

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ**  
**«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ**  
**імені ІГОРЯ СІКОРСЬКОГО»**  
**ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ**  
Кафедра інформаційної безпеки

«На правах рукопису»

УДК 004.056

«До захисту допущено»

В.о. завідувача кафедри

\_\_\_\_\_ М.В.Грайворонський

“ \_\_\_\_ ” \_\_\_\_\_ 2019 р.

**Магістерська дисертація**  
**на здобуття ступеня магістра**

зі спеціальності: 125 Кібербезпека

на тему: Політика безпеки для промислового Інтернету речей та оцінка її дієвості

Виконав (-ла): студент (-ка) 2 курсу, групи ФБ-81мп  
(шифр групи)

Кисіль Віктор Юрійович \_\_\_\_\_  
(прізвище, ім'я, по батькові) (підпис)

Науковий керівник к.т.н., доц. Стьопочкіна Ірина Валеріївна \_\_\_\_\_  
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Рецензент \_\_\_\_\_  
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації  
немає запозичень з праць інших авторів без  
відповідних посилань.

Студент \_\_\_\_\_  
(підпис)

Київ – 2019 року

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ**  
**«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ**  
**імені ІГОРЯ СІКОРСЬКОГО»**  
**ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ**  
Кафедра інформаційної безпеки

Рівень вищої освіти – другий (магістерський) за освітньо-професійною програмою  
Спеціальність (освітньо-професійна програма) – 125 Кібербезпека («Системи, технології та математичні методи кібербезпеки»)

ЗАТВЕРДЖУЮ

В.о. завідувача кафедри

\_\_\_\_\_ М.В.Грайворонський  
(підпис)

« \_\_\_\_ » \_\_\_\_\_ 2019 р.

**ЗАВДАННЯ**  
**на магістерську дисертацію студенту**

Кисілю Віктору Юрійовичу

(прізвище, ім'я, по батькові)

1. Тема дисертації Політика безпеки для промислового Інтернету речей та оцінка її дієвості \_\_\_\_\_

науковий керівник дисертації к.т.н., доц. Стьопочкіна Ірина Валеріївна \_ ,

\_\_\_\_\_ ,  
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від « \_\_\_\_ » \_\_\_\_\_ 2019 р. № \_\_\_\_\_

2. Термін подання студентом дисертації 10.12.2019 р.

3. Об'єкт дослідження \_\_\_\_\_  
\_\_\_\_\_

4. Вихідні дані \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

5. Перелік завдань, які потрібно розробити \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

6. Орієнтовний перелік ілюстративного матеріалу \_\_\_\_\_

\_\_\_\_\_

7. Орієнтовний перелік публікацій \_\_\_\_\_

\_\_\_\_\_

8. Дата видачі завдання \_\_\_\_\_

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка

Студент

\_\_\_\_\_  
(підпис)

\_\_\_\_\_  
(ініціали, прізвище)

Науковий керівник дисертації

\_\_\_\_\_  
(підпис)

\_\_\_\_\_  
(ініціали, прізвище)

## РЕФЕРАТ

Робота обсягом 130 сторінок містить 35 ілюстрацій, 35 таблиць, 6 літературних посилань та 2 додатки.

Метою даної кваліфікаційної роботи є розробка загального каркасу та конкретних рішень політики безпеки типової мережі промислового Інтернету речей та розробка методики оцінки дієвості політики.

Об'єктом дослідження є промисловий Інтернет речей.

Предметом дослідження є склад політики безпеки, яка призначена для попередження та зменшення ризиків притаманних мережам промислового Інтернету речей та методи оцінювання дієвості політики безпеки.

Результати роботи викладені у вигляді опису розробленої політики безпеки, створенні нової методики для оцінки дієвості політики безпеки, використанні регресійної моделі для оцінки зменшення ризиків проведення типових атак на промисловий IoT задля забезпечення безпеки мереж цього типу та кодів програмного модуля, який реалізує відповідну методику оцінки.

Методи дослідження: ознайомлення та опрацювання літератури, що представлено монографічними та журнальними матеріалами, електронними ресурсами, які стосуються досліджуваної теми, аналіз різних вразливостей та атак на промисловий IoT, структурування одержаних результатів.

Результати роботи можуть бути використані при побудові захищених мереж промислового IoT.

Ключові слова: Internet of Things, політика безпеки, регресійна модель, атака, вразливість, промисловий Інтернет речей, ризик.

## ABSTRACT

The work volume 130 pages contains 35 illustrations, 35 tables, 6 literary references and 2 appendices.

The purpose of this qualification work is development a common framework and specific security policy solutions for a typical Industrial Internet of Things network and development a method for evaluating policy effectiveness.

The object of research is the Industrial Internet of Things.

The subject of research is the composition of a security policy designed to prevent and reduce the risks inherent in the Industrial Internet of Things networks and methods for evaluating the effectiveness of security policy.

The results of the work are presented in the form of a description of the security policy developed, creating a new method for evaluating the effectiveness of security policy, the use of a regression model to reduce the risk of typical attacks on industrial IoT to ensure the security of networks of this type and program module codes that implements the appropriate assessment method.

Research methods: familiarization and processing of the literature, represented by monographic and journal materials, electronic resources related to the topic under study, analysis of various vulnerabilities and attacks on industrial IoT, structuring the results.

The results of the work can be used in the construction of secure networks of industrial IoT.

Keywords: Internet of Things, security policy, regression model, attack, vulnerability, Industrial Internet of Things, risk.

## ЗМІСТ

Перелік умовних позначень, символів, одиниць, скорочень і термінів .....	8
Вступ.....	11
1 Існуючі рішення у напрямі захисту пристроїв Інтернету речей.....	14
1.1 Розгляд типової архітектури IoT .....	14
1.2 Типові атаки на IoT .....	18
1.3 Існуючі програмні рішення із захисту промислового IoT .....	20
1.4 Існуючі апаратні рішення із захисту промислового IoT .....	21
Висновки до розділу 1 .....	25
2 Розробка моделі політики безпеки для промислового Інтернету речей.....	26
2.1 Аналіз таксономії загроз для промислового IoT .....	26
2.2 Обчислення ризиків при реалізації загроз для промислового Інтернету речей .....	44
2.3 Опис складових політики безпеки (описово).....	46
Висновки до розділу 2 .....	53
3 Методика оцінки дієвості політики безпеки.....	54
3.1 Критерії дієвості політики безпеки .....	54
3.2 Імплементация політики безпеки через засіб моделювання мережі IoT.....	55
3.3 Оцінка дієвості політики безпеки та прогнозування ризиків (на основі простої лінійної регресійної моделі).....	69
3.4 Модель прогнозування ризиків з використанням множинної регресії .....	80
3.5 Тестування на проникнення для IIoT .....	84
3.6 Оцінювання дієвості політики безпеки з використанням критеріїв по їх важливості.....	88
Висновки до розділу 3 .....	92
4 Стартап .....	94
4.1 Опис ідеї проекту .....	94
4.2 Технологічний аудит ідеї проекту.....	96
4.3 Аналіз ринкових можливостей запуску стартап-проекту.....	98
4.4 Розроблення ринкової стратегії проекту .....	106

4.5 Розроблення маркетингової програми стартап-проекту .....	110
Висновки до розділу 4 .....	115
Висновки .....	116
Перелік джерел посилання .....	118
Додатки.....	119
Додаток А.....	120
Програмний код застосунку для оцінки дієвості політики безпеки з використанням простої лінійної регресії.....	120
Додаток Б.....	127
Програмний код застосунку для оцінки дієвості політики безпеки з використанням множинної регресії.....	127

## **ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ**

ІТ – Інформаційні технології;

ОТ – Операційні технології;

ПЗ – Програмне забезпечення;

ARP – Address Resolution Protocol;

CRM – Customer Relationship Management;

CVSS – Common Vulnerability Scoring System;

DCS – Distributed Control Systems;

DDoS – Distributed Denial of Service;

DIS – Destination Oriented Directed Acyclic Graph Information Solicitation;

DMZ – Demilitarized Zone;

DODAG – Destination Oriented Directed Acyclic Graph;

DoS – Denial of Service;

ERP – Enterprise Resource Planning;

GDPR – General Data Protection Regulation;

IAM – Identity and Access Management;

ICMP – Internet Control Message Protocol;

IDS – Intrusion Detection System;

IIoT – Industrial Internet of Things;

IoT – Internet of Things;



IPS – Intrusion Prevention System;

MES – Manufacturing Execution System;

OSI – Open System Interconnection;

PAM – Privilege Access Management;

PLC – Programmable Logic Controller;

RFID – Radio Frequency Identification;

RPL – Routing Protocol for Low-Power and Lossy Networks;

RTU – Remote Terminal Unit;

SCADA – Supervisory Control And Data Acquisition;

SIEM – Security Information and Event Management;

SNMP – Simple Network Management Protocol;

SOC – Security Operation Center;

TLS – Transport Layer Security;

VLAN – Virtual Local Area Network;

WSAN – Wireless Sensor and Actuator Network;

WSN – Wireless Sensor Network.

Атака — певна послідовність дій, які, в разі успіху, призведуть до порушення безпеки інформації. Також атака – реалізація певної загрози.

Загроза — подія, яка може спричинити порушення політики безпеки інформації або нанесення збитків інформаційно-комунікаційній системі.

Зловмисник — фізична особа, яка умисно порушує політику безпеки.

API (англ. Application Programming Interface) – опис процедур, структур даних, методів за допомогою яких одна програма може взаємодіяти з іншою.

M2M (англ. Machine-to-Machine) – загальна назва технологій для взаємодії машин, тобто, обміну інформацією в односторонньому або в двосторонньому порядку.

Wi-Fi (англ. Wireless Fidelity) – високоточні бездротові технології передачі даних, які представляють собою набір стандартів передачі цифрових потоків даних по радіоканалам.

## ВСТУП

У зв'язку з швидким розвитком мереж Інтернету речей та зручністю їх використання люди все частіше надають їм перевагу у виборі при підключенні до мережі Інтернет.

Інтернет речей (англ. Internet of Things, IoT) – це способи взаємодії фізичних об'єктів, пристроїв і систем між собою і з навколишнім світом із застосуванням різних технологій зв'язку і стандартів з'єднання.

Будь-який пристрій Internet of Things є вразливим. Персональні дані, зібрані IoT-пристроями, завжди мають цінність для хакерів і викрадачів ідентифікаційної інформації. Крім того, кібератака на IoT-пристрої потенційно здатна завдати шкоди фізичним пристроям і об'єктам критичної інфраструктури.

Тому дуже важливо вміти вчасно виявляти різні вразливості й атаки на пристрої IoT, а саме на промисловий IoT.

**Актуальність роботи** зумовлюється тим, що на даний час немає ідеальних рішень для захисту пристроїв промислового IoT, для цієї сфери характерна велика кількість нових загроз. Завдяки цьому політика безпеки може багаторазово змінюватись і вдосконалюватись, і актуальним завданням є оцінка дієвості наявного варіанту та визначення того, чи буде оновлений варіант політики кращим, на основі об'єктивних критеріїв.

**Метою роботи** є розробка загального каркасу та конкретних рішень політики безпеки типової мережі промислового Інтернету речей та розробка методики оцінки дієвості політики.

**Завдання, які були поставлені** при виконанні даної роботи:

- 1) Аналіз архітектури мереж промислового Інтернету речей та найбільш розповсюджених атак на них;

- 2) Побудова моделі загроз для промислового Інтернету речей та виділення найбільш значних ризиків;
- 3) Опис каркасу політики безпеки для промислового IoT.
- 4) Вибір способу моделювання політики безпеки обраної мережі для оцінки її недоліків та переваг.
- 5) Розробка критеріїв дієвості політики безпеки;
- 6) Розробка методики оцінки ступеню дієвості політики безпеки, що заснована на критеріях 5);
- 7) Розробка програмного модуля, який автоматизує методику 6).

**Об'єктом дослідження** є промисловий Інтернет речей.

**Предметом дослідження** є склад політики безпеки, яка призначена для попередження та зменшення ризиків притаманних мережам промислового Інтернету речей та методи оцінювання дієвості політики безпеки.

**Методами дослідження** є ознайомлення та опрацювання літератури, що представлено монографічними та журнальними матеріалами, електронними ресурсами, які стосуються досліджуваної теми, аналіз різних вразливостей та атак на промисловий IoT, структурування одержаних результатів.

**Наукова новизна:** розроблена методика відрізняється від існуючих орієнтацією на промислові мережі з IoT пристроями, комплексністю врахування поточного та прогнозованого стану ризиків, і дозволяє оцінити дієвість політики безпеки за наявності регулярного аудиту загроз безпеки в мережах IoT. Методика включає в себе такі 7 критеріїв:

- 1) Спад прогнозованих значень основних ризиків;
- 2) Наявність кореляції між фінансовими вкладеннями в покращення захисту, вдосконаленням політики безпеки та значеннями ризиків;
- 3) Відповідність середньому рівню та вище, за чеклістами вимог безпеки;
- 4) Наявність успішних результатів моделювання майбутніх запроваджень політики безпеки (цей критерій застосовується для політик, які

використовуються уперше і ще не імплементовані повністю на реальному об'єкті);

- 5) Результати тестування на проникнення;
- 6) Виконання організаційних заходів із забезпечення політики безпеки, ініційованих вищим менеджментом;
- 7) Застосування шаблонів безпеки.

Ці критерії було зважено по важливості по методу Сааті за шкалою від 1 до 5. Використано методику обчислення приналежності рівня дієвості політики безпеки до нечітких множин: «не дієва», «не достатньо дієва», «достатня (середня) дієвість», «суттєво дієва», «ефективно діюча».

**Практичним значенням отриманих результатів** є створення політики безпеки спеціально для промислового IoT та створення нової методики для оцінювання дієвості політики безпеки. Результати можуть бути запроваджені в практиці керування безпекою пристроїв промислового IoT.

**Апробація результатів роботи:** результати оприлюднено на II Міжнародній науково-практичній конференції «Наука, технології, інновації: світові тенденції та регіональний аспект» (27-28 вересня 2019 р., м. Одеса).

**Публікації:** результати магістерської дисертації опубліковані у статті «Розробка політики безпеки для систем керування промисловими процесами».

# 1 ІСНУЮЧІ РІШЕННЯ У НАПРЯМІ ЗАХИСТУ ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ

## 1.1 Розгляд типової архітектури IoT

Інтернет речей (IoT) – це новітня технологія, яка фокусується на взаємозв'язку між речами або пристроями один з одним і людьми або користувачами для досягнення деяких спільних цілей. IoT забезпечується багатьма існуючими технологіями, такими як Wireless sensor and actuator networks (WSAN) і радіочастотна ідентифікація (RFID). Ідея Інтернету речей була вперше запропонована Кевіном Ештоном з Auto ID-Center MIT [1]. Відповідно до широкої доступності Інтернету у вигляді Wi-Fi, послуги мобільних мереж передачі даних (3G, 4G LTE), нові дослідження вже очевидні. Очікується, що кількість підключених пристроїв значно збільшиться, досягнувши число між 50 і 100 мільярдами до 2020 року [2]. Ця велика кількість підключених пристроїв буде призводити до повсюдного зондування та широкої доступності послуг. У парадигмі IoT інформаційно-комунікаційні системи будуть безперешкодно вбудовані у наше середовище. IoT є невід'ємною частиною розвитку розумних будинків, розумних міст та розумної системи охорони здоров'я. IoT буде широко прийнятий, якщо він завоює довіру користувача, забезпечуючи міцну безпеку та конфіденційність.

Безпека IoT - одна з найактуальніших наукових тем сьогодні. Багато дослідників по всьому світу використовують свої зусилля для вирішення різних проблем безпеки в IoT. Однак безпека IoT є великим викликом через свою неоднорідність. В Інтернеті є поєднанням багатьох технологій, усі ці технології мають свої традиційні вади безпеки та конфіденційності, які слід вирішувати в контексті IoT. Інфраструктура IoT дуже схильна до відомих атак на безпеку, таких як відмова в обслуговуванні (DoS), атаки повторення, людина посередині,

клонування речей, підслуховування та атака маршрутизації визначені в [4]. Атамлі та ін. [5] класифікують деякі кібер-атаки, характерні для IoT, такі як підроблення пристрою, порушення конфіденційності, розголошення інформації, DoS (відмова в обслуговуванні), підроблення, введення сигналу та атака по побічним каналам. Пристрої IoT обмежені в ресурсах, та існуючі рішення криптографічної безпеки не можуть бути застосовані до цих пристроїв, що робить їх схильним до проблем цілісності та конфіденційності даних. Окрім впливу на DoS-атаки, три властивості безпеки, тобто конфіденційність, цілісність та доступність, важко досягти. Аутентифікація пристрою та механізм контролю доступу також є головною проблемою безпеки в IoT. Проблеми з аутентифікацією та контролем доступу в IoT пояснюються великою кількістю пристроїв і машин до машини (M2M) характером зв'язку IoT.

Інтернет речей має широкий спектр застосувань, таких як розумний дім, розумні міста, розумна система охорони здоров'я, розумні світлофори, підключені транспортні засоби, розумне середовище моніторингу в галузях промисловості, розумних лічильників, моніторинг водної мережі та розумна логістика [3], [5] та багато іншого. Область застосування IoT не обмежується вищезгаданими прикладами.

Інтернет речей буде формувати світ найближчим часом і буде приносити затишок у життя людини. Однак його безпека дуже важлива і складна через його неоднорідну природу, широке розгортання, обмежені ресурсами вузли та генерацію величезної кількості даних щосекунди. Архітектура IoT-мереж складається з 4 рівнів [6], як показано на рисунку 1.1. Однак це не стандартна архітектура для IoT, більшість запропонованих архітектур мають ці рівні. Тому ми взяли цю архітектуру як орієнтовну архітектуру для виявлення та класифікації різних проблем з безпекою в IoT. На рисунку 1.1 показано найбільш широко прийняту IoT архітектуру. Далі будуть наведені ці рівні.

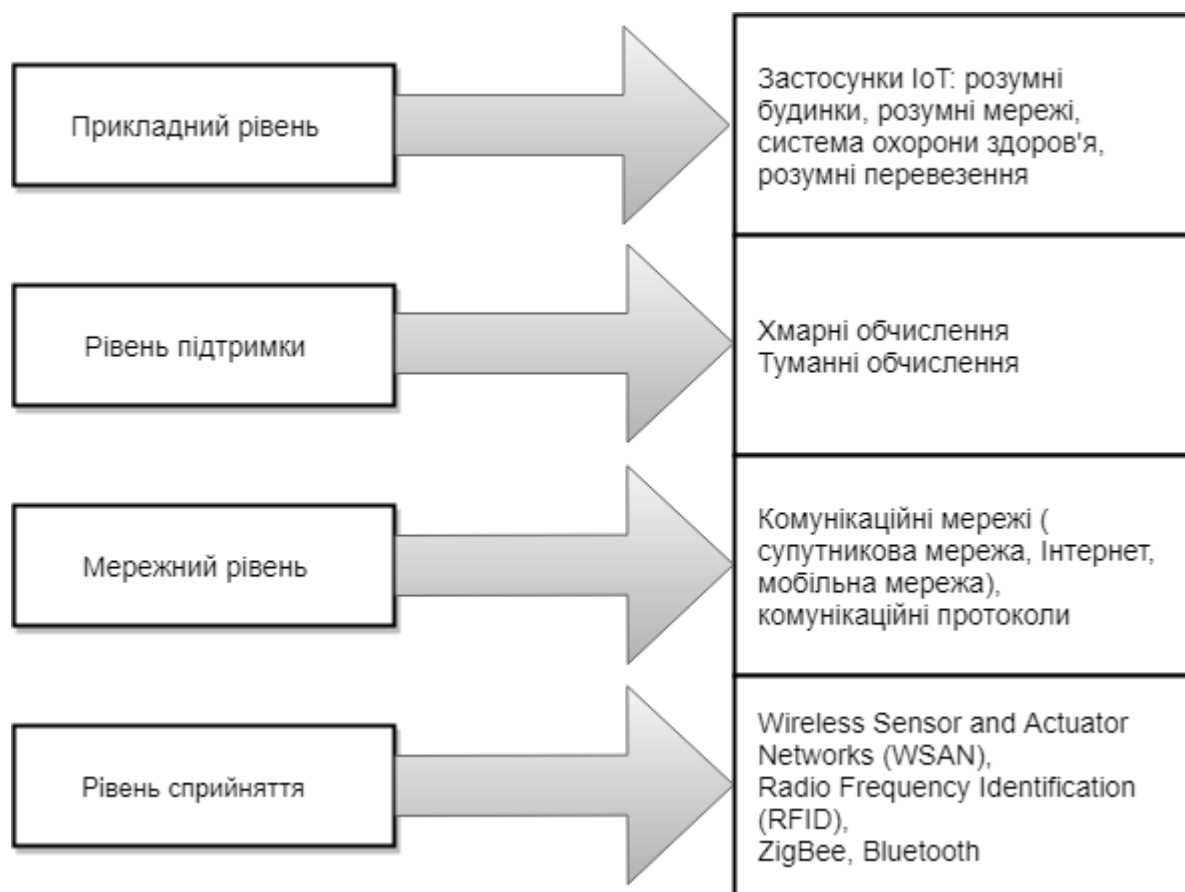


Рисунок 1.1 – Типова архітектура Інтернету речей

### 1.1.1 Рівень сприйняття

Цей рівень складається з таких пристроїв, як сенсори та радіочастотні ідентифікатори, що фіксують будь-яке фізичне явище реального світу, за допомогою міток RFID, стан погоди та рівень води в галузі сільського господарства. Бездротові мережі сенсорів і датчиків (WSAN) та радіочастотна ідентифікація (RFID) є ключовими елементами цього рівня.



### **1.1.2 Мережний рівень**

Цей рівень надійно передає інформацію, зібрану сенсорами пристроїв рівня сприйняття для «туманних» вузлів, головної хмари або безпосередньо в інший вузол IoT. При цьому різними технологіями на цьому рівні є мобільні мережі, супутникові мережі, бездротова Ad hoc мережа та багато захищених протоколів обміну даними, що використовуються в цих технологіях.

### **1.1.3 Рівень підтримки**

Рівень підтримки забезпечує підходящу та ефективну платформу для IoT застосунків. Різні IoT застосунки можна розмістити в «туманних» вузлах або в основній хмарі та вони будуть доступні через Інтернет через пристрої з обмеженими ресурсами. Він забезпечує місце зберігання та обчислювальну потужність для пристроїв з обмеженими ресурсами.

### **1.1.4 Прикладний рівень**

Цей рівень надає користувачам послуги Інтернету речей відповідно до їх потреб. Користувачі можуть отримати доступ до різних сервісів за допомогою інтерфейсу прикладного рівня. Різними застосунками є розумні будинки, розумна система охорони здоров'я, розумний транспорт, розумне сільське господарство, автоматизовані транспортні засоби та інше.

## 1.2 Типові атаки на IoT

Окрім величезної важливості та широкого застосування IoT, непросто розгорнути його в критичних областях застосування, де безпека та конфіденційність є найважливішими проблемами. Для прикладу, успішна атака на безпеку розумної системи охорони здоров'я може призвести до втрати багатьох життів пацієнтів, хоча це також може спричинити фінансові втрати та втрату людських життів у випадку розумної транспортної системи. Безпека IoT – це складна область і потребує подальшої науково-дослідної роботи, щоб впоратися з цими викликами.

