ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи

на тему:

«ТЕХНОЛОГІЯ ВИЯВЛЕННЯ ТА ЗАХИСТ ВІД КІБЕРАТАКИ В РОЗУМНОМУ БУДИНКУ. ЕКОСИСТЕМА ІНТЕРНЕТУ РЕЧЕЙ»

Виконав: студент 6 курсу, групи БСДМ-61
Спеціальності 125 Кібербезпека
Освітньо-професійної програми
«Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
_____Кузьменко О.Д._____
(прізвище та ініціали)

Керівник Борсуковський Ю.В._____
(прізвище та ініціали)

Рецензент _____
(прізвище та ініціали)

Нормоконтролер____Чумак Н.С._____
(прізвище та ініціали)

КИЇВ – 2022

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Інститут ННІЗІ
Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Г.І. Гайдур
«___» _____ 2022 року

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

Кузьменку Олександру Дмитровичу
(прізвище, ім'я, по батькові)

1. Тема магістерської роботи: «Технологія виявлення та захист від кібератаки в розумному будинку. Екосистема Інтернету речей»
керівник магістерської роботи Борсуковський Юрій Володимирович, к.т.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від «12»жовтня 2022 року № 122
2. Строк подання студентом магістерської роботи 15.12.2022 р.

3. Вихідні дані до магістерської роботи:

1. корпоративна інформаційна система;
2. наукова та технічна література;
3. експлуатаційна документація;
4. нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Аналіз сучасного стану захисту інформаційної безпеки та виявлення кібератаки в мережі IoT.
2. Дослідження методів та засобів захисту від кібератак мережі IoT.
3. Інтеграції та реалізація системи інформаційної безпеки в розумному будинку.

5. Перелік графічного матеріалу (презентація):

1) Об’єкт, предмет, мета дослідження, завдання дослідження;
2)
3)
4)
5)
6)
7)
8)
9) Висновки

6. Дата видачі завдання 13.10.2022

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської роботи	Строк виконання етапів магістерської роботи	Примітка
1.	Аналіз науково-технічної літератури.	13.10.2022 р.	виконано
2.	Дослідження функціональних особливостей та принципів роботи мережі IoT.	15.10.2022 р.	виконано
3.	Технології забезпечення безпеки та засобів захисту від кібератак мережі IoT.	08.11.2022 р.	виконано
4.	Налаштування можливостей концепції системи інформаційної безпеки в розумному будинку	20.11.2022 р.	виконано
5.	Оформлення результатів дослідження. Проходження плагіату.	05.12.2022 р.	виконано
6.	Підготовка доповіді до захисту.	15.12.2022 р.	виконано

Студент _____ Кузьменко О.Д.
(підпис) (прізвище та ініціали)

Керівник магістерської роботи _____ Борсуковський Ю.В.
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Текстова частина магістерської роботи: 80 сторінок, 20 рисунків, 70 джерел.

Об'єкт дослідження – безпека систем IoT.

Предмет дослідження – методи та засоби захисту систем Розумного дому від атак.

Мета роботи – розробка практичного рішення щодо побудови системи захисту комплексів Розумного дому та аналіз можливих ризків.

Методи дослідження – аналіз експлуатаційної документації, теорія складних систем, теорія алгоритмів та масового обслуговування, аналіз міжнародних стандартів, проведення дослідження за допомогою спеціального ПЗ.

Вивчено, в якому ступені систем розумних будинків захищені, щоб сприяти розвитку та поширенню. Проведено оцінювання наявності можливостей IoT з точки зору систем розумних будинків і то, як їх безпеку може бути посилено, щоб дійсно сприяти їх ефективному використанню.

Проаналізовано всі вразливості та загрози еталонної архітектури Розумного будинку, після чого вона була вдосконалена, та було запропоновано вимоги безпеки.

Використано спеціалізоване програмне забезпечення для розпізнавання зловмисників та складні зразки шкідливого програмного забезпечення, включаючи MITB, ін'єкції шкідливих сценаріїв або спроби автоматизованих передач.

Галузь використання – інформаційна безпека.

РОЗУМНИЙ БУДИНОК, IOT, ІНФОРМАЦІЙНА БЕЗПЕКА, АТАКИ, ЗАГРОЗИ, ШИФРУВАННЯ, ІНТЕРНЕТ.

6

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІТ – Інформаційні технології

ОС – Операційна система

ПЗ – Програмне забезпечення

ПК – Персональний комп’ютер

БД – База даних

API – (англ. Application Programming Interface) Прикладний програмний інтерфейс.

IoT – (англ. Internet of Things) Інтернет речей.

