Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри
кібербезпеки та захисту
інформації
_____Іван ПАРХОМЕНКО
«___» червня 2025 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітній ступень бакалавр

освітня програма Кібербезпека
(назва освітньо-професійної програми)

на тему: «Механізм підвищення рівня захисту інформаційних систем шляхом впровадження штучного інтелекту»

Виконавець: студент IV курсу, групи КБ-42
_____ **Дмитро МАНЬКОВСЬКИЙ**
(підпис) (ім'я, прізвище)

	Підпис	**Ім'я ПРІЗВИЩЕ**
Керівник		Сергій ДАКОВ
Нормоконтроль		Олександр ТОРОШАНКО

Київ 2025

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____Іван ПАРХОМЕНКО
«29» листопада 2024 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньо-професійної програми)

Студенту **КБ-42** (група) **Маньковському Дмитру Олексійовичу** (прізвище ім'я по батькові)

Тема кваліфікаційної роботи «Механізм підвищення рівня захисту інформаційних систем шляхом впровадження штучного інтелекту»

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №6 від 28.11.2024 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Системи кібербезпеки, технології штучного інтелекту

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Необхідно дослідити поточний стан кібербезпеки у інформаційних системах, дослідити наявні вектори атак, та методи їх протидії. Також необхідно розглянути методики кібербезпеки на основі штучного інтелекту, дослідити реальні приклади програмних рішень і наскільки вони ефективніші за звичайні. А також на прикладі розгортання ELK Stack та Suricata, з застосуванням Isolation Forest, дослідити, як методики штучного інтелекту дозволяють краще ідентифікувати загрози за допомогою аналізу логів.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Можливість застосування даної роботи для вибору методик покращення кібербезпеки за рахунок штучного інтелекту.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 29 листопада 2024 року

Завдання видав _____ Сергій ДАКОВ
(підпис) (ім'я, прізвище)

Завдання прийняв до виконання _____ Дмитро МАНЬКОВСЬКИЙ
(підпис) (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	29.11.2024 – 22.12.2025	*виконано*
2	Аналіз літератури	11.01.2025 – 05.02.2025	*виконано*
3	Обґрунтування вибору рішення	06.02.2025 – 10.02.2025	*виконано*
4	Огляд проблематики в наявних системах кібербезпеки	11.02.2025 – 25.02.2025	*виконано*
5	Дослідження методів покращення кібербезпеки в інформаційних системах	26.02.2025 – 10.03.2025	*виконано*
6	Реалізація систем захисту інформації за допомогою засобів штучного інтелекту	11.03.2025 – 31.03.2025	*виконано*
7	Вироблення рекомендацій щодо покращення кібербезпеки за рахунок штучного інтелекту	01.04.2025– 11.04.2025	*виконано*
8	Оформлення пояснювальної записки	01.05.2025 – 23.05.2025	*виконано*
9	Підготовка до захисту кваліфікаційної роботи	25.05.2025 – 10.06.2025	*виконано*

Завдання видав _____ Сергій ДАКОВ
(підпис) (ім'я, прізвище)

Завдання прийняв до виконання _____ Дмитро МАНЬКОВСЬКИЙ
(підпис) (ім'я, прізвище)

Термін подання кваліфікаційної роботи до ЕК 13 червня 2025 року

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел та додатків. Основний текст займає 54 сторінки, включає в себе зміст, вступ, три розділи кваліфікаційної роботи, висновки та список джерел. Крім того, робота містить 4 додатки із загальною кількістю сторінок 7. У пояснювальній записці кваліфікаційної роботи міститься 18 рисунків і 1 таблиця.

Метою роботи є підвищення рівня кіберзахисту шляхом впровадження методик забезпечення кібербезпеки в інформаційних системах за допомогою інструментів штучного інтелекту.

Для досягнення зазначеної мети поставлено наступні завдання:

- зробити огляд проблематики в наявних системах кібербезпеки;
- дослідити механізми і методи покращення кібербезпеки за рахунок штучного інтелекту;
- розробити програмні рішення з залученням нейромереж з метою покращення стану кібербезпеки.

Об’єктом дослідження є процес впровадження кіберзахисту в інформаційнихсистемах за допомогою інструментів штучного інтелекту.

Предметом дослідження є методи та технології застосування штучного інтелекту для підвищення кібербезпеки інформаційних систем.

Практичною цінністю отриманих результатів є можливість її застосування для покращення систем кібербезпеки за рахунок впровадження систем штучного інтелекту.

Ключові слова: кібербезпека, штучний інтелект, вразливості, методи впровадження, порушення, інциденти.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

SIEM	-	Security Information and Event Management
SOAR	-	Security Orchestration, Automation, and Response
IDS/IPS	-	Intrusion Detection System/Intrusion Prevention System
DDoS	-	Distributed Denial of Service
IoT	-	Internet of things
AI	-	Artificial intelligence
ML	-	Machine learning
ШІ	-	Штучний інтелект
ELK	-	Elasticsearch, Logstach Kibana
DL	-	Deep learning
ІТ	-	Інформаційні технології
ПЗ	-	Програмне забезпечення

ВСТУП

У сучасному цифровому середовищі інформаційні системи відіграють ключову роль у функціонуванні практично всіх сфер суспільного життя — від державного управління та фінансів до охорони здоров'я, освіти й приватного бізнесу. Інформація стала одним із найцінніших ресурсів, тому забезпечення її захисту є пріоритетним завданням для організацій різного масштабу. Проте зі стрімким розвитком цифрових технологій одночасно зростає і рівень кіберзагроз.

Сучасні атаки стають все складнішими, цілеспрямованішими й автоматизованими, а методи, які раніше вважалися ефективними для кіберзахисту,більше не забезпечують належного рівня безпеки. Серед найбільш поширених загроз — фішинг, атаки типу «відмова в обслуговуванні» (DDoS), шкідливе програмне забезпечення, витоки даних, а також використання соціальної інженерії.У відповідь на ці виклики зростає потреба у впровадженні новітніх технологій, здатних оперативно реагувати на загрози, виявляти аномалії та прогнозувати потенційні ризики.

Одним із найперспективніших напрямів у цій сфері є застосування технологій штучного інтелекту (ШІ). Штучний інтелект дозволяє значно розширити можливості традиційних систем кібербезпеки. У контексті зростання кількості цифрових пристроїв, поширення інтернету речей (IoT), хмарних технологій та віддаленого доступу до ресурсів, впровадження ШІ в систему кібербезпеки є не просто актуальним, а життєво необхідним кроком. Саме тому дослідження ролі та потенціалу штучного інтелекту в забезпеченні інформаційної безпеки набуває особливої важливості у сучасному світі.

Метою кваліфікаційної роботи є підвищення рівня кіберзахисту шляхом впровадження методик забезпечення кібербезпеки в інформаційних системах за допомогою інструментів штучного інтелекту.

Об'єкт дослідження: процес впровадження кіберзахисту в

інформаційних системах за допомогою інструментів штучного інтелекту.

Предмет дослідження: методи та технології застосування штучного інтелекту для підвищення кібербезпеки інформаційних систем.

Оцінка сучасного стану проблеми на основі вітчизняної та зарубіжної літератури. На основі аналізу наукових публікацій, звітів міжнародних організацій та досліджень провідних фахівців у галузі ІТ і кібербезпеки встановлено, щозастосування ШІ є одним з найбільш перспективних підходів у боротьбі з кіберзагрозами. Закордонні дослідження акцентують увагу на розробці адаптивних систем моніторингу, виявлення аномалій, прогнозування атак та інтелектуального аналізу поведінки користувачів. Вітчизняні науковці зосереджують увагу на прикладному аспекті впровадження ШІ в українських реаліях — зокрема в контексті фінансової безпеки, оборони та захисту критичної інфраструктури. Проте спостерігається брак комплексних підходів, що поєднують технічні, організаційні та етичні аспекти використання штучного інтелекту у сфері кібербезпеки, що і визначає потребу в подальших дослідженнях.

Пратична цінність. Дана робота може бути застосована для покращення систем кібербезпеки за рахунок впровадження систем штучного інтелекту.

Новизна. Було запропоновано методи оцінки вразливостей та протидії вторгенням у інформаційні системи шляхом залученням методик штучного інтелекту (Kibana, Suricata, ELK). Було доведено доцільність впровадження такихсистем та їх ефективність у порівнянні з наявними системами.

Методи дослідження, застосовані у кваліфікаційній роботі:

- Аналіз літератури та інтернет-джерел;
- Аналіз нормативно – правових документів;
- Аналіз проблематики систем кібербезпеки;
- Моделювання механіхмів аналізу за допомогою систем штучного інтелекту;
- Тестування механізмів аналізу за допомогою систем штучного інтелекту.

Апробація роботи. Основні результати роботи доповідались на таких наукових заходах:

— Участь у міжнародній конференції «IT&I Satellite», 21 листопада 2024 року.) з доповіддю на тему «Measures To Improve Cyber Security Using Advanced Artificial Intelligence Systems».

— Публікація статті у журналі № 8 (2024) «Безпека інформаційних систем і технологій» на тему «Artificial intelligence systems in cybersecurity and their capabilitiesfront modern cyber threats»

РОЗДІЛ 1
ОГЛЯД ПРОБЛЕМАТИКИ В НАЯВНИХ СИСТЕМАХ КІБЕРБЕЗПЕКИ

1.1. Загальна характеристика інформаційних систем

У XXI столітті інформаційні системи стали основою функціонування як державних структур, так і бізнесу, освіти, охорони здоров'я та повсякденного життя. Вони забезпечують зберігання, обробку й передачу даних, автоматизацію процесів, прийняття рішень і розвиток нових послуг. Проте стрімка цифровізація супроводжується зростанням складності та взаємозалежності між компонентами інформаційного середовища. Це, у свою чергу, породжує нові виклики — передусім у сфері кібербезпеки [20].

Кібербезпека в сучасних умовах — це вже не лише питання технічного захисту. Вона охоплює організаційні, правові та етичні аспекти, що пов'язані із захистом конфіденційності, цілісності та доступності інформації. Збільшення кількості кіберзагроз, зокрема атак на критичну інфраструктуру, крадіжок персональних даних і поширення зловмисного програмного забезпечення, висвітлює потребу в надійних системах безпеки та постійній готовності до реагування на інциденти.

Водночас із численними викликами у сфері кібербезпеки спостерігається стрімке впровадження новітніх цифрових технологій, серед яких провідну роль відіграє штучний інтелект . Його інтеграція в інформаційні системи поступово змінює традиційні підходи до обробки даних, аналізу поведінки користувачів, прогнозування подій, а також виявлення і нейтралізації загроз у кіберпросторі.

Системи на основі алгоритмів машинного навчання та глибокого навчання здатні обробляти великі обсяги інформації у реальному часі, виявляти аномалії, які можуть свідчити про потенційні атаки, і навіть передбачати їхнє виникнення на основі історичних патернів. Це дозволяє не лише підвищити

ефективність моніторингу безпеки, а й автоматизувати багато процесів, які раніше потребували постійного втручання спеціалістів. Зокрема, ШІ вже успішно застосовується для аналізу поведінки користувачів, виявлення шкідливого ПЗ шляхом розпізнавання нетипових дій програм або файлів, використання чат-ботів у службах підтримки, які оперативно реагують на запити щодо кіберінцидентів, оптимізації управління ІТ-ресурсами через предиктивну аналітику, а також автоматизованого реагування на інциденти в режимі реального часу без участі людини.

Проте, попри безперечні переваги, впровадження ШІ супроводжується і низкою суттєвих ризиків. Як і будь-яка потужна технологія, штучний інтелект не є універсально безпечним інструментом. Одним із найбільш актуальних викликів є етичне використання ШІ, зокрема забезпечення прозорості прийняття рішень, уникнення упередженості в алгоритмах, а також гарантування, що системи не порушують права людини.

Крім того, існує небезпека втрати контролю над автоматизованими процесами. Якщо алгоритм приймає рішення без належної можливості зовнішнього втручання, це може призвести до хибних реакцій на ситуацію — наприклад, блокування критично важливих систем або обмеження доступу для легітимних користувачів.

Ще одним серйозним ризиком є використання ШІ для зловмисних цілей. Зокрема, уже сьогодні існують приклади застосування генеративного ШІ для створення фішингових листів, глибоких фейків (deepfakes), автоматизованих шкідливих ботів і навіть моделей, що допомагають кіберзлочинцям прогнозувати вразливості в інформаційних системах.

1.2. Стан кібербезпеки у сучасних ІС та мотиви виникнення порушень

У сучасному цифровому світі кібербезпека стала не лише технічним викликом, а й ключовим фактором стабільного функціонування інформаційних

систем. Стрімке поширення цифрових сервісів, хмарних технологій, Інтернету речей і мобільних пристроїв призвело до зростання площини атак, а з нею — і до збільшення кількості та складності кібератак. Попри активний розвиток засобів захисту, таких як багатофакторна автентифікація, архітектура Zero Trust, системи виявлення вторгнень та аналітика поведінки, кіберзагрози продовжують залишатися серйозною проблемою як для бізнесу, так і для державного сектору.

Сучасні інформаційні системи зазвичай мають розгалужену інфраструктуру та використовують численні сервіси сторонніх постачальників, що створює додаткові вектори атак. Крім технічних вразливостей, однією з головних проблем залишається людський фактор: фішинг, соціальна інженерія, недбалість користувачів і внутрішні порушення часто призводять до компрометації систем. Значна частина атак супроводжується економічними збитками, втратою персональних або комерційних даних, пошкодженням репутації та призупиненням критичних процесів.

Окрім цього, глобальні тенденції, такі як активізація хактивізму, кібервійни та атак на критичну інфраструктуру, підвищують актуальність комплексної кібербезпеки. Регуляторні вимоги, зокрема GDPR, NIS2 та національні закони про захист інформації, зобов’язують організації впроваджувати формалізовані політики безпеки, проводити регулярний аудит і навчання персоналу. Водночас ринок відчуває дефіцит кваліфікованих фахівців.

Рисунок 1.1 - Мотиви порушень в інформаційних системах

Між іншим, існують різні мотиви вчинення порушень у інформаційних системах. Вони зображені схематично на рисунку 1.1.

Безвідповідальність є однією з основних причин порушень у різних сферах діяльності — від виробничих процесів до інформаційної безпеки.

