МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В СИСТЕМАХ БЕЗПЕКИ ІНТЕРНЕТУ РЕЧЕЙ (ІОТ) ДЛЯ ЗАХИСТУ ВІД КІБЕРАТАК ”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

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

_____ Владислав КОРОВІН
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав(ла): здобувач вищої освіти гр. УБД-41
Владислав КОРОВІН
Ім’я, ПРІЗВИЩЕ

Керівник: Віталій ТИЩЕНКО
Ім’я, ПРІЗВИЩЕ

Рецензент: Галина ГАЙДУР
Д.т.н., професор Ім’я, ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут захисту інформації

Кафедра управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УІКБ
_____ Світлана ЛЕГОМІНОВА
“____”_____2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Коровіну Владиславу Петровичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Застосування штучного інтелекту в системах безпеки інтернету речей (IOT) для захисту від кібератак”,
керівник кваліфікаційної роботи ТИЩЕНКО Віталій,
(ПРІЗВИЩЕ, Ім’я)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “27“ лютого 2024 р. №36.

2. Строк подання кваліфікаційної роботи “20” травня 2024р.

3. Вихідні дані до кваліфікаційної роботи: *Інтернет речей, системи безпеки, штучний інтелект, кібератака, міжнародні стандарти, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
4.1. Проаналізувати сутність інтернету речей, розкрити ризики, тенденції та сфери охоплення.
4.2. Розкрити основні методи штучного інтелекту у системах захисту інтернету речей, етичність використання та застереження.
4.3. Запропонувати рекомендації щодо застосування штучного інтелекту для захисту IoT від кібератак.
Перелік ілюстративного матеріалу: *презентація PowerPoint*

5. Дата видачі завдання “11“ березня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2024	виконано
2.	Збір та аналіз літератури.	29.03.2024	виконано
3.	Проаналізувати сутність інтернету речей, розкрити ризики, тенденції та сфери охоплення.	08.04.2024	виконано
4.	Розкрити основні методи штучного інтелекту у системах захисту інтернету речей, етичність використання та застереження.	22.04.2024	виконано
5.	Запропонувати рекомендації щодо застосування штучного інтелекту для захисту IoT від кібератак.	08.05.2024	виконано
6.	Формулювання висновків за результатами проведеного дослідження.	20.05.2024	виконано
7.	Оформлення роботи.	22.05.2024	виконано
8.	Оформлення презентації.	03.06.2024	виконано
9.	Отримання рецензії на роботу.	03.06.2024	виконано
10.	Захист в ЕК.	__.06.2024	

Здобувач вищої освіти _____ Владислав КОРОВІН
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Віталій ТИЩЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня бакалавра

Направляється здобувач Коровін В. П. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Застосування штучного інтелекту в системах безпеки інтернету речей (IOT) для захисту від кібератак"

Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ _____ Віталій САВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувачка КОРОВІН Владислав у кваліфікаційній роботі проаналізував сутність та подальші тренди розвитку інтернету речей, області його застосування, проблематику захисту, проаналізовано основні методи штучного інтелекту, особливу увагу приділено етичності застосування штучного інтелекту та аспектам стандартизації дій, запропонував рекомендації щодо застосування штучного інтелекту для захисту IoT від кібератак.

КОРОВІН Владислав показав розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довів володіння методами наукового дослідження, проявив себе як організований, відповідальний виконавець. Результати дослідження апробовані на конференції.

Все це дозволяє оцінити кваліфікаційну роботу здобувача КОРОВІНА Владислава на оцінку "відмінно" та присвоїти їй кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Віталій ТИЩЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____" _____2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Коровін В. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
управління інформаційною
та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти КОРОВІНА Владислава
на тему "Застосування штучного інтелекту в системах безпеки інтернету речей (IOT) для захисту від кібератак"

Актуальність. Безпека в системах інтернету речей в епоху штучного інтелекту має важливе значення через швидке зростання та впровадження пристроїв інтернету речей у різних сферах. Оскільки штучний інтелект продовжує відігравати вирішальну роль у покращенні можливостей інтернету речей, дуже важливо розуміти проблеми безпеки та можливі рішення. Проводячи комплексний аналіз викликів безпеки інтернету речей, технологій штучного інтелекту, інфраструктур безпеки, міркувань щодо конфіденційності та практичних прикладів із реального світу, дослідження є актуальним та вносить вагомий внесок в вирішення проблеми захисту систем інтернету речей.

Позитивні сторони.

1. У роботі досліджено особливості методів застосування штучного інтелекту у системах захисту інтернету речей, розкрито складнощі, проаналізовано основні інструменти, надано рекомендації щодо використання технології Fortinet.

2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Ключові положення роботи представлено у вигляді рисунків, таблиць.

3. Автор опрацювала значну джерельну базу: близько 65 публікацій, в більшому англомовних.

4. За результатами дослідження автор розробив та запропонував рекомендації щодо застосування штучного інтелекту для захисту IoT від кібератак.

Недоліки.

Доцільно було б проаналізувати існуючі технології декількох компаній, які застосовують штучний інтелект для захисту від кібератак та провести порівняльний аналіз, виявити основні позитивні риси та знайти недоліки.

Однак, вищезгадане зауваження не впливає на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки "добре", а здобувач КОРОВІН Владислав заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент: _____ Галина ГАЙДУР
д.т.н., професор *підпис* Ім'я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню застосування штучного інтелекту в системах безпеки інтернету речей (IOT) для захисту від кібератак. Робота складається зі вступу, трьох розділів, висновків і списку використаних джерел із 67 найменувань. Загальний обсяг роботи становить 67 аркушів, з яких 8 аркуші займають перелік умовних скорочень та список використаних джерел.

Метою роботи є дослідження підходів та методів застосування штучного інтелекту в системах безпеки інтернету речей (IOT) для захисту від кібератак.

Об'єктом дослідження є процеси застосування штучного інтелекту для захисту інформаційних систем.

Предмет дослідження – особливості застосування штучного інтелекту в системах безпеки інтернету речей (IOT) для захисту від кібератак.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, системного підходу до управління безпекою інтернету речей (IoT).

Як результат у роботі розкрито сутність інтернету речей, виявлено тенденції та проблеми його розвитку, проаналізовано основні методи штучного інтелекту у забезпеченні його безпеки та в частині відповіді на кібератаки. Запропоновано рекомендації застосування штучного інтелекту для захисту від кібератак.

Галузь застосування. Розроблені підходи можуть бути використані при плануванні та реалізації застосування методів штучного інтелекту в системах безпеки інтернету речей (IOT) для захисту від кібератак.

Ключові слова: ШТУЧНИЙ ІНТЕЛЕКТ, ІНТЕРНЕТ РЕЧЕЙ, КІБЕРАТАКИ, ІНФОРМАЦІЙНА БЕЗПЕКА, ОРГАНІЗАЦІЯ.

ABSTRACT

The qualification work is devoted to the study of the use of artificial intelligence in Internet of Things (IOT) security systems to protect against cyber attacks. The work consists of an introduction, three chapters, conclusions and a list of used sources from 67 names. The total volume of the work is 67 sheets, of which 8 sheets are occupied by a list of conventional abbreviations and a list of used sources.

The purpose of the work is to research approaches and methods of applying artificial intelligence in Internet of Things (IoT) security systems to protect against cyber attacks.

The object of research is the processes of applying artificial intelligence to protect information systems.

The subject of the study is the specifics of using artificial intelligence in Internet of Things (IOT) security systems to protect against cyber attacks.

Research methods. To solve the above-mentioned scientific task, the methods of analysis and synthesis, comparison, classification, system approach to the security management of the Internet of Things (IoT) are used in the work.

As a result, the work revealed the essence of the Internet of Things, identified trends and problems of its development, analyzed the main methods of artificial intelligence in ensuring its security and responding to cyber attacks. Recommendations for the use of artificial intelligence for protection against cyber attacks are offered.

Field of application. The developed approaches can be used in the planning and implementation of the application of artificial intelligence methods in Internet of Things (IOT) security systems to protect against cyber attacks.

Keywords: ARTIFICIAL INTELLIGENCE, INTERNET OF THINGS, CYBER ATTACKS, INFORMATION SECURITY, ORGANIZATION.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ШІ (AI)	Штучний інтелект
IoT	Інтернет речей
IIoT	Промисловий інтернет речей

ВСТУП

Актуальність теми. Довгострокове бачення ключових проблем, які стосуються впровадження Інтернету речей, його можливостей та вразливостей, вимагають враховувати виклики та загрози зі сторони сучасних технологій, особливо штучного інтелекту, які будуть також намагатись використовувати свої можливості для реалізації власних цілей, а саме порушення безпекового функціонування цих інформаційних систем, тому вивчення проблемних областей безпеки IoT, IIoT задля протидії кібератакам являється надзвичайно актуальним дослідженням.

Складність зростатиме, оскільки ключові системи все більше залежать від інтелектуальних або зв'язаних підходів до контролю роботи; наражаючи промислові процеси та людей, які з ними працюють, більшому ризику. Таким чином, вимоги до кібербезпеки для промислового Інтернету речей мають бути визначені зараз, щоб ми краще розуміли їх вразливі місця та були краще освіченими та обладнаними для управління пов'язаними ризиками. Обєктами дослідження є технології та соціально-технічні системи, що лежать в основі критично важливих систем, від яких залежить життя, визначаючи вимоги та варіанти реагування, щоб створити безпечнішу, стійкішу інфраструктуру та забезпечити безпечні та безпечніші інновації.

З огляду на зазначене дослідження зі застосування штучного інтелекту в системах безпеки інтернету речей (IoT) для захисту від кібератак є актуальним науковим завданням.

Метою роботи є дослідження підходів та методів застосування штучного інтелекту в системах безпеки інтернету речей (IoT) для захисту від кібератак.

Об'єктом дослідження є процеси застосування штучного інтелекту для захисту інформаційних систем.

Предмет дослідження **–** особливості застосування штучного інтелекту в системах безпеки інтернету речей (IoT) для захисту від кібератак.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання**:

1. Проаналізувати сутність інтернету речей, розкрити ризики тенденції та сфери охоплення.

2. Розкрити основні методи штучного інтелекту у системах захисту інтернету речей, етичність використання та застереження.

3. Запропонувати рекомендації щодо застосування штучного інтелекту для захисту IoT від кібератак.

Методи дослідження**.** Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, системного підходу до управління безпекою інтернету речей (IoT).

Практичне значення одержаних результатів**.** Розроблені підходи можуть бути використані при плануванні та реалізації застосування методів штучного інтелекту в системах безпеки інтернету речей (IoT) для захисту від кібератак.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 28 лютого 2024 року.

РОЗДІЛ 1 ОСОБЛИВОСТІ ІНТЕРНЕТУ РЕЧЕЙ ТА РИЗИКИ ВПРОВАДЖЕННЯ

1.1. Сутність та особливості інтернету речей (IoT), його види

Інтернет речей (IoT) принесе користь суспільству завдяки низці інтелектуальних платформ і величезному розширенню, оцінки відрізняються, але кількість пристроїв становить десятки мільярдів і швидко зростає.

Інтернет речей. Мережа технологій, які взаємодіють і обчислюють через Інтернет і пов'язані з ними протоколи зв'язку, здебільшого без втручання людини: часто (але не завжди) набір невеликих малопотужних пристроїв, призначених для роботи як частини скоординованої системи для збору даних та їх аналізу. Він являє собою масивну інструментізацію світу, де обчислювальні пристрої, великі й малі, широко поширені та вбудовані в найрізноманітніші середовища. Це не обмежується створенням нових технологій, але також передбачає додавання обчислювального обладнання та програмного забезпечення до об'єктів, які раніше не мали цифрових компонентів.

Важливо, щоб стати частиною IoT, цифрові компоненти повинні підключатися до Інтернету. Часто це додає кібер-елемент до чогось фізичного, в результаті чого виникає кібер-фізична система. Функціональність Інтернету вже є у роботі та соціальному житті, а IoT забезпечить більш тісний зв'язок, де зв'язки між пристроями, програмним забезпеченням і людьми будуть сильно відрізнятися за щільністю, часом, простором та автоматизацією.

Звичайні пристрої IoT включають датчики з підтримкою Інтернету (наприклад, датчики температури або якості повітря), маяки (наприклад, мітки, які транслюють місцезнаходження) і приводи (наприклад, двигуни для відкриття та закриття воріт за командою). Ці системи розроблені та використовуються людьми, тому будь-яке IoT має враховувати відповідні соціально-технічні системи, навчання, психологічні умови, інтерфейси

користувача.

Промислові системи керування (ICS) з підтримкою Інтернету, які за своєю природою мають тенденцію бути фізично більшими, ніж «традиційний» IoT, а також менші пристрої (іноді включаючи пристрої IoT споживчого рівня) стають значною частиною поточної та майбутньої критичної інфраструктури. IIoT часто створює нові мости між інформаційними технологіями (IT) і операційними технологіями (OT) – двома сферами, якими традиційно керували та регулювали [2;3].

Безпека IIoT має вирішальне значення, і важливо розуміти, як створити безпечну та стійку інфраструктуру. Короткостроковий ризик кібератак на інфраструктуру становив понад 76% у 2020 році, 54% у 2024 році [4;5].

Але у центрі уваги нашого дослідження – промисловий Інтернет речей (IIoT). Системи промислового керування (ICS) із підтримкою Інтернету речей, які стають значною частиною поточної та майбутньої критичної інфраструктури, з великим застосування у таких сферах, як енергетика, транспорт, антропогенне середовище та виробничі потужності. Наслідки відмови можуть бути серйозними в таких середовищах, тому важливо розуміти, як створити безпечну та стійку інфраструктуру.

IIoT загострює проблеми безпеки, які вже існують, і створює нові власні. Важливо визначити пріоритетність дій, визначивши ключові нові ризики та прогалини в можливостях. З точки зору безпеки IIoT складається з трьох ключових частин: фізичних пристроїв (особливо датчики), комунікаційних мереж, інформації та даних, які пов’язані з програмними та апаратними технологіями для обробки та аналітики. Розумні технології створюють нові сфери інновацій і нові форми контролю, дозволяючи організаціям передбачати та керувати поведінкою своїх систем і середовищ.

Необхідно визначити чотири ключові чинники, що спонукають до впровадження технологій IIoT:

- Покращення операційних процесів для безпеки, продуктивності, моніторингу, ефективності, адаптивності, управління ризиками або інших

результатів.

- Зелений порядок денний: оптимізована енергоефективність, підтвердження енергоспоживання тощо, чи то на підтримку внутрішніх пріоритетів, чи для зовнішньої відповідності.
- Ринки даних: чи монетизувати власні дані на відкритих ринках, чи створювати та розширювати внутрішні процеси та послуги.
- Зручність і досвід клієнтів: надання налаштувань на основі даних і зовнішніх вікон у стані реального часу, що стає все більш цінним.

Всі ці чинники сприяють виникненню характеристик IIoT, які, як очікується, збережуться і в майбутньому:

• Масштаб пристроїв, мереж і даних IIoT стрімко зростає.

• Системи IIoT всередині та між організаціями та галузями стають все більш пов’язаними одна з одною.

• Промисловість і суспільство все більше покладаються на системи IIoT та їх інтелектуальну функціональність.

• Швидший і надійніший зв’язок між компонентами IIoT забезпечує нові функції та можливість взаємодії.

