НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ВДОСКОНАЛЕННЯ МЕТОДІВ ЗАХИСТУ ВІД АТАК НА СИСТЕМИ ІНТЕРНЕТУ РЕЧЕЙ»

Виконав: здобувач 4 курсу
Рівень бакалавр
Галузь знань 12 «Інформаційні технології»,
спеціальність 125 «Кібербезпека»
Шагалін Кіріл Андрійович

Керівник: к.т.н., доцент
Кухаренко Сергій Вікторович

Рецензент: к.т.н., доцент
Бойко Віктор Дмитрович

Одеса – 2024

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
Факультет кібербезпеки та інформаційних технологій
Кафедра **кібербезпеки**
Галузь знань: **12 Інформаційні технології**
Спеціальність: **125 Кібербезпека**
Назва освітньої програми: **Кібербезпека**

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
професор С.А. Горбаченко
_____ «____»_____ 20__ року

З А В Д А Н Н Я
на кваліфікаційну (бакалаврську) роботу
здобувачу Шагаліну Кірілу Андрійовичу

1. Тема роботи: «Вдосконалення методів захисту від атак на системи інтернету речей»
Керівник роботи: к.т.н, доцент Кухаренко Сергій Вікторович
затверджені наказом НУ ОЮА від «02» квітня 2024 року № 809-06
2. Строк подання здобувачем роботи «20» травня 2024 рік
3. Дата видачі завдання«15» вересня 2023 рік

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської роботи	Строк виконання етапів роботи	Примітка

Здобувач _____
(підпис) (прізвище та ініціали)

Керівник роботи _____
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Шагалін К.А Кваліфікаційна робота на тему “Вдосконалення методів захисту від атак на системи Інтернету речей (IoT)” на здобуття першого (бакалаврського) рівня вищої освіти за спеціальністю 125 Кібербезпека, освітньою програмою: Кібербезпека, містить 10 рисунків та 15 літературних джерел за переліком посилань. Робота виконана на 40 сторінках загального тексту і 30 сторінках основного тексту.

Метою роботи є дослідження та вдосконалення методів захисту від атак на системи Інтернету речей (IoT). Визначено основні види загроз для IoT, включаючи фішинг, атаки типу "людина посередині" (MitM), відмови в обслуговуванні (DoS), експлуатацію вразливостей ПЗ, шкідливе ПЗ (Malware) та атаки на паролі, що актуалізує необхідність розробки ефективних методів захисту.

Досліджено ключові елементи IoT2-систем та методи їхнього захисту. Для розуміння роботи IoT-системи було створено топологію "розумного" будинку в Cisco Packet Tracer та розроблено математичну модель зараження вірусом вузлів мережі IoT. Проведено експерименти на імітаційній моделі IoT у мультиагентному середовищі NetLogo, визначено стійкість і резистентність мереж IoT до атак.

Результати даного дослідження можуть бути використані для розробки політик безпеки для корпорацій та установ, які прагнуть захистити свої IoT-системи від сучасних загроз. Зокрема, вони можуть слугувати основою для навчання співробітників з питань кібербезпеки, збільшуючи їх обізнаність щодо потенційних кіберзагроз та методів їхнього усунення.

Можливими напрямками подальших досліджень є розробка нових, більш ефективних методів захисту, які могли би забезпечити кращий захист IoT-систем від зростаючих загроз кібербезпеки.

ІНТЕРНЕТ РЕЧЕЙ, ЗАХИСТ, МЕХАНІЗМИ, МЕРЕЖА, ТЕХНОЛОГІЯ.

ABSTRACT

Shagalin K. A. The qualification paper on the topic “Improving Protection Methods Against Attacks on Internet of Things (IoT) Systems” for obtaining the first (bachelor’s) level of higher education in the specialty 125 Cybersecurity, educational program: Cybersecurity, contains 10 figures and 15 literature sources listed in the references. The paper is composed of 40 pages of total text and 30 pages of main text.

The purpose of this work is to research and improve protection methods against attacks on Internet of Things (IoT) systems. The main types of threats to IoT are identified, including phishing, man-in-the-middle (MitM) attacks, denial of service (DoS) attacks, exploitation of software vulnerabilities, malware, and password attacks, highlighting the necessity for developing effective protection methods.

Key elements of IoT systems and methods of their protection were studied. To understand the operation of an IoT system, a "smart" home topology was created in Cisco Packet Tracer, and a mathematical model of virus infection of IoT network nodes was developed. Experiments were conducted on an IoT simulation model in the multi-agent environment NetLogo, determining the resilience and resistance of IoT networks to attacks.

The results of this research can be used to develop security policies for corporations and institutions aiming to protect their IoT systems from modern threats. In particular, they can serve as a basis for training employees on cybersecurity issues, increasing their awareness of potential cyber threats and methods to mitigate them.

Possible directions for further research include developing new, more effective protection methods that could provide better security for IoT systems against growing cybersecurity threats.

INTERNET OF THINGS, PROTECTION, MECHANISMS, NETWORK, TECHNOLOGY.

ЗМІСТ

ВСТУП

Інтернет речей (IoT) – це концепція, яка стрімко розвивається та знаходить застосування у різних сферах життя. Від розумних будинків та міст до промислових систем і медицини, IoT забезпечує новий рівень автоматизації та ефективності, значно покращуючи якість життя та підвищуючи продуктивність. Проте, разом із широким впровадженням IoT з'являються нові загрози та виклики, пов'язані з безпекою даних та захистом інформації. Актуальність даного дослідження полягає у необхідності розробки надійних механізмів захисту IoT систем від різноманітних кібератак, що можуть призвести до значних фінансових втрат та порушення приватності користувачів.

Метою кваліфікаційної роботи є дослідження сучасних загроз для Інтернет речей, аналіз існуючих методів захисту та розробка нових механізмів, спрямованих на покращення безпеки IoT систем

Завдання роботи включають:

1. Аналіз ключових елементів систем IoT та вразливостей, які можуть бути використані для атак.

2. Розроблення математичної моделі зараження вірусами вузлів IoT мережі.

3. Дослідження існуючих та перспективних методів захисту систем IoT.

4. Формування рекомендацій для підвищення безпеки IoT систем.

Структура кваліфікаційної роботи складається з трьох розділів, вступу, висновків та переліку посилань.

Перший розділ присвячений загальним відомостям про Інтернет речей та областям його застосування, надається огляд історії розвитку IoT, його основних концепцій та можливостей.

В другому розділі описані ключові елементи систем IoT та методи їх захисту, а також математична модель зараження вірусами вузлів мережі IoT.

Третій розділ присвячений дослідженню атак на системи IoT та розробку заходів захисту. В цьому розділі аналізуються типові атаки на IoT системи та пропонуються рекомендації для їх попередження.

Об’єкт дослідження є система Інтернету речей (IoT), яка включає різноманітні пристрої, підключені до мережі для збору, обробки та передачі даних.

Предметом дослідження є методи та механізми захисту IoT систем від кібератак, зокрема моделювання процесів зараження вірусами та розробка заходів для мінімізації ризиків.

Практичне значення отриманих результатів роботи можуть бути використані при створення комплексної системи, що забезпечує загальне розуміння питань захисту, методів, моделей розвитку та їх взаємозв’язків з іншими сферами, а також надійно захищає всю інформаційну інфраструктуру IoT.

1. ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ ІНТЕРНЕР РЕЧЕЙ (IoT)

1.1 Загальні відомості про Інтернет речей (IoT)

Інтернет речей (IoT) – це концепція, що охоплює систему взаємопов'язаних об'єктів, здатних збирати, обмінюватися та аналізувати дані через інтернет. В основі IoT лежить ідея об'єднання фізичних об'єктів (речей) з цифровим світом, що дозволяє їм взаємодіяти між собою та з іншими пристроями, надаючи нові можливості для автоматизації та оптимізації процесів.

Основними компонентами IoT є:

– Пристрої (речі): фізичні об'єкти, обладнані сенсорами, виконавчими механізмами та іншими компонентами, які здатні збирати та передавати дані. Це можуть бути як прості сенсори, що вимірюють температуру або вологість, так і складніші пристрої, такі як розумні годинники, автомобілі чи виробничі машини.

– Мережі: канали зв'язку, які забезпечують передачу даних між пристроями та центральними системами обробки. Це можуть бути як локальні мережі (Wi-Fi, Bluetooth), так і глобальні мережі (інтернет, мобільні мережі).

