Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Чорненького Святослава Віталійовича

на здобуття ступеня вищої освіти магістра

Метод забезпечення стійкості корпоративних інформаційних систем до комплексних кіберзагроз

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

Шифр КРМКБЗІ. 2401101.24.01.15 ПЗ

Виконав студент 2 курсу група КБЗІм-24-1 Святослав ЧОРНЕНЬКИЙ
Керівник канд. техн. наук, доцент Володимир ДЖУЛІЙ
Нормоконтролер д-р. філософії, старший викладач Наталія ПЕТЛЯК

До захисту допускаю:
Завідувач кафедри кібербезпеки Юрій КЛЬОЦ

16 12 2025 р.

Хмельницький 2025

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Рівень вищої освіти Магістр

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека та захист інформації

Освітня програма Кібербезпека та захист інформації

ЗАТВЕРДЖУЮ

Завідувач кафедри кібербезпеки

Юрій КЛЬОЦ

01 09 2025 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Чорненькому Святославу Віталійовичу

1 Тема роботи Метод забезпечення стійкості корпоративних інформаційних систем до комплексних кіберзагроз

Керівник роботи канд. техн. наук., доц. Джулій В.М.

Затверджено наказом ректора університету від 25 08 2025 № 65

2 Строк подання студентом кваліфікаційної роботи на кафедру 1.12.2025 р.

3 Вихідні дані до роботи Спроєктувати й реалізувати архітектуру системи адаптивного захисту, вибрати програмні засоби та технологічну платформу для реалізації, розробити та обгрунтувати метод адаптивного захисту, розробити алгоритми динамічної оцінки ризиків, оптимізації параметрів реагування та алгоритм адаптивного захисту, розробити та налаштувати сценарії автоматизації для взаємодії компонентів системи захисту.

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)

Вступ, Теоретичні основи забезпечення стійкості корпоративних інформаційних систем, Моделі забезпечення стійкості корпоративних інформаційних систем, Система захисту корпоративних інформаційних систем від комплексних кіберзагроз, Висновки.

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

6 Консультанти розділів кваліфікаційної роботи

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

7 Дата видачі завдання 01 09 2025 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Затвердження теми кваліфікаційної роботи	01.09.2025 р.	Виконано
Ґрунтовне ознайомлення та дослідження предметної галузі	06.09.2025 р.	Виконано
Визначення змісту, структури кваліфікаційної роботи	14.09.2025 р.	Виконано
Підготовка першого розділу кваліфікаційної роботи	26.09.2025 р.	Виконано
Підготовка другого розділу кваліфікаційної роботи	11.10.2025 р.	Виконано
Підготовка третього розділу кваліфікаційної роботи	28.10.2025 р.	Виконано
Підготовка статті/тези за темою кваліфікаційної роботи	06.11.2025 р.	Виконано
Підготовка та оформлення ілюстративного матеріалу	18.11.2025 р.	Виконано
Оформлення кваліфікаційної роботи	24.11.2025 р.	Виконано
Попередній захист кваліфікаційної роботи	27.11.2025 р.	Виконано
Захист кваліфікаційної роботи на засіданні ЕК	01.12.2025 р.	Виконано

Студент _____ Святослав ЧОРНЕНЬКИЙ

Керівник кваліфікаційної роботи _____ Володимир ДЖУЛІЙ

АНОТАЦІЯ

Тема кваліфікаційної роботи: Метод забезпечення стійкості корпоративних інформаційних систем до комплексних кіберзагроз.

Автор роботи: Чорненький Святослав Віталійович.

Керівник роботи: к.т.н. доц. Джулій Володимир Миколайович.

Загальний обсяг роботи: 117 с., 29 рисунків, 1 таблиця, 6 формул, 64 джерел.

Ключові слова: корпоративна інформаційна система, комплексні кіберзагрози, адаптивний захист, система захисту, оркестрація безпеки, автоматизація реагування, динамічна оцінка ризику.

Сучасні корпоративні інформаційні системи стикаються з постійним зростанням кількості та складності комплексних кіберзагроз, які швидко еволюціонують та обходять стандартні засоби безпеки. У таких умовах, традиційні підходи до захисту КІС часто є занадто повільними та не ефективними.

У магістерській роботі вирішується наукова задача створення методу адаптивного захисту корпоративної інформаційної системи, що дозволить суттєво покращити динамічне реагування на інциденти в режимі реального часу. Розроблено методику, що дозволяє забезпечити високу стійкість КІС до комплексних кіберзагроз через комплексну систему захисту.

Запропоноване рішення характеризується впровадженням поєднання систем оркестрації, декількох різнорідних систем виявлення та реагування, алгоритмів динамічної оцінки ризику, адаптивного часу блокування та алгоритму адаптивного захисту КІС. Це дозволяє значно підвищити швидкість реагування, зменшити кількість помилкових спрацювань та, в загальному, збільшити ефективність прийняття рішень. Результати роботи можуть бути використані особами, що прагнуть підвищити автоматизацію процесів захисту та підвищити кіберстійкість підприємств.

01.12.2025 р.

ANNOTATION

Qualification work topic: Method for ensuring the resilience of corporate information systems to complex cyber threats.

Author: Sviatoslav Chornenkyi Vitaliyovych.

Mentor: Ph.D. Dzhulii Volodymyr Mykolayovych.

Total volume of work: 117 pages, 29 figures, 1 table, 6 formulas, 64 sources.

Keywords: corporate information system, complex cyber threats, adaptive protection, protection system, security orchestration, response automation, dynamic risk assessment.

Modern corporate information systems face a constant increase in the number and complexity of complex cyber threats that are rapidly evolving and bypassing standard security measures. In such conditions, traditional approaches to CIS protection are often too slow and ineffective.

The master's thesis addresses the scientific problem of creating a method for adaptive protection of corporate information systems, which will significantly improve dynamic response to incidents in real time. A methodology has been developed that ensures high resistance of CIS to complex cyber threats through a comprehensive protection system.

The proposed solution is characterized by the implementation of a combination of orchestration systems, several heterogeneous detection and response systems, dynamic risk assessment algorithms, adaptive blocking time, and an adaptive CIS protection algorithm. This significantly increases the response speed, reduces the number of false positives, and, in general, increases the effectiveness of decision-making. The results of the work can be used by those seeking to increase the automation of protection processes and improve the cyber resilience of enterprises.

01.12.2025р.

ЗМІСТ

Вступ 8
1 Теоретичні основи забезпечення стійкості корпоративних інформаційних систем 12
1.1 Поняття стійкості ІС та критерії її оцінювання 12
1.2 Класифікація кібератак та комплексних загроз 13
1.3 Сучасні підходи до захисту корпоративних систем (багаторівневий захист, Zero Trust, IDS/IPS і т.д.) 18
1.4 Аналіз стандартів та нормативних документів (ISO/IEC 27001, NIST CSF, ДСТУ, GDPR) 20
1.5 Постановка задачі 23
2 Моделі забезпечення стійкості корпоративних інформаційних систем 25
2.1 Формальні моделі загроз та сценаріїв атак й засобів захисту корпоративних інформаційних систем від комплексних кіберзагроз 25
2.2 Показники ефективності захисту корпоративних інформаційних систем від комплексних кіберзагроз 34
2.3 Модель функціонування корпоративної інформаційної системи, що захищається 37
2.4 Алгоритм оцінювання ефективності захисту корпоративних інформаційних систем із застосуванням марківських моделей 40
2.5 Метод адаптивного захисту корпоративної інформаційної системи від комплексних кіберзагроз 43
2.6 Висновки 46
3 Система захисту корпоративних інформаційних систем від комплексних кіберзагроз 47
3.1 Архітектура системи адаптивного захисту корпоративної інформаційної системи від комплексних кіберзагроз 47
3.2 Алгоритм адаптивного захисту корпоративної інформаційної системи від комплексних кіберзагроз 53
3.3 Система захисту корпоративних інформаційних систем від комплексних

кіберзагроз..... 62
3.4 Структура програмного забезпечення системи адаптивного захисту корпоративних інформаційних систем 69
3.5 Засоби виявлення комп'ютерних атак на корпоративних інформаційних систем 75
3.6 Висновки 84
Висновки 85
Перелік джерел посилання 87
Додаток А Фрагмент коду 94
Додаток Б Копії наукових публікацій 99

ВСТУП

Найважливішим моментом для визначенності є актуальність дослідження. Її варто підкреслити, адже актуальність саме цього дослідження високою. Адже у сучасному інформаційному середовищі корпоративні інформаційні системи трансформувалися з допоміжних інструментів в критично важливий елемент для різноманітних компаній, щоб забезпечувати безперервність та ефективність різних процесів. І також відбувається глобальна цифровізація та перехід до хмарних технологій, вводиться все частіше віддалена робота та інтеграція з системами Інтернету речей (IoT), що призводить до розмивання традиційного периметру безпеки. Тобто корпоративна інфраструктура стає все більше різнородною, розподіленою та надзвичайно складною для адміністрування. Це, у свою чергу, створює нові виклики для захисту даних та управління доступом, адже відбувається еволюція загроз у кіберпросторі. Таким чином, класичні моделі безпеки вже не здатні ефективно протидіяти багатовекторним атакам. Відповідно кіберзагрози стають комплексними. Тому й виникає потреба у впровадженні адаптивних систем захисту, що будуть враховувати контекст, швидко реагувати на інциденти, гнучко масштабуватися та інтегруватися з різними джерелами даних. Також для таких систем захисту важливим є поєднання аналітики, автоматизації та глибокого розуміння поведінкових патернів. Особливої гостро проблема захисту КІС набуває в Україні в умовах війни. Щодня державні установи, критична інфраструктура та приватний бізнес стикаються з атаками, які спрямовані не лише на крадіжку даних, а й на повне знищення інформаційних систем, блокування доступу до сервісів та дестабілізації економічних процесів. Такі дії мають на меті паралізувати роботу країни зсередини. Тому у таких умовах забезпечення кіберстійкості стає питанням національної безпеки. Аналіз сучасних підходів до кіберзахисту показує, що традиційні моделі переживають кризу. І як вже згадувалось, класичні інструменти вже не справляються з новими викликами. У відповідь на це компанії намагаються закривати такі виклики десятками різними підходами та за використанням різних систем безпеки (SIEM, EDR тощо). Але це створює іншу проблему –

нагромадження повідомлень щодо безпеки у потоках сповіщень так, що повідомлення про важливі інциденти можуть губитися серед великої кількості сигналів. Також сучасні атаки діють досить швидко, а час виявлення та реагування на інциденти досить великий при ручній обробці. Ця часова різниця стає критичною вразливістю. А людина фізично не здатна обробити тисячі подій і прийняти рішення з потрібною швидкістю та точністю. Вирішенням цієї проблеми є впровадження систем SOAR. Такі системи дозволять зробити захист адаптивним, автоматизувати рутинні дії та прискорити реагування. Ці системи можуть враховувати реальний контекст події (важливість активу, типи подій, джерела сповіщень, наявність інших контрольованих засобів захисту тощо). Таким чином, потрібні не просто автоматизовані, а розумні, контекстно-орієнтовані системи SOAR, що будуть здатні адаптувати свої дії до визначених ситуації, а не просто працювати за жорсткими шаблонами. Так що необхідний метод роботи такої системи, який поєднував би централізовану оркестрацію з адаптивними алгоритмами. Така система працювати в режимі реального часу, автоматично підлаштовувати різін конфігурації захисту та підтримувати потрібний баланс між безпекою і доступністю сервісів.

Отже, метою дослідження є створення та обґрунтування методу адаптивного захисту, що дозволятиме підвищити рівень безпеки та стійкості корпоративних інформаційних систем від складних, комплексних, багатовекторних кіберзагроз. Такий підхід має забезпечити здатність системи не лише протидіяти відомим атакам, а й також швидко адаптуватися до нових сценаріїв, щоб підтримувати безперервність роботи та збереження критично важливих даних.

Завдання дослідження полягають у підвищенні стійкості корпоративних інформаційних систем від комплексних кіберзагроз. У першу чергу, потрібно дослідити наявний стан цієї проблеми. Далі потрібно провести аналіз та класифікувати кіберзагрози, а також чітко визначити слабкі сторони наявних підходів до побудови систем захисту. Після цих дій, потрібно на основі цього аналізу розробити формальні моделі загроз та сценаріїв атак. І як заключення етапу, потрібно побудувати модель функціонування корпоративних систем в умовах

деструктивних впливів. Наступним етапом є створення алгоритму оцінювання ефективності захисту з використанням математичного апарату марківських ланцюгів для визначення ймовірності перебування системи у захищеному стані. Важливим завданням також є обґрунтування архітектури адаптивного захисту. У завданні важливу увагу потрібно приділити розробці алгоритму оцінки ризику для динамічного визначення оцінки ризику щодо інциденту та алгоритму адаптивного часу блокування для оптимізації часової конфігурацію захисту. Важливо також описати структуру програмного забезпечення системи адаптивного захисту, механізми інтеграції та сценарії автоматизованого їх реагування.

Предметом дослідження є методи адаптивного захисту, математичні моделі оцінювання кіберстійкості, моделі та методи забезпечення стійкості корпоративних інформаційних систем, алгоритми системи захисту та конкретно алгоритми адаптивного управління конфігурацією захисту, а також засоби автоматизованого реагування на інциденти пов’язані з протидією комплексним кіберзагрозам.

Об’єктом дослідження є процес функціонування та захисту корпоративних інформаційних систем в умовах впливу деструктивних комплексних кіберзагроз.

Методів дослідження використовує достатньо, і вони є досить різноманітними. У цій роботі застосовано комплексний науковий підхід, цей поєднує кілька взаємопов’язаних методів. У першу чергу, є метод системного аналізу. Він дозволить дослідити структурно-функціональну організацію корпоративних інформаційних систем, класифікувати основні вектори атак та визначити головні вимоги щодо побудови ефективної системи захисту. Для моделювання поведінки системи у різних станах доцільним є використання теорії ймовірностей та випадкових процесів (особливо, марківські моделі), щоб дати змогу оцінити ефективність запропонованих механізмів захисту. Також тут доцільно використовувати теорію алгоритмів та прийняття рішень, щоб можна було розробити чи покращити різноманітні алгоритми, що будуть забезпечувати гнучке реагування на інциденти. І остім методом є використання методів візуального моделювання та алгоритмізації процесів. Це потрібно для

проєктування та реалізації сценаріїв адаптивного захисту. Такий комплексний підхід забезпечує надійне виконання дослідження.

Наукова новизна у цій роботі є значною. Першим елементом новизни є пропонування використання організацію системи адаптивного захисту КІС, що базується на чіткому розподілі на чотири взаємодіючі рівні (сенсори, аналіз, оркестрація, виконання). Такий поділ забезпечить ефективну, гнучку та масштабовану архітектуру. Наступним елементом новизни є розроблення комплексу алгоритмів адаптивного управління безпекою. Такими є алгоритм RiskScore для динамічного визначення пріоритету інциденту та алгоритм для адаптації часу ізоляції пропорційно певному рівню ризику. І саме спільне їх застосування дозволяє ефективніше здійснювати баланс між надійністю блокування загроз і збереженням доступності потрібних сервісів. Та іншою чпстиною новизни є удосконалена модель кіберзахисту на основі марківських ланцюгів. Модель дасть змогу кількісно оцінити, як відповідна швидкість автоматизованої оркестрації впливає на ймовірність збереження працездатності цієї системи.

Практична цінність полягає в запропонованій архітектурі SOAR, щоб максимально покращити захист за допомогою головної деталі цієї системи – оркестрації. Важливою цінністю є також розроблення та формалізування алгоритму адаптивного часу блокування та алгоритму оцінки ризику, що покращює наявні процеси. Іще є чітко сформовані рекомендацій щодо інтеграції засобів EDR, UEBA, SIEM та TIP. Ці отримані результати роботи можна використати адміністраторам безпеки та SOC-аналітикам, щоб модернізувати наявні системи захисту.

Основні теоретичні положення та практичні результати дослідження є викладені у двох наукових працях, з яких одна стаття у фаховому журналі та інша це тези доповіді на науково-практичній конференції.

1 ТЕОРЕТИЧНІ ОСНОВИ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

1.1 Поняття стійкості ІС та критерії її оцінювання

Поняття стійкості корпоративної інформаційної системи є здатністю системи залишатися функціональною та доступною, продовжувати працювати без збоїв, навіть якщо відбуваються атаки та інші передбачувані й непередбачувані події. Тобто, попри несприятливі зовнішні чи внутрішні впливи, стійкість корпоративної ІС дозволяє системі забезпечувати безперервність бізнес-процесів. І це є дуже важливим тому, що її порушення може призвести до катастрофічних наслідків для компанії.

Цими наслідками можуть бути фінансові втрати, втрата репутації та довіри, порушення операційної діяльності, втрата даних та юридичні ризики [1, 2].

Критерії оцінювання стійкості для цих систем є дуже важливими для забезпечення стійкості корпоративної інформаційної системи. Вони дозволяють компаніям не просто реагувати на збої, а активно запобігати їм і планувати ефективне відновлення. Що в свою чергу дозволяє планувати безперервність бізнесу, ефективно інвестувати та підвищувати рівень конкурентоздатності.

Оцінювання стійкості корпоративної ІС відбувається за кількома ключовими критеріями, що дозволяють визначити її слабкі місця та потенціал для відновлення. До цих критеріїв належить безвідмовність, надійність, відновлюваність, масштабованість, безпека, гнучкість. Безвідмовність визначає, наскільки система доступна для використання та вимірюється, як правило, у відсотках часу, протягом якого система працює без збоїв. Надійність стосується здатності системи виконувати свої функції стабільно та без помилок протягом певного періоду часу. Відновлюваністю це є швидкість і ефективність, з якою система може повернутися до нормального стану після збою. Масштабованість це здатність системи ефективно адаптуватися до зростання навантаження, наприклад, збільшення кількості користувачів або обсягу даних, не втрачаючи при цьому своєї продуктивності та стабільності. Безпекою є рівень захищеності від

несанкціонованого доступу, кібератак, вірусів та інших загроз. Цей критерій є основою стійкості, бо запобігає збоям, спричиненим зловмисниками. Гнучкість є можливістю системи адаптуватися до змін, гнучка система легше інтегрується з новими інструментами та оновлюється без значних перерв [3, 4]. Усі ці критерії зображені на рисунку 1.1.

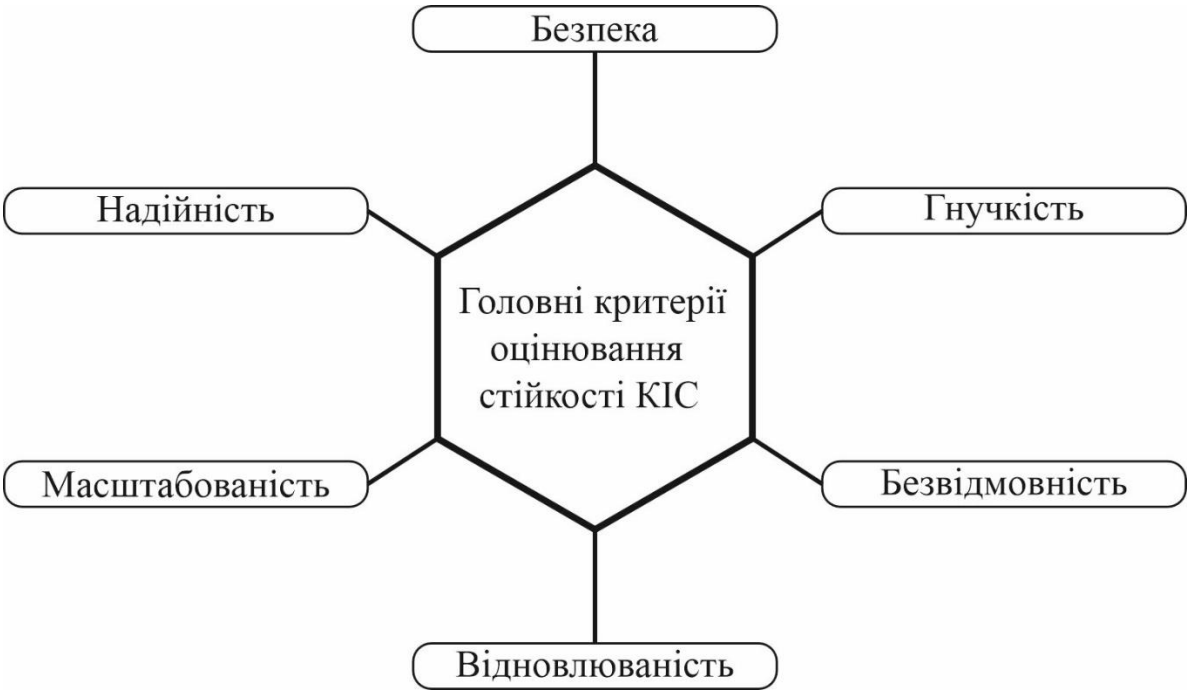


Рисунок 1.1 – Головні критерії оцінювання стійкості КІС

Ці критерії не існують окремо, а вони тісно взаємопов'язані та формують єдину систему. Оцінювання стійкості, що враховує всі ці взаємозв'язки, дозволяє компаніям не просто реагувати на збої, а будувати проактивну стратегію.

Це дає можливість мінімізувати ризики, зменшити потенційні фінансові втрати та забезпечити стабільну роботу IT-інфраструктури [5].

1.2 Класифікація кібератак та комплексних загроз

Кібератакою на корпоративну інформаційну систему є навмисне вторгнення, що здійснюється проти IT-інфраструктури компанії [6]. Головною метою є завдати

шкоди бізнесу, порушити його операції, викрасти дані або отримати контроль над системою. Кібератаки на корпоративні системи є цілеспрямованими та часто мають на меті фінансову вигоду або конкурентну перевагу. Зловмисники можуть прагнути викрасти конфіденційні дані, такі як комерційна таємниця чи персональна інформація клієнтів, щоб потім їх продати чи використати для шантажу. Іншою поширеною метою є саботаж, коли атака спрямована на порушення роботи бізнес-процесів і спричинення збитків. Також зловмисники можуть використовувати системи для шпигунства, щоб отримати доступ до інтелектуальної власності конкурентів [7, 8].

Класифікація кібератак (рисунок 1.2) може бути дуже різноманітною, оскільки вони постійно еволюціонують. Однак, існує кілька основних категорій, за якими їх можна класифікувати. Тобто за методом впливу, за об'єктом атаки, за ступенем складності та організації, за типом шкідливого ПЗ, за характером впливу, за джерелом атаки.

Рисунок 1.2 – Класифікація кібератак

За методом впливу, кібератаки класифікуються на атаки на конфіденційність (метою є несанкціонований доступ до даних, наприклад, викрадення паролів, що може бути атакою «Людина посередині»), атаки на цілісність (мета це зміна або пошкодження даних, наприклад, підробка фінансових записів, що може бути атакою «Людина посередині») та атаки на доступність (метою є перешкоджання доступу до системи, наприклад, DDoS-атаки чи програми-вимагачі). За об'єктом

атаки можуть бути поділені на атаки на програмне забезпечення (наприклад, використання вразливостей в операційних системах), на обладнання (наприклад, атаки на IoT-пристрої або мікропроцесори), на користувачів (методом соціальної інженерії, наприклад, через фішинг).

За ступенем складності та організації кібератаки можна класифікувати на масові атаки, що спрямовані на велику кількість випадкових цілей і є автоматизованими, наприклад, поширення вірусів-вимагачів; і на цільові (таргетовані) атаки, які спрямовані на конкретну організацію чи особу і є частиною складніших операцій, наприклад, APT-атаки. За типом шкідливого програмного забезпечення кібератаки можна поділити на віруси, що є шкідливими ПЗ, що приєднуються до файлів і розмножуються, заражаючи інші файли на пристроях жертви; черви, це є шкідливими ПЗ, які самовідтворюються та поширюються з одного файлу чи комп’ютера на інший без додаткового втручання людини; троянські коні, це є ПЗ, які маскуються під корисні програми, але містять шкідливий функціонал; шпигунське ПЗ, що збирає інформацію про користувача без його відома; вимагачі, програми, що шифрують дані та вимагають викуп за їх розблокування; руткити, є шкідливими ПЗ, які приховують свою присутність у системі, надаючи зловмисникам прихований контроль. Кібератаки за характером впливу можна поділити на пасивні атаки,які не змінюють дані та не порушують роботу системи (їхня мета це прихований збір інформації, наприклад, перехоплення трафіку, прослуховування мережі); активні атаки, що є руйнівними та мають на меті змінити дані або порушити роботу системи. Це можуть бути DDoS-атаки, віруси-вимагачі, зміна інформації в базі даних. Вони легко виявляються, оскільки їхній вплив помітний. За джерелом атаки можна поділити на інсайдерські атаки здійснюються особою, яка має авторизований доступ до системи (наприклад, співробітником, підрядником чи партнером) та зовнішні атаки, що виконуються зловмисниками, які знаходяться за межами захищеної мережі [9, 10]. Шість основних типів кібератак зображено на рисунку 1.3.

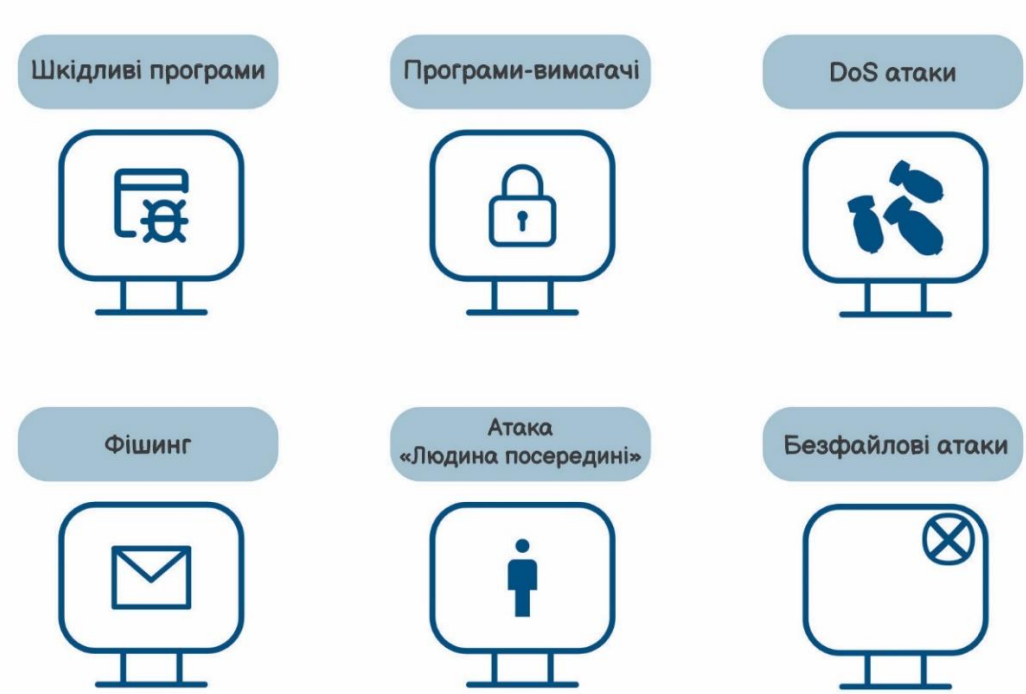


Рисунок 1.3 – Шість основних типів кібератак

Загрози для інформаційних систем можна класифікувати за кількома критеріями. За джерелом походження вони поділяються на природні (пожежі, повені і т. д.), техногенні (збої обладнання чи програмні помилки) та людські. Людські загрози можуть бути ненавмисними, тобто помилки користувачів, а також можуть бути умисними, а саме зовнішніми (хакерські атаки, фішинг), так і внутрішніми (недобросовісні співробітники). Схема поділу джерел походження загроз зображено на рисунку 1.4.

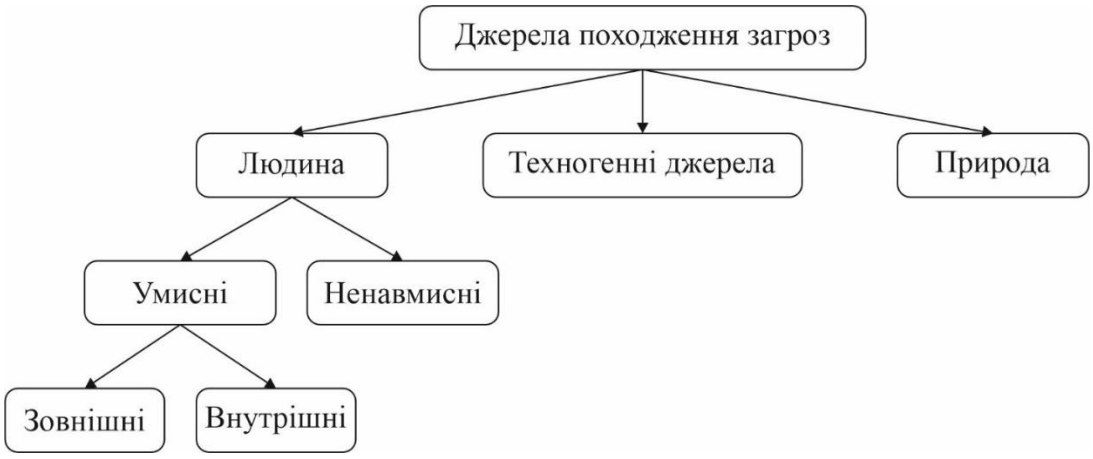


Рисунок 1.4 – Джерела походження загроз

За способом реалізації загрози поділяються на фізичні (крадіжка, пожежа), технічні (збої в апаратному забезпеченні), програмні (віруси, трояни) та організаційні (слабкі паролі, відсутність політик безпеки). І, нарешті, за наслідками для системи загрози можуть призвести до порушення конфіденційності (несанкціонований доступ до даних), порушення цілісності (зміна або знищення інформації) та порушення доступності (відмова в доступі до ресурсів) [11, 12].

Але можуть бути і складніші загрози, такими загрозами є комплексні загрози. Комплексними загрозами є не просто окремі атаки, а поєднання кількох, часто незалежних, факторів, які, взаємодіючи, створюють значно більший ризик, ніж кожен з них окремо. Такі загрози можуть призвести до системного збою, витоку даних, фінансових втрат, пошкодження репутації та навіть повного припинення діяльності компанії. Тобто, в порівнянні з окремими загрозами, комплексні є більш багатовимірні та є взаємозалежні між собою. Можна на багато елементів класифікувати комплексні загрози, але основними можна виділити це поєднання програмних і організаційних загроз, фізичних і програмних загроз, технічних і організаційних загроз. Прикладом взаємодії програмної та організаційної загрози є отримання доступу до ситеми зловмисником через недостатню обізнаність персоналу (погані паролі чи відкривання фішингово листа). Прикладом взаємодії фізичної та програмної загрози є випадок крадіжки фізичного обладнання, що перетворюється на несанкціонований доступ до конфіденційної інформації без необхідності складних кібератак. Прикладом взаємодії технічної та організаційної загрози є технічна несправність через відсутність належних організаційних процедур.

Ці всі загрози у різних випадках можуть по різному поєднуватись та по різному взаємодіяти між собою. Це не обов’язко пара загроз, це можуть бути декілька загроз, що в сукупності певним чином проявилися [13, 14, 15].

1.3 Сучасні підходи до захисту корпоративних систем (багаторівневий захист, Zero Trust, IDS/IPS і т.д.)

Для повноцінного захисту корпоративних систем потрібно розробляти цілісні підходи. Таких підходів є досить багато. Сучасні підходи до захисту корпоративних систем (рисунок 1.5) виходять за межі простого антивірусу та фаєрвола. Вони зосереджені на побудові багаторівневої, адаптивної та проактивної оборони. Ключові концепції включають багаторівневий захист, модель Zero Trust та використання систем виявлення/запобігання вторгненням (IDS/IPS), використання системи управління інформацією та подіями безпеки (SIEM), використання аналізу поведінки користувачів і об'єктів (UEBA) та використання центру управління безпекою (SOC).

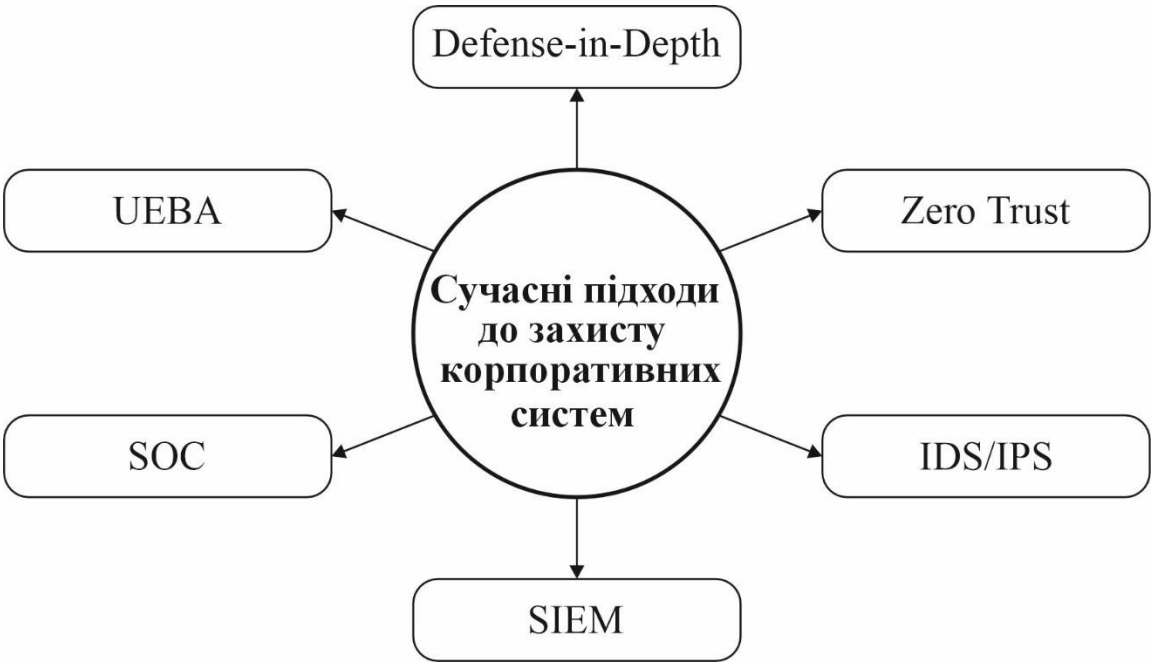


Рисунок 1.5 – Сучасні підходи до захисту корпоративних систем

Багаторівневим захистом (Defense-in-Depth) є стратегія, що передбачає використання декількох шарів захисту, щоб у разі зламу одного шару інші залишалися ефективними. Кожен шар допомагає уповільнити атаку та надає системі час для виявлення та реагування. Цими шарами можуть бути фізичний

захист (замки, охорона, відеоспостереження, обмеження доступу до серверних приміщень), мережевий захист (фаєрволи, сегментація мережі, VPN), захист хостів (антивірусне програмне забезпечення, персональні фаєрволи, системи виявлення загроз на кінцевих точках (EDR)), захист даних (шифрування даних під час зберігання та передачі) та організаційні заходи (політика безпеки, навчання персоналу, регулярні аудити) [16].