• Динамічність і гнучкість систем і мереж зростає в результаті автоматизації та визначення програмного забезпечення.

У міру розвитку Інтернету речей буде зростати потенціал кібератак, які будуть більш серйозними та потенційно системними, оскільки критично важливі системи підключені та автоматизовані.

Ці виклики є особливо гострими для промисловості та постачальників інфраструктури, де існують сильні економічні та безпекові вимоги підтримувати роботу основних систем за будь-яких обставин.

У майбутньому ризики для IIoT будуть групуватись та поширюватись, а саме:

• Традиційні ризики кібербезпеки розвиватиметься та збільшуватися разом зі збільшенням масштабів IIoT.

• Взаємозв'язок розвитку та небезпеки IIoT буде створювати спільні та

системні ризики.

• Ризики виникатимете безпосередньо через дані, створені IIoT.

• Нові технології, такі як штучний інтелект (ШІ) і квантові обчислення, можуть створити нові ризики.

• Галузеві ризики включають ймовірність загрози безпеці, непередбачувану взаємодію між застарілими системами, ризик зараження через невелику кількість виробників IIoT та ризики, пов'язані з необхідною еволюцією навчання та культури для включення IIoT.

Поточні темпи змін у можливостях операційної безпеки не відповідатимуть швидкій появі нових ризиків безпеці в середовищах IIoT. На концептуальному рівні існуючі стандарти безпеки та рекомендації все ще актуальні для IIoT.

Однак на практичному рівні здатність надавати ці можливості та способи їх надання змінюються в IIoT. Часто можливості не масштабуються, не сумісні, технічно неможливі, ще не існують або не перевірені. Як додаткове ускладнення, прогалини в деяких ключових можливостях мають наслідки для інших засобів контролю ризиків. Збільшуються прогалини в навичках та обізнаності. Ми перебуваємо на переломному етапі відновлення, оскільки ручне відновлення стає неможливим для складних систем і мережевих середовищ: потрібно буде змінити підхід до відновлення.

Існують також виклики для мислення, регулювання та страхування, оскільки ми прагнемо сприяти вдосконаленню практики безпеки.

Для вирішення проблеми необхідно прийняти до уваги основні керівні принципи для достатнього прискорення темпів операційної зміни кібербезпеки.

Вони прагнуть зміцнити позиції наступними способами:

- «припустити невдачу» як основу для планування сценарію ризику, розробки архітектури та стратегії безпеки;
- «припустити внутрішню загрозу» в системах і ланцюгах поставок;
- «припустити потенційний системний ризик» і шукати шляхи виявлення та перевірки того, де він може проявлятися, а також методи

обмеження поширення шкоди.

Ми зіткнемося зі значними проблемами щодо забезпечення кібербезпеки через різницю в системах, які створить IIoT.

Прогнозувати у сфері кібербезпеки складно, тому що ми повинні не лише враховувати відповідні досягнення в технологіях, але й те, як вони потенційно будуть використані та атакувані.

Особливо це стосується IIoT, де додатки зростають експоненціально, створюючи нові цифрові екосистеми, які можуть принести з собою нові типи можливих атак.

IIoT включає технічні компоненти, а також людей і процеси, які лежать в основі критичної інфраструктури від яких залежить суспільство.

Необхідно визначити сім наступних практичних кроків для організацій, які сьогодні використовують Інтернет речей. Це заходи, які слід враховувати при розробці продуктів і послуг на найближчу і віддалену перспективу: загалом організації повинні прагнути переходу від управління ризиками, що базується на відповідності, до управління ризиками, заснованого на результатах.

Необхідно розуміти нагальну потребу в подальших дослідженнях, спрямованих на розуміння та підтвердження ефективності контролю ризиків; вивчення моделей відповідальності, практичності та наслідків для ринків Інтернету речей; а також вивчення можливостей міжнародного співробітництва для розвитку довіри до ланцюга постачання пристроїв і програмного забезпечення IIoT.

IIoT загострює проблеми безпеки, які вже існують, і створює нові виклики. Важливо визначити пріоритетність дій шляхом визначення ключових нових ризиків і прогалин у спроможності, для яких поточні темпи змін в операційній кібербезпеці (тобто набір процесів управління ризиками кібербезпеки) будуть недостатніми.

Ландшафт виникнення ризиків IIoT концептуально можна поділити три ключові частини, що проілюстровано на рисунку 1.

• Фізичні пристрої, які включають датчики, які збирають дані з фізичного

світу, і компоненти керування, які виконують дії у фізичному світі на основі інформації, яка їм повідомляється, і обчислень, які вони здійснюють.

• Комунікаційні мережі, які з'єднують пристрої з Інтернетом та один з одним. Ці мережі передають дані для обробки та аналітики, а також отриману інформацію та контрольні інструкції. Нові комунікаційні технології, зокрема, новий 5G стандарт для стільникового зв'язку, а також однорангові технології, при значені для різкого покращення мобільного зв'язку; швидкість комунікацій і гучність кількість пристроїв, які можна підключити, продовжують стрімко зростати. Очікується, що це стане ключовим прогресом у сприянні розширенню IIoT.

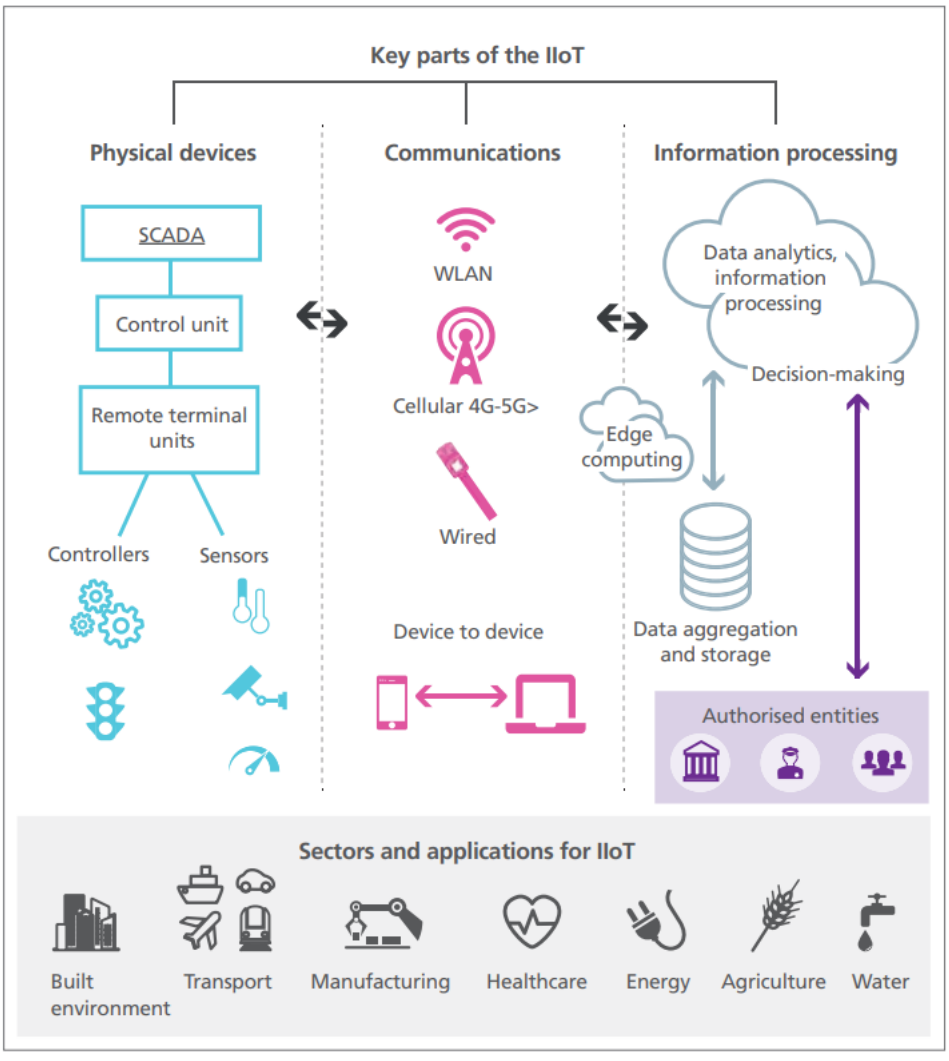

Рис. 1.1. Ландшафт виникнення ризиків IoT, IIoT : ключові складові

• Інформація та дані, а також пов’язані з ними програмні та апаратні технології для обробки та аналітики як у хмарних сервісних середовищах, так і все частіше на периферійних обчислювальних майданчиках.

Дані є основним джерелом цінності в IIoT: ключові питання зазвичай пов’язані з тим, як і куди дані збираються та надсилаються, а також про те, яку інформацію чи покращення можна отримати за допомогою їх обробки та навчання.

Таким чином, інші ключові технології включають штучний інтелект/машинне навчання та аналітику великих даних – нові методи в інформатиці та науці про дані, які дозволяють організаціям зрозуміти величезну кількість даних, які вони можуть зібрати.

Технології IoT у промисловому середовищі дають можливість підвищити ефективність і безпеку багатьма способами; наприклад, шляхом моніторингу стану обладнання або процесів, покращення обізнаності про ситуацію та мінімізації потреби людей у небезпечних середовищах. Технології IIoT впроваджуються в організаціях і секторах економіки.

Необхідно виділити чотири сектори: транспорт, енергетику, антропогенне середовище та виробничі потужності з трьох причин:

• Існує багато організацій у цих секторах, які вивчають використання IIoT, тому існує широкий спектр даних, на які можна спиратися.

• Вони забезпечують репрезентативний перетин проблем із широко застосовними уроками.

• Сектори відносно чітко визначені, з відомими ключовими гравцями, тому цілеспрямовані зусилля повинні забезпечити відчутний прогрес.

Ландшафт кіберризиків Інтернету речей

Ризики пов’язані з новими інноваціями, які створюють нові ризики; деякі загрози безпеці є спільними для всіх пристроїв з підтримкою Інтернету.

Ризик визначається як наявність загрози, що існує в середовищі (людина-зловмисник або фактор навколишнього середовища), і актив у системі з уразливістю, якою можна скористатися (також відомий як «поверхня атаки»).

Ризик кваліфікується та кількісно оцінюється шляхом оцінки ймовірності того, що ризик матиме місце (чи то у формі нещасного випадку, чи як послідовності подій, що складають напад), і рівня збитків, які можуть бути зазнані, якщо маніфест ризику.

Шкода є результатом виникнення одного або кількох ризиків.

Нові характеристики IIoT змінюються та змінюються кіберризики, що пов'язані з новими ризиками. Вони змінюють ландшафт загроз, атаки поверхні, набір підходів до управління ризиками захисників, що також може завдати шкоду, яка може виникнути в результаті кіберінциденту. На рисунку 2 відображено основні драйвери, які провокують розвиток IIoT та одночасно появу нових кіберризиків.

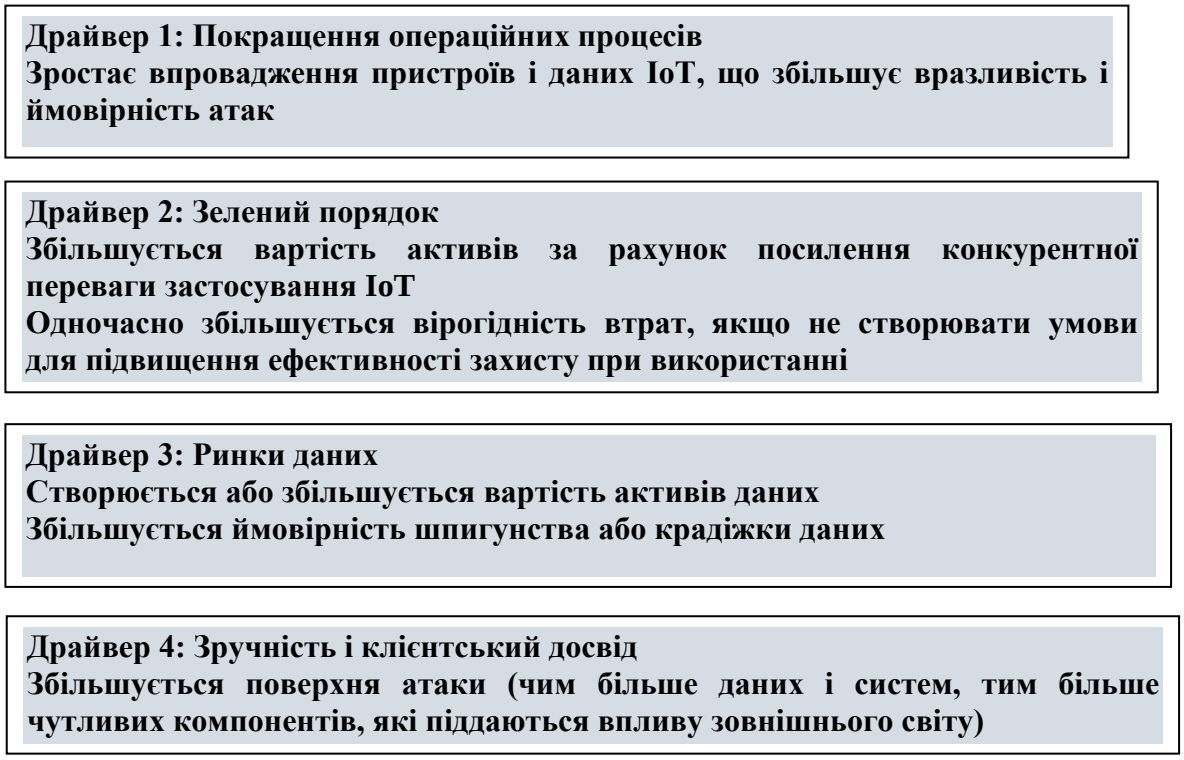

Рис. 1.2. Драйвери, які змінюють ландшафт кіберризиків

Інтернет речей (IoT) зробив революцію в різних сферах, дозволивши взаємопов'язаним пристроям спілкуватися та обмінюватися даними. Інтеграція штучного інтелекту (AI) у системи Інтернету речей ще більше розширює їхні можливості та потенційні переваги. На жаль, в епоху штучного інтелекту забезпечення конфіденційності та безпеки IoT стикається з новими та

специфічними проблемами. Безпека Інтернету речей є обов'язковою, що вимагає комплексних стратегій, включаючи розуміння викликів безпеки Інтернету речей, впровадження методологій штучного інтелекту, прийняття стійких інфраструктур безпеки та вирішення питань конфіденційності та етичних проблем для створення надійних і безпечних систем Інтернету речей [6].

Важливо зазначити, що термін «безпека» охоплює більш повний погляд, ніж лише кібератаки. Тому, акцентуючи увагу на захисті від кібератак, це комплексний захист має включати фізичні загрози безпеці в IoT. Він досліджує складності та рішення для систем Інтернету речей, приділяючи особливу увагу технікам безпеки на основі ШІ.

Класифікація проблеми, пов'язана із забезпеченням безпеки IoT, дослідженням використання штучного інтелекту в безпеці IoT, представленні рамки та стратегії безпеки, підкресленні конфіденційності та етичності міркування, а також розуміння на основі практичних прикладів.

1.2. Категорії ризику кібератак в IIoT

Традиційні ризики кібербезпеки розвиваються та збільшуються в міру розширення масштабів Інтернету речей.

