МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ПОЛІСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій,
обліку та фінансів

Кафедра комп'ютерних технологій
і моделювання систем

Кваліфікаційна робота
на правах рукопису

ІСМАЙЛОВ КАРЕН ЮРІЙОВИЧ

УДК 004.056:004.6

КВАЛІФІКАЦІЙНА РОБОТА

ДОСЛІДЖЕННЯ АТАК НА СИСТЕМИ ІНТЕРНЕТУ РЕЧЕЙ(IOT) І РОЗРОБКА ЗАХОДІВ ЗАХИСТУ

Спеціальність – 125 «Кібербезпека»

Галузь знань – 12 «Інформаційні технології»

Подається на здобуття освітнього ступеня магістр

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

_____ Карен ІСМАЙЛОВ

Керівник роботи:
Веретюк Сергій Михайлович,
кандидат технічних наук

Житомир-2023

АНОТАЦІЯ

Ісмайлов К. Ю. Дослідження атак на системи Інтернету речей(IoT) і розробка заходів захисту. – Кваліфікаційна робота на правах рукопису.

Кваліфікаційна робота на здобуття освітнього ступеня магістр за спеціальністю 125 «Кібербезпека» галузі знань 12 «Інформаційні технології». – Поліський національний університет, Житомир, 2023.

Дана робота присвячена дослідженню атак, спрямованих на системи Інтернету речей (IoT), та розробці ефективних заходів захисту. У першому розділі проведено аналіз сучасного стану безпеки IoT-систем, ідентифікація загроз та типів атак, що можуть впливати на їх працездатність та конфіденційність. У другому розділі акцент робиться на дослідження механізмів покращення елементів IoT систем. В заключному розділі відбувається проведення експерементів щодо вразливостей системи Інтернету речей та пропонуються заходи, спрямованих на підвищення стійкості та безпеки.

Ключові слова: Інтернет речей, захист, механізми, мережа, технологія.

SUMMARY

Ismailov K. Yu. Research on Attacks on Internet of Things (IoT) Systems and Development of Protection Measures. – Qualification work on the rights of a manuscript. Qualification work for the educational degree of Master in the specialty 125 "Cybersecurity," field of study 12 "Information Technologies." – Polissia National University, Zhytomyr, 2023.

This work is dedicated to the investigation of attacks targeting Internet of Things (IoT) systems and the development of effective protection measures. The first section analyzes the current state of security in IoT systems, identifying threats and types of attacks that can impact their functionality and confidentiality. The second section focuses on researching mechanisms to enhance elements of IoT systems. In the concluding section, experiments are conducted on vulnerabilities in the Internet of Things system, and measures aimed at improving resilience and security are proposed.

Keywords: Internet of Things, protection, mechanisms, network, technology.

ЗМІСТ

ВСТУП

В сучасному інформаційному суспільстві, де велика кількість пристроїв пов'язана через Інтернет у єдину мережу, питання кібербезпеки стає надзвичайно актуальним. Зокрема, системи Інтернету речей (IoT) виявляються особливо вразливими перед різноманітними загрозами та атаками. Ця кваліфікаційна робота присвячена дослідженню атак на системи Інтернету речей та розробці ефективних заходів захисту.

Актуальність теми дослідження. Інтернет речей, як важлива галузь сучасних технологій, надає безліч можливостей для покращення ефективності та комфорту в різних сферах життя. Проте разом із цим виникає ряд серйозних проблем щодо безпеки цих систем. Зростання кількості підключених пристроїв також збільшує ризик атак і порушення конфіденційності, цілісності та доступності даних.

Метою роботи є проведення комплексного дослідження атак на системи Інтернету речей та розробка надійних заходів захисту.

Предметом дослідження є виступають загрози, які можуть впливати на пристрої та мережі IoT, а також ефективні методи захисту, спрямовані на забезпечення безпеки та стабільності функціонування цих систем.

Об’єктом дослідження є системи Інтернету речей (IoT) та аспекти їх кібербезпеки.

Методологія дослідження. Для досягнення поставленої мети та завдань у роботі використано загальнонаукові та економічні **методи:** системно – структурного аналізу, аналізу і синтезу, наукового узагальнення, статистичного, порівняльного аналізу, аналогій та моделювання.

Перелік публікацій автора за темою дослідження:

1.Ісмайлов К. Ю. Вразливості системи IoT. *Безпека, технології, інновації: нові горизонти* : міжфакультетська науково-практична інтернет-конференція здобувачів вищої освіти і молодих вчених, 15 листопада 2023 р. м. Житомир.

2. Ісмайлов К. Ю. Опис ключових елементів системи Інтернету речей(IoT) та методів її захисту. *Сучасні аспекти та перспективні напрямки розвитку науки*: VI Міжнародна студентська конференція, 2023. м. Харків.

3. 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.

Наукова новизна та практичне значення отриманих результатів. Дослідження атак на системи Інтернету речей (IoT) та розробка заходів захисту мають велике значення як для академічного, так і для практичного напрямків в галузі кібербезпеки. Наукова новизна дослідження полягає в розширенні знань про сучасні загрози та атаки, спрямовані на IoT-системи. Розгляд різноманітних типів атак дозволяє визначити їхні особливості та виявити потенційні ризики для підключених пристроїв.