Zero Trust (Нульова довіра) це є архітектура безпеки, яка передбачає, що жодному користувачу, пристрою чи мережі не можна довіряти за замовчуванням, навіть якщо вони знаходяться всередині корпоративної мережі. Кожен запит на доступ має бути перевірений і дозволений. Головними принципами є постійна перевірка, тобто усі запити на доступ до ресурсів перевіряються, незалежно від того, звідки вони надходять (це вимагає постійної автентифікації та авторизації); обмежений доступ, тобто надавання лише мінімально необхідні права доступу для виконання конкретного завдання; мікросегментація, розділення мережі на невеликі ізольовані сегменти, щоб у разі компрометації одного сегм ента зловмисник не міг легко переміщатися по всій мережі [17].

Системи виявлення та запобігання вторгненням (IDS/IPS) є ключовими для моніторингу та захисту мережі в реальному часі. Ці системи поділяються на дві частини IDS та IPS. IDS виявляє підозрілу активність та аналізує мережевий трафік на предмет відомих шаблонів атак (сигнатурний аналіз) або аномалій. Ця система лише сповіщає адміністратора про загрозу. IPS виявляє та блокує підозрілу активність. IPS є проактивною системою, що може автоматично запобігти атаці, заблокувавши шкідливий трафік або розірвавши з'єднання. Цю систему часто розміщують між фаєрволом та внутрішньою мережею [18].

SIEM (Система управління інформацією та подіями безпеки) це програмне забезпечення, яке об'єднує функції управління інформацією про безпеку (SIM) та управління подіями безпеки (SEM). Взагальному, SIEM-системи допомагають організаціям централізовано збирати, аналізувати та корелювати дані про події безпеки з різних джерел у мережі.

UEBA (Аналіз поведінки користувачів і об'єктів) це сучасна технологія в галузі кібербезпеки, що використовує машинне навчання та алгоритми для виявлення аномалій і загроз. Тобто аналізують звичну поведінку кожного користувача і пристрою в мережі, щоб виявити, коли ця поведінка відхиляється від норми.

SOC (Центр управління безпекою) це є централізований підрозділ у компанії, який відповідає за моніторинг, аналіз та реагування на інциденти кібербезпеки. Тут команда експертів цілодобово спостерігає за мережею компанії, щоб виявити та запобігти атакам.

Це все загальні масивні підходи. Також є багато інших менших і таких самих концепцій та технологій. Такими є використання штучного інтелекту, аналіз мережевої поведінки (NBA), використання хмарної кібербезпеки, задіяння IoT (Інтернет речей) безпеки, використання Blockchain технології, застосовування різноманітних біометричних методів аутентифікації і т. д.

Отже, сучасні підходи до кібербезпеки будуються на трьох принципах: запобігати, виявляти та реагувати на загрози. Це означає, що недостатньо просто встановити захист, потрібно постійно його перевіряти. Такий підхід вимагає, щоб захист був комплексним. Це включає не тільки технічні інструменти, а й освіту працівників та постійне управління ризиками. Лише постійно оновлюючи ці методи, можна ефективно боротися з найскладнішими сучасними кіберзагрозами.

1.4 Аналіз стандартів та нормативних документів (ISO/IEC 27001, NIST CSF, ДСТУ, GDPR)

Існує декілька основних стандартів і нормативних документів. Всі вони потрібні для того, щоб створити чіткі правила та найкращі практики для захисту інформації в організації. Вони допомагають компаніям управляти кіберризиками, підвищувати довіру клієнтів і дотримуватися законодавчих вимог [19].

Серед них (рисунок 1.6) є ISO/IEC 27001, NIST CSF, ДСТУ та GDPR.

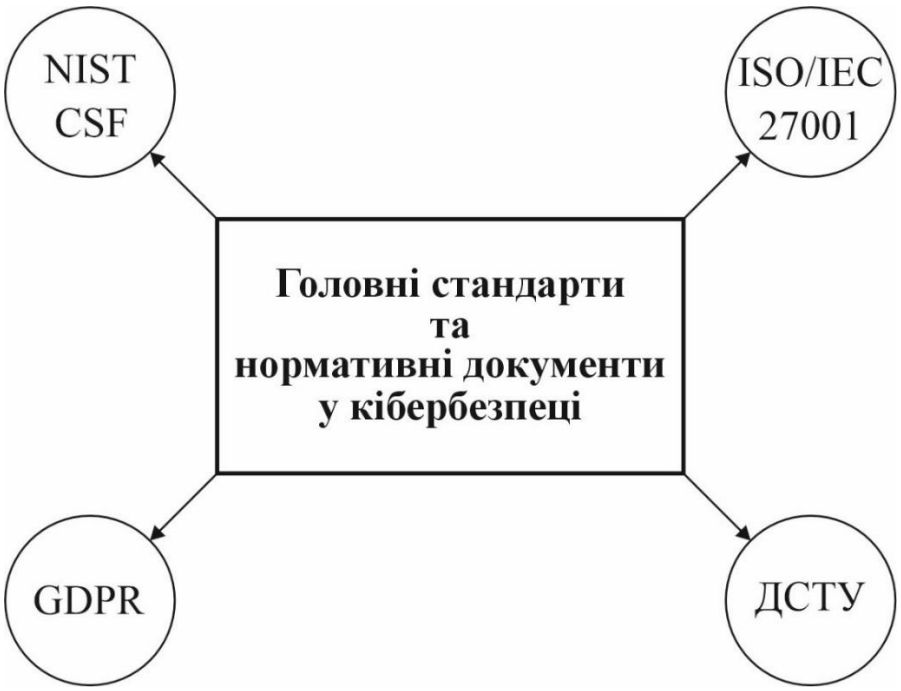


Рисунок 1.6 – Основні стандарти та нормативні документи

Стандарт ISO/IEC 27001 є головним світовим стандартом для визначення вимог до створення, впровадження, підтримки та постійного вдосконалення Системи управління інформаційною безпекою (СУІБ). Його мета є допомагати організаціям управляти та захищати свою інформацію, створюючи цілісну систему, яка не просто ставить антивірус, а охоплює всі аспекти захисту (від ризиків та контролю до навчання персоналу та постійного моніторингу) [20].

Стандарт побудований на підході, що базується на ризиках. Це означає, що спершу компанія виявляє всі можливі загрози для своєї інформації, а потім впроваджує технічні та організаційні заходи для їх контролю. Цей процес працює за принципом PDCA (Plan-Do-Check-Act), тобто Плануй-Виконуй-Перевіряй-Дій. Спочатку організація визначає свої інформаційні активи (дані, системи), аналізує ризики, пов'язані з ними, і розробляє політику безпеки. Далі йде етап «Виконуй», де впроваджуються заходи контролю та політики, що були заплановані. Потім організація проводить внутрішні аудити (етап «Перевіряй»), щоб перевірити, наскільки ефективно працює СУІБ (Системи управління інформаційною безпекою). Далі йде етап «Дій», що передбачає вживання різних заходів на основі того, що дізналися на етапі дослідження. Якщо зміна не спрацювала, проходиться

цикл ще раз з іншим планом. Після цього, якщо досягся успіх, включається те, що дізналися з тестування, у ширші зміни [21].

NIST Cybersecurity Framework (NIST CSF) є добровільним керівництвом від американського Національного інституту стандартів і технологій (The National Institute of Standards and Technology, тобто NIST), яке допомагає компаніям керувати ризиками кібербезпеки. Його основна ідея це побудувати гнучку систему захисту, яка може адаптуватися до потреб будь-якої організації. Цей фреймворк складається з п'яти ключових функцій, а саме ідентифікувати ризики, захистити, виявити загрози, відреагувати і відновити після можливого інциденту. Компанія спершу оцінює свій поточний стан безпеки, потім визначає, якого рівня вона хоче досягти, і розробляє план, як це можна зробити. NIST CSF важливий, бо надає універсальний підхід до безпеки, який зрозумілий як технічним спеціалістам, так і керівникам [22].

GDPR (General Data Protection Regulation), або українською мовою Загальний регламент про захист даних, це є не просто стандарт, а закон Європейського Союзу, який захищає особисті дані людей. Він вимагає, щоб кожна організація, яка працює з даними громадян ЄС, мала на це законну підставу. Компанії зобов'язані забезпечувати високий рівень безпеки даних і відкрито пояснювати користувачам, як їхні дані використовуються. Це все дає людям більший контроль над їхніми даними та уніфіковує правила захисту даних по всьому ЄС. За порушення цього закону передбачені дуже великі штрафи, тому його дотримання є обов'язковим для всіх, хто веде бізнес з країнами Європейського Союзу, незалежно від того, де знаходиться сама компанія [23].

ДСТУ (Державний стандарт України) є системою національних стандартів, що регулює різні сфери діяльності в Україні, зокрема й інформаційну безпеку. У сфері кібербезпеки Державні стандарти України (ДСТУ) відіграють ключову роль, особливо для державних установ і підприємств, що працюють з критичною інфраструктурою. На відміну від міжнародних стандартів, як-от ISO, які часто є добровільними, ДСТУ можуть бути обов'язковими для виконання, особливо при захисті державної інформації. Ці стандарти визначають, як правильно будувати

Комплексну систему захисту інформації (КСЗІ), визначають вимоги до систем управління інформаційною безпекою (СУІБ), надають настанови щодо засобів контролювання інформаційної безпеки, регламентують процес керування ризиками в інформаційній безпеці, а також встановлюють критерії оцінювання безпеки в ІТ. Така система поєднує в собі як технічні, наприклад, шифрування та фаєрволи, так і організаційні заходи, як-от розробка політик та навчання персоналу. Крім того, ДСТУ розробляються з урахуванням українського законодавства, що забезпечує їхню повну правову силу на території країни. А також правила адаптовані до національного контексту, навідмінно від міжнародних стандартів, хоча компанії, які працюють на міжнародному ринку, часто поєднують дотримання ДСТУ з міжнародними стандартами [24].

1.5 Постановка задачі

Отже, у першому розділі був проведений аналіз відносно сучасного стану безпеки корпоративних інформаційних систем. Цей аналіз нам дозволяє виявити ключові моменти. У світі спостерігається зростання складності та швидкості реалізації кіберзагроз. Так що такми загрозами стають загрози від багатовекторних атак і до автоматизованого шкідливого ПЗ. При цьому існуючі системи захисту залишаються недостатньо оперативними та не дуже пристосованими до динамічних умов.

Аналіз міжнародних стандартів та сучасних концепцій показує, що багато підходів до захисту КІС, але просте нарощування кількості таких інструментів без їхньої ефективної взаємодії та їх керування не вирішить сучасні проблеми щодо захисту КІС. Також система захисту має регулярно адаптовуватись під нові реалії. Тому для досягнення необхідного рівня стійкості корпоративних систем потрібено здійснити перехід від статичної моделі до адаптивної. Така модель буде здатна автоматично змінювати параметри захисту відповідно до контексту інцидентів.

Так що задачею роботи є розробка методу адаптивного захисту корпоративних інформаційних систем, що дозволятиме зробити КІС більш стійкими. До задач щодо підвищення стійкості входить мінімізувати час реакції на складні кіберзагрози, знизити ймовірність їхнього деструктивного впливу на корпоративну систему, зробити систему більш динамічною тощо.

Щоб виконати таку задачу необхідно пройти декілька взаємопов’язаних етапів. Спочатку потрібно розробити математичні моделі функціонування корпоративних систем в умовах кібератак, далі треба формалізувати процеси переходу між станами безпеки та обґрунтувати залежність ефективності захисту від швидкості реагування, використавши марківські процеси. Це дасть змогу отримати кількісні показники стійкості. Також до цих показників потрібно розглянути й інші показники стійкості. Далі потрібно створити архітектуру системи адаптивного захисту, що буде забезпечувати інтеграцію сенсорів, аналітичних модулів та виконавчих механізмів у єдину систему захисту, де буде відбуватись керування на базі технології SOAR. Наступним етапом є розробка алгоритмів, що покращуватимуть прийняття рішень. Йде мова про алгоритм оцінки ризику та алгоритм адаптивного часу блокування. І остаточно, потрібно описати систему SOAR, структуру програмного забезпечення, сценарії реагування (Playbooks) та механізмів інтеграції з системами виявлення атак.

Реалізація цих завдань дозволить створити комплексний метод, що покращить необхідну стійкість корпоративних інформаційних систем до комплексних загроз.

2 МОДЕЛІ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

2.1 Формальні моделі загроз та сценаріїв атак й засобів захисту корпоративних інформаційних систем від комплексних кіберзагроз

Формальні моделі загроз, сценаріїв атак, засобів захисту корпоративних ІС це є структуровані підходи, які допомагають компаніям систематично ідентифікувати, аналізувати та протидіяти комплексним кіберзагрозам. Вони дозволяють перетворити абстрактні ризики на конкретні, зрозумілі дії. Ці моделі є важливим елементом проактивного захисту, оскільки дають змогу не чекати атаки, а прогнозувати її можливий розвиток і заздалегідь підготувати засоби для оборони.

Моделювання загроз є процесом визначення потреб, загроз та вразливостей організації в кібербезпеці корпоративної ІС. Створені моделі надають загальний каркас для розуміння та класифікації загроз. Вони допомагають відповісти на питання "Що може статися?", що є дуже важливим для чіткого визначення та планування безпеки корпоративної інформаційної системи.

У сфері кібербезпеки існує декілька моделей загроз, що допомагають компаніям продумати та структурувати небезпеки, з якими вони можуть зіткнутися. Кожна така модель надає свій певний підхід для аналізу. Деякі моделі не просто орієнтуються тільки на моделюванні загроз, а й можуть поєднувати і моделювання загроз, і сценарії атак та засобів захисту [25].

Модель STRIDE (рисунок 2.1), назва є акронімом, що представляє шість найпоширеніших загроз (Spoofing identity, Tampering with data, Repudiation, Information disclosure, Denial of service, Elevation of privilege).

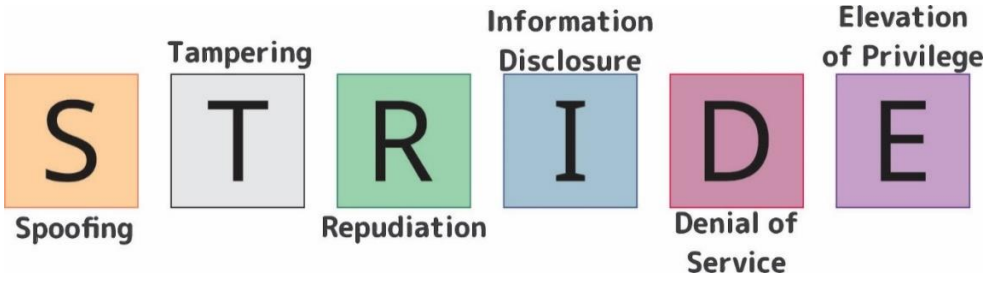


Рисунок 2.1 – Модель STRIDE

Spoofing identity (Підробка ідентифікаційної інформації) є підробкою ідентичності, тобто видаванням зловмисником себе за іншу особу чи ресурс. Tampering with data (Втручання в дані) є зміною або спотворенням інформації (наприклад, шифрування файлів або зміна файлу конфігурації). Repudiation (Відмова) є запереченням зловмисником відповідальності за атаку. Information disclosure (Розголошення інформації) є витоком конфіденційних даних та файлів. Denial of service (Відмова в обслуговуванні) є блокуванням доступу до ресурсів (наприклад, веб-сайту чи служби) для користувачів. Elevation of privilege (Підвищення привілеїв) це є отримання більших прав у системі, ніж дозволено [26].

Модель DREAD є системою оцінки та моделювання загроз, яка допомагає фахівцям з безпеки визначити пріоритетність вразливостей. На відміну від інших моделей, які фокусуються на класифікації загроз (наприклад, STRIDE), DREAD зосереджена на оцінці їхнього потенційного впливу. Тобто ця модель допомагає зрозуміти наскільки небезпечною є та чи інша загроза. DREAD (рисунок 2.2) є акронімом, кожна буква якого позначає один з п'яти факторів (Damage, Reproducibility, Exploitability, Affected users, Discoverability), що використовуються для оцінки ризику.

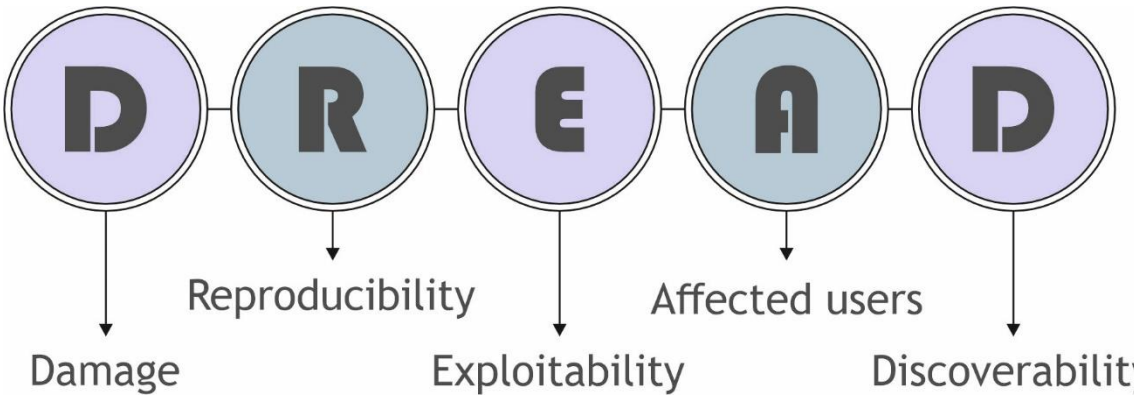


Рисунок 2.2 – Модель DREAD

Кожен фактор оцінюється за шкалою (зазвичай від 1 до 10). Першим фактором є Damage (Пошкодження), цей фактор вказує наскільки серйозною буде шкода, якщо загроза буде реалізована (втрата даних, збій системи або фінансові збитки). Другий фактор Reproducibility (Відтворюваність) вказує наскільки легко

зловмиснику відтворити атаку, тобто наскільки потрібні унікальні знання або спеціальні умови для атаки. Третій фактор Exploitability (Можливість експлуатації) вказує скільки роботи потрібно для запуску атаки. Четвертий фактор Affected users (Постраждалі користувачі) вказує на кількість користувачів, що постраждає від атаки. І п’ятий фактор Discoverability (Можливість виявлення) вказує наскільки легко виявити загрозу. Для кожної виявленої загрози фахівці з безпеки оцінюють усі п'ять факторів. Потім вони обчислюють загальну оцінку ризику, яка допомагає визначити, які вразливості потрібно виправляти в першу чергу. Наприклад, вразливість з високими показниками за всіма п'ятьма критеріями буде мати найвищий пріоритет. Модель DREAD є цінним інструментом для управління ризиками, оскільки вона надає структурований підхід до визначення пріоритетності виправлення вразливостей, що допомагає організаціям ефективно розподіляти свої ресурси безпеки [27].

Цікавою моделлю є OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) тому, що модель зосереджена на оцінці організаційних ризиків, а не технологічних. Розшифровка назки є на рисунку 2.3.

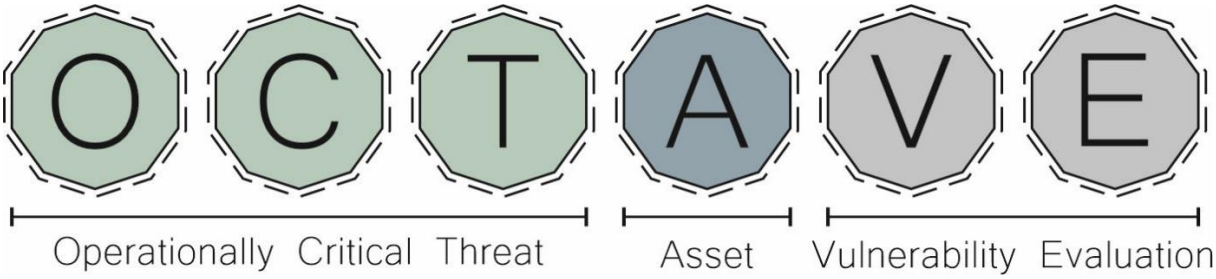


Рисунок 2.3 – Модель OCTAVE

OCTAVE використовує підхід, де за безпеку відповідають самі співробітники, тобто зазвичай команди керівництва та операцій. Але це може ускладнити масштабування, тому ця методологія орієнтована на малі та середні організації. Для малих і середніх компаній вона є особливо зручною, оскільки вона не потребує великих технічних команд. Завдяки такому підходу, OCTAVE допомагає не лише визначити, як зменшити ризики, а й підвищує обізнаність про

безпеку серед усіх команд. Вона також сприяє співпраці між різними відділами, що робить управління ризиками ефективнішим. OCTAVE є дуже гнучкою і не вимагає багато документації, що робить її легкою у використанні. Модель складається з трьох основних фаз: побудова профілю загроз, виявлення вразливостей, розробка стратегії захисту. На першій фазі команда визначає, які активи є критичними для бізнесу, та які існують загрози для них. На другій команда аналізує інфраструктуру, щоб знайти слабкі місця. Далі (на третій фазі) на основі зібраної інформації розробляється детальний план з управління ризиками та їх усуненням [28].

Також є методологія TRIKE для моделювання загроз з відкритим вихідним кодом, що використовується для аудиту безпеки та управління ризиками. Вона допомагає зрозуміти, як різні користувачі, їхні дії та IT-активи пов'язані між собою на основі наданої TRIKE електронної таблиці. На основі цих зв'язків користувачі можуть визначити, де потрібні заходи безпеки, щоб запобігти можливим загрозам. TRIKE складається з двох ключових етапів (моделювання загроз та управління ризиками) [29].

Яскравим прикладом моделі, що поєднує аналіз загроз та сценарії атак є модель PASTA, Process of Attack Simulation and Threat Analysis (Процес симуляції атак та аналізу загроз). Вона структурою моделювання загроз, що спрямована на атаки та ризики, які орієнтовані на бізнес-цілі. Вона допомагає зрозуміти, як може бути здійснена атака, що мотивує зловмисника, та які ризики це створює. Моделюючи сценарій, PASTA дозволяє визначити, які загрози є найнебезпечнішими, і зосередити ресурси на їх усуненні. Замість того, щоб захищати все, ви захищаєте те, що дійсно має значення для вашого бізнесу. Вона включає сім етапів, від визначення бізнес-мети до аналізу ризиків. Першим етапом є визначення цілей, що є найважливішими для бізнесу, і які активи потрібно захистити. Другим етапом є визначення технічного обсягу, тут створюється схема системи, що допомагає зрозуміти, з яких компонентів (кінцевих систем таких як мережі, сервери, мобільні пристрої, програми, бази даних, веб-сайтів) вона складається і як вони взаємодіють. Це візуалізація, яка показує, що саме потрібно захищати. Третім етапом є декомпозиція додатків, тут відбувається розбивання

системи на дрібні частини, щоб виявити потенційні точки вразливості та шляхи, якими зловмисник може атакувати; також тут створюються на основі попередніх зібраних даних діаграми потоку даних, що допомагають користувачам візуалізувати яким чином додатки працюють з даними для підготовки до глибшого аналізу. Четвертим етапом є аналіз загроз, де використовуються численні джерела інформації про загрози та активи для ідентифікації найбільш актуальних загроз для цих активів. П’ятим етапом є аналіз вразливостей, де проходить перевірка додатків на наявність проблем із безпекою, недоліків дизайну та інших слабких місцях в системі. Шостим етапом є аналіз атак, тут проходить моделювання атак, що імітують дії зловмисника для проникнення в систему, використовуючи вразливості. І останній етап (сьомий етап) є етапом з аналізом ризиків і впливу, де на основі всіх зібраних даних організація приймає рішення, які ризики вона готова прийняти, а які потрібно усунути, а також розробляється стратегія контрзаходів для усунення або пом’якшення проблем [30]. Етапи моделі PASTA зображено на рисунку 2.4.

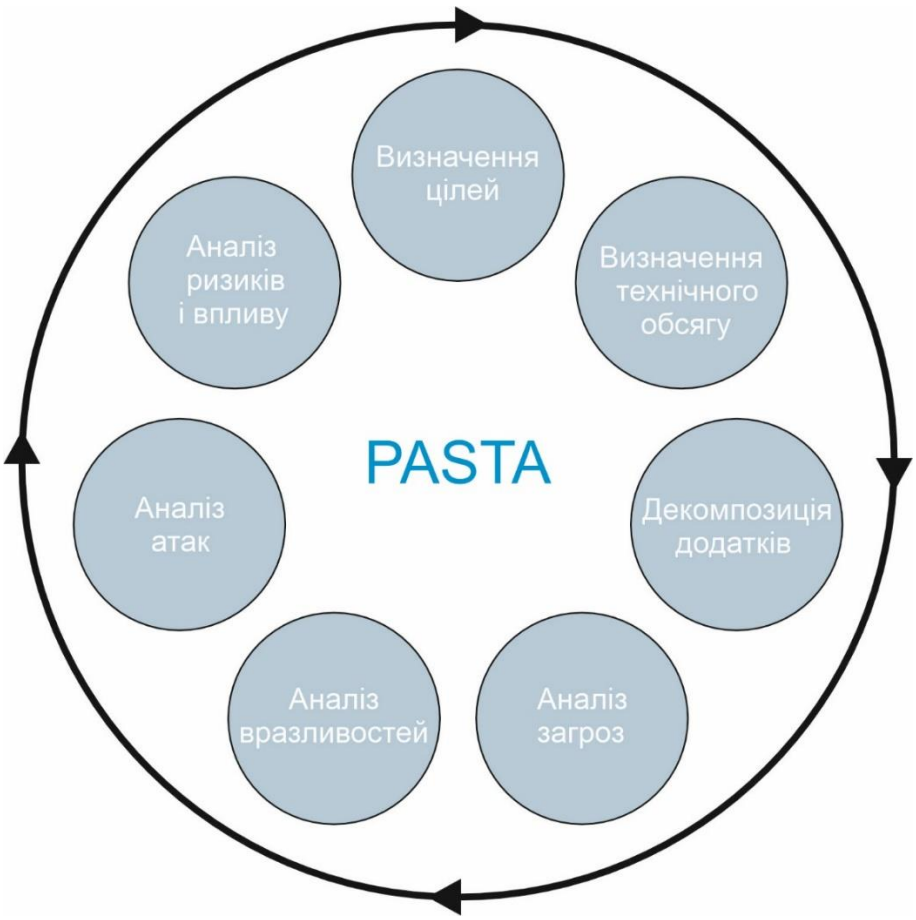


Рисунок 2.4 – Етапи моделі PASTA

Цікавою моделлю сценаріїв атак є модель Дерево атак (Attack Tree), це є візуальна модель, яка допомагає фахівцям з кібербезпеки зрозуміти, як зловмисник може досягти своєї мети. Це як діаграма, що показує можливі шляхи атаки, від кінцевої мети до найпростіших дій, забезпечуючи візуальний та організований спосіб моделювання шляхів атаки, потенційних вразливостей та їх залежностей. Дерева атак формуються за використанням ієрархічної структури та можуть бути підрозділені на менші дерева атак для представлення різних векторів атаки. У цій моделі головна мета зловмисника знаходиться в корені дерева. Щоб досягти цієї мети, існують різні шляхи, що представлені у вигляді гілок. Кожен такий шлях складається з конкретних, простих дій, що є листям дерева. Гілки можуть поєднуватися за логікою "І", що означає, що для успіху потрібні всі дії, або "АБО", коли достатньо виконати лише одну з кількох можливих. Взагальному, створення дерева атак включає шість кроків (рисунок 2.5).

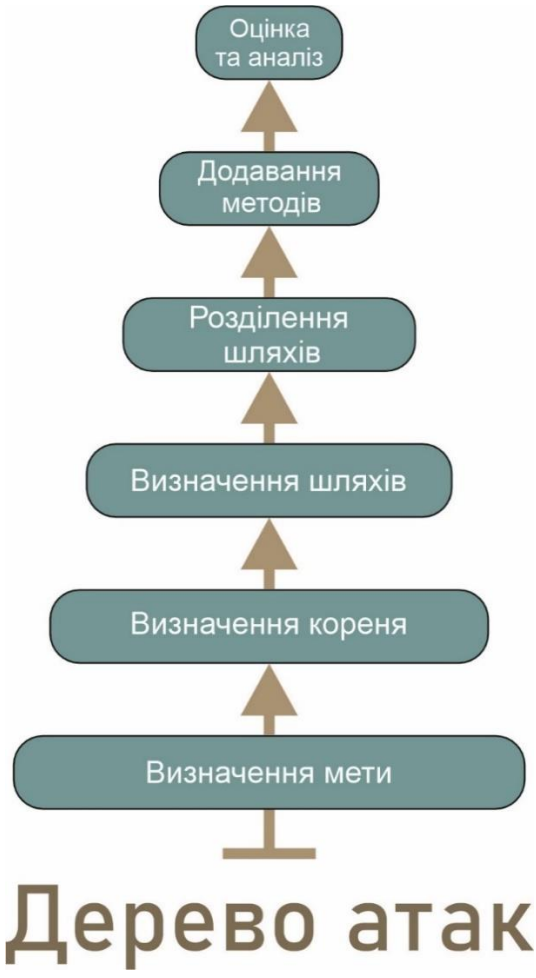


Рисунок 2.5 – Модель Дерево атак (Attack Tree)

Перший крок це є визначення мети, де потрібно спершу чітко зрозуміти, чого хоче досягти зловмисник (наприклад, отримати доступ до даних). Другим кроком є визначення кореня, тут ціль атаки стає головним, кореневим вузлом дерева. Третім кроком є визначення шляхів, на цьому кроці визначаються різні шляхи, якими хакер може досягти своєї мети. Четвертим кроком є розділення шляхів, на цьому кроці відбувається розбивається розбивання кожного шляху на менші, більш деталізовані кроки, поки не буде досягнутий найпростіший рівень. П’ятим кроком є додавання методів, де до кожного кроку додаються конкретні методи атак або вразливості, які можуть бути використані. Та шостим кроком є оцінка та аналіз, тут усі шляхи атаки аналізуються, щоб оцінити ризики, визначити пріоритети та розробити заходи захисту. Тобто таким чином, Дерево атак допомагає перетворити абстрактне поняття "атака" на чіткий, структурований план, що дозволяє ефективно будувати оборону [31].

Дуже важливою моделлю сценаріїв атак є Cyber Kill Chain (Кіберланцюг вбивства). Ця модель розбиває кібератаку на сім кроків (рисунок 2.6), що дозволяє компаніям визначити, на якому етапі можна зупинити зловмисника. Модель Cyber Kill Chain описує, які кроки потрібно виконати хакеру, щоб досягти своєї мети. Вона показує, як відбувається атака, від початкової розвідки до фінального виконання. Якщо зупинити зловмисника на будь-якому з цих етапів, ланцюг атаки буде розірвано. Це означає, що захист виявився успішним, і вторгнення зупинено. Атака вважається успішною лише тоді, коли хакер дійде до самого кінця, виконавши всі сім кроків. Отже, цими сімома кроками є Розвідка (Reconnaissance), Озброєння (Weaponization), Доставка (Delivery), Експлуатація (Exploitation), Встановлення (Installation), Командування та контроль (Command & Control, C2), Дії за ціллю (Actions on Objectives).