Ризики, загальні для традиційних обчислювальних середовищ, можуть збільшуватися разом із широкомасштабним впровадженням IIoT завдяки збільшенню темпів, масштабу, щільності та різноманітності пристроїв.

• *Нова технологія створює розширену поверхню атаки*. Пристрої вводяться фізичні, що змінює інфраструктури, створює нову поверхню для атаки. Це може бути результатом вразливості у самій технології, з використанням технології, що створює поверхню атаки операційних процесів або поверхню атаки в організмі людини в результаті їх взаємодії з технологією. Усі вразливості при експлуатації можуть створити додаткові можливості для компрометації даних та системи, оскільки зловмисники використовують їх як платформи для орієнтації через системи.

• *Програмна поверхня атаки*. Оскільки функції та комунікації все більше стають програмними в своїй основі (через програмно визначені мережі та віртуальні мережеві функції), існує вірогідність зростаючої поверхні атак на основі програмного забезпечення, в якій можна використовувати вразливості. Це може посилювати недоліки практики розробки та обслуговування програмного забезпечення, які часто недостатньо безпечні навіть в існуючих середовищах.

• *Атаки шкідливих програм.* Кількість атак зловмисного програмного забезпечення (вимагачів, викрадання даних та саботаж, наприклад) збільшуватиметься разом із збільшенням кількості підключених до Інтернету та керованих програмним забезпеченням пристроїв із зростаючою ймовірністю кіберфізичного впливу.

• *«Прихований ризик».* Існує ризик того, що незахищені пристрої будуть «приховані» або іншим чином занедбані, у масштабі підключених систем. Методології безпеки можуть бути відсутні на цих пристроях, які інтуїтивно класифікуються як неактуальні (наприклад, розумний чайник у їдальні або пристрої підрядників можуть використовуватися як вектор атаки, але нехтувати ними при перевірці безпеки організації).

Сучасні підходи до операційної безпеки та управління ризиками

Ризик кібербезпеки зазвичай розглядається з точки зору конфіденційності, цілісності та доступності (CIA) технологічних компонентів операційного середовища: систем і даних.

Ризики контролюються за допомогою технологій і процесів, а також передаються або розподіляються через кіберстрахування з метою забезпечення п’яти ключових сфер операційної безпеки. Запровадження засобів контролю ризиків і безпечної практики обумовлюється нормативно-правовими актами та законодавством, ринковою конкуренцією (включно з договірними вимогами та безпекою як конкурентною перевагою), мисленням організацій щодо кібербезпеки, спрямованим на пом’якшення шкідливих наслідків потенційного кіберінциденту, а також вимогами постачальників кіберстрахування.

Висновки до розділу 1

Інтернет речей швидко розвивається, і поточні підходи до кібербезпеки щодо запобігання атак виявлення та реагування на них не можна повністю застосувати в цій сфері, треба знаходити нові підходи та технології, такі як машинне навчання або штучний інтелект.

Додатки IIoT зростають експоненціально, створюючи нові цифрові екосистеми, які можуть принести з собою нові типи можливих атак, відповідь на які треба знаходити своєчасно та конструктивно.

Основними ризиками здійснення кібератак на системи безпеки IoT та IIoT визнано: нові технології, які створюють розширену поверхню атаки; програмні поверхні атаки; атаки зі сторони шкідливих програм; «приховані ризики».

РОЗДІЛ 2 МЕТОЛОДОГІЧНА ПРОБЛЕМАТИКА СИСТЕМ БЕЗПЕКИ IoT

2.1. Аналіз методів забезпечення безпеки IoT

Захист систем IoT створює унікальні проблеми, які необхідно вирішити, щоб забезпечити цілісність, конфіденційність і доступність послуг IoT [16:17].

Методи безпеки IoT

Методи Штучного інтелекту мають потенціал для значного підвищення безпеки систем IoT [7:8]. Використання алгоритмів і моделей ШІ може забезпечити інтелектуальне виявлення загроз, надійні механізми автентифікації та проактивну аналітику безпеки.

Технології виявлення та запобігання загрозам відіграють вирішальну роль у виявленні та запобіганні загрозам у системах Інтернету речей шляхом виявлення аномальних шаблонів і поведінки, які можуть свідчити про потенційні порушення безпеки. Ці методи використовують алгоритми машинного навчання та аналіз даних для підвищення рівня безпеки розгортання Інтернету речей. Основні методи виявлення та запобігання загрозам у системах IoT включають:

Системи виявлення вторгнень (IDS) з використанням алгоритмів AI:

- IDS на основі алгоритмів AI, таких як виявлення аномалій [19] або моделі на основі поведінки [9], можуть ідентифікувати потенційні порушення безпеки. Ці системи IDS постійно відстежують Мережевий трафік, дії пристроїв і системні журнали, щоб виявити відхилення від нормальної поведінки [20]. На основі отриманих даних і спостережень у реальному часі алгоритми штучного інтелекту можуть ідентифікувати шаблони, пов'язані з відомими кібератаками, або виявляти аномальні дії, які можуть вказувати на нові та нові загрози.
- Виявлення аномалій у потоках даних IoT на основі машинного

навчання: алгоритми штучного інтелекту можуть аналізувати дані в реальному часі потоки, створені пристроями Інтернету речей для виявлення ненормальних шаблонів, що сигналізують про потенційні загрози безпеці або несанкціоновані дії. Навчаючись на історичних даних і встановлюючи базову лінію нормальної поведінки, моделі машинного навчання можуть визначати відхилення та сповіщати, коли відбуваються аномальні дії. Це дозволяє проактивно ідентифікувати потенційні кібератаки, забезпечуючи своєчасне реагування та заходи пом'якшення, щоб запобігти порушенням безпеки [21].

- Аналіз поведінки для виявлення аномальних шаблонів у поведінці пристроїв Інтернету речей: методи штучного інтелекту можна використовувати для побудови моделей нормальної поведінки пристроїв Інтернету речей [22]. Ці моделі фіксують типові шаблони використання, шаблони зв'язку та взаємодії пристроїв у системі IoT. Порівнюючи спостережувану поведінку пристроїв із цими моделями, алгоритми штучного інтелекту можуть визначати відхилення та позначати підозрілу діяльність. Аналіз поведінки дозволяє виявляти тонкі аномалії, які не можуть бути виявлені традиційними системами на основі правил, покращуючи загальні можливості виявлення загроз рішень IoTsecurity.
- Сучасні інструменти штучного інтелекту для безпеки Інтернету речей: сучасні технології штучного інтелекту, включаючи DL, стохастичне та байєсовське навчання, трансформатори та GenAI:[15]. є важливими для посилення безпеки IoT від передових кіберзагроз у системах IoT, що швидко змінюються. DL ідеально підходить для захисту від вторгнення та виявлення аномалій завдяки своїй потужності обробки та здатності розпізнавати складні шаблони у великих наборах даних. Наприклад, системи безпеки мережі використовують алгоритми DL для виявлення підозрілих

шаблонів, які можуть бути ознаками атаки. Подібним чином, стохастичне та байєсівське навчання відіграють вирішальну роль у ситуаціях, які вимагають прийняття рішень в умовах невизначеності. Адаптуючи механізми безпеки, засновані на ймовірнісному міркуванні, ці технології забезпечують стійкість проти нових загроз у динамічному середовищі Інтернету речей. Однак кібербезпека Інтернету речей все більше використовує трансформатори, які добре відомі своєю ефективністю в обробці послідовних даних. З їх допомогою ми можемо проактивно захистити себе від порушень безпеки, аналізуючи дані часових рядів з пристроїв IoT. Так само існують значні наслідки для кібербезпеки в IoT від GenAI, як-от ChatGPT. Він допомагає створювати навчальні дані моделі безпеки, складні методи захисту та симулювати кібератаки. Ця технологія швидко стає ключовим компонентом передових систем кібербезпеки, які є проактивними. Використовуючи методи ШІ для виявлення та запобігання загрозам у системах IoT, організації можуть проактивно виявляти потенційні загрози безпеці та реагувати на них. IDS на основі алгоритмів штучного інтелекту, виявлення аномалій на основі машинного навчання та методів аналізу поведінки надають розширені можливості для виявлення нових загроз, пом'якшення кібератак 1 захисту розгортання IoT.

Ці методи підвищують загальну безпеку систем IoT, забезпечуючи своєчасне виявлення, реагування та запобігання порушенням безпеки даних IoT. Кожен підхід пропонує різні ключові заходи та переваги, разом сприяючи комплексним стратегіям безпеки IoT. Використовуючи методи безпечного керування даними, організації можуть захистити конфіденційність, цілісність і конфіденційність даних IoT. Класифікація даних і механізми контролю доступу гарантують, що доступ до даних мають лише уповноважені організації, безпечне зберігання та методи обробки захищають дані в стані очікування під

час обробки, а міркування щодо управління життєвим циклом даних мінімізують ризик порушення даних. У сукупності ці практики сприяють створенню безпечної та сумісної системи керування даними для систем Інтернету речей, дозволяючи організаціям отримувати користь від даних Інтернету речей, зберігаючи безпеку та конфіденційність даних.

2.1.1 Безпечна комунікація та автентифікація

Методи AI відіграють життєво важливу роль у підвищенні безпеки зв'язку та механізмів автентифікації в системах IoT. Використовуючи інтелектуальні алгоритми та моделі, ці методи підвищують конфіденційність, цілісність і автентичність передачі даних і покращують процес автентифікації.

Ключові методи безпечного зв'язку та автентифікації в системах IoT включають:

- Криптографічні методи, керовані AI для безпечної передачі даних: алгоритми AI можуть покращити криптографічні протоколи [23]і схеми керування ключами [24] для забезпечення безпечного та надійного зв'язку між пристроями IoT. Ці алгоритми можуть оптимізувати алгоритми шифрування, встановити безпечні механізми обміну ключами та підвищити загальну безпеку передачі даних у системах IoT. Використовуючи методи штучного інтелекту, організації можуть вирішувати проблеми, пов'язані з безпечними та ефективними криптографічними операціями в пристроях Інтернету речей з обмеженими ресурсами.
- Механізми автентифікації на основі штучного інтелекту, такі як біометрична або поведінкова автентифікація: методи штучного інтелекту можуть покращити механізми автентифікації в системах Інтернету речей. -tems, виходячи за межі традиційних схем імені користувача та пароля. Наприклад, алгоритми біометричної ідентифікації можуть використовувати розпізнавання обличчя [25],

розпізнавання голосу [26], розпізнавання відбитка долоні [27] або сканування відбитків пальців [28] для забезпечення безпечної та зручної автентифікації для пристроїв Інтернету речей. Алгоритми штучного інтелекту також можуть аналізувати шаблони поведінки користувачів для безперервної автентифікації, забезпечуючи динамічний адаптивний процес автентифікації. Впроваджуючи штучний інтелекту механізми автентифікації, організації можуть підвищити безпеку та користувацький досвід роботи з системами Інтернету речей.

– Встановлення та управління довірою за допомогою алгоритмів-ШІ: Алгоритми AI можна використовувати для встановлення довірчих відносин між пристроями IoT і керування довірою в динамічних середовищах IoT, що розвиваються. Ці алгоритми можуть оцінювати репутацію, поведінку та контекст пристроїв Інтернету речей, щоб визначити рівень надійності. Постійно оцінюючи довіру [29], алгоритми ШІ можуть динамічно коригувати привілеї та дозволи доступу, забезпечуючи безпечний і детальний контроль над взаємодією пристроїв. Він підвищує безпеку та цілісність систем Інтернету речей, запобігаючи несанкціонованому доступу та зловмисним діям.

Використовуючи методи штучного інтелекту для безпечного зв'язку та автентифікації, організації можуть посилити безпеку систем Інтернету речей. Криптографічні методи на основі штучного інтелекту підвищують безпеку передачі даних, механізми автентифікації на основі штучного інтелекту забезпечують надійні та зручні процеси автентифікації, а встановлення довіри та керування на основі штучного інтелекту забезпечує динамічний адаптивний контроль над взаємодією пристроїв. Ці методи підвищують загальну безпеку і надійність систем IoT, забезпечуючи конфіденційність, цілісність і автентичність даних і взаємодій у взаємопов'язаній екосистемі IoT.

2.1.2 Методи прогнозної аналітики безпеки штучного інтелекту систем IoT

Методи штучного інтелекту використовують потужність аналізу даних, щоб забезпечити прогнозовану аналітику безпеки для систем IoT [30]. Аналізуючи великі обсяги даних, ці методи можуть дозволити організаціям проактивно виявляти та зменшувати ризики безпеки, оцінювати потенційні вразливості та запобігати інцидентам безпеки. Ключові методи для прогнозної аналітики безпеки в системах IoT включають:

1. Штучний інтелект для прогнозованого обслуговування та оцінки ризиків у розгортанні IoT: моделі AI можуть аналізувати дані датчиків, зібрані з пристроїв IoT, щоб передбачити потреби в обслуговуванні та оцінити потенційні ризики. Виявляючи шаблони та аномалії в показаннях датчиків, алгоритми штучного інтелекту можуть передбачити, коли пристрій, ймовірно, вийде з ладу або потребує технічного обслуговування [31]. Це дозволяє організаціям завчасно вирішувати потреби в обслуговуванні, зменшуючи ризик системних збоїв або порушень безпеки. Крім того, моделі штучного інтелекту можуть оцінювати потенційні ризики [32] в розгортанні IoT шляхом аналізу історичних даних і факторів навколишнього середовища, допомагаючи організаціям визначати пріоритети заходів безпеки та ефективно розподіляти ресурси.
2. Проактивна розвідка та аналіз загроз за допомогою алгоритмів штучного інтелекту: методи штучного інтелекту можуть аналізувати різноманітні джерела даних, у тому числі журнали безпеки, канали розвідки про загрози та дані мережевого трафіку, щоб ідентифікувати потенційні загрози та вразливості. Використовуючи алгоритми машинного навчання, моделі штучного інтелекту можуть виявляти закономірності та ознаки компрометації, які можуть сигналізувати про неминучу загрозу безпеці. Це дає змогу організаціям проактивно реагувати на нові загрози, оновлювати заходи безпеки та зміцнювати свій захист від потенційних кібератак. Інтелектуальні дані та аналіз загроз на основі штучного інтелекту забезпечують цінну інформацію та дозволяють

організаціям залишатися на крок попереду кібератак [33].

3. Прогнозування та запобігання інцидентам безпеки за допомогою моделей ШІ: моделі ШІ можуть аналізувати історичні дані, щоб визначити закономірності, які передували інцидентам безпеки. Використовуючи попередні інциденти та пов’язані з ними дані, алгоритми штучного інтелекту можуть ідентифікувати індикатори, які вказують на потенційне порушення системи безпеки або атаку. Це дозволяє організаціям вживати проактивних заходів для запобігання майбутнім інцидентам, наприклад, запроваджувати патчі безпеки, оновлювати конфігурації або посилювати контроль доступу [34]. Прогнозуючи та запобігаючи інцидентам безпеки, організації можуть мінімізувати вплив кібератак і забезпечити безперервну безпеку своїх систем Інтернету речей.

У таблиці 2.1 представлено вичерпний огляд того, як технології штучного інтелекту можуть значно підвищити безпеку систем Інтернету речей. Він класифікує ці методи за трьома ключовими напрямами: «Виявлення та запобігання загрозам», «Безпечний зв’язок і автентифікація» та «Прогнозна аналітика безпеки».