– Платформи обробки даних: програмне забезпечення та інфраструктура, яка забезпечує збір, зберігання, обробку та аналіз даних. Платформи можуть включати хмарні сервіси, бази даних, аналітичні інструменти та інше.

– Інтерфейси користувача: засоби, за допомогою яких користувачі взаємодіють із системою IoT. Це можуть бути мобільні додатки, веб-інтерфейси, голосові асистенти тощо.

Основні характеристики IoT:

– Взаємозв'язок: пристрої можуть взаємодіяти між собою без участі людини, обмінюючись даними та координуючи свої дії.

– Автономність: багато IoT систем здатні працювати автономно, приймаючи рішення на основі зібраних даних та заздалегідь заданих алгоритмів.

– Масштабованість: система IoT може легко розширюватись, включаючи нові пристрої та збільшуючи обсяг оброблюваних даних.

– Інтелектуальність: використання аналітичних алгоритмів та машинного навчання дозволяє системам IoT самонавчатись та адаптуватись до змінних умов.

Переваги впровадження IoT включають підвищення ефективності процесів, зниження витрат, покращення якості життя, створення нових бізнес-моделей та можливостей. Однак, разом з цими перевагами існують і певні виклики, такі як питання безпеки та приватності, необхідність уніфікації стандартів та забезпечення сумісності між різними пристроями та платформами.

Інтернет речей є однією з ключових концепцій сучасної інформатики, яка активно впроваджується на практиці. Ця концепція має потенціал кардинально змінити сучасне суспільство, дозволяючи багатьом процесам відбуватися автономно, без безпосереднього втручання людини [1].

Інтернет речей (IoT) представляє собою глобальну мережу об’єктів, підключених до інтернету. Ці об’єкти, здебільшого цифрові пристрої, оснащені сенсорами, датчиками та засобами передачі сигналів, здатні сприймати різноманітні сигнали з навколишнього середовища, взаємодіяти між собою, обмінюватися даними для віддаленого моніторингу, аналізу та прийняття рішень. Прикладами таких об’єктів є гаражні двері, кавоварки, телевізори, мобільні телефони, відеокамери, датчики світла та температури.

Термін "Інтернет речей" був запропонований Кевіном Ештоном у 1999 році, засновником дослідницького центру AutoID Center в Массачусетському технологічному інституті. Він передбачив, що кожен фізичний об’єкт у майбутньому матиме свій цифровий еквівалент у Інтернеті речей, тобто віртуальне представлення.

Розвиток Інтернету речей прискорився на початку 2000-х років, коли кількість підключених до інтернету пристроїв перевищила кількість користувачів інтернету. Прогнозується, що протягом наступних 5-7 років IoT проникне в усі галузі промисловості, бізнесу, охорони здоров’я та споживчих товарів.

Екосистема Інтернету речей є комплексною та взаємодіючою системою, що включає різноманітні засоби, сервіси та технології, які забезпечують розвиток та функціонування IoT. Ця екосистема об’єднує апаратне та програмне забезпечення, комунікаційні пристрої, мережеві інфраструктури, сервіси з обробки даних, рішення з безпеки та інші компоненти, необхідні для впровадження та оптимальної роботи IoT.

У межах екосистеми IoT різні пристрої можуть взаємодіяти, обмінюватися даними та спільно працювати, створюючи сприятливі умови для розвитку різноманітних застосувань та послуг. Елементи екосистеми включають сенсори, датчики, засоби зв’язку, обчислювальні пристрої, програмне забезпечення для обробки даних, рішення з безпеки, а також інфраструктуру для зберігання та обміну інформацією.

Загалом, компоненти Інтернету речей можна розділити на чотири основні категорії: сервіси (Services), апаратну частину (Hardware), набір правил (Rules) та програмну частину (Software).

Таким чином, Інтернет речей являє собою комплексну та багатоаспектну систему, що потребує інтеграції різних технологій та підходів для забезпечення її ефективного функціонування та безпеки.

1.2 Область застосування Інтернету речей (IoT)

Інтернет речей (IoT) є однією з ключових технологічних трансформацій нашого часу, впливаючи на різні сфери людського життя. Ця інноваційна концепція передбачає підключення різноманітних пристроїв до мережі, що дозволяє їм обмінюватися даними та взаємодіяти для виконання різних завдань.

У наш час Інтернет речей виявляє свій величезний потенціал у різноманітних сферах, починаючи від побутових систем автоматизації та закінчуючи високотехнологічними застосування у промисловості та медицині. Цей розділ присвячений розгляду різних аспектів використання IoT у сучасному світі.

Розумні будинки, сільське господарство, промисловий сектор, охорона здоров’я, автомобільна промисловість, електроніка та розумне місто – це лише кілька з областей, де IoT розкриває свій потенціал та надає величезний вплив на покращення ефективності, безпеки та зручності життя людей.

Розглянемо більш детально можливі сфери застосування IoT:

– Розумні термостати, кондиціонери, колонки, годівниці для тварин та інші пристрої виконують різні домашні функції. Це одна з перспективних областей використання Інтернету речей.

– Різноманітні інструменти для аналізу ґрунту, прогнозу кліматичних змін, моніторингу здоров’я тварин та відстеження місцезнаходження хворих тварин використовуються в агрокультурі.

– У промисловості застосовується термін "промисловий інтернет речей". Сенсори, програмне забезпечення та аналіз великих даних використовуються для розробки футуристичних дизайнів та точних підрахунків. Розумні машини покращують продуктивність та виправляють людські помилки в контролі якості та екологічності.

– Розумні пристрої поліпшують досвід покупців, надаючи найбажаніші товари та послуги у відповідний момент. Інтернет речей дозволяє точно налаштовувати рекламу, оптимізувати постачання та аналізувати популярні товари.

– Інтернет речей впливає на життя людей у сфері охорони здоров’я, дозволяючи лікарям надавати допомогу через інтернет. Медичні дрони інноваційно втручаються, а IoT дозволяє індивідуальний підхід до лікування.

– Розумні автомобілі ретельно прораховують маршрут та забезпечують комфорт та безпеку. IoT вже використовується в машинах з штучним інтелектом та віддаленим керуванням.

– Фітнес-браслети, розумні імплантати, GPS-пояски та інші пристрої дозволяють відстежувати здоров’я та розробляються компаніями Apple, Samsung та Motorola.

– IoT-технології, такі як розумне паркування та освітлення, можуть підвищити безпеку на дорогах та зменшити забруднення міст.

1.3 Аналіз сучасних загроз та механізмів безпеки систем IoT

Сьогодні технологія Інтернету речей (IoT) відіграє вирішальну роль у нашому повсякденному житті. Ці пристрої, від розумних термостатів до охоронних систем, забезпечують зручність та ефективність. Однак зі збільшенням їхньої популярності зростають і ризики кібератак. Це особливо стосується охоронних систем, таких як AJAX, що використовуються в контексті розумного дому. Цей розділ зосередиться на аналізі потенційних кібератак на систему AJAX, їхніх наслідках та можливих заходах запобігання.

Система AJAX є комплексним рішенням для охорони приміщень, яке використовує різні датчики та пристрої, що зв’язуються через бездротові технології. Вона включає датчики руху, відкриття дверей/вікон, а також системи пожежної та протипожежної безпеки. Управління системою здійснюється через спеціалізований мобільний додаток, який дозволяє користувачам моніторити стан свого дому в реальному часі [2].

Типи кібератак на IoT системи

– Фішинг – це атака, що використовує методи соціальної інженерії для отримання конфіденційної інформації від користувачів. У контексті системи AJAX це може включати шахрайські електронні листи або SMS, що імітують офіційні повідомлення з метою отримання паролів або доступу до облікового запису користувача. Важливо навчати користувачів правилам кібербезпеки та використовувати двофакторну аутентифікацію.

– Атаки «людина посередині» (MitM) здійснюються шляхом перехоплення комунікації між двома сторонами, дозволяючи зловмисникам зчитувати або модифікувати передані дані. У випадку AJAX це може призвести до незаконного

доступу до системи керування охороною, дозволяючи зловмисникам контролювати або вимикати систему. Захист від таких атак включає використання шифрування для всіх переданих даних та застосування безпечних протоколів зв’язку.

– DoS атаки спрямовані на перевантаження системи з метою зробити її недоступною. Для системи AJAX це може означати відключення від мережі або порушення нормального функціонування системи охорони. Заходи безпеки включають захист від DoS атак, використання резервних каналів зв’язку та стратегії балансування навантаження.