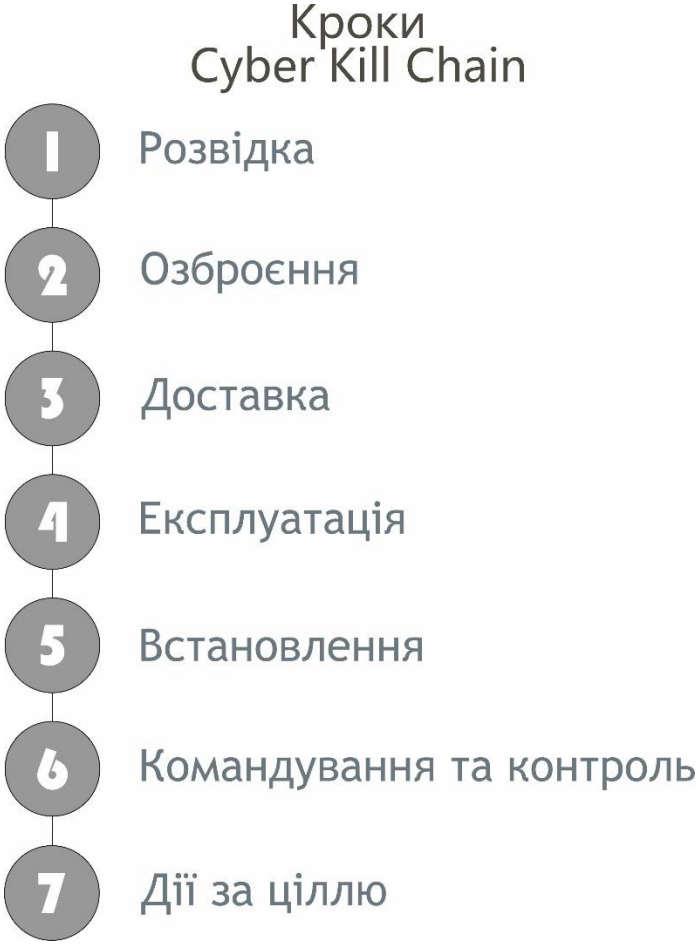


Рисунок 2.6 – Модель Cyber Kill Chain (Кіберланцюг вбивства)

На етапі розвідки зловмисник пасивно збирає інформацію про ціль, не вступаючи в пряму взаємодію з її системами. На етапі озброєння зловмисник створює інструмент для атаки. Далі на етапі доставки зловмисник передає створений інструмент до цілі. Після доставки зловмисник використовує вразливість у системі, щоб виконати шкідливий код (етап експлуатації). Далі на етапі встановлення відбувається встановлення постійних присутності в системі для довгострокового доступу. На етапі омандування та контролю хакер встановлює канал зв’язку зі своїм програмним забезпеченням. І фінальним етапом (дії за ціллю) є момент досягання зловмисником своєї кінцевої мети (викрадення даних, саботаж чи фінансова вигода) [32]. Отже, Cyber Kill Chain є ключовою моделлю для розуміння того, як відбуваються кібератаки та як від них захиститися. Попри деякі обмеження, вона добре адаптується до сучасних загроз. Завдяки інтеграції з новими

інструментами, як-от MITRE ATT&CK, компанії можуть ефективно протистояти атакам, що постійно змінюються.

MITRE ATT&CK, це є не зовсім традиційною моделлю сценарів атак, а більше базою знань, яка допомагає фахівцям з кібербезпеки створювати реалістичні сценарії атак. MITRE ATT&CK є більш деталізованою та гнучкою моделлю в порівнянні з Cyber Kill Chain (більш лінійна модель). Також MITRE ATT&CK є фреймворком. MITRE ATT&CK надає детальний, нелінійний огляд конкретних технік, які зловмисник може використати в будь-який момент атаки. Тобто ця база масивно каталогізує тактику, методи та процедури кіберзлочинців на кожному етапі життєвого циклу кібератаки (від початкового збору інформації та планування дій зловмисника до остаточного виконання атаки). Ця система складається з двох основних елементів: тактики та техніки. Тактики представляють цілі зловмисника на високому рівні, наприклад, початковий доступ, виконання, закріплення та переміщення по мережі. Техніки описують конкретні методи (наприклад, технікою для тактики "Початковий доступ" може бути "Фішинг"), які зловмисник використовує для досягнення тактичної мети. Фреймворк також включає субтехніки для більш детального опису та процедури, які є реальними прикладами того, як конкретні хакери реалізують ці техніки. MITRE ATT&CK організований у вигляді матриці. Матриця MITRE ATT&CK розділена на три основні частини, що відповідають різним сферам атак. Матриця підприємства охоплює методи атак на корпоративну інфраструктуру, включаючи операційні системи (Windows, MacOS, Linux), хмарні сервіси та контейнерні технології. Вона також містить матрицю підготовчих технік, що використовуються перед атакою. Мобільна матриця зосереджена на атаках, спрямованих на мобільні пристрої, а також на мережевих атаках, які їх використовують. Вона розділена на окремі підматриці для платформ iOS та Android. Матриця ICS (Industrial Control Systems) включає методи атак на промислові системи управління. Ці атаки спрямовані на обладнання та мережі, що використовуються для автоматизації заводів, комунальних послуг та інших критично важливих об'єктів. MITRE ATT&CK підтримує низку заходів та технологій (сортування сповіщень, виявлення загроз та

реагування; полювання на загрози; аналіз прогалин у безпеці та оцінка зрілості Центру операцій безпеки (SOC); емуляція зловмисників), які організації використовують для оптимізації своїх операцій безпеки та покращення загального стану безпеки [33, 34, 35].

Отже, є досить багато різних моделей загроз та сценаріїв атак й засобів захисту корпоративних ІС від комплексних кіберзагроз. Головне є те як їх буде застосовано, адже вони між собою зв’язані, і є багато прикладів як одна іншу вдало доповнює. Це є дуже важливим аспектом через те що загрози розвиваються, і відповідно потрібні досить гнучкі підходи для кібербезпеки.

2.2 Показники ефективності захисту корпоративних інформаційних систем від комплексних кіберзагроз

Дуже важливою є оцінка ефективності захисту корпоративних ІС. Це дозволяє чітко оцінити захист цих систем, щоб зрозуміти чи є достатніми заходи щодо захисту інформаційних систем. І якщо захист є недостатнім, то потрібно буде його покращувати. Ефективність захисту корпоративних ІС від комплексних кіберзагроз вимірюється за допомогою комбінації кількісних і якісних показників, які показують здатність системи запобігати, виявляти, реагувати та відновлюватися після інцидентів. Ці показники допомагають оцінити поточний стан кібербезпеки, виявити слабкі місця та обґрунтувати інвестиції в захист.

Якісні показники ґрунтуються на експертних оцінках і аудитах, вони допомагають оцінити готовність організації до комплексних загроз. Якісні показники не є чіткими, які можна виміряти, а є суб’єктивною оцінкою. Попри все, оцінка через якісні показники є дуже важливою частиною загальної оцінки. До якісних показників можна віднести результати пентестів (тестування на поникнення), рівень обізнаності співробітників та відповідність стандартам. Тестування на проникнення потрібне для ефективного оцінювання захисту і відбувається через імітацію реальної кібератаки. Після кібератаки можна буде

наочно побачити наскільки система стійка до атак. Рівнем обізнаності співробітників є те наскільки результативно співробітники тієї чи іншої компанії пройшли навчання з кібербезпеки (наприклад, розповідання про фішинг та як не стати жертвою цього). Цей показник є один з найважливіших тому, що при наявності добре обізнаних співробітників з кібербезпекою, компанія суттєво підвищує всю свою безпеку. А тому важливо знати ознаки фішингових атак (рисунок 2.7).

Рисунок 2.7 – Ознаки фішингових атак

Показник відповідності стандартам є також важливим, оскільки вказує на ступінь дотримання різних стандартів з кібербезпеки (наприклад, ISO 27001, NIST). Цей показник не тільки допомагає підігнати рівень безпеки під стандарти визначенні спеціалістами, а й несе репутаційний вплив на компанію, бо показує на якому рівні знаходиться компанія в плані кібербезпеки. Якісних показників є ще декілька, проте це є найголовніші з них.

Наступний тип показників є кількісні показники, ці показники є об'єктивними, і їх можна вимірювати та відстежувати. Тобто значення цих показників надають кількісний спосіб побачити, наскільки добре організація запобігає кіберзагрозам, виявляє їх та реагує на них. Такі показники кібербезпеки

різняться від кількості заблокованих спроб порушення до швидкості реагування організації на інциденти. Цих показників може бути досить багато, чим більше їх будуть використовувати, то більш багатогранно можна вирітяти захист організації. Але є декілька найголовніших показників. Першим показником є, можна сказати еталон для оцінки надійності, середній час між збоями (MTBF). Взагальному, цей показник показує середній часовий інтервал, який відбувся між двома послідовними збоями системи чи її компонента. Чим довший MTBF, тим надійніші системи. Другим показником є середній час до виявлення (MTTD). Показник вимірює середню тривалість часу, необхідну для виявлення потенційного інциденту. Цей показник є також дуже важливим, бо допомагає оцінити, наскільки ефективно і швидко системи можуть виявляти загрози. Чим коротший MTTD, тим швидше виявлення, що дозволяє оперативніше реагувати на ризики. Третім показником є середній час до підтвердження (MTTA). MTTA вимірює середню тривалість між початковим виявленням інциденту та його офіційним підтвердженням або реєстрацією. Показник є критично важливим, бо показує рівень готовності почати вирішення проблем безпеки. Четвертим показником є середній час до локалізації (MTTC). Показник відображає, наскільки швидко можна ізолювати та усунути загрозу, мінімізуючи її потенційну шкоду. MTTC є важливим, бо допомагає оцінити ефективність процедур локалізації інцидентів. П’ятим показником є середній час до вирішення (MTTR). Цей показник вимірює, наскільки швидко організація може виявити, відреагувати та повністю відновитися після інциденту. Тобто це є досить важливий показник, адже оцінює ефективність та швидкість в усуненні загроз та відновленні після них. Наступним, шостим, показником є сас на виправлення (Days to patch), що вказує на швидкість усунення вразливостей. Цей показник є одним з фундаментальних, оскільки вимірює, наскільки швидко організація реагує на виявлені вразливості. Сьомим показником є ефективність запобігання втраті даних (DLP). Цей показник оцінює здатність системи запобігати несанкціонованому доступу або витоку даних. Показник вказує кількісну оцінку ефективності DLP-системи (Data Loss Prevention) через співвідношення успішно зупинених інцидентів до загальної кількості спроб.

Восьмим показником є кількість спроб вторгнення. Цей показник показує кількість спроб зловмисників зламати мережі організації. Показник є важливим, бо дає уявлення про рівень інтересу з боку кіберзлочинців та допомагає оцінити стійкість заходів кібербезпеки [36, 37].

Отже, якісних та кількісних показників є досить багато. Згадані лише десяток з них, але це найголовніші з них, хоча ще є багато цікавих та потрібних показників.

Взагальному, щоб комплексно оцінити ефективність захисту необхідно аналізувати ці показники разом, оскільки вони доповнюють один одного, надаючи повну картину стану кібербезпеки організації.

2.3 Модель функціонування корпоративної інформаційної системи, що захищається

Модель функціонування корпоративної ІС можна дуже чітко відобразити при використанні марківських моделей. Марківські моделі (моделі Маркова) є стохастичними моделями у теорії ймовірностей. Взагальному стохастичні моделі це є моделі, що враховують випадковість з одною або більше випадкових величин. Стохастичні моделі допомагають передбачати чи пояснювати явища в моментах де результат не завжди одинаковий, навіть при схожих умовах. Головною суттю марківських моделей це є використання марківських процесів (випадкові процеси без післядії). Тобто це означає, що в деякій системі S (так буде позначатись і наша система) з дискретними станами (у нас їх буде декілька: S_1, S_2, S_3 і так далі) в будь-який моменту часу ймовірність будь-яких майбутніх станів системи залежить від її стану в теперішньому і не залежить від того як і скільки часу розвивався поточний випадковий процес (марківський процес) в минулому [38, 39].

Отже, ми будемо створювати модель функціонування нашої корпоративної ІС, використовуючи марківські моделі з урахуванням часу перебування системи в кожному стані та досягнутих прикладних ефектах.

Як вже згадано раніше, наша система позначатиметься S і матиме декілька дискретних станів. Виділимо десять станів ($S_1 – S_{10}$), які перераховані в таблиці 2.1. Відмінності цих станів полягатимуть в умовах, у яких функціонує система S в певний момент часу t. Також відбуватимуться переходи між цими станами, тобто зміна одного стану на інший. Ось цих десять станів це є повна група подій, а переходи між цими станами визначатимуться на основі характеру аналізованого процесу.

Таблиця 2.1 – Стан процесу функціонування системи

Номер стану	Умови функціонування
1	Реалізація захисних заходів для усунення виявленої загрози
2	Коректне оцінювання ситуації за відсутності загрози
3	Отримання правдивої інформації про наявність загрози
4	Отримання правдивої інформації про відсутність загрози
5	Відсутність інформації про загрози за наявності загрози
6	Відсутність інформації про загрози за відсутності загрози
7	Пропуск загрози за її наявності
8	Хибне розпізнавання загрози за її відсутності
9	Сприйняття хибної інформації як правдивої
10	Реалізація помилкових заходів захисту за відсутності загрози

Так що ми маємо різні стани системи, а переходи між ними потрібно також відобразити. Для зручного ілюстрування конкретних станів та які є переходи між ними можна використовувати граф станів. У цьому графі кружечками позначатимуться стани системи (в кружечках номер стану системи), а ось стрілками будуть позначатись можливі переходи зі стану в стан. Повністю складений граф, з відміченими станами та можливими переходами між ними, зображений на рисунку 2.8. У графі позначаються тільки безпосередні переходи, а не опосередковані переходи (переходи через інші стани). Цей граф чітко відображає модель функціонування нашої корпоративної ІС, що захищається.

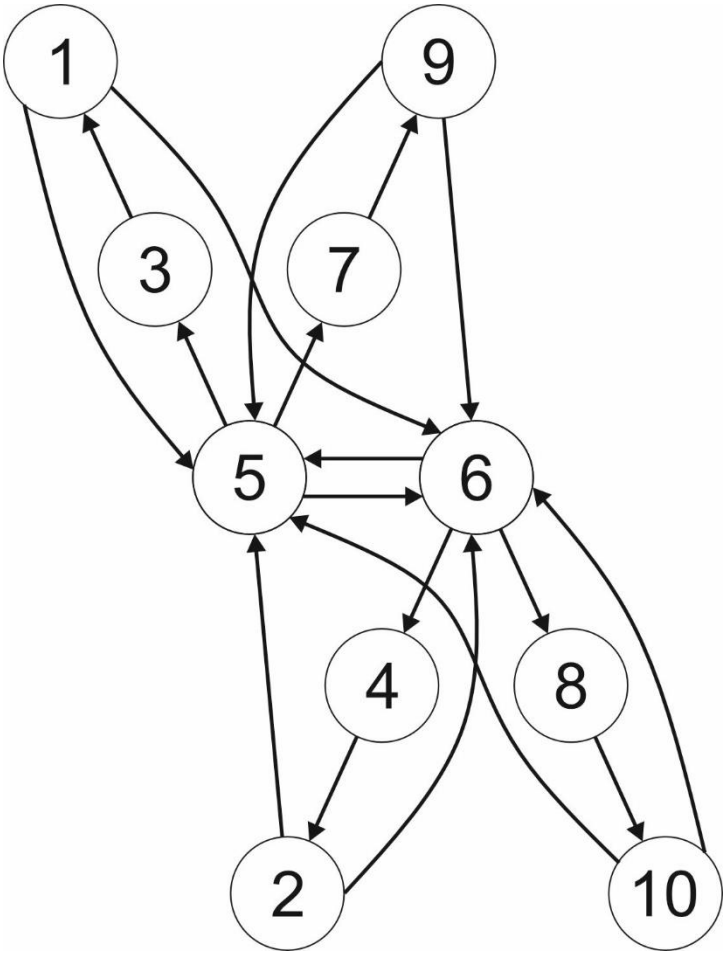


Рисунок 2.8 – Модель функціонування корпоративної інформаційної системи, що захищається

Отже, у нас є наступні переходи: $S_1 \rightarrow S_5$, $S_1 \rightarrow S_6$, $S_2 \rightarrow S_5$, $S_2 \rightarrow S_6$, $S_3 \rightarrow S_1$, $S_4 \rightarrow S_2$, $S_5 \rightarrow S_3$, $S_5 \rightarrow S_6$, $S_5 \rightarrow S_7$, $S_6 \rightarrow S_4$, $S_6 \rightarrow S_5$, $S_6 \rightarrow S_8$, $S_7 \rightarrow S_9$, $S_8 \rightarrow S_{10}$, $S_9 \rightarrow S_5$, $S_9 \rightarrow S_6$, $S_{10} \rightarrow S_5$, $S_{10} \rightarrow S_6$.

Тут переходи $S_5 \rightarrow S_6$ та $S_6 \rightarrow S_5$ можуть відбуватися у випадку посилення або послаблення активності зловмисників, переналаштування системи, зміни її контрагентів (партнери по взаємодії), а також модифікації інших умов функціонування системи. Зміна цих умов сильно впливає на процеси актуалізації та деактуалізації загроз.

2.4 Алгоритм оцінювання ефективності захисту корпоративних інформаційних систем із застосуванням марківських моделей

Для відображення алгоритму оцінювання ефективності захисту корпоративних ІС доцільно застосовувати марківські моделі, бо це зручно та ефективно, а також ми вже створити таку модель. Так що, використовуючи створену модель, потрібно визнвчити на яких основах буде будуватись алгоритм. Алгоритм буде на основі інтегрального показника. Оцінювання ефективності буде відбуватись з урахуванням часу перебування t_z в кожному стані системи S_z (z є номер стану) та які є досягнуті прикладні ефекти. Також оцінювання захищеності КІС буде не лише через інтегральний показник, але й вимірюючи зміни в роботі сервісів. Зміни в роботі сервісів можна відобразити через певні показники. Такими показниками є тривалість завантаження та ініціалізації застосунків, актуалізація даних у них; частка виконаних заявок та відмов; затримка часу у виконанні завдань користувача. Також в особливих випадках ефективність захисту КІС можна розрахувати, порівнюючи зважену суму цих показників, коли захист ввімкнений і коли він вимкнений. Взагальгому, ефективність завжди співвідноситься зі стандартними умовами роботи системи, для яких ми заздалегідь знаємо, яких бізнес-результатів (ефектів) вона має досягти.

Процесам функціонування КІС властивий потоковий характер, тому потрібно орієнтуватись на граничну теорему для сумарних потоків. Відповідно треба використати наш граф, що відображає модель функціонування корпоративної ІС, що захищається. Взявши до уваги граф, маємо побудувати систему з лінійних диференціальних рівнянь. Отже, тут буде система з 10 лінійних диференціальних рівнянь.

Оскільки, в нас система буде перебувати в певних дискретних станах, важливо відобразити ймовірності станів. Ймовірність певного z-го стану в момент t це є ймовірність того, що в момент t наша система S буде знаходитися в певному стані S_z. Ця ймовірність позначатиметься $P_z(t)$. Оцінювання показників буде у випадках без захисту та з захистом (використовуючи конкретну програму захисту

PRG_k). Ймовірність без захисту позначамитеться $P_z^*(t)$, час перебування без захисту t_z^*, а також сукупні ефекти без захисту L^*.

Отже, взявши усе до уваги, ми матимемо ці рівняння, які описуватимуть залежність ймовірностей перебування системи у відповідному стані S_z від часу та інтенсивностей переходів λ_{ij} з одних станів (i) в інші (j). Якщо ми будемо розв’язувати конкретну систему рівнянь, то це дасть нам змогу розраховувати ймовірності перебування системи в певний момент часу в можливих станах, при цьому система буде перебувати у захисті від конкретної загрози, використовуючи конкретну програму захисту PRG_k.

Якщо інтенсивності переходів та початкові умови відомі, то систему цих диференціальних рівнянь можна легко розв'язати при використанні чисельного або аналітичного метода. Розпізнавати актуальний стан системи S, щоб визначити початкові умови, можна через використання модуля аналізу ефектів системи захисту. А для кожного типу загроз і програм захисту модель буде мати свої початкові значення та параметри. Якщо будуть можливості розпізнавання актуального стану системи та відомих інтенсивностей λ_{ij}, то появу загроз можна передбачити.

Отже, на основі нашої марківської моделі при використанні інтегрального показника, алгоритм оцінювання ефективності захисту корпоративних ІС має декілька етапів. Цих етапів є п'ять [40, 41].

Перший етап включає розрахунок імовірностей $P_z^*(t)$ та $P_{zk}(PRG_k, t)$ перебування корпоративної ІС у виділених станах без застосування заходів захисту та з цими заходами на заданий момент часу. $P_{zk}(PRG_k, t)$ означає ймовірність перебування системи в стані z при реалізації захисної програми PRG_k.

Другим етапом є оцінювання t_z^* та $t_{zk}(PRG_k)$ сумарного часу перебування корпоративної інформаційної системи у станах $S_z \in \{S_1,\ldots,S_{10}\}$ у незахищеному режимі функціонування та в режимі реалізації захисної програми PRG_k відповідно (2.1):

$$t_z^* = \int_0^T P_z^*(t)dt \text{ та } t_{zk}(PRG_k) = \int_0^T P_{zk}(PRG_k,\ t)dt, \quad (2.1)$$

де T є аналізованим періодом часу.

На третьому етапі відбувається визначення ефекту стану. Тобто кожному стану z ставиться у відповідність величина ефекту V_z, що пов'язана з показниками якості обслуговування, яке надається користувачеві за певну одиницю часу.

Четвертим етапом є розрахунок сукупних ефектів. Розраховуються сукупні ефекти без заходів захисту L^* та з заходами захисту $L(PRG_k)$ за наступними формуламами (2.2):

$$L^* = \sum_{z=1}^{Z} V_z t_z^* \text{ та } L(PRG_k) = \sum_{z=1}^{Z} V_z t_{zk}(PRG_k), \quad (2.2)$$

де Z є число всіх станів нашої КІС.

Важливо зазначити, що значення ефектів V_z можуть бути як позитивними, так і негативними. Також враховуючи, що показники якості обслуговування можуть залежати від часу, то розрахунок сукупного ефекту може бути виконаний за наступними формулами (2.3) і (2.4):

$$L^* = \sum_{z=1}^{Z} L_z^* \text{ та } L(PRG_k) = \sum_{z=1}^{Z} L_z(PRG_k), \quad (2.3)$$

$$L_z^* = \int_0^T V_z(t)P_z^*(t)dt \text{ та } L_z(PRG_k) = \int_0^T V_z(t)P_{zk}(PRG_k,\ t)dt. \quad (2.4)$$

П'ятий етап це є розрахунок приросту ефективності ΔL. Цей приріст ефективності відбувається КІС за рахунок реалізованих заходів захисту [42] та розраховується за формулою (2.5):

$$\Delta L = L_z(PRG_k) - L_z^*. \quad (2.5)$$

Цей алгоритм можна використовувати для широкого кола КІС, які є різними за призначенням та структурними особливостями. Хоч етапів не так і багато, але кожен з етапів є досить змістовним, тому краще візуалізувати цей алгоритм для простішого візуального сприйняття. Цей алгоритм зображений на рисунку 2.9.

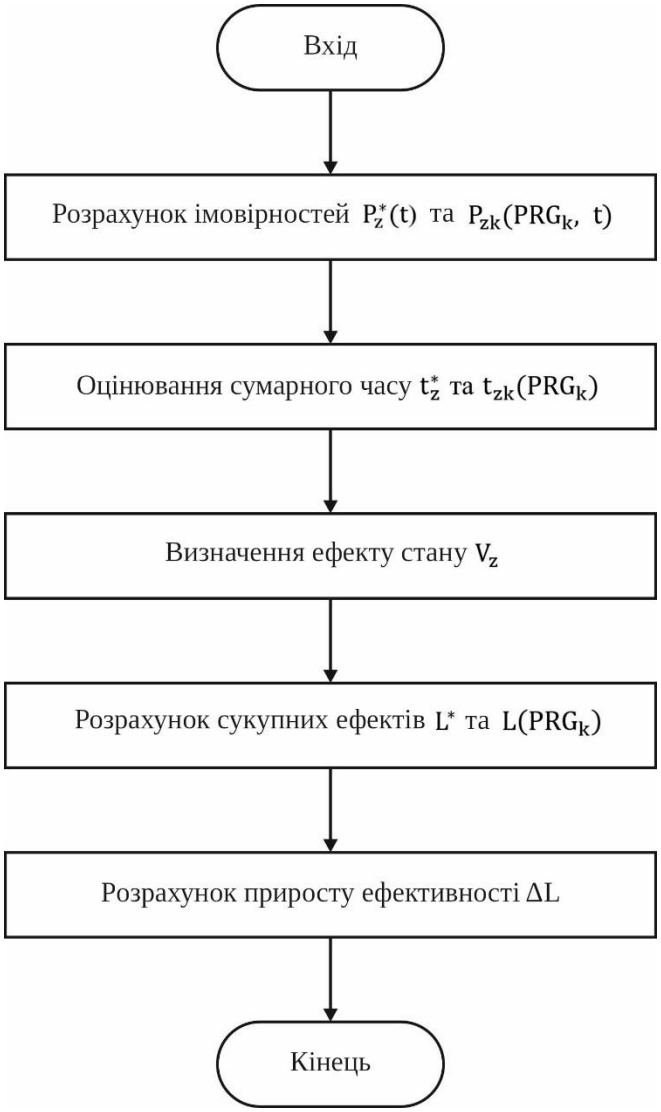


Рисунок 2.9 – Алгоритм оцінювання ефективності захисту КІС

2.5 Метод адаптивного захисту корпоративної інформаційної системи від комплексних кіберзагроз

Отже, після проведення аналізу загроз та здійснення математичного моделювання є змога побачити критичну залежність стійкості системи від часу

реакції. Також після взяття до уваги іншої отриманої інформації пропонується метод адаптивного захисту, що буде базуватися на концепції «замкнутої петлі автоматизації безпеки». Суть цього підходу буде в динамічному контурі керування, тут різноманітні параметри захисту будуть автоматично змінюватися в реальному часі у залежності від певного контексту інциденту та розрахованого рівня ризику. Такий принцип дозволяє мінімізувати час перебування системи у вразливому стані. Цей метод буде об'єднувати процеси моніторингу, аналізу, прийняття рішень та виконання контрзаходів в єдиний безперервний цикл.

Метод можна представити у вигляді сукупності етапів (2.6):

$$M = \langle S, E, R, O, A \rangle, \tag{2.6}$$

де S (Sensing) це є етап збору та нормалізації даних, E (Enrichment) є етап збагачення контекстом, R (Risk Assessment) – етап динамічної оцінки ризику, O (Orchestration) – етап вибору стратегії та оркестрації, A (Action) – етап виконання дій та адаптації.

Тобто є п’ять етапів:

1. Етап моніторингу (S) є у цьому методі основою. Його завдання є збирання розрізнених сигналів телеметрії від сенсорів (EDR, IDS, Firewall logs, SIEM, UEBA, TIP тощо). Потім вони перетворяться на стандартизовані події безпеки, придатні для автоматичної обробки. Для нормалізації даних здійснюється приведення різноформатних логів до єдиної моделі даних (JSON). Це дозволяє системі обробляти події з різних джерел за єдиними правилами, щоб були надійні вхідні дані для оркестрації та автоматичного реагування.

2. Етап збагачення (E) є важливою проміжною ланкою між виявленням аномалії та прийняттям рішень. Тут його завдання це підтвердити подію та надати їй семантичного змісту. Щоб це зробити система автоматично звертається до зовнішніх джерел загроз (TIP), внутрішніх реєстрів активів (CMDB) та служб управління ідентичностями (AD/LDAP, HR) [43]. Від вона отримує детальні атрибути індикаторів компрометації, бізнес-контекст атакованого ресурсу, ролі та

привілеї задіяного користувача тощо. У результаті цього на виході етапу ми отримуємо збагачений об’єкт інциденту,де суттєво знижується невизначеність, що дозволяє системі автоматично закривати очевидно хибні сповіщення та підвищувати пріоритет реальних інцидентів.

3. Етап динамічної оцінки ризику (R) є важливим, бо переводить систему від простого підрахунку подій до осмисленого прийняття рішень. Цей запропонований підхід працюватиме імовірнісно. Тобто система обчислює інтегральний показник рівня ризику як зважену суму кількох факторів, а це дає змогу врахувати контекст і тонко пріоритизувати інциденти. У результаті чого рішення щодо реагування стають більш ефективними.

4. Етап оркестрації та прицняття рішень (O) це є вершина щодо процесу прийняття рішення. В загальному, тут відбувається оркестрація, тобто керування. А центром координації процесів тут виступає система SOAR, вона приймає різноманітні дані та автоматично зіставляє його з набором доступних стратегій реагування та обирає відповідний Playbook [44]. SOAR синхронізує дії між усіма рівнями захисту, щоб забезпечити узгоджене, поетапне виконання, контроль результату та можливість відкату або корекції. Такий підхід гарантує швидке, скоординоване і передбачуване реагування з мінімальним впливом на бізнес-процеси.

5. Етап виконання (A) є фінальним активного циклу реагування. Тут під час рішення, що прийняті платформою SOAR, перетворюється на конкретні зміни в конфігурації інфраструктури. Етап включає параметричну адаптацію. Вона на цьому етапі забезпечує гнучкість і точність втручань. Перед процесом формування керуючих команд запускається алгоритм адаптивного часу блокування, що визначає оптимальні параметри ізоляції залежно від рівня ризику. Після цього SOAR ініціює виконання команд через API виконавчих механізмів. При цьому він синхронно застосовує дії на різних рівнях інфраструктури, щоб унеможливити обхід захисту. Дія захисту не завершується тільки виконанням певних команд, а тут також присутній механізм відновлення та зворотного зв’язку. Оновлені дані про інцидент повертаються в аналітичне ядро для навчання системи, тобто потім

результати будуть використовуватись для корекції, щоб підвищити точність майбутніх рішень. Таким чином, цей етап замикає петлю автоматизації, перетворюючи систему захисту в динамічний, самонавчальний механізм, що адаптується до змін середовища.

2.6 Висновки

У другому розділі проводились теоретичні узагальнення та математичне моделювання процесів для визначення стійкості корпоративних інформаційних систем. Був здійснений аналіз формальних моделей загроз та сценаріїв атак. Це дало змогу описати процеси, що пов’язані з можливими деструктивними впливами у вигляді чітких параметрів. Такі дії дозволяють створити основу для подільшої чіткої алгоритмізації процесів захисту, щоб дозволити системі автоматично ідентифікувати та класифікувати інциденти на основі формальних ознак. Також був аналіз системи показників ефективності. Аналіз дозволив визначити головні показники стійкості та визначити умові при яких система може бути стійкою до деструктивних впливів. Далі на основі графа станів і переходів була побудована модель функціонування корпоративної системи під впливом атак. Були виділені основні стани функціонування системи. Далі відбувся аналіз із використанням марківських моделей та диференційних рівнянь, що показав аналітичну залежність ймовірності перебування системи у безпечному стані від інтенсивності атак та швидкості реагування. Також було математично доведено, що традиційні системи з ручним управлінням не здатні забезпечити потрібну стійкість, тому шляхом до підвищення стійкості стає автоматизація процесів реагування та керування. Так що на основі отриманих результатів був сформований метод адаптивного захисту.

3 СИСТЕМА ЗАХИСТУ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ ВІД КОМПЛЕКСНИХ КІБЕРЗАГРОЗ

3.1 Архітектура системи адаптивного захисту корпоративної інформаційної системи від комплексних кіберзагроз

Архітектура цієї системи захисту не є простою. Це все через те, що тут кібербезпека потребує моделей захисту, що відносяться до адаптивної архітектури, здатної миттєво реагувати на багатовекторні загрози. Така архітектура базується на принципі багаторівневої оборони (Defense in Depth). Тут кожен компонент є частиною єдиної системи та не функціонує ізольовано. Отже, компоненти між собою по різному пов’язані. У цій моделі можна виділити чотири ключові функціональні зони: сенсори, аналіз, оркестрація та виконання. Центральним елементом, який забезпечує адаптивність і узгодженість роботи, виступає SOAR. Він в цій архітектурі захисту виконує роль інтелектуального ядра системи [45, 46, 47].

Розділення на ці зони є не фізичною чи програмною, а логічною. Тобто це можна сказати логічна архітектура (рисунок 3.1). Цей поділ забезпечує своєрідний поділ відповідальності та ефективне управління потоком даних від виявлення до реагування.

Рисунок 3.1 – Логічні зони системи захисту

Першою зоною є зона сенсорів. До цієї зони також можна віднести джерела. Зона сенсорів є розподіленою мережею інтелектуальних датчиків та джерел даних. Головним завданням, що відбуваєтьтся у цій зоні є безперервний збір сирих логів і генерація первинних сповіщень про підозрілу активність [48]. Тут збираються різноманітні дані. Ефективність усієї адаптивної системи безпосередньо залежить від якості та повноти цих даних. Тут виконується роль очей і вух системи. Ця роль забезпечує глибоку видимість ззовні та всередині корпоративної мережі. Зібрані низькорівневі логи є сировиною для подальшого аналізу в інших зонах. У контексті комплексних кіберзагроз ця зона допомагає долати сліпі зони. Також тут можна фіксувати горизонтальне переміщення зловмисників між сегментами мережі. Найбільш деталізованими сенсорами є EDR-агенти. Вони є встановленими на кожній кінцевій точці (робочих станціях та серверах). Вони моніторять активність процесів, зміни у файловій системі та реєстрі, а також мережеві з'єднання, ініційовані пристроєм. Таким чином EDR-агенти виконують роль постійного аудитора хоста [49, 50]. Саме EDR часто стає першим тригером для SOAR, оскільки здатний швидко виявляти аномалії, які можуть бути частиною атаки. Паралельно з цими використовуються різні мережеві пристрої та засоби безпеки периметру (брандмауери, IDS/IPS, WAF та VPN-шлюзи). Вони реєструють трафік, що перетинає межі мережі, фіксують спроби віддаленого доступу та автентифікації, а також надають SOAR необхідний мережевий контекст для прийняття рішень щодо блокування. Важливу роль тут також відіграють і системи ідентифікації. Вони тут забезпечують дані про користувачів та їхні права доступу. Ці системи фіксують успішні та невдалі спроби входу, зміни облікових записів і випадки блокування. Дані про ці події є критично важливими для SOAR у процесі оцінки ризику й прийняття рішень. Особливістю цієї зони є те, що дані можуть передаватись у дві сторони. З одної сторони, всі низькорівневі логи спрямовуються до SIEM для довготривалого зберігання та кореляції, а з іншої сторони, сповіщення надходять безпосередньо до SOAR. Це відбувається через механізм Webhook. Це є спеціальний HTTP-запит, що містить інформацію про інцидент і запускає відповідний Playbook SOAR. Завдяки використанню цієї особливості система може

розпочати реагування ще до того, як SIEM завершить повну кореляцію подій. Така характеристика забезпечує необхідну швидкість та ефективність захисту.