IPS – система запобігання вторгненням

RFID – (англ.Radio Frequency Identification) радіочастотна ідентифікація

GPS – (англ.Global Positioning System) глобальна система позиціонування

HAN – Home area network

LAN – Local Area Network

PAN – Personal Area Network

BAN – Body Area Network

WSN – Wireless sensor networks

SHEMS – Smart home energy management systems

HEMS – Home Energy Management System

SM – Smart Meters

SAU – Sensor or Actuator Unit

MCU – Microcontroller Unit

COM – Communication module

АЦП – аналого-цифровий перетворювач

ВСТУП

Актуальність дослідження. Сьогодні будь-який будинок можна легко модернізувати за допомогою персоналізованих, доступних та потенційно "інтелектуальних" пристроїв. Розумний будинок можна визначити як місце проживання, яке містить багато датчиків, систем та пристроїв, до яких можна віддалено доступитись, керувати та контролювати через мережу зв'язку [2]. Згідно з недавнім дослідженням [3], глобальний ринок інтелектуальних будинків у 2020 році оцінюється в 9,8 мільярда доларів і, за оцінками, досягне 43 мільярдів доларів у 2023 році. Згідно з іншим дослідженням [4], ринок інтелектуальних будинків, як очікується, подвоїться в США, оскільки безпека сім’ї є найбільшим мотиватором.

Проте зростаюче розгортання пристроїв, підключених до Інтернету, у домашніх умовах ставить під загрозу конфіденційність та безпеку, оскільки особиста інформація стає віддалено доступною новими способами. Зловмисник, наприклад, може підслуховувати бездротові передачі датчиків та виявляти такі дії, як приймання душу, туалет та сон [5]. Крім того, зловмисник може дистанційно перебирати контроль над домашніми пристроями, використовуючи їх, щоб зламати домогосподарство або як платформу для запуску атак на інші домени, наприклад, перевантажити енергосистему. Було проведено успішні атаки на різні комерційні продукти із незавершеного виробництва [6-8]. Ці напади не тільки гіпотетичні: наприклад, у 2021 році було виявлено, що дані з понад 73 000 відеокамер доступні в Інтернеті.

Ступінь наукової розробки: удосконалено застарілу архітектуру для додатків «інтернет речей», що надає можливість моніторингу розумного будинку та вбереження його від кібератаки..

Метою роботи є дослідження технології виявлення та захист від кібератаки в розумному будинку.

Для досягнення поставленої мети вирішуються такі *задачі:*

- Ознайомитися з теоретичними відомостями про технології виявлення кібератаки в розумному будинку;
- розглянути екосистеми «інтернет речей»;
- проаналізувати методи та засоби захисту від кібератак в розумному будинку;
- дослідити процес реалізації системи інформаційної безпеки в розумному будинку;
- розробити систему інформаційної безпеки.

Об'єктом дослідження є розумний будинок.

Предметом дослідження є кібератака в розумному будинку на основі інтернет речей.

Методи дослідження: теоретичні методи дослідження; сучасні програмні засоби проектування та дослідження; методи оцінки ефективності та моделювання.

Практичне значення одержаних результатів.: результати дослідження можуть бути використані як основа для покращення вимог безпеки розумних будинків на основі IoT.

Магістерська робота складається з вступу, трьох розділів, висновків, списку використаних джерел (70 найменувань). Робота містить 35 рисунків. Основний зміст викладено на 69 сторінках тексту. Загальний обсяг – 80 сторінок.

1 ТЕОРЕТИЧНІ ВІДОМОСТІ ПРО ТЕХНОЛОГІЇ ВИЯВЛЕННЯ КІБЕРАТАКИ В РОЗУМНОМУ БУДИНКУ ТА ЕКОСИСТЕМИ «ІНТЕРНЕТ РЕЧЕЙ»

1.1. Огляд інтернету речей

Інтернет речей (IoT) - це мережа фізичних об'єктів або людей, які називаються "речами", вбудованими в програмне забезпечення, електроніку, мережу та датчики, що дозволяє цим об'єктам збирати та обмінюватися даними. Мета IoT - розширити можливості підключення до Інтернету від стандартних пристроїв, таких як комп’ютер, мобільний телефон, планшет, до відносно німих пристроїв, таких як тостер.

Термін «Інтернет речей» був введений Кевіном Ештоном, який обговорював можливість пов’язати нову на той час ідею технології RFID у ланцюгах поставок з Інтернетом. З того часу та з розвитком технологій визначення IoT розвинулося до опису ширшого спектру застосувань у різних сферах, таких як транспорт і охорона здоров’я. Сьогодні IoT використовується для опису пов’язаної з речами екосистеми електронних пристроїв, у які вбудовано програмне забезпечення, датчики, виконавчі механізми та підключення до мережі, що дозволяє їм підключатися та обмінюватися даними з середовища без втручання людини. Пристрої Інтернету речей, такі як розумні та переносні пристрої, побутова техніка, а також системи сигналізації та камери, забезпечують різноманітні функції, які автоматизують і підтримують наші повсякденні дії та потреби. Завдяки повсюдному зв’язку, який дозволяє їм спілкуватися та обмінюватися інформацією з іншими технологіями, їхній інтелект і здатність приймати рішення викликають дії, різко зросла кількість розумних пристроїв. Дослідницький відділ Statista прогнозує, що до 2025 року в усьому світі буде підключено понад 75 мільярдів пристроїв IoT, що перевищить кількість персональних комп’ютерів і смартфонів разом

узятих[209].малюнок2.1ілюструє збільшення кількості підключених пристроїв IoT на рік між 2015 і 2025 роками.