– Атаки на основі вразливостей у програмному забезпеченні використовують відомі уразливості. Для AJAX це може означати використання вразливостей у мобільному додатку або самій охоронній системі для отримання несанкціонованого доступу або крадіжки даних. Регулярне оновлення ПЗ та своєчасне застосування патчів безпеки є ключовими для захисту від таких атак.

– Встановлення шкідливого ПЗ може дати зловмисникам контроль над системою або дозволити їм красти конфіденційну інформацію. У випадку AJAX це може включати встановлення шкідливого ПЗ на мобільний пристрій користувача. Захист від таких атак включає використання антивірусного ПЗ та файрволів.

– Перебір або викрадення паролів – атаки, що включають спроби злому паролів. У контексті AJAX це може призвести до несанкціонованого доступу до системи. Використання складних паролів, обмеження спроб входу в систему та двофакторна аутентифікація є ефективними засобами захисту.

Для забезпечення безпеки системи AJAX важливо регулярно оновлювати програмне забезпечення, використовувати складні паролі та двофакторну аутентифікацію, а також забезпечувати шифрування даних. Крім того, навчання користувачів основам кібергігієни може значно знизити ризик соціальної інженерії та фішингових атак.

Таблиця 1.1 – Типи кібератак на IoT

Тип Атаки	Опис	Потенційні Наслідки	Заходи Безпеки
Фішинг	Атака, що використовує шахрайські електронні листи або повідомлення для отримання конфіденційної інформації.	Несанкціонований доступ до системи.	Навчання користувачів, двофакторна аутентифікація.
Man-in-the-Middle (MitM)	Атака, при якій зловмисник перехоплює і модифікує комунікацію між двома сторонами.	Перехоплення та модифікація даних.	Шифрування трафіку, безпечні протоколи.
Denial of Service (DoS)	Атака, спрямована на перевантаження системи з метою зробити її недоступною.	Відмова у наданні послуг.	Захист від DoS-атак, балансування навантаження.
Вразливості ПЗ	Експлуатація помилок у програмному забезпеченні.	Несанкціонований доступ, крадіжка даних.	Регулярне оновлення ПЗ, використання патчів безпеки.
Шкідливе ПЗ (Malware)	Встановлення шкідливого програмного забезпечення для крадіжки даних або контролю над системою.	Контроль над системою, крадіжка даних.	Антивірусне ПЗ, файрволи.

Розглянемо особливості технічної експлуатації вразливостей у системі IoT на прикладі охоронної системи Ajax. Системи Ajax використовують бездротові технології для комунікації між компонентами, що може створювати потенційні точки входу для кібератак.

Припустимо, що в системі Ajax було виявлено вразливість у фірмовому ПЗ, яка дозволяє зловмисникам здійснювати незаконний віддалений доступ до системи. Ця

вразливість може бути пов’язана з недоліками у протоколі шифрування, що використовується для захисту комунікацій між центральним хабом і датчиками. Зловмисник може використовувати інструменти для сканування мережі з метою ідентифікації пристроїв Ajax у локальній мережі. Методи реверс-інжинірингу застосовуються для аналізу фірмового ПЗ пристроїв, щоб виявити слабкі місця у протоколі шифрування.

На основі виявлених вразливостей розробляється експлойт, який може використовувати слабкі сторони протоколу для перехоплення або модифікації даних. Експлойт може включати методи криптографічного аналізу для розшифровки або підробки комунікаційних пакетів. Зловмисник запускає експлойт у мережі, націлюючи його на центральний хаб або індивідуальні датчики. Використовуючи експлойт, зловмисник може надсилати фальшиві сигнали до центрального хабу, імітуючи відключення або активацію датчиків. Це дозволяє зловмиснику деактивувати систему безпеки або маніпулювати її поведінкою, створюючи умови для несанкціонованого доступу. Можливе відстеження стану системи безпеки та здійснення подальших атак таким чином:

Підготовка атаки: Зловмисник визначає цільову охоронну систему Ajax у мережі Smart Home. Використовуючи методи сканування мережі, він ідентифікує активні пристрої та з’ясовує, як пристрої взаємодіють між собою [3].

Встановлення контролю: Зловмисник використовує вразливості у Wi-Fi мережі для здійснення атаки типу "Man-in-the-Middle". Він може створити фальшиву точку доступу Wi-Fi, щоб обманути пристрої системи безпеки і змусити їх підключитися через його мережу

Перехоплення та маніпуляція даними: Після встановлення контролю над мережевим з’єднанням, зловмисник може перехоплювати і змінювати дані, що передаються між пристроями системи безпеки та центральним хабом. Це може включати підробку стану сенсорів, наприклад, імітацію відключення датчиків руху або відкриття дверей.

Реалізація атаки: Зловмисник може використовувати перехоплені та змінені дані для своїх цілей, таких як несанкціонований доступ до будинку без спрацювання системи безпеки. Також можливе віддалене відключення або деактивація системи безпеки.

Заходи протидії: Щоб запобігти таким атакам, важливо використовувати сильне шифрування мережевих з'єднань. Регулярне оновлення програмного забезпечення системи безпеки допоможе усунути вразливості. Використання захищених і надійних Wi-Fi мереж зі складними паролями та шифруванням WPA3 також є важливими заходами безпеки [13].

Висновки до першого розділу

У першому розділі було визначено поняття Інтернету речей, сфери його застосування та області використання. На прикладі системи Ajax було проведено аналіз сучасних загроз і механізмів безпеки систем IoT. Для забезпечення безпеки системи AJAX важливо регулярно оновлювати програмне забезпечення, використовувати складні паролі та двофакторну аутентифікацію, а також забезпечувати шифрування даних. Крім того, навчання користувачів основам кібергігієни може значно знизити ризик соціальної інженерії та фішингових атак.

2 МЕХАНІЗМИ ВДОСКОНАЛЕННЯ ЗАХИСТУ СИСТЕМ ІНТЕРНЕТУ РЕЧЕЙ (IoT)

2.1 Опис ключових елементів системи Інтернету речей (IoT) та методів її захисту

Для розробки засобів захисту мереж IoT важливо розуміти їхню структуру та протоколи зв’язку. Ключовими аспектами є знання будови IoT систем, механізмів аутентифікації в цих мережах, наявність відкритих каналів зв’язку (як дротових, так і бездротових), а також типів використовуваних пристроїв. Кожна IoT мережа є унікальною, оскільки створюється для конкретних завдань, але всі вони мають спільні риси в структурі, стандартах зв’язку між пристроями та їх управлінні [12].

Для прикладу можна розглянути типову топологію IoT системи розумного будинку від Cisco, що зображена на рисунку 2.1.

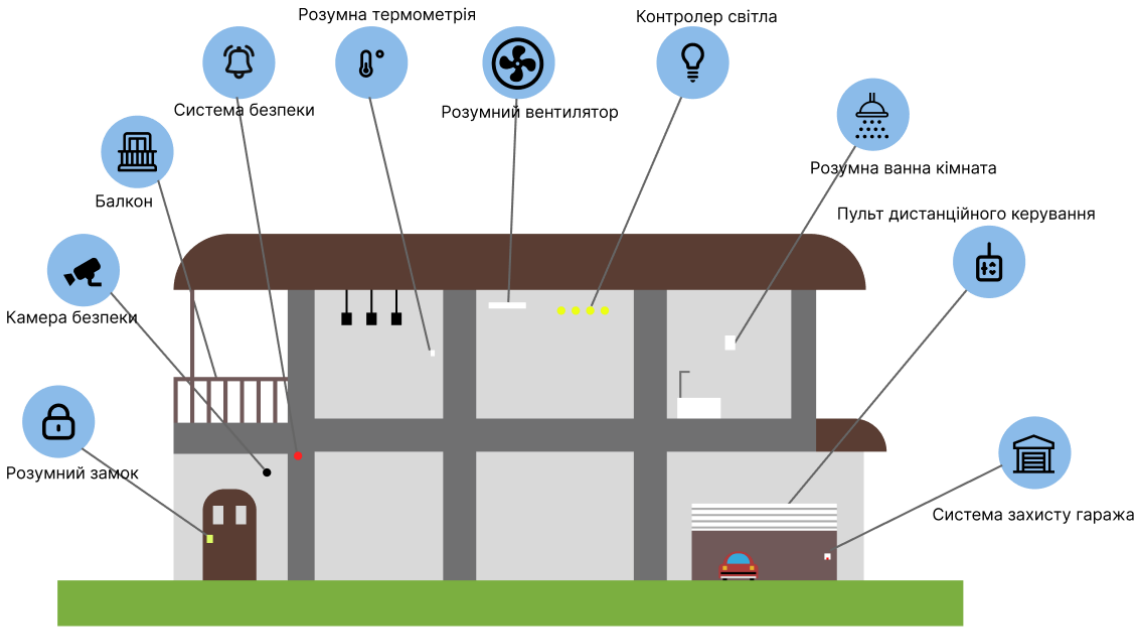

Рисунок 2.1 Типова топологія IoT розумного будинку

Виходячи з зображеного на рисунку можна зрозуміти, що система “розумний будинок” складається з таких пристроїв:

– центральний шлюз мережі

– системи кондиціонування приміщень

– системи контролю доступу до приміщень

– допоміжні системи в побутових пристроях(розумна кавоварка, пральна машина і т.д.)

