Вінницький національний технічний університет
Факультет інформаційних електронних систем
Кафедра інфокомунікаційних систем і технологій

Бакалаврська дипломна робота на тему:

МЕТОДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІНТЕРНЕТУ РЕЧЕЙ

Виконав: студент 4-го курсу, групи ПЗТ-20бз
спеціальності 172 – Телекомунікації та радіотехніка
11.06. Костьянін В.Ю.

Керівник: к.т.н., доц., доцент каф. ІКСТ
Семенова О.О.
«11» 06 2024 р.

Рецензент: к.т.н., доц., доцент каф. ІРТС
Осадчук Я.О.
«11» 06 2024 р.

Допущено до захисту
Завідувач кафедри ІКСТ
д.т.н., проф. Кичак В.М.
«11» 06 2024 р.

Вінниця ВНТУ – 2024 рік

Вінницький національний технічний університет
Факультет інформаційних електронних систем
Кафедра інфокомунікаційних систем і технологій
Галузь знань 17 – Електроніка та телекомунікації
Спеціальність 172 – Телекомунікації та радіотехніка
Освітня програма – Програмне забезпечення телекомунікаційних систем

ЗАТВЕРДЖУЮ
Зав.кафедри ІКСТ
ВНТУ,
докт.техн.наук, професор
В.М.Кичак
"6" 05 2024 р.

З А В Д А Н Н Я
НА ДИПЛОМНУ РОБОТУ СТУДЕНТУ

Костьяніну В'ячеславу Юрійовичу .
(прізвище, ім'я, по батькові)

1. Тема роботи: Методи забезпечення інформаційної безпеки Інтернету речей

керівник роботи Семенова Олена Олександрівна, к.т.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом ВНТУ від "11" березня 2024 року № 80
2. Строк подання студентом роботи: 7 червня 2022 року
3. Вихідні дані до роботи: територія покриття мережею – 10000м^2, вживана технологія – ZigBee; кількість пристроїв – 30; сила з'єднання - 6.5, коефіцієнт запитів - 9.8, рівень довіри - 5.4.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити): теоретичні відомості про Інтернет речей, аналіз загроз безпеки в Інтернеті речей, методи забезпечення безпеки Інтернету речей, забезпечення безпеки за допомогою методів штучного інтелекту, охорона праці.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень): загрози безпеки в IoT; класифікація атак; рішення безпеки рівнів IoT; еліптична криптографія; структурна схема нечіткого контролера; програмний код нечіткого контролера; результат роботи нечіткого контролера; архітектура нейронної мережі; програмний код нейронної мережі; результат тренування нейронної мережі

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Спеціальна частина	Семенова О.О., доцент кафедри ІКСТ	6.05.2024	11.06.2024
Охорона праці	Дембіцька С. В., доцент кафедри БЖДПБ	6.05.2024	11.06.2024

7. Дата видачі завдання «6» травня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської дипломної роботи	Строк виконання етапів роботи	Примітка
1	Формування та затвердження теми і технічного завдання бакалаврської дипломної роботи (БДР)	06.05.2024р.	
2	Виконання спеціальної частини БДР. Перший рубіжний контроль виконання БДР	20.05.2024р.	
3	Виконання спеціальної частини БДР. Другий рубіжний контроль виконання БДР	31.05.2024р.	
4	Виконання розділу «Охорона праці»	04.06.2024р.	
5	Нормоконтроль БДР	05.06.2024р.	
6	Попередній захист БДР	06.06.2024р.	
7	Рецензування БДР	07.06.2024р.	
8	Захист БДР	12.06.2024р.	

Студент _____ Костьянін В.Ю.
(підпис)

Керівник роботи _____ Семенова О.О.
(підпис)

АНОТАЦІЯ

УДК 621.397

Костьянін В’ячеслав Юрійович. Методи забезпечення інформаційної безпеки Інтернету речей . – Вінниця: ВНТУ, 2024. – 91с.

На українській мові. Бібліогр.: 30 назв; Рис.: 40; Табл.: 9.

Метою даної бакалаврської дипломної робото є присвячена дослідження та оптимізація методів забезпечення безпеки інформації у мережах Інтернету речей. У роботі проаналізовано сучасні методи забезпечення інформаційної безпеки. Запропоновано використовувати пристрої на базі нечіткої логіки та нейронних мереж у засобах інформаційної безпеки Інтернету речей. Розглянуто питання безпеки життєдіяльності та охорони праці.

Ключові слова: безпека, Інтернет речей, нечітка логіка, нейронна мережа.

ANNOTATION

UDK 621.397

Kostianin Viacheslav Yuriiovych. Methods of ensuring information security of the Internet of Things. Bachelor diploma work. – Vinnytsya: VNTU, 2024. – 91 pp.

In Ukrainian language. Refs.: 30 titles; Figs.: 40; Tables: 9.

The bachelor diploma thesis is aimed to the investigation and optimization of methods for ensuring information security in Internet of Things networks. Modern methods of ensuring information security are analyzed in the work. It is proposed to use devices based on fuzzy logic and neural networks in the means of information security of the Internet of Things. Issues of industrial and occupational safety were considered.

Keywords: security, Internet of things, fuzzy logic, neural network.

ЗМІСТ

ВСТУП

Актуальність теми. Інтернет речей (Internet of Things, IoT) – це сучасна інфокомунікаційна мережа, котра складається з досить великої кількості об’єктів, які називають вузлами, що підключаються до мережі Інтернет та спілкуються з його допомогою з метою виконання поставлених цілей. Вузлом можуть бути мобільні телефони, пристрої побутової технікі, автомобілі, люди. Кожен вузол приєднується до сенсора, котрий з’єднує його з навколишнім середовищем. Інтернет речей з’єднує пристрої різноманітні пристрої в одне ціле; всі інформація сортується, аналізується і зберігається. Наразі ця технологія широко застосовується в різних сферах людської діяльності, таких як енергетика, охорона здоров’я, транспорт. Також вона активно застосовується в телекомунікаційних мережах.

На сьогоднішній день існує багато перешкод для впровадження Інтернету речей у нашу повсякденну життя. Концепція Інтернету речей розширює поняття власне мережі Інтернет відповідними технологіями, такими як мобільні та сенсорні мережі. Мережі Інтернету речей володіють великим потенціалом, масштабованістю, гнучкістю, але їм притаманний високий ризик проблем з безпекою. Отже, одним із найважливіших питань є безпека мережі, оскільки дані передаються також через бездротове середовище, яке є більш уразливим через використання відкритого простору. На даний момент це є серйозною проблемою та актуальною задачею.

Аналіз останніх досліджень. Проведені літературний огляд та аналіз показали, що багато уваги аспектам забезпечення безпеки в мережі Інтернету речей присвятили вітчизняні науковці [1-6]. Особлива увага присвячена безпековим особливостям Промислового Інтернету речей, а також технології «розумного» будинку.

Мета та задачі дослідження. Метою даної бакалаврської дипломної роботи є дослідження механізмів забезпечення безпеки інформації у мережах Інтернету речей зв’язку.

Для досягнення мети необхідно розв’язати такі задачі:

- огляд механізмів забезпечення інформаційної безпеки у мережах Інтернету речей;
- аналіз проблемних місць у забезпеченні безпеки та способи їх подолання;
- розроблення методів підвищення інформаційної безпеки.

Апробація результатів роботи. Основні ідеї роботи доповідались і обговорювались на LIII Всеукраїнській науково-технічній конференції підрозділів Вінницького національного технічного університету (2024).

1 ТЕОРЕТИЧНІ ВІДОМОСТІ ПРО ІНТЕРНЕТ РЕЧЕЙ

1.1 Поняття Інтернету речей

Інтернет речей (англ.: Internet of Things, IoT) вважається наступним етапом еволюції глобальної мережі Інтернет, яка, забезпечує підключення великої кількості пристроїв обробки інформації. Основна мета побудови мережі Інтернету речей є інтеграція пристроїв комп'ютерних мереж в одне ціле, в той же час кожен окремий користувач є доволі автономним [6].

Наразі глобальна мережа Інтернет складається з десятків тисяч різних комп'ютерних мереж: домашніх, корпоративних, наукових, (рис. 1.1). Для об'єднання мережі з різними топологіями чи архітектурами використовують протокол IP. Всім користувачам мережі присвоюється постійна чи тимчасова IP-адреса.

Рисунок 1.1 – Інтернет речей та його пристрої

Власне термін «Інтернет речей» було запропоновано у 1999 році Кевіном Ештоном, засновником AutoID Center в Массачусетському технологічному ін-

ституті. Напрямок Інтернету речей став активно розвиватися на початку 2000-х років, коли число пристроїв, підключених до Інтернету речей, перевищило число кількість користувачів Інтернету.

Сьогодні Інтернет речей складається з безлічі мереж слабо пов'язаних між собою, кожна з котрих вирішує свої власні завдання. Так, у офісній будівлі можливо розгорнути кілька мереж відразу - для управління системами кондиціонування, опалення, освітлення, безпеки і т.п. Такі мережі можуть працювати згідно різних стандартів, а їх об'єднання в одну мережу було б нетривіальною задачею [4].

Хороший IoT додаток повинен володіти відповідними характеристиками, до яких можна віднести злагодженість протоколів маршрутизації, так як у випадку, коли IoT-пристрої переміщаються, то їхня IP-адреса зміниться; система повинна мати достатньо високий рівень надійності та відрізнятися швидкою реакцією на збір, передавання та приймання даних, а також гнучкість щодо числа користувачів. Сама концепція Інтернету речей передбачає підключення між собою сотень тисяч пристроїв.

Отже, перед системою ставлять задачу забезпечити таке управління, котре буде досить оптимальним. Окрім того, є ще задача швидкості реагування на можливі збої системи та їх усунення. Для розв’язання задачі швидкої і правильної конфігурації великого числа пристроїв, підключених до мережі та їх сумісності потрібні дієві протоколи управління. Додатково потрібно забезпечити високий рівень захисту особистої інформації, тобто вирішити питання конфіденційності даних [7].

Модель взаємодії, що використовується в Інтернеті речей має такий вигляд: датчики, кінцеві пристрої, сенсори спілкуються між собою способом D2D – Device to Device. Для зібраних та відправлених на сервери для подальшої обробки даних застосовується спосіб спілкування D2S – Device to Server.

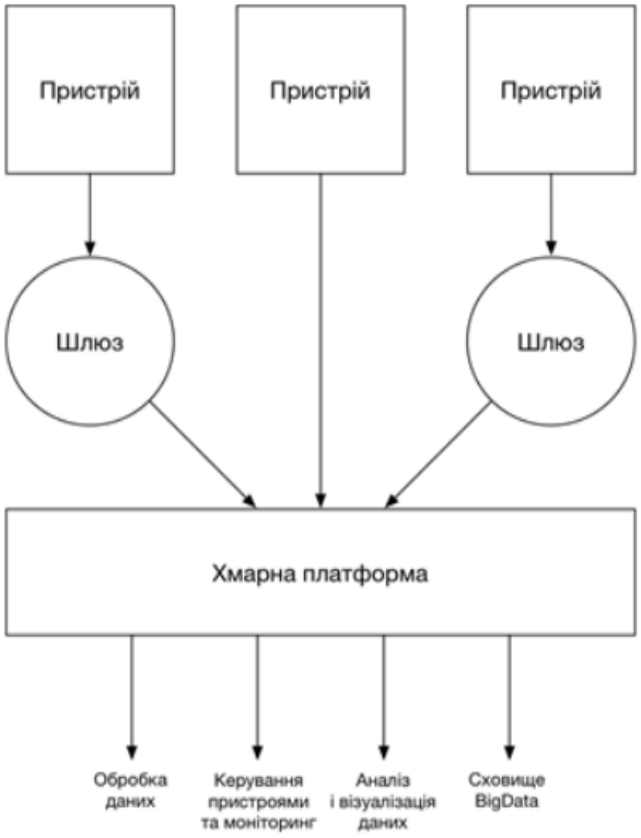


Рисунок 1.2 – Спрощена архітектура системи IoT

Базовим для складного Інтернету речей є спосіб простої міжмашинної взаємодії M2M – Machine to Machine, що передбачає найпростіше точкове з'єднання між двома машинами. Для такого способу не потрібне постійне підключення до мережі Інтернет, з точки зору швидкості він є маломасштабованим, і дає можливість підключати велике число користувачів. Окрім того, M2M мережа є ізольованою, тому досить добре захищеною.

Одним із найбільших сегментів Інтернету речей за числом підключених пристроїв є Промисловий Інтернет речей (Industrial internet of Things, IIoT) [8].

Важливою характеристик цього сегменту є потреба в наданні і режимі реального часу операційно технологічній системі готових рішень. Окрім того, важливим є забезпечення безпеки даних. Також є потреба в запасі потужності, хмарних мереж та сховищ даних.

1.2 Типи IoT мереж

Серед типів IoT мереж виділяють мережі з низьким показником енергоспоживання та малого радіусу дії і мережі з низьким показником енергоспоживання та великого радіусу дії. До першого типу відносять такі мережі [9]:

- Bluetooth – високошвидкісна передача даних на невелику відстань;

- WiFi – мережа з обмеженим радіусом дії, яка потребує для підтримання працездатності постійного споживанні енергії;

- Zigbee – ця мережа має велику зону покриття за рахунок використання меш-мережі та кращу стійкість до збоїв.

Другий тип включає в себе мережі, що надають стабільний зв'язок на відстані більше 500 метрів. Серед найбільш поширених є такі:

- NB-IoT – це специфікація стандарту на основі LTE призначена для обслуговування пристроїв, котрі генерують інформацію невеликого об'єму. Вона підходить для датчиків, сенсорів, лічильників. В такій мережі енергоспоживання дуже низьке і датчики можуть працювати до 10 років від однієї батареї. Вона характеризується хорошою завадостійкістю і пропускною здатністю, що задовольняє більшість IoT пристроїв.

- Sigfox – глобальна мережа для Інтернету речей, що була розроблена у Франції. Дає можливість IoT пристроям спілкуватись безпечно на великі відстані з мінімальним енергоспоживанням та забезпечує двосторонній зв'язок при обмеженій кількості повідомлень.

- LTE Category 0 (Cat 0) – це мережа на базі технології LTE; вона має найнижчу пропускну здатність і декілька важливих особливостей, що роблять її придатною для Інтернету речей: а) мінімальні енергозатрати; б) підтримка режиму електрозбереження.

- LTE Category 1 (Cat 1) – мережа на базі технології LTE для мобільного Інтернету речей. переваги та характеристики, співпадають із відповідними Category 0.

Блок-схема пристрою IoT зображена на рисунку 1.3:

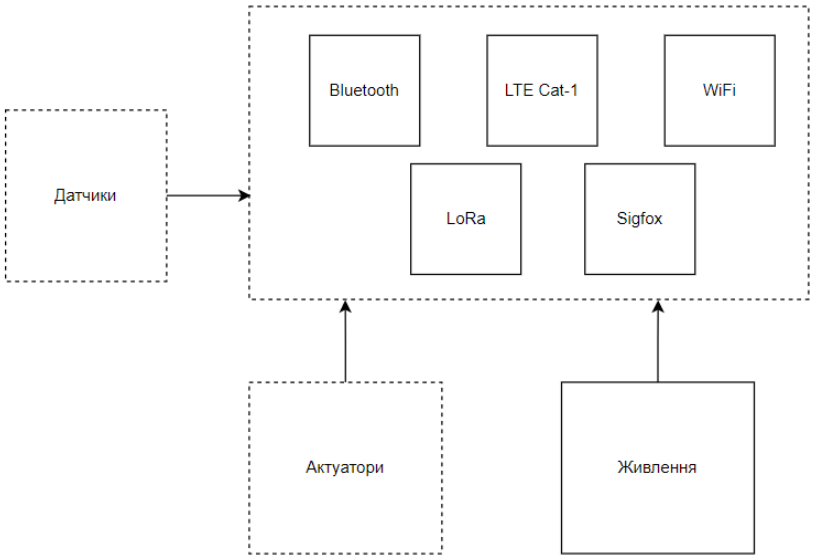


Рисунок 1.3 – Блок-схема пристрою IoT

1.3 Аналіз побудови мережі IoT

До головних елементів мереж Інтернету речей відносять такі:

- розумні датчики –це вбудовані системи, операційні системи в реальному часі, ДБЖ,;

- системи зв’язку з датчиками – для них зона охоплення становить від 0 до 100 метрів;

- агрегатори, шлюзи, маршрутизатори, пограничні пристрої;

- локальні мережі LAN – використовують IP протокол для швидкісного зв’язку.

- глобальна обчислювальна мережа – використовуються транспортні інтернет-протоколи для IoT.

- хмара;

- сервіси аналізу даних;

- безпека – вона стосується кожного елементу в системі. Тут не може бути слабких місць, необхідно забезпечити цілісність починаючи з найнижчих рівнів [5].

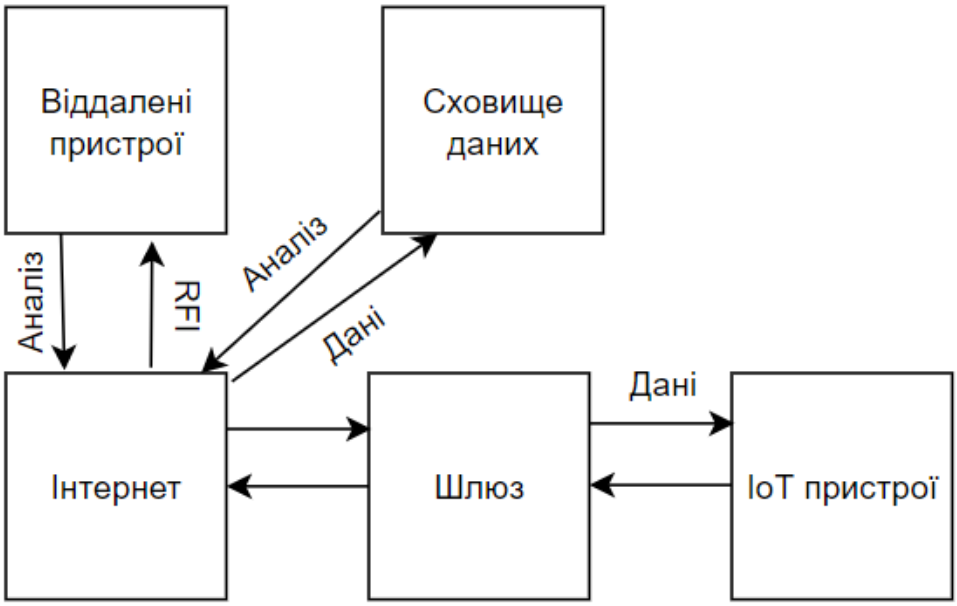


Рисунок 1.4 – Схема IoT екосистеми

1.4 Аналіз датчиків мережі IoT

Відомі 3 основні типи датчиків, що знайшли своє використання при конструюванні мереж Інтернету речей, а саме [10]:

- аналогові; призначені для генерації аналогового сигналу;

- цифрові; призначені для генерації цифрового сигналу – послідовності імпульсів;

- бінарні; призначені для генерації сигналу лише двох рівнів – 0 або 1.

Параметричні датчики працюють за допомогою спеціальних вимірювальних ланцюгів, які мають постійний або змінний струм живлення. Вони відстежують реакцію датчиків на струм або напругу, щоб виявити зміни параметрів.

Резистивні датчики працюють за допомогою зміни активного опопу відносно питомого опору чи площі перерізу. Вони включають фоторезистори, реостатні, контактні та тензорезисторні.

Контактні датчики є простими резисторами, які реагують на зміну опору ланцюга. Їх можна використовувати для контролю різних речей, таких як тем-

пература, переміщення та розмір об’єктів. Але їхній недолік полягає в тому, що їх важко постійно контролювати, а сама контактна система має дуже короткий термін служби. Загалом дані датчики дуже просто використовувати та виконувати.

Реостатні датчики - це резистори з змінним активним опором. Вхідна величина в даному випадку — це переміщення контакту, вихідна величина — це зміна його опору.

Тензорезистори вимірюють механічну напругу, вібрацію та деформацію в невеликій глибині. Ці датчики працюють на основі тензоефекту, який означає зміну активного опору напівпровідника або провідника під впливом сили.

Індуктивні датчики генерують електричний сигнал, отримуючи безконтактну інформацію про переміщення об’єктів. Датчик працює на основі зміни індуктивності обмотки.

Перевагою таких датчиків є їх зносостійкість. Недоліками є чутливість і досить велика зворотна дія датчика на величину, яка зараз вимірюється.

Ємність конденсатора залежить від його розмірів і діелектричної проникності середовища. Такі датчики мають переваги, такі як простота, висока чутливість і відносно низька інерційність. Складність вимірювальних пристроїв також є недоліком. Такі датчики часто використовуються для вимірювання дуже малих величин, таких як вібрації, кути, швидкості руху та ін.

Як слідує з назви, генераторні датчики генерують електричний сигнал. Таким чином перетворюють певну вхідну інформацію на електричний сигнал.

Термодатчики - датчики температури, включаючи кремнієві та біметалічні датчики, термометри для рідини та газу, термоіндикатори, термістори, термопари, термоперетворювачі опору та інфрачервоні датчики, є різноманітними.

Кремнієві датчики температури використовують температуру як опору напівпровідника кремнію. В електричних приборах можна виміряти температури в діапазоні від 50 до $+150^{oC}$.

Біметалічні датчики складаються з двох скріплених між собою металевих пластин. Коли метали нагрівають або охолоджують, вони вигинаються відповідно до свого коефіцієнта розширення, що замикає або розмикає електричне коло. Датчик може вимірювати температури від 40 до +550°C. Такі датчики можуть вимірювати температуру рідин і поверхні твердих тіл. Найчастіше вони використовуються в системах опалення та нагріву води.

Термоіндикатори застосовують спеціальні речовини, які змінюють колір, коли змінюється температура.

Відповідно до назви інфрачервоні датчики використовують для вимірювання температури поверхні на відстані інфрачервоне випромінювання.

П'єзоелектричні датчики використовують п'єзоефект, який означає, що коли кристал взаємодіє з ним, на його поверхні з'являється електричний заряд. Цифрові термометри, наприклад, містять такі датчики [5].

1.5 Архітектура мережі IoT

Інтернет речей має потенціал покращити життя людей на всій планеті. Розвиток цієї технології прискорює входження людства в високотехнологічну епоху. Через велике різноманіття систем IoT може здаватись занадто повільним.

Таким чином, фрагментація IoT конкурує з другою найбільшою проблемою, безпекою [11]. Щоб запустити будь-яку систему IoT, необхідно максимізувати доступну потужність, незалежно від того, наскільки вона велика, щоб створити єдину, цілісну, надійного та економічно вигідну структуру.

Таким чином, міцна архітектура необхідна для кожного запуску системи Інтернету речей, оскільки вона дозволяє виконувати свої обов'язки чітко та ефективно [9]. Кінцевий результат, який показує, наскільки ефективна та придатна система, безпосередньо залежить від якості архітектури.

