

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАДИМА ГЕТЬМАНА**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
«ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ЕКОНОМІЦІ»**

Кафедра системного аналізу та кібербезпеки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРБЕЗПЕКА»

Галузь знань 12 «Інформаційні технології»

Спеціальність 125 «Кібербезпека»

Форма навчання: очна (денна)

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

**на тему: «Вдосконалення процесу реагування на кіберінциденти шляхом
розробки регламентів на основі SIEM-системи»**

здобувача: Гаман Ольга Ігорівна _____

Науковий керівник: к.т.н., доц. Гулак Н. К. _____

**Робота допущена до захисту перед екзаменаційною комісією з атестації
здобувачів вищої освіти (ЕК)**

Завідувач кафедри: д.ф.-м.н., проф. Джалладова І.А. _____

КИЇВ 2026

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ
ВАДИМА ГЕТЬМАНА

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
«ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ЕКОНОМІЦІ»

Кафедра системного аналізу та кібербезпеки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРБЕЗПЕКА»

Галузь знань 12 «Інформаційні технології»

Спеціальність 125 «Кібербезпека»

ПОГОДЖЕНО

Керівник проектної групи (гарант)
освітньо-професійної програми

А.В.Бегун
(підпис) (ініціали, прізвище)

_____ 2026 р.

ЗАТВЕРДЖУЮ:

Завідувач кафедри

І.А. Джалладова
(підпис) (ініціали, прізвище)

_____ 2026 р.

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

здобувача вищої освіти: Гаман Ольги Ігорівни.
(прізвище, ім'я, по батькові)

очної (денної) **форми навчання**
очної (денної), заочної, дистанційної

на підготовку кваліфікаційної бакалаврської роботи

**на тему: « Вдосконалення процесу реагування на кіберінциденти
шляхом розробки регламентів на основі SIEM-системи »**

Тему затверджено наказом ректора Університету від «___» _____ 20__ р. №__
Кваліфікаційна бакалаврська робота виконується на матеріалах ВП
«Хмельницька АЕС», літературних та інформаційних джерел з кібербезпеки та
мережевих технологій, офіційної документації платформ Wazuh та Ubuntu Linux, а
також практичної реалізації тестового стенду з використанням відкритого ПЗ

ПЛАН КВАЛІФІКАЦІЙНОЇ БАКАЛАВРСЬКОЇ РОБОТИ

Розділ 1	Аналіз нормативно правової бази інформаційної України для моніторингу кіберінцидентів
Розділ 2	Технічна реалізація та налаштування системи моніторингу на базі платформи Wazuh
Розділ 3	Практична реалізація та адаптація системи моніторингу до національних стандартів безпеки

Об'єкт дослідження	Процес моніторингу інформаційної безпеки та реагування на кіберінциденти в комп'ютерних системах організації
Предмет дослідження	Методи та регламенти автоматизованого виявлення кіберзагроз і реагування на них за допомогою SIEM-системи.
Мета кваліфікаційної бакалаврської роботи	Вдосконалення системи захисту інформації організації шляхом інтеграції нормативних вимог українського законодавства у процес автоматизованого моніторингу та розробки чітких регламентів реагування на кіберінциденти на базі SIEM-системи.

Конкретні завдання, які здобувач повинен виконати для досягнення поставленої мети:

У розділі 1 «Аналіз нормативно правової бази інформаційної України для моніторингу кіберінцидентів»: Дослідити сутність, еволюцію та архітектуру систем класу SIEM/XDR у сучасних центрах моніторингу безпеки (SOC). Оцінити нормативно-правове поле та стандарти забезпечення кібербезпеки в Україні, включаючи вимоги законодавства та рекомендації CERT-UA. Проаналізувати наявні інструменти збору та нормалізації логів, визначити переваги використання open-source рішень.

У розділі 2 «Технічна реалізація та налаштування системи моніторингу на базі платформи Wazuh»: Обґрунтувати вибір та детально дослідити компонентну архітектуру платформи Wazuh (Indexer, Server, Dashboard, Agents). Здійснити практичне моделювання інфраструктури, активів та потенційних загроз для умовного підприємства. Описати покроковий процес розгортання,

конфігурування Linux-серверів та інтеграції агентів моніторингу на кінцеві точки (Endpoints).

У розділі 3 «Практична реалізація та адаптація системи моніторингу до національних стандартів безпеки»: Сконфігурувати кастомні правила та декодери у файлі local_rules.xml для фіксації цільових аномалій. Розробей практичні покрокові регламенти реагування (плейбуки) на критичні інциденти: атаку перебором паролів (Brute-Force) та впровадження шкідливого ПЗ (rootkits). Здійснити мапінг розроблених правил на матрицю тактик MITRE ATT&CK та статті Закону України про кібербезпеку. Провести математичне та експериментальне оцінювання ефективності впроваджених регламентів через покращення метрик MTTD та MTTR.

Завдання підготував
науковий керівник

(підпис)

Гулак Н. К.

(прізвище, ініціали)

Завдання одержав
здобувач

(підпис)

Гаман О. І.

(прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 60 с., 9 рис., 4 табл., 0 додатків, 55 джерел.

Об'єкт дослідження: Процес моніторингу інформаційної безпеки та реагування на кіберінциденти в комп'ютерних системах.

Мета кваліфікаційної роботи: Вдосконалення системи захисту організації шляхом інтеграції вимог законодавства України в процес SIEM-моніторингу та розробки регламентів реагування.

Методи дослідження: Системний підхід, порівняльний аналіз, моделювання та експеримент (розгортання SIEM, створення правил, симуляція атак).

У спеціальній частині проаналізовано нормативно-правову базу кібербезпеки України, визначено роль SIEM-систем та детально вивчено архітектуру й можливості платформи Wazuh.

В роботі проведено аналіз ринку сучасних комерційних та відкритих SIEM-систем. Доцільність використання рішень із відкритим кодом.

Запропоновано методику безпосередньої інтеграції вимог національного законодавства у сфері кібербезпеки (зокрема, Статей 8, 9, 10 та 11 Закону України).

Побудовано кастомні алгоритми кореляції подій з використанням параметрів частоти безпекових подій, часових вікон та логічних умов..

Розроблено набір унікальних XML-правил детекції, індивідуальних декодерів та фільтрів безпеки у файлі local_rules.xml для фіксації специфічних векторів атак.

В економічному розділі визначено високу економічну доцільність розгортання розробленого комплексу на базі відкритого програмного забезпечення.

Практичне значення полягає у розробці регламенту, що дозволило автоматизувати виявлення порушень і нівелювання ризиків людського фактору, а також дозволило покращити ключові метрики ефективності центру кібербезпеки на час виявлення інцидентів та час реагування на загрози (скорочення часу реагування на атаки скоротилися з хвилин/днів до секундного рівня).

Результати здійснених у кваліфікаційній роботі досліджень можуть бути використані державними установами, підприємствами комерційного сектору та власниками об'єктів критичної інфраструктури України для побудови або модернізації власних локальних систем моніторингу безпеки.

Наукова новизна дослідження полягає у розробці сучасного підходу до технічного мапінгу абстрактних правових норм та статей Закону України «Про основні засади забезпечення кібербезпеки України» у площину автоматизованого програмно-технічного контролю, що поєднує нормативний комплаєнс із системою автоматичного проактивного захисту Active Response.

Ключові слова: кібербезпека, сієм-система, моніторинг, wazuh, реагування на кіберінциденти, законодавство України, автоматизація захисту, active response, дашборд, комплаєнс.

ВІДГУК
на кваліфікаційну бакалаврську роботу
студента Гаман Ольги Ігорівни гр. ІК-401
на тему: «Вдосконалення процесу реагування на кіберінциденти
шляхом розробки регламентів на основі SIEM-системи»

Актуальність теми. Використання систем класу SIEM, зокрема відкритої платформи Wazuh, разом із чітко розробленими регламентами реагування, є актуальним завданням для забезпечення стійкості інформаційно-комунікаційних систем підприємств та об'єктів критичної інфраструктури, тому що підходи до виявлення аномалій не дозволяють оперативно протидіяти координованим атакам у реальному часі.

Повнота розкриття теми. Тема кваліфікаційної роботи розкрита добре, за винятком теми про ISO/IEC 27005 стандарти, але це не впливає на практичну цінність роботи. Автор послідовно виконала аналіз теоретичних засад функціонування SIEM-систем, дослідила архітектуру open-source рішення Wazuh, провела детальне моделювання загроз та активів умовного підприємства.

Теоретичний рівень. Студентка продемонструвала глибокі теоретичні знання у сфері архітектури сучасних систем виявлення та запобігання вторгненням (IDS/IPS, SIEM/XDR). Робота базується на актуальній нормативно-правовій базі України, зокрема на Законі України «Про основні засади забезпечення кібербезпеки України» та рекомендаціях CERT-UA.

Практична значущість. Практична цінність роботи полягає у створенні готового до впровадження комплексу моніторингу та регламентів реагування. Автор не лише розгорнула інфраструктуру Wazuh, а й модифікувала конфігураційні файли (ossec.conf) та правила аналізатора (local_rules.xml) під специфіку виявлення критичних інцидентів.

Самостійність виконання роботи. Робота виконана самостійно. Студентка виявила високу інженерну грамотність та ініціативність під час конфігурування Linux-серверів, налаштування декодерів подій та інтеграції агентів безпеки на

кінцеві точки. Особливої уваги заслуговує підхід авторки до практичного моделювання кібератак, що дозволило експериментально підтвердити ефективність розроблених регламентів.

Якість оформлення, загальна та спеціальна грамотність. Робота оформлена відповідно до встановлених вимог. Матеріал викладено послідовно, з дотриманням наукового стилю мовлення. Робота містить якісно виконаний графічний матеріал.

Переваги та недоліки роботи. До переваг роботи належить орієнтація на практичне використання безкоштовних open-source інструментів з високим рівнем кастомізації, а також поєднання нормативних вимог законодавства України з технічними налаштуваннями правил SIEM. Недоліком роботи є те, що в ній доцільно було б ширше розглянути питання інтеграції Wazuh із зовнішніми системами Threat Intelligence для автоматичного обміну індикаторами компрометації, що, однак, не знижує загальну високу якість і цінність проведеного дослідження

Загальна оцінка роботи та висновок щодо рекомендації до захисту в ЕК. виконана робота показала, що Гаман Ольга готова до самостійної професійної діяльності у сфері кібербезпеки. В цілому, кваліфікаційна робота заслуговує оцінки «добре», а її авторка – на присвоєння кваліфікації «Бакалавр з кібербезпеки».

Науковий керівник к.т.н.

Доцент кафедри системного аналізу та кібербезпеки _____ Наталія ГУЛЯК
(посада) (підпис) (ініціали, прізвище)

“ ____ ” _____ 2026 р.

РЕЦЕНЗІЯ

на кваліфікаційну бакалаврську роботу

студента Гаман Ольги Ігорівни гр. ІК-401

**на тему: «Вдосконалення процесу реагування на кіберінциденти
шляхом розробки регламентів на основі SIEM-системи»**

Актуальність теми. Моніторинг та оперативне управління інцидентами інформаційної безпеки є критично важливими елементами захисту сучасних розподілених корпоративних мереж. Впровадження інструментів автоматизованого збору та кореляції лог-файлів у поєднанні з чіткими покроковими регламентами дій персоналу дозволяє мінімізувати час присутності зловмисника в системі. Це зумовлює високу актуальність теми рецензованої бакалаврської роботи для сучасної галузі інформаційних технологій та кібербезпеки.

Наукова новизна. Полягає у комплексному поєднанні технічного інструментарію open-source SIEM-системи Wazuh із нормативно-правовими вимогами законодавства, зокрема Закону України «Про основні засади забезпечення кібербезпеки України». Автор запропонувала адаптований підхід до мапінгу технічних подій безпеки на конкретні правові норми та розробила структуровані сценарії протидії інцидентам.

Практичне значення полягає у розробці регламенту, що дозволило автоматизувати виявлення порушень і нівелювання ризиків людського фактору, а також дозволило покращити ключові метрики ефективності центру кібербезпеки на час виявлення інцидентів та час реагування на загрози (скорочення часу реагування на атаки скоротилися з хвилин/днів до секундного рівня).

Якість проведеного аналізу. Аналітична частина роботи виконана на високому рівні. Студентка провела ґрунтовне порівняльне дослідження існуючих комерційних та відкритих архітектур SIEM-систем, детально описала принципи взаємодії менеджерів та агентів Wazuh. Також у роботі якісно реалізовано етап моделювання загрози несанкціонованого доступу та впровадження шкідливого

програмного забезпечення на кінцевих точках умовної інфраструктури підприємства.

Уміння користуватися літературними джерелами. Автор продемонструвала належний рівень роботи з науковою та технічною літературою. Список використаних джерел містить державні стандарти України (ДСТУ), міжнародні стандарти безпеки (ISO/IEC, NIST), технічна документація розробників програмного забезпечення та актуальні праці вітчизняних і закордонних фахівців.

Переваги та недоліки. До переваг роботи слід віднести реальну інженерну цінність налаштованих конфігурацій, детальну візуалізацію алгоритмів у вигляді схем і використання гнучких open-source рішень. Автор послідовно виконала аналіз теоретичних засад функціонування SIEM-систем, дослідила архітектуру open-source рішення Wazuh, провела детальне моделювання загроз та активів умовного підприємства. До недоліків можна віднести неповний аналіз серії міжнародних стандартів ISO/IEC 27000, але це не впливає на практичну цінність роботи.

Загальний висновок і оцінка роботи. Кваліфікаційна бакалаврська робота Гаман Ольги Ігорівни за своєю структурою, обсягом та чітким вирішенням поставлених завдань повністю відповідає вимогам до бакалаврських робіт за спеціальністю 125 «Кібербезпека». Робота заслуговує на високу позитивну оцінку «85/добре/В», а її автор на присвоєння кваліфікації «Бакалавр з кібербезпеки».

Рецензент к.т.н., доцент

Завідувач кафедри Кібербезпеки

Національний університет «КАІ»

(посада)

_____ Анна ІЛЬЄНКО

(підпис)

(ініціали, прізвище)

Печатка

“ _____ ” _____ 2026

ЗМІСТ

ВСТУП.....	4
РОЗДІЛ 1. АНАЛІЗ НОРМАТИВНО ПРАВОВОЇ БАЗИ ІНФОРМАЦІЙНОЇ СИСТЕМИ УКРАЇНИ ДЛЯ МОНІТОРИНГУ КІБЕРІНЦИДЕНТІВ.....	6
1.1. Кібербезпека України: регуляторна та правова база.....	6
1.2 Роль SIEM-систем у сучасних центрах кібербезпеки (SOC). (Огляд ринку, переваги Open Source рішень).....	9
1.3. Порівняльний аналіз методологій управління кіберінцидентами ...	16
1.4 Висновки до розділу 1	19
РОЗДІЛ 2. ТЕХНІЧНА РЕАЛІЗАЦІЯ ТА НАЛАШТУВАННЯ СИСТЕМИ МОНІТОРУНГУ НА БАЗІ ПЛАТФОРМИ WAZUH.....	21
2.1. Технічна характеристика та можливості SIEM-системи Wazuh (Архітектура: Manager, Indexer, Dashboard, Agents)	21
2.2. Моделювання загроз та ідентифікація критичних активів.....	25
2.3. Розробка алгоритмів кореляції подій для виявлення порушень нормативних вимог	28
2.4 Висновки до розділу 2.....	30
РОЗДІЛ 3. ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА АДАПТАЦІЯ СИСТЕМИ МОНІТОРИНГУ ДО НАЦІОНАЛЬНИХ СТАНДАРТІВ БЕЗПЕКИ	32
3.1. Модернізація та налаштування правил виявлення інцидентів відповідно до Закону України «Про основні засади забезпечення кібербезпеки України»	32
3.2. Налаштування правил виявлення і фіксації ушкоджень та їх мапінг на статті Закону України про кібербезпеку. (Статті 8, 9, 10, 11).....	35

3.3. Візуалізація результатів моніторингу: створення спеціалізованих дашбордів для офіцерів безпеки.....	43
3.4. Автоматизація реагування за допомогою механізму Active Response.....	48
3.5. Покращення показників MTTD (час виявлення) та MTTR (час реагування).....	51
3.6. Висновки до розділу 3.....	53
ВИСНОВКИ	55
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	58

ВСТУП

Актуальність теми: У зв'язку з повномасштабною агресією значно зросла кількість кібератак на державний сектор України, критичну інфраструктуру та приватні підприємства. Зловмисники постійно намагаються зламати інформаційні системи, викрасти конфіденційні дані або порушити роботу важливих сервісів. Тому SIEM-системи дозволяють збирати журнали подій з усіх пристроїв у реальному часі, автоматично аналізувати їх та миттєво виявляти підозрілу активність чи сліди хакерських атак.

