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

Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ОРГАНІЗАЦІЯ ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМАХ АВТОМАТИЗОВАНОГО УПРАВЛІННЯ БУДИНКАМИ»

Виконав: здобувач 4 курсу

Рівень бакалавр

Галузь знань 12 Інформаційні технології»,

спеціальність 125 «Кібербезпека»

Солонар Сергій Михайлович

Керівник: д.ф.-м.н, професор

Василенко Микола Дмитрович

Рецензент: доцент, к.ф.-м.н.

Чепурна Олена Євгенівна

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
_____ «____ »_____ 2024 року

З А В Д А Н Н Я
на кваліфікаційну (бакалаврську) роботу
здобувачу Солонару Сергію Михайловичу

1. Тема роботи: «Організація захисту інформації в системах автоматизованого управління будинками»
Керівник роботи: д.ф.-м.н, професор Василенко Микола Дмитрович
затверджені наказом НУ ОЮА від «02» квітня 2024 року № 809-06
2. Строк подання здобувачем роботи «20» травня 2024 року
3. Дата видачі завдання«15» вересня 2024 року

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

Кваліфікаційна робота на тему «Організація захисту інформації в системах автоматизованого управління будинками» на здобуття першого (бакалаврського) рівня вищої освіти за спеціальністю 125 Кібербезпека, освітньою програмою: Кібербезпека.

Містить 14 рисунків, 4 таблиці, 25 літературних джерел за переліком посилань. Робота виконана на 49 сторінках загального тексту і 41 сторінках основного тексту.

Метою роботи є розробка та оцінка систем захисту інформації в автоматизованих системах управління будинками, зокрема, аналіз загроз і розробка методів захисту з використанням сучасних технологій.

Об’єктом розробки є автоматизовані системи управління будинками, предметом розробки є методи та засоби захисту інформації в цих системах. Шляхи досягнення мети включають аналіз сучасних загроз інформаційної безпеки, розробку і тестування методів захисту, а також інтеграцію цих методів у існуючі системи.

Робота має високий ступінь реалізації, оскільки запропоновані методи були успішно впроваджені у вигляді програмного забезпечення, що дозволяє автоматизовано виявляти та запобігати загрозам інформаційної безпеки.

Результати роботи можуть бути використані при розробці нових та покращенні існуючих систем захисту інформації для різних сфер, включаючи житловий сектор, комерційні організації та державні установи.

Можливими напрямками подальших досліджень є покращення методів захисту інформації для виявлення нових типів загроз, розширення функціональних можливостей систем захисту.

Ключові слова: КІБЕРБЕЗПЕКА, АВТОМАТИЗОВАНІ СИСТЕМИ, ЗАХИСТ ІНФОРМАЦІЇ, АНАЛІЗ ЗАГРОЗ, ІНФОРМАЦІЙНА БЕЗПЕКА, РОЗУМНИЙ ДІМ

ABSTRACT

Qualification work on the topic “Organisation of information protection in automated building management systems” for the first (bachelor's) level of higher education in the speciality 125 Cybersecurity, educational programme: Cybersecurity.

Contains 14 figures, 4 tables, 25 references according to the list of references. The work is executed on 39 pages of the general text and 41 pages of the main text.

The purpose of the work is to develop and evaluate information security systems in automated building management systems, in particular, threat analysis and development of protection methods using modern technologies.

The object of development is automated building management systems, the subject of development is methods and means of protecting information in these systems. Ways to achieve the goal include analysing modern information security threats, developing and testing security methods, and integrating these methods into existing systems.

The work has a high degree of implementation, as the proposed methods have been successfully implemented in the form of software that allows automated detection and prevention of information security threats.

The results of the work can be used in the development of new and improvement of existing information security systems for various fields, including the residential sector, commercial organisations and government agencies.

Possible areas for further research include improving information security methods to detect new types of threats and expanding the functionality of security systems.

Keywords: CYBERSECURITY, AUTOMATED SYSTEMS, INFORMATION PROTECTION, THREAT ANALYSIS, INFORMATION SECURITY, SMART

ЗМІСТ

ВСТУП

Актуальність теми. Зі зростанням використання автоматизованих систем для управління будівлями, які включають контроль за освітленням, опаленням, вентиляцією та іншими системами, важливість захисту інформації стає все більш очевидною. Ці системи збирають велику кількість даних про поведінку та переваги мешканців, що робить їх потенційною мішенню для кібератак.

Ефективна організація захисту інформації забезпечує не тільки конфіденційність та інтегральність даних, але й допомагає підтримувати функціональність та безпеку всієї системи. Враховуючи те, що автоматизовані системи можуть включати управління доступом до будівлі, надійний захист інформації також є ключовим для забезпечення фізичної безпеки мешканців.

З огляду на складність та взаємопов'язаність сучасних інформаційних систем, дослідження в цій галузі допоможе розробити більш ефективні методи захисту, враховуючи як технічні, так і організаційні аспекти безпеки. Це, в свою чергу, дозволить не тільки вдосконалити існуючі системи, але й розробити нові підходи та технології, які зможуть забезпечити кращий захист даних у майбутньому, адаптуючись до постійно змінюваних загроз.

Мета дослідження полягає в аналізі загроз інформаційної безпеки в системах автоматизованого управління будинками та розробці заходів щодо їх захисту.

Для досягнення поставленої мети в роботі було визначено завдання, які потрібно виконати:

- визначити різні типи інформації та автоматичні системи управління будинком;
- дослідити систему "Розумний дім" та розглянути аспекти її роботи;
- охарактеризувати особливості приватностні даних та їх вразливість в системі "Розумного будинку";
- проаналізувати методи атак за допомогою бічного каналу;
- надати класифікацію різновидів атак через бічний канал;

- охарактеризувати особливості атаки на основі сліду та вимірювання часу (FATS);
- скласти методи захисту мережевого трафіку;
- оцінити показники ефективності захисту, такі як EDR та TPR.

Об'єктом дослідження є системи "розумний дім", які об'єднують різноманітні технології для забезпечення комфорту, енергоефективності та безпеки.

Предмет дослідження включає аналіз уразливостей програмно-апаратних засобів систем "розумного будинку".

Практичне значення отриманих результатів. Результати допоможуть підвищити рівень безпеки в розумних будинках. Завдяки вдосконаленню методів захисту інформації, мешканці можуть бути впевнені у конфіденційності та безпеці своїх особистих даних. Крім того, ефективні рішення з захисту інформації знижують ризик кібератак, які можуть спричинити не тільки витік особистої інформації, але й серйозні збої в роботі систем управління будівлею. Таким чином, підвищується загальна надійність та стабільність системи. Результати дослідження можуть також сприяти розвитку нових стандартів і нормативних вимог до автоматизованих систем управління будинками, що зробить можливим впровадження цих систем на ширший ринок з упевненістю в їхній безпеці.

1 ТЕОРЕТИЧНІ АСПЕКТИ ПОНЯТТЯ ІНФОРМАЦІЇ ТА ВИЗНАЧЕННЯ СИСТЕМИ «РОЗУМНИЙ ДІМ»

1.1 Типи інформації та автоматичні системи управління будинком

В сучасному світі, де технології постійно розвиваються, роль інформаційної безпеки стає все більш важливою, особливо в контексті автоматизованих систем управління будинками, що зазвичай включають в себе інтелектуальні системи вимірювання, контролю доступу, енергозбереження та багато іншого. Ці системи збирають і обробляють велику кількість даних, що робить їх потенційною мішенню для кібератак.

Ключовими аспектами класифікації інформації в таких системах є:

1. Конфіденційність - забезпечення, що інформація доступна тільки тим, хто має на це право. В системах управління будинками це може означати, що особисті дані мешканців, такі як їх звички витрати енергії або графіки присутності вдома, захищені від сторонніх.

2. Цілісність - гарантія того, що інформація не була змінена або пошкоджена без дозволу. Це може бути забезпечено за допомогою криптографічних технологій та систем виявлення і запобігання вторгнень.

3. Доступність - інформація повинна бути доступною для авторизованих осіб та систем, коли вони цього потребують. Заходи, такі як резервне копіювання даних та використання відмовостійких систем, можуть допомогти забезпечити безперервність сервісу навіть у випадку технічних проблем [1].

Цілями безпеки інформації є конфіденційність, цілісність і доступність, тобто Тріада CIA, як зображена на рисунку 1.1.

Тріада CIA - це простий, але всеосяжний контрольний список високого рівня для оцінки ваших процедур та інструментів безпеки. Ефективна система задовольняє всі три компоненти: конфіденційність, цілісність і доступність. Система інформаційної безпеки, якій бракує одного з трьох аспектів тріади CIA, є недостатньою [2].

Рисунок 1.1 – Тріада CIA [2]

Інформаційна безпека в автоматизованих системах управління будинками має бути частиною загальної стратегії безпеки, що включає регулярні оцінки ризиків, а також розробку та імплементацію політик і процедур, спрямованих на мінімізацію потенційних загроз. Зокрема, слід враховувати потенційні загрози як ззовні, так і зсередини організації.

Інформація може набирати різноманітних форм і мати безліч облич. Вона може бути як чітко структурованою, так і вільно розкиданою, може надходити у формі цифр, тексту, зображень чи навіть звуків. Наприклад, наукові дані, представлені у вигляді таблиць і графіків, дають чітке розуміння досліджених явищ. Літературні твори, у свою чергу, використовують мову для створення образних і емоційних зображень, що дозволяє читачам відчувати і уявляти описані події. Водночас, візуальна інформація через фотографії та відео може передавати нюанси, які складно описати словами — від емоційних виразів облич до складних динамічних сцен. Звукові записи, як от музика чи розмови, зберігають тональність і нюанси голосу, що може бути критично важливим для повного розуміння переданої інформації. У цифрову епоху, інформація може також перебувати у формі даних, які обробляються та аналізуються за допомогою алгоритмів для виявлення тенденцій та встановлення зв'язків, невидимих на перший погляд [3]. Таким чином, розуміння різних типів інформації відіграє ключову роль у тому, як

ми інтерпретуємо і використовуємо дані в повсякденному житті та професійній діяльності.

1. За функціональним змістом:

- Правова інформація: Сукупність відомостей та документів про право, його систему, юридичні факти, правовідносини, правопорядок тощо.
- Економічна інформація: Відображає відносини та процеси, пов’язані з виробництвом, розподілом, обміном і споживанням матеріальних та нематеріальних благ.
- Соціальна інформація: Формується в суспільстві та використовується індивідами, соціальними групами для регулювання соціальної взаємодії [6, с. 1]

2. За джерелом одержання:

- Зовнішня інформація: Отримана з зовнішніх джерел, таких як інтернет, друковані видання, конференції тощо.
- Внутрішня інформація: Зібрана власними зусиллями або внутрішніми джерелами підприємства [6, с. 1]

3. За ступенем опрацювання:

- Виробнича інформація: Використовується в процесах виробництва, обслуговування, логістики тощо.
- Первинна інформація: Отримана безпосередньо від джерел, не піддавалася подальшій обробці [4]

Система автоматизованого управління будинками, яка інтегрує інформаційні та керуючі системи, створює унікальну платформу для оптимізації домашнього середовища. Інформаційні системи збирають дані через датчики та інші входи, такі як температура, вологість, рівень освітленості та стан енергоспоживання. Ця інформація аналізується для оцінки поточного стану будинку та потреб його мешканців.