У першій категорії ШІ використовується для виявлення та запобігання кібератак за допомогою таких методів, як IDS, виявлення аномалій на основі машинного навчання та аналіз поведінки.

Друга категорія підкреслює роль штучного інтелекту в підвищенні безпеки зв’язку та механізмів автентифікації за допомогою криптографічних методів, біометрії та динамічного управління довірою.

Нарешті, третя категорія обговорює, як штучний інтелект розширює можливості систем IoT за допомогою прогнозної аналітики безпеки, забезпечуючи прогнозне технічне обслуговування, проактивну розвідку про загрози та прогнозування інцидентів безпеки.

Крім того, таблиця містить розділ «Додаткові функції», у якому наголошується на важливості аудиту безпеки, плануванні реагування на

інциденти, навчання користувачів, а також дотримання правових і нормативних вимог [18]. Ці заходи та рішення, керовані штучним інтелектом, разом зміцнюють безпеку Інтернету речей, зменшуючи вразливості та забезпечуючи цілісність підключених систем. Використовуючи методи штучного інтелекту для прогнозної аналітики безпеки, організації можуть завчасно виявляти та усувати ризики безпеки, передбачати потреби в обслуговуванні та запобігати інцидентам безпеки.

Таблиця 2.1.

Методи Штучного інтелекту для безпеки IoT

Категорія	Опис	Заходи	Рішення
Загроза виявлення Профілактика	ШІ техніки для ідентифікації кібератак в IoT.	Системи виявлення вторгнень (IDS) з використанням алгоритмів AI Виявлення аномалій у потоках даних IoT на основі машинного навчання Аналіз поведінки для виявлення аномальних шаблонів у поведінці пристроїв IoT	Виявлення аномалій, поведінкові моделі Аналіз даних у реальному часі, виявлення аномалій Побудова моделей нормальної поведінки, поведінковий аналіз
Безпечний зв'язок Аутентифікація	ШІ техніки для підвищення безпеки і аутентифікація в IoT	Криптографічні методи на основі штучного інтелекту для безпечної передачі даних Механізми автентифікації на основі штучного інтелекту (наприклад, біометрія) Встановлення довіри та управління використання алгоритмів AI	Оптимізація шифрування, обмін захищеними ключами Розпізнавання обличчя, розпізнавання голосу, автентифікація на основі поведінки Динамічна оцінка довіри, контекстний контроль доступу
Прогностична Безпека Аналітика	ШІ техніки для прогностичної безпеки та аналітики в IoT.	AI для прогнозного обслуговування та оцінки ризиків у розгортанні IoT Проактивне розвідування загроз та аналіз за допомогою алгоритмів AI	Аналіз даних датчиків, оцінка ризиків Виявлення шаблонів загроз, проактивне реагування Розпізнавання шаблонів

		Прогнозування та запобігання інцидентам безпеки за допомогою моделей AI	інцидентів, попередньо - профілактичні заходи
Додаткові особливості	Додаткові міркування для підвищення IoT безпеки	Аудит безпеки План реагування на інциденти Навчання користувачів Безпеки Інтернету речей Відповідність законодавству та нормам	Регулярні аудити та оцінки План реагування на інциденти безпеки Навчання користувачів найкращим практикам Дотримання законів та нормативним актам щодо конфіденційності

Прогнозне технічне обслуговування та оцінка ризиків за допомогою штучного інтелекту, проактивна розвідка та аналіз загроз, а також прогнозування та запобігання інцидентам безпеки дозволяють організаціям зміцнити безпеку своїх систем IoT. Збільшуючи потужність даних і алгоритмів штучного інтелекту, організації можуть приймати обґрунтовані рішення, ефективно розподіляти ресурси та вживати профілактичних заходів для забезпечення безпеки та стійкості своїх розгортань IoT.

2.2. Підходи до забезпечення безпеки IoT

Захист систем Інтернету речей потребує комплексних основ і підходів. Класифікація цих фреймворків може бути представлена на основі основних принципів і стратегій впровадження:

АРХІТЕКТУРИ ПОГЛИБЕНОГО ЗАХИСТУ

Архітектури поглибленого захисту спрямовані на забезпечення багаторівневих механізмів безпеки для систем Інтернету речей, забезпечуючи надійний захист від різних векторів атак. Ці архітектури передбачають реалізацію кількох рівнів безпеки, враховуючи всю екосистему Інтернету речей, а також впроваджуючи стратегії проектування та впровадження безпечного апаратного забезпечення.

Ключові аспекти архітектур поглибленого захисту для безпеки IoT

включають:

1. Багаторівневі механізми безпеки для захисту пристроїв і мереж IoT: архітектури поглибленого захисту використовують кілька рівнів безпеки для захисту пристроїв і мереж IoT. Він включає в себе впровадження фізичних заходів безпеки, таких як безпечні корпуси та захист від несанкціонованого доступу, щоб запобігти несанкціонованому доступу до пристроїв IoT. Методи сегментації мережі, такі як віртуальні локальні мережі (VLAN) або брандмауери [35], можна розгорнути для ізоляції пристроїв IoT і запобігти переміщенню всередині мережі. Механізми контролю доступу, такі як надійна автентифікація та протоколи авторизації, гарантують, що лише авторизовані особи можуть взаємодіяти з пристроями та системами IoT. Розміщуючи ці механізми безпеки, організації створюють численні бар'єри для зловмисників, підвищуючи загальну стійкість безпеки своїх розгортань IoT.

2. Схеми безпеки, розроблені для наскрізної безпеки в системах IoT: архітектури поглибленого захисту враховують всю екосистему IoT, що включає пристрої, мережі та серверні системи. Такий підхід забезпечує цілісний і комплексний підхід до безпеки. Інфраструктури безпеки, розроблені для наскрізної безпеки в системах IoT, визначають політики безпеки, протоколи та найкращі практики, яких слід дотримуватися протягом усього життєвого циклу розгортання IoT. Ці фреймворки стосуються безпеки на різних рівнях, включаючи безпеку пристроїв [36], мережеву безпеку [37], безпеку даних [38] і контроль доступу [40] . Приймаючи такі фреймворки, організації можуть гарантувати послідовне застосування заходів безпеки в усій екосистемі IoT, мінімізація вразливостей і потенційних поверхонь для атак.

3. Стратегії розробки та реалізації безпечного апаратного забезпечення: архітектури глибокого захисту також включають стратегії проектування та впровадження безпечного апаратного забезпечення. Це передбачає включення функцій безпеки в дизайн апаратного забезпечення пристроїв Інтернету речей, наприклад мікросхем, захищених від втручання. [40], елементи безпеки або механізми безпечного завантаження [41]. Захищена

конструкція апаратного забезпечення спрямована на захист цілісності пристрою, запобігання несанкціонованому доступу чи втручанню, а також на гарантію того, що на пристрій можна завантажити лише надійну мікропрограму та програмне забезпечення. Впроваджуючи безпеку в розробку апаратного забезпечення та впроваджуючи безпечні практики виробництва та ланцюга постачання, організації можуть створити міцну основу для IoT безпеки пристроїв.

Застосовуючи архітектури з поглибленим захистом, організації можуть значно підвищити безпеку своїх систем Інтернету речей. Багаторівневі механізми безпеки захищають пристрої та мережі Інтернету речей від різних векторів атак. Інфраструктури безпеки забезпечують наскрізну безпеку в екосистемі Інтернету речей, а стратегії проектування та впровадження безпечного апаратного забезпечення забезпечують надійну основу для безпеки пристроїв. Ці підходи мінімізують уразливості, зменшують вплив потенційних кібератак і зміцнюють загальну стійкість безпеки розгортань IoT.

БЕЗПЕЧНА РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Безпечна практика розробки програмного забезпечення має вирішальне значення для побудови стійких систем Інтернету речей, стійких до кібератак. Дотримуючись методів безпечного кодування, запроваджуючи безпечні механізми оновлення та проводячи ретельне тестування безпеки, організації можуть мінімізувати вразливості та підвищити загальну безпеку програмного забезпечення Інтернету речей.

Основні припущення щодо безпечної розробки програмного забезпечення в системах Інтернету речей включають:

Практики безпечного кодування для пристроїв і програм Інтернету речей: дотримання вказівок із безпечного кодування та найкращих практик має важливе значення для мінімізації появи вразливостей під час процесу розробки. Він включає в себе такі практики, як перевірка вхідних даних [42], вихідне кодування [43] і належну обробку введених користувачем даних, щоб запобігти поширеним векторам атак, таким як ін’єкційні атаки або міжсайтовий сценарій

[44]. Впроваджуючи методи безпечного кодування в життєвий цикл розробки IoT-пристроїв і програм, організації можуть зменшити ризик вразливості системи безпеки та покращення загальної стійкості їх програмного забезпечення.

Безпечні механізми оновлення мікропрограми та програмного забезпечення: впровадження безпечних механізмів оновлення через бездротове (OTA) має вирішальне значення для того, щоб пристрої IoT могли отримувати та встановлювати виправлення та оновлення безпеки надійно. Він передбачає впровадження криптографічних протоколів для захисту процесу оновлення, перевірки цілісності та автентичності оновлень і безпечного розповсюдження оновлень на пристрої IoT. Механізми безпечного оновлення дозволяють організаціям усунути нещодавно виявлені вразливості та зменшити потенційні ризики, не вимагаючи фізичного доступу до пристроїв, підвищуючи загальну безпеку та ремонтопридатність розгортань IoT [10;45].

Тестування безпеки та методи оцінки вразливостей для систем IoT: проведення ретельної безпеки тестування має важливе значення для виявлення та усунення вразливостей у програмних компонентах IoT. Він включає такі методи, як тестування на проникнення, аудит коду та сканування вразливостей [46] для виявлення слабких місць і потенційних точок входу для зловмисників. Тестування безпеки допомагає організаціям виявити вразливі місця перед розгортанням і перевірити ефективність заходів безпеки [47]. Включивши тестування безпеки як невід’ємну частину процесу розробки програмного забезпечення, організації можуть завчасно виявляти та усувати проблеми безпеки, зменшуючи ймовірність успішних кібератак.

Застосовуючи методи безпечної розробки програмного забезпечення, організації можуть значно підвищити безпеку своїх систем Інтернету речей. Методи безпечного кодування зменшують ризик появи вразливостей, механізми безпечного оновлення дозволяють своєчасно виправляти недоліки безпеки, а тестування безпеки забезпечує ідентифікацію та усунення вразливостей. У сукупності ці методи сприяють створенню стійкого та

безпечного програмного забезпечення IoT, зменшуючи поверхню атак і покращуючи загальну ефективність стан безпеки розгортання IoT.

БЕЗПЕЧНЕ КЕРУВАННЯ ДАНИМИ

Ефективне керування даними має вирішальне значення для підтримки безпеки та конфіденційності даних IoT. Практики безпечного керування даними охоплюють класифікацію даних, механізми контролю доступу, безпечне зберігання даних, безпечні методи обробки даних і належне управління життєвим циклом даних. Ключові аспекти безпечного керування даними в системах Інтернету речей включають:

Механізми класифікації даних і контролю доступу: застосування міток класифікації даних до даних Інтернету речей допомагає організаціям зрозуміти чутливість і критичність даних, які вони збирають. Впроваджуючи детальні механізми контролю доступу, такі як керування доступом на основі ролей [48] або керування доступом на основі атрибутів [49], організації можуть гарантувати, що доступ до даних IoT мають лише уповноважені особи. Механізми контролю доступу повинні передбачати автентифікацію користувачів, політику авторизації та безпечні канали зв’язку для захисту конфіденційності та цілісності даних IoT.

Безпечне зберігання даних і методи обробки для IoT-середовища: механізми безпечного зберігання є життєво важливими для захисту даних IoT у стані спокою. Використання методів шифрування, таких як сильні симетричні або асиметричні алгоритми шифрування [50], гарантує, що дані залишаються конфіденційними, навіть якщо вони скомпрометовані або викрадені. Захищений анклав або апаратні модулі безпеки (HSM) можуть забезпечити додатковий захист шляхом ізоляції конфіденційних даних і криптографічних операцій від основної системи. Подібним чином безпечні методи обробки даних, такі як безпечні багатосторонні обчислення [51], дозволяють проводити спільний аналіз даних [11] без розголошення необроблених даних, забезпечуючи конфіденційність даних IoT під час обробки.

Управління життєвим циклом даних у системах IoT: Дані IoT протягом

усього життєвого циклу мають важливе значення для забезпечення їх безпеки. Це включає в себе встановлення відповідної політики зберігання даних, яка визначає, як довго дані повинні зберігатися, і визначення безпечних процедур видалення даних [52], щоб мінімізувати ризик порушення даних. Організаціям слід розглянути методи анонімізації або псевдонімізації даних, щоб захистити конфіденційність осіб і дотримуватися правил захисту даних. Впровадження надійних стратегій резервного копіювання та відновлення даних також сприяє безпечному управлінню даними, забезпечуючи доступність і цілісність даних IoT.

Основні механізми безпеки та підходи до захисту систем IoT можна класифікувати за трьома ключовими напрямками: архітектури з глибоким захистом, розробка безпечного програмного забезпечення та безпечне керування даними.

Архітектури поглибленого захисту підкреслюють багатошарові механізми безпеки, цілісні інфраструктури безпеки та надійний дизайн апаратного забезпечення для захисту розгортання IoT від різноманітних векторів атак. Практика розробки безпечного програмного забезпечення охоплює безпечне кодування, механізми бездротового оновлення та ретельне тестування безпеки, що зменшує вразливості та підвищує стійкість програмного забезпечення IoT. Безпечне керування даними передбачає класифікацію даних, контроль доступу, безпечне зберігання та керування життєвим циклом, забезпечуючи конфіденційність, цілісність і відповідність даних IoT. Кожен підхід пропонує різні ключові заходи та переваги, разом сприяючи комплексним стратегіям безпеки IoT. Використовуючи методи безпечного керування даними, організації можуть захистити конфіденційність, цілісність і конфіденційність даних IoT. Класифікація даних і механізми контролю доступу гарантують, що доступ до даних мають лише уповноважені організації, безпечне зберігання та методи обробки захищають дані в стані очікування під час обробки, а міркування щодо управління життєвим циклом даних мінімізують ризик порушення даних. У сукупності ці практики сприяють

створенню безпечної та сумісної системи керування даними для систем Інтернету речей, дозволяючи організаціям отримувати користь від даних Інтернету речей, зберігаючи безпеку та конфіденційність даних.