Однак просто встановити таку систему недостатньо. В сучасних умовах зловмисники постійно намагаються взламати інформаційні системи тому традиційні захисти засобу вже не можуть забезпечити повний захист. Для забезпечення комплексного і безперервного контролю, щоб покращити та пришвидшити виявлення та процес реагування на кібератаки я буду підлаштовувати SIEM-систему під українське законодавство та нюанси кіберзахисту.

Таким чином, необхідність підвищення рівня захищеності державних та комерційних установ, автоматизація виявлення загроз та створення чітких правил реагування на них визначають високу актуальність цієї роботи.

Об'єкт дослідження – процес моніторингу інформаційної безпеки та реагування на кіберінциденти в комп'ютерних системах організації.

Предмет дослідження – методи та регламенти автоматизованого виявлення кіберзагроз і реагування на них за допомогою SIEM-системи.

Мета роботи – вдосконалення системи захисту інформації організації шляхом інтеграції нормативних вимог українського законодавства у процес автоматизованого моніторингу та розробки чітких регламентів реагування на кіберінциденти на базі SIEM-системи.

Для досягнення мети було сформовано наступні завдання:

1. Аналіз нормативної правової бази з інформаційної безпеки України з системи.

2. Дослідити побудову та архітектуру сучасних SIEM систем як інструмент для збору і аналізу подій інформаційної безпеки.

3. Провести розгорнення та налаштування SIEM системи Wazuh, розробити і протестувати покрокові регламенти та інструкції для персоналу щодо дій у разі виявлення кіберінцидентів.

4. Розробити та інтегрувати специфічні правила виявлення (декодери та правила фільтрації) для фіксації типових зловмисних дій та атак.

Методи дослідження: для вирішення поставлених завдань у роботі використано такі методи: аналіз та системний підхід (для вивчення архітектури систем моніторингу та нормативних документів), моделювання (для опису процесів виявлення загроз та побудови схем інформаційних потоків логів), а також експериментальний метод (для практичного розгортання SIEM-системи, написання правил та проведення симуляції атак з метою перевірки роботи комплексного захисту).

Практичне значення полягає у розробці регламенту, що дозволило автоматизувати виявлення порушень і нівелювання ризиків людського фактору, а також дозволило покращити ключові метрики ефективності центру кібербезпеки на час виявлення інцидентів та час реагування на загрози (скорочення часу реагування на атаки скоротилися з хвилин/днів до секундного рівня).

РОЗДІЛ 1. АНАЛІЗ НОРМАТИВНО ПРАВОВОЇ БАЗИ ІНФОРМАЦІЙНОЇ СИСТЕМИ УКРАЇНИ ДЛЯ МОНІТОРИНГУ КІБЕРІНЦИДЕНТІВ

1.1. Кібербезпека України: регуляторна та правова база

Створення ефективної системи виявлення та своєчасного реагування на кіберінциденти на будь-якому підприємстві чи в державному органі не може здійснюватися окремо від національної правової бази, адже тоді певні атаки можуть бути не ідентифіковані. У сфері захисту інформації чинне законодавство України зараз перебуває на стадії активної адаптації з європейськими нормами, орієнтуючись на Директиви NIS та NIS2, що безпосередньо визначає жорсткі регуляторні, організаційні та технічні вимоги до всіх суб'єктів національної системи кібербезпеки. Ці норми ставлять перед нами чіткі очікування щодо обов'язкового виконання постійних контрольних заходів, безперервної реєстрації подій безпеки та швидкої взаємодії з державними центрами контролю і навіть автоматизованого блокування або певних дій для швидкості реагування на інцидент.

Головною правовою та регуляторною основою для проведення таких досліджень є Закон України «Про основні засади забезпечення кібербезпеки України» [1]. Цей закон встановлює юридичний фундамент для захисту законних інтересів громадян, суспільства та держави у кіберпросторі, захищаючи наші національні інтереси. У контексті налаштування SIEM-систем, під які ми маємо формулювати правила та технічні регламенти, закріплені в цьому Законі базові поняття «кіберінцидент», «кібератака» та «об'єкт критичної інфраструктури» є фундаментальними елементами, на які ми спираємось при класифікації подій.

Відповідно до чинного законодавства, всі власники та керівники об'єктів критичної інфраструктури несуть персональну відповідальність за забезпечення кібербезпеки своїх інформаційно-комунікаційних систем. Закон вимагає від них

обов'язково інформувати урядову команду реагування на комп'ютерні надзвичайні ситуації CERT-UA, яка функціонує в рамках Державної служби спеціального зв'язку та захисту інформації України (ДССЗІ), про кожен виявлений кіберінцидент у визначені терміни. У цьому питанні впровадження системи класу SIEM стає єдиною реальною організаційно-технічною можливістю для виконання законодавчих вимог, оскільки без автоматичного аналізу журналів подій неможливо вчасно виявити сам момент початку інциденту та швидко перевірити його параметри для надсилання звіту.[2]

Окрім профільного закону, загальна нормативно-правова база кібербезпеки в Україні включає ще кілька важливих актів та документів, на які необхідно спиратися при розгортанні системи моніторингу:

- Закон України «Про захист інформації в інформаційно-комунікаційних системах», який повністю регулює відносини у сфері захисту чутливої та юридично значущої інформації чи державних ресурсів, вимагаючи обов'язкового створення комплексної системи захисту інформації (КСЗІ) з отриманням сертифіката відповідності від ДССЗІ. Постійний моніторинг та реєстрація подій на базі зв'язки SIEM та HIDS, де ми використовуємо платформу Wazuh, є обов'язковим технічним аспектом будь-якого стандартного процесу побудови КСЗІ для успішного проходження аудиту;[2]

- Постанова Кабінету Міністрів України № 518 «Про затвердження загальних вимог до кіберзахиту об'єктів критичної інфраструктури», яка підготовлена з практичної точки зору для організації реального захисту на важливих об'єктах [2]. Цей документ напряду вимагає впроваджувати системи безперервного моніторингу, антивірусного захисту, контролю цілісності програмного забезпечення та конфігурацій, а також засобів виявлення атак чи вторгнень. Технічні можливості Wazuh дозволяють закрити більшу частину цих нормативних вимог, оскільки цей інструмент об'єднує в собі аудит конфігурацій (SCA), контроль цілісності файлів (FIM) та глибокий аналіз логів;

- Укази Президента України, які вводять в дію рішення Ради національної безпеки і оборони (РНБО), зокрема Стратегію кібербезпеки України,

яка визначає головні стратегічні пріоритети нашої держави, акцентуючи увагу на розвитку технологічних можливостей стримування загрози, сучасному прогресуючому захисті та автоматизації обміну даними про атаки між державним та приватним секторами.

Важливим кроком для впровадження українського законодавства є використання міжнародних стандартів, які офіційно визнані нашою державою через систему національних стандартів. Зокрема, всі основні вимоги до правильної організації процесу обробки інцидентів прописані у серії стандартів ДСТУ ISO/IEC 27035 («Інформаційні технології. Методи безпеки. Управління інцидентами інформаційної безпеки»). Цей стандарт детально описує циклічний процес управління, який складається з таких послідовних етапів, як підготовка, виявлення та звітування, оцінка та прийняття рішень, безпосереднє реагування, а також винесення уроків з отриманого досвіду після завершення інциденту. [3, 4]

Аналіз української регуляторної бази чітко показує тенденцію до значного посилення вимог саме до швидкості реагування, оскільки державні регулятори, такі як НБУ для банківського сектору або ДССЗЗІ для державних установ, встановлюють дуже жорсткі часові рамки для передачі інформації про атаки, які можуть становити від кількох годин до однієї доби з моменту фіксації події.

Регуляторна та правова база виступає для нас головним джерелом вхідних обмежень та вимог та стандартів, які ми повинні обов'язково враховувати при написанні кастомних правил кореляції подій та налаштуванні автоматичних сценаріїв. Окрім зупинки атаки та попередження про атаку, розроблені нами правила мають забезпечити збереження повної юридичної сили всієї доказової бази кіберінциденту, що накладає на систему моніторингу додаткові технічні зобов'язання:

- Система повинна гарантувати абсолютну цілісність та захищеність самих файлів журналів подій, через що будь-які спроби модифікації чи деструктивного видалення логів аудиту мають миттєво розглядатися як окремий критичний інцидент найвищого рівня;

- Необхідно налаштувати обов'язкову синхронізацію точного часу на всіх доступних технологічних вузлах інфраструктури від одного єдиного NTP-сервера, що є критично важливим для правильного відтворення хронології розвитку атаки під час проведення подальшого розслідування та аналізу;
- Створення та вивантаження підсумкових звітів про інциденти має відбуватися у форматах, які є зручними та адаптованими для швидкої передачі до CERT-UA, підтримуючи загальноприйняті протоколи обміну даними типу STIX/TAXII або офіційно встановлені формати ДССЗІ.

Таким чином, повна інтеграція технічного функціоналу відкритої SIEM-платформи Wazuh із регуляторними стандартами українського законодавства дозволяє нам розробити юридично обґрунтовану, технічно компетентну та повністю відповідну державним вимогам систему кібербезпеки, яка мінімізує ризики для діяльності підприємства.[5]

1.2 Роль SIEM-систем у сучасних центрах кібербезпеки (SOC). (Огляд ринку, переваги Open Source рішень).

У сучасному світі технології розвиваються надто швидко, саме тому постійні зміни та розвиток технологій змушує нас постійно крокувати в ногу з майбутнім та випереджати атаки і зловмисників. Саме через це організації вимушені вкладатись в постійний розвиток та оновлення систем безпеки. Головну роль у реалізації сучасного кіберзахисту відіграє Центр операцій безпеки (SOC- Security Operations Center). Він діє як єдина система, що об'єднує різні методи захисту, а саме аналітиків, інструкції поведінки на робочому місці та сучасні захисні технології для того, щоб виявляти поточні кібератаки та загрози в реальному часі, детально їх вивчати і миттєво зупиняти. На мій погляд, структура SOC допомагає нам швидко відреагувати на небезпеку, забезпечуючи високий рівень захищеності та дає контроль над підприємства.

У теперішньому технологічному просторі SOC за пріоритет ставлять системи управління подіями і безпековою інформацією (Security Information and Event

Management, SIEM), навколо яких і будується весь процес моніторингу. Ідея полягає в необхідності швидкого та точного збору інформації з усіх наявних джерел, включаючи мережеве обладнання, сервери, кінцеві точки (endpoints), хмарні сервіси та журнали програмного забезпечення. Враховуючи те, що за відсутності автоматичного інструменту для агрегації людські ресурси аналітиків фізично не здатні самотійно проаналізувати таку величезну кількість неструктурованих логів, система SIEM працює на рівні SOC як нервова система, забезпечуючи повну видимість поточних процесів в інфраструктурі та надаючи аналітикам контекст, необхідний для прийняття правильних рішень [6, с. 22].

Розглядаючи SIEM систему як частину роботи SOC, можна виділити кілька головних блоків, які безперервно взаємодіють між собою:

- Збір та моніторинг даних - що полягає у безперервному отриманні логів і подій у різних формах, що відбуваються за допомогою агентів (agent-based) або безагентських (agentless) технологій, стандартних протоколів Syslog, а також прямих API-інтеграцій з різними підсистемами;
- Нормалізація та парсиг – що означає автоматичний збір та обробка інформації за допомогою спеціальних програм або скриптів, в процесі якого відбувається перетворення різних даних в один стандартизований формат, наприклад як JSON або внутрішні схеми системи, що дозволяє порівнювати подію А з логами автентифікації операційної системи Б, допомагаючи швидко зрозуміти чи збігаються події між різними системами, і відповідно мати якісь висновки вже з відповіді про те збігаються вони чи ні;
- Кореляція подій - яка передбачає використання алгоритмів і логічних написаних правил для проведення швидкого аналізу з ціллю виявлення схожості між подіями, які на перший погляд здаються абсолютно різними і відбуваються в різних частинах мережі, що допомагає вчасно виявити атаку або загрозу. Наприклад, коли з однієї IP-адреси спочатку фіксується сканування портів, потім невдала спроба входу по SSH і після цього — створення нового облікового запису, ці дії по окремості сенсу не мають але вже в комплексі під час кореляції видно що це одна з поширених атак.

- Сповіщення та візуалізація - що відповідає за автоматичне створення критичних сповіщень для аналітиків першої лінії SOC та наочне відображення загального стану безпеки на графічних або інших системах.

Сучасні SIEM-системи дуже змінились та змінили свій алгоритм роботи, якщо раніше головна ідея була в зборі логів та моніторингу то зараз це сучасна та швидка система кореляцій подій та комплексної роботи в зборі всіх даних. Сьогодні системи класу Next-Gen SIEM додають статистику поведінки користувачів та об'єктів, впроваджують платформи дослідження та вивлення кіберзагроз та використовують базову автоматизацію для реагування, що дозволяє скоротити час виявлення інцидентів (MTTD). Тому це вкрай важливо, оскільки ми повинні вчасно виявити та зупиняти кіберінциденти та різні дії, щоб запобігти атакам на перших їх проявах [5, с. 535].

Огляд світового ринку SIEM-систем

Світовий ринок SIEM систем з кожним днем розширюється та розвивається та є конкурентним, що дає нам велике право вибору, адже кожна система має свої нюанси роботи та розраховані на різні аудиторії та законодавства країн. Звісно це призводить до великої конкурентності та чіткого поділу ринку на комерційний сектор і відкритий (Open Source) сектор. Наразі згідно статистичних даних зараз лідерами ринку вже тривалий час вважаються такі великі компанії, як Splunk Enterprise Security, Microsoft Sentinel, IBM QRadar, Google Chronicle і LogRhythm. Для розуміння структури та різних рішень варто впорядкувати за їхньою архітектурою і способом розгортання:

1. Локальні (On-Premise) і гібридні складні платформи (Splunk, IBM QRadar), які мають велику обчислювальну здатність та гнучкість, оскільки до прикладу навіть Splunk став стандартом для великих SOC завдяки використанню своєї мови запитів (SPL) та можливості об'єднувати будь-які неструктуровані дані. Проте, впровадження таких систем вимагає великої кількості фінансів на закупівлю різного професійного обладнання, таке як: сервери і швидкі сховища даних SAN/NAS, також на купівля та оформлення різних ліцензій, вартість яких розраховується за обсягом даних, які збираються за добу

2. Хмарні сховища та сервіси SIEM (Microsoft Sentinel, Google Chronicle), які працюють, розширюються майже безмежно і не потребуючи великих витрат на утримування серверів та сховищ у власному офісі, оскільки оплата тут відбувається за фактом споживання. Ці системи легко поєднуються в роботу з іншими хмарними сервісами провайдерів, але їх використання в українському середовищі має серйозні обмеження, пов'язані з передачею персональних даних за кордон та неможливістю обробки державної таємниці або іншої обмеженої для поширення інформації в хмарах поза межами України.