Незважаючи на те, що системи Інтернету речей відрізняються між собою, їхні архітектури та загальні процеси обробки інформації досить схожі. Він

складається з різних пристроїв, які підключені один до одного та збирають інформацію про навколишнє середовище за допомогою вбудованих датчиків і сенсорів. Далі інформація передається через шлюзи Інтернету речей. Після цього відбувається підготовка до аналізу зібраних даних. Необроблені дані накопичуються, збираються, перетворюються на цифрові потоки, фільтруються та піддаються попередній обробці. Далі можуть з'явитися кінцеві пристрої обробки інформації, а також віртуалізація та машинне навчання. Після цього дані передаються до спеціальних центрів обробки даних, які можуть бути локалізованими або хмарними, і там вони зберігаються та аналізуються [10]. Рисунок 1.5 показує структуру процесу, описаний вище:

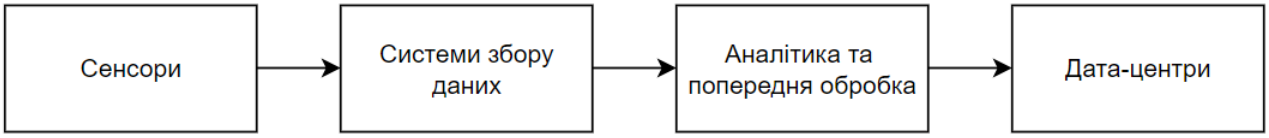


Рисунок 1.5 – Блок-схема процесу обробки інформації в IoT

Як відомо, основною метою пристроїв, підключених до Інтернету речей, є збір даних. Цього досягають датчики, розташовані всередині або зовні пристрою (рисунок 1.5). Наприклад, сільськогосподарські датчики можуть збирати дані про температуру та вологість повітря, ґрунт (а також його кислотність), вплив ультрафіолету на різні рослини та інші фактори.

Роз'ємні пристрої створюють дані, які потрібно обробляти та перетворювати, а також дії. Механізми виконують це. Наприклад, розумна система поливу, яка містить всі необхідні датчики. Система в режимі реального часу аналізує вхідні дані та автоматично поливає місця, де рівень вологості нижчий за встановлений. Крім того, очевидно, що людина не докладає своїх рук до цього.

IoT може регулювати кількість вітамінів у сільськогосподарських продуктах і мікроклімат, щоб гарантувати, що кінцеві продукти, такі як овочі та фрукти, завжди мають найвищу якість [7]. Збір і оброблення інформації про погоду дозволяє прогнозувати такі явища, як утворення льоду, засуха, пориви

вітру та їхні зміни, опади дощу та снігу. Такі дані допоможуть підтримувати правильний контроль температури та вологості. Вони також допоможуть запобігти розвитку грибка та інших мікробних заражень.

Об’єкти, підключені до Інтернету речей, також повинні мати можливість взаємодіяти як зі шлюзами, так і один з одним. І цього важко досягти. Такий зв’язок не повинен бути надто складним, щоб вимагати великої обчислювальної потужності та споживати забагато енергії і пропускної здатності в умовах обмежених ресурсів. Застосування спеціально розроблених протоколів, які безпечні та прості у використанні, найкраще працює в таких умовах. Наприклад, провідним стандартним протоколом для управління різними малопотужними пристроями Інтернету речей є Lightweight M2M [4, 5].

Рисунок 1.6 – Апаратні складові Інтернету речей

Шлюзи значно полегшують зв’язок між датчиками й іншими частинами системи, як показано на рисунку 1.6. Вони приймають дані від датчиків і перетворюють їх на формати, які можна читати іншими системними пристроями. Крім того, шлюзи мають здатність фільтрувати дані, щоб зменшити кількість даних, які будуть передані до хмарного сховища чи дата-центр. Це позитивно впливає на продуктивність системи.

Крім того, шлюзи впливають на безпеку, наприклад, вони можуть контролювати наплив даних між двома сторонами за допомогою правильного шифрування, щоб запобігти витоку даних та іншим зловмисним діям.

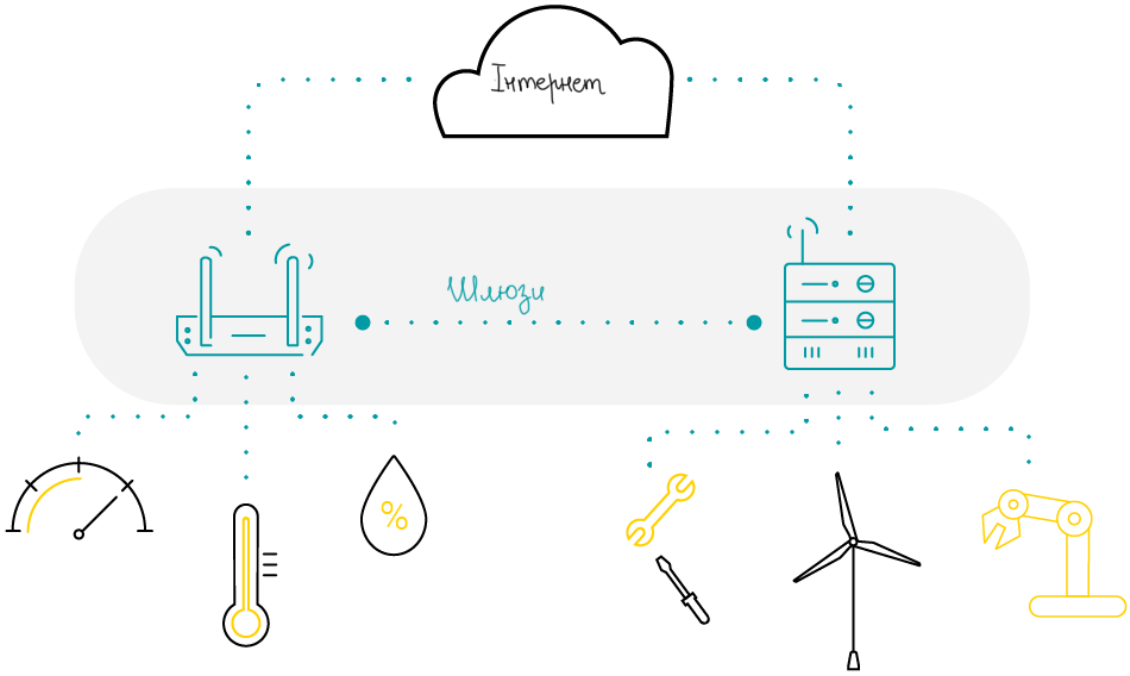


Рисунок 1.7 – Шлюзи системи збору даних

Мозок інформаційних технологій складається з центрів обробки даних і хмарних сховищ. Вони призначені для обробки, аналітики та зберігання великих кількостей даних, що сприяє глибшому розумінню цих даних (рисунок 1.7).

Підвищення показників виробництва, високе споживання енергії та запобігання довгим простоям — це деякі з проблем бізнесу, які можуть виникнути під час використання хмарних обчислень [7].

Рисунок 1.8 – Дата-центр

1.6 Висновки до першого розділу

В першому розділі даної роботи було розглянуто теоретичні засади побудови Інтернету речей.

Можна зробити наступний висновок: IoT є надзвичайно зручною технологією, яка покликана полегшити людське життя та позбавити його від незручностей. Використання цієї технології зменшує ризики небезпечних або травматичних ситуацій для людей, що є великим плюсом для промислової сфери користування, оскільки велика кількість операцій буде автоматизована, якщо не всі.

IoT також є важливим для бізнесу. Не потрібно збирати та аналізувати інформацію про ринок і тенденції. Зменшується час, необхідний для виконання будь-яких завдань.

Але ця технологія має низку недоліків. Одним із них є досить тривала підготовка до впровадження цієї системи. Маркування та налаштування об’єктів, а також організація постійного і надійного зв’язку між ними займають багато часу. Пристрої можуть взаємодіяти лише з продуктами одного виробника в багатьох випадках, наприклад Zigbee.

Попередній недолік призводить до сумісності даних. Багато стандартів обробки та передачі даних обмежують її. Безпека та конфіденційність даних також є серйозною проблемою. Пристрої передають величезний обсяг інформації, яка часто дуже особиста та конфіденційна. У зв’язку з тим, що такі складні дані повинні бути надзвичайно захищені, безпека є важливою частиною розвитку Інтернету речей.

2 АНАЛІЗ ЗАГРОЗ БЕЗПЕКИ В ІНТЕРНЕТІ РЕЧЕЙ

2.1 Аналіз існуючих проблем безпеки IoT

Інтернет речей, як зазначалося в першому розділі роботи, охоплює поняття «Інтернету» технологіями, такими як традиційний Інтернет, мобільні ісенсорні мережі тощо. Кожна «річ» Інтернету речей пов’язана з «Інтернетом», і ці «речі» також взаємодіють між собою. Незважаючи на те, що IoT пропонує багато можливостей, гнучкості та масштабованості, він також несе ризик проблем з безпекою, про які не варто забувати. Через масове поширення цієї технології виникає все більше питань щодо її безпеки, і якщо не буде прийнято відповідних рішень, прогрес або стане надто повільним [9].

Наразі є ряд вимог до безпеки Інтернету речей. Вони приведені в таблиці 2.1.

Таблиця 2.1 – Вимоги до безпеки IoT

Автентифікація	До конфіденційної інформації допускаються тільки лише санкціоновані користувачі
Авторизація	Доступ пристроїв та додатків обмежується так, що він можливий лише до тих ресурсів чи даних, які потрібні для виконання певного завдання
Конфіденційність	Передача інформації між вузлами має бути максимально захищена від сторонніх втручань
Цілісність	Інформація пов’язана з цілісністю системи не має бути неправдивою
Постійність та безперервність	Для максимального зниження ризик виникнення помилок, потрібно забезпечити безпеку безперервності та постійності системи

Звичайно, всі вимоги безпеки IoT, перелічені в таблиці 2.1, повинні бути виконані. Існує ряд проблем, які можуть цьому сприяти. Вони наведені в таблиці 2.2 нижче.

Таблиця 2.2 – Виклики IoT

Сумісність	Прийняті задля безпеки мережі рішення, не мають перешкоджати її функціонуванню
Обмежені ресурси	Більшості вузлів в архітектурах IoT часто бракує потужності, потужності та ЦП. Як відомо, в IoT часто використовуються малопотужні пристрої та пристрої з низькою пропускною здатністю. Ось чому певні методи безпеки, такі як стрибкоподібні зміни частоти або шифрування відкритим ключем, не можуть бути застосовані. В таких умовах налаштування безпеки системи є дуже складним завданням.
Обсяги даних	Деякі системи IoT можуть спричинити величезними обсягами даних завал на сервері.
Захист конфіденційності	Оскільки в значній кількості систем радіочастотної ідентифікації відсутні належні механізми автентифікації, будь-хто може відстежувати мітки та організацію, відповідальну за них. Шахраї й зловмисники можуть не лише читати дані, але й певним чином змінювати їх, змінюючи та навіть видаляючи.
Масштабованість	Всі пропоновані рішення безпеки мають бути масштабовані відповідним до мереж чином
Автономність контролювання	Сучасні комп’ютери потребують конфігурації та налаштувань користувача для різних типів завдань і спілкування. Навпаки, об’єкти в Інтернеті речей повинні встановити зв’язок і налаштувати себе відповідно до операційної платформи. Розглядаються такі механізми, як саморегуляція, самоуправління та самозахист.

Отже, на різних рівнях IoT існують такі загрози:

На рівні сприйняття це можуть бути спуфінг-атаки, радіоглушіння, підслуховування, PDoS-атаки, відключення вузлів.

На рівні мережі це так звань selective forwarding attack, sinkhole-атаки, MiM-атаки, wormhole attac), флуд-атаки HELLO-flood, атаки Сивілли.

На рівні підтримки це підробка даних, DDoS-атаки та неавторизований доступ.

На програмному рівні це можуть бути сніфери, логери, TCP Hijacking та DDoS-атаки.

2.2 Загрози мереж IoT

2.2.1 Загрози на рівні сприйняття

Атака спуфінгу — це атака, яка працює за схемою надсилання підроблених повідомлень у сенсорну мережу. У мережі вважають такі повідомлення справжніми, але насправді це не так. В результаті таких дій зловмисник отримує повний доступ до системи, що робить її вразливою.

Атаки спуфінгу загрожують цілісності та конфіденційності системи [18].

Глушіння бездротового сигналу – це тип DoS-атаки, яка проникає між двома вузлами, щоб зайняти канал і запобігти передачі даних. Це ставить під загрозу доступність системи та її цілісність [19].

PDoS - це тип DoS-атаки. Забагато запитів постійно надсилається до вузлів на великі відстані, виснажуючи як всю систему, так і акумулятор. Це загрожує цілісності та доступності системи [20].

Розділення вузлів може відбуватися фізично або логічно. В обох випадках деякі компоненти мережі перестають працювати, а служби, які читають і збирають дані та ініціюють роботу, виходять з ладу [21].

Радіоприрода систем радіочастотної ідентифікації дозволяє здійснювати прослуховування. Конфіденційна інформація може потрапити в руки зловмисника під час передачі від тега до зчитувача і навпаки. Звичайно, це робить систему вразливою. Можливість таких загроз робить систему вразливою з точки зору конфіденційності інформації [9, 12].

2.2.2 Загрози на мережевому рівні

Вибіркове пересилання – ці атаки характеризуються тим, що зловмисник займає деякі вузли та вибірково відкидає отримані від них повідомлення, таким чином перешкоджаючи їх доставці. Також можна маршрутизувати пошкоджений трафік без шкоди для пошкодження. Існує багато різних видів цієї атаки. В одному типі зловмисний вузол вибірково відкидає пакети з певного вузла або групи вузлів, створюючи високий ризик атаки DoS. В іншому типі під назвою «Недбалість і жадібність» зловмисний вузол випадковим чином не може правильно переслати деякі повідомлення [13].

Атака Sibylla полягає в підробці ідентифікаційних даних мережі (наприклад, облікових записів на основі IP) через один вузол. У міру поширення фальшивих ідентифікацій, контрольованих одним вузлом, вони набувають все більшого впливу в мережі. Успішні такі атаки становлять серйозну загрозу безпеці системи, оскільки в системі можуть здійснюватися несанкціоновані дії [14, 15].

Синхол-атаки типові для бездротових сенсорних мереж, які є мережами Інтернету речей. У таких атаках зловмисний вузол надсилає фальшиві повідомлення через сусідні вузли, щоб отримати контроль над обмеженою пропускною здатністю каналу. Подібні заходи зазвичай призводять до «перевантаження» і збільшення споживання енергії. Це створює воронку в мережі датчиків, яка згодом стає дуже вразливою до атак DoS [26, 27].

Атаки через червоточину є різновидом DoS-атак. Він складається з переміщення певних бітів даних з їх початкового розташування в мережі. Це робиться шляхом тунелювання бітів даних по каналу з низькою затримкою [27].

Атака MiM (атака «людина посередині») — це особлива форма прослуховування, яка дозволяє неавторизованій особі контролювати або контролювати приватний канал зв'язку між двома об'єктами. Крім того, ця неавторизована сторона може створити підроблену особу для спілкування з метою отримання додаткової інформації [9].

Атака HELLO flood полягає у створенні надмірного трафіку, який не містить корисної інформації. Як правило, це один шкідливий вузол, який надсилає дуже велику кількість безглуздих повідомлень іншим вузлам, які отримують відповіді, викликаючи ще більшу перевантаженість каналу [16].

2.2.3 Загрози на рівні підтримки

Підробка даних відбувається, коли інсайдери змінюють дані для власної вигоди або комерційної вигоди третьої сторони. Дані можна легко «видобути» та відповідним чином змінити [17].

DDoS-атаки характеризуються ефектом, подібним до DoS-атак. Сервери можуть впадають через велике навантаження, що унеможливить їх подальше використання.

Неавторизований і зловмисний доступ може мати катастрофічні наслідки для системи. Вони можуть проникати в системи та пошкоджувати їх зсередини, перешкоджаючи доступу до пов'язаних служб Інтернету речей або видаляючи певні набори конфіденційних даних [9].

2.2.4 Загрози на програмному рівні

Сніфери/логери. В систему вбудовується сніфер- чи логер-програми, вони перекачують конфіденційну інформацію з мережевого трафіку. Основна задача

сніфер-програм – викрадення паролів, логінів, файлів, текстів електронних листів [29].

TCP Hijacking. Ця атака виявляє недоліки в автентифікації та управлінні сеансами, і, використовуючи їх на власний розсуд, при цьому можна викрадати особисту інформацію. Цей тип нападу дуже поширений, і наслідки, зрозуміло, серйозні. Зловмисник може використовувати особистість реального користувача для виконання будь-яких дій, які може виконати реальний користувач [9].

2.3 Атаки у мережі IoT

Рисунок 2.1 ілюструє класифікацію атак, що можуть вразити мережу Інтернету речей.

Рисунок 2.1 – Класифікація атак

2.2.1 Пасивні атаки

Неавторизовані особи можуть використовувати комунікаційний канал для аналізу трафіку та прослуховування. Це відомо як пасивна атака. Атаки, націлені виключно на отримання переданих даних, по суті є пасивними. Найбільш поширеними типами атак, спрямованих на порушення конфіденційності даних, є наступні:

Моніторинг і прослуховування. Це найпоширеніший тип атак. Зловмисник може легко отримати доступ до переданих даних за допомогою підслуховування. Дані методи можуть представляти найбільшу загрозу для конфіденційності даних, коли передаються контрольні дані про конфігурацію мережі.

Аналіз трафіку. Зловмисник все ще може використовувати техніку аналізу комунікаційних патернів, навіть якщо інформація передається в зашифрованому вигляді. Активність сенсорів може дати зловмиснику можливість завдати шкоди сенсорній мережі.

2.2.2 Активні атаки

Активні атаки виникають, коли неавторизовані особи змінюють дані під час спілкування. Нижче наведено описи поточних атак.

2.2.2.1 Атаки маршрутизації

Атаки маршрутизації є атаками, які здійснюються на мережевому рівні моделі Open Systems Interconnection (OSI). Найпоширенішими типами атак маршрутизації є наступні:

Змінена маршрутна інформація. Децентралізовані мережі, у яких кожен вузол виступає як маршрутизатор і має здатність змінювати маршрутну інформацію, найбільш схильні до цієї атаки. Наслідки даної атаки можуть включати закільцьовування маршруту, збільшення часу доставки пакета даних до точки призначення та інші наслідки.

Вибіркова розсилка. Проблемний вузол сенсорної мережі може вибірково видаляти певні пакети. Атаки, які збирають велику кількість трафіку на одному вузлі мережі, можуть зробити цю атаку особливо ефективною. Дані атаки можуть значно порушити цілісність і доступність даних, що може значно знизити якість сервісу сенсорної мережі.

Атака «бездонна воронка». Характерною особливістю цієї атаки є те, що скомпрометований вузол мережі починає діяти, як воронка, використовуючи весь трафік сенсорної мережі. Зловмисник «слухає» запити на маршрути та «знає» найкоротший маршрут до базової станції за допомогою сенсорних вузлів, особливо в мережах з протоколом маршрутизації, заснованим на широкомовній розсилці. Скомпрометований вузол може виконувати будь-які дії з пакетами даних, що надходять, як тільки він зміг встати між базовою станцією та сенсорним вузлом, що транслює.

«Шаманська атака». Один скомпрометований вузол може використовувати кілька псевдоідентифікаторів, видаючи себе за кілька вузлів під час конкретної атаки. Такі атаки порушують процеси розподіленого зберігання, маршрутизації, агрегації даних, голосування в мережі та інші. По суті, будь-яка мережа з рівноправними вузлами є уразливою до цієї атаки. Це особливо стосується бездротових і децентралізованих мереж.

Атака Wormhole. Для однієї атаки необхідно створити унікальний шлях між двома або більше скомпрометованими вузлами сенсорної мережі, щоб перехоплювати пакети, які доступні лише для атакуючої системи. Подібні атаки не вимагають компрометації вузла сенсорної мережі, що поставляє під загрозу безпеку сенсорної мережі. Зловмисник передає запит маршруту до найближчого сусіда, коли вузол B (або базова станція) використовує широкомовну розсилку для запиту маршруту. У відповідь на подібний перенаправлений запит будь-який вузол розглядає себе як вузол, який знаходиться в зоні досяжності вузла B, і запам’ятовує вузол B як свого «батька». Цей вузол буде розглядати вузол B як наступний від себе, навіть якщо він знаходиться на великій відстані від вузла B і його відокремлюють багато сенсорних вузлів.

Флуд атака. Данна атака є широкомовною атакою, яка спрямовує велику кількість непотрібних повідомлень на сенсорну мережу, щоб позбавити мережу багатьох ресурсів, таких як канальна ємність, обчислювальна потужність і енергетичні ресурси. Під час такої атаки зловмисник використовує високочастотний радіопередавач, який має достатню обчислювальну потужність, щоб наді-

слати Hello пакети до кількох вузлів сенсорної мережі. Скомпрометований вузол є сусідом вузлів, які отримали Hello-пакети. Вони будуть використовувати адресу відправки Hello пакетів під час наступної передачі даних. Зловмисник таким чином отримає доступ до даних.

2.2.2.2 Відмова в обслуговуванні

Цей тип атаки може бути результатом дій зловмисників або ненавмисного виходу з ладу вузлів сенсорної мережі. Найпростіша атака цього типу спрямована на витрату всіх ресурсів, доступних скомпрометованому вузлу, відправляючи непотрібні пакети даних. Це перешкоджає законним користувачам мережі отримувати сервіси та ресурси, призначені їм. Цей тип атаки охоплює не лише спроби зловмисника зруйнувати мережу або розірвати з'єднання, але й будь-яку подію, яка знижує здатність мережі надавати певні послуги та ресурси. Подібні атаки можуть відбуватися на різних рівнях моделі відкритих систем (OSI).

2.2.2.3 Захоплення вузла

Зловмисник може захопити вузел і розкрити важливу інформацію, таку як криптографічні ключі, що може спричинити компрометацію всієї сенсорної мережі.

2.2.2.4 Несправність вузла

Несправний вузол може створити невірні дані, що може порушити цілісність сенсорної мережі, особливо якщо він є вузлом, який збирає дані, наприклад головним вузлом кластера.

2.2.2.5 Простій вузла

Коли вузол перестає працювати, він стає простим вузлом або виходить з ладу. Протокол сенсорної мережі повинен бути здатним запропонувати пакетам даних альтернативний шлях у разі несправності головного вузла кластера.

2.2.3 Фізичні атаки

Часто вузли мережі встановлюються в середовищах, які піддаються зовнішнім впливам. У таких умовах вузли сенсорної мережі є уразливими до різноманітних фізичних атак, оскільки вони мають маленький впливовий фактор і не знаходяться під постійним наглядом. Фізичні атаки руйнують сенсори незворотньо.

2.2.3.1 Хибний вузол

Такий тип атак включає впровадження вузла в мережу, який передає неправильні дані вузлам сенсорної мережі. Данна атака є однією з найбільш небезпечних, оскільки запроваджений вузол, який поширює зловмисний код, може знищити всю сенсорну мережу.

2.2.3.2 Копіювання вузла мережі

Зловмисник намагається впровадити заздалегідь підготовлені вузли в наявну сенсорну мережу, використовуючи ідентифікатори вузлів, які вже є в мережі. Для досягнення цього злочинець фізично захоплює один вузол мережі, щоб отримати його персональні дані. Після цього дані використовуються для створення заздалегідь підготовлених вузлів, які згодом є клонами захопленого вузла. Зловмисник може легко контролювати сегмент мережі, встановлюючи репліковані вузли в певні точки топології мережі.