На рисунку 1.2 зображені ці проблеми та можливі атаки на Інтернет речей.

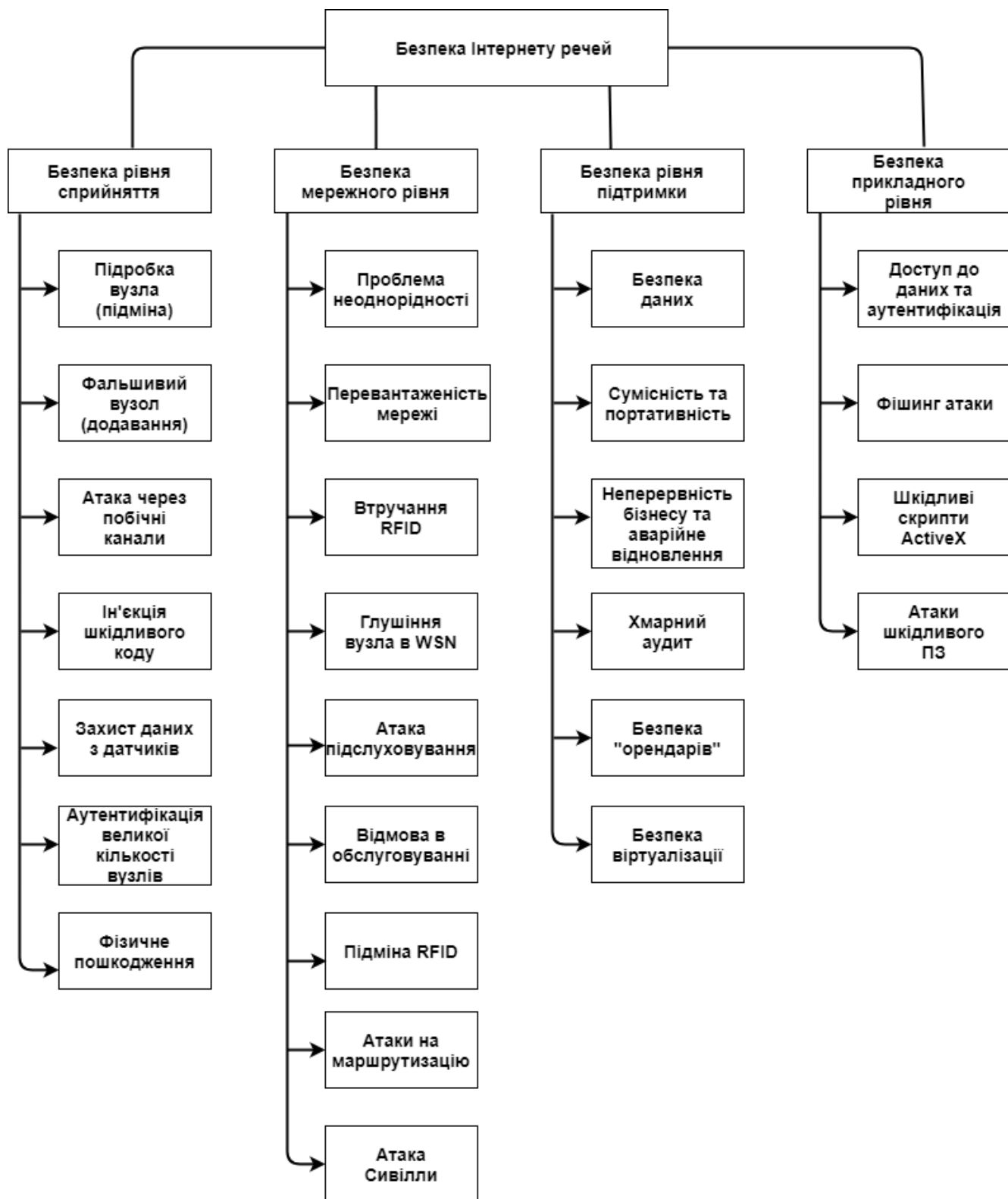


Рисунок 1.2 – Безпека та атаки на IoT

### 1.3 Існуючі програмні рішення із захисту промислового IoT

#### **Symantec Critical System Protection**

Продукт для захисту критичної системи Symantec версії 5.2.6 захищає від фізичного та віртуального простоїв на сервері за допомогою виявлення та запобігання на основі політики. Впроваджуйте гнучкі засоби контролю проти відомих і невідомих уразливостей, що впливають на ваші критичні системи. Використовуйте брандмауер, заснований на поведінці та вразливості, запобіганні вторгнень та управління застосунками та пристроями для захисту від атак нульового дня, зміцнення систем та підтримки відповідності. Централізована консоль управління дозволяє адміністраторам налаштовувати та підтримувати політики безпеки, керувати користувачами та ролями, переглядати сповіщення та запускати звіти в неоднорідних операційних системах.

Critical System Protection пропонує гнучку безпеку сервера, яка контролює поведінку користувачів та застосунків, блокує невідповідний мережевий трафік та події та забезпечує підходи, засновані на політиці без підпису, для розміщення навантажень сервера на основі різноманітних профілів сервера.

Поведінкою системи можна керувати, запобігаючи специфічним діям, які програма чи користувач може вчинити та перевіряти системні процеси, файли, дані журналу та критичні налаштування щодо невідповідної діяльності. Critical System Protection сприяє виконанню відповідності дотримання вимог, надаючи вичерпні аудиторські докази за допомогою зведених журналів подій, аналізу та звітності. Critical System Protection – це вичерпне рішення для безпеки сервера. Основна архітектура рішення наведена на рисунку 1.3.

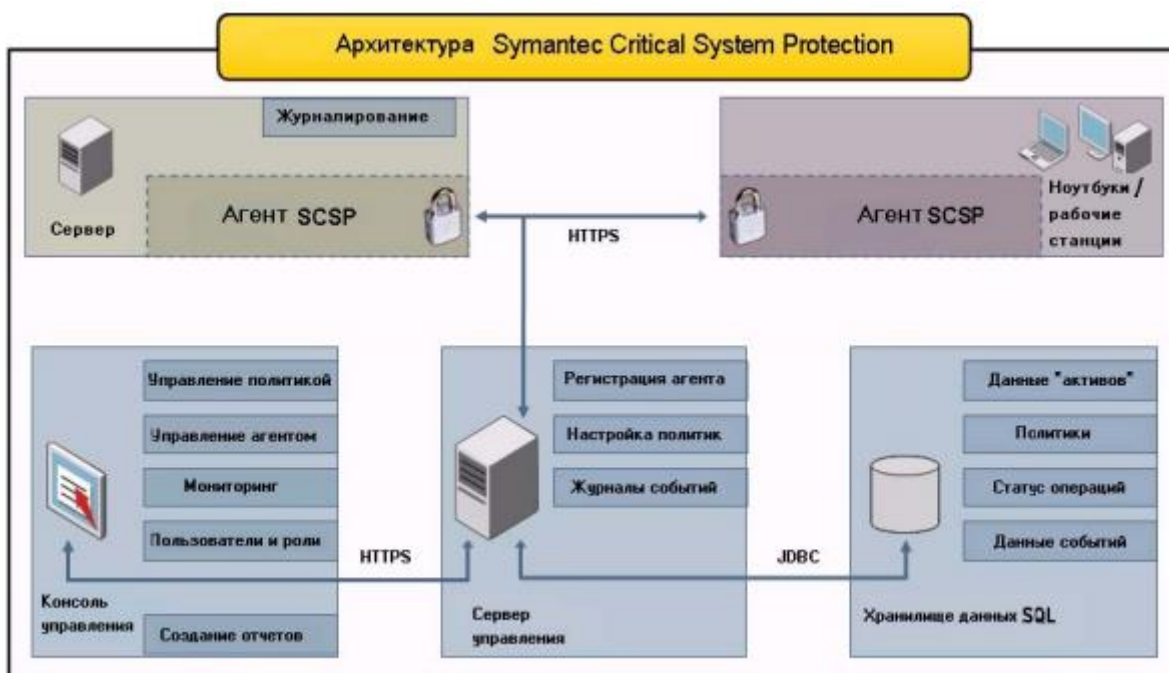


Рисунок 1.3 – Архітектура Symantec Critical System Protection

## 1.4 Існуючі апаратні рішення із захисту промислового IoT

### Cisco IPS Industrial Control Protection

Захист об'єктів критичної інфраструктури є вузькоспеціалізованою галуззю безпеки мережі, і наслідки відмови можуть бути критичними. Технологія Cisco IPS забезпечує набір ліцензійних підписів, написаних досвідченими фахівцями промислового IoT для безпечного огляду та захисту цих критичних мережевих комунікацій.

#### Огляд IPS

Датчики IPS Cisco забезпечують високоефективне інтелектуальне виявлення з точністю відповіді, що розширює можливості IPS від кінцевої точки мережі до центру обробки даних як для мереж IPv4, так і для IPv6.

## Інтелектуальне виявлення

Датчики IPS Cisco точно визначають, класифікують та зупиняють шкідливий трафік, перш ніж це вплине на ваш бізнес.

- Технологія Cisco IPS розроблена для запобігання зловмисній діяльності протягом усього життєвого циклу атаки та на всіх рівнях стеку застосунків.

- Створений на основі сучасних систем безпеки Cisco та мережевої розвідки, модульні можливості перевірки можуть виявляти та запобігати загрозам для всього стека мережі, від Address Resolution Protocol (ARP) до складних застосунків корпоративного рівня. Технологія Cisco IPS захищає від розширених обходів застосунків і може нормалізувати навіть найбільш фрагментований мережевий трафік.

- Технологія Cisco IPS забезпечує адаптивну вразливість та виявлення аномалії. Cisco зосередив свої підписи на потенційному зловживанні вразливостями, тож ваша здатність виявляти загрози залишається недоторканою навіть у випадку зміни експлойтів. Якщо виникають загрози нульового дня, датчик IPS Cisco дізнається про вашу мережу, виявляє як протокольні, так і поведінкові аномалії, а також зменшує атаки без оновлення підпису.

- Завдяки глобальній кореляції Cisco очолив галузь IPS у використанні каналів репутації. Глобальна інформація про загрозу перетворюється на діючу інформацію, таку як результати репутації, а також може використовуватися для чорного списку та стимулювання динамічних реакцій на загрозу.

Промислове обладнання та системи управління відрізняються між галузями, але мають дещо спільне. Протоколи, подібні в індустріальному просторі, можуть містити вразливості, які є повсюдними, тоді як деякі продукти постачальників можуть бути пропрієтарними або можуть впроваджувати стандарти унікальним чином. Результатом є потреба як у галузевих, так і в загальних захистах платформ.

Набір підписів захисту промислового контролю Cisco включає сукупність загальних детекторів протоколів SCADA та конкретних ідентифікаторів, які адресують інструменти та середовища, загальні для більшості керованих пристроїв.

Як показано на рисунку 1.4, правильне розміщення IPS в межах підприємства або мережі управління є критично важливим для захисту промислових систем в IT-інфраструктурі.

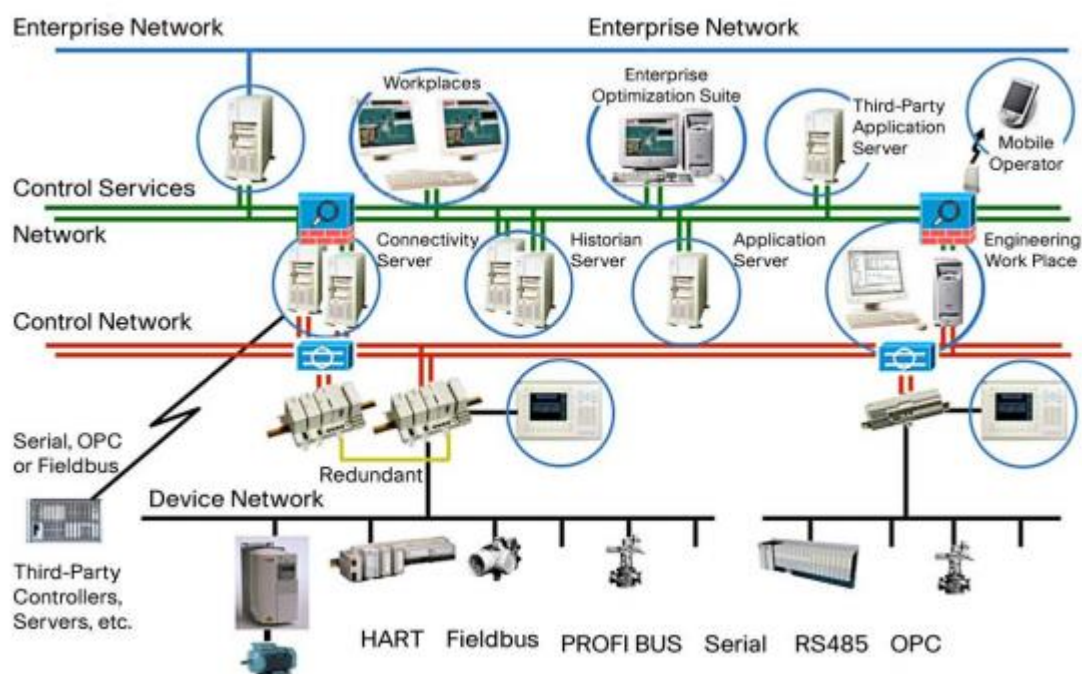


Рисунок 1.4 – Сценарій застосування Cisco IPS Industrial Control Protection

### IBM Proventia Network IPS

Мережева система запобігання вторгнень Proventia (IPS) автоматично блокує зловмисні атаки, зберігаючи пропускну здатність мережі та її доступність. Пристрої IPS Proventia Network є спеціалізованими мережевими пристроями захисту другого рівня, які можна розгорнути або на шлюзі, або в мережі для

блокування спроб вторгнення, атак відмови в обслуговуванні (DoS), шкідливого коду, бекдорів, шпигунських програм, не вимагаючи об'ємної конфігурації мережі.

Особливості систем запобігання вторгненням Proventia включають перевірені технології виявлення та запобігання, а також останні оновлення безпеки. Ці пристрої розуміють логічний потік і стан трафіку, в результаті чого забезпечується захист від мережевих загроз, включаючи трояни, бекдори та черв'яки.

IPS Proventia Network пропонує такі функції, щоб захистити вашу мережу від загроз:

- Динамічне блокування

IPS Proventia Network використовує ідентифікацію атак на основі вразливості, щоб забезпечити негайну та надійну блокуючу реакцію на небажаний трафік, одночасно дозволяючи легальному трафіку безперешкодно проходити. Тут застосовується процес глибокої перевірки руху, який використовує блокування на основі виявлення для зупинки як відомих, так і раніше невідомих атак.

- Правила брандмауера

Ви можете створити правила брандмауера, які дозволяють пристрою блокувати вхідні пакети з конкретних IP-адрес, номерів портів, протоколів або VLAN. Ці правила блокують багато атак, перш ніж вони впливають на вашу мережу.

- Автоматичне безпечне оновлення контенту на основі останніх досліджень безпеки

Ви можете автоматично завантажувати та активувати оновлений безпечний контент. Отримані вами оновлення безпеки є результатом постійних зобов'язань



IBM ISS X-Force Research and Development Team забезпечити найновіший захист від відомих і невідомих загроз.

- Карантин та блокування відповідей

Вбудовані пристрої використовують карантинну відповідь для блокування трафіку протягом певного часу після початкової атаки, і вони використовують блокуючу відповідь для блокування та скидання з'єднання, в якому відбувається подія, або для скидання пакета, який викликав подію.

- Захист через віртуальний Patch™

Можливість віртуального патчу Proventia забезпечує цінний буфер часу, виключаючи необхідність негайного виправлення всіх вразливих систем. Ви можете зачекати, поки ви не будете готові вручну оновлювати прилади або поки не відбудуться заплановані оновлення, а не необхідність виправлення та перезавантаження систем.

- Підтримка SNMP

Використовуючи пастки на основі SNMP, ви можете відстежувати ключові індикатори системних проблем або реагувати на безпеку чи інші події пристрою, використовуючи відповіді SNMP.

## **Висновки до розділу 1**

У даному розділі було розглянуто загальноприйняту архітектуру Інтернету речей, на зразок моделі OSI. Наведена архітектура включає в себе 4 основні рівні.

Було наведено основні проблеми безпеки для кожного з цих рівнів. Описано існуючі рішення у сфері захисту промислового IoT. Зокрема виділено актуальні програмні та апаратні рішення від найбільш передових компаній-розробників у світі.

## 2 РОЗРОБКА МОДЕЛІ ПОЛІТИКИ БЕЗПЕКИ ДЛЯ ПРОМИСЛОВОГО ІНТЕРНЕТУ РЕЧЕЙ

### 2.1 Аналіз таксономії загроз для промислового IoT

Розглянемо наступну класифікацію загроз для пристроїв Industrial IoT. Пропонується оцінювати імовірність виникнення загрози за шкалою від 0 до 1, а наслідки за шкалою від 1 до 5 (від дуже низького до дуже високого). Вони описані в таблиці 2.1. Також вказано, на які властивості інформації здійснюється вплив.

Таблиця 2.1 – Класифікація загроз для промислового IoT

Категорія	Загроза	Опис	На що впливає	Імовірність виникнення	Наслідки реалізації
1	2	3	4	5	6
Нечесна діяльність / Зловживання	Відмова в обслуговуванні	Атака відмови в обслуговуванні може бути двонаправленою. Вона може орієнтуватися на систему IoT, що призводить до недоступності системи та порушення виробництва, що спричинено	д	0.5	5

Продовження таблиці 2.1

1	2	3	4	5	6
		<p>великою кількістю запитів, надісланих до системи.</p> <p>З іншого боку, атакуючий може отримати перевагу у вигляді великої кількості пристроїв ПоТ в промисловому середовищі та створити «армію» ІоТ ботнетів як платформи для атаки на деякі інші системи.</p>			
	Шкідливе ПЗ	<p>Проникнення зловмисного програмного забезпечення в ПоТ, спрямоване на виконання небажаних та несанкціонованих дій, що може призвести до пошкодження системи ОТ, операційних процесів та</p>	к, ц, д, с	0.85	5

Продовження таблиці 2.1

1	2	3	4	5	6
		пов'язаних з ними даних. Вимагаюче ПЗ, віруси, троянські коні та шпигунські програми - поширені приклади цієї загрози.			
	Маніпуляція апаратним та програмним забезпеченням	Загроза несанкціонованого маніпулювання зловмисником програмного забезпечення пристроїв або застосунків у системі ОТ. Що стосується систем промислового IoT, дії зловмисника можуть включати маніпулювання промисловим роботом, маніпулювання віддаленим контролером пристроїв, що заглушають стан керуючого	к, ц, д, с	0.45	3

Продовження таблиці 2.1

1	2	3	4	5	6
		пристрою, та зміну його конфігурації.			
	Маніпуляція інформацією	Загроза зловмисником небажаної та несанкціонованої модифікації даних. Це може стосуватися компрометації ОТ або підтримуючих систем виробництва, таких як SCADA, MES, Historian-сервер та маніпуляції з обробкою даних. Можливі наслідки можуть включати невідповідні рішення, засновані на підроблених даних.	к, ц, д	0.35	4
	Націлені атаки	Загроза кібератаки, спрямованої на конкретну організацію (або конкретну особу в цій організації). Така атака	к, ц	0.4	3

Продовження таблиці 2.1

1	2	3	4	5	6
		<p>спрямована на заподіяння шкоди організації, можливо щоб взяти під контроль систему, використовуючи різні технічні засоби, такі як компрометація ключових пристроїв та фальсифікація телеметрії, що обманює необізнаних операторів. Інші наслідки включають пошкодження репутації або крадіжки секретів компанії. Коли ціль - компанія-виробник, зловмисник може, наприклад, спробувати вкрати формули чи рецепти і продати їх конкурентам. Зловмисник може</p>			

Продовження таблиці 2.1

1	2	3	4	5	6
		використовувати штучний інтелект, щоб виконати високо персоналізовану атаку з урахуванням вибраної групи людей чи окремих працівників. Ця атака відрізняється від широкомасштабних атак, метою яких є зараження будь-якої компанії, яка підключається до певного веб-сайту, підготовленого зловмисником, або будь-якої компанії, яка використовує пристрій або програмне забезпечення з певною вразливістю.			
	Зловживання персональними даними	Загроза компрометації особистої / конфіденційної	к, ц, д, с	0.5	3

Продовження таблиці 2.1

1	2	3	4	5	6
		інформації, що зберігається на пристроях або в хмарі. Мета зловмисника – отримати несанкціонований доступ до подібного роду даних та використовувати їх незаконним чином. У виробничих компаніях це може стосуватися імен та ролей користувачів систем ОТ. Дані про виробництво не вважаються предметом конфіденційності, але вони також можуть створювати проблеми, якщо вони можуть бути пов'язані з роботою окремих працівників.			
	Атака «грубої сили»	Загроза отримання несанкціонованого доступу до ресурсів	ц, д	0.67	3



Продовження таблиці 2.1

1	2	3	4	5	6
		організації (тобто даних, систем, пристроїв тощо) через велику кількість спроб відгадати правильний ключ або пароль. Організації Industry 4.0, які дозволяють використовувати прості або паролі за замовчуванням для промислових пристроїв та систем, можуть бути особливо вразливими до таких атак.			
Підслуховування / перехоплення / викрадення	Атака "людина посередині" / Викрадення сесії	Загроза активного підслуховування, коли зловмисники перехоплюють повідомлення, якими обмінюються між собою постраждалі сторони. Зловмисник може просто прослухати обмінювані	к, ц, д, с	0.47	4

Продовження таблиці 2.1

1	2	3	4	5	6
		повідомлення (наприклад, викрасти чутливу та конфіденційну інформацію компанії) або змінити чи видалити передану інформацію, що призведе до порушення обміну даними.			
	Викрадення даних протоколу зв'язку IoT	Загроза зловмиснику взяти під контроль існуючий сеанс зв'язку між двома мережевими компонентами, що може призвести до розкриття паролів та іншої конфіденційної інформації.	к, ц, д	0.6	3
	Мережева розвідка	Загроза виявлення інформації про внутрішню мережу (наприклад, підключені пристрої, використані	к, ц, д, с	0.35	2

Продовження таблиці 2.1

1	2	3	4	5	6
		протоколи, відкриті порти та використовувані служби тощо) зловмиснику, якому вдається пасивно сканувати мережу. Маючи ці знання, зловмисник може планувати, які дії слід вжити далі для компрометації системних операцій.			
Фізична атака	Вандалізм і крадіжка	Загроза заподіяння фізичної шкоди пристрою диверсантом, який отримує фізичний доступ до ОТ-середовища - або сторонніми особами, яким вдалося обійти недостатні заходи фізичної безпеки, або інсайдером, наприклад. незадоволений працівник, який	к, ц, д	0.16	1