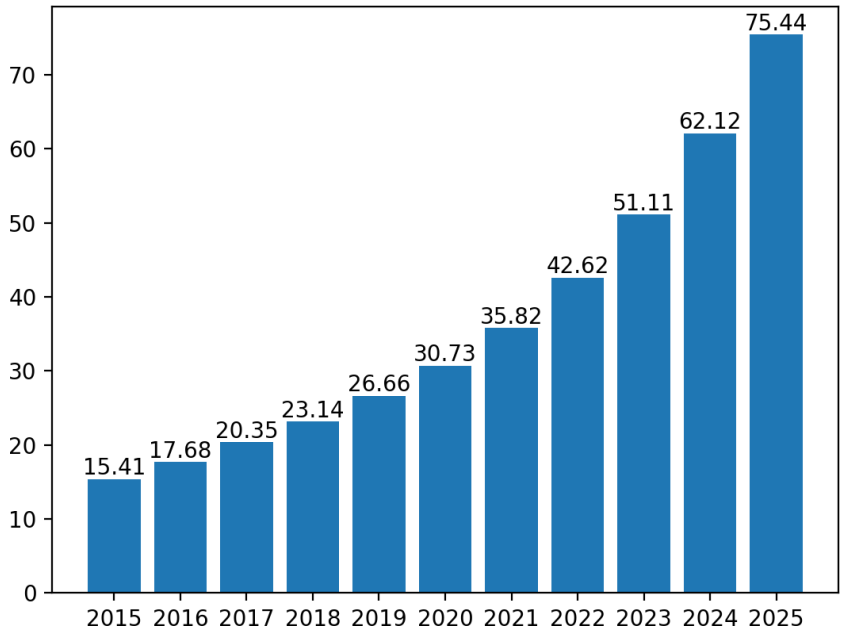

Рисунок 1.1. Збільшення кількості підключених пристроїв IoT на рік

Пристрої IoT можуть бути вбудовані в кілька різних доменів. Подібні пристрої широко використовуються, зокрема, в побутових умовах. Одним із найпопулярніших застосувань IoT є розумні будинки. Розумна побутова техніка включає розумні термостати, освітлення, лічильники та замки, якими можна дистанційно керувати зі смартфона чи ноутбука. Користувачі можуть контролювати використання таких пристроїв, надаючи більше інформації та дозволяючи користувачеві приймати більш обґрунтоване рішення щодо того, коли змінити таке використання. Наприклад, користувач може захотіти запланувати відключення системи опалення після досягнення певної температури, щоб заощадити енергію та гроші. Інші пристрої можуть включати розумні фітнес-трекери та переносні пристрої, такі як Fitbit, які дозволяють користувачам відстежувати свої фізичні рухи, щоб вимірювати та встановлювати особисті фітнес-цілі. Однак використання пристроїв IoT не обмежується розумними будинками та носимими пристроями. Інфраструктури IoT стали рушійною силою розвитку взаємопов’язаного світу,

заснованого на знаннях; наші економіки, суспільства, урядовий механізм та CNI. Сюди входять концепції, які можуть бути необхідними для функціонування країни і від яких залежить наше повсякденне життя, такі як розумні міста, інтелектуальні транспортні системи, розумні електромережі та системи охорони здоров'я. Наприклад, інтелектуальні лічильники та регулятори енергії вбудовані в інтелектуальну мережу для вимірювання енергетичних тенденцій з метою ефективного розподілу енергії між попитом[63]. Таким чином, очевидно, що IoT змінює спосіб роботи таких доменів, надаючи більш точні та автоматизовані вимірювання та функції в реальному часі.

Концепція інфраструктури IoT настільки ж потужна, наскільки й складна. IoT відноситься до широкої та різноманітної екосистеми, яка включає широкий спектр пристроїв, програм, протоколів і випадків використання. У результаті, щоб краще зрозуміти, як працює екосистема IoT, такі інфраструктури розділені на сім ключових рівнів:

1. Фізичні пристрої та контролери (рівень сприйняття)- Це найнижчий рівень в архітектурі екосистеми IoT. Він складається з ряду різних датчиків і пристроїв, які відповідають за збір інформації з навколишнього середовища.

