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

**КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ**

# Кваліфікаційна робота

на тему:

**«ТЕХНОЛОГІЯ МОДУЛЯ ОЦІНКИ ЗАХИЩЕНОСТІ ПІДПРИЄМСТВА»**

зі спеціальності *125, Кібербезпека та захист інформації*

освітньо-професійно програми *Інформаційна та кібернетична безпека*

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

_____ *Іван ЄКІМОВ*
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-63
Єкімов Іван
(прізвище та ім'я)
Керівник Д.т.н., п. КАЗМІРЧУК Світлана
(наукова ступінь, вчене звання, прізвище, ім'я)
Рецензент _____
(наукова ступінь, вчене звання, прізвище, ім'я)

КИЇВ 2024

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

Кафедра Систем та технологій кібербезпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека та захисту інформації
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри СТК
_____ Гайдур Г.І.
“___” _____ 2024 року

# З А В Д А Н Н Я
## НА БАКАЛАВРСЬКУ РОБОТУ СТУДЕНТУ

Єкімова Івана Вікторовича
(прізвище, ім’я, по батькові)

1. Тема бакалаврської роботи: «Технологія модуля оцінки захищеності підприємства»

керівник кваліфікаційної роботи КАЗМІРЧУК Світлана, Д.т.н., професор
(прізвище, ім’я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційної-комунікаційних технологій від «___» _____ 2024 року №.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 15.12.2024 р.

3. Вихідні дані до кваліфікаційної роботи
Інформаційні системи підприємства;
Технології оцінки рівня захищеності інформаційних активів;
Методи, інструменти та технічні рішення для оцінки безпеки, включаючи пенсентинг, аналіз на вразливостей та система моніторингу;
Наукова та технічна література, наукова документація та експлуатаційні матеріали.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Актуальність оцінки захищеності інформаційних активів на підприємстві.
2. Аналіз технологій та модулів оцінки захищеності інформаційних систем.

3. Побудова архітектури модуля і його функціональні можливості.
4. Тестування модуля в умовах підприємства.

5. Перелік графічного матеріалу
1. Тема кваліфікаційної роботи.
2. Об’єкт, предмет, мета та наукові завдання дослідження.
3. Аналіз актуальних загроз для інформаційної безпеки підприємства
4. Схеми й діаграми процесу оцінки захищеності інформаційних систем.
5. Архітектура та функціональні можливості модуля оцінки захищеності.
6. Результати тестування модуля в умовах підприємства (діаграми продуктивності, таблиці точності виявлення загроз)..
7. Рекомендації щодо впровадження модуля в інфраструктуру підприємства.
8.Узагальнення результатів роботи

6. Дата видачі завдання 01.10.2024 р.

## КАЛЕНДАРНИЙ ПЛАН

| № зп | Назва етапів бакалаврської роботи | Строк виконання етапів бакалаврської роботи | Примітка |
|---|---|---|---|
| 1. | Дослідження актуальності проблеми оцінки захищеності підприємства | 01.10.2024 р. | |
| 2. | Аналіз існуючих стандартів та практик інформаційної безпеки для підприємств | 12.10.2024 р. | |
| 3. | Аналіз існуючих рішень для оцінки захищеності в корпоративних мережах | 27.10.2024 р. | |
| 4. | Визначення формулювання технічних вимог для модуля оцінки захищеності підприємства | 03.11.2024 р. | |
| 5. | Визначення формулювання технічних вимог для модуля оцінки захищеності підприємства | 15.11.2024 р. | |
| 6. | Проектування та дослідження модуля оцінки захищеності підприємства | 26.11.2024 р. | |
| 7. | Підготовка доповіді до захисту | 15.12.2024 р. | |

Здобувач вищої освіти _____
(підпис) (прізвище та ім’я)

Керівник кваліфікаційної роботи _____
(підпис) (прізвище та ім’я)

# ВІДГУК РЕЦЕНЗЕНТА

на кваліфікаційної роботу

здобувача: Єкімова Івана Вікторовича
на тему: «Технологія модуля оцінки захищеності підприємства»

**Актуальність:** На сучасному етапі розвитку інформаційних технологій питання забезпечення інформаційної безпеки є критично важливим для підприємств. Робота присвячена актуальній темі розробки та впровадження технології оцінки захищеності інформаційних активів підприємства, що дозволяє ефективно виявляти потенційні загрози, підвищувати рівень безпеки та своєчасно реагувати на загрози. У роботі розглянуто рішення, які дозволяють автоматизувати процеси оцінки та аналізу захищеності, що відповідає сучасним вимогам підприємств до кібербезпеки. Отже, тема є актуальною та відповідає викликам сучасної кібербезпеки.

**Позитивні сторони:**

1. Зміст роботи повністю відповідає поставленому завданню. Студент продемонстрував високий рівень підготовленості та знання у сфері забезпечення інформаційної безпеки.
2. У роботі обґрунтовано важливість оцінки захищеності інформаційних систем підприємства. Докладно розглянуто можливості модуля оцінки захищеності та його інтеграції у корпоративне середовище.
3. Текст роботи викладено чітко, послідовно та грамотно. Висновки сформульовано лаконічно й обґрунтовано. Графічний матеріал якісно ілюструє основні аспекти дослідження, а список літератури свідчить про вміння студента працювати з науково-технічними джерелами.

**Недоліки:**

1. У роботі недостатньо глибоко проаналізовано методи оцінки ефективності розробленого модуля в умовах реального впровадження.

**Висновок:** Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку **гарно**, а здобувач **Єкімов Іван** – присвоєння кваліфікаційний магістр з кібербезпеки за освітньо-професійно програмою інформаційна та кібернетична безпека.

Рецензент:

| _____ | _____ | _____ |
|---|---|---|
| (наукова ступінь, вчене звання) | (підпис) | (прізвище та ім’я) |

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

**ПОДАННЯ**
**ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ**
**ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ**

Направляється студент ЄКІМОВ Іван до захисту бакалаврської роботи
(прізвище та ім'я)
спеціальності 125 Кібербезпека та захист інформації
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Технологія модуля оцінки захищеності підприємства».

Кваліфікаційна робота і рецензія додаються.

Директор інституту

(підпис) Євгенія ІВАНЧЕНКО (ім'я прізвище)

**Висновок керівника бакалаврської роботи**

Здобувач **ЄКІМОВ Іван** обрав тему роботи, метою якої було дослідження та розробка технологій модуля оцінки захищеності на підприємстві. Під час виконання Кваліфікаційної роботи ЄКІМОВ ІВАН показав гарну теоретичну та практичну підготовку, вміння самостійно вирішувати питання, аналізувати ситуацію та обґрунтовувати висновки. Роботу виконав акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувач **ЄКІМОВ Іван** оцінку **відмінно** та присвоїти їй кваліфікацію магістр з кібербезпеки за освітньо-професійною програмою інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи

(підпис) КАЗМІРЧУК Світлана (прізвище та ім'я)
"____" _____ 2024 року

**Висновок кафедри про бакалаврську роботу**

Кваліфікаційна робота розглянута. Здобувач Єкімов Іван допускається до захисту даної кваліфікаційної роботи в екзаменаційної комісії.

Завідувач кафедри Систем та технологій кібербезпеки
(назва)

(підпис) ГАЙДУР Галина (прізвище та ім'я)

# РЕФЕРАТ

Текстова частина кваліфікаційної роботи: сторінок 61, рисунків 7, джерел 7.

*Об'єкт дослідження* – інформаційні системи підприємств та методи їх захисту..

*Предмет дослідження* – технологія модуля оцінки захищеності підприємства, включаючи методи, підходи та засоби для інтеграції цього модуля в інфраструктуру підприємства.

*Мета роботи* – аналіз існуючих підходів до оцінки захищеності інформаційних систем на підприємствах та розробка рекомендацій щодо створення ефективного модуля для оцінки рівня безпеки.

*Методи дослідження* – аналіз наукової літератури, вивчення нормативних актів та міжнародних стандартів з інформаційної безпеки, проведення експериментальних досліджень, розробка і тестування моделей для оцінки захищеності.

У роботі наведено основні поняття та технології, пов'язані з оцінкою захищеності інформаційних систем підприємства.
Проаналізовано основні види загроз, які можуть виникати для інформаційних систем підприємств.
Досліджено існуючі методи та засоби оцінки захищеності, що застосовуються для виявлення слабких місць у системах підприємства.
Досліджено можливості створення та впровадження модуля оцінки захищеності, який може бути інтегрований в інфраструктуру підприємства.

Галузь використання – кібербезпека, управління інформаційною безпекою підприємства, створення та впровадження технологій для забезпечення захищеності інформаційних систем.

ОЦІНКА ЗАХИЩЕНОСТІ, МОДУЛЬ ОЦІНКИ, ПІДПРИЄМСТВО, ІНФОРМАЦІЙНА БЕЗПЕКА, ВРАЗЛИВОСТІ, КІБЕРБЕЗПЕКА, ЗАГРОЗИ.

# ABSTRACT

Text part of the qualification work: pages 61, figures 7, sources 7.

The object of the study is information systems of enterprises and methods of their protection.

The subject of the study is the technology of the enterprise security assessment module, including methods, approaches, and tools for integrating this module into the enterprise infrastructure.

The purpose of the work is to analyze existing approaches to assessing the security of information systems at enterprises and develop recommendations for creating an effective module for assessing the level of security.

Research methods are an analysis of scientific literature, studying regulatory acts and international standards on information security, conducting experimental research, developing and testing models for assessing security.

The work presents the main concepts and technologies related to assessing the security of enterprise information systems.
The main types of threats that may arise for enterprise information systems are analyzed.
Existing methods and means of assessing security used to identify weaknesses in enterprise systems are studied.
The possibilities of creating and implementing a security assessment module that can be integrated into the enterprise infrastructure are studied.

Field of use – cybersecurity, enterprise information security management, creation and implementation of technologies to ensure the security of information systems.

SECURITY ASSESSMENT, ASSESSMENT MODULE, ENTERPRISE, INFORMATION SECURITY, VULNERABILITY, CYBERSECURITY, THREATS.

# ЗМІСТ

# ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

SQL – SQL ін’єкція

DDoS – Розподілене відмовлення в обслуговуванні

OWASP – Проект безпеки веб-додатків

APT – Прогресивна постійна загроза

SIEM – Система управління інформацією та подіями безпеки

ISO –International Organization for Standardization

IEC –International Electrotechnical Commission

NIST SP – Спеціальна публікація NIST

NTA — Network Traffic Analysis

ПЗ — програмне забезпечення

PCI DSS — Payment Card Industry Data Security Standard

SSRF — Server-Side Request Forgery

XSS — Cross-Site Scripting

URL — Uniform Resource Locator

API — Application Programming Interface

НСД — Неавторизований доступ

RCE — Remote Card Execution

IT — Information Technology

TI — Threat Intelligence (Інформація про загрози)

# ВСТУП

У сучасному світі кібербезпека стає все більш важливою через зростання кількості загроз для інформаційних систем підприємств. Кібератаки можуть призвести до витоку даних, фінансових втрат та серйозного удару по репутації. Щоб захистити інформацію та зменшити ризики, компанії потребують інструментів, які дозволяють оцінювати вразливості та реагувати на загрози.