Структура та обсяг роботи. Кваліфікаційна робота складається з анотації, вступу, трьох розділів, висновків та списку використаних джерел. Загальний обсяг кваліфікаційної роботи становить 26 сторінок та містить 3 таблиці і 5 рисунків.

РОЗДІЛ 1. ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ ІНТЕРНЕТ РЕЧЕЙ(IoT)

1.1 Загальні відомості про Інтернет речей(IoT)

«Ідея Інтернету речей є однією з провідних концепцій у сучасній інформатиці та вже активно реалізується на практиці. Ця концепція має потенціал серйозно вплинути на сучасне суспільство, дозволяючи багатьом процесам відбуватися автономно, без прямого втручання людини.

Інтернет речей, або скорочено IoT, представляє собою глобальну мережу об'єктів, які підключені до Інтернету. Ці об'єкти в основному є цифровими пристроями, обладнаними сенсорами, датчиками та засобами передавання сигналів. Вони можуть сприймати різноманітні сигнали з навколишнього середовища, взаємодіяти між собою, обмінюватися даними для віддаленого моніторингу, аналізу та прийняття рішень. Прикладами можуть служити гаражні двері, кавоварки, телевізори, мобільні телефони, відеокамери, датчики світла та температури тощо.

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

Розвиток Інтернету речей набув активного ходу на початку 2000-х років, коли кількість підключених до Інтернету пристроїв перевищила кількість користувачів Інтернету, що свідчить про те, що Інтернет речей вийшов за рамки

«Прогнозується, що протягом наступних 5-7 років Інтернет речей проникне в усі галузі промисловості, бізнесу, охорони здоров'я та споживчих товарів масштабу Інтернету для людей»[6].

Також існує екосистема Інтернету речей представляє собою комплексну і взаємодіючу систему, що включає в себе різноманітні засоби, сервіси та технології, які сприяють розвитку та функціонуванню Інтернету речей (IoT).

Ця екосистема об'єднує апаратне та програмне забезпечення, комунікаційні пристрої, мережеві інфраструктури, сервіси з обробки даних, безпеку та інші компоненти, необхідні для впровадження та оптимальної функціональності Інтернету речей.

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

Така екосистема створює основу для розвитку і впровадження різноманітних рішень в галузях промисловості, бізнесу, охорони здоров'я та інших сферах, де Інтернет речей може бути застосований для оптимізації процесів та покращення ефективності.

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

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

Наразі технологія Internet of Things (IoT) відіграє ключову роль у повсякденному житті. Ці пристрої, від розумних термостатів до охоронних систем, забезпечують зручність та ефективність. Однак, зі збільшенням їхньої популярності, зростає і ризик кібератак. Особливо це актуально для охоронних систем, таких як AJAX, що використовуються в контексті Smart Home. Цей розділ зосередиться на аналізі потенційних кібератак на систему AJAX, їхніх наслідках та можливих заходах запобігання.

Система AJAX представляє собою комплексне рішення для охорони приміщень, використовуючи різні датчики та пристрої, що зв'язуються через бездротові технології. Вона включає в себе датчики руху, відкриття дверей/вікон, а також системи пожежної та протипожежної безпеки. Управління системою відбувається через спеціалізоване мобільний додаток, що дозволяє користувачам моніторити стан свого дому в реальному часі.

Типи Кібератак на IoT Системи:

Фішинг - це вид атаки, що використовує інженерні методи соціального маніпулювання 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. На важливість навчання користувачів правилам кібербезпеки та використання двофакторної аутентифікації не можна недооцінювати.

MitM атаки здійснюються шляхом перехоплення комунікації між двома сторонами, дозволяючи зловмисникам зчитувати або модифікувати передані дані. В контексті AJAX, це може призвести до незаконного доступу до системи

керування охороною, дозволяючи зловмисникам контролювати або вимкнути систему. Захист від таких атак включає в себе 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 перешкоду в нормальному функціонуванні системи охорони. Заходи безпеки включають захист від DoS атак, використання резервних каналів зв'язку та стратегій балансування навантаження.

Цей тип атак включає в себе використання відомих вразливостей у програмному забезпеченні. Для AJAX це може означати використання вразливостей в мобільному додатку або в самій охоронній системі для отримання несанкціонованого доступу або крадіжки даних. Регулярне оновлення ПЗ та своєчасне використання 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 з AJAX, це може включати в себе встановлення шкідливого ПЗ на мобільний пристрій користувача. Захист від таких атак включає в себе використання антивірусного ПЗ та файрволів.

Ці атаки включають в себе спроби перебору або викрадення паролів. В 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 експлуатацію 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, в системі Ajax було виявлено вразливість у фірмовому ПЗ, яка дозволяє зловмисникам виконувати незаконний віддалений доступ до

системи. Вразливість може бути пов'язана з недоліками у протоколі шифрування, що використовується для захисту комунікацій між центральним хабом і датчиками. Зловмисник використовує інструменти сканування мережі для ідентифікації пристроїв Ajax у місцевій мережі. Застосовуються методи реверс-інжинірингу для аналізу фірмового ПЗ пристроїв, виявлення слабких місць у протоколі шифрування.

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

1. Підготовка атаки:

Зловмисник визначає цільову охоронну систему Ajax у мережі Smart Home. Використовуючи методи сканування мережі, він ідентифікує активні пристрої та з'ясовує, яким чином пристрої комунікують між собою.