2. Підключення (комунікаційний рівень)- Це базовий рівень у системі IoT, який відповідає за підключення датчиків, мережевих пристроїв і серверів. На цьому рівні використовуються різні типи технологій, такі як Wi-Fi, WAN, локальна мережа(LAN),4G, 5G, LoRA тощо.

3. Граничні обчислення (Cloud Edge або Gateway)- Цей рівень інтерфейсує дані та контрольні площини до вищих рівнів хмари або програмного забезпечення. На цьому рівні реалізовано перетворення протоколів, маршрутизацію до функцій програмного забезпечення вищого рівня та логіку «швидкого шляху» для прийняття рішень із низькою затримкою.

4. Накопичення даних (рівень проміжного ПЗ)- Цей рівень відповідає за зберігання, аналіз і обробку даних, отриманих від датчиків і пристроїв.

5. Абстракція даних- На цьому рівні дані, зібрані з датчиків, організовуються та попередньо обробляються, щоб мати можливість використовувати їх для подальшої обробки.

6. застосування- Цей рівень розташований у верхній частині архітектури та відповідає за надання користувачам послуг, що стосуються конкретної програми. Крім того, він визначає різні домени, в яких можна розгортати IoT.

7. Співпраця та обробка- На цьому рівні оброблені дані на нижніх рівнях інтегруються в бізнес-додатки. Основним завданням тут є ефективне використання цінності IoT та його послуг і перетворення цього на економічне зростання, ефективне прийняття рішень та оптимізацію бізнесу.

1.2. Принципи проектування мережі «розумний дім»

«Розумний дім» це зручне домашнє середовище, в якому приладами та пристроями можна дистанційно керувати з будь-якого місця через Інтернетз'єднання за допомогою мобільного або іншого мережевого пристрою. Пристрої розумного будинку взаємопов’язані через Інтернет, що дозволяє користувачеві керувати такими функціями, як безпечний доступ до будинку, температура, освітлення, домашній кінотеатр та ін. [6].

Пристрої розумного будинку пов’язані між собою і доступ до них можна отримати через одну центральну точку - смартфон, планшет, ноутбук або ігрову консоль. Замками дверей, камерами відеоспостереження, системою клімат контролю, освітленням та навіть такими приладами, як холодильник та пральна машина, можна керувати за допомогою однієї системи домашньої автоматизації. Система встановлюється на мобільному або іншому

мережевому пристрої, і користувач може створювати графіки часу для вступу в силу певних змін.

Розумні побутові прилади мають навички самонавчання, щоб вони могли вивчити графіки власника дому та вносити коригування за потребою. Розумні будинки, що підтримують керування освітленням, дозволяють власникам будинків зменшити споживання електроенергії та отримати вигоду від економії витрат на енергію. Деякі системи домашньої автоматизації сповіщають власника будинку про виявлення будь-якого руху в будинку, коли він відсутній, а інші можуть викликати - поліцію чи пожежну службу у разі невідкладних ситуацій. «Розумний будинок» є частиною технології «Інтернету речей» (IoT) [6].

Зразок топології IoT наведено на рис.1.1. Пристрої можуть бути пов’язані між собою за допомогою дротового та бездротового зв’язку. Бездротові системи простіше інсталювати, що знижує вартість реалізації. З іншого боку, дротові системи вважаються більш надійними, але є і недолік – вища ціна. Встановлення такої системи може обійтися власникам будинків у десятки тисяч доларів [2].