2.3 Висновки до другого розділу

У другому розділі цього дослідження були детально розглянуті загрози Інтернету речей на різних рівнях і способи вирішення проблем безпеки на кожному з цих рівнів. IoT вразливий до багатьох атак, які можуть поставити під загрозу цілісність усієї системи. Тому виявлення та швидке усунення вразливостей системи безпеки має важливе значення для успішного розгортання мереж Інтернету речей у реальному часі.

Було проаналізовано та зібрано набір вимог і проблем IoT. Перелічено типи загроз, які можуть бути критичними під час розгортання мережі. Розглянуто особливості захисту від цих загроз.

Єдина перешкода, яка стоїть на шляху розвитку IoT, – це питання безпеки та захисту даних. У цьому відношенні вже досягнуто значного прогресу, але для ефективного розвитку мереж Інтернету речей необхідно приділяти увагу не лише придбанню додаткових заходів захисту, але й покращенню вже існуючих засобів захисту.

3 МЕТОДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНТЕРНЕТУ РЕЧЕЙ

Більшість пристроїв Інтернету речей вважаються «закритими системами». Після виходу пристроїв із заводу покупці не можуть встановлювати або змінювати програмне забезпечення безпеки. Таке втручання анулює гарантію, а час від часу його просто неможливо виконати. Таким чином, щоб пристрої IoT були безпечними за архітектурою, захисні функції повинні бути вбудовані в них із самого початку. Для більшої частини індустрії інформаційних технологій така «безпека всередині», яка включається в процес виготовлення пристрою на заводі, є новою формою захисту. Це включає класичні технології безпеки, такі як шифрування, перевірка справжності, перевірка цілісності, запобігання вторгненню та можливості безпечного оновлення. Іноді програмам для захисту легше використовувати розширені функції апаратної частини та створювати «зовнішні» рівні безпеки, оскільки апаратне забезпечення та програмне забезпечення тісно пов’язані в моделі Інтернету речей.

Для комплексного захисту зв’язку та пристроїв апаратний рівень є лише першим шаром. Комплексний захист вимагає інтеграції аналітиків безпеки, інфраструктури, захисту на основі хоста та функцій управління ключами. Відсутність навіть одного з наріжних каменів у фундаменті безпеки дозволить зловмисникам діяти. Оскільки промисловий інтернет і Інтернет речей включають мережевий інтелект у фізичні речі, необхідно приділити значну увагу безпеці цих технологій [15].

3.1 Модель довіри для IoT

Керованість, перевірка справжності та шифрування є основами стійкої безпеки. Навіть пристрої IoT з обмеженими обчислювальними ресурсами можуть шифрувати за допомогою бібліотек з відкритим вихідним кодом. Але, на жаль, більшість підприємств все ще піддаються різним ризикам, допускаючи помилки при керуванні ключами IoT. Мільярди користувачів і понад мільйон

компаній по всьому світу користуються простою і надійною моделлю довіри, яка забезпечує захист транзакцій на 4 млрд доларів на день електронної торгівлі. Цей тип довіри дозволяє системам безпечно виконувати перевірку достовірності своїх систем іншими компаніями та взаємодіяти з ними через зашифровані канали зв'язку. Сьогодні модель довіри, яка базується на короткому списку перевірених центрів сертифікації (CA), є важливим компонентом безпечної взаємодії в комп'ютерних середовищах.

Щорічно ці CA сертифікують мільярди пристроїв. Наприклад, сертифікати пристроїв дозволяють перевіряти справжність інтелектуальних лічильників електроенергетики, приставок у секторі кабельного телебачення та мобільних телефонів для безпечного підключення до базових станцій. Надійні адміністратори дозволяють створювати, видавати, реєструвати, контролювати та відкликати облікові дані, а також сертифікати, ключі та інші облікові дані легко та безпечно. Ці функції є важливими для забезпечення надійної перевірки справжності даних. Більшість сертифікатів пристроїв продаються великими партіями за невеликі суми грошей — десятки центів за сертифікат — через широкий доступ до сертифікатів безпеки IoT.

Безпека є важливою частиною надійного функціонування пристрою, а не додатком до нього. Щоб постійно підтримувати надійну обчислювальну базу, контроль безпеки програмного забезпечення потрібно ввести на рівні операційної системи, використовуючи переваги апаратних засобів безпеки, які зараз доступні на ринку, і розширюючи їх через стек пристрою. Розробники пристроїв зобов'язані встановлювати системи для пом'якшення небезпек і забезпечення безпеки своїх платформ для забезпечення безпеки на рівні операційної системи.

Перед передачею або отриманням даних пристрій повинен аутентифікувати себе, коли він підключається до мережі. Глибоко вбудовані пристрої часто не потребують користувачів, щоб вводити облікові дані, необхідні для доступу до мережі. Як же правильно визначити ці пристрої під час авторизації? Аутентифікація пристрою — це те саме, що аутентифікація користувача, вона дозво-

ляє користувачеві отримати доступ до корпоративної мережі на основі набору облікових даних, які зберігаються в безпечній зоні зберігання.

Для чого потрібна перевірка справжності? Існує ризик отримання даних від неперевірених пристроїв або сервісів. Зловмисники можуть отримати контроль над обладнанням, пошкодивши або скомпроментувавши систему. Використання надійної перевірки справжності для запобігання небажаним підключенням допомагає захистити системи IoT від таких небезпек і дозволяє споживачу зберігати контроль над пристроями та послугами. Завжди потрібно забезпечити безпеку зв'язку пристрою з іншими пристроями або з віддаленим сервісом, наприклад, хмарним, для обміну даними. Всі комунікації вимагають перевірки чесності та взаємної довіри. З цих причин видається, що економія на сертифікатах пристроїв не є розумною. Зокрема, багато правил було розроблено, щоб споживачі легше проводили надійні перевірки справжності кожної ланки ланцюга обміну даними [16].

Формати сертифікатів мають стандарти, і надійні центри сертифікації підтримують як стандартні, так і індивідуальні формати. У більшості випадків звичайні протоколи, такі як Simple Certificate Enrollment Protocol (SCEP), Enrollment over Secure Transport (EST) та Online Certificate Status Protocol (OCSP), можна легко використовувати для дистанційного керування сертифікатами. Потужні стандарти Transport Layer Security (TLS) та Datagram TLS (DTLS) — родинні SSL дозволяють проводити реальну перевірку справжності завдяки надійному центру сертифікації, який може обробляти облікові дані, ключі та сертифікати.

Взаємна перевірка справжності, коли обидві кінцеві точки перевіряють один одного, є важливою для якісного захисту систем Інтернету речей. Крім того, після завершення перевірки достовірності за TLS або DTLS дві кінцеві точки можуть обмінюватися ключами шифрування або отримувати їх для обміну даними, які підслуховуючі пристрої не можуть розшифрувати. У багатьох програмах IoT потрібна повна конфіденційність даних, і це легко досягається за допомогою сертифікатів і протоколів TLS/DTLS. Тим не менш, якщо конфіден-

ційність не є обов'язковою, будь-яка сторона може перевірити справжність переданих даних, якщо вони були підписані під час їх появи на датчику. Цей метод не обтяжує канал шифруванням, як це часто буває в архітектурах з кількома входами.

Часто виникають питання щодо ефективності та ціни чіпів IoT для криптографічних операцій. У цьому випадку потрібно взяти до уваги, що еліптична криптографія (ECC) навіть у пристроях, які мають обмежені обчислювальні ресурси, працює в десять разів швидше та ефективніше, ніж традиційне шифрування. Якість і швидкість досягаються без зниження безпеки. Використовуючи надзвичайно обмежені ресурси чіпа, ECC продемонстрував рівень захисту, рівний RSA 2048, наприклад, на 8-бітних 1-MHz процесорах і 32-бітних 1-KHz процесорах, які потребують лише мікроват енергії. DTLS, альтернатива TLS, була розроблена для невеликих пристроїв, які періодично працюють між циклами сну. Ціна 32-розрядних чіпів становить лише кілька десятків центів у доларах, тому потужність чи ціна чіпів не можна використовувати як аргумент для зниження вимог щодо захисту нижче розумних порогових значень, коли йдеться про безпеку.

3.2 Захист програмного коду IoT

Коли пристрій включається, він завантажує та запускає певний виконуваний код. Пристрої не можуть бути перепрограмовані на зловмисну поведінку сторонніми сторонами, що дуже важливо. Таким чином, першим кроком у захисті пристроїв є захист коду, щоб переконатися, що тільки необхідний код завантажується та запускається. На щастя, велика кількість виробників вже впровадили можливості безпечного завантаження в свої чіпи. Коли справа доходить до високорівневого коду, різні перевірені часом клієнтські бібліотеки з відкритим вихідним кодом, такі як OpenSSL, можуть використовуватися для перевірки підпису та дозволу коду, які мають бути отримані лише з авторизованого джерела. Підписані прошивки, образи завантаження та більш високорівневий

вбудований код, включаючи підписані базові програмні компоненти, які є частиною будь-якої операційної системи, через це все частіше використовуються. Усе більше людей використовують не просто підписані прикладні програми, а весь код пристрою. Такий метод гарантує, що всі важливі частини систем IoT, такі як датчики, механізми, контролери та реле, правильно сконфігуровані. Вони ніколи не запускатимуть непідписаний код, а тільки підписаний.

3.3 Ефективний хостовий захист для IoT

Пристрій також потребує брандмауера або функції глибокої перевірки пакетів, щоб контролювати трафік, який використовується для зупинки роботи пристрою. Якщо є місце для мережних пристроїв, чому брандмауер на базі хоста або IPS необхідний? Глибоко вбудовані пристрої мають протоколи, які відрізняються від протоколів IT-компаній. Так, сітка інтелектуальної енергії має протоколи, які регулюють спілкування між пристроями. Таким чином, необхідні фільтри протоколів і глибокі можливості перевірки пакетів, щоб знайти шкідливі платіжні навантаження, приховані в протоколах, не пов’язаних із IT. Пристрій не може фільтрувати велику кількість загальнодоступного Інтернет-трафіку, як це роблять мережеві пристрої; однак він повинен фільтрувати конкретні дані, котрі призначені для виконання завдань на цьому пристрої, щоб максимально використовувати його обмежені обчислювальні ресурси.

Пристрої, пов’язані з Інтернетом речей, стикаються з різноманітними небезпеками, в тому числі шкідливим кодом, який може поширюватися через перевірені з’єднання, скориставшись уразливими місцями або помилками в конфігурації. Кілька слабких місць, які часто експлуатуються в таких атаках, включають, але не обмежуються такими: невикористання безпечного завантаження та перевірки підпису коду; погано реалізовані моделі перевірки, які можна обійти. Атакуючі часто використовують ці недоліки для установки програмного забезпечення для збору даних, можливості передачі файлів для отримання конфіденційної інформації з системи, а іноді навіть для інфраструктури

керування, яка використовується для маніпулювання поведінкою системи. Особливо тривожить здатність деяких зловмисників використовувати вразливість для впровадження шкідливих програм прямо в пам’ять вже працюючих систем Інтернету речей. Причому іноді зараження використовується таким чином, що шкідлива програма зникає після перезавантаження пристрою, але все ще може завдати значної шкоди.

В той же час, хостовий захист у поєднанні з надійним підписом коду та моделлю перевірки може суттєво допомогти захистити пристрій від різних небезпек. Хостовий захист передбачає використання декількох технологій захисту, такі як пісочниця, обмеження доступу до системних ресурсів, захист на основі репутації та поведінки, захист від шкідливих програм і, нарешті, шифрування. Залежно від потреб кожної конкретної системи Інтернету речей комбінація таких технологій може забезпечити максимальний рівень захисту для кожного пристрою.

3.4 Контроль пристроїв

Зворотна розробка пристроїв рано чи пізно буде проведена, уразливості будуть виявлені, а пристроїв необхідно буде оновити дистанційно. Звичайно, механізми оновлення збільшують складність архітектури пристроїв IoT, тому багато інженерів намагаються уникати їх через страх і ризик. На щастя, ефективний механізм OTA (оновлення по повітрю) може використовуватися для багатьох цілей, а не лише для виправлення програмного забезпечення і для функціональних оновлень.

Більшість пристроїв виробляють телеметрію або дані з датчиків, які також необхідно безпечно і надійно збирати, передавати та аналізувати в місця зберігання та аналізу. На щастя, інфраструктури управління пристроями, котрі використовують загальноприйняті безпечні протоколи, можуть також застосовуватися до цього.

Різні методи керування ресурсами та доступом наразі використовуються. Обов'язкові або рольові елементи керування доступом, вбудовані в операційну систему, обмежують привілеї компонентів пристрою та програм. В результаті вони можуть отримати доступ лише до ресурсів, необхідних для виконання завдань. Контроль доступу гарантує, що вторгнення не матиме доступу до інших компонентів системи, наскільки це можливо, якщо який-небудь компонент буде скомпрометований. Механізми контролю доступу на базі пристроїв схожі на мережеві системи контролю доступу, такі як Microsoft Active Directory: навіть якщо хтось має здатність вкрасти облікові дані компанії, щоб отримати доступ до мережі, скомпрометована інформація буде обмежена лише такими областями мережі, які мають певні повноваження. Принцип мінімальних привілеїв передбачає, що найменший доступ, необхідний для виконання функції, повинен бути дозволений, щоб будь-яке порушення безпеки було мінімізовано.

3.5 Аналітика безпеки

Зловмисники мають достатньо ресурсів і можливостей для подолання захисту пристрою. Це стосується не лише того, наскільки добре захищено пристрій, код, зв'язок і керування безпекою, навіть якщо використано найкращу з можливих інфраструктур управління OTA. Таким чином, стратегічні загрози потребують стратегічних технологій, щоб мінімізувати негативні наслідки. Аналітики безпеки можуть використовувати телеметрію безпеки з пристроїв і мережевого обладнання, щоб краще зрозуміти, що відбувається в обчислювальному середовищі, а також виявити приховані загрози. Аналітичні системи також використовують ці дані для вирішення проблем оптимізації роботи систем Інтернету речей [17].

Шлюзи між застарілими та більш сучасними захищеними середовищами є додатковим засобом захисту, оскільки атака в одній частині оточення може поширюватися по всій мережі, якщо її не зупинити. Однонаправлені шлюзи даних забезпечують односпрямовану передачу між відкритими мережами та мережа-

ми з обмеженим доступом. Шлюзи між промисловими та загальними IT-мережами, головним блоком транспортного засобу та мобільною мережею, автомобільною системою приводу та інформаційно-розважальними системами є такими ж важливими об’єктами розподіленого моніторингу та централізованої аналітики.

Коли пристрій увімкнеться, він почне швидко отримувати оновлення та виправлення програмного забезпечення. Щоб уникнути споживання пропускної здатності або погіршення функціональної безпеки пристрою, оператори повинні згорнути патчі, а пристрої повинні бути аутентифіковані. Це один із способів, за допомогою якого корпорація Майкрософт надсилає оновлення користувачам Windows і встановлює зв’язки між ними на 15 хвилин. Це зовсім інше, коли тисячі пристроїв у цій галузі виконують важливі завдання або функції та залежать від патчів безпеки, щоб захистити їх від потенційної вразливості. Оновлення та патчі безпеки програмного забезпечення повинні надсилатися таким чином, щоб забезпечити обмежену смугу пропускання, переривчасте підключення вбудованого пристрою та повністю усунути будь-яку ймовірність погіршення функціональної безпеки.

3.6 Алгоритм забезпечення безпеки

Зокрема, традиційні моделі захисту кінцевої точки непрактичні через те, що пристрої IoT відрізняються за формою, розміром і функціями. Крім того, пристрої IoT мають обмежені ресурси щодо потужності, продуктивності та функціональності. Багато людей використовують надзвичайно унікальні та нестандартні операційні системи, такі як NANIX, версія Linux для переносних пристроїв.

У багатьох випадках доступ до пристроїв може бути обмежений, тому мережеві адміністратори майже не можуть знати, що відбувається з усіма складовими системою. Ускладнення цієї проблеми полягає в тому, що пристрої Інтернету речей мають тривалий життєвий цикл і майже не мають захисту, як-от

датчик температури в комерційних або промислових умовах. Крім того, через їх оригінальний дизайн або обмежені ресурси, такі як пам'ять та процесор, вони не можуть бути легко замінені або оновлені новим програмним забезпеченням.

Крім того, багато підключених пристроїв застосовують застарілі та нестандартні протоколи зв’язку (наприклад, M2M), які більшість продуктів безпеки не підтримують. Після аналізу потенційних проблем і методів захисту Інтернету речей наведемо основний алгоритм захисту такої системи:

1. Стандартизація: оскільки в даний час мережі Інтернету речей переважно працюють безпроводово, різноманітність нових протоколів і стандартів щодо радіочастот і радіозв’язку робить безпеку мережі набагато складнішою, ніж традиційні проводові мережі. Щоб забезпечити безпеку системи та запобігти уразливості для злочинців, пристрої та система в цілому мають відповідати стандартам.

2. Сертифікація пристроїв/перевірка справжності: крім дотримання стандартів, складові мережі повинні мати сертифікати, видані центрами сертифікації, щоб перевірити пристрої, які можуть проникнути в вашу мережу та завдати їй шкоди. Така перевірка допомагає проаналізувати пристрій на реєстрацію в своєрідній базі та надасть інформацію про якість і потенційні збитки.

3. Аутентифікація: пристрої IoT повинні ідентифікуватися як дозволені користувачі. Від статичних паролів до двофакторної аутентифікації, біометрії та цифрових сертифікатів існують різні підходи до цього типу аутентифікації. IoT відрізняється тим, що пристрої, такі як вбудовані датчики, мають здатність розпізнавати інші пристрої. Саме завдяки цьому ймовірність проникнення в систему чужого зменшується.

4. Шифровка даних необхідне, щоб запобігти несанкціонованому доступу. Завдяки різноманітності пристроїв IoT і апаратних профілів це важко забезпечити. З іншого боку, шифрування повинно бути частиною повного процесу управління безпекою. Зважаючи на те, що вчені поки що не погоджуються щодо того, наскільки надійним є певний варіант і чи можна його використо-

вувати в IoT, вже розроблено чіп для шифрування на еліптичних кривих, який може використовуватися в пристроях Інтернету речей.

5. Захист інтерфейсу: більшість розробників програмного забезпечення та обладнання доступні до пристроїв через API. Для їх функціонування потрібна авторизація та аутентифікація пристроїв, які вимагають обміну даними. Захищені пристрої можуть спілкуватися лише з авторизованими пристроями, розробниками та програмами.

6. Механізми доставки: для боротьби з кібератакерами, які постійно змінюються, потрібні постійні оновлення та патчі. Для того, щоб виправити прогалини в критичному програмному забезпеченні на льоту, необхідно знати про патчі.

7. Аналітика безпеки та прогнозування загроз: дані щодо безпеки повинні зберігатися та контролюватися, а також використовуватися для прогнозування майбутніх загроз. Вони повинні поєднуватися з традиційними методами, які шукають дії, що виходять за рамки існуючих правил. Прогноз передбачає впровадження нових алгоритмів і штучного інтелекту, щоб обмежити доступ до нетрадиційних стратегій нападу на вашу систему.

8. Контроль доступу: це забезпечує, щоб зловмисники мали найменший доступ до інших компонентів системи, коли який-небудь компонент скомпрометований[19]. Механізми контролю доступу на базі пристроїв схожі на мережеві системи, тому навіть якщо хтось зможе вкрасти корпоративні облікові дані, вони не зможуть отримати доступ до інформації, яка знаходиться в мережі, яка дозволена.

9. Фізична безпека: крім безпеки внутрішньої, мережі потрібна безпека ззовні. Наприклад, датчик має бути розташований таким чином, щоб зловмисник не міг до нього прямого доступу і він був непомітний для зловмисника.

Для пристроїв IoT можна використовувати «індекс довіри». для захисту інформації на етапах «спілкування» з чужорідним пристроєм на пошті. З точки зору схожості індекс довіри прямо пропорційний достовірності джерела. Високий показник довіри означає більшу ймовірність того, що систе-

ма вважатиме, що дані надійшли від авторизованого пристрою IoT або джерела. Алгоритм перевірки підключення до системи, що показано на рис. 3.1.

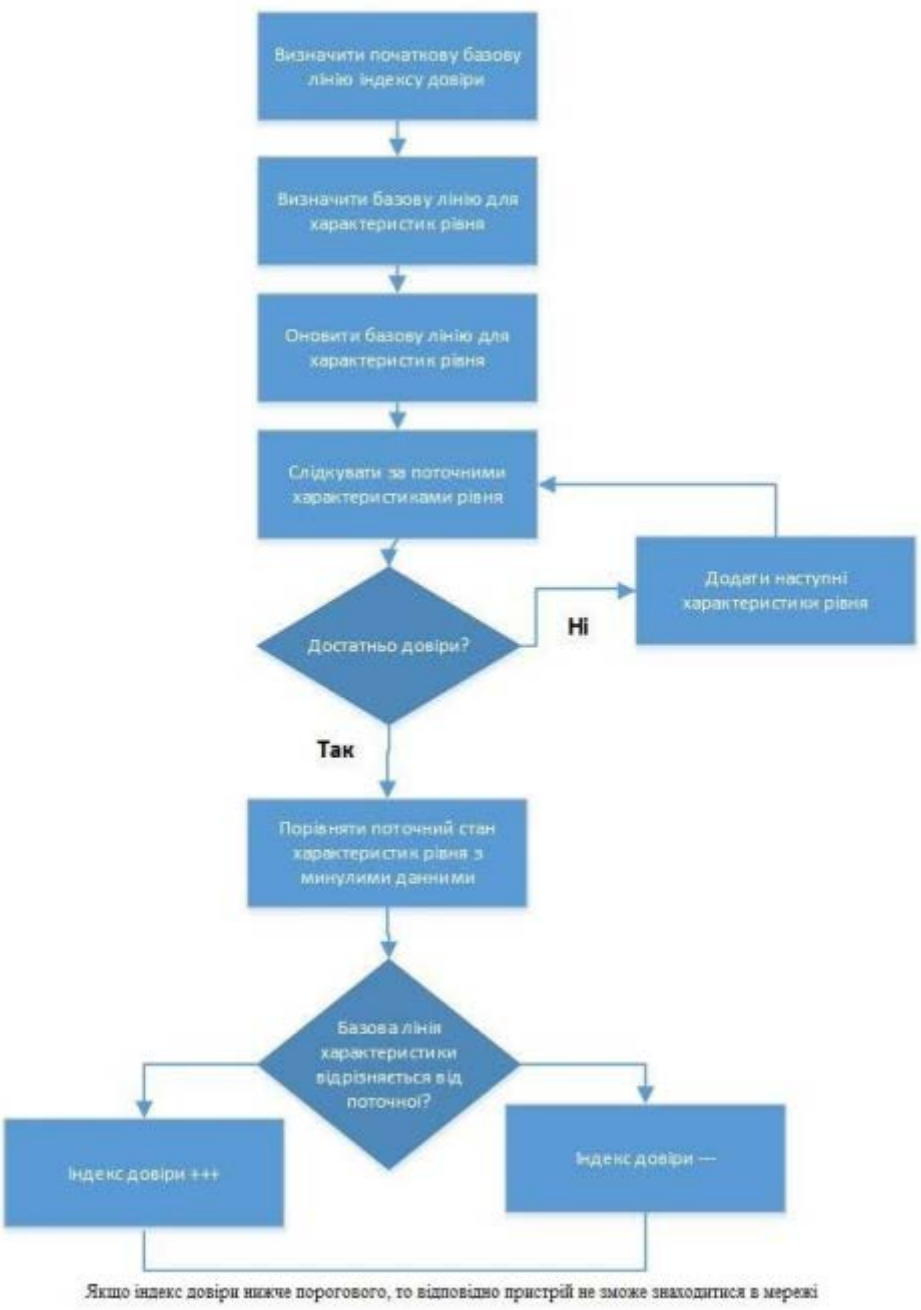


Рисунок 3.1 – Алгоритм перевірки безпеки

Пристрій не зможе бути в мережі, якщо його індекс довіри нижче порогового. Система переспрямовує трафік з пристрою на сервіс, який аналізує відповідь на напад і намагається зібрати додаткові дані. Підсистема безпеки отримує ці дані і змінює параметри характеристик рівня, щоб вивчити та аналізувати атаки або зупинити їх на першому ж етапі.