2. Встановлення контролю:

Зловмисник використовує вразливості у Wi-Fi мережі для створення атаки типу "Man-in-the-Middle". Він може використати фальшиву точку доступу Wi-Fi, щоб ввести в оману пристрої системи безпеки і змусити їх підключитися через його мережу.

3. Перехоплення та маніпуляція даними:

Після встановлення контролю над мережевим з'єднанням, зловмисник може перехоплювати і модифікувати дані, що передаються між пристроями системи безпеки та центральним хабом. Це може включати фальсифікацію

стану сенсорів, наприклад, імітування відключення датчиків руху або відкриття дверей.

4. Реалізація атаки:

Зловмисник може використовувати ці перехоплені та змінені дані для власних цілей, таких як несанкціонований доступ до будинку без спрацювання системи безпеки. Також можливе віддалене відключення системи безпеки або її дезактивація.

5. Заходи протидії:

Щоб запобігти таким атакам, важливо використовувати сильне шифрування мережевих з'єднань. Регулярне оновлення програмного забезпечення системи безпеки для усунення вразливостей. Використання захищених і надійних Wi-Fi мереж з сильними паролями і WPA3 шифруванням.

Висновки до розділу 1

В першому розділі було визначено, що таке Інтернет речей, область його застосування та сфери використання. На основі системи Ajax був проведений аналіз сучасних загроз та 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.

РОЗДІЛ 2. МЕХАНІЗМИ ПОКРАЩЕННЯ ЕЛЕМЕНТІВ СИСТЕМ ЗАХИСТУ ІНТЕРНЕТУ РЕЧЕЙ (IOT)

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

Для розробки засобів захисту мереж IoT, важливо розуміти їх будову та протоколи зв'язку. Ключовими аспектами є розуміння будови IoT систем, розуміння аутентифікаційних механізмів в цих мережах, наявність відкритих каналів зв'язку, як дротових так і бездротових, типи пристроїв, що використовуються і т.д. Кожна IoT мережа є по своєму унікальною, оскільки створюється під конкретні задачі, але всі вони містять спільні риси у будові, стандартах зв'язку між пристроями та їх керуванням.

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

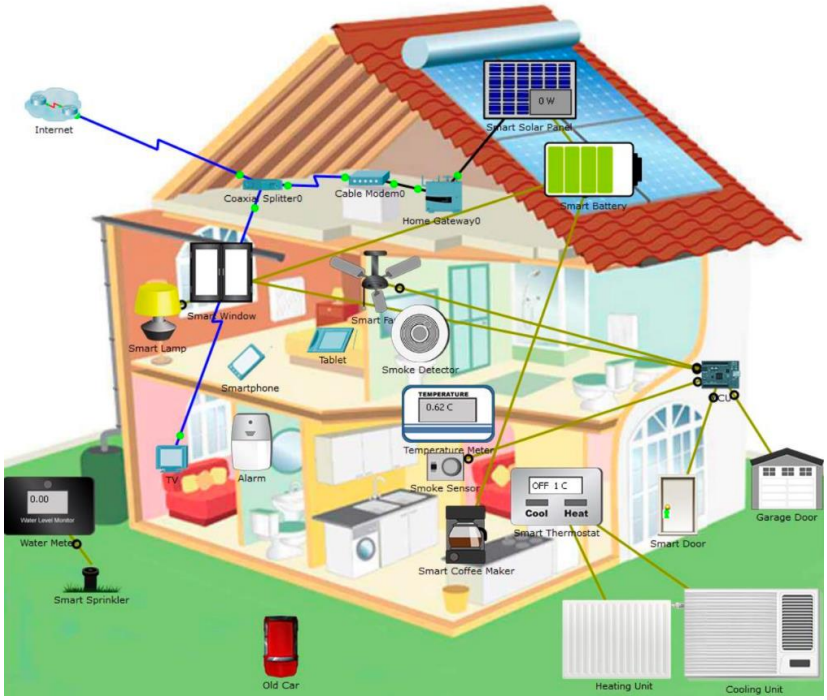


Рисунок 2.1 - Типова топологія IoT розумного будинку

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)