З іншого боку, керуючі системи використовують отримані дані для автоматизації різних процесів у будинку. Наприклад, вони можуть автоматично регулювати клімат-контроль, освітлення, системи безпеки, та навіть управління

енергозберігаючими заходами. Це не тільки збільшує комфорт мешканців, але й допомагає знизити витрати на енергію та підвищити загальну безпеку.

Також, система може бути інтегрована з мобільними застосунками або веб-інтерфейсами, дозволяючи користувачам моніторити та керувати всіма аспектами своїх домівок на відстані. Це особливо корисно для тих, хто часто знаходиться в дорозі або хоче мати можливість швидко реагувати на зміни в домашньому середовищі.

Завдяки використанню передових технологій, таких як штучний інтелект та машинне навчання, системи автоматизації будинку стають ще більш розумними та здатними передбачати потреби своїх користувачів, забезпечуючи не тільки комфорт, але й ефективність в кожному аспекті домогосподарства [5]. Види систем управління зображено на рисунку 1.2.

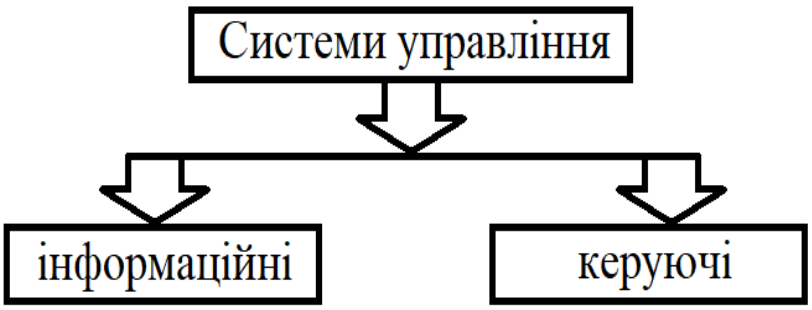

Рисунок 1.2 – Види систем управління [6]

Функції інформаційних систем є важливими для ефективного управління та моніторингу різноманітних технологічних та виробничих процесів. Вони забезпечують збір та видачу інформації, що дозволяє операторам отримувати актуальні дані про стан об’єктів управління. Ця інформація є критичною для прийняття обґрунтованих та своєчасних рішень.

1. Збір та аналіз даних: Інформаційні системи автоматично збирають дані з різних джерел і датчиків, розміщених у ключових точках технологічного процесу. Це можуть бути показники температури, тиску, швидкості,

вологості тощо, залежно від специфіки процесу. Після збору ці дані систематично аналізуються для виявлення тенденцій або непередбачених відхилень.

2. Представлення інформації: ЕОМ в інформаційних системах відіграє ключову роль у обробці зібраних даних і поданні їх у зручному для сприйняття форматі. Це можуть бути графіки, діаграми, інтерактивні панелі управління, що дозволяють операторам швидко оцінювати поточний стан процесів і приймати рішення без затримок.
3. Підтримка прийняття рішень: Оператори використовують інформацію, отриману від інформаційних систем, для прийняття обгрунтованих рішень. Системи можуть надавати рекомендації або автоматизовані попередження на основі алгоритмів обробки даних, здатних аналізувати складні сценарії та передбачати потенційні проблеми ще до їх виникнення.
4. Інтерфейси для взаємодії: Сучасні інформаційні системи часто оснащені зрозумілими та інтуїтивними інтерфейсами, які спрощують процеси моніторингу і управління для операторів. Ці інтерфейси можуть бути адаптовані до конкретних потреб користувача, забезпечуючи швидкий доступ до найважливішої інформації.
5. Інформаційні системи, таким чином, відіграють критичну роль у забезпеченні ефективності та безпеки технологічних і виробничих процесів, допомагаючи компаніям адаптуватися до змін умов роботи та вимог ринку [7]

Мета таких систем - отримання оператором інформації з високою вірогідністю для ефективного прийняття рішень. Характерною особливістю для інформаційних систем є робота ЕОМ в розімкнутої схемою управління. Причому можливі інформаційні системи різного рівня.

Інформаційні системи повинні, з одного боку, надавати звіти про нормальний хід виробничого процесу і, з іншого боку, інформацію про ситуації, викликаних будь-якими відхиленнями від нормального процесу.

Розрізняють два види інформаційних систем:

– інформаційно-довідкові (пасивні), які постачають інформацію оператору після його зв'язку з системою за відповідним запитом;

– інформаційно-радять (активні), які самі періодично видають абоненту призначену для нього інформацію [8].

У інформаційно-довідкових системах ЕОМ, які є важливою складовою сучасних технологічних процесів, основна роль припадає на збір та обробку інформації про керований об'єкт. Ці системи не лише забезпечують збір даних, а й виконують їх аналіз, перетворення та представлення у формі, зручній для оператора. Такий підхід дозволяє оператору приймати обґрунтовані рішення щодо управління об'єктом, враховуючи актуальний стан технологічного процесу.

Системи збору та обробки даних, як вже згадувалося, виконують подібні до централізованих систем контролю функції, але з вищим рівнем організації. Вони здатні інтегрувати великі обсяги інформації, забезпечуючи деталізоване та точне моделювання робочих процесів. Розширені аналітичні можливості дозволяють виробляти більш точні рекомендації для операторів, що сприяє покращенню управлінських рішень [8].

Системи управління, які видають безпосередньо команди виконавцям або виконавчим механізмам, мають кілька ключових характеристик, які забезпечують їх ефективність та відповідність вимогам сучасних виробничих і технологічних процесів.

В таблиці 1.1 описані основні характеристики та принцип роботи сучасних систем управління.

Таблиця 1.1 – Основні характеристики систем управління [9]

№	Характеристика	Опис
1.	Безпосереднє управління виконавчими механізмами	Системи здатні миттєво реагувати на зміни у виробничому процесі, відправляючи команди безпосередньо на виконавчі пристрої, такі як роботи, конвеєри, насоси тощо. Це дозволяє точно та оперативно коригувати робочі процеси в залежності від поточних потреб.

2.	Робота в реальному часі	Системи управління, які працюють у реальному часі, критично важливі для індустрій, де час є ключовим фактором. Це означає, що система здатна обробляти дані та видавати команди майже одночасно з отриманням інформації від датчиків або інших систем. Це забезпечує неперервність і безперебійність виробничих процесів.
3.	Роль людини як контролера	Незважаючи на високий рівень автоматизації, роль людини залишається важливою, особливо у вирішенні складних питань, які вимагають нестандартного підходу або креативного мислення. Людина контролює систему, приймаючи рішення у випадках, коли потрібно відхилитися від стандартних алгоритмів реакції або коли система стикається з непередбаченою ситуацією [8].

Керуюча система здійснює функції управління за визначеними програмами, заздалегідь передбачають дії, які повинні бути зроблені в тій чи іншій виробничій ситуації. За людиною залишається загальний контроль і втручання в тих випадках, коли виникають непередбачені алгоритмами управління обставини. Керуючі системи мають кілька різновидів.

Супервізорні системи управління. АСУ, яка функціонує в режимі супервізорного управління, призначена для організації багатопрограмного режиму роботи ЕОМ і представляє собою дворівневу ієрархічну систему, що володіє широкими можливостями і підвищеною надійністю. Управляюча програма визначає очевидність виконання програм і підпрограм і керує завантаженням пристроїв ЕОМ [10]

Системи прямого цифрового керування. ЕОМ безпосередньо виробляє оптимальні керуючі впливи і за допомогою відповідних перетворювачів передає команди управління на виконавчі механізми. Режим прямого цифрового керування дозволяє застосовувати більш ефективні принципи регулювання і управління і вибирати їх оптимальний варіант; реалізувати оптимізують функції і процес адаптації до змін зовнішнього середовища і змінним параметрами об'єкта

управління; знизити витрати на технічне обслуговування та уніфікувати засоби контролю і управління.

1.2 Система «Розумний дім» та аспекти її роботи.

У сучасному світі технологічний прогрес неухильно впливає на наше повсякденне життя, пропонуючи новітні рішення для покращення комфорту, безпеки та ефективності. Одним із яскравих прикладів таких інновацій є системи "розумного дому", які трансформують традиційне домашнє середовище в інтелектуальний простір, що здатний адаптуватися до потреб своїх мешканців. Ці системи використовують розширений спектр автоматизованих технологій для управління побутовими процесами, забезпечуючи високий рівень інтеграції та персоналізації. Такий підхід не лише спрощує повсякденні задачі, але й відкриває нові можливості для створення більш безпечного та енергоефективного дому.

Елементи, які можуть взаємодіяти між собою за допомогою даної системи зображено на рисунку 1.2.

Рисунок 1.2 – Елементи, які взаємодіють в системі «Розумний дім» [11]

Розумний будинок (також відомий як смарт-будинок) - це інноваційна технологія, яка змінює підхід до життя та забезпечує комфорт та зручність для мешканців.

Ця системи забезпечує власникам змогу дистанційно керувати побутовими приладами через смартфони чи інші пристрої, що веде до зручнішого та енергоефективнішого використання ресурсів. Наприклад, можливість дистанційно регулювати опалення або кондиціонування повітря дозволяє значно знизити енерговитрати, адже система може бути вимкненою, коли нікого немає вдома, та активованою перед поверненням домочадців.

Крім того, системи розумного дому підвищують рівень безпеки завдяки встановленню камер спостереження, сенсорів руху та систем сповіщення, що можуть надсилати повідомлення про будь-яку підозрілу активність незалежно від того, де перебуває власник.

З погляду практичності, розумний дім також сприяє більшій індивідуалізації житлового простору. Власники можуть налаштувати систему так, щоб вона відповідала їхнім унікальним потребам та звичкам, створюючи по-справжньому "розумне" житлове середовище, що забезпечує неперевершений рівень зручності та функціональності [11].

Система розумний дім складається з мережі, приладів, датчиків та програмного забезпечення, як зображено на рисунку 1.2.

Рисунок 1.3 – Технічні прилади, які використовують систему «Розумного дому» [12]

Пристрої, що входять у комплекти систем можливо поділити на 3 групи:

Хаб (відомий також як контролер, центр управління, шлюз або міст) є важливим з'єднувальним елементом в системі розумного будинку. Він приймає сигнали від усіх підключених устройств у будинку та керує їх діями, забезпечуючи збір даних та віддалене керування через Інтернет, у тому числі відправляючи необхідні команди.

Сенсори та датчики — це елементи, які відповідають за збір інформації про умови всередині та зовні будинку. Вони можуть вимірювати температуру повітря, фіксувати рух, виявляти присутність диму, контролювати рівень освітлення і багато іншого. Також можна встановити спеціальні безпекові датчики на двері та вікна, які моніторять їхнє надійне закриття.

