МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний університет імені В. Н. Каразіна

Факультет: **ННІ Каразінський банківський інститут**
Кафедра: **Інформаційних технологій та математичного моделювання**
Спеціальність: **122 Комп'ютерні науки**
Освітня програма: **Комп'ютерні науки та інформаційні технології в бізнесі**

Група: АК-41б **денна форма навчання**

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

на тему:

ДОСЛІДЖЕННЯ ТА АНАЛІЗ ПОПУЛЯРНИХ ПЛАТФОРМ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ ТА МОДЕЛЕЙ ШТУЧНОГО ІНТЕЛЕКТУ
ЗА НАКАЗОМ № 4601-5/335 ВІД 07 ЛЮТОГО 2025 РОКУ

здобувача вищої освіти **Кайдалової Ангеліни Євгеніївни**

Робота допущена до захисту в ЕК
протокол кафедри ІТММ № 13 від 31.05.2025 р

Завідувач кафедри
к. п. н.
_____ Н. І. Стяглик

Науковий керівник
к. ф.-м. н.
_____ Н. Н. Чеканова

м. Харків 2025 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Харківський національний університет імені В. Н. Каразіна

Факультет навчально-науковий інститут "Каразінський банківський інститут"
Кафедра інформаційних технологій та математичного моделювання
Рівень вищої освіти перший (бакалаврський)
Спеціальність 122 Комп'ютерні науки
Освітня програма Комп'ютерні науки та інформаційні технології в бізнесі

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ **Н. І. Стяглик**
Підпис ініціали, прізвище

08 лютого 2025 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ (ПРОЄКТ)

Кайдалової Ангеліни Євгеніївни
(прізвище, ім'я, по батькові студента)

1. Тема роботи "Дослідження використання штучного інтелекту в інформаційній безпеці "

керівник роботи к. ф.-м. н., доцент Н. М. Чеканова
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від 08 лютого 2025 року № 4601-5/335

2. Строк подання студентом роботи 10 травня 2025 року

3. Перелік питань, які потрібно розробити:
У розділі 1: Теоретичні основи інформаційної безпеки.
У розділі 2: Штучний інтелект: поняття, методи, інструменти.
У розділі 3: Сучасні підходи до застосування ШІ в інформаційній безпеці.

4. План роботи

№ з/п	Назви етапів роботи
1	Вибір здобувачем теми кваліфікаційної бакалаврської роботи
2	Затвердження плану і завдання кваліфікаційної бакалаврської роботи
3	Здача кваліфікаційної бакалаврської роботи керівнику
4	Підпис кваліфікаційної бакалаврської роботи керівника
5	Підпис кваліфікаційної бакалаврської роботи у нормоконтролера
6	Допуск завідувачем кафедри до захисту кваліфікаційної бакалаврської роботи
7	Захист кваліфікаційної бакалаврської роботи

5. Дата видачі завдання 08 лютого 2025 року

Студент _____ А. Є. Кайдалова
підпис ініціали, прізвище

Керівник роботи _____ Н. М. Чеканова
підпис ініціали, прізвище

РЕФЕРАТ
НА КВАЛІФІКАЦІЙНУ БАКАЛАВРСЬКУ РОБОТУ
«ДОСЛІДЖЕННЯ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ»

Кайдалової Ангеліни Євгеніївни

Кваліфікаційна бакалаврська робота містить: 53 сторінок, 6 таблиць, 2 рисунки, список літератури з 31 найменувань.

Кваліфікаційна бакалаврська робота присвячена вивченню теоретичних та практичних аспектів застосування технологій штучного інтелекту у сфері інформаційної безпеки. У ній розглянуто сучасні виклики, пов’язані зі зростанням кількості кіберзагроз, а також наголошено на необхідності впровадження інтелектуальних систем для виявлення, попередження та реагування на інциденти безпеки.

Метою роботи є дослідження можливостей і ефективності використання алгоритмів машинного навчання для автоматизації захисту інформаційних систем. Для досягнення поставленої мети були проаналізовані принципи роботи систем штучного інтелекту, методи класифікації даних, виявлення аномалій та обробки великих обсягів інформації в режимі реального часу.

У практичній частині було реалізовано модель машинного навчання, яка на основі аналізу мережевого трафіку дозволяє виявляти потенційні кіберзагрози. Для навчання та тестування моделі використано відкритий датасет NSL-KDD. Проведено оцінку точності моделі за відповідними метриками (точність, повнота, F1-оцінка).

Результати дослідження демонструють, що системи, побудовані з використанням ШІ, мають значний потенціал у сфері інформаційної безпеки, зокрема у швидкому реагуванні на загрози, зменшенні кількості помилкових спрацювань та покращенні загальної ефективності захисту.

Ключові слова: штучний інтелект, інформаційна безпека, машинне навчання, кіберзагроза, виявлення атак, NSL-KDD.

ANNOTATION
AT QUALIFICATION BACHELOR WORK
" RESEARCH ON THE USE OF ARTIFICAL INTELLIGENCE IN INFORMATION SECURITY"
Kaidalova Angelina Yevheniivna

The bachelor's thesis contains 53 pages, 6 tables, 2 drawings, a list of references of 31 titles.

This qualification work is dedicated to the study of theoretical and practical aspects of applying artificial intelligence technologies in the field of information security. It addresses modern challenges related to the increasing number of cyber threats and highlights the necessity of implementing intelligent systems for detecting, preventing, and responding to security incidents.

The aim of the thesis is to investigate the possibilities and effectiveness of using machine learning algorithms to automate the protection of information systems. To achieve this goal, the principles of artificial intelligence systems were analyzed, along with methods of data classification, anomaly detection, and the real-time processing of large volumes of information.

In the practical part, a machine learning model was implemented to detect potential cyber threats based on network traffic analysis. The open NSL-KDD dataset was used for training and testing the model. The model’s performance was evaluated using appropriate metrics (accuracy, recall, F1-score).

The research results demonstrate that systems built using AI have significant potential in the field of information security, particularly in rapid threat detection, reducing the number of false positives, and improving the overall efficiency of protection.

KEY WORDS: ARTIFICAL INTELLIGENCE, INFORMATION SECURITY, MACHINE LEARNING, CYBER THREAT, ATTACK DETECTION, NSL-KDD.

ЗМІСТ

ВСТУП

У сучасному цифровому світі, де обсяги інформації постійно зростають, а технології розвиваються надзвичайно швидкими темпами, питання інформаційної безпеки стає все більш актуальним. Кіберзагрози еволюціонують, набуваючи складніших форм і масштабів, що робить традиційні методи захисту недостатньо ефективними. У зв'язку з цим виникає потреба у впровадженні новітніх підходів до забезпечення безпеки інформаційних систем, серед яких особливе місце займають технології штучного інтелекту (ШІ).

Штучний інтелект відкриває нові можливості для виявлення, запобігання та нейтралізації кіберзагроз завдяки здатності аналізувати великі обсяги даних, виявляти аномалії, приймати рішення в реальному часі. Такі системи здатні навчатися на попередньому досвіді, адаптуватися до нових типів атак і значно знижувати навантаження на фахівців з кібербезпеки.

Актуальність дослідження полягає у необхідності вивчення ефективності застосування ШІ у сфері інформаційної безпеки, аналізу існуючих рішень, а також створення власної моделі виявлення кіберзагроз з використанням алгоритмів машинного навчання.

Метою дипломної роботи є дослідження можливостей застосування технологій штучного інтелекту для підвищення рівня захисту інформаційних систем.

Об'єктом дослідження є процеси забезпечення інформаційної безпеки.

Предметом дослідження є методи й інструменти штучного інтелекту, які використовуються для виявлення та протидії кіберзагрозам.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

1.1. Основні поняття та принципи інформаційної безпеки

У сучасному цифровому світі інформація є одним з найцінніших ресурсів, а її захист — стратегічним завданням як для державних структур, так і для бізнесу. Зі зростанням обсягів обробки, зберігання та передачі даних, питання забезпечення інформаційної безпеки набуває особливої актуальності. Інформаційна безпека — це стан захищеності інформаційних ресурсів та процесів обробки інформації від внутрішніх і зовнішніх загроз, що забезпечує їх конфіденційність, цілісність і доступність. Її метою є забезпечення безперервної та стабільної роботи інформаційних систем, а також захист даних від несанкціонованого доступу, змін або знищення.

Основні характеристики інформаційної безпеки:

1. Конфіденційність (Confidentiality) — гарантує, що доступ до інформації мають лише ті особи, які мають відповідні повноваження. Це запобігає несанкціонованому розголошенню даних.
2. Цілісність (Integrity) — забезпечує точність, повноту та достовірність інформації, а також гарантує, що вона не була змінена або пошкоджена сторонніми особами.
3. Доступність (Availability) — означає, що інформація та відповідні ресурси завжди доступні для авторизованих користувачів тоді, коли це необхідно.
4. Аутентифікація (Authentication) — процес перевірки особи або джерела даних для підтвердження їх справжності.
5. Авторизація (Authorization) — надання користувачам відповідних прав доступу до інформації чи системних функцій після аутентифікації.
6. Контроль доступу (Access Control) — механізм обмеження доступу до інформаційних ресурсів відповідно до встановлених політик

безпеки.

7. Неспростовність (Non-repudiation) — гарантія того, що суб'єкт не зможе заперечити свою участь у певних діях або транзакціях, що важливо для юридичної відповідальності.

8. Загроза (Threat**)** — потенційна подія або дія, яка може призвести до порушення безпеки інформаційної системи.

9. Вразливість (Vulnerability) — слабке місце системи або процесу, яке може бути використано для здійснення атаки або проникнення.

Принципи забезпечення інформаційної безпеки

Для ефективного забезпечення інформаційної безпеки застосовуються такі основні принципи:

1. Принцип мінімальних привілеїв: кожен користувач або процес має доступ лише до тих ресурсів, які необхідні для виконання його функцій. Це зменшує ризик зловживання або випадкових помилок.

2. Принцип розділення обов'язків: важливі процеси розподіляються між кількома особами чи системами, щоб уникнути концентрації повноважень в одних руках.

3. Принцип багаторівневого захисту (Defense in Depth): застосування кількох рівнів захисту, включаючи фізичні, адміністративні та технічні засоби. Це підвищує загальний рівень стійкості системи до атак.

4. Принцип безпеки за замовчуванням: інформаційні системи мають бути спочатку налаштовані з максимальним рівнем безпеки, з можливістю подальшого адаптування до конкретних потреб.