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

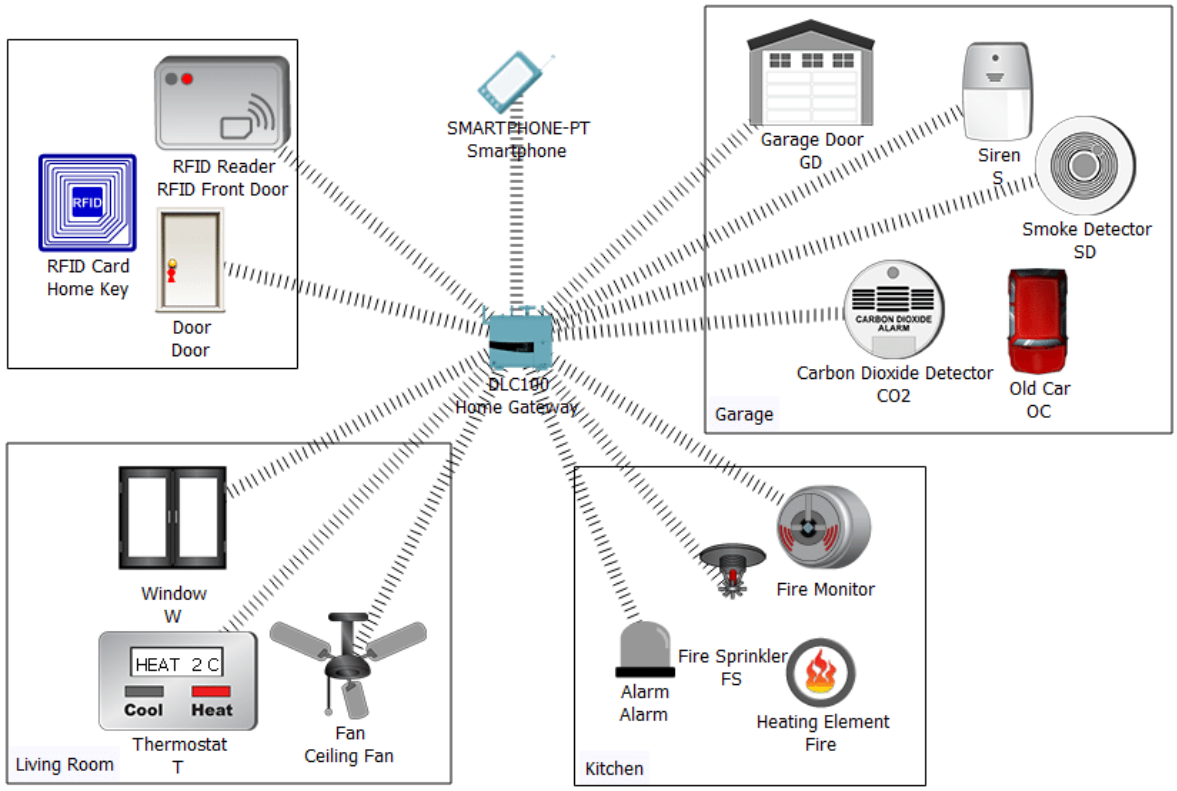


Рисунок 2.2 - Топологія IoT мережі у Cisco packet tracer

Також з додаткового в мережі розумного будинку може бути присутній контроль за альтернативними джерелами живлення та батареями, що накопичують отриману енергію.

Сучасні IoT пристрої використовують різні протоколи зв'язку між собою та шлюзом, найпоширеніші з них це:

ZigBee - протокол зв'язку між IoT пристроями, який частіше за все використовується для зв'язку з давачами та має такі характеристики:

- низька швидкість;

- висока пропускна здатність;
- низьке енергоспоживання;
- низька вартість.

BlueTooth - протокол зв’язку між IoT пристроями, протокол, який найчастіше використовують поодинокі пристрої, що працюють без шлюзу та керуються власним мобільним додатком, до характеристик можна віднести:

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

Wi-Fi - найпоширеніший на сьогодні протокол зв’язку що використовують в IoT для побудови систем розумного будинку, має такі характеристики:

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

На сьогодні, більшість IoT пристроїв використовують протокол Wi-Fi, так як вони є стаціонарними та не використовують елементи живлення на постійній основі, але ZigBee протокол також не втратив своєї актуальності та використовується у портативних давачах, що не підключені до живлення, а використовують акумулятори, або батарейні модулі.

Також більшість IoT мереж мають доступ до зовнішньої мережі, для можливості віддаленого керування ними, що робить їх більш вразливими до атак. На сьогодні існують такі найрозповсюдженіші типи атак на IoT мережі:

1. Фішинг
2. MitM атаки
3. Denial of Service (DoS)
4. Експлуатація Вразливостей ПЗ
5. Шкідливе ПЗ (Malware)
6. Атаки на Паролі

Кожна з наведених атак може нести за собою певну ціль, якщо брати до прикладу атаку типу DoS, то її можна використати для тимчасового обмеження роботи охоронної системи, в такому випадку, система може бути перевантажена і не працюватиме в штатному режимі. Тобто давачі побачать проникнення та ввімкне режим тривоги, але власник та охоронна компанія не отримають сповіщення про цю подію. ефективною протидією цьому є резервування каналів зв'язку та протоколи реакції, коли система випала з моніторингу через обрив зв'язку.

Також не менш ефективною атакою на охоронну систему є атака з використанням вразливостей програмного забезпечення. Знаючи про таку вразливість можна повністю відключити охоронну систему і в подальшому видалити записи систем відеоспостереження та службову інформацію, що ще більш ускладнить пошук зловмисника. Ефективним способом протидії цьому є використання охоронних систем, які отримують оновлення безпеки від виробника та своєчасне їх оновлення.

Не мало важливим є і внутрішня Wi-Fi мережа, в якій знаходиться обладнання. Вона має бути захищеною надійним паролем та шифруванням на достатньому рівні для унеможливлення сторонніх підключень з метою заволодіння доступом над мережею IoT. Важливим у такому випадку є наявність розмежованої гостьової мережі, яка слугуватиме для тимчасових підключень відвідувачів та не матиме доступу до внутрішньої мережі

Одним з найважливіших елементів таких мереж є користувач, оскільки існує досить багато випадків, коли такі мережі зламують вірусом, який користувач завантажив на свій пристрій, наприклад через електронний лист, або просто встановив простий пароль на керуюче ПЗ.