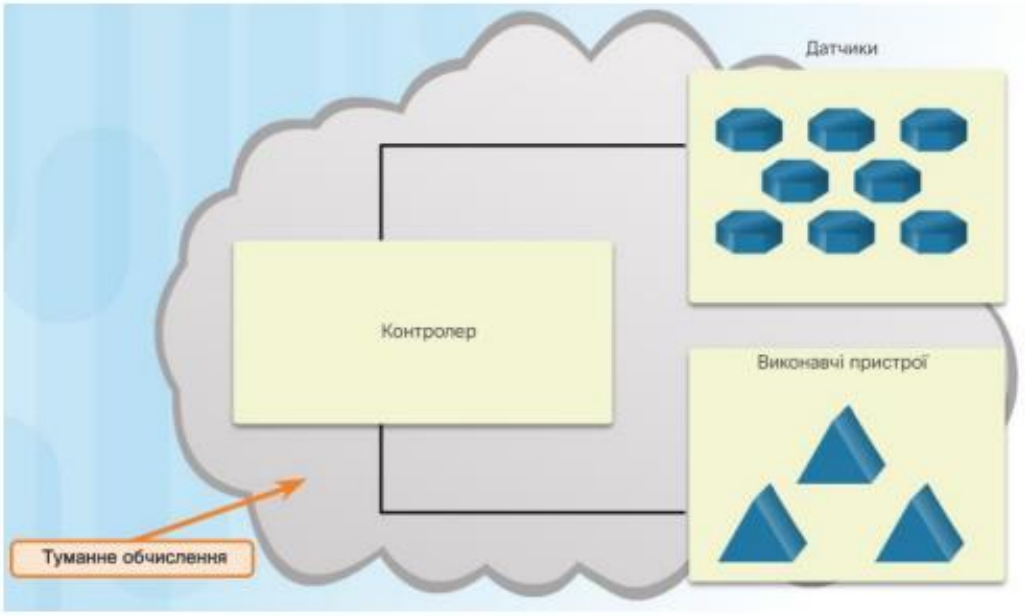

Рисунок 1.1. Зразок топології IoT

Контролери несуть відповідальність за збір даних з датчиків та забезпечення мережевого або інтернет-з'єднання. Контролери можуть мати можливість приймати негайні рішення, або вони можуть надсилати дані на більш потужний комп'ютер для аналізу. Цей більш потужний комп'ютер може бути в тій самій локальній мережі, що і контролер, або може бути доступний лише через підключення до Інтернету.

Датчики часто працюють разом із пристроєм, який називається виконавчим механізмом. Приводи приймають електричний струм і перетворюють його у фізичну дію. Як приклад, якщо датчик виявляє надлишок тепла в приміщенні, датчик передає значення температури на мікроконтролер. Мікроконтролер може надсилати дані на привід, який потім включить кондиціонер.

Більшість нових пристроїв, таких як фітнес-трекери, імплантовані кардіостимулятори, лічильники повітря в шахтах та лічильники води у фермерському середовищі вимагають бездротового підключення. Оскільки багато датчиків працюють від акумуляторів або сонячних панелей, необхідно враховувати споживання енергії. Для оптимізації та збільшення доступності датчика необхідно використовувати опції з низьким рівнем живлення.

Інтелектуальний будинок можна уявити собі у вигляді пазла, кожен елемент якого виконує певну функцію. Тому безперебійний зв'язок між усіма цими елементами дуже важливий. Для зв'язку пристрою використовуються як дротові, так і бездротові протоколи. Розглянемо ті, які є найбільш популярними.

Протокол 1-Wire – простий у виконанні і досить надійний дротовий протокол. Основна лінія для передачі інформації – двонаправлена шина, пара дротів. Перший дріт передає дані і живлення, другий використовується в якості заземлення. Топологія такої мережі буде представлена однією шиною. Обладнання підключається до загального кабелю. Можливе використання в

якості основи витої пари, пристрої в цьому випадку підключаються через RJрозетки. Передача даних здійснюється на досить великі відстані. При дотриманні деяких умов воно може досягати 300 м. Для підключення обладнання досить двох проводів. Невисока вартість є ще одним плюсом технології. З недоліків варто відзначити низьку відмовостійкість такого зв'язку. Її зазвичай вибирають економні користувачі, які передбачають використовувати мінімальний набір функцій «розумного дому».

X10 протокол активно використовується, незважаючи на свою сорокарічну історію. Головний плюс – висока універсальність. X10 використовується як дротовий протокол, але для цього не потрібно прокладати спеціальний кабель. Передача сигналу здійснюється на стандартній електропроводці. На додаток до цього X10 здатний забезпечувати зв'язок з бездротовими пристроями. Для цього використовуються трансивери, що перетворюють їх сигнал в формат, який підходить для передачі по кабелю. Переваги застосування: зручне управління, а також простий і швидкий монтаж. Зручні і гнучкі налаштування окремих елементів мережі. Вартість доступна. Значущих недоліків X10 кілька. Прокол дуже повільний. Передача однієї команди або адреси займає ¾ секунди, що дуже помітно при використанні двостороннього зв'язку. У конкретний момент часу в мережі може передаватися тільки одна команда. Для використання протоколу може знадобитися трохи доопрацювати існуючу проводку.

Протокол KNX один з найскладніших в інсталяції і проектуванні стандартів. Для передачі інформації може використовуватися електрична мережа, радіоканал або вита пара. Найчастіше застосовується останній варіант, в такому випадку шину укладають разом з силовими дротами в процесі будівництва. Топологія мережі може бути найрізноманітнішою: лінія, зірка, дерево. Зручне управління і широкий функціонал. Просте перепрограмування і модернізація, а також незалежне проектування і подальший монтаж сигнальних і силових ліній можна віднести до переваг

даної технології. А також число об'єднаних в мережу пристроїв може бути дуже великим. Недоліком можна вважати відносно повільну передачу даних і високу вартість. Протокол призначений в першу чергу для професійного використання.