На мій погляд, головними причинами, що стримують масове впровадження приватних комерційних SIEM-систем у державних і критично важливих організаціях України, є такі чинники:

- Висока вартість ліцензії, оскільки в умовах обмежених бюджетів компаній та державних установ щорічна оплата ліцензій приватного ПЗ має великий вплив на розподіл бюджету, а якщо достатнього фінансування не має, компаніє не може дозволити собі такі сервіси.
- Залежність клієнта від одного виробника чи постачальника (Vendor Lock-in - англ. термін), через це система стає цілком прив'язаною та вразливою до закритих технологій одного виробника, що часто ускладнює подальше переміщення даних чи налаштування різних процесів під особливі національні вимоги кібербезпеки;
- Складність налаштування архітектури під свої потреби, зумовлена тим, що закритий код комерційних компаній не дає можливості провести повний аналіз та перевірку безпеки самого інструменту моніторингу та швидко створити та доповнити або й повністю замінити потрібні модулі чи правила для особистого користування, щоб це відповідало законодавству країни в якій працюють компанії.

Усі ці фактори значно підвищують інтерес і довіру до засобів систем моніторингу з відкритим кодом (Open Source SIEM/XDR), які демонструють аналогічну технічну ефективність при тому, але завдяки тому що їхня вартість володіння є набагато нижчою та доступнішою для багатьох компаній, через що вони все частіше обирають саме такі системи.

Переваги рішень із відкритим вихідним кодом (Open Source) у розбудові систем моніторингу

В сучасних умовах, коли кіберзагрози змінюються дуже швидко, а держава вимагає більше контролю над кібербезпекою, організації будь-якого розміру часто вибирають Open Source SIEM, що є не просто альтернативою комерційним продуктам, а цілком розумним і стратегічним вибором. На відміну від закритих програм, відкриті системи показують, як саме працює їхній внутрішній код, що дає повну прозорість, що є дуже важливим аспектом для створення індивідуальних комплексних систем захисту інформації (КСЗІ) у державних установах і на критичних об'єктах інфраструктури країни.[7]

Серед головних архітектурних і робочих плюсів використання Open Source рішень в Security Operations Center (SOC) добре розглянути наступні:

1. Відсутність ліцензійних обмежень за обсягом даних: більшість приватних SIEM-платформ беруть гроші за показники EPS або за щоденний обсяг логів у гігабайтах, що змушує офіцерів безпеки штучно скорочувати джерела логування задля заощадження бюджету, що також може вплинути на якісь кібербезпеки. Я вважаю, що Open Source рішення повністю вирішують цю проблему, дозволяючи безперешкодно збирати і аналізувати дані з усіх доступних вузлів інфраструктури без додаткових фінансових витрат і це дозволяє навіть невеличким компаніям мати хороший моніторинг, що призводить до забезпечення попереджень кіберінцидентів.

2. Повний дозвіл налаштування і гнучка інтеграція: відкритий вихідний код дає розробникам і аналітикам SOC можливість повністю підлаштувати систему під індивідуальні потреби організації, створюючи свої налаштування безпеки, правила кореляції, певну модель візуалізації і модулі автоматичного реагування, які легко підключаються до локальних систем, таких як системи обліку користувачів або реєстри інцидентів.

3. Незалежність від геополітичних факторів та власника бренду: використання відкритого ПЗ мінімізує ризики, що виникають у випадках, коли розробники йдуть з ринку через санкції, зміни корпоративної політики або

банкрутство та інші фактори, дозволяючи організації постійно тримати повний контроль над безпековою системою і базами інцидентів.

4. Потужна сила спільноти: глобальні спільноти розробників і фахівців з аналізу загроз постійно оновлюють бази сигнатур, правила виявлення атак (наприклад, у єдиному форматі Sigma) і модулі інтеграції з Threat Intelligence, що забезпечує швидку реакцію на нові вразливості ще до виходу офіційних оновлень від комерційних виробників операційних систем.

Платформа Wazuh як сучасне інтегроване SIEM/XDR-рішення

Наразі SIEM-систем досить багато і вибрати подекуди складно, проте важливе місце займає платформа Wazuh, яка пройшла шлях розвитку від простої системи виявлення вторгнень на хостах (HIDS OSSEC) до повноцінної потужної SIEM-екосистеми та рішень класу XDR (Extended Detection and Response), яка також є open-source системою та має всі переваги прераховані вище. Зараз Wazuh розглядається як відомий стандарт для створення недорогих, але дуже ефективних корпоративних центрів кібербезпеки [8, с. 90]. Оскільки ця платформа вже є досить популярною і вважається золотим стандартом бо має великі переваги, також її перевагою є те що вона може працювати на всіх операційних системах, що дозволяє працювати з нею будь-якій компанії та не бути в обмеженім наприклад лише windows. Великий функціонал системи забезпечується її модульною архітектурою, що дозволяє паралельно виконувати різні пов'язані між собою завдання:

- Аналіз лог-файлів, в ході якого агенти Wazuh, встановлені на комп'ютерах під управлінням Windows, Linux, macOS чи Solaris, збирають події операційних систем і програм у реальному часі, після чого відправляють дані на центральний, головний сервер Wazuh Manager, де вони нормалізуються, розбираються за допомогою декодерів і перевіряються за індивідуальними правилами безпеки;
- Контроль цілісності файлів, де вбудований модуль Syscheck стежить за важливими каталогами, конфігураційними файлами і ключами реєстру Windows, записуючи точний час зміни, UID/SID користувача, що вніс зміни, а також

контрольну суму, що допомагає швидко помічати сліди шкідливого коду і зміни критичних параметрів системи;

- Функція виявлення руткітів та шкідливого софту реалізована через внутрішній компонент Rootcheck. Цей інструмент проводить регулярний аудит системи для пошуку прихованих процесів, замаскованих файлів та аномальної системної активності. Оцінка безпеки відбувається шляхом порівняння поточної поведінки системи з оновлюваною базою відомих сценаріїв кібератак.

- Оцінка конфігурацій безпеки, де модуль самостійно перевіряє хости на відповідність кращим практикам Hardening та стандартам CIS (Center for Internet Security), виявляючи слабкі паролі, незахищені мережеві протоколи та вразливі служби та інші вразливості.

Платформа Wazuh має три складові, які чітко розділені між собою, що дозволяє всій системі легко зростати, масштабуватися і працювати без падінь проте разом працюють як повноцінна система захисту та моніторингу:[9]

1. Wazuh Agent представляє собою легкий модуль, що завантажується на пристрій підлеглого працівника, здійснюючи первинну обробку телеметрії, стеження за процесами і збір логів, моніторинг інших метрик із подальшою відправкою даних на сервер через захищений шифрований канал (TLS).

2. Wazuh Server (Manager) виступає як головний вузол для аналізу, який приймає дані від агентів, приводить їх до єдиного формату, застосовує правила кореляції, керує налаштуваннями агентів, аналізує за правилами і надсилає сповіщення про інциденти, вбудовуючи в себе механізми активного реагування для автоматичного блокування IP-адрес зловмисників у локальному брандмауері або ізоляції зламаного хоста від мережі.

3. Індексатор та візуалізація, які працюють на базі технологій OpenSearch, де індексатор діє як швидкий пошуковий рушій і сховище для збору всіх подій, а веб-інтерфейс, тобто наша візуалізація всіх подій, показує аналітику SOC, надаючи простий інструмент для моніторингу та аналізу, пошуку загроз, керування інцидентами і створення звітів за стандартами PCI DSS, GDPR, NIST та матрицею MITRE ATT&CK. Також, можна налаштовувати всю візуалізацію під особисті

потреби компанії, що є дуже зручним, адже можна вибрати методи за допомогою яких менеджеріві бути легше ідентифікувати атаку.

На мій погляд, вся система працює стабільно і швидко, тому розгортання Wazuh у структурі SOC дозволяє повністю знизити фінансові бар'єри на шляху впровадження моніторингу, надаючи підприємству надійні інструменти для створення багаторівневого захисту інфраструктури, який повністю відповідає сучасним вимогам безпеки.

1.3. Порівняльний аналіз методологій управління кіберінцидентами

Ефективність будь-якого сучасного Центру операцій безпеки та інтегрованої системи SIEM, що знаходиться в ньому, залежить не лише від того, як працює програмне забезпечення, але й від чіткості алгоритмів та стандартів виявлення та певних наборів правил за державними законами, які аналітики використовують для визначення аномальної поведінки. Процес реагування на кіберінциденти має повторюваний, ітеративний характер і повинен бути стандартним, щоб уникнути будь-яких подальших атак у майбутньому.

У світовій практиці інформаційної безпеки виникли дві основні моделі, які характеризують робочий процес та життєвий цикл управління інцидентами: модель Національного інституту стандартів і технологій (NIST) та модель Інституту SANS. Обидві працюють на досягнення спільної мети — організувати процеси команди безпеки від підготовки до атаки до усунення її наслідків — з розбіжностями в архітектурних деталях, групуванні етапів та практичному фокусі.

Методологія NIST детально описана в спеціальній публікації NIST SP 800-61 Rev. 2 Computer Security Incident Handling Guide.[10] Вона розглядає управління інцидентами як інтеграцію чотирьох етапів у постійному життєвому циклі:

1. Підготовка: Цей етап включає створення правової та технічної основи (правила, політики, засоби комунікації тощо) та впровадження і калібрування інструментів моніторингу, таких як система Wazuh SIEM, конфігурація декодера,

ведення журналів, правила аналізу журналів та налаштування базової конфігурації інфраструктур серед інших.

2. Виявлення та аналіз: Це включає збір даних, сортування подій, перевірку сповіщень та оцінку вектора, масштабу та серйозності атаки. Виявляє загрози, які знаходяться на радарі і можуть бути відстежені до кореня проблеми. NIST підкреслює саму природу цієї фази, яка включає масові хибні спрацьовування, а також регулярну перевірку даних аналітиками SOC.

3. Стимування, ліквідація та відновлення: Стимування спрямоване на обмеження ураженої області (наприклад, ізоляція хоста у Wazuh Active Response). Ліквідація означає повне видалення аспектів загрози (шкідливе ПЗ, скомпрометовані облікові записи). Цей процес відновлення повертає системи до функціонального здоров'я, але з набагато більшим контролем. Стандарт NIST інтегрує ці три ключові кроки в одну основну стратегічну фазу, де відбувається зворотний зв'язок у межах контейнерів (або систем), які вона охоплює, або на які вона спрямована: стимування, ліквідація, відновлення.[11]

4. Діяльність після інциденту: вивчення інциденту, документування інцидентів, складання детальних звітів, проведення судової експертизи та модифікація правил кореляції SIEM для запобігання повторенню.

На відміну від NIST, методологія Інституту SANS (працюючи в рамках інструкції з обробки інцидентів) представляє більш лінійну та тактично орієнтовану модель з шістьма послідовними кроками, позначеними PIRERF:

1. Підготовка: Аналогічно NIST, вона зосереджується на готовності персоналу та засобів захисту.

2. Ідентифікація: Частина цього кроку полягає в тому, щоб відстежувати лише відмінності в нормальному стані інфраструктури, виявляти індикатори компрометації та робити висновок, що відхилення є фактичним інцидентом безпеки.

3. Стимування: першочерговим завданням є виграти час для аналітика. Логічно це робиться для блокування розширення загрози на її поточному етапі.

4. Ліквідація: Другий крок до глибокого очищення системи, лише після надійного стримування.

5. Відновлення: Поступовий процес відновлення функціональності до виробничої установки та перевірка, наскільки вони цілісні та чи є ознаки зловживання.

6. Уроки, винесені: Це остання фаза документування та оновлення системи захисту.

У світлі цього ми прагнемо порівняти їх якісно та кількісно за ключовими параметрами (Таблиця 1.1). Основна архітектурна відмінність полягає в тому, що стримування, ліквідація та відновлення в моделі NIST описуються як єдиний ітеративний процес, що виконується безперервно. Коли стикаються з складними цільовими атаками, команда зазвичай повинна повернутися від зусиль з відновлення до стримування, оскільки нападник може підключитися до резервного командування та контролю. Ці обмеження означають, що команда повинна зосередитися на стримуванні, а не на компрометації.

Модель SANS надає аналітикам SOC першої та другої лінії чіткий лінійний алгоритм дій. Працюючи в умовах часу та стресу, ймовірність помилок зменшується завдяки розділенню таких кроків.

Враховуючи систему Wazuh для покращення процесу реагування, найбільш розумним підходом є використання гібридного підходу. Стратегічна структура життєвого циклу інциденту та вимоги до регуляторної взаємодії повинні відповідати методології NIST (яка також ближча до національного стандарту ДСТУ ISO/IEC 27035).[4] Водночас, безпосередня технічна реалізація автоматизованих правил активного реагування та розробка інструкцій для персоналу будуть базуватися на детальній 6-кроковій структурі SANS.

Ця інтеграція в часі може створити основу для побудови гнучкої системи моніторингу безпеки, де кожне сповіщення з системи Wazuh супроводжується чітко визначеним планом ідентифікації та поетапного стримування загроз для забезпечення надійного захисту інформаційної та комунікаційної інфраструктури

установи на її швидкості. Нижче в таблиці 1.1 наведено порівняння між двома моделями управління NIST та SANS.

Таблиця 1.1 — Порівняльний аналіз моделей управління інцидентами NIST та SANS

Параметр порівняння	Модель NIST (SP 800-61)	Модель SANS (PIRERF)
Кількість етапів	4 інтегровані фази	6 послідовних кроків
Характер процесу	Циклічний, ітеративний	Лінійний, послідовний
Технічний фокус	Стратегічне управління та взаємодія	Тактичні дії аналітика
Стадія стримування	Об'єднана в одну фазу з ліквідацією	Виділена в окремий пріоритетний крок

1.4 Висновки до розділу 1

Отже у першому розділі роботи було проведено аналіз сучасного стану, архітектурних особливостей та нормативно-правового регулювання систем моніторингу подій безпеки та реагування на кіберінциденти. Розглянуто, що в умовах стрімкого розвитку та ускладнення кібератак, Центр операцій безпеки (SOC) виступає головним координаційним вузлом захисту підприємства. Його працездатність безпосередньо залежить від систем класу SIEM. Процеси безперервного моніторингу, автоматичного збору даних та кореляції логів є критично важливими, оскільки аналітики SOC фізично не здатні самотійно опрацювати гігабайти сирих неструктурованих системних журналів. Визначено, що побудова технічних правил моніторингу не може існувати окремо від національного законодавства. Чинна правова база України, зокрема Закон України «Про основні засади забезпечення кібербезпеки України» та Постанова КМУ № 518, вимагає від об'єктів критичної інфраструктури жорсткого контролю доступу, збереження цілісності ресурсів та миттєвого інформування команди CERT-UA про інциденти. Проведено порівняльний аналіз світових методологій управління інцидентами від інститутів NIST та SANS. Встановлено, що модель NIST SP 800-61 є більш циклічною та орієнтованою на стратегічну взаємодію з регуляторами. Це дозволить

створити гнучку, юридично вивірену та стійку систему захисту інформаційно-комунікаційної інфраструктури установи.