5. Принцип своєчасного оновлення: регулярне оновлення програмного забезпечення, систем управління безпекою та баз знань дозволяє вчасно реагувати на нові загрози.

6. Принцип економічної ефективності: заходи захисту повинні бути економічно обґрунтованими, тобто витрати на безпеку не повинні перевищувати потенційні збитки від її порушення.

7. Принцип відновлення та реагування: організація має бути готова до інцидентів безпеки, мати чіткий план реагування, резервного копіювання та відновлення функціонування після інцидентів.

Приклади застосування принципів безпеки:

1. Атака типу Ransomware: Рансомні програми, такі як WannaCry, використовують вразливості в системах для шифрування файлів і вимагання викупу. Принципи безпеки за замовчуванням і своєчасне оновлення допомогли б уникнути цієї атаки.

2. Фішинг: Фішингова атака, коли зловмисник видає себе за офіційну особу для отримання конфіденційної інформації, є яскравим прикладом важливості аутентифікації та принципу мінімальних привілеїв.

1.2. Класифікація загроз та вразливостей

У сфері інформаційної безпеки важливим аспектом є ідентифікація та класифікація загроз і вразливостей, що дозволяє ефективно керувати ризиками та будувати надійні системи захисту інформації. Загрози та вразливості визначають потенційні слабкі місця системи та можливі дії, які можуть порушити її цілісність, конфіденційність чи доступність.

Поняття загрози та вразливості

Загроза — це потенційна можливість виникнення події, яка може завдати шкоди інформаційній системі або даним. Загроза може бути як навмисною (хакерська атака), так і випадковою (збій обладнання, помилка користувача).

Вразливість — це слабке місце в системі, яке може бути використане для реалізації загрози. Це можуть бути технічні недоліки програмного забезпечення, недотримання політик безпеки, людський фактор тощо.

Загрози класифікують за кількома критеріями:

1. За джерелом походження:

- Природні — повені, пожежі, землетруси;

- Техногенні — збої в обладнанні, відмова живлення, помилки ПЗ;
- Людські: навмисні (вторгнення, шкідливе ПЗ, фішинг); ненавмисні (помилки користувача, випадкове видалення даних).
- За способом впливу:
- Пасивні — спостереження, перехоплення інформації без втручання;
- Активні — зміна, знищення чи блокування інформації або ресурсів.

2. За характером об’єкта атаки:

- на дані (знищення, спотворення, крадіжка інформації);
- на мережі (DoS-атаки, перехоплення трафіку);
- на системи управління (захоплення контролю, шкідливе ПЗ).

Класифікація вразливостей

Вразливості поділяються на такі категорії:

1. Технічні:

- помилки в архітектурі програмного забезпечення;
- неоновлене ПЗ, «дірки» в безпеці;
- неправильно налаштоване обладнання.

2. Організаційні:

- відсутність політик інформаційної безпеки;
- слабка система контролю доступу;
- ненавченість персоналу.

3.Фізичні:

- відсутність охорони приміщень;
- недостатній захист від стихійних лих чи крадіжок.

4.Соціальні (людський фактор):

- фішинг;
- соціальна інженерія;
- недбале поводження з конфіденційною інформацією.

Взаємозв’язок загроз, вразливостей та ризиків

Загроза не обов’язково призведе до інциденту без наявної вразливості. Ризик виникає лише тоді, коли загроза може використати вразливість. Таким чином, ефективне управління ризиками передбачає ідентифікацію обох складових та мінімізацію потенційних наслідків.

Коли говориться про інформаційну безпеку важливо розуміти, що захищати треба усю складну систему, включно з комп’ютерами, телефонами, програмами і мережами. Кожна з цих частин, або доменів, мають свої особливості щодо видів загроз.

Наприклад, у мережевій безпеці головна мета – захистити канали зв’язку та обладнання, через які йде трафік. Тут часто зустрічаються атаки, що намагаються завалити мережу запитами (DDoS), підслухати розмову або непомітно прибратися всередину.

Безпека додатків зосереджена на захисті програм від мобільних застосунків до складних веб-сервісів. Розробники можуть випадкову залишити вразливості в коді, якими зловмисники скористаються, щоб отримати доступ до даних або зламати сам додаток (класичні приклади – SQL ін’єкції чи XSS).

Коли говоримо про безпеку даних, це про те, як зберегти інформацію в таємниці (конфіденційність), незмінною (цілісність) і доступною. Тут ризики – це витоки персональних даних з баз, несанкціоноване копіювання або шифрування даних шифрувальниками-вимагачами.

З розвитком хмарних технологій з’явилися й нові виклики. Частина відповідальності за безпеки перекладається на провайдера хмари, але левова частка все одно залишається на користувачеві – це правильна конфігурація сервісів, управління доступом. Помилки тут можуть призвести до масштабних витоків.

Кінцеві точки – комп’ютера, смартфони – теж під прицілом. Віруси, програми-шпигуни, той самий фішинг, що намагається виманити паролі – це все про безпеку кінцевих пристроїв.

І навіть розумні пристрої Інтернету речей (IoT) – від камер відеоспостереження до чайників – можуть стати слабкою ланкою, якщо їх погано захистити. Вони можуть бути використані для створення ботнетів або стати точкою входу в домашню чи корпоративну мережу.

Реалізація будь-якої з цих загроз може мати дуже неприємні наслідки.

Це не просто зламали щось. Це може призвести до величезних фінансових втрат, завдати серйозної шкоди репутації компанії чи людини, спричинити юридичні проблеми через витік чутливих даних, повністю зупинити роботу бізнесу чи важливої інфраструктури і, підірвати довіру клієнтів чи партнерів. Тому розуміння цих загроз ті їхніх наслідків – перший крок до побудови надійного захисту.

Домени для інформаційної безпеки зазначені у таблиці:

Таблиця 1.2

Домен ІБ	Опис	Типові загрози	Ключові принципи, що застосовуються
Мережева безпека	Захист мережевої інфраструктури та трафіку	DDoS, сканування портів, перехоплення трафіку	Конфіденційність, доступність, цілісність
Безпека додатків	Захист програмного забезпечення та веб-сервісів	SQLi, XSS, уразливості «нульового дня»	Цілісність, конфіденційність

Продовження таблиці 1.2

Безпека даних	Захист інформації при зберіганні та передачі	Витік даних, несанкціонований доступ до БД	Конфіденційність, цілісність
Безпека кінцевих точок	Захист робочих станцій, ноутбуків	Malware, Rensomware, Фішинг	Цілісність, конфіденційність, доступність
Безпека хмарних систем	Захист ресурсів у хмарному середовищі	Неправильна конфігурація, зламані облікoвки, API-атаки	Спільна відповідальність, контроль доступу
IoT безпека	Захист підключених пристроїв	Боти для для DDoS, несанкціонований доступ до пристроїв	Автентифікація, цілісність, доступність

Джерело: розробка автора

Ця таблиця узагальнює ключові домени інформаційної безпеки, подаючи короткий опис кожного з них, типові загрози, що виникають у відповідному контексті, а також основні принципи захисту, які застосовуються. Вона охоплює як класичні напрями — мережеву безпеку, захист додатків та даних, так і сучасні виклики, пов’язані з безпекою кінцевих точок, хмарних середовищ і пристроїв Інтернету речей (IoT).

Кожен домен має власну специфіку: наприклад, хмарні системи вимагають дотримання моделі спільної відповідальності, тоді як безпека IoT пов’язана з обмеженими ресурсами пристроїв і слабким контролем доступу.

Типові загрози варіюються — від DDoS-атак і фішингу до складних атак через уразливості нульового дня або ненадійні API.

За додатковим варіантом, додаєм тріаду для розуміння класичної моделі інформаційної безпеки – тріаду ЦАС зображену на Рисунку 1.2.

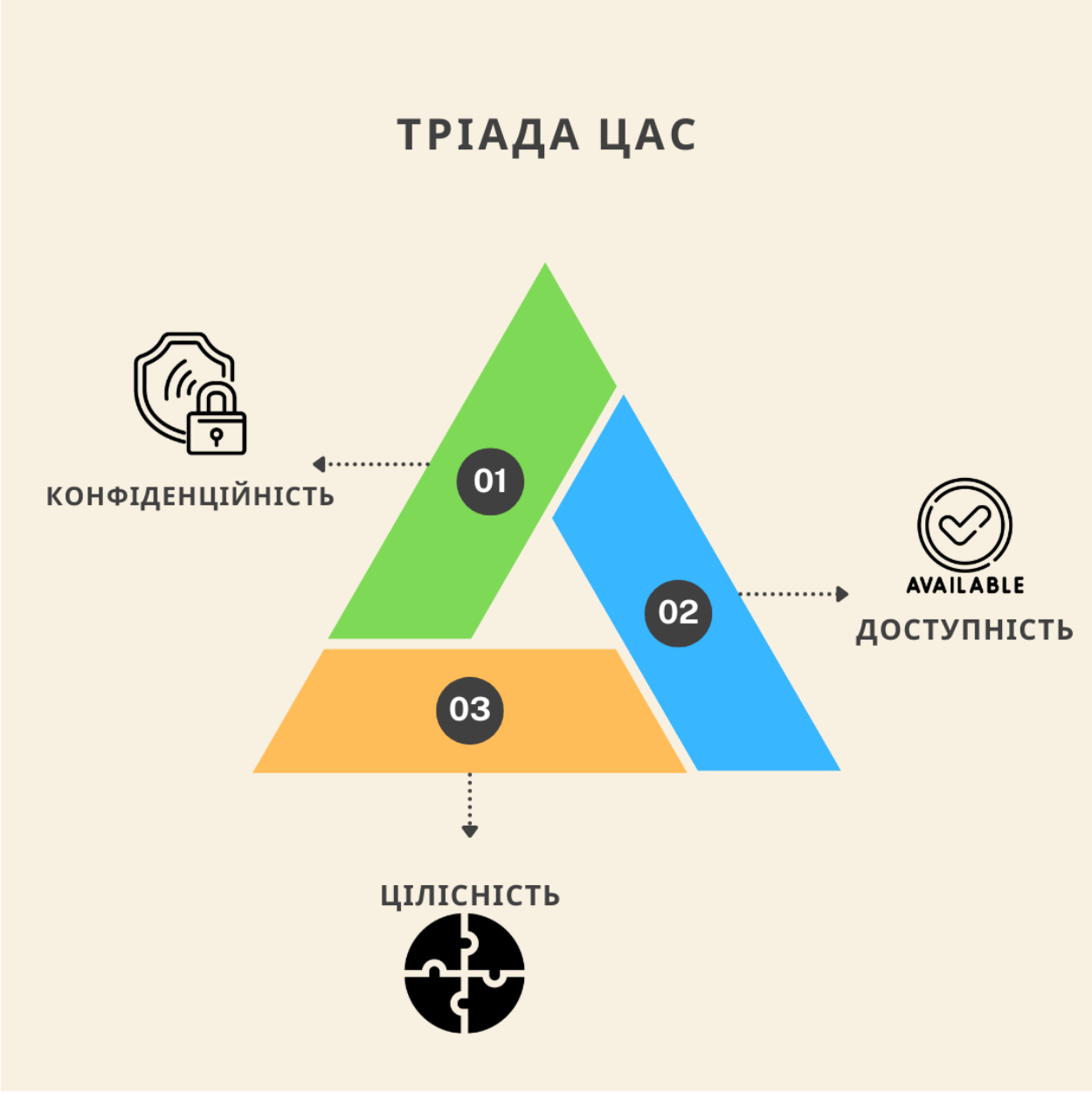

Рисунок 1.2. Тріада ЦАС

На рисунку зображено класичну модель інформаційної безпеки – тріаду ЦАС, яка складається з трьох ключових принципів: конфіденційість, цілісність