- Відсутність контролю з боку керівництва створює атмосферу безкарності. Коли управлінці не несуть відповідальності за дії підлеглих або самі подають негативний приклад, це сприяє формуванню толерантного ставлення до порушень у колективі.
- Пасивність співробітників, які усвідомлюють можливі загрози, але свідомо не вживають заходів (через байдужість або страх), також посилює ризики.
- Недбалість обслуговуючого персоналу, який не дотримується правил експлуатації обладнання чи зневажає інструкції, може призвести до аварій, витоків інформації або порушення техніки безпеки.
- Відсутність персональної відповідальності за вчинки стимулює порушення: якщо працівник знає, що його не покарають або провина буде перекладена на інших, він буде менш схильний дотримуватись встановлених норм і вимог.

Прикладом безвідповідальності є відсутність у компанії чітких санкцій за порушення правил поводження з конфіденційною інформацією. Працівник, незамислюючись, копіює робочі файли на особисту флешку, що в майбутньому призводить до витоку даних.

Неефективне управління, слабка внутрішня дисципліна й неконструктивна корпоративна культура можуть формувати сприятливе середовище для порушень.

- Недосконаліть системи управління (відсутність чітких регламентів, нестача контролюючих механізмів) часто сприяє хаосу і допускає зловживання.
- Брак контролю за дотриманням стандартів призводить до поступового «розмивання» правил. Якщо відсутній систематичний моніторинг або аудит, співробітники перестають дотримуватись вимог.

- Організаційна культура, що толерує порушення, — один із найнебезпечніших чинників. Висловлювання на кшталт «усі так роблять», «ми так завжди працювали», «важливий результат, а не спосіб» стають нормою поведінки.
- Нерівномірний розподіл відповідальності може створити відчуття несправедливості або безвиході серед співробітників.

Прикладом організаційних мотивів порушень вважається обхід процедур укладання договорів без юридичної перевірки, щоб не втрачати клієнта. Зрештою,це призводить до судових суперечок і фінансових збитків.
Фінансовий інтерес часто стає головною причиною свідомих порушень з боку як керівників, так і виконавців.

- Зниження витрат за рахунок порушення норм (наприклад, нехтуванням вимогами охорони праці або екологічними стандартами) дозволяє компаніям отримати короткострокову вигоду, але створює довгострокові ризики.
- Прагнення до максимізації прибутку будь-якою ціною призводить до того, що дотримання закону чи етики відходить на другий план.
- Уникнення витрат (податків, штрафів, компенсацій) стимулює ухилення від законодавчих вимог через сірі або чорні схеми.
- Нереальні KPI чи системи мотивації також можуть підштовхувати до порушень — якщо працівник розуміє, що виконати план чесно неможливо.

Наприклад, відділ безпеки вирішує не використовувати сертифіковане програмне забезпечення, а використовує дешевші аналоги, щоб вкластися в кошторис і отримати прибуток. Це знижує якість роботи систем та створює небезпеку.

Соціальний тиск, особисті амбіції або незадоволення умовами праці такожможуть сприяти порушенням.

- Нездорова конкуренція між працівниками або компаніями може формувати агресивну поведінку, коли заради перемоги дозволяються будь-які засоби — включно з неетичними чи незаконними.
- Відчуття несправедливості — коли працівники вважають, що їх не

цінують, недоплачують або ставляться упереджено, — знижує рівень лояльності та стимулює до саботажу, помсти або нехтування обов'язками.

- Погані умови праці, недостатній захист прав, небезпечне або токсичне середовище штовхають співробітників до порушень як форми протесту або виживання.
- Бажання самоствердитися, проявити силу, здобути особисту вигоду, вплив або статус — ще один мотив, що часто ігнорується в аналізах ризиків.
- працівники намагаються привернути увагу до себе, продемонструвати свою «винятковість» шляхом зухвалих або ризикованих дій.

Наприклад, співробітник, який почувається недооціненим, навмисно порушує правила безпеки, демонструючи, що система без нього не працює. Інший працівник продає внутрішню інформацію конкурентам, вважаючи, що компанія ставиться до нього несправедливо.

1.3. Загрози та вектори атак в інформаціних системах

Загрози інформаційним системам дуже широкі і багатогранні, при тому ж постійно зростає їх рівень. Таким чином, загрози у інформаційних системах розподілені за наступними категоріями, які зображені на рисунку 1.2:

Рисунок 1.2 - Основні загрози інформаційним системам

1) За властивістю інформації, що порушується

- Доступність означає, що інформаційні ресурси мають бути доступні користувачам тоді, коли це потрібно. Прикладом агрози є DDoS-атака

(розподілена атака на відмову в обслуговуванні), коли сервер перевантажується і перестає відповідати на запити.

- Цілісність означає, що інформація повинна залишатися незміненою та точною, не повинна бути змінена несанкціоновано Приклаом є віруси, трояни, атаки на бази даних, впровадження шкідливого коду, підробка даних.
- Конфіденційність означає доступ до чутливої інформації повинен бути лише у дозволених осіб, визначених системою безпеки. Прикладом порушень є перехоплення даних, крадіжка логінів і паролів, несанкціонований доступ до файлів.

2) За природою виникнення та способом здійснення

- Випадкові загрози виникають без навмисного впливу людини. Прикладами є природні катастрофи (пожежі, повені, землетруси), а також аварії обладнання (відмова роботи серверів, збій електропостачання) .
- Навмисні загрози вчиняються навмисно людьми з метою завдати шкоди. Прикладами є кіберзагрози (віруси, трояни, хакерські атаки, викрадення даних, фішинг, соціальна інженерія (психологічні методи впливу на працівників з метою викрадення даних (наприклад, фішинг, підроблені електронні листи, обман персоналу)).

3) За розташуванням джерела загроз

- Всередині контрольованої зони причиною порушень може бути недобросовісний персонал (співробітники, які мають доступ до систем і використовують його зі шкідливими намірами (навмисно або через недбалість), внутрішні кібератаки, які можуть бути здійснені через привілейований доступ, або після компрометації облікового запису.
- Зовнішні загрози, а саме хакери, шпигуни, конкуренти, які діють із зовнішнього середовища.

4) За наслідками

- Втрата чи пошкодження даних — часткова або повна втрата важливої інформації.
- Втрата конфіденційності — витік персональних або комерційних

даних.

- Втрата цілісності — дані змінені або підроблені.
- Втрата доступності — системи або сервіси стають недоступними для користувачів.
- Фінансові втрати — прямі (штрафи, відшкодування) або непрямі (втрата прибутку).
- Втрата репутації — втрата довіри клієнтів, партнерів, громадськості.
- Юридичні наслідки — судові позови, перевірки, санкції з боку регуляторів. Щодо векторів атак на інформаційні системи, то у зв’язку з дуже швидким ростом технологій зловмисники винаходять все нові й нові засоби вразити жертву.

Один із найпоширеніших способів — соціальна інженерія. Вона базується не на технічних вразливостях, а на людському факторі: обманом, шляхом фішингових листів або телефонних дзвінків, атакуючий змушує людину самостійно розкрити паролі, коди або іншу конфіденційну інформацію. Часто такі атаки маскуються під звернення від банку, технічної підтримки або навіть колеги.

Ще один важливий напрямок — мережеві атаки. Вони включають техніки перехоплення трафіку, підміни адрес, сканування вразливих портів і масові атаки на відмову в обслуговуванні. Наприклад, DDoS-атака може вивести з ладу вебсайт компанії, заблокувавши його для всіх користувачів через перевантаження серверів штучним трафіком. У складніших випадках мережевий трафік перехоплюється і змінюється в реальному часі, що дозволяє красти логіни, паролі або фінансові дані. Велике поширення мають атаки, пов’язані із зловмисним програмним забезпеченням. Це може бути вірус або троян, який маскується під легітимну програму й запускається користувачем. Таке ПЗ здатне викрадати файли, стежити за діями користувача, шифрувати дані з вимогою викупу або відкривати віддалений доступ до системи. Часто зараження відбувається через вкладення в електронній пошті або шкідливі посилання.

Також часто атакою стає використання вразливостей у програмному забезпеченні. Якщо код сайту чи програми містить помилки, вони можуть бути використані для проникнення в систему. Це може бути SQL-ін’єкція, яка дозволяє зловмиснику отримати доступ до бази даних, або впровадження шкідливого скрипту у вебсторінку, що буде виконаний у браузері користувача. Особливо небезпечні так звані zero-day вразливості — ті, про які розробники ще не знають, і тому не встигли випустити оновлення.

Значну загрозу становлять внутрішні атаки, коли дії зла чи необережності здійснює сам співробітник компанії. Наприклад, недобросовісний працівник може навмисно пошкодити або викрасти дані, або ж неуважний співробітник може випадково відкрити фішинговий лист чи вставити заражену флешку, що відкриє доступ до внутрішньої мережі організації.

Не варто недооцінювати і фізичний вектор атак. Якщо зловмисник отримає фізичний доступ до пристроїв або серверів, навіть найкращі захисти програмного рівня можуть виявитися марними. Викрадення ноутбуків, підключення шкідливих USB-носіїв або доступ до серверної кімнати — усе це потенційні шляхи атаки.

Ще однією тенденцією є атаки через ланцюг постачання. Замість прямого зламу організації, зловмисники заражають програмне забезпечення, яке постачає сторонній підрядник. У такий спосіб шкідливий код може бути легально встановлений в системах компанії під виглядом офіційного оновлення.

Крадіжка облікових даних також залишається популярним методом. Через підбір паролів, повторне використання логінів із попередніх витоків або фішингові кампанії зловмисники отримують доступ до чужих акаунтів і можуть використовувати їх для подальшого розповсюдження атаки.

З розвитком хмарних технологій з’явилися нові вектори атак, пов’язані з неправильною конфігурацією хмарних сервісів, вразливими API або недостатнім контролем доступу. У разі помилки адміністраторів конфіденційні дані можуть стати доступними публічно або потрапити до рук атакуючого.

1.4. Роль і можливості штучного інтелекту в сфері кіберзахисту

Штучний інтелект має доволі широке застосування у кібербезпеці, і його можливості дуже великі. Такі системи можуть допомогти як простим користувачам, так і експертам з кіберзахисту. За допомогою даних технологій кібербезпека може отримати новий імпульс розвитку та продуктивної роботи , що дозволить краще реагувати на інциденти, передбачати ризики та створювати ефективні стратегії протидії. На рисунку 1.3. показано, які є види програмного забезпечення на базі штучного інтелекту.

В останні роки все більше компаній в Україні впроваджують рішення на основі ШІ у сфері безпеки [1], [2], [3], [6]. ШІ допомагає створювати більш стійкі алгоритми шифрування та може автоматично виявляти слабкі місця в існуючих криптографічних схемах. Наприклад, машинне навчання може аналізувати шифротексти для виявлення потенційних вразливостей. Генеративні моделі можуть створювати складні ключі, які важко зламати традиційними методами. ШІ може автоматично підбирати найкращий тип шифрування залежно від середовища передачі даних.

ШІ також активно використовується у системах ідентифікації та контролю доступу. Наприклад, біометричні методи розпізнавання обличчя, голосу або відбитків пальців значною мірою ґрунтуються на глибокому навчанні. Крім того, системи можуть аналізувати поведінкові патерни користувачів, виявляючи спроби несанкціонованого доступу навіть у разі використання справжніх облікових даних. Моніторинг та аналіз подій у системі — ще один напрям, де ШІ проявляє свої сильні сторони. Автоматизовані алгоритми можуть аналізувати великі обсяги журналів подій у реальному часі, виявляючи аномалії або потенційні загрози до того, як вони встигнуть завдати шкоди. ШІ не лише розпізнає загрози, але й здатен прогнозувати майбутні атаки, ґрунтуючись на попередньому досвіді та поведінці системи. ШІ відіграє важливу роль у проактивному захисті мереж [5], [8], [12], [13].

Антивірусне програмне забезпечення завдяки штучному інтелекту

вийшло на новий рівень. Якщо традиційні антивіруси здебільшого орієнтуються на вже відомі сигнатури шкідливого ПЗ, то системи на базі ШІ аналізують поведінку файлів, дозволяючи виявляти навіть ті загрози, які ще не були офіційно зареєстровані. Це особливо важливо у боротьбі з так званими атаками нульового дня. Це може сформувати ефективну стратегію превентивного захисту.

Фаєрволи і брандмауери, доповнені ШІ, стають більш потужними — вони можуть динамічно змінювати правила фільтрації, реагуючи на зміни у мережевому трафіку, і виявляти підозрілу активність без необхідності ручного втручання. Те саме стосується і систем виявлення та запобігання вторгненням, які за допомогою ШІ здатні не лише виявляти загрози, а й миттєво їх блокувати.

Системи виявлення та запобігання вторгненням (IDS/IPS) є одним із найважливіших інструментів у сфері кібербезпеки, а штучний інтелект значно підсилює їхню ефективність. IDS/IPS-системи на основі ШІ здатні в реальному часі обробляти великі обсяги мережевого трафіку, виявляючи відхилення від нормальної роботи. Наприклад, якщо у певний час доби від конкретного пристрою зазвичай надходить 100 запитів, а раптово їх кількість зростає до 10 000 — це може сигналізувати про спробу атаки. ШІ розпізнає таку ситуацію як потенційну загрозу та може автоматично вжити заходів, наприклад, заблокувати IP-адресу джерела атаки або сповістити адміністратора.

Крім того, штучний інтелект допомагає організувати процес резервного копіювання та відновлення даних більш ефективно. Він може прогнозувати ризики втрати інформації, визначати, які саме дані потребують першочергового захисту, та оптимізувати процес збереження копій, зменшуючи навантаження на систему.

Одна з найважливіших функцій ШІ — це участь у стратегічному плануванні кіберзахисту. Штучний інтелект здатен аналізувати загальний стан безпеки інформаційної інфраструктури, виявляти слабкі місця, пропонувати рішення, а також моделювати потенційні сценарії атак. Це дає змогу не лише

реагувати на інциденти, а й запобігати їм на етапі планування. Схема створена за допомогою Xmind [14].