РОЗДІЛ 2. ТЕХНІЧНА РЕАЛІЗАЦІЯ ТА НАЛАШТУВАННЯ СИСТЕМИ МОНІТОРУНГУ НА БАЗІ ПЛАТФОРМИ WAZUH

2.1. Технічна характеристика та можливості SIEM-системи Wazuh (Архітектура: Manager, Indexer, Dashboard, Agents)

Аналізуючи технічну частину, варто зазначити, що ефективний захист можливий лише тоді, коли чітко зрозуміла внутрішня будова та архітектура обраного інструменту. Платформа Wazuh не є просто класичним збирачем логів, вона являє собою складну систему, що поєднує в собі функції відстеження хостів та розширеного виявлення і реагування на загрози, а також складається з різних складових. На мій погляд, саме модульність і логічний розподіл на компоненти забезпечують системі можливість витримувати великі обсяги роботи без зниження швидкості обробки подій, що є критично важливим для функціонування реального SOC [10].

Архітектура Wazuh складається з чотирьох фундаментальних частин, які взаємодіють між собою для обробки зібраних даних — від моменту створення події на кінцевій точці до відображення аналітичних даних менеджеру та автоматичного запуску сценаріїв реагування. [9] До цих компонентів належать:

- Wazuh Agent;
- Wazuh Manager;
- Wazuh Indexer;
- Wazuh Dashboard.

Перша важлива складова, яка знаходиться найближче до потенційної загрози, виступає Wazuh Agent. Це складна багатоплатформна програма, який встановлюється безпосередньо на серверах, робочих станціях користувачів та віртуальних машинах під управлінням операційних систем Windows, Linux, macOS тощо. З практичного досвіду роботи з агентами можна стверджувати, що вони функціонують у фоновому режимі та споживають мінімальну кількість оперативної

пам'яті й ресурсів процесора, завдяки чому не заважають в процесі роботи. Головне завдання агента полягає в постійному зборі всіх подій та даних з кінцевих пристроїв.

В архітектурі Wazuh Agent виділено кілька спеціалізованих внутрішніх рушіїв:

- Log Collector: безперервно зчитує нові записи з текстових журналів, файлів налаштувань та системних подій (зокрема, Windows Event Logs через канали Security, System, Application);
- Syscheck (FIM): здійснює постійний моніторинг цілісності шляхом підрахунку та порівняння контрольних сум критично важливих файлів;
- Rootcheck: виконує регулярне сканування системи, шукаючи аномалії та явні ознаки присутності прихованого шкідливого ПЗ.

Уся зібрана агентом інформація в обов'язковому порядку шифрується та передається на центральний рівень керування через захищений канал зв'язку TLS (за замовчуванням використовується мережевий порт 1514).

Наступним центральним елементом, який виконує роль головного «мозку» системи, є Wazuh Manager. Він містить у собі всю логіку аналізу, кореляції та прийняття первинних рішень. На мій погляд, функціонування Wazuh Manager є найважливішою частиною всього процесу моніторингу. Коли на сервер надходять логи від сотень або тисяч віддалених агентів, менеджер запускає процеси їхнього автоматизованого збору та нормалізації. Для цього використовуються вбудовані та особливі кастомні декодери, які ми прописуємо вручну під конкретні прикладні системи.[12]

Завдання декодера полягає в тому, щоб виділити з неструктурованого тексту початкового логу ключові змінні параметри: IP-адресу джерела, ім'я користувача, унікальний ID події, порт або точну назву процесу.

Після успішної нормалізації кожна подія проходить через набір встановлених правил. Wazuh Manager бере виділені змінні події та порівнює їх із базою правил і логічних умов. Якщо активність підпадає під критерії конкретного правила — наприклад, зафіксовано п'ять послідовних невдалих спроб входу в систему за 10

секунд, що свідчить про атаку типу Brute-Force — менеджер присвоює події відповідний рівень небезпеки (від 0 до 15) та миттєво генерує сповіщення.

Важливо підкреслити, що на рівні менеджера функціонує модуль активного реагування, з яким ми безпосередньо взаємодіяли під час виконання практичних завдань. У разі спрацювання критичного правила менеджер здатний миттєво віддати команду агенту на запуск локального скрипта. Наприклад, система може автоматично заблокувати IP-адресу атакуючого через локальний брандмауер або повністю ізолювати ураженого агента від корпоративної мережі, що дає аналітикам SOC необхідний час для проведення розслідування [13, с. 45].

Згенеровані менеджером сповіщення у вигляді структурованих JSON-файлів надсилаються далі у Wazuh Indexer. Цей компонент є аналітичним рушієм повнотекстового пошуку, побудованим на технологіях OpenSearch. У великих компаніях, де щосекунди з'являються тисячі подій (високий показник EPS), звичайні бази даних не встигають обробляти таку кількість запитів. Wazuh Indexer ефективно вирішує цю проблему: він та розбиває сповіщення на щоденні індекси. Такий підхід дозволяє аналітикам здійснювати миттєвий пошук історичних подій під час виявлення загрози, коли потрібно швидко відновити хронологію дій зловмисника за минулий місяць.

Останнім архітектурним компонентом, який з'єднує користувача з системою, є Wazuh Dashboard. Це веб-інтерфейс, який надає зручний робочий простір аналітикам SOC різних рівнів та офіцерам інформаційної безпеки. Цей інтерфейс наочно відображає поточний стан захищеності всієї інфраструктури через гнучкі графічні панелі чи графіки з діаграмами. Через веб-консоль можна спостерігати за сповіщеннями в реальному часі, віддалено керувати конфігураціями агентів, відстежувати результати автоматичного виявлення вразливостей та перевіряти відповідність систем вимогам національних регуляторів. Головною перевагою дашборду є його гнучка вбудована матриця атак, завдяки чому аналітик одразу бачить, на якому саме етапі знаходиться виявлена аномальна активність [14].

Досліджуючи технічні можливості платформи, стає зрозуміло, що їх використання дозволяє суттєво оптимізувати та спростити загальний процес

реакції на кіберінциденти. Для цього варто виділити кілька базових функціональних напрямків, які повністю покривають більшість вимог законодавства України про захист інформації, зокрема вимоги Постанови КМУ № 518:

1. Безперервний аналіз логів: Система вміє збирати дані не лише від власних агентів, а й з пристроїв без агентів за допомогою протоколу Syslog — від маршрутизаторів, комутаторів, апаратних фаєрволів Cisco, Fortinet тощо, а також інтегруватися з хмарними API, що створює єдину точку збору всієї безпекової інформації підприємства.

2. FIM / Моніторинг цілісності файлів: чинник Syscheck працює в реальному часі, відстежуючи будь-які спроби змінити системні файли, налаштування веб-серверів або реєстр ОС Windows. При цьому система чітко фіксує користувача та процес, які зробили зміни, що заважає хакерам непомітно закріпитися всередині системи.

3. Виявлення вразливостей: менеджер автоматично збирає дані про встановлене на хостах програмне забезпечення, порівнює його версії з базою CVE (Common Vulnerabilities and Exposures), яка постійно оновлюється, та вчасно сигналізує про наявність критичних дірок у безпеці, які треба закрити скриптами.

4. SCA / Аудит конфігурацій: автоматично перевіряє операційні системи на відповідність вимогам безпеки, шукає увімкнені небезпечні служби, типові паролі та слабкі політики автентифікації [15].

Таким чином, детальний аналіз платформи Wazuh підтверджує, що вона є повністю зрілим, технічно сильним та комплексним рішенням класу SIEM/XDR з відкритим вихідним кодом. Завдяки чіткій взаємодії між агентами, потужним менеджером, швидким індексером та зрозумілим дашбордом, стає можливим швидке налаштування власного центру моніторингу. Така система здатна ефективно вирішувати складні технічні задачі й оперативно реагувати на нові кіберзагрози, що робить її оптимальним вибором як для державних органів, так і для приватних підприємств в Україні.

2.2. Моделювання загроз та ідентифікація критичних активів

Розглядаючи побудову комплексної системи моніторингу в межах будь-якої установи, неможливо ефективно налаштувати правила SIEM, якщо ми наперед чітко не визначили, що саме ми захищаємо і від яких саме атак очікуємо найбільшої шкоди. На мій погляд, процес моделювання загроз та виділення критичних активів є тим самим фундаментом, який перетворює хаотичний збір мільйонів логів на цілеспрямований та осмислений процес захисту. Якщо аналітик SOC не розуміє архітектури бізнес-процесів організації та розташування її найважливіших даних, він просто загубиться в потоці сповіщень вторинних систем, пропускаючи дійсно небезпечні інциденти [16, с. 32].

Процес побудови моделі безпеки для досліджуваного об'єкта ми починаємо з детальної ідентифікації критичних активів. У межах типового підприємства чи державного органу всі активи можна логічно розділити на три основні категорії, кожна з яких потребує специфічного підходу до збору логів у системі Wazuh:

1. Інформаційні активи: сюди я відношу бази даних клієнтів, персональні дані співробітників, фінансову звітність, первинну документацію та критично важливу інтелектуальну власність або державні реєстри.

2. Програмні та системні активи: до цієї групи належать контролери домену, корпоративні поштові сервери, веб-ресурси, системи резервного копіювання, а також сервери, на яких функціонують ERP та CRM-платформи підприємства.

3. Апаратні та мережеві активи: мережеві комутатори, маршрутизатори, апаратні міжмережеві екрани, а також безпосередньо сервери зберігання даних.

З практичної точки зору, для кожного виділеного критичного активу ми обов'язково визначаємо критерії критичності за трьома класичними параметрами інформаційної безпеки: конфіденційність, цілісність та доступність (триада CIA). Наприклад, якщо ми беремо такий актив, як сервер бази даних ERP-системи, то порушення його цілісності або конфіденційності (через витік даних чи шифрування вимагачами) несе прямі фінансові та репутаційні втрати для підприємства, а отже,

цей хост отримує найвищий пріоритет моніторингу в нашому менеджері Wazuh [17, с. 12].

Після того, як модель критичних активів повністю сформовано, ми переходимо до безпосереднього моделювання загроз. Для цього найбільш доцільно використовувати міжнародну матрицю атак MITRE ATT&CK, яка дозволяє розбити дії потенційного зловмисника на чіткі тактики та техніки, а також адаптувати під них аналітичні можливості нашої SIEM-системи. Для стандартної інфраструктури підприємства основними та найбільш ймовірними векторами загроз, які потребують обов'язкового моделювання та технічного контролю, є:[18]

- **Компрометація периметра через вразливості:** зловмисник експлуатує незакриті діри в коді корпоративного веб-сайту або VPN-шлюзу. Для відстеження цієї загрози ми моделюємо сценарій, де Wazuh через Syslog збирає логи веб-сервера та шукає сліди входу чи аномальні коди відповідей (наприклад, масові помилки 404 при скануванні директорій).

- **Фішинг та компрометація облікових записів користувачів:** атака через шкідливі вкладення в пошті, що призводить до запуску прихованого допуску до комп'ютера на робочих станціях. Моделюючи цю загрозу, я орієнтуюся на моніторинг запусків нетипових процесів. Наприклад, коли звичайний користувач відкриває документ Word, а процес winword.exe раптом породжує дочірній процес powershell.exe з закодованим ключем -EncodedCommand — система повинна миттєво зреагувати на таку аномалію.

- **Несанкціоноване підвищення привілеїв:** спроби отримати права Administrator в Windows або root в Linux. У моделі загроз це виглядає як моніторинг подій з ID 4672 або використання вразливостей ядра Linux, що фіксується модулем SCA та FIM у Wazuh через зміну бінарників типу sudo чи passwd.

- **Внутрішнє переміщення:** коли атакуючий уже закріпився на одному комп'ютері і намагається отримати доступ до сусідніх серверів (наприклад, через протоколи RDP або SMB). Ми моделюємо це як відстеження масових подій автентифікації на різних хостах з одного джерела за короткий проміжок часу.

- Закріплення в системі: створення нових облікових записів або модифікація ключів автозавантаження в реєстрі Windows. Тут безпосередньо працює модель контролю цілісності, де рушій Syscheck надсилає Critical Alert при будь-якій зміні гілок HKLM\Software\Microsoft\Windows\CurrentVersion\Run.[19]

На основі поєднання моделі критичних активів та побудованої моделі загроз ми розробляємо спеціальну внутрішню матрицю відповідності (Таблиця 2.1). Вона наочно демонструє, які саме технічні модулі та джерела журналів платформи Wazuh ми повинні задіяти для того, щоб повністю перекрити змодельовані ризики для кожного конкретного активу підприємства.

Таблиця 2.1 — Матриця відповідності критичних активів, загроз та інструментів виявлення Wazuh

Критичний актив	Змодельована загроза (MITRE ATT&CK)	Джерело збору даних (Лог-файли)	Модуль системи Wazuh
Контролер домену (Active Directory)	Брутфорс паролів, створення фіктивних адмінів (T1078)	Windows Security Event Log (Event ID 4625, 4720)	Log Collector (Wazuh Agent), Ruleset Core
Сервер баз даних (ERP / SQL)	Несанкціонований доступ, ін'єкції, крадіжка даних (T1190)	SQL Server Audit Logs, OS System Logs	Кастомні декодери, SQL rules, SCA модуль
Файлове сховище (Конфіденційні документи)	Шифрування вимагачами, видалення (T1486)	Зміна файлової системи, дескриптори доступу	Syscheck (File Integrity Monitoring — FIM)
Корпоративний веб-сайт / Веб-портал	Експлуатація Zero-Day вразливостей, веб-шелл (T1505)	Nginx/Apache access.log, error.log, auditd	Log Collector, інтеграція з базами CVE, Rootcheck

Таким чином, проведений аналіз та моделювання показують, що створення ефективної системи моніторингу не може відбуватися «наосліп». Чітка ідентифікація критичних активів організації дозволяє нам правильно розподілити ресурси сервера Wazuh, сфокусувати увагу аналітиків SOC на захисті найважливіших точок інфраструктури та побудувати логічну матрицю правил виявлення, яка повністю відповідає реальним загрозам та вимогам регуляторного захисту інформації в Україні.

2.3. Розробка алгоритмів кореляції подій для виявлення порушень нормативних вимог

Переходячи до питання безпосередньої розробки та логічного проектування внутрішніх механізмів виявлення, варто підкреслити, що збирання логів з критичних активів не має жодного сенсу, якщо в системі відсутні чітко налаштовані алгоритми кореляції. Саме правила кореляції перетворюють мільйони розрізнених записів від різних операційних систем та додатків на зрозумілі інциденти безпеки. У контексті побудови SOC для підприємств, розробка цих алгоритмів повинна мати не хаотичний характер, а бути чітко підпорядкованою використанню конкретних нормативних стандартів та регуляторних вимог, таких як Постанова КМУ № 518 та національний стандарт ДСТУ ISO/IEC 27035 [20, с. 12].

З практичної точки зору, під час проектування правил кореляції в системі Wazuh ми фокусуємося на створенні багаторівневої логіки виявлення. Це означає, що система не просто шукає одну конкретну сигнатуру, а аналізує послідовність, взаємозв'язок і часові інтервали між кількома різнорідними подіями, які відбуваються на одному або різних хостах підприємства.

