Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

# КВАЛІФІКАЦІЙНА РОБОТА

Мельник Мар'яни Миколаївни

на здобуття ступеня вищої освіти магістра

Метод виявлення та розслідування цілеспрямованих атак на об'єкти критичної інфраструктури

Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека та захист інформації
Освітня програма Кібербезпека та захист інформації

Шифр КРМКБЗІ.240194.24.01.09 ПЗ

Виконала студентка 2 курсу група КБЗІм-24-1 Мар'яна МЕЛЬНИК
Керівник канд. техн. наук, доцент Віктор ЧЕШУН
Нормоконтролер PhD, старший викладач Наталія ПЕТЛЯК

До захисту допускаю:
Завідувач кафедри кібербезпеки Юрій КЛЬОЦ

16 12 2025 р.

Хмельницький 2025

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Рівень вищої освіти Магістр

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека та захист інформації

Освітня програма Кібербезпека та захист інформації

ЗАТВЕРДЖУЮ

Завідувач кафедри кібербезпеки

Юрій КЛЬОЦ

1 09 2025 р.

# З А В Д А Н Н Я

# НА КВАЛІФІКАЦІЙНУ РОБОТУ

Мельник Мар'яні Миколаївні

1 Тема роботи Метод виявлення та розслідування цілеспрямованих атак на об'єкти критичної інфраструктури

Керівник роботи канд.техн.наук, доцент Віктор ЧЕШУН

Затверджено наказом ректора університету від 25 08 2025 № 65

2 Строк подання студентом кваліфікаційної роботи на кафедру 1.12.2025р.

3 Вихідні дані до роботи Розробити універсальний метод виявлення та розслідування кіберінцидентів на об'єктах критичної інфраструктури, що відповідатиме державним вимогам, поєднуючи процедури моніторингу, автоматичного аналізу, виявлення аномалій, збору доказової інформації та формування аналітичних звітів, інструкцій для оперативного реагування

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити) Дослідження актуальних методів та технологій розслідування кіберінцидентів. Моделі та метод виявлення та розслідування цілеспрямованих атак на об'єкти критичної інфраструктури. Формування моделі процесу реагування та аналізу інцидентів. Модель збереження та відновлення цифрових доказів. Модель взаємодії учасників розслідування кіберінцидентів у державних інформаційних системах. Розробка методу розслідування кіберінцидентів. Практична реалізація та експериментальні дослідження. Побудова тестового середовища. Реалізація методу. Оцінка ефективності розробленого методу та практичні рекомендації.

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

–

6 Консультанти розділів кваліфікаційної роботи

| Розділ | Прізвище, ініціали та посада консультанта | Підпис, дата | |
|---|---|---|---|
| | | завдання видав | завдання прийняв |
| | | | |
| | | | |

7 Дата видачі завдання 1 09 2025 р.

## КАЛЕНДАРНИЙ ПЛАН

| Назва етапів (розділів) кваліфікаційної роботи | Строк виконання етапів роботи | Примітка |
|---|---|---|
| Ґрунтовне ознайомлення та дослідження предметної галузі | 15.09.2025 | |
| Визначення змісту, структури кваліфікаційної роботи | 22.09.2025 | |
| Підготовка першого розділу кваліфікаційної роботи | 29.09.2025 | |
| Підготовка другого розділу кваліфікаційної роботи | 10.10.2025 | |
| Підготовка третього розділу кваліфікаційної роботи | 20.10.2025 | |
| Підготовка статті/тези за темою кваліфікаційної роботи | 4.11.2025 | |
| Підготовка висновків до кваліфікаційної роботи | 17.11.2025 | |
| Підготовка та оформлення ілюстративного матеріалу | 24.11.2025 | |
| Оформлення кваліфікаційної роботи | 24.11.2025 | |
| Попередній захист кваліфікаційної роботи | 27.11.2025 | |
| Захист кваліфікаційної роботи на засіданні ЕК | 10.12.2025 | |

Студентка Мар'яна МЕЛЬНИК

Керівник кваліфікаційної роботи Віктор ЧЕШУН

# АНОТАЦІЯ

Тема кваліфікаційної роботи: Метод виявлення та розслідування цілеспрямованих атак на об'єкти критичної інфраструктури.

Автор роботи: Мельник Мар'яна Миколаївна

Керівник роботи: канд. техн. наук, доц. Чешун Віктор Миколайович

Загальний обсяг роботи: 104 сторінки, 21 рисунок, 8 таблиць, 1 додаток, 65 посилань.

Ключові слова: кіберінцидент, розслідування, цифрова криміналістика, журнали подій, критична інфраструктура, реагування на інциденти.

Кваліфікаційна робота присвячена розробці та практичній реалізації методу виявлення та розслідування цілеспрямованих кібератак на об'єкти критичної інфраструктури. У роботі проаналізовано сучасні підходи до реагування на кіберінциденти, міжнародні стандарти та особливості їх застосування в Україні.

Запропонований метод базується на автоматизованому зборі телеметрії, централізованому аналізі журналів подій, кореляції цифрових артефактів і використанні контексту загроз. Реалізація методу виконана у тестовому середовищі з використанням операційних систем Windows і Linux та інструментів моніторингу й управління інцидентами.

Експериментальні результати підтвердили ефективність методу щодо своєчасного виявлення кіберінцидентів, відтворення дій зловмисника та підвищення якості цифрових доказів і аналітичних звітів.

1.12.2025

# ABSTRACT

Title of the Qualification Thesis: Method for Detection and Investigation of Targeted Attacks on Critical Infrastructure Objects

Author: Melnyk Mariana Mykolaivna

Mentor: Ph.D. Cheshun Viktor Mykolaiovych

Total volume of the thesis: 104 pages, 21 figures, 8 tables, 1 appendix, 65 references.

Keywords: cyber incident, investigation, digital forensics, event logs, critical infrastructure, incident response.

The qualification thesis is devoted to the development and practical implementation of a method for detecting and investigating targeted cyberattacks on critical infrastructure facilities. The paper analyzes modern approaches to cyber incident response, international standards, and the specifics of their application in Ukraine.

The proposed method is based on automated telemetry collection, centralized event log analysis, correlation of digital artifacts, and the use of threat context. The method was implemented in a test environment using Windows and Linux operating systems, as well as monitoring and incident management tools.

Experimental results confirmed the effectiveness of the method in ensuring timely detection of cyber incidents, reconstruction of attacker actions, and improvement of the quality of digital evidence and analytical reports.

1.12.2025 

ЗМІСТ

# ВСТУП

Сьогодні майже всі процеси в державних установах, приватних компаніях і навіть у звичайному повсякденному житті так чи інакше пов’язані з цифровими технологіями. Через це, будь-який збій у роботі інформаційних систем може спричинити ланцюгову реакцію, яка торкається набагато ширшої аудиторії, ніж здається на перший погляд. Кібератаки перестали бути чимось винятковим – вони стали звичною частиною реальності. З кожним роком їх складність і кількість лише зростає.

Попри наявність законів і методичних документів, багато процесів у сфері розслідування кіберінцидентів в Україні залишаються несистемними. Кожна установа працює по-своєму: десь журнали подій майже не зберігаються, десь доказів взагалі немає через неправильне їх вилучення, а десь реагування зводиться до “перезапустити і подивитися, чи допоможе”. У результаті інколи навіть неможливо відтворити, що саме відбулося під час інциденту, і це фактично унеможливлює повноцінне розслідування.

З огляду на всі ці фактори виникає потреба у створенні єдиного, зрозумілого та практичного методу розслідування кіберінцидентів, який можна застосовувати в різних організаціях – від державних відомств до приватних компаній. Він повинен бути гнучким, містити як технічні, так і організаційні елементи, та передбачати чітку взаємодію між усіма сторонами, залученими до реагування. Така модель дозволить не лише краще протистояти атакам, а й у перспективі зменшити кількість інцидентів завдяки своєчасному виявленню слабких місць і вдосконаленню підходів до захисту.

Проблема створення подібної універсалізованої моделі в тому, що більшість сучасних атак уже не спрямовані просто на те, щоб «покласти сайт» чи викрасти окремий файл. Часто йдеться про тривалу приховану присутність у системі, збір даних, втручання у критичні процеси або спроби порушити роботу інфраструктури. У таких умовах звичайні методи реагування перестають бути ефективними, адже вони зосереджуються лише на усуненні видимих наслідків, а не на розумінні того,

як саме відбулася атака і що потрібно змінити, щоб вона не повторилася.

В українських реаліях потреба у системному підході ще гостріша. Ми маємо справу з регулярними кібератаками, багато з яких спрямовані саме на об’єкти критичної інфраструктури або державні органи. Події останніх років показали, що навіть великі й досвідчені організації можуть стати жертвами добре спланованих дій зловмисників. І саме в такі моменти стає очевидно, що відсутність чіткої, єдиної та зрозумілої моделі розслідування інцидентів створює додаткові ризики та ускладнює роботу команд, відповідальних за реагування.

Тому сьогодні питання не лише у тому, як швидко виявити інцидент, – важливо також правильно зібрати цифрові докази, зберегти їх у належному стані, провести детальний аналіз і зробити висновки, які дозволять зміцнити систему захисту. Без цього будь-яке реагування буде неповним і не дасть можливості попередити подібні атаки в майбутньому.

Саме тому тема цієї роботи є актуальною: наявність зрозумілого методу розслідування кіберінцидентів, який враховує українські реалії та міжнародний досвід, може суттєво підвищити рівень кіберзахисту державних і приватних структур.

Метою роботи є створення чіткого та практичного методу розслідування кіберінцидентів, який можна буде застосовувати на об’єктах критичної інфраструктури. Йдеться не просто про опис окремих технічних кроків чи перелік інструментів, а про побудову повноцінної моделі, яка допоможе організаціям діяти злагоджено, незалежно від того, який саме інцидент стався і якої складності він був.

Для цього потрібно розглянути цілу низку питань, починаючи від того, як саме виявляються інциденти, і закінчуючи тим, як аналізуються цифрові артефакти та як формується фінальний звіт. З огляду на те, що об’єкти критичної інфраструктури часто працюють у різних умовах, важливо було визначити підхід, який можна адаптувати під певні технічні обмеження, але водночас не втратити логіку й послідовність дій.

Щоб досягнути поставленої мети, у роботі визначено кілька основних завдань:

– провести огляд існуючих методів і рекомендацій щодо розслідування кіберінцидентів, які застосовуються в Україні та інших країнах;

– визначити, які підходи можуть працювати в українських умовах найбільш ефективно і де можуть виникати труднощі;

– описати модель розслідування, яка включає всі етапи – від моменту виявлення інциденту до його завершення;

– показати, як відкриті інструменти (такі як Wazuh, ELK, MISP чи TheHive) можуть допомогти автоматизувати процес збору й аналізу доказів;

– сформувати рекомендації щодо впровадження моделі в державних структурах або великих організаціях.

Об’єктом дослідження є процес розслідування кіберінцидентів у системах – об’єктах критичної інформаційної інфраструктури.

Йдеться про ті інформаційні ресурси, збій у роботі яких може призвести до серйозних наслідків: енергетичні підприємства, транспортні вузли, зв’язок, державні сервіси та інші подібні структури. Вони працюють у складних умовах, і будь-який інцидент у таких системах потребує швидкої та чіткої реакції.

Предметом дослідження є методи та етапи розслідування кіберінцидентів, методики фіксації подій, процедури формування і зберігання журналів систем, операції з цифровими доказами та підтримка їх цілісності, застосовувані криміналістичні інструменти та регламенти оформлення результатів.

Методи дослідження включають аналіз нормативних документів та міжнародних стандартів, моделювання атак, експериментальні дослідження у віртуальному середовищі, цифрову криміналістику (Volatility, Autopsy, log2timeline), аналіз логів (ELK Stack), кореляцію подій (Wazuh), обробку IoC (MISP) та керування інцидентами (TheHive). Використання різних джерел телеметрії дало можливість створити повну картину інциденту та оцінити працездатність запропонованої моделі.

Наукова новизна отриманих результатів:

1. Запропоновано дві оригінальні моделі процесів цифрової криміналістики :

модель збереження та відновлення цифрових доказів та модель взаємодії учасників розслідування кіберінцидентів у державних інформаційних системах.

2. Сформовано інтегрований метод реагування та аналізу, який об’єднує кілька платформ у єдину логічну систему, орієнтовану на потреби українських об’єктів критичної інфраструктури.

На відміну від типових моделей, запропонований підхід акцентує увагу на використанні відкритих інструментів, що робить його доступним і економічно ефективним.

Практична цінність полягає в можливості безпосереднього впровадження результатів у діяльність державних установ та організацій, які працюють у сфері кіберзахисту, що допоможе якісно структурувати реагування на інциденти, скоротити час їхнього аналізу, підвищити повноту зібраних доказів та рівень взаємодії між технічними групами. Крім того, він може бути основою для побудови внутрішніх процедур CSIRT/CERT-підрозділів та навчання персоналу.

Фактично, дослідження зосереджене на тому, щоб вибудувати зрозумілу та реалістичну модель роботи з інцидентами, яку можна застосувати в умовах української критичної інфраструктури. Це дозволить не тільки швидше реагувати на загрози, а й створювати накопичену базу знань, необхідну для підвищення рівня захищеності у майбутньому.

Результати та основні положення роботи пройшли апробацію у формі доповідей на міжфакультетській конференції Поліського національного університету, 2-х Всеукраїнських та міжнародній науково-практичних конференціях. За результатами роботи підготовлено та подано у фахове видання наукову статтю.

# 1 ДОСЛІДЖЕННЯ АКТУАЛЬНИХ МЕТОДІВ ТА ТЕХНОЛОГІЙ РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ

## 1.1 Аналіз сучасних підходів до розслідування кіберінцидентів

З переходом державних установ до цифрових сервісів кількість кібератак на критично важливі об’єкти продовжує зростати. За даними ENISA Threat Landscape Report 2023 [1], у 2022–2023 роках понад 40% усіх кіберінцидентів у Європі були спрямовані на енергетику, транспорт, урядові структури та зв’язок – саме ті сфери, на яких найбільше тримається безпека держав.

Схожа ситуація спостерігається і в Україні. Звіти ДССЗЗІ та CERT-UA показують не лише збільшення кількості інцидентів, але й помітне ускладнення самих атак [2,3]. Зловмисники дедалі частіше комбінують різні методи – від соціальної інженерії та фішингу до компрометації ланцюгів постачання та використання шкідливих програм типу wiper. Недостатня обізнаність персоналу, мала кількість ресурсів та халатне відношення до безпекових політик є однією з першопричин успішності більшості цілеспрямованих атак. Помилка однієї людини, в більшості випадків, несе за собою небезпеку для всієї системи.

Зросла кількість цілеспрямованих атак на військові об’єкти, у тому числі, на військових. Окрім того, варто враховувати безвідповідальне ставлення до питань захисту інформації. Багато організацій не звертають увагу на головне питання захисту – питання людського фактору.

Створення служб реагування та моніторингу є однією з умов вчасного виявлення та зупинення атаки на початкових етапах. Не відповідність систем до рівню, що регламентує законодавство України ставить під загрозу не тільки самі організації, але й усю структуру держави. У період військового стану в країні, питання захисту інформації мало би стояти одним і перших.

У цих умовах розслідування кіберінцидентів відіграє ключову роль у забезпеченні державної кібербезпеки. Йдеться не тільки про ліквідацію наслідків атаки, а й про збір цифрових доказів, встановлення причин події, визначення характерних ознак загроз і розробку заходів, які допомагають уникати схожих

інцидентів надалі.

Стандарт ISO/IEC 27035:2023 – Information Security Incident Management [4,5], визначає інцидент інформаційної безпеки як подію або низку пов’язаних подій, які становлять реальну або потенційну загрозу для конфіденційності, цілісності чи доступності інформаційних ресурсів. Це визначення на практиці означає будь-яку ситуацію, яка може вплинути на роботу інформаційних систем і потребує реакції.

Однією з найпоширеніших моделей розслідування є підхід з документа NIST SP 800-61 Rev.2. У цьому документі описується чотири ключові етапи роботи з інцидентом: підготовку, виявлення й аналіз, реагування та дії після завершення інциденту [6].

На першому етапі формується команда реагування на інциденти (CSIRT), визначаються правила роботи з інцидентами, прописуються політики безпеки. Створюються механізми моніторингу та канали комунікації. Далі ми маємо створити середовище, яке здатне фіксувати всі події безпеки: журнали систем, мережевий трафік, аутентифікаційні події [6,7].

Зазвичай, для цього використовуються SIEM-платформи, наприклад, Wazuh або ELK Stack. Вони забезпечують збір, агрегацію та кореляцію подій. Також обов’язково проводиться ідентифікація ознак атаки – так званих індикаторів компрометації.

Це можуть бути незвичні спроби входу в систему, підозрілі мережеві активності, зміни у важливих файлах або запуск процесів, яких раніше не було. Для їх виявлення зазвичай застосовується аналіз поведінки, системи виявлення вторгнень, а також алгоритми машинного навчання, які допомагають швидко класифікувати події [7].

У міжнародному досвіді, етап «реагування, ізоляції та відновлення» часто виконують у тісній взаємодії з платформами обміну інформацією MISP (Malware Information Sharing Platform) [8,9]. Це дозволяє швидше зрозуміти природу загрози. Головне завдання цього етапу – припинити поширення атаки, зменшити її наслідки та повернути систему до нормального режиму роботи. Для цього ізолюють

пошкоджені системи, перевіряють резервні копії, встановлюють оновлення безпеки й переконуються, що в системі не залишилися приховані бекдори або шкідливі файли, які могли залишити зловмисники. У державних структурах цей процес має проводитись відповідно до затверджених політик реагування та погоджуватись із органами ДССЗЗІ [2,9,10].

На фінальному етапі проводять детальний аналіз того, що саме стало причиною інциденту, формують технічний звіт, оцінюють, наскільки ефективними були заходи реагування, і розробляють рекомендації, щоб уникнути подібних випадків у майбутньому. Стандарт ISO/IEC 27035-3:2023 [4] наголошує на необхідності документування доказів для подальшого використання у судових або адміністративних розслідуваннях.

У різних країнах сформувалися три основні моделі того, як організовують розслідування кіберінцидентів.

Перший підхід – централізований, він характерний для більшості країн Європейського Союзу. У цій моделі головну роль відіграє національний центр реагування (CERT). Він координує діяльність усіх галузевих команд реагування (CSIRT). Прикладом такої системи є CERT-EU. Він забезпечує взаємодію та реагування на кіберінциденти в інституціях Європейського Союзу [9,11].

Другий підхід – децентралізований. Найбільш типовий для Сполучених Штатів Америки. У США кожна відомча структура має власну команду реагування на інциденти. Наприклад, у Міністерства енергетики (DOE), Департаменту внутрішньої безпеки (DHS) та Агентства з кібербезпеки і безпеки інфраструктури (CISA). Координація між цими структурами відбувається за допомогою федеральних протоколів реагування, це забезпечує швидкість дій у межах власних юрисдикцій і ефективну взаємодію на національному рівні [12,13].

Третій підхід – гібридний або змішаний. Він поєднує елементи централізованої та децентралізованої моделей. Його використовують країни Балтії, зокрема Литва та Естонія. Тут національний центр кібербезпеки встановлює єдині стандарти розслідування інцидентів, тоді як безпосереднє реагування здійснюють відомчі підрозділи. Ця система дає змогу зберігати гнучкість у реагуванні на події,

не втрачаючи централізованого контролю над аналітикою та координацією [14].

Хорошим прикладом є Естонія, де створено добровольче формування Cyber Defence League. Ця система об’єднує державних і громадських фахівців для участі у розслідуванні масштабних кіберінцидентів. Під час масових атак у 2007 році ця команда показала високу ефективність та стала однією з ключових сил у реагуванні.

У Фінляндії діє спільна програма CERT-FI та ENISA, у межах якої регулярно проводять навчальні кібератаки (cyber range). Такі тренування дозволяють відпрацьовувати реагування на інциденти в умовах, наближених до реальних [13,14].

В Україні процес розслідування кіберінцидентів на об’єктах критичної інфраструктури регламентується національним законодавством і актами. Зокрема, основні принципи визначені у законах «Про основні засади забезпечення кібербезпеки України» та «Про захист інформації в інформаційно-телекомунікаційних системах». Крім того, Постановою Кабінету Міністрів №518 від 19 червня 2019 року було затверджено порядок реагування на кіберінциденти. Ця постанова деталізує обов’язки суб’єктів критичної інфраструктури. Важливе значення мають також методичні рекомендації CERT-UA (2024), що описують послідовність дій при виявленні, фіксації та усуненні інцидентів інформаційної безпеки [8,9].

Попри наявність нормативної бази та окремих методичних документів, система розслідування кіберінцидентів в Україні досі стикається з низкою суттєвих проблем, які обмежують її ефективність, особливо в контексті захисту об’єктів критичної інфраструктури.

Одним із ключових недоліків є низький рівень автоматизації процесів збору та аналізу подій безпеки. У більшості державних установ моніторинг подій здійснюється фрагментарно, без централізованої обробки журналів подій (логів), що ускладнює оперативне виявлення інцидентів та їх кореляцію. За даними Держспецзв’язку у звіті про стан кібербезпеки за 2024 рік, лише близько 40% об’єктів критичної інфраструктури мають впроваджені системи моніторингу

безпеки (SIEM) [2]. Водночас, міжнародна практика демонструє значно вищий рівень автоматизації: наприклад, у країнах ЄС системи на кшталт Wazuh або ELK Stack інтегруються з платформами MISP для централізованого збору та обміну індикаторами компрометації [3].

Недостатня інтеграція між національними та галузевими CSIRT-командами призводить до затримки обміну інформацією про атаки та неузгодженості дій під час реагування. Відповідно до рекомендацій ENISA, ефективна модель взаємодії має ґрунтуватися на принципі взаємного обміну даними в режимі реального часу між секторальними CERT, проте в Україні ця взаємодія ще не є системною [13].

Суттєвою проблемою залишається нестача кваліфікованих фахівців із цифрової криміналістики, що обмежує спроможність оперативно проводити глибокий технічний аналіз інцидентів. У більшості випадків, навіть при наявності технічних артефактів (дампів пам’яті, логів, зразків шкідливого коду), процес розслідування затримується через дефіцит фахівців, здатних застосовувати інструменти, такі як Autopsy, FTK Imager, Volatility чи Wireshark, для відтворення подій атаки та визначення механізмів компрометації [15].

Крім того, інфраструктура моніторингу безпеки в Україні залишається фрагментованою. Кожен об’єкт критичної інфраструктури здебільшого використовує власні засоби виявлення аномалій, що призводить до різного рівня деталізації даних та ускладнює централізований аналіз загроз. Відсутність єдиного формату звітності про інциденти, незважаючи на існування стандарту ISO/IEC 27035 [4,5] та методичних рекомендацій CERT-UA [16], створює додаткові труднощі для обміну інформацією між установами.

Ще одним викликом є відсутність уніфікованої національної бази індикаторів компрометації, що могла б забезпечувати оперативне виявлення повторюваних або схожих атак на різних об’єктах. В європейських країнах подібні бази інтегруються через системи MISP або STIX/TAXII, що дає змогу здійснювати автоматизований обмін загрозами на міжвідомчому рівні [17,18]. В Україні ж цей процес відбувається переважно вручну або за запитом, що значно знижує швидкість реагування на інциденти [16].

Розробка комплексного методу, що інтегрує автоматизовані інструменти аналізу (Wazuh, ELK, MISP) із формалізованими процедурами реагування, має дозволити значно підвищити ефективність реагування на інциденти, скоротити час розслідування та зменшити ризики повторного компрометування об’єктів критичної інфраструктури [17].

## 1.2 Статистичний аналіз кіберінцидентів в Україні та світі

Останні роки характеризуються стрімким зростанням кількості кіберінцидентів, що уражають як державні, так і приватні інформаційні системи. За даними ENISA Threat Landscape Report 2023 [1], у світі зафіксовано понад 25% збільшення кількості атак на об’єкти критичної інфраструктури порівняно з попереднім роком. Особливої уваги заслуговують інциденти у сфері енергетики, телекомунікацій та державного управління, які мають безпосередній вплив на національну безпеку. Згідно з IBM Cost of a Data Breach Report 2024 [19], середня вартість одного кіберінциденту у державному секторі перевищила 2,6 млн доларів США, що свідчить про високу ціну відновлення після атак.

В Україні тенденція до збільшення кількості кіберінцидентів зберігається. За даними Державної служби спеціального зв’язку та захисту інформації України (ДССЗЗІ) [2,10], протягом 2024 року зафіксовано понад 2,5 тисячі підтверджених кібератак на державні інформаційні ресурси. Основну частку становили фішингові кампанії, розповсюдження шкідливого програмного забезпечення (зокрема, типу wiper), DDoS-атаки та спроби несанкціонованого доступу до інформаційно-телекомунікаційних систем [3].

У звіті CERT-UA (2024) [3] зазначається, що близько 60% інцидентів мали цілеспрямований характер і були спрямовані на викрадення даних або дестабілізацію роботи державних онлайн-сервісів. Одним із найгучніших прикладів став інцидент із телекомунікаційною компанією «Київстар», який відбувся у грудні 2023 року (рис 1.1 ).


Рисунок 1.1 – Схема атаки на Київстар

Кібератака призвела до масштабного відключення мобільного зв’язку, недоступності сервісів та часткової втрати даних клієнтів [20]. Розслідування показало, що зловмисники мали тривалий прихований доступ до корпоративної мережі, здійснювали збір облікових даних та використали зламані адміністративні облікові записи для масштабного знищення інфраструктури. Через недостатній моніторинг системи, зловмисники мали достатньо багато часу.

Цей випадок продемонстрував важливість своєчасного виявлення підозрілих активностей, ефективного управління журналами подій і наявності резервних процедур реагування, а також виявив брак автоматизованих систем моніторингу безпеки у національних операторів. Також важливою складовою є політика відновлення після інциденту. Саме за рахунок правильного зберігання інформації, час відновлення системи суттєво зменшується.

Згідно з оцінками CrowdStrike Global Threat Report 2024 [21], протягом останніх двох років значно зросла кількість атак із використанням складних багатовекторних технік (APT-угруповань), які поєднують соціотехнічні прийоми, фішинг, компрометацію облікових записів та експлуатацію вразливостей у критичних сервісах. Обізнаність персоналу має бути високою на всіх рівнях організації, також, відповідно до політик безпеки, рівні доступу до інформації мають бути чітко визначенні, так само як і інформація поділена.

У звіті FireEye M-Trends 2024 [22] зазначено, що середній час перебування зловмисника у мережі до його виявлення (так званий dwell time) у державному секторі становить близько 22 днів, тоді як у приватному секторі цей показник скоротився до 10 днів завдяки ширшому використанню систем SIEM і SOAR. У таблиці 1.1 представленні типові ситуації при розслідувані кіберзлочинів [23].

Аналізуючи ситуацію в Україні, можна відзначити поступове зростання ролі CERT-UA як координаційного центру реагування на інциденти. Проте рівень автоматизації та інтеграції державних і галузевих CSIRT-команд залишається недостатнім.

Таблиця 1.1 – Типові ситуації при розслідуванні кіберзлочинів

| Типова ситуація | Характеристика ситуації | Основні дії слідчих та аналітиків | Використовувані інструменти |
|---|---|---|---|
| Неавторизований доступ до інформаційних систем | Виявлено факт проникнення або спроби входу в систему без дозволу | Аналіз логів, ідентифікація облікового запису, відстеження джерела атаки | ELK Stack, Wazuh, Wireshark |
| Розповсюдження шкідливого програмного забезпечення | Виявлено виконання або зараження системи вірусом чи трояном | Ізоляція системи, форензик-аналіз, виявлення шляху зараження | Autopsy, FTK Imager, virustotal |
| Витік конфіденційної інформації | Виявлено передачу або копіювання даних без дозволу | Встановлення джерела витоку, аудит облікових записів, відновлення доказів | MISP, thehive, Splunk |
| Ddos-атака на критичний ресурс | Перевантаження серверів через масові запити | Аналіз мережевого трафіку, фільтрація ip, координація з провайдером | Cisco netflow, Wazuh, ELK Stack |
| Втручання у роботу веб-ресурсу (deface) | Змінено зовнішній вигляд вебсайту або вміст сторінок | Збір копій сторінок, аналіз вебсервера, пошук вразливостей у cms | Burp Suite, Nmap, Logstash |
| Використання фішингових повідомлень | Розповсюдження шкідливих листів для крадіжки даних | Аналіз зразків листів, доменів і вкладень, блокування поштових каналів | Thehive, virustotal, MISP |
| Несанкціоноване втручання в роботу scada або iot-систем | Порушення роботи промислових систем управління | Аналіз протоколів зв’язку, відновлення конфігурацій, перевірка безпеки | Wireshark, Zeek, Wazuh |

Багато організацій обмежуються локальним збором логів без подальшого централізованого аналізу, що значно ускладнює виявлення міжсистемних загроз. Водночас деякі установи починають впроваджувати рішення на базі ELK Stack та Wazuh [24], які дозволяють створювати власні SOC (Security Operations Center) з можливістю кореляції подій у реальному часі. Динаміка кіберінцидентів у період 2020-2025 років зображена у таблиці 1.2 та на рисунку 1.2.

Таблиця 1.2 – Динаміка кіберінцидентів в Україні

| Рік | Кількість зафіксованих інцидентів | Основні типи атак | Особливості року |
|---|---|---|---|
| 2020 | 820 | Фішинг, DDOS | Початок масових атак на державні вебпортали у період Covid-19 |
| 2021 | 1150 | Віруси, шкідливі вкладення, компрометація поштових систем | Зростання атак на МВС, мінфін, держпідприємства |
| 2022 | 2100 | Wiper-атаки, знищення даних, DDOS | Початок повномасштабної кібервійни проти України |
| 2023 | 2300 | Компрометація облікових записів, злам хмарних сервісів, APT | Атака на «Київстар», масштабні кампанії проти енергетики |
| 2024 | 2500 | Таргетовані фішингові кампанії, вразливості програмного забезпечення, соціальна інженерія | Активізація кібершпигунських угруповань, розвиток CSIRT-координації |

Порівняльний аналіз міжнародної статистики показує, що у більшості країн ЄС та США спостерігається тенденція до переходу від реактивного до

проактивного підходу у розслідуванні кіберінцидентів. Наприклад, у США завдяки впровадженню NIST Incident Response Framework [7] середній час реагування скоротився на 30%, а кількість успішно локалізованих інцидентів збільшилась. У країнах ЄС, відповідно до ENISA Cybersecurity Policy Implementation Guidelines [23], діє обов'язковий обмін індикаторами компрометації (IoC) між державними та приватними структурами, що дозволяє оперативно виявляти зв'язані атаки [25].

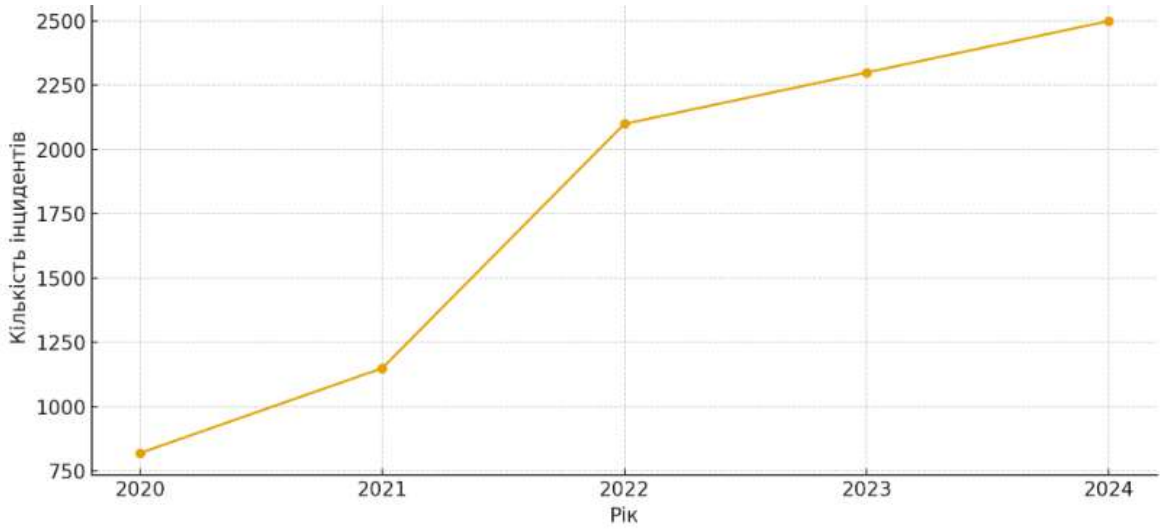


Рисунок 1.2 – Динаміка кількості кіберінцидентів в Україні

Графік показує різке зростання кількості інцидентів у 2022 році (переважно через ескалацію кібератак під час воєнних дій) та подальше зростання у 2023–2024 роках.

В Україні подібні механізми лише формуються. Спроби інтегрувати державні інформаційні системи у єдиний національний простір кіберобміну стикаються з технічними й організаційними обмеженнями. Зокрема, більшість державних структур не мають єдиної політики зберігання журналів подій, а формати звітності про інциденти різняться. Це призводить до складнощів у побудові комплексної картини атак, виявленні спільних індикаторів та визначенні джерела компрометації.