Для зменшення ймовірності спуфінга цей алгоритм вводиться в піраміду (рис. 3.2). Зловмисникам буде важко копіювати дані, коли ми перебуваємо в мережевому стеку. Це пов’язано зі зростанням рівня складності, що робить більш складним входження в систему або створення хибних характеристик. Наприклад, характеристики фізичного рівня, такі як орієнтація абонента або кут прибуття, у бездротовому зв’язку. Дані, які приймач отримує, не можна програмно визначити. Доки зловмисник використовує таке ж обладнання і навіть таке ж місцеположення, зловмисник не зможе створити такі характеристики.

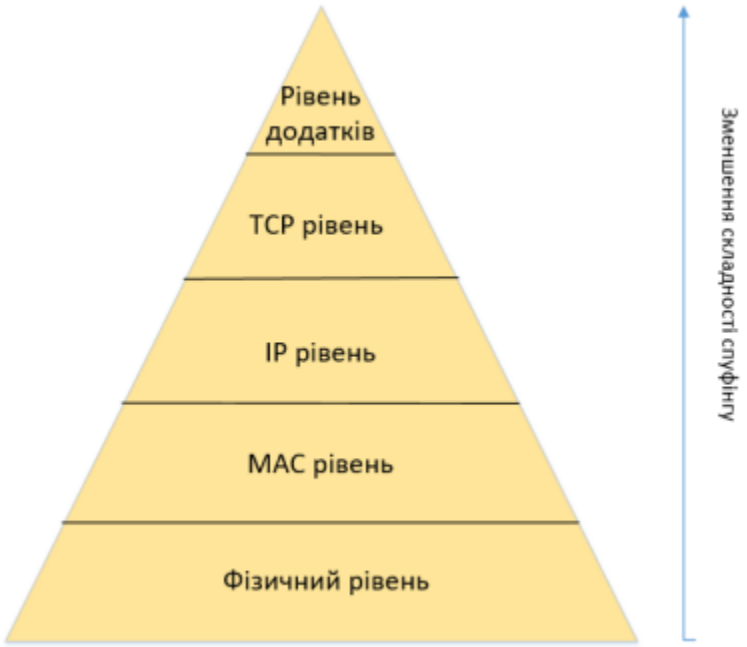


Рисунок 3.2 – Піраміда зменшення складності спуфінгу

3.7 Аналіз методів забезпечення безпеки мереж IoT

Методи захисту мереж IoT поділяються на три категорії відповідно до вищезазначених рівнів: безпека на рівні поінформованості, безпека на рівні мережі та поєднання безпеки на рівні програмного забезпечення та підтримки.

Цей поділ ілюструє рисунок 3.3.

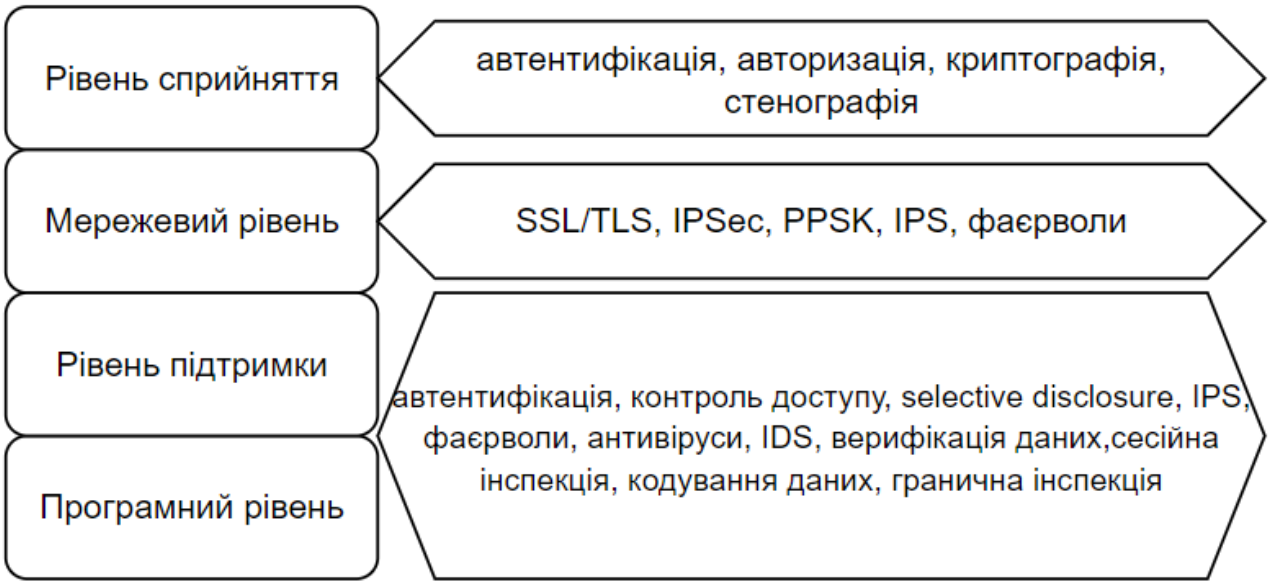


Рисунок 3.3 – Рішення безпеки рівнів IoT

3.7.1 Методи забезпечення безпеки рівня сприйняття

Пристрої, що використовуються в IoT, такі як різні датчики, шлюзи, GPS та інші подібні пристрої, вимагають належного та ефективного захисту. Відкритий проект безпеки веб-додатків OWASP (Open Web Application Security Project) розглянув тему безпеки IoT і створив список найбільших вразливостей [30].

Перший крок — довіряти правильній авторизації. Лише авторизовані особи повинні мати доступ до конфіденційних даних, зібраних об’єктами IoT. Це вимагає чіткого визначення того, що мається на увазі під фізичною ідентифікацією та контролем доступу. Таким чином, і автентифікація, і авторизація однаково відповідають вимогам.

Ключовим елементом на цьому рівні є збір даних. Рекомендовані методи захисту: стиснення мультимедійних файлів, скорочення, водяні знаки, шифрування та CRC.

Криптографія є однією з ключових технологій для механізмів безпеки, пов’язаних з пристроями IoT. Це свого роду гарантія безпеки ваших даних. Це включає шифрування та дешифрування. Виконується генерація ключів, хешу-

вання та перевірка хешів. У таблиці 3.1 наведено деякі з часто використовуваних алгоритмів шифрування для безпеки IoT [31].

Таблиця 3.1 – Криптографічні алгоритми

Тип	Алгоритм	Ціль
Симетричне шифрування	Advanced encryption standard (AES)	Конфіденційність
Асиметричне шифрування	Rivestshamir Adelman (RSA)/Elliptic curve cryptography (ECC)	Цифрові підписи, передача ключів
Асиметричне узгодження ключів	Diffie-hellman (DH)	Узгодження ключів
Хешування	SHA-1/SHA-256	Цілісність системи

Тут ми порівнюємо два асиметричні алгоритми: RSA (відкритий ключ) і ECC (еліптична криптографія). ECC більше підходить для датчиків і вузлів IoT з обмеженими ресурсами. Проте вчені все ще працюють над тим, щоб зробити асиметричне шифрування та механізми шифрування більш застосовними в контексті Інтернету речей. З’являються власні рішення для окремих осіб, але стандартизованого методу ще не створено.

Іншим, не менш важливим елементом безпеки є оцінка можливих ризиків. Багато організацій розробили рекомендації щодо проведення оцінки ризиків. Однією з таких організацій є Національний інститут стандартів і технологій (NIST), Міжнародна організація зі стандартизації (ISO) і Міжнародна електротехнічна комісія (IEC) [32].

3.7.2 Методи забезпечення безпеки мережевого рівня

Проблеми безпеки мережевого рівня можна розділити на дві категорії: проводові та безпроводові. Одним із головних завдань безпеки бездротового зв’язку є розробка протоколів аутентифікації та керування ключами. Протокол SSL/TLS призначений для шифрування та захисту з’єднань на транспортному

рівні, а протокол IP (IPSec) призначений для забезпечення безпеки на мережевому рівні. Разом вони можуть забезпечити відповідний рівень довіри та конфіденційності.

Іншим методом безпеки для Інтернету речей є використання технології PPSK (Private Pre-Shared Key) для всіх пристроїв, підключених до мережі IoT. Вони забезпечені різними унікальними ключами, що полегшує визначення вашого домену. Відразу після налаштування нової мережі вимкніть можливість використання гостьових паролів і паролів за замовчуванням на мережевих пристроях (таких як маршрутизатори та шлюзи). Для цього кроку потрібні надійні політики паролів і керування паролями.

Проводова безпека в першу чергу передбачає пристрої, які передають інформацію іншим пристроям в Інтернеті речей через канали дротового зв'язку. У таких випадках як засоби захисту використовуються брандмауери та системи запобігання вторгненням (IPS). Якщо ваша мережа має один із цих типів захисту, ви також можете виконати детальний аналіз мережевих пакетів, що проходять через вашу мережу. Однак сучасному Інтернету речей не вистачає цієї можливості з точки зору перевірки та фільтрації пакетів. Дослідження на цю тему ще тривають. Робляться спроби створити брандмауери з низьким ресурсом спеціально для IoT, щоб можна було перевіряти пакети [13].

В таблиці 3.2 приведена вищеописана інформація про захист мережевого рівня.

Таблиця 3.2 – Безпека мережевого рівня IoT

Тип з'єднання	Методи захисту	Призначення
Безпроводове	TLS/SSL, IPSec, PPSK	Автентифікація, конфіденційність, цілісність системи
Проводове	Брандмауери, IPS	

3.7.3 Методи забезпечення безпеки рівнів підтримки та програмного

Це питання поділено на два блоки: локальне питання та національне питання. Обговорюйте локальні питання про безпеку проміжного програмного забезпечення так, як вам підходить. Наприклад, варто використовувати методи шифрування абревіатур для інтелектуальних транспортних систем і розумних будинків. Питання національного типу стосуються національних застосувань систем безпеки. Зрозуміло, що такі системи використовують різні методи.

Механізми автентифікації для запобігання зловмисному доступу використовуються на рівнях підтримки та додатків і подібні до тих, що використовуються на мережевому рівні [9].

Безпека даних є ще однією проблемою на цих рівнях IoT. Нижче наведено деякі запобіжні заходи, які зараз вживаються в IoT.

– Безпечне програмування та тестування антивірусного програмного забезпечення для запобігання впровадженню потенційно небезпечного коду.

– Розробка перевірки даних і тимчасового кешування для запобігання зловмисним операціям.

– Механізми перевірки підключення та повторного підключення для запобігання атакам викрадення.

– Контроль кордонів, механізми шифрування даних і засоби контролю доступу до ресурсів для запобігання втраті конфіденційних даних.

3.8 Аналіз методу ECC для IoT

Еліптична криптографія є одним із найдосконаліших підходів до криптографії з відкритим ключем. Він заснований на алгебраїчній структурі еліптичних кривих зі скінченними полями. Цей метод ефективний, оскільки він зменшує розмір ключа для користувача та різко збільшує затримку виклику для зловмисника, який намагається зламати систему. За допомогою ECC 160-бітний

ключ забезпечує такий самий рівень безпеки, як і 1024-бітний ключ із двоключовим шифруванням RSA.

Методи еліптичної кривої потребують значно менше обчислювальної потужності та пам’яті, алгоритм не потребує субекспоненціального часу, а розмір ключа шифрування невеликий, що забезпечує кращий захист. ECC широко використовується в багатьох сферах, включаючи пристрої з малим об’ємом пам’яті та низьким енергоспоживанням, такі як мережеві об’єкти IoT і банківські картки. Насправді це ідеальне поле для реалізації еліптичної криптографії через малий розмір пристроїв і обмеження, що накладається на обчислювальну потужність і використовувані ресурси. Невеликий розмір самого ключа забезпечує швидке виконання завдання, але час є критичним фактором у цьому плані [14].

3.8.1 Імплементація методу ECC

Розглянемо цей метод криптографії детальніше. На рисунку 3.4 зображений його загальний принцип.

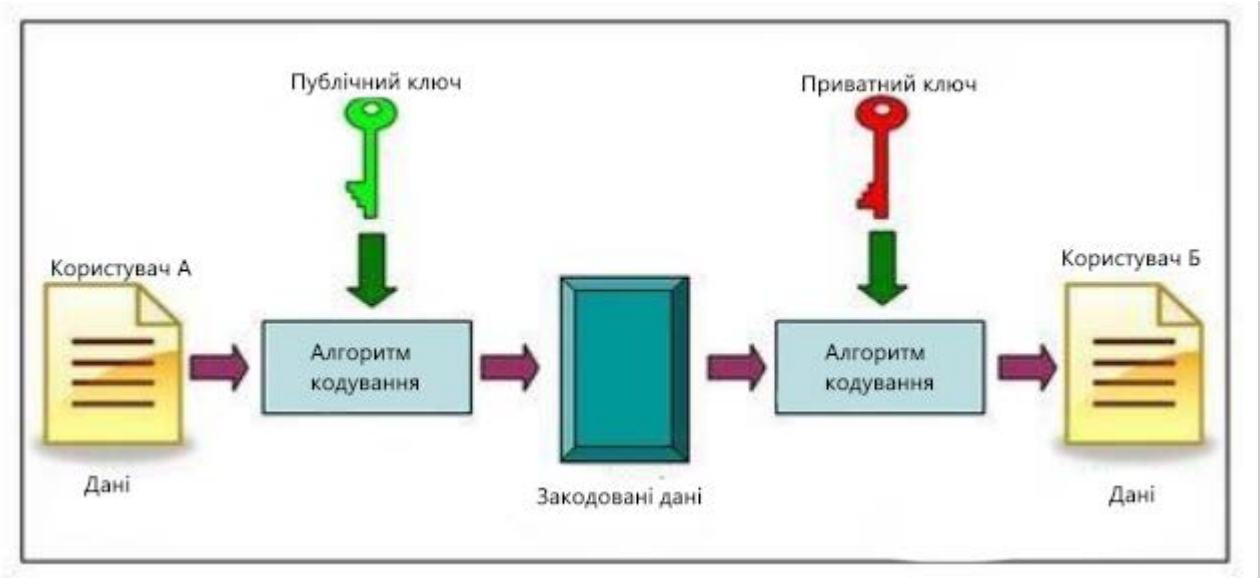


Рисунок 3.4 – Загальний принцип ECC

Генерація ключів є важливою частиною кодування. Створюються два ключі: відкритий і закритий. Відправник шифрує отримане повідомлення за допомогою відкритого ключа одержувача. Одержувач використовує закритий ключ для розшифровки повідомлення.

Ключ генерується так:

$$Q = d \cdot P, \tag{3.1}$$

де d – довільне число в межах n-1;

P – точка на кривій;

Q – відкритий ключ.

Нехай m буде надісланим повідомленням. Припустимо, що m має точку M на кривій E. Змінна k вибирається випадковим чином із діапазону [1 – (n – 1)]. Створюються та надсилаються дві форми, C1 і C2.

$$C1 = k \cdot P, \tag{3.2}$$

$$C2 = M + k \cdot Q. \tag{3.3}$$

Декодування відбувається за формулою:

$$M = C2 - d \cdot C1, \tag{3.4}$$

де M – це перше надіслане оригінальне повідомлення.

Доведення для даного методу:

$$M = C2 - d \cdot C1,$$
$$C2 - d \cdot C1 = (M + k \cdot Q) - d \cdot (k \cdot P),$$
$$(C2 = M + k \cdot Q, C1 = k \cdot P)$$
$$= M + k \cdot d \cdot P - d \cdot k \cdot P, = M.$$

Отже, закодована інформація декодована [34]. На рисунку 3.5 зображено графік точок на еліптичній кривій.

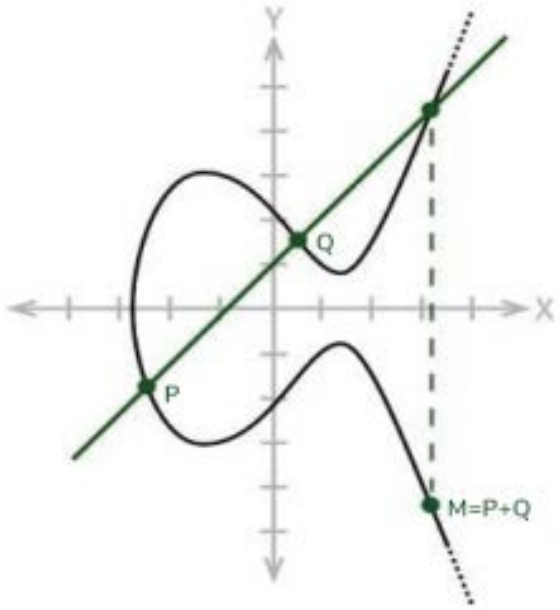


Рисунок 3.5 – Графік еліптичної кривої

3.8.2 Реалізація безпеки шляхом імплементації ECC

Криптографія еліптичної кривої ECC є найефективнішим методом криптографії з відкритим ключем, який використовує еліптичні криві для ключа шифрування.

В таблиці 3.3 наведено порівняння ECC з іншими існуючими методами.

Таблиця 3.3 – Порівняння ECC з іншими методами

Алгоритм	Обмін ключами	Кодування/декодування	Цифровий підпис
Diffie-Hellmen	+	+	-
DSA	-	-	+
RSA	+	+	+
ECC	+	+	+

На основі результатів, наведених у таблиці 3.1, можна зробити висновок, що метод ECC наразі є найкращим, оскільки він демонструє найкращу продук-

тивність серед інших методів, описаних у таблиці. Рисунок 3.6 містить алгоритм цифрового підпису, який також підтримує ECC [34].

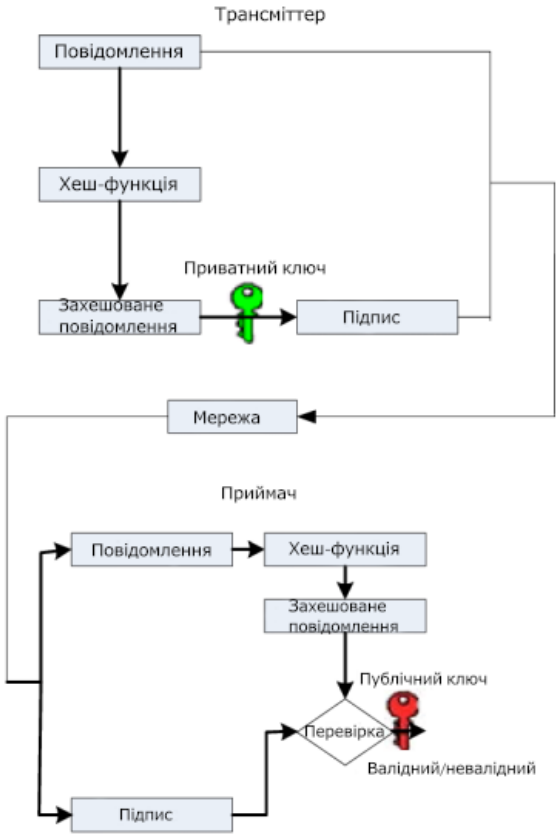


Рисунок 3.6 – Алгоритм цифрового підпису

3.9 Висновок до третього розділу

Третій розділ цієї кваліфікаційної роботи охоплює метод забезпечення безпеки Інтернету речей, особливо метод криптографічних еліптичних кривих. Було представлено алгоритм шифрування та проаналізовано його порівняно з іншими варіантами. У результаті порівняння було виявлено, що метод ECC був найбільш ефективним порівняно з іншими методами. Крім того, було розглянуто алгоритм цифрового підпису, який також застосовується в ECC.

4 ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЗА ДОПОМОГОЮ МЕТОДІВ ШТУЧНОГО ІНТЕЛЕКТУ

4.1 Нечіткий конролер

4.1.1 Загальні відомості про нечіткі контролери

Проблеми прийняття рішення у складних умовах у даний час займають особливе місце в інфокомунікаційних технологіях. Зокрема, традиційні методи недостатньо придатні для вирішення подібних задач саме, що вони не можуть описати невизначеність. Теорія нечіткої логіки для оцінки ризику – це новий підхід що динамічно розвивається. Останнім часом одним із найбільш перспективних і активних напрямів теоретичних і прикладних досліджень у галузі управління та прийняття рішень є нечітке моделювання.

Бази правил нечіткої логіки як і традиційні експертні системі, грунтуються на базі знань, яка будується на основі людського досвіду. В той же час є суттєві відмінності в обробленні і характеристиках таких знань. Реалізація процесу нечіткого моделювання бази правил відбувається за допомогою спеціальних програм які моделюють роботу так зааваних нечітких контролерів (рис.4.1).

Виконання нечіткого висновку здійснюється на основі алгоритму. Підготовка задачі для вирішення методами нечіткої логіки (тобто фазифікації) дає можливість конвертувати значення змінних у нечіткі. На цьому етапі необхідно задати функції належності для терм-множин вхідних та вихідних змінних.

Правила моделі формують на базі загальних закономірностей поведінки досліджуваної системи, що дозволяє вбудувати у механізм висновку логічну модель прикладного рівня. Загалом правила обчислюються на основі оцінки тверджень для кожного правила, які складаються з логічних комбінацій декількох тверджень. База правил у алгоритмі повинна задаватися у вигляді структури із декількома входами і одним виходом.

Функції належності дають можливість визначати нечіткі за своєю природою поняття: "дуже низька ймовірність ризику", "низька ймовірність ризику", "середня ймовірність ризику", "висока ймовірність ризику", "дуже висока ймовірність ризику".