Продовження таблиці 2.1

1	2	3	4	5	6
		хоче завдати шкоди організації. Ця загроза включає також крадіжки. Необхідність заміни пошкодженого або викраденого пристрою може призвести до непередбачуваного простою виробництва, пов'язаного з терміном доставки запасних частин.			
	Саботаж (диверсія)	Загроза підробити пристрій диверсантом, який отримує фізичний доступ до ОТ-середовища, або сторонніми особами, яким вдається обійти недостатні заходи фізичної безпеки, або інсайдером, наприклад, незадоволений працівник, який з	ц, д	0.27	2

Продовження таблиці 2.1

1	2	3	4	5	6
		<p>якихось причин хоче завдати шкоди організації.</p> <p>Зловмисник може скористатися неправильною конфігурацією портів та можливістю використання відкритих портів. Зловмисник також може використовувати доступ для здійснення несанкціонованих дій в ролі оператора.</p>			
Ненавмисні збитки (випадкові)	Ненавмисна зміна даних або конфігурації в ОТ-системі	<p>Загроза порушити операційний процес ненавмисними даними або зміною конфігурації в системі ОТ, яку виконує не досить навчений працівник. Навіть при добрих намірах некваліфікований</p>	к, ц	0.34	1

Продовження таблиці 2.1

1	2	3	4	5	6
		працівник, не знаючи про наслідки, може внести неналежні зміни в систему, особливо якщо він або вона отримає вищі, ніж необхідні, привілеї.			
	Неправильне використання або адміністрування пристроїв та систем	Загроза зриву операційного процесу або заподіяння фізичної шкоди пристрою ненавмисним неправильним використанням пристрою ІоТ / ОТ недостатньо навченим працівником. Некваліфікований працівник може ненавмисно не використовувати пристрій відповідно до посібників, тим самим порушуючи роботу	к, ц, д, с	0,3	2

Продовження таблиці 2.1

1	2	3	4	5	6
		пристрою або завдаючи йому фізичної шкоди.			
	Пошкодження, заподіяні третьою стороною	Загроза пошкодження активів ОТ, заподіяних третьою стороною. У Індустрії 4.0, третя сторона може мати доступ до системи ОТ, наприклад, для обслуговування або оновлення програмного забезпечення. Якщо цей доступ не контролюється в достатній мірі, порушення безпеки від третьої особи може вплинути на компанію, яка отримує послугу.	к, ц	0,64	3
Поломки несправності	/ Поломка або несправність датчика / приводу	Загроза виходу з ладу або несправності кінцевих пристроїв ПоТ. Іноді це може статися, особливо	ц, д, с	0,55	3

Продовження таблиці 2.1

1	2	3	4	5	6
		якщо під час експлуатації не забезпечено належне обслуговування та дотримання інструкцій з використання пристроїв.			
	Поломка або несправність системи управління (PLC, RTU, DCS)	Загроза виходу з ладу або несправності системи управління.	ц, д, с	0,4	4
	Експлуатація вразливостей програмного забезпечення	Загроза того, що зловмисник скористається вразливістю ПЗ або прошивки кінцевих пристроїв ІоТ. Такі пристрої часто вразливі через відсутність оновлень, використання слабких паролів або паролів за замовчуванням та	к, ц, д	0,72	5



Продовження таблиці 2.1

1	2	3	4	5	6
		неправильну конфігурацію.			
	Збій або зрив постачальників послуг	Загроза зриву процесів, які покладаються на сторонні послуги у разі несправності цих служб.	ц, д	0,4	2
Простій у роботі	Відключення мережі зв'язку	Загроза недоступності зв'язку комунікацій, пов'язаних із проблемами з кабельною, бездротовою чи мобільною мережею.	ц, д, с	0,2	3
	Відключення джерела живлення	Загроза несправності джерела живлення. Якщо в критичних системах не існує аварійного джерела живлення, будь-яке переривання живлення може призвести до серйозних наслідків	ц, д, с	0,1	5

Продовження таблиці 2.1

1	2	3	4	5	6
		через раптове припинення виробничих процесів.			
	Втрата служб підтримки (MES, ERP, CRM)	Загроза виходу з ладу або несправності систем, що підтримують виробництво чи логістику, тобто MES, ERP та CRM.	ц, д, с	0,28	2
Правові проблеми	Порушення правил та регламентів / Порушення законодавства / Зловживання персональними даними	Загроза юридичних питань та фінансові втрати, пов'язані з обробкою персональних даних, наприклад пов'язані з використанням кінцевих пристроїв IoT без дотримання місцевих законів чи правил.	к, ц	0,3	2
	Невиконання договірних вимог	Загроза порушення договірних вимог з боку виробників компонентів та постачальників програмного	к, ц	0,27	1

## Продовження таблиці 2.1

1	2	3	4	5	6
		забезпечення у разі ненадання необхідних заходів безпеки.			
Стихійне лихо	Природні катастрофи	Загроза стихійних лих, таких як повені, удари блискавки, сильний вітер, дощ та снігопад, які можуть завдати фізичної шкоди компонентам ОТ- середовища.	ц, д, с	0,15	3
	Екологічні катастрофи	Загроза інцидентів та несприятливі умови, такі як пожежі, забруднення, пил, корозія, вибухи, які можуть завдати фізичної шкоди компонентам ОТ- середовища.	ц, д, с	0,14	3

## 2.2 Обчислення ризиків при реалізації загроз для промислового Інтернету речей

Ризики можна обчислити за класичною формулою

$$R = P * V_i \quad (2.1),$$

де  $R$  – ризик,  $P$  – імовірність виникнення загрози,  $V$  – наслідки реалізації загрози. Ризики описані в таблиці 2.2.

Таблиця 2.2 – Обчислення ризиків у типовій системі промислового IoT

Загроза	Імовірність виникнення загрози	Наслідки реалізації загрози	Ризик
1	2	3	4
Відмова в обслуговуванні	0.5	5	2,5
Шкідливе ПЗ	0.85	5	4,25
Маніпуляція апаратним та програмним забезпеченням	0.45	3	1,35
Маніпуляція інформацією	0.35	4	1,4
Націлені атаки	0.4	3	1,2
Зловживання персональними даними	0.5	3	1,5
Атака «грубої сили»	0.67	3	2,01
Атака "людина посередині" / Викрадення сесії	0.47	4	1,88
Викрадення даних протоколу зв'язку IoT	0.6	3	1,8
Мережева розвідка	0.35	2	0,7
Вандалізм і крадіжка	0.16	1	0,16
Саботаж (диверсія)	0.27	2	0,54

## Продовження таблиці 2.2

1	2	3	4
Ненавмисна зміна даних або конфігурації в ОТ-системі	0,34	1	0,34
Неправильне використання або адміністрування пристроїв та систем	0,3	2	0,6
Пошкодження, заподіяні третьою стороною	0,64	3	1,92
Поломка або несправність датчика / приводу	0,55	3	1,65
Поломка або несправність системи управління (PLC, RTU, DCS)	0,4	4	1,6
Експлуатація вразливостей програмного забезпечення	0,72	5	3,6
Збій або зрив постачальників послуг	0,4	2	0,8
Відключення мережі зв'язку	0,2	3	0,6
Відключення джерела живлення	0,1	5	0,5
Втрата служб підтримки (MES, ERP, CRM)	0,28	2	0,56
Порушення правил та регламентів / Порушення законодавства / Зловживання персональними даними	0,3	2	0,6
Невиконання договірних вимог	0,27	1	0,27
Природні катастрофи	0,15	3	0,45
Екологічні катастрофи	0,14	3	0,42

## **2.3 Опис складових політики безпеки (описово)**

Модель політики безпеки має складатись із правил та рекомендацій, які поділені на певні категорії та підкатегорії. Можна виділити такі основні 4 категорії: 1) заходи з безпеки на початку розробки продукту, 2) заходи з розмежування доступу, 3) організаційні заходи, 4) захист від несанкціонованого доступу. Далі розглянемо їх усі.

### **2.3.1 Заходи з безпеки на початку розробки продукту**

А. Безпека по наміру:

- 1) Впроваджувати заходи з кібербезпеки за допомогою вбудованих функцій кінцевих точок, а не лише в мережному рівні.
- 2) Обладнати, якщо вважається доцільним після оцінки безпеки навіть найпростіші підключені пристрої, що мають дуже обмежені можливості обробки (наприклад, приводи, перетворювачі) за допомогою функцій ідентифікації та автентифікації та забезпечити сумісність із рішеннями класу IAM.
- 3) Провести аналіз ризиків та загроз за участю експертів з кібербезпеки на самих ранніх етапах процесу проектування пристрою, щоб з'ясувати, які функції безпеки будуть необхідні.

Б. Конфіденційність по наміру:

- 1) Вирішення проблем, пов'язаних з конфіденційністю, на основі застосованих місцевих та міжнародних норм, таких як Загальне положення про захист даних (GDPR).

2) Визначте обсяг даних, які будуть оброблятися пристроєм, а також цілі цієї обробки під час фази проектування, запобігаючи збору конфіденційних даних.

3) Встановіть фізичне місце зберігання даних та визначте, для яких організацій дані будуть передаватися з обмеженням доступу до зібраних персональних даних лише для авторизованих осіб.

4) Провести аналіз впливу на конфіденційність (PIA – privacy impact analysis) для даних, які будуть оброблятися пристроєм.

### **2.3.2 Заходи з розмежування доступу**

#### **А. Керування доступом для третіх осіб:**

- 1) Суворо контролювати доступ третіх осіб до контрольного або виробничого рівня, надаючи лише доступ на вимогу у визначений час для певної мети та з найменшими привілеями.
- 2) Не забезпечуйте прямого підключення постачальника до системи в контрольному або виробничому рівні. Дозволити доступ лише до необхідних вибраних функцій та частин мережі.
- 3) Чітко визначити всі відповідні аспекти партнерства з третіми сторонами, включаючи безпеку, у рамках відповідних угод та контрактів.

#### **Б. Контроль доступу:**

- 1) Відокремити віддалений доступ, тобто розробка набору правил для управління віддаленим зв'язком.

2) Забезпечити мінімальний рівень аутентифікації для пристроїв та систем ІоТ та забезпечити що авторизація дозволяє лише отримати доступ до певного сегменту системи.

3) Реалізація / використання багатофакторної автентифікації в рішеннях ІоТ.

4) Зміна паролів та імен користувачів за замовчуванням під час введення в експлуатацію / першого використання. Використовуйте сильний пароль та вимагайте встановлення нового пароля після визначеного періоду.

5) Застосовуйте принцип найменшого привілею та забезпечуйте що в середовищі з декількома користувачами ролі належним чином відокремлені та затверджені відповідною особою.

6) Створюйте індивідуальні акаунти для кожного користувача, коли це можливо.

7) Реалізація / використання функцій блокування облікового запису на пристроях ІоТ.

8) У разі розгалуженої та різноманітної мережі з великою кількістю пристроїв прийняти рішення привілею управління доступом (РАМ).

9) В рамках контролю доступу розгляньте аспекти фізичного доступу до будівель, кімнат та кабінетів.

### **2.3.3 Організаційні заходи**

#### **А. Життєвий цикл кінцевих точок**

1) Зосередьтеся на безпеці програмного та апаратного забезпечення на кожному етапі життєвого циклу кінцевої точки.

2) Враховуйте питання безпеки в усьому ланцюгу поставок.



3) Розглянути аспекти безпеки під час загального процесу закупівель, визначивши заходи безпеки та вимоги, призначені для конкретних пристроїв / рішень.

4) Під час фази передачі в процесі впровадження проекту належним чином створити та передати всю документацію, процеси та процедури з кібербезпеки.

#### Б. Безпека архітектури

1) Для забезпечення безпеки в комп'ютеризованій екосистемі прийняти цілісний підхід, заснований на архітектурі та розробити орієнтовану на ризик архітектуру безпеки на основі бізнес-вимог.

2) Визначаючи безпеку архітектури, переконайтеся, що вона містить усі відповідні аспекти безпеки – від організаційних питань до фізичної реалізації.

3) В рамках архітектури безпеки виділіть чіткі ролі та обов'язки щодо безпеки. Чітко визначати ролі як для систем ОТ, так і для безпечних процесів.

4) Інтегрувати контроль за дотриманням норм відповідності до встановленої безпеки архітектури та забезпечити відповідність вимогам для продукції.

#### В. Обробка інцидентів

1) Визначити кібер-інциденти, що стосуються вашої організації, залежно від сфери діяльності компанії та класифікувати їх відповідно до діючих стандартів.

2) Розглянути можливість створення Центру операцій з безпеки (SOC), що складається з спеціалістів ОТ та ІТ-кібербезпеки для підтримки інцидентів кібербезпеки, розділяючи їх на конкретні види підтримки з відповідними ролями та обов'язками.

3) Встановити процес обробки інцидентів, який складається з ідентифікації постраждалих активів, ідентифікації та класифікації вразливостей, розгортання та сповіщення.

4) Оперативно виявляти та досліджувати всі незвичайні події, пов'язані із безпекою.

#### Г. Управління вразливостями

1) Визначте комплексний процес управління вразливістю в межах організації, яка охоплює використання автоматичних та ручних інструментів, отриманих в результаті аналізу ризиків.

2) Усуваючи вразливості, почніть з найбільш критичних з урахуванням критичності активів та систем.

3) Встановити всебічний і чітко визначений процес розкриття вразливостей.

4) Провести тести на проникнення нових ІоТ рішень в контрольованому середовищі або до / під час етапу введення в експлуатацію, а також проводити тести регулярно і після кожного важливого оновлення системи.

#### Д. Моніторинг та аудит

1) Впровадити пасивне рішення для моніторингу в ІТ та ОТ середовищі для контролю мережевого трафіку.

2) Збирайте журнали безпеки та аналізуйте їх у режимі реального часу за допомогою спеціальних інструментів, наприклад рішення класу SIEM, наприклад, в Security operations center (SOC).

3) Виконувати періодичні огляди мережевих журналів, привілеїв контролю доступу та конфігурації ресурсів.

4) Контролюйте доступність пристроїв ІоТ в режимі реального часу, де це технічно можливо.

### 2.3.4 Захист від несанкціонованого доступу

#### А. Безпека M2M

- 1) Зберігайте довгострокові ключі рівня обслуговування (крім відкритих ключів) в HSM-сервері, що розміщено в інфраструктурному обладнанні.
- 2) Створити асоціацію безпеки із перевіреними та безпечними криптографічними алгоритмами для комунікації суб'єктів для забезпечення взаємної автентифікації, цілісності та конфіденційності.
- 3) Використовуйте протоколи обміну даними, які включають функціональність для виявлення, чи є все повідомлення або його частина несанкціонованим повторенням попереднього повідомлення.
- 4) Використовуйте білий список при перевірці вхідних даних для захисту від міжсайтового скриптингу та ін'єкції команд.

#### Б. Захист даних

- 1) Класифікуйте дані, що стосуються системи ОТ, на основі аналізу ризиків, оцініть його критичність та визначте необхідні заходи безпеки, які забезпечать належний рівень безпеки.
- 2) Надання доступу до певних категорій даних третім сторонам з найменшими привілеями.
- 3) Для даних з високою конфіденційністю реалізуйте шифрування та керування ключами, щоб інформацію могли читати лише авторизовані користувачі та використовувати рішення щодо запобігання втрати даних.
- 4) Анонімізуйте та захистіть будь-які персональні дані, що обробляються в компанії, наприклад за допомогою контролю доступу на основі ролей та шифрування, враховуючи всі відповідні законодавчі вимоги.

#### В. Мережі, протоколи та шифрування

- 1) Захистити канали зв'язку, пов'язані з рішеннями ПоТ, та шифрувати комунікації у випадку важливих даних, де це технічно можливо.
- 2) Поділити на сегменти мережі промислових підприємств на основі заздалегідь визначеної моделі зонування, яка включає встановлення демілітаризованих зон (DMZ) та контроль руху між зонами.
- 3) Дотримуйтесь мікросегментаційного підходу, тобто будуйте невеликі острівці компонентів у межах однієї мережі, які спілкуються лише один з одним і контролює мережевий трафік між сегментами.
- 4) Якщо можливо, ізолюйте безпечні мережі від корпоративних та контрольних мереж.
- 5) Для рішень ПоТ реалізуйте перевірені у використанні протоколи з відомими можливостями безпеки на основі стандартів та технічних рекомендацій. Вибирайте рішення, які використовують протоколи, що здатні захистити або вирішити попередні проблеми безпеки (наприклад, TLS 1.3) та уникати проблем із відомими вразливостями (наприклад, Telnet, SNMP v1 або v2).
- 6) Якщо можливо, обмежте кількість протоколів, реалізованих у заданому середовищі, і відключіть мережеві послуги за замовчуванням, які не використовуються.
- 7) Забезпечити безпечне середовище для обміну ключами та управління ключами, запобігаючи обміну криптографічними ключами між кількома пристроями.
- 8) Забезпечити належне та ефективне використання криптографії для захисту конфіденційності, достовірності та / або цілісності даних та інформації (включаючи контрольні повідомлення) під час передачі та в спокої. Переконайтесь, що правильно вибрані стандартні та стійкі алгоритми шифрування, а також відключено небезпечні протоколи. Перевірте надійність реалізації.

## **Висновки до розділу 2**

В цьому розділі було наведено склад загроз для пристроїв промислового Інтернету речей. Для кожної загрози вказано імовірність її виникнення та наслідки за визначеними шкалами. Визначено ризики для усіх загроз, використовуючи міжнародний стандарт ISO/IEC 27005.

Сформовано модель політики безпеки для промислового IoT, враховуючи вищенаведені загрози. Політика безпеки поділена на категорії, також наведена описово.

### 3 МЕТОДИКА ОЦІНКИ ДІЄВОСТІ ПОЛІТИКИ БЕЗПЕКИ

#### 3.1 Критерії дієвості політики безпеки

- 1) Спад прогнозованих значень основних ризиків;

Будується залежність кількості проведених атак певного типу від кількості днів. Далі оцінюється спад чи зростання ризиків по регресійній прямій.

- 2) Наявність кореляції між фінансовими вкладеннями в покращення захисту, вдосконалення політики безпеки та значеннями ризиків;

Будується залежність між фінансовими вкладеннями на покриття ризику та величиною ризику. Якщо залежність добре апроксимується регресійною прямою, це означає, що між рівнем фінансових вкладень на зменшення певного ризику, та рівнем ризику існує залежність. А це означає, що покращення політики безпеки, які запроваджуються цими фінансовими вкладеннями, дають позитивний ефект.

- 3) Використання фреймворків безпеки;

Фреймворки безпеки – це організований набір вимог безпеки, зазвичай розбитих на численні категорії, тобто чеклісти. Сюди належить відповідність середньому рівню та вище, за чеклістами вимог безпеки.

- 4) Наявність успішних результатів моделювання майбутніх запроваджень політики безпеки;

Моделюється тестова мережа з пристроями IoT. Демонструється одна з поширених атак на мережу та показується, що політика безпеки здатна захистити мережу від атаки.

- 5) Результати тестування на проникнення свідчать про відсутність можливостей здійснення НСД;

Проводяться тести на проникнення спеціально для мережі з IoT-пристроями. Якщо тести невдалі, то відсутня можливість несанкціонованого доступу. Якщо ж тести на проникнення успішні, то необхідно покращувати політику безпеки.

- б) Виконання організаційних заходів із забезпечення політики безпеки, ініційованих вищим менеджментом;

До основних організаційних заходів можна віднести розмежування рольового керування доступом, розробка правильної архітектури безпеки, встановлення систем моніторингу та аудиту тощо.

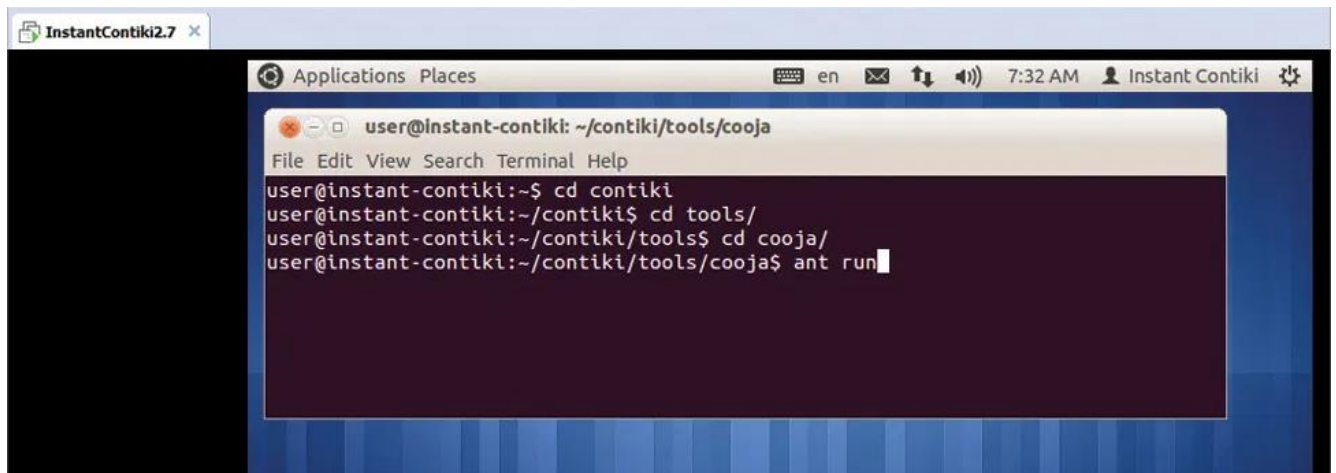
- 7) Застосування шаблонів безпеки.

Шаблони безпеки – це текстові файли, які використовуються для організації, налаштування та керування безпекою на комп'ютерах на всьому підприємстві з ОС Windows. Ці шаблони впорядковані в логічні розділи на основі різних категорій політик безпеки на всіх комп'ютерах під керуванням Windows. Після налаштування шаблону безпеки ви можете використовувати його для налаштування одного або декількох комп'ютерів у мережі. Шаблони безпеки пропонують метод централізації конфігурації та розгортання конфігурацій безпеки на комп'ютерах.

### **3.2 Імплементация політики безпеки через засіб моделювання мережі IoT**

На даний момент існує досить багато симуляторів мережі для різних типів Інтернету речей. Для промислового Інтернету речей найкраще підходить операційна система Contiki OS(яка являє собою модифіковану Ubuntu 14.04) та симулятор COOJA(Contiki OS Java simulator).

Contiki – це операційна система, орієнтована на низькопотужні пристрої IoT. Свої дозволяє імітувати великі та малі мережі з вузлів(кінцевих точок) Contiki. Запуск програми здійснюється за допомогою команд, зображених на рисунку 3.1.

A screenshot of a terminal window titled "InstantContiki2.7". The terminal shows a series of commands being entered to navigate to the Cooja directory and run it. The commands are: `cd contiki`, `cd tools/`, `cd cooja/`, and `ant run`. The prompt changes from `user@instant-contiki:~$` to `user@instant-contiki:~/contiki/tools/cooja$` after each `cd` command. The `ant run` command is entered at the end, with a cursor at the end of the line.

```
user@instant-contiki: ~/contiki/tools/cooja
File Edit View Search Terminal Help
user@instant-contiki:~$ cd contiki
user@instant-contiki:~/contiki$ cd tools/
user@instant-contiki:~/contiki/tools$ cd cooja/
user@instant-contiki:~/contiki/tools/cooja$ ant run
```

Рисунок 3.1 – Команди для запуску Свої

Результати симуляції подані на рисунку 3.2.