Актуатори — це виконавчі пристрої, призначені для активного керування побутовими приладами у будинку. До них належать розумні розетки, димери, вимикачі, а також трубні клапани, різноманітні реле, контролери клімату та інші подібні пристрої [12].

Завдяки проведеному аналізу сучасних систем було виведено ряд переваг таких систем:

1. Однією з головних переваг «розумного дому» є зручність, яку він надає мешканцям. Завдяки технології «розумного дому» ви можете налаштувати безліч процесів для кожного члена сім’ї, від включення будильника в певний день і час до запуску різноманітної побутової техніки. Це включає можливість дистанційного керування всіма системами в будинку за допомогою мобільного додатку або голосового помічника. Ви можете вимкнути світло, встановити температуру або перевірити систему безпеки, навіть якщо вас немає вдома [13].

2. Незважаючи на збільшення кількості технологічних продуктів, «розумні будинки» допомагають знизити витрати на електроенергію завдяки автоматизованим системам. Розумні термостати регулюють температуру відповідно до ваших потреб, а датчики світла вимикають світло в порожніх

кімнатах. Це не тільки зменшує рахунки за комунальні послуги, але й допомагає зменшити негативний вплив на навколишнє середовище [13]

3. Системи безпеки розумного будинку включають відеоспостереження, датчики диму, води та проникнення, а також сигналізацію. Ви можете отримувати миттєві сповіщення про будь-які інциденти чи загрози у вашому домі та дистанційно керувати системою безпеки. Важливо використовувати надійні паролі та регулярно оновлювати програмне забезпечення, щоб захистити від потенційних кіберзагроз і забезпечити високий рівень безпеки вашого «розумного дому» [13].

4. «Розумний дім» дозволяє насолоджуватися справжніми розвагами та відпочинком. Ви можете встановити звукову систему, великий телевізор або навіть домашній кінотеатр для максимального комфорту та задоволення. Для тих, хто любить готувати або смакувати коктейлі, «розумний будинок» можна обладнати смарт-баром і кухнею. У них вбудовані системи приготування напоїв, автоматичного приготування і вибору рецептів за допомогою голосових команд [13]

Щодо недоліків даної системи, можемо виокремити наступні пункти з таблиці 1.2.

Таблиця 1.2 – Недоліки системи «Розумного дому» [14]

№	Недолік	Опис
1.	Висока вартість установки	Варто встановити систему розумного дому, особливо якщо ви хочете охопити всі аспекти вашого будинку. Витрати включають дороге підключення обладнання, дротові та бездротові системи та професійне встановлення. Тому він може бути недоступним для багатьох людей [16].
2.	Професійний менеджмент	«Розумний дім» вимагає проведення певних спеціалізованих технічних операцій. Ви повинні бути готові регулярно оновлювати програмне забезпечення та підтримувати систему, щоб забезпечити її надійну роботу. Це вимагає додаткових витрат і зусиль [16].

3.	Залежність від Інтернету та електроенергії	«Розумний дім» повністю залежить від наявності Інтернету та електрики. При відключенні Інтернету або електропостачання можливості управління розумними системами можуть бути обмежені або повністю втратити свою функціональність. Це несе певні ризики, особливо в надзвичайних ситуаціях [16].
4.	Конфіденційність і кібербезпека	Розумні домашні пристрої, підключені до Інтернету, можуть стати об'єктами кібератак і порушень конфіденційності. Якщо не вжити відповідних заходів безпеки, зловмисники можуть отримати доступ до персональних даних і систем контролю. Запобігання кіберзагрозам вимагає постійного моніторингу та оновлення програмного забезпечення безпеки [16].
5.	Стандарти системи «Розумний дім» і сумісність опор	Системи розумного будинку можуть використовувати різні стандарти та протоколи зв'язку, що може спричинити проблеми сумісності між різними пристроями. Вибір сумісних пристроїв і систем може бути важливим завданням для уникнення проблем з інтеграцією та використанням «розумного будинку» [16].

Незважаючи на те, що більшість систем безпеки створюються як автономні блоки (з моніторингом або без нього), багатьма з них можна керувати та використовувати як частину системи розумного будинку. Так, якщо ви на роботі, ви можете перевірити показання системи домашньої безпеки за допомогою веб-браузера.

Крім звичайних пристроїв з автоматичним керуванням, "Розумний дім" має ряд спеціальних пристроїв з вправлення за освітленням. У цьому будинку можуть бути застосовані різні системи, які управляють роботою більш ніж 300 освітлювальних приладів та забезпечують функціонування ряду інших приємних доповнень.

Є кілька способів встановлення спеціального освітлення в будинку. Наприклад, можна порахувати, що у вітальні потрібен певний рівень яскравості вечірнього освітлення. Система це робить автоматично [14]

Майже всім у системі комунального забезпечення – від повітря до води – можна керувати за допомогою системи «Розумний Дім» [14].

В цьому розділі було здійснено аналіз ключових понять, пов'язаних з інформацією та її роллю в сучасних автоматизованих системах управління будинками. Розглянуто основні характеристики інформації, такі як її точність, актуальність, повнота та доступність, які є критичними для ефективного функціонування систем «Розумний дім».

У наступних розділах роботи планується детальніше розглянути конкретні методи і засоби захисту інформації, які можуть бути застосовані в системах «Розумний дім». Буде проведено аналіз сучасних технологій та методів авторизації користувачів, а також систем моніторингу та реагування на інциденти безпеки. Особлива увага буде приділена розробці рекомендацій щодо інтеграції захисних механізмів у різні компоненти системи «Розумний дім» для забезпечення комплексної інформаційної безпеки.

2 ПРИВАТНІСТЬ ДАНИХ ТА АНАЛІЗ ЗАГРОЗ ІНФОРМАЦІЇ В САУБ

2.1 Приватність даних та їх вразливість в системі «Розумного будинку»

Приватність даних у сучасних розумних будинках набуває все більшої ваги, оскільки мешканці щодня передають велику кількість інформації про свої повсякденні звички через численні вбудовані датчики. Ці дані аналізуються системами штучного інтелекту, які адаптують свою роботу до потреб користувачів. Однак такий потік інформації може бути використаний злочинцями для витоку особистих деталей життя мешканців.

Приватність у контексті розумних будинків розглядається як право особи зберігати своє особисте життя та інформацію в секретності, доступній тільки обраним особам. Це право захищене законом у більшості держав і охороняється від порушень, таких як незаконне стеження чи несанкціонований доступ.

Мотивація до порушення приватності може бути різною, включаючи пошук комерційної вигоди чи особисті образи. Навіть державні органи можуть зламувати приватність через незаконне стеження, що підкреслює необхідність підсилення захисту приватності в розумних будинках [16].

Атаки, як FATS, засновані на аналізі сигналів та часових відбитків, є значною загрозою. Системи виявлення вторгнень часто не здатні ефективно протидіяти таким пасивним атакам. Агресори можуть непомітно збирати дані, а жертви зазвичай виявляються беззахисними до швидкого реагування на ці загрози.

Застосування шифрування не завжди є ефективним, оскільки атаки проводяться, враховуючи контекстуальні характеристики бездротових передач. У зв’язку з цими викликами важливо розробляти надійні та активні механізми захисту у розумних будинках, які могли б забезпечити ефективний захист інформації користувачів, одночасно зберігаючи зручність користування.

SCA представляє серйозну загрозу для безпеки систем, оскільки нападники можуть маніпулювати пристроями, не маючи доступу до джерельних кодів, змісту комунікацій чи деталей функціональності систем. Розглянемо різні аспекти SCA, включно з фізичними характеристиками, відгуками системи та контекстуальними

даними, які відносяться до бездротового зв’язку інтелігентних пристроїв. Ці аспекти створюють різноманітні можливості для отримання критичної інформації.

Атака FATS, одна з форм SCA, використовує перехоплення емітованих сигналів для розуміння внутрішніх процесів мешканців. Це пасивне порушення конфіденційності ставить жертв у складну ситуацію, оскільки вони не можуть виявити атаку під час її проведення. Зібрані дані можуть бути використані для шантажу або продажу третім особам.

Для боротьби з ризиками атак FATS, науковці розробляють активні стратегії оборони, щоб паралізувати дію атак, оскільки їх повне блокування неможливе. Основна стратегія полягає у маскуванні бездротових шаблонів трафіку та розмиванні кореляцій між передачами, що включає введення штучної затримки перед передачею пакета і додавання фіктивних пакетів у мережевий трафік.

Щодо типового інтелектуального пристрою для смарт-дому, то вони зазвичай складаються з декількох базових компонентів, таких як мікропроцесор, інтерфейси вводу та виводу, носій для збереження даних, модулі безпровідного зв'язку (такі як WiFi та Bluetooth), джерело живлення та, залежно від призначення пристрою, набір сенсорів та актуаторів. Хакери, які застосовують атаки через бічні канали, можуть використовувати кожен з цих компонентів для витоку цінної інформації. Тому за останні десятиліття було розроблено багато нелегальних методів втручання в різні аспекти роботи інтелектуальних пристроїв.

SPA і DPA — це техніки атак, спрямовані на виявлення конфіденційних даних, наприклад, ключів шифрування, шляхом аналізу енергії, яку споживає пристрій під час роботи. Ці методи є особливо важливими для джерел живлення, оскільки хакери можуть використовувати витік енергії для добування ключових даних [17].

Атаки на безпровідні комунікації включають зловживання аналізом часу та об'єму передачі даних через безпровідні канали, такі як Wi-Fi та Bluetooth. Зловмисники можуть отримувати доступ до конфіденційної інформації, стежити за передачею даних або навіть змінювати їх.

Атака через порти вводу/виводу через аналіз помилок може включати введення шкідливих даних або витік інформації через ці порти. Захист від таких атак передбачає вжиття фізичних і програмних заходів безпеки.

Акустичний та електромагнітний аналіз базуються на використанні витоків звукових або електромагнітних сигналів, які генеруються пристроєм під час його функціонування. Ці витоки можуть допомогти зловмисникам отримати інформацію про внутрішні процеси пристрою.

Як показано на рисунку 2.1, кожна вбудована одиниця в пристрої стикається щонайменше з відповідною атакою.

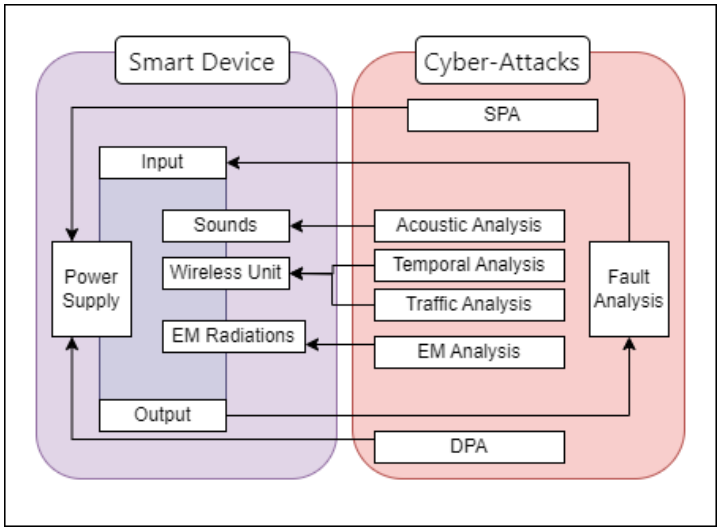

Рисунок 2.1 – Схема атак на смарт-пристрої

Простий аналіз потужності (SPA) та диференційний аналіз потужності (DPA) - це дві атаки, які загрожують системі через блок живлення.