Наступною зоною є зона аналізу. Ця зона функціонує як інтелектуальний фільтр і когнітивний центр архітектури. Її головною метою є перетворення величезного потоку сирих логів, які були отримані із зони сенсорів. Ці дані перетворюються на корельовані інциденти, що стали доповненими контекстом та оцінкою ризику. Саме дії цієї зони дозволяють SOAR приймати обґрунтовані та точні рішення щодо автоматичного реагування. Завдяки цьому зменшується кількість помилкових спрацювань. Функціонально зона аналізу виконує три основні функції. Першою такою функцією є кореляція. Ця функція поєднує розрізнені події в єдиний осмислений інцидент безпеки. Наступною функцією є виявлення аномалій. Тобто ця функція забезпечує фіксування поведінкових відхилень, які не можна визначити за допомогою сигнатур. І третьою функцією є забезпечення доповнення контекстом. Ця функція забезпечує додавання до внутрішніх інцидентів зовнішнього контексту (наприклад інформацію про те, чи пов’язаний хеш файлу з відомою APT-групою). Головними компонентами цієї зони аналізу є SIEM, UEBA та TIP платформи [51]. Також тут може використовуватись і EDR. Взаємодія у зоні аналізу також є двонаправленою. Тут дані (високопріоритетні інциденти з SIEM або аномалії з UEBA) надсилаються до SOAR як тригери для запуску Playbook. У свою чергу, SOAR використовує спеціальні додатки (Apps) для формування API-запитів до TIP і отримання контекстних звітів. Ці звіти інтегруються безпосередньо в логіку реагування. Завдяки цьому різні рішення спираються на внутрішній аналіз та зовнішній контекст. Це робить систему максимально ефективною та адаптивною.

Третьою зоною є зона оркестрації. Зона оркестрації є центральним ядром усієї системи адаптивного захисту. Основна функція цієї зони полягає у прийнятті рішень, координації та автоматизації. Саме тут реалізується принцип адаптивності, бо саме тут SOAR перетворює розрізнені сповіщення від зони сенсорів та зони аналізу на узгоджені дії, що будуть виконуватись у наступній зоні (зоні виконання). У цій архітектурі SOAR виступає як площина керування. SOAR тут забезпечує

централізовану координацію та інтеграцію різних систем через єдиний інтерфейс [52]. Він виконує заздалегідь визначені алгоритми реагування у вигляді Playbook. Це дозволяє діяти без участі людини та забезпечує високу швидкість реакції. Рішення SOAR не є простими. Бо SOAR приймає рішення не лише на основі факту загрози, він враховує контекст та ризиковий бал, що був отриманий від UEBA чи TIP. Така особливість робить реагування більш точним та адаптивним. Взаємодія SOAR з іншими зонами є багатовекторною та формує динамічний цикл адаптації. Система постійно очікує на вхідні сповіщення. Ці сповіщення найчастіше надходять у формі Webhooks від EDR або API-повідомлень від SIEM чи UEBA. Наприклад, після отримання такого тригера (це може бути повідомлення про високий ризиковий бал користувача), автоматично запускається відповідний Playbook. Після цього SOAR переходить до етапу збагачення контекстом. На цьому етапі використовуються системи TIP для перевірки індикаторів компрометації, а також відбуваються запити додаткових даних у SIEM. Завдяки цьому початкове сповіщення перетворюється на підтверджений інцидент. Внутрішня логіка Playbook визначає подальший шлях реагування. Завдяки використанню Playbook систему можна адаптувати під конкретні потреби. Отже, завдяки таким характеристикам зона оркестрації забезпечує швидкість, автоматизованість та максимальну точність дій. Це гарантує узгодженість роботи всієї архітектури та робить захист ефективним навіть проти складних і багатовекторних загроз.

І четвертою зоною є зона виконання. Ця зона є останнім рівнем архітектури адаптивного захисту. Зона виконання не виявляє загрози і не приймає рішень. Натомість її єдиною метою є миттєве і точне виконання будь-яких команд, які вона отримує від зони оркестрування. Саме в цій зоні відбуваються фактичні зміни в конфігурації корпоративної системи. Ці зміни спрямовані на обмеження або повне усунення загрози. Її компоненти діють як механізми виконання, які перетворюють рішення і логіку SOAR на фактичні дії. Ця зона забезпечує миттєву реакцію, бо автоматизовані команди SOAR працюють лічені секунди. Таким чином система виконує роль захисного бар’єра, який блокує дії зловмисника та не дозволяє йому довести атаку до завершальної стадії. Також тут на основі сформованих даних від

TIP, UEBA і т. д. відбувається виконання політик. Вона впроваджує ці політики на всіх рівнях. Головними виконавчими механізмами цієї зони є API ситеми EDR, різні мережеві інструменти та системи ідентифікації. У цій зоні EDR є виконавцем, у першій зоні він працював як сенсор. SOAR надсилає через його API команди для ізолювання зараженого комп'ютера, завершення шкідливого процесу тощо. Мережевими засобами тут є Firewall, NAC, IPS тощо. У цій зоні ці засоби дозволяють керувати трафіком і доступом. Також вони забороняють мережевий доступ певним пристроям, створюють нові правила блокування, оновлюють списки індикаторів і так далі. У зоні виконання також використовуються ідентифікаційні системи (Active Directory та SSO). Вони забезпечують контроль над обліковими записами. Наприклад, якщо UEBA повідомляє про високий ризик компрометації, то SOAR може примусово скинути пароль або заблокувати обліковий запис. Взаємодія у цій зоні є односпрямованою та суворо йде за протоколом. До прикладу, спочатку здійснюється виконання логіки Playbook SOAR, далі SOAR формує API-запит до конкретного механізму, потім цей механізм реалізує певну команду (наприклад, додає правило блокування чи ізолює хост). Цей механізм надсилає назад статус виконання. Завершення цього процесу фіксується у звіті інциденту. Цей звіт SOAR зазвичай передає до SIEM для аудиту, тим самим відбувається замикання циклу адаптивного реагування [53].

На основі розробленого методу адаптивного захисту запропоновано структурну схему системи для протидії деструктивним впливам на корпоративну інформаційну систему (рисунок 3.2).

Основною особливістю архітектури запропонованої системи є те, що вона має оновлену структуру функціональних блоків та зв'язків між ними. Така організація системи дозволяє їй працювати більш узгоджено та ефективно. Так вона забезпечує покращене автоматичне виявлення та усування загроз.

Головним призначення системи є підтримка належного рівня стійкості КІС шляхом забезпечення високого рівня адаптивності системи до різноманітних кіберзагроз, зокрема складних мережевих атак. Це все досягається завдяки властивості адаптивності, тобто переналаштування конфігурації системи до

актуальних умов. Таке переналаштування виконується через коригування параметрів блоків системи згідно наявної ситуації та вибору відповідних методів щодо захисту.

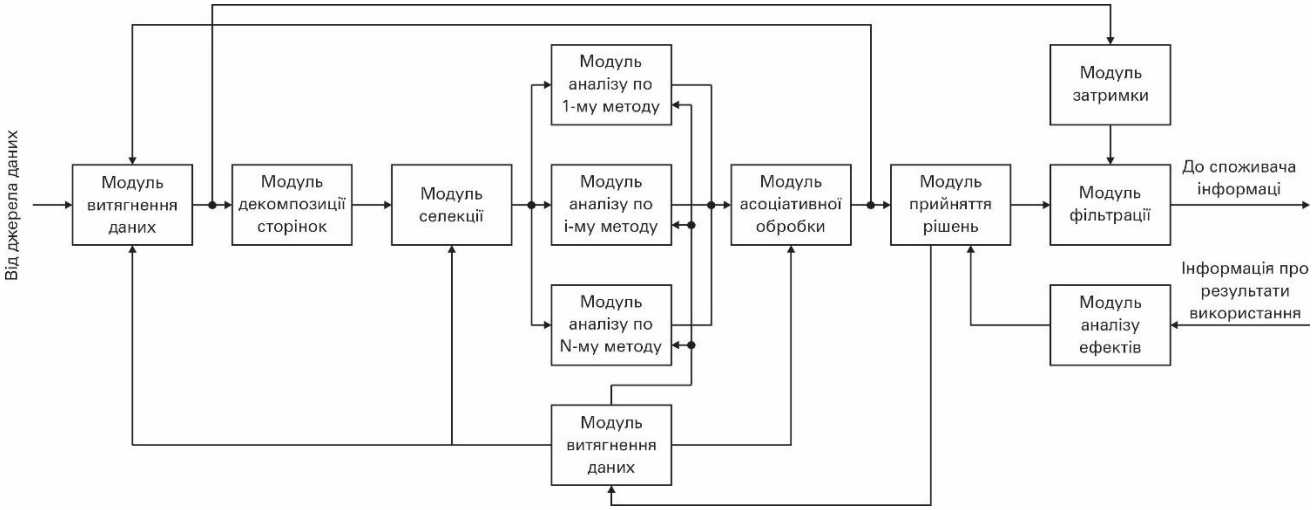


Рисунок 3.2 – Структура системи захисту КІС

У процесі адаптації через динамічну реконфігурацію обираються найбільш доречні методи протидії. У цьому процесі система захисту в реальному часі визначаються з оптимальним набором засобів захисту, а також вона налаштовує їхні параметри (наприклад, тривалість часу блокування або рівень логування). Цей вибір враховує характер активних атак, прогноз можливих загроз та поточний стан об’єкта захисту.

Так що, фактично, робота системи захисту зводиться до вирішення оптимізаційної задачі з багатьма критеріями, де її метою є знаходження найбільш ефективного способу захисту. Архітектура цієї системи надає надійний механізм для протидії комплексним кіберзагрозам. Завдяки ключовим перевагам цієї архітектури забезпечується необхідна швидкість та точність. Така архітектура перетворює розрізнені інструменти захисту на єдину, високостійку платформу. В загальному, запропонована архітектура системи повністю узгоджується з теперішніми тенденціями розвитку платформ безпеки. В таких системах безпеки фокус йде інтегровані екосистем збору та обробки даних (це є схоже до архітектури

SOAPA), щоб забезпечити ефективний збір телеметрії з великої кількості джерел для подальшої оркестрації.

3.2 Алгоритм адаптивного захисту корпоративної інформаційної системи від комплексних кіберзагроз

У системі SOAR будь-який алгоритм захисту реалізується через Playbook. Playbook не є просто певним набором автоматичних кроків, він є чіткою програмою. І ця програма описує, як система має реагувати на різні інциденти. Тобто він перетворює правила та рішення людей у інструкції для машини, що потім будуть точно визначати, що робити в тій чи іншій ситуації [54]. Тому там, де це безпечно і потрібно, це дозволяє системі діяти послідовно, передбачувано та без людської участі. Playbook у SOAR, можна сказати, відрізняється від звичайного скрипта тим, що він побудований як схема з блоків і зв’язків. Кожний блок тут це окрема дія (запуск скрипта або точка прийняття рішення), а стрілки між блоками показують, куди йдуть дані і що робити далі. Це дає змогу не виконувати все по черзі, а вибирати дії в залежності від ситуації. Система може в реальному часі перевіряти умови і спрямовувати виконання по потрібній гілці. Playbook також вміють робити вкладені перевірки і цикли. Через це є можливість у послідовному оброблені великих списків (наприклад багато підозрілих IP) і прийманні рішень з урахуванням додаткового контексту (наприклад, з рівнем критичності). Playbook з'єднує різні частини системи в один робочий процес. Playbook спочатку запускають тригери (визначають момент запуску алгоритму), це можуть бути або події від зовнішніх систем, або заплановані перевірки. Потім Playbook використовує змінні як короткочасну пам’ять, зберігає результати кроків і передає їх далі у вигляді вхідних аргументів, щоб рішення приймалися на основі актуальних даних. Playbook працює як виконуване середовище. Він приймає інцидент від тригера, крок за кроком проводить його через етапи збирання даних, збагачення контекстом та відправки команд виконавчим механізмам. Всередині Playbook є

можливість виконання скриптів або перевірок, які обчислюють різні значення (наприклад RiskScore), а потів вже за цим значення система вирішує, що робити далі. Для роботи з зовнішніми сервісами Playbook викликає додатки (Apps). По суті, додатки тут слугують модульними бібліотеками інтеграції, які ховають за собою всю складність API, тож не треба писати низькорівневі запити вручну, а достатньо буде викликати відповідний App для виконання необхідної операції [55]. І нарешті, як вже згадувалось раніше, дії це є окремі, прості операції всередині цих додатків, і саме їхня послідовність дає кінцевий результат алгоритму захисту. Формалізація алгоритмів у вигляді Playbook гарантує, що кожен інцидент обробляється однаково й передбачувано, що зменшує людські помилки та робить результати повторюваними й простішими для перевірки.

Отже, різні алгоритми можуть діяти у цій системі захисту. Є базові алгоритми роботи захисту, а є алгоритми, що можна створювати під конкретні потреби. Алгоритми, які можна створювати відповідно до різних потреб компанії, вимагають чіткого аналізу різних аспектів компанії. А ми розглянемо алгоритми, що по суті є базовими. Це не алгоритми в широкому значенні (наприклад, напрямок потоку тої чи іншої інформації з SIEM чи в SIEM). Це будуть алгоритми точкові, але вони також мають велике значення для всієї системи. Ці два алгоритми покращують наявні налаштування для реакції системи.

Спочатку потрібно розібрати передумови цих алгоритмів.

Традиційні системи безпеки часто генерують тисячі сповіщень щодня, через що аналітики перевантажені й важко стає важко відрізняти важливе від другорядного. Проблема тут не стільки в кількості повідомлень, скільки в браку контексту. Такі системи повідомляють сам факт спрацювання, але не прямо те, наскільки це є критичним. У ситуації складних атак, коли час реагування вимірюється хвилинами, потрібен механізм, який перетворює сирі сигнали на зважені рішення, тобто такий, що буде швидко оцінювати ризик і підказувати пріоритети для дій. Тому, спираючись на потреби, алгоритм (рисунок 3.3) оцінки ризику (RiskScore) покликаний вирішити цю задачу.

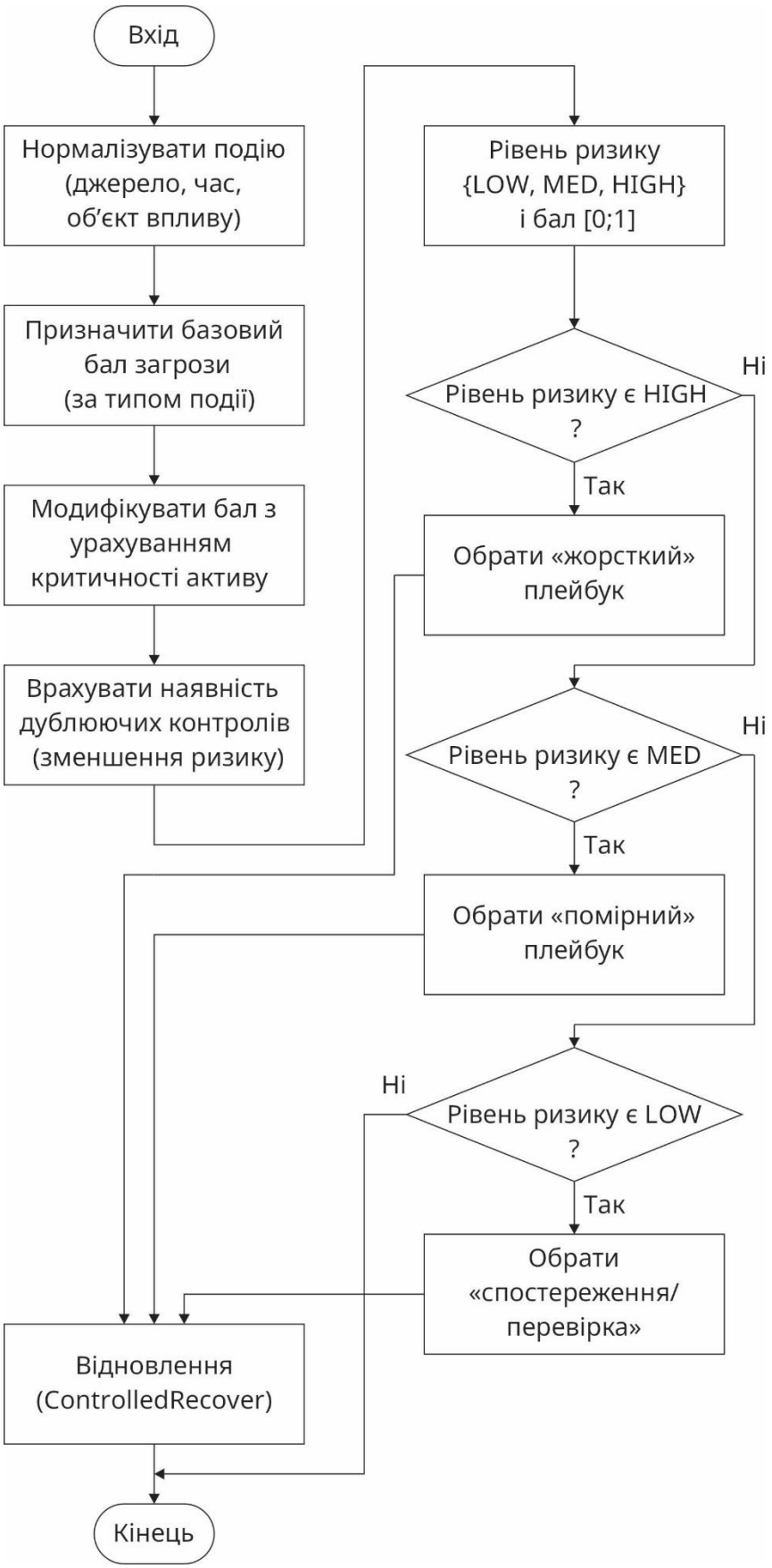


Рисунок 3.3 – Алгоритм оцінки ризику (RiskScore)

Алгоритм оцінки ризику (RiskScore) включає наступні кроки:

1. Вхід: подія/інцидент, критичність сервісу, контекст користувача.

2. Нормалізувати подію (джерело, час, об’єкт впливу).

3. Призначити базовий бал загрози (за типом події).

4. Модифікувати бал з урахуванням критичності активу.

5. Врахувати наявність дублюючих контролів (зменшення ризику).

6. Рівень ризику {LOW, MED, HIGH} і бал [0;1].

7. Вибір плейбука (PlaybookSelect)

7.1. Якщо ризик HIGH → обрати «жорсткий» плейбук (ізоляція, блокування, MFA reset).

7.2. Якщо ризик MED → обрати «помірний» плейбук (посилення політик, збір форензіки, обмеження доступу).

7.3. Якщо ризик LOW → обрати «спостереження/перевірка» (логування, сповіщення, відкладені дії).

8. Відновлення (ControlledRecover)

8.1. Перевірка цілісності конфігурацій і даних.

8.2. Відновлення з репліки/бекапу (тільки після ізоляції).

8.3. Перевірка прикладних тестів (smoke/health-check).

8.4. Повернення вузла в продуктивний сегмент.

8.5. Підтвердження бізнес-власника сервісу.

9. Кінець

Можна чітко побачити, що процес логічно поділяється на фази збору даних, адаптивної модифікації та вибору стратегії.

Виконання алгоритму ініціюється на першому кроці «Вхід». На цьому етапі SOAR отримує всю потрібну інформацію для роботи, тобто сам інцидент чи подію, яка зазвичай приходить як тригер від систем EDR, SIEM тощо. Також до інформації для роботи належить заздалегідь визначена важливість сервісу, що зв’язаний з активом, а ще сюди належить також контекст про користувача (наприклад, оцінка ризику з UEBA чи дані з Active Directory). Це дає системі необхідну інформацію для подальшої правильної роботи. Далі йде другий крок, де отримана подія має

бути нормалізована (стандартизована за такими параметрами, як джерело, час та об'єкт впливу). Це забезпечить єдність обробки, незалежно від її походження. Далі, на третьому кроці система призначає початковий (базовий) рівень загрози лише за типом події. Наприклад, якщо спрацювала сигнатура шкідливого програмного забезпечення програми-вимагача, то такий інцидент отримає значно вищий бал ризику, ніж ситуація з кількома невдалими спробами входу. Це дозволяє одразу відрізнити більш небезпечні події від менш небезпечних. Наступним є четвертий крок, де алгоритм стає розумним і враховує бізнес-контекст. Базовий бал загрози коригується залежно від того, наскільки важливий ресурс. Якщо інцидент трапляється на критичному сервері (наприклад, сервер із фінансовою базою даних), то система автоматично підвищить рівень ризику. Завдяки цьому, такий випадок отримає першочергову увагу й швидке реагування. Наступним кроком (п’ятий крок) є врахування наявності дублюючих контролів. Тут система перевіряє, чи вже є додаткові механізми захисту на об’єкті. Якщо, є вже певні дублюючі механізми захисту, то загальний рівень ризику знижується. Це допомагає оптимізувати оцінку та зменшити кількість хибних тривог. Після всіх модифікацій іде шостий крок, тут обчислюється фінальний рівень ризику, який конвертується у категорію {LOW, MED, HIGH} та фінальний бал у діапазоні [0;1]. Фінальний рівень ризику напряму визначає автоматизовану стратегію реагування. На Кроці 7 відбувається вибір плейбука (PlaybookSelect). Якщо ризик є HIGH, то SOAR обирає «жорсткий» плейбук (наприклад, ізоляція хоста, блокування мережі та примусовий скид MFA). Якщо ризик MED, система обирає «помірний» плейбук (посилення політик, збір форензіки та обмеження доступу). А для ризику LOW запускається «спостереження/перевірка» (логування та відкладені дії). Після того як загрозу успішно нейтралізували, запускається процес відновлення під контролем (крок 8, «Відновлення»). Спочатку перевіряється цілісність конфігурацій. І потім лише після повної ізоляції скомпрометованого вузла, якщо потрібно, відновлюють його з репліки або резервної копії. Далі виконуються швидкі прикладні тести (smoke/health-check). Це потрібно для перевірки, що сервіс працює коректно, потім

повертають вузол у продуктивну мережу і отримують фінальне підтвердження від власника бізнес-сервісу. Завершується алгоритм дкв’ятим кроком «Кінець».

Отже, алгоритм не просто підраховує загальну загрозу, а додає контекст, щоб система могла вибрати правильну дію замість автоматичного виконання одного шаблону. Таким чином система може перейти від простого виявлення до адаптивного вибору стратегії реагування. Він оцінює не тільки сам інцидент, а й враховує критичність активу. Також алгоритм враховує вже наявні засоби захисту. Якщо для об’єкта вже працюють певні контролі (наприклад, активний антивірус), то загальний бал знижується, що допомагає зменшити кількість помилкових спрацьовувань. Крім оцінки ризику, RiskScore автоматично підбирає відповідний плейбук (від м’якого моніторингу до жорсткіших дій). Таким чином забезпечується адаптивний підхід до реагування. У підсумку система починає діяти не за шаблоном, а розумно, фокусуючись на тому, що справді загрожує КІС.

Окрім попереднього алгоритму, у цій системі потрібно також ще один алгоритм для її покращення. Традиційні системи безпеки часто після виявлення загрози просто блокують ресурс на певний фіксований час, така характеристика часто зашкоджує. Якщо загроза виявилася несерйозною, то довге блокування може викликати зайві простої та витрати. А якщо ж атака серйозна, то фіксований час може закінчитися раніше, ніж проблему повністю ліквідують, і тоді система знову опиняється в ризику. Для вирішення подібної проблеми потрібен алгоритм адаптивного часу блокування [56]. Він буде вирішувати цю суперечність. Замість шаблонного таймера він обчислює, скільки потрібно блокувати, виходячи з контексту інциденту. Окрім загального рівня ризику, алгоритм враховує, наскільки можна довіряти сенсору, і наскільки критичний уражений сервіс, тому час блокування підбирається набагато точніше. Так що буде менше хибних тривог та менше перерв у бізнес-процесах, але й буде достатній захист там, де це потрібно. Отже, по суті головною задачою алгоритму (рисунок 3.4) буде замінити статичний час блокування (TTL) на динамічний, який буде розрахований на основі контексту інциденту та критичності активу.

Алгоритм адаптивного часу блокування включає наступні кроки:

1. Вхід: отримання рівня ризику (RiskScore).
2. Встановити межі часу для блокування (T_{min}, T_{max}).
3. Обчислити адаптивний TTL T_{block} ($T_{block} = T_{min} + (T_{max} - T_{min}) * RiskScore$).
4. Округлити та форматувати.
5. Виконати потрібні дії щодо блокування.
6. Реєстрація (аудит).
7. Кінець.

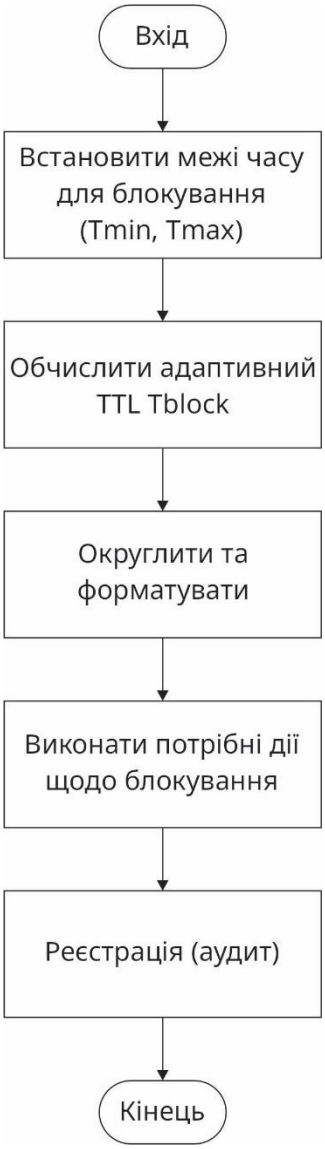


Рисунок 3.4 – Алгоритм адаптивного часу блокування

Алгоритм, по суті, реалізується як метод оптимізації, щоб реагування з пропорційністю реакції системи рівню загрози.

На першому кроці, відбувається вхід в алгоритм. Тут алгоритм отримує на вхід отримує ризиковий бал (RiskScore) та відбувається ініціалізація процесу. Бал був обчислений та нормалізований попереднім алгоритмом RiskScore. Значення RiskScore знаходиться в діапазоні [0, 1]. Далі, на другому кроці система встановлює межі часу. Тут будуть визначатися часові межі допустимого втручання. Часові межі можуть бути такими: мінімальний час буде 30 хвилин (потрібний аналітику для первинної перевірки) та максимальний час блокування буде 48 годин. Ці часи можна змінювати в залежності від бажань та потреб. Наступним кроком є розрахунок адаптивного часу (третій крок). Тут система обчислює значення за принципом лінійного масштабування. Береться мінімальний час блокування і додається до нього різницю між мінімальним часом блокування і максимальним помножену на рівень ризику. Таким чином, час блокування буде зростати разом з рівнем ризику, тобто при низькому ризику блокування час блокування буде близьким до мінімального, а при високому наближатиметься до максимального часу. Це дозволяє автоматично підлаштовувати тривалість втручання під поточний контекст інциденту. Далі, після обчислення йде четвертий крок, тут система підганяє отриманий час під технічні вимоги. Значення можуть округлюватись до зручного цілого числа і переводитись в ту одиницю, яку очікують. Це все для того, щоб блокування можна було застосувати без додаткових перетворень. Після підготовки цих даних відбувається п’ятий крок, де SOAR використовує відповідний конектор для надсилання команди блокування, передаючи обчислений динамічний час блокування. Цей процес ще супроводжується шостим кроком, де інформація про тривалість блокування та вихідний бал ризику записується в SIEM для звітності. І під кінець, алгоритм закінчується на сьомому кроці («Кінець»).

Отже, алгоритм адаптивного часу блокування ілюструє якісний перехід від простих автоматичних дій до розумної оптимізації. Впровадження динамічного часу блокування робить реакцію системи пропорційною реальній загрозі. Такий підхід ефективно вирішує проблему необґрунтованого простою через різні незначні підозри або помилкові спрацювання. Таким чином він зменшує кількість хибних спрацювань і непотрібних простоїв, але при цьому зберігається потрібний

рівень захисту для критичних сервісів і підтримання безперервності бізнес-процесів.

Загальний алгоритм адаптивного захисту КІС наведений на рисунку 3.5.

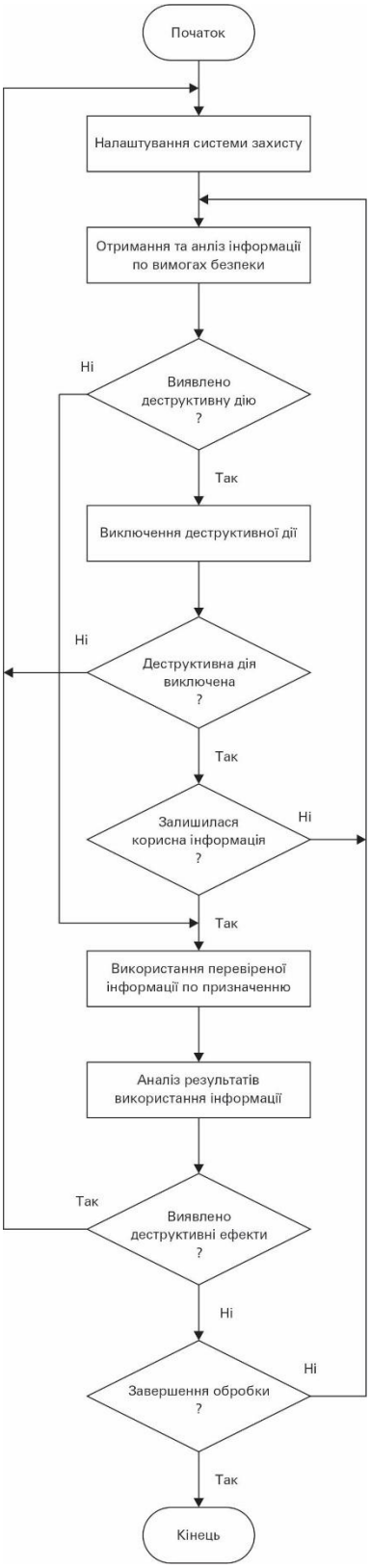


Рисунок 3.5 – Алгоритм адаптивного захисту КІС

В основі нашого запропонованого методу адаптивного захисту лежить розроблений алгоритм адаптивного реагування та метод оптимізації конфігурації, де здійснюється орієнтція на нову архітектуру корпоративної системи безпеки. Таке рішення розширює можливості систем захисту та дозволяє ефективніше виявляти й усунути деструктивні впливи.

3.3 Система захисту корпоративних інформаційних систем від комплексних кіберзагроз

Система захисту корпоративних інформаційних систем від комплексних кіберзагроз є досить складною. Це так, бо КІС мають велику кількість компонентів, і тут відбувається захист саме від комплексних кіберзагроз, а це є не поодинокі збої або віруси. Також ця система є досить складною й через динамічну природу самої загрози, а ще через необхідність забезпечити узгоджену взаємодію компонентів цієї системи захисту у реальному часі [57].

Отже, ми маємо багато різноманітних факторів, які впливають на складність реалізації захисту КІС. В основному, сучасні КІС є не просто ізольованими внутрішніми мережами, а є складними, багаторівневими екосистемами. Такі системи складаються з тисяч різноманітних компонентів, які взаємодіють один з одним у реальному часі. Саме ця різноманітність створює серйозні виклики для забезпечення цілісної та ефективної кібербезпеки. В таких системах одним із найважливіших аспектів захисту є кінцеві пристрої. До цих пристроїв відносяться різні робочі станції, ноутбуки, смартфони, планшети тощо. Проблемою тут стає їхня кількість. Вона може досягати сотень або навіть тисяч. І ці пристрої постійно переміщуються між різними мережами. Тобто, перміщуються між корпоративними, домашніми, публічними тощо. Це призводить до розмиття традиційного периметру безпеки, що робить класичні підходи до захисту недостатніми [58]. Також до загальної інфраструктури часто додаються інших видів виробничі системи та інше спеціалізоване обладнання. Ці системи часто

працюють на старих версіях програмного забезпечення та використовують нестандартні або закриті протоколи. Інтеграція їх у загальну систему безпеки вимагає особливого підходу. Це супроводжується додатковими зусиллями. До всієї цьої кількості об'єктів, які потребують захисту ще додаються й фізичні активи (файли, облікові записи, API-інтерфейси, правила брандмауерів, конфігурації систем доступу та багато іншого). Кожен з цих елементів може стати потенційною точкою атаки. Також важливим чинником є еволюція атак. Класичні методи злому все частіше змінюються. Більшість сучасних атак спираються на безфайлові атаки та концепцію, яка використовує легітимні системні інструменти (PowerShell або WMI). Це дозволяє їм обходити антивірус на основі сигнатур і залишатися невидимими для традиційних систем захисту. Атаки рідко обмежуються одним методом. Зловмисники поєднують різні тактики, методи та процедури (наприклад, фішинг для початкового доступу, експлуатацію логічної вразливості для ескалації привілеїв та використання легітимного VPN- доступу для встановлення плацдарму) [59]. Тобто тут вже традиційні, статичні засоби безпеки вже не можуть протистояти комплексним кіберзагрозам через такі обмеження. Така багатогранність вимагає, щоб рішення безпеки виявляло не ізольовані файли чи процеси, а аномальні послідовності дій, які виходять за рамки нормальної поведінки. Іншим чинником, що ускладнює безпеку є наявність великого обсягу даних. Кожен компонент корпоративної інфраструктури створює великі масиви даних. Серед цього інформаційного шуму реальна атака може виглядати як крихітна аномалія. Для її виявлення потрібні складні системи. Такими системами є SIEM, UEBA, EDR, TIP тощо. Також, варто зазначити, що сучасні системи кіберзахисту мають бути не лише розумними, але й надзвичайно швидкими. Саме ця вимога швидкодії значно підвищує складність її логіки та алгоритмів. Але попри це саме від ефективності реагування залежить стійкість усієї КІС.