– системи безпеки(пожежна, від проникнення, від витоку рідин та газів)

– пристрої керування розумним будинком(планшети, термінали, смартфони, термостати) [11].

До прикладу, на рисунку 2.2 також наведено топологію IoT мережі створеної у Cisco packet tracer.

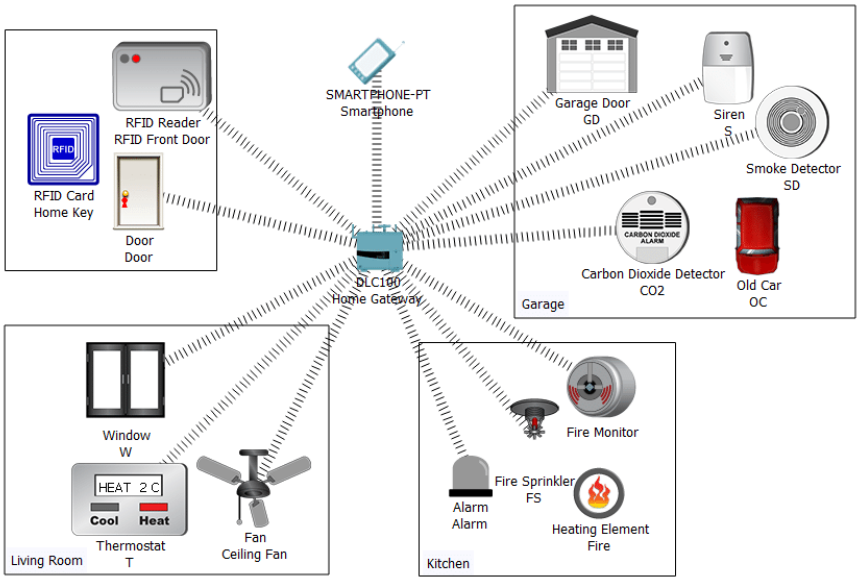

Рисунок 2.2 Топологія IoT мережі у Cisco packet tracer

Також у мережі розумного будинку може бути присутній контроль за альтернативними джерелами живлення та батареї, що накопичують отриману енергію. Сучасні IoT пристрої використовують різні протоколи зв’язку між собою та шлюзом, серед яких найпоширенішими є:

ZigBee: протокол зв’язку між IoT пристроями, що зазвичай використовується для взаємодії з датчиками та характеризується:

- низькою швидкістю;
- високою пропускною здатністю;
- низьким енергоспоживанням;
- низькою вартістю.

Bluetooth: протокол зв’язку між IoT пристроями, найчастіше використовується окремими пристроями, що працюють без шлюзу і керуються через мобільний додаток, з такими характеристиками:

- середня швидкість;
- відстань до кількох десятків метрів;
- низьке енергоспоживання.

Wi-Fi: найпоширеніший протокол зв’язку в IoT для створення систем розумного будинку, який має такі характеристики:

- висока швидкість;
- велика відстань передачі інформації;
- високе енергоспоживання.

Наразі більшість IoT пристроїв використовують Wi-Fi, оскільки вони стаціонарні та не потребують постійного живлення від батарей, проте протокол ZigBee також залишається актуальним для портативних датчиків, що використовують акумулятори або батарейні модулі. Багато IoT мереж мають доступ до зовнішньої мережі для віддаленого керування, що підвищує їх вразливість до атак [10]. Найпоширеніші типи атак на IoT мережі включають:

- Фішинг
- Атаки типу Man-in-the-Middle (MitM)
- Відмова в обслуговуванні (DoS)
- Експлуатація вразливостей програмного забезпечення
- Шкідливе програмне забезпечення (Malware)
- Атаки на паролі

Кожна з цих атак може мати конкретну мету. Наприклад, атака типу DoS може бути використана для тимчасового виведення з ладу охоронної системи, що призведе до її перевантаження і неможливості працювати в штатному режимі. Ефективною протидією є резервування каналів зв'язку та протоколи реакції на втрату моніторингу через обрив зв'язку [4].

Інший приклад атака з використанням вразливостей програмного забезпечення, яка може повністю відключити охоронну систему і видалити записи відеоспостереження та службову інформацію. Протидією є регулярне оновлення програмного забезпечення та своєчасне застосування оновлень безпеки. Також важлива захищеність внутрішньої Wi-Fi мережі, в якій знаходиться обладнання. Вона має бути захищена надійним паролем та достатнім рівнем шифрування, щоб запобігти стороннім підключенням. Корисно мати розмежовану гостьову мережу для тимчасових підключень відвідувачів без доступу до внутрішньої мережі [9].

Один з найважливіших елементів таких мереж - користувач, оскільки багато зламів відбуваються через віруси, що користувач завантажив на свій пристрій, або через слабкі паролі на керуюче ПЗ. Отже, забезпечення безпеки IoT систем - це комплекс заходів, спрямованих на унеможливлення проникнення зловмисників до системи керування, що включає захист як з боку програмного забезпечення, так і з боку користувача [6].

2.2 Розроблення математичної моделі зараження вірусом вузлів мережі IoT

Модель SIR (Susceptible-Infectious-Recovered) використовують для моделювання поширення інфекційних хвороб, проте, в силу аналогії процесів поширення вірусу в біологічних системах та поширення шкідливого програмного забезпечення в комп'ютерних мережах, дана модель може бути також застосована для оцінки стійкості та резистентності інтелектуальної мережевої інфраструктури IoT. В контексті комп'ютерних мереж можуть використовуватися аналогічні терміни:

"Схильні до інфекції" (Susceptible), "Інфіковані" (Infectious), та "Відновлені" (Recovered). Розглянемо, як модель SIR може бути застосована для аналіщу динаміки поширення вірусу в результаті кібератаки на мережу IoT [7].

1. Схильні до Зараження (S - Susceptible):

Кількість вузлів, які ще не заражені вірусом. Рівень схильних до зараження вузлів зменшується з часом пропорційно інтенсивності зараження (β) та кількості інфікованих вузлів ($I(t)$).

2. Інфіковані (I - Infectious):

Кількість вузлів, які вже заражені вірусом. Кількість інфікованих вузлів збільшується через зараження $\beta \cdot S(t) \cdot I(t)$, але зменшується через швидкість одужання або видалення вірусу $\gamma \cdot I(t)$.

3. Відновлені (R - Recovered):

Кількість вузлів, які вже відновилися від зараження та стали імунними. Кількість відновлених вузлів збільшується пропорційно швидкості відновлення (γ).

Система рівнянь, яка описує динаміку поширення зараження вузлів мережі шкідливим ПЗ

1. Диференціальне рівняння для S(t)

$$\frac{dS}{dt} = -\beta * \frac{S*I}{N} \quad (1.1)$$

2. Диференціальне рівняння для S(t)

$$\frac{dI}{dt} = -\beta * \frac{S*I}{N} - \gamma * I \quad (2.2)$$

3. Диференціальне рівняння для S(t)

$$\frac{dR}{dt} = \gamma * I \quad (3.3)$$

де S- схильні до зараження, I-інфіковані, R-відновлені

Після розрахунку за формулами (1) діаграма SIR моделі виглядає наступним чином рис.2.3:

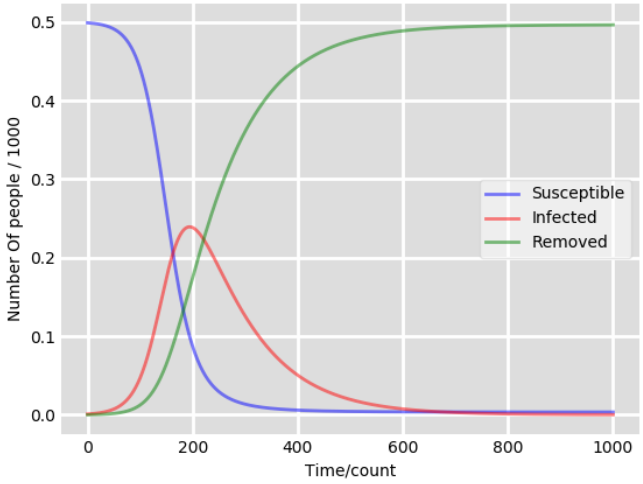

Рисунок 2.3 – Скриншот Діаграми SIR моделі

Модель SIR в контексті комп'ютерної мережі може бути використана для аналізу поширення комп'ютерних заражень, дослідження ефективності заходів безпеки та визначення параметрів, які впливають на стійкість мережі до вірусів чи інших атак.