2.3 Етичне використання штучного інтелекту в безпеці IoT

Забезпечення етичного використання ШІ в безпеці IoT має важливе значення для підтримки прозорості, справедливості та підзвітності. Етичні міркування допомагають усунути потенційні упередження, забезпечують прозорість і зрозумілість алгоритмів штучного інтелекту та встановлюють рамки підзвітності та відповідальності. Основні аспекти етичного використання штучного інтелекту в безпеці Інтернету речей включають:

1. Прозорість і зрозумілість алгоритмів штучного інтелекту, які використовуються в безпеці Інтернету речей: створення прозорих і зрозумілих алгоритмів ШІ та процесів прийняття рішень допомагає зміцнити довіру користувачів і забезпечує підзвітність. Користувачі та зацікавлені сторони повинні бачити, як навчаються алгоритми штучного інтелекту, дані, які використовуються, і критерії прийняття рішень. Методи пояснення, такі як можливість інтерпретації моделі та алгоритмічна прозорість, можуть надати уявлення про те, як моделі AI приходять до своїх рішень. Прозорий і зрозумілий штучний інтелект зміцнює довіру та дає змогу людям зрозуміти обґрунтування заходів безпеки та потенційних обмежень [53;54].
2. Міркування справедливості для пом’якшення упередженості при прийнятті рішень ШІ: усунення упереджень в алгоритмах і моделях ШІ, які використовуються в безпеці Інтернету речей, є надзвичайно важливо для запобігання дискримінаційним результатам і забезпечення справедливого ставлення до осіб. Упередженість може виникнути через упереджені навчальні дані, помилкові алгоритми або

вроджені суспільні упередження. Організації повинні прагнути виявляти та пом’якшувати упередження за допомогою ретельної попередньої обробки даних, методів алгоритмічної справедливості та постійного моніторингу [55]. Активно вирішуючи упередженість, організації можуть підвищити справедливість і справедливість систем безпеки з підтримкою штучного інтелекту, заохочуючи рівне ставлення та зменшуючи ризик різнорідних впливів.

3. Рамки підзвітності та відповідальності для систем безпеки Інтернету речей із підтримкою штучного інтелекту: створення основи для управління відповідальним використанням штучного інтелекту в безпеці Інтернету речей є важливою. Він включає визначення чітких рамок підзвітності та відповідальності, які розподіляють відповідальність [56] між організаціями, розробниками та операторами систем безпеки з підтримкою ШІ IoT.

Організації повинні забезпечити відповідність застосовним законам, нормам і етичним стандартам [57]. Вони також повинні розглянути потенційні ризики та небажані наслідки, пов’язані з розгортанням штучного інтелекту, і встановити механізми для відшкодування та захисту у разі збоїв у системі або неправильного використання. Запроваджуючи механізми підзвітності та відповідальності, організації можуть сприяти етичним практикам, підвищувати довіру користувачів і пом’якшувати потенційні ризики. Основні аспекти конфіденційності та етики в системах Інтернету речей спрямовані на необхідність захисту конфіденційності користувачів і забезпечення відповідального розгортання штучного інтелекту.

Перший аспект - «Захист конфіденційності даних», що охоплює такі методи збереження конфіденційності, як диференційована конфіденційність і безпечні багатосторонні обчислення, анонімізація, підходи псевдонімізації та оцінка впливу на конфіденційність.

Другий аспект - «Етичне використання ШІ» досліджує прозорість, справедливість і підзвітність у безпеці Інтернету речей за допомогою ШІ.

Третій аспект - «Виклики конфіденційності» розглядає проблеми, пов’язані зі збором даних, обробкою та згодою користувачів.

Віддаючи пріоритет етичному використанню штучного інтелекту в безпеці Інтернету речей, організації можуть створити прозорість, справедливість і підзвітність у своїх системах. Прозорі та зрозумілі алгоритми штучного інтелекту сприяють зміцненню довіри, міркування справедливості пом’якшують упередженість, а системи підзвітності забезпечують відповідальну практику. Ці етичні припущення сприяють прийняттю технологій штучного інтелекту відповідно до суспільних цінностей, поважають права особи та підвищують загальну безпеку та надійність систем Інтернету речей.

2.4 Безпека промислового Інтернету речей (IIoT)

Впровадження безпеки промислового Інтернету речей (IIoT) у виробництві та критичній інфраструктурі: промисловий сектор, включаючи виробничі потужності та критичну інфраструктуру, значною мірою покладається на системи Інтернету речей для оптимізації операцій, підвищення ефективності та моніторингу продуктивності обладнання. Однак ці системи часто є основними цілями для кібератак [58;59]. Методи штучного інтелекту використовуються для захисту промислових систем управління, виявлення аномалій [60] в оперативних даних і пом’якшення кібератак у критичній інфраструктурі. Алгоритми штучного інтелекту можуть аналізувати величезні обсяги даних, створених пристроями IIoT, такими як датчики та промислове обладнання, щоб ідентифікувати ненормальні шаблони, які можуть вказувати на кібератаки або несправності обладнання. Використовуючи можливості виявлення загроз і прогнозованого обслуговування на основі ШІ, організації можуть підвищити безпеку та стійкість своїх промислових розгортань IoT.

Ці специфічні для галузі випадки використання демонструють різноманітне застосування штучного інтелекту для підвищення безпеки систем Інтернету речей. У сфері охорони здоров’я штучний інтелект забезпечує безпечні та конфіденційні рішення Інтернету речей у сфері охорони здоров’я.

Наприклад, системи безпеки Smarthome використовують AI для виявлення вторгнень і безпечного контролю доступу. У промисловому секторі технології штучного інтелекту підвищують безпеку розгортання IIoT і забезпечують проактивне виявлення загроз. Розуміючи ці випадки використання, організації можуть досліджувати індивідуальні підходи до захисту систем Інтернету речей у своїй конкретній галузі, вирішуючи специфічні для галузі виклики та вимоги, одночасно використовуючи потужність штучного інтелекту для підвищення безпеки.

2.5 Удосконалення ШІ для безпеки інтернету речей

Удосконалення ШІ відкрили нові можливості для підвищення безпеки Інтернету речей. Ці нові вдосконалення використовують новітні технології штучного інтелекту для вирішення унікальних завдань IoTsecurity, забезпечуючи розподілене аналізування безпеки, обробку безпеки на пристрої та адаптивні самозахищаючі системи IoT. Деякі помітні досягнення в галузі безпеки ШІ для Інтернету речей включають:

Навчання для розподіленої інформації про безпеку в системах Інтернету речей: навчання — це техніка машинного навчання, що зберігає конфіденційність, яка забезпечує спільне навчання моделі на кількох пристроях Інтернету речей, зберігаючи при цьому конфіденційність даних.

Інтегроване навчання може бути застосоване до безпеки IoT для створення розподіленої інформації про безпеку. Замість того, щоб централізувати дані в одному місці, навчання дозволяє тренувати моделі на самих пристроях IoT. Цей підхід дає змогу пристроям Інтернету речей навчатися на своїх локальних даних, обмінюючись агрегованими знаннями з центральним сервером або іншими пристроями. Використовуючи навчання, системи IoT можуть отримати вигоду від колективного інтелекту, зберігаючи при цьому конфіденційність даних і вирішуючи проблеми власності на дані.

Edge AI для обробки безпеки на пристрої та прийняття рішень: Edge AI

стосується розгортання алгоритмів AI безпосередньо на пристроях IoT або на мережі Інтернету речей, що забезпечує обробку та прийняття рішень у режимі безпеки в реальному часі, не покладаючись на хмарні послуги. Розвиваючи можливості штучного інтелекту на мережі, пристрої IoT можуть аналізувати кібератаки та реагувати на них локально, мінімізуючи затримку та залежність від зовнішнього підключення. Edge AI забезпечує ефективну обробку даних, миттєве реагування на інциденти безпеки та меншу залежність від хмарних ресурсів. Завдяки обробці безпеки на пристрої пристрої IoT можуть автономно виявляти та пом'якшувати загрози безпеці, підвищуючи загальну безпеку та стійкість розгортань IoT.

Адаптивні та самозахистні системи IoT на основі штучного інтелекту: методи ШІ можуть дозволити системам IoT адаптуватися для еволюції кібератак, динамічно коригувати заходи безпеки та автономно реагувати на потенційні атаки. Алгоритми штучного інтелекту можуть безперервно відстежувати дані IoT, аналізувати шаблони та виявляти нові кібератаки чи вразливості. Використовуючи попередні інциденти, системи IoT на базі штучного інтелекту можуть проактивно коригувати заходи безпеки, такі як оновлення засобів контролю доступу, модифікацію алгоритмів шифрування або блокування підозрілих дій. Ця можливість адаптації та самозахисту допомагає системам IoT залишатися стійкими та швидко реагувати на нові проблеми безпеки, зниження ймовірності успішних кібератак та мінімізувати вплив порушень безпеки.

Роль і майбутнє бачення GenAI у кібербезпеці: Такі інструменти, як ChatGPT, які підпадають під егіду GenAI, з'явилися протягом останніх кількох років і змінюють форму кількох галузей, включаючи кібербезпеку [12].GenAI зробив революцію у виявленні загроз і системному захисті, що є важливим для безпеки IoT. Його здатність вивчати та дублювати складні шаблони даних виділяє його. Інтеграція GenAI у кібербезпеку означає помітний відхід від звичайних реактивних, захисних механізмів і прийняття більш проактивного підходу. Ці алгоритми штучного інтелекту вдосконалюють мистецтво пошуку

та прогнозування можливих порушень шляхом відсіювання даних про проблеми кібербезпеки. Завдяки чудовому виявленню загроз GenAI, ретельному аналізу даних і можливостям прогнозування ризиків кіберзахист тепер ефективніший. З іншого боку, існують специфічні перешкоди для впровадження таких технологій. Вирішення таких проблем, як потреба у великомасштабних обчислювальних ресурсах, ризик зловживання хакерами можливостями штучного інтелекту та етичні проблеми щодо захисту та контролю даних є вирішальним. Кілька передових продуктів кібербезпеки демонструють використання GenAI. Крім того, відбулися помітні прориви в власних інструментах аналітики безпеки на основі ШІ, таких як CrowdStrike's Charlotte AI [15], який надає практичні та прості методи управління ризиками кібербезпеки.

Процес штучного інтелекту в Xi-росімі G7 та китайська Глобальна ініціатива з управління штучним інтелектом є двома прикладами всесвітніх спроб контролювати штучний інтелект [61]. У делікатних сферах, таких як кібербезпека, ці нормативні рамки відіграють ключову роль у формуванні належного використання ШІ. Інтеграція GenAI у кібербезпеку має негайні наслідки для IoTsecurity. Тепер, як ніколи, коли пристрої IoT поширені та важливі для багатьох галузей, надзвичайно важливо, щоб ці моделі ШІ могли передбачати ризики та завчасно керувати ними. Щоб гарантувати безпеку та надійність систем Інтернету речей, дуже важливо обережно використовувати та регулювати GenAI, оскільки ми продовжуємо використовувати його потенціал. Ці досягнення в галузі безпеки ШІ для безпеки Інтернету речей пропонують багатообіцяючі можливості для підвищення безпеки та стійкості систем Інтернету речей. Інтегроване навчання забезпечує розподілену інформацію про безпеку, обробка безпеки на пристрої використовує edgeAI для прийняття рішень у режимі реального часу, а адаптивні та самозахисні системи IoT на основі штучного інтелекту автономно реагують на кібератаки. Використовуючи ці досягнення, організації можуть використовувати потужність штучного інтелекту для покращення стану безпеки своїх розгортань IoT, забезпечуючи

проактивне виявлення загроз, ефективну обробку безпеки та адаптивні механізми захисту.

Стандартизація та регулювання зусиль

Стандартизація та регулювання відіграють вирішальну роль у забезпеченні безпеки та надійності систем IoT. Оскільки впровадження Інтернету речей продовжує поширюватися в галузях і секторах, потреба в узгоджених заходах безпеки та правових структурах стає все більш важливою. Зусилля зі стандартизації зосереджені на розробці структур безпеки IoT, галузевих стандартів і найкращих практик, тоді як регулятивні зусилля спрямовані на юридичні аспекти та вимоги відповідності, що стосуються безпеки та конфіденційності IoT.

Ключові аспекти стандартизації та нормативних заходів у сфері безпеки IoT включають:

Структури безпеки IoT і галузеві стандарти: розробка стандартизованих інфраструктур і галузевих стандартів безпеки IoT є важливою для забезпечення послідовних заходів безпеки в різних розгортаннях IoT. Ці рамки та стандарти містять вказівки та найкращі практики щодо захисту пристроїв, мереж і даних IoT. Вони стосуються різних аспектів безпеки IoT, зокрема безпеки на рівні пристрою, безпеки мережі, безпеки даних та конфіденційності. Дотримуючись цих рамок і стандартів, організації можуть створити загальну базу для безпеки IoT, полегшити взаємодію та просувати належні методи безпеки в усій екосистемі IoT. Приклади інфраструктур і стандартів безпеки IoT включають Рамку безпеки промислового Інтернет-консорціуму (IIC), NIST Cybersecurity Framework та ISO/IEC серії 27000 [13].

Використовуючи стандарти AI/IoT, встановлені міжнародними організаціями, промислові підприємства повинні оновлювати системи відповідно до глобальних норм. ООН/МСЕ визначає безпечні та сумісні системи IIoT [62]. З тієї ж причини стандарти IEEE забезпечують структуру для включення ШІ в IIoT [14].

Галузі промисловості дотримувалися цих вимог, щоб гарантувати, що їхні

покращені системи були технологічно сучасними та відповідали найкращим практикам і нормам у всьому світі. Наприклад, виробнича компанія зіткнулася з труднощами через свою застарілу інфраструктуру та відсутність складних можливостей моніторингу в реальній ситуації. Стохастичні методи навчання забезпечують практичний і економічний спосіб модернізації пов'язаних з виробництвом пристроїв Інтернету речей, яким бракує інтелекту [63]. Інтеграція стохастичного навчання в існуючі структури може заощадити витрати на перебудову системи. Цей метод включає в себе моделі штучного інтелекту, які можуть обробляти щойно отримані дані, оснащуючи старі машини датчиками. Виробнича промисловість може запустити програму прогнозованого технічного обслуговування, інтегрувавши AI у свою структуру IIoT. Датчики цієї системи, підключені до життєво важливого обладнання, збирали дані про продуктивність обладнання в реальному часі. Аналізуючи ці дані, системи штучного інтелекту можуть виявити порушення, які можуть свідчити про те, що обладнання от-от виходить з ладу. За допомогою технології прогнозованого технічного обслуговування бригади технічного обслуговування могли діяти до того, як трапилася дорога поломка, запобігаючи вирішальному збою на критичній виробничій лінії. Завдяки цій дії було досягнуто значного скорочення витрат і уникнення основних виробничих простоїв. Успішне впровадження продемонструвало практичні переваги штучного інтелекту в промисловому середовищі, ще більше зміцнивши позицію заводу як лідера в технічному прогресі.

Юридичні та нормативні аспекти безпеки та конфіденційності IoT: вирішення правових і нормативних проблем у сфері безпеки IoT має вирішальне значення для створення надійної правової основи для безпечні й конфіденційні системи IoT. Розгортання IoT часто передбачає збір, обробку та зберігання великих обсягів даних, у тому числі особистої та конфіденційної інформації. Юридичні та нормативні аспекти охоплюють положення про захист даних, закони про конфіденційність і рамки відповідальності. Організації повинні дотримуватися чинних нормативних актів і гарантувати, що системи

Інтернету речей відповідають юридичним вимогам щодо конфіденційності даних, керування згодою, сповіщення про порушення даних і прав користувачів. Уряди та регулюючі органи активно працюють над оновленням існуючих законів або запровадженням нових нормативних актів, що стосуються безпеки та конфіденційності Інтернету речей, з метою досягнення балансу між інноваціями та захистом індивідуальних прав.