Іще до усіх викликів додається те, що необхідно змусити всі різнорідні елементи захисту КІС працювати як єдиний, узгоджений і швидкий механізм. Це завдання виходить далеко за межі простого налаштування, а в реальності воно

потребує комплексної інтеграції, стандартизації та постійного вдосконалення процесів.

І найкращим рішенням для вирішення багатьох цих проблем має стати система, що зв’яже між собою різні системи захисту в єдиний інтелектуальний командний центр. Таким рішенням є система SOAR.

SOAR відноситься до концепції багаторівневої оборони (Defense in Depth), що є прямою відповіддю на неефективність статичного захисту. Тут ідея полягає в тому, що жоден засіб безпеки не є досконалим. Саме тому захист тут будується шляхом впровадження кількох незалежних та надлишкових рівнів контролю. Якщо один рівень дає збій, то наступний рівень має його зупинити. А SOAR тут вирішує проблему ізольованості, перетворюючи розрізнені інструменти (EDR, Firewall, TIP) на єдину, адаптивну систему. Саме SOAR гарантує, що якщо EDR на другому рівні виявляє загрозу, SOAR автоматично активує Firewall на першому рівні для блокування зв'язку з командним сервером, тим самим забезпечуючи узгоджену ліквідацію загрози по всій системі. Різні рівні багаторівневої оборони (інтегровані з SOAR) з інструментами та діями на цих рівнях зображені на рисунку 3.6.

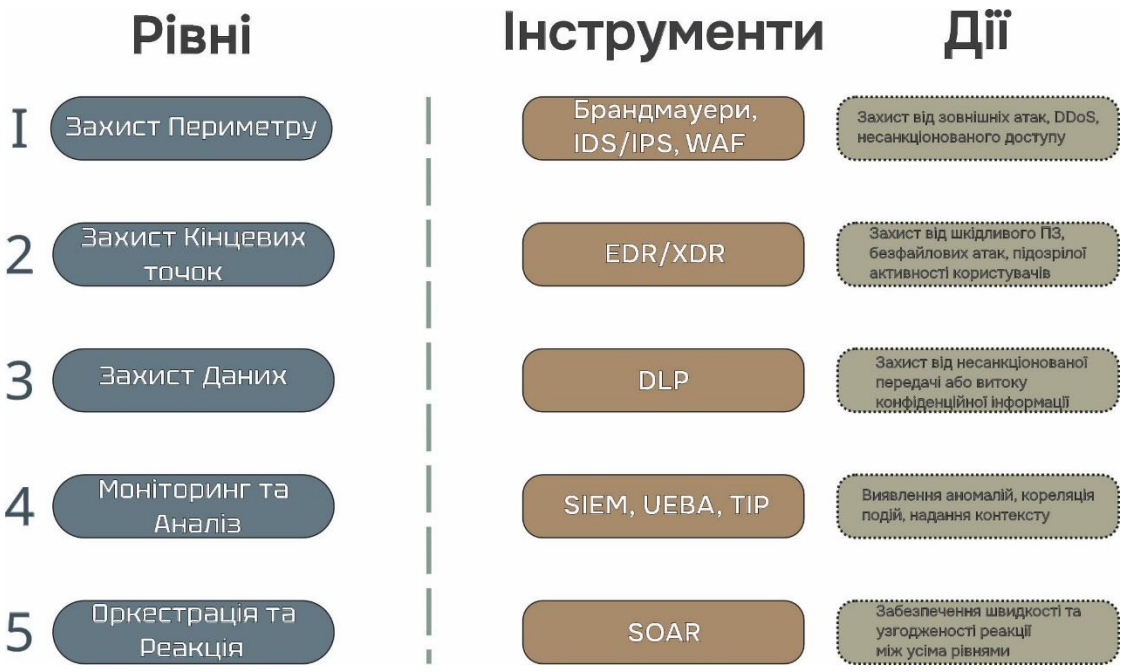


Рисунок 3.6 – Рівні багаторівневої оборони щодо нашої системи

Отже, наша система захисту КІС від комплексних кіберзагроз покладається на тип систем SOAR, бо це є єдина система, що зв’яже різні рівні захисту та дозволить забезпечити адаптивний, комплексний та автоматичний захист. Тобто ця система є центральним механізмом адаптивної системи захисту.

Суть SOAR є впроваджувати автоматизовані реакції на різноманітні події.

По суті, це є набір сумісних програм, що дозволяє організації збирати дані про кіберзагрози та реагувати на події безпеки практично без участі людини. Взагальному, ця система призначена для управління та координації операцій кібербезпеки. У контексті захисту корпоративних ІС від комплексних кіберзагроз, SOAR перетворює статичний набір засобів захисту на динамічну, адаптивну та швидку систему реагування. Систему SOAR також можна запрограмувати відповідно до потреб організації.

Функціонально система складається з трьох ключових модулів (рисунок 3.7), які є інтегровані. Це є управління загрозами та вразливостями (Оркестрація), автоматизація операцій безпеки (Автоматизація) та реагування на інциденти безпеки (Реагування). Таким чином, SOAR забезпечує систему управління загрозами від початку до кінця. Загрози виявляються, а потім впроваджується стратегія реагування. Після цього система автоматизується наскільки це можливо, щоб зробити її роботу більш ефективною.

Отже, першим модулем є оркестрація безпеки. Вона поєднує та інтегрує різоманітні внутрішні та зовнішні інструменти за допомогою вбудованих або налаштованих інтеграцій та інтерфейсів прикладного програмування. Цими елментами можуть бути сканери вразливостей, продукти захисту кінцевих точок, аналітика поведінки користувачів та об'єктів , брандмауери, системи виявлення та запобігання вторгненням (IDS/IPS), платформи керування інформацією та подіями безпеки (SIEM), програмне забезпечення для безпеки кінцевих точок, зовнішні канали інформації про загрози та інші сторонні джерела. Другим модулем є автоматизація безпеки. Обробка й аналіз даних, що були отримані під час оркестрації, а також створення повторюваних автоматизованих процедур, які існують замість ручних дій, виконують автоматизацію. Задачі, які раніше вимагали

участі аналітиків (сканування вразливостей, аналіз журналів подій, перевірка заявок, проведення аудиту), у системі SOAR вже у великій кількості можуть бути виконані автоматично. Автоматизація SOAR здатна пріоритезувати загрози, надавати рекомендації та забезпечувати автоматизоване реагування на майбутні інциденти. Це відбувається при використанні штучного інтелекту (ШІ) та алгоритмів машинного навчання для інтерпретації й адаптації даних. Також автоматизація SOAR може пріоритезувати загрози, надавати рекомендації та автоматизувати майбутні реагування. З іншого боку, автоматизація може підвищити рівень загроз, якщо потрібне втручання людини. Автоматизацію також можна також використовувати як інструмент для оркестрації. Як рішення для оркестрації, SOAR може автоматизувати завдання, які зазвичай потребують кількох інструментів безпеки. Функція автоматизації SOAR усуває ризик людської помилки. Цей елемент системи робить реагування точнішим та скорочує час, який є необхідний для усунення проблем безпеки. Третім модулем є реагування служби безпеки. Реагування на загрози пропонує аналітикам єдиний огляд на планування, управління, моніторингу та звітності про дії, що виконуються після виявлення загрози. Саме цей єдиний огляд дозволяє співпрацювати та обмінюватися інформацією про загрози між командами безпеки, мережею та системами. Він також включає заходи реагування після інциденту (управління випадками та звітність).

Рисунок 3.7 – Модулі системи захисту

Використання системи SOAR має багато різних переваг. Серед головних переваг є задоволення бюджетних потреб, покращення управління часом та ефективності, ефективніше управління інцидентами, гнучкість, покращена співпраця (рисунок 3.8).

Рисунок 3.8 – Переваги системи захисту

Першою перевагою є задоволення бюджетних потреб. Ця перевага реалізується через те, що є зростання кількості та різноманітності кіберзагроз, які створюють серйозні фінансові виклики для підприємств. І кожна нова загроза вимагає розробки окремого протоколу реагування. А це часто передбачає залучення додаткових фахівців для управління цими процесами. З появою нових типів атак організація змушена впроваджувати нові методи аналізу даних, адаптувати інструменти моніторингу та створювати механізми вирішення інцидентів. Ці дії потребують значних витрат часу, енергії та ресурсів. Однак завдяки впровадженню SOAR більшість етапів реагування можна оптимізувати та автоматизувати. Це дозволяє зменшити навантаження на команди безпеки, скоротити витрати та підвищити швидкість реагування, при цьому забезпечуючи більш ефективне управління кіберзагрозами [60]. Наступною перевагою є покращення управління часом та ефективності. Тут завдяки застосування підходу SOAR відбувається скорочення часу виконання рутинних завдань, що безпосередньо сприяє зростанню продуктивності. Це забезпечує більш ефективне використання людських ресурсів, а це вже зменшує потребу в розширенні штату або додатковому наймі. Поточна команда, що має доступ до автоматизованих інструментів, здатна досягати більшого без збільшення операційних витрат. У

результаті чого організація отримує не лише економію часу, а й оптимізацію бюджету та підвищення загальної ефективності. Наступною перевагою є ефективніше управління інцидентами. Підвищення швидкості реагування на загрози приносить підприємствам відчутну користь. Завдяки інфраструктурі SOAR організації можуть не лише оперативно реагувати на інциденти, а й здійснювати більш точне та обґрунтоване втручання. Автоматизовані механізми зменшують кількість помилок. Це, своєю чергою, скорочує час, необхідний для виправлення проблем. Зменшення людського фактору сприяє створенню більш стабільної та ефективної системи управління інцидентами, яка забезпечує надійність, економію ресурсів і безперервність бізнес-процесів. Ще одною перевагою є гнучкість. SOAR можна налаштувати відповідно до конкретних потреб організації. SOAR дозволяє змінювати його відповідно до потреб існуючої системи безпеки. Це означає, що його можна адаптувати до конфігурації без необхідності трудомісткого або ресурсомісткого перепроектування системи. SOAR може збирати дані з різних джерел, незалежно від того, чи надходять вони з ручного введення, машин чи електронної пошти. Потім можна буде вирішити, як відстежувати дані, відповідно до того, що найкраще відповідає потребам. Також є ще одна перевага, покращена співпраця. Оскільки центральна система SOAR вирішує різні типи загроз, команди, які зазвичай обробляють їх індивідуально, можуть співпрацювати над розробкою найкращих налаштувань та автоматизації SOAR. Це може призвести до більш уніфікованого набору протоколів, а також надати IT-командам можливість співпрацювати над інноваційними рішеннями.

Отже, саме через складність захисту корпоративних інформаційних систем (масштаб, різноманіття та динамічність сучасної інфраструктури), розглянута система SOAR є найкращим варіантом для автоматизації реагування на інциденти, оптимізації ресурсів і зменшенні людських помилок. Вона забезпечить швидке та чітке реагування на загрози, мінімізуючи ризики для бізнес-процесів. Завдяки інтеграції різноманітних інструментів у єдину платформу, система SOAR дозволить підвищити ефективність роботи команд безпеки. У результаті

підприємства зможуть отримати більш стійку, економічно вигідну та надійну архітектуру кіберзахисту.

3.4 Структура програмного забезпечення системи адаптивного захисту корпоративних інформаційних систем

Платформа SOAR є ядром адаптивної архітектури, вона має модульну структуру, що забезпечує гнучкість, відмовостійкість і масштабованість. Вона розроблена на основі принципу мікросервісної архітектури, в якій кожна частина є самостійним блоком. В результаті окремі частини платформи можуть розгортатися на різних фізично розділених хостах, що є критично важливою вимогою для забезпечення високої доступності у великих корпоративних середовищах [61].

Платформа складається з двох інтегрованих частин (рисунок 3.9): сервера (Server) та робочих процесів (Workers).

Сервер є хостом і керівним центром платформи у цілому, він тут виконує функцію єдиного входу користувачів та зовнішніх систем. Крім взаємодії з користувачем, він керує станом та API-активністю, а також надає хостинг фронтенду (frontend) та бекенду (backend). За допомогою портів 3001/3443 фронтенд надає графічний інтерфейс. Він дає можливість створювати, редагувати та моментально відстежувати Playbook. А бекенд тут керує основною логікою API та виконує роль реверс-проксі для внутрішніх сервісів. Сервер також контролює роботу API, перевіряє стан робочих процесів і відповідає за зберігання даних. Ця цих сервер використовує Opensearch та файлову систему для конфігураційних файлів і додатків, Opensearch забезпечує індексацію логів та метрик.

Робочі процеси (Workers) є такою силою системи, що забезпечує виконання роботи. Вони працюють як мікросервіси та напряму відповідають за виконання логіки автоматизації. Логіка є такою, що після того, як сервер отримує тригер, він здійснює передачу завдання робочим процесам (Workers), які вже виконують послідовність дій, що описані у Playbook. Мікросервісний підхід дозволяє

розганяти Workers на різних хостах та бути кластерним. Такі особливості забезпечують високу доступність та горизонтальне масштабування. Тобто якщо один Worker виходить з ладу, то інший приймає завдання на себе.

Між ядром платформи та зовнішніми системами розміщується та працює інтеграційний шар. Він забезпечує виконання інтеграційних функцій. Це середовище називається Runtime Location. Тут розміщуються та керуються Workers і Apps. Допоміжну роль у його оркестрації виконує компонент Orborus, який забезпечує життєвий цикл Workers. Runtime Location є окремим винесеним середовищем, яке є ключовим для гнучкості та масштабованості платформи. Runtime Location це є логічно відокремлене середовище всередині архітектури, яке відповідальне за хостинг і управління експлуатаційними компонентами. Найколовніше, що це включає елементи Workers, які безпосередньо виконують алгоритми автоматизації. Також сюди входять й Apps, що використовуються для інтеграції з зовнішніми системами через API. Винесення цього елемента дає цим робочим компонентам діяти автономно від основного сервера системи SOAR. Така особливість дозволяє реалізовувати додавання нових Workers і Apps для збільшення обсягу опрацювання завдань. Це називається горизонтальне масштабування. Orborus тут виконує роль локального оркестратора. Тобто цей допоміжний компонент здійснює управління життєвим циклом цього динамічного середовища. Orborus ініціює нових Workers за потреби, моніторить їхній стан і автоматично перезапускає або коректно завершує в разі збою. Він забезпечує готовність ресурсів до будь-якого призначення, що було отримане від сервера SOAR (доступ через порт 33333). Отже, тут Orborus виступає своєрідним менеджером ресурсів у зоні Runtime Location. Він буде гарантувати надійність та ефективний розподіл навантаження між виконавчими компонентами платформи [62].

Apps є критично важливим інтеграційним шаром. Завдяки ньому відбувається взаємодія SOAR з різнимии зовнішніми інструментами безпеки (SIEM, TIP тощо) та бізнес-системами. Apps отримують команди від Workers та виконують API-запити до систем таких, як SIEM, EDR, TIP, UEBA чи Email. Тобто

вони є типу конекторами до зовнішніх сервісів. Кожен App інкапсулює логіку взаємодії з API конкретного сервісу. Вони розташовані в зоні Runtime Location та є доступними через діапазон портів 33334–33399. Apps можуть забезпечувати двонаправлений зв'язок (вихідний та вхідний). Вихідний відбувається у випадках, коли Workers через Apps надсилають команди до зовнішніх сервісів, а вхідний, коли ці сервіси можуть надсилати Webhooks безпосередньо до API сервера, таким чином ініціюючи виконання робочих процесів.

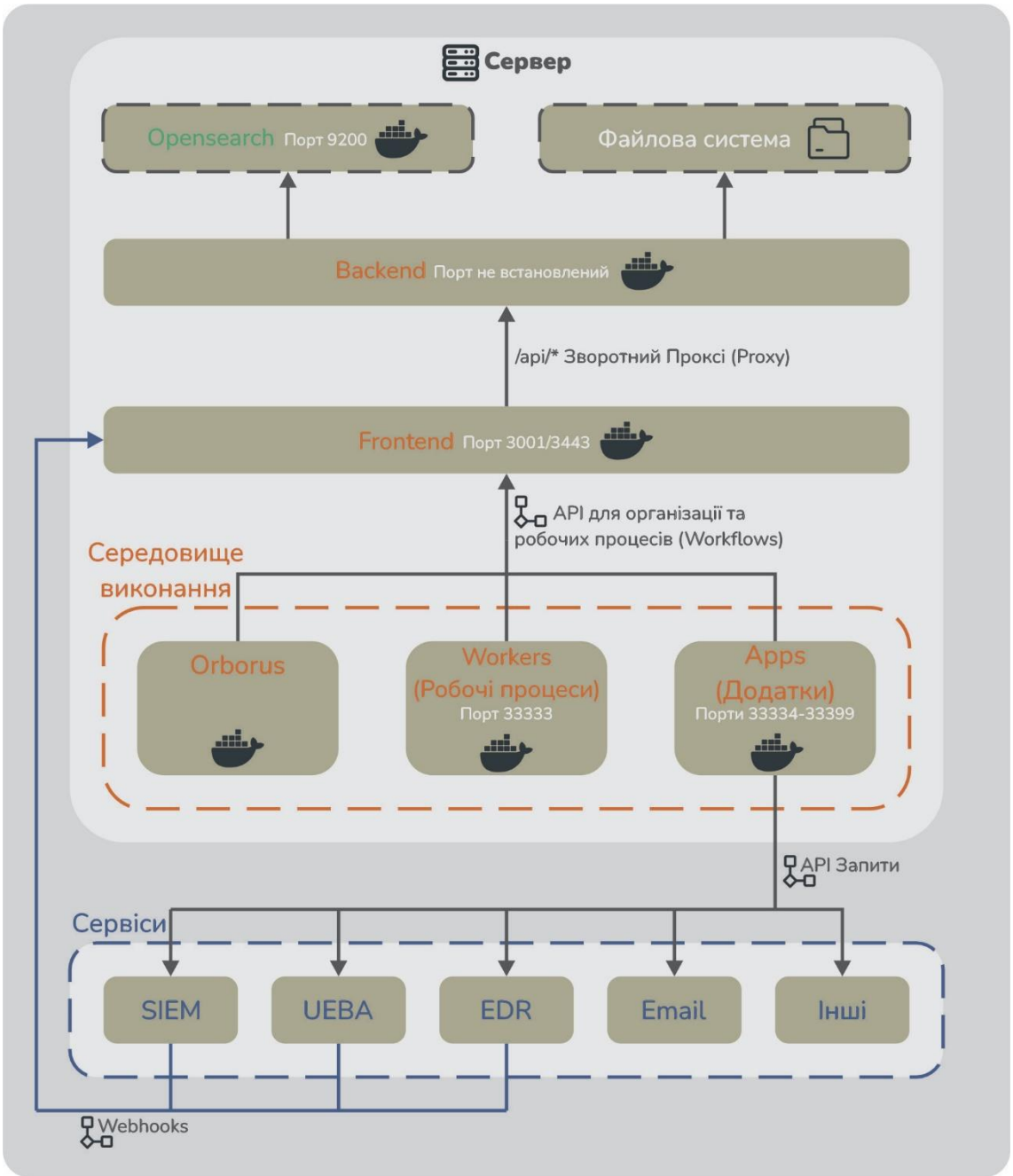


Рисунок 3.9 – Структура системи захисту КІС від комплексних кіберзагроз

Дуже важливим елементом цієї структури є Workflows (робочі процеси). Це є центральним елементом процесів, що перетворюють абстрактну логіку реагування на конкретні алгоритми. Робочі процеси є, по суті, ядром програмного забезпеченн, тут вся логіка автоматизації об’єднується та реалізується. Також можна сказати, що це та частина, де все об’єднується. Workflows є і візуальним, і програмним представленням алгоритмів адаптивного захисту. Такі алгоритми визначаючи чітку послідовність дій у відповідь на певний кіберінцидент. Кожен Workflow складається з модульних блоків (дії, аргументи та змінні), які взаємодіють між собою. Дії є командами, які виконуються додатками (Apps). Аргументи є, по суті, змінні, що потрібні для виконання конкретної дії. Вони допомагають дії працювати в потрібному контексті. Першими аргументами програми є зазвичай аргументи, що пов'язані з автентифікацією чи цільовою URL-адресою. Змінні дозволяють передавати дані між діями в межах одного робочого процесу (Workflow). Таким чином це створює гнучку логіку. Тут робочі процеси описуються у відкритому форматі JSON. Використання формату JSON для цього дозволяє легко інтегрувати Workflows у системи контролю версій. Завдяки цьому є можливість створити відкриту бібліотеку робочих процесів (Workflows), які потім можна буде зручно копіювати, змінювати та використовувати повторно [63]. Робочі процеси тут можна запускати трьома способами: автоматично через Webhook, вручну через інтерфейс або за розкладом. Найчастіше використовується Webhook. Webhook є механізмом для обробки даних у реальному часі. Webhook дозволяє зовнішнім системам миттєво повідомляти про подію, яка щойно відбулася. При цьому, він ініціює негайне виконання відповідного робочого процесу (Workflow). Це є основою для миттєвого адаптивного реагування. Webhooks приймають будь-який тип HTTP-запиту. Тут є два основні HTTP-методи для прийому Webhooks (POST і GET). Webhook для передачі даних для виконання є спеціальним POST-запитом (тригер), він надходить до системи від зовнішнього джерела (наприклад, EDR чи SIEM) та відразу активує потрібний сценарій реагування (Playbook). Дані в запиті POST будуть аргументом виконання. GET більше відноситься до передачі простих параметрів. Якщо в запиті GET присутні

HTTP-запити, то вони будуть автоматично перетворені в JSON. Webhook є найважливішим тригером для адаптивного реагування. Ручний запуск дозволяє аналітикам самостійно запускати процес безпосередньо через інтерфейс. Це є зручною властивістю для тестування, налагодження або виконання нестандартних дій. А запланований запуск використовується для регулярних завдань (наприклад, щоденний пошук загроз, створення звітів або перевірка SSL-сертифікатів). Щоб детальніше усе це розуміти, то потрібно детальніше знати про тригери в SOAR. Отже, тригерами є оператори, які використовуються для автоматичного виконання робочого процесу (Workflow). Вони пов'язані з діями всередині робочих процесів (Workflows). Тригери зазвичай використовують аргумент виконання, що потім буде використаний для виконання відповідного робочого процесу. Тригери є спеціально створені, щоб надавати користувачу доступ до кількох способів запуску робочого процесу. Тригери це є такі механізми, які дають користувачеві можливість запускати робочі процеси різними способами. Вони є своєрідними початковими вузлами та роблять так, що відбувається перетворення зовнішньої події чи внутрішнього розкладу на виконання алгоритму автоматизації. У системі є декілька основних типів тригерів: Webhook, Schedule, User Input, Subflow, Email, Rest API. Найважливішим є Webhook, і такий тип тригара був вже розглянутий. Іншим способом запуску є Schedule (розклад), він дозволяє виконувати робочі процеси за певним визначеним графіком і використовується для регулярних завдань (наприклад, щоденного пошуку загроз або щотижневої генерації звітів). Тригер введення користувачем (User Input) використовується тоді, коли потрібне людське втручання. Цей тригер призупиняє виконання певного процесу та очікує підтвердження чи введення даних (зазвичай використовується у критичних діях). Для гнучкості тригерів існує тригер підпотоку (Subflow). Він може запускати один робочий процес прямо з іншого (наприклад для стандартного збору додаткових даних). Ще важливим тригером є тригер, що запускається через електронну пошту (Email). Тобто факт отримання листа може автоматично активувати робочий процес. Використання такого тригера корисно для обробки інцидентів, таких як фішинг чи спам. А найуніверсальнішим способом є тригер REST API, цей тригер

може бути викликаний будь-яким зовнішнім програмним забезпеченням чи навіть іншим робочим процесом через RESTful-запит.

Завдяки використанню відкритого стандарту OpenAPI та продуманій структурі додатків (Apps) у SOAR забезпечується швидкість та гнучкість інтеграції. Додатки можна створювати автоматично на основі специфікацій OpenAPI або їх можна розробляти вручну за допомогою SDK SOAR. Якщо потрібна система для інтеграції (SIEM, Firewall, TIP тощо), і вона має відкриту специфікацію API у форматі OpenAPI, то SOAR, по суті, може автоматично завантажити її та створити готовий до роботи додаток. Ця дає командам безпеки можливість налаштовування нової інтеграції всього за кілька хвилин. Так забезпечується простота та швидкість. SDK це є ручний механізм для нестандартних або внутрішніх систем, які не мають специфікації OpenAPI. SDK надає розробникам набір бібліотек та інструментів (зазвичай Python), які дозволяють вручну кодувати взаємодію з API. Такий метод дає максимальну гнучкість і кастомізацію. Додатки, створені SDK легко інтегруються у середовище Workers. У результаті комбінація OpenAPI та SDK є гарантія, що можна інтегруватися з будь-якою системою для забезпечення широкої кількості додатків.

Отже, як було зазначено раніше, основою архітектури є мікросервіси. Вони реалізовані через Docker. Тому Workers та Apps розроблені як модульні образи, що можуть функціонувати незалежно від основного сервера та розгортатися у різних середовищах. Docker дозволяє системі забезпечити ізольоване та швидке виконання робочих процесів. Це дозволяє системі максимально миттєво реагувати на кіберзагрози. Мови програмування тут вибрані згідно вимогам до надійності екосистеми. Завдяки своїй стабільності й високій продуктивності було вибрано мову програмування Golang для для створення основного механізму автоматизації та компонентів ядра (в тому числі Backend, Worker, Orborus). Golang менш схильний до збоїв під час виконання, тому саме ця мова використовується для безперервної роботи SOAR-ядра. А мова Python є основною мовою для розробки багатьох додатків (Apps) та SDK, це тому, що Python широко застосовується у сфері кібербезпеки та має багату бібліотечну базу. Для реалізації Frontend було

використана мова програмування JavaScript. JavaScript забезпечує сучасний, динамічний і зручний інтерфейс користувача візуалізації робочого процесу.

Уся ця система не обмежується власними розробками, а також інтегрується з відомими фреймворками. Яскравим прикладом є використання Mitre ATT&CK. Цей фреймворк допомагає будувати універсальні робочі процеси та відображати загрози у зрозумілій структурі. Завдяки ньому робочі процеси можна прив’язати до конкретних технік і тактик Mitre, а їхнє виявлення буде показувати рівень ризику. Така функція дозволяє використовувати дані SOAR не тільки для реагування, а й для створення показників ефективності системи для подальшої аргументації інвестицій у кібербезпеку [64].

3.5 Засоби виявлення комп'ютерних атак на корпоративних інформаційних систем

Засобів виявлення комп'ютерних атак на КІС є декілька, ця кількість цих засобів є достатньою для максимального гарантування виявлення різних атак. Серед цих засобів є вже відомі системи такі як SIEM, EDR, UEBA та TIP. Тобто це є таких комплекс засобів виявлення кібератак (рисунок 3.10).

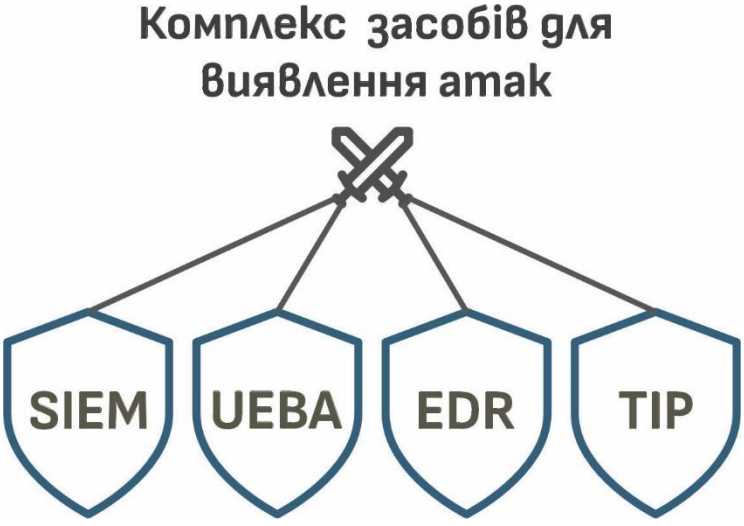


Рисунок 3.10 – Засоби для виявлення кібератак в системі захисту

Самі по собі ці засоби вдало виявляють різноманітні атаки. А якщо ж їх використовувати в сукупності, відповідно ефект буде набагато кращим. Тобто саме ймовірність виявлення та конкретизації атаки буде вища. Це дозволить швидше та чіткіше надіслати дані з цих засобів виявлення системі SOAR. Відповідно й система SOAR зможе швидше та чіткіше відреагувати.

Засіб виявлення SIEM є центральним хабом кореляції та збору даних. Він є ключовим постачальником тривог для нашої системи SOAR. Як вже відомо сама назва є акронімом та відображає Security Information and Event Management (рисунок 3.11).

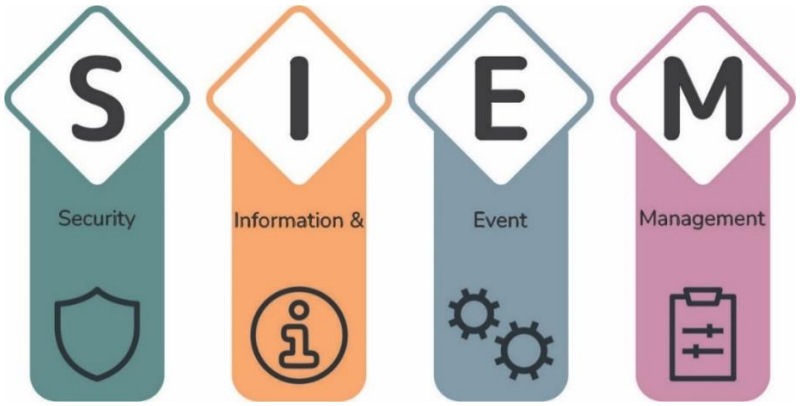


Рисунок 3.11 – Засіб для виявлення атак SIEM системи захисту

Тобто в перекладі це значить Управління інформацією та подіями безпеки. А це значить, що управляючи інформацією та подіями безпеки, цей засіб дозволяє централізовано збирати, обробляти та аналізувати великі обсяги даних з різних джерел в мережевому середовищі організації. Ці дані містять різні логи з фаєрволів, систем виявлення вторгнень, , антивірусних програм та інших джерел. Далі SIEM, використовуючи збір логів і даних про події, які отримав від пристроїв, додатків, мереж, інфраструктури та систем, проводить аналіз. Аналіз SIEM здійснюється при використанні розуміння контексту, ідентифікації потенційно небезпечних дій та виявлення аномальних патернів. Досліджуючи ці всі дані, він сортує поведінку загроз за певним рівнем ризику. Також завдяки використанню правил та статистичних кореляцій, SIEM надає цінні практичні висновки під час розслідування інцидентів. Щоб виявляти нові та складні загрози використовує

засоби штучного інтелекту (AI) та машинного навчання (ML). Завдяки цим всім характеристикам досягається видимість мережевої діяльності у реальному часі. Це дозволяє ефективно виявляти будь-які загрози безпеці.

В нашій комплексній системі захисту засіб SIEM виконує частково пасивні функції виявлення та попередження. А ось вже SOAR використовує інформацію від SIEM для активних дій. Тобто SOAR у відповідь на отримані сигнали, запускає власний алгоритм реагування. Ця взаємодія між системами реалізується двома основними способами. Першим методом є pull-метод (метод запиту). У цьому випадку SOAR надсилає запити до API SIEM, перевіряючи, чи з'являються нові критичні тривоги. Цей запит може виглядати типу як: "Чи є нові критичні тривоги?" Другим таким методом є push-метод (метод сповіщення). Тут засіб виявлення SIEM налаштований таким чином, що при генерації тривоги повідомлення автоматично надсилається на вхідний інтерфейс SOAR. Це зазвичай реалізується через webhook або API-запит. Push-метод є найпоширенішим способом інтеграції. У цій взаємодії кожна тривога, яку SIEM передає в SOAR, стає тригером для запуску відповідного Playbook. Також таке повідомлення містить необхідний контекст для подальшої обробки. В такому повідомленні вказується IP-адреса джерела або призначення, ім’я користувача, рівень критичності (визначає його SIEM), а також точний час події. Рішень SIEM є досить багато, тому для SOAR є досить широкий вибір. До таких систем належать Elastic Security, Microsoft Sentinel, Splunk SIEM, IBM Security QRadar SIEM, LogRhythm SIEM тощо.

Наступним засобом виявлення є EDR (рисунок 3.12). Назва є акронімом до Endpoint Detection and Response та означає Виявлення та реагування на кінцеві точки.