2.2 Метод атаки за допомогою бічного каналу

Проведення атаки через бічний канал передбачає використання фізичних характеристик пристрою для отримання критично важливої інформації, пов'язаної з ним. Основна передумова таких атак полягає в тому, що інформація неперервно витікає, тому злочинці можуть маніпулювати системою.

Атаки через бічний канал розділяють на активні та пасивні. Активні атаки вимагають безпосереднього доступу до цільового пристрою чи системи, або необхідності перебувати поряд. Одним із прикладів активної атаки є аналіз несправностей, коли зловмисники подають спеціально підготовлені дані та аналізують реакцію системи, щоб зрозуміти, як пристрій функціонує. Інший приклад – аналіз звуків, які виробляє пристрій, щоб виявити їх зв'язок із діяльністю системи, зокрема це стосується механічних виконавчих систем.

Пасивні атаки через бічний канал відбуваються непомітно для жертви. Вони використовують зовнішні ознаки пристрою, як наприклад, віддалене перехоплення мережевого трафіку і захоплення переданих даних для подальшого аналізу. Навіть зашифровані дані можуть містити корисну інформацію, яку злочинці можуть витягти з контексту сигналів.

Для захисту від пасивних атак рекомендується використання активних захисних методів, щоб унеможливити зловмисникам розшифровування захоплених пакетів даних [18].

Захист від атак через бічний канал вимагає уваги до фізичних та програмних аспектів безпеки пристроїв і систем. Фізичні заходи можуть включати обмеження доступу до пристрою, захист від електромагнітних випромінювань та використання антивірусних програм та систем детекції вторгнень.

Враховуючи збільшення кількості підключених пристроїв та розвиток Інтернету речей, забезпечення захисту від атак через бічний канал стає життєво важливим завданням. Адекватна відповідь на ці виклики та постійне вдосконалення захисних методів є ключовими для забезпечення безпеки пристроїв і конфіденційності користувачів.

2.3 Різновиди атак через бічний канал

Атаки бічного каналу поділяються на три категорії залежно від рівня фізичного втручання: інвазивні, напівінвазивні та неінвазивні. Інвазивні атаки безпосередньо впливають на фізичну інтеграцію цільового пристрою, часто

призводячи до його пошкодження або повного знищення. Для таких атак характерне руйнування компонентів з метою аналізу їхньої роботи або проведення лабораторних досліджень. Напівінвазивні атаки також вимагають фізичного доступу до апаратури, але без її повного розбирання — наприклад, шляхом відкриття корпусу для доступу до електроніки.

З іншого боку, неінвазивні атаки використовують лише зовнішні сигнали, такі як дані з портів, електричні кабелі, бездротові сигнали, електромагнітні випромінювання чи акустичні шуми. Ці джерела інформації надають цінні відомості про роботу системи, що дозволяє вивчати її характеристики без прямого втручання [19]. Неінвазивні методи можуть бути особливо складними та ефективними, оскільки вони залежать від точності вимірювальних інструментів та здатності системи обмежувати або ускладнювати доступ до таких даних.

Таксономія атак бічного каналу, представлена на рисунку 2.2, надає загальне уявлення про різні класи атак і підкреслює розмаїтість можливих методів, які можуть використовувати зловмисники. Забезпечення захисту від таких атак потребує комплексного підходу, включаючи заходи фізичної безпеки, криптографічні рішення та програмні механізми контролю доступу.

Аналіз споживання енергії та диференційний аналіз споживання енергії — це два методи, що використовуються для виявлення конфіденційної інформації у пристроях шляхом аналізу їхнього енергетичного витрату.

SPA (Симплексний аналіз споживання): Він моніторить зміни в енергоспоживанні пристрою під час виконання різноманітних алгоритмів і виявляє шаблони, які можна асоціювати з певними операціями. Зловмисники намагаються порівнювати ці виявлені шаблони з відомими алгоритмами, щоб з'ясувати функціональність пристрою. Наприклад, метод дозволяє відрізнити методи шифрування через їх різні енергетичні потреби. Однак слід зазначити, що раптові сплески енергії та електричний шум можуть обмежити ефективність цього методу [20].

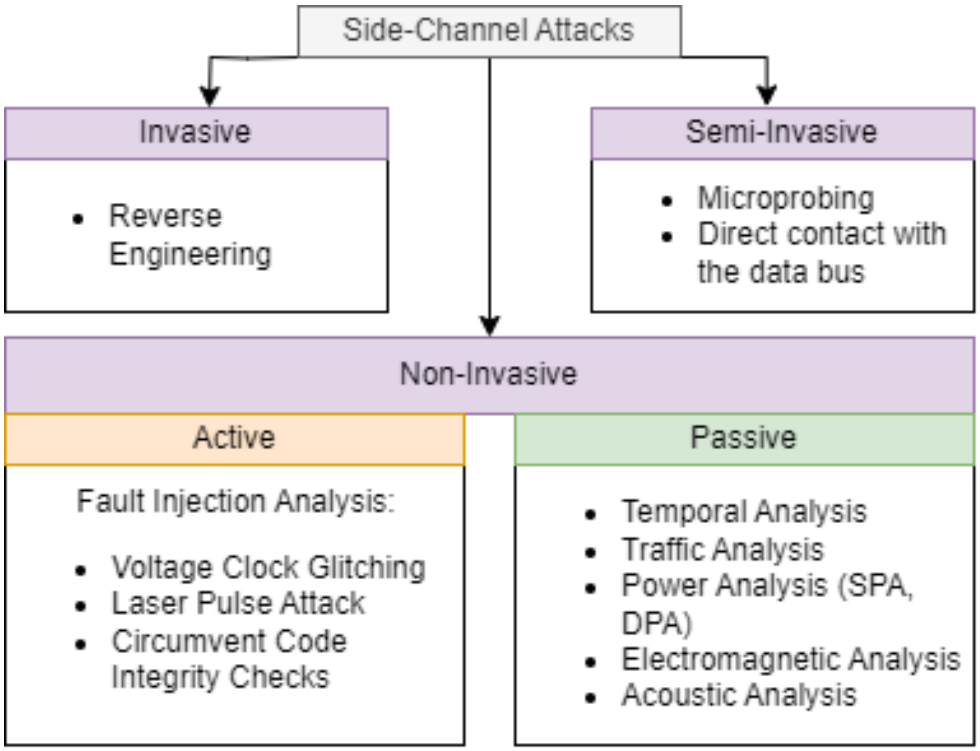

Рисунок 2.2 – Таксономія атак бічного каналу

DPA (Диференційний аналіз споживання): Цей більш вдосконалений метод використовує статистичні техніки для корекції помилок. Він аналізує енергоспоживання пристрою під час виконання криптографічних і некриптографічних операцій, порівнюючи спостереження для виявлення ключової інформації системи. DPA становить загрозу для всіх типів апаратного забезпечення, що використовують криптографічні захисти [21].

Аналіз несправностей: Цей метод передбачає введення різних типів несправностей у розумний пристрій для аналізу впливу на систему. Приклади включають підвищення температури пристрою, використання лазерного проміння певної частоти та введення штучних сигналів для збільшення ймовірності перехрестя сигналів [22].

Електромагнітний аналіз: Використовує електромагнітне випромінювання пристроїв під час шифрування або дешифрування для виявлення кореляцій між випромінюванням та шифрованим текстом. Цей метод може бути ефективним для віддалених атак, залежно від потужності приймального обладнання.

Акустичний аналіз: Використовує шуми електромеханічних компонентів пристрою для отримання конфіденційної інформації через аналіз акустичних коливань. Переваги цього методу включають точне відокремлення тихих звуків та використання простих записуючих пристроїв.

Аналіз часу: Фокусується на часових даних бездротових передач сигналів системи для виявлення тимчасових кореляцій у мережевому трафіку, що відкриває критичну інформацію про поведінку системи.

Аналіз трафіку: Досліджує мережевий трафік для визначення відправника, отримувача та місць їх перебування, використовуючи інформацію про передані пакети даних і асоційовані з ними сигнали.

2.4 Атака на основі сліду та вимірювання часу (FATS)

Кібератаки на основі прослуховування, завдяки своїй пасивності, становлять одну з найсерйозніших загроз для кіберфізичних систем. Хоча розроблено чимало криптографічних рішень для захисту комунікацій, вони виявляються недостатніми проти атак, спрямованих на контекстні дані системи. В цій статті ми аналізуємо одну з таких атак, відому як атака на основі сліду та вимірювання часу (FATS) [23]. Цей вид атаки розпочинається з перехоплення сигналів, що випромінюються з розумного будинку, знаходячись неподалік, наприклад, у будинку сусіда, навіть якщо всі дані зашифровані. Після цього алгоритм атаки аналізує зібрані пакети даних, використовуючи їх сигнальні сліди та часові позначки, щоб визначити повсякденні дії мешканців. Це є яскравим прикладом порушення конфіденційності.

Зловмисники, перехопивши дані з домашньої мережі, можуть отримати доступ до чутливої інформації про стиль життя мешканців, їх політичні погляди, фінансовий стан, стан здоров'я, особисте життя, розклади, переваги у покупках тощо. Ця інформація може бути використана для подальших серйозних атак на шкоду жертвам, таких як шантаж, продаж інформації третім особам, тероризм, дифамація або навіть державне стеження.

Реалізація атак FATS включає кілька рівнів, де використовуються техніки машинного навчання, такі як класифікація, кластеризація та відповідність на основі ознак. Атака кластеризує зібрані сигнали на основі їх радіослідів і намагається знайти зв'язок між часовими позначками передачі пакетів даних. Зрештою алгоритм визначає підключені пристрої, кімнати та події вдома; з цього моменту хакер отримує несанкціонований доступ до моніторингу розумного будинку. Чотири рівні цієї атаки охарактеризовані в таблиці 2.1.

Таблиця 2.1 – Рівні атаки FATS [24]

Рівень	Опис	Принципе роботи
0	Визначає розумні пристрої за їх унікальними радіослідами	Слід передачі даних — це набір ознак форми RF-хвилі, які розрізняють джерело сигналів, навіть якщо відправники сигналів мають одного виробника та модель. Атака визначає основні події, такі як зайнятість дому або сон, на цьому етапі.
1	Кластеризує визначені вузли, аналізуючи часові інтервали між передачами сигналів.	Припущення полягає в тому, що пристрої, які фізично розташовані близько один до одного, активуються приблизно в один і той же час. Таким чином, сформовані кластери можуть представляти місцезнаходження їхніх членів, наприклад, кімнату, або їх призначення, наприклад, приготування їжі.
2	Виконує кластеризацію з етикетуванням, використовуючи витягнуті ознаки з сформованих кластерів	цей процес надає пріоритет логічній категоризації, а не розташуванню пристроїв. Наприклад, пральна машина буде позначена як подія прання, хоча вона може знаходитися на кухні чи в підвалі.
3	Проводить ще один раунд класифікації, де алгоритм атаки використовує витягнуті вектори ознак кластерів вузлів та навчальні дані для позначення цих кластерів як пристроїв.	Наприклад, навчена модель атаки очікує, що плита буде на кухні; тому вона перевіряє кластери, розташовані в кластері кухні з вектором ознак плити, витягнутим з фактичного набору даних. У разі

		відповідності невідомий кластер пристрою визначається як плита.