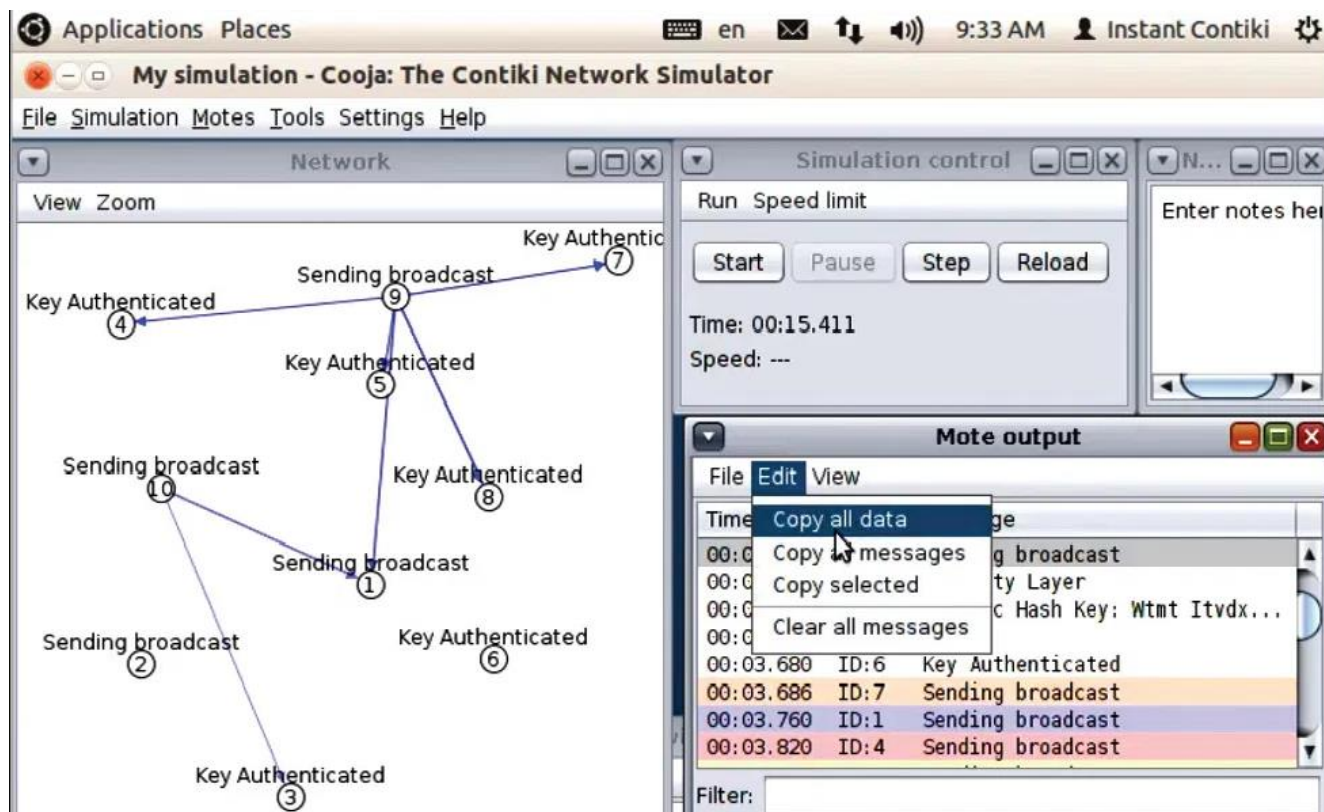


Рисунок 3.2 – Запуск симуляції та поведінковий аналіз вузлів

У цьому моделюванні мережі IoT виконується сценарій динамічного обміну ключами між вузлами. Тут динамічний ключ безпеки генерується та використовується в аутентифікації для зв'язку. У IoT з міркувань безпеки необхідно розробити та реалізувати протоколи та алгоритми, за допомогою яких можна забезпечити загальну конфіденційність та безпеку при обміні даними, щоб уникнути будь-яких вторгнень.

Після того, як моделювання завершено, аналізуються файли журналів мережі, які включають джерело і місце призначення для вузлів, час та загальну діяльність, що виконується під час моделювання. У вікні вихідних даних Mote дані журналу можна скопіювати та додатково проаналізувати за допомогою інструментів майнінгу даних та машинного навчання для прогнозованої аналітики.

Далі буде описана реалізація атаки відмови в обслуговуванні, здійснену в симуляторі Сooja для розгортання мережі, а також різні шкідливі вузли для імітації атак. Змодельована атака буде здійснена, змінюючи файли конфігурації RPL, що призводило до зміни поведінки вузла. Наслідки атаки будуть описані через збір даних про електроспоживання.

### 3.2.1 Моделювання тестової мережі

Побудова довідкової мережі включає наступні етапи:

1. Після запуску симулятора Сooja слід створити нове моделювання, натиснувши на File-> New simulation в рядку меню. Тут буде встановлено ім'я симуляції та тип радіосередовища(рисунок 3.3).

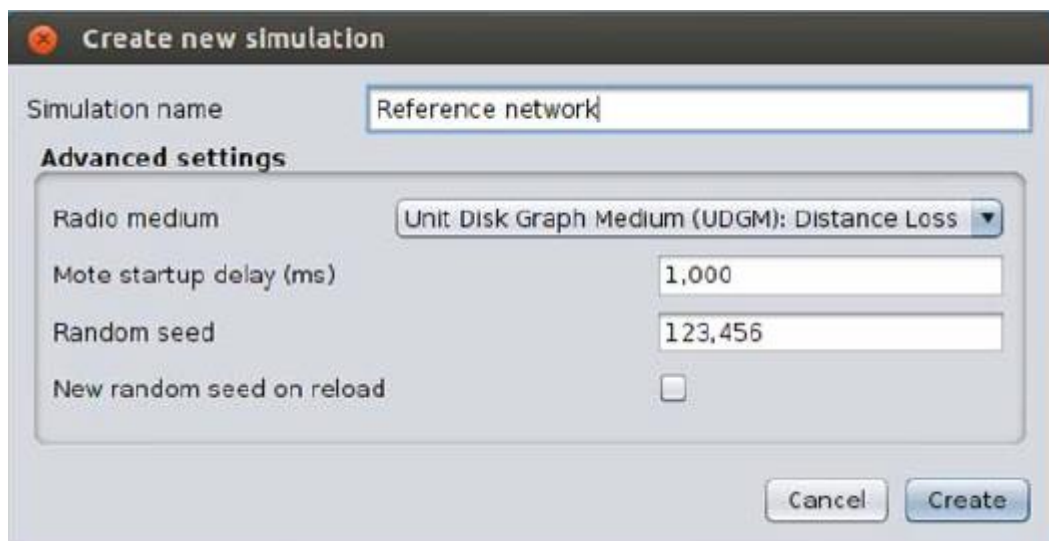


Рисунок 3.3 – Створення нової симуляції в COOJA

2. Наступним кроком буде створення типів вузлів, які становлять мережу. Тестова мережа матиме два типи вузлів: sink-вузол, який функціонуватиме як маршрутизатор DODAG, та листовий вузол, який буде функціонувати як простий бездротовий датчик для збору даних. Вузли базуються на таких файлах програмного забезпечення:

~ / Contiki / example / ipv6 / rpl-collection / sink.c – sink-вузол(маршрутизатор).

~ / Contiki / example / ipv6 / rpl-collection / udp-sender.c – вузли.

З'явиться вікно, далі натиснути Motes-> Add motes-> create new mote type-> sky mote на панелі меню. Тут буде скомпільовано прошивку різних вузлів для їх створення. Результат подано на рисунку 3.4.

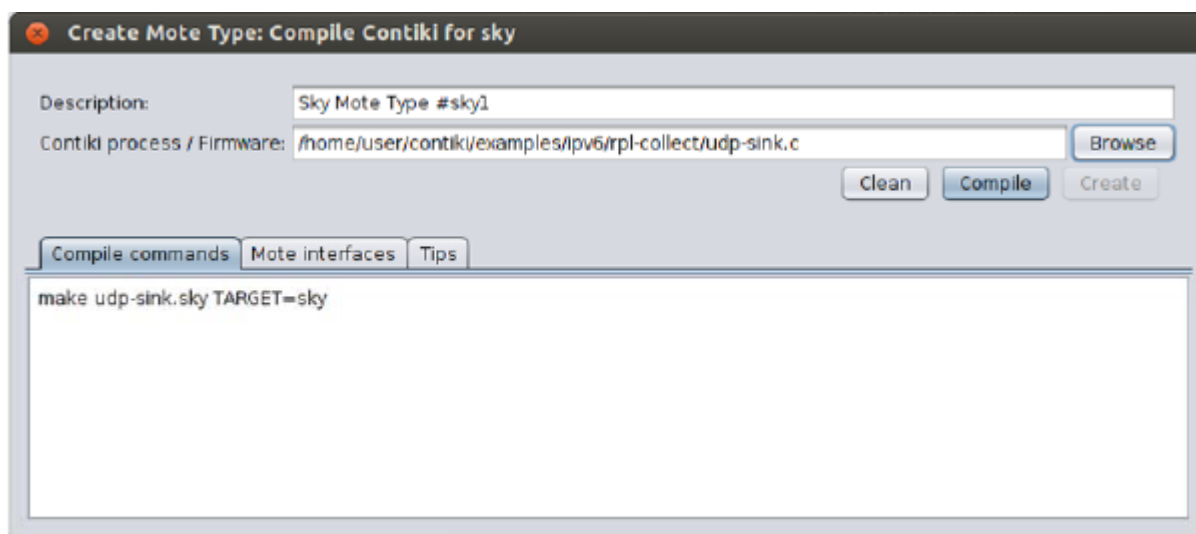


Рисунок 3.4 – Додавання нового вузла

Оскільки середовище моделювання має бути максимально реальним, то моделювання проводитиметься на площі 100x100 метрів з випадковим розподілом

вузлів. Остаточну мережу зображено на рисунку 3.5. На малюнку також показаний діапазон передачі та перешкод маршрутизатора DODAG.



Рисунок 3.5 – Остаточно побудована мережа

### 3.2.2 Проведення атаки

Основна мета під час імітації нападу – змінити поведінку вузлів, не змінюючи нормальну поведінку решти учасників мережі. Роблячи це, можна оцінити, як мережа реагує на незвичні ситуації. Метод, який використовується для досягнення цього підходу, може бути виконаний, дотримуючись наведених нижче кроків:

- Скопіюйте папку Contiki, щоб створити новий Contiki O.S. екземпляр.

- Змініть файли, відповідальні за атаку.
- Створіть новий вузол (шкідливий), компілюючи прошивку вузла в новому екземплярі Contiki.
- Додайте вузол до базової мережі.

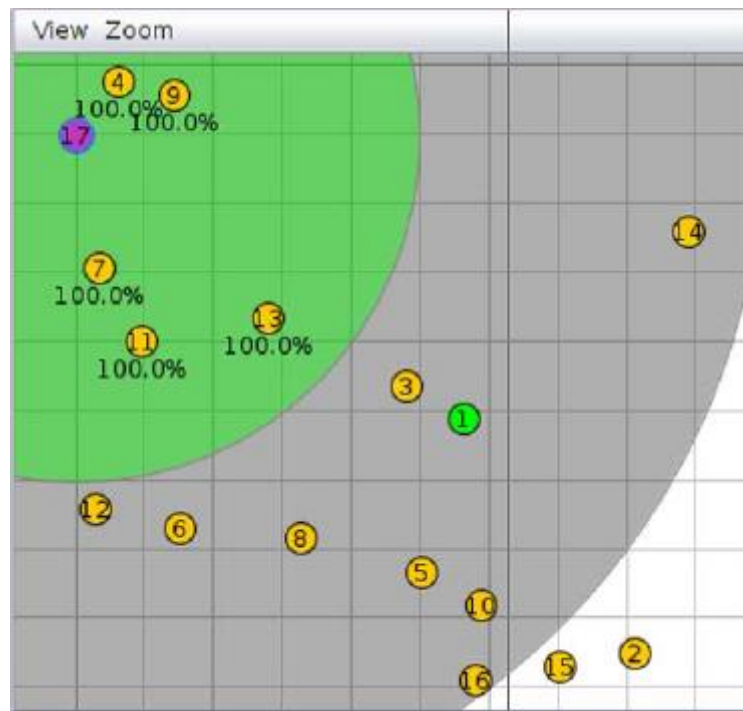


Рисунок 3.6 – Побудована мережа зі шкідливим вузлом

### 3.2.2.1 DIS-атака

#### а) Визначення

Атака DIS – це пряма атака на мережеві ресурси з використанням DODAG. Вона може бути віднесена до атаки переповнення, оскільки має на меті зробити вузли та комунікації недоступними через створення великої кількості трафіку.

Зловмисник може передавати широкомовно або одноразово передавати контрольні повідомлення DIS на інші вузли, що спричиняє більше витрат на трафік і, зрештою, надмірне використання енергії. Тому DIS-атаку можна вважати відмовою в обслуговуванні, оскільки метою є порушення роботи та недоступність мережі.

#### б) Мета

Метою симуляції атаки є розуміння впливу споживання енергії, яку зазнають листові вузли, коли шкідливий вузол викликає атаку DIS у бездротовій сенсорній мережі. Крім того, виходячи з результатів, буде розглянуто теоретичне рішення або, де можливо, реалізація для протидії цій конкретній атаці.

#### в) Впровадження

Файли RPL містяться у `~/Contiki/core/net/rpl/` всередині Contiki OS. Для реалізації DIS-атаки були змінені наступні файли:

#### **rpl\_private.h**

`rpl_private.h` визначає приватні декларації для ContikiRPL, такі як значення за замовчуванням для керуючих повідомлень ICMP, пов'язані з ними таймери, режим роботи, таблиці маршрутизації DAG серед інших постійних значень RPL. Існують дві директиви, що визначають інтервал повідомлень DIS та таймери затримки запуску. На рисунку нижче показаний фрагмент коду обох параметрів у файлі `rpl_private.h`. Мета зміни цього значення – змусити зловмисний вузол постійно надсилати повідомлення DIS. Обидва значення будуть встановлені до 0. Результати показано на рисунку 3.6.

```

/* DIS related */
#define RPL_DIS_SEND 1
#ifdef RPL_DIS_INTERVAL_CONF
#define RPL_DIS_INTERVAL RPL_DIS_INTERVAL_CONF
#else
#define RPL_DIS_INTERVAL 0 /*Value was 60*/
#endif
#define RPL_DIS_START_DELAY 0 /*Value was 5*/
/*-----*/

```

Рисунок 3.6 – Модифікований файл rpl\_private.h

### rpl\_timers.c

rpl\_timers.c відповідає за керування таймерами в ContikiRPL. Код, зображений на рисунку 3.7, змінює спосіб обробки повідомлень DIS.

```

static void
handle_periodic_timer(void *ptr)
{
    rpl_purge_routes();
    rpl_recalculate_ranks();

    /* handle DIS */
    #if RPL_DIS_SEND
    //next_dis++; //added next_dis++;int i=0;while (i<20) {i++; dis_output(NULL);}
    next_dis++;
    int i=0;
    while (i<20) {i++; dis_output(NULL);}
    if(rpl_get_any_dag() == NULL && next_dis >= RPL_DIS_INTERVAL) {
        next_dis = 0;
        dis_output(NULL);
    }
    #endif
    ctimer_reset(&periodic_timer);
}

```

Рисунок 3.7 – Модифікований файл rpl\_timers.c

### 3.2.3 Результати проведення атаки

На рисунку 3.8 представлені результати споживання енергії за чотирма різними показниками потужності:

Потужність процесора – це енергія, витрачена на обробку завдань вузла.

LPM Power – це відношення потужності, споживаної вузлом у режимі очікування (в режимі простою).

Power Power – енергія, витрачена вузлом на прослуховування повідомлень.

Потужність передачі – енергія, витрачена на передачу пакетів.

REFERENCE NETWORK					
Node	CPU Power	LPM Power	Listen Power	Transmitting Power	Total Power
2	0.351259437	0.152864645	0.422814329	0.068123179	0.99506159
3	0.402966403	0.151299073	0.44458598	0.054313812	1.053165268
4	0.34519587	0.153048236	0.451725911	0.12635619	1.076326207
5	0.390981064	0.151661962	0.442336061	0.064550613	1.049529701
6	0.390028782	0.151690795	0.452043233	0.051664957	1.045427769
7	0.368664058	0.152337671	0.46846239	0.120900421	1.110364541
8	0.407687391	0.151156132	0.468765278	0.061692786	1.089301588
9	0.353579924	0.152794386	0.461003905	0.156857681	1.124235896
10	0.381639008	0.151944819	0.437682245	0.064059644	1.035325715
11	0.388295784	0.151743267	0.470064099	0.11349267	1.123595818
12	0.352486028	0.152827507	0.451307177	0.114713928	1.07133464
13	0.40661359	0.151188644	0.469617594	0.059641637	1.087061464
14	0.316576616	0.153914763	0.406399439	0.053438422	0.93032924
15	0.36746598	0.152373947	0.425830448	0.048744534	0.994414908
16	0.367200585	0.152381982	0.428868742	0.054230558	1.002681868
Average	<b>0.372709368</b>	<b>0.152215188</b>	<b>0.446767122</b>	<b>0.080852069</b>	<b>1.052543748</b>

Рисунок 3.8 – Результати споживання енергії в нормальній мережі



Потужність LPM та потужність прослуховування не мають відповідних відмінностей між вузлами. Наведені нижче діаграми на рисунку 3.9 щодо споживання електроенергії підсумовують значення за вузлами:

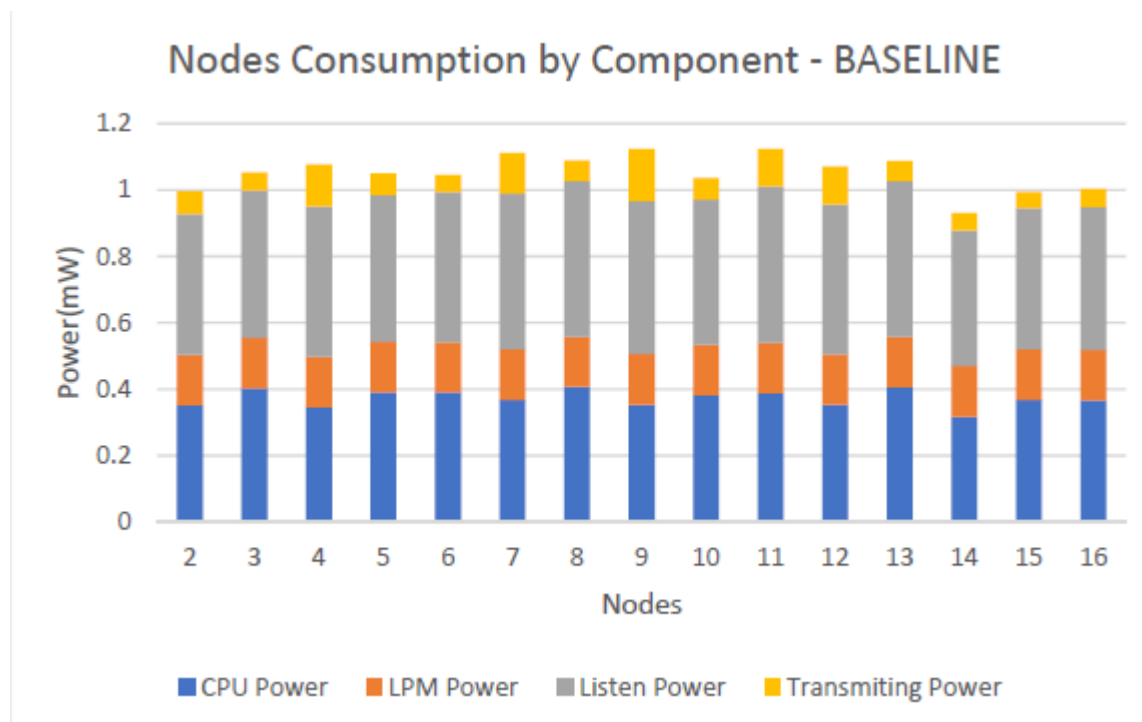


Рисунок 3.9 – Споживання енергії вузлами

На наступному рисунку 3.10 показані результати, отримані після запуску моделювання зі шкідливим вузлом протягом 10 хвилин (реальних). Використано ту саму методологію для збору споживання електроенергії.