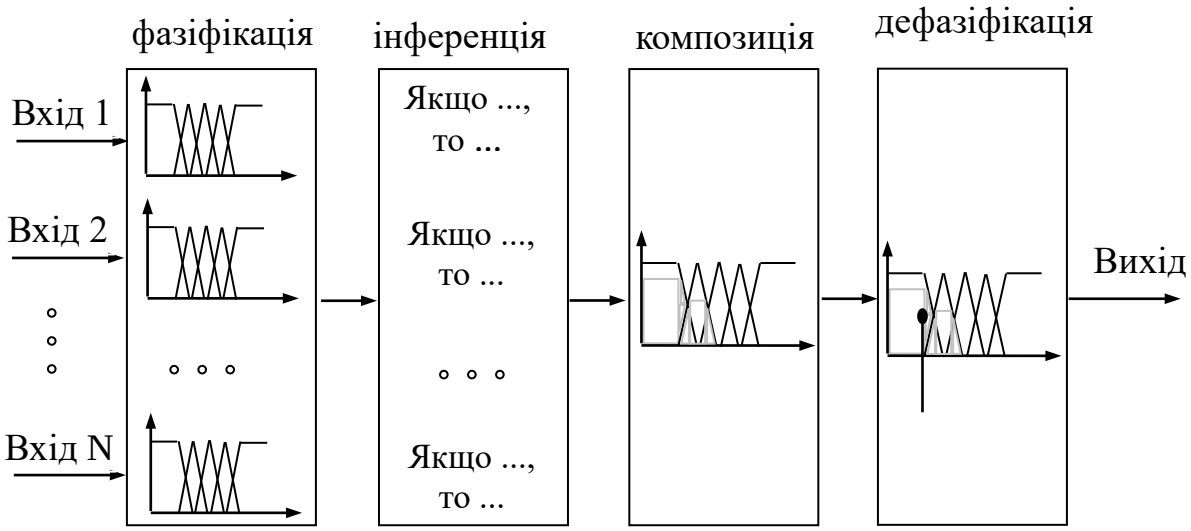


Рисунок 4.1 – Структурна схема нечіткого контролера

4.1.2 Оцінювання ризику за допомогою НК

Мета дослідження полягає в тому, щоб створити систему, яка допомагає спростити процес роботи системи Інтернету речей, усунення непотрібних варіантів, запобігання ризикам або виявлення підприємцями помилок, неточностей і недоліків у проєкті, оптимізація витрат на засоби контролю та захисту, комплексне планування та управління ризиками на всіх стадіях життєвого циклу інформаційних систем, скорочення часу на розробку та супровід корпоративної системи захисту інформації, Згідно з результатами проведеного аналізу, фактори ризику, які виникають на кожному з етапів розвитку, були визначені. Приміром, помилки, здійснені під час прийняття рішень щодо впровадження інформаційної системи та вибору, можуть посилити негативні наслідки факторів ризику на наступних етапах.

Рівень програмно-апаратного захисту, організаційного захисту та правового захисту є факторами, які можуть бути джерелами ризику для інформаційної безпеки під час аналізу факторів ризику.

Для оцінки інформаційної безпеки часто використовують методи оцінки шкоди від загрози хакерських атак і методи рентабельності витрат на реалізацію заходів щодо захисту інформації. Метод нечітких множин значно поширений. При цьому експерти оцінюють вірогідність подолання системи захисту інформації, ймовірність того, що одиниця інформації буде доставлена до споживача, час доставки та складність апаратури. Частка витрат на забезпечення інформаційної безпеки в узагальненій величині витрат і працівників інформаційного відділу у загальній кількості працівників є двома різними показниками. Деякі науковці також досліджують показники, такі як продуктивність інформації, коефіцієнт інформаційної озброєності та коефіцієнт захищеності інформації.

Перший етап включає визначення множини лінгвістичних термів, котрі складаються з сукупності лінгвістичних змінних. Важливо зазначити, що лінгвістична змінна визначається як змінна, яка отримує своє значення з переліку слів або фраз природної чи штучної мови.

Отже, при умові множини з трьох лінгвістичних термів маємо: L − низький, M – середній, H – високий.

Пропонований нечіткий контролер (НК) має три вхідні змінні: сила з’єднання, коефіцієнт запитів та рівень довіри. Вихідною змінною нечіткого контролера є рівень безпеки.

Використовуючи лінгвістичні змінні для опису рівня безпеки, можна використовувати такі -множини термів з метою визначення рівнів інформаційної безпеки:

- L - незадовільний, забезпечується початковий рівень захисту;
- M - достатній, забезпечується базовий інформаційний захист;
- H – високий, відповідає рівню конфіденційності інформації.

Бінарне нечітке відношення на декартовому множенні відповідних нечітких множин показує зв’язок між факторами і показниками ризику.

Нечіткий логічний висновок задається як причинно-наслідкове відношення між фактором і показником ризику. Нечітка логіка використовує спеціальні оператори для запису комбінацій логічних понять, щоб обчислювати ступені істинності. Використовуються звичайні логічні оператори, а саме: AND, OR, NOT.

Перевага моделі оцінки ризиків інформаційної безпеки на основі нечітких множин полягає у застосуванні апарата нечіткої логіки, так як процес захисту інформації не завжди можна описати формально.

За допомогою НК обчислюється ефект впливу загроз у мережі IoT. Така модель дозволяє розрахувати ймовірність реалізації загрози та при цьому визначає ризики реалізації відповідної загрози.

4.1.3 Моделювання НК

Програмний код мовою Python для моделювання нечіткого контролера поданий на рис. 4.1. Рис. 4.3 і рис. 4.4 показують вигляд функцій належності двох вхідних змінних у програмі Python. Результати роботи програми подано на рис.4.5.

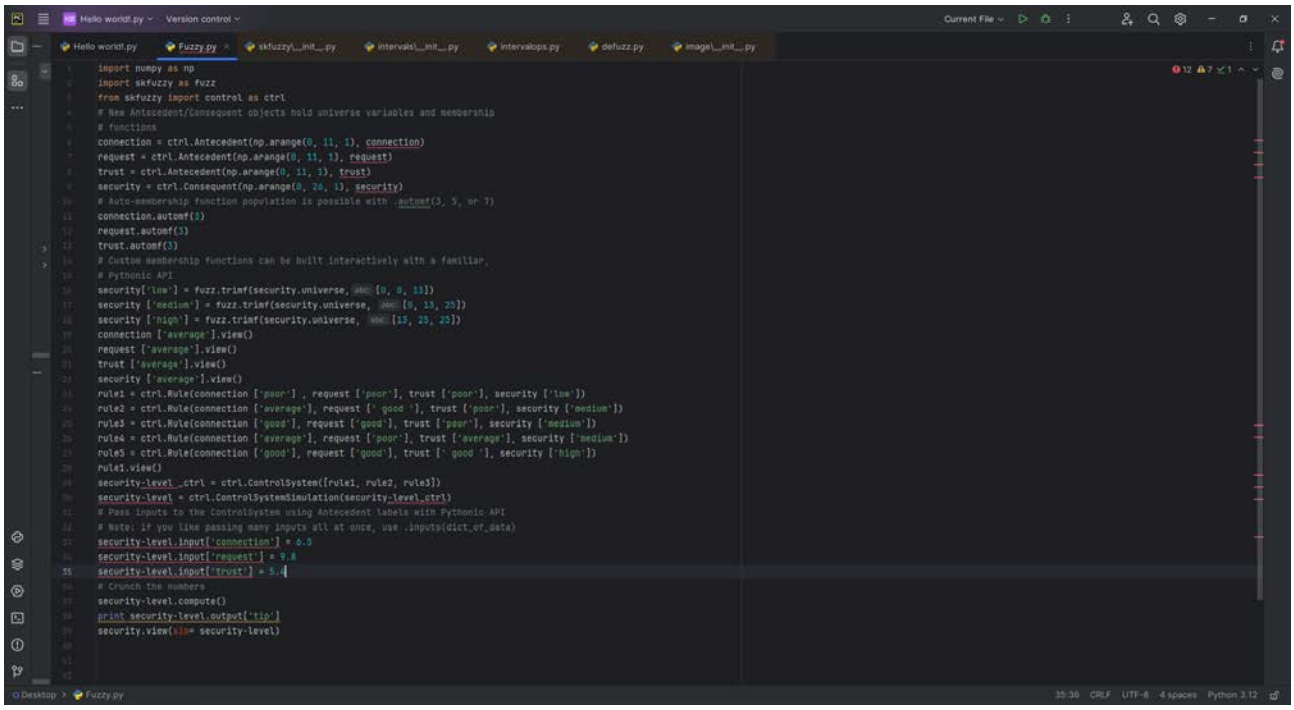
4.2 Нейронна мережа

4.2.1 Загальні відомості про нейронні мережі

Одним з найбільш ефективних засобів прискорення процесів обробки потоків даних у задачах виявлення закономірностей та класифікації даних є штучні нейронні мережі.

Під штучними нейронними мережами (НМ) розуміють сукупність моделей біологічних нейронних мереж. Структурно НМ являють собою мережу

елементів - штучних нейронів, пов'язаних між собою синаптичніми зв’язками.



```
import numpy as np
import skfuzzy as fuzz
from skfuzzy import control as ctrl
# New Antecedent/Consequent objects hold universe variables and membership
# functions
connection = ctrl.Antecedent(np.arange(0, 11, 1), 'connection')
request = ctrl.Antecedent(np.arange(0, 11, 1), 'request')
trust = ctrl.Antecedent(np.arange(0, 11, 1), 'trust')
security = ctrl.Consequent(np.arange(0, 26, 1), 'security')
# Auto-membership function population is possible with .automf(3, 5, or 7)
connection.automf(3)
request.automf(3)
trust.automf(3)
# Custom membership functions can be built interactively with a familiar,
# Pythonic API
security['low'] = fuzz.trimf(security.universe, [0, 0, 13])
security ['medium'] = fuzz.trimf(security.universe, [0, 13, 25])
security ['high'] = fuzz.trimf(security.universe, [13, 25, 25])
connection ['average'].view()
request ['average'].view()
trust ['average'].view()
security ['average'].view()
rule1 = ctrl.Rule(connection ['poor'] , request ['poor'], trust ['poor'], security ['low'])
rule2 = ctrl.Rule(connection ['average'], request [' good '], trust ['poor'], security ['medium'])
rule3 = ctrl.Rule(connection ['good'], request ['good'], trust ['poor'], security ['medium'])
rule4 = ctrl.Rule(connection ['average'], request ['poor'], trust ['average'], security ['medium'])
rule5 = ctrl.Rule(connection ['good'], request ['good'], trust [' good '], security ['high'])
rule1.view()
security_level_ctrl = ctrl.ControlSystem([rule1, rule2, rule3])
security_level = ctrl.ControlSystemSimulation(security_level_ctrl)
# Pass inputs to the ControlSystem using Antecedent labels with Pythonic API
# Note: if you like passing many inputs all at once, use .inputs(dict_of_data)
security_level.input['connection'] = 6.5
security_level.input['request'] = 9.8
security_level.input['trust'] = 5.4
# Crunch the numbers
security_level.compute()
print security_level.output['tip']
security.view(sim= security_level)
```

Рисунок 4.2 – Програма мовою Python для моделювання роботи нечіткого контролера

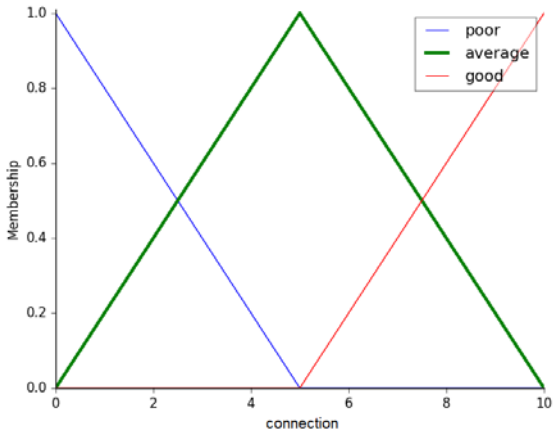


Рисунок 4.3 – Функції належності першої вхідної змінної у програмі Python

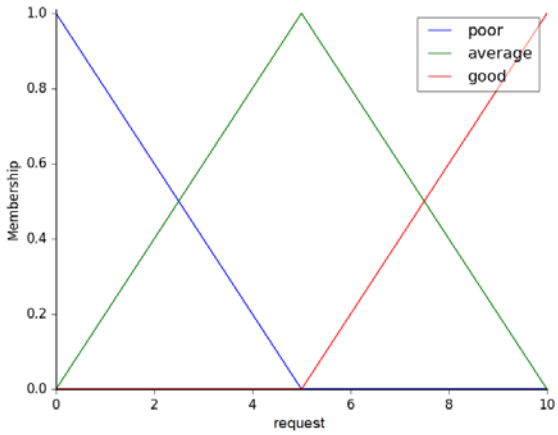


Рисунок 4.4 – Функції належності другої вхідної змінної у програмі Python

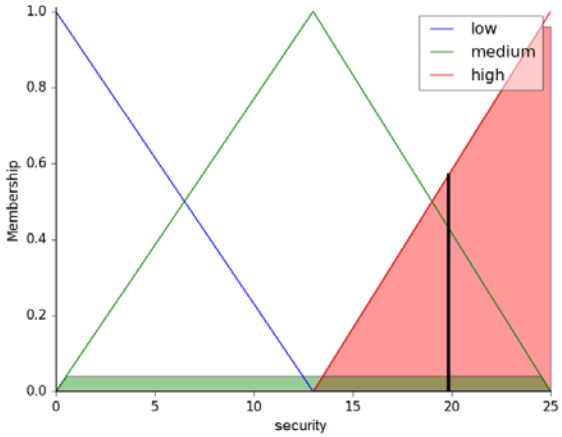


Рисунок 4.5 – Результати моделювання

НМ обробляє вхідну інформацію та в процесі зміни свого стану у часі формує сукупність вихідних сигналів [20].

Кожен нейрон характеризується своїм поточним станом за аналогією до нервовими клітинами головного мозку, які можуть бути збуджені або загальмовані. Він має групу синапсів – односпрямованих вхідних зв'язків, з'єднаних з виходами інших нейронів, а також має аксон – вихідний зв'язок даного нейрона, з якої сигнал (збудження або гальмування) надходить на синапс наступних нейронів. Загальний вигляд нейрона наведено на рис. 4.6.

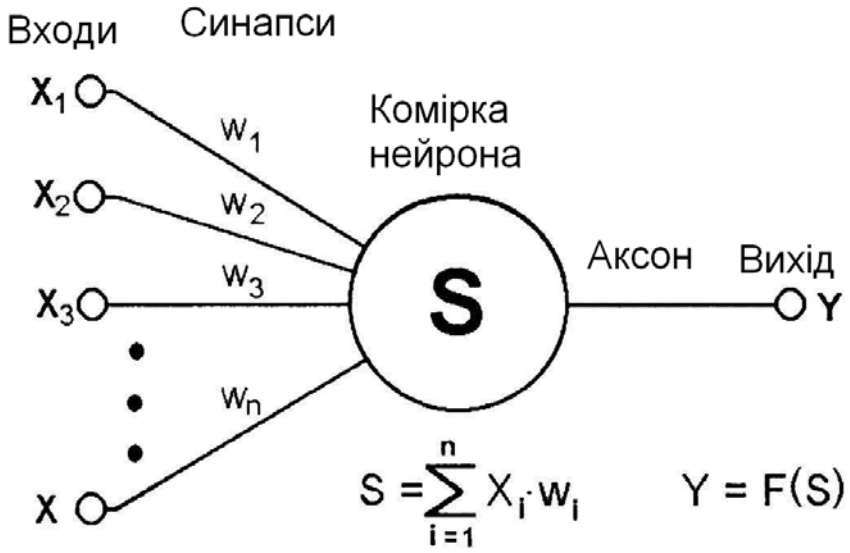


Рисунок 4.6– Штучний нейрон

В даний час найчастіше використовують багатошарові нейронns мережs. Зазвичай така мережа складається з вхідного шару, одного або кількох прихованих шарів та вихідного шару. Багатошарова мережа зображена на рис. 4.7.

4.2.2 Виявлення загроз за допомогою НМ

Виявлення загроз можна визначити як процес інтелектуального моніторингу подій, що відбуваються в мережі, їх аналіз на наявність ознак порушення політики безпеки та спроби поставити під загрозу конфіденційність, цілісність, доступність або обійти механізми безпеки хоста чи мережі. Система виявлення загроз аналізує дані, виявляє аномалії і повідомляє про це адміністратору.

Сучасні засоби виявлення загроз повинні включати інтелектуальні підсистеми, принаймні, як одну зі своїх складових частин.

Останнім часом все частіше для класифікації трафіку та виявлення мережевих атак використовуються сучасні методи машинного навчання та штучні нейронні мережі.

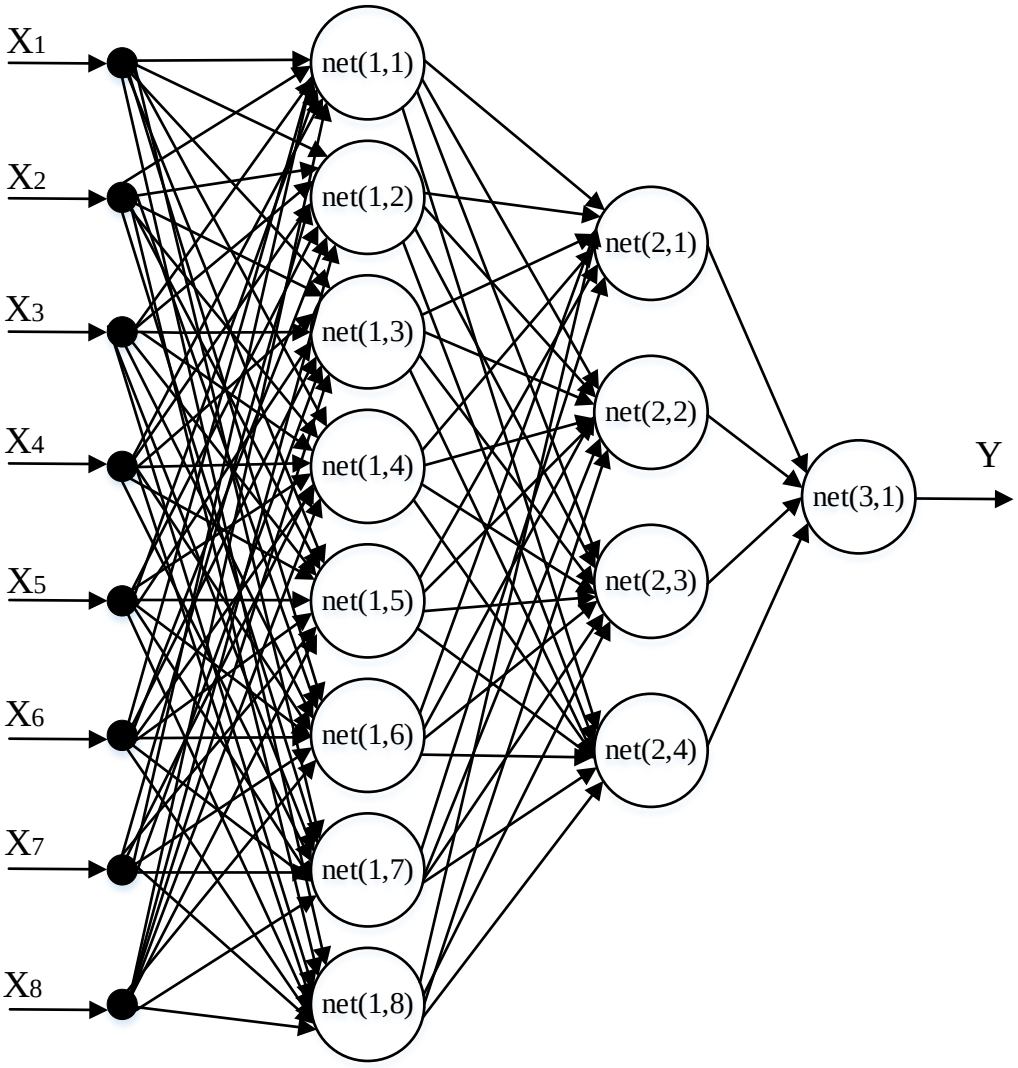


Рисунок 4.7 – Багатошарова нейронна мережа

Застосування нейронної мережі (НМ) для вирішення будь-якої задачі включає два етапи: етап навчання та етап розпізнавання. На етапі навчання на вхід НМ подається навчальна вибірка, що складається з заздалегідь відібраних та підготовлених вхідних та вихідних векторів [21]. Відповідно до обраного алгоритму навчання відбувається налаштування вагових коефіцієнтів, в результаті якої при подачі на вхід НМ навчального вектора на виході з’являється заданий вихідний вектор, що позначає клас вхідного вектора.

На етапі розпізнавання на НМ надходить заздалегідь невідомий вхідний вектор. При цьому на виході з’являється вектор – результат розпізнавання

відповідно до якого вхідний вектор зараховується до одного з найвідоміших класів.

Найважливіша перевага нейронних мереж при виявленні загроз – їх здатність вивчати характеристики навмисних атак та ідентифікувати елементи, не схожі на ті, що спостерігалися в мережі раніше.

Після того, як нейронна мережа навчена безліччю послідовних команд системи, що захищається, або однією з її підсистем, мережа є «образом» нормальної поведінки. Процес виявлення аномалій є визначення показника неправильно передбачених команд, тобто фактично виявляється відмінність у поведінці об'єкта.

Класифікація розв'язуваних задач у галузі даного методу:

- швидке розпізнавання загроз;
- боротьба зі шкідливим ПЗ, яке також самонавчається.
- отримання певних відомостей у процесі навчання та побудова на їх основі більш потужної системи захисту.

У прикладних задачах інформаційної безпеки нейронні мережі застосовуються в:

- системох виявлення атак. Сформований образ нормальної поведінки мережі дозволяє з високим ступенем ефективності знаходити та розпізнавати небезпечні аномалії.
- міжмережевих екранах. Подібно до експертної системи, нейронна проводить аналіз трафіку та створює припущення про можливе вторгнення. Плюсом нейронної мережі в даному випадку є її здатність самостійно вчитися, а не залежатиме від даних, які були закладені в неї людиною.

Розглянемо використання нейромережі на прикладі практичного завдання.

У цьому прикладі за допомогою НМ необхідно детектувати доступ до бази даних з боку якогось ПЗ, відмінного від автоматизованого робочого місця

(АРМ) користувача, або визначити аномалії у роботі користувача. НМ має чотири входи, на які подаються:

1. Обсяг інформації (кілобайт), що завантажується з бази даних за контрольний період. Отримане значення необхідно нормалізувати, оскільки зчитуваний з бази даних обсяг заздалегідь не відомий та індивідуальний для кожного завдання та для кожного користувача. Як нормалізація можна застосувати оцінку трафіку по десятибальною шкалою (0 – обсяг дорівнює нулю, 10 – максимальний обсяг трафіку).

2. Кількість транзакцій за хвилину.

3. Кількість операцій модифікації даних за хвилину. У цьому прикладі АРМ використовує "короткі транзакції", тобто в рамках однієї транзакції зазвичай буває 1-2 операції модифікації даних.

4. Ознаки звернення до словника бази даних. Ознаки будуть дискретними (0 – немає звернень, 1 – є), і їх буде кілька – по одному на кожну таблицю словник бази.

Вихід НМ може бути інтерпретований як процентна відповідність поточних дій діям хакера.

У такий же спосіб можна організувати визначення різних атак та адаптацію до нових типів загроз.

Зазвичай для навчання та тестування НМ наявні експериментальні дані розбиваються на навчальну базу даних (БД) та контрольну БД.

Елементи цієї БД по черзі подаються на вхід НМ для налаштування вагових (синаптичних) параметрів.