Процедура атаки FATS поєднує кілька статистичних методів та технік машинного навчання для ідентифікації кімнат, пристроїв та подій. Спочатку вона кластеризує записи на основі радіослідів. Потім, використовуючи часові позначки, вона створює тимчасову матрицю, що представляє близькість у часі між передачами. Далі вона перетворює тимчасову матрицю у метричну матрицю відстаней за допомогою алгоритму найкоротшого шляху Дейкстри. Застосовується класичне багатовимірне масштабування без параметрів (CMDS), щоб створити матрицю позицій на основі матриці відстаней [24]. Нарешті, алгоритм кластеризації K-mean групує кластери пристроїв, які часово корелюють. На рисунку 2.3 показана операційна діаграма атак FATS.

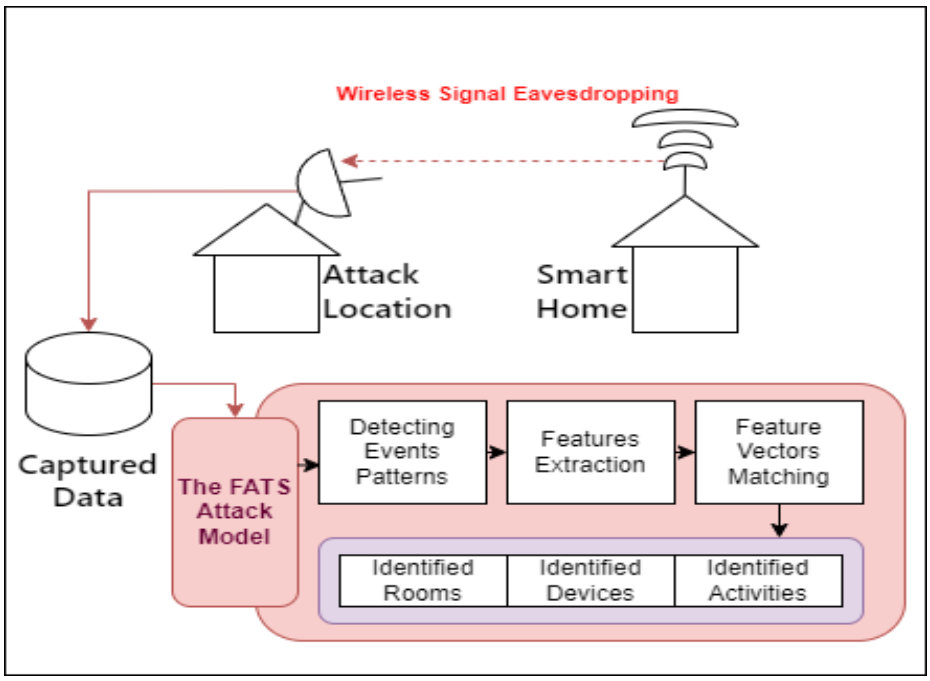

Рисунок 2.3 – Операційна діаграма атак FATS

Атака трансформує введення у геопросторову інформацію пристроїв, після чого спробує ідентифікувати пристрої, кімнати та події, порівнюючи вектори характеристик, що були створені для невідомих груп, з відомими векторами для

своєї моделі, використовуючи певні класифікатори. В результаті, без розкриття секретного ключа шифрування, приватність мешканців успішно порушується. На рисунку 2.4 наведено детальніші відомості про внутрішні процеси атаки FATS.

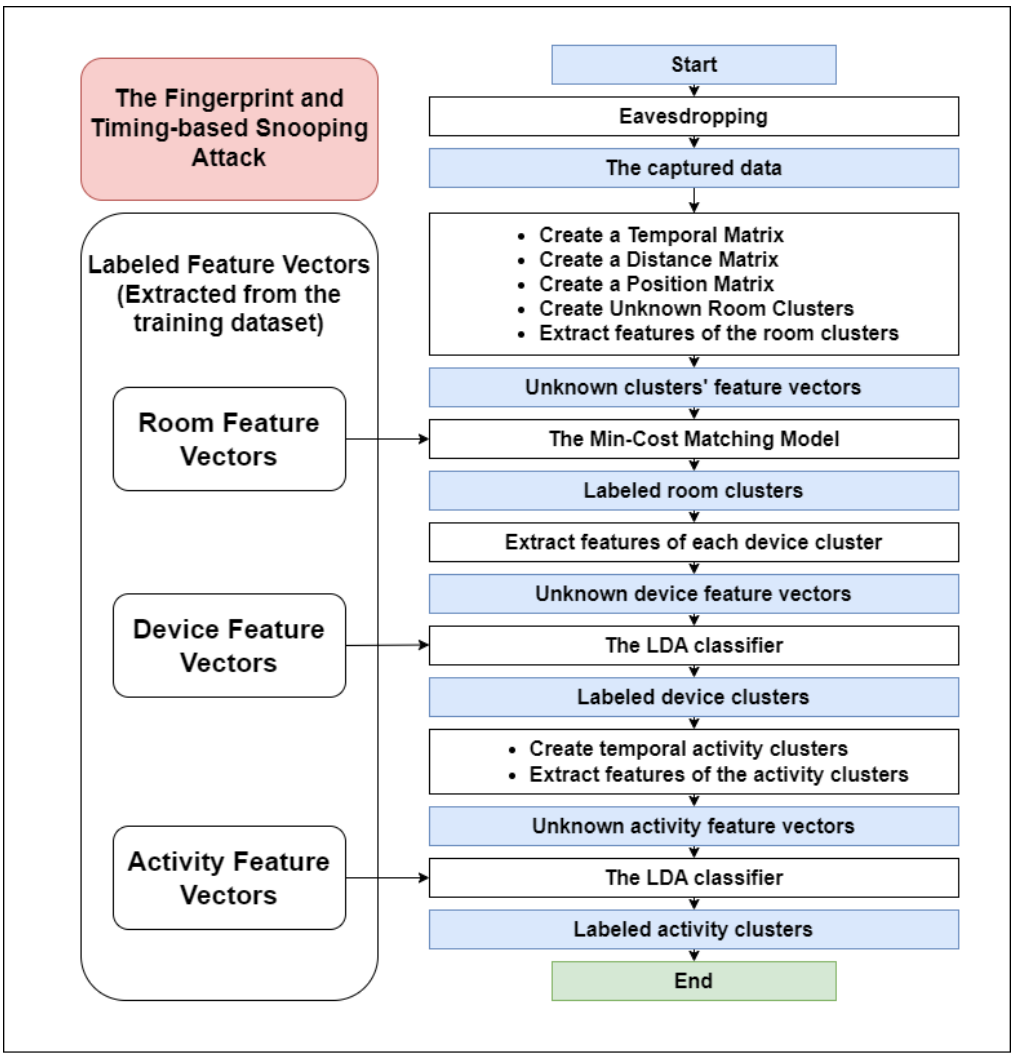

Рисунок 2.4 – Приклад внутрішніх процесів атак FATS

Атака направлена на ідентифікацію кластерів кімнат на наступному рівні, шляхом визначення максимального мінімального значення вартісного двостороннього відображення. Критичні параметри для процесу відповідності включають кількість передач на день з кімнати, загальну кількість передач протягом дня та вночі, середній інтервал між передачами в межах кімнати та середню довжину кластерів часової активності. У наступному етапі атака виявляє пристрої, виділяючи їх особливості, а потім порівнює їх з відомими векторами

ознак для навченої моделі; це виконується за допомогою класифікатора стандартного LDA. Після цього, створення кластерів часової активності для кожного кластера пристроїв призводить до генерації кількох векторів ознак активності. Ці параметри включають час початку, тривалість та кількість передач кожним пристроєм. Вдруге, класифікатор LDA виконує завдання відповідності на невідомих векторах ознак активності, щоб пов'язати їх з позначеним вектором моделі атаки [25]. Завершальним етапом є розкриття атакою ідентичності всіх кімнат, пристроїв та активностей зловмисника; таким чином, вони можуть відстежувати всі домашні активності та отримувати особисту інформацію мешканців.

3 ПРАКТИЧНІ ПОРАДИ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ СИСТЕМИ «РОЗУМНИЙ БУДИНОК»

3.1 Методи захисту мережевого трафіку

Захист мережевого трафіку є критично важливим аспектом інформаційної безпеки в сучасному світі, де кіберзагрози стають все більш складними і поширеними. Основною метою захисту мережевого трафіку є забезпечення конфіденційності, цілісності та доступності даних, що передаються через мережі.

Нижче наведено основні методи захисту мережевого трафіку:

1. Шифрування - є одним з найефективніших методів захисту даних під час їх передачі. Воно передбачає перетворення відкритого тексту в зашифрований текст за допомогою алгоритмів шифрування, які можуть бути симетричними або асиметричними.

- Симетричне шифрування використовує один і той же ключ для шифрування та дешифрування даних. Приклади: AES (Advanced Encryption Standard), DES (Data Encryption Standard).
- Асиметричне шифрування використовує пару ключів: публічний для шифрування і приватний для дешифрування. Приклади: RSA (Rivest-Shamir-Adleman), ECC (Elliptic Curve Cryptography).

2. Віртуальні приватні мережі (VPN) - забезпечують захист трафіку шляхом створення захищених тунелів між клієнтом та сервером. VPN шифрує всі дані, що передаються через мережу, забезпечуючи конфіденційність і цілісність інформації.

- IPsec (Internet Protocol Security) забезпечує захист IP-трафіку через шифрування і автентифікацію.
- SSL/TLS VPN (Secure Sockets Layer/Transport Layer Security)** використовується для захисту веб-трафіку.

3. Файрволи - контролюють та фільтрують мережевий трафік на основі визначених правил безпеки. Вони можуть бути апаратними або програмними і функціонують на різних рівнях мережевої моделі OSI.

- Пакетні фільтри аналізують заголовки пакетів і приймають рішення про пропуск або блокування на основі визначених критеріїв.
- Міжмережеві екрани на рівні додатків (Application-level gateways) аналізують трафік на рівні додатків, забезпечуючи більш детальну перевірку.

4. Системи виявлення та запобігання вторгненням (IDS/IPS) - IDS (Intrusion Detection Systems та IPS (Intrusion Prevention Systems) моніторять мережевий трафік для виявлення підозрілої активності. IDS виявляють та сповіщають про вторгнення, тоді як IPS активно запобігають їх.

- Сигнатурний метод базується на виявленні відомих атак за допомогою сигнатур.
- Аномалічний метод виявляє відхилення від нормальної поведінки в мережі.