Рисунок 3.12 – Засіб для виявлення атак EDR системи захисту

Тобто це є засіб виявлення та реагування, який сфокусований на кінцевих точках (ноутбуки, настільні комп’ютери, сервери та мобільні пристрої). Дані з усіх кінцевих точок мережі зберігається у центральному сховищі, зазвичай у хмарі. Для цього використовуються агенти або вбудовані можливості ОС. Ці зібрані дані є даними про процеси, продуктивність, зміни конфігурацій, мережеві підключення, передачу файлів та поведінкові патерни. Важливо те, що EDR забезпечує безперервний моніторинг активності на пристроях. Він спостерігає за файловими операціями, процесами, мережевими з’єднанями, змінами у реєстрі та поведінки користувачів. Завдяки цьому EDR здатне виявляти безфайлові атаки, рух шкідливого ПЗ, спроби обходу захисту. Цікавим є те, що він може також виявляти горизонтальне переміщення (Lateral Movement) між скомпрометованими машинами. EDR застосовує розширену аналітику та алгоритми машинного навчання, щоб виявляти закономірності, які можуть свідчити про відомі чи нові реальні загрози. Він аналізує як індикатори компрометації (IOC), що сигналізують про виявлену атаку, так і індикатори атаки (IOA), які є пов'язанами з тактиками та методами кіберзлочинців. Для підвищення точності співвідносються власні дані з розвідкою загроз (власною, сторонньою чи спільнотною) та базою знань MITRE ATT&CK. Це дозволяє відокремити реальні загрози від хибнопозитивних сигналів та зосередити увагу аналітиків на критичних інцидентах. Завдяки всьому цьому він забезпечує глибоку видимість та проактивне виявлення загроз в масштабах усього підприємства. EDR також можна інтегрувати з SIEM для збагачення аналітики додатковим контекстом із різних рівнів IT-інфраструктури. У нашому випадку EDR також інтегрований з SOAR. Це дозволяє автоматизувати сценарії реагування на інциденти. Усе це відображається в централізованій консолі. Ця консоль надає командам безпеки повний огляд стану кінцевих точок, інцидентів та інструменти для розслідування.

EDR взаємодіє з нашою системою SOAR двома основними способами. Перший є Trigger (EDR до SOAR). Прикладом такого сопособу є ситуація виявлення EDR критичної активності (наприклад, нетиповий запуск cmd.exe) і EDR самостійно генерує Alert, який запускає Playbook SOAR. Другим таким способом є

Orchestration (SOAR до EDR). Прикладом є те, що коли SOAR отримав тривогу від SIEM, SOAR запитує EDR для збагачення даних, а потім надсилає команду для реагування. EDR забезпечує SOAR критичним параметром (рівень критичності АКТИВУ). Наприклад, якщо EDR виявляє атаку на "Головний контролер домену", то SOAR застосує Playbook з максимальною жорсткістю. Тобто це є дії у відповідь. Тут система використовує потужний Public API для виконання команд реагування. Серед цих команд можуть бути ізоляція хоста, запуск скрипта або збір артефактів. Є декілька головних рішень EDR, що мають добре документовані API для інтеграції. До таких рішень належить CrowdStrike Falcon, SentinelOne Singularity, Microsoft Defender for Endpoint, LimaCharlie. Зв'язок між EDR та нашою платформою SOAR майже завжди реалізується за допомогою API. Як згадувалось раніше, взаємодія відбувається за двома основними методами. Для початку відбувається етап Тригер (Trigger), тут EDR виявляє підозрілу активність (це може бути спроба запуску шкідливого скрипта); далі EDR використовує свій API, щоб відправити сповіщення (Webhook) або створити запис у черзі (Kafka) про цей інцидент; потім SOAR отримує цей Webhook і отримане сповіщення стає певним тригером для запуску конкретного Playbook. В цьому випадку елемент Kafka транспортує ці події у реальному часі до різних систем. Тут Kafka забезпечує масштабовану доставку телеметрії з EDR-агентів, і це все дозволяє спростити інтеграцію з іншими системами (SIEM, TIP), бо дані отримуються не напряму від EDR, а через Kafka. Наступним етапом є Оркестрація (Orchestration). На цьому етапі, після отримання тригера, Playbook виконує певні дії, викликаючи API EDR-системи. Ці дії складаються з наступних етапів: Playbook отримує ID зараженого пристрою, SOAR робить API-запит до EDR (це робиться через HTTP-запит з відповідним токеном автентифікації), відбувається конкретна дія з різними командами, отримання результату. Командами щодо етапу конкретної дії можуть бути команди ізолювання кінцевої точки від мережі (POST /hosts/{host_id}/actions/isolate) чи отримання повного списку процесів, які брали участь в інциденті (GET /incidents/{incident_id}/details). Тут для прямої взаємодії (автоматизоване реагування, тригери, отримання команд) використовується

формат JSON. Але на рівні збору даних або інтеграції з іншими проміжними системами тут можуть використовуватися XML або протоколи логування (Syslog/CEF).

Наступним засобом для виявлення є UEBA. Назва є акронімом до User and Entity Behavior Analytics (рисунок 3.13) та означає Аналіз Поведінки Користувачів та Об'єктів.

Рисунок 3.13 – Засіб для виявлення атак UEBA системи захисту

Тут UEBA є ключем до виявлення складних внутрішніх загроз, а SOAR у нас забезпечує миттєве реагування. Система UEBA використовує машинне навчання, щоб безперервно аналізувати дані з різних джерел. Цими джерелами можуть бути логіни, мережевий трафік, файловий доступ і так далі. Система формує "нормальний" профіль поведінки для кожного користувача, пристрою чи програми. Ця система порівнює певну поточну активність з базовим профілем та будь-яке значне відхилення позначає як аномалію. Це є перший етап розпізнавання. UEBA не вважає одну аномалію атакою. Замість цього, вона корелює кілька аномалій протягом певного періоду часу та присвоює об'єкту підвищений ризиковий бал. А ось коли цей бал перевищує певний поріг, то система генерує інцидент (розпізнана атака чи активністи високого ризику). Є декілька основних рішень UEBA: Splunk UEBA, Microsoft Sentinel, Exabeam Security Intelligence Platform. Насправді їх є більше, і рідко одна платформа чисто сфокусована на SIEM чи UEBA (або інші). Зазвичай вони часто поєднуються. При взаємодії UEBA та SOAR проходить три етапи. На першому етапі виявлення аномалій відбувається відстеження певних

подій, які в подальшому можуть свідчити про аномалії. Наступним етапом є формування тригера. Тут у випадку коли аномалія перевищує певний встановлений поріг, UEBA генерує сповіщення та присвоює йому високий ризиковий бал (Risk Score). Наступним етапом є автоматичне реагування SOAR. Це сповіщення (тригер) передається в SOAR як тригер, а SOAR вже запускає відповідний Playbook, який може автоматично підтвердити, ізолювати чи сповістити.

Взаємодія тут також відбувається через API. Тобто спочатку сповіщення про високий ризиковий бал надходить до нашої SOAR системи через Webhook або шляхом опитування API засоба виявлення UEBA. Далі SOAR розбирає вхідний JSON-файл і витягує ідентифікатор користувача, його роль та рівень ризику. Потім відбувається етап дій, де автоматично виконується певна послідовність кроків. Ними є збір інформації (наприклад, Playbook запитує дані про користувача з Active Directory), перевірка (наприклад, Playbook запитує дані про кінцеву точку через EDR) та реагування (якщо ризик підтверджено, то Playbook через будь-який EDR (наприклад, Microsoft Defender API) виконує команду блокування облікового запису).

Наступним засобом для виявлення є TIP – Threat Intelligence Platform (рисунок 3.14).

Рисунок 3.14 – Засіб для виявлення атак TIP системи захисту

Це є Платформа Аналізу Загроз (Threat Intelligence Platform). TIP збирає, обробляє та аналізує інформацію про відомі загрози. Головна метою TIP є перетворення величезних обсягів сирих даних про загрози на зрозумілі та

практично застосовні знання для команд безпеки. TIP виконує кілька критично важливих функцій у системі кіберзахисту. Першою функцією є акумуляція інформації. Тут TIP автоматично підключається до різноманітних джерел. Цими джерелами можуть бути комерційні потоки загроз та відкриті ресурси OSINT до внутрішніх логів із SIEM чи EDR та міжмережевих екранів. Це дозволяє охопити максимально широкий спектр відомих і нових загроз. Другою функцією є обробка та нормалізація. Початкові дані (IP-адреси, хеші файлів, доменні імена) надходять у різних форматах і часто містять дублікати. Через це TIP приводить їх до єдиного стандарту та відсіює застарілі чи нерелевантні індикатори. Це дозволяє забезпечити своєрідну узгодженість інформації та підвищити якість подальшого аналізу. Третьою функцією є збагачення та контекст. Тут прості індикатори отримують додатковий контекст. TIP визначає чи пов’язана підозріла IP-адреса з конкретною APT-групою, чи використовувалася у фішингових атаках, чи зустрічалася лише у спам-розсилках. Такі дії допомагають аналітикам краще зрозуміти мотиви, можливості та тактики зловмисників. І четвертою функцією є поширення та інтеграція. На цьому етапі проходить передача збагаченої інформації до інших систем безпеки для його оперативного реагування. TIP можна інтегрвати з SOAR, SIEM, EDR та брандмауерами. Ця можливість є дуже корисною для нашої SOAR системи. До прикладу, засіб TIP може автоматично повідомити SOAR, що певний хеш належить відомому шкідливому ПЗ. Потім може одразу запуститись певний Playbook блокування.

Отже, TIP є дуже важливим елементом для виявлення для системи SOAR. Інтеграція TIP із SOAR дозволяє автоматизувати процес збагачення даних про інциденти та перевірку індикаторів компрометації. Взагальному, можна виділити декілька головних сценаріїв використання TIP в нашій системі. Першим таким сценарієм може бути перевірка IoC (індикатори компрометації). У цьому сценарії відбувається від SOAR автоматичне запитування даних про IP-адресу чи хеш файлу у TIP. Це може відбуватися, якщо було отримано сповіщення про підозрілий файл (хеш) чи IP-адресу. Якщо результат ґрунтується на десятках антивірусних двигунів, то певний Playbook переходить до ізоляції хоста. Наступним сценарієм може бути

автоматичне оновлення захисту. Цей сценарій відбувається, якщо SOAR отримує новий список шкідливих IP-адрес від TIP. При цьому сцинарії, він може автоматично передати цей список у брандмауер для створення нових правил блокування. Ще одним цікавим сценарієм може бути дії щодо контексту IP-адреси. Таке може відбуватися при виявленні невдалого входу. Тут , SOAR використовує TIP, щоб визначити, чи належить ця адреса до списку відомих ботнетів чи TOR-виходів. На основі цих даних можна чітко виділити чотири основних етапи принципу інтеграції TIP з SOAR: тригер, збагачення, аналіз, пріоритизація та реагування.

На першому етапі відбувається надходження сповіщення про потенційну загрозу(наприклад, спроба входу з підозрілої IP-адреси) до SOAR. На другому етапі SOAR автоматично запитує дані про цю IP-адресу чи хеш файлу у TIP. На третьому етапі засіб TIP відповідає чи фігурувала ця IP-адреса у відомих фішингових кампаніях та чи є цей хеш частиною відомого шкідливого ПЗ. Це відбувається при надаванні контексту. І вже на останньому етапі SOAR автоматично підвищує оцінку ризику інциденту та запускає автоматичний Playbook реагування на основі отриманої інформації. Таке може відбуватися якщо TIP підтвердив, що IP-адреса є шкідливою.

Як і у випадку з EDR, SIEM, UEBA, інтеграція TIP в нашій системі SOAR повністю залежить від API. API є ключовим механізмом для отримання інформації від зовнішніх засобів TIP. Практично як з іншими засоба виявлення, API тут бувають вхідні та вихідні. Вихідний API є основним способом, яким SOAR комунікує з TIP. SOAR формує GET-запит до API TIP, передаючи індикатор (IP, хеш, домен) як параметр. Вхідний API є API, що деякі засоби TIP можуть самі надсилати webhook до SOAR про нові критичні індикатори, які SOAR потім можуть використовувати для оновлення своїх списків блокування.

Взагальному, існує декілька головних рішень для засобу для виявлення TIP. Це Group-IB Threat Intelligence Platform, Anomali ThreatStream, MISP тощо.

3.6 Висновки

У третьому розділі на основі розроблених моделей та методів була запропонована та описана архітектура системи адаптивного захисту. Також був детальний опис взагальному системи захисту та її алгоритмів і програмного забезпечення. Серед алгоритмів було створено комплекс алгоритмів. Перший алгоритм стосується оцінки ризику, другий адаптивного часу блокування, третій усього алгоритму роботи системи захисту. Як технологічну основу було вибрано платформу Shuffle SOAR, що забезпечує потрібну масштабованість та відмовостійкість. Детально описано структуру програмного забезпечення. Також тут було приділено увагу механізмам інтеграції та розширення, використовуючи відкритий стандарт OpenAPI. Іще було визначено засоби виявлення атак цієї системи захисту.

ВИСНОВКИ

У цій роботі було вирішено важливу задачу – підвищення стійкості корпоративних інформаційних систем в сучасних умовах, де відбувається регулярне зростання кількості і складності кіберзагроз. Був проведений аналіз, який показав, що в динамічному середовищі загроз традиційні статичні підходи, сильно втрачають свою ефективність, що призводить до потреби переходу до адаптивних і автоматизованих рішень. Проаналізовано поняття стійкості інформаційних систем та класифіковано сучасні комплексні загрози. Було розглянуто актуальні підходи до захисту, включно з Defense in Depth, Zero Trust й інші. Також було проаналізовані вимоги міжнародних стандартів (ISO/IEC 27001, NIST CSF, GDPR) та ДСТУ. Була визначена необхідність переходу до адаптивних, автоматизованих систем захисту КІС, бо критичним недоліком простих систем є низька швидкість реагування на інциденти та високий рівень помилкових спрацювань. Були розглянуті різні моделі забезпечення стійкості КІС. Іще вдалося сформувати формальні моделі загроз та сценаріїв атак, що, у свою чергу, дозволило систематизувати вектори проникнення зловмисників у корпоративну мережу. Визначено також ключові показники ефективності захисту, вони базуються на часових характеристиках виявлення та реагування. Побудовано модель функціонування захищеної КІС та запропоновано алгоритм оцінювання ефективності захисту із застосуванням марківських моделей. Ця побудована модель функціонування КІС, що захищається, і застосування марківських моделей дали змогу математично показати зв’язок між швидкістю реакції і ймовірністю успішності відбиття атаки, що підтвердило важливість автоматизації реагування. Було розглянуто метод адаптивного захисту КІС від комплексних кіберзагроз. В рамках цього методу розроблено два ключові алгоритми: алгоритм оцінки ризику та алгоритм адаптивного часу блокування. Алгоритм оцінки ризику дозволятиме пріоритизувати інциденти з урахуванням типу події, критичності активу та наявності певних контрольних механізмів. А алгоритм адаптивного часу блокування буде динамічно визначати потрібний час ізоляції активів на основі

рівня ризику. Вибрано систему захисту на базі платформи SOAR та обґрунтовано, що характеристики SOAR забезпечують необхідні потреби (наприклад, гнучкість та масштабованість). Детально описано структуру програмного забезпечення системи та алгоритми, що забезпечують основу автоматизації та адаптивності. Розглянуто інтеграцію з різноманітними засобами для виявлення атак (EDR, UEBA, TIP, SIEM). Також, до цього, показано реалізацію замкнутої петлі автоматизації.

Так що, підсумовуючи результати роботи, можемо стверджувати, що запропонований комплексний підхід щодо захисту КІС від комплексних кіберзагроз дозволяє значно підвищити рівень захищеності корпоративних інформаційних систем, тому що тут поєднується багаторівнева архітектура, різні інтелектуальні алгоритми та технологія SOAR. Система вміє не тільки швидко реагувати на вже відомі загрози, а й підлаштовуватися під нові способи атак. Завдяки чому система є адаптивною, що робить систему захисту максимально ефективною.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Корпоративна інформаційна система. URL: https://uk.wikipedia.org/wiki/Корпоративна_інформаційна_система (дата звернення: 08.09.2025).

2. A technology survival guide for resilience. URL: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/a-technology-survival-guide-for-resilience (дата звернення: 09.09.2025).

3. Додонов О. Г., Кузнєцова М. Г., Горбачик О. С. Моделювання і оцінювання функціональної стійкості інформаційних систем. *Методи захисту інформації у комп'ютерних системах і мережах.* Київ, 2025. С. 77–82.

4. Миронюк М. Ю., Майстров О. О., Мусієнко А. П., Макарчук А. В. Аналіз побудови інтелектуальної інформаційної системи на основі поняття функціональної стійкості. *Зв'язок*. 2024. № 1. С. 3–8.

5. Lakshmi Goel, Dawn Russell, Steven Williamson, Justin Zuopeng Zhang. Information systems security resilience as a dynamic capability. *Journal of Enterprise Information Management*. 2023. Vol. 36, № 4. P. 906–924. DOI: 10.1108/JEIM-07-2022-0228

6. Кібератака. URL: https://uk.wikipedia.org/wiki/Кібератака (дата звернення: 09.09.2025).

7. Давиденко Є. А. Корпоративна безпека на українських підприємствах в умовах війни. *Економіка та суспільство*. 2023. № 58. С. 2–6.

8. Основи Кібербезпеки для бізнесу. URL: https://westelecom.ua/blog/osnovy-kiberbezopasnosti-dla-biznesa (дата звернення: 09.09.2025).

9. Комплексний погляд на кібератаки. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-a-cyberattack (дата звернення: 09.09.2025).

10. Різні типи кібератак та як не стати їх жертвою. URL: https://nordvpn.com/uk/blog/shcho-take-kiberataka/?srsltid=AfmBOoqlIfwpKtKr4GXDnwlrVkLpEH813XSEN41WC44rfi2_VqSRkZrz (дата звернення: 09.09.2025).

11. Комплексна система захисту інформації – що це? URL:

https://hostpark.ua/news-ua/kompleksna-systema-zahystu-informacziyi-shho-cze/ (дата звернення: 10.09.2025).

12. Захист корпоративних мереж від загроз: засоби та методи. URL: https://netwave.ua/blog/zahist-korporativnih-merezh-vid-zagroz-zasobi-ta-metodi/ (дата звернення: 10.09.2025).

13. В. Б. Дудикевич, Г. В. Микитин, Т. Є. Мурак. Комплексна система безпеки регіональної корпоративної мережі на основі еталонної моделі osi та моделі “Глибокого захисту”. *Computer systems and networks*. 2025. Том 7, № 1. С. 124–126.

14. Мехед Д. Аналіз вразливостей корпоративних інформаційних систем / Д. Мехед, Ю. Ткач, В. Базилевич, В. Гур’єв, Я. Усов // Захист інформації. 2018. Т. 20, № 1. С. 61-66.

15. Jouini Mouna, Latifa Ben Arfa Rabaia, Anis Ben Aissa. Classification of Security Threats in Information Systems. *Procedia Computer Science. 32*: 5th International Conference on Ambient Systems, Networks and Technologies (ANT-2014). Tunis, 2014. P. 489–496.

16. Defense in Depth: багаторівневий підхід до захисту інформації. URL: https://avolutech.com/blog/defense-in-depth-багаторівневий-підхід-до-захисту/ (дата звернення: 10.09.2025).

17. Zero Trust: Модель кібербезпеки, яка не вірить нікому – і саме тому рятує бізнес. URL: https://my-itspecialist.com/zero-trust-model-kyberbezpeky (дата звернення: 10.09.2025).

18. Що таке IPS/IDS і де застосовується. URL: https://www.hostzealot.com.ua/blog/about-solutions/shho-take-ipsids-i-de-zastosovujetsya (дата звернення: 10.09.2025).

19. Порівняння та вибір стандарту кібербезпеки URL: https://www.oksim.ua/porivnyannya-ta-vibir-standartu-kiberbezpeki/ (дата звернення: 10.09.2025).

20. Основні переваги сертифікації ISO/IEC 27001. URL: https://www.issp.training/post/osnovni-perevahy-sertyfikatsiyi-iso-iec-27001 (дата

звернення: 10.09.2025).

21. What is the Plan-Do-Check-Act (PDCA) Cycle? URL: https://asq.org/quality-resources/pdca-cycle?srsltid=AfmBOorjsGZ3ClVTu2cM1OsZDFM708DI47GQxdLkVsEF2adyAQqEpajD (дата звернення: 10.09.2025).

22. NIST CSF - стандарт, про який варто знати. URL: https://my-itspecialist.com/what-is-the-nist-csf-standartrt (дата звернення: 10.09.2025).

23. Що таке GDPR та чи варто його виконувати поза межами ЄС. URL: https://legalaid.ua/ua/shho-take-gdpr/ (дата звернення: 15.09.2025).

24. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT). – Київ : УкрНДНЦ, 2016.

25. Що таке моделювання загроз і якими є його переваги? URL: https://www.issp.training/post/shcho-take-modelyuvannya-zahroz-i-yakymy-ye-yoho-perevahy (дата звернення: 16.09.2025).

26. What Is the STRIDE Threat Model? Beginner’s Guide – 2025. URL: https://www.practical-devsecops.com/what-is-stride-threat-model/?srsltid=AfmBOooFRj5W_pOW2pZZMyk07BI-58z25VHsPzTOBjdwUMXr7e9ErIzH (дата звернення: 17.09.2025).

27. DREAD Threat Modeling. URL: https://threat-modeling.com/dread-threat-modeling/ (дата звернення: 17.09.2025).

28. Threat Modeling Methodology: OCTAVE. URL: https://www.iriusrisk.com/resources-blog/octave-threat-modeling-methodologies (дата звернення: 17.09.2025).

29. Threat Modeling Methodology: TRIKE. URL: https://www.iriusrisk.com/resources-blog/trike-threat-modeling-methodologies (дата звернення: 17.09.2025).

30. PASTA Threat Modeling. URL: https://threat-modeling.com/pasta-threat-modeling/ (дата звернення: 17.09.2025).

31. Guide to Threat Modeling using Attack Trees. URL: https://www.practical-

devsecops.com/threat-modeling-using-attack-trees/?srsltid=AfmBOooQk_TLjGOcetG8OZsLF7rWu-gabZ8AA3sU5JTgSQxwTQpRbUrT (дата звернення: 17.09.2025).

32. Cyber Kill Chain: Сучасні Загрози та Інструменти Протидії. URL: https://itorakul.com.ua/cyber-kill-chain/ (дата звернення: 17.09.2025).

33. Моделювання загроз за допомогою MITER ATT&CK Framework. URL: https://www.hostragons.com/uk/блог/моделювання-загроз-інфраструктури-mitre-attac/ (дата звернення: 17.09.2025).

34. MITRE ATT&CK framework. URL: https://www.ibm.com/think/topics/mitre-attack (дата звернення: 17.09.2025).

35. Cyber Kill Chain: Сучасні Загрози та Інструменти Протидії. URL: https://itorakul.com.ua/cyber-kill-chain/ (дата звернення: 17.09.2025).

36. 20 Cybersecurity Metrics & KPIs to Track in 2025. URL: https://securityscorecard.com/blog/9-cybersecurity-metrics-kpis-to-track/ (дата звернення: 23.09.2025).

37. Cybersecurity Metrics & KPIs: What to Track in 2025. URL: https://www.sentinelone.com/cybersecurity-101/cybersecurity/cybersecurity-metrics/ (дата звернення: 23.09.2025).

38. 1.1: Марківські процеси. URL: https://ukrayinska.libretexts.org/Хімія/Фізична_і_теоретична_хімія/Нерівноважна_статистична_механіка_(Cao)/01%3A_Стохастичні_процеси_та_броунівський_рух/1.01%3A_Марківські_процеси (дата звернення: 29.09.2025).

39. 3.7. Марківські моделі прийняття рішень. URL: https://studfile.net/preview/3275043/page:12/ (дата звернення: 29.09.2025).

40. Кльоц Ю. П., Джулій В. М., Чорненький С. В. Метод забезпечення стійкості корпоративних інформаційних систем до комплексних кіберзагроз. 2025.

41. Чорненький С.В., Джулій В.М. Метод взаємодії квантової апаратури з користувальницькими системами захисту. *Актуальні проблеми комп'ютерних наук АПКН-2025*: наукові праці за матеріалами XVII Всеукраїнської науково-практичної конференції, м. Хмельницький, 14–15 листопада 2025 р. / Міністерство освіти і

науки України, Хмельницький національний університет. Хмельницький, 2025. С. 433–436.

42. Ахрамович В. В. Спосіб дослідженнякількісних показників системи захисту корпоративної мережі. *КІБЕРБЕЗПЕКА: освіта, наука, техніка*. 2025. Том 4, № 28. DOI: 10.28925/2663-4023.2025.28.776.

43. Sneha Saxena. The Hybrid Cloud Security Imperative Integrating LDAP/AD with Modern Platforms for Protection. *International Journal of Scientific Research & Engineering Trends*. 2019. Vol. 5, № 4. P. 1–4.

44. Jani Purujoki. SOAR Playbook Implementation - Incident Deduplication and Its Effects. Jyväskylä: Jamk University of Applied Sciences, 2020. 46 p.

45. Integrated Adaptive Cyber Defense. URL: https://www.iacdautomate.com/ (дата звернення: 17.11.2025).

46. Kinyua J., Awuah L. AI/ML in Security Orchestration, Automation and Response: Future Research Directions. *Intelligent Automation & Soft Computing*. 2021. Vol. 28, № 2. P. 527–545. DOI: 10.32604/iasc.2021.016240.

47. Chadni Islam, Muhammad Ali Babar, Surya Nepal. A Multi-Vocal Review of Security Orchestration. *ACM Computing Surveys (CSUR)*. 2019. Vol. 52, № 2. P. 1–45. DOI: 10.1145/3305268.

48. CIS Critical Security Controls Version 8. URL: https://www.cisecurity.org/controls/v8 (дата звернення: 17.11.2025).

49. Mohajan, H. K. . (2025). Vulnerability of Cyber Security Is an Unexpected Threat to Global Internet System. *Art and Society*. 2025. Vol. 4, № 9. P. 1–14. DOI: 10.63593/AS.2709-9830.2025.10.001.

50. What is Endpoint Detection and Response (EDR)? URL: https://www.crowdstrike.com/en-us/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/ (дата звернення: 17.11.2025).

51. What Is User and Entity Behavior Analytics (UEBA)? URL: https://www.syteca.com/en/glossary/what-is-ueba (дата звернення: 17.11.2025).

52. Gartner: Market Guide for SOAR Solutions. URL: https://www.paloaltonetworks.com/blog/2020/10/secops-gartner-soar-solutions/ (дата

звернення: 17.11.2025).

53. CACAO Security Playbooks Version 2.0. URL: https://docs.oasis-open.org/cacao/security-playbooks/v2.0/security-playbooks-v2.0.html (дата звернення: 18.11.2025).

54. Federal Government Cybersecurity Incident and Vulnerability Response Playbooks. URL: https://www.cisa.gov/resources-tools/resources/federal-government-cybersecurity-incident-and-vulnerability-response-playbooks (дата звернення: 19.11.2025).

55. OpenAPI Specification v3.1.0. URL: https://spec.openapis.org/oas/v3.1.0 (дата звернення: 18.11.2025).

56. H. Alipour, Y. B. Al-Nashif, P. Satam, S. Hariri. Wireless Anomaly Detection Based on IEEE 802.11 Behavior Analysis. *IEEE Transactions on Information Forensics and Security*. 2015. Vol. 10, № 10. P. 2158–2170. DOI: 10.1109/TIFS.2015.2433898.

57. Florian Skopik, Giuseppe Settanni, Roman Fiedler. A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security*. 2016. Vol. 60. P. 154–176. DOI: 10.1016/j.cose.2016.04.003.

58. Implementing a Zero Trust Architecture. URL: https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture (дата звернення: 18.11.2025).

59. Akbar Siami Namin, Rattikorn Hewett, Keith S. Jones, Rona Pogrund. Sonifying Internet Security Threats. CHI EA '16: Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems, c. New York, 7–12 may 2016 p. / Association for Computing Machinery. New York, 2016. P. 2306–2313.

60. Markus Riek, Rainer Böhme. The costs of consumer-facing cybercrime: an empirical exploration of measurement issues and estimates. *Journal of Cybersecurity*. 2018. Vol. 4, № 1. P. 16–22. DOI: 10.1093/cybsec/tyy004.

61. Sam Newman. Building Microservices: Designing Fine-Grained Systems.

O'Reilly Media, Inc.: Sebastopol, 2021. 616 p.

62. Shuffle Architecture. URL: https://shuffler.io/docs/architecture (дата звернення: 20.11.2025).

63. Crockford Douglas, Morningstar Chip. Standard ECMA-404 The JSON Data Interchange Syntax. Ecma Internationa: Geneva, 2017. 16 p.

64. Bader Al-Sada, Alireza Sadighian, Gabriele Oligeri. MITRE ATT&CK: State of the Art and Way Forward. ACM Comput. *ACM Computing Surveys*. 2024. Vol. 57, № 1. P. 1–37. DOI: 10.1145/3687300.

ДОДАТОК А

Фрагмент коду

```
import asyncio
import json
import re
import subprocess
from walkoff_app_sdk.app_base import AppBase
class snort3(AppBase):
    __version__ = "1.0.0"
    app_name = "snort3"
    def __init__(self, redis, logger, console_logger=None):
        super().__init__(redis, logger, console_logger)
    def create_snort_file(self, file_ref):
        print(f"Retrieving file {file_ref}.")
        re_hash = re.compile("[a-fA-F0-9]{8}-([a-fA-F0-9]{4}-){3}[a-fA-F0-9]{12}")
        if re_hash.match(file_ref) is None:
            raise (ValueError("File reference must be a supported hash value."))
        target_dir = "/app"
        ref_dict = self.get_file(file_ref)
        target_path = target_dir + "/" + ref_dict["filename"]
        with open(target_path, "xb") as tmp_file:
            tmp_file.write(ref_dict["data"])
            tmp_file.close()
        return target_path
    def run_snort_scan(self, config_path, rules_path, pcap_path):
        cmd = [
            "snort",
            "-c",
            config_path,
```

```
            "-R",
            rules_path,
            "-r",
            pcap_path,
            "-A",
            "alert_fast",
        ]
        print("Executing the following command: {}".format(" ".join(cmd)))
        result = subprocess.run(
            cmd,
            capture_output=True,
            text=True,
        )
        alerts = []
        for line in result.stdout.split("\n"):
            if "[**]" in line:
                alerts.append(line)
        return_data = {
            "success": True,
            "return_code": result.returncode,
            "alerts": alerts,
            "errors": result.stderr,
            "pcap": {"name": pcap_path},
            "cmd": cmd,
        }
        return return_data
    def simple_analyze_file(self, config_file, rules_file, pcap_file):
        rules_path = self.create_snort_file(rules_file)
        pcap_path = self.create_snort_file(pcap_file)
        config_path = "/usr/local/etc/snort/snort.lua"
```

```
    if len(config_file) > 0:
        config_path = self.create_snort_file(config_file)
    return_data = self.run_snort_scan(config_path, rules_path, pcap_path)
    try:
        return json.dumps(return_data)
    except (json.JSONDecodeError, TypeError):
        return return_data
def version_check(self):
    result = subprocess.run(
        ["snort", "-V", "-u", "snort3"], capture_output=True, text=True)
    return_data = {
        "success": True,
        "return_code": result.returncode,
        "output": result.stdout,
        "errors": result.stderr,
    }
    try:
        return json.dumps(return_data)
    except (json.JSONDecodeError, TypeError):
        return return_data
def custom_rule_scan(self, config_file, custom_rule, pcap_file):
    pcap_path = self.create_snort_file(pcap_file)
    config_path = "/usr/local/etc/snort/snort.lua"
    if len(config_file) > 0:
        config_path = self.create_snort_file(config_file)
    rules_path = "/app/my.rules"
    with open(rules_path, "xb") as tmp_file:
        tmp_file.write(custom_rule.encode("utf-8"))
        tmp_file.close()
    return_data = self.run_snort_scan(config_path, rules_path, pcap_path)
```

```
        try:
            return json.dumps(return_data)
        except (json.JSONDecodeError, TypeError):
            return return_data
if __name__ == "__main__":
    snort3.run()

import socket
import asyncio
import time
import random
import json
import requests
from walkoff_app_sdk.app_base import AppBase
class Siemonster(AppBase):
    __version__ = "1.0.0"
    app_name = "siemonster"  # this needs to match "name" in api.yaml
    def __init__(self, redis, logger, console_logger=None):
        """
        Each app should have this __init__ to set up Redis and logging.
        :param redis:
        :param logger:
        :param console_logger:
        """
        super().__init__(redis, logger, console_logger)
    def ping(self, username, password, url):
        message = f"SIEMonster welcomes from {socket.gethostname()} in workflow
{self.current_execution_id}!"
        # This logs to the docker logs
        self.logger.info(message)
```

```
        return message
    def es_get_cluster_health(self, username, password, url):
        return requests.get(url + "/_cluster/health", auth=(username, password), verify=False).text
    def es_query(self, method, username, password, url, path, body):
        headers = {
            "Accept": "application/json",
            "Content-type": "application/json",
        }
        return requests.request(method, url + path, auth=(username, password), data=body, headers=headers, verify=False).text
if __name__ == "__main__":
    Siemonster.run()
```

ДОДАТОК Б

КОПІЇ НАУКОВИХ ПУБЛІКАЦІЙ

УДК 004.056:621.397.3:004.942

ЮРІЙ КЛЬОЦ
Хмельницький національний університет
ORCID http://orcid.org/
e-mail:

ВОЛОДИМИР ДЖУЛІЙ
Хмельницький національний університет
ORCID http://orcid.org/0000-0003-1878-4301
e-mail: dzhuliivm@khmnu.edu.ua

СВЯТОСЛАВ ЧОРНЕНЬКИЙ
Хмельницький національний університет
ORCID http://orcid.org/
e-mail: svchor@gmail.com

МЕТОД ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ ДО КОМПЛЕКСНИХ КІБЕРЗАГРОЗ

У статті запропоновано практичний метод забезпечення стійкості корпоративних інформаційних систем до комплексних кіберзагроз. Метод об'єднує чотири взаємопов'язані контури: багатоджерельний моніторинг подій, оцінювання ризиків у реальному часі, адаптивне реагування на інциденти та кероване відновлення сервісів. Наведено математичну модель для інтегральної оцінки стійкості, референтну архітектуру, алгоритми виконання. Показано, що впровадження методу скорочує середній час виявлення та відновлення, а також підвищує індекс стійкості системи. Робота орієнтована на практичне застосування в організаціях різного масштабу.