та доступність. Ці принципи візуалізовано у вигляді рівностороннього трикутника, кожна вершина якого відповідає одному з базових компонентів захисту інформації:

- Конфіденційність – забезпечення захисту інформації від несанкціонованого доступу. Це передбачає політику доступу, шифрування, автентифікацію користувачів тощо.
- Цілісність – гарантує, що інформація не була змінена або знищена сторонніми особами без відповідних повноважень. Засобами забезпечення є контроль цілісності, цифрові підписи, хешування.
- Доступність – означає, що дані та ресурси мають бути доступними для уповноважених користувачів у потрібний момент часу. Це досягається за допомогою захисту від DDoS-атак, резервного копіювання, відмовостійких систем.

Трикутник символізує рівноцінність і взаємозалежність усіх трьох складових. Порушення хоча б одного з елементів триади ставить під загрозу всю систему безпеки. Наприклад, надмірне посилення конфіденційності може ускладнити доступність, або ж доступність без контролю цілісності – відкриває шлях до маніпуляцій з даними.

РОЗДІЛ 2
ШТУЧНИЙ ІНТЕЛЕКТ: ПОНЯТТЯ, МЕТОДИ, ІНСТРУМЕНТИ

2.1. Визначення та класифікація штучного інтелекту

Штучний інтелект — це галузь комп'ютерної науки, що вивчає способи створення систем, які можуть виконувати завдання, що потребують людського інтелекту. Серед них — розпізнавання образів, розуміння мови, навчання, логічне мислення, планування, прийняття рішень, автономні дії в середовищі тощо.

Одне з класичних визначень належить Джону Маккарті, одному з «батьків» ШІ:

Штучний інтелект — це наука та інженерія створення інтелектуальних машин, зокрема інтелектуальних комп'ютерних програм».

Європейська комісія у 2019 році визначила ШІ як системи, які відображають інтелектуальну поведінку, аналізуючи навколишнє середовище та приймаючи автономні рішення для досягнення поставленої мети.

Таким чином, штучний інтелект не обмежується лише програмуванням, а включає в себе математику, нейронауки, психологію, лінгвістику, робототехніку тощо, що дозволяє моделювати й розуміти процеси мислення [1, 2, 3, 4].

Штучний інтелект можна класифікувати за різними критеріями: за рівнем інтелекту, за функціональністю, за сферою застосування, а також за здатністю до самонавчання. У кожній із класифікацій є свої особливості та підходи, що розкривають різні грані цієї складної і динамічної галузі[6, 7].

1.За рівнем інтелекту:

Слабкий Штучний Інтелект (Narrow AI)

Це системи, які виконують конкретне завдання і не мають здатності до універсального мислення. Прикладами є голосові помічники (Siri, Alexa), системи рекомендацій (YouTube, Spotify), чат-боти у банках, навігаційні

програми. Слабкий ШІ вже сьогодні широко використовується в бізнесі, медицині, освіті та багатьох інших сферах.

Сильний Штучний Інтелект (Artificial General Intelligence, AGI)

Це гіпотетичні системи, які здатні розв'язувати будь-які інтелектуальні завдання так само добре, як і людина. Такий ШІ повинен мати свідомість, розуміння контексту, адаптивність до змін і самонавчання. На сьогоднішній день сильний ШІ ще не існує, проте науковці активно працюють над створенням таких систем, і дослідження в цьому напрямі тривають з великою відданістю.

Надінтелект або суперінтелект (Super Artificial Intelligence, Super AI)

Це ще один гіпотетичний рівень розвитку ШІ, коли інтелект машини перевершує інтелект людини в усіх галузях, включаючи науку, творчість, соціальні навички. Такий сценарій породжує як великі надії (швидкий прогрес), так і серйозні побоювання (втрата контролю над системами).

2. За функціональними можливостями:

Реактивні системи штучного інтелекту (Reactive Machines)

Ці системи не мають пам'яті, не аналізують минулі дії, а просто реагують на поточні стимули. Вони добре працюють у стабільному середовищі з чітко визначеними правилами (наприклад, комп'ютер Deep Blue, який переміг чемпіона світу в шахи).

Системи з обмеженою пам'яттю (Limited Memory)

Це більш складні системи, які можуть аналізувати деякі дані з минулого для прийняття рішень. Наприклад, автономні автомобілі використовують дані з попередніх поїздок для покращення навігації та безпеки.

Системи з теорією розуму (Theory of Mind)

Такі системи поки не реалізовані, але ідея полягає в тому, що ШІ зможе розуміти думки, емоції та наміри інших суб'єктів. Це відкриває нові можливості для взаємодії з людьми, але потребує складного моделювання поведінки.

Самосвідомі системи (Self-aware AI)

Найвищий рівень розвитку ШІ передбачає створення машин, здатних усвідомлювати своє існування, розуміти власну сутність і переживати емоції. Наразі це залишається лише теоретичною концепцією, що розглядається в рамках філософських і футуристичних досліджень[5, 6].

3. За напрямками застосування ШІ:

Штучний інтелект можна також класифікувати за сферами, у яких він застосовується:

- Аналітичний ШІ — аналізує великі обсяги даних, виявляє закономірності та тренди (застосовується у фінансах, медицині, маркетингу).
- Інтерактивний ШІ — забезпечує спілкування з людьми, наприклад, чат-боти, віртуальні асистенти.
- Автономний ШІ — самостійно приймає рішення та виконує дії без участі людини (дрони, роботи, автономні машини).
- Креативний ШІ — генерує нові ідеї, тексти, зображення, музику (технології генеративного ШІ, такі як DALL·E, ChatGPT, Midjourney).

2.2. Методи машинного та глибинного навчання

Машинне навчання (ML) та глибинне навчання (DL) — це ключові підрозділи штучного інтелекту, які дають змогу комп’ютерам навчатися на основі даних без явного програмування. Вони відіграють центральну роль у розпізнаванні образів, обробці природної мови, автономному водінні, рекомендаційних системах, кібербезпеці та інших галузях. У цій частині розглянемо основні методи машинного та глибинного навчання, їхню класифікацію, принципи роботи та застосування[9, 13].

Машинне навчання — це підхід до створення моделей, які здатні виявляти закономірності в даних та робити прогнози або класифікації на основі нової інформації. Основні категорії методів машинного навчання[9, 13]:

Навчання з учителем (Supervised Learning)

Це найбільш поширений тип машинного навчання, при якому модель навчається на основі пар «вхідні дані – правильний результат». Мета — навчитися передбачати мітку (output) для нових прикладів.

Основні алгоритми:

- Лінійна регресія — використовується для прогнозування числових значень.
- Логістична регресія — застосовується для бінарної класифікації.
- Підтримувальні вектори (SVM) — ефективні для класифікації з чітким розділенням класів.
- k-найближчих сусідів (k-NN) — прогнозує мітку на основі найближчих прикладів у просторі ознак.
- Дерева рішень та випадкові ліси (Random Forest) — популярні завдяки простоті інтерпретації та високій точності.

Застосування**:** виявлення шахрайства, діагностика хвороб, розпізнавання зображень.

Навчання без учителя (Unsupervised Learning)

У цьому підході дані не мають міток, і мета — знайти приховані структури або закономірності.

Основні алгоритми:

1. Кластеризація (наприклад, k-середніх) — групує схожі об’єкти в кластери.
2. Зниження розмірності (PCA, t-SNE) — спрощує дані для візуалізації або подальшого аналізу.
3. Асоціативні правила (Apriori, FP-growth) — знаходять залежності між подіями (наприклад, у маркетингу).

Застосування**:** сегментація клієнтів, виявлення аномалій, рекомендаційні системи.

Напівконтрольоване та самонавчання

Ці методи поєднують контрольоване та неконтрольоване навчання: для

навчання використовується невелика кількість розмічених даних і велика кількість нерозмічених. Популярні в обробці природної мови та комп’ютерному баченні.

Підкріплювальне навчання (Reinforcement Learning)

Агент взаємодіє з середовищем і отримує винагороду за правильні дії. З часом він навчається вибирати стратегію, яка максимізує довгострокову винагороду.

Ключові елементи:

- Агент — приймає рішення.

- Середовище — реагує на дії агента.

- Нагорода (reward) — сигнал успішності дій.

Алгоритми: Q-learning, Deep Q-Networks, Policy Gradient.

Застосування: робототехніка, автономне керування, ігри (наприклад, AlphaGo).

Методи глибинного навчання

Глибинне навчання — це підмножина машинного навчання, яка використовує нейронні мережі з великою кількістю шарів (глибину). Вони здатні автоматично виявляти важливі ознаки без ручного втручання.

Багатошарові перцептрони (Multilayer Perceptrons, MLP)

Це класичні глибокі нейронні мережі, які складаються з вхідного шару, кількох прихованих шарів та вихідного шару. Кожен нейрон використовує функцію активації (ReLU, Sigmoid, Tanh) для нелінійного перетворення даних.

Застосування: базові задачі класифікації та регресії.