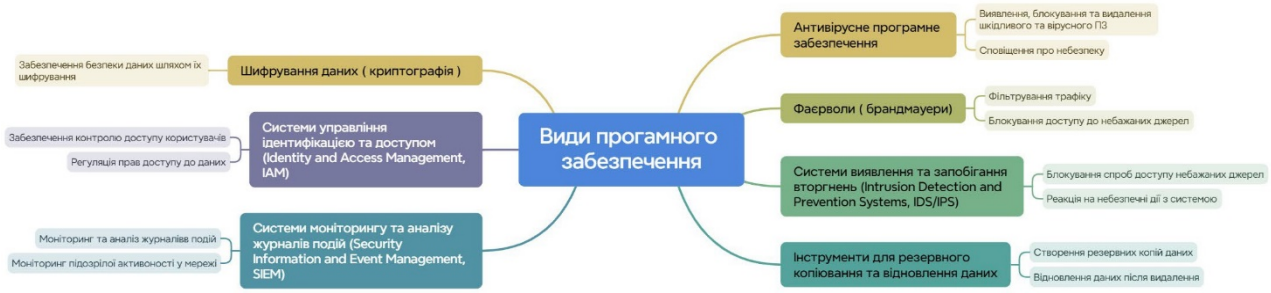


Рисунок 1.3 - Види ПЗ з залученням методик штучного інтелекту

В Україні є концепція розвитку технологій штучного інтелекту в інформаційній та кібербезпеці[1], [4] і вона виглядає доволі розлого та перспективно. Вона спрямована як на технічну модернізацію, так і на системне підвищення інформаційної стійкості країни. Її реалізація є важливим кроком у напрямку цифрової суверенності та технологічної незалежності, особливо в умовах поствйно зростаючих загроз. Зображена на рисунку 2.4., з ухилом на технічну та безпекову частину розвитку.

- Створення захищенного національного інформпростору. Передбачається впровадження методик штучного інтелекту для виявлення та фільтрації дезінформації, інформаційних впливів, бот-мереж і фейкових джерел. Такі системи здатні моніторити соціальні мережі, інформаційні платформи та ресурси, оперативно реагуючи на спроби зовнішнього інформаційного втручання або маніпуляцій. Це особливо важливо під час війни, коли ворог намагається зламати українців дезінформацією.
- Виявлення, запобігання та нейтралізація інформаційних загроз включає в себе не тільки технічні засоби кіберзахисту, але й системи аналізу інформаційних джерел. Алгоритми можуть автоматично виявляти загрози, що походять із зовнішніх джерел — від кібернападів до інформаційних кампаній впливу — і навіть передбачати можливі сценарії їх розвитку, щоб забезпечити

превентивну відповідь. Це особливо актуально і із інформаціними психологічними операціями (ІПСО)

- Удосконалення законодавства та створення сучасної правової бази - необхідна умова для інтеграції методик штучного інтелекту у державне управліннята захист даних. Це включає регулювання використання технологій, захист персональних даних, етичні аспекти застосування ШІ, а також відповідальність за автоматизовані рішення. Україна поступово впроваджує відповідні положення, орієнтуючись на досвід ЄС та світові практики.
- Розроблення інноваціних систем кібербезпеки базується на алгоритмах машинного навчання, аналізу великих даних, нейромереж. Такі системи дозволяють державним та приватним структурам оперативно виявляти атаки, прогнозувати поведінку зловмисників і автоматизовано реагувати на загрози. Вони можуть інтегруватися в критичну інфраструктуру країни — енергетику, транспорт,державні реєстри тощо.
- Створення програмних та управлінських рішень для державних установ стосується автоматизації управління безпековими процесами, побудови централізованих платформ моніторингу, управління ризиками, обробки інцидентів, а також цифровізації кібербезпекових процедур на всіх рівнях державного управління. Такі рішення роблять систему не лише більш ефективною, а й гнучкою до нових типів загроз.

Рисунок 1.4. - Концепція розвитку технологій штучного інтелекту в Україні

1.5. Постановка задачі дослідження

Таким чином, задача дослідження у даній роботі буде наступною:

- Провести дослідження механізмів та відповідних методів підвищення рівнякібербезпеки шляхом використання технологій штучного інтелекту.
- Проаналізувати сучасні засоби кіберзахисту, що базуються на технологіях штучного інтелекту, та оцінити їхню ефективність у виявленні й нейтралізації загроз.
- Вивчити алгоритми машинного навчання, які забезпечують більш точне й оперативне виявлення кіберзагроз.
- Оцінити результативність методик підвищення кібербезпеки з використанням ШІ та визначити, яким чином вони впливають на стійкість і захищеність інформаційних систем.
- Дослідити процеси інтеграції технологій штучного інтелекту в структури такомпоненти сучасних інформаційних систем.
- Проаналізувати можливості застосування ШІ для вдосконалення систем виявлення та протидії вторгненням на прикладі таких рішень, як Suricata, ELK Stack та Kibana.
- Сформулювати практичні рекомендації щодо ефективного впровадження, супроводу й розвитку систем штучного інтелекту в контексті підвищення кібербезпеки організацій.

Висновки за розділом 1

У цьому розділі було здійснено всебічне та комплексне дослідження сучасного стану кібербезпеки як на глобальному рівні, так і в контексті України. Вивчення охопило широкий спектр проблем, з якими сьогодні стикаються уряди, приватні організації, установи та окремі користувачі у сфері захисту інформаційних систем. Окреслено головні тенденції, пов’язані з еволюцією кіберзагроз, а також вказано на зростаючу складність та

витонченість методів, які використовують зловмисники.

Особливу увагу приділено аналізу ситуації в Україні, яка, враховуючи геополітичний контекст, зазнає постійного кібертиску. У цьому контексті розглянуто не лише загальні виклики, спільні для більшості країн світу, а й специфічні особливості українського кіберпростору, включаючи активізацію атак на критичну інфраструктуру та державні установи. Паралельно проаналізовано розвиток та інтеграцію технологій штучного інтелекту (ШІ) у різних секторах, таких як оборона, енергетика, охорона здоров'я, освіта та комерційний сектор. Розглянуто приклади впровадження ШІ в контексти кіберзахисту, зокрема автоматизовані системи моніторингу, виявлення загроз та прогнозування атак.

Окремим напрямом дослідження стала мотивація зловмисників, а також способи здійснення кібератак. Визначено основні цілі, яких намагаються досягти кіберзлочинці: крадіжка конфіденційної інформації, фінансова вигода, дестабілізація інфраструктури, політичний або ідеологічний вплив. Детально проаналізовано профілі потенційних ініціаторів атак — від одиночних хакерів до організованих угруповань і державних акторів. Надано класифікацію найбільш поширених методів атак, включаючи фішинг, DDoS-атаки, використання шкідливого ПЗ, експлуатацію вразливостей, соціальну інженерію тощо. Розглянуто типовий життєвий цикл кібератаки, її технічні характеристики, рівень складності, методи маскування, а також потенційні наслідки для об'єктів критичної інфраструктури, таких як енергетичні системи, системи водопостачання, транспорті зв'язок.

Значна частина дослідження була присвячена аналізу програмного забезпечення, що використовує штучний інтелект для забезпечення кібербезпеки. Вивчено основні типи таких систем, зокрема ті, що займаються виявленням аномальної поведінки користувачів, загроз у режимі реального часу, автоматизованим аналізом логів і телеметрії, моделюванням ризиків, формуванням рекомендацій щодо реагування, а також автономною протидією кібератакам.

Розкрито принципи функціонування цих систем, зокрема застосування машинного навчання, глибоких нейронних мереж, алгоритмів обробки великих даних. Розглянуто виклики, пов’язані з навчанням моделей, потребою у великих обсягах якісних даних, а також ризики помилкових спрацьовувань або навмисної маніпуляції алгоритмами.

Оцінено переваги впровадження ШІ-рішень у сферу кіберзахисту, серед яких висока швидкість обробки інформації, здатність до самообучення, адаптація до нових типів загроз, зниження навантаження на персонал. Водночас, акцентовано увагу на потенційних загрозах, що можуть виникнути через надмірну залежність від автоматизованих систем, можливість експлуатації вразливостей в алгоритмах ШІ, а також проблему прозорості прийняття рішень у таких системах.

РОЗДІЛ 2
ДОСЛІДЖЕННЯ МЕХАНІЗМІВ І МЕТОДІВ ПОКРАЩЕННЯ КІБЕРБЕЗПЕКИ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

2.1. Огляд існуючих рішень на базі ШІ в кібербезпеці

Відомо, що штучний інтелект – це технологія, яка швидко розвивається та вдосконалюється, і з’являються нові методики використання ШІ у різних сферах, в тому числі у кібербезпеці. І впровадження методик на основі штучного інтелекту здатне повкращити інформаціну безпеку різних систем. Детальніше про це розповідається в джерелах [12, 13]. А ринок штучного інтелекту зовсім скоро зросте до 30 мільярдів доларів [7].

ШІ виступає як високопродуктивний аналітик, здатний обробляти величезніпотоки інформації та виявляти закономірності, які можуть вказувати на атаку. Його здатність до навчання дозволяє йому ідентифікувати навіть нові, невідомі раніше загрози, на відміну від традиційних сигнатурних методів.

Інтеграція ШІ в IDS перетворює їх з пасивних реєстраторів подій на інтелектуальних помічників, які можуть не лише фіксувати аномалії, але й прогнозувати потенційні вторгнення на основі аналізу поведінки та виявлення складних, багатоетапних атак.

Цей підхід є критично важливим для виявлення внутрішніх загроз та скомпрометованих облікових записів. ШІ створює "нормальний" профіль поведінки для кожного користувача і миттєво сигналізує про будь-які відхилення, які можуть свідчити про зловмисну діяльність.

У фінансовому секторі ШІ є потужним інструментом для боротьби з шахрайством. Аналізуючи величезну кількість транзакцій, він може виявляти нетипові патерни, які можуть вказувати на шахрайські дії, допомагаючи запобігтифінансовим втратам.

Швидкість реагування є критично важливою у випадку кібератаки. ШІ може

автоматично виконувати певні дії у відповідь на виявлені загрози, такі як ізоляція заражених систем або блокування шкідливих IP-адрес, що значно зменшує час простою та потенційний збиток. У банківській сфері це особливо цінно для боротьби з соціальною інженерією та фішингом, де швидка реакція може запобігтивтраті коштів клієнтів.

ШІ може допомогти автоматизувати процес аудиту безпеки, швидко виявляючи відомі вразливості в програмному забезпеченні та конфігураціях систем. Це дозволяє командам безпеки оперативно усувати слабкі місця та знижувати ризик успішної експлуатації.

Аналізуючи дані про минулі кібератаки, ШІ може виявляти тенденції та прогнозувати потенційні майбутні загрози. Це дозволяє організаціям розробляти проактивні стратегії захисту та завчасно вживати заходів для запобігання атакам.

ШІ стає незамінним помічником для аналітиків SOC, допомагаючи їм впоратися з величезним обсягом попереджень безпеки. Фільтруючи нерелевантні запити, надаючи контекстну інформацію та пропонуючи рекомендації щодо дій, ШІ підвищує ефективність роботи SOC та допомагає швидше реагувати на реальнізагрози.

Платформи EDR (Endpoint Detection and Response) з інтегрованим ШІ забезпечують багаторівневий захист окремих пристроїв. Вони можуть виявляти таблокувати шкідливу активність на основі поведінкового аналізу, навіть якщо сигнатури для конкретного шкідливого ПЗ ще не існують.

ШІ значно покращує можливості фільтрації спаму та виявлення фішинговихлистів. Аналізуючи мовні патерни, вміст, посилання та вкладення, ШІ може з високою точністю ідентифікувати спроби фішингу, навіть якщо вони є дуже складними та добре замаскованими.

Також швидкий розвиток набувають конкретні програмні рішення на основіштучного інтелекту, які впроваджуються на комп’ютерні системи, які їх потребують. Наприклад, Darktrace використовує підхід "Enterprise Immune System" (Корпоративна імунна система), який повністю базується на ШІ. Він

полягає у створенні динамічної моделі "нормальної" поведінки мережі та всіх її користувачів і пристроїв. Будь-яке відхилення від цієї норми розглядається як потенційна загроза. ШІ в Darktrace не потребує попередніх знань про конкретні загрози (сигнатур), що дозволяє йому виявляти новітні та невідомі атаки в режимі реального часу. Крім того, інструменти відстеження, реагування та аналізу інцидентів також використовують ШІ для надання контексту та рекомендацій.

CylancePROTECT використовує ШІ та машинне навчання для прогнозуваннята запобігання кібератакам ще до їхнього виконання. Замість того, щоб покладатися на сигнатури, Cylance аналізує характеристики файлів та виконуваного коду, щоб визначити, чи є вони шкідливими. Цей "цілісний" підхід дозволяє йому ефективно блокувати як відоме, так і невідоме шкідливе програмне забезпечення та інші кіберзагрози на проактивному рівні.

Як SIEM-платформа, IBM QRadar інтегрує дані з різних джерел безпеки та використовує ШІ для виявлення аномалій та кореляції подій, які можуть свідчити про атаку. ШІ допомагає виявляти складні загрози, які можуть бути непомітними при аналізі окремих подій. Він також сприяє автоматизації класифікації інцидентів та процесів реагування, допомагаючи зменшити час на виявлення та усунення загроз.

FireEye Helix поєднує в собі можливості моніторингу, аналізу та реагування на інциденти, використовуючи ШІ для підвищення їхньої ефективності. ШІ допомагає аналізувати атаки з різних точок зору, виявляти складні закономірності та надавати аналітикам контекстну інформацію для прийняття обґрунтованих рішень. Прогнозування майбутніх ризиків на основі аналізу попередніх атак такожє однією з ключових функцій, що підтримуються ШІ.

Як розширення для платформи Splunk, Enterprise Security використовує ШІ для аналізу подій безпеки в реальному часі та виявлення кіберзагроз. ШІ допомагає покращити точність виявлення, зменшити кількість хибних спрацьовувань та автоматизувати процеси реагування. Постійний моніторинг та

адаптивні протоколи реагування, підсилені ШІ, роблять цю платформу потужним інструментом для забезпечення безпеки.

Cisco Stealthwatch використовується для моніторингу мережевої безпеки використовує аналіз трафіку та ШІ для виявлення та реагування на кіберзагрози в режимі реального часу. ШІ дозволяє аналізувати великі обсяги мережевих даних, виявляти аномальну поведінку та потенційні вразливості, а також автоматично вживати заходів для пом'якшення загроз.

ChatGPT та інші чат-боти, які хоч і не є прямими інструментами для виявлення та запобігання загрозам у режимі реального часу, вони можуть бути цінними помічниками у розробці стратегій кібербезпеки, наданні порад щодо найкращих практик та вирішенні різноманітних завдань і проблем. Їхні можливості аналізу тексту та генерації відповідей можуть допомогти в ідентифікації вразливостей та пропонуванні рішень. Однак, як ви правильно зазначили, необхідно проявляти обережність, щоб уникнути неналежного використання цих технологій.