5. Протоколи захисту передачі даних використовуються для забезпечення захисту мережевого трафіку на різних рівнях.

- HTTPS (Hypertext Transfer Protocol Secure) забезпечує захист веб-трафіку через шифрування SSL/TLS.
- SSH (Secure Shell) забезпечує захищений канал для віддаленого управління серверами та передачі файлів.
- FTPS (File Transfer Protocol Secure) та SFTP (SSH File Transfer Protocol) забезпечують безпечну передачу файлів.

6. Захист від DDoS атак - DDoS (Distributed Denial of Service) атаки спрямовані на перевантаження мережевих ресурсів. Для захисту від DDoS атак використовуються такі методи:

- Аналіз трафіку для виявлення аномалій та відхилень.
- Розподіл навантаження для зменшення впливу атак.
- Фільтрація трафіку для блокування шкідливих запитів.

7. Політики безпеки та моніторинг - політики безпеки визначають правила і процедури для забезпечення безпеки мережевого трафіку. Моніторинг трафіку дозволяє виявляти потенційні загрози та вживати відповідні заходи.

- SIEM (Security Information and Event Management) системи забезпечують централізований збір і аналіз даних про безпеку.

- Моніторинг журналів дозволяє виявляти підозрілу активність та реагувати на неї.

Захист мережевого трафіку вимагає комплексного підходу, що включає використання шифрування, VPN, файрволів, IDS/IPS систем, безпечних протоколів, захисту від DDoS атак, а також політик безпеки та моніторингу. Ефективне поєднання цих методів дозволяє забезпечити високий рівень безпеки та захистити дані від різноманітних загроз.

3.2 Показники ефективності захисту: EDR та TPR

Збереження конфіденційності у розумних будинках є критично важливим для уникнення непередбачених наслідків можливих витоків даних. Одним з типів атак, які становлять значну загрозу, є атаки типу FATS. Ці атаки дозволяють зловмисникам дізнаватися про приватні аспекти життя мешканців розумного будинку, аналізуючи їхню домашню активність. Основні характеристики цієї атаки можна підсумувати наступним чином:

1. Пасивність атаки - атака виконується пасивно, тобто зловмисники спостерігають за мережею без активного втручання, що робить її вкрай важкою для виявлення під час виконання.
2. Витягування інформації з контекстуальних даних - атака витягує інформацію з контекстуальних даних комунікацій будинку, таких як відбитки сигналів і мітки часу передачі. Це означає, що традиційні методи шифрування не можуть її запобігти.
3. Мінімальні вхідні дані - зловмисний алгоритм потребує мінімум вхідних даних, що включають відбитки сигналів і мітки часу передачі, тому складно заблокувати йому доступ до цих даних.

Зважаючи на неможливість повністю зупинити таку атаку, стає очевидним, що зменшення ризику цієї загрози вимагає впровадження проактивних рішень. Ці рішення повинні забезпечити захист таким чином, щоб патерни трафіку витоку

даних були змінені, що не дозволить зловмисному алгоритму точно їх інтерпретувати.

Дослідження існуючих методів захисту показує, що основна тактика в цих підходах полягає в максимізації затемнення мережевого трафіку. Це ускладнює здатність атаки визначати патерни. Основні методи включають:

1. Тимчасова маніпуляція сигналами - введення затримок або зміна часу передачі сигналів, щоб порушити послідовність подій.
2. Введення випадкових фальшивих пакетів даних - випадкові дані, що вводяться в мережевий трафік, створюють хибні патерни, які зловмисники не можуть правильно інтерпретувати.

Однак, слід зазначити, що такі методи супроводжуються певними витратами для системи. Це може призвести до затримок у комунікаціях або підвищених енергетичних витрат.

Приватність дому обернено пропорційна точності атаки, тому зниження точності атаки означає збільшення приватності. Два основні показники для обчислення точності атаки – це EDR і TPR. EDR вказує на частку правильно виявлених домашніх подій серед усіх фактичних активностей. Наприклад, виявлення 75 подій у будинку з 100 фактичних активностей дає EDR 75%. TPR вказує на відсоток правильності звіту. Наприклад, якщо у списку з 100 подій 60 є помилковими, TPR буде 40%. Точність атаки обчислюється як добуток EDR і TPR, тому в наведеному прикладі точність атаки становить 33,75%.

Моє дослідження наголошує на зниженні EDR атаки як основної мети. Логіка цього вибору проста, але ефективна: якщо атака не виявляє події, вона не може їх ідентифікувати. Результати кількох рецензованих схем захисту, таких як "ConstRate", "ProbeRate" і "FitProbRate", підтримують цей аргумент, забезпечуючи майже ідеальну конфіденційність для домашніх систем. Проте, недоліки цих рішень варто враховувати. Вони змінюють часові кореляції переданих сигналів, затримуючи їх пересилання, що призводить до неприйнятних затримок у реальному часі для домашніх послуг. Це впливає на час реакції систем, чутливих

до затримок, і шкодить їх ефективності, наприклад, у випадку падіння літньої людини, виявлення пожежі або запізнілого виконання розумних замків.

Крім того, приховання фактичних активностей і патернів трафіку вимагає введення численних фальшивих пакетів. Кількість цих пакетів не є детермінованою через вимогу випадковості в процедурах захисту. Результати показали, що для забезпечення відповідної конфіденційності кількість фальшивих пакетів значно перевищує кількість фактичних. У цьому контексті FVR вказує на співвідношення фальшивих пакетів до фактичних. Оскільки передача обох типів пакетів споживає однакові енергетичні ресурси, енергетичні накладні витрати системи можуть бути значними, що підриває доступність рішень.

На відміну від інших методів, метод імітації фактичної діяльності спрямовується на TPR для зменшення точності атаки. Цей метод намагається змусити атаку виявляти якнайбільше активностей, вводячи більше фальшивих патернів активності в кінцевий результат атаки, що знижує TPR. Введення меншої кількості фальшивих пакетів знижує енергетичні витрати системи та усуває затримки у бездротовому зв'язку.

Критичним показником для оцінки методу захисту конфіденційності є компроміс між рівнем конфіденційності, затримкою та енергоспоживанням. Ідеальним методом буде той, який максимізує рівень конфіденційності, утримуючи два інші фактори на найнижчому рівні. На рисунку 3.6 зображено взаємозв'язок між параметрами конфіденційності, затримки та енергоспоживання.

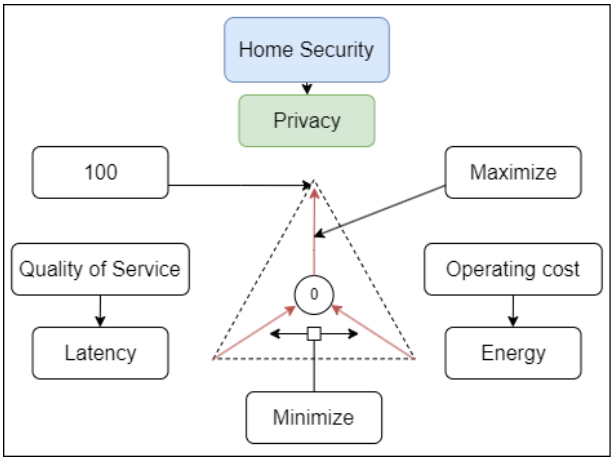

Рисунок 3.6 – Схема взаємозв`язку між параметрами конфіденційності, затримки та енергоспоживання

Перше обґрунтування необхідності врахування цього компромісу полягає в існуванні чутливих до затримок системних підсистем розумного будинку, які повинні відповідати високим вимогам до якості обслуговування. Така чутливість може бути критичною для ефективності різних служб, таких як системи моніторингу здоров'я або аварійного повідомлення. Друге обґрунтування випливає з непередбачуваного зростання операційних витрат, спричиненого значним енергетичним навантаженням, яке виникає через додаткові затримки в передачі даних.

Таблиця 3.1 підсумовує різні методи захисту конфіденційності з точки зору їх підходів до захисту та порівнює їх продуктивність за тріадою параметрів: рівень конфіденційності, затримка комунікації системи та споживання енергії. Варто зазначити, що кожен метод має свої переваги та обмеження. Наприклад, схема ConstRate, яка забезпечує рівномірний розподіл сигналів у мережевому трафіку, ускладнює виявлення часових кореляцій для атак, але може призвести до надмірної затримки. З іншого боку, схема ProbRate, що базується на експоненційному розподілі інтервалів очікування, може зменшити затримки, але вимагає додаткових ресурсів та уваги до регулювання параметрів розподілу.

Ураховуючи потреби систем розумного будинку, де важливо забезпечити швидку реакцію на події та зберігати конфіденційність даних, вибір оптимального методу захисту є завданням, яке вимагає балансу між цими факторами. Результати та аналіз методів, представлених у таблиці, допомагають визначити та підкреслити переваги та обмеження кожного підходу для подальшого вдосконалення та оптимізації систем безпеки розумних будинків.

Таблиця 3.1

Методи збереження конфіденційності

Методи захисту	**Концепція вирішення**	**Конфіденційність**	**Затримка**	**Енергоспоживання**

ConstRate	Випадкове введення фальшивих пакетів зі сталими інтервалами	Висока	Дуже висока	Дуже високе
ProbRate	Випадкове введення фальшивих пакетів із експоненційним скороченням інтервалів	Висока	Висока	Дуже високе
FitProbRate	Випадкове введення фальшивих пакетів із експоненційним скороченням інтервалів	Висока	Висока	Дуже високе
Поведінковий семантичний аналіз	Випадкове введення фальшивих пакетів із використанням найближчих експоненційних інтервалів для фактичного передавання	Середня	Середня	Високе
SDASL	Адаптивне введення фальшивих пакетів	Середня	Середня	Високе
Мімика фактичної активності	Випадкове введення фальшивих активностей	Висока	Низька	Середнє

Висновки з таблиці показують, що кожен метод захисту конфіденційності має свої сильні та слабкі сторони. Методи ConstRate, ProbRate, та FitProbRate забезпечують високу конфіденційність, але мають значну затримку і дуже високе енергоспоживання. Це означає, що вони надійні у захисті даних, але можуть уповільнювати систему та споживати багато енергії.

Поведінковий семантичний аналіз та SDASL пропонують середній рівень конфіденційності та затримки, при цьому їхнє енергоспоживання також високе. Ці методи можуть бути корисними у випадках, коли необхідний баланс між рівнем захисту і продуктивністю системи.

Метод мімики фактичної активності забезпечує високу конфіденційність при низькій затримці та середньому енергоспоживанні. Це робить його ефективним вибором для систем, де важлива швидкість передачі даних і збереження енергії, але при цьому необхідно забезпечити високий рівень захисту.

3.3 Особливості процесу розробки і реалізації програмно-апаратного комплексу «Розумний будинок» на прикладі Arduino

Щоб розпочати роботу з програмно-апаратним комплексом, користувачеві необхідно підключити плату Arduino до маршрутизатора за допомогою Ethernet-шилду. Це важливо для забезпечення можливості дистанційного керування системою через web-інтерфейс. Для доступу до web-інтерфейсу потрібно ввести його адресу в рядок браузера, у нашому випадку це http://192.168.10.101/. Після запуску web-інтерфейсу на екрані користувача з'являється сторінка управління освітленням, навантаженням та індикацією сигналізації (рис. 3.7).