Згорткові нейронні мережі (Convolutional Neural Networks, CNN)

CNN ефективно обробляють зображення та відео. Вони використовують згорткові фільтри для автоматичного виділення ознак (контурів, текстур, об’єктів).

Застосування: розпізнавання облич, медичні знімки, автономне керування.

Рекурентні нейронні мережі (Recurrent Neural Networks, RNN)

RNN обробляють послідовності даних, маючи пам’ять про попередні елементи. Ідеальні для задач, де порядок важливий: тексти, музика, фінансові ряди.

Покращення: LSTM (Long Short-Term Memory), GRU (Gated Recurrent Units) — вирішують проблему «забування» в довгих послідовностях.

Застосування: машинний переклад, прогнозування часу, генерація тексту.

Генеративні змагальні мережі (Generative Adversarial Networks, GAN)

Ці мережі складаються з двох моделей: генератора (створює зображення) та дискримінатора (оцінює їх правдоподібність). GAN здатні генерувати фотореалістичні зображення, нову музику, тексти.

Застосування: deepfake, доповнення даних, творчі продукти.

Трансформери (Transformers)

Найсучасніший підхід до обробки природної мови. Замість рекурентності використовують механізм уваги (attention), що дозволяє моделі одночасно враховувати всю послідовність.

Відомі архітектури: BERT, GPT, T5.

Застосування: ChatGPT, машинний переклад, автоматичне резюмування, питання-відповіді.

Порівняльна таблиця методів ML та DL

Таблиця 2.2

Метод	Потребує розмічених даних	Можливість обробки великих даних	Автоматичне виділення ознак	Вимоги до ресурсів
Логістична регресія	Так	Низька	Ні	Низькі
Random Forest	Так	Середня	Частково	Середні

Продовження таблиці 2.2

k-Means	Ні	Середня	Ні	Низькі
CNN	Так	Висока	Так	Високі
RNN/LSTM	Так	Висока	Так	Високі
GAN	Так	Висока	Так	Дуже високі
(GPT, BERT)	Так	Дуже висока	Так	Дуже високі

Джерело: розробка автора

Методи машинного та глибинного навчання є серцевиною сучасного штучного інтелекту. Машинне навчання ефективне в задачах класифікації, прогнозування й аналізу даних. Глибинне навчання, у свою чергу, дає змогу вирішувати складні завдання зображень, мовлення та текстів завдяки потужності нейронних мереж[9].

Обидва підходи постійно вдосконалюються, а їх поєднання дає змогу створювати потужні інтелектуальні системи, які змінюють наше уявлення про можливості машин.

Занурюючись глибше у методи, які стали особливо корисними для аналізу даних у сфері безпеки, варто окремо згадати про кілька з них.

Наприклад, рекурентні нейронні мережі (RNN) та їхні вдосконалені варіанти, таки як, LSTM (Long Short-Term Memory) та GPU(Gated Recurrent Units). Уявімо собі мережевий трафік або довгий лог-файл – це не просто набір окремих подій, а послідовність, де порядок має значення. Саме тут RNN з їхньою «пам’яттю», здатністю враховувати попередні дані при обробці поточних, стають незамінними. Вони можуть «читати» послідовності пакетів або записів у логах і виявляти аномальні патерни, які розгортаються у часі.

Інший важливий підхід, особливо для виявлення аномалій, коли ми не знаємо, як саме виглядає атака, - це методи кластеризації та автокодувальники. Кластеризація допомагає згрупувати схожі об’єкти. У безпеці це може бути групування «нормальних» сесій користувачів або типів мережевого трафіки. Все, що значно відрізняється від цих груп, потенційно є аномалією, яку варто

перевірити. Автокодувальники, вчаться «стискати» та потім відновлювати дані, які вони бачили під час навчання. Якщо модель погано відновлює нові дані, це означає, що вони сильно відрізняються від «норми», тобто є аномальними.

Також у безпеці часто використовуються ансамблеві методи, наприклад, Випадковий Ліс (Random Forest). Вони будують багато «слабких» моделей і голосують за остаточне рішення. Це робить їх стійкішими та точнішими, наприклад, для класифікації файлів на шкідливі/безпечні або виявлення спаму.

2.3. Інструменти реалізації ШІ в практиці

Реалізація штучного інтелекту (ШІ) у практичних застосуваннях неможлива без потужних інструментів — як програмних, так і апаратних. Вони забезпечують розробку, тренування, тестування та впровадження моделей машинного і глибинного навчання. У цьому розділі розглянемо основні платформи, мови програмування, бібліотеки, середовища та сервіси, що використовуються для побудови ШІ-систем, а також проаналізуємо їх переваги та особливості.

1. Мови програмування для ШІ

Python — найпопулярніша мова програмування у сфері ШІ завдяки своїй простоті, читабельності та великій кількості бібліотек. Вона підтримує всі основні парадигми машинного навчання, обробку даних, візуалізацію тощо.

Популярні бібліотеки Python для ШІ:

- NumPy, Pandas — обробка та аналіз даних.
- Scikit-learn — базові алгоритми ML.
- TensorFlow, PyTorch, Keras — глибинне навчання.
- OpenCV — комп’ютерне бачення.
- NLTK, SpaCy — обробка природної мови.

R — популярна в академічному середовищі для статистичного аналізу. Має бібліотеки для машинного навчання (caret, randomForest), але менш

популярна для глибинного навчання.

Java та C++ використовуються переважно в продуктивних ШІ-рішеннях із високими вимогами до швидкодії (наприклад, вбудовані системи, обробка зображень у реальному часі).

Фреймворки та бібліотеки

TensorFlow — відкрита платформа від Google для розробки та розгортання моделей глибинного навчання. Підтримує як навчання на CPU, так і на GPU/TPU. Може працювати в браузері (TensorFlow.js), на мобільних пристроях (TensorFlow Lite) та на серверах.

PyTorch — гнучкий фреймворк від Facebook, який став популярним завдяки простій інтеграції з Python і динамічним обчислювальним графам. Ідеально підходить для наукових досліджень і прототипування.

Keras — високорівнева оболонка над TensorFlow, що дозволяє швидко створювати та тестувати моделі. Підходить для початківців і прототипування невеликих проєктів.

Scikit-learn — бібліотека машинного навчання для Python, яка охоплює більшість базових алгоритмів класифікації, регресії, кластеризації, вибору ознак тощо.

Google Cloud AI

Google пропонує потужні сервіси для навчання моделей (Vertex AI), розпізнавання зображень (Vision AI), обробки мовлення, тексту, перекладу. TensorFlow інтегрований за замовчуванням.

Microsoft Azure AI

Azure надає Cognitive Services для роботи з мовою, зображеннями, знаннями, чат-ботами. Також доступні інструменти для створення моделей ML без глибоких знань програмування (Azure Machine Learning Studio).

Amazon Web Services (AWS)

AWS має платформу SageMaker для повного циклу розробки ML. Також підтримує сервіси для аналітики, розпізнавання об’єктів, перекладу, аудіоаналізу.

OpenAI API

OpenAI надає API для доступу до моделей GPT, DALL·E та інших. Це хмарний інтерфейс, який дозволяє інтегрувати ШІ у власні продукти з мінімальним кодом.

Інструменти для підготовки та візуалізації даних

- Tableau, Power BI — інтерактивна візуалізація та аналітика.
- Jupyter Notebook — інтерактивне середовище для програмування, яке підтримує візуалізацію результатів прямо в коді.
- Pandas Profiling, Seaborn, Matplotlib — аналіз та побудова графіків.

Апаратні засоби для ШІ

Високопродуктивні графічні карти (NVIDIA CUDA, RTX) є стандартом для тренування глибоких моделей.

Tensor Processing Units (TPU)

TPU — спеціалізовані чипи від Google, які забезпечують високу продуктивність при виконанні операцій TensorFlow.

Одноплатні комп’ютери

Такі пристрої, як NVIDIA Jetson, Raspberry Pi 4, дозволяють створювати вбудовані рішення зі ШІ в автономному режимі.

Інструменти реалізації штучного інтелекту — це поєднання мов програмування, бібліотек, апаратних засобів і хмарних сервісів, що дають змогу створювати й розгортати інтелектуальні системи в найрізноманітніших сферах — від медицини до фінансів, від автономного транспорту до кібербезпеки. Вибір конкретного інструменту залежить від завдань, досвіду команди, масштабів проєкту та вимог до продуктивності.

2.4. Переваги і обмеження використання ШІ в практиці

Перше – це здатність штучного інтелекту працювати з величезними обсягами даних. У сучасному світі системи безпеки генерують терабайти логів, записів трафіку, сповіщень. Людина просто фізично не може

переглянути та проаналізувати все це. Штучний інтелект робить це миттєво, знаходячи приховані зв’язки та аномалії, які залишилися б непоміченими.

Друга велика перевага – це швидкість реагування в якій штучний інтелект може виявляти загрозу і, що важливо, приймати рішення про реакцію значно швидше, ніж людина. В умовах кібератаки, коли кожна секунда на рахунку, це може стати вирішальним фактором для мінімізації збитків.

Також штучний інтелект здатний виявляти нові та невідомі загрози. Традиційні системи безпеки часто працюють за принципом «чорного списку» - шукають те, про що вже знають (наприклад, конкретний підпис вірусу). ШІ ж може аналізувати поведінку і виявляти аномалії – тобто дії, які не відповідають «нормі», навіть якщо вони є частиною абсолютно нової атаки, що робить захист більш проактивним.

ШІ здатен до навчання та адаптації завдяки системам безпеки, інтелект може навчатися на нових даних про атаки або зміни в нормальній поведінці системи і з часом ставати ефективнішими, адаптуючись до тактик зловмисників, що постійно еволюціонують.

І нарешті, штучний інтелект може автоматизувати рутинні та трудомісткі задачі, в яких аналітики безпеки часто витрачають багато часу на перегляд однотипних сповіщень або збір інформації про інцидент. Штучний інтелект бере на себе всю «чорнову» роботу, звільняючи людей для виконання більш складних, творчих та стратегічних завдань.

Але, як і будь-яка потужна технологія, штучний інтелект має свої обмеження та виклики, які потрібно враховувати при роботі з ним:

Найбільша проблема – це якість та кількість даних для навчання. Він вчиться на даних. Якщо дані неповні, містять помилки або не відображають усіх можливих ситуацій (наприклад, мало прикладів рідкісних атак або, навпаки, не враховано специфічну «нормальну» активність конкретної організації), модель штучного інтелекту працювати погано. Особливо гостро стоїть проблема дисбалансу класів: нормальної активності в тисячі разів більше, ніж реальних атак. Навчити модель ефективно виявляти рідкісні події

– складне завдання.