Незважаючи на позитивну динаміку у розвитку національної системи кіберзахисту, рівень зрілості процесів розслідування кіберінцидентів в Україні

залишається нижчим, ніж у країнах ЄС [3]. Відсутність повноцінної системи автоматизованого збору, зберігання та аналізу даних про інциденти, а також слабка інтеграція з міжнародними платформами обміну загрозами створюють передумови актуалізації розробки нового уніфікованого методу розслідування кіберінцидентів у державних інформаційних системах. Такий метод має враховувати сучасні стандарти ISO/IEC 27035 і NIST SP 800-61, забезпечувати централізоване управління розслідуванням, обмін даними між установами та підтримку інструментів цифрової криміналістики [4,7].

## 1.3 Огляд міжнародних стандартів та нормативної бази (ISO/NIST, законодавство України)

Сучасна система кіберзахисту критичної інфраструктури ґрунтується на поєднанні міжнародних стандартів, рекомендацій провідних організацій з інформаційної безпеки та національного законодавства. Основна мета цих документів – створити єдиний підхід до управління ризиками, реагування на кіберінциденти та забезпечення безперервності роботи інформаційних систем.

На міжнародному рівні ключову роль відіграють стандарти ISO/IEC 27000-серії, зокрема ISO/IEC 27001:2022 та ISO/IEC 27002:2022 [4,5], які визначають вимоги до створення, впровадження й підтримки системи управління інформаційною безпекою (ISMS). Вони встановлюють структуру для оцінки ризиків, планування заходів захисту, моніторингу ефективності та постійного вдосконалення процесів. Стандарт ISO/IEC 27035:2023 деталізує процедури управління інцидентами інформаційної безпеки – від виявлення до розслідування та відновлення [4,5]. Цей документ акцентує увагу на важливості документування всіх етапів реагування, а також створенні систематизованої бази інцидентів, що дозволяє накопичувати досвід для майбутнього аналізу.

Зі свого боку, Національний інститут стандартів і технологій США (NIST) пропонує методологічну основу для побудови процесів кіберзахисту. Документ

NIST SP 800-61 Rev.2 "Computer Security Incident Handling Guide" описує детальний цикл управління інцидентами: підготовка, виявлення, стримування, ліквідація та відновлення. Крім того, NIST Cybersecurity Framework (CSF) структурує роботу організацій за п’ятьма функціями – Identify, Protect, Detect, Respond, Recover, – що забезпечує гнучку інтеграцію безпекових процесів у бізнес-моделі будь-якого підприємства. Цей підхід широко використовується у США для критичної інфраструктури (енергетика, транспорт, зв’язок) та рекомендований до впровадження в країнах ЄС і НАТО [7,26].

Європейський Союз розвиває власну нормативну екосистему у сфері кіберзахисту. Центральним документом є Директива NIS2 (2022/2555/ЄС), що встановлює обов’язкові вимоги до кіберстійкості державних і приватних структур, зокрема вимоги до звітності про інциденти та обміну інформацією між національними CERT.

Агентство ENISA розробляє практичні керівництва, серед яких «Good Practice Guide for Incident Management» (2023), що містить рекомендації для організації реагування на інциденти на рівні держав і підприємств [13,27].

Україна поступово гармонізує національне законодавство з міжнародними стандартами. Основними нормативними актами є Закон України “Про основні засади забезпечення кібербезпеки України” №2163-VIII від 05.10.2017 [4] та Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” №80/94-ВР від 05.07.1994 [28,29]. Вони визначають основні принципи державної політики у сфері кібербезпеки, категорії об’єктів критичної інфраструктури, повноваження державних органів (зокрема ДССЗЗІ, CERT-UA) та порядок реагування на кіберінциденти.

Також важливим документом є Постанова Кабінету Міністрів України №518 від 19.06.2019, яка затверджує порядок реагування на кіберінциденти. Вона регламентує процедури фіксації, обліку, класифікації та повідомлення про інциденти безпеки в державних установах [30]. Методичні рекомендації CERT-UA (2024) деталізують технічні аспекти реагування, порядок аналізу цифрових артефактів, взаємодію з міжнародними партнерами та підготовку звітності [16].

Таким чином, нормативно-правова база у сфері кібербезпеки демонструє тенденцію до уніфікації з міжнародними практиками. Однак, попри формальну відповідність стандартам ISO та NIST, на практиці залишається потреба у створенні єдиного методологічного підходу до впровадження цих вимог в українських реаліях, особливо для об’єктів критичної інфраструктури [4,6].

## 1.4 Інструменти та платформи для розслідування кіберінцидентів

У сучасному світі складно уявити розслідування кіберінцидентів без цілої екосистеми інструментів, які допомагають фахівцям розібратися в тому, що насправді відбулося у комп’ютерній системі або мережі. Проблема в тому, що цифрові сліди можуть бути будь-де – у системних журналах, у тимчасових файлах, у пам’яті комп’ютера, навіть у мережевих пакетах, які пролетіли між пристроями за долі секунди. І щоб усе це побачити, правильно інтерпретувати та не переплутати, потрібно мати під рукою набір інструментів, які працюють разом і доповнюють один одного [31].

Коли говорять про розслідування кіберінцидентів, зазвичай починають саме з журналів подій. Це основа, яка дозволяє зрозуміти, що відбувалося в системі у певний момент часу. Проте сучасні системи генерують так багато логів, що людина просто не встигне все це перечитати – не те що проаналізувати. Саме тому однією з найважливіших платформ вважається ELK Stack. Це такий собі “центр збору всього”, який перетворює хаотичні текстові журнали на щось набагато структурованіше.

Зазвичай, коли пояснюєш про ELK, виглядає все досить просто: Elasticsearch [24] зберігає та шукає, Logstash збирає та чистить, а Kibana візуалізує [32]. Але насправді кожна з цих частин робить більше, ніж здається. Logstash, наприклад, може перетворювати дані з абсолютно різних джерел у єдиний формат – і це критично, бо журнали Windows, журнали Linux, логи мережі та записи антивірусів виглядають по-різному. А для розслідування треба бачити їх поруч, у єдиній

часовій послідовності. І саме ELK дозволяє побудувати цю “картину з пазлів”.

Поруч із ELK майже завжди працює Wazuh, який можна назвати “вухами та очима” всієї системи. Його агенти інсталюють на кожен пристрій, і вони фіксують буквально все: які файли створюються, які процеси запускаються, які з’єднання встановлюються. Усе це передається на центральний сервер, і саме завдяки цій інформації вдається зрозуміти, що в системі щось пішло не так [33].

Wazuh зручний тим, що він одразу підсвічує підозрілі дії. Наприклад, якщо програма намагається отримати привілеї суперкористувача – це вже сигнал. Або якщо раптом з’являється підключення на порт, яким у нормальному стані ніхто не користується. І хоча іноді ці “тривоги” бувають хибними, вони допомагають не пропустити реальну загрозу [33].

Далі йде інструмент, який не займається безпосередньо збором даних, але відіграє ключову роль у розслідуванні – платформа MISP для обміну інформацією про загрози. Скажімо, під час розслідування виявлений дивний файл, а ти не знаєш, що з ним робити. MISP дозволяє порівняти хеш цього файла з величезною базою відомих загроз: може, це частина якогось шкідливого програмного забезпечення (ПЗ), яке вже вивчали в іншій країні або в іншій організації [17]. Це надзвичайно важливо, бо атаки рідко бувають унікальними – у них часто повторюються техніки, інструменти, поведінка. Якщо є збіг, це може різко скоротити час розслідування.

Ще одна важлива річ – TheHive, система, яка дозволяє організувати усе розслідування “в одному місці”. У ній можна створювати справи, додавати докази, вести журнал дій, призначати завдання різним фахівцям [34]. Це допомагає не заплутатися і завжди бачити, на якому етапі розслідування ти зараз знаходишся.

Уявімо ситуацію: є багато подій, різні джерела логів, кілька аналітиків працюють над одним інцидентом. Без системи управління все це перетворюється на хаос. Саме тому TheHive має таку цінність – він структурує роботу, але не нав’язує “ідеальний” підхід, а дає свободу організувати все так, як зручно команді.

Платформи розслідування – це чудовий інструмент, але є ситуації, коли цього недостатньо. Наприклад, коли потрібно “витягнути” інформацію з оперативної пам’яті або знайти дані, які видалили, але які ще залишилися на диску. Тоді вже

потрібні спеціальні інструменти цифрової криміналістики.

Volatility – це фактично “мікроскоп” для оперативної пам’яті. Він дає змогу побачити процеси, які давно закрилися, але залишили сліди в RAM [30]. Часто саме там можна знайти залишки шкідливих програм, тимчасові дані, паролі або ключі шифрування, які ніколи не потрапили у журнали [35].

FTK Imager дозволяє створювати точні копії дисків, які можна вивчати без ризику зіпсувати оригінал. У криміналістиці це необхідно, бо будь-яка зміна оригіналу може зробити доказ недійсним [36].

Autopsy – зручний інструмент для перегляду файлової системи. З його допомогою можна знайти залишки видалених файлів, історію браузера, артефакти, про які користувач навіть не здогадувався [37].

І, звісно, Wireshark, який дозволяє побачити мережевий трафік у деталях. Часто саме там ховаються найцікавіші моменти: спроби підключення до зовнішнього сервера, передача підозрілих пакетів, неочікувані протоколи. Для досвідчених аналітиків Wireshark – це окремий всесвіт даних [38].

Загалом, у розслідуванні кіберінцидентів важливий не лише набір інструментів, а те, як вони працюють разом. Один збирає дані, другий аналізує, третій порівнює з відомими загрозами, четвертий допомагає організувати роботу команди. І ця взаємодія дозволяє побачити повну картину того, що сталося, навіть якщо події на перший погляд не пов’язані між собою.

Ще один момент, який варто згадати, – це створення тестових середовищ, або “кіберполігонів”, де можна моделювати атаки без ризику. Це дозволяє перевірити інструменти, знайти слабкі місця, відпрацювати сценарії реагування. У багатьох країнах такі полігони стали обов’язковою частиною кіберакадемій, і в Україні ця практика теж починає набирати обертів.

Проте, не усі сфери діяльності мають достатньо ресурсів для забезпечення достатнього захисту. Об’єкти критичної інфраструктури України, в більшості, державні об’єкти, не мають достатнього фінансування, що значно впливає на створення безпечних систем. Чисельність спеціалістів сфери захисту в організаціях, зазвичай, зводиться до мінімуму. Особливу увагу варто звернути

також на міста з невеликою чисельністю. Процес діджиталізації для багатьох спеціалістів став травмуючим, оскільки навчання персоналу не проводилось на достатньому рівні і як наслідок, велика кількість помилок у системах.

У підсумку, інструменти та платформи, які використовуються при розслідуванні кіберінцидентів, – це не просто програми, а цілісна система, де кожна частина займає своє місце. Вони допомагають зібрати інформацію, обробити її, порівняти з відомими загрозами та організувати роботу так, щоб розслідування було повним і точним. І хоча кожен інструмент сам по собі вже корисний, їхня справжня сила проявляється саме в тому, як вони працюють разом.

## 1.5 Постановка задачі

У межах цього розділу було проведено комплексний огляд сучасних методів, підходів та практик, що застосовуються під час розслідування кіберінцидентів у світі та в Україні. Аналіз показав, що кіберзагрози продовжують розвиватися швидше, ніж класичні інструменти захисту, тому процес реагування на інциденти не може базуватися виключно на традиційних засобах журналювання або окремих рішеннях для антивірусного контролю. Ефективне розслідування сьогодні – це поєднання автоматизованого збору подій, кореляції, поведінкового аналізу, цифрової криміналістики та оперативного залучення розвідувальної інформації про загрози.

Статистичні дані, розглянуті у підрозділі, підтвердили тенденцію до зростання кількості складних атак як у світі, так і в Україні. Більшість інцидентів пов’язана із цілеспрямованими кампаніями, що включають кібершпигунство, компрометацію ланцюгів поставок, використання соціальної інженерії. На фоні цього значно зростає роль структурованої реакції, стандартизованих методик і точного документування артефактів, що згодом стають ключем до встановлення причин і механізмів атаки.

У ході огляду міжнародних стандартів стало очевидно, що регуляторна база дедалі активніше спрямовує організації до впровадження процесного підходу. Особлива увага приділяється неперервності моніторингу, забезпеченню цілісності цифрових доказів та документуванню усіх дій під час реагування. Таким чином, стандарти не лише задають рамки, а й формують практичні орієнтири для побудови власних систем розслідування.

Загалом, проведений огляд підкреслює, що сучасне розслідування кіберінцидентів є багаторівневим процесом, який неможливо забезпечити одним інструментом чи однією методикою. Лише об'єднання моніторингу, інтелектуальної кореляції, загрозової розвідки та цифрової криміналістики у єдину узгоджену систему дозволяє побудувати ефективний цикл реагування [39].

Такий підхід формує основу для подальшої практичної частини роботи, де ці технології інтегруються у тестове середовище та демонструють свою реальну ефективність у моделюванні кіберінцидентів. У сучасних умовах цифровізації державного управління та функціонування критичної інфраструктури України, питання ефективного розслідування кіберінцидентів набуває особливої актуальності.

Щороку фіксується зростання кількості атак на державні інформаційні ресурси, енергетичні системи, транспортні вузли та телекомунікаційні мережі. Приклади масштабних інцидентів, таких як кібератака на «Київстар» у грудні 2023 року, демонструють, що навіть великі організації із сучасною інфраструктурою можуть зазнати суттєвих втрат унаслідок відсутності належно структурованого процесу розслідування та реагування.

У більшості випадків державні установи мають обмежені технічні засоби для аналізу подій безпеки, не використовують централізовані бази індикаторів компрометації та не інтегрують власні системи моніторингу з міжнародними платформами кіберобміну. Крім того, відсутність єдиного методу, що охоплює технічний, організаційний та процедурний рівні розслідування, ускладнює виявлення причин інцидентів і знижує якість реагування. Першою та основною проблемою більшості установ є застарілі системи та недостатнє фінансування та

обізнаність працівників.

З огляду на це, основна мета дослідження полягає у розробці комплексного методу розслідування кіберінцидентів у державних інформаційних системах, який би забезпечував уніфікацію етапів збору, аналізу, документування та реагування на події безпеки.

Варто зазначити, що до об’єктів критичної інфрастуркути належать і приватні підприємства, що ускладнює загальний процес реагування, оскільки, власники систем є власниками інформації.

Для досягнення поставленої мети передбачається розв’язання низки взаємопов’язаних наукових і практичних завдань. Насамперед необхідно провести системний аналіз існуючих підходів до управління інцидентами у сфері кібербезпеки, виявити їхні переваги та обмеження в контексті державного сектору та об’єктів критичної інфраструктури. Оцінити стан систем захисту.

Наступним етапом є побудова моделі процесу розслідування, яка враховуватиме специфіку функціонування критичних об’єктів – від моменту виявлення інциденту до етапу усунення його наслідків.

Розроблюваний метод повинен забезпечити можливість виявлення індикаторів компрометації у реальному часі, формування звітності у стандартизованому форматі, а також інтеграцію із системами раннього попередження та реагування на загрози.

Очікується, що впровадження такого підходу дозволить підвищити рівень захищеності державних інформаційних систем, скоротити час виявлення та усунення інцидентів, а також створити підґрунтя для побудови національної моделі управління кіберінцидентами, узгодженої з вимогами ЄС та НАТО [26].

# 2 МОДЕЛІ ТА МЕТОД ВИЯВЛЕННЯ ТА РОЗСЛІДУВАННЯ ЦІЛЕСПРЯМОВАНИХ АТАК НА ОБ'ЄКТИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

## 2.1 Формування моделі процесу реагування та аналізу інцидентів

У сучасному цифровому середовищі реагування на кіберінциденти є ключовим елементом системи управління інформаційною безпекою, особливо в контексті об'єктів критичної інфраструктури. З огляду на зростання кількості цілеспрямованих атак на державні установи, фінансові системи, енергетичні підприємства та телекомунікаційні мережі, традиційні підходи, орієнтовані лише на виявлення загроз, втрачають ефективність. Необхідним стає створення цілісної моделі реагування, яка охоплює увесь життєвий цикл кіберінциденту – від моменту його виявлення до аналізу наслідків і впровадження профілактичних заходів.

Розроблення такої моделі базується на міжнародних стандартах та рекомендаціях Європейського агентства з кібербезпеки ENISA, які визначають структурований підхід до управління інцидентами. Основна ідея полягає в тому, що процес реагування має бути не лише технічним, а й організаційно керованим – тобто охоплювати не лише інструменти виявлення, але й механізми комунікації, розподілу ролей, документування та постінцидентного навчання [13,23].

Побудова ефективної моделі передбачає створення взаємопов'язаних компонентів, які забезпечують збір і кореляцію даних, швидке прийняття рішень, централізовану координацію дій та аналітичну підтримку процесу реагування. Успішність функціонування системи залежить від низки базових принципів – таких як безперервність, автоматизація, верифікація інформації, стандартизація звітності та взаємодія між відомствами. Кожен із цих принципів визначає певну властивість моделі, без якої ефективна реакція на кіберзагрози неможлива.

Крім того, модель повинна враховувати специфіку українського кіберпростору, де об'єкти критичної інфраструктури мають різні рівні технологічної зрілості, неоднакову якість логування подій та обмежені кадрові ресурси. Це вимагає впровадження підходів, які дозволяють поєднати централізований контроль (через національні платформи, такі як CERT-UA) із

локальним управлінням інцидентами на рівні окремих організацій [3].

У результаті, визначено, що створення моделі процесу реагування має ґрунтуватися на низці основоположних принципів, які формують концептуальний каркас системи. Вони наведені у таблиці 2.1.

Таблиця 2.1 – Принципи побудови моделі реагування на кіберінциденти

| Принцип | Характеристика |
|---|---|
| Безперервність циклу | Реагування не завершується усуненням наслідків, а переходить у фазу вдосконалення процесів |
| Автоматизація процесів | Застосування siem і soar-рішень (зокрема Wazuh, Elk Stack) для зменшення часу обробки інцидентів |
| Ієрархічна побудова | Розподіл ролей і відповідальності між технічними, аналітичними та управлінськими рівнями |
| Верифікація даних | Забезпечення достовірності зібраних логів, артефактів і показників перед аналізом |
| Міжвідомча взаємодія | Налагодження інформаційного обміну між CSIRT/ISIRT-підрозділами, cert-ua та галузевими структурами |

Після визначення базових принципів побудови моделі реагування необхідно сформулювати чітку послідовність етапів, що охоплюють повний життєвий цикл кіберінциденту (рисунок 2.1).

У межах об’єктів критичної інфраструктури цей процес має бути системним, повторюваним і документованим. Його ефективність визначається не лише швидкістю виявлення загроз, але й здатністю організації здійснювати аналіз, відновлення та постінцидентне вдосконалення.

Міжнародні стандарти, зокрема ISO/IEC 27035:2023 та NIST SP 800-61 Rev.2, рекомендують багатофазний підхід до управління інцидентами, який включає підготовку, виявлення, оцінювання, реагування, відновлення та навчання [4,6].


Рисунок 2.1 – Процедура реагування на інциденти

У той час як ISO акцентує увагу на організаційних і процедурних аспектах, NIST зосереджується на технічній реалізації кожного етапу.

Для підвищення достовірності та оперативності реагування важливо забезпечити автоматизований збір артефактів, централізовану обробку логів та інтеграцію результатів аналізу у спільну базу знань, наприклад, за допомогою таких платформ, як MISP, TheHive або Wazuh. Це дозволяє створити екосистему, у якій кожен інцидент розглядається не ізольовано, а як частина загальної картини кіберзагроз. Основна увага приділяється не лише технологічним рішенням, але й процедурним аспектам – формуванню команд реагування, узгодженню каналів комунікації та стандартизації звітності.

Модель процесу реагування на кіберінциденти для об’єктів критичної інфраструктури може бути представлена у вигляді послідовності основних етапів, кожен із яких має власні цілі, завдання та очікувані результати. Узагальнена структура цього процесу наведена у таблиці 2.2.

Таблиця 2.2 – Основні етапи процесу реагування на кіберінциденти

| Етап | Характеристика |
|---|---|
| Підготовка | Формування політик, створення CSIRT-команди, налагодження каналів комунікації, підготовка інструментів і планів реагування |
| Виявлення та ідентифікація | Збір, аналіз і кореляція подій безпеки, визначення типу, масштабу й рівня критичності інциденту |
| Реагування | Локалізація інциденту, ізоляція скомпрометованих систем, усунення шкідливих компонентів і відновлення працездатності |
| Аналіз та звітування | Вивчення джерел загрози, аналіз шкідливих артефактів, складання технічних і управлінських звітів для керівництва |
| Відновлення та вдосконалення | Повернення систем до штатного режиму, оновлення політик безпеки, проведення тренінгів і оновлення баз індикаторів компрометації |

Ключовим моментом у розробленні процесної моделі є забезпечення зворотного зв’язку між етапами. Це означає, що кожен інцидент має не лише розслідуватися, а й аналізуватися з метою підвищення ефективності майбутніх заходів реагування. Таким чином формується цикл безперервного вдосконалення, який є невід’ємним компонентом сучасних систем кіберзахисту.

Важливим аспектом побудови ефективної моделі реагування є чітке визначення взаємодії між усіма компонентами системи кіберзахисту – від технічних засобів моніторингу до управлінських структур і зовнішніх партнерів. Успішне розслідування кіберінциденту неможливе без узгоджених комунікацій, швидкої передачі даних та формалізованих механізмів ескалації.

У міжнародній практиці наголошується на необхідності створення чіткої структури обміну інформацією, яка забезпечує простежуваність, достовірність та

своєчасність реагування.

Для об’єктів критичної інфраструктури така взаємодія має особливе значення, оскільки різні системи безпеки – моніторингові, аналітичні, управлінські – можуть функціонувати в ізольованих сегментах. Тому модель реагування повинна передбачати не лише технічну інтеграцію (через централізовані SIEM-платформи, такі як Wazuh або ELK Stack), але й організаційну узгодженість дій – зокрема, координацію між CERT-UA, галузевими CSIRT-командами, IT-службами підприємства та державними регуляторами.

Одним із ключових елементів цієї взаємодії є інформаційні потоки, які забезпечують обмін даними про події, індикатори компрометації, результати аналізу та звіти розслідувань. Дані потоки можуть бути як автоматизованими (через інтеграцію SIEM, IDS/IPS, SOC-платформ), так і ручними – у вигляді комунікацій між відповідальними підрозділами.

Для підвищення рівня прозорості та уніфікації процесу аналізу рекомендується використовувати стандартизовані формати даних, наприклад STIX/TAXII, які підтримуються системами MISP і TheHive.

Таблиця 2.3 узагальнює структуру інформаційних потоків та ролей учасників процесу реагування на кіберінциденти в межах моделі управління інцидентами.

Додатковим елементом ефективної моделі реагування є визначення рівнів зрілості процесу управління інцидентами, що дозволяє оцінювати готовність організації до протидії кібератакам. На початкових рівнях така система має реактивний характер – реагування відбувається лише після виявлення інциденту. На більш високих рівнях зрілості організація переходить до проактивного управління, коли події безпеки постійно моніторяться, а потенційні загрози прогнозуються за допомогою інтелектуальних систем аналізу.

Використання підходів на основі Machine Learning та Threat Intelligence дозволяє виявляти відхилення у поведінці мережі або користувачів ще до того, як вони призведуть до компрометації систем [40,41].

Таблиця 2.3 – Структура інформаційних потоків та взаємодії під час розслідування кіберінцидентів

| Джерело або учасник | Тип інформації | Призначення | Інструменти або платформи |
|---|---|---|---|
| Системи моніторингу (ids/ips, wazuh, elk stack) | Логи, попередження, сигнатури загроз | Виявлення та первинна ідентифікація інцидентів | Wazuh SIEM, ELK Stack, Suricata |
| Csirt або soc-команда | Аналітичні звіти, технічні індикатори, хеші, ip-адреси | Кореляція подій, визначення джерел атаки | Thehive, Cortex, MISP |
| Керівництво об’єкта критичної інфраструктури | Підсумкові звіти, оцінка впливу, рекомендації | Прийняття управлінських рішень, визначення пріоритетів реагування | Звіти SIEM, внутрішні аналітичні системи |
| Державні органи (cert-ua, держспецзв’язку) | Оповіщення про масштабні загрози, загальні індикатори | Координація дій між організаціями, попередження ескалації інцидентів | MISP, TAXII feeds |
| Підрядники або партнери | Дані про вразливості, оновлення пз, аналітика загроз | Зміцнення захисту спільних систем і сервісів | CVE база, Threat Intelligence Reports |

Ключовою особливістю сучасних процесів реагування є впровадження автоматизації через оркестрацію подій. Цей підхід забезпечує інтеграцію між різними засобами кіберзахисту – від SIEM-систем до аналітичних платформ, таких

як TheHive чи Cortex [42,43]. Автоматизовані сценарії дозволяють значно зменшити час між виявленням інциденту та його локалізацією, а також мінімізувати вплив людського фактора.

Завдяки стандартизованим інтерфейсам, зокрема REST API або TAXII, системи обміну інформацією можуть взаємодіяти з національними базами індикаторів компрометації, що забезпечує оперативне оновлення знань про нові загрози [43].

У процесі побудови моделі також важливим є забезпечення надійності та достовірності цифрових доказів, які збираються під час розслідування інцидентів. Ці дані можуть бути використані не лише для технічного аналізу, а й як доказова база у судових або дисциплінарних розслідуваннях. Тому під час збору артефактів необхідно дотримуватися принципів цифрової криміналістики – фіксації ланцюга зберігання (chain of custody), використання контрольних сум (наприклад, SHA-256) та забезпечення цілісності копій.

Застосування інструментів, таких як FTK Imager, Autopsy або Volatility, сприяє проведенню глибокого аналізу системної пам’яті, логів та файлових структур без ризику змінення оригінальних даних [35,36,37].

Окрім технічних аспектів, модель реагування має охоплювати управлінський рівень – розподіл ролей між учасниками процесу, порядок взаємодії із зовнішніми структурами та внутрішні механізми контролю. Для цього в організаціях створюються політики реагування на інциденти, де фіксуються алгоритми дій, відповідальні особи, пріоритети відновлення та критерії завершення розслідування.

Такі політики повинні узгоджуватися з державними документами, зокрема із Законом України «Про основні засади забезпечення кібербезпеки України» (№2163-VIII), який вимагає обов’язкового повідомлення про інциденти на об’єктах критичної інфраструктури до CERT-UA [28].

Додатковим чинником, який підвищує ефективність моделі, є навчання персоналу та проведення симуляційних тренувань (cyber range exercises). Регулярні навчальні сценарії, що моделюють реальні кібератаки, дозволяють перевірити готовність організації, уточнити процедури реагування та виявити слабкі місця в

комунікації між підрозділами.

Такі тренування вже давно практикуються у країнах ЄС за підтримки ENISA та в Україні на базі Держспецзв'язку у рамках програми підвищення кіберстійкості державних систем.

Побудова комплексної моделі реагування на кіберінциденти передбачає інтеграцію технічних, організаційних і правових складових. Вона повинна бути не лише технічною схемою дій, а й частиною загальної системи управління інформаційною безпекою підприємства. Така модель сприяє створенню єдиного цифрового простору безпеки, у межах якого обмін даними, аналіз інцидентів і постінцидентне вдосконалення утворюють безперервний цикл підвищення кіберстійкості об'єктів критичної інфраструктури.

## 2.2 Модель збереження та відновлення цифрових доказів

Під цифровими доказами в контексті кіберінцидентів та цифрової криміналістики розуміють будь-яку інформацію, що існує в електронній формі та має потенційну цінність для встановлення фактів, обставин, послідовності подій або ідентифікації осіб, причетних до події, що розслідується. Джерела цих доказів є надзвичайно різноманітними, охоплюючи не лише традиційні журнали подій (logs) операційних систем, серверів і робочих станцій, а й такі специфічні артефакти, як знімки оперативної пам'яті (RAM dumps), що містять волатильні дані, повні посекторні копії дисків (forensic images), детальні мережеві дампи, що фіксують комунікацію на рівні пакетів, файли системної конфігурації, а також ключі шифрування та метадані з хмарних сховищ, мобільних пристроїв та систем Інтернету речей (IoT).

Ключова, і найбільш небезпечна, особливість таких доказів полягає у їхній високій нестабільності та волатильності. На відміну від фізичних доказів, цифрові дані можуть бути легко, іноді навіть автоматично, змінені, безповоротно знищені або перезаписані внаслідок звичайної роботи операційної системи, відключення

живлення чи навіть через дії самого зловмисника, спрямовані на приховування слідів. Саме тому пріоритетом фахівців є вилучення найбільш волатильних даних у першу чергу, дотримуючись суворого порядку волатильності, щоб не втратити критичну інформацію, яка існує лише частки секунди.

З огляду на цю крихкість, критично важливо забезпечити бездоганний ланцюг збереження доказів (chain of custody). Цей процесуальний механізм є основою судової достовірності, оскільки він гарантує, що від моменту виявлення інциденту і до представлення результатів розслідування, жодна зміна, забруднення чи втрата даних не відбулася без детального документованого підтвердження. Кожен крок від вилучення до аналізу повинен бути зафіксований, а цілісність вилучених даних підтверджена за допомогою криптографічних хеш-функцій (наприклад, SHA-256 або SHA-512), які слугують унікальним цифровим відбитком доказу, що унеможливлює непомітну маніпуляцію.

Модель процесу збереження та відновлення цифрових доказів є складною методологією, яка передбачає послідовність чітко регламентованих дій, починаючи від фази ідентифікації та виявлення інциденту, переходячи до етапу колекції та збереження волатильних і постійних даних, а потім включаючи глибокий аналіз вилучених артефактів для реконструкції повної картини подій. Завершальні етапи передбачають документування усіх знахідок та презентацію висновків у зрозумілому та юридично обґрунтованому форматі. Ця модель успішно поєднує технічні процедури вилучення даних, суворі процесуальні вимоги до їхнього обліку та організаційні компоненти взаємодії між командами реагування, юристами та правоохоронними органами.

Процес починається з моменту, коли система моніторингу безпеки фіксує аномальну активність. Інцидент передається до чергової команди реагування, яка ініціює процедуру збору цифрових доказів. На цьому етапі важливо зупинити подальше поширення атаки, але водночас не порушити дані, які можуть бути корисними для аналізу.

На рисунку 2.2 представлено схему моделі роботи з електронними доказами.

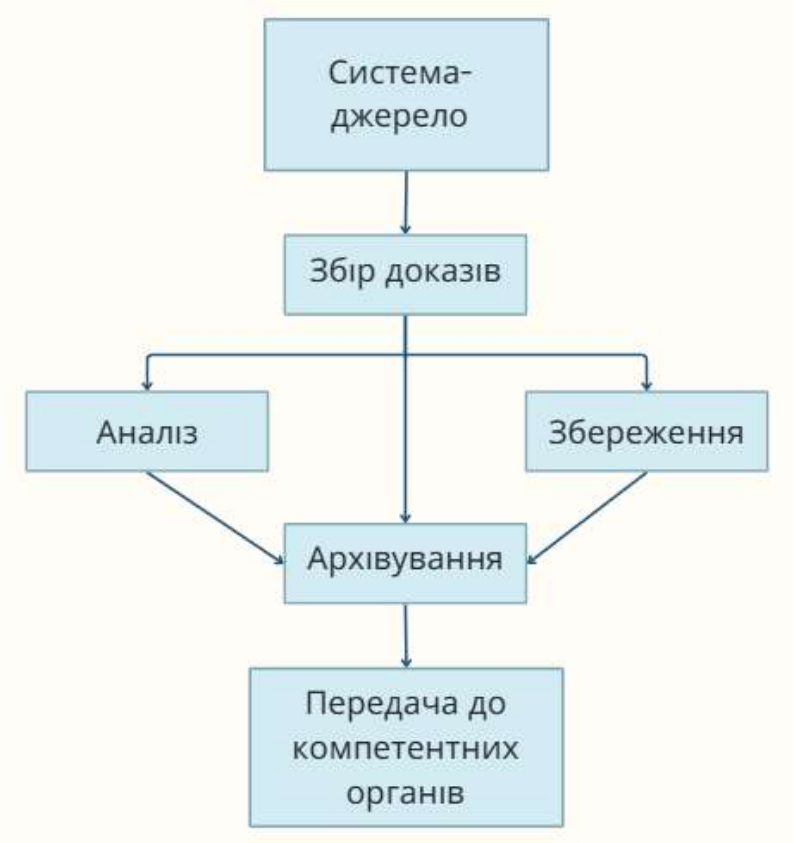


Рисунок 2.2 – Модель роботи з електронними доказами при розслідуванні кіберзлочинів

Етапи моделі збереження та відновлення цифрових доказів описані в таблиці 2.4.

Першим кроком є ідентифікація потенційних джерел доказів – це журнали системних подій, тимчасові файли, резервні копії, сесії користувачів, мережеві потоки, таблиці маршрутизації тощо.