Ключові слова: кіберстійкість, корпоративна інформаційна система, комплексні загрози, моніторинг, інцидент, ризик, реагування, відновлення.

YURIY KLOTS, VOLODYMYR DZHULIY, SVIATOSLAV CHORNENSKY
Khmelnytsky National University

METHOD OF ENSURING RESILIENCE OF CORPORATE INFORMATION SYSTEMS TO COMPLEX CYBER THREATS

Abstract. The article proposes a practical method for ensuring the resilience of corporate information systems to complex cyber threats. The method combines four interconnected circuits: multi-source event monitoring, real-time risk assessment, adaptive incident response, and managed service recovery. A mathematical model for an integrated resilience assessment, reference architecture, and execution algorithms are presented. It is shown that the implementation of the method reduces the average detection and recovery time, and also increases the system resilience index. The work is focused on practical application in organizations of various scales.

The developed methods allow to quantitatively assess the processes occurring in the CIS being protected. The proposed models and methods can be applied for high-level formalization of the processes of functioning of corporate information systems at production enterprises, in social institutions, transport facilities, malls, etc. Similar models and methods can also be successfully applied in the tasks of planning and selecting countermeasures to counteract threats in the networks of these organizations. This possibility can be justified by the correctness of the initial assumptions, the compliance of the modeling results with general laws.

Keywords: cyber resilience, corporate information system, complex threats, monitoring, incident, risk, response.

Вступ

Сучасні корпоративні інформаційні системи складаються з великої кількості компонентів: сервери застосунків і баз даних, віртуальна інфраструктура, хмарні сервіси, мережеве обладнання, мобільні та віддалені робочі місця. За таких умов зростає кількість векторів атак і складність їх комбінацій. Традиційний підхід «захист периметру» поступово втрачає ефективність: атаки заходять через фішинг і скомпрометовані облікові записи, використовують вразливості ланцюга постачання, латеральний рух усередині мережі, приховані канали ексфільтрації даних. На перший план виходить стійкість: здатність КІС підтримувати критичні функції під час інцидентів, зменшувати їх вплив на бізнес-процеси та швидко повертатися до нормального стану. Такий підхід вимагає не лише технічних засобів, а й налаштованих процесів і показників ефективності [1,2,3].

Одним із найбільш значущих класів систем, що підлягають захисту від деструктивних впливів, виступають корпоративні інформаційні системи (КІС). Від їхнього успішного функціонування багато в чому залежить ефективність багатьох сучасних підприємств та організацій. Це масштабовані системи, призначені для комплексної автоматизації всіх видів господарської діяльності підприємств, і навіть корпорацій, потребують єдиного управління [1,4,5,8]. Такі системи часто ґрунтуються на поглибленому аналізі даних, широкому використанні систем інформаційної підтримки прийняття рішень, електронному документообігу та діловодстві. КІС організуються на основі комп'ютерних мереж і схильні до мережних атак, але також мають певну специфіку як об'єктів захисту від деструктивних інформаційних впливів, які постійно вчиняються [6,7,11].

Не є рідкістю масштабні мережеві атаки на інформаційну інфраструктуру підприємств і держав. Інша мета зловмисників – хмарна інфраструктура. Хмарні технології використовуються в освіті, науці, банківській сфері. Такі сервіси, як Amazon, GoogleDrive, Dropbox, Яндекс.Диск, не тільки налічують сотні мільйонів приватних користувачів, але і пропонують корпоративні акаунти організаціям. Несанкціонований доступ зловмисника до хмарних сховищ дозволяє йому отримати не лише дані про користувачів (включно з такою інформацією, як реквізити платіжних карток, паролі від акаунтів, копії посвідчень особи), а й дані, що становлять комерційну та навіть, можливо, державну таємницю [9,10,13, 24,25].

Поняття стійкості корпоративної інформаційної системи є здатністю системи залишатися функціональною та доступною, продовжувати працювати без збоїв, навіть якщо відбуваються атаки та інші передбачувані й непередбачувані події. Тобто, попри несприятливі зовнішні чи внутрішні впливи, стійкість корпоративної ІС дозволяє системі забезпечувати безперервність бізнес-процесів. І це є дуже важливим тому, що її порушення може призвести до катастрофічних наслідків для компанії. Цими наслідками можуть бути фінансові втрати, втрата репутації та довіри, порушення операційної діяльності, втрата даних та юридичні ризики [3,13,14].

Критерії оцінювання стійкості для цих систем є дуже важливими для забезпечення стійкості корпоративної інформаційної системи. Вони дозволяють компаніям не просто реагувати на збої, а активно запобігати їм і планувати ефективне відновлення. Що в свою чергу дозволяє планувати безперервність бізнесу, ефективно інвестувати та підвищувати рівень конкурентоздатності [14,16,27].

Оцінювання стійкості корпоративної ІС відбувається за кількома ключовими критеріями, що дозволяють визначити її слабкі місця та потенціал для відновлення. До цих критеріїв належить безвідмовність, надійність, відновлюваність, масштабованість, безпека, гнучкість. Безвідмовність визначає, наскільки система доступна для використання та вимірюється, як правило, у відсотках часу, протягом якого система працює без збоїв. Надійність стосується здатності системи виконувати свої функції стабільно та без помилок протягом певного періоду часу. Відновлюваністю це є швидкість і ефективність, з якою система може повернутися до нормального стану після збою. Масштабованість це здатність системи ефективно адаптуватися до зростання навантаження, наприклад, збільшення кількості користувачів або обсягу даних, не втрачаючи при цьому своєї продуктивності та стабільності. Безпекою є рівень захищеності від несанкціонованого доступу, кібератак, вірусів та інших загроз. Цей критерій є основою

стійкості, бо запобігає збоям, спричиненим зловмисниками. Гнучкість є можливістю системи адаптуватися до змін, гнучка система легше інтегрується з новими інструментами та оновлюється без значних перерв [3,21,22,26,27]. Усі ці критерії зображені на рис. 1.

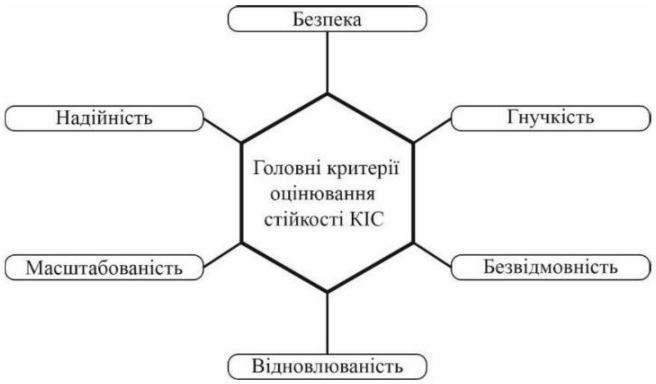


Рис. 1. Головні критерії оцінювання стійкості КІС

Наведені критерії не існують окремо, а вони тісно взаємопов'язані та формують єдину систему. Оцінювання стійкості, що враховує всі ці взаємозв'язки, дозволяє компаніям не просто реагувати на збої, а будувати проактивну стратегію. Це дає можливість мінімізувати ризики, зменшити потенційні фінансові втрати та забезпечити стабільну роботу IT-інфраструктури [5,12,13].

Загрози для інформаційних систем можна класифікувати за кількома критеріями. За джерелом походження вони поділяються на природні (пожежі, повені і т. д.), техногенні (збої обладнання чи програмні помилки) та людські. Людські загрози можуть бути ненавмисними, тобто помилки користувачів, а також можуть бути умисними, а саме зовнішніми (хакерські атаки, фішинг), так і внутрішніми (недобросовісні співробітники) [12,14,21,22]. Схема поділу джерел походження загроз зображено на рис. 2.

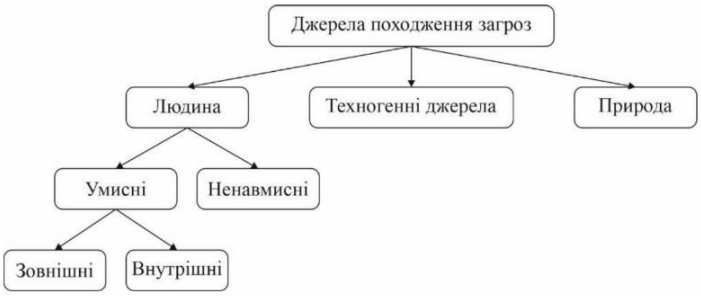


Рис. 2. Джерела походження загроз

За способом реалізації загрози поділяються на фізичні (крадіжка, пожежа), технічні (збої в апаратному забезпеченні), програмні (віруси, трояни) та організаційні (слабкі паролі, відсутність політик безпеки). І, нарешті, за наслідками для системи загрози можуть призвести до порушення конфіденційності (несанкціонований доступ до

даних), порушення цілісності (зміна або знищення інформації) та порушення доступності (відмова в доступі до ресурсів) [11, 12,21,22,23].

Але можуть бути і складніші загрози, такими загрозами є комплексні загрози. Комплексними загрозами є не просто окремі атаки, а поєднання кількох, часто незалежних, факторів, які, взаємодіючи, створюють значно більший ризик, ніж кожен з них окремо. Такі загрози можуть призвести до системного збою, витоку даних, фінансових втрат, пошкодження репутації та навіть повного припинення діяльності компанії. Тобто, в порівнянні з окремими загрозами, комплексні є більш багатовимірні та є взаємозалежні між собою. Можна на багато елементів класифікувати комплексні загрози, але основними можна виділити це поєднання програмних і організаційних загроз, фізичних і програмних загроз, технічних і організаційних загроз. Прикладом взаємодії програмної та організаційної загрози є отримання доступу до ситеми зловмисником через недостатню обізнаність персоналу (погані паролі чи відкривання фішингово листа). Прикладом взаємодії фізичної та програмної загрози є випадок крадіжки фізичного обладнання, що перетворюється на несанкціонований доступ до конфіденційної інформації без необхідності складних кібератак. Прикладом взаємодії технічної та організаційної загрози є технічна несправність через відсутність належних організаційних процедур.

Дані загрози у різних випадках можуть по різному поєднуватись та по різному взаємодіяти між собою. Це не обов'язко пара загроз, це можуть бути декілька загроз, що в сукупності певним чином проявилися [13, 14, 15].

Незважаючи на спроби захисту корпоративних інформаційних систем від комплексних деструктивних інформаційних впливів, вони не мають тенденцій до зниження. До причин цього відноситься поява нових видів загроз, невисока адаптивність методів і систем захисту до умов функціонування корпоративних інформаційних систем, що змінюються. Необхідний пошук нових методів і моделей захисту корпоративних інформаційних систем від таких впливів.

Постановка задачі

Сучасні підходи до захисту корпоративних систем (рис. 3) виходять за межі простого антивірусу та фаєрвола. Вони зосереджені на побудові багаторівневої, адаптивної та проактивної оборони. Ключові концепції включають багаторівневий захист, модель Zero Trust та використання систем виявлення/запобігання вторгненням (IDS/IPS), використання системи управління інформацією та подіями безпеки (SIEM), використання аналізу поведінки користувачів і об'єктів (UEBA) та використання центру управління безпекою (SOC) [17,18,19].

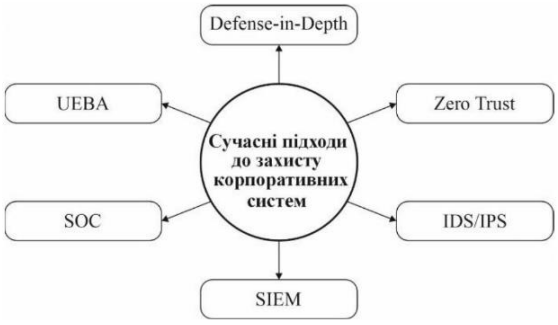


Рис. 3. Сучасні підходи до захисту корпоративних систем

Багаторівневим захистом (Defense-in-Depth) є стратегія, що передбачає використання декількох шарів захисту, щоб у разі злому одного шару інші залишалися ефективними. Кожен шар допомагає уповільнити атаку та надає системі час для виявлення та реагування. Цими шарами можуть бути фізичний захист (замки, охорона,

відеоспостереження, обмеження доступу до серверних приміщень), мережевий захист (фаєрволи, сегментація мережі, VPN), захист хостів (антивірусне програмне забезпечення, персональні фаєрволи, системи виявлення загроз на кінцевих точках (EDR)), захист даних (шифрування даних під час зберігання та передачі) та організаційні заходи (політика безпеки, навчання персоналу, регулярні аудити) [9,11,15,16].

Сучасні підходи до кібербезпеки будуються на трьох принципах: запобігати, виявляти та реагувати на загрози. Це означає, що недостатньо просто встановити захист, потрібно постійно його перевіряти. Такий підхід вимагає, щоб захист був комплексним. Це включає не тільки технічні інструменти, а й освіту працівників та постійне управління ризиками. Лише постійно оновлюючи ці методи, можна ефективно боротися з найскладнішими сучасними кіберзагрозами [9,11,12,13,15].

Більшість організацій мають розрізнені засоби безпеки: окремо моніторинг, окремо копії даних, окремо інцидент-респонс. Немає узгодженого механізму, який би автоматично оцінював ризик, запускав потрібні дії та контролював відновлення. Слабке місце — відсутність інтегрованого циклу. Детекція не завжди автоматично переходить у реагування, а відновлення часто запускається вручну і не прив'язане до оцінки ризику. Запропонований метод якраз «зшиває» ці частини в одну керовану послідовність.

Основна частина

Формальні моделі загроз, сценаріїв атак, засобів захисту корпоративних ІС це є структуровані підходи, які допомагають компаніям систематично ідентифікувати, аналізувати та протидіяти комплексним кіберзагрозам. Вони дозволяють перетворити абстрактні ризики на конкретні, зрозумілі дії. Дані моделі є важливим елементом проактивного захисту, оскільки дають змогу не чекати атаки, а прогнозувати її можливий розвиток і заздалегідь підготувати засоби для оборони.

На етапі розвідки зловмисник пасивно збирає інформацію про ціль, не вступаючи в пряму взаємодію з її системами. На етапі озброєння зловмисник створює інструмент для атаки. На етапі доставки зловмисник передає створений інструмент до цілі. Після доставки зловмисник використовує вразливість у системі, щоб виконати шкідливий код (етап експлуатації). На етапі встановлення відбувається встановлення постійних присутності в системі для довгострокового доступу. На етапі командування та контролю хакер встановлює канал зв'язку зі своїм програмним забезпеченням. І фінальним етапом (дії за ціллю) є момент досягання зловмисником своєї кінцевої мети (викрадення даних, саботаж чи фінансова вигода) [25,26,27]. Cyber Kill Chain є ключовою моделлю для розуміння того, як відбуваються кібератаки та як від них захиститися. Попри деякі обмеження, вона добре адаптується до сучасних загроз. Завдяки інтеграції з новими інструментами, як MITRE ATT&CK, компанії можуть ефективно протистояти атакам, що постійно змінюються.

MITRE ATT&CK, є не зовсім традиційною моделлю сценарів атак, а більше базою знань, яка допомагає фахівцям з кібербезпеки створювати реалістичні сценарії атак. MITRE ATT&CK є більш деталізованою та гнучкою моделлю в порівнянні з Cyber Kill Chain. Також MITRE ATT&CK є фреймворком. MITRE ATT&CK надає детальний, нелінійний огляд конкретних технік, які зловмисник може використати в будь-який момент атаки. Тобто ця база масивно каталогізує тактику, методи та процедури кіберзлочинців на кожному етапі життєвого циклу кібератаки (від початкового збору інформації та планування дій зловмисника до остаточного виконання атаки). Дана система складається з двох основних елементів: тактики та техніки. Тактики представляють цілі зловмисника на високому рівні, наприклад, початковий доступ, виконання, закріплення та переміщення по мережі. Техніки описують конкретні методи (наприклад, технікою для тактики "Початковий доступ" може бути "Фішинг"), які зловмисник використовує для досягнення тактичної мети. Фреймворк також включає субтехніки для більш детального опису та процедури, які є реальними прикладами того, як конкретні хакери реалізують ці техніки. MITRE ATT&CK організований у вигляді матриці. Матриця MITRE ATT&CK розділена на три основні частини, що відповідають різним сферам атак. Матриця

підприємства охоплює методи атак на корпоративну інфраструктуру, включаючи операційні системи (Windows, MacOS, Linux), хмарні сервіси та контейнерні технології. Вона також містить матрицю підготовчих технік, що використовуються перед атакою. Мобільна матриця зосереджена на атаках, спрямованих на мобільні пристрої, а також на мережевих атаках, які їх використовують. Вона розділена на окремі підматриці для платформ iOS та Android. Матриця ICS (Industrial Control Systems) включає методи атак на промислові системи управління. Ці атаки спрямовані на обладнання та мережі, що використовуються для автоматизації заводів, комунальних послуг та інших критично важливих об'єктів. MITRE ATT&CK підтримує низку заходів та технологій (сортування сповіщень, виявлення загроз та реагування; полювання на загрози; аналіз прогалин у безпеці та оцінка зрілості Центру операцій безпеки (SOC); емуляція зловмисників), які організації використовують для оптимізації своїх операцій безпеки та покращення загального стану безпеки [23, 24].

Таким чином, є досить багато різних моделей загроз та сценаріїв атак й засобів захисту корпоративних ІС від комплексних кіберзагроз. Головне є те як їх буде застосовано, адже вони між собою зв’язані, і є багато прикладів як одна іншу вдало доповнює. Це є дуже важливим аспектом через те що загрози розвиваються, і відповідно потрібні досить гнучкі підходи для кібербезпеки.

Дуже важливою є оцінка ефективності захисту корпоративних ІС. Це дозволяє чітко оцінити захист систем, щоб зрозуміти чи є достатніми заходи щодо захисту інформаційних систем. І якщо захист є недостатнім, то потрібно буде його покращувати. Ефективність захисту корпоративних ІС від комплексних кіберзагроз вимірюється за допомогою комбінації кількісних і якісних показників, які показують здатність системи запобігати, виявляти, реагувати та відновлюватися після інцидентів. Ці показники допомагають оцінити поточний стан кібербезпеки, виявити слабкі місця та обґрунтувати інвестиції в захисті [24,26,27].

Якісні показники ґрунтуються на експертних оцінках і аудитах, вони допомагають оцінити готовність організації до комплексних загроз. Якісні показники не є чіткими, які можна виміряти, а є суб’єктивною оцінкою. Попри все, оцінка через якісні показники є дуже важливою частиною загальної оцінки. До якісних показників можна віднести результати пентестів (тестування на проникнення), рівень обізнаності співробітників та відповідність стандартам. Тестування на проникнення потрібне для ефективного оцінювання захисту і відбувається через імітацію реальної кібератаки. Даний показник є один з найважливіших тому, що при наявності добре обізнаних співробітників з кібербезпекою, компанія суттєво підвищує всю безпеку.

Показник відповідності стандартам є також важливим, оскільки вказує на ступінь дотримання різних стандартів з кібербезпеки (наприклад, ISO 27001, NIST). Цей показник не тільки допомагає підігнати рівень безпеки під стандарти визначенні спеціалістами, а й несе репутаційний вплив на компанію, показує на якому рівні знаходиться компанія в плані кібербезпеки [25,26,27].

Наступний тип показників є кількісні показники, ці показники є об'єктивними, і їх можна вимірювати та відстежувати. Такі показники кібербезпеки різняться від кількості заблокованих спроб порушення до швидкості реагування організації на інциденти. Першим показником є (еталон для оцінки надійності), середній час між збоями (MTBF). Взагальному, цей показник показує середній часовий інтервал, який відбувся між двома послідовними збоями системи чи її компонента. Другим показником є середній час до виявлення (MTTD). Показник вимірює середню тривалість часу, необхідну для виявлення потенційного інциденту. оцінює, наскільки ефективно і швидко системи можуть виявляти загрози. Чим коротший MTTD, тим швидше виявлення, що дозволяє оперативніше реагувати на ризики. Третім показником є середній час до підтвердження (MTTA). MTTA вимірює середню тривалість між початковим виявленням інциденту та його офіційним підтвердженням або реєстрацією. Показник є критично важливим, показує рівень готовності почати вирішення проблем безпеки. Четвертим показником є середній час до локалізації (MTTC). Показник відображає, наскільки швидко можна ізолювати та усунути загрозу, мінімізуючи її потенційну шкоду. MTTC оцінює ефективність процедур локалізації інцидентів. П’ятим показником

є середній час до вирішення (MTTR). Даний показник вимірює, наскільки швидко організація може виявити, відреагувати та повністю відновитися після інциденту, оцінює ефективність та швидкість в усуненні загроз та відновленні після них. Наступним, шостим, показником є час на виправлення (Days to patch), що вказує на швидкість усунення вразливостей. Сьомим показником є ефективність запобігання втраті даних (DLP). Даний показник оцінює здатність системи запобігати несанкціонованому доступу або витоку даних. Показник вказує кількісну оцінку ефективності DLP-системи (Data Loss Prevention) через співвідношення успішно зупинених інцидентів до загальної кількості спроб. Восьмим показником є кількість спроб вторгнення. Даний показник показує кількість спроб зловмисників зламати мережі організації, надає представлення про рівень інтересу з боку кіберзлочинців та допомагає оцінити стійкість заходів кібербезпеки [15,16,17].

Взагальному, щоб комплексно оцінити ефективність захисту необхідно аналізувати ці показники разом, оскільки вони доповнюють один одного, надаючи повну картину стану кібербезпеки організації.

Модель функціонування корпоративної ІС можна відобразити при використанні марківських моделей. Марківські моделі є стохастичними моделями у теорії ймовірностей. Взагальному стохастичні моделі враховують випадковість з одною або більше випадкових величин. Стохастичні моделі допомагають передбачати чи пояснювати явища в моментах де результат не завжди однаковий, навіть при схожих умовах. Головною суттю марківських моделей це є використання марківських процесів (випадкові процеси без післядії), це означає, що в деякій системі S з дискретними станами $S_1, S_2, S_3 \ldots$ в будь-який моменту часу ймовірність будь-яких майбутніх станів системи залежить від її стану в теперішньому і не залежить від того як і скільки часу розвивався поточний випадковий процес (марківський процес) в минулому.

Для більшості практичних випадків процес функціонування корпоративної інформаційної системи в умовах комплексних деструктивних інформаційних впливів пропонується формалізувати у вигляді графа станів на рис. 4.

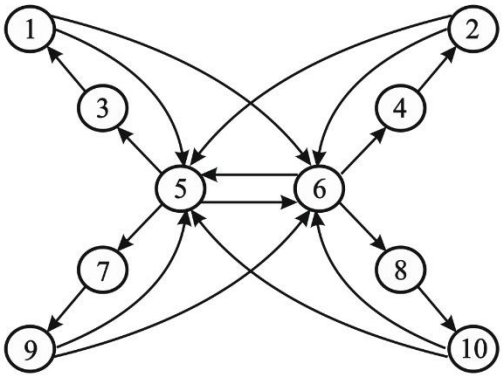


Рис. 4. Модель функціонування захищеної КІС

Вершини графа позначають стани процесу, дуги - переходи з одних станів в інші. Виділяються 10 станів ($S_1 \ldots S_{10}$) розглянутого процесу, які перераховуються в табл. 1. Відмінності цих станів полягають в умовах, у яких функціонує система в заданий момент часу. Наведена множина станів є повною групою подій. Переходи між станами, показані на рис.4, визначаються на основі характеру аналізованого процесу.

Переходи $S_5. \to S_6, S_6. \to S_5$ можуть відбуватися при посиленні чи ослабленні активності зловмисників, реконфігурації системи, зміні її контрагентів, а також модифікації інших умов функціонування системи. Зміна цих умов суттєво впливає на процеси актуалізації та деактуалізації загроз.

Беручи до уваги потоковий характер, властивий процесам функціонування КІС, а також орієнтуючись на граничну теорему для сумарних потоків, розглянутому вище графу відповідає система з 10 лінійних диференційних рівнянь. Кожне з рівнянь описує залежність ймовірностей знаходження системи у відповідному стані $S_1 ... S_{10}$ від часу та інтенсивностей переходів λ_{ij} з одних станів до інших.

Таблиця 1

Стан процесу функціонування системи

Номер стану	Умови функціонування
1	Реалізація захисних заходів для усунення виявленої загрози
2	Коректна оцінка ситуації за відсутності загрози
3	Отримання справжньої інормації про наявність загрози
4	Отримання справжньої інормації про відсутність загрози
5	Відсутність інформації про загрози за наявності загрози
6	Відсутність інформації про загрози за відсутності загрози
7	Пропуск загрози за її наявності
8	Хибне розпізнавання загрози за її відсутності (хибна тривога)
9	Сприйняття неправдивої інформації як істинної
10	Реалізація помилкових заходів захисту за відсутності загрози

Рішення конкретної системи рівнянь дозволяє розраховувати ймовірності, знаходження системи на момент часу, що цікавить, у можливих станах при захисті від конкретної загрози за допомогою конкретної програми захисту PRG_k. Якщо інтенсивності переходів та початкові умови відомі, система диференціальних рівнянь легко вирішується відомими методами чисельно чи аналітично. Розпізнавання актуального стану системи визначення початкових умов може виконуватися модулем аналізу ефектів системи захисту. Крім того, для кожного типу загроз і програм захисту, модель матиме свої початкові значення та параметри. За наявності можливості розпізнавання актуального стану системи та відомих інтенсивностях λ_{ij} поява загроз може бути передбачена.

Алгоритм оцінювання ефективності захисту КІС за інтегральним показником із застосуванням розробленої марківської моделі включає наступні кроки:

1. Розрахунок ймовірностей $P_z^*(t), P_{zk}(PRG_k, t)$ знаходження КІС у виділених станах без застосування заходів захисту та з цими заходами на заданий момент часу.

2. Оцінювання $t_z^*(t)$ і $t_{zk}(PRG_k)$ сумарного часу знаходження КІС у станах $S_z \in \{S_1 ... S_{10}\}$ у разі відсутності та реалізації захисної програми PRG_k (1):

$$t_z^k = \int_0^T P_z(t)dt,\ t_{zk}(PRG_k) = \int_0^T P_{zk}(PRG_k, t)dt, \tag{1}$$

де $P_{zk}(PRG_k, t)$ означає ймовірність знаходження системи в стані z при реалізації цій захисної програми PRG_k; T – аналізований період часу.

3. Кожному стану z ставиться у відповідність величина ефекту V_z, пов'язана з показниками якості обслуговування, що доставляється користувачеві в одиницю часу.

4. Розраховуються сукупні ефекти $L^*, L(PRG_k)$ КІС без заходів захисту та з ними (2):

$$L^* = \sum_{z=1}^{Z} V_z \cdot t_z^*,\ L(PRG_k) = \sum_{z=1}^{Z} V_z \cdot t_{zk}(PRG_k), \tag{2}$$

де Z - Число всіх станів КІС. Слід врахувати, що значення ефектів V_z можуть бути як додатніми, так і від'ємними (за наявності шкоди). Враховуючи, що показники якості обслуговування залежать від часу, розрахунок сукупного ефекту може виконуватися за формулами (3,4):

$$L^* = \sum_{z=1}^{Z} L_z^*,\ L(PRG_k) = \sum_{z=1}^{Z} L_z(PRG_k) \tag{3}$$

$$L_z^* = \int_0^T V_z(t) P_z^*(t) dt,\ L_z(PRG_k) = \int_0^T V_z(t) P_{zk}(PRG_k, t) dt \tag{4}$$

5. Розрахунок приросту $\Delta L = L_z(PRG_k) - L_z^*$ ефективності КІС за рахунок реалізованих заходів захисту.

Пропонований метод оцінювання ефективності захисту корпоративних інформаційних систем від комплексних деструктивних впливів може бути використаний для широкого кола різних за призначенням і структурним особливостями КІС.

На основі розробленого методу запропоновано структуру системи захисту корпоративної інформаційної системи від деструктивних впливів. Структура системи наведено на рис. 5. Відмінна риса даної системи полягає в новій множині функціональних блоків і зв'язків між ними. Вона дозволяє підвищити здатність прикладної системи виявляти та усувати деструктивні інформаційні впливи в автоматичному режимі.

Задача системи – забезпечення високої адаптивності від гетерогенних деструктивних інформаційних впливів на комп'ютерні мережі, зокрема – мережевих атак. Адаптація системи до актуальних умов функціонування виконується за допомогою її реконфігурування. Реконфігурування передбачає підналаштування блоків системи до поточної ситуації, а також вибір відповідних методів захисту.

У процесі конфігурування системи захисту визначається склад застосовуваних методів та систем захисту, а також їх параметри. Конфігурування повинно виконуватися з урахуванням як активних, так і можливих загроз, а також стану системи, що захищається. У загальному випадку необхідно вирішувати оптимізаційну задачу для знаходження відповідного способу захисту від розглянутих загроз.

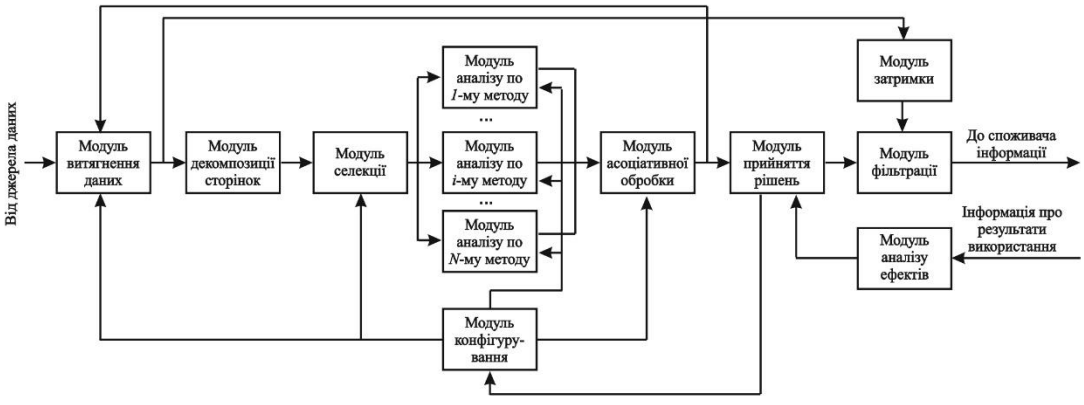


Рис. 5. Структура системи захисту корпоративної інформаційної системи від деструктивних впливів

Для оптимізації такої конфігурації потрібно знайти оптимальну програму PRG_{opt} для конфігурації системи захисту від вибраних загроз, при реалізації якої досягається максимум сукупного ефекту $L_{opt}(PRG_{opt})$ на інтервалі часу $[0;T]$ (5):

$$L_{opt}(PRG_{opt}) = \max_{k} \sum_{z=1}^{Z} \int_{0}^{T} V_z(t) P_{zk}\left(PRG_k, k\right) dt \tag{5}$$

при наступних обмеженнях: $t_k(PRG_k) \le t_D, PRG_k \in R, z = \overline{1,Z}, k = \overline{1,K}$,

де R - кінцева множина результативних програм конфігурації системи захисту (програма, яка досягає мети за кінцеве число кроків); K – кількість програм у множині R; Z – кількість станів у моделі системи, що захищається; $V_z(t)$ – ефект, що досягається системою в момент часу t за умови, що система перебуває у стані z; $P_{zk}\left(PRG_k, t\right)$ – ймовірність знаходження системи, що захищається, в стані z в момент часу t за умови, що програма PRG_k реалізована; T – інтервал часу, протягом якого оцінюються сукупні ефекти; $t_k(PRG_k)$ - час виконання програми PRG_k; t_D – максимально допустимий час виконання програми.

Ця модель передбачає, що пошук оптимальної програми PRG_{opt} для конфігурації системи захисту може виконуватися лише на багатьох програмах, які відповідають наведеним обмеженням. Врахування цих обмежень істотно скорочує складність завдання.

Алгоритм вирішення сформульованої задачі пошуку оптимальної програми PRG_{opt} складається з наступних кроків:

1. Визначення початкових даних - T, Z, K, t_D, множин $V_z(t)$, $P_{zk}\left(t=0\right)$, PRG_k, $t_k(PRG_k)$, λ_{ijk} – інтенсивностей переходу в марківській моделі процесу, що захищається після реалізації конфігураційної програми PRG_k. Встановлення початкових значень: $k = 0$, $L_{opt} = 0$.

2. $k = k + 1$; $z = 0$; $L_k = 0$.

3. Якщо $k > K$, перейти до кроку 16.

4. Вибрати k- альтернативну програму з множини PRG_k.

5. Перевірити умову: $PRG_k \in R$. Якщо умова не виконується, перейти кроку 2.

6. Перевірити умову: $t_k(PRG_k) \le t_D$. Якщо умова не виконується, перейти до кроку 2.

7. Вибрати відповідні програмі PRG_k інтенсивності переходів λ_{ijk}.

8. $z = z + 1$.

9. Якщо $z > Z$, перейти до кроку 14.

10. Обчислити значення $P_{zk}\left(PRG_k, t\right)$

11. Обчислити $L_{kz} = \int_{0}^{T} V_z\left(t\right) P_{zk}\left(PRG_k, t\right) dt$

12. $L_k = L_k + L_{kz}$

13. Перейти до кроку 8.

14. Якщо $L_{opt} < L_k, L_{opt} = L_k, PRG_{opt} = PRG_k$.

15. Перейти до кроку2.

16. Вибрати програму PRG_{opt} на виконання.

Для великої кількості альтернативних програм повний пошук може бути замінений відомими методами оптимізації, наприклад, методом гілок та кордонів тощо.