Wi-Fi – бездротовий протокол, який використовується майже в кожній домашній системі. Основне застосування: здійснення управління розумним будинком з мобільного пристрою. Для цього розроблені спеціальні програми, що працюють на різних платформах. Wi-Fi використовується і для зв'язку з автономним обладнанням, функціонуючим окремо від автоматизованої системи. Мережу можна розгорнути без прокладки кабелю. Частоти, на яких працює протокол, не створюють перешкод і безпечні для людей. Обладнання, що підтримує технологію Wi-Fiшироко розповсюджене. Тобто сумісність таких пристроїв гарантована. Однією з найзначніших переваг Wi-Fiє висока швидкість передачі даних. З недоліків стандарту слід відзначити високу вартість модулів, їх велику енергоємність і відсутність можливості тривалої роботи обладнання від автономних джерел живлення.

ZigBee протокол, його друга назва IEEE 802.15.4. Бездротовий протокол з дуже низьким електроспоживанням. Основною перевагою вважається можливість створення комірчастої мережі, здатної до самоорганізації і самовідновлення (рис. 1.2) Вихід двох-трьох елементів з ладу не призведе до серйозних наслідків. При поломці одного з них решта зв'язуються між собою безпосередньо або через проміжні об'єкти. До переваг можна віднести можливість створення складних мережевих рішень з автоматичної маршрутизацією. Рівень захисту даних є достатньо високим. Одна мережа здатна підтримувати до декількох тисяч елементів. Наявна можливість гнучкого налаштування вузлів мережі. Вартість технології невисока, досить простий монтаж. Головний недолік ZigBee - відсутність стандартизації, внаслідок чого устаткування різних брендів рідко виявляється сумісним. Ще один мінус полягає в тому, що швидкість передачі даних відносно невисока.

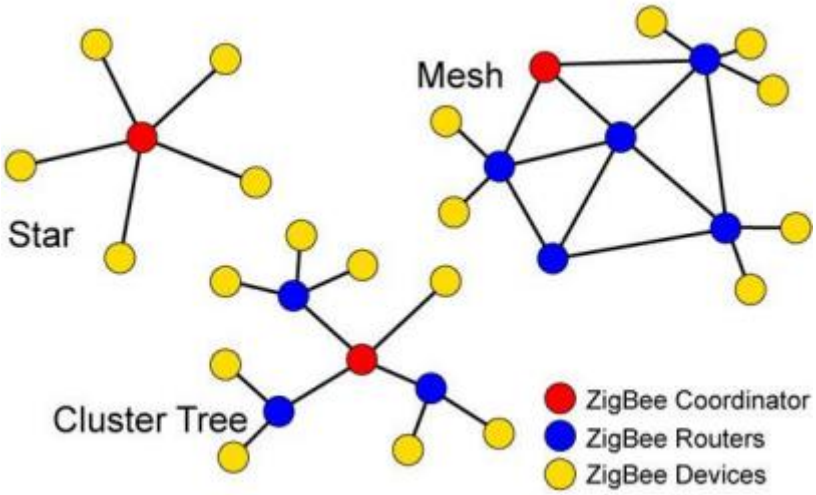

Рисунок 1.2. Зразок топології ZigBee

Z-Wave – бездротовий протокол (рис. 1.3.) багато в чому схожий на ZigBee. Характеризується низьким енергоспоживанням, здатний формувати мережу комірчастої топології. Цілком можна порівняти з аналогом і за ціною обладнання.

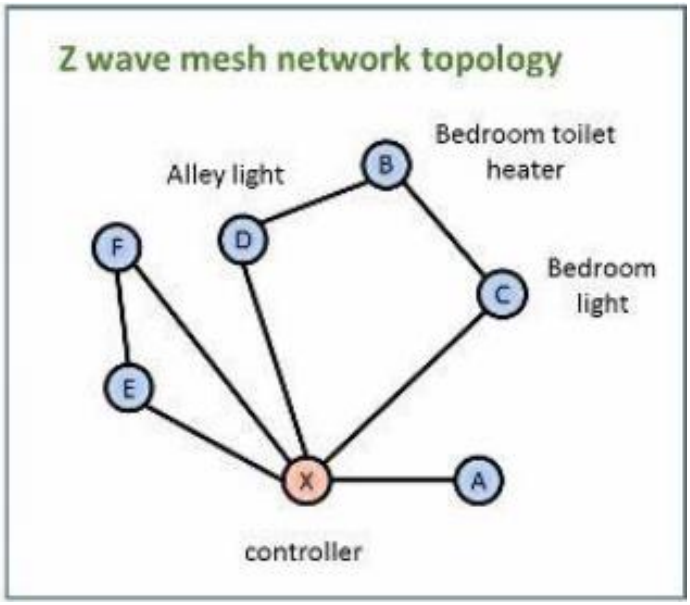

Рисунок 1.3. Зразок топології Z-Wave

Головна перевага Z-Wave - в стандартизації. Усі працюючі за цим протоколом прилади базуються на модулях Sigma Designs, тому сумісні між

собою. Взаємодія пристроїв з таким протоколом надійна і безпечна. Є можливість розширення у мережі, простота використання. Рівень випромінювання низький, безпечний для людини. Вартість невисока. З недоліків можна відзначити відносно невисоку швидкість передачі даних. Z-Wave вважається одним з кращих рішень для самостійної збірки «розумного будинку».