Node	CPU Power	LPM Power	Listen Power	Transmitting Power	Total Power
2	0.529436921	0.147469827	1.164172012	1.216901283	3.057980043
3	0.519455896	0.14777203	1.342622192	0.804243921	2.814094039
4	1.86286332	0.107096638	20.62036859	2.087472321	24.67780087
5	0.558203595	0.146598836	1.208506478	1.067168285	2.980477194
6	0.669932865	0.143215922	1.941257247	1.65360238	4.408008415
7	2.055413487	0.101266647	21.08135045	2.653331238	25.89136183
8	0.658032383	0.143576242	1.804332116	1.607205219	4.21314596
9	2.249477821	0.09539081	24.84559236	2.339792252	29.53025325
10	0.536049017	0.147269627	1.319687584	1.183416375	3.186422603
11	1.94191986	0.104702982	21.68966294	1.578212204	25.31449799
12	1.911479121	0.10562466	22.16001002	1.839849311	26.01696312
13	2.081403993	0.100479712	22.60831345	1.082049479	25.87224663
14	0.401297404	0.151349606	0.628188563	0.652141249	1.832976823
15	0.43814213	0.15023403	0.977077521	0.628442475	2.193896156
16	0.32433355	0.153679901	1.311768531	0.451706762	2.241488743

Рисунок 3.10 – Результати після проведення DIS-атаки

Графічні подання зібраних даних зображені на рисунках 3.11 і 3.12, щоб спростити результати, показані вище:

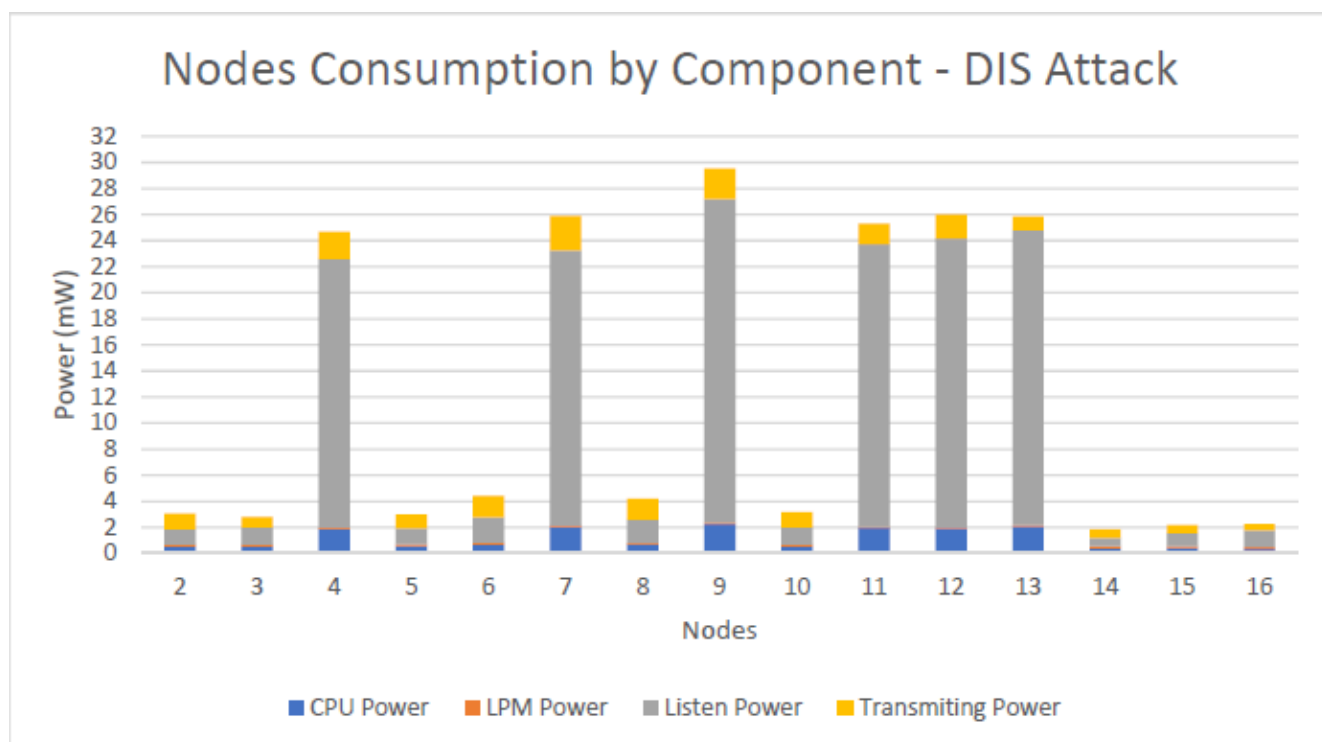


Рисунок 3.11 – Споживання енергії вузлами після DIS-атаки

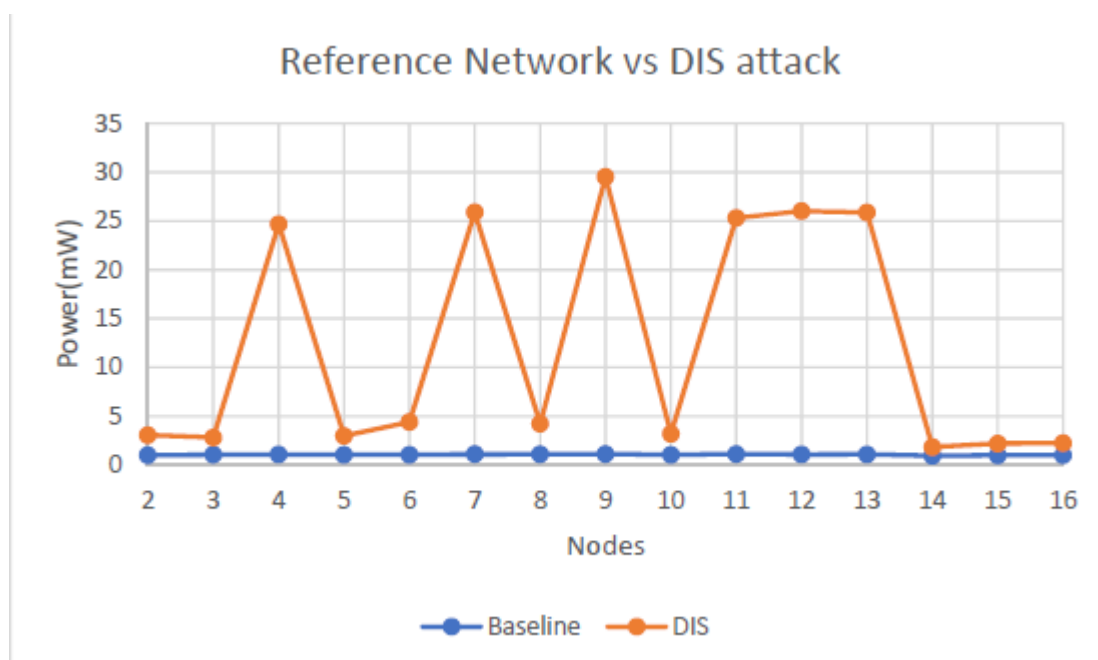


Рисунок 3.12 – Різниця у споживанні енергії до та після атаки

Далі на рисунку 3.13 наводиться співвідношення споживання енергії вузлами у відсотках.

Node	CPU Power	LPM Power	Listen Power	Transmitting Power	Total Power
2	50.73%	-3.53%	175.34%	1686.32%	207.32%
3	28.91%	-2.33%	201.99%	1380.74%	167.20%
4	439.65%	-30.02%	4464.80%	1552.05%	2192.78%
5	42.77%	-3.34%	173.21%	1553.23%	183.98%
6	71.76%	-5.59%	329.44%	3100.63%	321.65%
7	457.53%	-33.52%	4400.12%	2094.64%	2231.79%
8	61.41%	-5.01%	284.91%	2505.18%	286.77%
9	536.20%	-37.57%	5289.45%	1391.67%	2526.70%
10	40.46%	-3.08%	201.52%	1747.37%	207.77%
11	400.11%	-31.00%	4514.19%	1290.59%	2152.99%
12	442.29%	-30.89%	4810.18%	1503.86%	2328.46%
13	411.89%	-33.54%	4714.20%	1714.25%	2280.02%
14	26.76%	-1.67%	54.57%	1120.36%	97.02%
15	19.23%	-1.40%	129.45%	1189.26%	120.62%
16	-11.67%	0.85%	205.87%	732.94%	123.55%

Рисунок 3.13 – Співвідношення споживання енергії вузлами

Побачивши вплив, який викликають DIS-атаки щодо споживання електроенергії на вузлах, рішення для виявлення цього типу атаки можна описати таким чином:

- IDS повинен виявити аномалії в поведінці споживання енергії та кількості пакетів. Він може базуватися на заздалегідь визначених шаблонах, таких як режим роботи RPL або на основі аномалій (наприклад, спрацьовує попередження, якщо показник споживання енергії перевищує певний поріг або попередження, якщо кількість певних типів повідомлень перевищує нормальну поведінку).

- З точки зору масштабованості та енергоспоживання, було б ідеально реалізувати мережеву IDS. У такий спосіб можна буде додати нові вузли в мережу, не хвилюючись про встановлення host-based IDS у кожному новому вузлі. Це також дозволило б уникнути можливих несумісностей (ОС, прошивка).

- У цьому конкретному випадку механізми шифрування, що шифрують вміст інформації, не допоможуть виявити атаку. Однак механізм аутентифікації дозволить виявити, якщо не авторизований вузол намагається надсилати повідомлення.

### 3.3 Оцінка дієвості політики безпеки та прогнозування ризиків (на основі простої лінійної регресійної моделі)

Зміна функції (залежної змінної, результату) в залежності від зміни одного чи декількох аргументів (незалежних змінних, факторів) називається *регресією*.

Методи регресійного аналізу успішно використовуються для аналізу експериментальних даних в економіці, соціології, біології, психології, медицині, техніці тощо, причому найбільш поширені так звані лінійні регресійні моделі.

Для прогнозу частоти небажаних подій (загроз  $i$ -го виду) будемо використовувати рівняння виду  $y = ax + b + \varepsilon$  (лінійної регресії), де  $y$  – залежна (результуюча змінна),  $x$  – незалежна змінна (регресор),  $a$  та  $b$  – параметри,  $\varepsilon$  – помилка. У нас  $y$  – частота небажаної події (частота певної атаки, яку ми вимірювали за даними за деякий попередній період). Показників може бути декілька (наприклад, вартість пошкоджених активів, катастрофічність наслідків атаки для репутації (у кількісному виразі)), за кожним можна будувати своє рівняння регресії.

Для розрахунку параметрів моделей  $a$  та  $b$  використовується метод найменших квадратів (МНК).

Послідовність етапів знаходження параметрів моделей:

1) Заповнення таблиці зі статистичними даними «час» – «показник». Наприклад, на 10.01.19 було  $N_1$  DDos атак, на дату 10.02.19 –  $N_2$ , на дату 10.03.19 –  $N_3$ . Якщо прийняти першу дату за показник часу  $t_1=30$ , другий показник часу –  $t_2=60$ ; третій показник часу  $t_3=90$  днів, і т.д. то одержуємо ряд значень часових даних  $x_i=t_i: 30, 60, 90 \dots$ , де  $i=1..T$ , і відповідні значення показника ефективності для відповідного часового моменту  $y_i=N_i: N_1, N_2, N_3 \dots$ .

2) Розрахунок параметрів лінійної регресії:

$$a_{\text{МНК}} = \frac{\text{cov}_{x,y}}{\sigma^2} \quad (3.1) \text{ та } b = \bar{y} - a_{\text{МНК}} \cdot \bar{x} \quad (3.2), \text{ де}$$

$$\bar{x} = \frac{\sum_{i=1}^T x_i}{T} - \text{середнє значення незалежної змінної}, \quad (3.3)$$

$$\bar{y} = \frac{\sum_{i=1}^T y_i}{T} - \text{середнє значення залежної змінної}, \quad (3.4)$$

$$\sigma^2 = \frac{\sum_{i=1}^T (x_i - \bar{x})^2}{T-1} - \text{дисперсія}, \quad (3.5)$$

$$\text{cov}_{x,y} = \frac{\sum_{i=1}^T (x_i - \bar{x})(y_i - \bar{y})}{T-1} - \text{коваріація змінних } x \text{ і } y. \quad (3.6)$$

Перевірка адекватності моделі. Розрахунок коефіцієнта детермінації  $R^2$  та обчислення похибки апроксимації  $\varepsilon$ :

$$R^2 = \frac{\sum_{i=1}^T (y_i^* - \bar{y})^2}{\sum_{i=1}^T (y_i - \bar{y})^2}, \quad (3.7)$$

$$\varepsilon = \frac{1}{T} \cdot \sum_{i=1}^T \left| \frac{y_i - y_i^*}{y_i} \right| \cdot 100, \quad (3.8)$$

$$\text{де } y_i^* = ax_i + b. \quad (3.9)$$

Якщо коефіцієнт детермінації близький до 1, це свідчить про лінійний взаємозв'язок між змінними  $X$  та  $Y$ . Значення похибки апроксимації  $\varepsilon$  показує точність побудованої моделі для опису явища залежності частоти атак, чи їх катастрофічності в залежності від часу (фактично, від терміну експлуатації системи захисту із налаштованою політикою).

Для оцінювання ефективності політики будуть використовуватись дані про частоту здійснених DDoS-атак за 6 місяців. Вони наведені в таблиці 3.1. Для

інших атак в таблицях 3.2-3.3. Обчислення виконуються з допомогою застосунку, який наведено в Додатку А.

Таблиця 3.1 – Дані, необхідні для побудови регресійної моделі DDoS-атак

Час(дні)	30	60	90	120	150	180
К-сть атак DDoS	532	414	699	538	322	217

Було розроблено програмний застосунок на мові програмування Python, який дозволяє обчислити параметри лінійної регресії та побудувати графік для визначення ефективності політики безпеки. Обчислені параметри показані на рисунку 3.14. Для інших атак результати на рисунках 3.16, 3.18. Програмний код наведено в Додатку А.

```
D:\11 семестр\мій диплом\Scripts>python linear_regression.py
Dataset Headers :: ['days' 'attacks_frequency']
x' = 105.0
y' = 453.666666667
variance_x = 3150.0
variance_y = 29671.4666667
covariance = -6035.999999999999
a = -1.916190476190476
b = 654.8666666666667
R^2 numerator = 57830.6285714
R^2 denominator = 148357.333333
R^2 = 0.38980633631
error of approximation = 25.2748633407
```

Рисунок 3.14 – Одержані параметри лінійної регресії для DDoS-атак

Враховуючи знайдені параметри  $a$  і  $b$ , можна побудувати графік залежності частоти атак від кількості пройдених днів. Він зображений на рисунку 3.15. Для інших атак результати на рисунках 3.17, 3.19.

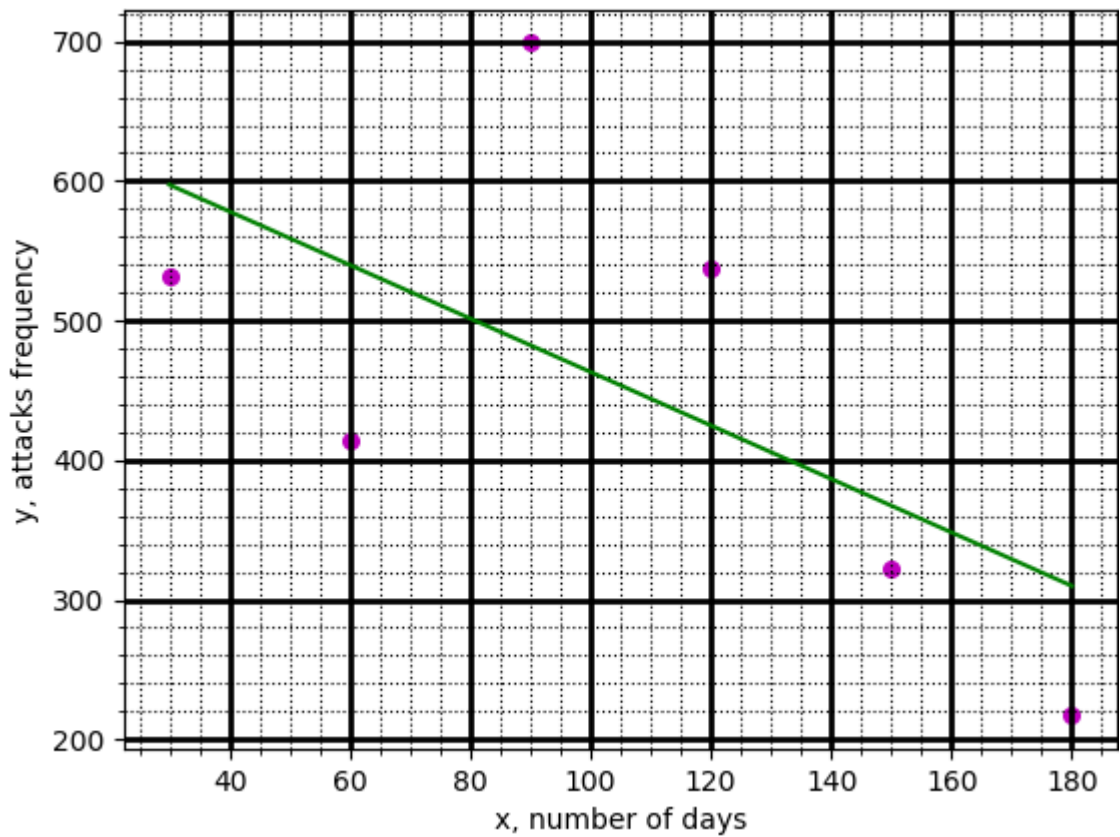


Рисунок 3.15 – Графік залежності частоти DDoS-атак від кількості днів

Таблиця 3.2 – Дані, необхідні для побудови регресійної моделі атак шкідливого ПЗ

Час(дні)	30	60	90	120	150	180
К-сть атак шкідливого ПЗ	184	216	151	133	121	95



```

D:\11 семестр\мій диплом\Scripts>python linear_regression.py
Dataset Headers :: ['days' 'attacks_frequency']
x' = 105.0
y' = 150.0
variance_x = 3150.0
variance_y = 1933.6
covariance = -2244.0
a = -0.7123809523809523
b = 224.8
R^2 numerator = 7992.91428571
R^2 denominator = 9668.0
R^2 = 0.826739168982
error of approximation = 6.93599252901

```

Рисунок 3.16 – Одержані параметри лінійної регресії для атак шкідливого ПЗ

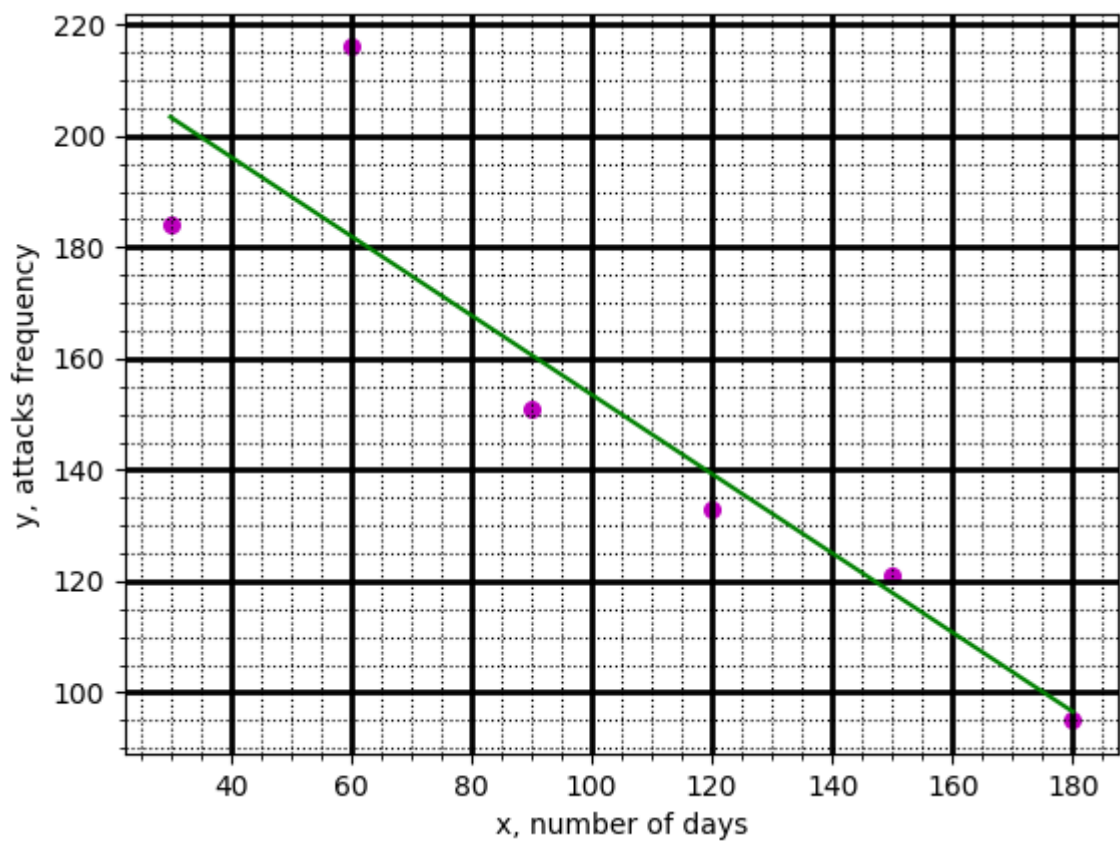


Рисунок 3.17 – Графік залежності частоти атак шкідливого ПЗ від кількості днів

Таблиця 3.3 – Дані, необхідні для побудови регресійної моделі атак через експлойти ПЗ

Час(дні)	30	60	90	120	150	180
К-сть атак через експлойти ПЗ	64	82	77	96	87	92

```

D:\11 семестр\мій диплом\Scripts>python linear_regression.py
Dataset Headers :: ['days' 'attacks_frequency']
x' = 105.0
y' = 83.0
variance_x = 3150.0
variance_y = 132.8
covariance = 522.0
a = 0.1657142857142857
b = 65.6
R^2 numerator = 432.514285714
R^2 denominator = 664.0
R^2 = 0.651376936317
error of approximation = 6.89320757881

```

Рисунок 3.18 – Одержані параметри лінійної регресії для атак через експлойти ПЗ

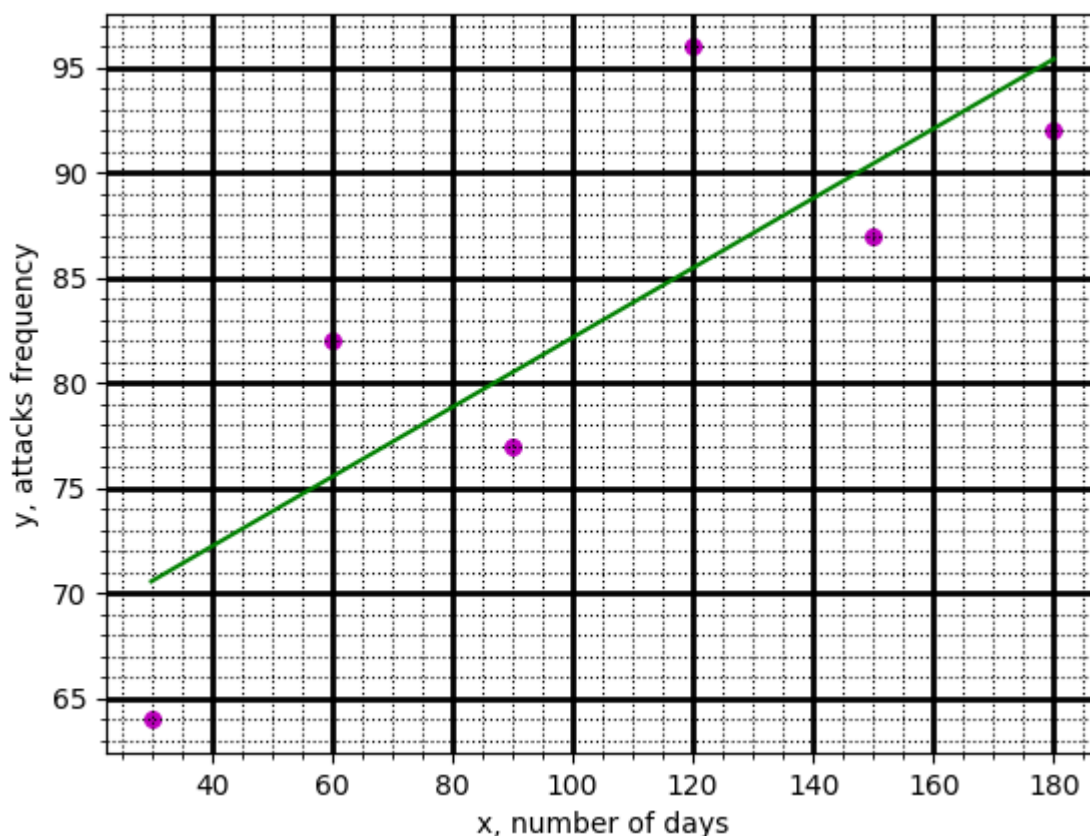


Рисунок 3.19 – Графік залежності частоти атак через експлойти ПЗ від кількості днів

Далі визначимо кореляцію між рівнем фінансових вкладень на зменшення певного ризику (в грн, вісь X) та величиною ризику за 6 місяців (180 днів, вісь Y). Будуть оцінюватись ті ж 3 атаки (DDoS-атаки, атаки шкідливого ПЗ та експлойти ПЗ), для яких наслідки реалізації є найвищими. Вхідні дані наведені в таблицях 3.4-3.6.