Серйозний виклик – це атакувальний ШІ (Adversarial AI). Як ми вже згадували, зловмисники можуть цілеспрямовано створювати дані, які виглядають майже нормально для людини чи традиційних систем, але змушують модель ШІ зробити помилковий висновок (наприклад, пропустити вірус). Це постійні «перегони озброєнь» між захисниками, що використовують штучний інтелект, та зловмисниками, що вчаться його обманювати.

Ще одна складність – проблема пояснюваності. Висловлюється це тим, що глибокі нейронні мережі, працюють як «чорний ящик». Вони дають відповідь, що це атака, але не можуть надати чітке пояснення, чому саме вона відбулась. У сфері безпеки, де потрібні чіткі докази для розслідування інциденту або представлення їх у суді, це може бути серйозною перешкодою. Аналітик має чітко розуміти логіку рішення, щоб робити висновок, чи довіряти системі та ефективно реагувати, чи ігнорувати.

Використання ШІ потребує значних обчислювальних ресурсів, де навчання складних моделей, особливо глибокого навчання, потребує потужного «заліза» (графічних процесорів) та часу, що може бути дорого і недоступно для невеликих компаній.

Також не варто забувати про етичні питання та упередженість. Якщо дані, на яких навчається модель штучного інтелекту, містять приховані упередження (історично системи безпеки спрацьовують частіше на окремих користувачів чи типи активності), модель може успадкувати ці упередження, призводячи до несправедливих або неефективних рішень.

Враховуючи ці переваги та обмеження, стає зрозуміло, що штучний інтелект в інформаційній безпеці – це потужний інструмент, але він вимагає грамотного впровадження, постійного моніторингу, актуалізації та, що найважливіше, роботи в тандемі з досвідченими фахівцями з безпеки. Штучний інтелект допомагає їм, автоматизує процеси та виявляє неочевидне, але остаточне рішення та відповідальність часто залишаються за людиною.

Розглянемо виклики використання ШІ в інформаційній безпеці за

допомогою Таблиці 2.4 :

Таблиця 2.4

Ключові виклики ШІ

Виклик	**Опис**	**Наслідки для ІБ**	**Шляхи подолання**
Якість та дисбаланс даних	Необхідність великих, чистих даних	Пропуск атак та помилкові спрацьовання	Збір якісних даних
Атакувальний ШІ	Зловмисники обманюють моделі ШІ шляхом модифікації даних	Обхід систем виявлення, компрометація моделей	Стійкіші моделі
Проблема пояснюваності	Складність інтерпретації рішень «чорних скриньок»	Ускладнення розслідування інцидентів	Візуалізація важливості ознак
Обчислювальні ресурси	Високі вимоги до потужності для навчання та розгортання складних моделей	Обмеження для малих організацій та високі витрати на інфраструктуру	Оптимізація моделей, використання хмарних сервісів
Постійна актуалізація	Необхідність регулярного перенавчення на нових даних загроз	Зниження ефективності моделі проти нових атак	Автоматизовані конвеєри перенавчання моделей

Джерело: розробка автора

Таблиця 2.4 узагальнює ключові виклики, з якими ми стикаємося при використанні штучного інтелекту у сфері інформаційної безпеки. У ній ми бачимо не просто перелік проблем, а й короткий опис кожного з них, пояснення, до яких саме наслідків для інформаційної безпеки вони можуть призвести (чому саме неякісні дані можуть змусити систему пропускати реальні атаки), а також згадку про можливі шляхи подолання.

Ця таблиця допомагає наочно побачити, що хоча штучний інтелект є потужним інструментом, його впровадження вимагає уваги до деталей і постійного вдосконалення та врахування специфічних «слабкостей» самих ШІ-систем.

РОЗДІЛ 3
СУЧАСНІ ПІДХОДИ ДО ЗАСТОСУВАННЯ ШІ В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

3.1. Виявлення аномалій і атак за допомогою ШІ

Із зростанням складності інформаційних систем і збільшенням обсягу кіберзагроз традиційні методи захисту даних втрачають ефективність. У цьому контексті штучний інтелект (ШІ) набуває ключової ролі у виявленні аномалій і кіберзагроз, здатний автоматично виявляти, класифікувати та реагувати на потенційно небезпечну активність у режимі реального часу.

Виявлення аномалій — це процес ідентифікації подій або патернів, які відхиляються від очікуваної поведінки. В інформаційній безпеці аномалії можуть свідчити про вторгнення, витік даних, шкідливе програмне забезпечення або інші форми атак.

Роль ШІ у виявленні аномалій

ШІ дозволяє автоматично аналізувати великі обсяги даних, виявляти нетипові дії, формувати моделі нормальної поведінки та оперативно реагувати на відхилення. Особливо корисним є машинне та глибинне навчання для виявлення прихованих або нових атак, які важко розпізнати традиційними методами.

Методи машинного навчання для виявлення аномалій

- Наглядове навчання (Supervised learning): використовується, коли є мічені дані (наприклад, атакуючі та безпечні пакети). Моделі навчаються розрізняти нормальну та шкідливу активність.
- Ненаглядове навчання (Unsupervised learning): актуальне при відсутності мічених даних. Наприклад, кластеризація (k-means), методи зниження розмірності (PCA) чи автоенкодери дозволяють виявити аномалії як віддалені об’єкти.
- Напівнаглядове навчання (Semi-supervised): використовує обмежену

кількість мічених даних та велику кількість немічених для побудови моделей нормальної поведінки.

Глибинне навчання у виявленні атак

Глибинне навчання дозволяє виявляти складні шаблони в багатовимірних даних. Зокрема, використовуються:

- Рекурентні нейронні мережі (RNN) — для аналізу часових рядів, поведінки користувача.
- Конволюційні нейронні мережі (CNN) — для аналізу мережевого трафіку у вигляді зображень.
- Autoencoders — для реконструкції нормальної поведінки та виявлення аномалій через високі помилки реконструкції.

Типи атак, які можна виявити за допомогою ШІ

- Атаки типу «відмова в обслуговуванні» (DDoS)
- Аномальна поведінка користувачів (наприклад, внутрішні інсайдери)
- Вторгнення в мережу (Intrusion Detection)
- Шкідливе ПЗ (Malware Detection)
- Фішинг, соціальна інженерія
- Ботнети, сканування портів

Наведемо такі приклади систем на основі ШІ

- IBM QRadar Advisor with Watson — використовує NLP і машинне навчання для виявлення та розслідування загроз.
- Darktrace — платформа з елементами глибинного навчання для створення «цифрового імунітету» в мережі.
- Azure Sentinel — SIEM-система з вбудованими аналітичними модулями на базі ML.

7. Переваги застосування ШІ для кібербезпеки

- Можливість обробки великих обсягів даних у реальному часі.
- Виявлення раніше невідомих (zero-day) загроз.
- Зниження рівня помилкових спрацювань у порівнянні з традиційними правилами.

- Адаптація до нових атак шляхом повторного навчання моделі.

Виклики та обмеження

- Необхідність якісного навчального набору даних.
- Вразливість до атак на саму модель (наприклад, adversarial attacks).
- Проблема інтерпретації — моделі можуть бути «чорними скриньками».
- Потреба в обчислювальних ресурсах для тренування складних моделей.

Застосування ШІ у виявленні аномалій і атак забезпечує новий рівень ефективності в сфері інформаційної безпеки. Інтелектуальні системи здатні не лише ідентифікувати відомі загрози, а й виявляти нові, адаптуватися до змін поведінки атакувальників та автоматизувати реагування. Втім, для максимальної ефективності потрібна комбінація технологій ШІ, людського аналізу та глибокої інтеграції з іншими системами безпеки.

Щоб краще зрозуміти, як Штучний інтелект «загрожує», давайте детальніше розглянемо кілька типових сценаріїв:

1. Виявлення мережевої інвазії (NIDS/HID) за допомогою AI: Зобразіть постійний потік інформації, що подорожує через мережу вашої компанії. Системи виявлення вторгнень (IDS) вивчають мережевий трафік або дії на кожному комп'ютері. AI виступає обережним спостерігачем у цій ситуації. Він має можливість вивчати окремі пакети даних, а також весь сеанс або ряд подій. Наприклад, рецидивуючі нейронні мережі (RNN) або довгострокові мережі пам'яті (LSTM), про які ми обговорювали в розділі 2, Excel при вивченні порядок пакетів даних у мережевих з'єднаннях. Вони можуть помітити непарні шаблони або ряд дій, які можуть запропонувати комусь перевірити наявність відкритих мережевих портів, намагається відгадати паролі або запустити атаку DOS. AI вивчає статистичні особливості трафіку, включаючи кількість даних, кількість з'єднань до певного сервера та географічне розташування IP -адрес. Раптом із сервера, який завжди спілкувався лише з внутрішньою мережею, гігабайт даних про якийсь зовнішній IP,

AI, який навчився розпізнавати "норму" для цього сервера (можливо, використання кластеризації або методи виявлення аномалій) миттєво посилається на нього як підозрілу діяльність.

2. Аналіз поведінки користувачів та сутності (UBA): У цьому контексті ШІ звертає увагу на дії користувачів, серверів чи програм. Системи UBA створюють стандартні моделі поведінки для кожного користувача чи пристрою, а не визначають конкретні атаки.

3. Виявлення шкідливого програмного забезпечення (виявлення шкідливих програм):

Штучний інтелект перетворив методи, що використовуються для виявлення вірусів та небезпечного програмного забезпечення. Замість того, щоб просто відповідати файлу проти відомих шаблонів вірусів, системи AI вивчають власну структуру та код (статичний аналіз) та спостерігають за його діями під час виконання у безпечному налаштуванні, відомі як "пісочниця" (динамічний аналіз SHI, які були навчені на численних прикладах як шкідливих, так і безпечних програм, можуть виявити незначні показники та шаблони типового класу, навіть при цьому, причому до цього, що є новим вірусом. Сценарій, такі як методи глибокого навчання, які можуть визначити ключові особливості у великому наборі даних без ручного втручання.