Алгоритм адаптивного захисту КІС від інформаційних загроз наведений на рис. 6.

Рис. 6. Алгоритм адаптивного захисту від інформаційних загроз

Розглянутий метод оптимізації конфігурації системи захисту корпоративної інформаційної системи відрізняється від інших відомих рішень новим набором правил, що дозволяють реалізовувати адаптивний захист від інформаційних загроз. Реконфігурування системи захисту має виконуватися з метою досягнення максимального зростання сукупного ефекту або мінімальної шкоди в рамках заданого часового інтервалу з обмеженнями на час пошуку та реалізації керуючої програми.

Таким чином, запропонований метод адаптивного захисту корпоративної інформаційної системи від деструктивних впливів орієнтований на нову архітектуру системи захисту корпоративної інформаційної системи від деструктивних впливів. В його основі лежить розроблений алгоритм адаптивного захисту (рис. 6), а також метод оптимізації конфігурації системи такого захисту. Метод дозволяє розширити можливості систем захисту з виявлення та усунення деструктивних впливів.

Алгоритм оцінки ризику (RiskScore) включає наступні кроки:

1. Вхід: подія/інцидент, критичність сервісу, контекст користувача.
2. Нормалізувати подію (джерело, час, об’єкт впливу).
3. Призначити базовий бал загрози (за типом події).
4. Модифікувати бал з урахуванням критичності активу.
5. Врахувати наявність дублюючих контролів (зменшення ризику).
6. Рівень ризику {LOW, MED, HIGH} і бал [0;1].
7. Вибір плейбука (PlaybookSelect)
    7.1. Якщо ризик HIGH → обрати «жорсткий» плейбук (ізоляція, блокування, MFA reset).
    7.2. Якщо MED → «помірний» (посилення політик, збір форензіки, обмеження доступу).
    7.3. Якщо LOW → «спостереження/перевірка» (логування, сповіщення, відкладені дії).
8. Відновлення (ControlledRecover)
    8.1. Перевірка цілісності конфігурацій і даних.
    8.2. Відновлення з репліки/бекапу (тільки після ізоляції).
    8.3. Перевірка прикладних тестів (smoke/health-check).
    8.4. Повернення вузла в продуктивний сегмент.
    8.5. Підтвердження бізнес-власника сервісу.
9. Кінець

Архітектура системи адаптивного захисту корпоративної інформаційної системи від комплексних деструктивних інформаційних впливів, відрізняється новою сукупністю пов'язаних блоків збору, передобробки та аналізу даних та вибору контрзаходів для захисту від мережевих атак та інших деструктивних впливів, що дозволяє розширити функціональні можливості такого захисту.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

Запропоновано метод забезпечення стійкості корпоративних інформаційних систем до комплексних кіберзагроз, який поєднує моніторинг, оцінювання ризику, адаптивне реагування та відновлення в єдиний керований цикл. Подано просту формулу інтегральної оцінки стійкості, референтну архітектуру, алгоритми і практичні кроки впровадження. Експериментальна перевірка показала скорочення MTTD і MTTR, а також зростання індексу стійкості. Метод придатний для організацій різного масштабу та може впроваджуватися поступово, починаючи з критичних сервісів.

Розроблені методи дозволяють кількісно оцінювати процеси, що протікають в КІС, що захищаються. Запропоновані моделі та методи можуть бути застосовані для високорівневої формалізації процесів функціонування корпоративних інформаційних систем на виробничих підприємствах, у соціальних установах, транспортних об'єктах,

моллах, і т. д. Подібні моделі та методи можуть також успішно застосовуватися в завданнях планування та вибору контрзаходів для протидії загрозам у мережах цих організацій. Ця можливість може бути обґрунтована коректністю вихідних передумов, відповідністю результатів моделювання загальним закономірностям.

Подальші дослідження включають побудову приватних моделей, що відображають процеси, що протікають у сервісах КІС в умовах загроз. Також передбачається розвиток методів, що дозволяють визначати склад заходів захисту, у тому числі – формалізація захисних програм для конкретних умов функціонування КІС, аналіз та вибір найбільш ефективних методів оптимізації для пошуку захисних програм, що забезпечують кращі значення показників функціонування КІС.

Літертура

1. Корпоративна інформаційна система. URL: https://uk.wikipedia.org/wiki/ Корпоративна інформаційна система (дата звернення: 08.09.2025).

2. A technology survival guide for resilience. URL: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/a-technology-survival-guide-for-resilience (дата звернення: 09.09.2025).

3. Додонов О. Г., Кузнєцова М. Г., Горбачик О. С. Моделювання і оцінювання функціональної стійкості інформаційних систем. *Методи захисту інформації у комп'ютерних системах і мережах.* Київ, 2025. С. 77–82.

4. Аналіз побудови інтелектуальної інформаційної системи на основі поняття функціональної стійкості. / М. Ю. Миронюк та ін. *Зв'язок*. 2024. №1. С. 3–8.

5. Lakshmi Goel, Dawn Russell, Steven Williamson. Information systems security resilience as a dynamic capability. *Journal of Enterprise Information Management*. 2023. Vol. 36, № 4. P. 906–924. URL: https://doi.org/10.1108/JEIM-07-2022-0228 (дата звернення: 09.09.2025).

6. Кібератака. URL: https://uk.wikipedia.org/wiki/ Кібератака (дата звернення: 09.09.2025).

7. Давиденко Є. А. Корпоративна безпека на українських підприємствах в умовах війни. *Економіка та суспільство*. 2023. № 58. С. 2–6.

8. Основи Кібербезпеки для бізнесу. URL: https://westelecom.ua/blog/osnovy-kiberbezopasnosti-dla-biznesa (дата звернення: 09.09.2025).

9. Комплексний погляд на кібератаки. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-a-cyberattack (дата звернення: 09.09.2025).

10. Різні типи кібератак та як не стати їх жертвою. URL: https://nordvpn.com/uk/blog/shcho-take-kiberataka/?srsltid=AfmBOoqlIfwpKtKr4GXDnwlrVkLpEH813XSEN41WC44rfi2_VqSRkZrz (дата звернення: 09.09.2025).

11. Комплексна система захисту інформації – що це? URL: https://hostpark.ua/news-ua/kompleksna-systema-zahystu-informacziyi-shho-cze/ (дата звернення: 10.09.2025).

12. Захист корпоративних мереж від загроз: засоби та методи. URL: https://netwave.ua/blog/zahist-korporativnih-merezh-vid-zagroz-zasobi-ta-metodi/ (дата звернення: 10.09.2025).

13. В. Б. Дудикевич, Г. В. Микитин, Т. Є. Мурак. Комплексна система безпеки регіональної корпоративної мережі на основі еталонної моделі osi та моделі "Глибокого захисту". *Computer systems and networks*. 2025. Vol. 7, № 1. P. 124–126.

14. Мехед Д. Аналіз вразливостей корпоративних інформаційних систем / Д. Мехед, Ю. Ткач, В. Базилевич, В. Гур'єв, Я. Усов // Захист інформації. 2018. Т. 20, № 1. С. 61-66. URL: http://nbuv.gov.ua/UJRN/Zi_2018_20_1_10 (дата звернення: 10.09.2025).

15. Defense in Depth: багаторівневий підхід до захисту інформації. URL: https://avolutech.com/blog/defense-in-depth-багаторівневий-підхід-до-захисту/ (дата звернення: 10.09.2025).

16. Zero Trust: Модель кібербезпеки, яка не вірить нікому – і саме тому рятує бізнес. URL: https://my-itspecialist.com/zero-trust-model-kyberbezpeky (дата звернення: 10.09.2025).

17. Що таке IPS/IDS і де застосовується. URL: https://www.hostzealot.com.ua/blog/about-solutions/shho-take-ipsids-i-de-zastosovujetsya (дата звернення: 10.09.2025).

18. Порівняння та вибір стандарту кібербезпеки URL: https://www.oksim.ua/porivnyannya-ta-vibir-standartu-kiberbezpeki/ (дата звернення: 10.09.2025).

19. Основні переваги сертифікації ISO/IEC 27001. URL: https://www.issp.training/post/osnovni-perevahy-sertyfikatsiyi-iso-iec-27001 (дата звернення: 10.09.2025).

20.What is the Plan-Do-Check-Act (PDCA) Cycle? URL: https://asq.org/quality-resources/pdca-cycle?srsltid=AfmBOorjsGZ3ClVTu2cM1OsZDFM708DI47GQxdLkVsEF2adyAQqEpajD (дата звернення: 10.09.2025).

21. Що таке моделювання загроз і якими є його переваги? URL: https://www.issp.training/post/shcho-take-modelyuvannya-zahroz-i-yakymy-ye-yoho-perevahy (дата звернення: 16.09.2025).

22. What Is the STRIDE Threat Model? Beginner's Guide – 2025. URL: https://www.practical-devsecops.com/what-is-stride-threat-model/?srsltid=AfmBOooFRj5W_pOW2pZZMyk07BI-58z25VHsPzTOBjdwUMXr7c9ErIzH (дата звернення: 17.09.2025).

23. DREAD Threat Modeling. URL: https://threat-modeling.com/dread-threat-modeling/ (дата звернення: 17.09.2025).

24. Guide to Threat Modeling using Attack Trees. URL: https://www.practical-devsecops.com/threat-modeling-using-attack-trees/?srsltid=AfmBOooQk_TLjGOcctG8OZsLF7rWu-gabZ8AA3sU5JTgSQxwTQpRbUrT (дата звернення: 17.09.2025).

25. Cyber Kill Chain: Сучасні Загрози та Інструменти Протидії. URL: https://itorakul.com.ua/cyber-kill-chain/ (дата звернення: 17.09.2025).

26. Моделювання загроз за допомогою MITER ATT&CK Framework. URL: https://www.hostragons.com/uk/блог/моделювання-загроз-інфраструктури-mitre-attac/ (дата звернення: 17.09.2025).

27. Cybersecurity Metrics & KPIs: What to Track in 2025. URL: https://www.sentinelone.com/cybersecurity-101/cybersecurity/cybersecurity-metrics/ (дата звернення: 23.09.2025).

References

1. Korporatyvna informatsiina systema. URL: https://uk.wikipedia.org/wiki/ Korporatyvna informatsiina systema (data zvernennia: 08.09.2025).

2. A technology survival guide for resilience. URL: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/a-technology-survival-guide-for-resilience (data zvernennia: 09.09.2025).

3. Dodonov O. H., Kuznietsova M. H., Horbachyk O. S. Modeliuvannia i otsiniuvannia funktsionalnoi stiikosti informatsiinykh system. Metody zakhystu informatsii u kompiuternykh systemakh i merezhakh. Kyiv, 2025. C. 77–82.

4. Analiz pobudovy intelektualnoi informatsiinoi systemy na osnovi poniattia funktsionalnoi stiikosti. / M. Yu. Myroniuk ta in. Zviazok. 2024. №1. S. 3–8.

5. Lakshmi Goel, Dawn Russell, Steven Williamson. Information systems security resilience as a dynamic capability. Journal of Enterprise Information Management. 2023. Vol. 36, № 4. P. 906–924. URL: https://doi.org/10.1108/JEIM-07-2022-0228 (data zvernennia: 09.09.2025).

6. Kiberataka. URL: https://uk.wikipedia.org/wiki/ Kiberataka (data zvernennia: 09.09.2025).

7. Davydenko Ye. A. Korporatyvna bezpeka na ukrainskykh pidpryiemstvakh v umovakh viiny. Ekonomika ta suspilstvo. 2023. № 58. C. 2–6.

8. Osnovy Kiberbezpeky dlia biznesu. URL: https://westelecom.ua/blog/osnovy-kiberbezopasnosti-dla-biznesa (data zvernennia: 09.09.2025).

9. Kompleksnyi pohliad na kiberataky. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-a-cyberattack (data zvernennia: 09.09.2025).

10. Rizni typy kiberatak ta yak ne staty yikh zhertvoiu. URL: https://nordvpn.com/uk/blog/shcho-take-kiberataka/?srsltid=AfmBOoqlIfwpKtKr4GXDnwlrVkLpEH813XSEN41WC44rfi2_VqSRkZrz (data zvernennia: 09.09.2025).

11. Kompleksna systema zakhystu informatsii – shcho tse? URL: https://hostpark.ua/news-ua/kompleksna-systema-zahystu-informacziyi-shho-cze/ (data zvernennia: 10.09.2025).

12. Zakhyst korporatyvnykh merezh vid zahroz: zasoby ta metody. URL: https://netwave.ua/blog/zahist-korporativnih-merezh-vid-zagroz-zasobi-ta-metodi/ (data zvernennia: 10.09.2025).

13. V. B. Dudykevych, H. V. Mykytyn, T. Ye. Murak. Kompleksna systema bezpeky rehionalnoi korporatyvnoi merezhi na osnovi etalonnoi modeli osi ta modeli "Hlybokoho zakhystu". Computer systems and networks. 2025. Vol. 7, № 1. P. 124–126.

14. Mekhed D. Analiz vrazlyvostei korporatyvnykh informatsiinykh system / D. Mekhed, Yu. Tkach, V. Bazylevych, V. Huriev, Ya. Usov // Zakhyst informatsii. 2018. T. 20, № 1. S. 61-66. URL: http://nbuv.gov.ua/UJRN/Zi_2018_20_1_10 (data zvernennia: 10.09.2025).

15. Defense in Depth: bahatorivnevyi pidkhid do zakhystu informatsii. URL: https://avolutech.com/blog/defense-in-depth-bahatorivnevyi-pidkhid-do-zakhystu/ (data zvernennia: 10.09.2025).

16. Zero Trust: Model kiberbezpeky, yaka ne viryt nikomu – i same tomu riatuie biznes. URL: https://my-itspecialist.com/zero-trust-model-kyberbezpeky (data zvernennia: 10.09.2025).

17. Shcho take IPS/IDS i de zastosovuietsia. URL: https://www.hostzealot.com.ua/blog/about-solutions/shho-take-ipsids-i-de-zastosovujetsya (data zvernennia: 10.09.2025).

18. Porivniannia ta vybir standartu kiberbezpeky URL: https://www.oksim.ua/porivnyannya-ta-vibir-standartu-kiberbezpeki/ (data zvernennia: 10.09.2025).

19. Osnovni perevahy sertyfikatsii ISO/IEC 27001. URL: https://www.issp.training/post/osnovni-perevahy-sertyfikatsiyi-iso-iec-27001 (data zvernennia: 10.09.2025).

20.What is the Plan-Do-Check-Act (PDCA) Cycle? URL: https://asq.org/quality-resources/pdca-cycle?srsltid=AfmBOorjsGZ3ClVTu2cM1OsZDFM708DI47GQxdLkVsEF2adyAQqEpajD (data zvernennia: 10.09.2025).

21. Shcho take modeliuvannia zahroz i yakymy ye yoho perevahy? URL: https://www.issp.training/post/shcho-take-modelyuvannya-zahroz-i-yakymy-ye-yoho-perevahy (data zvernennia: 16.09.2025).

22. What Is the STRIDE Threat Model? Beginners Guide – 2025. URL: https://www.practical-devsecops.com/what-is-stride-threat-model/?srsltid=AfmBOooFRj5W_pOW2pZZMyk07BI-58z25VHsPzTOBjdwUMXr7e9ErIzH (data zvernennia: 17.09.2025).

23. DREAD Threat Modeling. URL: https://threat-modeling.com/dread-threat-modeling/ (data zvernennia: 17.09.2025).

24. Guide to Threat Modeling using Attack Trees. URL: https://www.practical-devsecops.com/threat-modeling-using-attack-trees/?srsltid=AfmBOooQk_TLjGOcetG8OZsLF7rWu-gabZ8AA3sU5JTgSQxwTQpRbUrT (data zvernennia: 17.09.2025).

25. Cyber Kill Chain: Suchasni Zahrozy ta Instrumenty Protydii. URL: https://itorakul.com.ua/cyber-kill-chain/ (data zvernennia: 17.09.2025).

26. Modeliuvannia zahroz za dopomohoiu MITER ATT&CK Framework. URL: https://www.hostragons.com/uk/bloh/modeliuvannia-zahroz-infrastruktury-mitre-attac/ (data zvernennia: 17.09.2025).

27. Cybersecurity Metrics & KPIs: What to Track in 2025. URL: https://www.sentinelone.com/cybersecurity-101/cybersecurity/cybersecurity-metrics/ (data zvernennia: 23.09.2025).

УДК 004.891

Чорненький С.В., Джулій В.М.

Хмельницький національний університет

МЕТОД ВЗАЄМОДІЇ КВАНТОВОЇ АПАРАТУРИ З КОРИСТУВАЛЬНИЦЬКИМИ СИСТЕМАМИ ЗАХИСТУ

В результаті проведеного аналізу виявлено проблеми, що виникають у процесі формування загальних секретів, при узгодженні послідовностей квантової мережі для системи захисту інформації та при передачі цих секретів. Запропоновано метод взаємодії квантової апаратури з користувальницькими системами захисту, уточнює процеси синхронізації ключів квантової мережі та їх передачі в систему захисту інформації.

As a result of the analysis, problems that arise in the process of forming shared secrets, when coordinating quantum network sequences for the information protection system and when transferring these secrets are identified. A method of interaction of quantum equipment with user protection systems is proposed, which clarifies the processes of synchronization of quantum network keys and their transfer to the information protection system.

Технологія квантового розподілу ключів – отримання ідентичних випадкових послідовностей абонентами, отриманих із використанням передачі між абонентами деякої інформації, з використанням квантових частинок. Абоненти використовують квантові пристрої, що реалізують протокол квантового розподілу ключів. Протокол квантового розподілу ключів включає: підготовку та перетворення інформаційних квантових станів в пристрої, який повинен мати джерело квантових станів; спосіб передачі квантовим каналом інформаційних квантових станів; спосіб інтерпретації, реєстрації та перетворення результатів вимірювань на з'єднаному пристрої; спосіб обробки отриманої за результатами вимірювань, послідовності, із застосуванням відкритого автентифікованого каналу зв'язку [1,2,3].

Результатом роботи протоколу квантового розподілу ключів є отримання секретного квантового ключа, ідентичного на обох вузлах мережі квантового каналу. Квантовий комплекс, що реалізує протокол квантового розподілу ключів, є апаратура з двох пристроїв, з'єднаних квантовим каналом. Архітектура комплексу наведена на рисунку 1.

Клієнт квантового розподілу ключів містить джерело (генератор) одиночних фотонів. Під'єднаний пристрій, що містить приймач (детектор) одиночних фотонів, називають Сервер квантового розподілу ключів. Кожен із вузлів квантового каналу містить датчик випадкових чисел. Таким чином можна отримати випадкову істинну послідовність, з якої в подальшому буде формуватиметься квантовий секретний ключ.

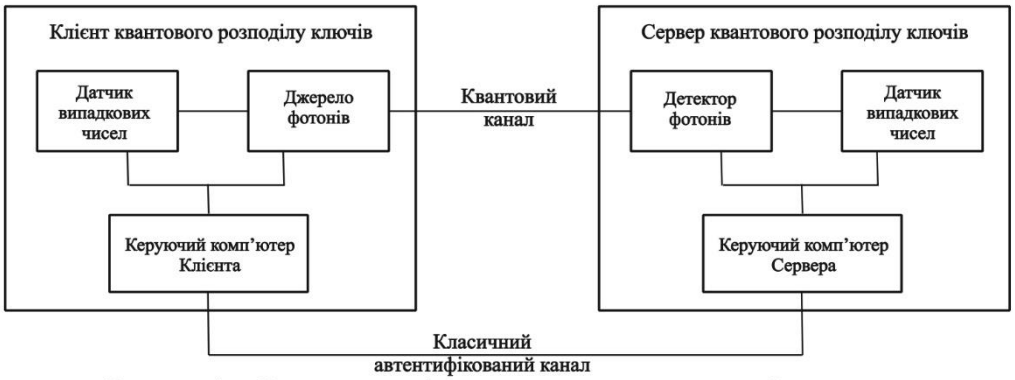


Рисунок 1 – Спрощена архітектура комплексу квантової апаратури

Сервер та Клієнт квантового розподілу ключів з'єднані двома логічними каналами: класичним та квантовим. Квантовий канал, зазвичай реалізується оптоволокном, призначений для передачі фотонів, квантових інформаційних станів. Існують системи квантового розподілу ключів, в яких використовується повітряне середовище передачі, як квантовий канал, проте вони знаходяться ще в стадії лабораторних розробок [2, 3, 4].

Системи квантового розподілу ключів мають граничну довжину квантового каналу, визначається протоколом квантового розподілу ключів. Пристрої користувача, для яких генеруються квантові ключі, можуть довільно розташовуватися, на відстанях, що перевищують допустиму довжину квантового каналу. Необхідно розглянути задачу розподілу квантових ключів для довільних пар пристроїв квантової мережі, що розташовані поза граничної довжини квантового каналу.

В результаті проведеного дослідження та аналізу виявлених недоліків пропонується структура комплексу квантової апаратури захисту інформації, наведена на рисунку 2. У запропонованому комплексі квантової апаратури використовується одна транспортна лінія зв'язку, яка з'єднує дві системи захисту інформації, два вузли квантової мережі системи квантового розподілу ключів.

Логічний канал системи квантового розподілу ключів передачі службових повідомлень складається з каналів передачі інформації: автентифікований канал передачі службової інформації з використанням квантових ключів мережі та квантових ключів із приймального вузла квантової мережі системи квантового розподілу ключів з пов'язаною системою захисту інформації; автентифікований канал передачі користувальницької інформації з використанням квантових ключів мережі між системами захисту інформації; автентифікований канал передачі квантових ключів та службової інформації з використанням квантових ключів із передавального вузла квантової мережі системи квантового розподілення ключів з повязаною системою захисту інформації.

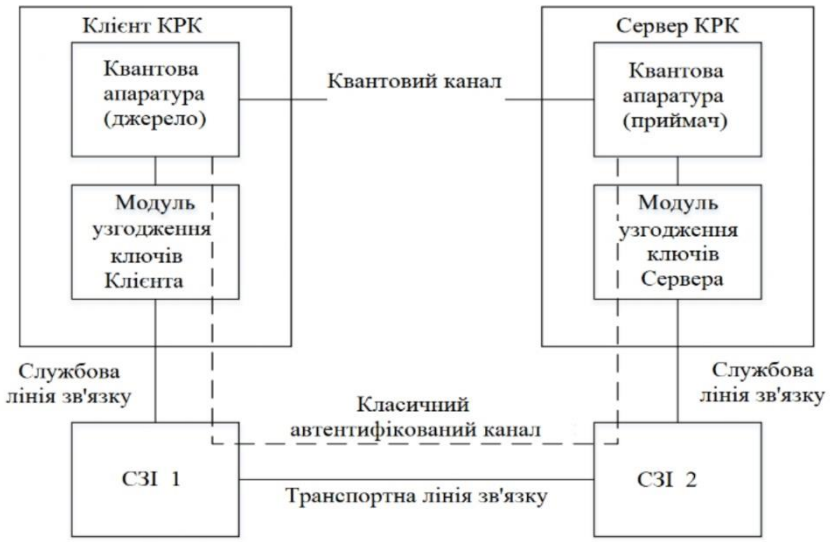


Рисунок 2 – Комплекс квантової апаратури захисту інформації

Таким чином, порівняно з розглянутими підходами, в запропонованому рішенні немає необхідності в окремому каналі мережі для обміну службовою інформацією вузлів системи квантового розподілення при генерації квантових ключів, використовується один канал для передачі зашифрованих даних користувача та службових повідомлень системи квантового розподілення ключів, в результаті знижуються витрати на розгортання, експлуатацію, створення комплексу.

У запропонованому комплексі квантової апаратури реалізовані додаткові модулі узгодження квантових ключів, що виконують функції формування квантових ключів мережі та накопичення випадкової послідовності. Після накопичення необхідної кількості ключів, формуються загальні секрети для системи захисту інформації та ключі для аутентифікації службової інформації системи квантового розподілення ключів, для передачі між Сервером та Клієнтом у процесі виконання протоколу квантового розподілення ключів (достатня кількість накопичених ключів квантової мережі - кількість квантових ключів, довжина яких більше сумарної довжини ключа аутентифікації та загального секрету, довжини ключів аутентифікації та загального секрету визначаються способом аутентифікації та застосовуваним алгоритмом шифрування системою захисту інформації).

Перед подальшим формуванням ключів аутентифікації та шифрування, за рахунок використання накопичення квантових ключів, досягається підвищення надійності комплексу квантової апаратури у випадку непередбачених збоїв системи квантового розподілення ключів (тимчасове припиненні генерації квантових ключів, атаки на квантовий канал зв'язку). У даній ситуації, згенеровані квантові

ключі зберігаються, після відновлення системи квантового розподілення ключів продовжується накопичення квантових ключів до згенерованих.

Пропонується на двох кінцях квантового канал, два варіанти контролю ідентичності квантових ключів в залежності від збоїв при роботі квантової апаратури.

У першому випадку, що випадкове повідомлення, отримане в результаті роботи протоколу квантового розподілення ключів ідентичне, формування квантових ключів з повідомлення відбувається без збоїв. Контроль цілісності передачі в систему захисту інформації від квантової апаратури проводиться безпосередньо засобами квантового каналу, через службову лінію зв'язку, і передача інформації, в даному випадку, захищена від випадкових спотворень. У такому підході можливе узгодження квантових ключів та їх ідентифікаторів шляхом порівняння. Якщо ідентифікатори не співпадають, то ключі видаляються (відкидаються). За рахунок порівняння ідентифікаторів переданих секретів у систему захисту інформації досягається підвищення надійності комплексу квантової апаратури у разі спотворень, які вносяться службовою лінією зв'язку.

Результатом запропонованого методу взаємодії квантової апаратури з користувальницькими системами захисту є:

1. Підвищення надійності комплексу квантової апаратури, у разі спотворень (навмисних, випадкових), які вносяться службовою лінією зв'язку; у разі виникнення короткочасних збоїв системи квантового розподілення ключів (припиненні генерації квантових ключів); у разі спотворень ідентифікаторів ключів.

2. Зниження витрат на експлуатацію, створення, розгортання комплексу за рахунок зменшення класичних ліній зв'язку.

3. Підвищення стійкості квантових ключів, згенерованих системою квантового розподілення ключів, за рахунок аутентифікації службової інформації системи розподілу на ключах аутентифікації, згенерованих з квантових ключів, та аутентифікації службової інформації системи квантового розподілення ключів, розбиття на блоки, при передачі по лінії зв'язку, та наступного шифрування службової інформації у транспортній лінії зв'язку між системами захисту інформації.

Перелік посилань

1. Доктрина інформаційної безпеки України, затвердженої Указом Президента України від 25 лютого 2017 року № №47/2017, 15с.
2. Квантова криптографія. Пояснення [Електронний ресурс] // Quantum Xchange. – 2019. – Режим доступу: https://quantumxc.com/blog/quantum-cryptography-explained/ (дата звернення 02.03.2025).
3. Satish Kumar. Quantum Cryptography [Електронний ресурс] // Tutorialspoint. – 2023. – Режим доступу: http://surl.li/fjebs (дата звернення 05.03.2025).
4. Грамблінг Е., Горовіц М. Квантові обчислення. Прогрес і перспективи. Вашингтон: Національні академії наук, техніки та медицини, 2019. 272 с.

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
здобувача вищої освіти
Чорненького Святослава Віталійовича
студента ФІТ, 2 курсу, групи КБЗІм-24-1

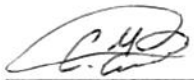
ЗАЯВА

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

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

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

08.12.2025р.
дата


підпис

Протокол аналізу звіту подібності науковим керівником

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

Автор: Чорненький Святослав Віталійович

Співавтор:

Назва: Метод забезпечення стійкості корпоративних інформаційних систем до комплексних кіберзагроз

Науковий керівник: Джулій Володимир Миколайович

Підрозділ: Кафедра кібербезпеки

Коефіцієнт подібності 1:1.6%

Коефіцієнт подібності 2:0.3%

Мікропробіли: 0

Заміна букв: 4

Інтервали: 0

Білі знаки: 0

Дата створення звіту: 2025-12-11 13:53:59.0

Після аналізу Звіту подібності констатую наступне:

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

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

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

Обгрунтування:

Дата 12.12.2025р. експерт

Anti-Plagiarism (UA) v-15.281 Educational

The maximum coincidence with one document 1.0%

Dictionaries check: en_US, ru_RU, ua_UA. **Errors in the documents: 7%**

	Document		Sum coincidence on the DB	
	Symbols	Lexemes	Symbols	Lexemes
ID: 252419 Title: Метод забезпечення стійкості корпоративних інформаційних систем до комплексних кіберзагроз Added in a DB: 2025-12-10 Authors: Чорненький Святослав Віталійович Heads: Джулій В.М. Consultants: Opponents:	112546	1742	1347 (1%)	16 (1%)

Plagiarism sources

ID	Description	Plagiarism presence in the document	
		Symbols	Lexemes

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Назва кваліфікаційної роботи: Метод забезпечення стійкості корпоративних інформаційних систем до комплексних кіберзагроз
Автор: Чорненький Святослав Віталійович
Освітня програма: Кібербезпека та захист інформації
Рівень вищої освіти: другий (магістерський)
Спеціальність: 125 – Кібербезпека та захист інформації
Науковий керівник: канд.техн.наук, доц. Джулій Володимир Миколайович
На основі аналізу кваліфікаційної роботи на дотримання вимог академічної доброчесності (у т.ч. відсутності ознак академічного плагіату) з урахуванням результатів перевірки роботи спеціалізованим програмним засобом(ами) комісія зробила такий висновок:

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

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою StrikePlagiarism складає 98,40%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism складає 99%.

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

Дата: 16.12.2025

Завідувач кафедри кібербезпеки _____ Юрій КЛЬОЦ

Гарант освітньої програми _____ Віра ТІТОВА

Керівник кваліфікаційної роботи _____ Володимир ДЖУЛІЙ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітньо-кваліфікаційного рівня «магістр»

Студент Чорненький Святослав Віталійович

Тема: «Метод забезпечення стійкості корпоративних інформаційних систем до комплексних кіберзагроз»

Галузь знань 12 «*Інформаційні технології*»

Спеціальність 125 «*Кібербезпека та захист інформації*»

Освітня програма «*Кібербезпека та захист інформації*»

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «магістр»: кількість сторінок записки 93;

1. Короткий зміст КР та прийнятих рішень: Кваліфікаційна робота присвячена вирішенню актуальної задачі щодо забезпечення стійкості від комплексних кіберзагроз. Це забезпечується шляхом впровадження методу системи адаптивного захисту. Метою роботи є мінімізація часу перебування зловмисника в інфраструктурі та зменшення навантаження на персонал захисту. Для досягнення поставленої мети були проаналізовані недоліки традиційних методів реагування, був розроблений метод адаптивного захисту, були спроєктовані та реалізовані алгоритми динамічної оцінки ризику та адаптивного часу блокування. Також був розроблений важливий алгоритм адаптивного захисту КІС. Також цей метод супроводився проєктуванням та створенням програмного комплексу з використанням мікросервісної архітектури та системи оркестрації, що забезпечує автоматизацію засобів безпеки.

2. Висновок про відповідність КР завданню: Кваліфікаційна робота у повній мірі відповідає поставленому завданню як в теоретичній так і у практичній частині роботи.

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі обгрунтовується актуальність теми роботи, її зв'язок з галуззю знань «Інформаційні технології» та спеціальністю «Кібербезпека та захист інформації», чітко формулюється мета та основні завдання кваліфікаційної роботи. У першому розділі проводиться аналіз сучасних кіберзагроз і чинників, що впливають на стійкість корпоративних систем. Розглядаються різноманітні підходи щодо забезпечення стікості КІС від комплексних кіберзагроз та обґрунтовується потреба в автоматизованих рішеннях У другому розділі пропонується метод адаптивного захисту. Створюються математичні моделі оцінки ризиків і алгоритм для оцінки ефективності адаптивного захисту. У третьому розділі описується розроблена архітектура системи адаптивного захисту, демонструється розроблений алгоритм адаптивного захисту та пов'язані з ним алгоритми, описується розроблена структура ПЗ та використанні засоби виявлення кібератак.

4. Позитивні сторони кваліфікаційної роботи: Запропонований метод адаптивного захисту вирізняється використанням динамічного підходу до оцінки інцидентів, що дозволяє автоматично пріоритизувати загрози без участі оператора. Такий метод та його алгоритми забезпечують баланс між безпекою та доступністю бізнес-сервісів. Система характеризується високим рівнем автоматизації завдяки використанню систем оркестрації, що суттєво знижує вплив людського фактору та витрати. Використання відкритої архітектури та стандартизованих API забезпечує гнучкість інтеграції та можливість його швидкого масштабування в умовах функціонування корпоративних інформаційних систем.

5. Негативні сторони проекту: Не було достатньо чітко описано вимоги до апаратних ресурсів серверної частини при масштабуванні системи, а також у роботі не повністю розкрито поведінку системи та стабільність мікросервісів при пікових навантаженнях.

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

7. Відгук про роботу в цілому: У загальному, кваліфікаційна робота виконана на високому рівні. Матеріал пояснювальної записки викладений системно та у чіткій логічній послідовності. Структура цієї роботи є продуманою та збалансованою, а всі її розділи чітко взаємопов'язані між собою, що забезпечує цілісне розкриття обраної теми. Зміст роботи повністю відповідає поставленим завданням, а наведені аргументи є переконливими та зрозумілими.

8. Інші зауваження: -

9. Оцінка дипломної роботи: Розглянувши позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що робота заслуговує оцінки 100 балів (відмінно).

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи)

Бойко Юлій Миколайович, професор кафедри ТМІТ, доктор технічних наук, професор Хмельницького національного університету

«15» 12 2025 р. (підпис)