Висновки до другого розділу

У цьому розділі описано ключові елементи системи Інтернет речей (IoT) та методи її захисту. Для розуміння функціонування системи IoT була побудована топологія «розумного» будинку в Cisco Packet Tracer. Встановлено, що сучасні IoT пристрої використовують різні протоколи зв'язку, серед яких найпоширеніші: ZigBee, Bluetooth та Wi-Fi. Також розглянуто найбільш поширені типи атак на IoT мережі: фішинг, атаки типу Man-in-the-Middle (MitM), відмову в обслуговуванні (Denial of Service, DoS), експлуатацію вразливостей програмного забезпечення, шкідливе програмне забезпечення (Malware) та атаки на паролі. Крім того, розроблено математичну модель зараження вірусом вузлів мережі IoT [8].

3 ДОСЛІДЖЕННЯ АТАК НА СИСТЕМИ ІНТЕРНЕТУ РЕЧЕЙ ТА РОЗРОБКА МЕТОДІВ ЗАХИСТУ

3.1 Дослідження атак на систему (мережу) Інтернету речей (IoT)

Метою дослідження є аналіз динаміки поширення вірусу в мережі IoT, визначення ефективних стратегій контролю, а також проведення порівняльного аналізу стійкості та резильєнтності IoT мереж, побудованих на різних архітектурах: централізованій, децентралізованій та розподіленій (Mesh) (рис. 3.1).

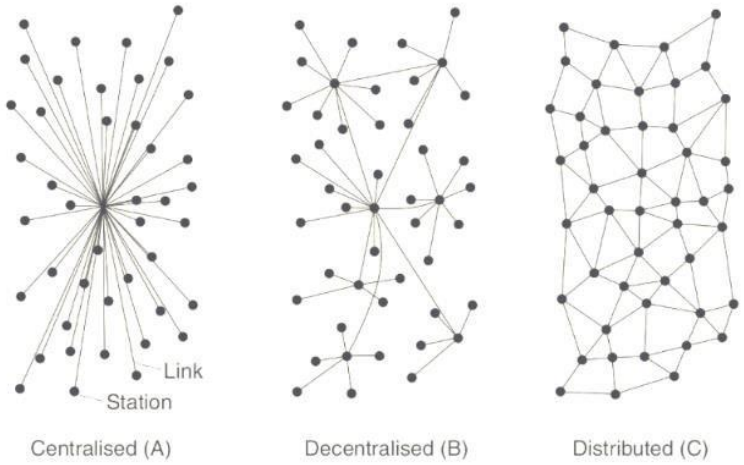

Рисунок 3.1 – Скриншот архітектури побудови IoT мереж

Середовищем моделювання обрано програмне забезпечення для мультиагентного імітаційного моделювання NetLogo. NetLogo є платформою для агентного моделювання та симуляцій, що дозволяє вченим, дослідникам та студентам створювати та вивчати моделі складних систем. Ця платформа фокусується на створенні взаємодіючих агентів, які взаємодіють у віртуальному середовищі. NetLogo часто використовується для досліджень у таких галузях, як соціальні науки, екологія, економіка та інші, де важливо вивчати емерджентні властивості систем і їхній вплив на динаміку. Вона пропонує зручний інтерфейс для моделювання, візуалізації та аналізу різноманітних взаємодій у системах [5].

Для встановлення програми необхідно відвідати офіційний сайт NetLogo та вибрати Desctop або Web-версію.

Після чого знадобиться задати параметри моделі. Параметри реалізованої моделі включають характеристики, наведені в таблиці. 3.1:

Таблиця 3.1 – Параметри моделі

Параметр	Опис	Значення
Architecture		Centralized, Decentralized, Distributed
number-of-nodes	Кількість вузлів мережі	300
average-node-degree	Середня кількість зв’язків, що виходять з кожного вузла (актуально для децентралізованої архітектури)	3
initial-outbreak-size	Початкова кількість заражених вузлів мережі IoT	3 (1% від загальної кількості)
virus-spread-chance	Ймовірність передачі вірусу від узла до узла	0.025
virus-check-frequency	Частота перевірки вірусів, тактів симуляції шт	4
recovery-chance	Ймовірність видалення вірусу у випадку його виявлення	0.002
gain-resistance-check	Ймовірність набуття імунітету (вузол стане стійким для майбутніх атак)	0.005

Проведемо експеримент для аналізу залежності параметрів стійкості та резистентності мережі IoT від рівня зв’язності мережі (для розподіленої архітектури):

Експеримент № 1: Визначення параметрів стійкості та резистентності архітектури мережі IoT. Синтезуємо мережу агентів відповідно до типу архітектури (результати синтезу в програмному середовищі представлені на рис. 3.2):

Ініціація початкових умов моделі, виконано налаштування моделі відповідно до таблиці 3.1:

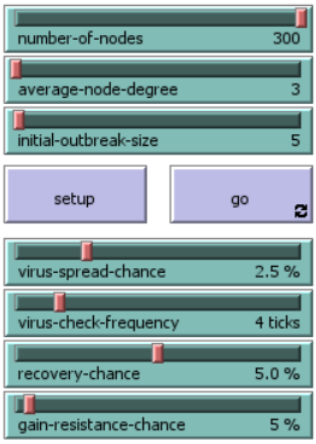

Рисунок. 3.3. – Скриншот з програми NetLogo Початкові умови симуляції

Програмний код який реалізує всі симуляції див. Додатку А

Кількість симуляцій для кожного типу моделі – 100. Синтез критеріїв порівняльного аналізу наведено у таблиці 3.2:

Таблиця 3.2. Критерії для проведення порівняльного аналізу

Критерій	Опис	Параметр моделі
Критерій скомпроментованості мережі IoT	Кількість одночасно заражених вузлів мережі >50%	Number_of_infected/ Number_of_nodes
Критерій стійкості K_s	Час за який мережа з стану скомпроментованості повертається в стан нормальної експлуатації (час стабілізації)	ticks-infected
Критерій резистивності K_R	Час за який мережу буде скпомпроментовано (час зараження)	ticks-infected-grow
Критерій зупинки симуляції	Вихід з симуляції після 2000 тактів (величину отримано феноменологічно)	ticks<2000

Далі виконаємо запуск симуляції рис.3.4:

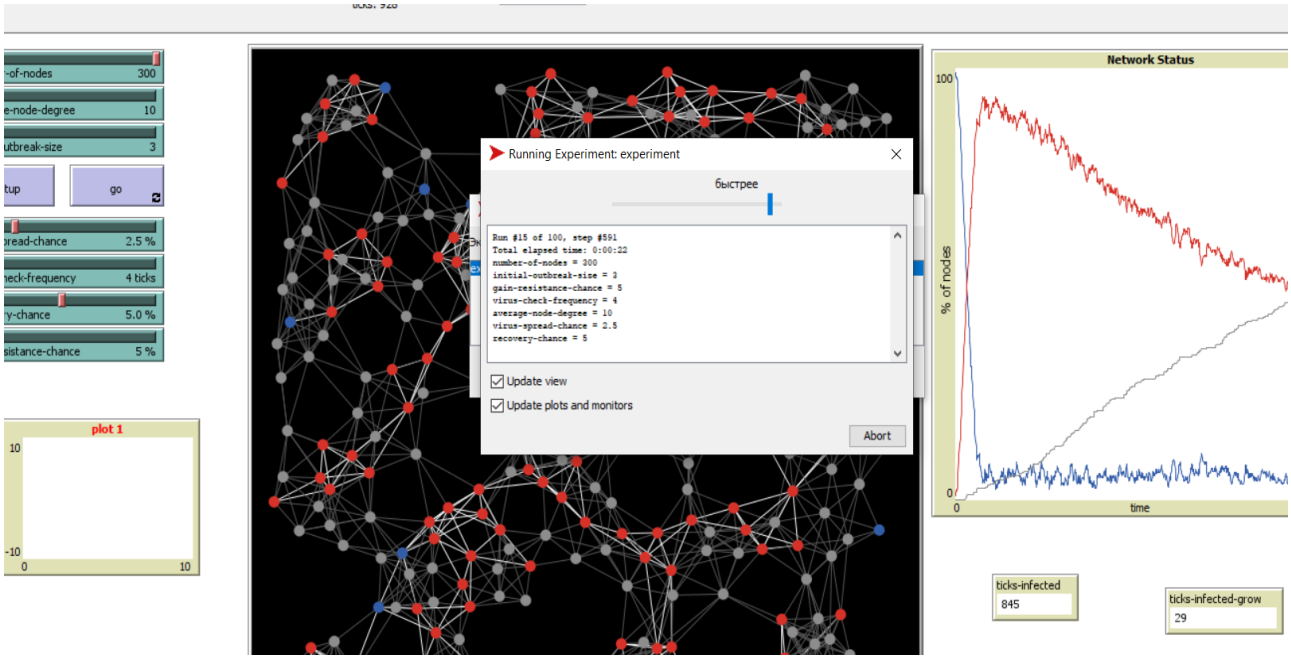

Рисунок 3.4 – Скриншот прикладів окремих симуляцій для різних архітектур (децентралізована та розподілена) IoT

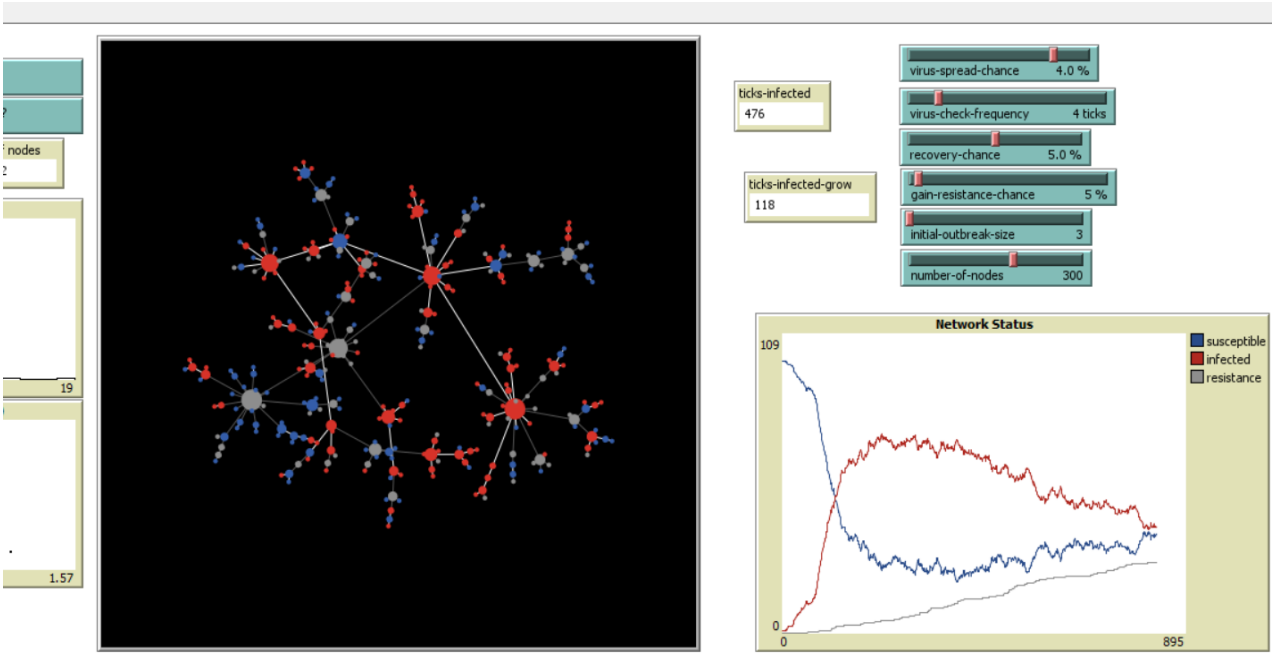

Рисунок 3.5 – Скриншот прикладів окремих симуляцій для різних архітектур (децентралізована та розподілена) IoT

Статистична обробка результатів експерименту. Візуалізація розподілу отриманих результатів експерименту рис. 3.5:

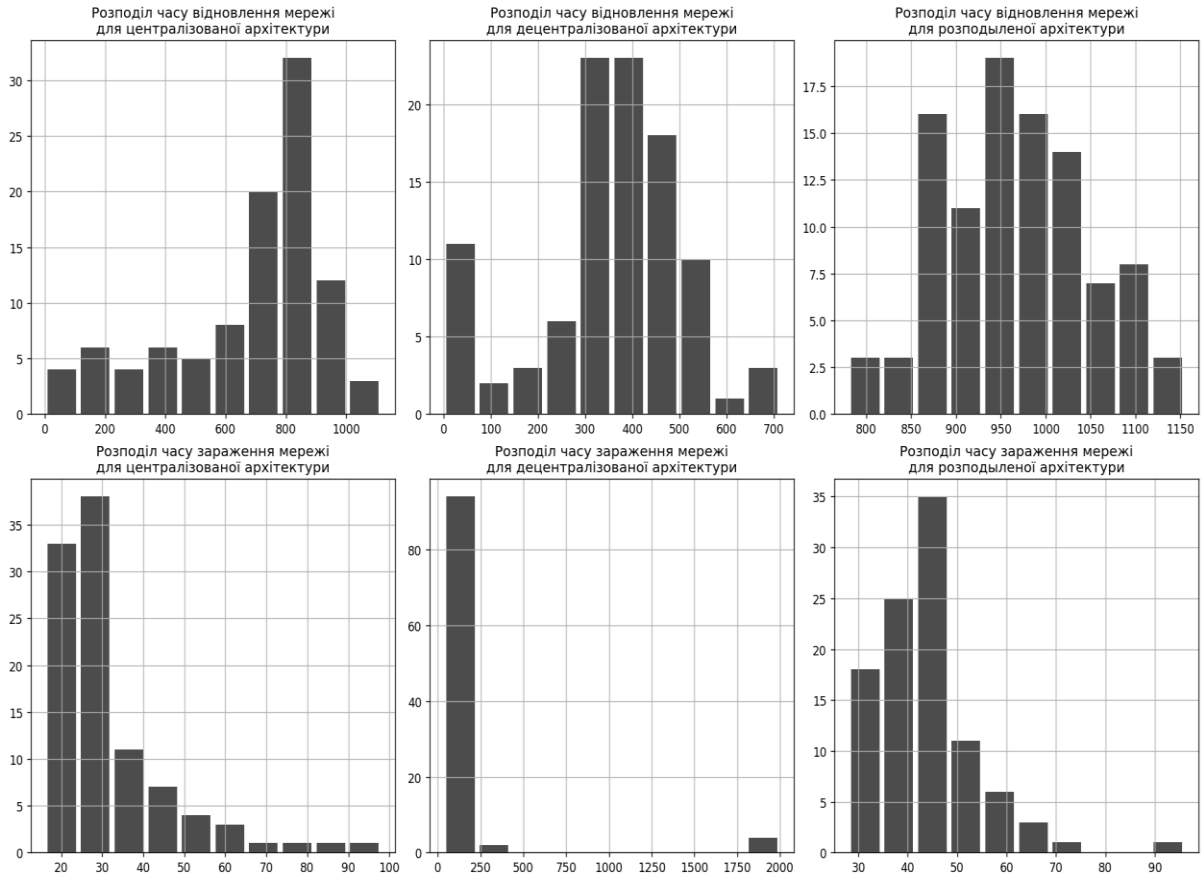

Рисунок 3.5 – Скриншот розподілу результатів експерименту для різних типів мережі IoT

Для розрахунку математичних очікувань отриманих даних вважатимемо, що дані розподілені за нормальним законом. Результати обчислень наведено в табл.3.3 Визначення математичного очікування часу зараження та часу відновлення для різних типів архітектури.