Після ініціалізації ваг у процесі навчання нейронної мережі виконуються такі кроки: пряме поширення сигналу; обчислення помилки нейронів останнього шару; зворотне поширення помилки. Пряме поширення сигналу проводиться пошарово, починаючи з вхідного шару, при цьому розраховується сума вхідних сигналів для кожного нейрона і за допомогою функції активації генерується відгук нейрона, який поширюється наступний шар з урахуванням ваги міжнейронного зв'язку. В результаті виконання цього етапу ми отримуємо вектор вихі-

дних значень нейронної мережі. Наступний етап навчання – обчислення помилки нейронної мережі як різниці між очікуваним та дійсним вихідними значеннями. Отримані значення помилок поширюються від останнього, вихідного шару нейронної мережі до першого. При цьому обчислюються величини корекції ваги нейронів залежно від поточного значення ваги зв'язку, швидкості навчання та помилки, внесеної даним нейроном. Після завершення цього етапу кроки описаного алгоритму повторюються до тих пір, поки помилка вихідного шару досягне необхідного значення. Результати навчання та тестування спроектованої нейронної мережі показують можливість її застосування для вирішення задачі виявлення мережевих атак.

По завершенні цих етапів НМ повністю готова до етапу запуску, який полягає у виявленні та класифікації активних аномальних та нормальних з'єднань.

При емулюванні мережевих з'єднань дані зчитуються з контрольної БД.

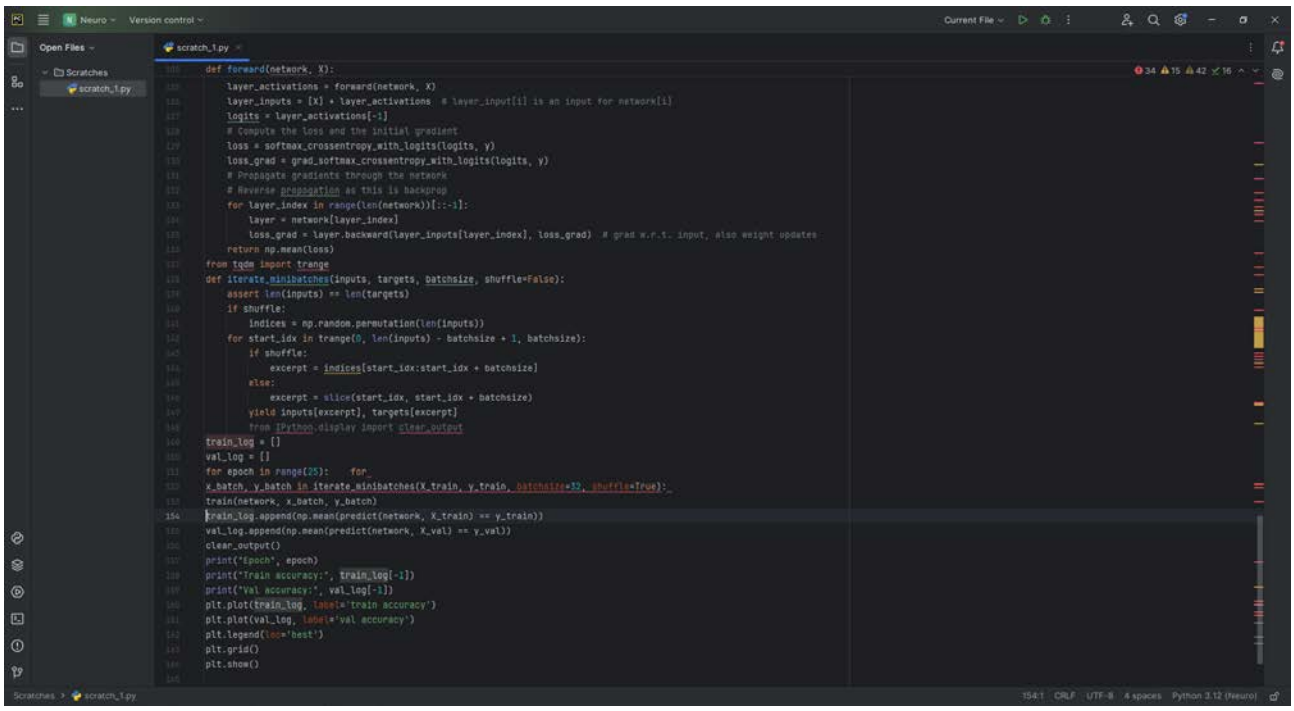
На основі результатів цього етапу визначається статистика та дається аналіз ефективності НМ по критеріям якості розпізнавання типів аномальних з'єднань та наявності хибних спрацьовувань (коли нормальне з'єднання приймається за атаку).

Для навчання НМ застосовується алгоритм зворотного поширення помилки (ітеративний градієнтний алгоритм, який використовується з метою мінімізації помилки роботи багатошарового перцептрону та отримання бажаного виходу) з симетричною функцією сигмоїдальної активації.

НМ, яка виявила підозрілу мережеву активність, сигналізує про це.

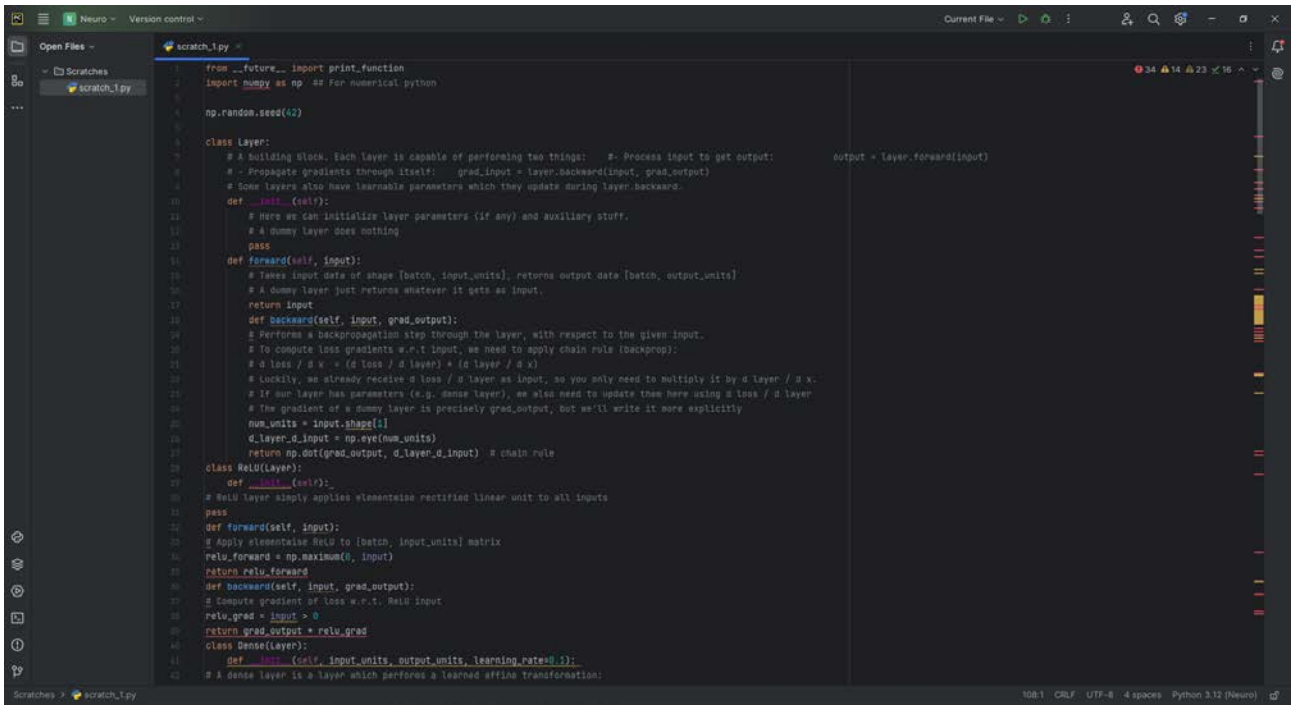
4.2.3 Моделювання НМ

Програмний код мовою Python для моделювання нейронної мережі, а саме – багатошарового перцептрона поданий на рис. 4.8 і рис .4.9. Результати роботи цієї програми подано на рис.4.10.



```
def forward(network, X):
    layer_activations = forward(network, X)
    layer_inputs = [X] + layer_activations  # layer_input[i] is an input for network[i]
    logits = layer_activations[-1]
    # Compute the loss and the initial gradient
    loss = softmax_crossentropy_with_logits(logits, y)
    loss_grad = grad_softmax_crossentropy_with_logits(logits, y)
    # Propagate gradients through the network
    # Reverse propagation as this is backprop
    for layer_index in range(len(network))[::-1]:
        layer = network[layer_index]
        loss_grad = layer.backward(layer_inputs[layer_index], loss_grad)  # grad w.r.t. input, also weight updates
    return np.mean(loss)
from tqdm import trange
def iterate_minibatches(inputs, targets, batchsize, shuffle=False):
    assert len(inputs) == len(targets)
    if shuffle:
        indices = np.random.permutation(len(inputs))
    for start_idx in trange(0, len(inputs) - batchsize + 1, batchsize):
        if shuffle:
            excerpt = indices[start_idx:start_idx + batchsize]
        else:
            excerpt = slice(start_idx, start_idx + batchsize)
        yield inputs[excerpt], targets[excerpt]
        from IPython.display import clear_output
train_log = []
val_log = []
for epoch in range(25):    for
x_batch, y_batch in iterate_minibatches(X_train, y_train, batchsize=32, shuffle=True):
train(network, x_batch, y_batch)
train_log.append(np.mean(predict(network, X_train) == y_train))
val_log.append(np.mean(predict(network, X_val) == y_val))
clear_output()
print("Epoch", epoch)
print("Train accuracy:", train_log[-1])
print("Val accuracy:", val_log[-1])
plt.plot(train_log, label='train accuracy')
plt.plot(val_log, label='val accuracy')
plt.legend(loc='best')
plt.grid()
plt.show()
```

Рисунок 4.8 – Програма мовою Python для моделювання роботи нейронної мережі



```
from __future__ import print_function
import numpy as np  ## For numerical python

np.random.seed(42)

class Layer:
    # A building block. Each layer is capable of performing two things:    #- Process input to get output:          output = layer.forward(input)
    # - Propagate gradients through itself:    grad_input = layer.backward(input, grad_output)
    # Some layers also have learnable parameters which they update during layer.backward.
    def __init__(self):
        # Here we can initialize layer parameters (if any) and auxiliary stuff.
        # A dummy layer does nothing
        pass
    def forward(self, input):
        # Takes input data of shape [batch, input_units], returns output data [batch, output_units]
        # A dummy layer just returns whatever it gets as input.
        return input
        def backward(self, input, grad_output):
        # Performs a backpropagation step through the layer, with respect to the given input.
        # To compute loss gradients w.r.t input, we need to apply chain rule (backprop):
        # d loss / d x  = (d loss / d layer) * (d layer / d x)
        # Luckily, we already receive d loss / d layer as input, so you only need to multiply it by d layer / d x.
        # If our layer has parameters (e.g. dense layer), we also need to update them here using d loss / d layer
        # The gradient of a dummy layer is precisely grad_output, but we'll write it more explicitly
        num_units = input.shape[1]
        d_layer_d_input = np.eye(num_units)
        return np.dot(grad_output, d_layer_d_input)  # chain rule
class ReLU(Layer):
    def __init__(self):
# ReLU layer simply applies elementwise rectified linear unit to all inputs
pass
def forward(self, input):
# Apply elementwise ReLU to [batch, input_units] matrix
relu_forward = np.maximum(0, input)
return relu_forward
def backward(self, input, grad_output):
# Compute gradient of loss w.r.t. ReLU input
relu_grad = input > 0
return grad_output * relu_grad
class Dense(Layer):
    def __init__(self, input_units, output_units, learning_rate=0.1):
# A dense layer is a layer which perfores a learned affine transformation:
```

Рисунок 4.9 – Програма для моделювання роботи нейронної мережі (продовження)

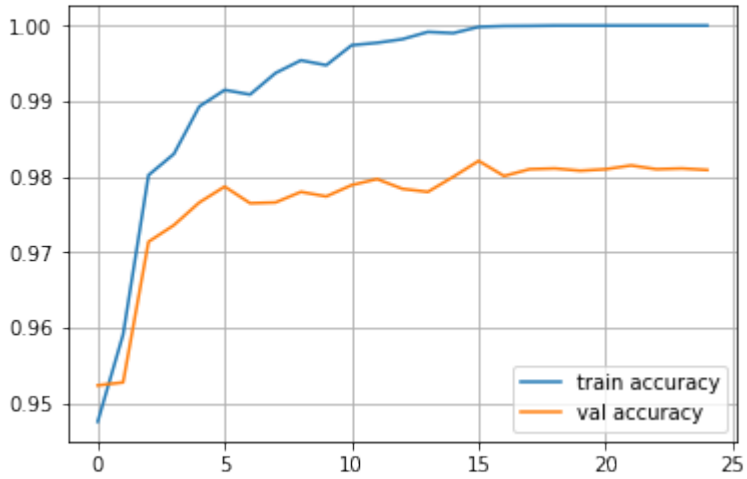


Рисунок 4.10 – Результати моделювання

5 ОХОРОНА ПРАЦІ

Охорона праці має величезне значення як в цілому, так і в конкретних галузях, зокрема в контексті методів забезпечення інформаційної безпеки Інтернету речей (IoT). Важливість охорони праці полягає в забезпеченні безпеки та здоров'я працівників, запобіганні травматизму та захисті від негативного впливу робочих умов на здоров'я.

Під час виконання кваліфікаційної роботи на розробника мали вплив наступні небезпечні та шкідливі виробничі фактори:

- Фізичні фактори: підвищена запиленість; підвищена чи понижена температура повітря робочої зони; підвищений рівень шуму на робочому місці; підвищена чи понижена вологість повітря; підвищений рівень електромагнітного випромінювання; підвищена чи понижена іонізація повітря; недостатня освітленість робочої зони; відсутність чи нестача природного освітлення.
- Психофізіологічні фактори: статичне перевантаження; розумове перевантаження; емоційні перевантаження.
- Фактори трудового процесу: важкість (тяжкість) праці - характеристика трудового процесу, що відображає рівень загальних енергозатрат, переважне навантаження на опорно-руховий апарат, серцево-судинну, дихальну та інші системи.

5.1 Технічні рішення з безпечного виконання роботи

5.1.1 Технічні рішення з безпечної організації робочих місць

Безпека робочих місць в галузі IoT вимагає комплексного підходу, який включає в себе різноманітні технічні рішення для забезпечення безпеки працівників та захисту від можливих ризиків і небезпек.

Одним з основних аспектів безпеки робочих місць є фізична безпека. Це охоплює захист працівників від можливих травм та ушкоджень, пов'язаних з

роботою з обладнанням IoT. Для цього можуть використовуватися різноманітні технічні рішення, такі як захисні оболонки для пристроїв, автоматизовані системи безпеки та контролю за доступом до небезпечних зон.

Крім того, важливо забезпечити ергономічне розташування робочих місць та обладнання, щоб уникнути зайвого фізичного навантаження та травматичних ситуацій. Це може включати в себе правильне розміщення моніторів, клавіатур, мишей та інших пристроїв, а також належне налаштування стільців та столів для забезпечення комфортної позиції під час роботи.

Крім того, безпека робочих місць також включає в себе захист від можливих електро небезпечних ризиків. Для цього рекомендується використовувати захисні пристрої, такі як вимикачі аварійного відключення, захисні оболонки та заземлення обладнання.

Загалом, технічні рішення з безпечної організації робочих місць у галузі IoT мають на меті забезпечити безпеку та комфорт працівників під час роботи з обладнанням IoT. Це включає в себе заходи для захисту від фізичних травм, оптимізації робочого середовища та захисту від електро небезпечних ризиків.

5.1.2 Електробезпека

Електробезпека в приміщенні, де виконувалася кваліфікаційна робота відігравала критично важливу роль у забезпеченні безпеки працівників та уникненні небезпечних ситуацій. Тип електромережі в приміщенні використовувалась "однофазна" мережа потужністю 10 квт, напруга 220 В з заземленням та захисними пристроями "Диференційні автомати". Категорія умов з небезпеки електро-травматизму – без підвищеної небезпеки.

Оскільки в приміщенні можуть існувати різноманітні загрози, такі як короткі замикання, перевантаження мережі, пошкодження електричних проводів, недоліки у роботі електроприладів або неправильна експлуатація обладнання.

Для запобігання цим загрозам були прийняти наступні заходи:

Регулярна перевірка стану електропроводки та електрообладнання з метою виявлення можливих проблем.

Використання захисних пристроїв, таких як автоматичні вимикачі та реле струму короткого замикання.

Правильна експлуатація та використання електроприладів, включаючи дотримання вимог до навантаження та використання розеток.

Проведення навчання та інструктажу працівників з питань електробезпеки та правил використання електрообладнання.

5.2 Технічні рішення з виробничої санітарії

5.2.1 Мікроклімат

Інтенсивність праці, що є індикатором важкості виконання роботи, напряму залежить від вироблення тепла в організмі людини. Кількість тепла, яку виробляє наш організм, може змінюватися від 40-50 кДж/год. у стані спокою до 3340 кДж/год. при виконанні важких фізичних завдань. Важливою умовою для забезпечення нормального теплового режиму є те, щоб теплові виділення повністю поглиналися оточуючим середовищем, що визначається наявністю теплового балансу. Праця в умовах підвищеної температури повітря (30 °С) при вологості 80 – 90% може призвести до зниження працездатності на 5% після 5 годин безперервної роботи. Низькі температури повітря, зі своєю чергою, можуть призвести до місцевого або загального переохолодження організму, що спричиняє зниження працездатності.

Мікроклімат на робочому місці нормується згідно ДСН 3.3.6.042-99

«Санітарні норми мікроклімату виробничих приміщень». Допустимі параметри мікроклімату для цієї категорії наведені в табл.5.1.

Для забезпечення необхідних за нормативами параметрів мікроклімату виробничих приміщень, відповідно до ДБНВ.2.5-67:2013 "Проектування вентиляції та кондиціонування", проектом передбачено наступні заходи:

- Розгортання сенсорної мережі IoT для постійного моніторингу температури та вологості повітря у виробничих приміщеннях.
- Використання розумних систем управління опаленням та кондиціонуванням для автоматичного регулювання температури відповідно до вимог нормативів.
- Проведення систематичних аналізів даних, зібраних від сенсорів IoT, для виявлення тенденцій у зміні мікроклімату та прийняття необхідних заходів у разі виявлення аномальних показників.
- Автоматичне включення та регулювання систем вентиляції в разі перевищення допустимих рівнів шкідливих речовин у повітрі.
- Забезпечення можливості дистанційного моніторингу та керування системами мікроклімату через веб-інтерфейс або мобільний додаток.

Таблиця 5.1 – Параметри мікроклімату

Період року	Допустимі		
	t,°C	W, %	V, м/с
Теплий	22-28	40-60	0,1-0,3
Холодний	20-24	75	0,2

Ці заходи спрямовані на покращення умов праці, забезпечення безпеки та комфорту працівників, а також відповідність вимогам стандартів щодо мікроклімату у виробничих приміщеннях.

5.2.2 Склад повітря робочої зони

Створення безпечних та сприятливих умов праці включає в себе ряд заходів, що полягають у нормуванні вмісту шкідливих речовин, точному визна-

ченні їх концентрації в повітрі та застосуванні сучасних технологій та організаційних методів для їх ефективного усунення. Оцінка гігієнічних умов праці на робочих місцях здійснюється враховуючи класифікацію праці за показниками шкідливості та небезпечності факторів виробничого середовища, важкості та напруженості трудового процесу, а також перелік речовин, які можуть бути канцерогенними для людини.

У приміщенні, де проводиться розробка Інтернету речей (IoT), можуть виявлятися шкідливі речовини у повітрі, такі як вуглекислий газ, пил та озон. Джерелами цих речовин є офісна техніка, а пил може потрапляти у приміщення ззовні. Нормативи гранично допустимих концентрацій шкідливих речовин у досліджуваному приміщенні подані в таблиці 5.2.

Параметри іонного складу повітря на робочому місці повинні відповідати допустимим нормам (табл.5.3).

Таблиця 5.2 – ГДК шкідливих речовин у повітрі

Назва речовини	ГДК, мг/м^3		Клас небезпечності
	Максимально разова	Середньодобова	
Вуглекислий газ	3	1	4
Пил нетоксичний	10	4	4
Озон	0,16	0,03	1

Для забезпеченняскладу повітря робочої зони відповідно до ДБНВ.2.5-67:2013, в роботі передбачені такі рішення:

- Використання систем вентиляції та кондиціонування повітря, які відповідають вимогам стандарту, для забезпечення належних умов роботи у приміщенні.

- Проведення регулярного технічного обслуговування та перевірок систем вентиляції для забезпечення їх ефективності та безперебійної роботи.
- Впровадження системи автоматичного керування параметрами повітряного середовища з метою забезпечення постійного контролю та оптимізації умов працівників.

Ці заходи спрямовані на підтримку здоров'я та комфорту працівників, а також відповідають вимогам нормативних документів щодо якості повітря у виробничому середовищі.

Таблиця 5.3 – Рівні іонізації повітря приміщень при роботі на ПК

Рівні	Кількість іонів в 1 $см^3$	
	n+	n-
Мінімально необхідні	400	600
Оптимальні	1500-3000	3000-5000
Максимально необхідні	50000	50000

5.2.3 Виробниче освітлення

Виробниче освітлення має велике значення для забезпечення комфортної та безпечної робочої зони для працівників. Воно впливає на їхню продуктивність, концентрацію та здоров'я. Технічні рішення в цій області спрямовані на забезпечення належного рівня освітлення з урахуванням різних факторів, таких як тип роботи, розміщення приміщення та індивідуальні потреби працівників.

Норми освітленості при штучному освітленні та КПО (для III поясу світлового клімату) при природному та суміщеному освітленні відповідно до ДБН В.2.5-28:2018 зазначені у таблиці 5.4.

Для забезпечення нормованого значення штучної освітленості в роботі передбачено:

- Використання енергоефективних світлодіодних (LED) джерел світла, які забезпечують високу якість освітлення та споживають менше електроенергії.
- Розробка оптимальної системи розташування та розподілу світильників для рівномірного освітлення робочої зони.
- Використання сенсорів освітленості та автоматичних систем регулювання освітлення для підтримки необхідного рівня освітленості відповідно до нормативних вимог.
- Проведення регулярного технічного обслуговування систем освітлення для забезпечення їх надійної та ефективної роботи.
- Аналіз даних з сенсорів освітленості для виявлення потенційних проблем та удосконалення системи освітлення з метою досягнення нормованих значень штучної освітленості.

Ці заходи спрямовані на створення комфортних та безпечних умов праці для працівників, а також відповідають вимогам нормативних документів щодо освітленості робочих приміщень.

5.2.4 Виробничий шум

Виробничий шум може бути серйозним джерелом стресу для працівників та може призводити до погіршення здоров'я, зниження продуктивності та навіть до появи проблем зі слухом. Санітарні норми виробничого шуму, ультразвуку та інфразвуку (ДСН 3.3.6.037-99) встановлюють допустимі рівні звукового тиску у октавних смугах частот та еквівалентні рівні звуку на місцях праці. У таблиці 5.5 наведено витяг з цих нормативів.