Інтероперабельність і структури сертифікації для рішень безпеки Інтернету речей: розробка стандартів сумісності та структур сертифікації для рішень безпеки Інтернету речей надзвичайно важливо, щоб різні компоненти безпеки могли бездоганно працювати разом і відповідати встановленим вимогам безпеки. Стандарти сумісності визначають протоколи та інтерфейси, які забезпечують інтеграцію та взаємодію різноманітних пристроїв і систем IoT. Ці стандарти допомагають встановити безпечний зв'язок, забезпечують узгоджені механізми автентифікації та полегшують обмін інформацією, пов'язаною з безпекою. Системи сертифікації надають засоби для перевірки та перевірки можливостей безпеки пристроїв, мереж або рішень IoT. Завдяки оцінці та сертифікації третіми сторонами організації можуть продемонструвати відповідність встановленим стандартам безпеки та отримати впевненість у безпеці своїх розгортань IoT.

Приклади стандартів сумісності та основ сертифікації для IoTsecurity включають Zigbee Alliance, Thread Group і Common Criteria for Information TechnologySecurity Evaluation. Стандартизація та регулятивні заходи щодо безпеки IoT є важливими для встановлення послідовних заходів безпеки, забезпечення дотримання законодавства та сприяння взаємодії. Рамки IoTsecurity та галузеві стандарти керують впровадженням ефективних заходів безпеки, юридичні та нормативні міркування вирішують питання конфіденційності та відповідальності, а рамки взаємодії та сертифікації забезпечують сумісність і надійність рішень безпеки IoT. Використовуючи ці зусилля зі стандартизації та регулювання, організації можуть підвищити рівень безпеки своїх систем Інтернету речей, зміцнити довіру між користувачами та

зацікавленими сторонами та сприяти широкому впровадженню безпечних і конфіденційних розгортань Інтернету речей

Проблеми з фізичною та інфраструктурною безпекою в IoT.

Захист систем IoT вимагає фізичних та інфраструктурних міркувань на додаток до цифрових. Значною проблемою в цій сфері є мінімізація ризиків, пов'язаних із несанкціонованими фізичними вторгненнями в інфраструктуру або пристрої IoT. Важливо запобігти будь-якому втручанню в роботу цих пристроїв, щоб забезпечити їх постійне функціонування та цілісність.

Захист пристроїв Інтернету речей від фізичної крадіжки: забезпечення безпеки пристроїв Інтернету речей і конфіденційних даних, які вони містять, від крадіжки є надзвичайно важливим. Крім того, фізична відмовостійкість є ключовим аспектом, який вимагає, щоб компоненти інфраструктури та пристрої Інтернету речей були розроблені таким чином, щоб протистояти викликам навколишнього середовища, включаючи, але не обмежуючись, екстремальні температури, вологість та інші несприятливі умови. Важливо бути обережним при виборі місця розгортання, щоб зменшити сприйнятливість до фізичних небезпек. Щоб зменшити ризик фальсифікації або компрометації протягом усього життєвого циклу пристроїв IoT, включаючи їх виробництво, транспортування та встановлення, безпека ланцюга постачання має однакове значення. стихійні умови, такі як сувора погода, забруднення та фізичні пошкодження. Вкрай важливо захистити пристрої IoT від навмисного фізичного втручання, яке може порушити їхню роботу або поставити під загрозу цілісність даних.

Захист від фізичного втручання та забезпечення безперебійного живлення: також важливо забезпечити захист від фізичного втручання. Ми повинні звернути увагу на надійність джерела живлення для IoT-пристроїв. І фізичне втручання, і втрата живлення можуть призвести до переривання зв'язку та втрати конфіденційних даних. Також важливо захистити фізичну інфраструктуру центрів обробки даних або хмарних серверів, які зберігають і обробляють дані IoT, на додаток до мережевої інфраструктури, яка полегшує

зв’язок IoT. Він включає захист фізичних загроз від маршрутизаторів, комутаторів і шлюзів. У світлі різноманітних фізичних та інфраструктурних викликів безпеці, які спричиняють ці системи, і різноманітних загроз, з якими вони можуть зіткнутися під час практичного розгортання, необхідно прийняти всеохоплюючу стратегію для забезпечення безпеки IoT.X.

Висновки до розділу 2

Захист Інтернету речей в епоху штучного інтелекту потребує комплексного та багатовимірного підходу. Вирішуючи проблеми, використовуючи технології штучного інтелекту, дотримуючись інструкцій безпеки та враховуючи конфіденційність і етичні наслідки, він може створити надійні та стійкі системи Інтернету речей, які покращують безпеку, захищають конфіденційність користувачів і зміцнюють довіру.

Розкрито проблеми, які виникають під час захисту систем Інтернету речей, і досліджувалися різні методи штучного інтелекту, які можна використовувати для підвищення їх безпеки. Завдяки класифікації викликів безпеки на рівні пристрою, викликів безпеки мережі, викликів безпеки даних, проблем конфіденційності та етичних міркувань, підкреслено багатогранний характер захисту Інтернету речей у контексті ШІ.

РОЗДІЛ 3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В СИСТЕМАХ БЕЗПЕКИ ІНТЕРНЕТУ РЕЧЕЙ (IoT) ДЛЯ ЗАХИСТУ ВІД КІБЕРАТАК

Цифрова трансформація створює зростаючий тягар безпеки для лідерів мережевої інженерії. Ініціативи DX призводять до появи в мережі більшої кількості мобільних пристроїв і пристроїв Інтернету речей (IoT), а також зростаючого портфоліо хмарних програм, що працюють на кількох хмарних платформах. Усе це збільшує площу атаки підприємства, надаючи більше векторів для кіберзлочинців, щоб проникнути в мережу, викрасти дані та використати ресурси [64].

3.1. Переваги штучного інтелекту (ШІ) для захисту від кібератак інтернету речей (IoT)

Впровадження ШІ в кібербезпеку пропонує широкий спектр переваг для організацій, які прагнуть керувати захистом від кібератак. Типові переваги:

1. Постійне навчання: можливості штучного інтелекту постійно вдосконалюються, коли він вивчає нові дані. Такі методи, як глибоке навчання та машинне навчання, дозволяють ШІ розпізнавати закономірності, встановлювати базову лінію регулярної активності та виявляти будь-яку незвичну або підозрілу діяльність, яка відхиляється від неї. Здатність ШІ постійно навчатися ускладнює хакерам обхід захисту організації.

2. Виявлення невідомих загроз: оскільки кіберзлочинці винаходять складніші вектори атак , організації залишаються вразливими до невідомих загроз, які можуть завдати величезної шкоди мережам. Штучний інтелект надає рішення для відображення та запобігання невідомим загрозам, включаючи вразливості, які ще не виявлені або виправлені постачальниками програмного забезпечення.

3. Величезні обсяги даних: системи штучного інтелекту можуть

обробляти та розуміти величезні обсяги даних, яких не можуть професіонали з безпеки. Таким чином, організації можуть автоматично виявляти нові загрози серед величезних обсягів даних і мережевого трафіку, які можуть залишитися непоміченими традиційними системами.

4. Покращене керування вразливими місцями: окрім виявлення нових загроз, ШІ дозволяє організаціям краще керувати вразливими місцями. Це допомагає їм ефективніше оцінювати свої системи, покращувати вирішення проблем і приймати кращі рішення. Він також може виявити слабкі місця в мережах і системах, щоб організації постійно зосереджувалися на найважливіших завданнях безпеки.

5. Покращена загальна безпека: вручну керувати ризиками низки загроз, від атак на відмову в обслуговуванні (DoS) і фішингових атак до програм-вимагачів , може бути складно та займати багато часу. Але за допомогою штучного інтелекту організації можуть виявляти різні типи атак у реальному часі та ефективно визначати пріоритети та запобігати ризикам.

6. Краще виявлення та реагування: виявлення загроз є необхідним елементом захисту даних і мережі. Кібербезпека з підтримкою штучного інтелекту може призвести до швидкого виявлення ненадійних даних і більш систематичної та негайної реакції на нові загрози.

На рисунку 3.1. представлені основні переваги штучного інтелекту у забезпеченні безпеки IoT.

Global Threat Research Labs.

Лабораторії постачальників безпеки з дослідження загроз проклали шлях до розробки штучного інтелекту в кібербезпеці. Маючи глобальні погляди та охоплення, багато з цих груп були одними з перших, хто зрозумів, що аналіз загроз, розроблений людьми, не зможе встигати за ландшафтом загроз, що швидко розвивається.

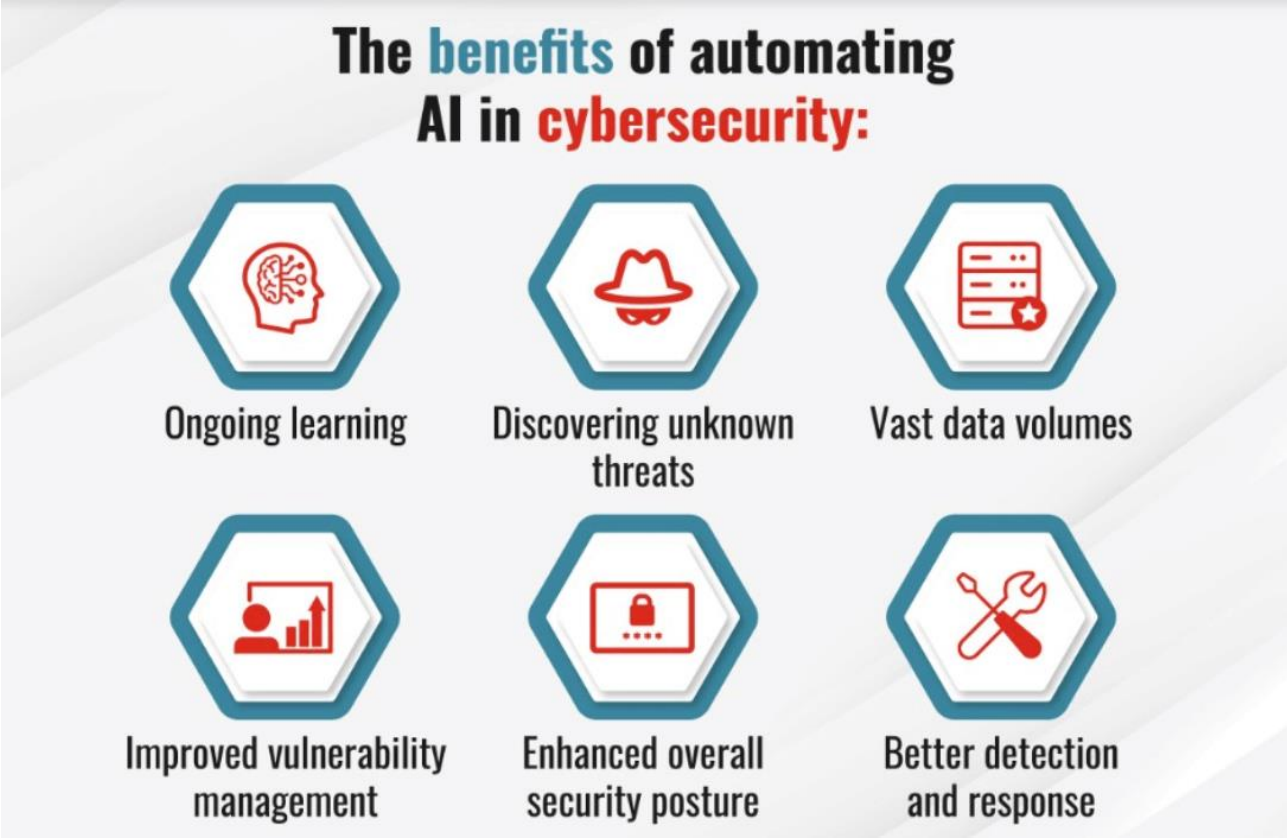

Рис.3.1. Переваги штучного інтелекту (AI) у забезпеченні безпеки IoT

У той же час, перед завданням (і справді фінансовим стимулом) захисту сотень тисяч клієнтів, комерційне обґрунтування для інвестицій у розширену аналітику було вагомим. Сьогодні, як правило, машинне навчання (ML) використовується, зокрема, для прискорення ідентифікації нових кібератак і, що більш важливо, індикаторів компрометації (IOC), пов'язаних з ними. Ці IOC складають значну частину оновлень аналізу загроз, що надаються для продуктів і служб безпеки, які захищають клієнтів постачальника безпеки.

Ключові переваги аналізу загроз на основі штучного інтелекту від глобальних лабораторій дослідження загроз включають:

1. Величезний набір даних для кількох класів загроз і повних життєвих циклів загроз для початкової розробки та постійного вдосконалення моделей ШІ

2. Масово масштабована обчислювальна потужність, вартість якої можна розподілити між великою клієнтською базою

3. Деякі з провідних експертів із безпеки постійно перевіряють точність

вихідних даних.

Однак цей ультрацентралізований підхід також має значні обмеження, наприклад:

1. Окремий клієнт отримує лише IOC, і ці IOC стосуються лише загроз, які досягають глобальної лабораторії.

2. Процес перевірки та доставки цих IOC зазвичай займає години або більше.

3. У таких складних, багатодисциплінарних і віддалених дослідницьких місцях клієнти мають обмежене бачення того, як постачальник систем безпеки насправді використовує штучний інтелект. Клієнти глобальних лабораторій дослідження загроз отримують результати штучного інтелекту у вигляді оновлень аналізу загроз, розроблених для захисту від останні кіберзагрози. Це може включати оновлення продуктів безпеки, розгорнутих в організації, як-от оновлення антивірусної програми (AV) для брандмауера наступного покоління (NGFW) або платформи захисту кінцевих точок, або канал загроз для підписки, що надає необроблений список відомих зловмисних IP-адрес тощо МОК.

Популярний сучасний підхід полягає в тому, щоб перенести штучний інтелект власноруч у централізоване місце для окремої організації через «озеро даних». Цей підхід компенсує обмеження глобального аналізу загроз шляхом поєднання моделей ШІ, подібних до тих, що використовуються в дослідницьких лабораторіях з даними, специфічними для організації.

В результаті:

1. Захищена організація визначає IOC, специфічні для кіберзагроз, яким вона піддається.

2. Ці IOC, а також відповідна інформація про кампанію загроз та її етапи, часто доступні для персоналу після застосування аналізу ШІ.

3. Організація точно знає тип (модель) і область (клас загрози) застосованого ШІ.

Однак у цього підходу до конкретної організації також є недоліки, такі як:

1. Втрачено видимість глобальної загрози, яка може досягти їх у

майбутньому.

2. Дорога інфраструктура, така як зберігання, обробка, простір і електроенергія, необхідні для центрального «озера даних».

3. Час, необхідний для збору даних, нормалізації та затримки результатів аналізу. Цей останній пункт є одним із найбільш значущих обмежень, оскільки це означає, що штучний інтелект може бути розгорнутий лише в якості детектива.

На момент завершення аналізу атака вже сталася і потребує усунення.

Зокрема, «озера даних» і аналіз штучного інтелекту, виведений у формі сповіщень, повинні бути пріоритетними, дослідженими та підтвердженими або визнаними недійсними. IOC та інші дані про загрози визначаються персоналом безпеки організації, а не глобальними дослідниками загроз, і їх потрібно додати до засобів контролю безпеки організації вручну або за допомогою автоматизації. І, звичайно, персонал повинен очистити зламані системи.

Третій підхід до застосування ШІ для кібербезпеки передбачає розгортання моделей ШІ, де дані (файли, IP-адреси, активність системи тощо), що підлягає аналізу, проходить або перебуває. Як правило, це включає вхідний, вихідний і внутрішній трафік, пункти перевірки, серверні та хост-пристрої кінцевих користувачів, а також доставка локальних або хмарних додатків.