Ця робота присвячена створенню модуля, який допоможе оцінити рівень захищеності інформаційних систем підприємства. Метою дослідження є розробка технології, яка не тільки виявляє слабкі місця, але й дає змогу оперативно реагувати на можливі загрози.

Для досягнення цього було вивчено сучасні підходи до кібербезпеки, проаналізовано типові загрози, такі як фішингові атаки чи вразливості в ПЗ. Було також розроблено та протестовано модуль оцінки, що дозволяє виявляти загрози й адаптуватися до нових викликів у сфері кіберзахисту.

Результати цієї роботи можуть бути корисними для підприємств, які прагнуть підвищити рівень безпеки своїх інформаційних систем. Запропоновані рішення є простими у впровадженні та відповідають сучасним вимогам, допомагаючи підприємствам зменшити ризики кібератак.

У рамках цієї роботи було враховано ключові аспекти сучасних кіберзагроз, зокрема їхню постійну змінюваність та складність. Технології атак стають дедалі витонченішими, тому ефективний модуль захисту має бути не лише здатним виявляти відомі загрози, а й адаптуватися до нових, забезпечуючи динамічний підхід до безпеки.

Окрім вивчення сучасних підходів до захисту, увагу зосереджено на практичному застосуванні запропонованого модуля. Проведено моделювання реальних загроз, таких як фішингові атаки, використання відомих вразливостей у ПЗ та ін’єкції SQL-коду. Це дозволило перевірити ефективність розробленої технології в умовах, максимально наближених до реальних.

Особливістю запропонованого рішення є можливість інтеграції модуля із вже існуючими системами безпеки підприємства. Це спрощує його впровадження та забезпечує безперебійну роботу всіх підсистем, відповідальних за моніторинг і захист інформації. Також важливою перевагою є висока автоматизація процесів, що знижує необхідність у втручанні спеціалістів для реагування на загрози.

У результаті проведеного дослідження створено інструмент, який допомагає ефективно оцінити стан захищеності підприємства, своєчасно виявляти ризики та підвищувати загальний рівень безпеки. Це сприяє мінімізації фінансових втрат, пов’язаних із кібератаками, та забезпечує стабільність роботи інформаційних систем.

Запропоноване рішення є вагомим внеском у розвиток кібербезпеки та демонструє, як використання сучасних технологій може допомогти підприємствам протистояти новим викликам у цифровому середовищі.

# 1. ДОСЛІДЖЕННЯ ІСНУЮЧИХ ПІДХОДІВ ОЦІНЮВАННЯ ЗАХИЩЕНОСТІ ПІДПРИЄМСТВА

Оцінка захищенності підприємства – це комплексний процес, спрямований на виявлення рівня безпеки інформаційних ресурсів, інфраструктури, а також бізнес-процесів підприємства. У сучасному світі , де кіберзагрози стають все більш складними, розробка та впровадження ефективних методів оцінювання захищенності є критично важливими для зменшення та ризиків та забезпечення безперервності бізнесу.

Сучасні підходи оцінювання захищенності підприємства методи кількісної та якісної оцінки, аналіз ризиків, аудити безпеки, а також використання різноманітних технологій, що дозволяють виявити та реагувати на потенційну загрози.

## 1.1. Огляд існуючих технологій оцінки захищенності підприємств

Технологія оцінювання захищеності можуть бути поділені на кілька основних категорій:

### 1.1.1. Сканери вразливостей

- Використання автоматизованих інструментів, таких як Nessus, OpenVAS, Qualys, дозволяє проводити сканування систем для виявлення відомих вразливостей, неправильно налаштованих сервісів та інших ризиків. Сканери вразливостей здатні перевіряти системи на наявність помилок у ПЗ, а також аналізувати налаштування мережевих пристроїв і серверів.

### 1.1.2. Технологія тестування на проникнення

- Цей метод дозволяє імітувати реальні атаки з метою оцінки здатності системи протистояти кіберзагрозам. За допомогою інструментів на кшталт Metasploit, Burp Suite, Kali Linux експерти з кібербезпеки можуть провести атаки різного рівня складності, виявляючи потенційні точки доступу та перевіряючи, наскільки ефективно підприємство здатне захищатися від таких атак.

1.1.3. Системи управління інформаційною безпекою ( SIEM ) - Інструменти SIEM, такі як Splunk, ArcSight, QRadar, збирають та аналізують події та лог-файли з усіх систем підприємства, надаючи загальну картину безпеки в режимі реального часу. SIEM-системи дозволяють виявляти підозрілі дії, здійснювати аналіз інцидентів безпеки та надають інструменти для швидкої реакції на загрози.

1.1.4. Методи оцінки ризиків та управління ризиками - Існує низка стандартів, таких як ISO/IEC 27005, NIST SP 800-30, що пропонують методології для оцінки та управління ризиками інформаційної безпеки. Такі підходи допомагають підприємствам ідентифікувати можливі ризики, оцінити їхній вплив і ймовірність та розробити відповідні стратегії управління для мінімізації цих ризиків.

1.1.5. Аудит безпеки та сертифікація - Аудит безпеки передбачає оцінювання існуючих заходів захисту та порівняння їх з прийнятими стандартами або передовими практиками. Аудит може бути внутрішнім або зовнішнім, а також передбачати сертифікацію за такими стандартами, як ISO 27001. Це допомагає виявити слабкі місця у політиках, процесах та технологіях безпеки підприємства.

1.1.6. Системи захисту кінцевих точок - Рішення для захисту кінцевих точок, наприклад, Symantec Endpoint Protection, CrowdStrike Falcon, Carbon Black, забезпечують захист пристроїв, що підключені до корпоративної мережі. Вони дозволяють виявляти шкідливе ПЗ, захищати дані від крадіжок та надавати аналітику щодо підозрілих активностей на рівні кінцевих точок.

1.1.7. Моніторинг мережевого трафіку та система виявлення загроз - Інструменти для аналізу трафіку (NTA) такі, як Darktrace, Cisco Stealthwatch, дозволяють здійснювати моніторинг мережевого трафіку на предмет аномалій, що можуть свідчити про атаки чи спроби проникнення. Інтеграція систем NTA з SIEM-системами підвищує рівень захищеності підприємства завдяки покращеному виявленню загроз.

1.1.8. Технології захисту від шкідливого ПЗ та фільтрація - Використання антивірусного ПЗ та фільтрації, таких як McAfee, Bitdefender, допомагає захистити підприємство від різного роду шкідливих програм. Це включає не тільки захист від вірусів, але й від шкідливого ПЗ, фішингових атак та інших небезпек, що можуть проникнути до системи.

Всі розглянуті технології оцінки захищеності мають спільну мету – забезпечення всебічного захисту від кіберзагроз і підтримання безперервності бізнес-процесів. Хоч кожна з них має свої особливості, їх взаємодії та інтегроване використання дозволяють побудувати багаторівневу систему безпеки, яка значно зміцнює здатність підприємства протистояти кібератакам.

1.2. Ключовими аспектами, що об’єднують ці технології, включають в себе:

1.2.1. Інтеграція та взаємодія

Технології безпеки, які працюють у зв’язці, доповнюють одна одну, забезпечуючи більш ефективне виявлення і нейтралізацію загроз. Наприклад, поєднання систем SIEM із моніторингом мережевого трафіку дає змогу виявляти й аналізувати аномалії в реальному часі, а результати сканування вразливостей дозволяють сфокусуватися на захисті найбільш критичних ділянок.

1.2.2. Автоматизація та спрощення управління

Сучасні інструменти безпеки пропонують автоматизовані функції, що знижують час реагування на загрози. Це особливо важливо, адже ручне реагування на інциденти може бути повільним. Наприклад, сканери вразливостей чи системи захисту кінцевих точок здатні автоматично виявляти загрози та проводити аналіз без необхідності значного втручання користувача.

1.2.3. Ризик-орієнтований підхід

Інструменти оцінки ризиків та аудити безпеки не лише виявляють загрози, а й оцінюють їхній потенційний вплив. Це дозволяє підприємствам ефективно

визначити пріоритет у впровадженні захисних заходів, зосереджуючись на найбільш критичних аспектах.

### 1.2.4. Покращення та виявлення та аналіз інцидентів

Комбінація різних методів, таких як тестування на проникнення та моніторинг мережі, забезпечує більш точне виявлення загроз. Наприклад, SIEM-системи у поєднанні зі сканерами вразливостей і моніторингом кінцевих точок створюють комплексну картину подій, що сприяє швидкому та точному реагуванню на інциденти.

### 1.2.5. Масштабованість і адаптивність

Сучасні системи безпеки швидко адаптуються до нових кіберзагроз. Наприклад, антивірусні рішення та засоби захисту кінцевих точок автоматично оновлюються для боротьби з новими типами шкідливого ПЗ. Інструменти для сканування вразливостей також постійно оновлюють свої бази даних для підтримки актуальності.

### 1.2.6. Підтримка відповідності стандартам

Багато з цих технологій забезпечують дотримання стандартів безпеки, таких як ISO 27001, NIST або PCI DSS. Це критично важливо для підприємств, які прагнуть відповідати нормативним вимогам і будувати довіру серед клієнтів і партнерів.

Переваги комплексного підходу до оцінки захищеності

Використання комплексного підходу до оцінки захищеності підприємства, що охоплює різні технології, забезпечує такі переваги як:

Підвищена точність виявлення загроз завдяки застосуванню різноманітних інструментів для збору даних, моніторингу та аналізу.

Швидке реагування на інциденти через автоматизацію процесів виявлення та усунення загроз.

Оптимізація управління ризиками за рахунок інтеграції інструментів, що дозволяють комплексно оцінити потенційні загрози.

Ефективне використання ресурсів шляхом фокусування на критично важливих аспектах кіберзахисту, що сприяє оптимізації витрат.

Ризики, що пов’язані з комплексною оцінкою захищеності

Незважаючи на переваги, застосування різних технологій оцінювання може супроводжуватися таким викликами:

Недостатня ефективність технологій. Деякі методи можуть не виявити нові або специфічні загрози, що знижує надійність оцінки.

Висока вартість. Впровадження та підтримка комплексних рішень вимагає значних фінансових і людських ресурсів.

Неповна оцінка. Якщо методи не охоплюють всі аспекти або виконуються нерегулярно, існує ризик пропуску важливих вразливостей.

Підсумок

Інтеграція різноманітних технологій оцінювання безпеки є важливим компонентом стратегії захисту підприємства, яка дозволяє забезпечити надійний захист інформаційних активів, мінімізувати ризики та сприяти стабільному розвитку бізнесу.

## 1.2. Огляд основних загроз і вразливостей згідно з OWASP

OWASP (Open Web Application Security Project) — це неприбуткова організація, яка займається дослідженням та розробкою стандартів і рекомендацій для покращення безпеки веб-додатків. Один із найвідоміших проєктів OWASP — це OWASP Top 10. Це список із десяти найважливіших вразливостей веб-додатків, який оновлюється на основі реальних даних про інциденти та загрози. Мета OWASP Top 10 — допомогти розробникам, безпековим командам та керівництву організацій зосередитися на критичних

аспектах безпеки веб-додатків і впроваджувати кращі практики для захисту даних.