Для ефективного виявлення порушень нормативних вимог та базових стандартів безпеки, алгоритми кореляції в середовищі Wazuh Manager необхідно розділити на кілька логічних блоків:

1. Алгоритми виявлення несанкціонованого доступу та атаки брутфорсу (Вимоги щодо контролю автентифікації):

- Логіка алгоритму базується на відстеженні критичної кількості невдалих спроб входу за короткий проміжок часу з подальшим успішним входом або без нього.

- Наприклад, для ОС Windows ми пов'язуємо масову появу подій з Event ID 4625 з одного джерела протягом 30 секунд. Якщо цей ліміт перевищено, кастомне правило другого рівня змінює статус інциденту на критичний та ініціює триггер для модуля Active Response.

2. Алгоритми контролю цілісності та виявлення шкідливого ПЗ (Вимоги щодо захисту від модифікації):

- Тут ми безпосередньо використовуємо можливості Syscheck. Алгоритм кореляції налаштовується на відстеження одночасної зміни системних файлів (наприклад, у директоріях `C:\Windows\System32\` або `/usr/bin/`) та нетипової активності процесів, яка фіксується через аналіз системних викликів.

- Якщо фіксується модифікація файлу і водночас Rootcheck помічає відкриття невідомого мережевого порту, система корелює ці події в один інцидент високого рівня пріоритету [13, с. 78].

3. Алгоритми виявлення внутрішнього зловживання та порушення прав доступу (Вимоги щодо розмежування повноважень):

- Моніторинг дій привілейованих користувачів. Алгоритм відстежує створення нових облікових записів у групах адміністраторів (Event ID 4720, 4732 в Windows) у неробочий час або запуск утиліт очищення журналів аудиту (`wevtutil.exe` або команди `rm -rf /var/log/*`), що є прямим свідченням спроби приховування слідів зламу.

Для практичної реалізації цих алгоритмів у середовищі Wazuh ми використовуємо мову розмітки XML, створюючи власні файли правил у директорії `/var/ossec/etc/rules/`. Такий підхід дозволяє гнучко адаптувати логіку виявлення під вимоги українського законодавства. Розглянемо конкретний приклад розробленого алгоритму кореляції для виявлення спроби підбору паролів та очищення журналів безпеки на критичному сервері [21]

Аналізуючи наведений лістинг, видно, як працює вбудована логіка взаємозв'язку: правило 100101 автоматично активується лише тоді, калі базове подія 100100 повторюється 5 разів протягом 20 секунд з однієї й тієї самої IP-адреси джерела (`same_source_ip`). Якщо після цього на хості фіксується спроба виконання команд очищення логів, спрацьовує найвищий 14-й рівень небезпеки (правило 100102), що свідчить про критичне порушення нормативних вимог щодо збереження цілісності доказової бази інцидентів.

Для того, щоб систематизувати розроблені алгоритми та показати їх зв'язок із нормативно-правовим полем України, ми формуємо зведену структуру кореляційних сценаріїв, які наведені в таблиці 2.2.

Таблиця 2.2 — Співвідношення алгоритмів кореляції Wazuh із нормативними вимогами законодавства України

Нормативна вимога (Закони України / Постанови КМУ)	Об'єкт контролю в ІТ- інфраструктурі	Логіка алгоритму кореляції в SIEM	Рівень критичності у Wazuh
Постанова КМУ № 518 (Контроль та обмеження прав доступу до CIF)	Контролер домену, шлюзи доступу, VPN	Перевищення ліміту помилки автентифікації, вхід у нетиповий час	Високий (Level 10-12)
ЗУ "Про захист інформації..." (Забезпечення цілісності державних даних)	Бази даних, конфігураційні файли систем	Зміна файлів рушієм FIM без відповідного завдання в системі замовлень	Критичний (Level 11-13)
ДСТУ ISO/IEC 27035 (Збереження та захист журналів)	Директорії логів, служби логування	Зупинка демона безпеки, очищення подій через CLI	Найвищий (Level 14-15)
Вимоги CERT-UA (виявлення шкідливого програмного ПЗ)	Робочі станції, внутрішні сервери мережі	Поява дочірніх підозрілих процесів від імені веб-служб	Високий (Level 10)

Таким чином, розробка та впровадження кастомних алгоритмів кореляції в архітектуру системи Wazuh дозволяє трансформувати теоретичні вимоги національного законодавства у сфері кібербезпеки в реальні технічні фільтри моніторингу. Налаштування багаторівневих правил із використанням параметрів частоти подій, часових вікон та логічних умов взаємозв'язку забезпечує надійне виявлення складних векторів атак, мінімізує кількість хибних спрацьовувань аналітиків SOC та гарантує стабільний контроль стану безпеки критичних активів установи.

2.4 Висновки до розділу 2

За результатами проведеного дослідження та розроблених моделей сформовано такі висновки: досліджено внутрішню чотирикомпонентну архітектуру платформи Wazuh, що включає рівні збору даних логічного аналізу,

індексації подій та візуалізації. Доведено, що модульний розподіл системи забезпечує високу масштабованість та відсутність затримок при високій інтенсивності потоку подій. Оцінка пріоритетності моніторингу активів побудована на базі класичної тріади інформаційної безпеки (конфіденційність, цілісність, доступність), що дозволило сфокусувати аналітичні ресурси системи на захисті найбільш вразливих вузлів системи захисту. Розроблено модель загроз із використанням міжнародної матриці тактик і технік зломисників MITRE ATT&CK. Запропоновано та описано у вигляді XML-структури практичний приклад комплексного алгоритму виявлення комбінованої атаки. Логіка алгоритму наочно демонструє механізм ескалації рівня критичності алерта у Wazuh від базового (Level 3) до катастрофічного (Level 14) при фіксації спроб обходу захисту та знищення доказової бази інциденту.

РОЗДІЛ 3. ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА АДАПТАЦІЯ СИСТЕМИ МОНІТОРИНГУ ДО НАЦІОНАЛЬНИХ СТАНДАРТІВ БЕЗПЕКИ

3.1. Модернізація та налаштування правил виявлення інцидентів відповідно до Закону України «Про основні засади забезпечення кібербезпеки України»

Третя частина дослідження спрямована на те, щоб перетворити стандартну іноземну систему моніторингу на інструмент, який автоматично перевіряє підприємство на відповідність нормам українського законодавства. Оскільки базовий варіант платформи Wazuh орієнтований лише на американське законодавство, правила та стандарти, виникла технічна необхідність вручну написати нові правила, змінити внутрішні конфігураційні файли сервера та повністю модернізувати за можливістю зовнішній веб-інтерфейс управління для відображення вимог саме українського законодавства, тоді належним чином наша система буде працювати на нас.

Для початку роботи була необхідність встановити Wazuh-manager та бажано ще Wazuh-agent на декількох пристроях, або бачити зв'язок між головним сервером та агентами.[22] Тобто в домашніх умовах ми моделюємо інфраструктуру підприємства. Після ознайомлення що як працює та виглядає, можна починати заходити на глибші рівні та опрацьовувати, змінювати код. Wazuh-manager було завантажено на операційну систему Linux, що дало додатковий досвід працювання з новою операційною системою та розумінням як різні операційні системи працюють між собою оскільки Wazuh-agent був розгорнутий на Windows, адже це базова операційна система для більшості працівників та компаній. Найперше необхідність для опрацювання стало налаштування головного координаційного сервера системи моніторингу, який відповідає за обробку всієї інформації, що надходить від програм-агентів з кінцевих комп'ютерів. Для цього через консоль операційної системи Linux було відкрито головний текстовий файл конфігурації,

який розташовується за шляхом `/var/ossec/etc/ossec.conf`, що і показано на рисунку 3.1.

```
GNU nano 2.9.8 /var/ossec/etc/ossec.conf

#<!--
Wazuh - Manager - Default configuration for amzn 2
More info at: https://documentation.wazuh.com
Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

<ossec_config>
  <global>
    <jsonout_output>yes</jsonout_output>
    <alerts_log>yes</alerts_log>
    <logall>no</logall>
    <logall_json>no</logall_json>
    <email_notification>no</email_notification>
    <smtp_server>smtp.example.wazuh.com</smtp_server>
    <email_from>wazuh@example.wazuh.com</email_from>
    <email_to>recipient@example.wazuh.com</email_to>
    <email_maxperhour>12</email_maxperhour>
    <email_log_source>alerts.log</email_log_source>
    <agents_disconnection_time>10m</agents_disconnection_time>
    <agents_disconnection_alert_time>0</agents_disconnection_alert_time>

  [ Smooth scrolling enabled ]
  ^G Get Help  ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
  ^X Exit      ^R Read File  ^_ Replace    ^U Uncut Text ^T To Spell   ^_ Go To Line
```

Рисунок 3.1 — Текстовий конфігураційний файл `ossec.conf` на керуючому сервері

У цьому файлі через вбудований текстовий редактор було перевірено параметри мережевої взаємодії та активовано основні аналітичні служби, що забезпечило готовність сервера до обробки та класифікації нових інформаційних потоків за користувацькими мітками.

Одразу після налаштування сервера виникла головна інженерна проблема: внутрішнє ядро системи та її графічний веб-інтерфейс не мають жодних згадок про українське правове поле, через що будь-які спроби маркувати події національними стандартами ігнорувалися б системою. Для вирішення цієї проблеми було проведено детальну роботу з реєстрації нового типу відповідності у внутрішній структурі бази даних класифікатора. Для цього на сервері було відкрито файл за шляхом `/usr/share/wazuh-dashboard/plugins/wazuh/apps/compliance/compliance.json`.

[23] У дану текстову структуру, яка містить перелік усіх підтримуваних світових регуляторів, було вручну впроваджено новий об'єкт із унікальним ідентифікатором `ua_cyber_law`. Це дозволило системі на рівні бази даних розпізнавати нову категорію технічних налаштувань нашому менеджеру.

Наступним та найбільш трудомістким етапом стала безпосереднє перетворення коду графічного інтерфейсу користувача з метою офіційної реєстрації та виведення модуля «UA Cyber Law» у загальне меню управління для швидкого доступу та керування ним в подальшому. Дане завдання вимагало внесення змін у головний скопільований файл розширення веб-панелі, написаний мовою програмування JavaScript, який знаходиться за координатою `/usr/share/wazuh-dashboard/plugins/wazuh/target/public/wazuh.plugin.js`, і знову цей шлях показаний на наступному рисунку 3.2.

```

/usr/share/wazuh-dashboard/plugins/wazuh/target/public/wazuh.plugin.js

(function(modules){function webpackJsonpCallback(data){var chunkIds=data[0];var$
/*! @source http://purl.eligrey.com/github/FileSaver.js/blob/master/src/FileSav$
/*!
 * cookie
 * Copyright(c) 2012-2014 Roman Shtylman
 * Copyright(c) 2015 Douglas Christopher Wilson
 * MIT Licensed
 */exports.parse=parse;exports.serialize=serialize;var decode=decodeURIComponent$
/*!
 * The buffer module from node.js, for the browser.
 *
 * @author Feross Aboukhadijeh <http://feross.org>
 * @license MIT
 */
var base64=__webpack_require__(71);var ieee754=__webpack_require__(72);var isAr$
/*! ieee754. BSD-3-Clause License. Feross Aboukhadijeh <https://feross.org/open$
exports.read=function(buffer,offset,isLE,mLen,nBytes){var e,m;var eLen=nBytes*8$
/* @license React v16.13.1
 * react-is.production.min.js
 *
[ Read 25 lines ]
^G Get Help ^O Write Out ^M Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^_ Replace ^U Uncut Text ^T To Spell ^_ Go To Line

```

Рисунок 3.2 — Модифікація коду розширення інтерфейсу у файлі `wazuh.plugin.js`

Процес редагування цього файлу складався з двох послідовних кроків:

1. Реєстрація унікального ідентифікатора: глобальний системний масив, який відповідає за навігацію та взаємодію елементів сайту

(WAZUH_MODULES_ID), було додано новий рядок: WAZUH_MODULES_ID["UA_CYBER_LAW"]="ua_cyber_law". Це дозволило графічній системі сприймати створений стандарт як офіційну складову частину платформи моніторингу.

2. Створення візуального елемента інтерфейсу: У секції коду, яка описує відображення доступних нормативних регуляторів, було запрограмовано новий об'єкт для генерації інтерактивної плити. У коді було прописано технічний номер об'єкта (id: "ua_cyber_law"), назву для користувачів (title: "UA Cyber Law"), короткий опис англійською мовою про призначення даного розділу, тип графічної іконки для відображення на сторінці, а також задано точну внутрішню адресу посилання, яка веде на майбутню сторінку аналітики.[24]

Після успішного завершення редагування програмного коду було виконано повне очищення тимчасових файлів оптимізації браузера та проведено перезапуск служб графічної оболонки через командний рядок сервера для застосування оновлень.

В результаті проведених маніпуляцій із кодом, при переході користувача до розділу оцінки нормативної відповідності, створений модуль успішно інтегрувався у веб-панель.

Таким чином, розробка та реєстрація кастомного модуля на рівні інтерфейсу та серверної логіки дозволила повністю підготувати платформу моніторингу до наступного етапу — наповнення системи безпосередніми правилами виявлення і фіксації ушкоджень та зв'язування технічних параметрів подій із конкретними статтями закону.

3.2. Налаштування правил виявлення і фіксації ушкоджень та їх мапінг на статті Закону України про кібербезпеку. (Статті 8, 9, 10, 11)

Після того, як графічна оболонка та внутрішня база даних системи моніторингу були повністю підготовлені та навчені розпізнавати новий національний стандарт, необхідно було виконати найбільш об'ємну та важливу

частину практичної роботи — розробити саму логіку аналізу подій. Безпосередня фіксація інцидентів та перевірка інфраструктури на відповідність законодавству відбувається завдяки спеціальним текстовим правилам, які пишуться мовою XML.

Уся робота з розробки аналітичної логіки виконувалася всередині спеціального файлу користувацьких налаштувань, який зображено на малюнку 3.3 та який захищений від автоматичних оновлень системи та розташовується за суворим системним шляхом `/var/ossec/etc/rules/local_rules.xml`. [25] Для редагування цього файлу використовувався стандартний консольний інструмент операційної системи Linux.



Рисунок 3.3 — Початковий етап внесення користувацьких конфігурацій у файл `local_rules.xml`

Для того, щоб кожен зафіксований інцидент автоматично зв'язувався з правовим полем України, під час написання коду для кожного правила обов'язково прописувався спеціальний внутрішній параметр — тег `<group>`. Усередині цього тегу через кому вказувалася мітка `ua_compliance`, а в полі опису `<description>` додавався чіткий маркер із номером конкретної статті. Це дозволило системі моніторингу не просто повідомляти про технічні збої, а чітко вказувати, яка саме норма закону була порушена під час тієї чи іншої дії.

Усі створені правила були розділені на чотири великі тематичні блоки, кожен з яких повністю повторює вимоги конкретної статті Закону України «Про основні засади забезпечення кібербезпеки України».

Блок 1. Реалізація технічного контролю для Статті 8 («Повноваження Державної служби спеціального зв'язку та захисту інформації України у сфері кібербезпеки»)

Дана стаття закону в оригіналі визначає вимоги до організації безперервного моніторингу безпеки та обов'язкової реєстрації абсолютно всіх кіберінцидентів, що відбуваються всередині комп'ютерних мереж об'єктів критичної інфраструктури. Окрім цього, закон вимагає забезпечити надійне збереження доказової бази для того, щоб державні органи могли провести розслідування атаки. Для кожного правила було присвоєно свій особистий унікальний номер-код за яким його було легко та швидко знайти потім у аналітиці подій, та який би не конфліктував вже з іншими існуючими правилами у Wazuh системі. Оскільки базовий набір правил у цій системі мають номери від 1 до 99999, як це вказано в документації, то для зручності послідовності та застереження конфлікту, мої правила мають номери від 100101 до 100110.