Таблиця 5.4 - Норми освітленості в приміщенні

Характеристика зорової роботи	Найменший розмір об'єкта розрізнювання	Розряд зорової роботи	Підрозряд зорової роботи	Контраст об'єкта розрізнення з фоном	Характеристика фона	Освітленість, лк		КПО, $e_н$, %			
						Штучне освітлення		Природнє освітлення		Сумісне освітлення	
						Комбіноване	Загальне	Верхнє або верхнє і бокове	Бокове	Верхнє або верхнє і бокове	Бокове
Високої точності	0,3 -0,5	III	г	великий	світлий	700	300	5	2	3	1,2

Таблиця 5.5 – Допустимі еквівалентні рівні шуму на робочих місцях

Вид професійної діяльності, місце праці	Еквівалентні рівні шуму, дБ
Творча діяльність, керівна робота з підвищеними вимогами, наукова діяльність, конструювання та проектування, програмування, викладання та навчання, лікарська діяльність; місця праці у приміщеннях – дирекції, проектно-конструкторських бюро, програмістів обчислювальних машин, у лабораторіях для теоретичних робіт та опрацювання даних, прийому хворих у медпунктах	50
Висококваліфікована робота, що вимагає зосередження, адміністративно-керівна діяльність, вимірювальні та аналітичні роботи у лабораторії; місця праці в приміщеннях цехового керівного апарату, контор, лабораторій	60

Для забезпечення допустимих параметрів шуму (поліпшення шумового клімату) в приміщенні згідно з ДСН 3.3.6.037-99 "Санітарні норми виробничого шуму" проектом передбачено наступні заходи:

- Встановлення звукоізоляційних матеріалів на стіни та стелі приміщення для поглинання звукових хвиль та зменшення внутрішнього шуму.
- Використання шумопоглинаючих матеріалів для підлоги з метою зменшення вібрацій та шуму, що виникає при руху обладнання та працівників.
- Встановлення акустичних панелей чи перегородок для розділення приміщень та зменшення внутрішнього шуму.
- Встановлення та регулярне обслуговування звукопоглинаючих систем вентиляції та кондиціонування повітря для зменшення рівня шуму в приміщенні.

Ці заходи спрямовані на створення комфортних та безпечних умов праці для працівників та відповідають вимогам санітарних норм щодо виробничого шуму.

5.2.5 Виробничі випромінювання

У роботі розглядаються умови, що можуть призводити до виникнення різних видів виробничих випромінювань, таких як електромагнітні поля (ЕМП) та ультрафіолетове випромінювання. Джерелами цих випромінювань можуть бути електронне обладнання, виробничі процеси, комп’ютерне та офісне обладнання.

Допустимі значення цих параметрів встановлюються національними стандартами та нормативами з охорони праці та безпеки, які базуються на рекомендаціях Всесвітньої організації охорони здоров'я та інших міжнародних організацій. Наприклад, для електромагнітних полів допустимі значення можуть бути встановлені згідно з рекомендаціями Міжнародної комісії з захисту від неіонізуючих випромінювань.

Гранично допустимі значення характеристик електромагнітних полів для умов праці, в яких знаходиться розробник, вказані в таблиці 5.6.

Таблиця 5.6 - Гранично допустимі значення характеристик ЕМП

Найменування параметрів	Допустиме Значення
Напруженість електромагнітного поля по електричної складової на відстані 50 см від поверхні відеомонітора	10 В / м
Напруженість електромагнітного поля по магнітної складової на відстані 50 см від поверхні відеомонітора	0,3 А / м
Напруженість електростатичного поля не повинна перевищувати для дорослих користувачів	20 кВ / м
Напруженість електромагнітного поля на відстані 50 см навколо ВДТ по електричній складовій повинна бути не більше:	
в діапазоні частот 5 Гц - 2 кГц;	25 В / м
в діапазоні частот 2 - 400 кГц	2,5 В / м
Щільність магнітного потоку повинна бути не більше:	
в діапазоні частот 5 Гц - 2 кГц;	250нТл
в діапазоні частот 2 - 400 кГц	25 нТл
Поверхневий електростатичний потенціал не повинен перевищувати	500 В

Технічні рішення щодо попередження шкідливого впливу цього випромінювання на працюючих можуть включати використання екранування, збільшення відстані до джерела випромінювання, використання засобів індивідуального захисту (наприклад, екранувальних костюмів, окулярів тощо), регулярний моніторинг рівня випромінювання та впровадження заходів для зниження експозиції.

5.3 Технічні рішення з пожежної безпеки

Запобігання виникненню пожеж – головний пріоритет у будь-якому приміщенні, де проводиться розробка інтернет-речей (IoT). Це досягається шляхом усунення потенційних джерел загоряння та джерел запалювання. На кожному етапі слід дотримуватися відповідних пожежних заходів безпеки, спрямованих на попередження небезпечних пожежних ситуацій, які можуть загрожувати безпеці людей та призвести до матеріальних збитків.

Метою системи пожежної безпеки є не лише уникнення виникнення пожежі в межах нормативів, але й обмеження її поширення, раннє виявлення та швидке ліквідування у разі виникнення, а також захист персоналу і майна. У приміщеннях категорії "Д" можливі причини пожежі включають порушення правил техніки безпеки та надмірне навантаження електричної мережі, що може призвести до перегріву проводів та з'єднань.

Система запобігання пожежі передбачає низку заходів, включаючи уникнення накопичення горючих матеріалів у приміщенні, встановлення системи захисту від атмосферних розрядів, регулярну перевірку ізоляції, створення спеціальних зон для куріння та проведення періодичних навчань з пожежної безпеки.

Технічні рішення системи протипожежного захисту мають на меті уникнення можливих причин пожежі, таких як коротке замикання електричних кіл чи порушення правил техніки безпеки. Серед заходів з попередження пожежі –

систематична перевірка електроприладів, проведення навчань з пожежної безпеки та дотримання всіх вимог безпеки на робочому місці.

Для позначення місць розташування головних засобів загашування пожежі рекомендується встановлювати покажчики відповідно до чинних нормативів, що діють на рівні держави. Ці покажчики мають бути розміщені на видному місці на встановленій стандартами висоті. Відповідно до вимог, орендарі, власники підприємств, установ і організацій, або уповноважені ними органи повинні вживати наступних заходів:

- Розробляти та впроваджувати нові технологічні рішення для забезпечення безпеки в разі пожежі.
- Забезпечувати дотримання вимог щодо пожежної безпеки та рекомендацій контролюючих органів.
- Організовувати навчання та роботу з пожежної безпеки в колективі.
- Забезпечувати належний стан пожежного обладнання, комунікаційних мереж та інших засобів протипожежного захисту.
- Створювати і підтримувати ефективну систему пожежного контролю та захисту.
- Надавати необхідні відомості та документи на вимогу органів державного пожежного нагляду.
- Впроваджувати автоматизовані системи для виявлення та гасіння пожеж.
- Систематично повідомляти пожежну службу про будь-які несправності у пожежному обладнанні.

Після завершення роботи всі електроприлади, а також їх живлення, повинні бути відключені від електромережі, за винятком пристроїв протипожежного та охоронного призначення. Електропроводи для з'єднання комп'ютерів та інших пристроїв повинні прокладатися через матеріали, які не піддаються горінню.

Згідно зі стандартами [12], рекомендується розміщення одного порошкового або вуглекислотного вогнегасника масою заряду від 3 до 5 кг на кожні 20 м^2 приміщення вказаних категорій пожежної безпеки, а також класів пожеж –

A, B і E. Крім того, на поверсі, де розташоване приміщення, рекомендується наявність двох порошкових вогнегасників масою заряду 10 кг.

Таким чином, в приміщенні планується встановити два порошкових вогнегасники, які будуть розміщені на протилежних сторонах приміщення. Вони будуть закріплені на висоті не більше 1,5 метра від підлоги до нижнього краю вогнегасника, забезпечуючи достатню відстань від дверей для повного доступу. Розташування вогнегасників завжди буде чітко позначено та доступно. Для цього планується встановити вказівний знак на видному місці на висоті від 2,0 до 2,5 метра від підлоги.

ВИСНОВКИ

В першому розділі даної роботи було розглянуто основні аспекти Інтернету речей. IoT — це надзвичайно зручна технологія, яка покликана полегшити життя людей і позбавити їх від труднощів. Використання цієї технології зменшує ризики небезпечних чи травматичних ситуацій для людей, що є великим плюсом для промислової сфери користування, оскільки велика кількість операцій буде автоматизована.

В другому розділі роботи наведено сучасні вимоги до мереж Інтернету речей, а також потенційні загрози на кожному рівні Інтернету речей (IoT): рівні сприйняття, мережі, підтримки та програми. Показано, що безпека та конфіденційність є єдиною перешкодою на шляху розвитку IoT.

У третьому розділі роботи розглядаються методи захисту інформації у мережі IoT. Обговорюється метод криптографічних еліптичних кривих, його основні характеристики та те, як він використовується для шифрування даних. Цей метод двоключового шифрування має позитивний рівень надійності. Він забезпечує таку надійність за допомогою різних технологій, таких як цифровий підпис і обмін ключами шифрування. Ці технології роблять його більш ефективним і безпечним, ніж методи, подібні до RSA.

У четвертому розділі роботи запропоновано для підвищення забезпечення інформаційної безпеки Інтернету речей використовувати методи штучного інтелекту, а саме – нечіткий контролер та штучну нейронну мережу.

П’ятий розділ присвячено охороні праці. Було розглянуто кілька технічних рішень для забезпечення безпечного виконання роботи, а також гігієни та санітарії на робочому місці. У рамках гігієни праці та виробничої санітарії було вивчено такі фактори, як мікроклімат, склад повітря робочої зони, освітлення, шум і випромінювання. Крім того, було розглянуто пожежну безпеку та технічні рішення для систем запобігання та протипожежного захисту.

Таким чином, можна стверджувати, що цілі, наведні у вступі до цієї бакалаврської кваліфікаційної роботи, були виконані, про що можна зробити відповідний висновок.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kovalenko O. Knowledge Driven Cyber-Convergent Systems Based on Situational Agents. IEEE 17th International Conference on Computer Sciences and Information Technologies (CSIT). 2022. P. 243–246. DOI: 10.1109/CSIT56902.2022.10000762.

2. Kovalenko O. Systems Convergence for Situational Control and Decision Making in Distributed Environments. IEEE 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET). 2022. P. 344–347. DOI: 10.1109/TCSET55632.2022.9767006.

3. Дугінець Г. В. Концепція "Інтернет речей" у глобальному виробництві: досвід для України. Економіка і регіон. 2018. No 1. С. 127-133.

4. Дявіл А. Г. Концепція IoT-проекту системи розумного приміщення / А. Г. Дявіл // Збірник матеріалів XX Міжнародної наукової конференції молодих вчених, аспірантів та студентів «Проблеми розвитку фінансово-кредитної системи» до 80-річчя Львівського інституту ДВНЗ «Університет банківської справи». — Київ : ДВНЗ «Університет банківської справи», 2020. — С. 295—297

5. Internet of Things for Industrial Systems: Trainings / Yu.P. Kondratenko and V.S. Kharchenko (Eds.) – Ministry of Education and Science of Ukraine, Petro Mohyla Black Sea National University, Zaporizhzhia National Technical University, National Aerospace University “KhAI”, 2019. – 143 p. Мунистер В.Д. Дом, который построил сам себя. Сетевой практикум. IoT. – Самиздат, 2020. – 154 с.

6. К.П. Сторчак, А.М. Тушич, І.М. Срібна, Н.Д. Яковенко, Д.В. Кравець. «Технології Інтернет речей». - 2021.

7. Пулеко І. В. Єфіменко А. А. Архітектура та технології Інтернету речей: навч. посіб. / І.В. Пулеко, А.А. Єфіменко. – Електронні дані. – Житомир: Державний університет «Житомирська політехніка», 2022. – 234 с.

8. Технології Інтернету речей в управлінні пристроями на мікроконтролерах: Навчальний посібник [Електронний ресурс] / І.Ш. Невлюдов, В.А. Андрусевич, С.П. Новоселов, О.Г. Резніченко. –Електронне видання. – Харків: ХНУРЕ, 2023. – 214 с.

9. Архітектура та технології Інтернету речей: навч. посіб. / І.В. Пулеко, А.А. Єфіменко. – Електронні дані. – Житомир: Державний університет «Житомирська політехніка», 2022. – 234 с.

10.Жураковський, Б. Ю. Технології інтернету речей. Навчальний посібник: навчальний посібник для здобувачів ступеня бакалавра за освітньою програмою «Інформаційне забезпечення робототехнічних систем» за спеціальністю 126 «Інформаційні системи та технології» / Б. Ю. Жураковський, І. О. Зенів ; КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, 2021. – 271 с.

11.Смирнов О.С. Розвиток «Інтернету речей», доповненої реальності та комунікаційних технологій: стаття / К. С. Голохваст, О. В. Тумялис. — Далекосхідний федеральний університет — Режим доступу: https://arxiv.org/ftp/arxiv/papers/1902/1902.08008.pdf

12.Тюрин В.А. Інтернет речей: нові можливості для світу та бізнесу — Мережа. Фактори — Режим доступу: https://megamozg.ru/post/25334/

13.Вічугова А. Криптографія в IoT та Big Data: захищенні протоколи та мікросхеми [Електронний ресурс] — Режим доступу: https://www.bigdataschool.ru/bigdata/iot-protocol-microchip-crypto-bigdata.html

14.Могильний С. Б. Покрокова побудова системи для Інтернету речей // Вісник Національного технічного університету України "Київський політехнічний інститут". Серія : Радіотехніка. Радіоапаратобудування. - 2016. - Вип. 65. - С. 73-78. – Те саме [Електронний ресурс] // Вісник Національного технічного університету України "Київський політехнічний інститут": [сайт]. http://nbuv.gov.ua/UJRN/VKPI_rr_2016_65_8. - Назва з екрану.

15.Архітектура та технології Інтернету речей: навч. посіб. / І.В. Пулеко, А.А. Єфіменко. – Електронні дані. – Житомир: Державний університет «Житомирська політехніка», 2022. – 234 с.

16.Даник Ю. Г. Визначення сутності та змісту кібернетичної загрози / Ю.Г. Даник, В. І. Шестаков, С. В. Чернишук // Проблеми створення, випробування та експлуатації складних інформаційних систем: зб. наук. праць. – Житомир: ЖВІНАУ, 2012. – Спецвипуск 2. – С. 5-1 8. Присяжнюк М. М. Особливості забезпечення кібербезпеки / М. М. Присяжнюк, Є. І. Цифра // Реєстрація, зберігання та обробка даних. – 2017. – Т. 19. – № 2. –С. 61 – 68.

17.Дудатьєв А. В. Захист комп'ютерних мереж. Теорія та практика. Навчальний посібник / Дудатьєв А. В., Войтович О. П., Каплун В. А.- Вінниця ВНТУ, 2010.-219 с.

18.Нечіткі множини в системах управління та прийняття рішень: навч. посіб. / Т.А. Желдак, Л.С. Коряшкіна, С.А. Ус, за редакцією С.А. Ус ; М-во освіти і науки України, Нац. техн. ун-т ≪Дніпровська політехніка≫. – Дніпро : НТУ ≪ДП≫, 2020. – 387 с.

19.Синтез нечітких регуляторів в системах автоматичного керування: навчальний посібник / О. В. Разживін, О. В. Суботін. – Краматорськ : ЦТРІ «Друкарський дім», 2017. – 212 с.

20.Кондратенко Ю. П. Нечіткі множини та нечітка логіка. Методичні рекомендації та вказівки для виконання лабораторних робіт студентами спеціальності 122 «Комп’ютерні науки» / Ю. П. Кондратенко, Г. В. Кондратенко, Є. В. Сіденко ; під ред. д-р техн. наук, професор Ю. П. Кондратенка. – Миколаїв : ЧНУ ім. Петра Могили, 2019. – 36 с.

21.Кононюк А.Ю. Нейроні мережі і генетичні алгоритми – К.:«Корнійчук», .2008. – 446 с.

22.Штучні нейронні мережі: навчальний посібник / С. В. Ткаліченко. – Кривий Ріг, 2023. –150 с.

23.Основи нейрокомп’ютингу : навчально-методичний посібник до практичних занять / В. Д. Дмитрієнко, О. Ю. Заковоротний, В. І. Носков, М. В. Мезенцев. – Х.: НТМТ, 2014. – 140 с.

24.Теорія та практика нейронних мереж : навч. посіб. / Л. М. Добровська, І. А. Добровська. – К. : НТУУ «КПІ» Вид-во «Політехніка», 2015. – 396 с. – Бібліогр. : с. 385–387.

25.ДСН 3.3.6.042-99 “Санітарні норми мікроклімату виробничих приміщень” - [Електронний ресурс] - Режим доступу: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=1 4283

26.ДБНВ.2.5-67:2013 "Проектування вентиляції та кондиціонування" - [Електронний ресурс] - Режим доступу: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=5 0154

27.ДБН В.2.5-28:2018 “Природне і штучне освітлення” - [Електронний ресурс] - Режим доступу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=79 885

28.ДСанПіН 3.3.2.007-98 “Державні санітарні правила і норми роботи з візуальними дисплейними терміналами” електронно-обчислювальних машин. - [Електронний ресурс] - Режим доступу: https://zakon.rada.gov.ua/rada/show/v0007282-98#Text

29.НПАОП 0.00-7.15-18 “Вимоги щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями”. - [Електронний-ресурс] - Режим доступу: http://sop.zp.ua/norm_npaop_0_00-7_15-18_01_ua.php

30.Правила улаштування електроустановок - [Електронний ресурс] - Режим доступу: http://www.energiy.com.ua/PUE.html

Додаток А
(обов’язковий)

ІЛЮСТРАТИВНА ЧАСТИНА
МЕТОДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІНТЕРНЕТУ РЕЧЕЙ
назва бакалаврської дипломної роботи