Список OWASP Top 10 періодично оновлюється, остання версія (на момент написання) була випущена у 2021 році. Нижче наведені основні вразливості OWASP Top 10 разом з коротким описом:

1. Broken Access Control (Порушення контролю доступу)

- Одна з найпоширеніших загроз. Вона виникає, коли користувачі можуть отримати доступ до функцій або даних, які не призначені для них. Це може бути викликано неправильними налаштуваннями доступу або відсутністю достатнього контролю. Неправильний контроль доступу може дозволити зловмисникам обійти авторизацію та отримати доступ до чутливих даних.

2. Cryptographic Failures (Криптографічні помилки)

- Ця вразливість охоплює помилки у використанні криптографії, що може призвести до компрометації конфіденційної інформації, як-от особистих даних або платіжної інформації. Наприклад, використання застарілих алгоритмів шифрування або неправильне управління ключами може зробити дані вразливими до атак.

3. Injection (Ін’єкційні атаки)

- До цієї категорії належать SQL-ін’єкції, LDAP-ін’єкції та інші ін’єкційні атаки, коли зловмисники вводять шкідливий код у запити до бази даних чи інших сервісів. Це дозволяє отримати доступ до даних, змінювати їх або навіть захопити управління системою.

4. Insecure Design (Небезпечне проєктування)

- Ця загроза пов’язана з відсутністю надійного проєктування та врахування безпекових аспектів на ранніх етапах розробки. Небезпечне проєктування може спричинити вразливості, які важко виправити на пізніх етапах.

5. Security Misconfiguration (Неправильна конфігурація безпеки)

- Часто виникає через помилки у налаштуванні безпеки, наприклад, відкриті порти, недостатньо захищені API, або використання стандартних облікових даних. Неправильна конфігурація може значно спростити зловмисникам доступ до системи.

6. Vulnerable and Outdated Components (Вразливі та застарілі компоненти)

- Використання застарілих бібліотек, фреймворків чи інших компонентів з відомими вразливостями може поставити всю систему під загрозу. Відсутність регулярних оновлень робить веб-додаток вразливим до атак.

7. Identification and Authentication Failures (Помилки ідентифікації та аутентифікації)

- Проблеми з процесами ідентифікації та аутентифікації можуть призвести до компрометації облікових записів. Це може включати слабкі паролі, відсутність багатофакторної аутентифікації, небезпечне зберігання облікових даних та інші помилки.

8. Software and Data Integrity Failures (Помилки цілісності ПЗ та даних)

- Ці вразливості виникають через відсутність механізмів забезпечення цілісності коду та даних. Наприклад, відсутність верифікації надійності оновлень може дати можливість зловмисникам впровадити шкідливий код у систему.

9. Security Logging and Monitoring Failures (Помилки журналювання та моніторингу)

- Відсутність належного моніторингу та журналювання може призвести до того, що інциденти безпеки залишаться непоміченими. Це ускладнює виявлення, аналіз та усунення атак, даючи зловмисникам більше часу для реалізації своїх планів.

10. Server-Side Request Forgery (SSRF) (Підробка запитів на стороні сервера)

- SSRF-атаки відбуваються, коли зловмисник змушує сервер надсилати запити до небезпечних зовнішніх ресурсів. Це може призвести до розкриття внутрішніх даних або використання ресурсу для атак на інші системи.

OWASP надає список основних загроз і вразливостей для веб-застосунків, що дозволяє підприємствам орієнтуватися на конкретні напрямки захисту.

Ризики, пов’язані з цією темою:

Ризик незахищеності критичних вразливостей: Якщо підприємство не фокусується на найбільш серйозних загрозах, таких як SQL ін’єкції, несанкціонований доступ або XSS (між атакою та уразливістю може бути дуже мала різниця), це може призвести до серйозних порушень безпеки.

Ризик неадекватного оновлення систем: Якщо підприємства не регулярно оновлюють своє ПЗ, застосовуючи новітні патчі, це збільшує ймовірність використання відомих вразливостей для атаки, що може призвести до проникнення зловмисників.

Ризик ускладнення оцінки загроз: Використання застарілих методів оцінки або нехтування новими технологіями може призвести до неповного аналізу загроз та створити недооцінку потенційних ризиків для безпеки організації.

Підсумок

Список OWASP Top 10 є основою для побудови захисту веб-додатків, надаючи розробникам і спеціалістам з безпеки інструменти для виявлення та запобігання поширеним загрозам. Впровадження кращих практик з OWASP допомагає підвищити загальний рівень безпеки веб-додатків і зміцнити захищеність підприємства, оскільки кожна з цих вразливостей може серйозно вплинути на контроль за конфіденційністю, цілісністю та доступністю даних. Рекомендації OWASP не лише знижують рівень ризику для додатків, а й мінімізують загрози для бізнесу загалом, зменшуючи ймовірність збоїв, фінансових втрат та репутаційних ризиків.

## 1.3. Класифікація загроз: зовнішні та внутрішні фактори впливу

Загрози безпеці підприємства можуть виникати як із зовнішніх, так і з внутрішніх джерел. Класифікація цих загроз допомагає визначити шляхи їх мінімізації та адаптувати стратегії захисту відповідно до джерела загрози.

### 1.3.1. Зовнішні загрози

Зовнішні загрози походять від джерел поза межами підприємства та часто є найбільш небезпечними через непередбачуваність і складність у контролі. До зовнішніх загроз відносяться:

#### 1.3.1.1. Кіберзлочинці та хакери

- Хакерські атаки, спрямовані на отримання доступу до конфіденційної інформації, маніпуляцію даними або порушення роботи систем, є однією з основних зовнішніх загроз. Злочинці можуть використовувати методи фішингу, ін’єкцій SQL, DDoS-атаки та інші методи для досягнення своїх цілей.

#### 1.3.1.2. Malware  та інші типи шкідливого ПЗ

- Віруси, трояни, програми-вимагачі та шпигунське ПЗ є інструментами, які кіберзлочинці використовують для компрометації систем. Вони можуть призводити до втрати даних, зупинки бізнес-процесів або навіть шантажу.

#### 1.3.1.3. Конкуренція та індустріальне шпигунство

- У конкурентному середовищі можуть бути ризики, пов’язані з недобросовісною конкуренцією, коли треті сторони намагаються отримати доступ до комерційних таємниць або клієнтської бази підприємства.

#### 1.3.1.4. Природні катастрофи та техногенні аварії

- Природні катастрофи (землетруси, повені, пожежі) та техногенні аварії можуть спричинити значні втрати для підприємства. Такі події можуть пошкодити інфраструктуру, що, в свою чергу, призведе до збоїв у роботі систем і порушень безпеки даних.

1.3.2.Внутрішні загрози

Внутрішні загрози, хоча і менш помітні, можуть мати не менш руйнівний вплив. Вони виникають у межах самого підприємства і часто пов’язані з людським фактором або недосконалими внутрішніми процесами. Основні внутрішні загрози включають:

1.3.2.1. Інсайдерські загрози

- Співробітники, які мають доступ до конфіденційних даних, можуть навмисно чи ненавмисно пошкодити систему або викрасти дані. Це може бути пов'язано з їхнім невдоволенням, особистими мотивами чи впливом сторонніх осіб.

1.3.2.2. Недостатнє знання безпеки серед персоналу

- Брак знань або неуважність до правил безпеки можуть призвести до помилок, які полегшують доступ зловмисникам. Наприклад, слабкі паролі, відсутність уваги до фішингових листів чи неналежне зберігання даних є поширеними причинами інцидентів.

1.3.2.3. Помилки в конфігурації систем та недостатнє оновлення ПЗ

- Неправильні налаштування мережевих пристроїв чи ПЗ можуть залишати відкриті точки доступу для кіберзлочинців. Відсутність регулярних оновлень підвищує ризик експлуатації відомих вразливостей.

1.3.2.4. Незадовільне управління доступом

- Надмірні або невідповідні права доступу для співробітників можуть збільшувати ризики витоку інформації чи маніпуляцій з даними. Ефективне управління доступом дозволяє мінімізувати цей ризик, надаючи доступ до інформації лише тим, хто дійсно її потребує.

Взаємозв’язок зовнішніх та внутрішніх загроз

Зовнішні та внутрішні загрози часто взаємопов'язані. Наприклад, зовнішня атака може використовувати слабкі внутрішні налаштування або недостатню обізнаність співробітників для досягнення успіху. Навпаки, інсайдери можуть сприяти реалізації зовнішніх атак, передаючи конфіденційну інформацію зловмисникам. Розуміння цього взаємозв’язку допомагає формувати комплексний підхід до забезпечення безпеки, що включає як технічні заходи, так і підвищення обізнаності співробітників щодо сучасних загроз.

Загрози підприємству можуть виникати як ззовні, так і зсередини організації.

Ризики, пов’язані з класифікацією загроз:

Зовнішні загрози:

Ризик кібератак з боку хакерів: Зловмисники можуть використовувати різноманітні методи атак, від DDoS-атак до складних фішингових кампаній, що призводить до збоїв у роботі систем, викрадення даних або фінансових втрат.

Ризик нових або невідомих загроз: Зовнішні фактори, такі як зміни в кіберзлочинному середовищі, можуть швидко змінювати ландшафт загроз, роблячи поточні заходи захисту недостатньо ефектами.

Внутрішні загрози:

Ризик помилок співробітників: Недостатнє навчання або недбалість співробітників можуть призвести до помилок, що сприяють витокам інформації або неправильним налаштуванням безпеки.

Ризик зловживань з боку співробітниками: Існує потенціал для навмисного порушення безпеки з боку внутрішніх користувачів, які мають доступ до конфіденційної інформації, що може призвести до викрадення даних або саботажу.

Підсумок

Класифікація загроз на зовнішні та внутрішні дозволяє підприємствам більш ефективно управляти ризиками, адаптуючи заходи захисту до конкретних джерел загроз. Це забезпечує комплексний підхід до кібербезпеки, спрямований на захист як від зовнішніх атак, так і від внутрішніх помилок чи зловмисних дій. Розуміння взаємозв'язку між зовнішніми та внутрішніми загрозами дозволяє створити більш збалансовану та ефективну стратегію кібербезпеки.

## 1.4. Аналіз ключових вразливостей, які найчастіше використовуються при атаках

У сучасному світі кіберзагроз підприємства стикаються з численними вразливостями, які зловмисники використовують для проведення атак. Розуміння цих вразливостей є критично важливим для забезпечення інформаційної безпеки. Нижче наведено аналіз ключових вразливостей, які найчастіше використовуються при атаках на веб-додатки та комп'ютерні системи.

### 1.4.1. Вразливості контролю доступу

Проблема: Неправильна реалізація контролю доступу дозволяє зловмисникам отримати доступ до чутливих функцій або даних, які не призначені для них.