4. Виявлення фішингу та спаму:

Електронна пошта продовжує бути часто використовуваним методом кібер -атак. AI допомагає сортувати електронні листи, шукати показники шахрайства чи спаму. Інструменти NLP перевіряють текст листа на будь -які незвичайні фрази, ознаки емоційного стресу та термінові вимоги до приватних даних:

1. Оглянув заголовки листа.

2. Перевірив наявність посилань та те, як вони виглядають.

3. Зібрав деталі про людину, яка надіслала лист. Здатність AI адаптуватися до нових загроз має вирішальне значення в боротьбі з

кіберзлочинністю.

Взагалі використання ШІ в цих та багатьох інших проблемах виявлення дозволяє переходити від реактивного "латування отворів" після інциденту до більш ініціативної "допомоги на дим" до спалаху пожежі.

Приклади застосування ШІ у різних задачах інформаційної безпеки розглянуто у Таблиці 3.1 :

Таблиця 3.1

Застосування ШІ в інформаційній безпеці

Задача ІБ	**Описання роботи ШІ**	**Приклад використовуваних даних**	**ШІ-методи (приклади)**
Виявлення мережевих вторгнень	Аналіз трафіку для пошуку аномальної активності	Пакети, потоки, метадані з мережевих пристроїв	LSTM, Кластеризація, Anomaly Detection, Класифікатори
Аналіз поведінки (UEBA)	Моделювання нормальної поведінки та виявлення відхилень	Логи систем, додатків, доступу до ресурсів	Кластеризація, Часові ряди, Статистичні моделі
Виявлення шкідливого ПЗ	Аналіз файлів/процесів на наявність шкідливих ознак	Байт-код, поведінка у пісочниці, хеші файлів	Класифікатори (SVM, RF, NN), Аналіз ознак
Виявлення фішингу/спаму	Аналіз вмісту та метаданих електронних листів	Текст листа, заголовки, URL, вкладення	NLP (класифікація тексту), Класифікатори

Продовження таблиці 3.1

Аналіз загрозної розвідки (TI)	Обробка великих обсягів даних для виявлення нових загроз	Звіти про інциденти, дані сканування, інформація з відкритих джерел	Кластеризація, NLP, Графові моделі
Оцінка вразливостей	Допомога в пошуку та пріоритезації слабких місць	Результати сканування, дані конфігурації	Класифікатори, Rule Mining
Автоматизоване реагування (у SOAR)	Прийняття рішень, збагачення даних, автоматизація дій	Дані інцидентів, бази загроз, телеметрія систем	Системи прийняття рішень на базі ML, Класифікатори ризиків

Джерело: [31]

Ця таблиця дає змогу наочно побачити, наскільки широким є поле застосування ШІ в інформаційній безпеці. Для кожної ключової задачі ми бачимо, що саме ШІ допомагає робити, які типи даних він зазвичай аналізує, та які з методів, описаних у Розділі 2, найчастіше для цього використовуються.

3.2. Автоматизовані системи реагування

Сучасні інформаційні системи щоденно стикаються з численними загрозами кібербезпеки. Ручне управління інцидентами не завжди є ефективним через велику кількість подій, обмежені ресурси аналітиків та необхідність миттєвої реакції. У відповідь на ці виклики з’явилися автоматизовані системи реагування, які дозволяють забезпечити швидке, точне та ефективне

реагування на інциденти безпеки.

Автоматизовані системи реагування — це сукупність інструментів та процесів, що дозволяють автоматично здійснювати дії з реагування на кіберінциденти без участі людини або з мінімальним її втручанням. Вони реалізуються як частина більш широких платформ кіберзахисту, таких як SIEM (Security Information and Event Management), SOAR (Security Orchestration, Automation and Response) та XDR (Extended Detection and Response).

Основні компоненти систем:

До основних елементів автоматизованих систем реагування належать:

- Збір і моніторинг подій: автоматизоване відстеження логів, трафіку, поведінки користувачів, мережевої активності.
- Аналіз загроз: класифікація подій за критичністю, зіставлення з базами даних про загрози.- Прийняття рішень: на основі заданих сценаріїв або алгоритмів штучного інтелекту система обирає оптимальну відповідь.
- Виконання дій: ізоляція пристрою, блокування IP-адрес, зміна політик доступу, інформування співробітників безпеки.3. Приклади автоматичних реакцій

Автоматизовані системи можуть виконувати низку заходів у відповідь на інциденти, зокрема:

1. Ізоляцію заражених пристроїв від мережі.
2. Блокування підозрілих облікових записів.
3. Застосування нових правил фаєрвола.
4. Створення заявки в системі обліку інцидентів.
5. Надсилання повідомлень відповідальним особам.

У сучасному світі кібербезпеки важливим аспектом є не лише своєчасне виявлення загроз, а й ефективна реакція на них. Оскільки кількість і складність кіберінцидентів зростають, стає необхідним впровадження автоматизованих та інтегрованих рішень для швидкого реагування та мінімізації ризиків.

Одним із таких рішень є використання SOAR-систем, що дозволяють організаціям значно покращити ефективність процесів реагування на інциденти. SOAR-системи об'єднують різні інструменти безпеки в єдину платформу, що дозволяє автоматизувати багато рутинних процесів, таких як аналіз загроз, коригування налаштувань безпеки та виконання заходів щодо нейтралізації атак. Вони також забезпечують швидку координацію між різними відділами та службами, що дозволяє зменшити час на прийняття рішень і мінімізувати наслідки інцидентів.

Впровадження таких рішень дає змогу знижувати навантаження на команди безпеки, дозволяючи їм зосередитись на більш складних задачах, а також підвищує загальний рівень захищеності організації. У свою чергу, автоматизовані системи дозволяють отримувати більш точні та своєчасні аналітичні звіти, що полегшує моніторинг інцидентів, виявлення вразливостей та поліпшення стратегій реагування. Тому застосування SOAR-систем стає невід'ємною частиною сучасної стратегії кібербезпеки у великих та середніх організаціях, які прагнуть ефективно захистити свої дані і ресурси.

SOAR (Security Orchestration, Automation and Response) — це комплексні платформи, що поєднують автоматизацію, координацію дій та аналітику в сфері кібербезпеки. Вони дозволяють інтегрувати кілька інструментів кіберзахисту в єдину централізовану систему, забезпечуючи ефективне управління інцидентами, швидке реагування на загрози та оптимізацію процесів безпеки.

SOAR-системи автоматизують рутинні завдання, такі як збирання даних про загрози, валідацію інцидентів, оповіщення зацікавлених сторін, запуск скриптів реагування та виконання дій за наперед визначеними сценаріями. Це значно знижує навантаження на аналітиків SOC (Security Operations Center) і скорочує час реагування на інциденти.

Завдяки SOAR організації можуть покращити видимість подій у мережі, зменшити кількість помилкових спрацювань.

Використання ШІ в автоматизованому реагуванні

Штучний інтелект дозволяє створювати адаптивні сценарії реагування, які можуть враховувати контекст ситуації. Наприклад, системи можуть:

1. Визначати, чи є поведінка користувача типовою.
2. Аналізувати загрози за допомогою класифікаторів.
3. Прогнозувати подальші дії атакувальника.
4. Самостійно навчатись на історичних даних інцидентів.

Це значно підвищує ефективність реагування на нові, раніше невідомі атаки.

Переваги автоматизації:

1. Швидкість реагування. Реакція відбувається миттєво після виявлення загрози.
2. Зменшення людського фактору. Виключаються помилки, пов’язані з втомою або неуважністю.
3. Економія ресурсів. Автоматизація зменшує навантаження на команди безпеки.
4. Масштабованість. Системи можуть обробляти тисячі подій за секунду.
5. Безперервність. Працюють 24/7 без втручання оператора.

Ризики та обмеження:

Попри переваги, автоматизовані системи мають певні виклики:

1. Хибні спрацювання: неправильна класифікація подій може призвести до блокування легітимного трафіку.
2. Складність налаштування: потребують висококваліфікованого персоналу.
3. Безпека самої системи: вона також може стати ціллю для атак.
4. Висока вартість впровадження: особливо для малих компаній.

Перспективи розвитку:

У найближчі роки очікується ще глибша інтеграція ШІ та глибинного навчання в системи реагування, що дозволить:

1. Автоматично передбачати майбутні атаки.
2. Створювати самонавчальні моделі реагування.
3. Взаємодіяти з іншими IT-системами для координації безпеки.

Автоматизовані системи реагування стали ключовим елементом сучасної кібербезпеки. Вони дозволяють організаціям оперативно захищатися від загроз, зменшувати втрати і підвищувати загальну стійкість IT-інфраструктури. Успішне впровадження таких рішень потребує грамотного проєктування, постійного оновлення сценаріїв реагування та ефективної взаємодії з аналітиками безпеки.

Для того, щоб автоматизована реакція була не просто виконанням жорстко встановлених команд, але й справді інтелектуальними, системи повинні мати можливість приймати рішення, враховуючи зміну контексту атаки. Саме тут штучна розвідка відіграє ключову роль, особливо на сучасних платформах Soar. Soar System діє як лідер групи з безпеки, керуючи ними разом. Він отримує інформацію від різних інструментів (SIEM, IDS/IPS, антивірусів), організовує свою взаємодію та запускає ігрові книги - попередньо визначені сценарії для конкретних типів інцидентів. AI інтегрується в ці відтворення на кількох рівнях: Коли система помічає щось підозріле, AI може потім оцінити, наскільки серйозна загроза. Наприклад, чи ця нерегулярність є серйозною загрозою, яка потребує відразу сервера, чи це лише незначна проблема, яку можна виправити та повідомляти аналітиком? CI-Модель, навчений історичними даними про інциденти та їх наслідки, може дати таку оцінку ризику, дозволяючи системі SOAR автоматично вибирати найбільш адекватне відтворення відповідей. Щоб забезпечити аналітик безпеки або автоматизовану систему може прийняти правильне рішення, важливо мати повну інформацію про інцидент. AI може впорядкувати завдання збору та вивчення додаткових даних: він може автоматично перевіряти підозрілі IP -адреси в базах даних про загрозу, сканувати файли для вірусів за допомогою декількох двигунів та визначити потенційно порушені

облікові записи користувачів. Це збагачення даних, яким керує AI, значно прискорює процес розслідування та реагування.