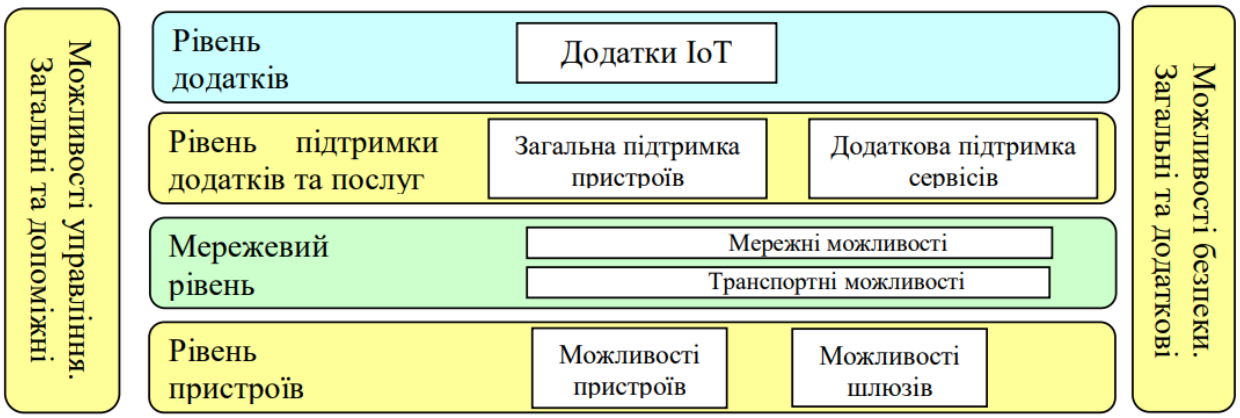


Рисунок 1 – Еталонна модель IoT

Рисунок 2 – Класифікація атак

Рисунок 3 – Загрози безпеки в IoT

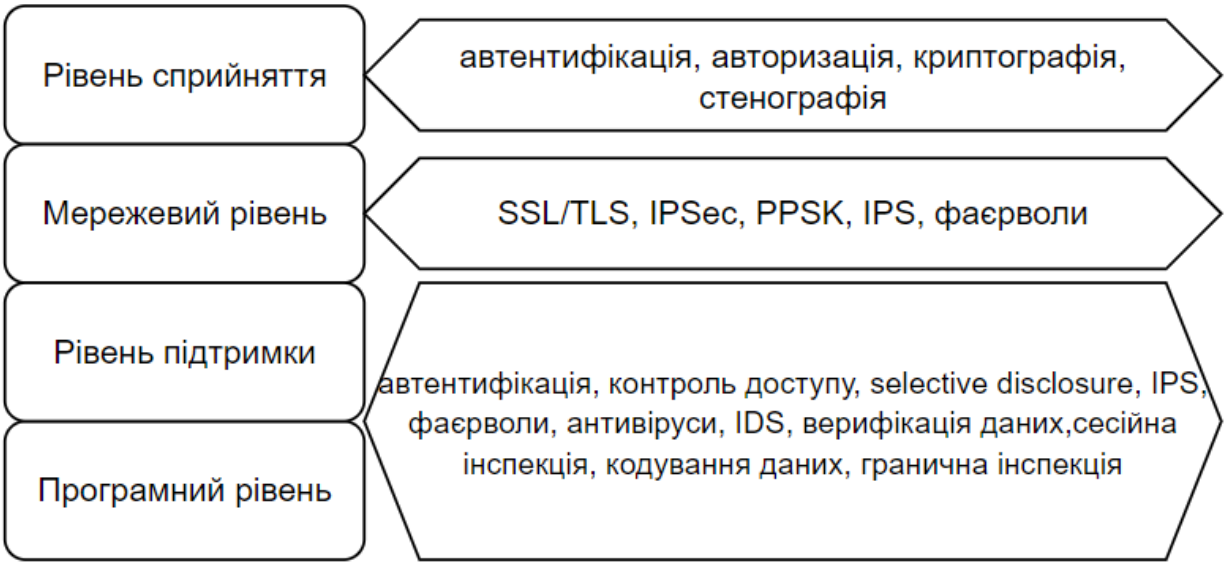


Рисунок 4 – Рішення безпеки IoT

Рисунок 5 – Методи забезпечення інформаційної безпеки

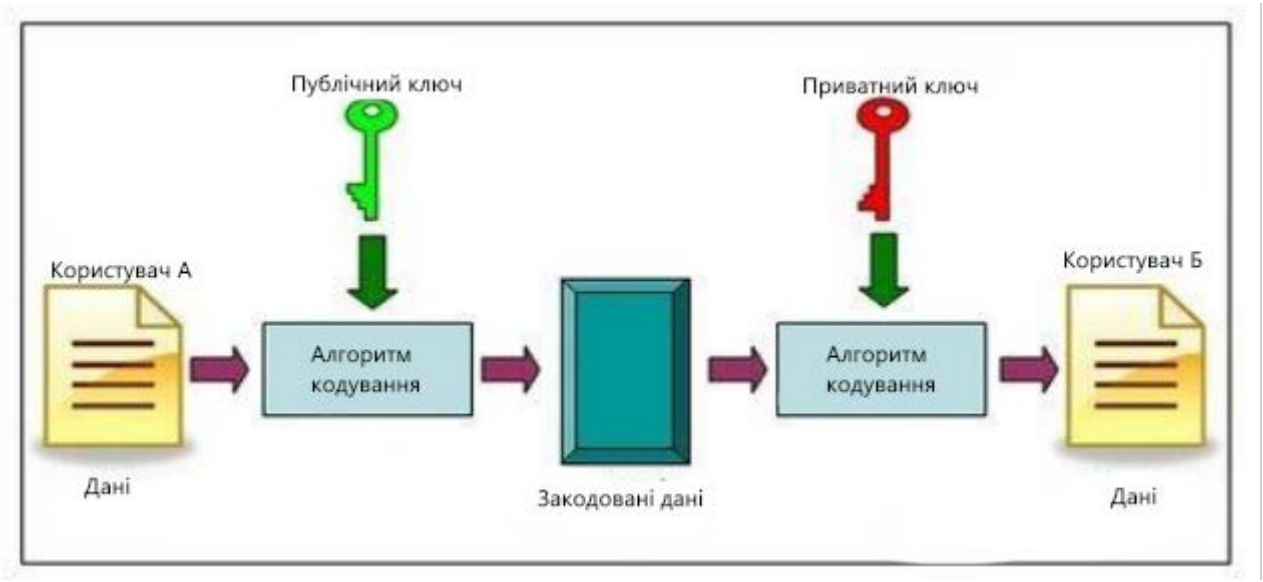


Рисунок 6 – Еліптична криптографія

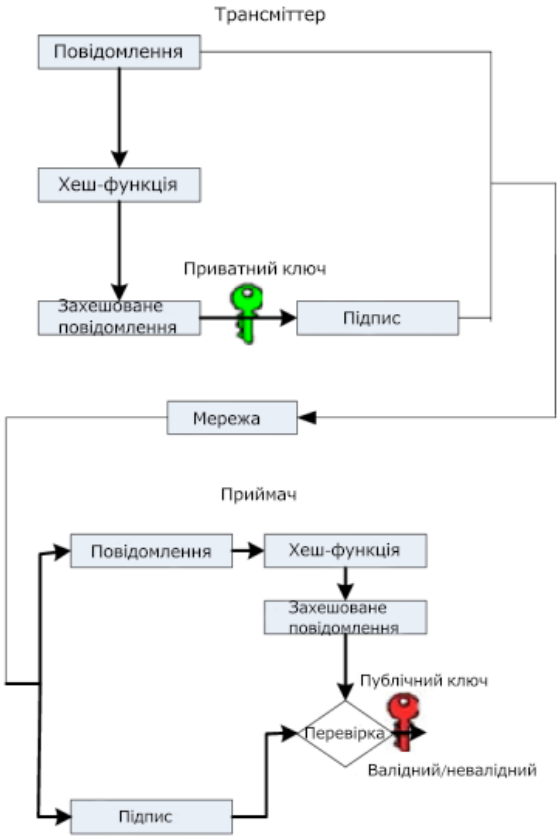


Рисунок 7 – Алгоритм цифрового підпису

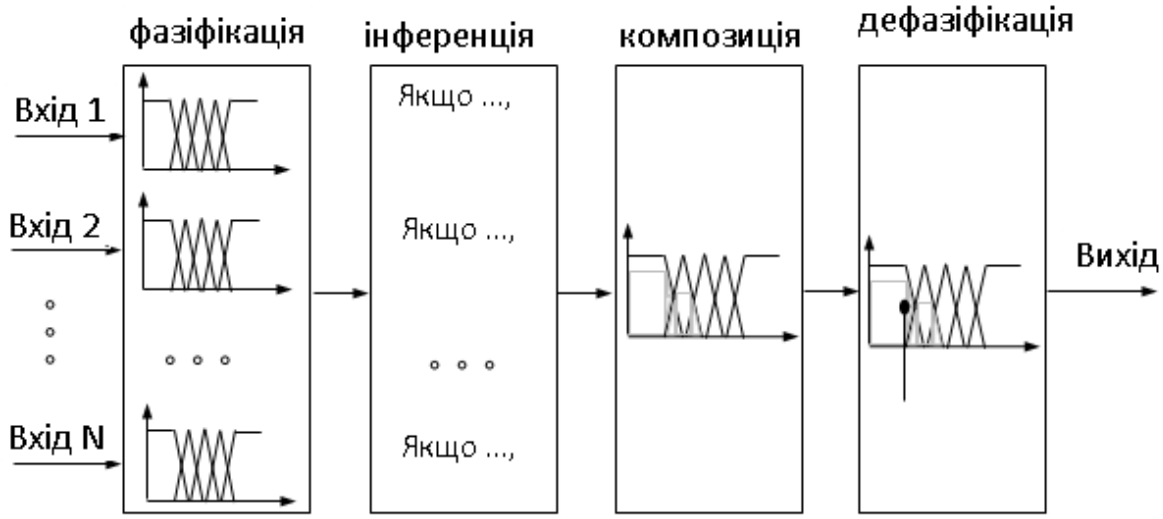
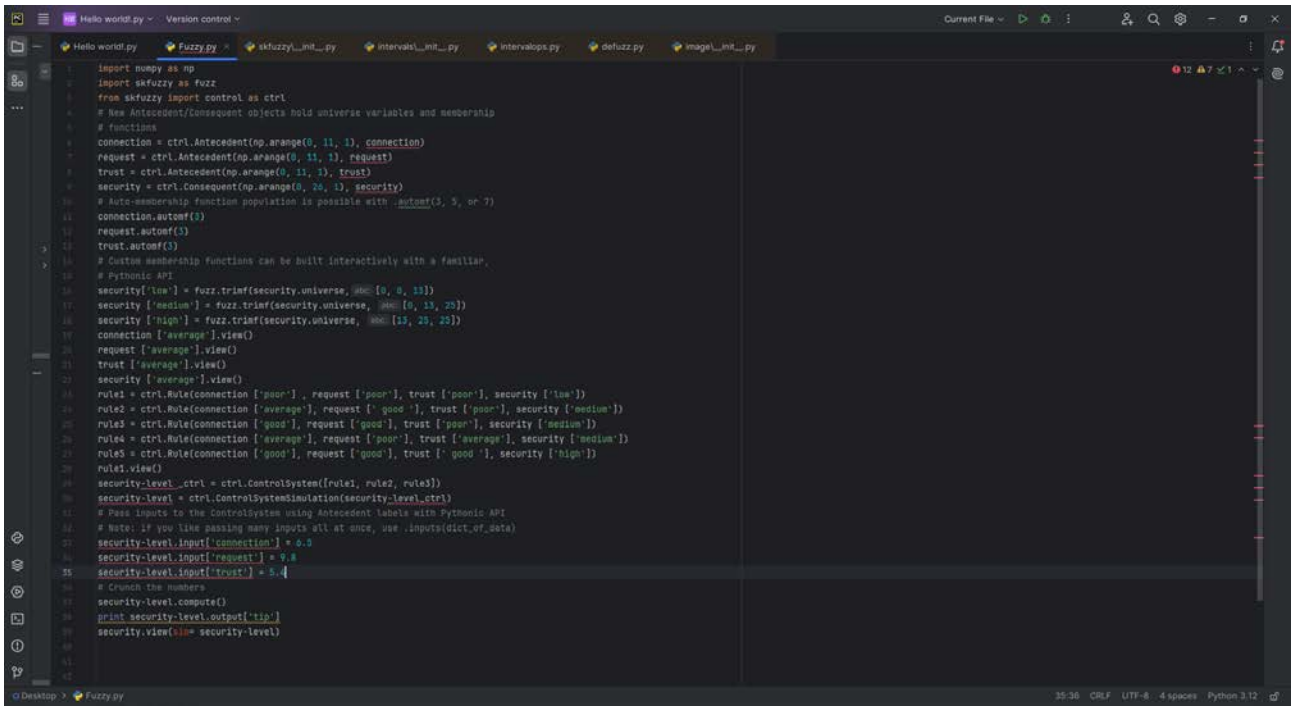


Рисунок 8 – Стуктурна схема нечіткого контролера



```
import numpy as np
import skfuzzy as fuzz
from skfuzzy import control as ctrl
# New Antecedent/Consequent objects hold universe variables and membership
# functions
connection = ctrl.Antecedent(np.arange(0, 11, 1), 'connection')
request = ctrl.Antecedent(np.arange(0, 11, 1), 'request')
trust = ctrl.Antecedent(np.arange(0, 11, 1), 'trust')
security = ctrl.Consequent(np.arange(0, 26, 1), 'security')
# Auto-membership function population is possible with .automf(3, 5, or 7)
connection.automf(3)
request.automf(3)
trust.automf(3)
# Custom membership functions can be built interactively with a familiar,
# Pythonic API
security['low'] = fuzz.trimf(security.universe, abc [0, 0, 13])
security ['medium'] = fuzz.trimf(security.universe, abc [0, 13, 25])
security ['high'] = fuzz.trimf(security.universe, abc [13, 25, 25])
connection ['average'].view()
request ['average'].view()
trust ['average'].view()
security ['average'].view()
rule1 = ctrl.Rule(connection ['poor'] , request ['poor'], trust ['poor'], security ['low'])
rule2 = ctrl.Rule(connection ['average'], request [' good '], trust ['poor'], security ['medium'])
rule3 = ctrl.Rule(connection ['good'], request ['good'], trust ['poor'], security ['medium'])
rule4 = ctrl.Rule(connection ['average'], request ['poor'], trust ['average'], security ['medium'])
rule5 = ctrl.Rule(connection ['good'], request ['good'], trust [' good '], security ['high'])
rule1.view()
security_level_ctrl = ctrl.ControlSystem([rule1, rule2, rule3])
security_level = ctrl.ControlSystemSimulation(security_level_ctrl)
# Pass inputs to the ControlSystem using Antecedent labels with Pythonic API
# Note: if you like passing many inputs all at once, use .inputs(dict_of_data)
security_level.input['connection'] = 6.5
security_level.input['request'] = 9.8
security_level.input['trust'] = 5.4
# Crunch the numbers
security_level.compute()
print security_level.output['tip']
security.view(sim= security_level)
```

Рисунок 9 – Програмний код нечіткого контролера

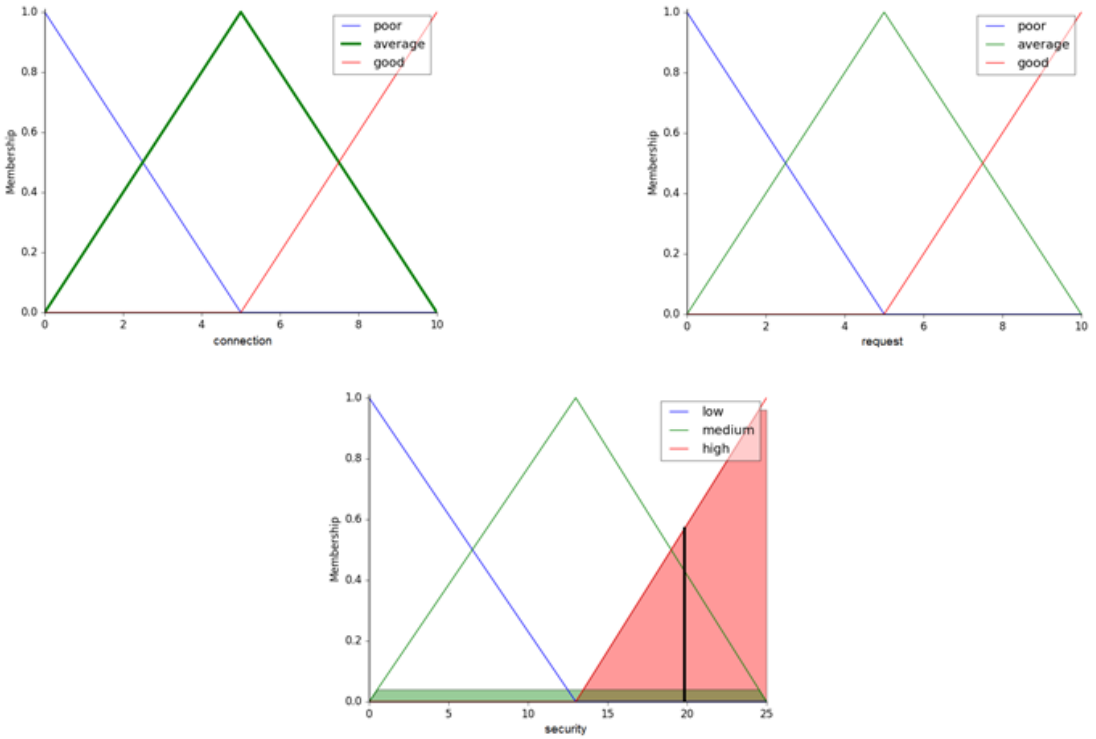


Рисунок 10 – Результат роботи нечіткого контролера

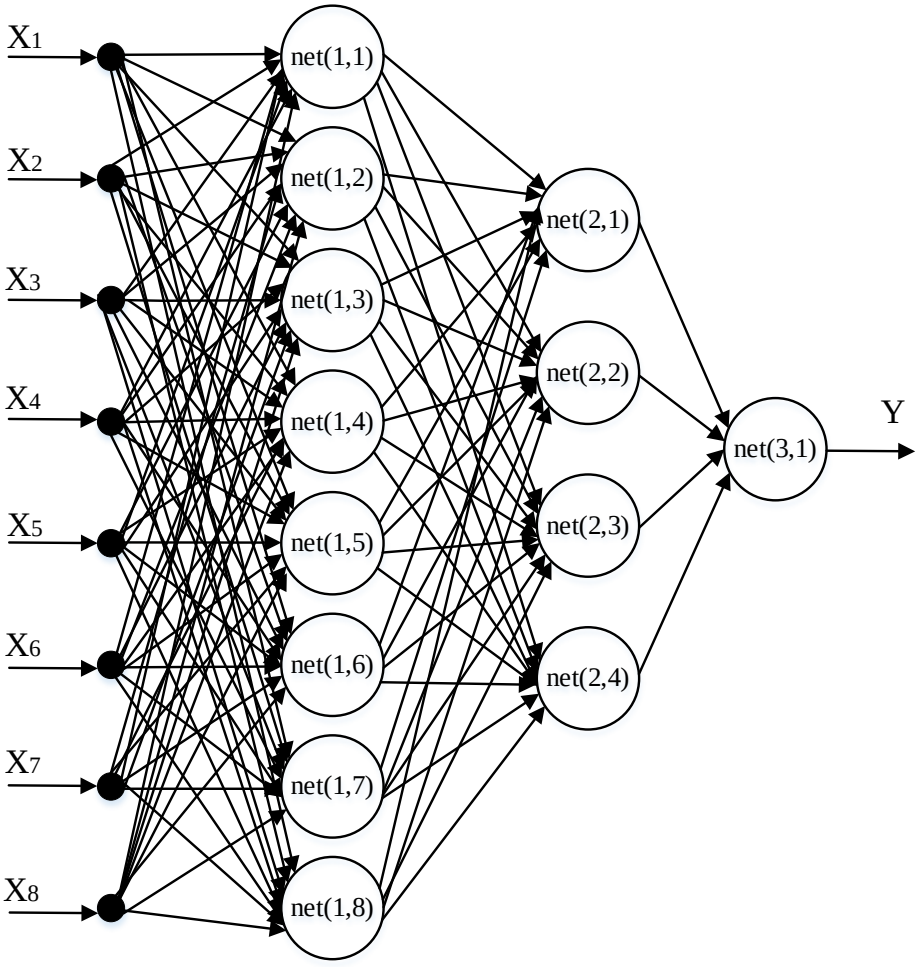


Рисунок 11 – Архітектура нейронної мережі

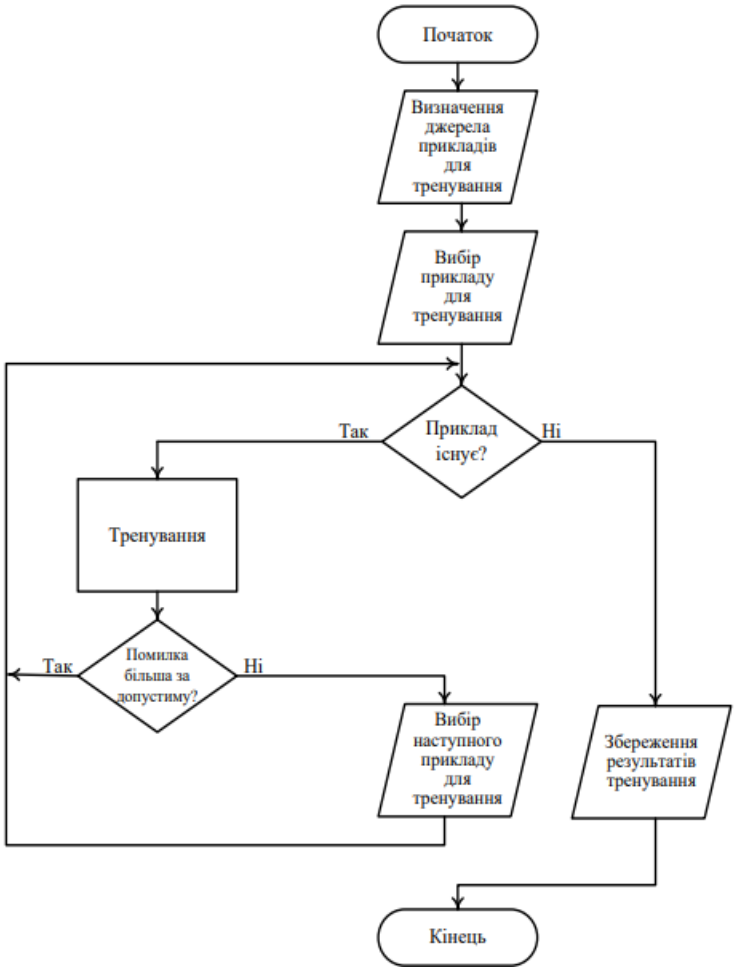


Рисунок 12 – Алгоритм навчання нейронної мережі

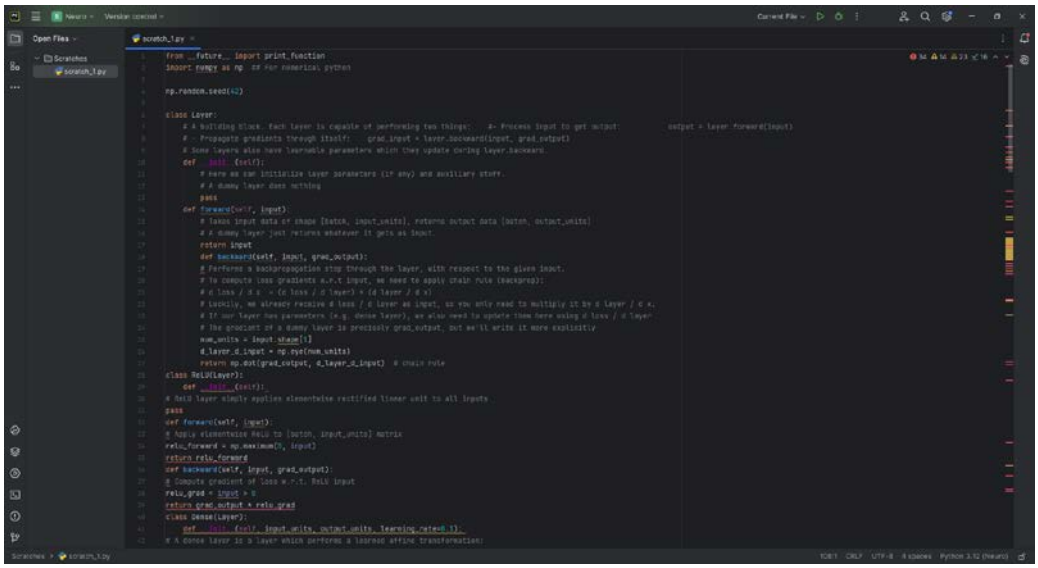


Рисунок 13 – Програмний код нейронної мережі

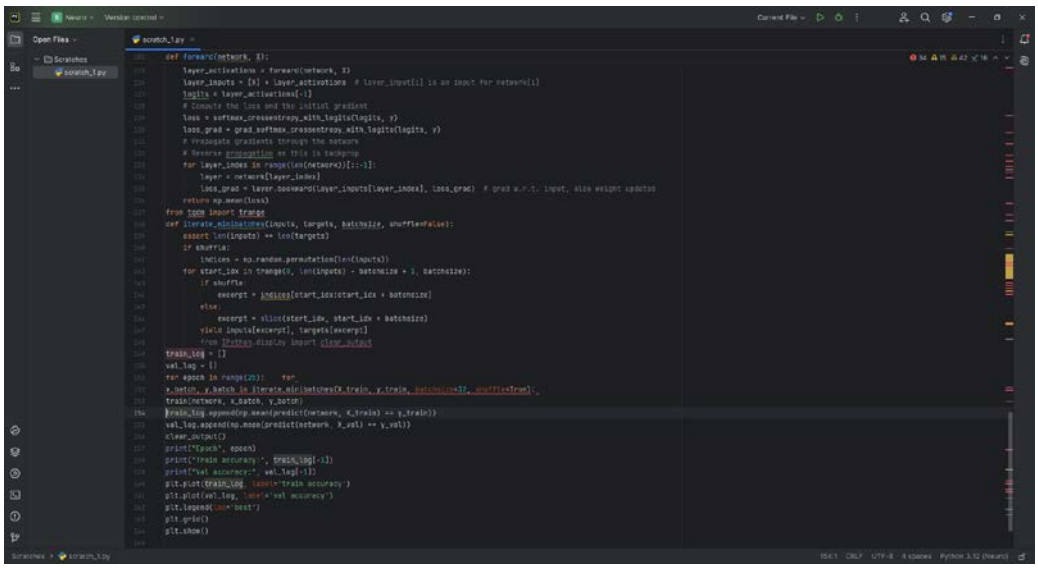


Рисунок 14 – Програмний код нейронної мережі (продовження)

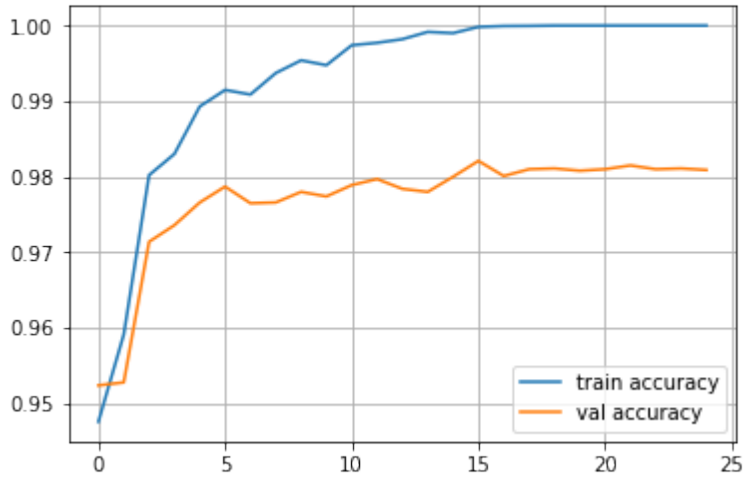


Рисунок 15 – Результат навчання нейронної мережі

Додаток Б
(обов`язковий)

ПРОТОКОЛ
ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ
НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: Методи забезпечення інформаційної безпеки Інтернету речей

Тип роботи: Бакалаврська дипломна робота
(БДР, МКР)

Підрозділ кафедра Інфокомунікаційних систем і технологій, факультет Інформаційних електронних систем
(кафедра, факультет)

Показники звіту подібності Unicheck

Оригінальність 93,76 % Схожість 6,24 %

Аналіз звіту подібності (відмітити потрібне):

■ 1. Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.

☐ 2. Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.

☐ 3. Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа відповідальна за перевірку _____ Васильківський М.В.
(підпис) (прізвище, ініціали)

Ознайомлені з повним звітом, який був згенерований системою Unicheck щодо роботи.

Автор роботи _____ Костьянін В. Ю.
(підпис) (прізвище, ініціали)

Керівник роботи _____ Семенова О.О.
(підпис) (прізвище, ініціали)