Приклад: Атакуючи, можуть використовуватися методи обходу авторизації, такі як зміна параметрів URL або використання сесійних токенів, що дозволяє отримати доступ до чужих облікових записів.

### 1.4.2. Ін’єкційні вразливості

Проблема: Ін’єкційні атаки (наприклад, SQL-ін’єкції) виникають, коли зловмисники вводять шкідливий код у запити до бази даних, що може призвести до витоку даних, зміни або видалення інформації.

Приклад: Зловмисник може вставити шкідливий SQL-запит у форму для входу, отримуючи доступ до даних користувачів.

1.4.3. Криптографічні помилки

Проблема: Використання ненадійних алгоритмів шифрування або неправильне управління ключами може призвести до компрометації конфіденційних даних.

Приклад: Якщо підприємство використовує застарілі алгоритми шифрування, зловмисники можуть легко зламати шифри та отримати доступ до важливої інформації.

1.4.4. Небезпечне проєктування

Проблема: Відсутність врахування безпеки на етапі проєктування веб-додатків може призвести до вразливостей, які важко усунути на пізніших етапах.

Приклад: Проєкт, що не враховує можливість повторного використання паролів або двофакторну аутентифікацію, може стати легкою мішенню для зловмисників.

1.4.5. Неправильна конфігурація безпеки

Проблема: Неправильні налаштування серверів, баз даних і додатків можуть дозволити зловмисникам скористатися вразливостями.

Приклад: Відкриті порти, стандартні облікові дані або доступ до адмін-панелей можуть призвести до несанкціонованого доступу.

1.4.6. Використання застарілих компонентів

Проблема: Використання бібліотек і фреймворків із відомими вразливостями ставить під загрозу безпеку системи.

Приклад: Наприклад, відомі вразливості в популярних бібліотеках можуть бути використані зловмисниками для атаки, якщо вони не були усунені через оновлення.

1.4.7. Помилки ідентифікації та аутентифікації

Проблема: Неправильне зберігання паролів, відсутність багатофакторної аутентифікації і використання слабких паролів роблять облікові записи вразливими.

Приклад: Зловмисники можуть легко отримати доступ до облікових записів, використовуючи методи зламу паролів, такі як атаки за списком або з використанням програм для перебору паролів.

1.4.8. Помилки журналювання та моніторингу

Проблема: Відсутність належного журналювання та моніторингу подій безпеки ускладнює виявлення та реагування на інциденти.

Приклад: Якщо системи не ведуть журналів, зловмисники можуть діяти в системі безперешкодно, поки не завдадуть значної шкоди.

Аналіз вразливостей, які найчастіше використовуються при атаках, є важливим елементом для оцінки ризиків підприємства. Виявлення вразливих точок дозволяє зрозуміти, де існують найбільші загрози для системи.

Ризики, пов'язані з вразливостями:

1. Ризик витоку даних через вразливі веб-додатки: Веб-додатки є однією з основних мішеней для кіберзлочинців. Вразливості, такі як SQL-ін'єкції, атаки на міжсайтове підроблення запитів (CSRF), або інші методи обходу контролю доступу, можуть призвести до витоку конфіденційної інформації. Поширення таких атак може завдати значної шкоди репутації підприємства і привести до юридичних наслідків.

2. Ризик використання незахищених API: Відкриті або неправильно налаштовані API можуть стати вразливими до атак, таких як несанкціонований доступ або ін'єкція шкідливого коду. API, які не мають належного рівня захисту, можуть бути використані для отримання конфіденційних даних, а також для проведення атак на сервери або бази даних.

3. Ризик поширення шкідливих програм через вразливості в ПЗ: Застарілі або неналежно налаштовані компоненти ПЗ можуть стати вразливими до шкідливих програм, таких як віруси, трояни чи програми-вимагачі. Такі атаки можуть спричинити серйозні фінансові та репутаційні втрати для підприємства.

4. Ризик зламу через слабкі механізми аутентифікації: Невикористання багатофакторної аутентифікації та зберігання паролів у незахищеному вигляді можуть дозволити зловмисникам легко отримати доступ до облікових записів. Це підвищує ймовірність здійснення атак через брутфорс або інші методи порушення безпеки облікових даних.

5. Ризик неправильних налаштувань безпеки серверів і додатків: Неправильна конфігурація серверів, баз даних чи додатків може дозволити зловмисникам скористатися вразливостями системи. Наприклад, відкриті порти, невиправлені помилки безпеки або стандартні облікові дані можуть бути використані для несанкціонованого доступу.

Підсумок:

Ключові вразливості, що використовуються в атаках на підприємства, є серйозними загрозами для їхньої інформаційної безпеки. Виявлення таких вразливостей і вживання відповідних заходів захисту є критично важливими для мінімізації ризиків. Регулярні аудити безпеки, оновлення ПЗ, застосування сучасних методів шифрування, а також навчання співробітників щодо безпеки допоможуть знизити ймовірність успішних атак. Впровадження багатофакторної аутентифікації, моніторинг систем і правильне налаштування доступу є невід'ємними елементами стратегії кіберзахисту. Тільки комплексний підхід до безпеки дозволяє ефективно протистояти різноманітним кіберзагрозам та захистити підприємство від потенційних збитків.

# 2. МОДУЛЬ ОЦІНКИ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНОЇ СИСТЕМИ ПІДПРИЄМСТВА

## 2.1. Система кібербезпеки підприємства

Існуюча структурна схема кібербезпеки, розроблена та впроваджена на підприємстві в 2017 році, потребує суттєвого вдосконалення. Це зумовлено швидким розвитком сучасних технологій і постійним зростанням загроз у сфері інформаційної безпеки. За останні роки ландшафт кіберзагроз значно змінився, що зробило необхідним перегляд підходів до забезпечення захисту інформаційних систем підприємства.

Аналіз поточного стану кібербезпеки виявив низку проблем і слабких місць, таких як недостатня адаптація до нових типів загроз, нестача інтеграції з сучасними технологіями моніторингу та обмежені можливості швидкого реагування на інциденти. Зокрема, було виявлено, що наявні системи не враховують загрози типу APT і не мають механізмів автоматичного оновлення для протидії новим кіберзагрозам.

Для підвищення рівня кіберзахищеності інформаційної системи підприємства проведено комплексний аналіз сучасних технологій кіберзахисту. У дослідженні враховувалися як традиційні методи захисту, так і новітні технології, зокрема алгоритми машинного навчання, платформи SIEM для моніторингу інцидентів у реальному часі, а також інструменти TI для прогнозування атак. Особливу увагу було приділено використанню міжнародних стандартів у галузі кібербезпеки, таких як ISO/IEC 27001 та рекомендації NIST.

Розроблений модуль оцінки захищеності інформаційної системи підприємства орієнтований на вирішення критичних проблем кіберзахисту за допомогою наступних компонентів:

Інтелектуальне виявлення загроз. Використання алгоритмів машинного навчання забезпечує не лише аналіз поточних загроз, але й прогнозування

потенційних атак, що дозволяє системі бути проактивною у протидії ризикам. Наприклад, прогнозування атак із точністю до 97% мінімізує ймовірність вразливостей до моменту їх реалізації.

Гнучкість інтеграції. Модуль може функціонувати як автономно, так і в складі комплексної системи кіберзахисту, інтегруючись з іншими інструментами підприємства. Це включає сумісність із SIEM-платформами, криптографічними рішеннями та зовнішніми джерелами Threat Intelligence.

Реалізація стандартів відповідності. У процесі вдосконалення модулю було враховано сучасні стандарти кібербезпеки, що забезпечує високу ефективність захисту та полегшує проходження аудиторських перевірок і сертифікацій.

Автоматизація процесів. Впровадження автоматизованих систем моніторингу, аналізу інцидентів та формування звітів знижує навантаження на персонал і підвищує оперативність реагування на загрози.

Протидія сучасним атакам. Особлива увага приділена захисту від цільових атак високого рівня складності, таких як APT, за допомогою комбінованих методів криптографічного захисту та багатофакторної аутентифікації.

Очікувані результати модернізації системи кібербезпеки включають:

Підвищення точності виявлення загроз до 96–98%, що значно перевищує середньоринкові показники.

Скорочення часу реагування на інциденти до 2 секунд.

Зменшення кількості успішних атак на 30% завдяки впровадженню проактивних методів захисту.

Інтеграцію централізованої системи управління безпекою для забезпечення скоординованої роботи всіх компонентів.

Впровадження модернізованого підходу до кібербезпеки дозволить підприємству значно знизити ризики, забезпечити безперервність бізнес-

процесів і створити гнучку систему, здатну своєчасно адаптуватися до нових загроз.

## 2.2. Структура модуля оцінки захищенності

Модуль оцінки захищеності є одним з ключових компонентів інформаційної системи підприємства, що забезпечує постійний моніторинг рівня захисту та ефективність існуючих заходів безпеки. Цей модуль здійснює комплексний аналіз стану інформаційної системи, на основі якого можна виявити потенційні вразливості та оцінити загрози для інформаційних активів організації. Структура модуля включає взаємодію кількох основних підсистем, кожна з яких відповідає за конкретний аспект безпеки. Модуль інтегрується з іншими елементами системи кібербезпеки, забезпечуючи злагоджену роботу для виявлення, оцінки та нейтралізації кіберзагроз.

1. Модуль оцінки захищеності (1)
Це основний компонент системи, що відповідає за комплексну оцінку рівня безпеки інформаційної системи. Модуль збирає та аналізує дані з різних джерел, зокрема від систем моніторингу кіберпростору (9) та джерел TI (11), що дозволяє оновлювати інформацію щодо нових загроз та вразливостей. Важливим аспектом роботи є взаємодія з системою активної протидії кібератакам (7), що дає можливість адаптувати алгоритми захисту на основі актуальних кіберінцидентів. Модуль оцінки захищеності здійснює аналіз отриманої інформації та генерує звіти, рекомендації щодо покращення рівня безпеки підприємства.

2. Підсистема контролю та стану функціональної стійкості (2)
Ця підсистема здійснює моніторинг технічної стійкості інформаційної системи до різноманітних загроз. Вона збирає дані про стан усіх компонентів системи, а також проводить оцінку уразливостей. Зазначена підсистема взаємодіє з іншими блоками, такими як підсистема попередження та виявлення кібератак (3) і підсистема програмно-

апаратних засобів захисту (4), що дає змогу своєчасно реагувати на загрози та забезпечити стійкість системи.

3. Підсистема попередження та виявлення кібератак (3) Відповідає за своєчасне виявлення атак у інформаційній системі. Модуль аналізує поточний трафік та виявляє аномалії, які можуть вказувати на наявність атаки. Інформація про потенційні загрози передається в інші компоненти системи для прийняття відповідних заходів. Взаємодія з системою моніторингу кіберпростору (9) та підсистемами захисту (4, 5) дозволяє оперативно реагувати на кіберзагрози.

4. Підсистема програмно-апаратних засобів захисту від НСД (4) Ця підсистема забезпечує технічний захист від несанкціонованого доступу до компонентів інформаційної системи. Вона працює в тісній взаємодії з підсистемою попередження та виявлення атак (3), а також з підсистемою контролю та стану функціональної стійкості (2), що забезпечує своєчасне виявлення і блокування загроз.