У підсумку можна сказати, що забезпечення безпеки IoT систем, це комплекс мір захисту спрямованих на те, щоб унеможливити проникнення зловмисників до системи керування, що включає в себе захист як зі сторони програмного забезпечення таких систем так і зі сторони користувача.

2.2. Розроблення математичної моделі зараження вірусом вузлів мережі IoT

Модель SIR (Susceptible-Infectious-Recovered) використовують для моделювання поширення інфекційних хвороб [1], 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.

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):**
$$\frac{dS}{dt} = -\beta \cdot \frac{S \cdot I}{N}$$
2. **Диференціальне рівняння для I(t):**
$$\frac{dI}{dt} = \beta \cdot \frac{S \cdot I}{N} - \gamma \cdot I$$
3. **Диференціальне рівняння для R(t):**
$$\frac{dR}{dt} = \gamma \cdot I$$

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

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

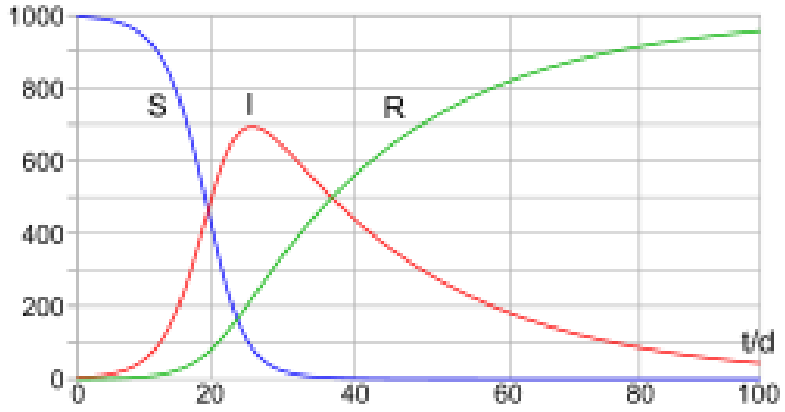


Рисунок 2.3 Діаграма SIR моделі

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 розділу 2

В даному розділі проведено опис ключових елементів системи Інтернет речей та методів її захисту. Для розуміння як працює система IoT була побудована топологія «розумного» будинку в Cisco Packet Tracer. Визначено, що сучасні IoT пристрої використовують різні протоколи. Найпоширеніші з них це: ZigBee, BlueTooth, WI-FI. Також найрозповсюдженіші типи атак на IoT мережі: фішинг, MitM атаки, Denial of Service (DoS), експлуатація вразливостей ПЗ, шкідливе ПЗ (Malware), атаки на паролі. Крім того, було розроблено математичну модель зараження вірусом вузлів мережі IoT.

3 ДОСЛІДЖЕННЯ АТАК НА СИСТЕМИ ІНТЕРНЕТУ РЕЧЕЙ І РОЗРОБКА ЗАХОДІВ 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, проведення порівняльного аналізу стійкості та резильєнтності IoT мереж, які побудовані на основі різних архітектур (централізована, децентралізована, розподілена (Mesh) рис.3.1.