Після визначення джерел виконується збір копій даних за допомогою спеціалізованих засобів, таких як FTK Imager або DD, які дозволяють створювати точні образи дисків без зміни оригінальних файлів. Для кожного створеного образу розраховуються контрольні суми (MD5, SHA-256), які фіксуються у протоколі збору доказів.

Таблиця 2.4 – Етапи моделі збереження та відновлення цифрових доказів

| Етап | Зміст процесу | Інструменти | Результат |
|---|---|---|---|
| Ідентифікація | Визначення джерел цифрових доказів (системні журнали, пам’ять, мережеві потоки) | Wazuh, elk stack | Список артефактів, що мають доказове значення |
| Збір | Отримання копій даних без змін оригіналу, фіксація контрольних сум | Ftk imager, dd, hashdeep | Цілісна копія цифрових доказів |
| Збереження | Архівація та зберігання даних у ізольованому сховищі з обмеженим доступом | Veracrypt, truenas | Гарантована недоторканість доказів |
| Аналіз | Вивчення отриманих даних для встановлення причин інциденту | Autopsy, volatility, wireshark | Виявлення слідів несанкціонованого доступу |
| Відновлення | Відтворення подій, файлової структури, сесій, мережевої активності | Autopsy, log2timeline | Повна картина кіберінциденту |
| Документування | Формування звіту для внутрішнього аудиту або правоохоронних органів | Thehive, misp, ms word | Офіційний звіт про результати розслідування |

Наступний етап – збереження цифрових артефактів. Для цього застосовуються ізольовані файлові сховища (наприклад, NAS або TrueNAS), до яких мають доступ лише уповноважені особи. Дані можуть бути додатково зашифровані з використанням VeraCrypt або сертифікованих засобів ДССЗЗІ України [10]. Важливо, щоб протягом усього часу зберігання доказів велося

журналювання доступів – хто, коли і з якою метою переглядав або копіював інформацію.

Після завершення етапу збереження розпочинається аналітична фаза, під час якої здійснюється реконструкція подій. Використовуючи інструменти Autopsy, Volatility, Wireshark або Log2Timeline [44], фахівці з цифрової криміналістики досліджують активні процеси, відкриті порти, часові позначки файлів, історію мережевих з'єднань тощо. Особливу увагу приділяють артефактам, що можуть свідчити про вторгнення: підозрілі виконувані файли, скрипти автозавантаження, несанкціоновані зміни реєстру або системних служб.

Процес відновлення полягає у реконструкції інформації, втраченої або зміненої внаслідок кібератаки. Для цього використовуються як автоматизовані інструменти, так і ручні методи аналізу. Наприклад, Autopsy дозволяє відновлювати вилучені або пошкоджені файли, відтворювати структуру каталогів, знаходити залишкові дані у файловій системі. Volatility Framework дає змогу проаналізувати дампи оперативної пам'яті, визначити активні процеси, сесії користувачів та підозрілі модулі.

Використання стандартизованих форматів даних (JSON, STIX, CSV) забезпечує сумісність між аналітичними платформами. Крім того, застосування централізованих репозиторіїв, таких як MISP, дозволяє інтегрувати отримані докази у загальну базу індикаторів компрометації для попередження повторних атак. Відновлення цифрових доказів на основі сформованої моделі сприяє не лише технічній реконструкції подій, а й побудові профілю атакуючого, визначенню векторів проникнення та оцінці ефективності наявних систем безпеки.

## 2.3 Модель взаємодії учасників розслідування кіберінцидентів у державних інформаційних системах

Модель взаємодії учасників розслідування кіберінцидентів у державних інформаційних системах передбачає чіткий розподіл функцій між суб'єктами

кібербезпеки, визначеними законодавством України, та узгоджену комунікацію між ними під час усіх етапів реагування.

Процес взаємодії починається на рівні об’єкта критичної інфраструктури, де виявляється інцидент інформаційної безпеки. На цьому етапі адміністратор безпеки або локальна CSIRT-команда фіксує аномалію, проводить первинний аналіз і формує повідомлення про інцидент відповідно до вимог Порядку реагування на кіберінциденти [45].

Далі інформація передається до галузевої CSIRT, яка здійснює технічну оцінку, кореляцію подій та виявлення можливих індикаторів компрометації. Цей рівень забезпечує централізований збір даних з декількох об’єктів однієї сфери (наприклад, енергетики, транспорту, освіти) [45,46].

У разі підтвердження масштабного або цільового інциденту повідомлення надходить до національного координатора – CERT-UA, який координує розслідування, надає методичні рекомендації та організовує взаємодію з Держспецзв’язку та СБУ.

CERT-UA аналізує отримані цифрові артефакти, формує узагальнені звіти про типи атак, використовувані індикатори компрометації, а також попереджає інші об’єкти критичної інфраструктури через систему обміну MISP.

На заключному етапі відбувається формування аналітичного звіту, який надсилається до Національного координаційного центру кібербезпеки при РНБО для оцінки рівня загрози національній безпеці та формування стратегічних рекомендацій [46].

Таким чином, модель взаємодії передбачає чотири рівні інформаційного обміну:

– локальний рівень – об’єкт критичної інфраструктури (виявлення, локалізація);

– галузевий рівень – координація CSIRT у межах відомства;

– національний рівень – централізована аналітика CERT-UA, координація з НКЦК;

– міжнародний рівень – обмін інформацією з ENISA, FIRST, InterCERT для відстеження глобальних кампаній атак.

Ця модель забезпечує не лише оперативне реагування, але й системне накопичення знань про інциденти, що у перспективі дозволяє вдосконалювати політики безпеки, проводити прогнозування загроз і формувати проактивну стратегію кіберзахисту державного сектору.

## 2.4 Розробка методу розслідування кіберінцидентів

У сучасних умовах активного розвитку цифрової економіки, зростання кількості кіберінцидентів та еволюції шкідливого програмного забезпечення, виникає нагальна потреба у створенні уніфікованого методу розслідування кіберінцидентів, орієнтованого на об’єкти критичної інформаційної інфраструктури. Висока складність таких систем, а також їх залежність від автоматизованих процесів керування, обумовлюють необхідність не лише реагувати на інциденти, а й забезпечувати належне збереження цифрових доказів, їх аналітичну обробку та подальше використання для запобігання подібним атакам у майбутньому.

Запропонований метод розслідування кіберінцидентів базується на принципах циклічності, комплексності та стандартизації. Його метою є створення послідовного алгоритму дій, який охоплює повний життєвий цикл інциденту – від виявлення ознак аномалії до формування висновків та рекомендацій щодо удосконалення безпеки інформаційних систем.

На відміну від традиційних підходів, орієнтованих на ізольований аналіз технічних артефактів, запропонована модель передбачає інтеграцію організаційних, процедурних і технічних компонентів у єдину систему реагування. Такий підхід дозволяє скоротити середній час реагування на інцидент (mean time to response), підвищити точність класифікації загроз і забезпечити узгодженість дій

між усіма суб’єктами кібербезпеки.

Метод передбачає, що розслідування кіберінцидентів здійснюється як послідовність етапів, де кожен має чітко визначену мету, вхідні та вихідні дані, набір застосованих інструментів і відповідальних осіб. У межах цієї роботи виділено п’ять основних етапів, що формують логічну структуру методу (рис 2.3).


Рисунок 2.3 – Загальна структура методу

Кожен етап має свій набір технічних засобів і програмних рішень, серед яких важливу роль відіграють платформи Wazuh, ELK Stack, MISP та TheHive, які інтегруються у єдине інформаційне середовище реагування.

Деталізація етапів приведена в таблиці 2.4.

Таблиця 2.4 – Етапи методу розслідування кіберінцидентів

| Етап | Основна мета | Ключові дії | Очікувані результати |
|---|---|---|---|
| Ідентифікація | Виявлення інциденту | Збір логів, аналіз SIEM, фіксація події | Первинне повідомлення |
| Класифікація | Визначення типу і пріоритету | Порівняння з базами IOC, оцінка ризику | Присвоєння рівня критичності |
| Технічний аналіз | Встановлення джерела та механізму | Форензичний аналіз, перевірка логів, реверс шкідливого ПЗ | Виявлення причин інциденту |
| Відновлення | Усунення наслідків | Відновлення даних, оновлення конфігурацій | Відновлена система |
| Документування | Збереження знань | Підготовка звіту, внесення в бази MISP | База знань для попередження атак |

На етапі ідентифікації інциденту проводиться збір інформації про потенційні події безпеки. Джерелами можуть бути: системні журнали, мережеві потоки, IDS/IPS системи, SIEM-платформи, або повідомлення користувачів. Основна мета полягає у виявленні аномалій, що виходять за межі типової поведінки мережі або користувачів.

Після фіксації події необхідно визначити, чи є вона дійсним кіберінцидентом, і встановити її критичність. Аналітик порівнює виявлені індикатори компрометації (IP-адреси, домени, хеші файлів) із записами в базі MISP – платформі обміну кіберзагрозами.

Додатково проводиться оцінка потенційного впливу за критеріями:

– масштаб порушення (локальний, корпоративний, національний);

– категорія активу, на який здійснено вплив (система керування, сервер, користувацька станція);

– наявність загрози безперервності бізнес-процесів.

На цьому етапі формується рішення, чи передати інцидент у розслідування або обмежитися моніторингом. Результатом класифікації є рівень пріоритетності реагування, який визначає ресурси, що будуть задіяні у подальшому.

Технічний етап є найбільш складним і ресурсомістким. Він охоплює збір та обробку цифрових артефактів, а також форензичний аналіз даних. Цей процес забезпечує встановлення механізму атаки, джерела компрометації та потенційних наслідків.

Ключова особливість полягає в тому, що під час аналізу цифрових доказів не допускається їх модифікація, тому робота проводиться з копіями (форензичними образами).

Після завершення аналізу формується ланцюжок подій, який відображає послідовність дій зловмисника. Це дозволяє побудувати причинно-наслідкову модель інциденту.

Етап відновлення передбачає усунення наслідків атаки та повернення систем до стабільного стану. Проводиться відновлення з резервних копій, перевірка цілісності баз даних, оновлення облікових записів користувачів, а також усунення вразливостей, через які було здійснено вторгнення.

Особливу увагу приділяють системам моніторингу, які вдосконалюються з урахуванням виявлених недоліків. Відновлення завершується перевіркою цілісності цифрових підписів, логів та сертифікатів безпеки.

Після усунення інциденту всі дії повинні бути задокументовані.

Формується звіт про розслідування (Incident Report), який містить:

– хронологію подій;

– опис знайдених артефактів;

– результати технічного аналізу;

– рекомендації щодо запобігання подібним подіям.

Дані про інцидент публікуються у MISP, що сприяє обміну інформацією між національними та галузевими CSIRT-командами. Зібрані індикатори надалі

використовуються для вдосконалення систем виявлення атак, а також для тренування персоналу на реальних кейсах.

Запропонований метод орієнтований на взаємодію автоматизованих систем і людського фактору. На архітектурному рівні він передбачає взаємодію таких компонентів:

– wazuh/elk stack, виявлення інцидентів, первинна обробка подій;

– thehive – управління кейсами, розподіл завдань між аналітиками;

– misp, обмін індикаторами компрометації, інтеграція з зовнішніми базами даних;

– forensic tools (autopsy, volatility, ftk imager), технічне підтвердження інциденту.

Таким чином, формується замкнутий цикл реагування, де кожен інцидент стає джерелом знань для вдосконалення політик безпеки.

Перевагами пропонованого методу є масштабованість, а саме те, що метод може застосовуватись як у державних органах, так і в комерційних структурах. Сумісність із міжнародними стандартами дозволяє інтегрувати його у національну систему кіберзахисту. Використання Wazuh та TheHive дозволяє зменшити вплив людського фактору та автоматизацію процесів. Кожне розслідування поповнює базу знань, яка використовується для навчання аналітиків [23]. Усі звіти мають єдину структуру, що спрощує взаємодію між командами реагування.

Запропонований метод розслідування кіберінцидентів є комплексною системою, яка забезпечує не лише технічне реагування на події безпеки, а й стратегічне управління кіберризиками. Його впровадження дозволяє створити єдиний стандарт дій для суб’єктів, що обслуговують об’єкти критичної інформаційної інфраструктури.

Метод забезпечує повну трасованість дій, прозорість збору доказів та підвищення ефективності реагування. Завдяки інтеграції інструментів відкритого коду, таких як Wazuh, MISP, TheHive та ELK Stack, він не потребує значних фінансових витрат і може бути реалізований у рамках державних або

корпоративних систем моніторингу безпеки.

Щоб метод розслідування кіберінцидентів вважався надійним і придатним до практичного застосування, необхідно не лише описати послідовність дій, а й обґрунтувати його ефективність кількісними показниками. Для цього пропонується багаторівневий підхід: розробка набору метрик, експериментальна перевірка на визначеній вибірці інцидентів, статистична оцінка результатів, встановлення порогів і правила прийняття рішень. Для оцінки методу пропонуються наступні метрики:

– *MTTD* (Mean Time To Detect) – середній час від початку інциденту до першого коректного сповіщення;

– *MTTR* (Mean Time To Respond) – середній час від сповіщення до початку коригувальних дій (ізоляція/локалізація);

– *Precision* – частка подій, позначених системою як інциденти, що дійсно були інцидентами;

– *Recall* – частка реальних інцидентів, які система виявила;

– *F*1-score – гармонічне середнє precision і recall;

– *FPR* (False Positive Rate) – частка нормальних подій, помилково відмічених як інциденти;

– *Coverage* (покриття інструментами), частка необхідних джерел логів (Windows Event, Sysmon, IIS, Netflow тощо), які реально збираються і аналізуються; відсоток автоматичних реакцій, частка інцидентів, де первинні виконані автоматично, без ручного втручання.

Розрахунок точності детекції *Precision* здійснюється за формулою:

$$Precision = \frac{TP}{TP+FP}, \quad (1)$$

де $TP$ – істинно-позитивні рішення (True Positive); $FP$ – хибно-позитивні рішення (False Positive).

Розрахунок чутливості *Recall* здійснюється за фомулою:

$$Recall = \frac{TP}{TP+FN}, \quad (2)$$

де $FN$ – хибно-негативні рішення (False Negative).

Розрахунок гармонічного середнього $F1$-score здійснюється за формулою:

$$F1 = 2 \times \frac{Precision \times Recall}{Precision+Recall}. \quad (3)$$

Розрахунок помилково відмічених подій $FPR$ здійснюється за формулою:

$$FPR = \frac{FP}{FP+TN}, \quad (4)$$

де $TN$ – істинно-негативні рішення (True Negative).

Експериментальна перевірка методу повинна охоплювати різноманітні типи інцидентів (фішинг, ransomware-like activity, lateral movement, web exploitation, data exfiltration).

Щоб оцінити метрики точності з допустимою похибкою $e$, визначають обсяг вибірки $n$ за формулою:

$$n = \frac{z^2 p(1-p)}{e^2}, \quad (5)$$

де $z$ – довірчий інтервал; $p$ – показник імовірності.

Припустимо, що потрібно оцінити *Recall* з похибкою $e$=0.05 (5%) на рівні довірчої інтервалу 95% ($z$=1.96). Найконсервативніший варіант за імовірності $p$=0.5 дає максимальний розмір вибірки.

За формулою 5 отримуємо:

$$n = \frac{1.96^2 \times 0.5 \times 0.5}{0.05^2} \approx 384.16 \approx 385.$$

Отже, для оцінки Recall з 5% похибкою потрібна вибірка ≈385 інцидентів. Якщо очікується вища (або нижча) реально спостережувана чутливість, замість $p$=0.5 можна підставити очікуване значення для зменшення $n$.

Припустимо, що під час тестування методу на N = 200 інцидентах отримано:

– *TP* = 150 (правильно виявлені інциденти);

– *FP* = 25 (визнані інцидентами нормальні події);

– *FN* = 25 (пропущені інциденти);

– *TN* = 3000 (зафіксовані нормальні події, не інциденти).

Розрахунки точності детекції та чутливості:

$$Precision = \frac{150}{150+25} = \frac{150}{175} = 0.857\ (85.7\%),$$

$$Recall = \frac{150}{150+25} = \frac{150}{175} = 0.857\ (85.7\%).$$

Розрахунок середнього та помилково відмічених подій:

$$F1 = 2 \times \frac{0.857 \times 0.857}{0.857+0.857} = 0.857,$$

$$FPR = \frac{25}{25+3000} = \frac{25}{3025} \approx 0.0083\ (0.83\%).$$

Метод слід вважати придатним, якщо валідаційні тести дають:

- *Precision* ≥ 0.75;
- *Recall* ≥ 0.80 (або бажано ≥ 0.85 для об’єктів критичної інфраструктури);
- *FPR* ≤ 1%;
- *MTTD* скоротився мінімум на 50% від базового рівня;
- *Coverage* ≥ 0.9 (тобто ≥ 90% критичних джерел логів підключено).

Ці пороги можуть бути адаптовані залежно від специфіки об’єкта (наприклад, критичні енергетичні системи – більш жорсткі вимоги).

Щоб зменшити *FP* і збільшити оперативність реагування, доцільно ввести бальну модель оцінки події. Кожному типу артефакта присвоюється вага wiw_iwi.

Порогові значення підбираються емпірично на тренувальній вибірці та перевіряються на тестовій.

## 2.5 Висновки

У другому розділі була сформована цілісна картина того, як саме має виглядати сучасний підхід до розслідування кіберінцидентів у державних інформаційних системах. Доведено, що це не окремі дії чи ізольовані технічні операції, а пов’язаний, багаторівневий процес, у якому кожен етап залежить від попереднього і критично впливає на кінцевий результат. Розслідування кіберінциденту розглядається як своєрідна хірургічна операція: вона вимагає не лише високоточних інструментів, але й чітко відпрацьованої, регламентованої послідовності дій.

Опрацьовані моделі реагування дозволяють побачити, що ефективність розслідування значною мірою визначається підготовленістю організації і здатністю команди безпеки швидко переходити від виявлення інциденту до аналізу, стримування та ліквідації наслідків. Замість реактивного гасіння пожежі, акцент робиться на проактивному та стратегічному підході. Ця послідовність і логічність дій забезпечують можливість не лише оперативно зупинити розвиток інциденту і мінімізувати збитки, а й зібрати максимально повну, незабруднену інформацію, яка стане основою для подальших висновків, незалежно від того, чи будуть вони використані для посилення захисту, чи для юридичного переслідування зловмисників.

Питання збереження цифрових доказів виявилося набагато більш складним і тонким, ніж може здаватись на перший погляд, оскільки воно стосується природи самих даних. Докази мають властивість швидко змінюватися або зникати внаслідок звичайної роботи системи, що вимагає від спеціалістів чіткого розуміння порядку волатильності даних – послідовності вилучення інформації від найбільш швидкоплинної (дані оперативної пам'яті, мережеві сесії) до найбільш постійної

(повні копії дисків). Процес фіксації потребує абсолютної чіткості, процедурної дисципліни та постійного підтвердження цілісності даних за допомогою криптографічних хеш-функцій. У цьому контексті критично важливим є дотримання ланцюга збереження доказів (chain of custody) — процедурної послідовності, яка забезпечує юридичну достовірність матеріалу, зберігаючи дані у тому вигляді, у якому вони можуть бути використані для подальшого технічного чи судового аналізу без жодних сумнівів щодо їхньої автентичності.

Модель взаємодії між учасниками розслідування показала, що комунікаційна складова є не менш значущою, ніж технічна. Інциденти, особливо у державних структурах, рідко стосуються лише однієї системи. Вони зачіпають кілька рівнів управління, різні підрозділи та зовнішні організації. Тому узгоджена взаємодія, своєчасний обмін інформацією і чіткий розподіл ролей формують основу для стабільної та прогнозованої роботи у разі масштабних або складних подій.

Розробка методу розслідування кіберінцидентів стала підсумком цього розділу. Метод об’єднує технічні інструменти, правила реагування та порядок роботи з даними, формуючи єдиний підхід, який можна застосовувати в умовах державного сектору. Його перевага полягає в тому, що він враховує як міжнародні стандарти, так і специфіку українських інформаційних систем, де рівень автоматизації, технічна база та організаційні можливості можуть суттєво відрізнятися.

У цілому зміст розділу дозволяє зробити висновок, що ефективність розслідування кіберінцидентів визначається не окремими інструментами, а їх взаємодією та здатністю працювати як єдиний механізм. Саме поєднання моделей реагування, процедур збереження доказів та системи взаємодії між суб’єктами створює основу для побудови надійного процесу, який відповідає сучасним вимогам кібербезпеки і може бути адаптований до реальних умов роботи державних інформаційних систем.

# 3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ

## 3.1 Побудова тестового середовища

Для проведення дослідження було створено окреме тестове середовище, що імітує базову структуру корпоративної інфраструктури з системою моніторингу безпеки та робочою станцією користувача. Архітектура складалася з двох віртуальних машин, об’єднаних у спільну мережу, розгорнутих у віртуальному середовищі VMware [47]. Така конфігурація дозволяє однаково ефективно моделювати взаємодію нападника та цільової системи, зберігаючи необхідний рівень контролю над середовищем та мінімізуючи вимоги до апаратних ресурсів.

Kali Linux – серверна частина, на якій були розгорнуті компоненти для збору, індексації та аналізу журналів подій (Elasticsearch, Cassandra, TheHive 4). Окрім того, ця машина була і нападником [48,49,55].

Windows 10 із набором FLARE VM – клієнтська машина, що генерувала події та telemetry рівня Sysmon, які надсилалися до серверної частини для подальшого аналізу [50].

Таке розділення дозволило створити середовище, близьке до реальних умов роботи SOC або лабораторії з цифрової криміналістики. Серверна машина відповідала за централізований збір і аналіз даних, тоді як Windows виступала джерелом потенційно шкідливої активності, яка могла бути зафіксована та використана для формування інцидентів.

У ролі атакуючої системи застосовано Kali Linux, який надає багатий набір утиліт для проведення легітимного тестування безпеки та моделювання дій зловмисника. На Kali налаштовано основні інструменти для розвідки і генерації мережевої активності, причому акцент ставився на використанні контрольованих, «безпечних» сценаріїв, що не включають розповсюдження шкідливих бінарних файлів поза межі лабораторії. Симуляції завжди виконуються з явною метою створити репрезентативні патерни поведінки – наприклад, портсканування, формування нестандартних з’єднань або запуск benign-скриптів, які залишають відбиток у системних журналах Windows. Такий підхід дозволяє відтворити етапи

атаки без етичних і правових ризиків, зберігаючи аналітичну цінність отриманих подій.

Цільовою системою виступає Windows 10 із комплексом інструментів FLARE, що забезпечує можливості глибокого збору телеметрії та форензичного дослідження. На цій машині інстальовано Sysmon для детального логування запусків процесів, мережевих підключень, створення файлів та змін у реєстрі; наведення правил конфігурації Sysmon здійснюється з урахуванням потреб дослідження, щоб отримувати інформативні, але не надмірні журнали.

Додатково був інстальований набір FLARE-інструментів, серед яких присутні утиліти для статичного та динамічного аналізу виконуваних файлів, засоби знімання пам’яті та образів диска, а також програми для роботи з журналами Windows. Ця конфігурація дозволяє фіксувати як явні, так і приховані прояви тестової активності, формуючи багатошарову картину інциденту.

Організація процесу збору доказів спроектована таким чином, щоб мінімізувати зміну стану досліджуваної системи під час аналізу. Перед початком активності виконуються снепшоти обох машин, а під час розслідування здійснюється послідовне знімання пам’яті та експортування логів Sysmon із подальшим хешуванням артефактів для підтвердження цілісності. Аналіз пам’яті і статичний аналіз потенційних зразків проводяться в окремому ізольованому середовищі FLARE із дотриманням заходів безпеки.

Таймлайн інциденту формується на основі поєднання мережевих слідів, записів Sysmon та знімків стану системи; у ньому відображається хронологія ключових подій, що дозволяє відтворити сценарій проникнення, встановлення персистентності та спроби ексфільтрації [51].

Winlogbeat збирав ці події і передавав їх у Elasticsearch, що розгорнутий на Kali Linux. Elasticsearch індексував події у вигляді структурованих документів, дозволяючи швидко здійснювати пошук, аналіз і фільтрацію. TheHive 4 отримував доступ до цих індексів та забезпечував можливість створювати інциденти, аналізувати артефакти та виконувати розслідування [52,53].

Особлива увага приділена документуванню та відтворюваності

експериментів. Кожне відтворення сценарію супроводжується фіксацією вхідних параметрів, версій встановленого ПЗ, часових міток та команд, що виконувалися. Такий підхід не тільки підвищує наукову валідність результатів, а й дозволяє в подальшому використовувати отримані артефакти для налаштування більш складних середовищ або для інтеграції із зовнішніми SIEM-системами.

Компактність лабораторії з двома машинами робить її зручною для демонстрації в межах магістерської роботи, враховуючи обмеження апаратних ресурсів та необхідність оперативної підготовки експериментів, при цьому зберігаючи всі ключові можливості для дослідження поведінки нападника і розслідування інцидентів на кінцевій точці.

Після розгортання Kali Linux у віртуальному середовищі відбувається налаштування основних компонентів, необхідних для подальшого аналізу мережевої активності та моделювання кіберінцидентів [49].

Kali за замовчуванням містить значний набір інструментів, однак для коректної роботи лабораторного стенду потрібно активувати мережеві служби, перевірити доступність інтерфейсів та оновити системні пакети. У першу чергу виконується ініціалізація мережі. За допомогою стандартних команд користувач перевіряє, чи отримала система IP-адресу від віртуального маршрутизатора, визначає параметри мережевого інтерфейсу та переконується, що віртуальна машина коректно взаємодіє з підмережею тестового середовища (рис 3.1).

На цьому етапі відбувається базова діагностика маршрутизації та перевірка здатності системи генерувати мережеві пакети. Якщо мережа функціонує коректно, інструмент ping демонструє стабільну затримку та відсутність втрат пакетів, що підтверджує працездатність віртуальної інфраструктури.

Основою середовища став Docker. Установка виглядала стандартно:

- *sudo apt update;*
- *sudo apt install -y docker.io docker-compose;*
- *sudo systemctl enable --now docker.*

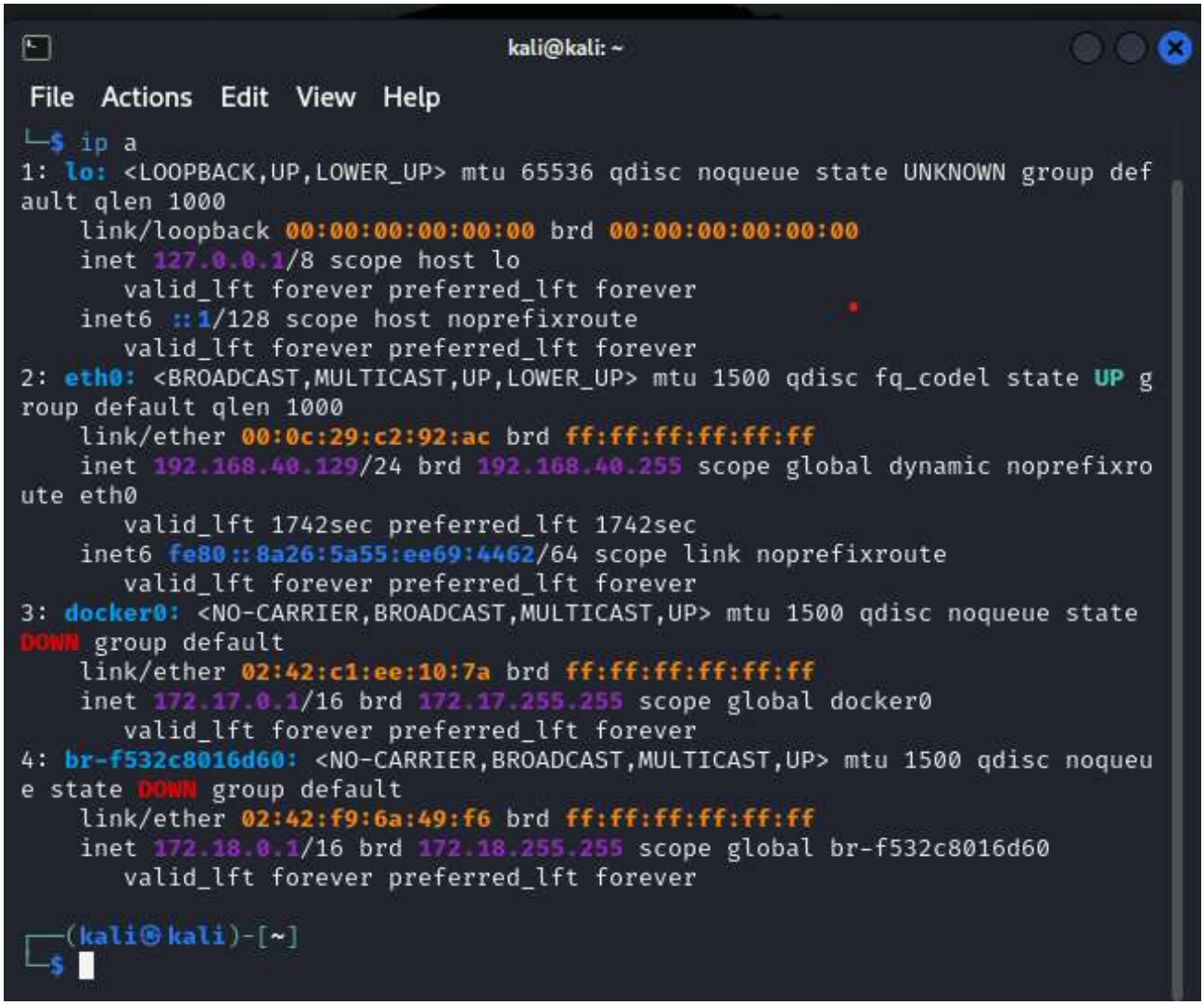


Рисунок 3.1 – Перевірка ip

Під проєкт було створено окремий каталог:

– *mkdir ~/thehive4-stack;*

– *cd ~/thehive4-stack.*

У каталозі сформовано docker-compose.yml, що включав три сервіси:

– Elasticsearch 7.17.9;

– Cassandra 3.11;

– TheHive 4.1.23.

Композиція запускалася так (рис 3.2): *sudo docker-compose up -d.*

Після успішного старту перевірка статусу виконувалася командою (рис3.2): *docker ps.*

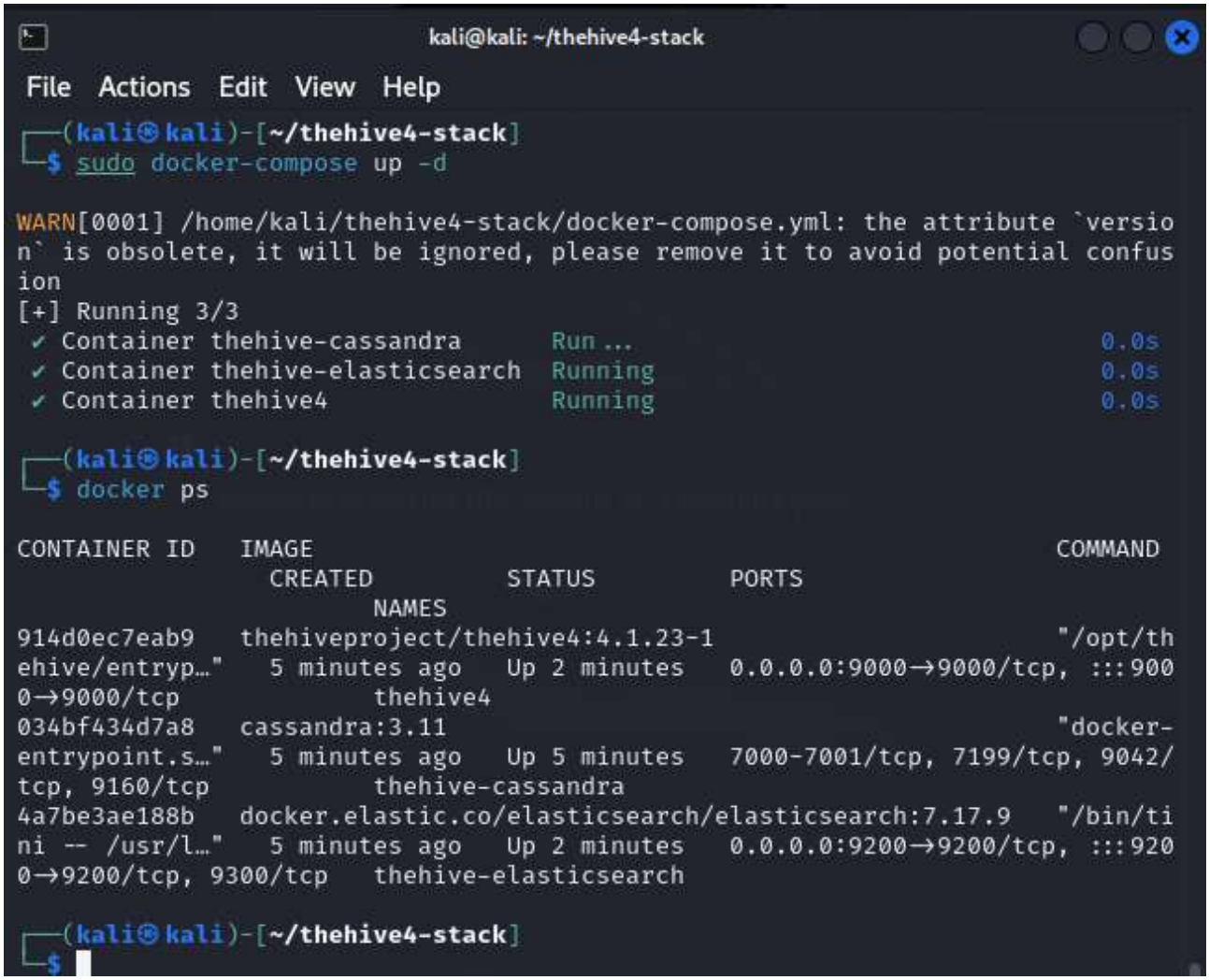


Рисунок 3.2 – Перевірка роботи TheHive

У результаті середовище запускалося з нуля за лічені хвилини, що стало суттєвою перевагою порівняно з традиційною установкою.