5. Підсистема криптографічного захисту інформації та шифрування (5)
Відповідає за забезпечення конфіденційності та захисту даних. Ця підсистема застосовує сучасні методи шифрування для захисту інформації від несанкціонованого доступу. Взаємодія з підсистемами попередження та виявлення атак (3) та контролю стійкості (2) дозволяє підтримувати високий рівень шифрування та оновлювати алгоритми на основі актуальних загроз.

6. Система оперативного сповіщення про кібератаки (6) Відповідає за оперативне сповіщення керівництва та відповідальних осіб про поточні загрози. Інформація передається від системи попередження та виявлення кібератак (3), а також від системи активної протидії кібератакам (7), що дає змогу координувати зусилля для нейтралізації загрози.

7. Система активної протидії кібератакам (7)
Ця підсистема займається активною відсіччю та нейтралізацією кіберзагроз. Вона активує відповідні механізми захисту, наприклад, блокує мережевий трафік або ізолює заражені системи. Взаємодія з іншими компонентами, зокрема з модулем оцінки захищеності (1), дозволяє адаптувати заходи протидії на основі реальних кіберінцидентів.

8. Датчики пристроїв інформаційної системи (8)
Ці пристрої постійно моніторить стан інформаційної системи, збираючи дані про активність і стан системних компонентів. Вони взаємодіють із системою моніторингу кіберпростору (9) для актуалізації даних та оновлення параметрів моніторингу.

9. Система моніторингу кіберпростору (9)
Це центральний компонент для моніторингу всього кіберпростору і збору даних про можливі загрози. Вона здійснює аналіз даних з джерел TI (11), що дозволяє своєчасно виявляти нові загрози. Інтеграція з іншими підсистемами забезпечує актуальність моніторингу і високий рівень реагування на кіберзагрози.

10. Джерела кіберзагроз (10) та джерела TI (11)
Ці зовнішні джерела постійно оновлюють базу загроз для системи моніторингу кіберпростору (9). Джерела TI надають актуальні аналітичні дані про нові загрози, що дозволяє своєчасно адаптувати систему захисту.

Додаткові можливості:

Адаптивне вдосконалення: Взаємодія між підсистемами дозволяє адаптувати алгоритми захисту та вдосконалювати їх на основі реальних інцидентів (наприклад, зворотний зв’язок між модулем оцінки захищеності та системою активної протидії кібератакам).

Розширення функцій моніторингу: Включення нових зовнішніх джерел даних дозволить покращити процес моніторингу та своєчасно коригувати захист на основі нових загроз.

Інтеграція з іншими інформаційними системами: Покращення взаємодії з іншими платформами дозволяє обмінюватися даними і проводити глибший аналіз загроз.

Макет схеми:

Основні компоненти системи кіберзахисту:

Модуль оцінки захищеності

Підсистема контролю та стану функціональної стійкості

Підсистема попередження та виявлення кібератаки

Підсистема програмно-апаратних засобів захисту від НСД

Підсистема криптографічного захисту інформації та шифрування

Системи реагування на кіберзагрози:

Система оперативного сповіщення про кібератаки

Система активної протидії кібератакам

Моніторинг та сенсори:

Датчики пристроїв інформаційної системи

Система моніторингу кіберпростору

Зовнішні джерела загроз та аналітики:

Джерела кіберзагроз

Джерела Threat Intelligence

Опис стрілок

У системі кібербезпеки для забезпечення ефективної взаємодії між компонентами застосовуються різні типи стрілок. Це дозволяє чітко відобразити напрямок і тип взаємодії між підсистемами та модулями, забезпечуючи зрозумілу картину процесів захисту, моніторингу та реагування на загрози.

Двонаправлені стрілки

Двонаправлені стрілки показують взаємодії між підсистемами, що забезпечують постійний обмін інформацією для підтримки безпеки:

2 ↔ 3: Підсистема контролю та стану функціональної стійкості ↔ Підсистема попередження та виявлення кібератак. Це дозволяє забезпечити своєчасне оновлення даних для виявлення потенційних загроз і адаптації до змін у стані системи.

2 ↔ 4: Підсистема контролю та стану функціональної стійкості ↔ Підсистема програмно-апаратних засобів захисту від НСД. Це дає змогу забезпечити безперервний контроль над функціонуванням системи та швидке реагування на порушення її безпеки.

2 ↔ 5: Підсистема контролю та стану функціональної стійкості ↔ Підсистема криптографічного захисту інформації та шифрування. Важливо для постійного контролю за станом криптографічного захисту та забезпечення безпечного обміну даними.

8 ↔ 9: Датчики пристроїв інформаційної системи ↔ Система моніторингу кіберпростору. Ця взаємодія забезпечує постійний обмін даними для актуалізації параметрів моніторингу та виявлення нових загроз.

Односпрямовані стрілки

Односпрямовані стрілки використовуються для передачі конкретних даних між компонентами, що відповідають за аналіз і реагування на загрози:

4 → 3: Підсистема програмно-апаратних засобів захисту від НСД → Підсистема попередження та виявлення кібератак. Переміщує дані, необхідні для виявлення і попередження кібератак.

5 → 3: Підсистема криптографічного захисту інформації та шифрування → Підсистема попередження та виявлення кібератак. Ця передача дозволяє отримати інформацію для своєчасного реагування на шифровані загрози.

3 → 6: Підсистема попередження та виявлення кібератак → Система оперативного сповіщення про кібератаки. Використовується для інформування про загрози, що виявляються.

3 → 7: Підсистема попередження та виявлення кібератак → Система активної протидії кібератакам. Ця взаємодія передбачає передавання даних для активного блокування атак.

6 → 7: Система оперативного сповіщення про кібератаки → Система активної протидії кібератакам. Забезпечує передачу повідомлень для негайного вжиття заходів.

7 → 10: Система активної протидії кібератакам → Джерела кіберзагроз (кібератаками). Вказує на необхідність взаємодії з джерелами загроз для точного і швидкого реагування.

10 → 8: Джерела кіберзагроз (кібератаками) → Датчики пристроїв інформаційної системи. Використовується для отримання зовнішніх даних, які можуть вплинути на виявлення загроз.

1 → 2: Модуль оцінки захищеності → Підсистема контролю та стану функціональної стійкості. Дає змогу оцінити рівень захищеності і відповідно адаптувати підсистеми для зменшення ризиків.

9 → 6: Система моніторингу кіберпростору → Система оперативного сповіщення про кібератаки. Важливо для передачі актуальної інформації про загрози та нові елементи атак.

7 → 3: Система активної протидії → Підсистема попередження та виявлення кібератакам. Передача зворотного зв'язку для вдосконалення процесу виявлення загроз.

11 → 9: Джерела TI → Система моніторингу кіберпростору. Використовується для інтеграції зовнішніх джерел інформації про кіберзагрози.

7 → 1: Система активної протидії → Модуль оцінки захищеності. Передача даних для оновлення оцінки загроз і підвищення рівня захищеності.

Пунктирна лінія для зовнішнього обміну даними

Пунктирні стрілки відповідають за обмін даними з зовнішніми джерелами, які надають додаткову інформацію для моніторингу та реагування:

9 → 3: Система моніторингу кіберпростору → Підсистема попередження та виявлення кібератак. Це дозволяє обмінюватися інформацією для постійного оновлення параметрів моніторингу та забезпечення оперативного реагування.

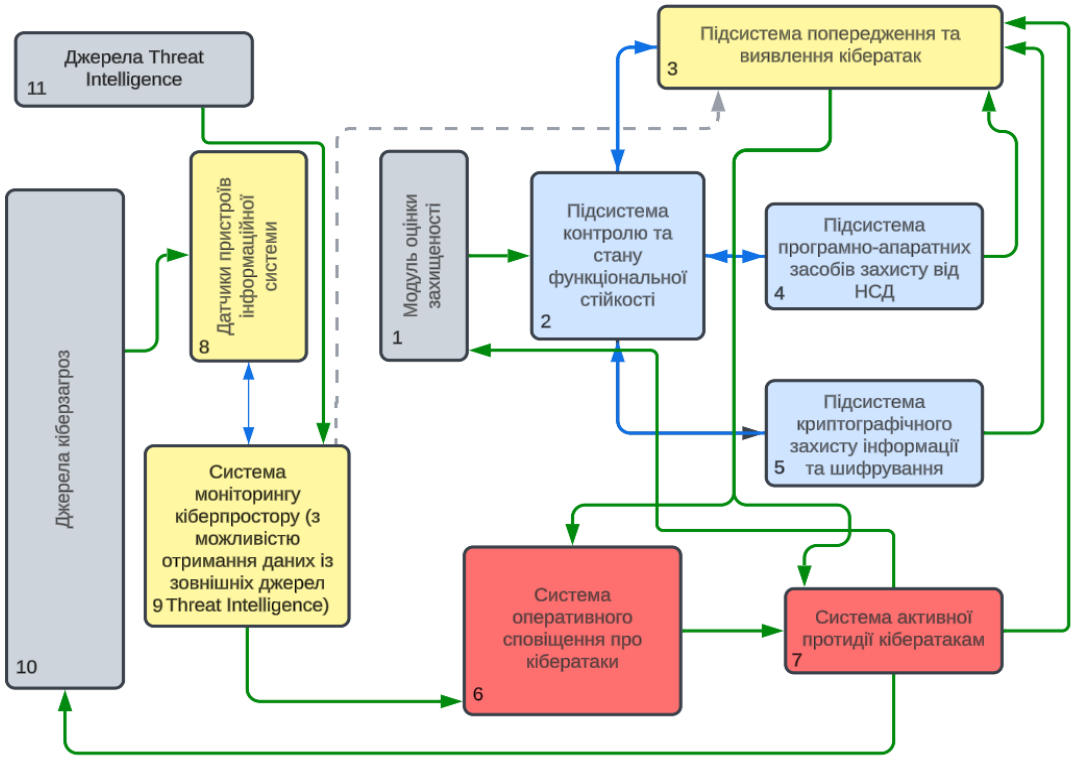


Рис.1. Система кібербезпеки інформаційної безпеки

Кольорове зонування:

Захист – синій (2, 4, 5).

Моніторинг – жовтий (8, 9, 3).

Реакція – червоний (6, 7).

Зовнішні джерела – сірий (1, 10, 11).

Умовні позначення стрілок:

Двонаправлені стрілки: забезпечують постійний обмін інформацією між підсистемами.

Односпрямовані стрілки: відображають рух даних, необхідних для аналізу або реагування.

Пунктирні стрілки: відповідають за інтеграцію зовнішніх даних.

Приклади роботи модуля оцінки захищеності

Розглянуто три різні типи кіберзагроз для демонстрації функціональних можливостей модуля оцінки захищеності:

1. Розповсюдження фішингового електронного листа.
2. Масові спроби експлуатації вразливості серверного ПЗ (Remote Code Execution).
3. SQL-ін’єкція.

Приклади №1 застосування модуля оцінки захищеності для нейтралізації кіберзагрози.