Цей підхід до штучного інтелекту має кілька переваг, таких як:

- Можливість застосовувати ШІ як для запобігання, так і для виявлення;
- ШІ, що визначає конкретні загрози, з якими стикається організація;
- Повне розуміння типів ШІ, які використовуються, і класів загроз, які вони вирішують.

Однак цей підхід має свої обмеження, зокрема:

- Зосередженість на загрозах на організаційному, а не глобальному рівні;
- Обмежена потужність обробки для розподіленого ШІ;
- Зосередження лише на класах загрози, які проходять певну точку перевірки.

Вихідні дані розподілених моделей штучного інтелекту можуть бути використані для запобігання потенційній загрозі або для створення попередження для подальшого розслідування та реагування. Оптимальна конфігурація залежить від особливостей розгортання, наприклад від точного розгортання місцезнаходження, аналізованих даних, тривалості аналізу, бажаної конфігурації.

Наприклад, у кінцевій точці ML, який перевіряє характеристики файлів або ранню поведінку, пов’язану зі спробами експлойтів, може часто використовуватись як механізм профілактики. Навпаки, легкий датчик, який передає активність головної системи на Cloud for ML analytics зазвичай генерує сповіщення для подальшого дослідження.

Окрім фізичного розташування аналітики та характеру результату, важливо враховувати кібератаку фази, до якої він застосовується. Компанія Lockheed Martin створила ланцюжок кіберзнищень, окресливши сім загальних етапів кіберзагроз, усі вони мають бути успішними, щоб кіберзлочинець міг досягти своєї кінцевої мети. Це розвідка, озброєння, доставка, експлуатація, встановлення, командування та контроль, а також дії по цілях, що успішно перешкоджає кіберзлочинцям на будь-якій окремій стадії відмовляє зловмисникові в їх кінцевій меті.

Етап у ланцюжку кіберзнищення, на якому діє організація, визначає, чи вдалося запобігти атаці до удару чи вимагає дорожчого виявлення та реагування. Розвідка про загрози, отримана в глобальних лабораторіях дослідження загроз, часто є корисною для профілактики. Бази даних репутації IP можуть виявляти спроби розвідки та розвідки про загрози, що надаються розгорнутими системами безпеки, призначені для переривання етапів доставки, експлуатації та встановлення.

Однак стратегія лише запобігання не завжди ефективна, про що свідчить постійний потік заголовків про витоки даних. більшістьорганізації інвестують у можливості виявлення загроз, які, за словами Gartner, «все ще мають велику вагу у ланцюгі кіберубивств».

Підхід «озера даних» часто служить основою для виявлення кінцевих точок і реагування на основі штучного інтелекту, поведінки користувачів і об’єктів аналітики (UEBA) та інші методи виявлення. Ці елементи керування застосовуються після етапу встановлення для виявлення аномальной діяльності, яка часто пов’язана з командуванням і управлінням або діями щодо цілей, що часто є викраденням даних. На цьому етапі ШІ призначений для виявлення атаки, що триває, до того, як відбудуться цілі кінцевої стадії, такі як викрадання даних.

Розподілений підхід до штучного інтелекту має великі перспективи, оскільки він дає змогу застосовувати моделі штучного інтелекту для конкретної організації на початку ланцюга кіберубивств. Орієнтуючись на етапи доставки, експлуатації та встановлення, організація зменшується ймовірність того, що знадобиться дорога відповідь [65].

3.2. Захист IoT від кібератак на основі технології Fortinet

Як один з варіантів рішення щодо забезпечення захисту IoT від кібератак є пропозиція компанії Fortinet.

Fortinet і DefendEdge

Рішення безпеки інтегроване й автоматизоване для виявлення інсайдерської загрози на основі штучного інтелекту та реагування на них. Резюме Fortinet і DefendEdge об’єдналися, щоб надати провідне в галузі рішення шляхом інтеграції FortinetSecurity Fabric і SiON, щоб надати організаціям проактивне машинне навчання на основі правил. у виявленні аномальних загроз співробітників і реагуванні на них.

Виклики

Поверхня атак продовжує розширюватися, і хоча багато команд безпеки зосереджені насамперед на запобіганні зловмисникам ззовні використовувати нові місця атак, у звіті Verizon про розслідування витоку даних за 2018 рік було виявлено, що близько 30% підтверджених зломів сьогодні стосуються

інсайдерів. Однак сьогодні все більше складні мережі, що ускладнюється поширенням даних, пристроїв, програм і користувачів, які отримують доступ до мережевих ресурсів, ускладнюють групам безпеки виявлення та запобігання внутрішнім загрозам, незалежно від того, чи є ці порушення зловмисними чи результатом недбалості.

У міру того, як прогресивні загрози швидко розвиваються, CISO повинні впроваджувати засоби контролю безпеки, які захищають дані, інтелектуальну власність і репутацію компанії як всередині, так і зовні. І вони повинні робити це, одночасно задовольняючи галузеві вимоги відповідності.

Спільне рішення DefendEdge і Fortinet встановили технологічне партнерство, щоб забезпечити організації дієвою аналітикою діяльності співробітників і допомогти приймати рішення щодо загроз у реальному часі. Власна платформа машинного навчання SiON усуває помилкові спрацьовування під час пошуку загроз і дозволяє командам із кібербезпеки зосередитися на підтверджених індикаторах загрози.

Компоненти спільного рішення DefendEdge SiON Рішення SiON від DefendEdge — це корпоративна платформа, яка об’єднує та аналізує численні корпоративні джерела даних і надає можливість виконувати робочі процеси, визначені організацією на основі поведінки кінцевих користувачів.

Брандмауер наступного покоління FortiGate

Брандмауери наступного покоління FortiGate (NGFW) забезпечують роботу в мережі, керовану безпекою, і консолідують провідні в галузі можливості безпеки, такі як система запобігання вторгненням (IPS), веб-фільтрація, перевірка рівня захищених сокетів (SSL) і автоматизований захист від загроз. Fortinet NGFW задовольняють потреби продуктивності високомасштабованих гібридних IT-архітектур, дозволяючи організаціям зменшити складність і керувати ризиками безпеки.

FortiClient Enterprise Management Server

Як інтегрований агент, FortiClient ділиться телеметрією кінцевої точки з Security Fabric і забезпечує широку видимість кінцевої точки, контроль

відповідності та керування вразливістю. Він забезпечує розширений захист кінцевих точок із захистом від шкідливих програм на основі шаблонів, захистом від експлойтів на основі поведінки, веб-фільтрацією та брандмауером програм. FortiClient вбудовано інтегрується з FortiSandbox для виявлення загроз нульового дня та спеціальних шкідливих програм. FortiClient також забезпечує безпечний віддалений доступ із вбудованою віртуальною приватною мережею (VPN), єдиним входом і двофакторною автентифікацією для додаткової безпеки.

FortiSandbox

FortiSandbox із найвищим рейтингом на базі штучного інтелекту (ШІ) є частиною рішення Fortinet для захисту від злому, яке інтегрується з платформою Fortinet Security Fabric для протидії загрозам, що швидко розвиваються та мають більш цілеспрямований характер, включаючи програмне забезпечення-вимагач, криптошкідливе програмне забезпечення та інші на широкій поверхні цифрових атак. Зокрема, він надає оперативну інформацію в режимі реального часу за допомогою автоматизації розширеного виявлення зловмисного програмного забезпечення та реагування на нього.

Платформа SiON від DefendEdge завантажує дані журналу з Fortinet Security Fabric на платформу та використовує авторитетні передові системи й додатки корпоративного рівня, а також ідентифікацію користувачів для кореляції й аналізу даних, виявлення аномальної поведінки кінцевих користувачів і виконання автоматизованих процедур. На основі архітектури кінцевого стану клієнта платформа може бути розміщена локально або в хмарі. Інтеграція з цільовими системами безперебійна й виконується за допомогою інтерфейсу прикладного програмування (API), плоских файлів або інших методів, орієнтованих на підключення. SiON пропонує декілька профілів доступу на основі ролей для керівників, директорів і аналітиків безпеки з кількома варіантами звітів для аудиторів і відповідальних працівників.

На рисунку 3.2. представлена модіфікація системи захисту IoT від кібератак на основі штучного інтелекту.

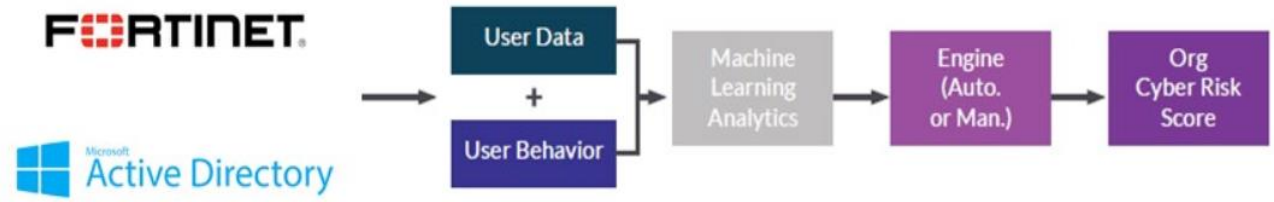

Рис. 3.2. Fortinet Security Fabric і DefendEdge SiON

Приклади використання системи

Приклад використання 1:

SiON допомагає розв'язати викрадання даних, коли співробітник має привілейований доступ до конфіденційної інформації та намагається завантажити дані на флешку. SiON сповіщає організацію про те, що дані викрадаються, і ізолює всю діяльність кінцевих користувачів FortiGate і FortiEMS.

Приклад використання 2:

Інтеграція SiON і FortiGate допомагає забезпечити можливість моніторингу поведінки кінцевих користувачів і часу входу, геолокації та сесії даних. SiON може вжити заходів, щоб припинити аномальну поведінку та ініціювати відкликання пароля для підозрілого скомпрометований обліковий запис Active Directory LDAP користувача.

Отже, основними компонентами системи є: Fortinet Security Fabric — Fortinet FortiGate Nextgeneration Firewall, FortiClient Enterprise Management Server, FortiSandbox, DefendEdge SiON.

Переваги спільного рішення

1. Відстежує, ідентифікує та реагує на дії користувача
2. Розгортає швидкі засоби контролю безпеки для конкретних кінцевих користувачів
3. Виключає рівень некоректного виявлення в усіх мережевих активностях кінцевих користувачів.
4. Повний контроль доступу до реєстрації, передачі, припинення роботи.

Висновки до розділу 3

Організація може застосовувати штучний інтелект у різних місцях, чи то в глобальних дослідницьких лабораторіях, чи всередині організації, а також у різних місцях та етапах кіберланцюжка вбивств. Результати штучного інтелекту також можна застосовувати для виявлення або запобігання. Кожен підхід має свої переваги, а також обмеження, і організації повинні прорізати ажіотаж і гіперболу, щоб визначити поєднання підходів, які оптимальні для їхньої ситуації.

Це повинно включати поєднання кожного типу ШІ. Постачальник засобів безпеки організації повинен забезпечити широке охоплення загроз, типів розвідки. Це дає змогу розгорнутим засобам безпеки виявляти та блокувати загрози на ранній стадії кіберзагрози та перервати ланцюг.

Безпековий ландшафт загроз слід доповнювати продуктами безпеки, такими як AV наступного покоління, брандмауери веб-додатків(WAF), захищені шлюзи електронної пошти (SEG) і пісочниці з інтегрованим штучним інтелектом. Цей вбудований штучний інтелект часто дозволяє запобігти загрозам, характерним для організації, або раннє реагування на глобальні виклики.

Якщо це можливо, організація також повинна використовувати розширені системи виявлення та реагування, такі як виявлення кінцевих точок і відповідь (EDR), інформацію про безпеку та управління подіями (SIEM) і UEBA. Ці доповнення контролюють націлювання ранніх стадій ланцюга знищення, що забезпечує комплексне виявлення та реагування на атаки, які уникають запобіжного контролю.

Однак важливо, щоб групи безпеки були належним чином укомплектовані та кваліфіковані для ефективного реагування.

ВИСНОВКИ

У кваліфікаційній роботі проведено аналіз та практичне дослідження застосування штучного інтелекту в системах безпеки інтернету речей (IoT) для захисту від кібератак, що дало змогу узагальнити основну проблематику та сформувати наступні висновки.

Обгрунтовано необхідність розуміння потенціалу системного ризику в IoT, оскільки це може мати значні наслідки для громадської безпеки та глобальної безпеки, економічного добробуту, а також доведено концептуальну загрозу кібербезпеці для нових середовищ IIoT, що пов’язано з поширенням передового досвіду та нарощування потенціалу по всьому світу.

Підтверджена доцільність спостереження розвитку IIoT, що спровокувало надання рекомендацій ефективного захисту на основі технологій штучного інтелекту для додатків промислового Інтернету речей (IIoT), щоб створювати безпечніші, надійніші та стійкіші інфраструктури.

Акцентовано на важливості фізичної безпеки, уразливості мікропрограми та програмного забезпечення, автентифікації та механізмів контролю доступу на рівні пристрою.

Досліджено проблеми безпеки даних і конфіденційності, а також етичні міркування щодо прозорості та пояснюваності алгоритмів ШІ. Надано приклади використання в конкретних галузях і сценарії розгортання в реальному світі, щоб проілюструвати, як методи ШІ застосовуються для захисту систем IoT у різних доменах.

Розкрито поточні стандартизаційні та регулятивні зусилля щодо безпеки IoT, які охоплюють розробку інфраструктур безпеки IoT, галузевих стандартів, юридичні та нормативні міркування, а також рамки взаємодії та сертифікації. Оскільки IoT продовжує розвиватися та розширюватися, майбутні напрямки досліджень мають бути зосереджені на вирішенні нових проблем безпеки, вивченні нових методів штучного інтелекту та забезпеченні відповідального та

етичного використання штучного інтелекту в безпеці Інтернету речей.

Доведено, що прогресивні загрози швидко розвиваються, CISO повинні впроваджувати засоби контролю безпеки, які захищають дані, інтелектуальну власність і репутацію компанії як всередині, так і зовні. І вони повинні робити це, одночасно задовольняючи галузеві вимоги відповідності.

Запропоновано використання рішення компанії Fortinet для захисту від кібератак IoT на основі спільного рішення DefendEdge і Fortinet, щоб забезпечити організації дієвою аналітикою діяльності співробітників і допомогти приймати рішення щодо загроз у реальному часі. Власна платформа машинного навчання SiON дозволяє усуває помилкові спрацьовування під час пошуку загроз і дозволяє командам із кібербезпеки зосередитися на підтверджених індикаторах загрози.