TheHive ставав доступним на Kali за адресою: http://192.168.40.129:9000 (рис 3.3).

Після завершення налаштування Kali Linux необхідним етапом у формуванні повноцінного тестового середовища є підготовка робочої станції на базі Windows 10, яка в моделі розслідування виконує роль цільової системи. Її використання дозволяє наблизити експериментальні умови до реальних, оскільки більшість корпоративних мереж, включно з об’єктами критичної інфраструктури, функціонують саме на ОС Windows.

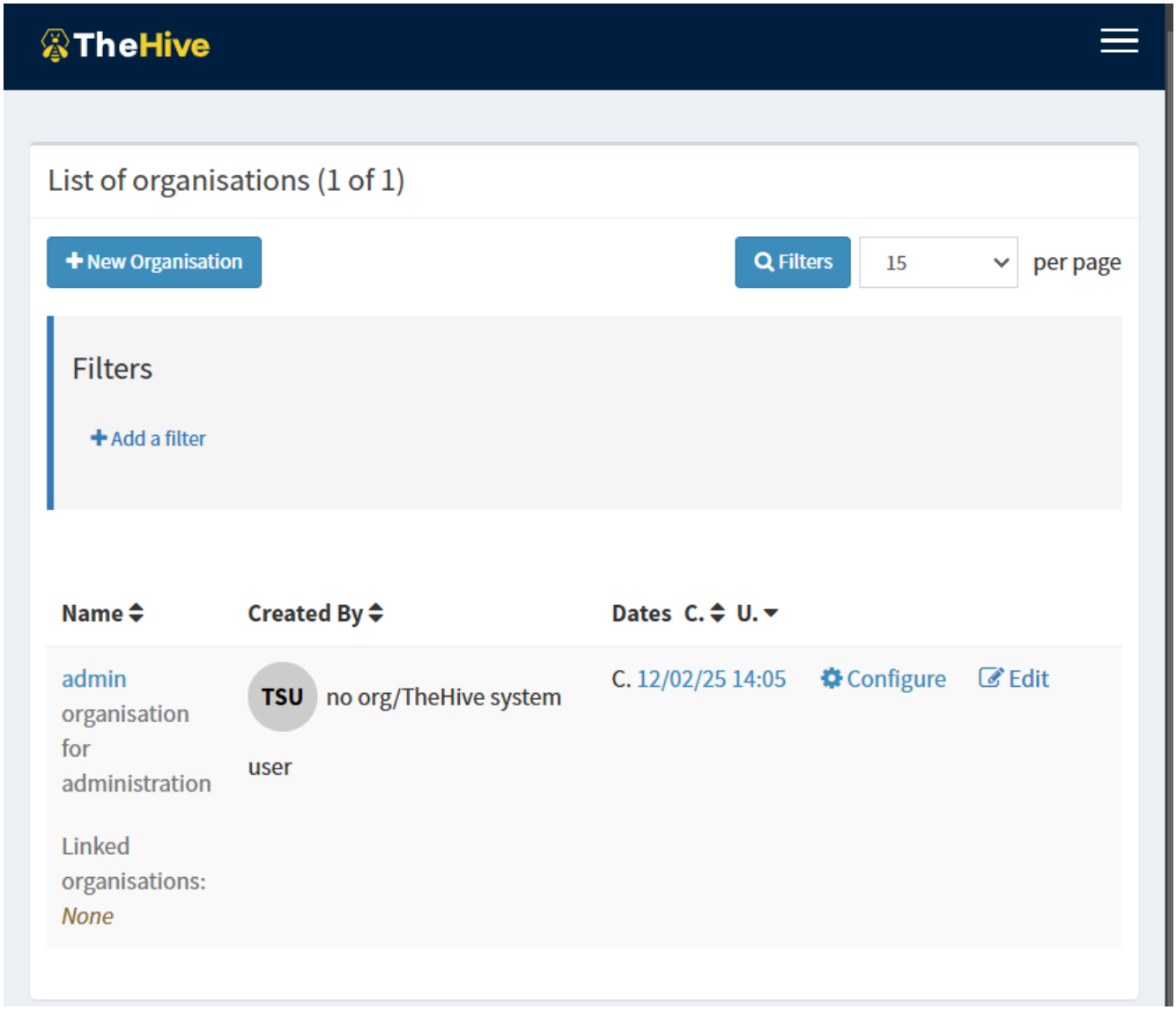


Рисунок 3.3 – Робоче середовище TheHive

На першому етапі здійснюється перевірка системи, оновлення компонентів та активація необхідних служб, що забезпечує стабільність та коректну роботу інструментів для фіксації та аналізу дій потенційного зловмисника.

Установлення інструментів починається з налаштування пакету Windows Sysinternals Suite, який є базовим набором утиліт для моніторингу процесів, мережевої активності та змін у системі. Цей пакет не потребує інсталяції у класичному розумінні, проте його запуск забезпечує доступ до таких компонентів, як Process Explorer, TCPView, Autoruns (рис 3.4) та інші інструменти, що дозволяють детально відстежувати активність у системі.

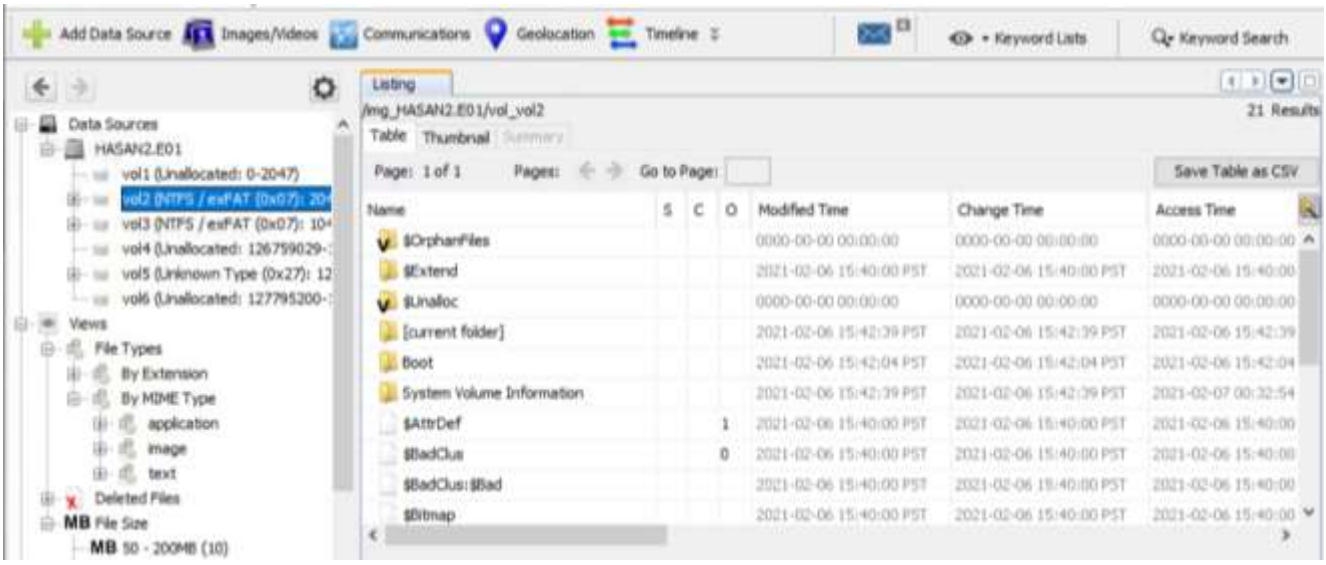


Рисунок 3.4 – Робота Autopsy

Оскільки частина експериментів передбачає аналіз фонових процесів після моделювання атаки, Sysinternals відіграє ключову роль у фіксації змін в операційному середовищі.

Наступним етапом є інсталяція Wireshark – мережевого аналізатора, що дозволяє досліджувати трафік, який надходить до Windows машини під час атаки. Його використання дає можливість переглядати структуру пакетів, визначати порти взаємодії та виявляти сліди сканування або несанкціонованого доступу (рис 3.5).

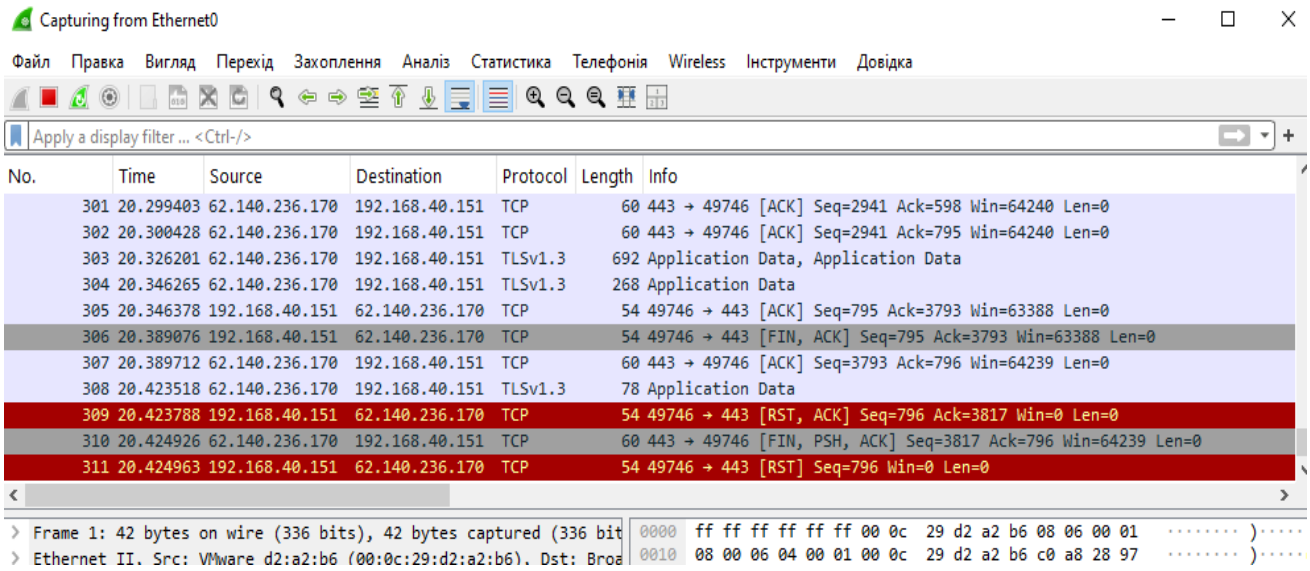


Рисунок 3.5 – Робота Wireshark

Після встановлення проводиться первинне налаштування інтерфейсів, у тому числі активація драйвера WinPcap або Npcap, що забезпечує можливість перехоплення трафіку навіть на рівні низькорівневих мережевих подій.

Для збору та аналізу журналів подій використовується Windows Event Viewer, який є вбудованим компонентом системи. На цьому етапі активуються додаткові категорії логування, включно з подіями PowerShell, мережевими з'єднаннями, входами в систему та змінами в службах. Розширений рівень логування є критично важливим для подальшої реконструкції послідовності дій зловмисника під час моделювання інциденту.

Одним із ключових елементів підготовки Windows-машини є встановлення FTK Imager. Цей інструмент використовується для створення форензічних копій дисків, каталогів або окремих файлів із гарантією незмінності цифрових доказів. На етапі інсталяції визначаються каталоги збереження образів, налаштовуються алгоритми хешування (MD5, SHA-1, SHA-256), що дозволяє забезпечити подальшу доказову цінність отриманих даних.

У дослідницькому середовищі FTK Imager відіграє роль інструмента фіксації стану Windows-системи до та після моделювання атаки, що дозволяє порівняти зміни у файловій структурі та реєстрі.

Завершальним етапом підготовки Windows 10 є встановлення додаткових інструментів, орієнтованих на цифрову криміналістику, таких як Autopsy, LogParser та PowerShell-скриптів для збору артефактів. Використання цих засобів забезпечує можливість глибокого аналізу після атаки, включно з відновленням видалених файлів, аналізом тимчасових директорій, визначенням часу доступу до об'єктів та дослідженням поведінки користувачів.

Після завершення встановлення формується повноцінне робоче середовище, здатне обробляти події безпеки, отримувати дані з мережевих журналів та зберігати цифрові докази для подальшого розслідування.

Для розгортання платформи розслідування кіберінцидентів було використано окремий сервер на базі операційної системи Ubuntu Server 20.04 LTS, що забезпечує стабільність роботи, сумісність із компонентами Wazuh та офіційну

підтримку з боку розробників. Попередня підготовка системи є важливим етапом, оскільки саме від коректності первинної конфігурації залежить працездатність усіх подальших модулів, включно з менеджером, індексером та веб-панеллю керування.

Після встановлення операційної системи (рис 3.6) було виконано оновлення базових системних компонентів. Це необхідно, оскільки Wazuh використовує сучасні криптографічні механізми, а застарілі версії бібліотек можуть викликати помилки залежностей.

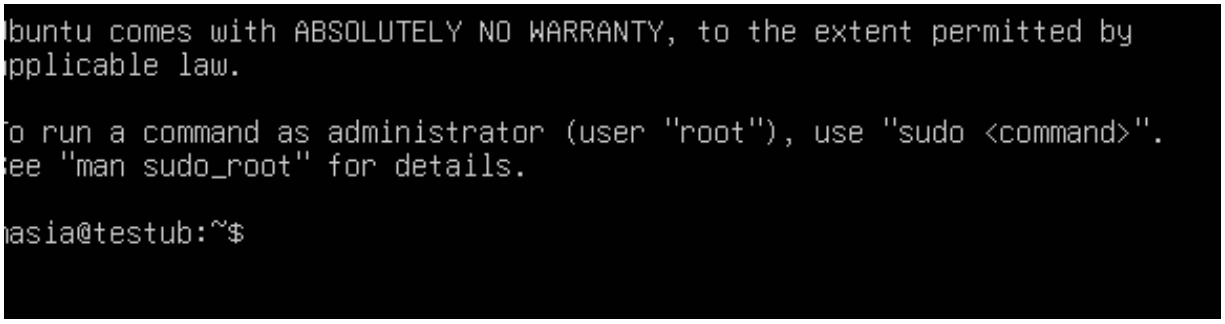


Рисунок 3.6 – Сервер Ubuntu

Wazuh не міститься в стандартних пакетах Ubuntu, тому перед інсталяцією потрібно вручну додати репозиторій. Wazuh Indexer (на базі OpenSearch) є критично важливим елементом, оскільки саме він забезпечує зберігання подій безпеки, журналів та результатів кореляції (рис 3.7) [33]: *sudo systemctl status wazuh-indexer.*


Рисунок 3.7 – Перевірка стану Wazuh-indexer

Wazuh Manager обробляє всі події, виконує кореляцію, генерує алерти та

здійснює логічний аналіз отриманих даних (рис 3.8): *sudo systemctl status wazuh-manager.*

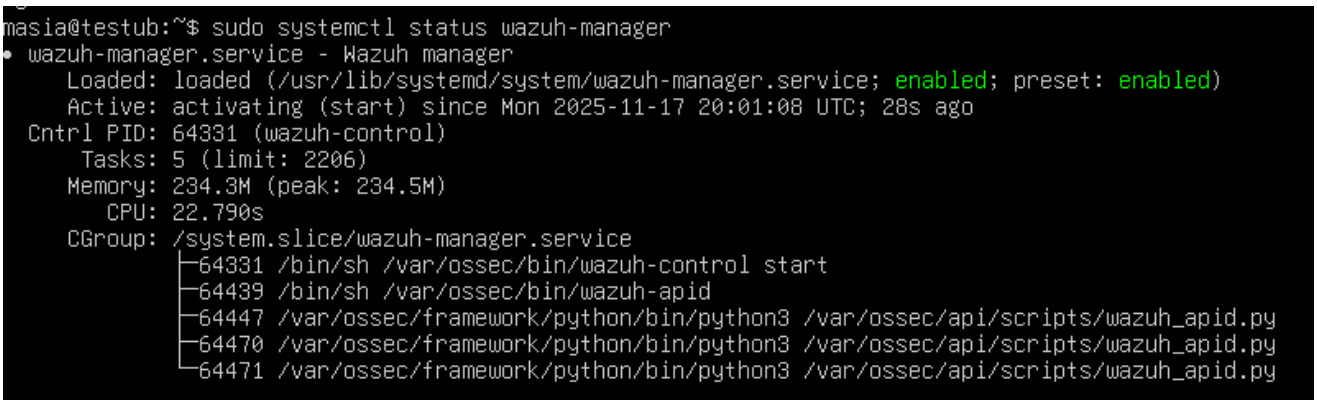


Рисунок 3.8 – Перевірка Wazuh-manager

Dashboard – це веб-інтерфейс, який дозволяє переглядати події, статус агентів, виконувати аналіз, працювати з MITRE ATT&CK та цифровими доказами [54].

Windows-машина у стенді виконувала роль джерела подій. Вона мала генерувати реальні артефакти, характерні для шкідливих дій або внутрішньої активності користувача. Вибір FLARE VM пояснюється її орієнтованістю на реверсинг, аналіз загроз і роботу з підозрілими виконуваними файлами.

Sysmon (рисунок 3.9) було обрано як основне джерело телеметрії, тому що він здатен фіксувати події на дуже низькому рівні. До вигляду системи Sysmon працював у фоновому режимі, фіксуючи кожен створений процес, мережеве з’єднання, зміну файлу або запуск скрипта.

Після встановлення Sysmon почав генерувати події у спеціальному журналі: microsoft – windows – sysmon – operational (рис 3.9, 3-10).

Щоб події Windows були доступні для аналізу на стороні Kali, було використано Winlogbeat –легкий агент від Elastic, який створений саме для експорту Windows-журналів у Elasticsearch [51,52].

У конфігураційному файлі winlogbeat.yml були визначені всі журнали, які потрібно передавати. Це дозволило отримати достатньо широкий спектр подій як для інцидент-аналізу, так і для криміналістичних досліджень.

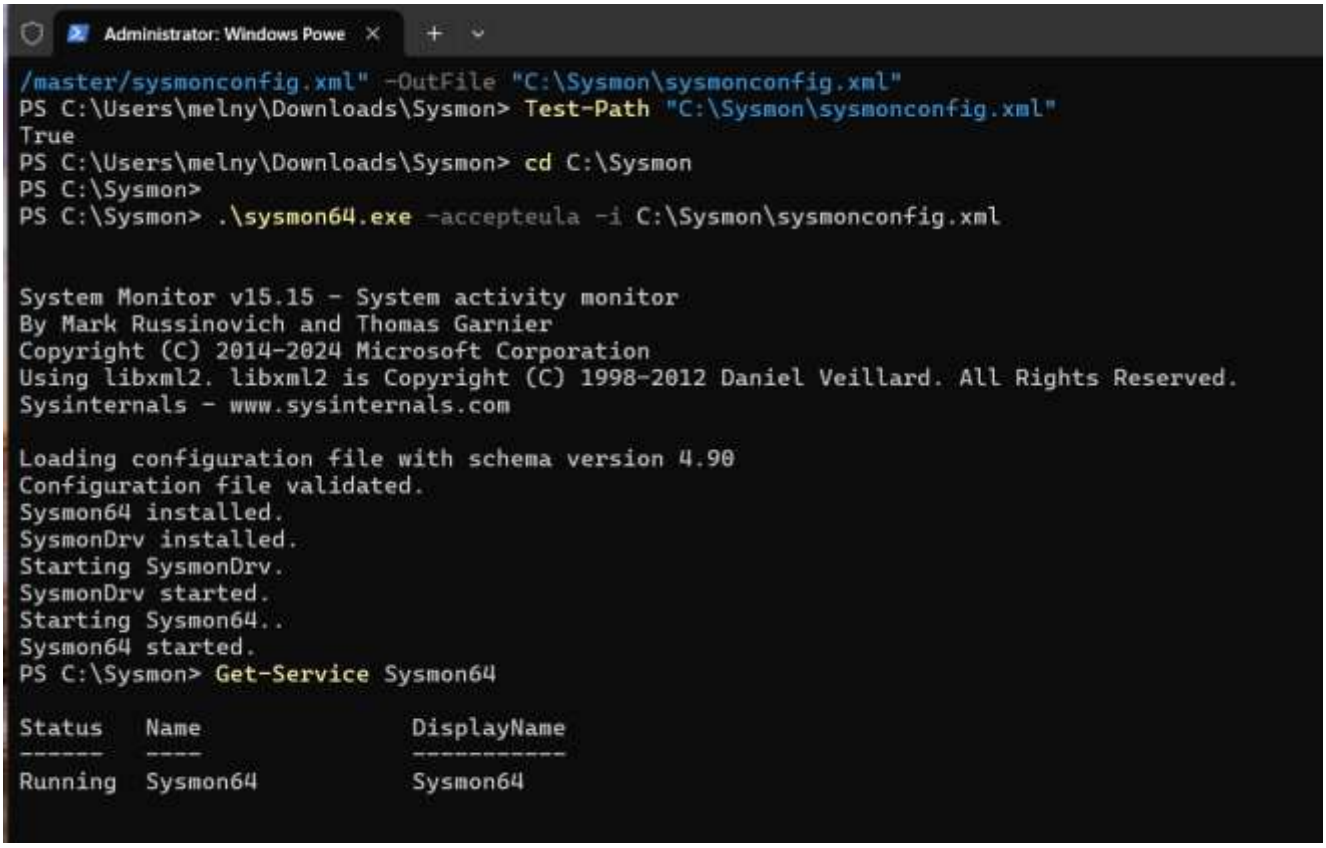


Рисунок 3.9 – Встановлення Sysmon

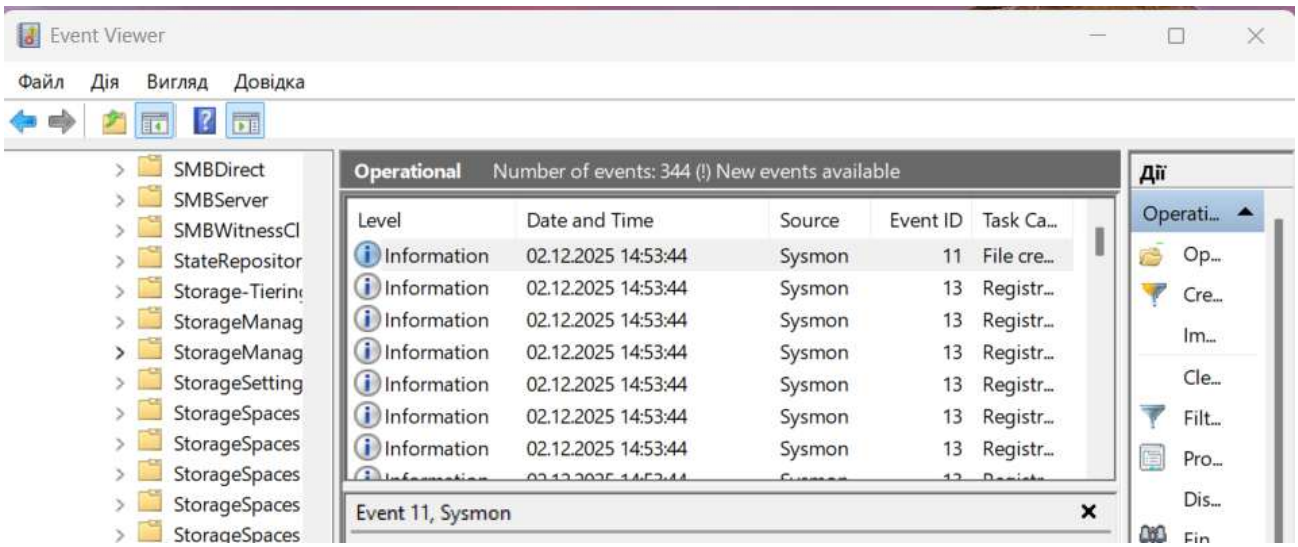


Рисунок 3.10 – Перевірка роботи Sysmon

Для встановлення Winlogbeat як сервісу потрібно виконати PowerShell-скрипт install-service-winlogbeat.ps1. Після цього сервіс Winlogbeat запускався і починав надсилати всі події з Windows у Elasticsearch (рис 3.11).

```
PS C:\winlogbeat\winlogbeat-7.17.9-windows-x86_64> Set-ExecutionPolicy -Scope Process
PS C:\winlogbeat\winlogbeat-7.17.9-windows-x86_64> .\install-service-winlogbeat.ps1

Status   Name               DisplayName
------   ----               -----------
Stopped  winlogbeat         winlogbeat


PS C:\winlogbeat\winlogbeat-7.17.9-windows-x86_64> Start-Service winlogbeat
PS C:\winlogbeat\winlogbeat-7.17.9-windows-x86_64> Get-Service winlogbeat

Status   Name               DisplayName
------   ----               -----------
Running  winlogbeat         winlogbeat


PS C:\winlogbeat\winlogbeat-7.17.9-windows-x86_64>
```

Рисунок 3.11 – Встановлення Winlogbeat

Тепер коли система налаштована та повністю працює можна переходити до наступного етапу, а саме реалізації методу.

## 3.2 Реалізація методу

Коли інфраструктура була готова, наступним кроком стала імітація атаки. Метою було не просто запустити підозрілий файл, а відтворити кілька типових дій зловмисника, які часто зустрічаються у реальних інцидентах. На Windows-машині було створено файл mal.exe у директорії користувача (рисунок 3.12). Це не був шкідливий файл у буквальному сенсі, його завданням було спровокувати роботу Sysmon та продемонструвати, як поведінкові події відображаються в системі.

```
PS C:\Users\melny> echo "test" > C:\Users\melny\mal.exe
PS C:\Users\melny> powershell -Command "(Get-Item 'C:\Users\melny\mal.exe').Cr
eationTime=('01 January 2010 10:00:00')"
PS C:\Users\melny> Start-Process "C:\Users\melny\mal.exe"
```

Рисунок 3.12 – Тестовий шкідливий файл

Далі, для імітації приховування слідів, було змінено час створення файлу – класична техніка timestomping. Sysmon негайно зафіксував цю зміну як подію з

кодом 2, що відображає зміну file creation time. Саме такі артефакти в реальних інцидентах дозволяють зрозуміти, що хтось намагався маскувати діяльність.

Після цього файл був запущений вручну, і Sysmon створив подію ProcessCreate (код 1), де чітко видно батьківський процес, командний рядок, користувача, шлях до файла і його хеш. Це дозволило побачити стартовий ланцюг атаки та процес, який стоїть за нею (рис 3.13).

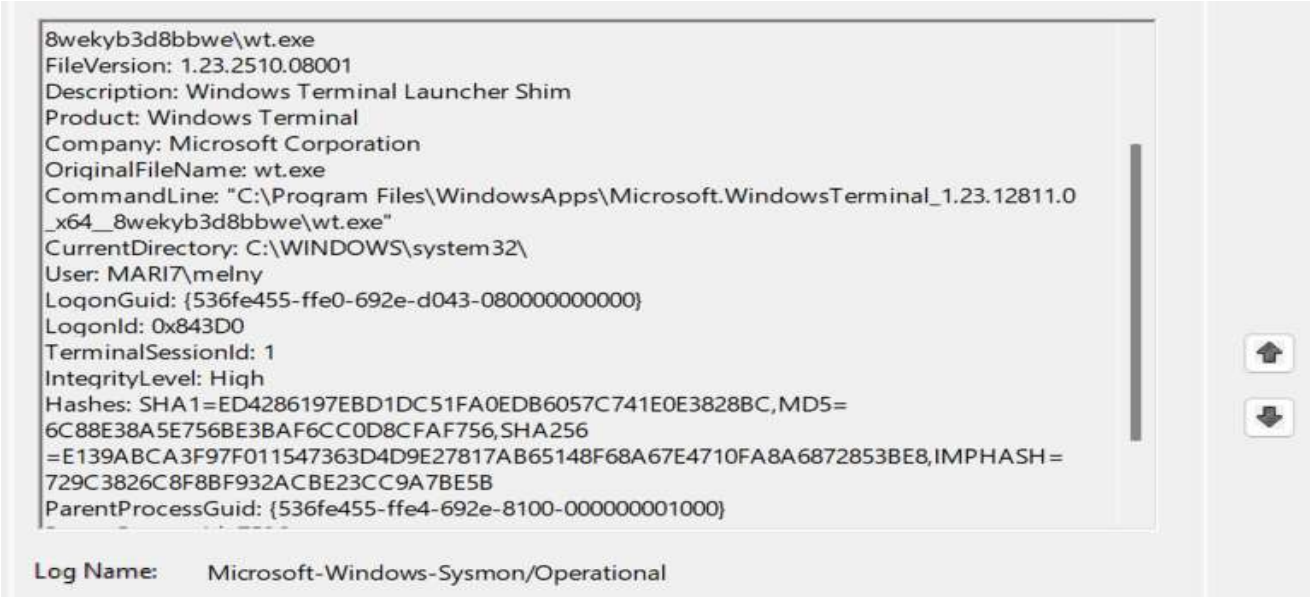


Рисунок 3.13 – Перегляд подій Sysmon

Щоб додати реалістичності, було ініційовано PowerShell-команду з обходом ExecutionPolicy – ситуація, яка часто зустрічається у практиці fileless-атак. У поєднанні з мережевим викликом це створювало класичний шаблон поведінки зловмисника: запуск файлу, виконання додаткової команди, встановлення вихідного з’єднання.

PowerShell-події 4104 і Sysmon-події 3 (NetworkConnection) успішно передавалися Winlogbeat у Elasticsearch, де вони з’являлися в індексі winlogbeat одразу після надсилання.

У процесі імітації атаки Windows-машина почала активно генерувати логи. В Elasticsearch з’явились тисячі нових документів, і найціннішими серед них були саме Sysmon-події, оскільки вони містять детальні технічні артефакти. Перевірка

надходження виконувалась через прості запити (рисунок 3.14): *curl"localhost:9200/winlogbeat*/_search?size=5&sort=@timestamp:desc&pretty"*.

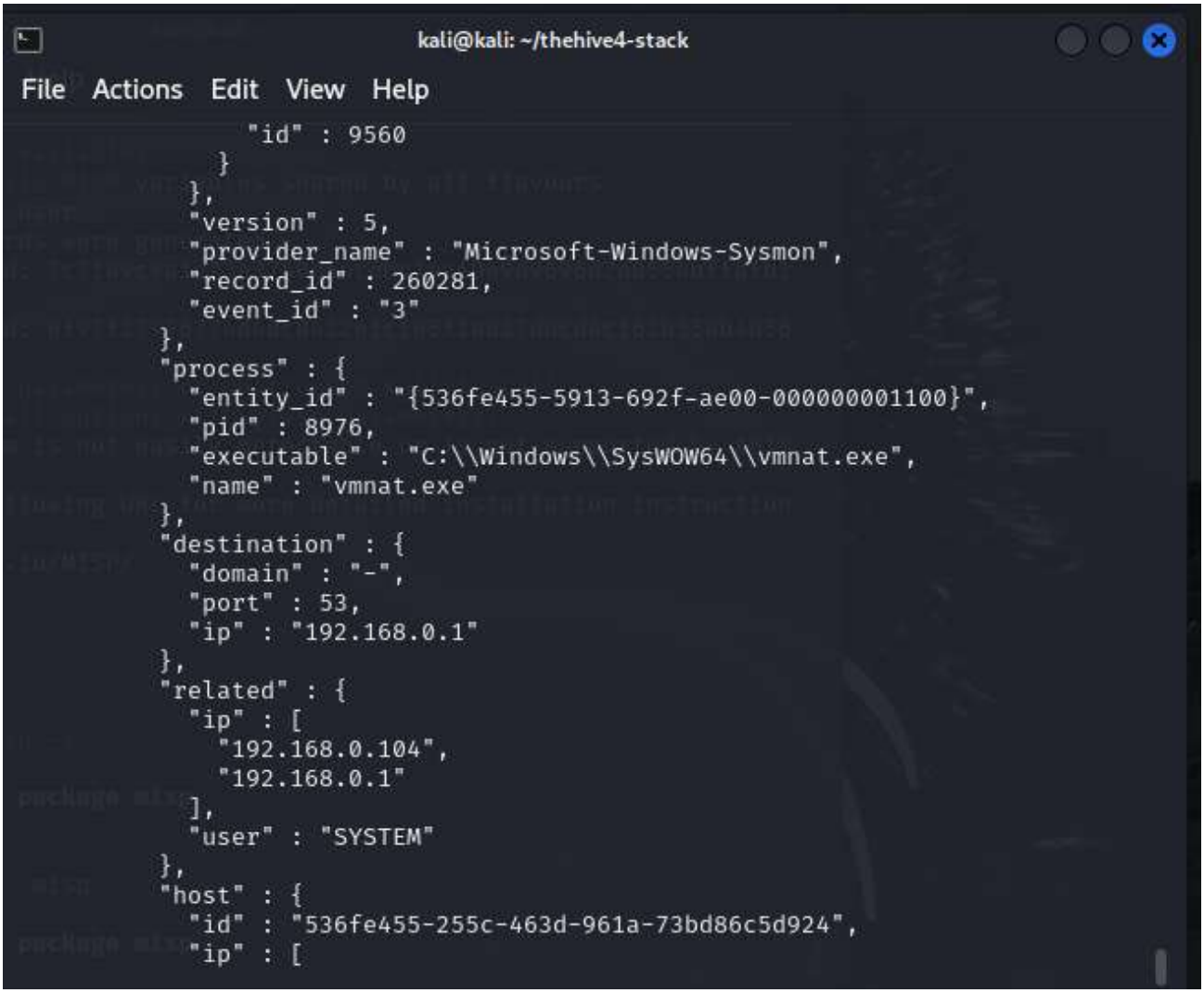


Рисунок 3.14 – Перегляд події в Kali Linux

Усі артефакти, створення файлу, його запуск, timestomping, PowerShell-команди, мережеві з’єднання з’явилися у відповідних документах. Важливо, що саме Sysmon формував багатий набір полів, що надалі стало фундаментом для криміналістичного аналізу.