Таблиця 3.4 – Дані, необхідні для побудови регресійної моделі ризиків DDoS-атак

Фінансові вкладення(грн)	23000	25000	14000	17000	25500	32000
Ризик	2.1	2.0	2.5	2.15	1.8	1.7
Час(дні)	30	60	90	120	150	180

```

D:\11 семестр\мій диплом\Scripts>python linear_regression_2.py
Dataset Headers :: ['financial_investments' 'risk_quantity']
x' = 22750.0
y' = 2.04166666667
variance_x = 41575000.0
variance_y = 0.0804166666667
covariance = -1707.5
a = -4.107035478051714e-05
b = 2.9760172379234313
R^2 numerator = 0.350638153939
R^2 denominator = 0.402083333333
R^2 = 0.872053439847
error of approximation = 4.18467128272

```

Рисунок 3.20 – Одержані параметри лінійної регресії для ризиків від DDoS-атак

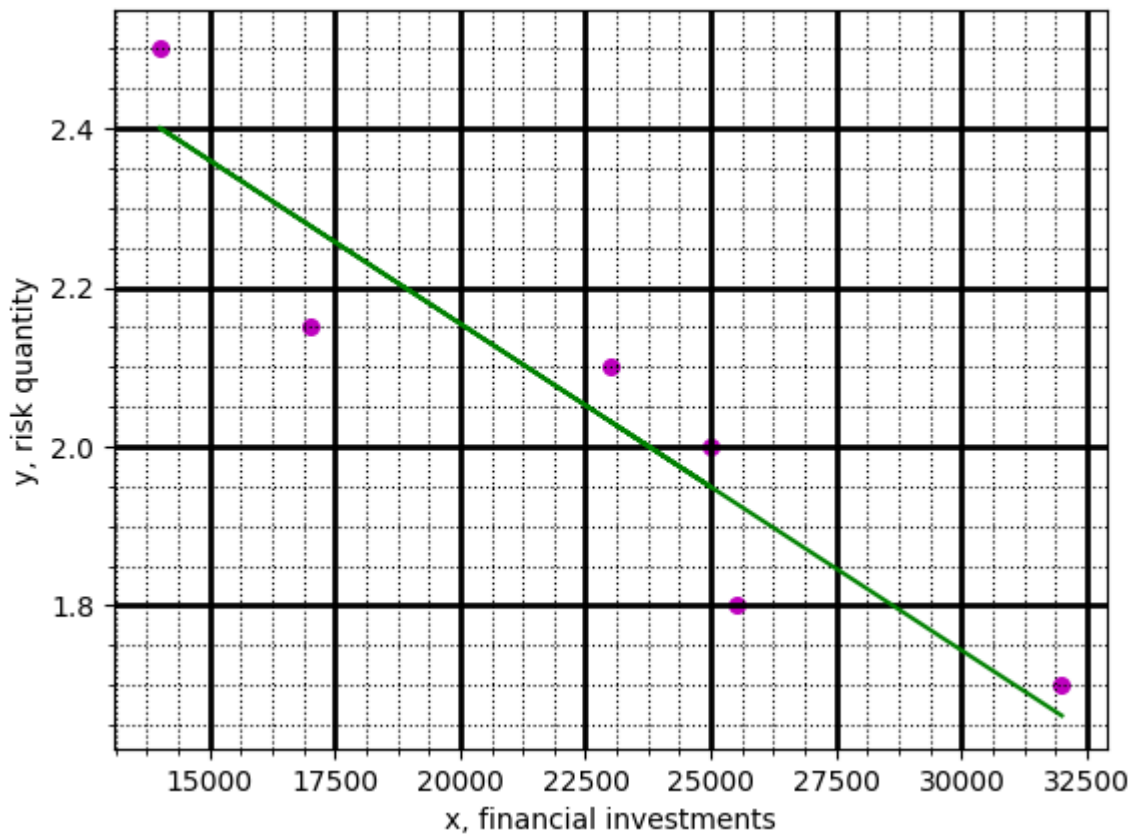


Рисунок 3.21 – Графік залежності фінансових вкладень та величини ризику для DDoS-атак

Таблиця 3.5 – Дані, необхідні для побудови регресійної моделі ризиків атак шкідливого ПЗ

Фінансові вкладення(грн)	21000	18000	25500	27000	31000	35000
Ризик	3.9	4.25	3.6	3.5	3.2	3.0
Час(дні)	30	60	90	120	150	180

```
D:\11 семестр\мій диплом\Scripts>python linear_regression_2.py
Dataset Headers :: ['financial_investments' 'risk_quantity']
x' = 26250.0
y' = 3.575
variance_x = 39175000.0
variance_y = 0.20775
covariance = -2832.4999999999999
a = -7.230376515634969e-05
b = 5.472973835354179
R^2 numerator = 1.02400207403
R^2 denominator = 1.03875
R^2 = 0.98580223733
error of approximation = 1.26004135073
```

Рисунок 3.22 – Одержані параметри лінійної регресії для ризиків від атак шкідливого ПЗ

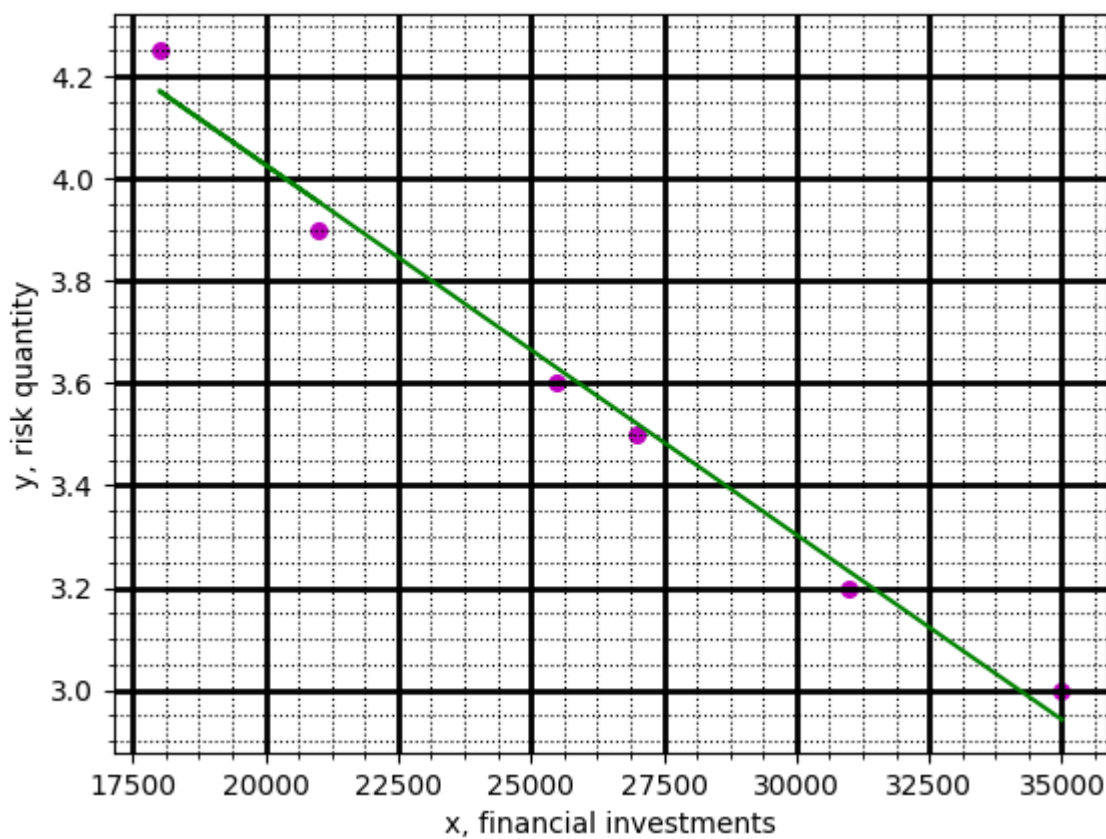


Рисунок 3.23 – Графік залежності фінансових вкладень та величини ризику для атак шкідливого ПЗ

Таблиця 3.6 – Дані, необхідні для побудови регресійної моделі ризиків атак через експлойти ПЗ

Фінансові вкладення(грн)	38000	35000	30000	19000	24000	28000
Ризик	2.22	2.9	2.65	3.6	3.15	3.4
Час(дні)	30	60	90	120	150	180



```

D:\11 семестр\мій диплом\Scripts>python linear_regression_2.py
Dataset Headers :: ['financial_investments' 'risk_quantity']
x' = 29000.0
y' = 2.98666666667
variance_x = 48800000.0
variance_y = 0.256466666667
covariance = -3024.0
a = -6.19672131147541e-05
b = 4.783715846994536
R^2 numerator = 0.936944262295
R^2 denominator = 1.28233333333
R^2 = 0.730655780318
error of approximation = 7.46204353675

```

Рисунок 3.24 – Одержані параметри лінійної регресії для ризиків від атак через експлойти ПЗ

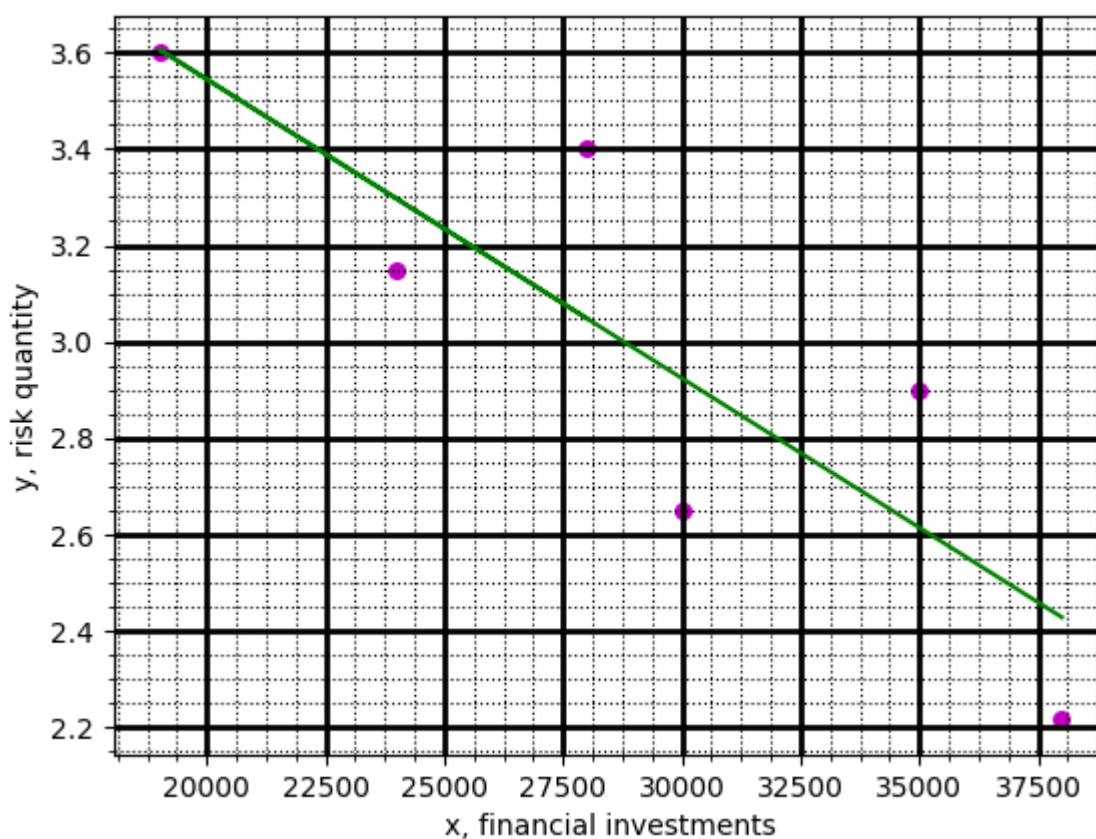


Рисунок 3.25 – Графік залежності фінансових вкладень та величини ризику для атак через експлойти ПЗ

Отже, бачимо, що чим більше фінансових вкладень для найбільш небезпечних атак, тим більшу величину ризику вони покривають. Залежність добре апроксимується, що показує значення коефіцієнту детермінації, яке наближається до 1. Тобто покращення політики безпеки, які запроваджені цими фінансовими вкладеннями, дають позитивний ефект.

### **3.4 Модель прогнозування ризиків з використанням множинної регресії**

Кількісне прогнозування схильності до атак може допомогти організаціям протистояти атакам. Загальна система оцінювання вразливості (CVSS) – це стандартний фреймворк, який використовується багатьма організаціями. Він передає характеристики та наслідки вразливостей в ІТ сфері.

У запропонованій моделі потенційний вплив вразливості прогнозується задовго до випуску ІТ-програми для використання. За допомогою цієї інформації про вплив можна забезпечити адекватну вартість та ресурси для усунення вразливих ситуацій, тим самим зменшуючи вплив.

Метод множинної регресії обраний для прогнозування впливу атак. Множинні регресії мають певні основні припущення, такі як лінійність, відсутність мультиколінеарності, гомоскедастичності та нормальності.

Нижче описано визначення метрик кібербезпеки.

$Y$  – це загальна оцінка CVSS, залежна змінна. CVSS прогнозується, виходячи з середовища та характеристик IoT-пристрою.

$X_1$  – кількість уразливостей, а саме загальна кількість уразливостей, виявлених статичними та динамічними інструментами виявлення вразливостей для IoT-пристрою. У даній моделі вразливості, про які повідомляють



інструменти, можна широко класифікувати на 23 категорії. Вони були описані в моделі загроз у розділі 2.

$X_2$  – середній мережевий трафік вхідного сигналу, записаний протягом тижня атаки в MBPS(мегабайт/секунду).

В таблиці 3.7 будуть наведені дані про атаки(оцінка CVSS), кількість зафіксованих вразливостей та швидкість інтернет-трафіку.

Таблиця 3.7 – Дані, необхідні для рівняння множинної регресії

№	$X_1$ Вразливість	$X_2$ Мережевий трафік, MBPS	$Y$ Оцінка CVSS
1	2	3	4
1	20	0.324	2.1
2	53	0.623	5.3
3	15	0.235	1.0
4	85	0.832	8.0
5	28	0.438	2.9
6	25	0.498	3.0
7	38	0.391	3.8
8	18	0.132	1.0
9	16	0.177	1.2
10	63	0.823	5.9
11	39	0.579	4.3
12	30	0.455	2.8
13	14	0.231	1.1
14	35	0.725	4.2
15	51	0.740	5.4
16	21	0.345	1.9
17	25	0.432	2.0
18	37	0.467	4.1

Продовження таблиці 3.7

1	2	3	4
19	58	0.845	6.2
20	15	0.111	1.1
21	22	0.191	2.3
22	16	0.182	1.2
23	30	0.292	2.8

Були отримані такі результати для множинної регресії з використанням методу градієнтного спуску. Він дозволив зменшити похибку апроксимації. Це зображено на рисунках 3.26-3.27. Код програми наведено у Додатку Б.

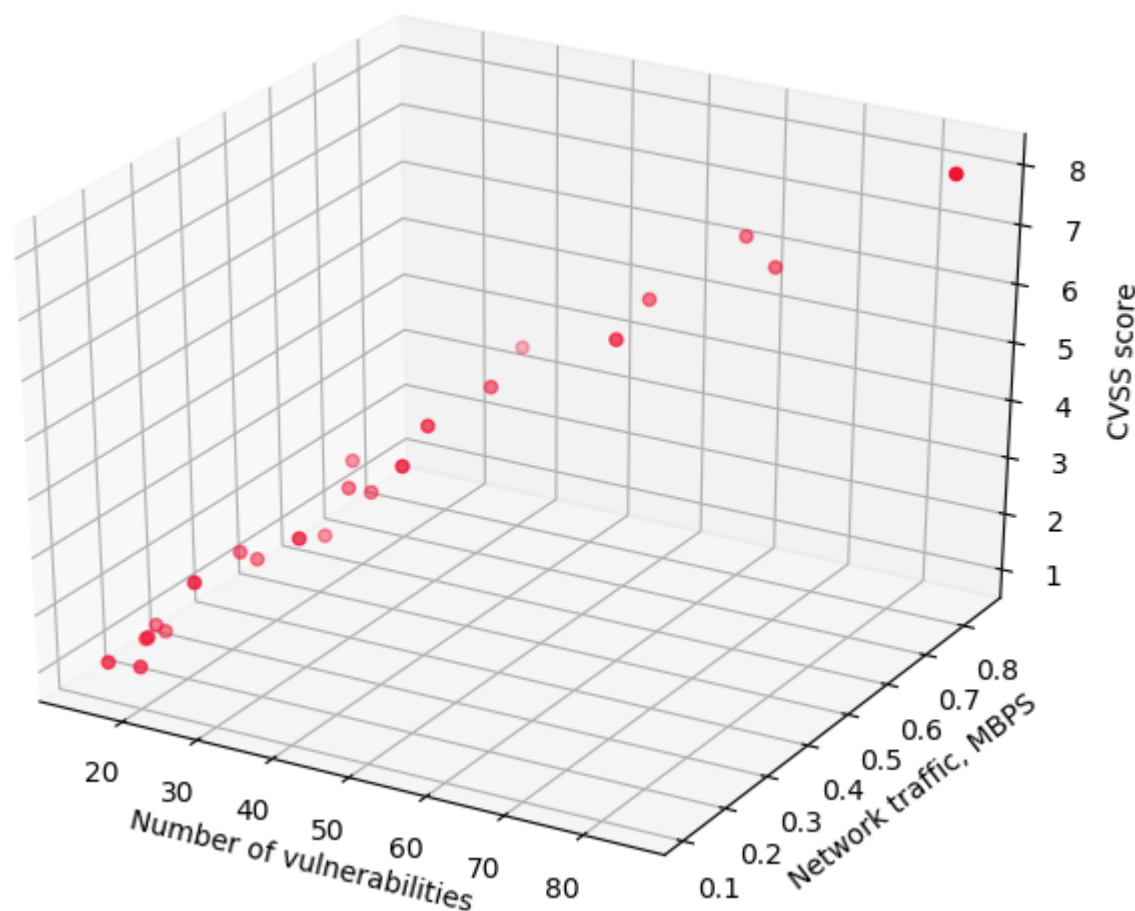


Рисунок 3.26 – Одержаний графік для множинної регресії

```

D:\11 семестр\мій диплом\Scripts>python multiple_regression.py
Initial Error of Approximation
6.947391304347825
New Coefficients
[-0.20121785  0.10074424  0.23957254]
Final Error of Approximation
0.06608968020607295
R2 Score
0.9638338652215162

```

Рисунок 3.27 – Параметри для множинної регресії та коефіцієнт детермінації

В таблиці 3.8 наведені параметри для рівняння множинної регресії.

Таблиця 3.8 – Параметри рівняння регресії

Intercept (перетин з віссю Y)	Вразливість	Мережевий трафік
-0.20121785	0.10074424	0.23957254

Як показано в таблиці 3.8, вразливість позитивно впливає на показник CVSS. Зі збільшенням вразливості показник CVSS збільшується, а отже, вплив на ІТ-активи високий. Вплив мережевого трафіку на CVSS позитивний. Це означає, що коли мережевий трафік великий, вплив вразливостей великий, а показник CVSS теж буде великим. Отже, на показник CVSS позитивно впливає як вразливість, так і мережевий трафік. Його можна обчислити за формулою:

Прогнозована оцінка CVSS =  $-0.20121785 + 0.10074424 * \text{Кількість вразливостей на ПоТ-пристрої} + 0.23957254 * \text{Пропонований середній вхідний мережевий трафік ПоТ-пристрою за тиждень, виміряний в MBPS}$  (3.10)

Прогнозування оцінки CVSS допомагає розставити пріоритети вразливості та усунути ті, що мають великий ризик. Оцінки CVSS поширюються постачальниками застосунків зі своїми клієнтами. Це допомагає клієнтам зрозуміти ступінь вразливості та дозволяє їм ефективно управляти своїми ризиками. Бюлетені про вразливість поширюються між кількома організаціями. Ці бюлетені описують дату атаки, системи, на які впливають, та виконані виправлення. Таким чином, модель прогнозування CVSS життєво важлива і повинна використовуватись широко. Технічним аналітикам слід використовувати модель прогнозування. Для кожного сценарію аналітик повинен документувати припущення та пов'язані з цим ризики. Має бути розроблений детальний план запобігання атакам. На кожному кроці напад, його тип, причина та профілактичні дії повинні бути задокументовані. Після виявлення першопричини слід також продумати наступні кроки щодо коригувальних та профілактичних дій.

Моделі прогнозування повинні бути багаторазово здійснені. Технічні аналітики повинні використовувати цю модель постійно, а також пропонувати недоліки. Виходячи з балів, рішення повинні прийматися з урахуванням впливу на витрати та безпеку. Моделі прогнозування мають статистичний та імітаційний характер. Ці моделі повинні допомогти моделювати сценарії, а також визначати результати. Вони також можуть моделювати різні коефіцієнти варіації та допомагати аналітику з передбачуванним діапазоном або варіацією його результатів.

### **3.5 Тестування на проникнення для ІоТ**

Тестування на проникнення для промислового ІоТ проводяться для протоколів обміну даними, таких як: Modbus TCP, Profinet, S7comm, WDB RPC. Типовим фреймворком для здійснення пентестів є ISF (Industrial Exploitation

Framework). В таблиці 3.9 наведено клієнти для промислових протоколів обміну даними. А в таблиці 3.10 показані модулі для проведення експлойтів.