Системи AI з вдосконаленими можливостями, особливо тими, що використовують підкріплення, розроблені для прогнозування майбутніх кроків зловмисника, аналізуючи їх сучасну поведінку та минулі схеми атаки. Система вдосконалюється, аналізуючи результати своїх автоматичних відповідей, з'ясовуючи, що рухається найкраще, найкраще спрацювало проти конкретних загроз, і відповідно коригуючи свої майбутні дії. Це крок до створення систем реагування на самостійність, які можуть покращити їх стратегію захисту з часом. AI перетворює основні платформи з просто дотримання сценаріїв у більш пристосовані та розумні системи. Ці системи можуть діяти швидко і, певною мірою, зрозуміти контекст нападу та відповідно коригувати їх відповіді.

Таблиця 3.2

Основні дії системи та їх покращення

Дія реагування	**Опис**	**Дія для покращення**
Блокування підозрілої IP-адреси	Автоматичне додавання IP до "чорного списку" на фаєрволі	ШІ підтверджує з високою вірогідністю, що цей IP дійсно є джерелом атаки (на основі аналізу трафіку, репутації тощо)
Ізоляція зараженого пристрою	Відключення комп'ютера або сервера від мережі	ШІ ідентифікує пристрій як скомпрометований на основі аналізу його аномальної поведінки

Продовження таблиці 3.2

Запит додаткової аутентифікації	Вимога повторного введення пароля або 2FA при підозрілому вході	ШІ виявляє аномалію у спробі входу (незвичний час, локація, пристрій) та ініціює перевірку
Автоматичне закриття порту/сервісу	Блокування доступу до певного порту або мережевого сервісу	ШІ визначає, що атака використовує саме цей порт/сервіс як вектор вторгнення
Збір додаткової інформації	Автоматичний пошук даних про індикатор компрометації (IoC)	ШІ аналізує контекст інциденту та автоматично збирає дані з різних джерел (бази загроз, VirusTotal тощо)
Пріоритезація сповіщень	Сортування та ранжування сповіщень для уваги аналітика	ШІ оцінює реальний ризик та потенційний вплив інциденту, допомагаючи аналітику зосередитись на найважливішому
Створення/оновлення тікета інциденту	Автоматичне створення запису в системі обліку інцидентів	ШІ може автоматично додати до тікета збагачену інформацію та попередню оцінку ризику

Джерело: розробка автора

Таблиця 3.2 ілюструє, що системи, керовані комп'ютером, можуть проводити різні заходи безпеки. Коли AI поєднується з цими процесами, система не працює просто автоматично. Натомість це робить кращий вибір після ретельного вивчення ситуації за допомогою розумних алгоритмів. Це покращує точність відповідей і знижує виникнення неправильної поведінки.

Приклади використання у відомих продуктах

Смартфони (Google Assistant, Siri, Alexa)

Однією з найбільш поширених реалізацій ШІ є віртуальні асистенти, такі як Google Assistant, Siri від Apple та Alexa від Amazon. Ці системи активно використовують алгоритми машинного навчання для взаємодії з користувачами за допомогою голосових команд.

- Функції: Віртуальні асистенти здатні виконувати різноманітні завдання: від надання погодних прогнозів до керування розумними пристроями в будинку. Завдяки ШІ вони можуть розпізнавати природну мову, аналізувати запити користувача та адаптуватися до індивідуальних переваг.

- ШІ-методи: Використовуються методи обробки природної мови (NLP) для розуміння голосових команд і відповіді на них. Крім того, ШІ допомагає в прогнозуванні потреб користувача, базуючись на його історії взаємодії з пристроєм.

Рекомендаційні системи (Netflix, Amazon, YouTube)

Рекомендаційні системи є ще одним потужним інструментом, що використовує ШІ для персоналізації досвіду користувачів. Вони використовуються у таких продуктах, як Netflix, Amazon та YouTube для покращення пропозицій та рекомендацій.

- Функції: Netflix і YouTube використовують ШІ для аналізу поведінки користувачів і пропонують персоналізовані рекомендації щодо фільмів, серіалів і відео на основі їхніх попередніх переглядів. Amazon пропонує товари, які користувач може захотіти придбати, спираючись на історію покупок і переглядів.

- ШІ-методи: Рекомендаційні системи працюють на основі алгоритмів

колаборативної фільтрації, де аналізуються подібності між користувачами або продуктами, а також контентної фільтрації, що аналізує характеристики самого контенту (фільмів, товарів тощо).

Автономні транспортні засоби (Tesla, Waymo)

Одним з найбільш інноваційних і перспективних напрямків застосування ШІ є розвиток автономних автомобілів. Такі компанії, як Tesla і Waymo (підрозділ Google), використовують технології ШІ для створення автономних транспортних засобів.

- Функції: Автономні автомобілі використовують сенсори (камери, радар, Лідар) для сприйняття навколишнього середовища і машинне навчання для прийняття рішень під час руху. Це дозволяє їм уникати перешкод, дотримуватися правил дорожнього руху і навіть виконувати складні маневри.

- ШІ-методи: В основі таких систем лежать глибокі нейронні мережі, які використовуються для розпізнавання об'єктів, прогнозування руху інших транспортних засобів і адаптації до різних дорожніх умов. Також застосовуються алгоритми reinforcement learning, що дозволяють автомобілю «навчатися» на практиці, покращуючи свої навички водіння.

Програмне забезпечення для медичних досліджень та діагностики (IBM Watson Health), ші активно використовується у медичних технологіях для діагностики захворювань та надання медичних рекомендацій. Одним з таких прикладів є IBM Watson Health, який використовує ШІ для допомоги в медичних дослідженнях і лікуванні:

- Функції: Watson Health здатний аналізувати медичні зображення, такі як рентгенівські знімки та МРТ, а також працювати з великими обсягами медичних даних для виявлення захворювань та прогнозування результатів лікування.

- ШІ-методи: В основі Watson лежать глибокі нейронні мережі для розпізнавання патернів у медичних зображеннях, а також обробка природної мови для аналізу текстової інформації з медичних записів.

Фінансові послуги (Ant Financial, Revolut)

ШІ також знаходить широке застосування в галузі фінансів, особливо у таких компаніях, як Ant Financial (платіжна система Alipay) і Revolut. Ці компанії використовують ШІ для поліпшення фінансових послуг та забезпечення безпеки транзакцій.

- Функції: ШІ допомагає у виявленні шахрайства, автоматизації кредитування, управлінні ризиками та наданні персоналізованих фінансових консультацій.

- ШІ-методи: Використовуються алгоритми машинного навчання для прогнозування фінансових тенденцій, виявлення аномальних транзакцій і автоматичного аналізу даних для прийняття рішень про кредитування.

Розумні будинки та Інтернет речей (Amazon Echo, Google Nest)

ШІ використовується в пристроях для розумного дому, таких як Amazon Echo та Google Nest. Вони використовують технології ШІ для автоматизації управління домашніми системами:

- Функції: Пристрої можуть контролювати освітлення, температуру, безпеку, а також взаємодіяти з іншими розумними пристроями. Вони можуть також навчатися і адаптуватися до режимів життя користувачів, створюючи комфортні умови.

- ШІ-методи: Основні методи — це обробка природної мови для голосових команд і машинне навчання для прогнозування потреб користувачів на основі їхньої поведінки.

Ці модулі можуть автоматично виявляти аномалії та потенційні загрози, значно скорочуючи час та зусилля, необхідні для ручного аналізу. Наприклад, такі елементи, як Splunk Enterprise Security або Microsoft Azure Sentinel, використовують машинне навчання для автоматичного зв’язку подій з різних джерел. AI допомагає виявити дивні зв’язки між подіями, які здаються не пов'язаними, що насправді може бути частинами однієї витонченої атаки, яку людина може не помітити серед величезної кількості журналів. Вони також використовують алгоритми для виявлення аномалій для пошуку нетипової

активності. Інструменти виявлення та реагування на кінцеву точку (EDR), які встановлюються на комп'ютерах та серверах користувачів, використовують AI, щоб помітити загрози прямо на пристрої. Провідні компанії, такі як Crowdstrike або SentineLone, використовують машинне навчання для моніторингу та аналізу дій та процесів, як вони відбуваються. Вони можуть розпізнати шкідливу діяльність (наприклад, спроба зашифрувати файли, як у атаці викупу або спроби несанкціонованого доступу до пам'яті), на основі поведінки, а не лише підписи вірусів. Brandmauers нового покоління (NGFW - Наступний брандмауер -генерація) з Palo Alto Networks або Fortinet Company отримують "розумніші" завдяки AI. Вони використовують методи машинного навчання для ретельного вивчення мережевих даних, виявлення прихованих небезпек у зашифрованих даних (після розшифровки) та класифікують програми та користувачів для виконання заходів безпеки. AI допомагає їм швидше адаптуватися до нових типів загроз, що поширюються через мережу. Штучний інтелект допомагає їм швидко пристосуватися до нових мережевих загроз. Запрошені інструменти, такі як Cortex XSOAR від Palo Alto або IBM Resilient Використовуйте AI, щоб допомогти автоматизувати процес реагування на інциденти безпеки. Як ми вже обговорювали, AI може допомогти Soar System приймати рішення щодо необхідних дій (наприклад, ізолювати пристрій, заблокувати користувача), оцінити ризик інциденту та автоматично збирати додаткову інформацію для аналітика безпеки. Також важливо виділити унікальні рішення, пропоновані UBA (аналітика поведінки користувачів та сутності), які сильно залежать від ШІ, щоб вивчити, як діють користувачі та системи, спрямовані на те, щоб виявити внутрішні ризики або зламані акаунти.