2.2. Алгоритми машинного навчання для виявлення загроз

У сфері кібербезпеки машинне навчання відіграє дедалі важливішу роль, дозволяючи ефективно виявляти як відомі, так і нові загрози. Завдяки здатності аналізувати великі обсяги даних і виявляти приховані закономірності, алгоритми машинного навчання значно підвищують рівень захисту інформаційних систем. Існує кілька основних підходів до використання машинного навчання у виявленні кіберзагроз: наглядове навчання, ненаглядове навчання, напівнаглядове навчання та навчання з підкріпленням.

Наглядове навчання застосовується тоді, коли є доступ до розмічених даних, тобто прикладів мережевої активності чи поведінки, де вже відомо, чи є вона шкідливою. На основі цих даних модель навчається розрізняти загрозу від нормальної активності. До найпопулярніших алгоритмів цього типу належать логістична регресія, дерева рішень, випадкові ліси (Random Forest), метод

опорних векторів (SVM) та градієнтний бустинг (наприклад, XGBoost). Такі методи часто застосовуються для класифікації мережевого трафіку, виявлення фішингових листів або аналізу шкідливого програмного забезпечення. У більш складних задачах, наприклад, для аналізу поведінки користувачів чи виявлення складно маскованих атак, застосовують глибокі нейронні мережі.

Ненаглядове навчання використовується у випадках, коли дані не мають чітких міток. У такому разі модель самостійно шукає аномальні патерни або кластеризує дані. Це особливо корисно для виявлення нових, ще невідомих загроз. Класичні алгоритми ненаглядового навчання включають кластеризацію (наприклад, K-Means), DBSCAN (який добре працює з шумними даними), аналіз головних компонент (PCA) для зниження розмірності та виявлення аномалій, а також ліс ізоляції (Isolation Forest), який створений спеціально для виявлення аномалій. У цій групі також активно використовуються автоенкодери — нейронні мережі, які навчаються відновлювати нормальні зразки, а невідповідність на виході може сигналізувати про аномалію.

Напівнаглядове навчання поєднує підходи перших двох. Воно є особливо ефективним, коли велика частина даних не має міток, але наявна невелика кількість класифікованих прикладів. У такому випадку модель може спочатку навчитися на відомих загрозах, а потім застосовувати знання для аналізу великого обсягу невідомих даних. Цей підхід дозволяє значно знизити витрати на ручну розмітку даних.

Ще один перспективний підхід — навчання з підкріпленням, яке дозволяє агенту навчатися на основі винагород і покарань за дії в середовищі. У контексті кібербезпеки це може бути, наприклад, автоматичне налаштування міжмережевого екрану (фаєрволу), адаптація до нових типів атак у реальному часі або керування реагуванням на інциденти.

Усі ці підходи можуть використовуватися в різних сценаріях, таких як системи виявлення вторгнень (IDS), аналіз журналів подій (логів), виявлення ботнетів, виявлення аномальної поведінки користувачів (UBA/UEBA) або захист кінцевих точок (Endpoint Detection and Response). Залежно від

доступності даних, ресурсів та цілей, вибираються відповідні алгоритми або їх комбінації.

Таким чином, машинне навчання відкриває нові горизонти у виявленні кіберзагроз, дозволяючи швидко адаптуватися до нових методів атак і зменшувати ризики безпеки в цифровому середовищі.

2.3. Методи обробки даних для підвищення точності виявлення атак

Для ефективного виявлення кіберзагроз за допомогою штучного інтелекту (ШІ) ключову роль відіграє не лише сама модель, а й правильна обробка та підготовка даних. Чим якісніше оброблені вхідні дані, тим точніше модель здатна розпізнати загрози, особливо складні та невідомі. Існує низка методів, які дозволяють суттєво покращити якість даних і, відповідно, точність виявлення атак.

Першим етапом завжди є очищення й нормалізація даних. Це включає видалення дублікатів, заповнення або усунення пропущених значень, фільтрацію некоректної інформації, а також нормалізацію числових ознак до одного масштабу, що особливо важливо для багатьох алгоритмів машинного навчання. Така базова обробка дозволяє уникнути помилкових висновків і забезпечує стабільну роботу моделей.

Наступним важливим кроком є інженерія ознак — процес створення нових або перетворення наявних характеристик даних, щоб краще представити сутність проблеми для моделі. У сфері кібербезпеки це можуть бути поведінкові ознаки користувача, частота доступу до певних ресурсів, кількість з’єднань із зовнішніми IP-адресами, зміни у шаблонах трафіку тощо. Часто створюються часові ознаки, якідозволяють моделі розуміти, в який час доби або з якою періодичністю відбуваються потенційні атаки.

Оскільки багато кіберзагроз проявляються як аномальна поведінка, велику роль відіграють методи виявлення аномалій. Для цього застосовують

зниження розмірності (наприклад, метод головних компонент — PCA), кластеризацію або побудову дерев, що ізолюють аномальні випадки. Такі підходи дозволяють помітити незвичну активність навіть без попереднього знання про тип атаки.

У випадках, коли джерело даних є неструктурованим, як-от журнали подій або текстові повідомлення, використовуються методи обробки природної мови. Тексти очищаються від зайвих слів, лематизуються, розбиваються на токени, післячого перетворюються у числові вектори (наприклад, за допомогою TF-IDF чи Word2Vec), які модель може аналізувати. Також у сфері логів поширеним є виділення шаблонів для структурування даних, що дозволяє об’єднувати подібні події й виявляти відхилення від звичного шаблону.

Однією з великих проблем у кібербезпеці є незбалансованість даних: більшість трафіку або поведінки є нормальною, а загрози — рідкісні. У таких випадках застосовуються методи балансування, наприклад, збільшення меншості за допомогою синтетичних даних (SMOTE) або зменшення кількості прикладів більшості. Також моделі можуть бути навчено з урахуванням ваги кожного класу, надаючи атакам більшу важливість у функції втрат.

Ще одним важливим аспектом є правильне маркування даних. Для навчання наглядових моделей необхідно мати точні мітки — чи є активність шкідливою чи ні. Це може досягатися як вручну експертами, так і автоматично, наприклад, на основі чорних списків, сигнатур або зовнішніх джерел даних про загрози (Threat Intelligence). Додаткове збагачення даних — наприклад, інформацією про геолокацію IP-адрес або відомі вразливості — дозволяє дати моделі ширший контекст і підвищити її здатність до правильних рішень.

У складніших сценаріях обробка даних включає побудову ланцюгів подій або сесій, що дозволяє аналізувати атаки, які розгортаються у кілька етапів. У таких випадках застосовуються моделі, здатні працювати з послідовностями, наприклад, рекурентні нейронні мережі (RNN, LSTM), які зберігають контекст попередніх подій.

2.4. Інтеграція штучного інтелекту в інформаційні системи

Інтеграція засобів штучного інтелекту в існуючі системи є складним, але вкрай важливим процесом для підвищення їхньої ефективності, автоматизації та здатності приймати обґрунтовані та правильні рішення. Цей процес може варіюватися залежно від типу існуючої системи, цілей інтеграції та доступних ресурсів. А також системи, яку планується впровадити , навчити та адаптувати до реальних проблем. У 2024 році хакери атакували австралійські банки, використовуючи складні методи соціальної інженерії [9], [10], [11]. Саме штучний інтелект може допомогти у попередженні таких атак.

Першим кроком є глибоке розуміння поточної архітектури, функціональності, даних та обмежень існуючої системи. Визначаються конкретні області, де ШІ може принести найбільшу користь. Це можуть бути завдання,пов'язані з обробкою великих обсягів даних, автоматизацією рутинних процесів, покращенням точності прогнозування, персоналізацією взаємодії з користувачами тощо. Потім визначаються очікувані результати від інтеграції ШІ. Наприклад, підвищення ефективності на X відсотків, зменшення кількості помилок на Y відсотків, покращення задоволеності клієнтів на Z відсотків. Після виконання всіхзаходів встановлюються метрики для вимірювання успіху інтеграції технологій штучного інтелекту.

Залежно від поставлених цілей, обираються відповідні методи машинного навчання (наприклад, класифікація, регресія, кластеризація, навчання з підкріпленням), обробки природної мови (NLP), комп'ютерного зору тощо. Потім обираються фреймворки машинного навчання (наприклад, TensorFlow, PyTorch, scikit-learn), хмарні сервіси (наприклад, AWS AI, Google Cloud AI Platform, Azure Machine Learning), інструменти для обробки даних та візуалізації. Також розробляється план взаємодії ШІ-компонентів з існуючою системою. Це може включати використання API, інтеграцію на рівні баз даних, створення окремих мікросервісів тощо.

ШІ потребує великих обсягів даних для навчання та тренування.

Збираються відповідні дані з існуючої системи та зовнішніх джерел, проводяться процедури очищення, усунення дублікатів, обробки відсутніх значень. У такому випадку дані розподіляються у вигляді, придатному для навчання моделей ШІ. Після цього данірозділяються на навчальну, валідаційну та тестову вибірки для навчання,налаштування гіперпараметрів та оцінки якості впровадженої моделі.

Обирається відповідна модель машинного навчання та проводиться її навчання на підготовлених даних. Потім, за допомогою валідаційної вибірки оптимізуються гіперпараметри моделі для досягнення найкращої продуктивності, а якість навченої моделі оцінюється на тестовій вибірці за допомогою відповіднихметрик (наприклад, точність, F1-міра, AUC).

Навчена модель розгортається в робочому середовищі. Це може бути локальний сервер, хмарна платформа або вбудований пристрій, потім розробляються API для забезпечення взаємодії між існуючою системою та розгорнутою моделлю ШІ. А готова ШІ-функціональність інтегрується в бізнес-процеси існуючої системи. Наприклад, результати прогнозування використовуються для прийняття рішень, а виявлені аномалії запускають певні дії. Перевіряється коректність роботи інтегрованої системи, включаючи взаємодію між існуючими компонентами та ШІ-моделлю. Також оцінюється вплив інтеграції ШІ на продуктивність системи (час відгуку, навантаження на ресурси), а у деяких випадках проводиться порівняння продуктивності системи до та після інтеграції ШІ або порівняння різних підходів інтеграції. Також система тестується в реальному робочому середовищі для забезпечення її стабільності та відповідності очікуваним результатам.

На цьому етапі відстежується якість роботи розгорнутої моделі ШІ в часі. З часом продуктивність моделі може знижуватися через зміну даних (data drift), а за потреби модель перенавчається на нових даних для підтримки її актуальності та високої якості. Також важливе забезпечення стабільної роботи інфраструктури, на якій розгорнута модель ШІ. У рамках роботи також збирається зворотний зв'язок від користувачів та операторів системи для

виявлення проблем та можливостей дляпокращення.

2.5. Оцінка ефективності методів та порівняння підходів

Виявлення мережевих аномалій за допомогою штучного інтелекту передбачає використання інтелектуальних алгоритмів для аналізу мережевого трафіку та поведінки користувачів у системі. Замість того, щоб покладатися лише на заздалегідь відомі сигнатури атак, як це роблять традиційні антивіруси чи фаєрволи, AI навчається розпізнавати шаблони поведінки в мережі. Коли відбувається рідозріла дія — наприклад, різке зростання обсягу трафіку, нетипові з'єднання або незвичні дії користувача — система одразу виявляє це як аномалію. Такі рішення можуть автоматично сповіщати адміністраторів, блокувати трафік або ізолювати підозрілі дії ще до того, як вони переростуть у повноцінну атаку. Наприклад, штучний інтелект здатен розпізнати початок DDoS-атаки або спробу зламу внутрішньої системи навіть тоді, коли ця загроза є новою і раніше не фіксувалася. Завдяки цьому підходу вдається зменшити кількість невиявлених загроз на 30–50%, оскільки AI працює в режимі реального часу і постійно вдосконалює свою здатність розпізнавати нові форми атак. Це дозволяє компаніям швидше реагувати на інциденти та запобігати серйозним збоям у роботі. Прикладами таких систем є Microsoft Azure Sentinel, Vectra, Darktrace – всі ці рішення є SIEM – системами на основі штучного інтелекту.

Штучний інтелект відіграє ключову роль у сучасній боротьбі з шкідливим програмним забезпеченням. На відміну від традиційних антивірусів, які спираються на сигнатури відомих загроз, AI здатен виявляти нові, раніше невідомі форми малварі — включаючи так звані "нульового дня" (zero-day) атаки. Штучний інтелект аналізує вихідний код програм, структуру файлів, спосіб їхньої взаємодії з системою та інші ознаки, характерні для шкідливих дій. Завдяки алгоритмам машинного навчання, він може визначити, що файл поводиться як вірус або троян, навіть якщо такого файлу ще ніколи не існувало

в базах даних безпеки. AI може виявити, що новий файл намагається приховано змінити системні файли, записати себе в автозавантаження або зв’язатися з зовнішнім сервером — і класифікувати його як загрозу, навіть без попереднього зразка. Завдяки такому підходу рівень виявлення нових типів шкідливого ПЗ зростає на 40–60% у порівнянні з традиційними методами. Це дозволяє захищати системи набагато ефективніше, особливо в період, коли нові варіанти загроз з’являються щодня. Прикладами таких систем є Microsoft Defender for Endpoint , CrowdStrike Falcon , CylancePROTECT, SentinelOne.

SOAR (Security Orchestration, Automation and Response) — це платформи, які поєднують дані з різних джерел безпеки (SIEM-систем, антивірусів, мережевого моніторингу тощо) та дозволяють автоматизувати дії у відповідь на інциденти. У поєднанні зі штучним інтелектом такі системи стають ще потужнішими, оскільки AI може не лише фіксувати загрози, а й автоматично ініціювати відповідні заходи реагування. Коли AI виявляє загрозу, він може одразу запускати заздалегідь визначені сценарії (playbooks) у SOAR-системі. Наприклад, якщо фіксується підозріла активність з певної IP-адреси, система може автоматично заблокувати цю IP-адресу на фаєрволі. А якщо виявлено інфікований пристрій у мережі — його можна ізолювати, щоб запобігти поширенню шкідливого ПЗ. Це значно скорочує час реагування — на 30–40% швидше, ніж за ручної обробки. Завдяки цьому компанії можуть мінімізувати потенційні збитки, не чекаючи на втручання спеціалістів. Прикладами є Splunk SOAR , IBM QRadar SOAR , Cortex XSOAR (Palo Alto Networks).

