УДК 004.056.55

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ДЛЯ ПІДВИЩЕННЯ ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ

Гуменюк І.О.., науковий керівник Панкратьєв В.О.

Актуальність. У сучасних умовах стрімкого розвитку цифрових технологій та зростання кількості кіберзагроз, питання безпеки інформаційних систем набуває особливої актуальності. Інформація стала одним із ключових ресурсів, втрата або компрометація якої може призвести до суттєвих фінансових збитків, втрати репутації, а в окремих випадках — навіть до припинення діяльності організацій.

Більшість підприємств використовує широкий спектр IT-рішень, проте часто їхній рівень безпеки є недостатнім для ефективного протистояння сучасним загрозам. Це зумовлює потребу в розробці й впровадженні спеціалізованого програмного забезпечення, що забезпечує комплексний підхід до захисту інформаційних систем, включаючи запобігання, виявлення та реагування на інциденти.

Мета подальшого магістерського дослідження полягає у розробці та теоретично обґрунтуванні концепції програмного забезпечення для підвищення захисту інформаційних систем, що поєднує інструменти моніторингу, аналізу, попередження та реагування на кіберзагрози з урахуванням сучасних технологічних підходів.

У межах дослідження передбачається:

- провести аналіз існуючих засобів забезпечення інформаційної безпеки;
- дослідити теоретичні підходи до побудови систем виявлення вторгнень (IDS/IPS), SIEM-систем і Zero Trust-архітектур;
- спроєктувати архітектуру програмного рішення з функціями автоматичного моніторингу, оцінки ризиків і адаптивного реагування;
- реалізувати прототип із можливістю інтеграції з корпоративною

IT-інфраструктурою та підтримкою машинного навчання для виявлення аномалій.

Наукова новизна полягає в інтеграції принципів Zero Trust, штучного інтелекту та інструментів глибокого аналізу мережевої активності в єдине програмне середовище, що дозволяє автоматизувати виявлення загроз і зменшити час реакції на інциденти.

Очікувані результати: Створення програмного забезпечення, здатного не лише пасивно реєструвати інциденти безпеки, а й активно запобігати їм, оперативно реагувати на підозрілу активність, проводити аналітику та надавати рекомендації для підвищення рівня захищеності інформаційної системи.

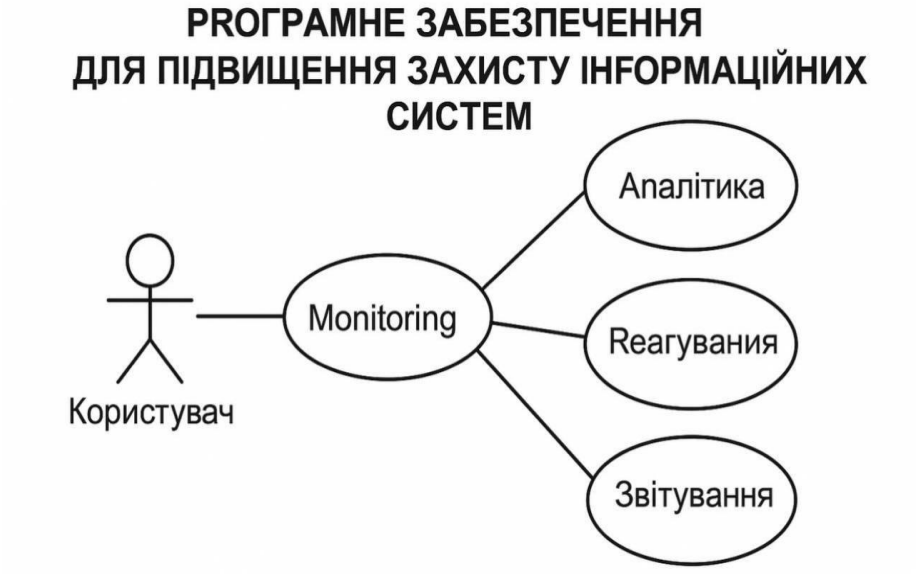

Рис. 1. Діаграма прецедентів

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Stallings W. Network Security Essentials. – 6th ed. – Pearson, 2023.

2. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS). – NIST Special Publication 800-94.

3. Microsoft. What is Microsoft Sentinel? – *https://learn.microsoft.com/en-us/azure/sentinel/*

4. Zero Trust Architecture – NIST Special Publication 800-207 – *https://csrc.nist.gov/publications/detail/sp/800-207/final*

5. Андрущенко І.О. Системи інформаційної безпеки: сучасні підходи та технології // Інформаційні технології. – 2022. – №1. – С. 33–40.

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ АСПЕКТИ РОЗРОБКИ КОМП'ЮТЕРНИХ СИСТЕМ

ЗБІРНИК НАУКОВИХ ПРАЦЬ ЗА МАТЕРІАЛАМИ
VII ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ
СТУДЕНТІВ І АСПІРАНТІВ
24 квітня 2025 року

Київ 2025

УДК 004

Відповідальна за випуск: М.І. Лендєл

Збірник наукових праць за матеріалами VII Всеукраїнської науково-практичної конференції студентів і аспірантів «ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ АСПЕКТИ РОЗРОБКИ КОМП'ЮТЕРНИХ СИСТЕМ '2025», 24 квітня 2025 року, НУБіП України, Київ. – 452 с. (електронне видання)

Відповідальність за зміст публікацій несуть автори.