Insteon протокол використовує одночасно бездротовий і дротовий тип зв'язку. Для передачі сигналу використовується електропроводка, але в порівнянні з X10 дані передаються набагато швидше. Стандарт сумісний з X10. Бездротова складова протоколу реалізується за допомогою радіозв'язку.

Протокол Insteon підтримує коміркову типологію мережі. Можливе створення децентралізованої мережі. Передача даних надійна і швидка. Наявна сумісність з X10, що дає можливість поступового переведення системи на новий протокол. Сумісність приладів гарантує жорстка стандартизація обладнання. Присутня можливість поступового доповнення систем «розумного будинку». З недоліків варто виділити труднощі з доступністю необхідного обладнання, оскільки протокол спочатку розроблявся для США.

BLE – Стандарт Bluetooth з малим енергоспоживанням. Його використовують для передачі даних між двома приладами, що знаходяться поблизу один від одного. Широко застосовується в домашній автоматизації в якості додаткового протоколу. Стандарт добре захищений від несанкціонованого доступу. Перевагами BLE вважаються: висока швидкість передачі даних, простота у використанні, відсутність дротів, невелике споживання енергії. З недоліків відзначають обмежений радіус дії.

Для зв'язку між елементами «розумного будинку» використовуються різні протоколи. Кожен з них має переваги і недоліки. Для знайомства з основами домашньої автоматизацією оптимальним варіантом стане Z-Wave або ZigBee. Ці стандарти дозволять створити розгалужену повноцінну мережу. Якщо потрібно перейти до бездротового протоколу від встановленого раніше

X10, оптимально використовувати Insteon. [7] Для професіоналів хорошим вибором стане KNX.

1.3. Кібербезпека IoT

IoT є одним з найшвидших зростаючих технологій, які мають величезний вплив у різних областях [8]. Однак, хоча IoT і поставляється з кількома перевагами, одним з головних питань, що оточують такі пристрої - це їх величезні недоліки безпеки. Визначним дослідженням у галузі є Hewlett Packard Enterprise, яке у 2016 р. продемонстрували, що 70% найпопулярніших пристроїв IoT на ринку є вразливими до ряду загроз безпеці. Зокрема, вони виявили, що у кожного пристрою є необачно висока кількість вразливостей безпеки, кожна з яких страждає в середньом 25 випусків. Інші дослідження, виявили подібні обмеження, такі як OWASP TOP 10 IoT вразливості і дослідження Synopsys [9] і Abouzakhar et al. [9], хто виявив незахищеність у медичних приладах. Останнім часом з'явилися пристрої IoT зайняті в рамках ботнетів і запущені кілька найбільших DDoS-атак. Нещодавнє дослідження IBM X-Force показало зростання на 500% в цілому Атаки, які значною мірою керувалися новим варіантом ботнету.

З тих пір, IoT пристрої були розроблені, щоб включити деякі поліпшення безпеки, такі як транспортне шифрування. Однак статистика показує, що як число Іот пристрої збільшуються, кількість атак кібербезпеки проти них також збільшується і більшість цих пристроїв досі не захищені. Більш конкретно, в 2019 році програмне забезпечення Avast [10] повідомило, що був відкликаний розумний годинник німецького виробництва Childrenâs до ЄС, коли було виявлено, що його контролерний додаток має значні вразливості. Стало відомо, що пристрій було скомпрометовано, щоб хакери могли відстежувати переміщення дітей в реальному часі або розсування даних про розташування GPS для обману батьків. Крім того, інше дослідження Кумара та ін. виявив,

що багато IoT пристроїв мали порти і протоколи залишилися відкритими, навіть якщо вони не використовуються виключно пристроєм. Крім того, вони повідомили, що було знайдено багато пристроїв, які мають протокол передачі файлів (FTP) і послуги Telnet відкриті. Більш детально, 17.4% пристроїв мали слабкі FTP-вірчі дані У той час як 2.1% мали слабкі повноваження Telnet. Ще більш недавнє дослідження, проведене в 2020 році Mangino et al., виявили, що велика кількість пристроїв IoT, знайдених в Інтернеті, були вразливі до вищезгаданих вразливостей. Як результат, як загрози по відношенню до IoT прогресивно збільшуються їх складність і тяжкість, видно, що стан в їх безпека залишається слабкою; таким чином, вимагаючи подальшої уваги.