Фішингові атаки залишаються однією з найпоширеніших кіберзагроз, націлених на крадіжку облікових даних, фінансової інформації чи доступу до систем. Традиційні фільтри спаму часто не справляються з новими, добре замаскованими фішинговими листами. Саме тут у гру вступає штучний інтелект. AI аналізує електронні листи, повідомлення в месенджерах і веб-форми, шукаючи ознаки фішингу. При цьому він не обмежується лише ключовими словами, а враховує структуру тексту, заголовки, URL-адреси, вкладення, відправника, час надсилання, а також поведінкові шаблони

користувача. Завдяки машинному навчанню, AI навчається на великій кількості прикладів фішингових і звичайних повідомлень, і з часом стає дедалі точнішим у розпізнаванні загроз. Наприклад, якщо користувач отримує листа нібито від банку, але AI фіксує, що домен відправника — підроблений, а текст має ознаки соціальної інженерії (наприклад, терміновий заклик до дії, помилки в мові, підозрілі посилання), система попереджає користувача або автоматично блокує повідомлення. Завдяки такому підходу вдається зменшити кількість успішних фішингових атак на 25–40%, що суттєво знижує ризики втрати даних, зламу облікових записів чи фінансових збитків. Прикладом таких систем є Microsoft Defender for Office 365, Google Workspace (Gmail), Proofpoint, Barracuda Sentinel.

Традиційні методи аутентифікації — як-от логін і пароль — усе частіше стають недостатніми для надійного захисту. Користувачі можуть використовувати слабкі паролі, повторювати їх у різних сервісах або стати жертвами фішингу. Щоб зміцнити безпеку, сучасні системи дедалі частіше впроваджують поведінкову аутентифікацію, підкріплену штучним інтелектом. AI відстежує й аналізує унікальні моделі поведінки кожного користувача — наприклад, швидкість і ритм набору тексту, спосіб переміщення мишки, типові маршрути навігації, час активності, місце входу, а також біометричні дані (наприклад, розпізнавання обличчя або відбитка пальця). На основі цих ознак створюється унікальний "цифровий профіль" користувача. Якщо при наступному вході в систему AI виявляє відхилення від звичного шаблону — наприклад, хтось вводить правильний пароль, але друкує повільніше або використовує іншу мову інтерфейсу, — система може зажадати додаткову перевірку або заблокувати доступ. Такий підхід дозволяє зменшити кількість зламаних облікових записів на 20–30%, адже навіть якщо зловмисник отримає пароль, йому буде складно імітувати типову поведінку справжнього користувача. Прикладом є Microsoft Azure Active Directory , BehavioSec , TypingDNA.

У сучасному світі кіберзагрози постійно еволюціонують, і організаціям

більше не достатньо лише реагувати на атаки після їх виникнення. Штучний інтелект дозволяє перейти до проактивної кібербезпеки, коли система не тільки фіксує загрози, а й передбачає їх появу та допомагає створювати ефективні стратегії захисту наперед. AI аналізує великі обсяги даних із різних джерел: логів безпеки, сповіщень з мережевих пристроїв, поведінкових даних користувачів, глобальних баз вразливостей, аналітики з попередніх атак та навіть інформації з даркнету. На основі цього аналізу моделі машинного навчання можуть виявляти потенційні вразливі місця в інфраструктурі до того, як ними скористається зловмисник, прогнозувати типи атак, які найімовірніше можуть бути здійснені на організацію з урахуванням її профілю. пропонувати стратегії превентивного захисту — оновлення політик безпеки, закриття портів, встановлення патчів або зміни конфігурацій, а також автоматично пріоритезувати ризики і формувати рекомендації для IT-відділу або служби безпеки. Такий аналітичний підхід забезпечує 30–50% покращення готовності до нових типів загроз, знижуючи вірогідність того, що організація буде захоплена зненацька. Такими системами є IBM Watson for Palo Alto, Cortex XDR, FireEye Helix , Recorded Future.

Щодня корпоративні системи генерують величезні обсяги логів: записи з серверів, мережевих пристроїв, додатків, систем доступу, антивірусів тощо. У цьому інформаційному потоці можуть ховатися ознаки кіберзагроз, зловживань доступом або порушень політик безпеки. Проте ручний аналіз таких даних практично неможливий. Саме тут вступає в дію штучний інтелект. AI-системи використовують машинне навчання та обробку природної мови (NLP), щоб автоматично переглядати, фільтрувати, корелювати та аналізувати логи й події в режимі реального часу. Вони виявляють аномальні шаблони поведінки, які можуть свідчити про вторгнення до системи, використання викрадених облікових даних, встановлення шкідливого ПЗ, порушення внутрішніх правил або політик доступу, внутрішні загрози з боку працівників. Наприклад, якщо обліковий запис адміністратора раптом виконує дії у нетиповий час або з нової IP-адреси, AI відзначає це як аномалію та може ініціювати автоматичне

розслідування. Завдяки такому підходу вдається зменшити кількість непомічених інцидентів на 20–40%, адже AI фокусується не лише на відомих загрозах, а й на нових або нестандартних схемах поведінки. Прикладами є Splunk, Elastic SIEM , Exabeam, Securonix, LogRhythm.

Соціальна інженерія — це вид кіберзагроз, коли зловмисники намагаються обманом змусити людину розкрити конфіденційну інформацію або виконати небезпечні дії, наприклад, натиснути на шкідливе посилання або передати логін і пароль. Найпоширеніший приклад — фішингові листи, які імітують повідомлення від банку, колеги чи керівника. Щоб цьому запобігти, штучний інтелект допомагає навчати користувачів і робити їх уважнішими до таких загроз. AI аналізує поведінку працівників — як вони взаємодіють з електронною поштою, як реагують на підозрілі повідомлення, хто найчастіше відкриває потенційно небезпечні листи. На основі цих даних система формує персоналізовані навчальні матеріали, адаптовані під кожного працівника. AI також може автоматично надсилати тестові (але безпечні) фішингові листи, щоб перевірити, хто "клює" на обман. Якщо користувач відкриває такий лист або вводить дані, система одразу пояснює, чому це була загроза, і пропонує коротке навчання. Таким чином працівники навчаються на практиці й краще запам’ятовують ознаки фішингу. Завдяки такому підходу ризик успішних атак соціальної інженерії зменшується приблизно на 10–25%. Люди починають краще розпізнавати шахрайство, а отже — рідше стають жертвами. Такий тип навчання не тільки ефективний, а й зручний, бо відбувається автоматично, без потреби у довгих лекціях чи курсах. AI постійно вдосконалюється та адаптується до нових методів шахрайства, допомагаючи тримати компанію в безпеці. Прикладамиє KnowBe4, Cofense PhishMe, Proofpoint Security Awareness, Hoxhunt .

Висновки за розділом 3

Отже, у межах цього розділу було всебічно проаналізовано ключові

алгоритми та методики застосування штучного інтелекту в сфері кібербезпеки. Особливу увагу зосереджено на практичних аспектах реалізації інтелектуальних систем — розглянуто приклади їхнього використання на основі конкретних програмних рішень, таких як системи виявлення вторгнень (IDS), інструменти моніторингу поведінки користувачів (UEBA), автоматизовані платформи для реагування на інциденти (SOAR), а також модулі аналізу загроз на основі великих даних.

Детально вивчено особливості впровадження зазначених технологій у сучасні інформаційні інфраструктури — зокрема, технічні вимоги, етапи інтеграції, адаптацію до специфіки корпоративних мереж і середовищ. Проведено оцінку ефективності функціонування таких систем у реальних умовах, враховуючи типові кіберзагрози, рівень помилкових спрацьовувань, швидкість реагування та масштабованість.

Окремий акцент зроблено на аналізі методів машинного навчання, що найчастіше застосовуються в галузі кібербезпеки. До них належать методи класифікації (наприклад, дерева рішень, SVM, нейронні мережі), алгоритми виявлення аномалій (ізольований ліс, кластеризація), а також моделі прогнозування на основі часових рядів. Оцінено не лише їхню ефективність, а й практичні виклики впровадження: необхідність якісних та репрезентативних наборів даних, боротьбу з розбалансованістю класів, перенавчання моделей та забезпечення їх стійкості до змін середовища.

Крім того, розглянуто ефективні стратегії обробки, фільтрації та оцінки даних, які становлять основу функціонування інтелектуальних систем кіберзахисту. Особливо підкреслено важливість коректної підготовки даних (data preprocessing), вибору релевантних ознак (feature engineering) та механізмів постійного оновлення моделей.

Зроблено висновок, що використання технологій штучного інтелекту суттєво підвищує здатність організацій оперативно виявляти та локалізовувати кіберзагрози, знижує рівень людської помилки та дозволяє будувати гнучкі, адаптивні системи захисту. Проте водночас підкреслено необхідність

забезпечення етичних, правових та технічних засад застосування ШІ, аби уникнути нових ризиків і гарантувати безпеку на всіх рівнях функціонування цифрової інфраструктури.

РОЗДІЛ 3
РОЗРОБКА ПРОГРАМНИХ РІШЕНЬ З ЗАЛУЧЕННЯМ МАШИННОГОНАВЧАННЯ

3.1. Постановка задачі та вибір інструментів

Метою даної роботи є розгортання та дослідження системи виявлення мережевих загроз з використанням засобів Suricata, ELK Stack та елементів штучного інтелекту (Python, Isolation Forest) Для досягнення цієї мети було поставлено наступні задачі:

- Розгорнути тестове середовище на основі ОС Ubuntu з попереднім налаштуванням мережі.
- Встановити систему мережевого моніторингу Suricata та налаштувати її для збору подій у форматі eve.json.
- Інтегрувати стек ELK (Elasticsearch, Kibana, Filebeat) для централізованого збору, обробки та візуалізації журналів.
- Реалізувати механізм виведення подій Suricata до Kibana для наочного аналізу активності в мережі.
- Побудувати візуалізації: розподіл типів атак, активність по IP-адресах, часові діаграми та геолокаційні карти.
- Застосувати базовий метод штучного інтелекту (Isolation Forest) для виявлення аномальної поведінки на основі мережевих логів.
- Порівняти результати сигнатурного та поведінкового аналізу, зробити висновки щодо ефективності комбінованого підходу.
- Реалізація цих задач дозволяє дослідити ефективність комплексного підходу до мережевого моніторингу, який поєднує класичні інструменти виявлення загроз з алгоритмами машинного навчання. Також у цьому розділі буде порівняно класичнні методи виявлення загроз, і такі з застосуванням штучного інтелекту.

3.2. Побудова моделі моніторингу мережевого трафіку

Спочатку в роботу вступає Filebeat — легкий агент, що працює на сервері або вузлі, де знаходиться Suricata. Filebeat постійно слідкує за логами Suricata (наприклад, файлом eve.json), автоматично їх читає, додає метадані (наприклад, часові мітки, теги) та відправляє дані до Elasticsearch. Filebeat також може парсити логи за допомогою готових модулів, таких як модуль suricata, що полегшує подальший аналіз. Схема 3.1. створена за допомогою Lucid app [15].

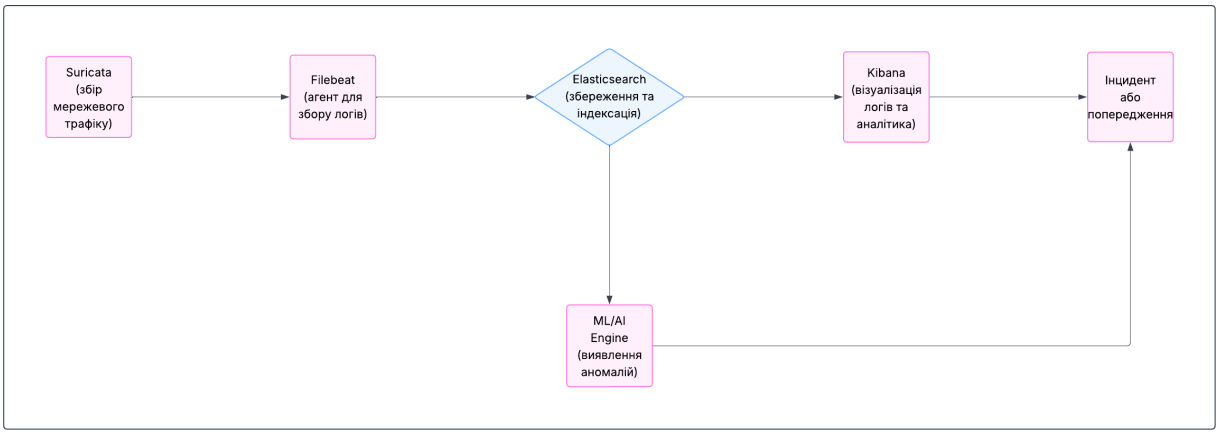


Рисунок 3.1 - Схема роботи моделі моніторингу мережевого трафіку

Elasticsearch є основним сховищем даних у цьому пайплайні. Він не лише зберігає отримані лог-події, а й індексує їх, забезпечуючи швидкий і ефективний пошук. Його можливості дозволяють будувати гнучкі запити, застосовувати фільтри, аналізувати трафік у розрізі IP-адрес, протоколів, портів, часових проміжків тощо. Він також слугує бекендом для візуалізації даних через Kibana.

Kibana — це інтерфейс користувача до Elasticsearch. Вона дозволяє створювати динамічні дашборди, будувати графіки, діаграми, таблиці та фільтрувати дані за будь-якими параметрами. Крім того, Kibana має вбудований модуль машинного навчання, який може автоматично виявляти аномалії в даних на основі аналізу тимчасових рядів, наприклад, раптове зростання кількості певних подій або нетипову активність з конкретного хоста. Це

дозволяє виявляти потенційні атаки або підозрілу активність без необхідності створювати вручну сигнатури або правила.

У випадках, коли потрібен глибший або спеціалізований аналіз, до пайплайну додаються зовнішні засоби машинного навчання. Для цього можна використовувати Python-скрипти з бібліотеками, такими як Scikit-learn, PyTorch або TensorFlow. Дані з Elasticsearch витягуються за допомогою REST API або Elastic Python Client, аналізуються в окремому середовищі, наприклад, для класифікації подій, кластеризації поведінки користувачів чи побудови моделей прогнозування. Результати такого аналізу можуть зберігатися назад в Elasticsearch і візуалізуватися через Kibana [16] ,[18]

У підсумку, весь процес виглядає так: Suricata генерує логи трафіку, Filebeat їх збирає та пересилає в Elasticsearch, де вони зберігаються й аналізуються, а Kibana використовується для візуалізації й виявлення загроз. Додатково до цього підключається машинне навчання, яке дозволяє автоматизувати процес виявлення аномалій та глибше розуміти поведінку в мережі.