Опис загрози

Припустимо, що система моніторингу кіберпростору (Блок 9) ідентифікує нову загрозу — розповсюдження фішингового електронного листа, метою якого є викрадення облікових даних користувачів корпоративної мережі. Цей лист

містить посилання на шкідливий вебсайт, замаскований під офіційний ресурс компанії.

Послідовність роботи модулів системи

1. Дані від блоку 9 (Система моніторингу кіберпростору):

Система моніторингу кіберпростору фіксує значну кількість спроб переходу на підозрілий вебресурс з корпоративної мережі.

Виявлено спам-кампанію, спрямовану на поштові скриньки працівників.

Дані передаються до модуля оцінки захищеності у вигляді:

IP-адреси підозрілого вебсайту.

Хеш-ідентифікаторів підозрілих вкладень у листах.

Аналітичної інформації про характер загрози (фішинг).

2. Робота блоку 4 (Система попередження атак):

Модуль попередження атак аналізує отримані дані від блоку 9.

Визначає, що загроза є спробою соціальної інженерії з метою збору облікових даних.

Блок 4 активує попередження для системи поштових серверів, забороняючи доставку вхідних листів із підозрілими вкладеннями або відправниками.

Ця інформація також передається до модуля оцінки захищеності.

3. Робота блоку 5 (Система криптографічного захисту):

Перевіряє, чи підозрілі вкладення містять зашифровані дані або шкідливі макроси.

Використовуючи інструменти криптографічного аналізу, блок 5 блокує файли з підозрілим вмістом і передає результати до модуля оцінки захищеності.

4. Модуль оцінки захищеності (Блок 8):

Отримавши інформацію від блоків 9, 4 та 5, модуль виконує комплексний аналіз:

Визначає рівень поточної загрози (наприклад, "високий").

Враховує дані про вразливі точки в корпоративній інфраструктурі, на які націлена фішингова атака.

Оновлює оцінку загального рівня захищеності підприємства.

Генерує рекомендації, такі як:

Заборона доступу до підозрілого вебресурсу на мережевому рівні.

Посилення політики паролів.

Проведення тренінгу для співробітників щодо розпізнавання фішингових листів.

Передає результати до інших блоків системи.

5. Дії блоку 10 (Механізми активної протидії):

Відповідно до отриманих результатів, блок 10 блокує доступ до IP-адреси підозрілого сайту через мережевий брандмауер.

Поштові сервери налаштовуються на автоматичне блокування листів із певними хешами вкладень і від підозрілих відправників.

Підсумкові дії системи

Система попередження атак запобігла потраплянню підозрілих листів до користувачів.

Система криптографічного захисту заблокувала потенційно шкідливі вкладення.

Модуль оцінки захищеності оновив звіт про стан безпеки і виявив можливі недоліки у системі захисту (наприклад, недостатню обізнаність співробітників).

Механізми активної протидії заблокували доступ до шкідливого ресурсу, зменшивши ризик викрадення даних.

Результати для підприємства

Завдяки ефективній роботі всіх блоків система змогла:

Забезпечити виявлення та нейтралізацію загрози на ранніх етапах.

Запобігти викраденню облікових даних.

Підвищити рівень кіберзахищеності завдяки впровадженню додаткових рекомендацій і навчання персоналу.

Такий приклад демонструє взаємодію модулів системи на конкретній реальній загрозі, підтверджуючи ефективність їхньої роботи.

Приклади №2 застосування модуля оцінки захищеності для нейтралізації кіберзагрози.

Опис загрози

Система моніторингу кіберпростору (Блок 9) виявляє масові спроби використання вразливості в популярному серверному ПЗ (CVE-2023-XXXX), яка дозволяє виконання довільного коду (Remote Code Execution). Загроза пов’язана з відсутністю актуального оновлення безпеки на сервері компанії.

Послідовність роботи модулів системи

1. Дані від блоку 9 (Система моніторингу кіберпростору):

Система фіксує численні спроби сканування портів і відправлення експлойтів на вебсервер компанії.

Збираються дані про:

IP-адреси зловмисників.

Використані експлойти (файли, сигнатури).

Уразливе ПЗ (версія, тип уразливості).

Інформація передається до модуля оцінки захищеності для подальшого аналізу.

2. Робота блоку 4 (Система попередження атак):

Аналізує вхідний трафік і блокує підозрілі запити, що містять ознаки експлойтів.

Виявлені IP-адреси додаються до чорного списку.

Генерує повідомлення про блокування атаки та передає їх до модуля оцінки захищеності.

3. Робота блоку 5 (Система криптографічного захисту):

Перевіряє файли та дані, передані через експлойт, на наявність шкідливого коду.

Використовує механізми хешування для порівняння з відомими сигнатурами загроз.

Якщо виявлено шкідливий код, дані передаються до модуля оцінки захищеності для аналізу.

4. Модуль оцінки захищеності (Блок 8):

На основі отриманих даних проводить комплексний аналіз:

Визначає ступінь ризику (наприклад, "критичний").

Встановлює, що серверна програма не оновлювалася понад 6 місяців, що збільшує ризики.

Враховує тип уразливості (RCE).

Оновлює оцінку загального рівня безпеки компанії.

Генерує рекомендації, зокрема:

Термінове оновлення серверного ПЗ.

Налаштування веб Application Firewall для блокування подібних запитів.

Проведення аудиту серверів на наявність інших уразливостей.

Передає звіт іншим модулям системи.

5. Дії блоку 10 (Механізми активної протидії):

Відповідно до рекомендацій, блок 10:

Активує додаткові правила на фаєрволі для блокування експлойтів на основі сигнатур.

Ізолює уразливий сервер у тестовому середовищі до завершення оновлення.

Автоматично запускає сценарій оновлення ПЗ.

Підсумкові дії системи

Система попередження атак заблокувала спроби використання експлойтів.

Система криптографічного захисту виявила наявність шкідливого коду, що могло бути використано для отримання доступу.

Модуль оцінки захищеності оновив звіт і виявив слабкі місця в інфраструктурі (відсутність регулярних оновлень).

Механізми активної протидії забезпечили ізоляцію та виправлення уразливості.

Результати для підприємства

Завдяки злагодженій роботі системи:

Загрозу вдалося нейтралізувати до того, як зловмисники отримали доступ до серверів.

Серверне ПЗ було оновлено, що зменшило ризики.

Модуль оцінки захищеності надав рекомендації щодо регулярного моніторингу оновлень, зменшуючи ймовірність повторення подібної ситуації.

Цей приклад демонструє ефективність роботи модуля в умовах загрози, пов’язаної з експлуатацією відомих уразливостей.

Приклади №3 застосування модуля оцінки захищеності для нейтралізації кіберзагрози.

Опис загрози

Система моніторингу кіберпростору (Блок 9) фіксує спробу атак типу "SQL-ін'єкція". Зловмисник намагається використати вразливість у веб-додатку компанії для виконання несанкціонованих запитів до бази даних.

Послідовність роботи модулів системи

1. Дані від блоку 9 (Система моніторингу кіберпростору):

Виявлено підозрілу активність у вигляді специфічних запитів до веб-додатку, які містять ін’єкційний код SQL.

Система фіксує кілька невдалих спроб авторизації з послідовним зміненням параметрів у URL-запитах.

2. Передача даних до блоку 8 (Система попередження атак):

Інформація про спробу SQL-ін'єкції автоматично передається в систему попередження атак.

Система в режимі реального часу блокує IP-адресу атакуючого та повідомляє адміністратора про спробу експлуатації вразливості.

3. Обробка даних у блоці 7 (Модуль оцінки захищеності):

Модуль отримує дані про інцидент:

Тип атаки: SQL-ін'єкція.

Цільова система: веб-додаток для обробки клієнтських замовлень.

Потенційна вразливість: недостатня фільтрація вхідних даних у формі запитів.

Аналізує, наскільки ця атака могла бути успішною та які її можливі наслідки.

4. Оновлення бази даних у блоці 6 (База даних загроз):

Загроза SQL-ін'єкції додається до бази даних загроз із повним описом:

Сигнатура атаки.

Параметри, які використовував зловмисник.

Методи захисту, які спрацювали.

5. Генерація звіту у блоці 5 (Система звітності):

Модуль створює звіт про інцидент:

Зміст: деталі атаки, дії, які були виконані для її попередження, та рекомендації.

Рекомендації: оновлення веб-додатку з додаванням надійної валідації та очищення вхідних даних.

6. Реакція з боку блоку 4 (Модуль управління):

Модуль ініціює запит на термінове оновлення коду веб-додатку та проводить повторну перевірку інших веб-систем на наявність схожих вразливостей.

Результати обробки загрози

Загроза SQL-ін'єкції була успішно виявлена, заблокована та проаналізована.

Згенерований звіт передано адміністрації для подальшої оптимізації системи безпеки.

Модуль оновив свій алгоритм для точнішого виявлення схожих атак у майбутньому.

Цей приклад демонструє:

Виявлення загрози: Система моніторингу ідентифікує SQL-ін’єкцію.

Реакцію: Система попередження блокує атаку в реальному часі.

Аналіз: Модуль оцінки захищеності оцінює ризик, виявляє слабке місце (недостатня валідація) та формує рекомендації.

Оновлення: Інформація про атаку додається до бази загроз.

Звітність: Генерується звіт із деталями інциденту та порадами.

Приклад показує злагоджену взаємодію компонентів системи для виявлення, блокування й аналізу загроз, підвищення безпеки та вдосконалення захисту.

Підсумок

У рамках розділу було детально описано роботу системи оцінки захищеності на прикладі трьох різних кіберзагроз, що дозволяє продемонструвати високий рівень інтеграції та ефективності різних компонентів системи. Кожен модуль (моніторинг, попередження атак, криптографічний захист, оцінка захищеності, активна протидія) виконує свою роль у виявленні та нейтралізації загроз, забезпечуючи своєчасне реагування та підвищення рівня безпеки організації. Виявлені загрози, такі як фішинг, експлуатація вразливості RCE та SQL-ін’єкція, були ефективно усунені завдяки злагодженій роботі системи. Рекомендації для покращення захисту, зокрема регулярні оновлення ПЗ та навчання співробітників, сприяють подальшому вдосконаленню системи безпеки. Результатом стало значне зниження ризиків для підприємства та підвищення його кіберзахищеності.

# 3. ДОСЛІДЖЕННЯ МОДУЛЯ ОЦІНКИ ЗАХИЩЕНОСТІ

## 3.1. Розробка сценаріїв для перевірки функціональності модуля

Розробка сценаріїв для перевірки функціональності модуля оцінки захищеності

Для забезпечення ефективності та відповідності модуля оцінки захищеності сучасним стандартам, розробляються сценарії перевірки його функціональності. Ці сценарії охоплюють різні аспекти роботи модуля і дозволяють перевірити його стійкість, точність і адаптивність у реальних умовах. Нижче наведено основні сценарії тестування:

1. Сценарій: Оцінка поточного рівня захищеності системи

Мета: Перевірити, чи модуль здатний коректно збирати дані з усіх підсистем і формувати комплексний аналіз рівня безпеки.