На цьому етапі користувач може вибрати один із цікавих розділів для подальшого управління: освітлення або навантаження. Інтерфейс надає зручний доступ до всіх необхідних функцій, дозволяючи користувачеві легко налаштовувати і контролювати різні аспекти системи. Зокрема, можливості управління освітленням включають вмикання та вимикання світла, регулювання яскравості та налаштування таймерів. Управління навантаженням дозволяє контролювати підключені електроприлади, вимірювати їх споживання та встановлювати відповідні параметри роботи.

Користувач може легко перейти між різними розділами web-інтерфейсу, отримуючи повний контроль над системою з будь-якого пристрою, підключеного до локальної мережі. Цей підхід забезпечує високу гнучкість та ефективність в управлінні системою, роблячи її зручною та доступною для всіх користувачів.

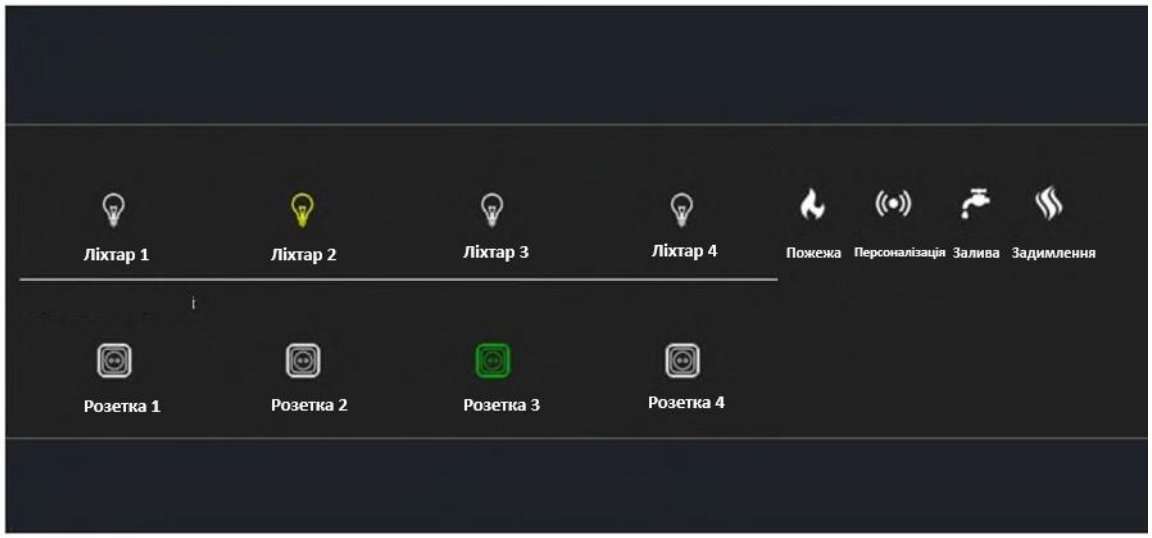

Рисунок 3.7 – Сторінка web-сервісу з індикацією

На сторінці веб-ресурсу представлено кілька основних розділів, що охоплюють різні аспекти управління системами. Перший розділ присвячений управлінню освітленням, де користувачі можуть знайти інформацію про способи налаштування та контролю освітлювальних приладів. Другий розділ зосереджений на управлінні навантаженням, що включає в себе можливості моніторингу та регулювання споживання електроенергії для оптимізації роботи систем. Останній розділ стосується сигналізації, де детально описані функції та можливості системи оповіщення про різні події або загрози. Кожен розділ надає детальну інформацію та керівництво для ефективного використання відповідних функцій.

За управління освітленням та навантаженням на платі Arduino відповідають цифрові виходи з 22 по 29. Виходи пінів реалізовані таким чином:

```
pinMode(22, UTPUT);
pinMode(23, OUTPUT);
pinMode(24, OUTPUT);
pinMode(25, OUTPUT);
pinMode(26, OUTPUT);
pinMode(27, OUTPUT);
 pinMode(28, OUTPUT);
pinMode(29, OUTPUT);
```

За сигналізацію відповідають цифрові входи з 46 до 49. Приклад реалізації:

```
pinMode(46, INPUT);
digitalWrite(46, HIGH);
 pinMode(47, INPUT);
digitalWrite(47, HIGH);
pinMode(48, INPUT);
digitalWrite(48, HIGH);
pinMode(49, INPUT);
digitalWrite(49, HIGH);
```

У даному web ресурсі зображення кнопок та індикацій реалізована завантаженням з web ресурсу. Приклад завантаження картинок:

```
if (_gtv11)
{
_swi8 =
String("http://provuz22.ru/arduino/rozetka1.png");
}
```

```
else
{
 _swi8 = String("http:// provuz22.ru/arduino
 /rozetka0.png");
}
```

У нашому випадку rozetka0-це вимкнений стан, а rozetka1 - включене. Всі інші кнопки реалізовані за тим самим принципом. Індикація зображена рис. 3.8.

Рисунок 3.8 – Приклад стану модулів увімк/викл

У представленому проекті для реалізації веб-сервера використовується шилд Arduino W5100. Для створення веб-сервісу необхідно вказати бібліотеки, що використовуються для управління Ethernet.

Крім того, важливо налаштувати мережевий пристрій, для чого вказується MAC-адреса. Обрана MAC-адреса не повинна збігатися з MAC-адресами інших мережевих пристроїв у вашій мережі. Так само і IP-адреса повинна бути унікальною, але перебувати у межах вашої підмережі. Наприклад, у проектованій системі роутер має IP-адресу 192.168.0.1, а ПК – 192.168.0.4. Виходячи з цього, даний пристрій може мати IP-адресу 192.168.0.101.

Ці налаштування дозволять коректно інтегрувати пристрій у вашу мережу, забезпечуючи його безперебійну роботу в якості веб-сервера.

Далі потрібно вказати порт. За замовчуванням це 80 , тому що веб-браузер за промовчанням опитують саме його. Приклад коду:

```
byte ethernet_mac [] = {0x78, 0xAC, 0xC0,
0x90, 0x04, 0x30}; IPAddress
ethernet_ip(192, 168, 10, 101);
byte ethernet_dns [] = {192, 168, 10, 1};
byte ethernet_gateway [] = {192, 168, 10, 1};
byte ethernet_subnet [] =
{255, 255, 255, 0};
```

```
EthernetServer
_tspWebServer(80);
```

На нашому web-ресурсі частина сторінки, де знаходиться сигналізація оновлюється раз на 10 секунд. Це зроблено для зручності, щоб щоразу не оновлювати сторінку вручну.

Схема підключення Arduino для керування електронними системами будинку показано на рис. 3.9.

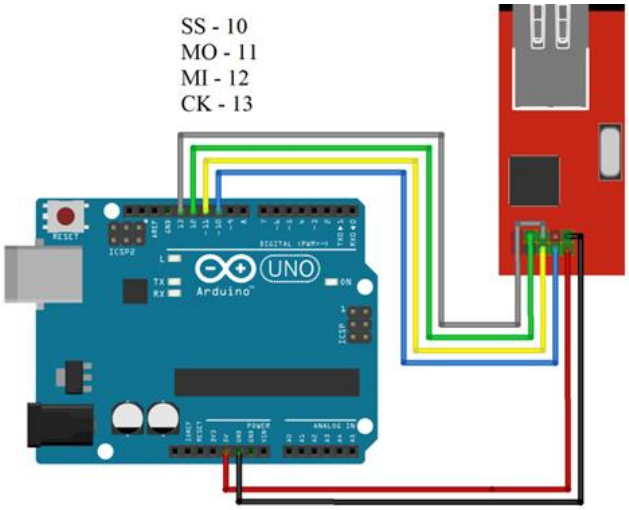

Рисунок 3.9 – Схема підключення Arduino

Підключення Ethernet шилду до Arduino mega 2560 показано на рис. 3.10.

Також варто відзначити, що в нашій програмі передбачено розширення системи розумного будинку, для цього в коді програми оголошено змінні, які при потребі можна задіяти.

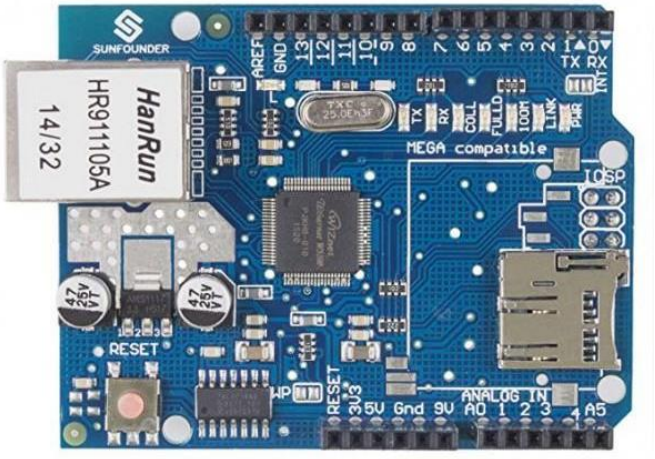

Рисунок 3.10 – Ethernet шилд + Arduino Mega 2560

Розглянемо варіант підключення для керування системою віддалено. Для початку Користувачеві необхідно зареєструватися на сайті noip.com. Реєстрація потрібна для щоб тільки ви могли редагувати адресу призначення web ресурсу. Після реєстрації на сайті слід перейти до розділу Dynamic DNS. У цьому розділі додається ip-адреса розробленого web-ресурсу (рис. 3.11).