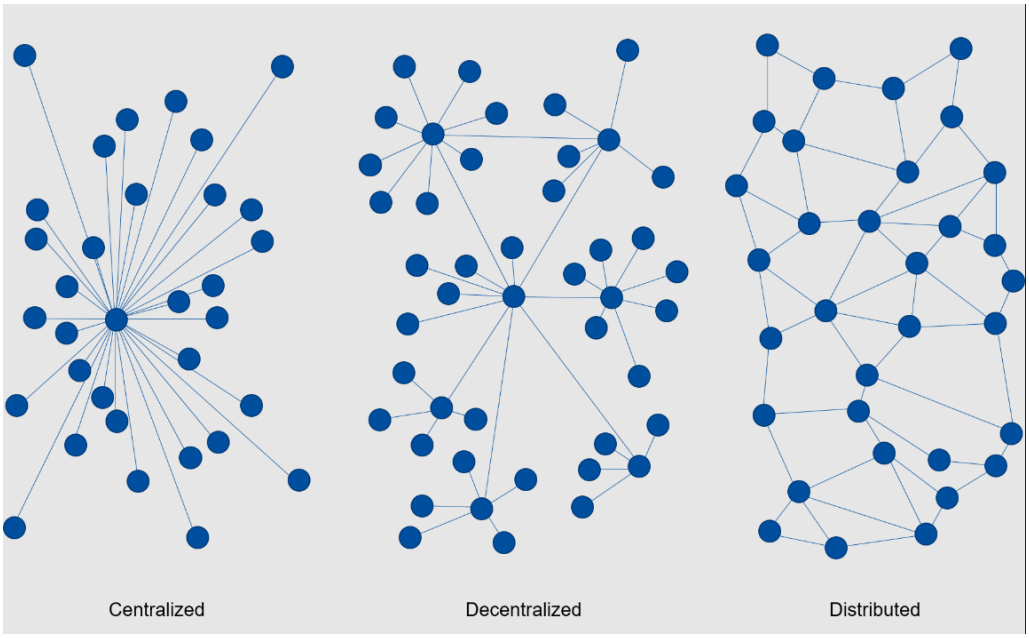


Рисунок 3.1 Архітектури побудови IoT мереж

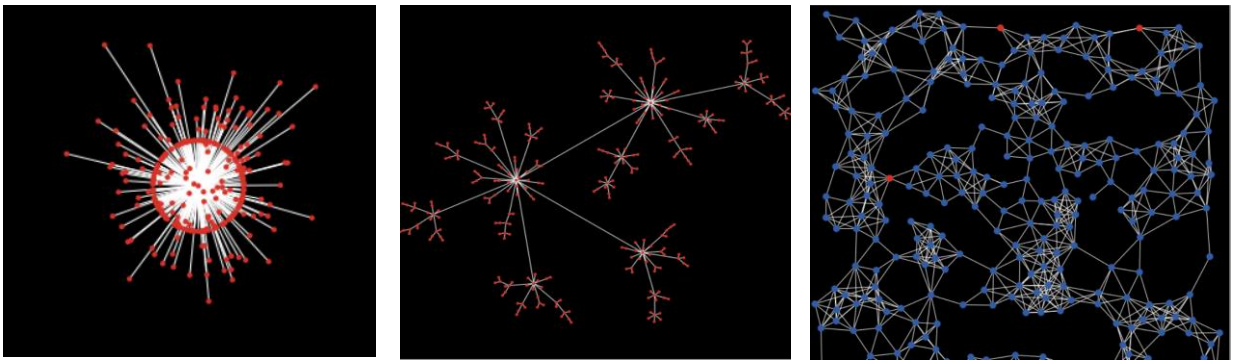
Середовищем моделювання обрано програмний застосунок мультиагентного імітаційного моделювання NetLogo. NetLogo - це платформа для агентного моделювання та симуляцій, яка дозволяє вченим, дослідникам та студентам створювати та вивчати моделі складних систем. Ця платформа зосереджена на створенні взаємодіючих агентів, які взаємодіють у віртуальному середовищі. NetLogo часто використовується для досліджень у галузях, таких як соціальні науки, екологія, економіка та інші, де важливо вивчати емерджентні властивості систем та їхні впливи на динаміку систем. Вона надає зручний інтерфейс для моделювання, візуалізації та аналізу різноманітних взаємодій в системах[6]. Параметри моделі, що реалізується включає в себе характеристики, що наведені в табл. 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 визначення залежності параметрів стійкості та резистентності мережі IoT в залежності від рівня зв'язності мережі (для розподіленої архітектури):

Експеримент №1: Визначення параметрів стійкості та резистивності архітектури мережі IoT. Синтез мережі агентів у відповідності до типу архітектури (результати синтезу в програмному середовищі представлено на рис 3.2:



а) централізована б) децентралізована в) розподілена

Рисунок 3.2 Результати синтезу різних архітектур мережі IoT

Ініціація початкових умов моделі, виконано налаштування моделі відповідно до табл.1 :

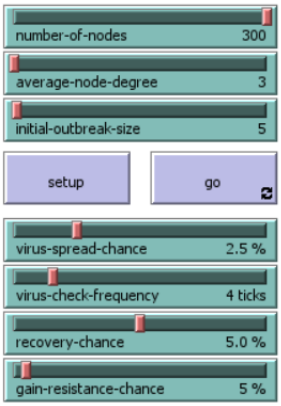


Рисунок. 3.3. Початкові умови симуляції

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

Таблиця 3.2. Критерії для проведення порівняльного аналізу

Критерій	Опис	Параметр моделі
Критерій скомпроментова-ності 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:

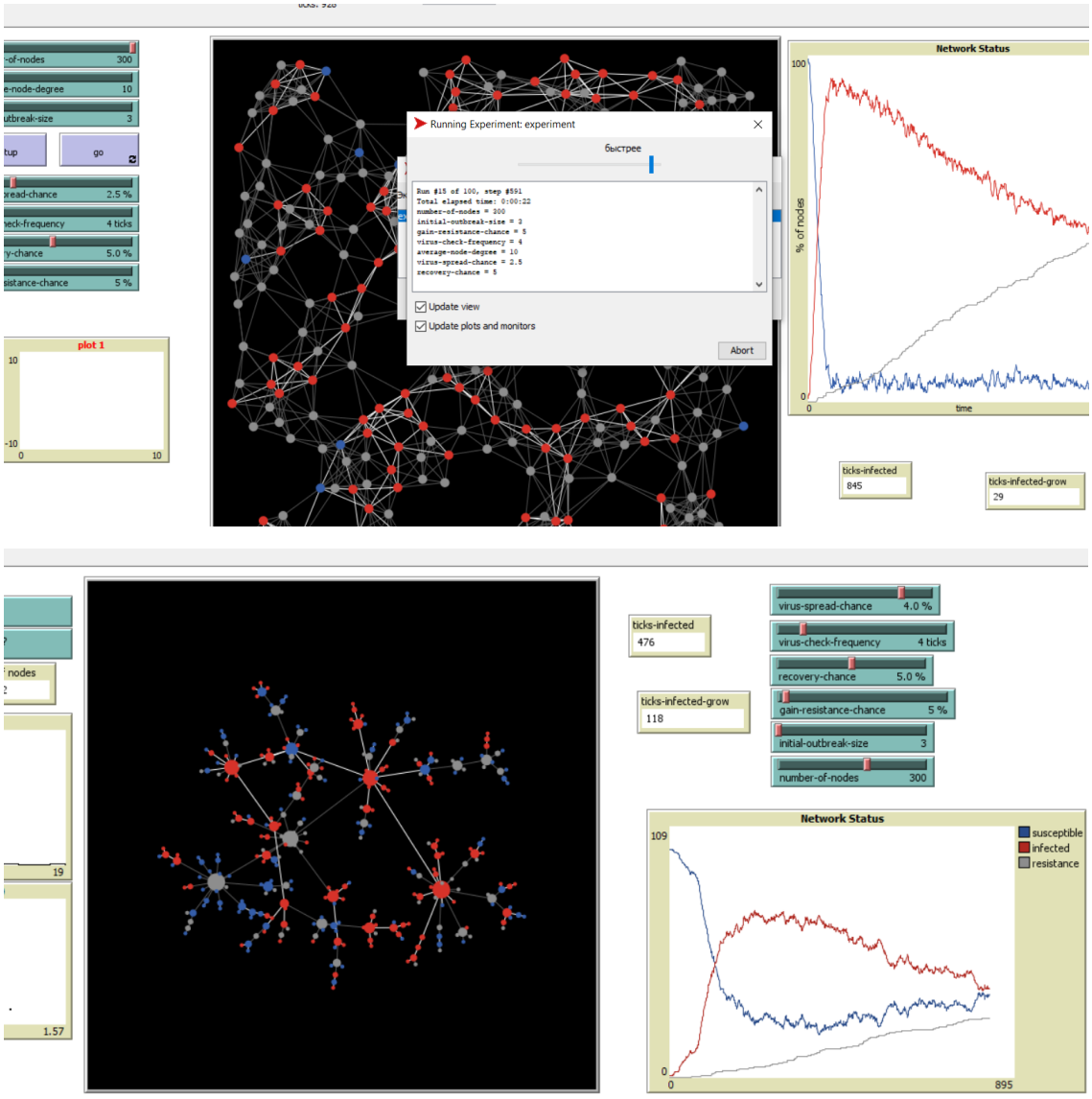


Рисунок 3.4 Приклади окремих симуляцій для різних архітектур (децентралізована та розподілена) IoT

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

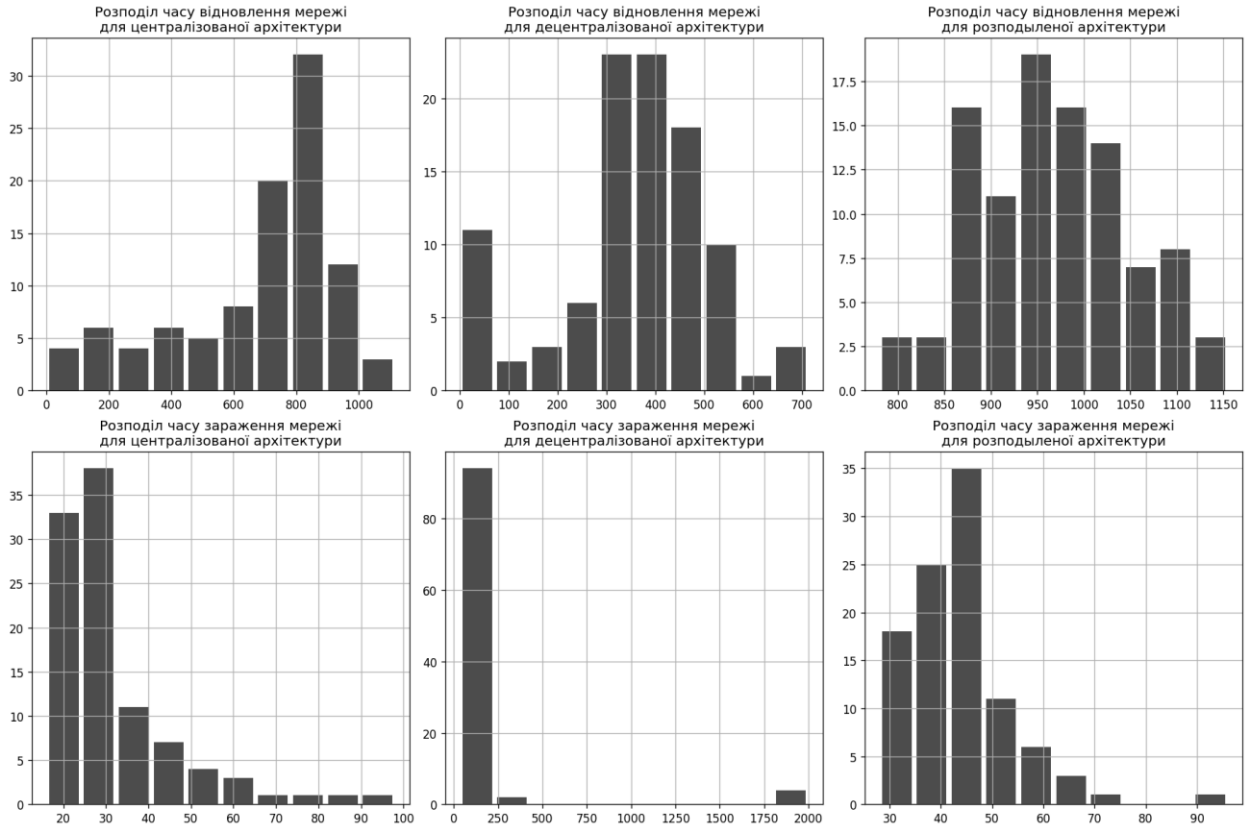


Рисунок 3.5 Розподіл результатів експерименту для різних типів мережі IoT

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, також ця архітектура є більш резистивною (максимальний час для компроментації). Найменш стійкою виявилась розподілена архітектура, що пояснюється великою кількістю надлишкових зв’язків, що відповідним чином збільшує ризик зараження вузла. Питання залежності