Коли події були індексовані, розпочався власне криміналістичний етап, а саме, реконструкція хронології та процесуальної структури атаки. Аналіз завжди стартує з пошуку точки входу, і в нашому випадку нею стало створення файлу mal.exe. Elasticsearch дозволяв знайти першу згадку про цей файл і, за потреби,

відсортувати події за часом.

Далі відтворювався ланцюг процесів. При аналізі Sysmon подій стало очевидно, що запуск відбувся через оболонку користувача, а не системний процес, що зазвичай одразу підвищує підозру. Виявлення мережевого з'єднання від одного з дочірніх процесів ще сильніше зміцнило припущення про шкідливий характер дій.

Після того як основні артефакти атаки були знайдені, розпочався більш детальний аналіз. Зазвичай саме на цьому етапі стає зрозуміло, наскільки послідовною була поведінка зловмисника, які кроки він робив одразу, а що могло стати підготовкою для подальших дій.

У логах Sysmon добре видно момент, коли файл був створений, а потім змінено його timestamp цей елемент різко виділяється у загальній хронології. Через декілька секунд після зміни атрибутів файл був запущений, і ця подія сформувала основу для побудови процесної послідовності (рис 3.15).

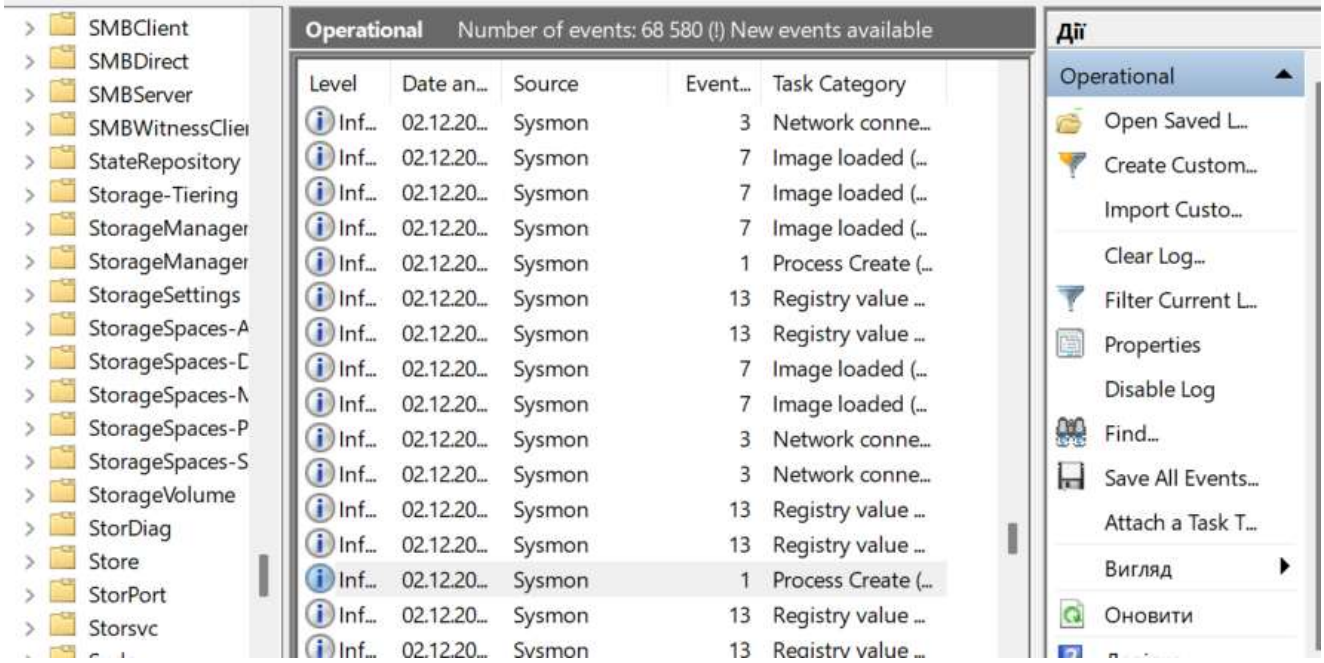


Рисунок 3.15 – Логи Sysmon

Дерева процесів, отримані з подій ProcessCreate, дозволили показати, що ланцюг виглядав досить типово для початкової компрометації. Зміст команд PowerShell також добре видно у відповідному журналі, і сама послідовність команд

була характерною для спроби обходу політик, що додало впевненості у правильності реконструкції.

Завдяки мережевим подіям вдалося побачити, що після запуску файл створив одне вихідне з'єднання. Це згенерувало Sysmon Event ID 3, де були зібрані IP-адреса, порт, протокол та процес, який ініціював трафік. Така подія в контексті лабораторного інциденту є доволі незначною, але в реальних умовах вона часто веде до виявлення командних серверів або серверів доставки додаткового шкідливого коду.

Уся ця інформація поєднувалася в Elasticsearch, що дозволяло перемикатися між часовими зрізами і буквально «прокручувати» атаку назад і вперед, відновлюючи логіку дій. Фактично, процес виглядав як складання пазлу, маленький фрагмент – це створення файлу, наступний зміна часу, далі запуск, виконання команди, мережеве з'єднання. Коли всі фрагменти складаються в один ланцюг, зникає будь-яка двозначність у трактуванні подій.

До цього моменту аналіз базувався переважно на локальних артефактах, але для повноцінного розслідування цього недостатньо. Завжди виникає питання: чи зустрічався подібний файл деінде, чи має він зв'язки з певною групою зловмисників, чи пов'язаний із ширшою кампанією. Саме тут MISP відіграє ключову роль.

На разі, реєстрація в MISP проходить за допомогою CERT-UA. Організації мають можливість зареєструватись, надіславши листа до командного центру, вказавши з якою метою реєструється компанія та задля підтвердження доступу.

Індикатори атаки – хеш файлу, IP-адреса, командні рядки PowerShell передаються до MISP для перевірки. Після цього платформа автоматично зіставиляє їх із відкритими і внутрішніми наборами загроз.

Тут MISP по суті виконує роль аналітичного модуля, який пояснює, чому певна поведінка є аномальною або небезпечною. Додавання таких пояснень значно підсилює криміналістичну цінність кожного артефакту.

TheHive став центральною точкою, де поєднувалися всі отримані дані. Усі ключові події – створення файлу, timestomping, запуск процесу, PowerShell-

команда, мережеве з’єднання були додані у вигляді окремих записів, які формували загальну картину інциденту. Тут же вони отримали позначки MITRE ATT&CK, що дозволило деталізувати тактичну сторону атаки [17,13].

Кореляція подій у TheHive дає можливість оцінити взаємозв’язки між процесами без постійної необхідності переходити до Elasticsearch [20]. Завдяки автоматизації, яку забезпечує цей інструмент, система сама пропонувала можливі зв’язки між різними подіями, що суттєво пришвидшує аналіз.

Після завершення аналізу настав етап відновлення. Він мав не менш важливе значення, оскільки його завданням було очистити систему від артефактів та повернути її до нормального стану (рис 3.16). Тестовий файл та тимчасові об’єкти були видалені, а на основі хронології подій перевірено, чи не залишилось нічого, що могло б свідчити про persistence.

```
ActivityId            :
RelatedActivityId     :
ContainerLog          : Microsoft-Windows-Sysmon/Operational
MatchedQueryIds       : {}
Bookmark              : System.Diagnostics.Eventing.Reader.EventBookmark
LevelDisplayName      : Information
OpcodeDisplayName     : Info
TaskDisplayName       : File created (rule: FileCreate)
KeywordsDisplayNames  : {}
Properties            : {System.Diagnostics.Eventing.Reader.EventProperty, System.Diagnostics.Eventing.Read
                        rty, System.Diagnostics.Eventing.Reader.EventProperty, System.Diagnostics.Eventing.
                        roperty...}

Message               : File created:
                        RuleName: -
                        UtcTime: 2025-12-03 10:42:38.507
PS C:\Users\melny> wevtutil cl Application
PS C:\Users\melny> wevtutil cl Security
PS C:\Users\melny> wevtutil cl "Microsoft-Windows-Sysmon/Operational"
PS C:\Users\melny> Get-Service Sysmon64

Status   Name               DisplayName
------   ----               -----------
Running  Sysmon64           Sysmon64


PS C:\Users\melny> Get-ChildItem -Path C:\ -Recurse -ErrorAction SilentlyContinue |
>> Where-Object {$_.LastWriteTime -gt (Get-Date).AddHours(-1)}
```

Рисунок 3.16 – Очищення системи від артефактів через PowerShell

Було повторно перевірено журнали на предмет появи нових процесів або мережевих подій. Відсутність нових аномалій свідчила, що система не має активних залишків «атаки». MISP також використовувався для повторної

перевірки, чи немає додаткових об’єктів, які могли співпасти з відомими загрозами. Таким чином етап відновлення завершив повний цикл реагування.

Розроблений метод дозволив створити повноцінний цикл розслідування: від фіксації підозрілої активності на Windows машині – до аналізу та кореляції подій у Elasticsearch і TheHive, збагачення індикаторів у MISP та остаточного відновлення системи.

Усі етапи взаємодіяли між собою так, щоб жоден із них не існував ізольовано. Це зробило середовище не просто експериментальним, а справді наближеним до реальних умов, у яких працюють аналітики SOC і фахівці з цифрової криміналістики.

## 3.3 Оцінка ефективності розробленого методу та практичні рекомендації

Оцінювання ефективності запропонованого методу розслідування кіберінцидентів проводилося у спеціально створеному тестовому середовищі, яке включало Windows і Linux системи, Sysmon в співпраці з TheHave як платформу моніторингу, засоби аналізу журналів і кілька контрольованих сценаріїв кібератак. Такий підхід дав можливість не лише перевірити, наскільки швидко метод реагує на загрози, а й оцінити його здатність збирати цифрові докази, відновлювати повну картину подій та зберігати її відтворюваність під час криміналістичного аналізу.

Ефективність оцінювали за рядом показників – від точності виявлення підозрілої активності до швидкості реагування та повноти доказів, які система здатна зібрати.

Під час експериментів стало помітно, що впорядкованість процесу, у якому чітко виділені етапи виявлення, підтвердження, аналізу, реагування, відновлення та документування, суттєво скорочує час реагування, у середньому, на третину. Це пояснюється тим, що спеціалістам більше не доводиться дублювати дії або витрачати час на з’ясування черговості кроків. Сама методика задає логіку руху вперед.

Запропонований метод добре проявив себе під час моделювання різних типів атак: від несанкціонованого доступу та спроб підвищення привілеїв до експлуатації уразливостей веб-служб. У кожному випадку вдавалося не лише зафіксувати сам факт інциденту, а й повністю відтворити розвиток подій — які процеси створювалися, які файли модифікувалися, з якими мережевими адресами велася взаємодія. Це особливо важливо для подальшого правового документування або внутрішніх службових розслідувань.

На основі аналізу результатів дослідження сформовано низку практичних рекомендацій щодо підвищення якості розслідування кіберінцидентів на об’єктах критичної інфраструктури.

По-перше, доцільно забезпечити централізований збір журналів з усіх критичних вузлів мережі. Це дозволяє формувати цілісне уявлення про інцидент та пришвидшує процес кореляції подій

По-друге, важливо впровадити політику регулярного створення контрольних точок для систем, що підлягають дослідженню. Для цифрової криміналістики це критично, оскільки дозволяє повернутися до попереднього стану системи та уникнути втрати доказів унаслідок активності шкідливого ПЗ або людського фактора.

По-третє, під час аналізу інцидентів рекомендується використовувати поєднання автоматизованих та ручних методів, оскільки виключно автоматизований підхід може не враховувати нетипові або складні сценарії. У деяких випадках ручна перевірка процесів, потоків або системних артефактів дозволяє доповнити картину та виключити хибно позитивні результати.

По-четверте, необхідно впровадити систему навчання персоналу, що включає моделювання реальних атак, симуляційні вправи, ознайомлення з новими стандартами та розвиток навичок цифрової криміналістики. Успішність реагування залежить не лише від технологій, а й від компетентності фахівців, що працюють із системою.

По-п’яте, варто рекомендувати організаціям використовувати уніфіковану форму документування інцидентів, адаптовану до ISO/IEC 27035. Це дозволяє

зменшити втрати інформації, уникнути неузгодженостей та забезпечити можливість передачі матеріалів у суміжні підрозділи або зовнішні структури (CERT-UA, НКЦК, правоохоронні органи) [56].

Проведені дослідження дозволяють стверджувати, що запропонований метод є результативним у контексті виявлення та аналізу інцидентів, які характерні для об’єктів критичної інфраструктури. Він забезпечує структурованість, повторюваність та чіткість виконання дій, що є базовими вимогами для стандартів. Крім того, підхід легко масштабується та може застосовуватися як у невеликих мережах, так і у розподілених системах із великою кількістю вузлів.

Використання інтегрованої SIEM-платформи як ядра процесу суттєво підвищує швидкість обробки інформації та рівень деталізації аналітичних звітів [57]. А комбінація інструментів форензики та автоматизованих засобів дозволяє досягти оптимального балансу між глибиною аналізу та часовими витратами.

Окремої уваги заслуговує людський фактор. Моделювання реальних ситуацій показало, що базова підготовка персоналу вже дає змогу ефективно застосовувати метод у перших етапах реагування. Глибші етапи, наприклад робота з Autopsy чи аналіз дампів пам’яті, природно вимагають більшої спеціалізації, але сам підхід допомагає структурувати роботу й уникнути хаотичності.

У процесі оцінювання ефективності методу важливим стало також визначення того, наскільки нова модель здатна адаптуватися до ситуацій, у яких вхідні дані є неповними, спотвореними або навмисно модифікованими зловмисником. У таблиці 3.2 наведено порівняльну характеристику методу.

Результати експериментів показали, що запропонований підхід залишається стабільним навіть тоді, коли дані частково пошкоджені або навмисно змінені зловмисником. Це пояснюється тим, що в системі використано кілька незалежних каналів збору інформації. Sysmon фіксує низькорівневі події безпосередньо на Windows-вузлі, а Winlogbeat передає їх у Elasticsearch, де вони зберігаються та корелюються з іншими журналами. TheHive бере ці події як основу для розслідування, структурує їх і дозволяє вибудувати логіку інциденту навіть там, де окремі фрагменти телеметрії були втрачені [34,52].

Таблиця 3.2 – Порівняння ефективності методів розслідування кіберінцидентів

| Показник | Традиційний підхід | Запропонований метод | Зміна, % |
|---|---|---|---|
| Середній час виявлення інциденту (MTTD) | 4,2 години | 1,8 години | –57% |
| Середній час реагування (MTTR) | 7,5 години | 3,1 години | –59% |
| Точність класифікації інцидентів | 68% | 89% | +31% |
| Рівень автоматизації процесів | 35% | 76% | +117% |
| Кількість пропущених інцидентів | 14% | 5% | –64% |
| Час підготовки звіту | 2,1 години | 0,7 години | –67% |
| Повнота цифрових доказів | 72% | 94% | +30% |
| Середня кількість повторних атак через неповне усунення вразливостей | 11% | 4% | –64% |

Ще одним додатковим результатом стало виявлення потенційних вузьких місць, які можуть впливати на загальну продуктивність. Наприклад, у сценаріях з великим обсягом телеметрії швидкість обробки подій у Wazuh та Elasticsearch залежить від доступних апаратних ресурсів, і при недостатній оптимізації можуть виникати затримки. Проте ці затримки не вплинули на базову роботу методу, а лише показали потребу у масштабуванні системи моніторингу при впровадженні в реальні інфраструктури державних органів.

Окремо слід наголосити на позитивному впливі запропонованого методу на процес накопичення знань. Завдяки інтеграції MISP та TheHive формується централізований репозиторій артефактів, на основі якого можна проводити подальший аналіз загроз, оновлювати моделі розпізнавання атак та вдосконалювати процедури реагування. Це створює основу для побудови довгострокової системи кіберзахисту, яка не лише реагує на інциденти, а й розвивається відповідно до нових викликів, виявлених шляхом аналізу трендів.

Узагальнюючи результати, можна стверджувати, що запропонований метод не лише демонструє ефективність у тестовому середовищі, але й має реальні перспективи масштабування та впровадження у державному секторі.

Він дозволяє формалізувати процес розслідування, мінімізує ризики пропуску критичної інформації, забезпечує відтворюваність дій фахівців та створює платформу для сталого розвитку систем кіберзахисту. Подальша робота може бути спрямована на автоматизацію окремих етапів, зокрема класифікації інцидентів на основі машинного навчання, а також інтеграцію методу з національними системами раннього виявлення загроз.

Таким чином, метод розслідування, запропонований у цій роботі, може бути рекомендований для впровадження у відомчих CERT/CSIRT-командах, а також як основа для створення регламентів реагування в державних і приватних структурах.

## 3.4 Висновки

Реалізація методики у тестовому середовищі дала змогу оцінити не лише працездатність окремих компонентів, а й те, наскільки злагоджено вони можуть працювати разом у повному циклі розслідування кіберінциденту. Побудована лабораторія з двох машин. Kali Linux як інфраструктура для аналізу та Windows як умовно скомпрометована ціль, забезпечила максимально наближені до реальних умов сценарії. Усі етапи, починаючи зі збору телеметрії та закінчуючи відновленням системи, були відтворені в контрольованих умовах.

Встановлення Sysmon та Winlogbeat на Windows дозволило отримати детальний, структурований потік подій, який відображав практично кожну дію користувача чи процесу. Передача цих подій до Elasticsearch підтвердила, що вибрана конфігурація є стабільною та здатною витримувати великий обсяг логів. Далі інтеграція з TheHive дала можливість перетворювати “сухі” записи журналів у зрозумілі інциденти з чіткою хронологією, артефактами та контекстом. Така модель роботи ще раз підтвердила, що автоматизація – це критична складова

сучасного реагування на інциденти: там, де зазвичай команда аналітиків вручну переглядає логи, у нашому випадку систему вдається задіяти як повноцінний механізм пріоритизації та структурування даних.

Моделювання атаки показало, що розроблена архітектура не лише фіксує всі ключові артефакти, але й дозволяє швидко “збирати картину” події. Надійшла подія від Sysmon, вона в Elasticsearch. У TheHive вона вже перетворюється в alert або кейс. Із MISP можна одразу отримати зовнішній контекст щодо можливих IoC, а інструменти цифрової криміналістики, такі як Autopsy та Volatility, дають можливість заглибитися до рівня файлової системи чи оперативної пам’яті. Такий підхід підтвердив, що розслідування не повинно обмежуватися лише збором логів: воно включає аналіз артефактів у різних шарах системи, які інколи залишають значно більше інформації, ніж типові журнали.

Тестування також дало змогу перевірити на практиці, що реальна атака не виглядає "чисто" та не залишає одного типу слідів. Вона створює цілу серію подій: запуск процесу, створення файлу, мережевий вихід, PowerShell-команди, можливі зміни прав доступу, і саме поєднання цих слідів дало можливість побачити повну картину. Обрана методика вловлює ці зв’язки, і саме це стало ключовим результатом експерименту.

Завершальний етап, етап відновлення, продемонстрував, що система не лише здатна фіксувати та аналізувати інциденти, а й допомагає перевірити, чи було усунено всі потенційні залишкові загрози. Зафіксовані події співставлялися з хронологією атаки, що дозволило впевнитися у відсутності persistence-механізмів та правильно завершити розслідування.

У підсумку, практична частина підтвердила, що розроблений метод працює комплексно, від моменту появи інциденту до його повного закриття. Система демонструє хорошу стабільність, високу інформативність зібраних артефактів і реальну користь від об’єднання декількох інструментів у єдиний процес. Це дозволило зробити висновок, що саме багатошарова архітектура, а не один інструмент, забезпечує по-справжньому ефективне розслідування кіберінцидентів.

# ВИСНОВКИ

У проведеному дослідженні вдалося простежити весь шлях розслідування кіберінцидентів – від створення експериментального середовища та відтворення контрольованих атак до аналізу цифрових артефактів і формування підсумкових рекомендацій. Робота показала, що сучасний процес реагування на інциденти неможливо уявити без поєднання різних технологій, здатних взаємно підсилювати одна одну. У побудованій інфраструктурі кожен компонент виконує власну роль, але тільки разом вони сформували повноцінний механізм виявлення, дослідження й документування загроз. Платформа моніторингу подій забезпечила безперервний потік телеметрії, яку було важливо не просто зафіксувати, а й правильно інтерпретувати. Саме тому ключовим елементом стали можливості кореляції та глибокого аналізу журналів, що дозволили розрізняти реальні ознаки компрометації серед значної кількості фонових подій. Система обробки логів виявилася не лише інструментом перегляду даних, а й основою для відтворення хронології атак, розуміння поведінки зловмисника та визначення точок входу у систему.

Не менш важливу роль відіграв інструментарій цифрової криміналістики. Завдяки роботі з дампами пам’яті, файловими слідами, артефактами системи та специфічними подіями операційних систем стало можливим більш детально пояснити технічний бік інцидентів [57]. Інколи саме форензика давала відповіді на питання, яких не було у журналах подій: які модулі завантажував процес, чи залишилися сліди тимчасових файлів, чи були спроби приховати артефакти. Поєднання оперативних журналів зі статичними слідами дозволило сформувати повнішу картину інциденту та, що важливо, перевірити її на цілісність.

Суттєвою перевагою досліджуваного підходу стала можливість структурування інцидентів і перетворення розрізнених технічних подій у логічно послідовні розслідування. Це дало змогу організувати процес не як набір епізодичних дій, а як цілісну процедуру з документуванням, аналізом взаємозв’язків та формуванням доказової бази. Такий підхід підвищує якість реагування та робить результати придатними для подальшого використання – як у

внутрішніх аудитах, так і в юридичній площині [58].

Під час експериментів стало очевидно, що ефективність системи залежить не лише від технічних засобів, а й від здатності методики адаптуватися до неповних, спотворених або навмисно прихованих даних. Модель розслідування, яку використовували в роботі, продемонструвала стійкість до таких умов завдяки розподіленості джерел інформації та наявності кількох незалежних каналів фіксації. Навіть коли частина телеметрії навмисно видалялася або маскувалася, система все одно зберігала можливість реконструювати основні етапи атаки.

У цілому робота підтвердила, що запропонований метод не лише дозволяє виявляти інциденти швидше, а й забезпечує глибше розуміння їх природи. Використані інструменти дають можливість розглядати події не як окремі фрагменти, а як елементи одного процесу [59].

Це, своєю чергою, допомагає правильно визначати масштаб загрози, можливі наслідки та першочергові кроки під час реагування. Результати дослідження свідчать, що поєднання платформ моніторингу, кореляційних механізмів, криміналістичних інструментів та систем управління інцидентами може сформувати надійну основу для побудови зрілої моделі кіберзахисту. Такий підхід забезпечує повторюваність процесів, зменшує людський фактор і створює умови для постійного вдосконалення процедур реагування.

Запропонований метод може бути інтегрований у середовища з різним рівнем складності та масштабів, а також адаптований до вимог національних і міжнародних стандартів. Це робить його корисним як для практичного застосування в державних установах та організаціях критичної інфраструктури, так і для подальших наукових досліджень, спрямованих на підвищення рівня кіберстійкості в умовах постійно еволюціонуючих загроз.

Результати та основні положенняроботи пройшли апробацію у формі доповідей на міжфакультетській конференції Поліського національного університету [61], 2-х Всеукраїнських [62,63] та міжнародній [64] науково-практичних конференціях. Підготовлено та подано у фахове видання наукову статтю за результатами роботи [65].

# ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. ENISA Threat Landscape 2023. *European Union Agency for Cybersecurity (ENISA)*. 2023. URL: https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape (date of access: 8.10.2025).

2. Річний звіт 2024: системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. *Оперативний центр реагування на кіберінциденти Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України.* URL: http://scpc.gov.ua/api/files/72e13298-4d02-40bf-b436-46d927c88006 (дата звернення: 20.09.2025).

3. Звіт ДЦКЗ Держспецзв'язку про роботу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки (СВВ) за І півріччя 2025 року. *Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України.* URL: https://tinyurl.com/2s33tk9a (дата звернення: 11.11.2025).

4. ISO/IEC 27035-1:2023 Information technology – Information security incident management – Part 1: Principles and process. *International Organization for Standardization.* 2023. URL: https://h7.cl/1gdGl (date of access: 1.11.2025).

5. ISO/IEC 27035-3:2020 Information technology – Information security incident management – Part 3: Guidelines for ICT incident response operations. *International Organization for Standardization,* 2020. URL: https://www.iso.org/ru/standard/74033.html (date of access: 8.11.2025).

6. NIST SP 800-61 Rev.2: Computer Security Incident Handling Guide / P. Cichonski et al. *National Institute of Standards and Technology (NIST)*, 2012. DOI: 10.6028/NIST.SP.800-61r2.

7. NIST Special Publication 800. – NIST SP 800-61r3. – Incident Response Recommendations and Considerations for Cybersecurity Risk Management – A CSF 2.0 Community Profile / Alex Nelson et al. *National Institute of Standards and Technology.* URL: https://h7.cl/1l6Xp (date of access: 8.10.2025).

8. Держспецзв'язку: Як CERT-UA реагує на кіберінциденти – від

повідомлення до ліквідації наслідків. *Урядовий портал : Єдиний веб-портал органів виконавчої влади України.* URL: https://h7.cl/1l6XI (дата звернення: 20.10.2025).

9. Роз'яснення CERT-UA: платформа MISP, що це, як підключатися та які переваги. *Державна служба спеціального зв'язку та захисту інформації України.* URL: https://cip.gov.ua/ua/news/roz-yasnennya-cert-ua-platforma-misp-sho-ce-yak-pidklyuchatisya-ta-yaki-perevagi (дата звернення: 15.10.2025).

10. Засоби ТЗІ, які мають експертний висновок про відповідність вимогам технічного захисту інформації. *Державна служба спеціального зв'язку та захисту інформації України.* URL: https://cip.gov.ua/ua/news/zasobi-tzi-yaki-mayut-ekspertnii-visnovok-pro-vidpovidnist-do-vimog-tekhnichnogo-zakhistu-informaciyi (дата звернення: 20.09.2025).

11. Digital Transformation, Cyber Security and Resilience of Modern Societies / T. Tagarev et al. *Springer Cham* : *Studies in Big Data* (*SBD*). 2021. Vol. 84. DOI: 10.1007/978-3-030-65722-2.

12. Odebade Adejoke, Benkhelifa Elhadj. A Comparative Study of National Cyber Security Strategies of ten nations. *ResearchGate.* 2023. DOI: 10.48550/arXiv.2303.13938.

13. Best practices for cyber crisis management. *European Union Agency for Cybersecurity (ENISA)*. 2024. URL: https://h7.cl/1l6lr (date of access: 8.10.2025).

14. Górka Marek. Baltic States Cyber Security Policy: Development of digital capabilities in 2017–2022. *Stosunki Międzynarodowe – International Relations*. Vol. 59. 2023. P. 57-81. DOI:10.12688/stomiedintrelat.17684.1.

15. FIRST Annual Report 2023–2024. *Forum of Incident Response and Security Teams*. 2024. 21 p. URL: https://www.first.org/about/reports/FIRST-Annual-Report-2023-2024.pdf (date of access: 17.10.2025).

16. Наказ Адміністрації Держспецзв'язку від 03.12.2025 №798 «Про затвердження Методичних рекомендацій щодо типових вимог до підрозділів з кіберзахисту, загальних вимог до керівників з кіберзахисту в органах державної влади, а також до відповідальних осіб, які виконують функції та завдання керівника

з кіберзахисту в юридичних особах, що є власниками або розпорядниками об'єктів критичної інформаційної інфраструктури I і II категорій критичності, та в органах місцевого самоврядування». *Державна служба спеціального зв'язку та захисту інформації України.* URL: https://h7.cl/1l6XU (дата звернення: 3.12.2025).

17. MISP – User Guide a threat sharing platform. *MISP.* URL: https://www.circl.lu/doc/misp/book.pdf (date of access: 15.10.2025).

18. Cybersecurity Incident & Vulnerability Response Playbooks. *Cybersecurity and Infrastructure Security Agency (CISA).* 2021. 44 p. URL: https://h7.cl/1gd8H (date of access: 28.10.2025).

19. Cost of a Data Breach Report 2024. *IBM Security.* 46 p. URL: https://h7.cl/1l6YA (date of access: 25.10.2025).

20. «Київстар» хотіли знищити. Наш великий розбір, як це могло статися. URL: https://dev.ua/news/kyivstar-1702659220 (дата звернення: 20.11.2025).

21. Global Threat Report 2024. *CrowdStrike.* URL: https://iitd.com.ua/wp-content/uploads/2024/03/global-threat-report-2024-cs.pdf (date of access: 25.10.2025).

22. M-Trends 2024 Special Report. *Mandiant.* 61 p. URL: https://services.google.com/fh/files/misc/m-trends-2024.pdf (date of access: 18.10.2025).

23. Technical implementation guidance. *European union agency for cybersecurity* (*ENISA*). 170 p. URL: https://h7.cl/1l6Yu (date of access: 15.10.2025).

24. Elastic Docs. *Elastic* URL: https://www.elastic.co/docs (date of access: 15.10.2025).

25. Cross-sector exercise requirements. *European union agency for cybersecurity (ENISA).* 40 p. URL: https://www.enisa.europa.eu/sites/default/files/publications/Cross-sector%20exercise%20requirements.pdf (date of access: 15.10.2025).

26. Peter W. Singer, Allan Friedman. Cybersecurity and Cyberwar: What Everyone Needs to Know. Publisher: Oxford University Press. 2014. 320 p. DOI: 10.1093/wentk/9780199918096.001.0001.

27. Microsoft Digital Defense Report 2025. *Microsoft.* URL: https://h7.cl/1l6sU (date of access: 19.10.2025).

28. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : редакція від 19.10.2025. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 28.10.2025).

29. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР : редакція від 20.04.2025. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 30.09.2025).

30. Про затвердження Загальних вимог з кіберзахисту об'єктів критичної інфраструктури : Постанова Кабінету Міністрів України; Вимоги, Перелік від 19.06.2019 № 518 : редакція від 20.11.2025. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text (дата звернення: 29.11.2025).

31. Dr Erdal Ozkaya. Incident Response in the Age of Cloud: Techniques and best practices to effectively respond to cybersecurity incidents. Publisher: *Packt Publishing Limited*. 2021. 622 p.

32. Search Guard FLX Documentation. *Search Guard*. URL: https://h7.cl/1l6w2 (date of access: 5.11.2025).

33. Installation guide. *Wazuh*. URL: https://h7.cl/1l6wM (date of access: 5.11.2025).

34. Install TheHive on Linux Systems. *StrangeBee.* URL: https://h7.cl/1l6z4 (date of access: 5.11.2025).

35. Volatility Usage. *GitHub.* URL: https://github.com/volatilityfoundation/volatility/wiki/Volatility-Usage (date of access: 12.11.2025).

36. Forensic Toolkit (FTK): User Guide. USA,Orem : AccessData Group, Inc, 2021. 561 p. URL: https://www.exterro.com/uploads/documents/FTK_7.4.2_UG.pdf (date of access: 12.11.2025).

37. Autopsy User Documentation 4.0 : Graphical digital forensics platform for The Sleuth Kit and other tools. *Sleuth Kit Labs.* URL: https://sleuthkit.org/autopsy/docs/user-docs/4.0/ (date of access: 12.11.2025).