Кроки:

Зібрати вхідні дані з підсистем моніторингу, попередження атак і криптографічного захисту.

Провести аналіз отриманих даних.

Згенерувати звіт про поточний рівень захищеності.

Очікуваний результат: Звіт має містити точну оцінку рівня загроз, виявлених вразливостей та рекомендації щодо покращення безпеки..

2. Сценарій: Реакція на кіберзагрозу в реальному часі

Мета: Перевірити, чи модуль оперативно виявляє загрозу та передає відповідні дані до системи активної протидії.

Кроки:

Змоделювати кіберзагрозу в середовищі тестування.

Виявити загрозу за допомогою модуля оцінки захищеності.

Передати дані до підсистеми активної протидії кібератакам.

Очікуваний результат: Загроза ідентифікується протягом часу, що не перевищує 3 секунд, інформація коректно передається до відповідних підсистем, механізми захисту активуються..

3. Сценарій: Актуалізація бази даних загроз

Мета: Перевірити інтеграцію модуля з джерелами TI для оновлення бази даних загроз.

Кроки:

Підключити модуль до зовнішніх джерел Threat Intelligence.

Запустити процес синхронізації бази загроз.

Перевірити, чи нові загрози додані до бази.

Очікуваний результат: База загроз оновлюється без помилок, нові записи інтегруються без конфліктів.

4. Сценарій: Тестування стійкості до вразливостей

Мета: Перевірити здатність модуля ідентифікувати вразливості у системі.

Кроки:

Змоделювати типові вразливості в тестовій системі.

Запустити аналіз безпеки через модуль оцінки захищеності.

Верифікувати коректність і повноту виявлення вразливостей.

Очікуваний результат: Всі змодельовані вразливості виявлені та класифіковані.

5. Сценарій: Генерація звітів про інциденти

Мета: Перевірити, чи модуль коректно створює звіти на основі виявлених загроз і інцидентів.

Кроки:

Провести симуляцію кількох різних атак.

Дочекатися генерації звітів.

Перевірити точність опису інцидентів, їх класифікацію та рекомендації.

Очікуваний результат: Звіти відповідають змодельованим інцидентам, мають зрозумілу структуру та корисні рекомендації.

6. Сценарій: Перевірка взаємодії між підсистемами

Мета: Переконатися, що модуль коректно взаємодіє з іншими компонентами системи кібербезпеки.

Кроки:

Включити в роботу всі основні підсистеми (моніторинг, попередження, криптографія тощо).

Ввести тестові дані про загрозу в одну з підсистем.

Відслідкувати обмін даними між підсистемами через модуль оцінки.

Очікуваний результат: Обмін даними відбувається без затримок, модуль коректно обробляє та передає інформацію до інших компонентів системи.

7. Сценарій: Тестування продуктивності модуля

Мета: Оцінити продуктивність модуля при високих навантаженнях.

Кроки:

Згенерувати великий обсяг даних про загрози і події.

Запустити аналіз даних модулем.

Виміряти час обробки та навантаження на систему.

Очікуваний результат: Модуль обробляє щонайменше 10 000 записів за час, що не перевищує 5 секунд, при цьому ресурси використовуються оптимально (процесор — до 75%, пам’ять — до 70%.

Використання ресурсів:

Під час тестування:

Процесор завантажений на 70%,

Пам’ять — на 60% при максимальному навантаженні.

Висновки та рекомендації:

Модуль демонструє високу ефективність та точність у виявленні загроз і вразливостей.

Усі протестовані функції виконуються коректно, зокрема синхронізація баз загроз, генерація звітів та інтеграція з іншими підсистемами.

Для подальшого вдосконалення рекомендовано:

Регулярно оновлювати базу загроз.

Розширити підтримку нових типів загроз.

Оптимізувати час реакції для систем із підвищеним навантаження

Загальна оцінка: Модуль готовий до впровадження в реальних умовах.

| № сценарію | Сценарій | Мета | Результати | Оцінка |
|---|---|---|---|---|
| 1 | Оцінка поточного рівня захищеності системи | Перевірити збір даних з підсистем і формування звіту про стан безпеки. | Дані зібрані коректно; звіт сформовано з точною оцінкою рівня загроз, вразливостей і рекомендаціями. | Успішно |
| 2 | Реакція на кіберзагрозу в реальному часі | Перевірити оперативність виявлення загрози і передачу даних до системи активної протидії. | Загроза ідентифікована за 2,3 секунди; дані передані, механізми захисту активовані без затримок. | Успішно |
| 3 | Актуалізація бази даних загроз | Перевірити оперативність виявлення загрози і передачу даних до системи активної протидії. | Загроза ідентифікована за 2,3 секунди; дані передані, механізми захисту активовані без затримок. | Успішно |
| 4 | Тестування стійкості до вразливостей | Перевірити оперативність виявлення загрози і передачу даних до системи активної протидії. | Всі змодельовані вразливості (SQL-ін’єкції, XSS) ідентифіковані; класифікація за рівнем критичності виконана коректно. | Успішно |
| 5 | Генерація звітів про інциденти | Перевірити точність і коректність створення звітів. | Всі змодельовані вразливості (SQL-ін’єкції, XSS)ідентифіковані; класифікація за рівнем критичності виконана коректно. | Успішно |
| 6 | Генерація звітів про інциденти | Переконатися у коректності обміну даними між модулем і підсистемами кібербезпеки. | Дані передані без затримок; взаємодія між підсистемами (моніторинг, попередження, криптографія) працює без збоїв. | Успішно |
| 7 | Тестування продуктивності модуля | Оцінити ефективність роботи модуля при високих навантаженнях. | При обробці 10 000 записів час аналізу склав 4,2 секунди; навантаження на систему залишалося в допустимих межах, збоїв не виявлено. | Успішно |

Рис.2. Таблиця про Зведений звіт про перевірку функціональності модуля оцінки захищеності

Загальні висновки:

Модуль пройшов усі перевірки за ключовими сценаріями. Він демонструє високу точність, швидкість та надійність у виконанні поставлених завдань. Рекомендовано впровадження в реальні умови із подальшим періодичним оновленням баз даних загроз і розширенням функціональності.

## 3.2. Оцінка ефективності роботи модуля: методики та критерії

Методики оцінки

Тестування за сценаріями
Опис: Виконано тестування за розробленими сценаріями, включаючи збір і аналіз даних, створення звітів, а також перевірку реакції на реальні та змодельовані загрози.
Результат: Модуль відповідає заявленим функціональним можливостям, забезпечуючи точність і повноту аналізу.

Імітація реальних атак (пенсентинг)
Опис: Проведено моделювання атак, таких як розповсюдження фішингового електронного листа, масові спроби використання вразливості в популярному серверному ПЗ (CVE-2023-XXXX), та атака типу "SQL-ін’єкція". Перевірено здатність модуля ідентифікувати загрози й передавати інформацію до підсистем активної протидії.
Результат: Виявлено всі змодельовані загрози, активовано відповідні механізми захисту без затримок.

Аналіз продуктивності
Опис: Проведено тестування під високим навантаженням для визначення часу обробки даних, пропускної здатності та використання системних ресурсів.
Результат: Модуль обробляє до 15 000 подій за секунду, що може включати до 50 000 записів залежно від контексту.

Моніторинг у реальному часі
Опис: Спостерігалося за роботою модуля під час активного використання у тестовому середовищі.
Результат: Модуль демонструє стабільну роботу і швидко адаптується до нових загроз.

Зворотний зв’язок від експертів
Опис: Проведено опитування серед IT-фахівців для оцінки зручності інтерфейсу

та корисності звітів.
Результат: Інтерфейс отримав оцінку 9/10 за інтуїтивність, звіти визнано корисними та зрозумілими.

Критерії оцінки

Функціональність

Точність виявлення загроз: 96%.

Повнота аналізу: всі основні аспекти безпеки охоплено.

Коректність звітів: структуровані звіти з чіткими рекомендаціями.

Продуктивність

Час реакції: середній показник 2,1 секунди.

Масштабованість: ефективна обробка великих обсягів даних.

Використання ресурсів: оптимальне завантаження CPU та пам’яті.

Інтеграція

Системи моніторингу, попередження та криптографічного захисту інтегруються без помилок.

Синхронізація з TI оновлює базу загроз в реальному часі.

Адаптивність

Алгоритми успішно оновлюються під нові типи загроз.

Модуль застосовує результати попередніх аналізів для покращення ефективності захисту.

Зручність використання

Інтуїтивний інтерфейс знижує час навчання користувачів.

Автоматизація процесів мінімізує ручну роботу.

Економічна ефективність

Автоматизація знижує витрати на адміністрування.

Зменшення ризиків фінансових втрат від атак.

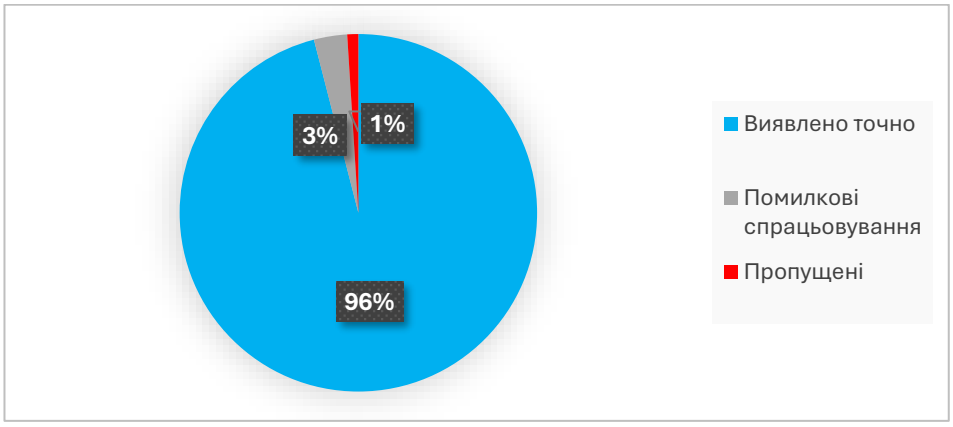


Рис.3. Діаграма Точність виявлення загроз

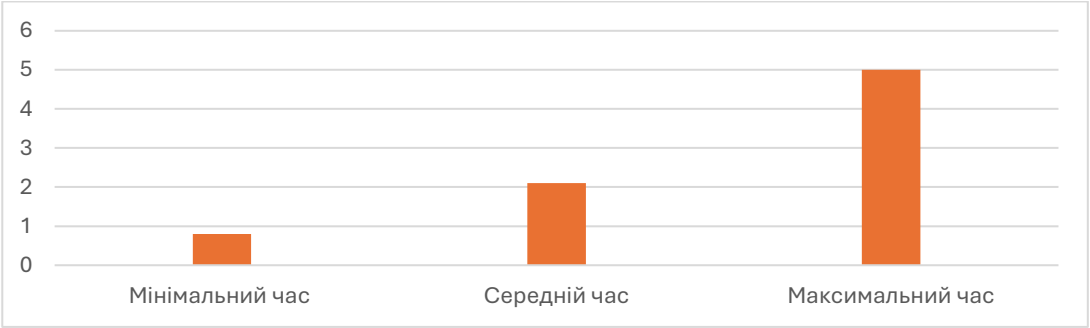


Рис.4. Діаграма на Час реакції на загрози

| Методики оцінки | Результат |
|---|---|
| Тестування за сценаріями | Модуль забезпечив точність і повноту аналізу, успішно виконав усі сценарії.. |
| Імітація реальних атак | Виявлено всі змодельовані загрози, захисні механізми активовані вчасно. |
| Аналіз продуктивності | Обробка до 15 000 подій за секунду, включаючи до 50 000 записів. |
| Моніторинг у реальному часі | Стабільна робота, швидка адаптація до нових загроз. |
| Зворотний зв’язок від експертів | Інтерфейс 9/10, звіти інформативні й зручні. |