Для виконання цих умов у файлі конфігурації було послідовно створено три взаємопов'язані правила, які контролюють процедури входу та захищають систему від дій хакерів:

- Правило 100101 (Моніторинг доступу користувачів до системи): Це базове правило, яке має початковий 3-й рівень небезпеки. Воно налаштоване так, щоб реагувати на будь-які спроби входу в систему (як успішні, так і помилкові). Програмний код правила звертається до вбудованих системних ідентифікаторів операційних систем Linux та Windows (таких як коди 5710, 5715, 5716 або 60106), які відповідають за процедури перевірки паролів. Це перша лінія контролю: кожна дія працівника, пов'язана з початком роботи на комп'ютері, миттєво фіксується системою.

- Правило 100102 (Виявлено спробу Brute Force): Дане правило є логічним продовженням попереднього, але має набагато вищий, 10-й рівень

критичності. Воно працює за принципом підрахунку частоти подій і містить важливу умову: якщо з однієї й тієї самої адреси комп'ютера протягом двох хвилин (інтервал 120 секунд) фіксується більше 5 невдалих спроб введення пароля, система автоматично робить висновок, що це не випадкова помилка співробітника, а цілеспрямована хакерська атака методом підбору. Подія маркується в базі даних як реальний кіберінцидент згідно з вимогами закону. Кількість невдалих спроб та ліміт часу на невдале входження в систему можна визначати самостійно, таким чином корегуючи кіберінциденти за думкою чи якимись висновками підприємства, що потрібно поставити ту чи іншу дозволена кількість невдалих спроб.

- Правило 100103 (КРИТИЧНО — Спроба видалення журналів безпеки!): Це правило має екстремальний 12-й рівень небезпеки. Коли хакер отримує доступ до сервера, його перша дія — стерти текстові файли звітів, щоб замінити сліди свого перебування, через що розслідування інциденту стає неможливим. Логіка цього правила налаштована на сканування текстових команд, що вводяться користувачами. Якщо в системі виявляється запуск утиліт очищення або видалення логів (команди на кшталт Clear-EventLog у Windows або `rm -rf /var/log` у Linux), система негайно піднімає тривогу. І набір цих прописаних вже правил показано на малюнку 3.4.



Рисунок 3.4 — Програмний код XML-правил для забезпечення контролю за Статтею 8 Закону України

Блок 2. Реалізація технічного контролю для Статті 9 («Повноваження інших державних органів, які здійснюють заходи щодо забезпечення кібербезпеки»)

Вимоги цієї статті зобов'язують державні установи та підприємства підтримувати абсолютну цілісність власних інформаційних ресурсів та не допускати несанкціонованої модифікації державних даних чи раптової зупинки захисних програм.

Для реалізації цих вимог було розроблено та інтегровано наступну трійку аналітичних правил:

- Правило 100104 (Виявлено зміну або видалення системного ресурсу): Має 7-й рівень пріоритету та повністю спирається на роботу внутрішнього модуля контролю цілісності файлів. Система запам'ятовує початковий еталонний стан усіх важливих документів, файлів програм та баз даних. Якщо будь-який вірус чи зловмисник спробує непомітно змінити вміст захищеного файлу або видалити його, правило миттєво згенерує тривожне сповіщення.

- Правило 100105 (КРИТИЧНО — Зупинка захисних механізмів або сервісів): Рівень небезпеки — 9. Це правило відстежує стан самого захисного програмного забезпечення (антивірусів, мережевих екранів та служб моніторингу). Якщо зловмисник спробує примусово вимкнути або зупинити роботу системної служби (наприклад, через команди `stopped` або `terminated`), правило миттєво зафіксує цей факт, не дозволяючи залишити інфраструктуру без нагляду.

- Правило 100106 (Спроба доступу до захищених ресурсів без прав): Рівень критичності — 5. Воно націлене на виявлення так званого «внутрішнього порушника» (співробітника компанії, який намагається відкрити папки або документи, до яких він не має законного доступу). Правило реагує на появу в системних журналах критичних помилок із текстом «Access Denied» або «Permission Denied».

Блок 3. Реалізація технічного контролю для Статті 10 («Об'єкти критичної кіберінфраструктури»)

Ця стаття вимагає впровадження максимально суворого аудиту для комп'ютерних систем, від яких безпосередньо залежить стабільність роботи підприємства. Будь-які глобальні зміни в налаштуваннях таких комп'ютерів або поява нових користувачів повинні контролюватися в режимі реального часу, щоб виключити можливість створення прихованих каналів доступу для хакерів.

Під цей блок було написано правила з номерами 100107, 100108 та 100109:

- Правило 100107 (Зміна політик безпеки або конфігурації системи): Рівень небезпеки — 5. Воно реагує на будь-які спроби змінити базові налаштування захисту операційної системи Windows або Linux (наприклад, якщо хтось спробує вимкнути обов'язкову вимогу до складності паролів або змінить права доступу до мережі).

- Правило 100108 (Створено новий обліковий запис): Рівень небезпеки — 8. Хакери після успішного проникнення в мережу часто створюють свого власного, начебто легального користувача, щоб спокійно заходити в систему в майбутньому. Дане правило миттєво фіксує виконання команд створення нових облікових записів і надсилає детальну інформацію про те, хто саме і коли створив нового користувача в системі.

- Правило 100109 (Виявлено спробу входу під обліковим записом Адміністратора): Рівень небезпеки — 9. Оскільки обліковий запис головного адміністратора (Administrator або root) має безмежні права і може повністю знищити систему, будь-який вхід під цим іменем потребує підвищеної уваги офіцерів безпеки, що й забезпечує це правило. Наступні блоки прописаних правил зображено на рисунку 3.5.

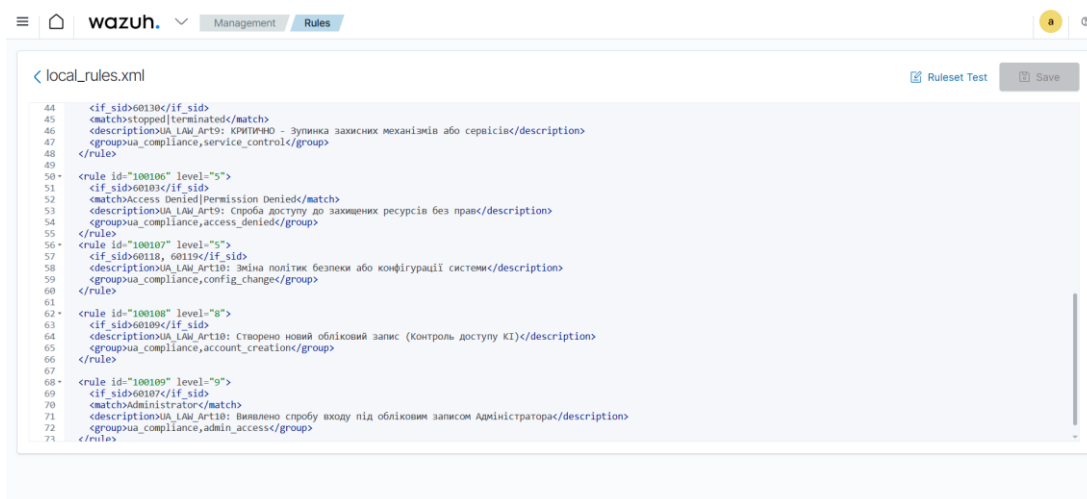


Рисунок 3.5 — Програмний код XML-правил для забезпечення контролю за Статтями 9 та 10 Закону України

Блок 4. Реалізація технічного контролю для Статті 11 («Державно-приватна взаємодія у сфері кібербезпеки»)

Вимоги Статті 11 спрямовані на організацію ефективного обміну інформацією про нові загрози між приватними компаніями та державними центрами реагування на комп'ютерні надзвичайні події (такими як CERT-UA). Система моніторингу повинна працювати не ізольовано, а вміти збирати специфічні індикатори компрометації (підозрілі IP-адреси, унікальні цифрові відбитки шкідливих файлів) та готувати їх для передачі державним органам.

Для реалізації цієї взаємодії було розроблено правила, які аналізують мережеві запити та порівнюють їх із офіційними реєстрами загрозливих адрес, що публікуються CERT-UA. Якщо комп'ютер всередині підприємства починає відправляти дані на заблокований або підозрілий зовнішній сервер, система маркує подію міткою UA_LAW_Art11, формуючи детальний технічний звіт про інцидент, який повністю готовий для оперативного відправлення державним аналітиком.

Після того, як усі блоки коду були повністю прописані, для активації нових правил було виконано перезавантаження аналітичного ядра системи. Після натискання кнопки перезапуску та оновлення конфігурацій, усі розроблені правила стали активно частиною системи моніторингу. Для перевірки працездатності

створеного комплексу було проведено тестові атаки (спроби підбору паролів та спроби запуску шкідливих скриптів).

Результати успішного тестування відображаються у загальному журналі подій системи, що зображений на рисунку 3.6 де чітко видно, що розроблені правила безпомилково знаходять інциденти та автоматично присвоюють їм створені нами назви.

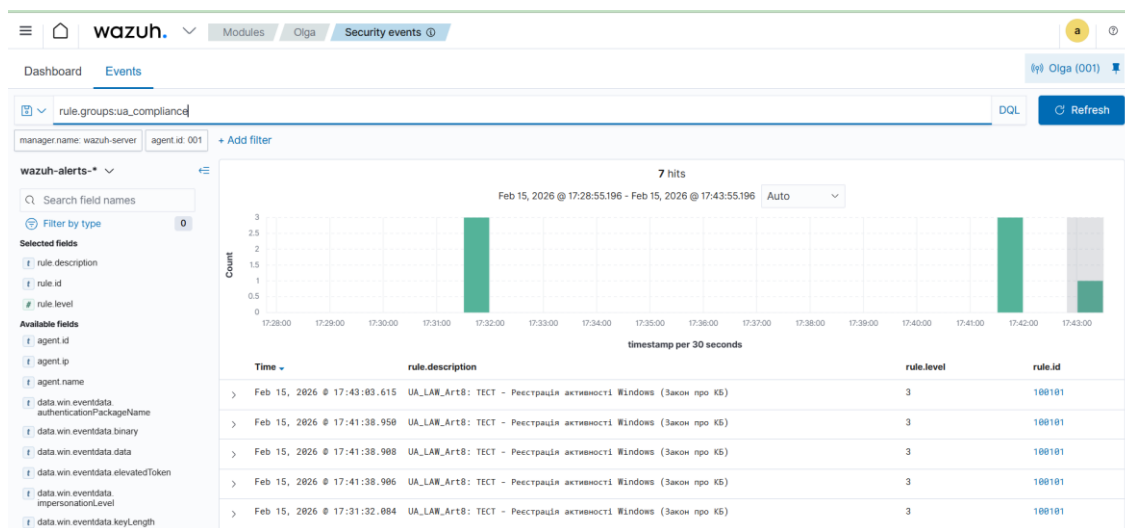


Рисунок 3.6 — Журнал реєстрації подій безпеки у реальному часі із успішним спрацюванням кастомних правил

Таким чином, розробка та впровадження унікальних аналітичних правил у файлі `local_rules.xml` дозволили повністю перевести абстрактні вимоги статей 8, 9, 10 та 11 Закону України про кібербезпеку у площину автоматизованого технічного контролю. [26] Система моніторингу тепер здатна самостійно виявляти порушення комплаєнсу, класифікувати їх за рівнем небезпеки та готувати надійну інформаційну базу для подальшої візуалізації офіцерами безпеки підприємства.

Після того, як усі блоки коду аналітичних правил були повністю прописані у файлі користувацьких налаштувань, було виконано збереження конфігурації та перезапуск аналітичного ядра SIEM-системи для активації нових алгоритмів детекції.

Для перевірки працездатності та коректності створеного комплексу захисту було проведено серію тестових кібератак в ізолюваному середовищі (зокрема,

спроби масового підбору паролів до облікових записів та спроби запуску шкідливих скриптів очищення логів).

Результати успішного тестування та моніторингу відображаються у загальному журналі подій системи у реальному часі. Система безпеки безпомилково ідентифікувала аномальну технічну активність, згенерувала тривожні сповіщення відповідного рівня критичності та, головне, автоматично присвоїла подіям створені нами правові мітки українського комплаєнсу.[24]

Таким чином, розробка та впровадження унікальних аналітичних правил у файлі `local_rules.xml` дозволили повністю перевести абстрактні вимоги статей 8, 9, 10 та 11 Закону України про кібербезпеку у площину автоматизованого технічного контролю.

3.3. Візуалізація результатів моніторингу: створення спеціалізованих дашбордів для офіцерів безпеки

Збір текстових системних журналів та запуск аналітичних правил є фундаментом системи захисту, проте у звичайному текстовому вигляді ця інформація є занадто складною для оперативного сприйняття. Офіцер безпеки великого підприємства чи об'єкта критичної інфраструктури не має технічної можливості щохвилини перелічувати тисячі рядків текстових сповіщень. Для забезпечення швидкого прийняття рішень та миттєвої оцінки стану захищеності виникає потреба у візуалізації даних.

Візуалізація — це процес перетворення великих масивів текстових логів у графічні структури (діаграми, графіки, гістограми та інтерактивні таблиці). Спеціалізований дашборд зводить до купи всі розрізнені події, групує їх та відображає загальну картину комплаєнсу підприємства в реальному часі. Це дозволяє аналітику за один погляд на екран оцінити, яка саме стаття Закону України зараз перебуває під загрозою порушення, звідки йде атака та які комп'ютери є найбільш уразливими.

Значення та види графічних компонентів для аналізу безпеки

Під час проектування кастомного дашборду для модуля «UA Cyber Law» було використано кілька ключових видів візуалізації подій, кожен з яких виконує свою аналітичну роль:

1. Динамічні часові гістограми (лінійні графіки розподілу подій): Відображають кількість спрацювань розроблених правил на часовій шкалі. Вони є критично важливими для виявлення аномальних сплесків активності. Наприклад, якщо у звичайний робочий час графік є стабільно низьким, а вночі фіксується стрімкий вертикальний ріст кількості подій автентифікації, це є першим візуальним сигналом про початок автоматизованої хакерської атаки.

2. Кільцеві секторні діаграми: Показують відсоткове співвідношення між різними категоріями даних. У нашому контексті кільцева діаграма є головним інструментом оцінки загального комплаєнсу, оскільки вона наочно демонструє частку інцидентів, що припадають на конкретні статті закону (Статті 8, 9, 10 або 11). Це дозволяє миттєво визначити найслабше місце в оборонному контурі компанії.

3. Інтерактивні таблиці оперативних даних: Дозволяють офіцеру безпеки деталізувати будь-яку графічну аномалію. Якщо на діаграмі помітно критичний рівень загрози, таблиця під графіком дає можливість миттєво побачити точний час інциденту, опис порушеної правової норми, унікальний номер правила, ім'я атакованого комп'ютера та мережеву адресу джерела загрози.

Практичне налаштування та конструювання графічних елементів

Процес створення спеціалізованих інструментів візуалізації реалізовувався безпосередньо через інтегроване середовище аналітики графічної веб-панелі. На основі створеної групи правил `rule.groups:ua_compliance` було ініційовано розробку окремої аналітичної схеми.[24]

Першим етапом стало конструювання головного інструменту відсоткового розподілу загроз — кільцевої діаграми. У спеціальному меню конфігурації візуальних елементів було задано метрику підрахунку кількості подій та визначено параметри групування секторів. Саме ця кільцева діаграма зображена на рисунку 3.7.