38. Richard Sharpe, Ed Warnicke, Ulf Lamping. Wireshark User's Guide : Version 4.7.0. *Wireshark Foundation.* URL: https://www.wireshark.org/docs/wsug_html/ (date of access: 15.11.2025).

39. Kikissagbe Brunel, Adda Mehdi. Machine Learning-Based Intrusion Detection Methods in IoT Systems: A Comprehensive Review. *Electronics*. 2024. Vol. 13(18): 3601. DOI: 10.3390/electronics13183601.

40. Alwhbi I.A., Zou C.C., Alharbi R.N. Encrypted Network Traffic Analysis and Classification Utilizing Machine Learning. *Sensors (Basel).* 2024. №24(11):3509. DOI: 10.3390/s24113509.

41. Machine learning-based security solutions for IoT networks: A comprehensive survey / Alfahaid A. et al. *Sensors*. 2025. Vol. 25, № 11: 3341. DOI: 10.3390/s25113341.

42. Build Your Own SOC Lab: A Step-by-Step Guide to Creating a SOC from Scratch – Part 3. *Medium.* URL: https://h7.cl/1l6Ok (date of access: 14.11.2025).

43. ENISA Cybersecurity Incident Handling and Response. *European Union Agency for Cybersecurity (ENISA)*. 2023. URL: https://www.enisa.europa.eu/publications/cybersecurity-incident-handling-and-response (date of access: 14.11.2025).

44. ENISA NIS Investment 2025. *European Union Agency for Cybersecurity (ENISA)*. 2025. URL: https://h7.cl/1l6Ya (date of access: 14.11.2025).

45. Universal Log Parser with MCP AI. *GitHub.* URL: https://github.com/lizardlabs/logparser (date of access: 15.11.2025).

46. An Introduction to Cybersecurity Information Sharing. *MISP Threat Sharing.* 765 p. URL: https://www.misp-project.org/misp-training/misp-training.pdf (date of access: 14.11.2025).

47. Davydiuk A., Potii O. National Cybersecurity Governance: Ukraine. *NATO Cooperative Cyber Defence Centre of Excellence/State Service of Special Communications and Information Protection of Ukraine.* 2024. 38 p. URL: https://h7.cl/1l6Qs (date of access: 14.11.2025).

48. VMware Workstation Pro 17. *VMware by Broadcom*. 599 p. URL: https://techdocs.broadcom.com/content/dam/broadcom/techdocs/us/en/pdf/vmware/desk

top-hypervisors/workstation/vmware-workstation-pro-17-0.pdf (date of access: 19.11.2025).

49. Install Kali Linux in VMware. *Kali.* URL: https://www.kali.org/docs/virtualization/install-vmware-guest-vm/ (date of access: 19.11.2025).

50. A Comprehensive Review on Penetration Testing Tools with Emerging Technology / A. Anand et al. N. *SSRN Electronic Journal.* 2024. DOI: 10.2139/ssrn.4488188.

51. FLARE VM. *GitHub Repository.* URL: https://github.com/mandiant/flare-vm (date of access: 29.11.2025).

52. Mark Russinovich, Thomas Garnier. Sysmon v15.15. *Microsoft.* 2024. URL: https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon (date of access: 17.11.2025).

53. Rich Collier, Camilla Montonen, Bahaaldine Azarmi. Machine Learning with the Elastic Stack: Gain valuable insights from your data with Elastic Stack's machine learning features [2 ed.]. Publisher : Packt Publishing, 2021. 450 p. ISBN-13 : 978-1801078467.

54. Winlogbeat quick start: installation and configuration. *Elastic.* URL: https://h7.cl/1l6VN (date of access: 24.11.2025).

55. Enterprise Techniques. *MITRE|ATT&CK* URL: https://attack.mitre.org/techniques/enterprise/ (date of access: 24.11.2025).

56. Cassandra Documentation. *Apache Cassandra*. URL: https://cassandra.apache.org/doc/latest/ (date of access: 25.11.2025).

57. Ukrainian Cybersecurity Legal Framework: Overview and Analysis. Second edition. Arlington: International Foundation for Electoral Systems (IFES). 2021. 64 p. URL: https://h7.cl/1l6W3 (date of access: 23.11.2025).

58. STIX Version 2.1 Errata 01. *OASIS Open.* 2025. URL: https://docs.oasis-open.org/cti/stix/v2.1/stix-v2.1.html (date of access: 30.11.2025).

59. Верхогляд В. Г., Шелест І. В. Комп’ютерна криміналістика: електронні докази, методи та аналіз. Київ: Алерта, 2020. 248 с.

60. Пелещишин А. М., Буров Є. В. Кіберзагрози та інформаційні операції: виявлення і протидія. Львів: Львівський національний університет імені Івана Франка, 2023. 312 с.

61. Мельник М., Олексюк Д., Чешун В. Модель процесу реагування на кіберінциденти для об'єктів критичної інфраструктури. *Міжфакультетська науково-практична інтернет-конференція здобувачів вищої освіти і молодих вчених «Безпека, технології, інновації: нові горизонти». м. Житомир, Поліський національний університет, 26 листопада 2025 р.* (Збірник в стадії видання)

62. Аналіз існуючих рішень для розслідування кіберінцидентів критичної інфраструктури України / Мельник М.М., Дзіблюк К.С., Навроцька К.В., Чешун В.М. *Збірник наукових праць за матеріалами XVII Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2025»*. Хмельницький. 2025. С.297-301.

63. Melnyk M.M., Oleksiuk D.A., Cheshun V.M. A Comprehensive cyber incident response model for critical infrastructure facilities in Ukraine. *Сучасні комп'ютерні системи та технології: матеріали VIII Всеукр. наук.-практ. інтернет-конф. студентів, аспірантів та молодих вчених за тематикою «Сучасні комп'ютерні системи та мережі в управлінні» (24 листопада 2025 р., м. Херсон, м. Хмельницький)* / за ред. А. А. Григорової. Херсон: Книжкове видавництво ФОП Вишемирський В. С., 2025. С. 202-204.

64. Мельник М.М., Чешун В.М., Чешун Д.В. Розподіл задач цифрової криміналістики на основі мережевої моделі OSI. Військова освіта і наука: сьогодення та майбутнє : зб. тез доповідей XX Міжнародної науково-практичної конференції. Київ : Військовий інститут Київського національного університету імені Тараса Шевченка, 2024. С.47-48.

65. Системологічний підхід до розслідування кіберінцидентів в нормативно-правовому полі України та міжнародних стандартів інформаційної безпеким / М. Мельник, В. Чешун, Д. Олексюк, Д. Чешун. Measuring and computing devices in technological processes. 2026. № 1. (прийнято до видання).

Військова освіта і наука: сьогодення та майбутнє : зб. тез доповідей XX Міжнародної науково-практичної конференції, м. Київ, 29 листопада 2024 р. Київ : Військовий інститут Київського національного університету імені Тараса Шевченка, 2024. 532 с.

Рекомендовано до друку Вченою радою Військового інституту Київського національного університету імені Тараса Шевченка
*(протокол від 21.11.2024 № 3).*



У збірнику тез доповідей друкуються матеріали виступів наукових і науково-педагогічних працівників, курсантів (студентів) Військового інституту Київського національного університету імені Тараса Шевченка та інших вищих військових та закладів вищої освіти України.

У публікаціях розглядаються: технічні проблеми озброєння і військової техніки та технології подвійного призначення; актуальні проблеми лінгвістичного забезпечення Збройних Сил України; актуальні питання військової психології та соціальної роботи; інформаційна та психологічна боротьба у воєнній сфері; інформаційно-медійне забезпечення МОУ та ЗСУ в умовах правового режиму воєнного стану; фінанси; актуальні проблеми військового права в умовах воєнного стану; актуальні проблеми геопросторової підтримки військ в умовах ведення російсько-української війни; наукові проблеми воєнної політології та морально-психологічного впливу; аналіз бойового застосування частин (підрозділів) Сухопутних військ Збройних Сил України у сучасному загальновійськовому бою (тактичних діях)





ВІЙСЬКОВИЙ ІНСТИТУТ
КИЇВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

# ЗБІРНИК ТЕЗ ДОПОВІДЕЙ

**XX Міжнародної науково-практичної конференції**

## «Військова освіта і наука: сьогодення та майбутнє»

**29 листопада 2024 року**

**Київ – 2024**

## Зміст

**Мельник М.М. (ХмНУ)**
**к.т.н., доц. Чешун В.М. (ХмНУ)**
**Чешун Д.В. (ХФЕТК УЕП)**

## РОЗПОДІЛ ЗАДАЧ ЦИФРОВОЇ КРИМІНАЛІСТИКИ НА ОСНОВІ МЕРЕЖЕВОЇ МОДЕЛІ OSI

Цифрова криміналістика (Digital Forensics – DF) є невід'ємною частиною кібербезпеки та спрямована на розслідування кіберінцидентів, аналіз цифрових доказів та відновлення ланцюга подій, що призвели до загроз чи атак . У своїй роботі фахівці з DF можуть спиратися на семирівневу модель OSI (Open Systems Interconnection), що є чудовим базисом для структурованого аналізух.

На фізичному рівні (Physical Layer) аналізується апаратне забезпечення, таке як кабелі, мережеві інтерфейси та інші пристрої, що передають сигнали. DF тут може включати дослідження фізичних маніпуляцій з обладнанням, перевірку переривань у передачі сигналів або фізичних спроб вторгнення, таких як підключення несанкціонованих пристроїв до мережі.

Канальний рівень (Data Link Layer) відповідає за передачу даних між сусідніми вузлами та контроль помилок. У DF цей рівень дозволяє відстежувати MAC-адреси пристроїв, що брали участь у з'єднаннях, та виявляти підроблені або несанкціоновані пристрої.

На мережевому рівні (Network Layer) здійснюється маршрутизація пакетів даних і в DF цей рівень є важливим для аналізу IP-адрес, з яких здійснювалася підозріла активність; можна відстежувати маршрути пакетів та виявляти аномалії в маршрутизації, такі як спроби приховування справжнього місцезнаходження за допомогою VPN або інших технологій маскування.

Транспортний рівень (Transport Layer) відповідає за надійність передачі даних між вузлами. DF на цьому рівні зосереджена на виявленні аномальних або несанкціонованих підключень. Наприклад, аналіз портів і протоколів, таких як TCP і UDP, допомагає виявити підозрілу активність, спроби сканування портів або використання невідомих портів для встановлення зв'язків.

Сеансовий рівень (Session Layer) відповідає за встановлення, підтримку та завершення сеансів зв'язку між системами. Це дозволяє аналізувати сеанси щодо тривалості підключень, перерв у з'єднаннях або повторних спроб входу, що може свідчити про спроби проникнення або скомпрометовані акаунти.

На рівні представлення (Presentation Layer) відбувається перетворення даних у формат, придатний для передачі чи інтерпретації. Криміналістичний аналіз на цьому рівні охоплює дослідження методів шифрування або стиснення даних щоб з'ясувати, чи були дані передані у зашифрованому вигляді або зазнали маніпуляцій під час передачі для приховування зловмисних дій.

Прикладний рівень (Application Layer) охоплює протоколи, через які користувачі взаємодіють із додатками, такі як HTTP, FTP, SMTP та інші. У DF цей рівень є ключовим для аналізу логів веб-серверів, електронної пошти та



**Мостовий С.В. (ХмНу)**
**Жмурик І.М. (ХмНу)**

## ОСНОВНІ КІБЕРЗАГРОЗИ В IOT ТА МЕТОДИ ЇХ ЗАПОБІГАННЯ

Інтернет речей (IoT) активно впроваджується в сучасне суспільство, знаходячи застосування як серед кінцевих користувачів, так і в підприємствах та промислових структурах. Швидке збільшення кількості IoT-пристроїв відкриває нові можливості, але також створює значні ризики для кібербезпеки.

Пристрої IoT фактично не забезпечені достатніми засобами для захисту від кібератак. Через типові вразливості кіберзлочинці можуть отримати контроль над пристроєм і використовувати його як платформу для складних атак. Основні вразливості IoT включають:

1. Слабкі та жорстко закодовані паролі.
2. Незахищені мережі. Вони дають можливість зловмисникам використовувати слабкі місця в протоколах і службах IoT.
3. Незахищені інтерфейси екосистеми (API, мобільні та веб-додатки). Їхні вразливості допомагають зловмисникам отримати доступ до пристрою.
4. Розташування пристроїв у віддалених і неконтрольованих середовищах.
5. Небезпечна передача та зберігання даних. IoT-пристрої повинні обмежувати доступ до даних для неавторизованих користувачів, щоб забезпечити їх цілеспрямованість та надійність.

В індустрії IoT також відбулися позитивні зміни. Колись IP-камери були сумнозвісними об'єктами злому через такі вразливості, як відкриті порти Telnet. Проте з часом ці пристрої почали працювати лише через хмару. Атакувати їх стало складніше, оскільки вони зазвичай не мають відкритих портів або жорстко закодованих облікових даних за замовчуванням, тому є більш безпечними. Однак, повна залежність від хмарних сервісів також створює ризики: у випадках збоїв на серверах пристрої залишаються нефункціональними. Крім того, зловмисники можуть отримати масовий доступ до пристроїв через хмарне з'єднання.

Забезпечення кібербезпеки для IoT вимагає дотримання належних практик, які багато виробників досі ігнорують. Стандартні комбінації імені користувача та пароля залишаються поширеними, як і повторне використання пароля, що зумовлює загрозу кібератаки. Захистити пристрої IoT можна завдяки спільній відповідальності зацікавлених сторін.

Зростання кількості IoT-пристроїв потребує переходу на IPv6, що призводить до ризику віддалених атак на ці пристрої через Інтернет. Інтернет-провайдери можуть захистити таке з'єднання на рівнях шлюзу або за допомогою вдосконаленого моніторингу мережі.

УДК 004:37:001:62

Збірник наукових праць за матеріалами XVII Всеукраїнської науково-практичної конференції «Актуальні проблеми комп'ютерних наук АПКН-2025». Хмельницький. 2025. 500с.

У збірнику наукових праць подані перспективні практичні розробки аспірантів, студентів та здобувачів в області сучасних інформаційних технологій. Розглянуто актуальні проблеми комп'ютерних наук, комп'ютерної інженерії, прикладної математики й інженерії програмного забезпечення, приведено ряд робіт по впровадженню інформаційних технологій у виробництво та управління. Висвітлено перспективні розробки сучасних систем пошуку, обробки й захисту інформації, медійних та комунікаційних системи.

УДК 004:37:001:62

Матеріали конференції відтворені з авторських оригіналів, друкуються в авторській редакції та наведені в алфавітному порядку прізвищ авторів. При макетуванні можливі незначні зміни компоновки контенту авторських оригіналів. Відповідальність за якість та зміст публікацій несе автор.

Участь у конференції та складові всіх її етапів (розгляд праць, перевірка на плагіат, макетування, публікація збірника наукових праць та видача сертифікатів) є безкоштовними для всіх учасників. Оргкомітет конференції висловлює подяку учасникам конференції та сподівається на подальшу співпрацю.

З питань проведення конференції та подальшого обміну інформацією звертатись на e-mail конференції: *apkt.khnu@gmail.com*





Міністерство освіти і науки України
Хмельницький національний університет


# ЗБІРНИК НАУКОВИХ ПРАЦЬ

за матеріалами XVII Всеукраїнської науково-практичної конференції
«Актуальні проблеми комп'ютерних наук АПКН-2025»

***14-15 листопада 2025***

Хмельницький 2025

УДК 004.056.5

Мельник М.М., Дзіблюк К.С., Навроцька К.В., Чешун В.М.

*Хмельницький національний університет*

## АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ ДЛЯ РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

*В роботі розглядаються особливості розслідування кіберінцидентів у всіх сферах діяльності критичної інфраструктури України. Основний напрямок зосереджений на виявленні, розкриті, розслідувані та документації подій. Також враховано довід Європи, США та інших країн.*

*The paper examines the specifics of cyber incident investigation in all areas of critical infrastructure activity in Ukraine. The main focus is on the detection, disclosure, investigation, and documentation of events. Evidence from Europe, the USA, and other countries is also taken into account.*

Прогрес розвитку інформаційних технологій у суспільстві характеризується великим обсягом цифрових даних та зростанням кількості загроз та кіберінцидентів в усіх сферах життя та на об'єктах критичної інфраструктури, що спрямованні на порушення цілісності, доступності та конфіденційності важливих державних інформаційних ресурсів. Особливої уваги потребує питання вчасного виявлення, реагування та розслідування кіберінцидентів. Захист інформації – це перший етап забезпечення безпеки, проте, рівень кіберзлочиності зростає кожного дня. Важливо розуміти, що робити коли вже відбувається інцидент. В цій статті розглянуто етапи кіберінцидентів та методи, що можуть забезпечити швидку реакцію на інциденти та завершити атаки на початковому етапі.

**Метою дослідження** є аналіз сучасних підходів до розслідування кіберінцидентів та розроблення методичних рекомендацій для впровадження ефективного процесу реагування у державних інформаційних системах.

Відповідно до даних CERT-UA з початку 2025 року фіксується близько 15 кіберінцидентів на день та існує понад 150 кластерів кіберзагроз. Основне джерело для більшість загроз на інфраструктуру України є росія [1, 2]. Найбільш поширеними типами хакерської активності є шпигунство, саботаж та фінансово вмотивовані злочини. За період 2022-2025 стали поширені атаки на військову інфраструктуру та військовослужбовців. [8]

Активна цифровізація державного управління, впровадження електронних сервісів та систем обробки даних призводить до збільшення кількості кіберінцидентів, що становлять серйозну загрозу для стабільності функціонування державних інформаційних систем [1, 2]. Сучасні кібератаки характеризуються високим рівнем складності, цілеспрямованістю та використанням методів соціальної інженерії, що ускладнює їх своєчасне виявлення та нейтралізацію [3].

Незважаючи на наявність нормативно-правової бази України у сфері кібербезпеки – зокрема, Законів України «Про основні засади забезпечення кібербезпеки України» [4], «Про інформацію» [5], «Про захист інформації в інформаційно-телекомунікаційних системах» [6] – більшість державних установ не мають чітко визначених процедур розслідування інцидентів інформаційної безпеки. Це ускладнює процеси збору цифрових доказів, аналізу причин інцидентів та формування звітів, що відповідають міжнародним вимогам [7].

Ключовою проблемою є відсутність уніфікованого методу розслідування кіберінцидентів, який би враховував специфіку архітектури державних IT-систем, різнорівневість доступу до ресурсів, а також обмеження у технічному забезпеченні. Через це процес реагування часто має фрагментарний характер, а взаємодія між адміністраторами систем, фахівцями з ІБ та аналітиками CERT здійснюється без належної координації [8].

Міжнародний досвід, викладений у стандартах ISO/IEC 27035:2023 [9] та NIST SP 800-61 Rev.2 [10], демонструє ефективність системного підходу до управління кіберінцидентами, який включає етапи виявлення, аналізу, реагування, документування та вдосконалення процесів. Також цінними є рекомендації ENISA [11] і CERT-EU, що деталізують практичні аспекти організації роботи команд реагування на інциденти у державному секторі (таблиця 1).

Отже, актуальною задачею є розроблення адаптованого методу розслідування кіберінцидентів для державних інформаційних систем України, який би поєднував вимоги міжнародних стандартів з можливостями національної інфраструктури кіберзахисту.

Виклад основного матеріалу. Розслідування кіберінцидентів у державних інформаційних системах є одним із ключових напрямів забезпечення кіберстійкості державного сектору. На відміну від приватних організацій, державні структури мають справу з конфіденційними даними, які становлять державну таємницю або містять персональні відомості громадян, що робить їх потенційною ціллю для складних цілеспрямованих атак [1, 2].

Згідно зі стандартом ISO/IEC 27035:2023, процес управління інцидентами інформаційної безпеки включає п'ять основних етапів: підготовку, виявлення, оцінювання, реагування та відновлення [3]. У контексті державних інформаційних





систем особливо важливим є перший етап – підготовка, який передбачає створення політики реагування, формування команди CSIRT (Computer Security Incident Response Team), налаштування моніторингу та визначення каналів комунікації між підрозділами [4].

Математична модель оцінювання ризику кіберінциденту використовується узагальнена формула [10]:

$$R=P_i \times I_i$$

де $P_i$ – ймовірність виникнення інциденту; $I_i$ – вплив інциденту (наслідки).

Таблиця 1 – Організація реагування на інциденти в різних країнах

| Країна | Відповідальний орган / структура | Основна модель реагування | Стандарти | Ключові інструменти та технології | Особливості та результати впровадження |
|---|---|---|---|---|---|
| США | US-CERT (Department of Homeland Security) | "Incident Lifecycle" за NIST | NIST SP 800-61 Rev.2, ISO/IEC 27035 | Splunk ES, QRadar, STIX/TAXII, MISP | Централізована система моніторингу інцидентів у державних установах; високий рівень автоматизації реагування. |
| Велика Британія | National Cyber Security Centre (NCSC) | Модель реагування "Cyber Essentials" | ISO/IEC 27035, ISO/IEC 27001 | ArcSight, AlienVault, TheHive, Cortex | Високий рівень стандартизації процесів; обов'язкові політики реагування для державного сектору. |
| Естонія | CERT-EE (Information System Authority) | Національна інтегрована система кіберзахисту | ISO/IEC 27035, NIST SP 800-61 | MISP, ELK Stack, Suricata, Wireshark | Повна інтеграція між державними IT-системами; оперативне реагування на національному рівні. |
| Німеччина | BSI-CERT (Federal Office for Information Security) | Модель BSI IT-Grundschutz | ISO/IEC 27001, ISO/IEC 27035 | SIEM BSI Suite, OpenVAS, Nessus, Cortex | Висока регламентація процедур; глибокий аудит IT-інфраструктури держустанов. |
| Україна | CERT-UA, ДССЗЗІ України | Формування національної системи реагування | ISO/IEC 27035, NIST SP 800-61, Закон №2163-VIII | Wazuh, ELK Stack, MISP, IBM QRadar | Активна розбудова національної системи кіберзахисту; створення навчальних лабораторій у ЗВО. |

Важливим інструментом для реалізації методів розслідування є впровадження систем централізованого моніторингу безпеки (SIEM), зокрема таких як Wazuh, ELK Stack (Elasticsearch, Logstash, Kibana) або IBM QRadar, що дозволяють збирати, корелювати та аналізувати події з різних джерел [5].

Методика розслідування, запропонована у дослідженні, базується на поєднанні вимог ISO/IEC 27035 та NIST SP 800-61 Rev.2 [6], які визначають структурований підхід до інцидент-менеджменту. Згідно з рекомендаціями NIST, процес складається з таких етапів: підготовка, виявлення та аналіз, усунення, нейтралізація та відновлення, післяінцидентний аналіз [7]. Додатковим елементом методу є використання форензик-інструментів – Autopsy, Volatility, FTK Imager, Wireshark, що дозволяють відновлювати хронологію подій, аналізувати трафік та ідентифікувати джерела компрометації [8].

Запропонована методика передбачає створення локального полігону розслідування кіберінцидентів, який дозволяє моделювати атаки, фіксувати події, проводити аналіз логів та тестувати алгоритми реагування без ризику для реальних систем. Вона може бути адаптована для використання у державних установах, де є потреба у створенні безпечних середовищ для відпрацювання сценаріїв реагування на інциденти без залучення зовнішніх систем [9]. Впровадження розробленого підходу дає можливість:

– скоротити час виявлення та реагування на інциденти;

– уніфікувати дії фахівців при розслідуванні;

– підвищити якість документування доказової бази;

– забезпечити відповідність вимогам міжнародних стандартів у сфері кібербезпеки [10, 11].

Таким чином, запропонований метод розслідування кіберінцидентів дозволяє підвищити рівень готовності державних інформаційних систем до реагування на загрози, мінімізувати наслідки атак і сформувати основу для подальшої автоматизації процесів кіберзахисту.

**Висновок.** Проведене дослідження показало, що ефективне розслідування кіберінцидентів у державних інформаційних системах потребує комплексного підходу, який поєднує технічні, організаційні та процедурні заходи. Аналіз існуючих міжнародних стандартів (ISO/IEC 27035, NIST SP 800-61 Rev.2, ENISA Guidelines) та нормативно-правової бази України свідчить про необхідність адаптації кращих світових практик до національних умов функціонування державного сектору. Запропонований метод розслідування передбачає поетапну процедуру: виявлення інциденту, класифікацію, збір цифрових доказів, аналітичну обробку, формування звіту та коригування політик безпеки. Реалізація такого





підходу дозволяє скоротити час реагування на інциденти, знизити рівень інформаційних ризиків і підвищити достовірність результатів розслідування.

**Перелік посилань**

1. Symantec. Internet Security Threat Report. 2023. URL: https://devfolio.co/projects/symantec-internet-security-threat-report-pdf-c39e (date of access: 25.10.2025).
2. Kaspersky. Incident Response Trends 2024. Kaspersky Lab, 2024. URL: https://securelist.com/kaspersky-incident-response-report-2024/115873/ (date of access: 25.10.2025).
3. ENISA Threat Landscape 2025/ European Union Agency for Cybersecurity, 2025. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025 (date of access: 25.10.2025).
4. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : редакція від 20.04.2025. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 28.08.2025).
5. Про інформацію : Закон України від 02.10.1992 № 2657-XII : редакція від 14.06.2025. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 28.08.2025).
6. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР : редакція від 20.04.2025. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 28.08.2025).
7. Державна служба спеціального зв'язку та захисту інформації України. Звіт про стан кібербезпеки України за 2024 рік. URL:https://h7.cl/1iD43 (date of access: 25.10.2025).
8. Методичні рекомендації щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі. Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 03 липня 2023 року № 570. URL: https://h7.cl/1iD47 (date of access: 25.10.2025).
9. ISO/IEC 27035:2023. Information technology. Information security incident management. Part 1: Principles and process. URL: https://www.iso.org/ru/standard/78973.html (date of access: 25.10.2025).
10. NIST SP 800-61 Rev.2 — Computer Security Incident Handling Guide. URL: https://csrc.nist.gov/pubs/sp/800/61/r2/final (date of access: 25.10.2025).
11. ENISA. Best Practices For Cyber Crisis Management. 2024. URL: https://h7.cl/1iD4a (date of access: 25.10.2025).

УДК 330.111.66:005.8
С 91

**С 91** **Сучасні комп'ютерні системи та технології**: матеріали VIII Всеукр. наук.-практ. інтернет-конф. студентів, аспірантів та молодих вчених за тематикою «Сучасні комп'ютерні системи та мережі в управлінні» (24 листопада 2025 р., м. Херсон, м. Хмельницький) / за ред. А. А. Григорової. – Херсон: Книжкове видавництво ФОП Вишемирський В. С., 2025. – 229 с.

**ISBN 978-617-8187-62-0 (електронне видання)**
**https://doi.org/10.5281/zenodo.17711825**

Доповіді наукової конференції містять результати наступних досліджень: сучасні тенденції розвитку інформаційних технологій; впровадження інновацій та сучасних технологій; моделювання та оптимізація систем управління; інформаційні технології в науці, освіті, економіці, логістиці, туристичній сфері, транспорті; новітні технології в енергетичних системах та в галузі енергозбереження.

Роботи друкуються в авторській редакції, в збірці максимально зменшено втручання в обсяг та структуру відібраних до друку матеріалів. Редакційна колегія не несе відповідальність за достовірність статистичної та іншої інформації, що надано в рукописах, та залишає за собою право не розподіляти поглядів деяких авторів на ті чи інші питання.

Збірник становить інтерес для студентів, аспірантів, викладачів та наукових працівників.



**УДК 330.111.66:005.8**

ISBN 978–617–8187–62–0 (електронне видання)



Міністерство освіти і науки України
Херсонський національний технічний університет
Вінницький національний технічний університет
Криворізький національний університет
Кременчуцький національний університет ім. М. Остроградського
Хмельницький національний університет
Львівський національний університет
ветеринарної медицини та біотехнологій імені С.З. Ґжицького

***Матеріали***

***VIII Всеукраїнської***

***науково-практичної інтернет-конференції***

***молодих вчених та студентів***

# «Сучасні інформаційні системи та технології»

за тематикою:
***«Сучасні комп'ютерні системи та мережі в управлінні»***

*24 листопада 2025 року*
*Хмельницький*

UDC 004.056.5

***Melnyk M. M.,***
*2nd year master of the specialty "Cybersecurity and Information Protection" OPP "Cybersecurity and Information Protection"[1]*

***Oleksiuk D. A.,***
*lecturer[2]*

***Cheshun V. M.,***
*PhD, associate professor, Department of Cybersecurity[1]*

## A COMPREHENSIVE CYBER INCIDENT RESPONSE MODEL FOR CRITICAL INFRASTRUCTURE FACILITIES IN UKRAINE

*Khmelnytskyi National University, Ukraine[1]*
*Khmelnytskyi Professional College of Economics and Technology UEP, Ukraine[2]*

**Statement of the problem**

The digital transformation of the government sector is directly linked to a sustained increase in the volume and sophistication of cyber incidents. Reports, including the ENISA Threat Landscape Report 2025 [1], confirm that over 53% of recorded incidents target key entities such as public administration, transport, finance, and critical infrastructure (CI). In Ukraine, a similar trend is confirmed by reports from the State Service for Special Communications and Information Protection [2] and the Computer Emergency Response Team CERT-UA [3], which document a significant escalation in attack complexity, often involving multi-vector approaches, social engineering, supply chain attacks, and destructive wiper malware [2]. Focused attacks, such as those by groups UAC-0184 and UAC-0200 against military targets, underscore the hostile environment [3]. In this context, cyber incident investigation and response is a critical element of national cybersecurity, necessary not only for mitigation but also for collecting digital evidence, analyzing root causes, and developing proactive countermeasures.

**Analysis of recent research and publications**

Contemporary scientific literature on Cyber Incident Response (CIR) is built upon the synthesis and modification of three primary classical models.

The NIST SP 800-61 Rev.2 [4] framework, the most widely adopted, defines a four-phase lifecycle (Preparation; Detection and Analysis; Containment, Eradication, and Recovery; Post-Incident Activity). It heavily emphasizes the integration of Cyber Threat Intelligence (CTI) and automation (SOAR).

The SANS Incident Handler's Handbook [5] ("Six Steps of SANS") adopts a more operational and forensically-oriented sequence, prioritizing rapid Containment and integrating digital forensics into the identification phase.

The ISO/IEC 27035 [6] international standard provides a management-centric approach, crucial for integrating the response process into the organization's Information Security Management System (ISMS) for regulatory compliance.

Modern research [7-11] highlights a shift from purely technical steps to comprehensive, integrated, and risk-oriented models. These adapt classical frameworks to address the complexities of hybrid threats, cloud environments, and the strict requirements of regulators like GDPR and NIS2.

**Problem statement**

Given the persistent volume of targeted, sophisticated attacks on CI, traditional detection-only approaches are proving insufficient. A holistic and integrated response model covering the entire life cycle of a cyber incident from initial detection to post-incident improvement is essential to transition from a reactive to a proactive security posture.

The development of an effective model requires interconnected components for data collection and correlation, rapid decision-making, and centralized coordination. Success is contingent upon key

principles: continuity, automation, standardization of reporting, and seamless interagency interaction.

Critically, the model must be tailored to the Ukrainian cyberspace, specifically addressing challenges like varying technological maturity and limited resources. This mandates an approach that combines centralized control through national platforms like CERT-UA with localized incident management.

**Presentation of the main material**

The proposed Cyber Incident Response Process Model for Critical Infrastructure is conceptually structured as a sequence of major stages, each with its own defined objectives, specific tasks, and measurable expected outcomes. The generalization of this critical process is summarized in the referenced Table 1.

Table 1

| № | Stage | Description |
|---|---|---|
| 1 | Preparation | Forming policies, establishing a CSIRT team, setting up communication channels, preparing tools and response plans. |
| 2 | Detection and Identification | Collection, analysis, and correlation of security events, determination of the incident type, scale, and criticality level. |
| 3 | Containment (Response) | Incident containment (localization), isolation of compromised systems, elimination of malicious components, and restoration of functionality. |
| 4 | Analysis and Reporting | Studying threat sources, analysis of malicious artifacts, preparing technical and managerial reports for leadership. |
| 5 | Recovery and Improvement | Returning systems to normal operation, updating security policies, conducting training sessions, and updating Indicators of Compromise (IoC) databases. |

The full implementation of this comprehensive CIR model requires the explicit integration of technical, organizational, and legal components . It must be viewed not merely as a technical flowchart of actions, but as an integral part of the enterprise's overall Information Security Management System (ISMS) . Such a unified model facilitates the creation of a cohesive, digital security space within which data exchange, incident analysis, and post-incident improvement coalesce to form a continuous cycle for enhancing the cyber-resilience of critical infrastructure assets.

A key defining element in the development of this process model is the establishment of a robust feedback loop between the stages. This implies that every single incident must not only be investigated and resolved but also meticulously analyzed with the explicit goal of improving the effectiveness of future response measures . This continuous analysis forms the crucial cycle of continuous improvement , which is an indispensable component of modern, advanced cyber defense systems.