3.3. Реалізація системи з використанням ШІ

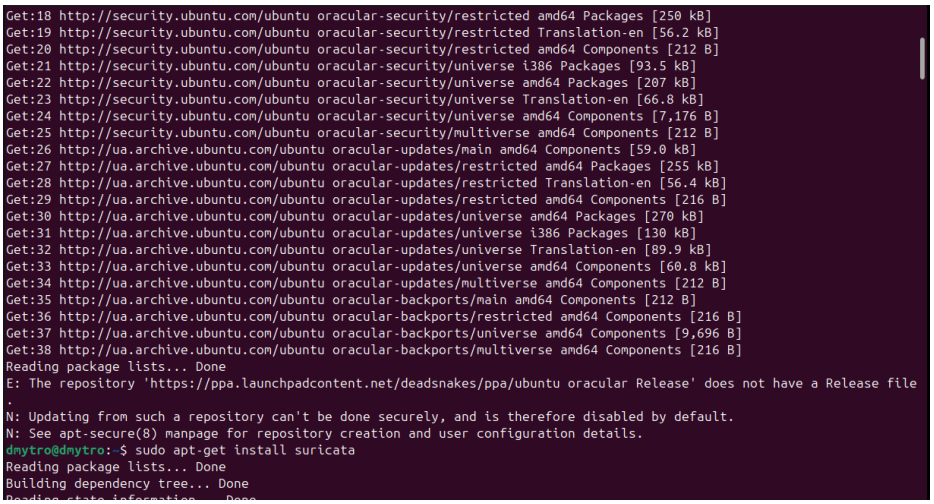


Рисунок 3.2 - Оновлення програмного забезпечення та встановлення Suricata

```
dmytro@dmytro:~$ sudo systemctl enable suricata.service
Synchronizing state of suricata.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable suricata
dmytro@dmytro:~$ suricata --build-info
This is Suricata version 7.0.6 RELEASE
Features: NFQ PCAP_SET_BUFF AF_PACKET HAVE_PACKET_FANOUT LIBCAP_NG LIBNET1.1 HAVE_HTP_URI_NORMALIZE_HOOK PCRE_JIT HAVE_N
SS HTTP2_DECOMPRESSION HAVE_LUA HAVE_JA3 HAVE_JA4 HAVE_LUAJIT HAVE_LIBJANSSON TLS TLS_C11 MAGIC RUST POPCNT64
SIMD support: SSE_4_2 SSE_4_1 SSE_3 SSE_2
Atomic intrinsics: 1 2 4 8 16 byte(s)
64-bits, Little-endian architecture
GCC version 13.3.0, C version 201112
compiled with _FORTIFY_SOURCE=2
L1 cache line size (CLS)=64
thread local storage method: _Thread_local
compiled with LibHTP v0.5.48, linked against LibHTP v0.5.48
```

Рисунок 3.3 - Запуск Suricata та перевірка версії

```
dmytro@dmytro:~$ sudo apt install kibana -y
The following packages were automatically installed and are no longer required:
  linux-headers-6.11.0-21          linux-modules-6.11.0-21-generic        linux-tools-6.11.0-21-generic
  linux-headers-6.11.0-21-generic  linux-modules-extra-6.11.0-21-generic  python3-netifaces
  linux-image-6.11.0-21-generic    linux-tools-6.11.0-21
Use 'sudo apt autoremove' to remove them.

Installing:
  kibana

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 21
  Download size: 293 MB
  Space needed: 744 MB / 5,853 MB available

Get:1 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 kibana amd64 7.17.28 [293 MB]
Fetched 293 MB in 28s (10.5 MB/s)
Selecting previously unselected package kibana.
(Reading database ... 258041 files and directories currently installed.)
Preparing to unpack .../kibana_7.17.28_amd64.deb ...
Unpacking kibana (7.17.28) ...
```

Рисунок 3.4 - Встановлення Kibana

```
dmytro@dmytro:~$ wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
sudo apt install apt-transport-https
echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-7.x.list

sudo apt update
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).
OK
The following packages were automatically installed and are no longer required:
  linux-headers-6.11.0-21          linux-modules-6.11.0-21-generic        linux-tools-6.11.0-21-generic
  linux-headers-6.11.0-21-generic  linux-modules-extra-6.11.0-21-generic  python3-netifaces
  linux-image-6.11.0-21-generic    linux-tools-6.11.0-21
Use 'sudo apt autoremove' to remove them.

Installing:
  apt-transport-https

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 21
  Download size: 3,970 B
  Space needed: 39.9 kB / 5,871 MB available

Get:1 http://ua.archive.ubuntu.com/ubuntu oracular-updates/universe amd64 apt-transport-https all 2.9.8ubuntu0.1 [3,970
B]
Fetched 3,970 B in 0s (18.8 kB/s)
Selecting previously unselected package apt-transport-https.
(Reading database ... 258037 files and directories currently installed.)
Preparing to unpack .../apt-transport-https_2.9.8ubuntu0.1_all.deb ...
Unpacking apt-transport-https (2.9.8ubuntu0.1) ...
Setting up apt-transport-https (2.9.8ubuntu0.1) ...
deb https://artifacts.elastic.co/packages/7.x/apt stable main
Hit:1 http://ua.archive.ubuntu.com/ubuntu oracular InRelease
Hit:2 http://ua.archive.ubuntu.com/ubuntu oracular-updates InRelease
```

Рисунок 3.5 - Встановлення Elasticsearch

```
  GNU nano 6.2                                                  eve.json *
filebeat.inputs:
- type: log
  paths:
    - /var/log/suricata/eve.json
  json.keys_under_root: true
  json.add_error_key: true

output.elasticsearch:
  hosts: ["localhost:9200"]
```

Рисунок 3.6 - Встановлення логів Filebeat

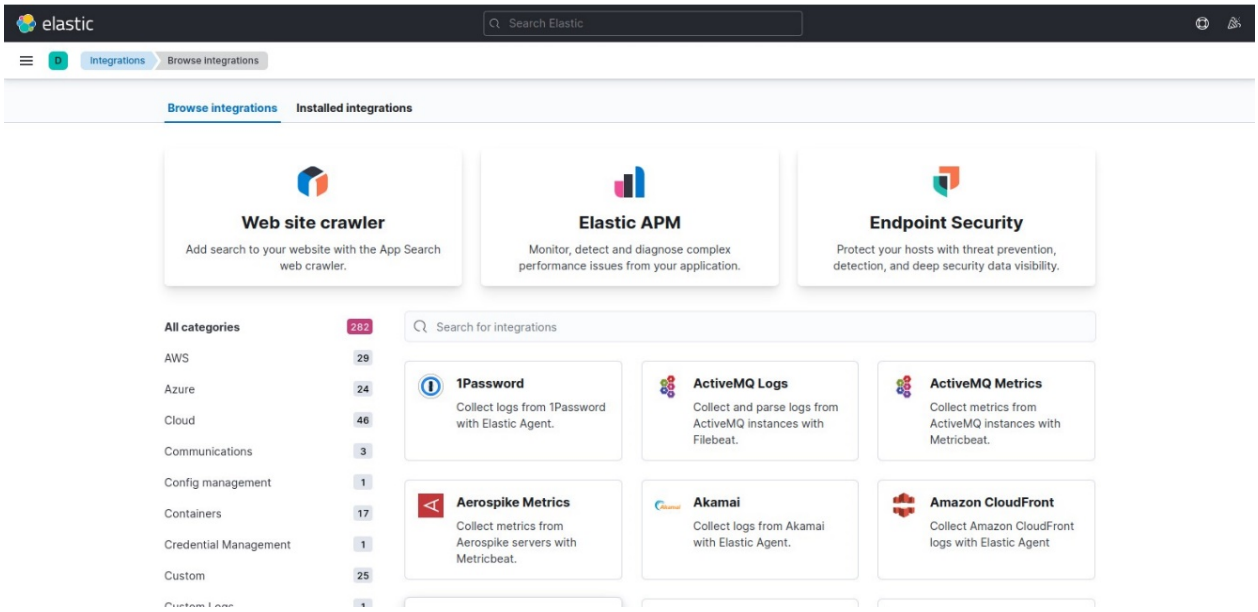


Рисунок 3.7 - ELK у роботі

```
dmytro@dmytro-virtual-machine:~$ pip3 install numpy pandas scikit-learn matplotlib seaborn
Defaulting to user installation because normal site-packages is not writeable
Collecting numpy
  Downloading numpy-2.2.6-cp310-cp310-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (16.8 MB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 16.8/16.8 MB 12.8 MB/s eta 0:00:00
Collecting pandas
  Downloading pandas-2.2.3-cp310-cp310-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (13.1 MB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 13.1/13.1 MB 11.7 MB/s eta 0:00:00
Collecting scikit-learn
  Downloading scikit_learn-1.6.1-cp310-cp310-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (13.5 MB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 13.5/13.5 MB 10.0 MB/s eta 0:00:00
Collecting matplotlib
  Downloading matplotlib-3.10.3-cp310-cp310-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (8.6 MB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 8.6/8.6 MB 10.5 MB/s eta 0:00:00
Collecting seaborn
  Downloading seaborn-0.13.2-py3-none-any.whl (294 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 294.9/294.9 KB 10.1 MB/s eta 0:00:00
Requirement already satisfied: pytz>=2020.1 in /usr/lib/python3/dist-packages (from pandas) (2022.1)
Collecting python-dateutil>=2.8.2
  Downloading python_dateutil-2.9.0.post0-py2.py3-none-any.whl (229 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 229.9/229.9 KB 18.6 MB/s eta 0:00:00
Collecting tzdata>=2022.7
  Downloading tzdata-2025.2-py2.py3-none-any.whl (347 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 347.8/347.8 KB 10.7 MB/s eta 0:00:00
Collecting joblib>=1.2.0
  Downloading joblib-1.5.1-py3-none-any.whl (307 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 307.7/307.7 KB 10.2 MB/s eta 0:00:00
Collecting scipy>=1.6.0
  Downloading scipy-1.15.3-cp310-cp310-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (37.7 MB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 37.7/37.7 MB 8.1 MB/s eta 0:00:00
Collecting threadpoolctl>=3.1.0
  Downloading threadpoolctl-3.6.0-py3-none-any.whl (18 kB)
Requirement already satisfied: pyparsing>=2.3.1 in /usr/lib/python3/dist-packages (from matplotlib) (2.4.7)
Collecting packaging>=20.0
  Downloading packaging-25.0-py3-none-any.whl (66 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 66.5/66.5 KB 12.4 MB/s eta 0:00:00
Collecting cycler>=0.10
  Downloading cycler-0.12.1-py3-none-any.whl (8.3 kB)
Collecting kiwisolver>=1.3.1
  Downloading kiwisolver-1.4.8-cp310-cp310-manylinux_2_12_x86_64.manylinux2010_x86_64.whl (1.6 MB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 1.6/1.6 MB 12.6 MB/s eta 0:00:00
Requirement already satisfied: pillow>=8 in /usr/lib/python3/dist-packages (from matplotlib) (9.0.1)
Collecting contourpy>=1.0.1
```

Рисунок 3.8 - Встановлення залежностей Python

У рамках практичної частини було реалізовано налаштування системи виявлення загроз на основі зв’язки Suricata, ELK Stack (Elasticsearch, Logstash/Filebeat, Kibana) [17], [19] та елементів штучного інтелекту. На першому етапі було встановлено операційну систему Ubuntu, після чого виконано базове оновлення системних пакетів. Далі встановлювалася система Suricata через офіційний PPA- репозиторій. На рисунках 3.2, 3.3 зображено успішне встановлення Suricata та перевірку її працездатності за допомогою команди suricata --build-info.

Наступним етапом було налаштування системи моніторингу мережевого трафіку. Suricata була запущена в режимі прослуховування мережевого інтерфейсу, про що свідчить відповідний скріншот з терміналу. Після налаштування Suricata логи у форматі JSON (файл eve.json) почали зберігатися в директорії /var/log/suricata/, що підтверджено знімком каталогу з відповідними журналами подій.

Для обробки та візуалізації подій було розгорнуто стек ELK. (рисунки 3.4, 3.5). Спершу інстальовано Elasticsearch, який слугує для зберігання і швидкого пошуку логів. На скріншоті видно успішний запуск служби Elasticsearch. Далі було встановлено Kibana — вебінтерфейс для візуалізації даних. Після запуску служби користувач отримав доступ до панелі за адресою http://localhost:5601, що зафіксовано на зображенні браузера.

Щоб передавати журнали Suricata до Elasticsearch, було налаштовано Filebeat. У конфігураційному файлі Filebeat (filebeat.yml) (рисунок 3.6.) вказано шлях до файлу eve.json, а також вихід на Elasticsearch та Kibana. Скріншоти ілюструють правильне розпізнавання індексу у Kibana (filebeat-*) та подальший перегляд даних у розділі Discover.

Наступним кроком стало створення власного дашборду (рисунок 3.7). У Kibana були додані візуалізації, зокрема графіки частоти атак, карти геолокації IP-адрес джерел загроз, кругові діаграми типів атак тощо. На скріншотах показано приклади цих візуалізацій, які наочно демонструють потік мережевого трафіку та поведінкові аномалії.

Окрему увагу було приділено реалізації базової системи машинного навчання для виявлення аномалій. У середовищі Python з використанням бібліотек pandas та scikit-learn (рисунок 3.8.)було завантажено логи Suricata, здійснено попередню обробку даних, після чого застосовано алгоритм Isolation Forest для виявлення відхилень у мережевій поведінці. Результати аналізу подано у вигляді таблиці з відмітками аномальних подій, а також у вигляді графіка, на якому відображено співвідношення нормальних і підозрілих з'єднань. Відповідні скріншоти ілюструють як фрагмент коду, так і візуалізацію результатів.

3.4. Тестування та аналіз результатів

У процесі дослідження було реалізовано аналіз мережевого трафіку за допомогою логів, отриманих від системи виявлення атак Suricata (рис.3.8). Для виявлення аномальної активності було використано методи машинного навчання, зокрема алгоритм Isolation Forest. Цей алгоритм ефективно працює у випадках, коли переважна більшість даних є нормальними, а аномалії (наприклад, спроби зламу, порт-сканування чи brute-force атаки) трапляються рідко. Його основною ідеєю є те, що аномальні записи легше "ізолювати" на дереві рішень, тому вони швидше відсікаються, ніж звичайні.