Таблиця 3.9 – Клієнти для промислових протоколів

Ім'я	Шлях	Опис
modbus_tcp_client	icssplit/clients/modbus_tcp_client.py	Клієнт Modbus-TCP
wdb2_client	icssplit/clients/wdb2_client.py	Клієнт WdbRPC версії 2 (Vxworks 6.x)
s7_client	icssplit/clients/s7_client.py	Клієнт s7comm (S7 300/400 PLC)

Таблиця 3.10 – Модулі для використання експлойтів

Ім'я	Шлях	Опис
1	2	3
s7_300_400_plc_control	exploits/plcs/siemens/s7_300_400_plc_control.py	S7-300/400 PLC запуск/зупинка
s7_1200_plc_control	exploits/plcs/siemens/s7_1200_plc_control.py	S7-1200 PLC запуск/зупинка/скидання
vxworks_rpc_dos	exploits/plcs/vxworks/vxworks_rpc_dos.py	Віддалена DoS Vxworks RPC (CVE-2015-7599)
quantum_140_plc_control	exploits/plcs/schneider/quantum_140_plc_control.py	Schneider Quantum 140 серії PLC запуск/зупинка
crash_qnx_inetd_tcp_service	exploits/plcs/qnx/crash_qnx_inetd_tcp_service.py	DoS служби QNX Inetd TCP

## Продовження таблиці 3.10

qconn_remote_exec	exploits/plcs/qnx/qconn_remote_exec.py	Віддалене виконання коду QNX qconn
profinet_set_ip	exploits/plcs/siemens/profinet_set_ip.py	Налаштування IP для Profinet DCP

На рисунках 3.28-3.31 показано процес проведення тестування на проникнення для протоколу S7comm.

```

root@kali:~/Desktop/temp/isf# python isf.py

  ICS SPLOIT

      ICS Exploitation Framework

Note    : ICS SPLOIT is fork from routersploit at
          https://github.com/reverse-shell/routersploit
Dev Team : wenzhe zhu(dark-lbp)
Version  : 0.1.0

Exploits: 2 Scanners: 0 Creds: 13

ICS Exploits:
  PLC: 2      ICS Switch: 0
  Software: 0

isf > use exploits/plcs/
exploits/plcs/siemens/  exploits/plcs/vxworks/
isf > use exploits/plcs/siemens/s7_300_400_plc_control
exploits/plcs/siemens/s7_300_400_plc_control
isf > use exploits/plcs/siemens/s7_300_400_plc_control
isf (S7-300/400 PLC Control) >

```

Рисунок 3.28 – Запуск та використання експлойтів

```

r00t@r00t-KitPloit: ~
isf (S7-300/400 PLC Control) > show options

Target options:

  Name      Current settings  Description
  ----      -
  target     192.168.1.1          Target address e.g. 192.168.1.1
  port       102                  Target Port

Module options:

  Name      Current settings  Description
  ----      -
  slot       2                  CPU slot number.
  command    1                  Command 0:start plc, 1:stop plc.

isf (S7-300/400 PLC Control) >

```

Рисунок 3.29 – Зображення опцій модуля

```

r00t@r00t-KitPloit: ~
isf (S7-300/400 PLC Control) > run
[*] Running module...
[+] Target is alive
[*] Sending packet to target
[*] Stop plc
isf (S7-300/400 PLC Control) >

```

Рисунок 3.30 – Запуск модулю

```

isf (S7-300/400 PLC Control) > show info

Name:
S7-300/400 PLC Control

Description:
Use S7comm command to start/stop plc.

Devices:
- Siemens S7-300 and S7-400 programmable logic controllers (PLCs)

Authors:
- wenzhe zhu <jtrkid[at]gmail.com>

References:

isf (S7-300/400 PLC Control) >

```

Рисунок 3.31 – Відображення інформації про експлойт

### 3.6 Оцінювання дієвості політики безпеки з використанням критеріїв по їх важливості

Рівень дієвості політики безпеки визначається по результатам оцінювання експертами важливості визначених критеріїв. Це робиться за допомогою методу Сааті.

Метод Сааті. Використовується для експертного визначення важливості критеріїв дієвості політики безпеки. Сааті запропонував використовувати шкалу порівняння показників:

- 1 – рівна важливість критеріїв;
- 2 – помірна перевага одного критерію над іншим;
- 3 – суттєва перевага одного критерію над іншим;
- 4 – значна перевага одного критерію над іншим;
- 5 – дуже сильна перевага одного критерію над іншим.

В нашому випадку можна визначити критерії оцінки дієвості політики безпеки таким способом (бали – порівняння важливості одного критерію над іншим):

- 1) Спад прогнозованих значень основних ризиків – 4 бали
- 2) Наявність кореляції між фінансовими вкладеннями в покращення захисту, вдосконалення політики безпеки та значеннями ризиків – 5 балів

Для 1) і 2) шкала оцінки від 0 до 5:

Значення  $R^2$  в діапазоні  $[0, 0.01]$  – 0 балів;  $R^2$  в діапазоні  $[0.02, 0.2]$  – 1 бал;  $R^2$  в діапазоні  $[0.21, 0.4]$  – 2 бали;  $R^2$  в діапазоні  $[0.41, 0.6]$  – 3 бали;  $R^2$  в діапазоні  $[0.61, 0.8]$  – 4 бали;  $R^2$  в діапазоні  $[0.81, 1]$  – 5 балів.

- 3) Відповідність середньому рівню та вище, за чеклістами вимог безпеки – 3 бали



Шкала оцінки від 0 до 5:

Відсутність чеклістів вимог безпеки – 0 балів; Дуже низький рівень безпеки за чеклістами – 1 бал; Низький рівень безпеки за чеклістами – 2 бали; Середній рівень безпеки за чеклістами – 3 бали; Рівень вище середнього за чеклістами – 4 бали; Високий рівень безпеки за чеклістами – 5 балів.

4) Наявність успішних результатів моделювання майбутніх запроваджень політики безпеки – 3 бали

Шкала оцінки від 0 до 5:

Відсутність моделювання запроваджень – 0 балів; Змодельовано мережу з 1 атакою з низьким ризиком – 1 бал; Змодельовано декілька атак з низьким ризиком – 2 бали; Змодельовано атаки з середнім ризиком – 3 бали; Змодельовано 1 атаку з високим ризиком – 4 бали; Змодельовано декілька атак з високим ризиком – 5 балів.

5) Результати тестування на проникнення свідчать про відсутність можливостей здійснення НСД (несанкціонованого доступу) – 4 бали

Шкала оцінки від 0 до 5:

Переважає кількість тестів свідчить про можливість НСД – 1 бал; Значна кількість тестів свідчить про НСД – 2 бали; Половина тестів свідчить про успішне виконання НСД – 3 бали; Незначна частина тестів свідчить про НСД – 4 бали; Тести свідчать про неможливість НСД – 5 балів.

6) Виконання організаційних заходів із забезпечення політики безпеки, ініційованих вищим менеджментом – 2 бали

Шкала оцінки від 0 до 5:

Організаційні заходи відсутні – 0 балів; Дуже мала кількість заходів – 1 бал; Мала кількість заходів – 2 бали; Середня кількість заходів – 3 бали; Більше середньої кількості заходів – 4 бали; Велика кількість заходів – 5 балів.

7) Застосування шаблонів безпеки – 1 бал

Шкала оцінки від 0 до 5:

Повна відсутність шаблонів безпеки – 0 балів; 1-2 шаблони безпеки – 1 бал; 3-5 шаблонів безпеки – 2 бали; 6-8 шаблонів безпеки – 3 бали; 9-12 шаблонів – 4 бали; 13 і більше шаблонів – 5 балів.

Попередньо експерти визначають коефіцієнти важливості (КВ)  $P_j, j = 1 \dots n$ . При цьому використовується метод відносного ранжування.

#### Метод відносного ранжування

Кожні два критерії порівнюються за важливістю, і експерт віддає свій голос одному з них, або розділяє голос навпіл при однаковій важливості. Після формування КВ голоси, одержані кожним критерієм, нормуються по формулі:

$$W_j = \frac{P_j}{\sum_{j=1}^n P_j} \quad (3.11)$$

таким чином, щоб виконувалось  $\sum_{j=1}^n W_j = 1$ .

Далі вводиться лінгвістична змінна «дієвість політики», базова термножина якої представлена п'ятьма нечіткими термами  $T = \{T_1, \dots, T_5\}$ , які мають назви «не дієва», «не достатньо дієва», «достатня (середня) дієвість», «суттєво дієва», «ефективно діюча». Задається діапазон зміни параметрів (носителів)  $X_j^*$ ,  $j=1\dots n$  ( $n=7$  – кількість критеріїв), де  $X_j^*$  – це усереднені оцінки критеріїв експертами в балах. Наприклад, для  $X_j^*$  ( $j = 1,2$ ) обчислюється середнє значення коефіцієнта детермінації для загроз із найбільшим значенням ризику. На діапазон  $[0, 1]$  (в ньому знаходиться значення коефіцієнту детермінації  $R^2$ ) переноситься 5-бальна шкала для оцінки критерію експертами.

Для побудови показника експерт повинен оцінити  $n$  критеріїв по  $N$ -бальній шкалі.

Функції приналежності  $\mu_i^j(X_j^*), i = 1 \dots L$  нечіткого терма з номером  $i$  визначаються так:

$$\mu_i^j(X_j^*) = \left( \frac{1}{1+(X_j^*-i+1)^2} \right)^{W_j} \quad (3.12)$$

Далі формується показник оцінки дієвості:

$$\mu_s(X_j^*) = \bigvee_{i=1}^L \bigwedge_{j=1}^n \mu_i^j, \quad (3.13)$$

$j = 1 \dots L$  – номер терма з базової терм-множини,  $j = 1 \dots n$  – номер критерію. Операції  $\bigwedge, \bigvee$  знаходяться як мінімальне та максимальне значення відповідно по заданій множині значень функції  $\mu_i^j$ . Отримані результати наведені в таблицях 3.11-3.12

Таблиця 3.11 – Результати обчислень важливості критеріїв

№	1	2	3	4	5	6	7	Pj	Wj, j = 1...7	X*j, j = 1...7	шкала оцінки
1	1	2,3	2,9	2,5	2,9	3,4	3,9	18,9	0,16875	2,7	5
2	2,7	1	3,1	2,7	3,1	3,5	4,1	20,2	0,180357	4,9	5
3	2,1	1,9	1	2,1	2,5	3	3,6	16,2	0,144643	3,8	5
4	2,5	2,3	2,9	1	2,9	3,4	3,9	18,9	0,16875	4,8	5
5	2,1	1,9	2,5	2,1	1	3	3,6	16,2	0,144643	3,5	5
6	1,6	1,5	2	1,6	2	1	3,4	13,1	0,116964	2,8	5
7	1,1	0,9	1,4	1,1	1,4	1,6	1	8,5	0,075893	3,2	5
Сума								112	1		

Таблиця 3.12 – Результати обчислень (продовження)

	$\mu_1$	$\mu_2$	$\mu_3$	$\mu_4$	$\mu_5$
1	2	3	4	5	6
1	0,699832	0,795144	0,934921	0,985563	0,846212
2	0,559552	0,605072	0,667431	0,759096	0,898516
3	0,673086	0,72963	0,811439	0,930946	0,994343

## Продовження таблиці 3.12

1	2	3	4	5	6
4	0,584746	0,630109	0,692287	0,783668	0,919909
5	0,688144	0,750859	0,843257	0,968239	0,968239
6	0,774995	0,844541	0,94378	0,995423	0,900926
7	0,832251	0,874651	0,934544	0,997028	0,963152
	$\min \mu_1$	$\min \mu_2$	$\min \mu_3$	$\min \mu_4$	$\min \mu_5$
$\mu_i$	0,559552	0,605072	0,667431	0,759096	0,846212
					max

Отже, обчислили  $\mu_S = \max_i \mu_i = 0,846212$ . Тому дієвість політики безпеки відповідає значенню терма «ефективно діюча».

### Висновки до розділу 3

У ході роботи було запропоновано нову методику по оцінці дієвості політики безпеки. Для цього використовуються певні критерії, які порівнюються між собою за важливістю за методом відносного ранжування. З використанням функцій приналежності та нечітких термів обчислюється рівень дієвості політики безпеки.

В розділі описано моделювання DIS-атаки на WSN-мережі промислового Інтернету речей та наведено способи протидії, відповідно до політики безпеки. Побудовано 2 математичні моделі з використанням лінійної та множинної регресій. За допомогою цих моделей можна визначити дієвість політики безпеки, зокрема з використанням прогнозу ризиків. Також встановлено залежність між фінансовими вкладеннями на покриття ризиків та величиною ризику.

Модель множинної регресії дозволяє прогнозувати вплив атак на основі значущих факторів, які впливають на кібербезпеку. Вразливості та мережевий трафік були вибрані як фактори, що впливають на прогнозування показника CVSS. На основі цих оцінок технічний аналітик може проаналізувати вплив та вжити необхідних профілактичних заходів.

## 4 СТАРТАП

В розділі необхідно провести маркетинговий аналіз перспективи реалізації запропонованого в роботі програмно-технічного рішення, а саме реалізації політики безпеки для IoT та способу оцінки її дієвості, а також оцінити можливість його ринкового впровадження.

### 4.1 Опис ідеї проекту

На першому кроці маркетингового аналізу потрібно розглянути ідею проекту. Поетапно треба проаналізувати: зміст ідеї (що саме пропонується), потенційні напрями застосування, основні переваги, які може одержати користувач товару (за кожним напрямком застосування), чим відрізняється від існуючих аналогів та замінників.

Перші три пункти (таблиця 4.1) дають цілісне уявлення про зміст ідеї та можливі базові потенційні ринки, в межах яких потрібно здійснювати пошук групи потенційних клієнтів.

Таблиця 4.1 – Опис ідеї стартап-проекту

Зміст ідеї	Напрямки застосування	Вигоди для користувача
1	2	3
Розробка політики безпеки та застосунку, що буде оцінювати	Захист мереж промислового IoT	Зменшення кількості потенційних атак на мережу

Продовження таблиці 4.1

1	2	3
дієвість розробленої політики безпеки.	Перевірка дієвості розроблених правил та налаштувань мережі	Демонстрація, які саме розділи в політиці можна покращувати

Аналіз можливих техніко-економічних переваг ідеї передбачає визначення переліку техніко-економічних властивостей та характеристик ідеї, визначення попереднього кола конкурентів, порівняльний аналіз показників (W – Слабка сторона, N – Нейтральна сторона, S – Сильна сторона, які показано в таблиці 4.2).

Таблиця 4.2 – Визначення сильних, слабких та нейтральних характеристик ідеї проекту

Техніко-економічні характеристики ідеї	W Слабка сторона	N Нейтральна сторона	S Сильна сторона
1	2	3	4
Економічні	Ринком збуту будуть скоріш за все компанії, що надають апаратні чи програмні засоби захисту мереж	Відсутність аналогів на ринку (не вдалось знайти)	Допомагає зменшити кількість атак на мережу, в результаті колосальна економія від

## Продовження таблиці 4.2

1	2	3	4
	промислового Інтернету речей		потенційних збитків
Технологічні	Покриває лише мережі одного типу Інтернету речей	Немає	Забезпечує захист IoT- мережі, як апаратно, так і програмно
Надійності	Може не враховувати найновіші типи атак	Немає	Усі рекомендації, які показує застосунок, базуються на найкращих світових практиках

**4.2 Технологічний аудит ідеї проекту**

Наступним проводиться аудит технології, за допомогою якої можна реалізувати ідею проекту (технології створення товару) (Таблиця 4.3).



Таблиця 4.3 – Технологічна здійсненність ідеї проекту

Ідея проекту	Технології її реалізації	Наявність технологій	Доступність технологій
Використання вхідних даних, а саме кількості проведених атак по місяцям	Використання Python для алгоритмізації, та реалізації оцінки дієвості політики	Так	Усі технології доступні для використання
Розробка власної політики безпеки, на основі найкращих практик	Аналіз практик, та синтез основних положень, щодо покращення загального стану захищеності	Так	Перелік найкращих практик в загальному доступі, його слід використовувати при побудові абсолютно усіх мереж промислового IoT

Обрана технологія реалізації ідеї: використання можливостей Python, для обчислення регресії, а також для побудови відповідних графіків. В такому випадку, технологічно реалізація ідей відбувається за допомогою дуже гнучкого механізму, що дає змогу до найменших деталей проаналізувати вхідні дані.

### 4.3 Аналіз ринкових можливостей запуску стартап-проекту

Визначення ринкових можливостей, які можна використати під час ринкового впровадження проекту, та ринкових загроз, які можуть перешкодити реалізації проекту, дозволяє спланувати напрями розвитку проекту із урахуванням стану ринкового середовища, потреб потенційних клієнтів та пропозицій проектів-конкурентів. Спочатку проводиться аналіз попиту: наявність попиту, обсяг, динаміка розвитку ринку (таблиця 4.4).

Таблиця 4.4 – Попередня характеристика потенційного ринку стартап-проекту

Показники стану ринку (найменування)	Характеристика
Кількість головних гравців, од	0 (попередньо)
Загальний обсяг продаж, грн/ум. од	> 10 млрд. \$
Динаміка ринку (якісна оцінка)	Зростає
Наявність обмежень для входу (вказати характер обмежень)	Обмежена кількість клієнтів, потрібна інтеграція з компаніями, що представляють такі послуги
Специфічні вимоги до стандартизації та сертифікації	Залежить від законодавства окремої країни
Середня норма рентабельності в галузі (або по ринку), %	> 50 %

За результатами аналізу таблиці можна сказати, що загалом ринок є досить привабливим, але існує значне обмеження – потенційними покупцями є компанії, що виробляють апаратні та програмні рішення для промислового IoT та об'єктів критичної інфраструктури.

Середня норма рентабельності в галузі (або по ринку) порівнюється із банківським відсотком на вкладення. За умови, що останній є вищим, можливо, має сенс вкласти кошти в інший проект. Але в даній галузі рентабельність є досить високою, а отже вхід в галузь більш привабливий, ніж вкладення коштів в банк.

Потім визначаються потенційні групи клієнтів, їх характеристики, та формується орієнтовний перелік вимог до товару для кожної групи (таблиця 4.5).

Таблиця 4.5 – Характеристика потенційних клієнтів стартап-проекту

Потреба, що формує ринок	Цільова аудиторія (цільові сегменти ринку)	Відмінності у поведінці різних потенційних цільових груп клієнтів	Вимоги споживачів до товару
1	2	3	4
Забезпечення захисту мереж промислового Інтернету речей	Компанії, що виробляють продукти для ПОТ та об'єктів критичної інфраструктури	Компанія-виробник, займається виробництвом пристроїв з різними протоколами обміну даними	Точність та дієвість оцінки політики безпеки
Планується побудова власної мережі	Нова компанія, що будує власну мережу Інтернету речей	Відмінностей майже немає. Окрім відсутності	Точність та дієвість оцінки політики безпеки

Продовження таблиці 4.5

1	2	3	4
		єдиного стандарту/стеку технологій	

Також окремо можна виділити підгрупи у відповідних сегментах. Компанії, що займаються промисловим IoT або ті, що планують запустити власну мережу, можуть бути великими та середніми компаніями приватної та державної форми власності з відповідними особливостями функціонування.

Після визначення потенційних груп клієнтів проводиться аналіз ринкового середовища: складаються таблиці факторів, що сприяють ринковому впровадженню проекту, та факторів, що йому перешкоджають (таблиці 4.6-4.7).

Таблиця 4.6 – Фактори загроз

Фактор	Зміст загрози	Можлива реакція компанії
1	2	3
Покриває лише пристрої промислового IoT	Неможливо застосувати політику безпеки для мереж, які є іншими типами IoT	Розширювати кількість вендорів, що підтримає програмний продукт для мереж IoT інших типів

Продовження таблиці 4.6

1	2	3
Відсутність імені продукту	Від імені напряду залежить кількість продаж	Підвищення рейтингів, та постійний пошук компаній для інтеграції продукту у їх повсякденну роботу

Таблиця 4.7 – Фактори можливостей

Фактор	Зміст можливості	Можлива реакція компанії
Попит	У багатьох компаній, які займаються промисловим IoT, є мережі різних розмірів та складностей. Цим зумовлено попит на політику безпеки.	Розширення ринків збуту

Надалі проводиться аналіз пропозиції: визначаються загальні риси конкуренції на ринку (таблиця 4.8). Вказується тип конкуренції: монополія, олігополія, монополістична, чиста; рівень боротьби: локальний, національний, глобальний; галузева ознака: міжгалузева, внутрішньогалузева; вид: товарно-родова, товарно-видова, між бажаннями; характер переваг: цінова, нецінова; інтенсивність: марочна, не марочна. Описуються прояви відповідних характеристик та необхідні для конкурентоспроможності компанії.

Таблиця 4.8 – Ступеневий аналіз конкуренції на ринку

Особливості конкурентного середовища	В чому проявляється дана характеристика	Вплив на діяльність підприємства (можливі дії компанії, щоб бути конкурентоспроможною)
1	2	3
Тип конкуренції: чиста	Схожі програмні продукти знаходяться в рівних з нами обставинах	Постійний пошук нових компаній для інтеграції продукту
Рівень: глобальна	Ринок промислового IoT є глобальним, та по суті не жорстко географічно залежним	Використання англійської мови, як мови міжнародного спілкування, участь в міжнародних конференціях
Галузева ознака: внутрішньогалузева	Відбувається всередині галузі промислового Інтернету речей	Розробка додаткових заходів з підвищення дієвості
За видами товарів: між бажаннями, товарно-родова	Конкуренція як в аспекті задоволення бажання побудувати процес чи покращити технологію, так і в засобах покращення технології	Розширення покриття бажань, що задовольняються, та/або вдосконалення існуючого методу

## Продовження таблиці 4.8

1	2	3
За характером конкурентних переваг: цінова та нецінова	Ціна важлива, але також важливі інші показники	Встановлення певного співвідношення ціна/вигода
За інтенсивністю: не марочна	Ціни можуть значно відрізнятися	Виділення унікальних рис своєї марки

На основі аналізу конкуренції, а також із урахуванням характеристик ідеї проекту (таблиця 4.2), вимог споживачів до товару (таблиця 4.5) та факторів маркетингового середовища (таблиця 4.6-4.7) визначається та обґрунтовується перелік факторів конкурентоспроможності (таблиці 4.9).

Таблиця 4.9 – Обґрунтування факторів конкурентоспроможності

Фактор конкурентоспроможності	Обґрунтування (чинники, що роблять фактор значущим)
1	2
Ціновий	Вартість придбання послуги для клієнта досить важлива (для України зокрема, через придбання в форматі тендеру)
Репутаційний	Значний вплив імені та репутації компанії, що надає послугу на вибір клієнта
Технологічний	Як особливості технологічного покращення, так і співвідношення

## Продовження таблиці 4.9

1	2
	ціна/якість є дуже важливим аспектом у виборі конкретного товару споживачем

За визначеними факторами конкурентоспроможності (таблиця 4.9) проводиться аналіз сильних та слабких сторін стартап-проекту (таблиця 4.10).

Таблиця 4.10 – Порівняльний аналіз сильних та слабких сторін проекту

Фактор конкурентоспроможності	Бали	Рейтинг товарів-конкурентів (в порівнянні)						
		3	2	1	0	+1	+2	+3
Ціновий	18						+	
Репутаційний	12							+
Технологічний	16						+	

Фінальним етапом ринкового аналізу можливостей впровадження проекту є складання SWOT-аналізу (матриці аналізу сильних (Strength) та слабких (Weak) сторін, загроз (Troubles) та можливостей (Opportunities) (таблиця 4.11) на основі виділених ринкових загроз та можливостей, та сильних і слабких сторін (таблиця 4.10)).



Таблиця 4.11 – SWOT-аналіз стартап-проекту

<b>Сильні сторони:</b> Простота використовуваного методу, Новизна, Мінімальні витрати на технологію	<b>Слабкі сторони:</b> Відсутність «імені», Проблеми з початковими капіталовкладеннями
<b>Можливості:</b> Збільшення попиту на відповідну політику безпеки, Зростання видатків на ІБ департаменти компаній промислового IoT	<b>Загрози:</b> Зменшення клієнтських бюджетів на ІБ, Поява нових конкурентів

На основі SWOT-аналізу розробляються альтернативи ринкової поведінки (перелік заходів) для виведення стартап-проекту на ринок та орієнтовний оптимальний час їх ринкової реалізації з огляду на потенційні проекти конкурентів, що можуть бути виведені на ринок. Визначені альтернативи аналізуються з точки зору строків та ймовірності отримання ресурсів (таблиця 4.12).