To further enhance the reliability, accuracy, and operational speed of the response, it is vital to ensure automated artifact collection, centralized log processing , and the integration of analysis results into a shared knowledge base . This can be achieved through the implementation of collaborative threat intelligence platforms such as MISP (Malware Information Sharing Platform), TheHive (Security Incident Response Platform), or Wazuh (Open Source Security Platform) . This approach fosters a security ecosystem where no incident is treated in isolation; instead, each event contributes to the comprehensive global picture of cyber threats facing the sector.

A fundamental aspect of building a truly effective response model is the clear definition of interaction protocols and responsibilities between all system components—ranging from technical monitoring tools and SOC personnel to senior management structures and external regulatory partners. Successful cyber incident investigation is entirely dependent upon synchronized communications, rapid and secure data transfer, and formalized escalation mechanisms .

International best practices strongly emphasize the necessity of creating a distinct information exchange structure that guarantees traceability, authenticity, and timeliness of the response actions. For critical infrastructure entities, this interoperability is particularly crucial because diverse security systems (monitoring, analytical, and managerial) often operate in isolated network segments. Therefore, the CIR



model must mandate not only technical integration but also absolute organizational alignment of actions . This specifically includes establishing formal coordination channels between CERT-UA , industry-specific CSIRT teams, the organization's internal IT services, and relevant state regulators .

A core element of this critical interoperability is the information flow itself, which ensures the systematic exchange of data on security events, indicators of compromise (IoCs), analysis results, and investigation reports. These data flows can be both automated (achieved through deep integration of SIEM, IDS/IPS, and dedicated SOC platforms ) and manual (in the form of formalized communications between designated responsible units).

**Conclusions**

The developed comprehensive incident response model provides a robust solution that delivers not only swift and effective operational response to immediate threats but also ensures the systematic accumulation of knowledge derived from every incident. This capability, in turn, allows organizations to proactively refine security policies, conduct accurate threat forecasting, and ultimately formulate a resilient, proactive strategy for cyber defense across the entire government and critical infrastructure sector.

**References**


1. ENISA Threat Landscape 2025. URL: https://tinyurl.com/386mxhwf (date of access: 16.11.2025).
2. Звіт ДЦКЗ Держспецзв'язку про роботу Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки (СВВ) за І півріччя 2025 року. URL: https://tinyurl.com/2s33tk9a (дата звернення: 11.11.2025)
3. Огляд кіберзагроз та стратегій захисту в 2025 році: досвід CERT-UA. URL: https://tinyurl.com/5xyn3be7 (дата звернення: 19.11.2025).
4. NIST SP 800-61 Revision 2, Computer Security Incident Handling Guide. URL: https://csrc.nist.gov/pubs/sp/800/61/r2/final (date of access: 18.11.2025).
5. Incident Handler's Handbook. SANS Institute. URL: https://www.sans.org/white-papers/33901 (date of access: 18.11.2025).
6. ISO/IEC 27035-1:2023. Information security incident management. URL: https://www.iso.org/ru/standard/78973.html (date of access: 19.11.2025).
7. Rajiv Katos. Dynamic Risk Assessment Models for Predictive Threat Intelligence and Proactive Incident Response in Complex Cybersecurity Ecosystems. International Journal of Cyber Security. 2025. №6(1). P.1-8. URL: https://tinyurl.com/t6w6ywwe (date of access: 18.11.2025).
8. Tope Oladele Jooda. The impact of business continuity planning on cybersecurity risk management in financial institutions. World Journal of Advanced Engineering Technology and Sciences. 2025. №14(03). P.56-66. URL: https://tinyurl.com/kd9wrazr (date of access: 18.11.2025).
9. Gaurav Malik. Business Continuity & Incident Response. Journal of Information Systems Engineering and Management. 2025. Vol. 10, №45. P. 451-473. DOI: https://doi.org/10.52783/jisem.v10i45s.8891 (date of access: 15.11.2025).
10. Implications of GDPR and NIS2 for Cyber Threat Intelligence Exchange in Hospitals / Rajamäki Jyri et al. Wseas Transactions on Computers. 2024. №23. P.1-11. DOI: 10.37394/23205.2024.23.1. (date of access: 19.11.2025).
11. Sandra Schmitz-Berndt. Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive, Journal of Cybersecurity, 2023. Volume 9, Issue 1. tyad009,1-11. DOI: https://doi.org/10.1093/cybsec/tyad009 (date of access: 19.11.2025).
12. Cyber Threats in Hospitals: GDPR and NIS2 Regulations in Preventing USB Injections / Tikanmäki Ilkka, Rajamäki Jyri, Boateng Forster, Kaikkonen Jesse, Ketene Batuhan, Lehtiaho Joni, Miestamo Jussi. International Conference on Cyber Warfare and Security. 2025. №20. P.461-468. DOI: 10.34190/iccws.20.1.3308 (date of access: 19.11.2025).

УДК 004.056

**МАР'ЯНА МЕЛЬНИК**
Хмельницький національний університет
https://orcid.org/0009-0000-2137-8721
e-mail: melnyk.masia@gmail.com
**ЧЕШУН ВІКТОР**
Хмельницький національний університет
https://orcid.org/0000-0002-3935-2068
e-mail: cheshunvn@khmnu.edu.ua
**ОЛЕКСЮК ДМИТРО**
Хмельницький фаховий економіко-технологічний коледж УЕП
https://orcid.org/0009-0006-3735-1930
e-mail: oleksuk.dima@gmail.com
**ЧЕШУН ДМИТРО**
Хмельницький фаховий економіко-технологічний коледж УЕП
https://orcid.org/0009-0007-9937-9450
e-mail: dmitry_95@ukr.net

# СИСТЕМОЛОГІЧНИЙ ПІДХІД ДО РОЗСЛІДУВАННЯ КІБЕРІНЦИДЕНТІВ В НОРМАТИВНО-ПРАВОВОМУ ПОЛІ УКРАЇНИ ТА МІЖНАРОДНИХ СТАНДАРТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

*Дослідження присвячене комплексному аналізу організаційних, методологічних та технологічних аспектів розслідування кіберінцидентів (DFIR) у державних інформаційних системах та на об'єктах критичної інфраструктури, що функціонують в умовах інтенсивних гібридних загроз. Обґрунтовано, що DFIR виконує стратегічну функцію, перетворюючись на механізм забезпечення національної кіберстійкості шляхом ітеративного застосування моделі NIST SP 800-61 Rev. 2 та вимог ISO/IEC 27035 щодо управління інцидентами та збереження доказів. Визначено критичні технологічні імперативи: впровадження SIEM та UEBA, а також обов'язкова інтеграція з платформами обміну MISP. Проведено компаративний аналіз міжнародних моделей і доведено оптимальність гібридного підходу для національної системи. Критичний огляд виявив системні дефіцити української практики: низький рівень автоматизації моніторингу, інституційну фрагментацію обміну індикаторами компрометації та гострий дефіцит фахівців із цифрової криміналістики. У зв'язку з цим, запропоновано комплексний, інтегрований метод розслідування, що передбачає уніфікацію процедур, імплементацію гібридної організаційної моделі та технологічне посилення через поєднання автоматизованих інструментів аналізу (SIEM, MISP) із формалізованими процедурами реагування. Реалізація підходу критична для скорочення часу розслідування та підвищення стійкості критичної інфраструктури.*

*Ключові слова: нормативно-правове регулювання, інформаційна безпека, цифрова криміналістика, розслідування кіберінцидентів.*

**MARIANA MELNYK, CHESHUN VIKTOR**
Khmelnytsky National University
**OLEKSIUK DMYTRO, CHESHUN DMYTRO**
Khmelnytskyi Vocational Economic and Technological College of the UEE

# SYSTEMOLOGICAL APPROACH TO THE INVESTIGATION OF CYBER INCIDENTS IN THE REGULATORY AND LEGAL FIELD OF UKRAINE AND INTERNATIONAL INFORMATION SECURITY STANDARDS

*This research provides a detailed and systemological analysis of the organizational, methodological, and technological dimensions of Digital Forensics and Incident Response (DFIR) implementation within governmental information systems and critical national infrastructure facilities. This operational domain is currently subjected to extreme pressure due to the intense and sustained nature of hybrid threats. The paper fundamentally substantiates that DFIR transcends a purely technical or reactive function, fulfilling a primary strategic role by transforming into a robust, cyclical mechanism essential for guaranteeing national cyber resilience and ensuring state stability. This crucial transformation is meticulously examined through the lens of recognized international standards, notably the four-phased model detailed in NIST SP 800-61 Rev. 2, and the stringent requirements of ISO/IEC 27035:2023 concerning incident management and the legally verifiable preservation of digital evidence. Key technical imperatives for achieving effective national response capabilities are clearly defined: these include the necessity for ubiquitous and consistent deployment of sophisticated Security Information and Event Management (SIEM) and User and Entity Behavior Analytics (UEBA) systems. Furthermore, the mandatory integration with specialized Threat Intelligence (TI) exchange platforms, such as the Malware Information Sharing Platform (MISP), is identified as a non-negotiable condition for achieving real-time threat synchronization and enabling coordinated containment actions. A critical review of existing national practices in Ukraine revealed pervasive systemic deficiencies. These structural weaknesses include a critically low level of monitoring*

*automation, institutional fragmentation in the protocols for exchanging Indicators of Compromise (IoC), and a significant deficit of highly qualified digital forensics specialists. In direct response to these profound systemic shortcomings, a comprehensive, integrated cyber incident investigation methodology is formally proposed. Reinforcement is to be achieved through the symbiotic combination of automated analytical tools (including SIEM, MISP, and advanced forensic suites) with strictly formalized, standardized, and legally binding response and reporting procedures.*

*Keywords: regulatory and legal regulation, information security, digital forensics, cyber incident investigation.*

**Вступ**

Зі вступом світу в епоху тотальної цифровізації та прискореної трансформації державного сектору, де критично важливі послуги переносяться в онлайн-середовище, кількість, інтенсивність та складність кіберінцидентів постійно зростає, набуваючи загрозливих масштабів. Це явище стало глобальною тенденцією, що визначена як пріоритетний виклик для національної безпеки. Відповідно до ключових аналітичних звітів, зокрема, звіту Агенції Європейського Союзу з питань кібербезпеки ENISA [1], чітко простежується концентрація атак на життєво важливих секторах економіки та державного управління. За даними звіту, на ключові суб'єкти господарювання, які охоплюють державне управління, транспортну логістику, цифрову інфраструктуру та послуги, фінансовий сектор і промислове виробництво, припадає понад половина (53,7%) від загальної кількості зареєстрованих інцидентів. Це свідчить про те, що цілями зловмисників є саме ті системи, збій у роботі яких може спричинити найбільший соціальний та економічний ефект, що найчастіше робиться з метою шпигунства, економічного саботажу чи дестабілізації.

У відповідь на цю системну загрозу Європейський Союз ухвалив Директиву NIS2 про заходи для високого спільного рівня кібербезпеки в ЄС (EU Directive 2022/2555) [2], яка значно посилює вимоги до кіберстійкості організацій у ключових секторах, вводячи жорсткі зобов'язання щодо управління ризиками та звітності про інциденти. Цей нормативний акт відображає глобальне усвідомлення того, що кібербезпека більше не є лише технічною проблемою, а стратегічним питанням стійкості держави та суспільства.

В Україні, яка перебуває під постійним гібридним тиском, ця загрозлива тенденція підтверджується і набуває особливої гостроти. Звіти Державної служби спеціального зв'язку та захисту інформації (Держспецзв'язку) [3] та Команди реагування на комп'ютерні надзвичайні події України CERT-UA [4] фіксують не просто кількісне зростання, а й якісну еволюцію ворожих кібероперацій. Атаки стали більш цілеспрямованими, тривалими та складними, часто використовують комбінацію витончених тактик, технік і процедур (TTPs). До них належать масові кампанії соціальної інженерії та фішингу, націлені на персонал, атаки на ланцюги постачання програмного забезпечення та сервісів для компрометації кінцевих користувачів, а також застосування високодеструктивного шкідливого програмного забезпечення типу wiper – спеціалізованих програм, метою яких є не викрадення, а повне та незворотне знищення даних, що є характерним інструментом кібервійни [3]. Особливо зросла кількість цілеспрямованих атак, які концентруються на військових об'єктах та критичній інфраструктурі, що підтверджується активністю таких відомих російських угруповань, як UAC-0184 і UAC-0200 [4], які використовують кіберпростір як поле бою для збору розвідувальної інформації та порушення функціонування систем.

У такому екстремальному та постійно мінливому контексті розслідування кіберінцидентів (Digital Forensics and Incident Response – DFIR) стає не просто функцією, а критичним, незамінним елементом державної кібербезпеки. Його роль виходить далеко за межі звичайного усунення наслідків події та відновлення працездатності систем. Розслідування є єдиним надійним механізмом, що має забезпечувати накопичення якісних цифрових доказів із дотриманням ланцюга збереження (chain of custody), необхідних для встановлення юридичної відповідальності.

**Аналіз досліджень та публікацій**

Систематизовані докази кіберзлочинів дозволяють провести глибокий аналіз першопричин інциденту (Root Cause Analysis), що включає ідентифікацію початкової точки проникнення (Initial Access), аналіз інструментів, що використовувалися зловмисником, та виявлення прихованих точок закріплення (Persistence) [5,6].

Отримані дані дозволяють сформувати детальний профіль загроз (Threat Profile), який є основою для стратегічного планування захисту [7]. Фахівці використовують результати розслідування для розуміння тактик, технік і процедур (TTPs), які використовують ворожі групи, та їхніх кінцевих цілей, що дозволяє проактивно розробляти та впроваджувати заходи запобігання подібним інцидентам у майбутньому [7,8].

В аналітичному звіті директора з корпоративного та брендового маркетингу кібербезпеки Xage Security [9] наведено огляд реальних інцидентів, що ілюструють еволюцію векторів атак на КІ. Серед них виявлення трьох нульових вразливостей у продуктах Cisco, відомих як ArcaneDoor, які були використані для компрометації IT-систем. Також наголошується на появі шкідливого ПЗ FrostyGoop, спеціально розробленого для експлуатації протоколу Modbus в середовищах ICS. Ці приклади прямо вказують на необхідність форензики, адаптованої до промислових протоколів, що вимагає специфічних знань та інструментів для розслідування.

Сучасні наукові дослідження в галузі цифрової криміналістики державного сектору та критичної інфраструктури (КІ) зосереджені на трьох ключових напрямках: автоматизація DFIR-процесів за допомогою штучного інтелекту, розробка моделей стійкості КІ до цільових атак та удосконалення методів управління

інцидентами в умовах гібридних загроз.

Публікації останніх років, особливо українських та європейських авторів, містять потужний акцент на кіберстійкості та протидії державним (APT) атакам. У роботі [10] розроблено інноваційну, керовану даними модель кіберстійкості, призначену для оцінки та підвищення здатності КІ відновлюватися після кібератак. Автори підкреслюють, що у відповідь на складність загроз, захист і відновлення стають невідкладними потребами, а стійкість вимірюється не лише запобіганням, але й швидкістю та повнотою відновлення.

Дослідження [11] відзначає, що загрози КІ посилюються через складні атаки на ланцюги постачання, соціальну інженерію та використання нульових вразливостей. Вони виступають за посилення співпраці між державним і приватним секторами та впровадження архітектур Zero Trust для мінімізації ризику. Робота [12] конкретизує ці виклики, зазначаючи, що сучасні загрози вже не обмежуються вірусами чи фішингом, а включають державні APT-атаки, що використовують приховані та високоскладні методи для проникнення в мережі та саботажу, що робить розслідування набагато складнішим.

В роботі [13] авторами акцентовано увагу на необхідності комплексного аналізу ризиків. Автори формулюють модель загроз для КІ, виділяючи тріаду основних дій для захисту: впровадження ефективних заходів безпеки, регулярний моніторинг мереж та навчання персоналу.

У контексті КІ, де важлива не лише швидкість, але й точність, дослідження [14] пропонує гібридні алгоритми машинного навчання для проактивного пошуку загроз. Автори використовують реальні дані з відкритих джерел, що імітують аномалії в банківських транзакціях та SWIFT-атаках (типові для фінансової КІ), доводячи, що гібридні моделі ефективніші у виявленні аномалій у потоках даних у реальному часі.

Низка досліджень підкреслює необхідність автоматизації етапів цифрової криміналістики та реагування на інциденти (DFIR) через зростаючий обсяг даних та швидкість сучасних атак. У роботі [15] аналізується інтеграція машинного навчання та роботизованої автоматизації процесів (RPA) у DFIR-робочі процеси. Автори стверджують, що ручні DFIR-процеси є занадто ресурсомісткими та повільними для реагування на сучасні адаптивні загрози (наприклад, поліморфний зловмисний код). Застосування штучного інтелекту (ШІ) пропонується для автоматизації збору доказів, розпізнавання патернів атак та прискорення часових затримок, які виникають під час ручного аналізу журналів. Подібні висновки містяться і в дослідженні [16], де підкреслюється, що ШІ здатен трансформувати DFIR з реактивного процесу на проактивну, інтелектуальну систему безперервного захисту.

Особлива увага приділяється моделюванню загроз та управлінню інцидентами, зважаючи на унікальну складність операційних технологій (OT) та систем промислового контролю (ICS). У статті [17] пропонується метод управління IT-інцидентами в об'єктах критичної інформаційної інфраструктури (КІІ). Метод комбінує модель загроз STRIDE з методологією багатокритеріального прийняття рішень TODIM, що дозволяє систематично ідентифікувати, оцінювати та пріоритизувати загрози з урахуванням критичності об'єктів КІІ. Експериментальна валідація показала, що такий підхід суттєво покращує безпеку КІІ за рахунок систематичної пріоритизації ризиків.

Проаналізовані публікації демонструють загальносвітову тенденцію до переходу від реактивних до проактивних стратегій захисту. Наукова спільнота чітко зазначає, що виявлення та розслідування атак на державні органи та КІ вимагає парадигмального зсуву від традиційної IT-безпеки до адаптивних, автоматизованих та гібридних DFIR-систем, здатних працювати в умовах високої волатильності, складності та постійного геополітичного тиску.

## Формулювання цілей статті

**Метою роботи є:** формулювання концептуальних положень методу розслідування кіберінцидентів, орієнтованого для застосовування на об’єктах критичної інфраструктури України з урахуванням вимог чинного державного законодавства та міжнародних регулюючих документів.

## Правові і організаційні аспекти виявлення та розслідування атак на об’єкти критичної інфраструктури

Створення та функціональна стійкість національних систем реагування на кіберінциденти та механізмів безперервного моніторингу є не просто технічною вимогою, а стратегічною умовою забезпечення національної кіберстійкості та функціональної цілісності державних інформаційних систем. Недотримання нормативно-правових та технічних вимог, які регламентуються законодавством України, створює системні вразливості, що ставлять під загрозу не лише дискретні організації, але й усю структуру державного управління.

У цих умовах розслідування кіберінцидентів відіграє ключову і, водночас, подвійну роль: тактичну та стратегічну. На тактичному рівні йдеться про оперативну ліквідацію наслідків атаки та відновлення функціональності. На стратегічному рівні DFIR є єдиним механізмом для збору достовірних цифрових доказів, встановлення кореневих причин події, визначення характерних ознак загроз та розробки адаптивних заходів запобігання схожим інцидентам у майбутньому.

Базове концептуальне визначення інциденту інформаційної безпеки надається міжнародним стандартом ISO/IEC 27035:2023 [18]. Цей документ визначає інцидент як подію або низку пов’язаних подій, які становлять реальну або потенційну загрозу для конфіденційності, цілісності чи доступності інформаційних ресурсів (C-I-A Triad). На практиці це охоплює будь-яку аномальну ситуацію, що вимагає негайної, регламентованої реакції з боку уповноважених суб’єктів.

Фундаментальною методологічною основою для організації процесу реагування є Керівництво щодо обробки інцидентів комп'ютерної безпеки Національного інституту стандартів і технологій США NIST SP 800-61 Rev. 2 [19]. Цей стандарт встановлює циклічну, чотирифазну модель, яка підкреслює ітеративний характер процесу розслідування:

- Фаза 1: підготовка (Preparation) – створення інституційної та технічної бази;
- Фаза 2: виявлення й аналіз (Detection and Analysis) – ідентифікація та верифікація інциденту;
- Фаза 3: реагування, стримування (ізоляція), ліквідація та відновлення (Containment, Eradication, and Recovery) – обмеження шкоди та повернення до нормальної роботи;
- Фаза 4: дії після завершення інциденту (Post-Incident Activity) – аналіз уроків та вдосконалення.

Такий підхід трансформує розслідування з реактивного інструменту на фундаментальний компонент кіберстійкості, забезпечуючи безперервне навчання системи та її адаптацію до динаміки кіберзагроз.

Перша фаза зосереджена на створенні формалізованої архітектури реагування. Формується команда реагування на інциденти (CSIRT), яка отримує чіткий мандат, прописуються політики безпеки, визначаються правила роботи з інцидентами (SOP) та створюються канали кризової комунікації – як внутрішні, так і зовнішні. З технічного погляду, критичною є побудова інфраструктури фіксації подій безпеки, що включає збір журналів системних подій, мережевого трафіку та аутентифікаційних подій [19,20]. Ця фаза також включає проактивну діяльність, таку як пошук прихованих загроз та створення високоточних образів систем (forensic images) для швидшого відновлення.

У фазі виявлення та аналізу для оперативного виявлення інцидентів застосовується централізована агрегація логів та подій. Зазвичай, для цього використовуються платформи Security Information and Event Management (SIEM), такі як Wazuh або ELK Stack. Ці системи забезпечують збір, нормалізацію, агрегацію та кореляцію величезних обсягів даних, перетворюючи розрізнені системні повідомлення на осмислені інциденти.

Ключовим завданням цього етапу є ідентифікація індикаторів компрометації. Це можуть бути незвичні спроби входу, підозрілі мережеві активності, маніпуляції з важливими файлами чи запуск аномальних процесів. Для підвищення ефективності виявлення застосовуються такі передові методики [20]:

- аналіз поведінки користувачів та сутностей (User and Entity Behavior Analytics, UEBA);
- системи виявлення вторгнень (IDS/IPS);
- машинне навчання (ML) та штучний інтелект (AI).

Аналіз поведінки користувачів та сутностей застосовується для иявлення аномалій, які відхиляються від встановлених базових ліній нормальної поведінки (наприклад, незвичний час доступу чи обсяг завантажених даних). Системи виявлення вторгнень здійснюють моніторинг мережевого трафіку на основі сигнатур або аномалій. Машинне навчання та ШІ використовуються для автоматичної класифікації подій, виявлення Zero-Day атак та зменшення кількості хибних спрацьовувань тощо.

Етап реагування, стримування, ліквідації та відновлення є найбільш критичним у часовому вимірі. Його головна мета – припинити поширення атаки, зменшити її наслідки та повернути систему до нормального режиму роботи. Стримування включає ізоляцію пошкоджених систем шляхом їх відключення від мережі або застосування мікросегментації для обмеження латерального руху зловмисника. Ліквідація вимагає глибокого форензичного аналізу для видалення всіх прихованих бекдорів, шкідливих файлів та модифікацій, внесених зловмисником. Відновлення базується на перевірці та розгортанні криптографічно чистих резервних копій та встановленні оновлень.

У міжнародному досвіді цей процес посилюється інтеграцією з платформами обміну інформацією про загрози, такими як MISP (Malware Information Sharing Platform) [21]. Це дозволяє командам оперативно обмінюватися індикаторами компрометації (IoC), що значно підвищує швидкість і точність ідентифікації природи загрози. У державних структурах України цей процес обов'язково регламентується затвердженими політиками реагування та узгоджується з органами Державної служби спеціального зв'язку та захисту інформації (ДССЗЗІ) [3,21].

На фінальному етапі (фаза діяльності після інциденту) проводиться детальний аналіз першопричин (RCA) для виявлення фундаментальних прогалин, які дозволили інциденту статися. Результатом є формування технічного звіту, оцінка ефективності застосованих заходів реагування та розробка обгрунтованих рекомендацій для уникнення подібних випадків. Ключовим елементом цієї фази є забезпечення юридичної значущості зібраних артефактів. Стандарт ISO/IEC 27035-3:2020 [22] та вимоги цифрової криміналістики наголошують на необхідності бездоганного документування доказів із дотриманням ланцюга збереження (Chain of Custody), включаючи створення форензичних образів носіїв інформації та підтвердження їхньої цілісності за допомогою криптографічного хешування. Це необхідно для подальшого використання матеріалів у судових або адміністративних розслідуваннях.

Організаційна структура національного реагування на кіберінциденти суттєво варіюється. Сформувалися три основні моделі:

- централізована модель (Європейський Союз);
- децентралізована модель (Сполучені Штати Америки);
- гібридна/змішана модель (країни Балтії).

В централізованій моделі головну роль виконує єдиний національний або наднаціональний центр реагування (CERT/CSIRT), який відповідає за координацію, стандартизацію та обмін інформацією з усіма

галузевими та відомчими командами. Прикладом є CERT-EU [21], який забезпечує взаємодію та реагування на кіберінциденти в інституціях Європейського Союзу, підтримуючи єдиний, узгоджений рівень безпеки відповідно до вимог директиви NIS2. Перевага централізованій моделі у високій упорядкованості дій, централізованому зборі національного профілю загроз та ефективній координації при великомасштабних інцидентах.

В децентралізованій моделі США кожна відомча структура або сектор КІ має власну, значною мірою автономну команду реагування. Зокрема, Міністерство енергетики (DOE), Департамент внутрішньої безпеки (DHS) та Агентство з кібербезпеки і безпеки інфраструктури (CISA) мають окремі, але взаємодіючі підрозділи. Координація відбувається через федеральні протоколи та платформи обміну інформацією (ISACs). Перевага децентралізованої моделі – швидкість реагування у межах власної юрисдикції, глибока доменна експертиза у специфічних секторах (наприклад, енергетика чи фінанси).

Гібридна модель поєднує елементи обох моделей: національний центр кібербезпеки встановлює єдині методологічні стандарти та політики, тоді як безпосереднє реагування здійснюють відомчі підрозділи. Прикладом є Литва та Естонія [23]. Естонія, зокрема, створила добровольче формування Cyber Defence League, яке інтегрує державних і громадських фахівців для участі у розслідуванні масштабних кіберінцидентів, як це було під час масових атак у 2007 році. Ця система забезпечує гнучкість у реагуванні та мобілізацію ресурсів, зберігаючи при цьому централізований контроль над аналітикою.

В Україні процес розслідування кіберінцидентів на об'єктах КІ регламентується Законами «Про основні засади забезпечення кібербезпеки України» [24], «Про захист інформації в інформаційно-телекомунікаційних системах» [25] та Постановою Кабінету Міністрів №518 від 19 червня 2019 року [26], що деталізує порядок реагування. Однак, попри наявність нормативної бази та методичних рекомендацій CERT-UA [21,27], система розслідування стикається з низкою системних проблем, що обмежують її ефективність, особливо в умовах інтенсивних гібридних атак.

Одним із найбільш критичних недоліків є низький рівень автоматизації процесів збору та аналізу подій безпеки. За даними Держспецзв'язку, лише близько 40% об'єктів КІ мають впроваджені системи моніторингу безпеки SIEM [3]. Це означає, що у більшості державних установ моніторинг здійснюється фрагментарно, без централізованої кореляції логів, що ускладнює оперативне виявлення та формування цілісної картини інциденту. На відміну від країн ЄС, де системи Wazuh або ELK Stack інтегруються з платформами обміну MISP [21], в Україні інфраструктура моніторингу залишається горизонтально фрагментованою. Кожен об'єкт часто використовує власні засоби виявлення аномалій, що призводить до різного рівня деталізації даних та істотно ускладнює централізований аналіз загроз.

Недостатня інтеграція між національною CERT-UA та галузевими/відомчими CSIRT-командами призводить до затримки обміну критичною інформацією про атаки та неузгодженості дій під час реагування. Рекомендації ENISA [28] вимагають, щоб ефективна модель взаємодії ґрунтувалася на принципі взаємного обміну даними в режимі реального часу, проте в Україні цей обмін ще не є системним та стандартизованим. Відсутність уніфікованої національної бази індикаторів компрометації, інтегрованої через формати STIX/TAXII [29], як це реалізовано в європейських країнах, змушує команди реагування працювати з застарілими або неповними даними, що значно знижує швидкість виявлення повторюваних атак.

Суттєвою проблемою залишається нестача висококваліфікованих фахівців із цифрової криміналістики (Digital Forensics). Це обмежує спроможність оперативно проводити глибокий технічний аналіз інцидентів (форензика кінцевих точок, мережева форензика, аналіз шкідливого коду). Процес розслідування затримується через дефіцит спеціалістів, здатних професійно застосовувати інструменти, такі як Autopsy, FTK Imager, Volatility (для аналізу дампу пам'яті) чи Wireshark (для мережевого аналізу), з дотриманням криміналістичних вимог. Наявність технічних артефактів без належної експертизи для їхнього аналізу та інтерпретації є недостатньою для встановлення механізмів компрометації та цілей зловмисника.

Крім того, відсутність єдиного формату звітності про інциденти, незважаючи на існування ISO/IEC 27035 [18,22] та методичних рекомендацій CERT-UA [27], створює додаткові труднощі для обміну інформацією між відомствами та для подальшого використання матеріалів у судових процесах. Належне документування та звітність є невід'ємною частиною post-incident activity і має забезпечувати відтворюваність та прозорість розслідування.

**Комплексний підхід до виявлення та розслідування кіберінцидентів**

Для подолання виявлених системних проблем, які критично обмежують ефективність національної кібербезпеки в умовах перманентних гібридних атак, необхідна розробка та впровадження комплексного підходу до виявлення та розслідування інцидентів. Цей підхід має ґрунтуватися на глибокій інтеграції технологічних рішень та організаційно-процедурної уніфікації. На технологічному рівні метод повинен забезпечити автоматизований, безперервний збір та інтелектуальний аналіз подій безпеки. Це досягається за рахунок щільної інтеграції платформ SIEM/ELK (для агрегації та кореляції логів) з системами SOAR (Security Orchestration, Automation and Response), які автоматизують рутинні операції реагування, скорочуючи час, необхідний для первинного стримування. На процедурному рівні критично важливим є запровадження формалізованих і стандартизованих процедур реагування (на основі NIST SP 800-61 Rev. 2 та ISO/IEC 27035), що гарантує юридичну достовірність зібраних доказів та повноту охоплення всіх етапів інциденту. Крім того, ключовим елементом інтеграції є забезпечення системного обміну інформацією про загрози (Threat Intelligence) на

національному рівні через стандартизовані платформи (як-от MISP та формати STIX/TAXII), що дозволяє швидко виявляти повторювані або схожі атаки на різних об'єктах критичної інфраструктури.

Реалізація такого інтегрованого підходу дозволить кардинально підвищити оперативну ефективність реагування на інциденти, скоротити середній час розслідування (Dwell Time – час перебування зловмисника в мережі) та мінімізувати ризики повторного компрометування об'єктів КІ. Це, у свою чергу, є критично важливим для забезпечення сталої кіберстійкості держави в цілому.

Запропонований спосіб розслідування кіберінцидентів базується на фундаментальних принципах циклічності, комплексності та стандартизації. Його стратегічною метою є створення універсального, верифікованого алгоритму дій, який охоплює повний життєвий цикл інциденту – від проактивного виявлення ознак аномалії до формування детальних висновків та обґрунтованих рекомендацій щодо удосконалення архітектури безпеки інформаційних систем. На відміну від традиційних, лінійних підходів, орієнтованих переважно на ізольований аналіз технічних артефактів (форензику), запропонована модель передбачає нерозривну інтеграцію організаційних, процедурних і технічних компонентів у єдину, керовану систему реагування. Ця інтеграція дозволяє значно скоротити середній час реагування на інцидент, підвищити точність класифікації загроз завдяки постійному обміну ТІ та забезпечити бездоганну узгодженість дій між усіма суб'єктами кібербезпеки (CERT-UA, відомчі CSIRT та експертні групи).

Метод передбачає, що розслідування кіберінцидентів здійснюється як жорстка послідовність п'яти взаємозалежних етапів, де кожен має чітко визначену мету, контрольовані вхідні та вихідні дані, стандартизований набір застосованих інструментів і чітко призначених відповідальних осіб. Для забезпечення цієї послідовності та взаємодії критично важливу роль відіграють платформи Wazuh (для збору та моніторингу EDR), ELK Stack (для централізованої аналітики), MISP (для обміну ТІ) та TheHive (як платформа керування інцидентами, що координує всі дії). Всі ці компоненти інтегруються у єдине, високонадійне інформаційне середовище реагування, що мінімізує людський фактор та підвищує прозорість процесу.

Деталізація етапів приведена в таблиці 1.