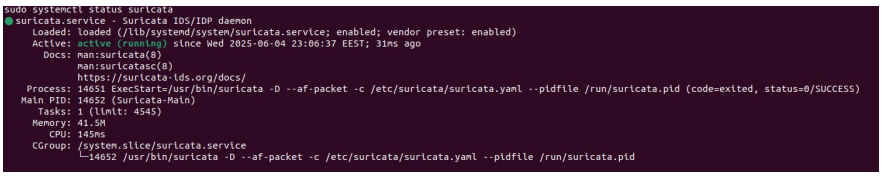


Рисунок 3.9 - Перевірка працездатності Suricata

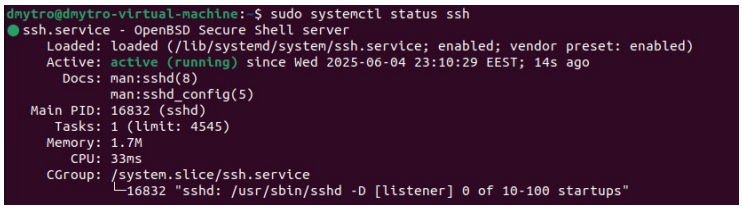


Рисунок 3.10 - Перевірка працездатності SSH

```
dmytro@dmytro-virtual-machine:~$ hydra -l test -P ~/rockyou.txt ftp://127.0.0.1
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these
*** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-04 22:37:12
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task
[DATA] attacking ftp://127.0.0.1:21/
[STATUS] 320.00 tries/min, 320 tries in 00:01h, 14344111 to do in 747:06h, 16 active
[STATUS] 316.67 tries/min, 950 tries in 00:03h, 14343481 to do in 754:56h, 16 active
```

Рисунок 3.11 - Запуск bruteforce – атаки з залученням Hydra

```
dmytro@dmytro-virtual-machine: ~
 GNU nano 6.2                                    analysis2.py
import pandas as pd
import json
from sklearn.ensemble import IsolationForest
import matplotlib.pyplot as plt

# 1. Зчитування логів eve.json
data = []
with open("eve.json", "r") as f:
    for line in f:
        try:
            data.append(json.loads(line))
        except json.JSONDecodeError:
            continue

df = pd.json_normalize(data)

# 2. Фільтрація потрібних полів
df = df[df['event_type'].isin(['alert', 'flow'])]
features = ['src_port', 'dest_port', 'proto']
df = df[features]

# Протоколи в числовий формат
df['proto'] = df['proto'].astype('category').cat.codes

# Видалення порожніх значень
df.dropna(inplace=True)

# 3. Isolation Forest
model = IsolationForest(contamination=0.1, random_state=42)
df['anomaly'] = model.fit_predict(df)

# 4. Побудова 3 окремих графіків
fig, axs = plt.subplots(1, 3, figsize=(18, 5))

# src_port
axs[0].scatter(df.index, df['src_port'], c=df['anomaly'].map({1: 'blue', -1: 'red'}))
axs[0].set_title('src_port (синє – нормально, червоне – аномалія)')
axs[0].set_xlabel('Індекс')
axs[0].set_ylabel('src_port')

# dest_port
```

Рисунок 3.12 - Код Python з застосуванням Isolation Forest

```
dmytro@dmytro-virtual-machine:~$ python3 analysis.py
Загальна кількість подій: 9
Виявлено аномалій: 1
```

Рисунок 3.13 - Результат роботи коду – виявлено 1 аномалія

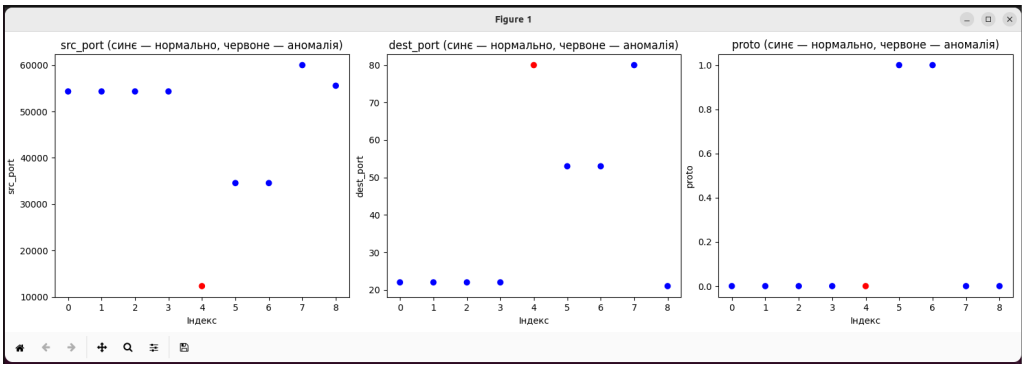


Рисунок 3.14 - Параметри аномалії на графіку

Рисунок 3.15 - Логи у Kibana, використані для аналізу

Під час обробки логів Suricata з файлу eve.json (рисунок 3.15) було відібранолише події типу alert та flow, які є найбільш значущими з точки зору аналізу безпеки. Далі проводилася попередня обробка даних — відбір релевантних полів (таких як source port, destination port, protocol), перетворення протоколів у числовий формат та очищення даних. Навчена модель Isolation Forest (рисунок 3.12). дозволила виявити записи, які могли вказувати на сканування портів або атаки на SSH (рисунки 3.13, 3.14). Для наочності аномалії було візуалізовано за допомогою бібліотек matplotlib та seaborn у вигляді кластерних графіків, де підозрілі точки були виділені окремим кольором.

Окрім аналізу в Python, важливою складовою дослідження став аналіз логів Suricata в Kibana. Цей інструмент, який є частиною стеку ELK (Elasticsearch, Logstash, Kibana), дозволив аналізувати та фільтрувати події, виводити таблиці з деталями кожного інциденту, а також створювати дашборди для комплексного моніторингу мережевої активності. Зокрема, за допомогою Kibana вдалося виявитита візуально підтвердити спроби brute force атак на SSH-порт з боку утиліти Hydra,(рисунок 3.11) що було зафіксовано у вигляді alert'ів Suricata з сигнатурою “ET SCAN Likely Hydra SSH Brute Force Attempt”.

У таблиці 3.1. вказано відмінності систем захисту інформації на основі штучного інтелекту за ті, які їх не використовують (сигнатурними, на основі правил).

Таблиця 3.1

Порівняння традиційних систем захисту інформації з такими на основі технологійштучного інтелекту

	Традиційні IDS	IDS на основі ШІ
Метод виявлення	Сигнатурний або на основі правил	Машинне навчання, поведінковий аналіз
Виявлення нових атак	Не виявляє невідомих атак	Здатні виявляти Zero-Day атаки
Помилкові спрацювання	При складних шаблонах	Знижується з часом завдяки самонавчанню
Налаштування та підтримка	Вимагає ручного налаштування правил	Потребує підготовки даних і навчання моделей
Масштабованість	Обмежена	Добре масштабується для великих обсягів даних
Швидкість реакції на загрози	Залежить від бази сигнатур	Реагує в реальному часі на нетипову поведінку
Адаптивність до новихзагроз	Практично відсутня – потребує ручного оновлення	Адаптується до нових шаблонів без втручання людини
Потреба в експертних знаннях	Адміністратор повинен розуміти правила	Фокус на підготовці навчальних даних
Візуалізація та аналітика	Обмежена (залежить від додаткових інструментів)	Часто інтегрована заналітикою та прогнозуванням
Складність впровадження	Відносно проста	Вища – через потребу в AI-інфраструктурі

3.5. Рекомендації щодо покращення

Ефективне впровадження систем штучного інтелекту у сфері кібербезпеки організацій потребує системного підходу, що охоплює всі етапи життєвого циклу таких рішень.

- Насамперед необхідно визначити актуальні потреби та цілі організації — якісаме задачі має вирішувати ШІ: виявлення аномальної активності, аналіз логів, автоматичне реагування на інциденти чи прогнозування загроз. Виходячи з цього, здійснюється вибір відповідних інструментів і технологій: перевагу слід надавати рішенням, що мають перевірену ефективність, підтримують машинне навчання, обробку великих даних та легко інтегруються з наявною інфраструктурою (SIEM, IDS/IPS, антивіруси тощо). При цьому особливу увагу слід приділяти захисту персональних і службових даних — використовувати анонімізацію, шифрування тапринципи Zero Trust.
- Після впровадження ШІ-системи необхідний постійний супровід. Доцільно впровадити інструменти моніторингу ефективності, включно з метриками точності виявлення загроз, рівнями хибнопозитивних та хибнонегативних спрацьовувань. Необхідно регулярно оновлювати або перевчати моделі на основі нових даних, атак і поведінкових шаблонів, забезпечуючи адаптивність до змін кіберсередовища. Водночас важливо зберігати людський контроль: рішення, прийняті ШІ, мають бути прозорими й доступними для аудиту, а аналітики — мати змогу втручатись уразі помилок чи неоднозначних ситуацій.
- Розвиток систем ШІ у сфері кібербезпеки має спиратися на інвестиції в дослідження та інновації. Рекомендується налагоджувати співпрацю з науковими установами, вивчати новітні підходи, зокрема генеративні моделі для виявлення фішингових атак, аналіз поведінкових профілів користувачів, автоматизовану обробку інцидентів тощо. Важливо також забезпечити постійне підвищення кваліфікації фахівців: проводити навчання з технологій ШІ, нових типів кіберзагроз і сучасних інструментів аналізу даних. Такий підхід сприяє

створеннюкультури інформаційної безпеки в організації.

- ШІ-системи мають бути прозорими та пояснюваними: користувачі повинні розуміти логіку їхніх рішень. Необхідно забезпечити відповідність чинному законодавству, таким як GDPR, а також дотримання галузевих стандартів (ISO/IEC 27001, NIST тощо). Регулярний аудит рішень ШІ з позиції безпеки, етики та законності — обов'язковий елемент сталого розвитку таких систем.

Висновки за розділом 3

У процесі реалізації було використано комплекс сучасних інструментів для виявлення та аналізу мережевих загроз, зокрема систему мережевого моніторингу Suricata, стек ELK (Elasticsearch, Logstash, Kibana), а також методи штучного інтелекту для поглибленого аналізу даних. Suricata забезпечила можливість фіксації подій у мережі на основі сигнатурних правил, що дозволило виявляти спроби сканування портів, підозрілі з'єднання та інші види небажаної активності. Зібрані логи у форматі JSON були автоматично передані до Elasticsearch за допомогою Filebeat або Logstash, де дані зберігалися у зручному для пошуку та обробки вигляді. За допомогою Kibana було побудовано візуальні дашборди, що дозволяють наочно аналізувати трафік, визначати найбільш активні IP-адреси, типиатак та їхню географію.

Для підвищення ефективності аналізу було застосовано алгоритм машинного навчання Isolation Forest, що дозволив виявити аномальні події у мережевому трафіку, які не були визначені Suricata. Такий підхід дав змогу доповнити сигнатурний метод аналізу поведінковою аналітикою, що суттєво підвищило точність виявлення потенційних загроз і зменшило кількість хибнопозитивних спрацювань. У підсумку побудована система є адаптивною, масштабованою та ефективною для моніторингу мережі в реальному часі. Її застосування дозволяє не лише виявляти вже відомі атаки, а й ідентифікувати нові загрози за рахунок використання інтелектуального аналізу, що робить таку

архітектуру доцільною длявпровадження в сучасні системи кібербезпеки.

Також у цьому розділі були досліджені рекомендації щодо покращення роботи систем штучного інтелекту у кібербезпеці, для їх злагодженої та якісної роботи і правильної ідентифікації загроз.

ВИСНОВКИ

У межах даної кваліфікаційної роботи було здійснено всебічне дослідження сучасного стану кібербезпеки як на глобальному рівні, так і в контексті України. Проаналізовано основні загрози, методи здійснення кібератак і сучасні підходи до їхнього запобігання, з особливим акцентом на можливості використання технологій штучного інтелекту (ШІ).

Особлива увага приділялася дослідженню ролі ШІ в кіберзахисті: розглянуто ключові алгоритми, методи машинного навчання, приклади реальних програмних рішень та оцінено їхню ефективність у виявленні та нейтралізації загроз. Окремо проаналізовано технічні й організаційні аспекти впровадження таких рішень у різних секторах — зокрема, в обороні, енергетиці, охороні здоров’я, освіті та фінансовій сфері.

Узагальнення результатів підтвердило високу ефективність застосування технологій штучного інтелекту в забезпеченні кібербезпеки, особливо в аспектах виявлення загроз, поведінкового аналізу користувачів та автоматизованого реагування на інциденти. Це робить ШІ потужним інструментом для підсилення захисту як окремих організацій, так і цілих секторів критичної інфраструктури.

У межах реалізації було застосовано сучасні інструменти для виявлення та аналізу мережевих загроз. Зокрема, система мережевого моніторингу Suricata забезпечила виявлення аномальної активності на основі сигнатур, дозволяючи фіксувати спроби сканування портів, підозрілі з’єднання та інші загрози. Зібрані логи у форматі JSON автоматично передавалися до Elasticsearch за допомогою Filebeat або Logstash, де зберігалися у зручному для пошуку форматі. Візуалізацію даних забезпечувала Kibana, що дозволило аналізувати трафік, активність IP-адрес,типи атак та їх географічне походження.

Для підвищення точності аналізу було застосовано алгоритм машинного навчання Isolation Forest, який дозволив виявляти аномальні події в трафіку,

непомічені сигнатурним методом Suricata. Така комбінація інструментів поєднує класичний сигнатурний підхід із поведінковою аналітикою, що суттєво підвищує якість виявлення загроз і знижує кількість хибнопозитивних спрацювань. У результаті було побудовано адаптивну, масштабовану та ефективну систему для моніторингу мережі в реальному часі. Вона дозволяє виявляти як відомі типи атак, так і нові загрози завдяки інтелектуальному аналізу, що робить її доцільною для впровадження в сучасних системах кіберзахисту.

Також у межах дослідження було розроблено низку практичних рекомендацій для покращення роботи систем штучного інтелекту в сфері кібербезпеки. Вони спрямовані на забезпечення їх стабільного функціонування, підвищення точності ідентифікації загроз та інтеграції в загальну структуру інформаційної безпеки організації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Strategic Sectors and Applications of AI in Ukraine [Електронний ресурс]. – Digital State, червень 2025. – Режим доступу: доступно онлайн digitalstate.gov.ua.