Таблиця 3.3

Використання ШІ у комерційних продуктах

Продукт / Тип рішення (Приклад Компанії)	**Основне призначення**	**Як використовується ШІ (приклад функції/задачі)**	**Типові ШІ-методи (приклади)**
SIEM (Splunk ES, Azure Sentinel)	Збір, агрегація та аналіз логів і подій безпеки	Кореляція подій, виявлення аномалій у логах, приорітезація сповіщень	ML (кластеризація, класифікація), Anomaly Detection
EDR (CrowdStrike, SentinelOne)	Виявлення та реагування на загрози на кінцевих точках	Аналіз поведінки процесів та файлів, виявлення Malware без сигнатур, ідентифікація шкідливої активності	ML (поведінковий аналіз), Класифікація
NGFW (Palo Alto Networks, Fortinet)	Фільтрація мережевого трафіку, контроль додатків	Виявлення нових загроз у трафіку, класифікація додатків, аналіз зашифрованого трафіку на наявність	ML (класифікація трафіку, Anomaly Detection)

Продовження таблиці 3.3

SOAR (Cortex XSOAR, IBM Resilient)	Оркестрація, автоматизація та реагування на інциденти	Оцінка ризику інцидентів, автоматичний збір даних про загрози, прийняття рішень у плейбуках	ML (класифікація ризиків), Аналіз даних
UEBA (Спеціалізовані рішення)	Аналіз поведінки користувачів та сутностей	Побудова профілів нормальної поведінки, виявлення відхилень (інсайдери, зламані облікові)	ML (кластеризація, Anomaly Detection, часові ряди)
Рішення для захисту пошти (напр., в M365)	Фільтрація спаму та фішингу	Аналіз тексту, заголовків, посилань та вкладень листів для ідентифікації шахрайства	NLP, Класифікація

Джерело: розробка автора

Ця таблиця демонструє приклади основних рішень у сфері кібербезпеки та їхнє застосування ШІ-технологій для підвищення ефективності захисту.

Схема, що показує, як різні системи безпеки, що використовують ШІ,

можуть взаємодіяти представлена на Рисунку 3.3. :

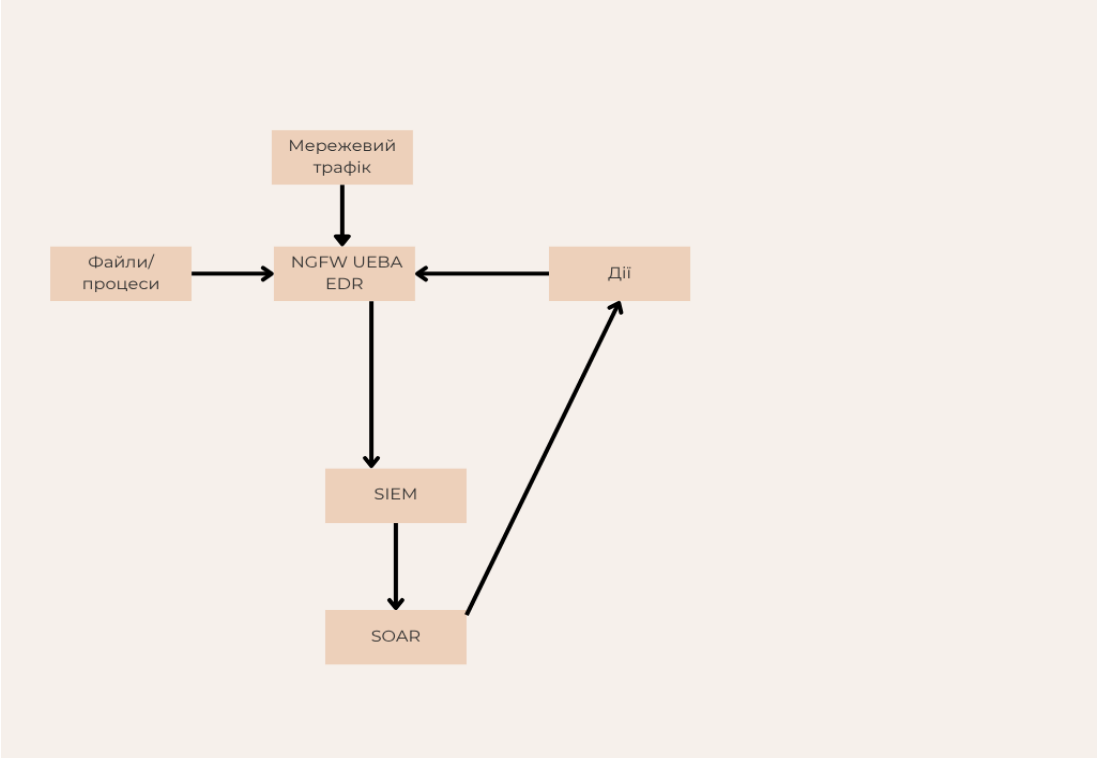

Рис. 3.3. Блок-схема багаторівневого трафіку

Така схема на рисунку дуже добре візуалізує ідею багаторівневого захисту, де різні системи з інтелектуальними можливостями співпрацюють, передаючи дані від первинного аналізу до централізованої платформи і далі до автоматизованого реагування.

ВИСНОВКИ

У процесі дослідження теми "Штучний інтелект і його застосування в практиці" було вивчено широке коло питань, що стосуються визначення, класифікації, методів, інструментів та реальних прикладів використання ШІ в різних сферах. На основі цього аналізу можна зробити кілька важливих висновків:

Штучний інтелект як потужний інструмент трансформації сучасних технологій. ШІ вже став невід'ємною частиною багатьох сучасних продуктів та сервісів. Він дозволяє значно покращити ефективність і продуктивність у таких сферах, як фінанси, охорона здоров'я, транспорт, електронна комерція та багато інших.

Методи машинного навчання та глибинного навчання. Системи на основі ШІ активно використовують методи машинного навчання та глибинного навчання для розпізнавання патернів у великих обсягах даних, прогнозування майбутніх подій та автоматизації процесів. Використання нейронних мереж, алгоритмів класифікації, регресії та reinforcement learning дає можливість розв’язувати складні завдання, які раніше були неможливі або занадто трудомісткі для традиційних технологій.

Інструменти реалізації ШІ в практиці. Для реалізації ШІ в практиці використовуються різноманітні інструменти, такі як TensorFlow, PyTorch, Keras, Scikit-learn, які дозволяють ефективно будувати і тестувати моделі для різних задач. Програмні платформи, розроблені великими компаніями, дозволяють масштабувати використання ШІ для різних бізнес-потреб і спрощують інтеграцію в існуючі системи.

Виявлення аномалій та атак. Використання ШІ для виявлення аномалій та атак є одним із важливих аспектів забезпечення інформаційної безпеки. За допомогою алгоритмів машинного навчання можна автоматично виявляти несанкціоновані дії в системах, знижувати ризики витоків інформації та атак на інфраструктуру.

Автоматизовані системи реагування в яких ші дозволяє автоматизувати процеси реагування на інциденти безпеки, що значно підвищує швидкість та точність реагування на загрози. Це дозволяє зменшити людський фактор та оперативно виявляти й нейтралізувати потенційні загрози для систем.

Реальні приклади використання ШІ в продуктах. Багато великих компаній вже активно використовують ШІ в своїх продуктах, таких як Google Assistant, Amazon Alexa, Tesla Autopilot, IBM Watson Health. ШІ надає можливість створювати персоналізовані рішення для користувачів, покращувати досвід взаємодії з продуктами та автоматизувати процеси для зручності та безпеки.

Перспективи розвитку та застосування ШІ. Штучний інтелект продовжує розвиватися, і в майбутньому можна очікувати появу ще більш ефективних та інноваційних рішень, що зможуть змінити підходи до роботи в різних галузях. Прогнози щодо розвитку ШІ показують, що його вплив на бізнес і суспільство лише зростатиме.

Етичні та соціальні аспекти. Разом з розвитком ШІ виникають питання етики та соціальних наслідків. Важливо розглядати питання прозорості алгоритмів, захисту персональних даних і створення справедливих умов для використання технологій ШІ. Рішення цих проблем буде необхідним для забезпечення довіри до таких систем та мінімізації ризиків для суспільства.

Таким чином, штучний інтелект сьогодні є однією з найбільш важливих технологій, що активно трансформує не тільки бізнес-середовище, а й всі сфери життя. Впровадження та використання ШІ відкриває нові можливості для поліпшення ефективності, безпеки та персоналізації продуктів і послуг, водночас ставлячи перед нами нові виклики щодо етики, безпеки і соціальних аспектів.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ISO/IEC 27001:2013 — міжнародний стандарт для систем управління інформаційною безпекою, що описує вимоги до створення, впровадження, підтримки та вдосконалення системи безпеки інформації.
2. Рекомендації NIST SP 800-53 — стандарт, який описує контролі безпеки для федеральних організацій США та дає настанови для побудови комплексних систем інформаційної безпеки.
3. Laudon, K. C., & Laudon, J. P. (2020). "Management Information Systems: Managing the Digital Firm" — книга, яка охоплює основи інформаційних систем і забезпечення їх безпеки.
4. Anderson, R. (2020). "Security Engineering: A Guide to Building Dependable Distributed Systems" — книга, що охоплює технічні аспекти побудови безпечних систем.
5. ISO/IEC 27001:2022 — Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою.
6. Стадник В. В., Кузнецова Т. А. «Інформаційна безпека: навчальний посібник», Київ: КНЕУ, 2020.
7. NIST SP 800-30 Rev.1 — Guide for Conducting Risk Assessments.
8. Anderson R. *Security Engineering: A Guide to Building Dependable Distributed Systems*, Wiley, 2020.
9. Goodfellow I., Bengio Y., Courville A. *Deep Learning*. MIT Press, 2016.
10. Géron A. *Hands-On Machine Learning with Scikit-Learn, Keras & TensorFlow*. O'Reilly, 2022.
11. Chollet F. *Deep Learning with Python*. Manning Publications, 2021.
12. Lecun Y., Bengio Y., Hinton G. *Deep learning*. Nature, 2015.
13. Bishop C. *Pattern Recognition and Machine Learning*. Springer, 2006.
14. 15. Géron A. *Hands-On Machine Learning with Scikit-Learn, Keras & TensorFlow*. O'Reilly, 2022.
15. 16. Chollet F. *Deep Learning with Python*. Manning, 2021.
16. 17.Google Cloud Documentation – https://cloud.google.com/products/ai
17. Microsoft Azure AI – https://azure.microsoft.com/en-us/services/machine-learning
18. AWS SageMaker – https://aws.amazon.com/sagemaker
19. PyTorch Official Site – https://pytorch.org
20. TensorFlow Official Site – https://www.tensorflow.org
21. Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. Journal of Network and Computer Applications.
22. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection.
23. Darktrace. https://www.darktrace.com
24. IBM QRadar. https://www.ibm.com/security/qradar
25. Microsoft Azure Sentinel. https://azure.microsoft.com/en-us/services/microsoft-sentinel/

26. IBM Resilient. Security Orchestration and Automation Platform.
27. Palo Alto Networks. Cortex XSOAR Overview.
28. Splunk SOAR Documentation.
29. ENISA Threat Landscape Reports.
30. Gartner Report on SOAR Market Guide, 2023.
31. Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. Journal of Network and Computer Applications.