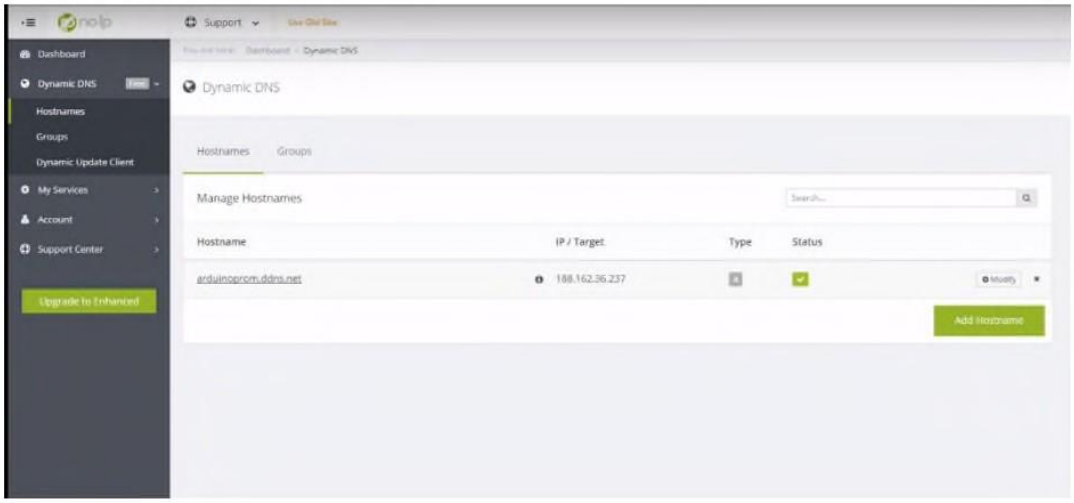

Рисунок 3.11 – Приклад додавання IP-адреси

Після складання макету системи «розумного будинку» на платі Arduino Mega 2560 та Ethernet шилда w5100 було проведено налагодження програмного коду та подальше тестування даного макету. В процесі тестування програмно-апаратного комплексу було виявлено кілька недоліків. Основним з них є відсутність безпеки при використанні віддаленого управління системою. Це пов'язано з тим, що

сторінка управління не має аутентифікації, і будь-яка особа, знаючи IP-адресу обладнання, може втрутитися в роботу системи. Також було виявлено недолік у вигляді необхідності вручну оновлювати сторінку для побачення індикації сигналізації. Цей недолік було виправлено шляхом оновлення блоку сигналізації кожні 10 секунд, використовуючи наступний код:

```
`_tspWebServer_client.println(""meta
http=Refresh""content =""10"" />);`.
```

Для налаштування маршрутизатора, необхідно зайти в його налаштування. Це здійснюється шляхом введення IP-адреси маршрутизатора у веб-браузері, наприклад, 192.168.0.1. Однак, адреса налаштувань може бути іншою, залежно від провайдера та моделі маршрутизатора. У налаштуваннях маршрутизатора потрібно обрати розділ "Налаштування локальної мережі" і вказати MAC та IP-адреси пристрою, що підключається. Ці дані беруться з вихідного коду:

```
```cpp
byte ethernet_mac [] = {0x78, 0xAC, 0xC0, 0x90, 0x04,
0x30};
IPAddress ethernet_ip(192, 168, 10, 101);
byte ethernet_dns [] = {192, 168, 10, 1};
byte ethernet_gateway [] = {192, 168, 10, 1};
byte ethernet_subnet [] = {255, 255, 255, 0};```
```

Після налаштування маршрутизатора система може керуватися віддалено. Великим недоліком віддаленого управління є відсутність безпеки. Це означає, що будь-який користувач, який знає IP-адресу веб-ресурсу, може керувати створеною системою.
```

ВИСНОВКИ

Захист мережевого трафіку є критично важливим аспектом інформаційної безпеки в сучасному світі, де кіберзагрози стають все більш складними і поширеними. Основною метою захисту мережевого трафіку є забезпечення конфіденційності, цілісності та доступності даних, що передаються через мережі.

Одним із найефективніших методів захисту даних під час їх передачі є шифрування, яке передбачає перетворення відкритого тексту в зашифрований текст за допомогою алгоритмів шифрування, що можуть бути симетричними або асиметричними. Симетричне шифрування використовує один і той же ключ для шифрування та дешифрування даних, прикладами є AES та DES. Асиметричне шифрування використовує пару ключів: публічний для шифрування і приватний для дешифрування, прикладами є RSA та ECC.

Віртуальні приватні мережі (VPN) забезпечують захист трафіку шляхом створення захищених тунелів між клієнтом та сервером. VPN шифрує всі дані, що передаються через мережу, забезпечуючи конфіденційність і цілісність інформації. Прикладами є IPsec, що забезпечує захист IP-трафіку через шифрування і автентифікацію, та SSL/TLS VPN, що використовується для захисту веб-трафіку.

Файрволи контролюють та фільтрують мережевий трафік на основі визначених правил безпеки. Вони можуть бути апаратними або програмними і функціонують на різних рівнях мережевої моделі OSI. Пакетні фільтри аналізують заголовки пакетів і приймають рішення про пропуск або блокування на основі визначених критеріїв, а міжмережеві екрани на рівні додатків аналізують трафік на рівні додатків, забезпечуючи більш детальну перевірку.

Системи виявлення та запобігання вторгненням (IDS/IPS) моніторять мережевий трафік для виявлення підозрілої активності. IDS виявляють та сповіщають про вторгнення, тоді як IPS активно запобігають їх. Сигнатурний метод базується на виявленні відомих атак за допомогою сигнатур, а аномалічний метод виявляє відхилення від нормальної поведінки в мережі.

Безпечні протоколи використовуються для забезпечення захисту мережевого трафіку на різних рівнях. HTTPS забезпечує захист веб-трафіку через шифрування SSL/TLS, SSH забезпечує захищений канал для віддаленого управління серверами та передачі файлів, FTPS та SFTP забезпечують безпечну передачу файлів.

Захист від DDoS атак включає аналіз трафіку для виявлення аномалій та відхилень, розподіл навантаження для зменшення впливу атак та фільтрацію трафіку для блокування шкідливих запитів.

Політики безпеки визначають правила і процедури для забезпечення безпеки мережевого трафіку. Моніторинг трафіку дозволяє виявляти потенційні загрози та вживати відповідні заходи. Системи SIEM забезпечують централізований збір і аналіз даних про безпеку, а моніторинг журналів дозволяє виявляти підозрілу активність та реагувати на неї.

Захист мережевого трафіку вимагає комплексного підходу, що включає використання шифрування, VPN, файрволів, IDS/IPS систем, безпечних протоколів, захисту від DDoS атак, а також політик безпеки та моніторингу. Ефективне поєднання цих методів дозволяє забезпечити високий рівень безпеки та захистити дані від різноманітних загроз.

ПЕРЕЛІК ПОСИЛАНЬ

1. Ярмакі Х.П., Музика С.С. Класифікація конфіденційної інформації // *Південноукраїнський правничий часопис*. 2021. № 1. С. 94 - 98.
2. Scientific Collection «InterConf» : with the Proceedings of the 5 th International Scientific and Practical Conference «Theory and Practice of Science: Key Aspects» (November 7-8, 2021). Rome, Italy: Dana, 2021. 478 p.
3. Залужний, В. В. Модель контролю доступу для забезпечення безпеки «розумного будинку» = Access Control Model for Smart Home Security / Василь Вікторович Залужний ; наук. керівник д.т.н., проф. М. М. Касянчук. Тернопіль : ЗУНУ, 2023. 63 с.
4. Поняття та класифікація інформації. URL: http://moodle.nati.org.ua/mod/book/view.php?id=5283
5. Мірошниченко А. А.Світ гібридів як небезпека від штучного інтелекту. *Освітня робототехніка*: зб.наук.пр.за матеріалами II Всеукр. наук.-практ. конф. м. Дніпро. 14 квітня 2022 р. Дніпро, 2022С. 150-155.
6. Гевко В. Класифікація інформаційних систем управління взаємовідносинами з клієнтами / В. Гевко // *Соціально-економічні проблеми і держава*. 2013. Вип. 2 (9). С. 44–57
7. Чумак Д. С. Властивості та функції інформаційних систем. *Сучасні напрямки розвитку економіки і менеджменту на підприємствах України*: зб. матеріалів IV всеукр. наук.-практ. конф. студентів, аспірантів та молодих вчених, м. Харків, 28 листопада 2018 року. Харків, ХНАДУ, 2018. С. 195-198.
8. Зелінська О.В., Потапова Н.А., Волонтир Л.О. Інформаційні системи та технології в галузі. навч. посіб. / О.В. Зелінська, Н.А. Потапова, Л.О. Волонтир, - Вінниця: ВНАУ, 2020. 263 с.
9. Тулуб В .О. Методи підвищення рівня ефективності роботи автоматизованих систем. Системні технології. Регіональний міжвузівський збірник наукових праць. Дніпро, 2023. Вип.4 (147). С. 91-98.

10. Черкашин І. С. Розроблення системи розпізнавання команд на основі технології захвату рухів для інтелектуального керування мобільним роботом. Харків. нац. ун-т радіоелектроніки. Харків, 2022. 67 с.
11. Алексов, С. і Дідик, А. Перспективи впровадження системи ‘розумний дім’ у заклади освіти, *Трансформаційна економіка*, 2023. №2 (02), с. 5-9.
12. Інформаційна безпека та інформаційні технології: збірник тез доповідей : матеріали IV Міжнар. наук.-практ. конф. м. Львів, 30 листопада 2022 року. Львів: Растр-7, 2022. 380 с.
13. The 4 th International scientific and practical conference ―Priority directions of science and technology development‖ (December 20-22, 2020) SPC ―Sci-conf.com.ua‖, Kyiv, Ukraine. 2020. 1472 p.
14. Дяченко О. С. Аналіз сучасних розробок в області розумного будинку / Є. С. Дяченко. *Автоматизація та розробка електронних пристроїв ADED-2023*: зб. студ. наук. праць. Харків : Вид-во Харківського національного університету радіоелектроніки, 2023. Ч. 1. С. 15-18.
15. Розумний будинок: переваги та недоліки. URL: https://buduemo.com/ua/news/smart_systems/what-is-a-smart-home.html
16. Van der Sloot B. Where is the harm in a privacy violation. URL: https://heinonline.org/HOL/LandingPage?handle=hein.journals/jipitec8&div=38&id= &page=
17. Fafoutis X., Marchegiani L., Papadopoulos G.Z., Piechocki R., Tryfonas T., Oikonomou G. Privacy leakage of physical activity levels in wireless embedded wearable systems. URL: https://ieeexplore.ieee.org/abstract/document/7792352
18. Boerman S.C., Kruikemeier S., Zuiderveen Borgesius F.J. Exploring motivations for online privacy protection behavior: Insights from panel data. URL: https://journals.sagepub.com/doi/full/10.1177/0093650218800915
19. Shouran Z., Ashari A., Priyambodo T. Internet of things (IoT) of smart home: Privacy and security. URL: https://www.researchgate.net/profile/ZaiedShouran/publication/331133954_Internet_of_Things_IoT_of_Smart_Home_Privacy_

and_Security/links/5c692af14585156b57016c66/Internet-of-Things-IoT-of-SmartHome-Privacy-and-Security.pdf

20. Conti M., Nati M., Rotundo E., Spolaor R. Mind the plug! laptop-user recognition through power consumption. pp. 37–44. URL: https://dl.acm.org/doi/abs/10.1145/2899007.2899009
21. Kocher P., Jaffe J., Jun B., Rohatgi P. Introduction to differential power analysis. URL: https://link.springer.com/article/10.1007/s13389-011-0006-y
22. Li Y., Chen M., Wang J. Introduction to side-channel attacks and fault attacks. pp. 573–575. URL: https://ieeexplore.ieee.org/abstract/document/7522801
23. Srinivasan V., Stankovic J., Whitehouse K. Protecting your daily inhome activity information from a wireless snooping attack. pp. 202–211. URL: https://dl.acm.org/doi/abs/10.1145/1409635.1409663
24. Saeed N., Nam H., Haq M.I.U., Muhammad Saqib D.B. A survey on multidimensional scaling. URL: https://dl.acm.org/doi/abs/10.1145/3178155
25. Balakrishnama S., Ganapathiraju A., Picone J. Linear discriminant analysis for signal processing problems. pp. 78–81. URL: https://ieeexplore.ieee.org/abstract/document/766096