2. Роль штучного інтелекту в кібербезпеці: передбачення та запобігання атакам [Електронний ресурс]. – eba.com.ua, оновлена стаття 2025 р. journals.politehnica.dp.ua+1apcssm.vnu.edu.ua+1.

3. ШТУЧНИЙ ІНТЕЛЕКТ: КІБЕРБЕЗПЕКА НОВОГО ПОКОЛІННЯ [Електронний ресурс]. – PDF-стаття (2024) dblp.org+12researchgate.net+12apcssm.vnu.edu.ua+12.

4. ШТУЧНИЙ ІНТЕЛЕКТ У СФЕРІ КІБЕРБЕЗПЕКИ: ВИКЛИКИ [Електронний ресурс]. – ResearchGate, 2025 researchgate.net+1apcssm.vnu.edu.ua+1.

5. Russian Cyber Onslaught was Blunted by Ukrainian Cyber Resilience, not Merely Security [Електронний ресурс]. – ArXiv, серпень 2024 researchgate.net+11arxiv.org+11themoonlight.io+11.

6. Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research [Електронний ресурс]. – ArXiv, серпень 2022 (XAI у кібербезпеці) arxiv.org+8arxiv.org+8ijirset.com+8.

7. Artificial Intelligence (AI) In Cyber Security Market Will Reach to USD 30.9 Billion By 2025: Zion Market Research [Електронний ресурс]. – GlobeNewswire, 2019.

8. Проблеми кібербезпеки інформаційно-телекомунікаційних систем: Збірник матеріалів доповідей та тез; Київ, 26 квітня 2024 р.; КНУ ім. Т. Шевченка / редкол.: В. В. Ільченко та ін. – К.: ВПЦ «Київський університет», 2024. – 171 с. – С. 122–124.

9. Aussie banks targeted in global cyber heist as Chinese hackers infiltrate telcos [Електронний ресурс] // The Australian. 2024.– Режим доступу:

https://www.theaustralian.com.au/business/technology/aussie-banks-targeted-in-global- cyber-heist-as-chinese-hackers-infiltrate-telcos/news-story/c066b6818dad4039babbf900b46715cd.

10. Research finds most Aussie banks fail to fully protect customers from email scams [Електронний ресурс] // News.com.au. – 2024. – Режим доступу: https://www.news.com.au/technology/online/security/research-finds-most-aussie-banks-fail-to-fully-protect-customers-from-email-scams/news story/cc9a1d6981b0c8dfb38ca5ff73727320.

11. Social engineering tactics targeting banking employees [Електронний ресурс]// Authentic8 Blog. – 2024. – Режим доступу: https://authentic8.com/blog/social- engineering-tactics-targeting-banking-employees.

12. Проблеми кібербезпеки інформаційно-телекомунікаційних систем: Збірник матеріалів доповідей та тез; м. Київ, 26 квітня 2024 року; Київський національний університет імені Тараса Шевченка / Редкол.: В.В. Ільченко, д.ф.-м.н., проф., (голова) та ін. – К.: ВПЦ "Київський університет", 2024. – 171 с. – С. 122–124.

13. Маньковський Д.О, Даков С.Ю СИСТЕМИ ШТУЧНОГО ІНТЕЛЕКТУ В КІБЕРБЕЗПЕЦІ ТА ЇХНІ МОЖЛИВОСТІ ПРОТИСТОЯТИ СУЧАСНИМ КІБЕРЗАГРОЗАМ. (2025). Безпека інформаційних систем і технологій, 2(8), 42- 48. https://doi.org/10.17721/ISTS.2024.8.42-48

14. Xmind [Електронний ресурс]. – Режим доступу: https://www.xmind.net.

15. Lucidchart [Електронний ресурс]. – Режим доступу: https://www.lucidchart.com.

16. Ковальчук, С. О., Марченко, І. М. (2020). Використання систем виявлення вторгнень Suricata в комп’ютерних мережах. Інформаційні технології та комп’ютерна інженерія, 1(47), 68–73.

17. Іванченко, А. Ю., & Романчук, М. С. (2021). Застосування стека ELK для аналізу подій інформаційної безпеки. Захист інформації, 23(2), 45–52.

18. Open Information Security Foundation. Suricata User Guide [Електронний ресурс]. – Режим доступу: https://suricata.readthedocs.io/en/latest/.

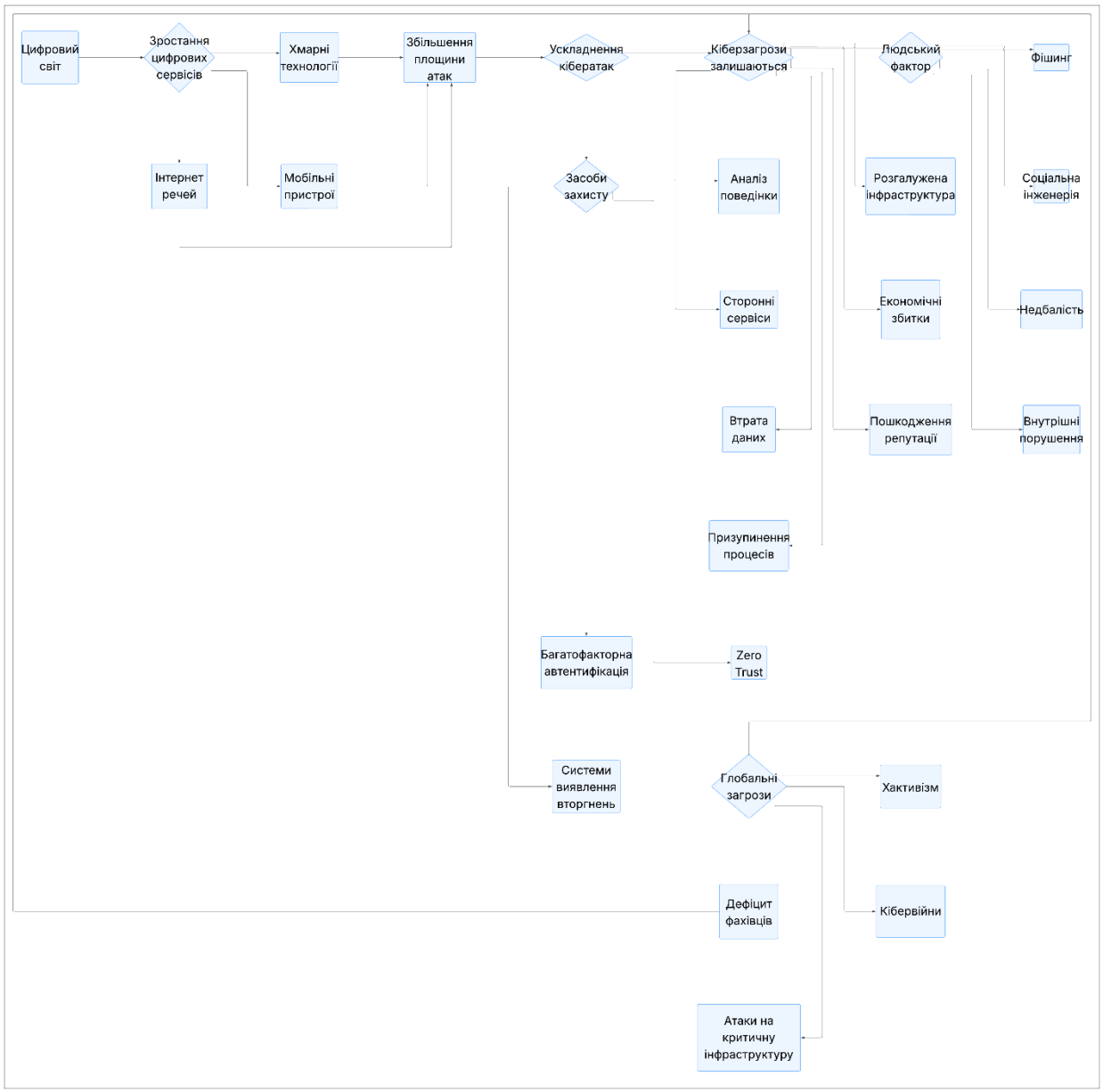
19. Elastic NV. The Elastic Stack: Elasticsearch, Logstash, Kibana Documentation [Електронний ресурс]. – Режим доступу: https://www.elastic.co/guide/index.html.

20. *Global Cybersecurity Outlook 2025* [Електронний ресурс] – World Economic Forum PDF, 2025

ДОДАТКИ

ДОДАТОК А

Схема загроз та проблематики у кібербезпеці



ДОДАТОК Б

Код реалізації Isolation Forest з залученням Python

```
import pandas as pd
import json
from sklearn.ensemble import IsolationForest
import matplotlib.pyplot as plt
# 1. Зчитування логів eve.json
data = []
with open("eve.json", "r") as f:
    for line in f:
        try:
            data.append(json.loads(line))
        except json.JSONDecodeError:
            continue
df = pd.json_normalize(data)
# 2. Фільтрація потрібних полів
df = df[df['event_type'].isin(['alert', 'flow'])]
features = ['src_port', 'dest_port', 'proto']
df = df[features]
# Протоколи в числовий формат
df['proto'] = df['proto'].astype('category').cat.codes
# Видалення порожніх значень
df.dropna(inplace=True)
# 3. Isolation Forest
model = IsolationForest(contamination=0.1, random_state=42)
df['anomaly'] = model.fit_predict(df)
# 4. Побудова 3 окремих графіків
fig, axs = plt.subplots(1, 3, figsize=(18, 5))
# src_port
```

Продовження додатку Б

```
axs[0].scatter(df.index, df['src_port'], c=df['anomaly'].map({1: 'blue', -1: 'red'}))
axs[0].set_title('src_port (синє — нормально, червоне — аномалія)')
axs[0].set_xlabel('Індекс')
axs[0].set_ylabel('src_port')
# dest_port
axs[1].scatter(df.index, df['dest_port'], c=df['anomaly'].map({1: 'blue', -1: 'red'}))
axs[1].set_title('dest_port (синє — нормально, червоне — аномалія)')
axs[1].set_xlabel('Індекс')
axs[1].set_ylabel('dest_port')
# proto
axs[2].scatter(df.index, df['proto'], c=df['anomaly'].map({1: 'blue', -1: 'red'}))
axs[2].set_title('proto (синє — нормально, червоне — аномалія)')
axs[2].set_xlabel('Індекс')
axs[2].set_ylabel('proto')
plt.tight_layout()
plt.show()
# 5. Збереження аномалій
anomalies = df[df['anomaly'] == -1]
anomalies.to_csv("suricata_anomalies.csv", index=False)
print("Збережено аномалії у файл suricata_anomalies.cs
```

ДОДАТОК В

Приклад логів, які генерує Suricata

{"timestamp":"2025-06-
04T21:00:01.000000+0000","flow_id":1000001,"in_iface":"lo","event_type":"alert","
src_ip":"192.168.1.10","src_port":54321,"dest_ip":"127.0.0.1","dest_port":22,"proto"
:"T
CP","alert":{"action":"allowed","gid":1,"signature_id":200001,"rev":1,"signatur
e":"SS H Brute Force Attempt","category":"Attempted Administrator Privilege
Gain","severity":2}}
{"timestamp":"2025-06-
04T21:00:02.000000+0000","flow_id":1000002,"in_iface":"lo","event_type":"alert","
src_ip":"192.168.1.10","src_port":54322,"dest_ip":"127.0.0.1","dest_port":22,"proto"
:"T
CP","alert":{"action":"allowed","gid":1,"signature_id":200001,"rev":1,"signatur
e":"SS H Brute Force Attempt","category":"Attempted Administrator Privilege
Gain","severity":2}}
{"timestamp":"2025-06-
04T21:00:03.000000+0000","flow_id":1000003,"in_iface":"lo","event_type":"alert","
src_ip":"192.168.1.10","src_port":54323,"dest_ip":"127.0.0.1","dest_port":22,"proto"
:"T
CP","alert":{"action":"allowed","gid":1,"signature_id":200001,"rev":1,"signatur
e":"SS H Brute Force Attempt","category":"Attempted Administrator Privilege
Gain","severity":2}}
{"timestamp":"2025-06-
04T21:00:04.000000+0000","flow_id":1000004,"in_iface":"lo","event_type":"alert","
src_ip":"192.168.1.10","src_port":54324,"dest_ip":"127.0.0.1","dest_port":22,"proto"
:"T
CP","alert":{"action":"allowed","gid":1,"signature_id":200001,"rev":1,"signatur
e":"SS H Brute Force Attempt","category":"Attempted Administrator Privilege

Продовження додатку В

Gain","severity":2}}

{"timestamp":"2025-06-
04T21:00:05.000000+0000","flow_id":1000005,"in_iface":"lo","event_type":"flow","
src_ip":"127.0.0.1","src_port":12345,"dest_ip":"127.0.0.1","dest_port":80,"proto":"T
CP"}
{"timestamp":"2025-06-
04T21:00:06.000000+0000","flow_id":1000006,"in_iface":"lo","event_type":"flow","
src_ip":"10.0.2.15","src_port":34567,"dest_ip":"8.8.8.8","dest_port":53,"proto":"UD
P"}
{"timestamp":"2025-06-
04T21:00:07.000000+0000","flow_id":1000007,"in_iface":"lo","event_type":"flow","
src_ip":"10.0.2.15","src_port":34568,"dest_ip":"1.1.1.1","dest_port":53,"proto":"UD
P"}
{"timestamp":"2025-06-
04T21:00:08.000000+0000","flow_id":1000008,"in_iface":"lo","event_type":"alert","
src_ip":"192.168.1.20","src_port":60000,"dest_ip":"127.0.0.1","dest_port":80,"proto"
:"T
CP","alert":{"action":"allowed","gid":1,"signature_id":200002,"rev":1,"signature
":"Pos sible Web Attack","category":"Web Application Attack","severity":3}}
{"timestamp":"2025-06-
04T21:00:09.000000+0000","flow_id":1000009,"in_iface":"lo","event_type":"flo
w","src_ip":"192.168.1.15","src_port":55555,"dest_ip":"127.0.0.1","dest_port":2
1,"proto":"T CP"}

ДОДАТОК Г

Скрипт Logstash для взаємодії ELK та Kibana

```
input {
  file {
    path => "/var/log/suricata/eve.json"
    codec => json
    start_position => "beginning"
  }
}

filter {
  if [event_type] == "alert" {
    mutate {
      add_tag => [ "suricata", "alert" ]
    }
  }
}

output {
  elasticsearch {
    hosts => ["http://localhost:9200"]
    index => "suricata-%{+YYYY.MM.dd}"
  }
}
```