показника стійкості та резистивності від зв’язності вимагає додаткового дослідження. (див. Експеримент №2)

Експеримент №2 Визначення залежності параметрів стійкості та резистентності мережі IoT в залежності від рівня зв’язності мережі (для розподіленої архітектури). Синтез мережі агентів розподіленої архітектури (рис 3.2), ініціація початкових умов моделі:

Виконано налаштування моделі відповідно до табл.1, додатково в даному експерименті параметр average-node-degree (середня кількість вузлів під’єднаних до будь-якого вузла) є змінною величиною від 1 до 20 з кроком 1.

Кількість симуляцій для кожного значення average-node-degree – 20. Синтез критеріїв порівняльного аналізу:

Таблиця 3.3 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:

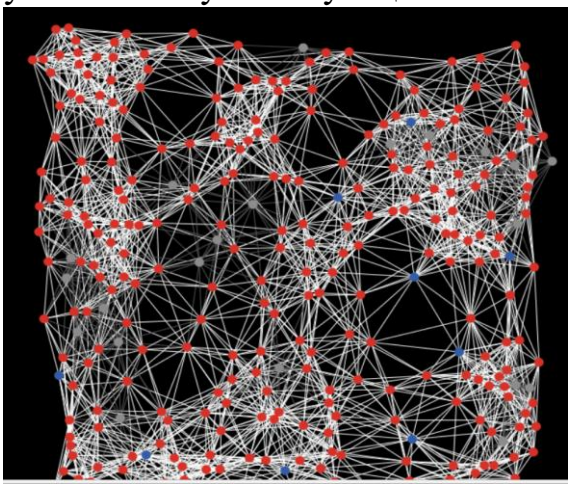


Рисунок 3.6 Симуляція зараження IoT мережі (зв’язність мережі -10)

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 резистивність мереж IoT побудованих за розподіленою архітектурою критично залежать від показника зв’язності. Оптимальним за критерієм максимуму часу зараження можна вважати показник зв’язності – 4.

3.2. Рекомендації та подальші дослідження

Отримані результати експериментів дозволяють сформувати перелік рекомендацій, які доцільно враховувати під час проектування мережі IoT:

1. В залежності від поставленої з побудови IoT задачі необхідно притримуватись децентралізованої архітектури. Оскільки такий підхід дозволяє на фізичному рівні підвищити ступінь стійкості та резистентності мережі.

2. При побудові мереж IoT за розподіленою архітектурою необхідно зважати на показник зв’язності мережі, адже він суттєво впливає на стійкість та резистентність. Орієнтиром може виступати значення показника зв’язності.

Висновки до розділу 3

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

ВИСНОВКИ

В епоху стрімкого розвитку технологій та підключених пристроїв, системи Інтернету речей (IoT) стають не лише необхідністю, але й об'єктом зростаючих загроз кібербезпеки. У цьому контексті виникає необхідність в глибокому дослідженні атак, спрямованих на системи IoT, та розробці ефективних заходів захисту. У нашому дослідженні ми вивчали не лише сучасні загрози, що ставлять під загрозу безпеку IoT-систем, але й впроваджували інноваційні підходи до їхнього захисту.

У першому розділі було розглянуто поняття Інтернету речей, його сфери застосування та можливості використання. З використанням системи Ajax проведено аналіз сучасних загроз та заходів безпеки в контексті систем Інтернету речей. Для забезпечення 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.

В другому розділі проведено опис ключових елементів системи Інтернет речей та методів її захисту. Для розуміння як працює система IoT була побудована топологія «розумного» будинку в Cisco Packet Tracer. Визначено, що сучасні IoT пристрої використовують різні протоколи. Найпоширеніші з них це: ZigBee, BlueTooth, WI-FI. Також найрозповсюдженіші типи атак на IoT мережі: фішинг, MitM атаки, Denial of Service (DoS), експлуатація вразливостей ПЗ, шкідливе ПЗ (Malware), атаки на паролі. Крім того, було розроблено математичну модель зараження вірусом вузлів мережі IoT

У третьому розділі було проведено дослідження в формі двух експериментів на імітаціній моделі IoT в мультиагентному середовищі NetLogo. Визначено, що стійкість і резистивність мереж IoT побудованих за розподіленою архітектурою критично залежать від показника зв’язності.

Отримані результати покладено в основу практичних рекомендацій щодо проєктування IoT мереж для забезпечення адекватного рівня захищеності мережі в контексті показників стійкості та резистентності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Molodetska, K., & Tymonin, Y. (2020). Mathematical modeling covid-19 wave structure of distribution. In CEUR Workshop Proc. (pp. 292-301).