Таблиця 4.12 – Альтернативи ринкового впровадження стартап-проекту

Альтернатива (орієнтовний комплекс заходів) ринкової економіки	Ймовірність отримання ресурсів	Строки реалізації
1	2	3
Участь в конкурсах стартапів, стартап-	Відповідно до конкуренції у відборах	До року (місяці-роки)

Продовження таблиці 4.12

1	2	3
акселератори для отримання початкових вкладень		
Прямий пошук початкових інвестицій	Досить імовірно	Місяці
Вихід з мінімальними початковими вкладеннями, еволюційний розвиток	~~1	Мінімально (тижні-місяці)

Загалом кожна з альтернатив може бути реалізованою, але з огляду на терміни реалізації доцільно спробувати отримати початкові інвестиції напряду(венчурні фонди, банківські кредити), а у випадку невдачі скористатись третьою альтернативою. Також можна брати участь у конкурсах.

#### 4.4 Розроблення ринкової стратегії проекту

Розроблення ринкової стратегії першим кроком передбачає визначення стратегії охоплення ринку: опис цільових груп потенційних споживачів (таблиця 4.13).

Таблиця 4.13 – Вибір цільових груп потенційних споживачів

Опис профілю цільової групи потенційних клієнтів	Готовність споживачів сприйняти продукт	Орієнтовний попит в межах цільової групи (сегменту)	Інтенсивність конкуренції в сегменті	Простота входу у сегмент
Компанії, що займаються безпекою промислового IoT	Можливо	Середній	Між бажаннями	Середня
Компанії, що будують свою мережу промислового IoT	Можливо	Середній	Між бажаннями	Середня

З огляду на загальну схожість характеристик обрано всі вказані цільові групи.

За результатами аналізу потенційних груп споживачів (сегментів) автори ідеї обирають цільові групи, для яких вони пропонуватимуть свій товар, та визначають стратегію охоплення ринку:

— якщо компанія зосереджується на одному сегменті – вона обирає стратегію концентрованого маркетингу;

— якщо працює із кількома сегментами, розробляючи для них окремо програми ринкового впливу – вона використовує стратегію диференційованого маркетингу;

— якщо компанія працює із всім ринком, пропонуючи стандартизовану програму (включно із характеристиками товару/послуги) – вона використовує масовий маркетинг.

Загалом на початковому етапі програма стандартизована, та робота відбувається в загальному по ринку, а отже застосовуватиметься масовий маркетинг. Але, сегменти мають певні відмінні один від одного риси, та бажано, принаймні в майбутньому використовувати стратегію диференційованого маркетингу.

Для роботи в обраних сегментах ринку необхідно сформувати базову стратегію розвитку (таблиця 4.14).

Таблиця 4.14 – Визначення базової стратегії розвитку

Обрана альтернатива розвитку	Стратегія охоплення ринку	Ключові конкурентоспроможні позиції відповідно до обраної альтернативи	Базова стратегія розвитку
Еволюційний розвиток з мінімальними початковими вкладеннями	Ексклюзивний розподіл	Низькі витрати, Індивідуальний підхід	Лідерство за витратами

Другий пункт ключових конкурентоспроможних позицій додає риси диференційованої стратегії розвитку, до лідерства за витратами. Адже

індивідуальний підхід та наявність власних, не скопійованих особливостей «товару» притаманна саме цій стратегії.

Наступним кроком є вибір стратегії конкурентної поведінки (таблиця 4.15).

Таблиця 4.15 – Визначення базової стратегії конкурентної поведінки

Чи є проект «першопрохідцем» на ринку ?	Компанія шукатиме нових споживачів, або забиратиме існуючих у конкурентів ?	Чи буде компанія копіювати основні характеристики товару конкурентів	Стратегія конкурентної поведінки
Так	Переважно нових	Ні	Стратегія зайняття конкурентної ніші

На основі вимог споживачів з обраних сегментів до постачальника (стартап-компанії) та до продукту (таблиця 4.5), а також в залежності від обраної базової стратегії розвитку (таблиця 4.14) та стратегії конкурентної поведінки (таблиці 4.15) розробляється стратегія позиціонування (таблиця 4.16), що полягає у формуванні ринкової позиції (комплексу асоціацій), за яким споживачі мають ідентифікувати торгівельну марку/проект.

Таблиця 4.16 – Визначення стратегії позиціонування

Вимоги до товару цільової аудиторії	Базова стратегія розвитку	Ключові конкурентоспроможні позиції власного стартап-проекту	Вибір асоціацій, які мають сформувати комплексну позицію власного проекту (три ключових)
Впровадження без порушення процесу функціонування, помітний результат, коректне співвідношення ціни послуги та вигоди клієнта	Лідерство за витратами	Індивідуальний підхід, Мінімізація власних витрат	Виправдана вартість, Дієва політика безпеки, Якісна оцінка політики безпеки

#### 4.5 Розроблення маркетингової програми стартап-проекту

Першим кроком є формування маркетингової концепції товару, який отримає споживач. Для цього (у таблиці 4.17) потрібно підсумувати результати попереднього аналізу конкурентоспроможності товару.

Таблиця 4.17 – Визначення ключових переваг концепції потенційного товару

Потреба	Вигода, яку пропонує товар	Ключові переваги перед конкурентами (існуючі або такі, що потрібно створити)
Зменшення ризиків завдяки впровадженні політики безпеки	Оцінка дієвості політики дозволяє зменшити ризики	Підвищення рівня захисту мереж промислового IoT
Структура політики безпеки, що відповідає найкращим практикам	Переформування структури з виділенням чітких правил	Індивідуальний підхід у визначенні правил для політики безпеки

Надалі розробляється трирівнева маркетингова модель товару: уточнюється ідея продукту та/або послуги, його фізичні складові, особливості процесу його надання (таблиця 4.18).

Таблиця 4.18 – Опис трьох рівнів моделі товару

Рівні товару	Сутність та складові	
1	2	
1. Товар за задумом	Оцінка дієвості політики безпеки з використанням програмного засобу	
2. Товар у реальному виконанні	Властивості/характеристики	Оцінка
	Дієвість політики безпеки Зменшення ризиків проведення атак	В кількісному вираженні оцінюється індивідуально

Продовження таблиці 4.19

1	2
	Якість: вигода також оцінюється індивідуально, для підтвердження порівнюється результат з існуючими політиками безпеки
3.Товар із підкріпленням	До продажу: полегшення захисту мереж промислового IoT та розробка політики безпеки під кожен компанію окремо
	Після продажу: гарантійне обслуговування при виявленні помилок чи вразливостей
За рахунок чого потенційний товар буде захищено від копіювання: захист ідеї товару – унікальність застосовуваної реалізації	

Наступним кроком є визначення цінових меж, якими необхідно керуватись при встановленні ціни на потенційний товар (остаточне визначення ціни відбувається під час фінансово-економічного аналізу проекту), яке передбачає аналіз ціни на товари-аналоги або товари-субститути, а також аналіз рівня доходів цільової групи споживачів. Аналіз проводиться експертним методом.

Наступним кроком є визначення оптимальної системи збуту, в межах якого приймається рішення (таблиця 4.20):

- проводити збут власними силами або залучати сторонніх посередників (власна або залучена система збуту);
- вибір та обґрунтування оптимальної глибини каналу збуту;
- вибір та обґрунтування виду посередників.



Таблиця 4.20 – Формування системи збуту

Специфіка закупівельної поведінки цільових клієнтів	Функції збуту, які має виконувати постачальник товару	Глибина каналу збуту	Оптимальна система збуту
Тендерні закупівлі та пряме придбання послуги	Пошук клієнтів, установлення контактів Переговори Транспортування – Впровадження (в даному контексті)	Нульового рівня – виробник сам продає товар кінцевому споживачу	Збут власними силами – власна система

Останньою складовою маркетингової програми є розроблення концепції маркетингових комунікацій, що спирається на попередньо обрану основу для позиціонування, визначену специфіку поведінки клієнтів (таблиця 4.21).

Таблиця 4.21 – Концепція маркетингових комунікацій

Специфіка поведінки цільових клієнтів	Канали комунікацій, якими користуються цільові клієнти	Ключові позиції, обрані для позиціонування	Завдання рекламного повідомлення	Концепція рекламного звернення
1	2	3	4	5

Продовження таблиці 4.21

1	2	3	4	5
Закупівля через тендери, прямий пошук товару	Портали про публічні закупівлі, виставки, релізи, відгуки, прямі продажі	Задоволення специфічних потреб, реалізація певних переваг	Надати інформацію про товар (послугу) потенційним споживачам	Послуга допоможе вам зменшити ризики від потенційних атак, та поліпшити рівень захищеності мережі промислового IoT

В результаті аналізу вказаних таблиць описана ринкова (маркетингова) програма, що включає в себе концепції товару, збуту, просування та попередній аналіз можливостей ціноутворення, спирається на цінності та потреби потенційних клієнтів, конкурентні переваги, ідеї, стан та динаміку ринкового середовища, в межах якого буде впроваджено проект, та відповідну обрану альтернативу ринкової поведінки.

## Висновки до розділу 4

У розділі проведено маркетинговий аналіз перспектив реалізації запропонованого в роботі науково-технічного рішення та оцінку можливості його ринкового впровадження.

Ринкова комерціалізація проекту є можливою, адже попит на ринку кібербезпеки та промислового Інтернету речей взагалі зростає, та бюджети компаній на відповідні витрати збільшуються. Рентабельність надання описаного типу послуг є високою, з огляду на переваги, які полягають у оцінці дієвості політики безпеки та відповідно зменшення ризиків можливих атак.

Основною проблемою при впровадженні є відсутність так званого «імені» компанії, репутації, що є досить важливим аспектом у виборі постачальника послуг клієнтом. Водночас, кількість споживачів у цільових групах є обмеженою, а відновлюваність низька. Забезпечити відновлюваність можна за допомогою використання монетизації в форматі підписки, з тривалою підтримкою.

Імплементація проекту можлива, але є більш доцільною не в форматі окремого стартапу, а в якості підрозділу існуючої компанії.

## ВИСНОВКИ

- 1) Проаналізовано архітектуру мереж промислового Інтернету речей та найбільш розповсюджених атак на них. Зроблено огляд типової архітектури IoT, наведено вичерпний перелік атак на IoT. Описано програмні та апаратні рішення по захисту промислового IoT. Найбільш ефективними є продукти компаній Cisco, Symantec і IBM.
- 2) Побудовано модель загроз для промислового Інтернету речей та виділення найбільш значних ризиків. Розподіл ризиків по загрозах задано приблизно, значення імовірностей атак взято із статистичних даних у відкритому доступі, значення втрат задано із міркувань шкідливості та критичності наслідків від скоєння атаки. При обчисленні ризиків враховано рекомендації стандарту ISO/IEC 27005.
- 3) Здійснено опис каркасу політики безпеки для промислового IoT, виділено основні складові політики безпеки для цієї сфери, визначено основні рекомендації, які повинні здійснюватись.
- 4) Обрано інструментарій для моделювання політики безпеки обраної мережі для оцінки її недоліків та переваг (симулятор Cooja під Contiki OS). Було проведено моделювання запровадження політики з використанням DIS-атаки на бездротову сенсорну мережу та наведено способи протидії відповідно з розробленою політикою безпеки. Обрано набір тестів на проникнення для типових промислових протоколів обміну даними.
- 5) Запропоновано критерії дієвості політики безпеки, які включають: 1) Спад прогнозованих значень основних ризиків; 2) Наявність кореляції між фінансовими вкладеннями в покращення захисту, вдосконаленням політики безпеки та значеннями ризиків; 3) Відповідність середньому рівню та вище, за чеклістами вимог безпеки; 4) Наявність успішних результатів моделювання майбутніх запроваджень політики безпеки (цей критерій застосовується для політик, які використовуються уперше і ще не

імplementовані повністю на реальному об'єкті); 5) Результати тестування на проникнення; 6) Виконання організаційних заходів із забезпечення політики безпеки, ініційованих вищим менеджментом; 7) Застосування шаблонів безпеки.

- 6) Розроблено методику оцінки ступеню дієвості політики безпеки, що заснована на критеріях 5); Критерії порівнюються між собою з використанням методу відносного ранжування. За допомогою функцій приналежності до нечітких множин визначається підсумкова оцінка дієвості політики безпеки. Заданий варіант політики безпеки перевірено на дієвість, зокрема з використанням прогнозування ризиків на основі регресійної моделі. Лінійна регресія використовувалась для визначення залежності атаки певного типу від кількості днів. Також встановлено залежність між фінансовими вкладеннями на покриття ризику та величиною ризику. Для заданого випадку регресійна пряма добре апроксимується, а отже політика безпеки дає позитивний ефект (збільшення фінансових вкладень призводить до зменшення ризиків). Множинну регресію використали для прогнозування коефіцієнтів CVSS, що показують рейтинг можливих вразливостей та дозволяють передбачати можливі ризики, вчасно реагувати на них зокрема.
- 7) Розробка програмного модуля, який автоматизує методику 6). Програмний модуль розроблений на мові Python і може бути доповнений новими складовими із урахуванням потреб користувача.

**ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ**

- 1 Ashton K. That «Internet of Things» thing [Electronic resource]. RFID Journal. – June 2009. – Access mode: <http://www.rfidjournal.com/article/view/4986> (04-04-2014)
- 2 Sundmaeker H. Vision and challenges for realizing the Internet of Things [Text]. / H. Sundmaeker, P. Guillemin, P. Friess, and S. Woelffl'e // Cluster of European Research Projects on the Internet of Things, European Commision. – 2010.
- 3 Gubbi J. Internet of things (IoT): A vision, architectural elements and future directions [Text]. / J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami // Future generation Computer Systems [ELSEVIER] Journal. – 2013.
- 4 Kasinathan P. Denial of service detection in 6LoWPAN based internet of things [Text]. / P. Kasinathan, C. Pastrone, M.A. Spirito and M. Vinkovits // 9th international conference wireless and mobile computing, Networking and communications. – 2013. – pp. 600-607.
- 5 Atamli A.W. Threat based security analysis for the internet of things [Text]. / A.W. Atamli, A. Martin // International workshop on secure internet of things. – 2014. – pp. 35-43.
- 6 Yang G. Security characteristic and technology in the internet of things [Text] / G. Yang, J. Xu, W. Chen, Z. H. Qi, and H. Y. Wang // Journal of Nanjing University of Posts and Telecommunications (Natural Science), vol. 30, no. 4. – Aug 2010.

## ДОДАТКИ

## ДОДАТОК А

### ПРОГРАМНИЙ КОД ЗАСТОСУНКУ ДЛЯ ОЦІНКИ ДІЄВОСТІ ПОЛІТИКИ БЕЗПЕКИ З ВИКОРИСТАННЯМ ПРОСТОЇ ЛІНІЙНОЇ РЕГРЕСІЇ

#### **linear\_regression.py**

```
#-*- coding:utf-8 -*-
```

```
import pandas as pd
```

```
from math import pow, fabs
```

```
import matplotlib.pyplot as plt
```

```
def get_headers(dataframe):
```

```
    """
```

```
    Отримати імена заголовків датафрейму
```

```
    :param dataframe:
```

```
    :return:
```

```
    """
```

```
    return dataframe.columns.values
```

```
def cal_mean(readings):
```

```
    """
```

```
    Функція для обчислення середнього значення зчитаних даних
```

```
    :param readings:
```



```

:return:

"""

readings_total = sum(readings)

number_of_readings = len(readings)

mean = readings_total / float(number_of_readings)

return mean

```

```
def cal_variance(readings):
```

```
    """
```

```
    Обчислення дисперсії зчитаних даних
```

```
    :param readings:
```

```
    :return:
```

```
    """
```

```
    # Для обчислення дисперсії нам потрібно середнє значення
```

```
    # Обчислення середнього значення з функції cal_mean()
```

```
    readings_mean = cal_mean(readings)
```

```
    # середнє значення різниці квадратів
```

```
    mean_difference_squared_readings = [pow((reading - readings_mean), 2) for reading in readings]
```

```
    variance = sum(mean_difference_squared_readings)
```

```
    return variance / float(len(readings) - 1)
```

```
def cal_covariance(readings_1, readings_2):
```

```
"""
```

Обчислення коваріації між двома різними стовпцями даних

```
:param readings_1:
```

```
:param readings_2:
```

```
:return:
```

```
"""
```

```
readings_1_mean = cal_mean(readings_1)
```

```
readings_2_mean = cal_mean(readings_2)
```

```
readings_size = len(readings_1)
```

```
covariance = 0.0
```

```
for i in xrange(0, readings_size):
```

```
    covariance += (readings_1[i] - readings_1_mean) * (readings_2[i] - readings_2_mean)
```

```
return covariance / float(readings_size - 1)
```

```
def cal_determination(actual_readings, predicted_readings, attacks_frequency_mean):
```

```
"""
```

Обчислення коефіцієнту детермінації

```
"""
```

```
numer_total = 0.0
```

```
total_readings = len(actual_readings)
```

```
for i in xrange(0, total_readings):
```

```
    numer_diff = predicted_readings[i] - attacks_frequency_mean
```

```
    numer_total += pow(numer_diff, 2)
```

```
print "R^2 numerator =", numer_total
```

```

denomin_total = 0.0

for i in xrange(0, total_readings):

    denomin_diff = actual_readings[i] - attacks_frequency_mean

    denomin_total += pow(denomin_diff, 2)

print "R^2 denominator =", denomin_total


coef_determination = numer_total / denomin_total

print "R^2 =", coef_determination

return coef_determination


def cal_errap(actual_readings, predicted_readings):

    """

    Обчислення похибки апроксимації

    :param actual_readings:

    :param predicted_readings:

    :return:

    """

    error_total = 0.0

    total_readings = len(actual_readings)

    for i in xrange(0, total_readings):

        error = (actual_readings[i] - predicted_readings[i]) / actual_readings[i]

        error_total += fabs(error)

    errap = error_total * 100 / float(total_readings)

    print "error of approximation =", errap

    return errap

```

```
def plot_regression_line(x, y, c):  
    plt.scatter(x, y, color = "m",  
               marker = "o", s = 30)  
  
    # Прогнозований вектор вихідних значень  
    y_pred = c[1] + c[0]*x  
  
    # Побудова лінії регресії  
    plt.plot(x, y_pred, color = "g")  
  
    # Підписування осей  
    plt.xlabel('x, number of days')  
    plt.ylabel('y, attacks frequency')  
  
    plt.minorticks_on()  
  
    # Визначити зовнішній вигляд ліній основної сітки:  
    plt.grid(which='major',  
            color = 'k',  
            linewidth = 2)  
  
    # Визначити зовнішній вигляд ліній додаткової сітки:  
    plt.grid(which='minor',  
            color = 'k',
```

```

        linestyle = ':')

plt.show()

def simple_linear_regression(dataset):
    """
    Реалізація простої лінійної регресії
    :param dataset:
    :return:
    """

    # Отримати назви заголовків датасету
    dataset_headers = get_headers(dataset)
    print "Dataset Headers :: ", dataset_headers

    # Розрахунок середнього значення кількості днів та частоти здійснених атак
    days_mean = cal_mean(dataset[dataset_headers[0]])
    print "x' =", days_mean

    attacks_frequency_mean = cal_mean(dataset[dataset_headers[1]])
    print "y' =", attacks_frequency_mean

    days_variance = cal_variance(dataset[dataset_headers[0]])
    print "variance_x =", days_variance

    attacks_frequency_variance = cal_variance(dataset[dataset_headers[1]])
    print "variance_y =", attacks_frequency_variance

```

```

# Обчислення коефіцієнтів регресії

covariance_of_attacks_frequency_and_days = cal_covariance(dataset[dataset_headers[0]],
dataset[dataset_headers[1]])

print "covariance =", covariance_of_attacks_frequency_and_days

a = covariance_of_attacks_frequency_and_days / float(days_variance)

print "a =", a

b = attacks_frequency_mean - (a * days_mean)

print "b =", b

# Прогнозовані дані

dataset['Predicted_Attacks_Frequency'] = b + a * dataset[dataset_headers[0]]

cal_determination(dataset[dataset_headers[1]], dataset['Predicted_Attacks_Frequency'],
attacks_frequency_mean)

cal_errap(dataset[dataset_headers[1]], dataset['Predicted_Attacks_Frequency'])

return a, b

if __name__ == "__main__":

    input_path = '../Inputs/data.csv'

    new_dataset = pd.read_csv(input_path)

    c = simple_linear_regression(new_dataset)

    plot_regression_line(new_dataset['days'], new_dataset['attacks_frequency'], c)

```

## ДОДАТОК Б

### ПРОГРАМНИЙ КОД ЗАСТОСУНКУ ДЛЯ ОЦІНКИ ДІЄВОСТІ ПОЛІТИКИ БЕЗПЕКИ З ВИКОРИСТАННЯМ МНОЖИННОЇ РЕГРЕСІЇ

#### **multiple\_regression.py**

```
#-*- coding:utf-8 -*-

import numpy as np

import pandas as pd

import matplotlib.pyplot as plt

from mpl_toolkits.mplot3d import Axes3D


data = pd.read_csv('cvss.csv')

data.head()


vulnerability = data['Vulnerability'].values

network_traffic = data['Network_traffic'].values

cvss = data['CVSS_score'].values


# Побудова графіку в 3D

fig = plt.figure()

ax = Axes3D(fig)

ax.scatter(vulnerability, network_traffic, cvss, color='#ef1234')

ax.set_xlabel('Number of vulnerabilities')

ax.set_ylabel('Network traffic, MBPS')

ax.set_zlabel('CVSS score')
```

```

plt.show()

m = len(vulnerability)

x0 = np.ones(m)

X = np.array([x0, vulnerability, network_traffic]).T

# Початкові коефіцієнти

B = np.array([0, 0, 0])

Y = np.array(cvss)

alpha = 0.0001

def cost_function(X, Y, B):

    m = len(Y)

    J = np.sum((X.dot(B) - Y) ** 2)/(2 * m)

    return J

inital_cost = cost_function(X, Y, B)

print("Initial Error of Approximation")

print(inital_cost)

# Метод градієнтного спуску

def gradient_descent(X, Y, B, alpha, iterations):

    cost_history = [0] * iterations

    m = len(Y)

    for iteration in range(iterations):

```



```

# Значення гіпотези

h = X.dot(B)

# Різниця між гіпотезою та Y

loss = h - Y

# Обчислення градієнта

gradient = X.T.dot(loss) / m

# Зміна значень B використовуючи градієнт

B = B - alpha * gradient

# Нове значення функції витрат(помилки апроксимації)

cost = cost_function(X, Y, B)

cost_history[iteration] = cost


return B, cost_history


# 100000 ітерацій

newB, cost_history = gradient_descent(X, Y, B, alpha, 100000)


# Нове значення B

print("New Coefficients")

print(newB)


# Остаточне значення помилки апроксимації B

print("Final Error of Approximation")

print(cost_history[-1])

```

# Оцінка моделі - коефіцієнт детермінації R2

```
def r2_score(Y, Y_pred):
```

```
    mean_y = np.mean(Y)
```

```
    ss_tot = sum((Y - mean_y) ** 2)
```

```
    ss_res = sum((Y - Y_pred) ** 2)
```

```
    r2 = 1 - (ss_res / ss_tot)
```

```
    return r2
```

```
Y_pred = X.dot(newB)
```

```
print("R2 Score")
```

```
print(r2_score(Y, Y_pred))
```