Таблиця 1

**Етапи методу розслідування кіберінцидентів**

| Етап | Основна мета | Ключові дії | Очікувані результати |
|---|---|---|---|
| Ідентифікація | Виявлення інциденту | Збір логів, аналіз SIEM, фіксація події | Первинне повідомлення |
| Класифікація | Визначення типу і пріоритету | Порівняння з базами IOC, оцінка ризику | Присвоєння рівня критичності |
| Технічний аналіз | Встановлення джерела та механізму | Форензичний аналіз, перевірка логів, реверс шкідливого ПЗ | Виявлення причин інциденту |
| Відновлення | Усунення наслідків | Відновлення даних, оновлення конфігурацій | Відновлена система |
| Документування | Збереження знань | Підготовка звіту, внесення в бази MISP | База знань для попередження атак |

На етапі ідентифікації інциденту проводиться систематичний і безперервний збір інформації про потенційні події безпеки. Джерелами цієї інформації виступають різноманітні телеметричні та логістичні дані, зокрема: системні журнали операційних систем та додатків, мережеві потоки (NetFlow), сигнали від систем виявлення та запобігання вторгнень (IDS/IPS), агреговані дані з платформ SIEM, а також повідомлення, отримані від кінцевих користувачів або внутрішніх підрозділів. Основна мета цього етапу полягає у виявленні будь-яких аномалій, що критично виходять за межі типової чи заздалегідь встановленої базової поведінки мережі, інфраструктури або окремих облікових записів користувачів.

Після первинної фіксації події та її валідації аналітичною системою, ключовим завданням стає визначення, чи є вона дійсним кіберінцидентом (уникаючи хибних спрацьовувань) та встановлення її критичності згідно з внутрішніми політиками та міжнародними стандартами. Аналітик відділу реагування здійснює оперативне порівняння виявлених індикаторів компрометації, таких як підозрілі IP-адреси, шкідливі домени, криптографічні хеші потенційно скомпрометованих файлів або аномальні патерни взаємодії, із записами у базі MISP. Цей крос-аналіз із зовнішніми та внутрішніми базами загроз дозволяє швидко підтвердити природу та походження атаки, що є критично важливим для переходу до наступних, більш рішучих дій зі стримування та ліквідації. Процес вимагає високої точності та швидкості для мінімізації часу перебування зловмисника в системі.

Додатково проводиться оцінка потенційного впливу за критеріями:

- масштаб порушення (локальний, корпоративний, національний);
- категорія активу, на який здійснено вплив (система керування, сервер, користувацька станція);
- наявність загрози безперервності бізнес-процесів.

На цьому етапі класифікації події формується обґрунтоване рішення щодо подальшої долі інциденту: чи передати його для повноцінного розслідування, залучивши форензичні ресурси, чи обмежитися посиленим моніторингом, якщо ризики визнані низькими. Результатом класифікації є присвоєння інциденту рівня пріоритетності реагування, який безпосередньо визначає склад команди, обсяг фінансових та технічних ресурсів,

що будуть задіяні у подальшому процесі, а також встановлює граничні терміни для стримування та ліквідації.

Технічний етап розслідування, який часто називають саме цифровою криміналістикою, є найбільш складним, критичним і ресурсомістким. Він охоплює методологічний збір та обробку цифрових артефактів з усіх скомпрометованих або потенційно скомпрометованих вузлів, а також глибокий форензичний аналіз цих даних. Цей процес є єдиним способом забезпечити встановлення точного механізму атаки, ідентифікувати джерело компрометації (точку входу) та оцінити повні потенційні наслідки вторгнення. Ключова особливість криміналістичного етапу полягає у суворій вимозі: під час аналізу цифрових доказів не допускається їхня модифікація. Тому вся робота проводиться виключно з криптографічно перевіреними копіями (форензичними образами) оригінальних носіїв, що гарантує дотримання ланцюга збереження доказів. Після завершення аналізу збирається детальний ланцюжок подій, який відображає послідовну хронологію дій зловмисника, що дозволяє побудувати вичерпну причинно-наслідкову модель інциденту.

Етап відновлення передбачає комплексне усунення наслідків атаки та повернення скомпрометованих систем до їхнього доінцедентного, стабільного стану. Проводиться відновлення функціональності та даних з чистих, перевірених резервних копій, перевірка цілісності критичних баз даних та конфігураційних файлів, обов'язкове оновлення та скидання облікових записів користувачів з підвищеними привілеями, а також, що є найважливішим, усунення першопричинних вразливостей, через які було здійснено вторгнення. Особливу увагу приділяють системам моніторингу та захисту, які вдосконалюються з урахуванням виявлених уразливостей. Відновлення завершується фінальною верифікацією цілісності цифрових підписів, аутентифікаційних логів та сертифікатів безпеки, що підтверджує успішну ліквідацію.

Після остаточного усунення інциденту всі виконані дії, отримані докази та прийняті рішення повинні бути ретельно задокументовані для формування звіту та аналізу уроків. Формується звіт про розслідування (Incident Report), який містить:

- хронологію подій;
- опис знайдених артефактів;
- результати технічного аналізу;
- рекомендації щодо запобігання подібним подіям.

Дані про інцидент публікуються у MISP, що сприяє обміну інформацією між національними та галузевими CSIRT-командами. Зібрані індикатори надалі використовуються для вдосконалення систем виявлення атак, а також для тренування персоналу на реальних кейсах.

Запропонований метод орієнтований на взаємодію автоматизованих систем і людського фактору. На архітектурному рівні він передбачає взаємодію таких компонентів:

- wazuh/elk stack, виявлення інцидентів, первинна обробка подій;
- thehive – управління кейсами, розподіл завдань між аналітиками;
- misp, обмін індикаторами компрометації, інтеграція з зовнішніми базами даних;
- forensic tools (autopsy, volatility, ftk imager), технічне підтвердження інциденту.

Таким чином, формується замкнутий цикл реагування, де кожен інцидент стає джерелом знань для вдосконалення політик безпеки.

Перевагами пропонованого методу є масштабованість, а саме те, що метод може застосовуватись як у державних органах, так і в комерційних структурах. Сумісність із міжнародними стандартами дозволяє інтегрувати його у національну систему кіберзахисту. Використання Wazuh та TheHive дозволяє зменшити вплив людського фактору та автоматизацію процесів. Кожне розслідування поповнює базу знань, яка використовується для навчання аналітиків [26]. Усі звіти мають єдину структуру, що спрощує взаємодію між командами реагування.

Запропонований метод розслідування кіберінцидентів є комплексною системою, яка забезпечує не лише технічне реагування на події безпеки, а й стратегічне управління кіберризиками. Його впровадження дозволяє створити єдиний стандарт дій для суб'єктів, що обслуговують об'єкти критичної інформаційної інфраструктури.

Метод забезпечує повну трасованість дій, прозорість збору доказів та підвищення ефективності реагування. Завдяки інтеграції інструментів відкритого коду, таких як Wazuh, MISP, TheHive та ELK Stack, він не потребує значних фінансових витрат і може бути реалізований у державних або корпоративних системах моніторингу безпеки.

**Висновки**

За результатами проведеного дослідження було досягнуто глибокого розуміння системних та операційних аспектів розслідування кіберінцидентів у державному секторі та на об'єктах критичної інфраструктури, особливо в умовах інтенсивних гібридних загроз. Доведено, що розслідування кіберінцидентів виконує стратегічну, а не лише тактичну функцію, трансформуючись із засобу ліквідації наслідків на фундамент національної кіберстійкості. Дослідження формалізувало цей процес на основі міжнародних стандартів, зокрема циклічної чотирифазної моделі NIST SP 800-61 Rev. 2 та визначень ISO/IEC 27035.

Критичний огляд національної системи розслідування виявив системні недоліки, які обмежують її ефективність. Зокрема, було встановлено низький рівень автоматизації процесів моніторингу, фрагментацію інфраструктури та недостатню інтеграцію між секторальними та національними командами реагування.

Для підвищення ефективності процесу розслідування кіберінцидентів запропоновано системологічний

підхід, реалізований в нормативно-правовому полі України та міжнародних стандартів інформаційної безпеки.

Запропонований підхід до розслідування кіберінцидентів базується на ідеї комплексного збору, кореляції та аналізу подій безпеки з різних рівнів інформаційної системи. Його основою є поєднання централізованого моніторингу, цифрової криміналістики та обміну інформацією про загрози, що дозволяє розглядати інцидент не як окрему подію, а як послідовний процес із чіткою логікою розвитку.

Метод орієнтований на використання агентного моніторингу кінцевих вузлів, централізованого збору журналів та аналітичних платформ, які забезпечують збереження цілісності цифрових доказів і можливість відтворення хронології подій. Особливу увагу приділено тому, щоб кожен етап розслідування, від виявлення підозрілої активності до відновлення системи, був формалізований і міг бути повторений незалежно від типу інциденту. Концепція методу передбачає інтеграцію різних джерел даних: системних журналів операційних систем, подій безпеки, мережевої активності та артефактів файлової системи. Це дозволяє компенсувати втрату або спотворення окремих даних за рахунок багатоканального збору інформації та підвищує стійкість методу до спроб приховування слідів атаки.

**Література**


1. ENISA Threat Landscape 2025. *European Union Agency for Cybersecurity (ENISA)*. 2025. URL: https://h7.cl/1l8EO (date of access: 15.12.2025).
2. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). European Union. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj (date of access: 6.12.2025).
3. Річний звіт 2024: системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. *Оперативний центр реагування на кіберінциденти Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України.* URL: http://scpc.gov.ua/api/files/72e13298-4d02-40bf-b436-46d927c88006 (дата звернення: 29.11.2025).
4. Огляд кіберзагроз та стратегій захисту в 2025 році: досвід CERT-UA. URL: https://h7.cl/1l8ED (дата звернення: 30.11.2025).
5. Evolution Cybercrime – Key Trends, Cybersecurity Threats, and Mitigation Strategies from Historical Data / Muhammad Abdullah, Muhammad Munib Nawaz, Bilal Saleem, Maila Zahra, Effa binte Ashfaq, Zia Muhammad. *Analytics*. 2025. № 4(3):25. DOI: 10.3390/analytics4030025.
6. Duraid Thamer Salim, Manmeet Mahinderjit Singh, Pantea Keikhosrokiani. A systematic literature review for APT detection and Effective Cyber Situational Awareness (ECSA) conceptual model. *Heliyon*. 2023. Volume 9, Issue 7. DOI: 10.1016/j.heliyon.2023.e17156.
7. Evolving techniques in cyber threat hunting: A systematic review / Arash Mahboubi et al. *Journal of Network and Computer Applications*. 2024. Volume 232. DOI: 10.1016/j.jnca.2024.104004.
8. Gulbay Burak, Demirci Mehmet. A Framework for Developing Strategic Cyber Threat Intelligence from Advanced Persistent Threat Analysis Reports Using Graph-Based Algorithms. *Preprints.org*. 2024. DOI: 10.20944/preprints202407.1408.v1.
9. Celine Rosak. 2024 in Review: Cyber Threats and the Fight to Secure Critical Infrastructure. *Global Security Magazine*. 2024. URL: https://h7.cl/1gfjs (date of access: 15.12.2025).
10. Guarding Our Vital Systems: A Metric for Critical Infrastructure Cyber Resilience / Muharman Lubis, Muhammad Fakhrul Safitra, Hanif Fakhrurroja, Alif Noorachmad Muttaqin. *Sensors*. 2025. № 25(15):4545. DOI: 10.3390/s25154545.
11. Protecting the cybersecurity of critical infrastructures and their supply chains. *ICC Working Paper*. 2024. 35 p. URL: https://h7.cl/1l8E5 (date of access: 8.12.2025).
12. Rajender Pell Reddy. Cybersecurity for Critical Infrastructure: Protecting National Assets in the Digital Age. *International Journal of Computer Trends and Technology (IJCTT)*. 2025. Vol. 73, № 2. P. 7-17. DOI: 10.14445/22312803/ IJCTT-V73I2P102.
13. Cybersecurity challenges and solutions for critical infrastructure protection / A. Tkachov, R. Korolov, I. Rahimova, I. Aksonova. *Ukrainian Scientific Journal of Information Security*. 2024. Vol. 30, issue 1. P. 58-66. DOI: 10.18372/2225-5036.30.18604.
14. Shan A., Myeong S. Proactive Threat Hunting in Critical Infrastructure Protection through Hybrid Machine Learning Algorithm Application. *Sensors*. 2024. № 24(15):4888. DOI: 10.3390/s24154888.
15. John Kuforiji. Digital Forensics and Incident Response (DFIR) Automation: Leveraging AI to Accelerate Breach Investigation, Evidence Collection, and Cyberattack Mitigation. *Journal of Data Analysis and Critical Management*. 2025. Vol. 1, № 04. DOI: 10.64235/tsvfvz27.
16. Artificial intelligence integration in cyber incident response teams to enable faster containment, forensic accuracy, and resilient business continuity / Kwaku Gyamfi Boamah, AFUA Asante, Ashley Timean, Kwadwo Fening Okai. *International Journal of Science and Research Archive*. 2025. №17(01). P.1263-1280. DOI: 10.30574/ijsra.2025.17.1.2933.
17. Method for managing IT incidents in critical information infrastructure facilities / S. Gnatyuk, V. Sydorenko, A. Polozhentsev, V. Sokolov. *CPITS-II 2024: Workshop on Cybersecurity Providing in Information and*

*Telecommunication Systems II*. 2024. URL: https://h7.cl/1l8Dk (date of access: 8.12.2025).

18. ISO/IEC 27035-1:2023 Information technology – Information security incident management – Part 1: Principles and process. *International Organization for Standardization*. 2023. URL: https://h7.cl/1gdGl (date of access: 12.12.2025).

19. NIST SP 800-61 Revision 2, Computer Security Incident Handling Guide. URL: https://csrc.nist.gov/pubs/sp/800/61/r2/final (date of access: 15.12.2025).

20. NIST SP 800-61r3. Incident Response Recommendations and Considerations for Cybersecurity Risk Management – A CSF 2.0 Community Profile / Alex Nelson et al. *National Institute of Standards and Technology*. URL: https://h7.cl/1l6Xp (date of access: 8.12.2025).

21. Роз'яснення CERT-UA: платформа MISP, що це, як підключатися та які переваги. *Державна служба спеціального зв'язку та захисту інформації України.* URL: https://h7.cl/1gfiS (дата звернення: 15.12.2025).

22. ISO/IEC 27035-3:2020 Information technology – Information security incident management – Part 3: Guidelines for ICT incident response operations. *International Organization for Standardization*, 2020. URL: https://www.iso.org/ru/standard/74033.html (date of access: 8.12.2025).

23. Górka Marek. Baltic States Cyber Security Policy: Development of digital capabilities in 2017–2022. *Stosunki Międzynarodowe – International Relations*. Vol. 59. 2023. P. 57-81. DOI:10.12688/stomiedintrelat.17684.1.

24. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : редакція від 19.10.2025. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 16.12.2025).

25. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР : редакція від 20.04.2025. URL: https://h7.cl/1l8Dv (дата звернення: 30.11.2025).

26. Про затвердження Загальних вимог з кіберзахисту об'єктів критичної інфраструктури : Постанова Кабінету Міністрів України; Вимоги, Перелік від 19.06.2019 № 518 : редакція від 20.11.2025. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text (дата звернення: 29.11.2025).

27. Наказ Адміністрації Держспецзв'язку від 03.12.2025 №798 «Про затвердження Методичних рекомендацій щодо типових вимог до підрозділів з кіберзахисту, загальних вимог до керівників з кіберзахисту в органах державної влади, а також до відповідальних осіб, які виконують функції та завдання керівника з кіберзахисту в юридичних особах, що є власниками або розпорядниками об'єктів критичної інформаційної інфраструктури I і II категорій критичності, та в органах місцевого самоврядування». *Державна служба спеціального зв'язку та захисту інформації України.* URL: https://h7.cl/1l6XU (дата звернення: 3.12.2025).

28. Best practices for cyber crisis management. *European Union Agency for Cybersecurity (ENISA)*. 2024. URL: https://h7.cl/1l6lr (date of access: 8.12.2025).

29. Cybersecurity Incident & Vulnerability Response Playbooks. *Cybersecurity and Infrastructure Security Agency (CISA)*. 2021. 44 p. URL: https://h7.cl/1gd8H (date of access: 28.11.2025).

**References**

1. ENISA Threat Landscape 2025. *European Union Agency for Cybersecurity (ENISA)*. 2025. URL: https://h7.cl/1l8EO (date of access: 15.12.2025).

2. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). European Union. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj (date of access: 6.12.2025).

3. Richnyy zvit 2024: systemy vyyavlennya vrazlyvostey i reahuvannya na kiberintsydenty ta kiberataky. Operatyvnyy tsentr reahuvannya na kiberintsydenty Derzhavnoho tsentru kiberzakhystu Derzhavnoyi sluzhby spetsialnoho zvyazku ta zakhystu informatsiyi Ukrayiny. URL: http://scpc.gov.ua/api/files/72e13298-4d02-40bf-b436-46d927c88006 (data zvernennya: 29.11.2025).

4. Ohlyad kiberzahroz ta stratehiy zakhystu v 2025 rotsi: dosvid CERT-UA. URL: https://h7.cl/1l8ED (data zvernennya: 30.11.2025).

5. Evolution Cybercrime – Key Trends, Cybersecurity Threats, and Mitigation Strategies from Historical Data / Muhammad Abdullah, Muhammad Munib Nawaz, Bilal Saleem, Maila Zahra, Effa binte Ashfaq, Zia Muhammad. *Analytics*. 2025. № 4(3):25. DOI: 10.3390/analytics4030025.

6. Duraid Thamer Salim, Manmeet Mahinderjit Singh, Pantea Keikhosrokiani. A systematic literature review for APT detection and Effective Cyber Situational Awareness (ECSA) conceptual model. *Heliyon*. 2023. Volume 9, Issue 7. DOI: 10.1016/j.heliyon.2023.e17156.

7. Evolving techniques in cyber threat hunting: A systematic review / Arash Mahboubi et al. *Journal of Network and Computer Applications*. 2024. Volume 232. DOI: 10.1016/j.jnca.2024.104004.

8. Gulbay Burak, Demirci Mehmet. A Framework for Developing Strategic Cyber Threat Intelligence from Advanced Persistent Threat Analysis Reports Using Graph-Based Algorithms. *Preprints.org*. 2024. DOI: 10.20944/preprints202407.1408.v1.

9. Celine Rosak. 2024 in Review: Cyber Threats and the Fight to Secure Critical Infrastructure. *Global Security Magazine*. 2024. URL: https://h7.cl/1gfjs (date of access: 15.12.2025).

10. Guarding Our Vital Systems: A Metric for Critical Infrastructure Cyber Resilience / Muharman Lubis, Muhammad Fakhrul Safitra, Hanif Fakhrurroja, Alif Noorachmad Muttaqin. *Sensors*. 2025. № 25(15):4545. DOI:

10.3390/s25154545.

11. Protecting the cybersecurity of critical infrastructures and their supply chains. *ICC Working Paper*. 2024. 35 p. URL: https://h7.cl/1l8E5 (date of access: 8.12.2025).

12. Rajender Pell Reddy. Cybersecurity for Critical Infrastructure: Protecting National Assets in the Digital Age. *International Journal of Computer Trends and Technology (IJCTT)*. 2025. Vol. 73, № 2. P. 7-17. DOI: 10.14445/22312803/ IJCTT-V73I2P102.

13. Cybersecurity challenges and solutions for critical infrastructure protection / A. Tkachov, R. Korolov, I. Rahimova, I. Aksonova. *Ukrainian Scientific Journal of Information Security*. 2024. Vol. 30, issue 1. P. 58-66. DOI: 10.18372/2225-5036.30.18604.

14. Shan A., Myeong S. Proactive Threat Hunting in Critical Infrastructure Protection through Hybrid Machine Learning Algorithm Application. *Sensors*. 2024. № 24(15):4888. DOI: 10.3390/s24154888.

15. John Kuforiji. Digital Forensics and Incident Response (DFIR) Automation: Leveraging AI to Accelerate Breach Investigation, Evidence Collection, and Cyberattack Mitigation. *Journal of Data Analysis and Critical Management*. 2025. Vol. 1, № 04. DOI: 10.64235/tsvfvz27.

16. Artificial intelligence integration in cyber incident response teams to enable faster containment, forensic accuracy, and resilient business continuity / Kwaku Gyamfi Boamah, AFUA Asante, Ashley Timean, Kwadwo Fening Okai. *International Journal of Science and Research Archive*. 2025. №17(01). P.1263-1280. DOI: 10.30574/ijsra.2025.17.1.2933.

17. Method for managing IT incidents in critical information infrastructure facilities / S. Gnatyuk, V. Sydorenko, A. Polozhentsev, V. Sokolov. *CPITS-II 2024: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II*. 2024. URL: https://h7.cl/1l8Dk (date of access: 8.12.2025).

18. ISO/IEC 27035-1:2023 Information technology – Information security incident management – Part 1: Principles and process. *International Organization for Standardization*. 2023. URL: https://h7.cl/1gdGl (date of access: 12.12.2025).

19. NIST SP 800-61 Revision 2, Computer Security Incident Handling Guide. URL: https://csrc.nist.gov/pubs/sp/800/61/r2/final (date of access: 15.12.2025).

20. NIST SP 800-61r3. Incident Response Recommendations and Considerations for Cybersecurity Risk Management – A CSF 2.0 Community Profile / Alex Nelson et al. *National Institute of Standards and Technology*. URL: https://h7.cl/1l6Xp (date of access: 8.12.2025).

21. Rozyasnennya CERT-UA: platforma MISP, shcho tse, yak pidklyuchatysya ta yaki perevahy. Derzhavna sluzhba spetsialnoho zvyazku ta zakhystu informatsiyi Ukrayiny. URL: https://h7.cl/1gfiS (data zvernennya: 15.12.2025).

22. ISO/IEC 27035-3:2020 Information technology – Information security incident management – Part 3: Guidelines for ICT incident response operations. *International Organization for Standardization*, 2020. URL: https://www.iso.org/ru/standard/74033.html (date of access: 8.12.2025).

23. Górka Marek. Baltic States Cyber Security Policy: Development of digital capabilities in 2017–2022. *Stosunki Międzynarodowe – International Relations*. Vol. 59. 2023. P. 57-81. DOI:10.12688/stomiedintrelat.17684.1.

24. Pro osnovni zasady zabezpechennya kiberbezpeky Ukrayiny : Zakon Ukrayiny vid 05.10.2017 № 2163-VIII : redaktsiya vid 19.10.2025. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (data zvernennya: 16.12.2025).

25. Pro zakhyst informatsiyi v informatsiyno-komunikatsiynykh systemakh : Zakon Ukrayiny vid 05.07.1994 № 80/94-VR : redaktsiya vid 20.04.2025. URL: https://h7.cl/1l8Dv (data zvernennya: 30.11.2025).

26. Pro zatverdzhennya Zahalnykh vymoh z kiberzakhystu obyektiv krytychnoyi infrastruktury : Postanova Kabinetu Ministriv Ukrayiny; Vymohy, Perelik vid 19.06.2019 № 518 : redaktsiya vid 20.11.2025. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text (data zvernennya: 29.11.2025).

27. Nakaz Administratsiyi Derzhspetszvyazku vid 03.12.2025 №798 «Pro zatverdzhennya Metodychnykh rekomendatsiy shchodo typovykh vymoh do pidrozdiliv z kiberzakhystu, zahalnykh vymoh do kerivnykiv z kiberzakhystu v orhanakh derzhavnoyi vlady, a takozh do vidpovidalnykh osib, yaki vykonuyut funktsiyi ta zavdannya kerivnyka z kiberzakhystu v yurydychnykh osobakh, shcho ye vlasnykamy abo rozporyadnykamy obyektiv krytychnoyi informatsiynoyi infrastruktury I i II katehoriy krytychnosti, ta v orhanakh mistsevoho samovryaduvannya». *Derzhavna sluzhba spetsialnoho zvyazku ta zakhystu informatsiyi Ukrayiny*. URL: https://h7.cl/1l6XU (data zvernennya: 3.12.2025).

28. Best practices for cyber crisis management. *European Union Agency for Cybersecurity (ENISA)*. 2024. URL: https://h7.cl/1l6lr (date of access: 8.12.2025).

29. Cybersecurity Incident & Vulnerability Response Playbooks. *Cybersecurity and Infrastructure Security Agency (CISA)*. 2021. 44 p. URL: https://h7.cl/1gd8H (date of access: 28.11.2025).

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
здобувача вищої освіти
Мельник Мар'яни Миколаївни
студента ФІТ, 2 курсу, групи КБЗІм-24-1

ЗАЯВА

З правилами чинного Положення про систему забезпечення академічної доброчесності у Хмельницькому національному університеті, згідно з яким виявлення академічного плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту і застосування заходів академічної відповідальності, ознайомлена. Про використання спеціалізованих програмних засобів (СПЗ) StrikePlagiarism та Anti-Plagiarism для перевірки кваліфікаційних робіт здобувачів вищої освіти на наявність академічного плагіату оповіщена. Надаю університету право на передачу моєї роботи для обробки та збереження в базах даних СПЗ і використання роботи для виявлення академічного плагіату в інших роботах, які перевіряються СПЗ.

Також надаю свою згоду на обробку й збереження університетом моєї роботи в Інституційному репозитарії Хмельницького національного університету.

Робота надається для перевірки в електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

1.12.2025
дата

підпис

# Anti-Plagiarism (UA) v-16.693

**The maximum coincidence with one document 1.0%**

Dictionaries check: UA, US, RU. **Errors in the documents: 77%**

| ID: 253057<br>Title: Метод виявлення та розслідування цілеспрямованих атак на об'єкти критичної інфраструктури<br>Added in a DB: 2025-12-15<br>Authors: Мельник Мар'яна Миколаївна<br>Heads: Чешун В.М.<br>Consultants:<br>Opponents: | Document | | Sum coincidence on the DB | |
|---|---|---|---|---|
| | Symbols | Lexemes | Symbols | Lexemes |
| | 95957 | 1429 | 1053 (1%) | 14 (1%) |

Plagiarism sources

| ID | Description | Plagiarism presence in the document | |
|---|---|---|---|
| | | Symbols | Lexemes |

**Протокол аналізу звіту подібності науковим керівником**

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

**Автор:** Мельник Мар'яна Миколаївна

**Співавтор:**

**Назва:** Метод виявлення та розслідування цілеспрямованих атак на об'єкти критичної інфраструктури

**Науковий керівник:** Чешун Віктор Миколайович

**Підрозділ:** Кафедра кібербезпеки

**Коефіцієнт подібності 1:**1.3%

**Коефіцієнт подібності 2:**0.3%

**Мікропробіли:** 0

**Заміна букв:** 0

**Інтервали:** 0

**Білі знаки:** 0

**Дата створення звіту:** 2025-12-15 15:52:38.0

**Після аналізу Звіту подібності констатую наступне:**

☑ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

*Дата* 16.12 2025 р експерт Сергій МОСТОВИЙ

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Назва кваліфікаційної роботи: Метод виявлення та розслідування цілеспрямованих атак на об'єкти критичної інфраструктури
Автор: Мельник Мар'яна Миколаївна
Освітня програма: Кібербезпека та захист інформації
Рівень вищої освіти: другий (магістерський)
Спеціальність: 125 – Кібербезпека та захист інформації
Науковий керівник: канд. техн. наук, доц. Чешун Віктор Миколайович
На основі аналізу кваліфікаційної роботи на дотримання вимог академічної доброчесності (у т.ч. відсутності ознак академічного плагіату) з урахуванням результатів перевірки роботи спеціалізованим програмним засобом(ами) комісія зробила такий висновок:

| № | Висновок | Позначка про відповідність |
|---|---|---|
| 1 | Ознаки академічного плагіату | |
| 1.1 | Запозичення, виявлені в роботі, є законними і не є академічним плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних, якщо потрібно). Робота приймається до захисту | відповідає |
| 1.2 | Виявлені запозичення не є академічним плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована | |
| 1.3 | Виявлені запозичення не є академічним плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. Робота може бути допущена до захисту після того як буде відкоригована та доопрацьована і успішно пройде повторну перевірку на академічний плагіат | |
| 1.4 | Робота містить навмисні текстові спотворення, передбачувані спроби укриття текстових запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту. | |
| 2 | Інші види порушень академічної доброчесності | |

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою StrikePlagiarism складає 99%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism складає 98.7%

Згідно з Положенням про систему забезпечення академічної доброчесності у ХНУ (https://khmnu.edu.ua/wp-content/uploads/normatyvni-dokumenty/polozhennya/pro-systemu-zabezpechennya-akademichnoyi-dobrochesnosti.pdf, Додаток В) кваліфікаційна робота, виконана за освітньо-професійною програмою, кількісні показники рівня унікальності тексту у відсотках до загального обсягу матеріалу в якій складає 75-100 %, визнається роботою з високим рівнем унікальності тексту: «Текст вважається унікальним і не потребує додаткових дій щодо запобігання неправомірним запозиченням».

Дата: 15.12.2025

Завідувач кафедри кібербезпеки _____ Юрій КЛЬОЦ

Гарант освітньої програми _____ Віра ТІТОВА

Керівник кваліфікаційної роботи _____ Віктор ЧЕШУН

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

# РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «магістр»

Студентка Мельник Мар'яна Миколаївна
Тема Метод виявлення та розслідування цілеспрямованих атак на об'єкти критичної інфраструктури
Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека та захист інформації

**Обсяг кваліфікаційної роботи освітнього ступеня «магістр»:**

кількість листів креслень - ; кількість сторінок записки 84

1. Короткий зміст роботи та прийнятих рішень Кваліфікаційна робота присвячена вирішенню актуальної науково-прикладної задачі підвищення ефективності розслідування кіберінцидентів в інформаційних системах. У роботі розроблено та реалізовано комплексний метод розслідування кіберінцидентів, що базується на централізованому зборі журналів, кореляції подій та використанні інструментів цифрової криміналістики. Запропонований підхід поєднує автоматизований аналіз подій, збагачення індикаторів компрометації та структуроване управління інцидентами, що дозволяє забезпечити відтворюваність розслідування та підвищити якість аналітичних висновків

2. Висновок про відповідність кваліфікаційної роботи завданню Кваліфікаційна робота відповідає поставленому завданню як в теоретичній, так і в практичній частині.

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі роботи обґрунтовано актуальність проблеми розслідування кіберінцидентів в умовах зростання кількості атак на інформаційні системи, визначено об'єкт і предмет дослідження, сформульовано мету та основні завдання, а також окреслено наукову новизну і практичну цінність отриманих результатів. У першому розділі здійснено аналіз сучасних підходів до розслідування кіберінцидентів, розглянуто міжнародні стандарти та нормативні документи, а також проаналізовано можливості існуючих платформ моніторингу та реагування. Наведено обґрунтування доцільності використання інтегрованого підходу, що поєднує автоматизований збір журналів, кореляцію подій та аналітичну обробку цифрових артефактів. У другому розділі розроблено метод розслідування кіберінцидентів, який охоплює всі етапи реагування — від виявлення підозрілої активності до аналізу та документування результатів. Запропоновано архітектуру взаємодії компонентів системи та визначено роль кожного інструмента в процесі збору й аналізу доказів. У третьому розділі виконано практичну реалізацію методу у тестовому середовищі з використанням операційних систем Windows і Linux, а також проведено експериментальне дослідження ефективності підходу. Результати тестування підтвердили здатність запропонованого методу своєчасно виявляти інциденти, відтворювати хронологію подій та підвищувати якість криміналістичного аналізу порівняно з традиційними підходами.

4. Позитивні сторони роботи Кваліфікаційна робота має практичну та прикладну цінність. Перевагою роботи є комплексний підхід до розслідування кіберінцидентів, який поєднує централізований збір журналів, кореляцію подій, збагачення індикаторів компрометації та елементи цифрової криміналістики. Запропонований метод базується на використанні сучасних відкритих платформ і може бути адаптований до умов функціонування об'єктів критичної інфраструктури. Окремо слід відзначити практичну апробацію методу в тестовому середовищі, що підтверджує його працездатність і прикладну корисність

5. Негативні сторони роботи До недоліків роботи можна віднести те, що реалізація методу орієнтована переважно на аналітичний та криміналістичний рівень і не передбачає повної автоматизації реагування на інциденти. Візуалізація результатів аналізу потребує додаткового налаштування та може бути розширена за рахунок інтерактивних аналітичних панелей

6. Оцінка графічного оформлення та пояснювальної записки роботи Оформлення всіх матеріалів кваліфікаційної роботи є якісним, здійснене з дотриманням актуальних стандартів та інституційних положень ХНУ. Пояснювальна записка відповідає нормам щодо її оформлення як за структурою, так і за представленням і форматуванням матеріалу

7. Відгук про роботу в цілому Кваліфікаційна робота заслуговує позитивної оцінки. Матеріал роботи викладено логічно та послідовно, усі розділи взаємопов'язані й відповідають поставленій темі. Запропонований підхід до розслідування кіберінцидентів є обґрунтованим і практично орієнтованим. Презентаційні та ілюстративні матеріали наочно демонструють ефективність обраних рішень і підтверджують доцільність використання інтегрованих інструментів моніторингу та аналізу безпеки

8. Інші зауваження

9. Оцінка кваліфікаційної роботи Враховуючи всі позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що вона заслуговує оцінки 95 балів

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи)
Мартинюк Валерій Володимирович
завідувач кафедри автоматизації, комп'ютерно-інтегрованих технологій та робототехніки , доктор технічних наук, професор

« 16 » 12 2025. (підпис)