Компоненти спільного рішення DefendEdge SiON Рішення SiON від DefendEdge — це корпоративна платформа, яка об’єднує та аналізує численні корпоративні джерела даних і надає можливість виконувати робочі процеси, визначені організацією на основі поведінки кінцевих користувачів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Foresight review of cyber security for the Industrial IoT. Enabling safer more resilient infrastructures. July 2020 Lloyd's Register Foundation Report Series: No.2020.1. URL: http://surl.li/udovm

2. Desai, N. (27 April 2016). IT vs. OT for the industrial internet – Two sides of the same coin? URL: https://www.globalsign.com/en/blog/it-vs-ot-industrial-internet

3. Leal-Ayala, D; Castañeda-Navarrete, J; Carlos López-Gómez, C. (2019). OK computer? The safety and security dimensions of Industry 4.0. University of Cambridge. URL: https://www.ciip.group.cam.ac.uk/reports-and-articles/ok-computer-safety-and-securitydimensions-industr/download/OK_Computer.pdf

4. World Economic Forum (2020). The Global Risks Report 2020. http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf

5. World Economic Forum (2024). The Global Risks Report 2024. URL: http://surl.li/udovm

6. Securing the Internet of Things in Artificial Intelligence Era: A Comprehensive Survey / M. Humayun et al. *IEEE Access*. 2024. P. 1. URL: https://doi.org/10.1109/access.2024.3365634

7. Hanif M., H. Ashraf, Z. Jalil, N. Z. Jhanjhi, M. Humayun, S. Saeed, and A. M. Almuhaideb, "Ai-based wormhole attack detection techniques in wireless sensor networks," Electronics, vol. 11, no. 15, p. 2324, 2022.

8. Kalutharage C. S., X. Liu, C. Chrysoulas, N. Pitropakis, and P. Papadopoulos, "Explainable ai-based ddos attack identification method for IOT networks," Computers, vol. 12, no. 2, p. 32, 2023.

9. Bhardwaj A., F. Al-Turjman, M. Kumar, T. Stephan, and L. Mostarda, "Capturing-the-invisible (cti): Behavior-based attacks recognition in iot-oriented industrial control systems," IEEE access, vol. 8, pp. 104956–104 966, 2020.8

10. El Jaouhari S. and E. Bouvet, "Secure firmware over-the-air updates foriot: Survey, challenges, and discussions," Internet of Things, vol. 18, p.100508, 2022.

11. Sun D., J. Hu, H. Wu, J. Wu, J. Yang, Q. Z. Sheng, and S. Dustdar, "A comprehensive survey on collaborative data-access enablers in the iiot," ACM Comput. Surv., vol. 56, no. 2, sep 2023. [Online]. URL: https://doi.org/10.1145/3612918

12. Alwahedi F., A. Aldhaheri, M. A. Ferrag, A. Battah, andN. Tihanyi, "Machine learning techniques for iot security:Current research and future vision with generative ai and large language models," Internet of Things and Cyber-PhysicalSystems, vol. 4, pp. 167–185, 2024. [Online]. URL: https://www.sciencedirect.com/science/article/pii/S2667345223000585

13. Dhirani L. L., E. Armstrong, and T. Newe, "Industrial iot, cyber threats,and standards landscape: Evaluation and roadmap," Sensors, vol. 21, no. 11, p. 3901, 2021.

14. Leitão, S. Karnouskos, T. I. Strasser, X. Jia, J. Lee, and A. W. Colombo, "Alignment of the ieee industrial agents recommended practice standard with the reference architectures rami4. 0, iira, and sgam," IEEE Open Journal of the Industrial Electronics Society, vol. 4, pp. 98–111, 2023.

15. Dhoni P. and R. Kumar, "Synergizing generative ai and cybersecurity: Roles of generative ai entities, companies, agencies, and government in enhancing cybersecurity," Aug. 2023. [Online]. URL: http://dx.doi.org/10.36227/techrxiv.23968809.v1

16. Hassan T., M. Asim, T. Baker, J. Hassan, and N. Tariq, "Ctrust-rpl: A control layer-based trust mechanism for supporting secure routing in routing protocol for low power and lossy networks-based internet of things applications," Transactions on Emerging Telecommunications Technologies, vol. 32, no. 3, p. e4224, 2021.

17. Javed M., N. Tariq, M. Ashraf, F. A. Khan, M. Asim, and M. Imran, "Securing smart healthcare cyber-physical systems against blackhole and greyhole attacks using a blockchain-enabled gini index framework," Sensors, vol. 23, no. 23, p. 9372, 2023.

18. Hadzovic S., S. Mrdovic, and M. Radonjic, "A path towards an internetof things and artificial intelligence regulatory framework," IEEE Communications Magazine, vol. 61, no. 7, pp. 90–96, 2023.

19. Dixit P., P. Bhattacharya, S. Tanwar, and R. Gupta, "Anomaly detection in autonomous electric vehicles using ai techniques: A comprehensive survey," Expert Systems, vol. 39, no. 5, p. e12754, 2022.

20. Kipongo J., T. G. Swart, and E. Esenogho, “Design and implementation of intrusion detection systems using rpl and aovd protocols-based wireless sensor networks,” International Journal of Electronics and Telecommunications, pp. 309–318, 2023.

21. Yahyaoui A., H. Lakhdhar, T. Abdellatif, and R. Attia, “Machine learningbased network intrusion detection for data streaming iot applications,” in 2021 21st ACIS International Winter Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD-Winter). IEEE, 2021, pp. 51–56

22. Wong C. M. V., R. Y.-Y. Chan, Y. N. Yum, and K. Wang, “Internet of things (iot)-enhanced applied behavior analysis (aba) for special education needs,” Sensors, vol. 21, no. 19, p. 6693, 2021.

23. Zeadally S., A. K. Das, and N. Sklavos, “Cryptographic technologies and protocol standards for internet of things,” Internet of Things, vol. 14, p. 100075, 2021.

24. Bettayeb S., M.-L. Messai, and S. M. Hemam, “A robust and efficient vector-based key management scheme for iot networks,” Ad Hoc Networks, vol. 149, p. 103250, 2023.

25. Meddeb H., Z. Abdellaoui, and F. Houaidi, “Development of surveillance robot based on face recognition using raspberry-pi and iot,” Microproces- sors and Microsystems, vol. 96, p. 104728, 2023.

26. Spachos P., S. Gregori, and M. J. Deen, “Voice activated iot devices for healthcare: Design challenges and emerging applications,” IEEETransactions on Circuits and Systems II: Express Briefs, vol. 69, no. 7, pp. 3101–3107, 2022.

27. Martey A. S., A. Ali, and E. Ebenezer, “Ai-based palm print recognition system for high-security applications,” in 2023 IEEE AFRICON. IEEE, 2023, pp. 1–6.

28. Annadurai C., I. Nelson, K. N. Devi, R. Manikandan, N. Jhanjhi, M. Masud, and A. Sheikh, “Biometric authentication-based intrusion detectionusing artificial intelligence internet of things in smart city,” Energies, vol. 15, no. 19, p. 7430, 2022.

29. Guo J., A. Liu, K. Ota, M. Dong, X. Deng, and N. N. Xiong, “Itcn: Anintelligent trust collaboration network system in iot,” IEEE transactionson network science and engineering, vol. 9, no. 1, pp. 203–218, 2021.

30. Rehman Z., N. Tariq, S. A. Moqurrab, J. Yoo, and G. Srivastava, “Ma-chine learning and internet of things applications in enterprise architectures: Solutions, challenges, and open issues,” Expert Systems, p. e13467, 2023.

31. Ayvaz S. and K. Alpay, “Predictive maintenance system for production lines in manufacturing: A machine learning approach using iot data in real-time,” Expert Systems with Applications, vol. 173, p. 114598, 2021.

32. Montasari R., F. Carroll, S. Macdonald, H. Jahankhani, A. Hosseinian-Far, and A. Daneshkhah, “Application of artificial intelligence and machine learning in producing actionable cyber threat intelligence,” Digital Forensic Investigation of Internet of Things (IoT) Devices, pp. 47–64, 2021.

33. Samtani S., Y. Chai, and H. Chen, “Linking exploits from the dark web to known vulnerabilities for proactive cyber threat intelligence: Anattention-based deep structured semantic model1,” MIS quarterly, vol. 46, no. 2, 2022.

34. . Chen M and W. Du, “The predicting public sentiment evolution on public emergencies under deep learning and internet of things,” The Journal of Supercomputing, vol. 79, no. 6, pp. 6452–6470, 2023.

35. Tomar D., “A network architecture for secure traffic management for the internet of things using virtual local area network,” International Journal of Computer Trends and Technology, vol. 68, pp. 11–14, 2020.

36. Pattewar G., N. Mahamuni, H. Nikam, O. Loka, and R. Patil, “Management of iot devices security using blockchain—a review,” Sentimental Analysis and Deep Learning: Proceedings of ICSADL 2021, pp. 735–743, 2022.

37. Sambandam N., M. Hussein, N. Siddiqi, and C.-H. Lung, “Network security for iot using sdn: Timely ddos detection,” in 2018 IEEE Conference on Dependable and Secure Computing (DSC). IEEE, 2018, pp. 1–2.

38. Rajawat A. S., R. Rawat, K. Barhanpurkar, R. N. Shaw, and A. Ghosh,“Blockchain-based model for expanding iot device data security,” Advances in Applications of Data-Driven Computing, pp. 61–71, 2021.

39. Ragothaman K., Y. Wang, B. Rimal, and M. Lawrence, "Access control for IOT: A survey of existing research, dynamic policies and future directions," Sensors, vol. 23, no. 4, p. 1805, 2023.

40. Alyahya S., W. U. Khan, S. Ahmed, S. N. K. Marwat, and S. Habib, "Cyber secure framework for smart agriculture: Robust and tamper-resistant authentication scheme for iot devices," Electronics, vol. 11, no. 6, p. 963, 2022.

41. Ling Z., H. Yan, X. Shao, J. Luo, Y. Xu, B. Pearson, and X. Fu, "Secure boot, trusted boot and remote attestation for arm trustzone-based iot nodes," Journal of Systems Architecture, vol. 119, p. 102240, 2021.

42. Khalaf O. I., M. Sokiyna, Y. Alotaibi, A. Alsufyani, and S. Alghamdi, "Web attack detection using the input validation method: Dpda theory." Computers, Materials & Continua, vol. 68, no. 3, 2021.

43. Basati A., and M. M. Faghih, "Apae: an iot intrusion detection system using asymmetric parallel auto-encoder," Neural Computing and Applications, vol. 35, no. 7, pp. 4813–4833, 2023.

44. Kaur J., U. Garg, and G. Bathla, "Detection of cross-site scripting (xss) attacks using machine learning techniques: a review," Artificial Intelligence Review, pp. 1–45, 2023.

45. Tsaur W.-J., J.-C. Chang, and C.-L. Chen, "A highly secure iot firmware update mechanism using blockchain," Sensors, vol. 22, no. 2, p. 530, 2022.

46. Fatima A., T. A. Khan, T. M. Abdellatif, S. Zulfiqar, M. Asif, W. Safi, H. Al Hamadi, and A. H. Al-Kassem, "Impact and research challenges of penetrating testing and vulnerability assessment on network threat," in 2023 International Conference on Business Analytics for Technology and Security (ICBATS). IEEE, 2023, pp. 1–8.

47. Rak M., G. Salzillo, and D. Granata, "Esseca: An automated expert system for threat modelling and penetration testing for iot ecosystems,"computers and Electrical Engineering, vol. 99, p. 107721, 2022.

48. Rashid M., S. A. Parah, A. R. Wani, and S. K. Gupta, "Securing e-health IOT data on cloud systems using novel extended role based access control model," Internet of Things (IoT) Concepts and Applications, pp. 473–489, 2020.

49. Ameer S., J. Benson, and R. Sandhu, “An attribute-based approach toward a secured smart-home iot access control and a comparison with a role- based approach,” Information, vol. 13, no. 2, p. 60, 2022.

50. Henriques M. S. and N. K. Vernekar, “Using symmetric and asymmetriccryptography to secure communication between devices in iot,” in 2017 International Conference on IoT and Application (ICIOT). IEEE, 2017, pp. 1–4.

51. Goyal H. and S. Saha, “Multi-party computation in iot for privacy- preservation,” in 2022 IEEE 42nd International Conference on Distributed Computing Systems (ICDCS). IEEE, 2022, pp. 1280–1281.

52. Mohiyuddin A., A. R. Javed, C. Chakraborty, M. Rizwan, M. Shabbir, and J. Nebhen, “Secure cloud storage for medical iot data using adaptive neuro-fuzzy inference system,” International Journal of Fuzzy Systems, vol. 24, no. 2, pp. 1203–1215, 2022.

53. Kök, F. Y. Okay, Muyanlı, and S. Özdemir, “Explainable artificial intelligence (xai) for internet of things: A survey,” IEEE Internet of Things Journal, vol. 10, no. 16, pp. 14 764–14 779, 2023.

54. Kabir M. H., K. F. Hasan, M. K. Hasan, and K. Ansari, “Explainable artificial intelligence for smart city application: a secure and trusted platform,” in Explainable Artificial Intelligence for Cyber Security: NextnGeneration Artificial Intelligence. Springer, 2022, pp. 241–263.

55. Usmani U. A., A. Happonen, and J. Watada, “Human-centered artificial intelligence: Designing for user empowerment and ethical considerations,” in 2023 5th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). IEEE, 2023, pp. 01–05.

56. El-Haddadeh R., A. Fadlalla, and N. M. Hindi, “Is there a place for responsible artificial intelligence in pandemics? a tale of two countries,” Information Systems Frontiers, pp. 1–17, 2021.

57. Tjondronegoro D., E. Yuwono, B. Richards, D. Green, and S. Hatakka, “Responsible ai implementation: A human-centered framework for accelerating the innovation process,” arXiv preprint arXiv:2209.07076, 2022.

58. Tsiknas K., D. Taketzis, K. Demertzis, and C. Skianis, “Cyber threats to industrial iot: a survey on attacks and countermeasures,” IoT, vol. 2, no. 1, pp. 163–186, 2021.

59. Priya N., “Cybersecurity considerations for industrial iot in critical infrastructure sector,” International Journal of Computer and Organization Trends, vol. 12, no. 1, pp. 27–36, 2022

60. Nath M. D. and T. Bhattasali, “Anomaly detection using machine learning approaches,” Azerbaijan Journal of High Performance Computing, vol. 3,no. 2, pp. 196–206, 2020

61. Jelinek T., A. Bhave, N. Buchoud, M. M. Bühler, P. Glauner, O. Inder- wildi, M. Kraft, C. Mok, K. Nübel, and A. Voss, “International collaboration: Mainstreaming artificial intelligence and cyberphysical systems for carbon neutrality,” IEEE Transactions on Industrial Cyber-Physical Systems, 2024.

62. Atsu F. and P. S. Adams, “New insights in the ict and environmental degradation: Accounting for policy uncertainty and ict quality,” URL at SSRN 4688541.

63. Wu G., X. Chen, Y. Shen, Z. Xu, H. Zhang, S. Shen, and S. Yu, “Combining lyapunov optimization with actor-critic networks for privacy-aware iiot computation of loading,” IEEE Internet of Things Journal, 2024.

64. AI-DRIVEN CYBER CRIME PUTS NETWORK ENGINEERING IN THE HOT SEAT. https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-ai-driven-cybercrime.pdf

65. Applying Artificial Intelligence to Cybersecurity Beyond the Hype. URL:https://www.fortinet.com/content/dam/fortinet/assets/ebook/eb-applying-artificial-intelligence-to-cybersecurity.pdf

66. Fortinet and DefendEdge Security Solution. URL: https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-fortinet-and-defendedge-security-solution.pdf

67. Humayun M.et al Securing the Internet of Things in Artificial Intelligence Era: A Comprehensive Survey /. IEEE Access. 2024. P. 1. URL: https://doi.org/10.1109/access.2024.3365634