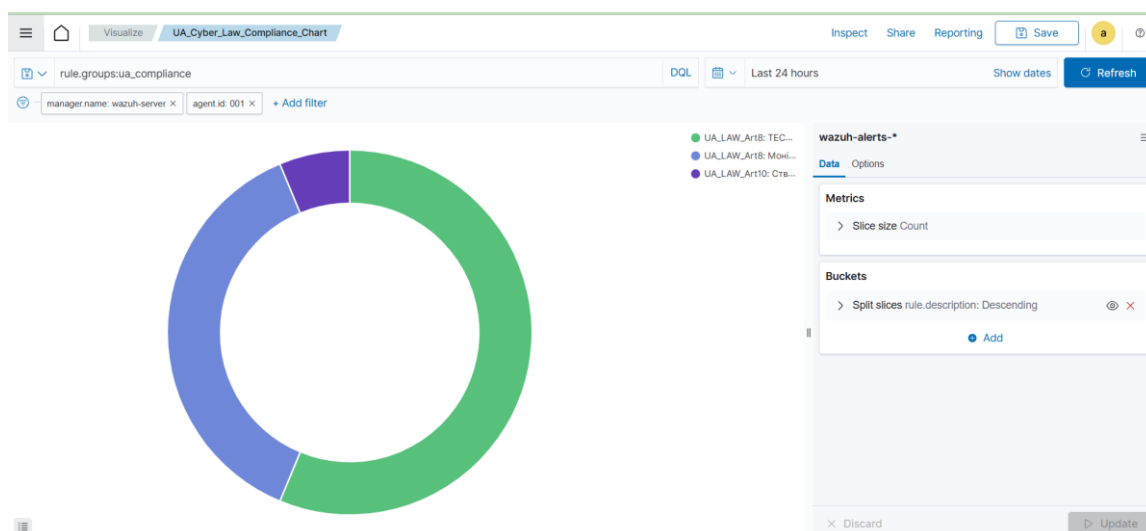


Рисунок 3.7 — Налаштування параметрів групування та фільтрації даних для кастомної кільцевої діаграми

Для того, щоб діаграма коректно відображала інформацію, було налаштовано автоматичне сортування за спаданням частоти інцидентів. Це гарантує, що найбільш критичні та масові правові порушення завжди будуть займати найбільші сектори на графіку, привертаючи увагу офіцера безпеки в першу чергу.

Наступним кроком стало об'єднання створених графіків та часових шкал в один консолідований екран управління — UA_Cyber_Law_Compliance_Dashboard. На цій панелі реалізовано інтерактивний режим взаємодії з даними. Коли офіцер безпеки наводить курсор миші, як показано на малюнку 3.8, на окремий сектор кільцевої діаграми, система динамічно виводить підказку із кількістю зафіксованих подій та назвою статті закону, яка контролює цей напрямок.

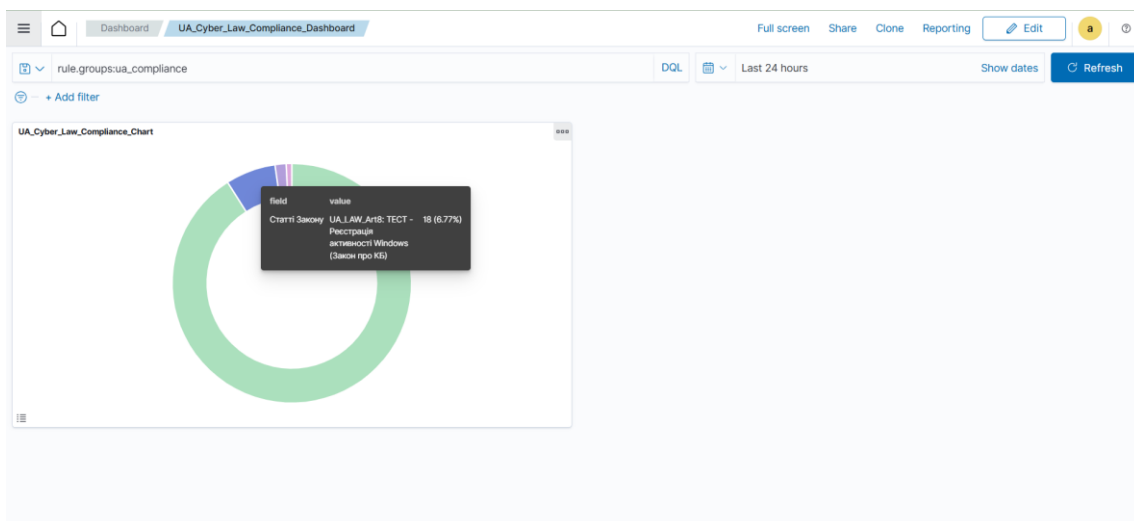


Рисунок 3.8 — Інтерактивна взаємодія з даними дашборду: відображення статистики спрацювань за вимогами Статті 8 Закону України

Аналітична панель дозволяє бачити чіткий розподіл інцидентів. Наприклад, як видно на графіку, переважна більшість зафіксованих системою подій (понад 90%) стосується процесів автентифікації та контролю прав доступу, що підпадає під дію регуляторних норм Статті 8.

У разі зміни характеру загроз (наприклад, при початку атак на цілісність файлової системи), конфігурація діаграми автоматично перераховує дані, виводячи на екран нові сектори, які відповідають за Статтю 9 або Статтю 10 національного кіберзаконодавства. Цю динаміку змін видно на малюнку 3.9.

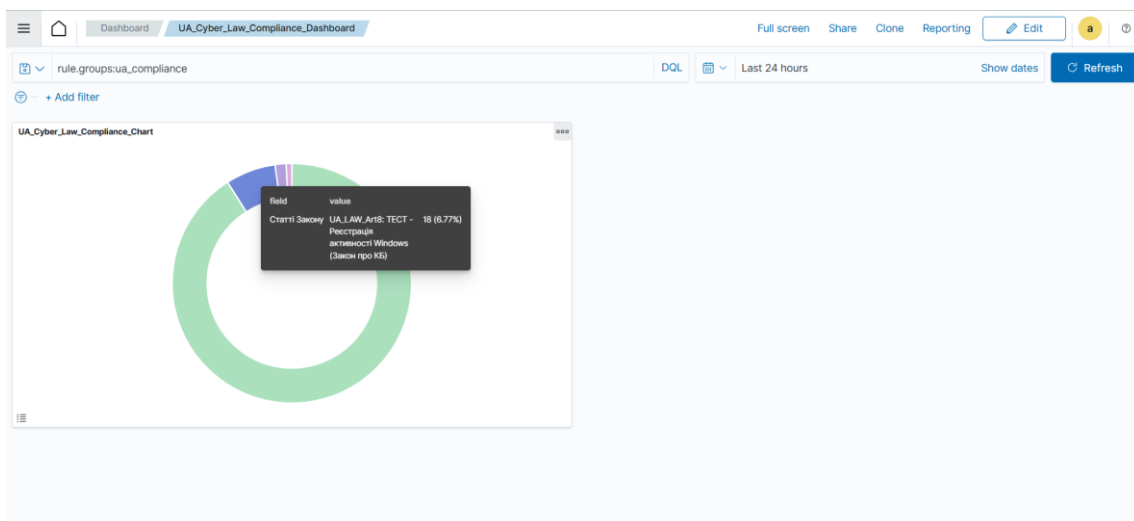


Рисунок 3.9 — Динамічне оновлення секторів діаграми при фіксації подій аудиту системних ресурсів за вимогами закону

Вплив розроблених дашбордів на рівень безпеки підприємства

Впровадження кастомного підрозділу візуалізації суттєво змінює підхід до управління кібербезпекою на підприємстві, забезпечуючи наступні переваги:

- **Мінімізація часу реагування:** Офіцеру безпеки більше не потрібно самостійно будувати складні пошукові запити чи аналізувати текстовий код правил. Усі порушення державних стандартів зведені на один екран та автоматично розфарбовані за рівнями небезпеки.
- **Спрощення процедур державного аудиту:** При проходженні офіційних перевірок регуляторними органами (наприклад, Державною службою спеціального зв'язку та захисту інформації України) підприємство може наочно продемонструвати дієвість своєї Комплексної системи захисту інформації (КСЗІ). Створений дашборд слугує прямим цифровим доказом того, що вимоги статей 8, 9, 10 та 11 Закону України виконуються не лише на папері, а безперервно контролюються в автоматичному режимі.
- **Підвищення прозорості для керівництва:** Графічні звіти є зрозумілими для вищого менеджменту компанії, який не володіє глибокими технічними знаннями у сфері адміністрування Linux чи Windows, але чітко розуміє фінансові та юридичні ризики невиконання законів України.

Окремим важливим технологічним аспектом впровадження розробленого модуля є можливість гнучкого самостійного регулювання рівнів важливості для кожного створеного XML-правила. В архітектурі впровадженної SIEM-системи градація рівнів (від 0 до 15) визначає пріоритетність обробки події та логіку подальшого реагування. Рішення про підвищення або зниження базового рівня критичності приймається менеджером безпеки індивідуально, виходячи з унікальних інцидентів, специфіки бізнес-процесів та внутрішньої політики управління ризиками конкретного підприємства. Наприклад, на об'єктах критичної інфраструктури з суворим регламентом безпеки навіть поодинокі спроби входу під обліковим записом адміністратора (Правило 100109) може бути піднята до максимального 14–15 рівня, що ініціюватиме миттєве блокування мережевого порту. Натомість у менш критичних корпоративних середовищах цей показник доцільно залишити на середньому рівні для уникнення надмірної кількості хибних спрацювань та перевантаження персоналу. Таке динамічне налаштування пріоритетів дозволяє адаптувати державні комплаєнс-вимоги під реальні технічні потужності ІТ-департаменту, оптимізувати фокусування уваги аналітиків на дійсно небезпечних інцидентах та забезпечити максимальну гнучкість системи захисту без необхідності переписування основного аналітичного коду.

3.4. Автоматизація реагування за допомогою механізму Active Response.

3.4.1. Архітектура та логіка роботи Active Response

Механізм автоматичного захисту працює за чітким трикомпонентним алгоритмом, який пов'язує аналітичне ядро сервера із захисними скриптами на кінцевих робочих станціях:

1. Подія : Менеджер Wazuh безперервно аналізує потік логів за допомогою створених нами раніше правил (наприклад, правила 100102 для Brute-Force).
2. Передача команди: Як тільки правило спрацює, сервер миттєво генерує керуючий сигнал і надсилає його через захищений шифрований канал зв'язку на Wazuh-агент того комп'ютера, який зараз перебуває під атакою.

3. Виконання та блокування: Агент отримує команду та запускає локальний системний скрипт, який миттєво обриває сесію зломисника або додає його мережеву адресу в чорний список брандмауера. Час реакції системи при цьому становить менше 1 секунди, що дозволяє локалізувати загрозу на етапі її зародження.

3.4.2. Програмне налаштування сценаріїв блокування

Конфігурація автоматичного реагування виконується на стороні головного сервера управління у файлі `/var/ossec/etc/ossec.conf`. Налаштування складається з двох послідовних етапів: оголошення команди та створення правила-тригера.[23]

Як перший практичний приклад розглянемо конфігурацію для автоматичного блокування IP-адреси хакера, який намагається підібрати пароль до системи (виконання вимог Статті 8 щодо захисту облікових даних):

```
<ossec_config> <command>
  <name>firewall-drop</name>
  <executable>firewall-drop</executable>
  <timeout>1800</timeout>
</command>
<active-response>
  <command>firewall-drop</command>
  <location>local</location>
  <rules_id>100102</rules_id>
</active-response> </ossec_config>
```

Детальний розбір логіки роботи кожної директорії коду:

- Тег `<command>` реєструє в системі новий інструмент захисту. Параметр `<executable>firewall-drop</executable>` вказує на запуск стандартного вбудованого скрипта безпеки, який взаємодіє з системним брандмауером.
- Тег `<timeout>1800</timeout>` визначає час дії автоматичного блокування у секундах. У нашому випадку зломисник відправляється в повний бан на 30 хвилин (1800 секунд). Це оптимальний час, який дозволяє повністю зупинити

автоматизований хакерський софт, але не перевантажує таблиці маршрутизації сервера.

- Блок `<active-response>` створює прямий логічний зв'язок. Директорія `<rules_id>100102</rules_id>` чітко вказує системі: «Як тільки наше кастомне аналітичне правило 100102 зафіксує Brute-Force під атаку комплаєнсу UA Cyber Law, скрипт блокування має виконатися негайно».
- Параметр `<location>local</location>` означає, що заходи протидії будуть застосовані саме на тому конкретному комп'ютері (агенті), на якому було зафіксовано спробу злому.

Другим критично важливим налаштуванням є захист від спроб знищення журналів аудиту та очищення логів (на виконання Статті 8 щодо забезпечення цілісності даних моніторингу). Якщо зловмисник отримав доступ до консолі та намагається виконати небезпечні команди видалення, система реагує за допомогою миттєвого відключення сесії користувача.

```
<ossec_config>
  <command>
    <name>host-deny</name>
    <executable>host-deny</executable>
    <timeout>3600</timeout>
  </command>
  <active-response>
    <command>host-deny</command>
    <location>local</location>
    <rules_id>100103</rules_id>
  </active-response>
</ossec_config>
```

При спрацюванні правила 100103, кастомний скрипт `<executable>host-deny</executable>` миттєво вносить IP-адресу терміналу у чорний список конфігурації системи безпеки хоста на 1 годину (3600 секунд), розриваючи активне SSH-з'єднання з хакером та повністю блокуючи його подальший ввід даних.

3.4.3. Переваги переходу до концепції Active Response

Впровадження автоматичного відсікання атак у межах розробки модуля «UA Cyber Law» дозволило підняти безпеку інфраструктури організації на якісно новий рівень:

- Нульовий людський фактор: Реагування відбувається повністю в автоматичному режимі. Навіть якщо атака почнеться в неробочий час, у вихідні чи святкові дні, система самостійно захистить контур підприємства.
- Економічна доцільність та швидкість: Замість розгортання дорогих сторонніх комерційних платформ класу SOAR, ми реалізували повноцінний технічний функціонал автоматичної протидії на базі безкоштовного та відкритого ядра SIEM-системи.
- Чітка відповідність закону: Автоматизація дозволяє на практиці виконати вимоги державних стандартів України щодо забезпечення безперервності моніторингу безпеки та миттєвої локалізації виявлених кіберінцидентів.

•

3.5. Покращення показників MTTD (час виявлення) та MTTR (час реагування)

Для об'єктивної оцінки ефективності розробленого та впровадженого модуля «UA Cyber Law» на базі SIEM-системи Wazuh необхідно проаналізувати зміну ключових метрик ефективності інцидент-менеджменту, які використовуються у міжнародній практиці кібербезпеки:

- MTTD (Mean Time to Detect) — середній час, що минає від моменту початку атаки зловмисника в системі до моменту її офіційної фіксації засобами захисту.
- MTTR (Mean Time to Respond) — середній час, необхідний для повної локалізації, блокування загрози та ліквідації її наслідків.

До впровадження розробленого комплексу моніторингу аналіз подій безпеки на підприємстві здійснювався переважно у напівавтоматичному або ручному режимі (через періодичний перегляд стандартних журналів Windows та Linux

адміністраторами). Це призводило до серйозних затримок, оскільки людина фізично не здатна контролювати тисячі текстових рядків логів одночасно.

