10.6028/NIST.SP.800-145 (дата звернення: 01.10.2025).

14. W. Jansen, T. Grance, «Guidelines on Security and Privacy in Public Cloud Computing (SP 800-144)» NIST, Dec. 2011. DOI: https://doi.org/10.6028/NIST.SP.800-144 (дата звернення: 05.10.2025).

15. Верховна Рада України, «Закон України Про захист персональних даних» URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 06.10.2025).

16. Верховна Рада України**,** «Про основні засади забезпечення кібербезпеки України». URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 06.10.2025).

17. Верховна Рада України, «Про захист інформації в інформаційно-телекомунікаційних системах». URL: https://zakon.rada.gov.ua/laws/show/80/94-вр (дата звернення: 06.10.2025).

18. E. Barker, «Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms». DOI: https://doi.org/10.6028/NIST.SP.800-175Br1 (дата звернення: 08.10.2025).

19. K. A. McKay et al., «Guidelines for the Selection, Configuration, and Use of Transport Layer Security Implementations». DOI: https://doi.org/10.6028/NIST.SP.800-52r2 (дата звернення: 09.10.2025).

20. NIST, «FIPS 140-3: Security Requirements for Cryptographic Modules» DOI: https://doi.org/10.6028/NIST.FIPS.140-3 (дата звернення: 11.10.2025).

21. Joint Task Force, «Security and Privacy Controls for Information Systems and Organizations» DOI: https://doi.org/10.6028/NIST.SP.800-53r5 (дата звернення: 12.10.2025).

22. CISA, «Implementing Phishing-Resistant Multi-Factor Authentication: Fact Sheet» URL: https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf (дата звернення: 13.10.2025).

23. Hasan, Muhammad Zulkifl & Sarwar, Nadeem & Alam, Intakhab & Hussain, Muhammad Zunnurain & Siddiqui, Adeel & Irshad, Asma. Data Recovery and Backup management: A Cloud Computing Impact. DOI: https://doi.org/10.1109/ICEST56843.2023.10138852 (дата звернення: 14.10.2025).

24. ISO/IEC, «ISO/IEC 27001:2022 — Information security management systems — Requirements» ISO Standard Overview, 2022. DOI: — (дата звернення: 17.10.2025).

25. Joint Task Force, «Security and Privacy Controls for Information Systems and Organizations» NIST Special Publication, 2020. DOI: https://doi.org/10.6028/NIST.SP.800-53r5 (дата звернення: 17.10.2025).

26. V. A. Stafford et al., «Zero Trust Architecture (SP 800-207)» NIST Special Publication, 2020. DOI: https://doi.org/10.6028/NIST.SP.800-207 (дата звернення: 17.10.2025).

27. UK National Cyber Security Centre, «The Cloud Security Principles» Government Guidance, 2024–2025. DOI: — (дата звернення: 18.10.2025).

28. U.S. General Services Administration, “FedRAMP — Federal Risk and Authorization Management Program,” (in English) Official Program Page, 2025. DOI: — (дата звернення: 18.10.2025).

29. A. Nelson et al., “Computer Security Incident Handling Guide (SP 800-61 Rev.3),” (in English) NIST Special Publication, 2025. DOI: https://doi.org/10.6028/NIST.SP.800-61r3 (дата звернення: 19.10.2025).

30. K. Dempsey et al., “Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations (SP 800-137),” (in English) NIST Special Publication, 2011. DOI: — (дата звернення: 20.10.2025).

31. Cloud Security Alliance, «Cloud Controls Matrix v4 — Framework and Guidelines» CSA Artifact Set, 2024. URL: https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4 (дата звернення: 26.10.2025).

32. Google Threat Analysis Group, "Fog of war: how the Ukraine conflict transformed the cyber threat landscape," (in English) Blog, Feb. 16, 2023. URL: https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/ (дата звернення: 27.10.2025).

33. Цифрова трансформація як інструмент створення інклюзивної економіки в Україні під час воєнного часу DOI: http://dx.doi.org/10.21511/ppm.22(3).2024.34 (дата звернення: 28.10.2025).

34. Cloud Under Siege: Unveiling Security Threats and Strategic Defences in the Era of Virtual Infrastructure. DOI: https://doi.org/10.36676/urr.v10.i3.1578 (дата звернення: 29.10.2025).

35. Cloud Computing as a Key Enabler for Digital Government across Asia and the Pacific. DOI: http://dx.doi.org/10.22617/WPS210196-2 (дата звернення: 29.10.2025).