Таблиця 3.3 – Результати обчислень

Тип архітектури мережі IoT	K_S [тактів симуляції]	K_R [тактів симуляції]
Централізована	680	32
Децентралізована	354	204
Розподілена	965	43

Таким чином, за однакових умов поширення вірусу децентралізована архітектура IoT відновлюється після зараження та виявлення швидше за інші види архітектур і є більш резистентною (максимальний час для компрометації). Найменш стійкою виявилась розподілена архітектура через велику кількість надлишкових зв'язків, що підвищує ризик зараження вузла. Питання залежності стійкості та резистентності від зв'язності потребує додаткового дослідження (див. Експеримент № 2).

Експеримент № 2: Визначення залежності параметрів стійкості та резистентності мережі IoT від рівня зв'язності мережі (для розподіленої архітектури). Синтез мережі агентів розподіленої архітектури (рис. 3.2), ініціація початкових умов моделі: Модель налаштовано відповідно до табл. 1, де параметр average-node-degree (середня кількість вузлів, під'єднаних до будь-якого вузла) є змінною величиною від 1 до 20 з кроком 1.

Таблиця 3.4 – Критерії для проведення експерименту № 2

Критерій	Опис	Параметр моделі
Критерій скомпроменто-ваності мережі IoT	Кількість одночасно заражених вузлів мережі >50%	Number_of_infected/ Number_of_nodes
Критерій стійкості	Час за який мережа з стану скомпроментованості повертається в стан нормальної експлуатації	ticks-infected
Критерій резистивності	Час за який мережу буде скомпроментовано	ticks-infected-grow
Критерій зупинки симуляції	Вихід з симуляції після 2000 тактів (величину отримано феноменологічно)	ticks<2000

Після чого відбувається запуск симуляції:

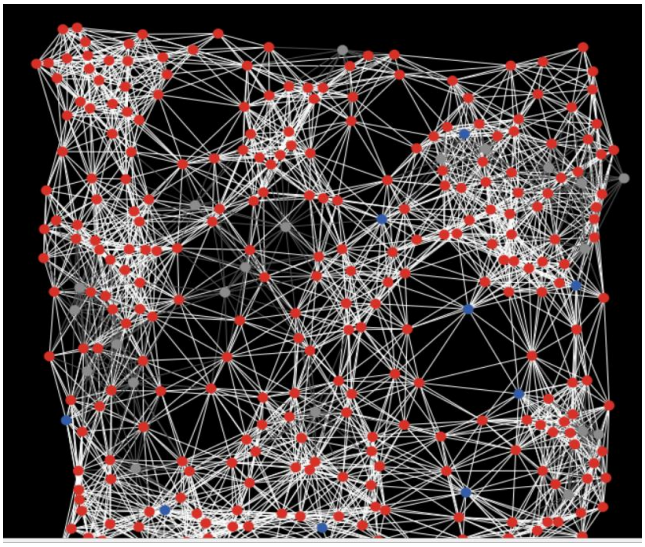

Рисунок 3.6 – Скриншот з програми NetLogo симуляції зараження IoT мережі (зв’язність мережі – 10)

Статистична обробка результатів експерименту зображена на рис.3.7.

Рисунок 3.7 - Залежність часу стабілізації мережі та часу зараження від показника зв’язності для розподіленої архітектури

Отже, стійкість і резистентність мереж IoT, побудованих за розподіленою архітектурою, критично залежать від рівня зв’язності. Оптимальним показником зв’язності за критерієм максимального часу до зараження можна вважати значення 4.

3.2 Рекомендації та подальші дослідження

Отримані результати експериментів дозволяють сформулювати рекомендації, які варто враховувати під час проєктування мереж IoT:

1. Залежно від поставлених завдань для побудови IoT, слід дотримуватись децентралізованої архітектури. Такий підхід дозволяє на фізичному рівні підвищити стійкість та резистентність мережі.

2. При побудові мереж IoT за розподіленою архітектурою необхідно враховувати показник зв’язності мережі, оскільки він значно впливає на стійкість та резистентність. Орієнтиром може слугувати оптимальне значення показника зв’язності [15].

Рекомендації для вдосконалення методів захисту.

Впровадження передових методів шифрування:

– Використовувати квантово-стійкі алгоритми шифрування для забезпечення довгострокової безпеки даних.

– Забезпечити шифрування не тільки під час передачі, але й на самому пристрої та в хмарних сховищах.

Розширена аутентифікація та авторизація:

– Впроваджувати біометричні методи аутентифікації, такі як відбитки пальців, розпізнавання обличчя або голосу.

– Використовувати контекстуальну аутентифікацію, яка враховує додаткові фактори, такі як місцезнаходження користувача або час доступу.

Покращення сегментації мережі:

– Впроваджувати Zero Trust Network Architecture (ZTNA), яка передбачає перевірку кожного доступу незалежно від місцезнаходження користувача.

– Використовувати мережеві мікросегментації для обмеження впливу потенційних атак.

Автоматизація оновлень:

– Використовувати системи автоматичного розповсюдження оновлень безпеки для пристроїв IoT.

– Розробляти механізми для забезпечення безпеки оновлень, такі як підписування коду та верифікація автентичності.

Інтеграція штучного інтелекту (AI) для виявлення загроз:

– Використовувати машинне навчання для аналізу поведінкових патернів пристроїв IoT і виявлення аномалій.

– Застосовувати AI для автоматичного реагування на виявлені загрози.

Покращення дизайну пристроїв:

– Впроваджувати Secure Boot, який гарантує запуск лише довіреного програмного забезпечення.

– Забезпечувати апаратний корінь довіри (Hardware Root of Trust) для перевірки цілісності системи.

Розширений контроль доступу:

– Використовувати динамічний контроль доступу, який враховує поведінкові фактори та контекст взаємодії.

– Впроваджувати політики Least Privilege, надаючи мінімально необхідні привілеї для виконання завдань.

Постійний моніторинг і аналіз:

– Використовувати системи Security Information and Event Management (SIEM) для централізованого збору, аналізу та кореляції даних безпеки.

– Регулярно проводити аудит та тестування на проникнення (penetration testing) для виявлення вразливостей.

Використання блокчейн-технологій:

– Впроваджувати блокчейн для забезпечення цілісності логів та транзакцій, що ускладнює їх підробку або маніпуляцію.

– Використовувати смарт-контракти для автоматизації та забезпечення безпечних взаємодій між пристроями.

Підвищення рівня обізнаності та освіти:

– Розробляти інтерактивні навчальні програми з кібербезпеки для користувачів і адміністраторів IoT.

– Організовувати регулярні тренінги з моделювання кіберзагроз для підготовки до можливих атак.

Висновки до третього розділу

У третьому розділі було проведено два експерименти для аналізу залежності параметрів стійкості та резистентності мережі IoT від рівня зв’язності мережі (для розподіленої архітектури). Встановлено, що стійкість і резистентність мереж IoT, побудованих за розподіленою архітектурою, критично залежать від показника зв’язності.

Вдосконалення методів захисту від атак на системи Інтернету речей потребує комплексного підходу, який включає технологічні інновації, покращення процесів безпеки, навчання та підвищення обізнаності користувачів. Впровадження рекомендованих заходів допоможе забезпечити надійний захист IoT-систем і мінімізувати ризики, пов’язані з кіберзагрозами [14].

ВИСНОВКИ

Під час виконання кваліфікаційної роботи було проведено пошук та аналіз різноманітної інформації про сучасні підходи і методи захисту систем Інтернету речей (IoT), що є однією з основних задач і метою даної роботи. Було досліджено нормативно-правове забезпечення у сфері захисту IoT, визначені основні загрози, які порушують основні властивості інформації в цих системах (цілісність, конфіденційність, доступність).

У період швидкого розвитку технологій та підключених пристроїв, системи Інтернету речей (IoT) стають не лише необхідністю, але й об’єктом зростаючих загроз кібербезпеки. У цьому контексті виникає потреба у глибокому дослідженні атак на системи IoT та розробці ефективних заходів захисту. У нашому дослідженні ми вивчали не лише сучасні загрози для безпеки IoT-систем, але й впроваджували інноваційні підходи до їх захисту.

У першому розділі було розглянуто поняття Інтернету речей, його сфери застосування та можливості використання. На прикладі системи Ajax було проведено аналіз сучасних загроз та заходів безпеки в контексті IoT. Для захисту системи Ajax важливо регулярно оновлювати програмне забезпечення, використовувати складні паролі та двофакторну аутентифікацію, а також застосовувати шифрування даних. Крім того, навчання користувачів основам кібергігієни може суттєво зменшити ризик соціальної інженерії та фішингових атак.