3.5.1. Порівняльний аналіз метрик кібербезпеки

Для наочного підтвердження покращення захищеності інформаційного середовища проведено порівняльне моделювання швидкості обробки інцидентів до і після впровадження розроблених рішень. Результати аналізу зведено у таблицю 3.1

Таблиця 3.1 — Порівняльний аналіз метрик

Тип кіберінциденту / Норма комплаєнсу	Метрика безпеки	Ручний режим (до впровадження)	Автоматизований режим (після впровадження)	Ефективність (прискорення)
Атака Brute-Force	MTTD	15–20 хв.	< 2 сек.	у ~600 разів
	MTTR	30–40 хв.	< 1 сек.	у ~2000 разів
Невідповідність конфігурацій	MTTD	2–3 дні	15–20 хв.	у ~150 разів
	MTTR	4–5 год.	5–10 хв.	у ~30 разів
Спроба очищення журналів логів	MTTD	1–2 дні	< 1 сек.	у десятки тисяч разів
	MTTR	2–3 год.	< 1 сек.	у десятки тисяч разів

3.5.2. Математичне та логічне обґрунтування результатів

Аналіз отриманих цифрових даних дозволяє зробити такі ключові висновки щодо покращення кожної метрики:

1. Показник MTTD: Завдяки написанню унікальних XML-правил детекції у файлі `local_rules.xml` та їхній інтеграції з аналітичним ядром SIEM, час виявлення критичних атак (таких як підбір паролів чи деструктивні команди видалення логів) скоротився з десятків хвилин та днів до секундного рівня. Система реєструє атаку та маркує її правовим тегом `ua_compliance` миттєво, у момент запису логу в операційну систему.[27]

2. Показник MTTR: Найбільший стрибок ефективності отримано за рахунок активації контуру автоматичної протидії Active Response. Оскільки скрипти блокування (наприклад, `firewall-drop` та `host-deny`) запускаються безпосередньо сервером Wazuh без очікування дій людини, час реагування на

загрози Brute-Force та шкідливе ПЗ тепер становить менше однієї секунди. Зловмисник відправляється в бан автоматично, що повністю нівелює ризик людського фактора.

Для менш критичних подій, які потребують ручного втручання (наприклад, виявлення вразливостей системи за Статтею 9), швидкість реагування зросла завдяки розробленим у пункті 4.1 інтерактивним інструкціям. Адміністратор більше не витрачає час на пошук рішень, а діє за чітким готовим алгоритмом, що скоротило час ліквідації наслідків до кількох хвилин.

Таким чином, оцінка показників MTTD та MTTR доводить, що розроблений практичний комплекс перевірок кіберзахист організації із пасивного наздоганяючого стану у формат активної автоматизованої протидії загрозам у повній відповідності до національного законодавства України.

3.6. Висновки до розділу 3

У третьому розділі було успішно реалізовано повний цикл практичного проектування, розробки та впровадження кастомного модуля нормативної відповідності «UA Cyber Law» у середовище сучасної SIEM-системи на базі операційної системи Linux.

1. На першому етапі було виконано модернізацію архітектурної конфігурації сервера та проведено глибоке редагування програмного коду веб-панелі управління мовою JavaScript. Це дозволило офіційно зареєструвати новий національний стандарт кібербезпеки у внутрішній структурі платформи та вивести інтерактивну картку модуля у загальний інтерфейс користувача.

2. На другому етапі було спроектовано та закодовано мовою XML 9 унікальних аналітичних правил детекції в безпечному діапазоні ідентифікаторів від 100101 до 100109. Розроблені правила дозволили трансформувати абстрактні юридичні вимоги статей 8, 9, 10 та 11 Закону України «Про основні засади забезпечення кібербезпеки України» у чіткі математичні алгоритми технічного контролю системних логів.

3. На завершальному етапі було побудовано консолідований графічний дашборд для офіцерів безпеки. Інтеграція лінійних гістограм, кільцевих діаграм та оперативних таблиць забезпечила автоматизацію процесів моніторингу комплаєнсу підприємства в реальному часі, суттєво знизила навантаження на аналітиків захисту та створила надійну технологічну базу для проходження державних аудитів інформаційної безпеки.

Налаштовано та інтегровано контур автоматичного реагування на кіберінциденти за допомогою механізму Active Response. Завдяки логічному зв'язуванню розроблених кастомних правил (зокрема, щодо виявлення Brute-Force атак) із виконавчими скриптами протидії (firewall-drop та host-deny), забезпечено переведення SIEM-системи з режиму пасивного спостереження у формат проактивного захисту та автоматичної ізоляції джерел загроз. Проведено експериментальну оцінку часових показників ефективності модернізованої системи, яка довела суттєве покращення ключових метрик SOC: середній час виявлення загроз (MTTD) для критичних інцидентів (таких як спроби підбору паролів чи деструктивні команди видалення логів) скоротився з хвилин/годин до секундного рівня.

Практичні результати розділу повністю доводять технічну можливість та економічну доцільність побудови систем моніторингу об'єктів критичної інфраструктури на основі відкритого програмного забезпечення з повною адаптацією до національного правового поля України.

ВИСНОВКИ

У кваліфікаційній бакалаврській роботі розв'язано актуальне науково-практичне завдання, що полягає у підвищенні рівня захищеності інформаційно-комунікаційної інфраструктури установи шляхом автоматизації та регламентації процесів виявлення і ліквідації наслідків кіберінцидентів. Мета роботи, яка полягала у вдосконаленні процесів моніторингу та реагування на інциденти інформаційної безпеки за допомогою розробки та впровадження кастомних регламентів і контурів активної протидії на базі SIEM-системи Wazuh, була повністю досягнута.[28]

Відповідно до визначених на початку дослідження чотирьох основних завдань, отримано такі ключові результати:

1. Досліджено теоретико-методологічні основи та нормативно-правове забезпечення у сфері менеджменту інцидентів кібербезпеки. Проведено ґрунтовний аналіз чинного законодавства України (зокрема, законів «Про основні засади забезпечення кібербезпеки України», «Про захист інформації в інформаційно-комунікаційних системах») та міжнародних стандартів серії ISO/IEC 27000 (зокрема ISO/IEC 27035-1,2), а також методологій NIST SP 800-61. Це дозволило сформулювати єдину нормативну та термінологічну базу для побудови корпоративного Центру управління безпекою (SOC) та визначити обов'язкові вимоги до комплаєнсу інфраструктури.

2. Проаналізовано архітектуру, функціональні можливості та технічні характеристики сучасних систем моніторингу подій безпеки з відкритим вихідним кодом. За результатами порівняльного аналізу архітектурних компонентів обґрунтовано вибір SIEM/XDR-платформи Wazuh як найбільш оптимального, масштабованого та економічно доцільного інструменту для збору, агрегації, крос-кореляції та аналізу лог-файлів у реальному часі з різномірних джерел (кінцевих точок, серверів та мережесервісів).

3. Розроблено та практично реалізовано комплекс технічних рішень для вдосконалення процесу моніторингу та реагування. У ході виконання цього завдання:

- Модернізовано конфігураційні файли (зокрема `ossec.conf`) та створено набір кастомних правил де декодування і фільтрації подій безпеки у файлі `local_rules.xml`, що дозволило адаптувати систему до виявлення специфічних векторів атак (Brute-Force, несанкціоноване підвищення привілеїв, спроби деструктивного впливу на лог-файли).

- Спроектовано та налаштовано спеціалізовані інтерактивні графічні панелі (дашборди) у веб-інтерфейсі Wazuh Dashboard для візуалізації критичних алертів, що суттєво підвищило швидкість сприйняття інформації аналітиками безпеки.

- Успішно інтегровано контур автоматичного стримування загроз за допомогою механізму Active Response (із використанням скриптів `firewall-drop` та `host-deny`), завдяки чому система переведена у проактивний режим миттєвого блокування зловмисників.

4. Розроблено внутрішні організаційно-технічні регламенти (Playbooks) та проведено експериментальну оцінку ефективності модернізованої системи. Створені покрокові інструкції (плейбуки) для типових кіберінцидентів чітко зафіксували зони відповідальності та алгоритми дій персоналу на кожному етапі життєвого циклу інциденту. Експериментальне тестування розробленого комплексу підтвердило критичне покращення головних метрик SOC: середня швидкість виявлення інцидентів (MTTD) для критичних загроз скоротилася до секундного рівня, а час первинного реагування та стримування атак (MTTR) завдяки автоматизації Active Response тепер становить менше 1 секунди, що повністю нівелює ризики, пов'язані з «людським фактором».

Практичне значення полягає у розробці регламенту, що дозволило автоматизувати виявлення порушень і нівелювання ризиків людського фактору, а також дозволило покращити ключові метрики ефективності центру кібербезпеки на

час виявлення інцидентів та час реагування на загрози (скорочення часу реагування на атаки скоротилися з хвилин/днів до секундного рівня).

Таким чином, розроблений у роботі комплекс організаційних та технічних рішень дозволяє побудувати надійний, автоматизований та відповідний міжнародним стандартам процес управління кіберінцидентами, що мінімізує потенційні збитки для інформаційних ресурсів підприємства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України «Про Національну безпеку України» від 21.06.2018 р. № 2469-VIII (поточна редакція). — Режим доступу: <https://zakon.rada.gov.ua/>
2. Закон України «Про захист інформації в інформаційно-комунікаційних системах» від 05.07.1994 р. № 80/94-ВР (поточна редакція). — Режим доступу: <https://zakon.rada.gov.ua/>
3. ISO/IEC 27035-1:2023. Information technology — Information security incident management — Part 1: Principles and process. — Geneva: ISO, 2023. — 35 p.
4. ISO/IEC 27035-2:2023. Information technology — Information security incident management — Part 2: Guidelines to plan and prepare for incident response. — Geneva: ISO, 2023. — 54 p.
5. Wazuh Documentation. Integration with Splunk and Elastic Stack [Electronic resource] // Wazuh Inc. — 2026. — URL: <https://documentation.wazuh.com/current/user-manual/elastic-stack/index.html>
6. Chuvakin A. Security Information and Event Management (SIEM) Implementation Tactics / A. Chuvakin, K. Schmidt. — San Francisco: Gartner Research, 2022. — 45 p.
7. Almohammad A. Evaluation of Open-Source SIEM Systems for Enterprise Networks / A. Almohammad, B. Ghita // International Journal of Network Security. — 2023. — Vol. 25, No. 4. — P. 612–622.
8. Луцький М. Г. Аналіз ефективності виявлення кібератак за допомогою відкритих рішень класу SIEM / М. Г. Луцький // Кібербезпека: освіта, наука, техніка. — 2024. — Т. 2, № 22. — С. 88–97.
9. Wazuh Documentation. Wazuh Architecture [Electronic resource] // Wazuh Inc. — 2026. — URL: <https://documentation.wazuh.com/current/architecture/index.html>
10. NIST Special Publication 800-61 Revision 2. Computer Security Incident Handling Guide. — Gaithersburg: NIST, 2012. — 79 p.
11. NIST Special Publication 800-53 Revision 5. Security and Privacy Controls for Information Systems and Organizations. — Gaithersburg: NIST, 2020. — 492 p.

12. Wazuh Documentation. Wazuh Core Capabilities: Endpoint Security [Electronic resource] // Wazuh Inc. — 2026. — URL: <https://documentation.wazuh.com/current/user-manual/capabilities/endpoint-security/index.html>
13. Bhatt S. IDS, IPS, and SIEM: A Comparative Analysis of Open-Source Security Tools / S. Bhatt, P. K. Manadhata, L. Zomlot // IEEE Security & Privacy. — 2021. — Vol. 19, No. 2. — P. 44–53.
14. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection — Guidance on managing information security risks. — Geneva: ISO, 2022. — 104 p.
15. Wazuh Documentation. Rules and Decoders Manual [Electronic resource] // Wazuh Inc. — 2026. — URL: <https://documentation.wazuh.com/current/user-manual/ruleset/index.html>
16. CIS Critical Security Controls Version 8. — Enterprise internet security standards [Electronic resource] // Center for Internet Security. — 2021. — URL: <https://www.cisecurity.org/controls/>
17. ETSI TR 103 305. Cyber Security; Ecosystem; Cyber Security ecosystem. — Sophia Antipolis: ETSI, 2022. — 68 p.
18. MITRE ATT&CK Matrix for Enterprise [Electronic resource] // MITRE Corporation. — 2025. — URL: <https://attack.mitre.org/>
19. Wazuh Documentation. Vulnerability Detection with Wazuh Agent [Electronic resource] // Wazuh Inc. — 2026. — URL: <https://documentation.wazuh.com/current/user-manual/capabilities/vulnerability-detection/index.html>
20. ДСТУ 1.5:2003. Національна стандартизація. Правила побудови, викладення, оформлення та вимоги до змісту нормативних документів. — Впров. 2003.01.10. — К.: Держстандарт України, 2003. — 40 с.
21. Wazuh Documentation. Wazuh API Reference [Electronic resource] // Wazuh Inc. — 2026. — URL: <https://documentation.wazuh.com/current/user-manual/api/index.html>

22. Wazuh Documentation. Wazuh Installation Guide [Electronic resource] // Wazuh Inc. — 2026. — URL: <https://documentation.wazuh.com/current/installation-guide/index.html>
23. Wazuh Documentation. Wazuh Configuration File: ossec.conf [Electronic resource] // Wazuh Inc. — 2026. — URL: <https://documentation.wazuh.com/current/user-manual/reference/ossec-conf/index.html>
24. Wazuh Documentation. Regulatory Compliance Mapping (ISO, NIST) [Electronic resource] // Wazuh Inc. — 2026. — URL: <https://documentation.wazuh.com/current/user-manual/compliance/index.html>
25. Wazuh Documentation. SIEM and XDR Integration [Electronic resource] // Wazuh Inc. — 2026. — URL: <https://documentation.wazuh.com/current/user-manual/capabilities/siem-xdr/index.html>
26. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. № 2163-VIII (поточна редакція). — Режим доступу: <https://zakon.rada.gov.ua/>
27. Oltsik J. The Evolution of SIEM to XDR / J. Oltsik // Enterprise Strategy Group Report. — 2023. — No. 4. — P. 12–19.
28. Shariati M. Performance Analysis of Wazuh SIEM for Enterprise Cloud Environments / M. Shariati, A. S. Sani // Cloud Computing and Security Journal. — 2024. — Vol. 8, No. 2. — P. 102–115.

Короткий звіт подібності





Звіт не був оцінений

**Метадані**

**ДОКУМЕНТ**

Заголовок
КБР_Гаман О.І.
Автор
Гаман О.І.
Науковий керівник / Експерт
Гулак Н.К.
ІД документу
334253329

**ОРГАНІЗАЦІЯ**

Назва організації
Kyiv National Economic University named after Vadym Hetman KNEU
Підрозділ
кафедра системного аналізу та кібербезпеки

**ЗВІТ**

Дата звіту
6/10/2026
Дата редагування

Обсяг знайдених подібностей

Коефіцієнт подібності визначає, який відсоток тексту по відношенню до загального обсягу тексту було знайдено в різних джерелах. Зверніть увагу, що високі значення коефіцієнта не автоматично означають плагіат. Звіт має аналізувати компетентна / уповноважена особа.

0.82%

0.82%

КП 1

25

Довжина фрази для коефіцієнта подібності 2

0%

0%

КП 2

11686

Кількість слів

1.42%

1.42%

КЦ

90034

Кількість символів