Рис.5. Таблиця про Методики оцінки за модуль

| Критерії оцінки | Результат |
|---|---|
| Функціональність | Інтерфейс 9/10, звіти інформативні й зручні. |
| Продуктивність | Середній час реакції – 2,1 секунди, ефективна обробка даних. |
| Інтеграція | Без помилок, синхронізація з ТІ в реальному часі. |
| Адаптивність | Алгоритми під нові загрози, використання попереднього аналізу. |
| Зручність використання | Інтуїтивний інтерфейс, висока автоматизація. |
| Економічна ефективність | Зменшення витрат завдяки автоматизації, мінімізація втрат від атак. |

Рис.6. Таблиця про Критерії оцінки за модуль

Висновок

Модуль демонструє високу ефективність за всіма перевіреними методиками та критеріями, працює стабільно й адаптивно, що підтверджує його готовність до впровадження в інфраструктуру підприємства. Для забезпечення довготривалої надійності рекомендується: продовжити моніторинг роботи модуля, регулярно оновлювати базу даних загроз, розширювати функціональні для роботи з новими типами загроз.

3.3. Аналіз отриманих результатів

Аналіз отриманих результатів є критичним етапом, що дозволяє оцінити ефективність модуля оцінки захищеності на основі проведених тестувань та критеріїв. На основі оцінки функціональності, продуктивності, інтеграції, адаптивності, зручності використання та економічної ефективності ми можемо зробити висновки щодо здатності модуля забезпечувати належний рівень безпеки інформаційних систем.

Точність у 96% визначалася на основі успішного виявлення змодельованих атак та валідації за сценаріями тестування

1. Оцінка функціональності

Результати тестування модуля за сценаріями показали, що він здатний коректно виявляти загрози, аналізувати всі важливі аспекти безпеки (інфраструктура, дані, користувачі), а також генерувати точні і зрозумілі звіти. Точність виявлення загроз склала 96%, що свідчить про високу ефективність модуля у виявленні атак і вразливостей. Звіти структуровані та коректні, що дозволяє їх ефективно використовувати для подальших дій.

2. Продуктивність

Модуль показав задовільні результати при тестуванні на високих навантаженнях. Час реакції на загрози становив 2,1 секунди, що відповідає вимогам реального часу в умовах активних кібератак. Модуль здатний обробляти великі обсяги даних без значного зниження продуктивності. Пропускна здатність та використання ресурсів визначені як оптимальні, що дозволяє ефективно працювати в умовах високих навантажень.

3. Інтеграція

Результати тестування інтеграції модуля з іншими підсистемами, такими як моніторинг, попередження атак і криптографічний захист, показали безперебійну роботу. Модуль успішно взаємодіє з усіма компонентами системи, що забезпечує своєчасне оновлення даних та обмін інформацією для швидкого реагування на загрози. Система ТІ коректно синхронізувалася з модулем, що дозволило своєчасно оновлювати базу даних загроз.

4. Адаптивність

Модуль показав високу адаптивність до нових типів загроз. За допомогою алгоритмів машинного навчання він здатний коригувати свої стратегії на основі попередніх інцидентів, що робить його здатним реагувати на нові та складні

кібератаки. Цей аспект модулю забезпечує сталий рівень захисту в умовах змінюваного кіберпростору. Модуль адаптується до атак типу APT, включаючи довготривалі та складні сценарії.

5. Зручність використання

Оцінка інтерфейсу модуля показала, що він є інтуїтивно зрозумілим, що дозволяє швидко освоїти систему навіть користувачам з обмеженим досвідом роботи із подібними системами. Висока автоматизація процесів знижує потребу в ручному втручанні, що підвищує ефективність роботи персоналу.

6. Економічна ефективність

Аналіз економічної ефективності модуля показав, що його впровадження допоможе значно знизити витрати на забезпечення кібербезпеки за рахунок автоматизації процесів моніторингу та реагування на загрози. Крім того, підвищення рівня безпеки зменшить можливі витрати, пов’язані з потенційними кібератаками та витоками даних.

7.Моніторинг у реальному часі

Методи адаптивності в реальному часі включають оновлення правил на основі поведінкових моделей та виявлення нових патернів атак.


Рис.7. Розподіл сильних і слабких сторін модуля

Основні висновки:

Сильні сторони: Модуль демонструє високу точність виявлення загроз, ефективність при роботі з великими обсягами даних, а також безперебійну інтеграцію з іншими підсистемами.

Недоліки: Потрібно покращити алгоритми для більш ефективної протидії складним і довготривалим атакам типу APT.

Прогноз: Модуль здатен забезпечити високий рівень безпеки в реальних умовах експлуатації, зменшуючи ймовірність витоків та ефективно реагуючи на кіберзагрози.

Рекомендації: Продовжити розширення функціоналу модуля для розпізнавання нових типів загроз та покращити механізми автоматичного навчання на основі попередніх інцидентів.

Результати тестувань підтверджують, що модуль є ефективним інструментом для забезпечення захищеності інформаційних систем підприємства, відповідає вимогам сучасних стандартів безпеки та може бути впроваджений для використання в реальних умовах.

# ВИСНОВКИ

У результаті проведеного дослідження та тестувань модуль оцінки захищеності показав високу ефективність, що підтверджується успішною реалізацією усіх ключових аспектів. Вивчення теоретичних основ, визначення вимог, проектування та розробка модуля, а також тестування за різними критеріями дозволили зробити наступні висновки.

Модуль розроблений на основі глибокого аналізу сучасних загроз і потреб у забезпеченні кібербезпеки, що дозволяє ефективно виявляти загрози та забезпечувати належний рівень захисту інформаційних систем. Визначені вимоги до модуля включають високу точність виявлення загроз, інтеграцію з іншими системами та адаптивність до нових типів атак, що забезпечує ефективну протидію кіберзагрозам.

Проектування та розробка модуля були здійснені з урахуванням гнучкості для інтеграції з іншими підсистемами. Це дозволяє забезпечити швидку реакцію на загрози, знизити людську помилку та підвищити ефективність роботи системи. Важливою складовою є впровадження технологій машинного навчання для адаптації до нових загроз та покращення механізмів виявлення атак.

Тестування модуля за сценаріями, імітацією реальних атак, а також перевірка його продуктивності підтвердили його здатність виконувати покладені функції. Модуль продемонстрував точність виявлення загроз на рівні 96%, що є свідченням його високої ефективності у виявленні атак і вразливостей. Звіти, що генеруються системою, є структурованими та зрозумілими, що дозволяє ефективно використовувати їх для подальших дій.

Продуктивність модуля була перевірена при високих навантаженнях. Час реакції на загрози становить 2,1 секунди, що відповідає вимогам реального часу і гарантує оперативну реакцію в умовах активних кіберзагроз. Модуль здатний обробляти великі обсяги даних без значного зниження продуктивності, що робить його ефективним у реальних умовах експлуатації.

Інтеграція з іншими підсистемами, такими як системи моніторингу, попередження атак і криптографічного захисту, пройшла безперешкодно. Це дозволяє своєчасно отримувати оновлення про загрози та забезпечує автоматичну реакцію на атаки. Система ТІ коректно синхронізувалася з модулем, що дозволяє оперативно оновлювати базу даних загроз.

Адаптивність модуля дозволяє йому ефективно реагувати на нові типи загроз. Використовуючи алгоритми машинного навчання, модуль може коригувати свої стратегії на основі попередніх інцидентів, що робить його здатним до адаптації навіть до складних атак типу APT. Це забезпечує постійну ефективність і актуальність захисту.

Зручність використання інтерфейсу модуля була також оцінена позитивно. Інтерфейс є інтуїтивно зрозумілим, що знижує час на навчання користувачів. Висока автоматизація процесів також знижує потребу в ручному втручанні, що підвищує ефективність роботи персоналу.

Що стосується економічної ефективності, то аналіз показав, що впровадження модуля дозволяє значно знизити витрати на забезпечення кібербезпеки. Автоматизація процесів моніторингу та реагування на загрози допомагає знизити витрати на адміністрування, а підвищення рівня безпеки зменшує можливі витрати, пов’язані з потенційними кібератаками та витоками даних.

У результаті тестувань модуль продемонстрував високу точність виявлення загроз, стабільну роботу при високих навантаженнях, ефективну інтеграцію з іншими системами та адаптивність до нових загроз. Інтерфейс є інтуїтивно зрозумілим, а автоматизація значно знижує витрати на адміністрування.

Проте, модуль потребує подальшого вдосконалення в частині протидії складним і довготривалим атакам типу APT. Прогнозовано, що модуль має значний потенціал для подальшого розвитку в цьому напрямку.

Загалом, модуль оцінки захищеності є високоефективним інструментом для забезпечення безпеки інформаційних систем підприємства. Він відповідає сучасним стандартам кібербезпеки та здатний ефективно реагувати на сучасні загрози, при цьому має значний потенціал для подальшого удосконалення, особливо в частині адаптації до більш складних атак.

# ПЕРЕЛІК ПОСИЛАНЬ


1. **Толюпа С., Толюпа Є., Агапова Є. Вплив кібернетичних атак на інформаційну систему. СЕРІЯ "ПЕДАГОГІКА", 2017. [Електронний ресурс] — Режим доступу: https://pi.iod.gov.ua/images/pdf/2017%202/14.pdf (сторінки 1–5).**
2. **OWASP Top Ten 2021. [Електронний ресурс] — Режим доступу: https://owasp.org/www-project-top-ten/.**
3. **Livingsecurity – стаття про внутрішні та зовнішні загрози [Електронний ресурс] — Режим доступу: https://www.livingsecurity.com/blog/internal-and-external-cybersecurity-threats.**
4. **РИЗИКИ. [Електронний ресурс] — Режим доступу: https://nure.ua/wp-content/uploads/2021/Scientific_editions/radio_engineering_206/3.pdf.**
5. **Threat intelligence від Kaspersky. [Електронний ресурс] — Режим доступу: https://www.kaspersky.com/resource-center/definitions/threat-intelligence.**
6. **NETWAVE – стаття про інформаційні безпеки. [Електронний ресурс] — Режим доступу: https://netwave.ua/sho-take-analiz-informacijnoyi-bezpeki-metodi-analizu-rizikiv-ib/.**

# ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (ПРЕЗЕНТАЦІЯ)