36. Cloud Infrastructure Security: Essential Controls for Government Systems in 2025. URL: https://www.blott.com/blog/post/cloud-infrastructure-security-essential-controls-for-government-systems (дата звернення: 1.11.2025)

37. What is the CIA Triad and Why is it important? URL: https://www.fortinet.com/resources/cyberglossary/cia-triad (дата звернення: 2.11.2025)

38. Building a holistic cybersecurity framework for e-Government based on a systematic analysis of proposals. URL: https://link.springer.com_/article/10.1007/s10207-025-01024-0 (дата звернення: 2.11.2025)

39. IBM Security QRadar SIEM and 9 Custom Security Tools for 70+ US State Agencies URL: https://www.scnsoft.com/case-studies/siem-solution-for-70-us-state-agencies (дата звернення: 4.11.2025)

40. Qradar architecture overview URL: https://www.ibm.com/docs/en/qsip/7.4.0?topic= deployment-qradar-architecture-overview (дата звернення: 5.11.2025)

41. https://www.paloaltonetworks.com/cyberpedia/what-is-an-incident-response-playbook

42. CrowdStrike Quarantine Endpoint : Contain Host&Network Isolation URL: https://inventivehq.com/knowledge-base/crowdstrike/how-to-quarantine-and-contain-a-compromised-endpoint-in-crowdstrike -falcon (дата звернення: 5.11.2025)

43. CrowdStrike vs Microsoft Defender: Which EDR is better? URL: https://inventivehq.com/blog/crowdstrike-vs-microsoft-defender-which-solution-protects-your-business-best (дата звернення: 7.11.2025)

44. Which Tool Is Best: Splunk vs. QRadar vs. ELK Stack? URL: https://www.hackers4u.com/which-siem-tool-is-best-splunk-vs-qradar-vs-elk-stack (дата звернення: 7.11.2025)

45. Microsoft Defender vs. CrowdStrike Falcon: Comparing Endpoint Security Approaches. URL: https://www.wiz.io/academy/microsoft-defender-vs-crowdstrike-falcon (дата звернення: 8.11.2025)

46. Wincollect Powershell/Sysmon/Taskscheduler logs collection. URL: https://community.ibm.com/community/user/discussion/wincollect-powershellsysmontaskscheduler-logs-collection (дата звернення: 8.11.2025)

47. Top 9 Open Source SIEM Tools for 2025. URL: https://www.sentinelone.com/cybersecurity-101/data-and-ai/open-source-siem-tools/ (дата звернення: 9.11.2025)

48. A Guide to Incident Response Plans, Playbooks, and Policy. URL: https://www.fortinet.com/blog/ciso-collective/incident-response-plans-playbooks-policy (дата звернення: 9.11.2025)

49. Understanding Playbook in Cyber Security. URL: https://medium.com/@trout.software/understanding-playbooks-in-cyber-security-2afc93ff8029 (дата звернення: 10.11.2025)

50. SIEM for Government and Public Sector Security. URL: https://searchinform.com/articles/cybersecurity/measures/siem/use-cases/government-and-public-sector/ (дата звернення: 13.11.2025)

51. Your Comprehensive Guide to ISO 27001 Controls. URL: https://heimdalsecurity.com/blog/iso-27001-controls/ (дата звернення: 14.11.2025)

52. Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r4.pdf (дата звернення: 14.11.2025)

53. IBM Security. Try QRadar SIEM | IBM Security QRadar Community Edition (CE). URL: https://www.ibm.com/community/101/qradar/ce/ (дата звернення: 15.11.2025)

54. *IBM* QRadar: Installation Guide. URL: https://www.ibm.com/docs/en/SS42VS_7.4/pdf/b_siem_inst.pdf (дата звернення: 16.11.2025)

55. IBM QRadar WinCollect: WinCollect User Guide V7. URL: https://www.ibm.com/docs/en/SS42VS_SHR/pdf/b_wincollect.pdf (дата звернення: 15.11.2025).

56. Microsoft Learn (Sysinternals). *Sysmon - Sysinternals.* URL: https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon (дата звернення: 15.11.2025).

57. CrowdStrike Falcon Intel QRadar Integration App Installation and User Guide. URL: https://exchange.xforce.ibmcloud.com/api/hub/extensionsNew/6ff798

eb260827520b80b52a9f3bb11f/CrowdStrike_Falcon_Intel_QRadar_Integration_App_Installation_and_User_Guide.pdf (дата звернення: 15.11.2025).

58. MITRE ATT&CK® Enterprise Matrix. URL: https://attack.mitre.org /matrices/enterprise/ (дата звернення: 14.12.2025).

59. IBM QRadar: QRadar User Guide. URL: https://www.ibm.com/docs/en/ SS42VS_7.4/ pdf/b_qradar_users_guide.pdf (дата звернення: 15.11.2025).

60. Offense management in IBM QRadar. URL: https://www.ibm.com/docs /en/qradar-on-cloud?topic=siem-offense-management (дата звернення: 15.12.2025).

61. Priority logs for SIEM ingestion: practitioner guidance. URL: https://media.defense.gov/2025/May/27/2003722069/-1/-1/0/PRIORITY-LOGS-FOR-SIEM-INGESTION-PRACTITIONER-GUIDANCE.PDF (дата звернення: 14.12.2025).