У другому розділі описано ключові елементи системи Інтернету речей та методи її захисту. Для розуміння роботи IoT-системи було створено топологію «розумного» будинку в Cisco Packet Tracer. Визначено, що сучасні IoT пристрої використовують різні протоколи, серед яких найпоширеніші: ZigBee, BlueTooth, Wi-Fi. Також проаналізовано найпоширеніші типи атак на IoT мережі, такі як фішинг, атаки типу "людина посередині" (MitM), відмова в обслуговуванні (Denial of Service, DoS),

експлуатація вразливостей ПЗ, шкідливе ПЗ (Malware) та атаки на паролі. Крім того, було розроблено математичну модель зараження вірусом вузлів мережі IoT.

У третьому розділі проведено дослідження у формі двох експериментів на імітаційній моделі IoT у мультиагентному середовищі NetLogo. Визначено, що стійкість і резистентність мереж IoT, побудованих за розподіленою архітектурою, критично залежать від показника зв'язності. Отримані результати лягли в основу практичних рекомендацій щодо проєктування IoT-мереж для забезпечення адекватного рівня захищеності з урахуванням показників стійкості та резистентності.

Захист систем IoT розглядається як комплексна система, що забезпечує загальне розуміння питань захисту, методів, моделей розвитку та їх взаємозв'язків з іншими сферами. Галузі знань у сфері захисту IoT формуються і розвиваються на основі практичного досвіду.

На сьогоднішній день захист окремих елементів IoT поступово втрачає свою актуальність. Натомість пріоритетним є створення комплексної системи, яка надійно захищає всю інформаційну інфраструктуру IoT. Впроваджуючи систему безпеки, необхідно враховувати не тільки характеристики окремих елементів, але і їх взаємодію один з одним, що означає існування невід'ємних характеристик взаємопов'язаних елементів.

Завдання захисту всіх інформаційних ресурсів IoT є зрозумілим, але його реалізація потребує значних ресурсів. Зі збільшенням вимог до системи інформаційної безпеки IoT, ця задача стає більш складною і комплексною. Все більше джерел інформації використовують концепцію "системного підходу" при створенні систем інформаційної безпеки IoT. Системний підхід означає, що процес створення і підтримки системи захисту IoT є постійним і охоплює всі етапи її розвитку: від проєктування до введення в дію, від експлуатації до припинення функціонування. Всі засоби, методи та заходи захисту інформації інтегруються в єдиний комплексний механізм.

На жаль, необхідність системного підходу до забезпечення безпеки IoT ще не завжди визнається власниками таких систем. Отже, для оцінки захищеності системи IoT пропонується наступний алгоритм дій:

1. На першому етапі складається перелік загроз з точки зору забезпечення інформаційної безпеки IoT. Визначається ймовірність виникнення загроз та їх знешкодження системою захисту. Складається кошторис інформаційної системи IoT.

2. На другому етапі встановлюються обмеження на вартість системи захисту IoT. Визначається мінімально необхідний рівень захисту для системи IoT.

3. На третьому етапі за допомогою математичних формул оцінюється загальний рівень захищеності системи IoT.

4. На четвертому етапі з розглянутих та оцінених альтернатив обирається та, що максимально відповідає нормам та вимогам захисту.

В практичній діяльності рівень захисту визначається як відношення ризику захищеної системи IoT до ризику незахищеної системи. Такий підхід дозволяє точніше описати інформаційні ресурси IoT через їх вразливості, визначити критичність ресурсів, скласти перелік ризиків.

Теорія захисту інформації в системах IoT повинна включати такі моменти:

1. Надання повної та адекватної інформації про походження, природу та розвиток проблем захисту IoT.

2. Відображення структури і змісту зв’язку з суміжними галузями знань.

3. Накопичення досвіду попередніх досліджень, розробок і практичних рішень проблем захисту IoT.

4. Визначення найбільш ефективних напрямків вирішення основних проблем захисту IoT.

5. Формування теорії наукового захисту інформації в IoT та практичного напряму розвитку.

Отже, актуальним є розширення комплексу методів та підходів класичної теорії систем, що дозволить моделювати процеси, які залежать від непередбачуваних

факторів. Найбільш підходящий метод можна визначити на основі нечітких множин, лінгвістичних змінних, неформальної оцінки та пошуку найкращого рішення.

ПЕРЕЛІК ПОСИЛАНЬ

1. Molodetska, K., & Tymonin, Y. (2020). Mathematical modeling covid-19 wave structure of distribution. In CEUR Workshop Proc. (pp. 292-301).
2. Ісмайлов К. Ю. Аналіз сучасних загроз та механізмів безпеки IoT. Science of XXI century: development, main theories and achievements. V Міжнародна науково-теоретична конференція, 2023. м. Гельсінкі, Фінляндська Республіка.
3. Будова IoT URL: http://surl.li/tzwkv
4. Linux Rabbit загроза атаки на IoT пристрої: URL: https://attack.mitre.org/software/S0362/
5. Програма для моделювання вірусної атаки в мережі: URL: http://surl.li/tzwkp
6. Enabling privacy and security in Cloud of Things: Architecture, applications, security & privacy challenges URL: http://surl.li/tzwkm
7. Flynn D. IoT considerations — cloud services — IaaS, PaaS, SaaS, build your own URL: http://surl.li/tzwkk
8. What Is Platform-as-a-Service (PaaS)? URL: http://surl.li/tzwkh
9. Jaimunk, J. Privacy-Preserving Cloud-IoT Architecture (Abstract). 2019 IEEE/ACM 6th International Conference on Mobile Software Engineering and Systems (MOBILESoft), 2019.
10. “How the internet of things can help create a better new normal” – URL: http://surl.li/tzwkd
11. “IoT Architecture: the Pathway from Physical Signals to Business Decisions” – URL: http://surl.li/tzwjd
12. “Internet of Things: security and privacy implications” – URL : http://surl.li/tzwjn
13. “Privacy” – URL: http://surl.li/tzwjt
14. “RFID and Inclusive Model for the Internet of Things” – URL: http://surl.li/tzwjy
15. “IoT Privacy and Security: Challenges and Solutions” ” –URL: http://surl.li/tzwkb

ДОДАТКИ

Додаток А: Програмний код який реалізує симуляції

```
turtles-own
[
  infected?
  resistant?
  virus-check-timer
]

to setup
  clear-all
  setup-nodes
  setup-spatially-clustered-network
  ask n-of initial-outbreak-size turtles
    [ become-infected ]
  ask links [ set color white ]
  reset-ticks
end

to setup-nodes
  set-default-shape turtles "circle"
  create-turtles number-of-nodes
  [
    ; for visual reasons, we don't put any nodes *too* close to the
edges
    setxy (random-xcor * 0.95) (random-ycor * 0.95)
    become-susceptible
    set virus-check-timer random virus-check-frequency
  ]
end

to setup-spatially-clustered-network
  let num-links (average-node-degree * number-of-nodes) / 2
  while [count links < num-links ]
  [
    ask one-of turtles
    [
      let choice (min-one-of (other turtles with [not link-neighbor?
myself])
                   [distance myself])
      if choice != nobody [ create-link-with choice ]
    ]
  ]
```

```
  ; make the network look a little prettier
  repeat 10
  [
    layout-spring turtles links 0.3 (world-width / (sqrt number-of-
nodes)) 1
  ]
end

to go
  if all? turtles [not infected?]
    [ stop ]
  ask turtles
  [
     set virus-check-timer virus-check-timer + 1
     if virus-check-timer >= virus-check-frequency
       [ set virus-check-timer 0 ]
  ]
  spread-virus
  do-virus-checks
  tick
end

to become-infected  ;; turtle procedure
  set infected? true
  set resistant? false
  set color red
end

to become-susceptible  ;; turtle procedure
  set infected? false
  set resistant? false
  set color blue
end

to become-resistant  ;; turtle procedure
  set infected? false
  set resistant? true
  set color gray
  ask my-links [ set color gray - 2 ]
end

to spread-virus
  ask turtles with [infected?]
    [ ask link-neighbors with [not resistant?]
        [ if random-float 100 < virus-spread-chance
            [ become-infected ] ] ]
```

```
end

to do-virus-checks
  ask turtles with [infected? and virus-check-timer = 0]
  [
    if random 100 < recovery-chance
    [
      ifelse random 100 < gain-resistance-chance
        [ become-resistant ]
        [ become-susceptible ]
    ]
  ]
end
```