Існує три основні причини, чому пристрої IoT вразливі до кібератак:

1. Гетерогенність пристроїв значно розширює поверхню атаки екосистем IoT. Таким чином, реалізація механізмів безпеки, які можуть бути універсально застосовний до IoT складається складний виклик.

2. Обмеження в обчислювальній потужності пристроїв IoT сильно впливають на їх охорону. Це, як правило, не можливо для IoT пристроїв з обчислювальним обмеженням потужності, пам'яті, радіопропускної здатності і ресурсу батареї для виконання обчислювально інтенсивних і чутливих до латентності задач безпеки, які генерують важкі обчислення і комунікаційне навантаження. В результаті цього не можна працевлаштовувати легкі, складні та міцні заходи безпеки.

3. Оновити програмне забезпечення важко або застосувати патчі на таких пристроях.

Враховуючи, що вони страждають від вразливостей безпеки і що вони часто глибоко вбудовані в мережі, IoT пристрої розглядаються як одні з найслабших посилань для прорватися в захищену інфраструктуру.

Багаторазові дослідження показали, що IoT пристрої є вразливий до широкого спектру кібератак.

Типи атак, які можуть відбуватися в мережах IoT. До них належать фізичні, мережеві, прошивка і атаки шифрування.

Фізичні та близькі атаки

Фізичні атаки зосереджуються на пошкодженні апаратних компонентів пристрою за допомогою таргетування їх порти, пам'ять, джерело живлення тощо Такі атаки можуть порушити функціональність пристрою і можуть змінити його поведінку. Для того, щоб супротивник міг розгорнути ці атаки, вони повинні мати фізичний доступ до пристроїв.

Нижче наведені приклади фізичних атак, в яких IoT пристрої уразливі проти:

• Радіочастотна інтерференція/заклинювання: Здебільшого це стосується DoS-атак, які може бути спричинена створенням і передачею сигналів шуму по радіочастоті.

• Фізична проникність: Супротивник потенційно може отримати доступ до експоновано-девайсного інтерфейсу пристрою (наприклад, JTAG), і, таким чином, може легко отримати доступ до пам'яті, чутливого матеріалу ключа, паролі, дані конфігурації і різновид інших чутливих параметрів [11].

• Фізичні пошкодження: Зловмисник фізично пошкоджує пристрій з метою удару наявність сервісу.

• Зловмисний викид вузла: Зловмисник виснажує пристрій Rogue в мережі це потенційно може бути використано для спостереження за мережевим трафіком і перехоплення зв'язку. Ця атака також може розглядатися як атака на основі мережі.

Атака соціальної інженерії

• Соціальна інженерія: А не сам пристрій, ці психологічні атаки є Спрямований у бік користувача IoT-пристрою. Мета — зібрати довіру користувача до обміну чутливою інформацією. Атаки на основі мережі Мережеві атаки можуть бути розгорнуті на екосистемах IoT через мережу з

будь-якого місця у світі. Зловмиснику не потрібно мати фізичний доступ до пристроїв для запуску таких атак, як:

• Пасивний аналіз дорожнього руху: Супротивник пасивно стежить за мережею в порядку щоб спробувати перехопити чутливі дані користувача. Інформацію можна зібрати шляхом моніторингу трафіку мережі. Зловмисник також може втрутитися в рух транспорту, відомий Як MITM.

• Spoofing: Під час таких атак противники імпонують законні пристрої зробити злісних об'єктів такими, як якщо вони є законними, так, щоб атаки могли запускається.

• Sinkhole: Скомпрометований пристрій намагається залучити мережевий трафік шляхом реклами підроблених оновлень маршрутизації.

Одним з ударів таких атак є те, що він може бути використовується для запуску інших атак.

• DoS/DDoS: DOS і DDoS — найбільш поширені види атак, що відбуваються в мережах IoT. Такі атаки зменшують, переривають або повністю усувають с комунікація та діапазон мережі від відносно простого заклинювання до більшого витончені атаки. Їх можна запустити дистанційно і виявити важко перед тим, як мережа або послуга стає недоступною.

• Депривація сну: В мережах IoT пристрої мають можливість входити в режими енергозбереження, щоб зберегти свій ресурс і зменшити споживання енергії. Ця атака зосереджується на забороні цим пристроям перейти в режим енергозбереження, постійно посилаючи на них трафік і тому виснажує їх ресурс батареї.

• MITM Attack: — Це атака, при якій зловмисник робить самостійний зв'язок з жертвами B і C, роблячи їх вважають, що вони спілкуються один одного. Зловмисник перехоплює повідомлення, що надходить від B до C, і віце і навпаки, і перетрати їх.

Атаки прошивки

Атаки прошивки пов'язані з програмним забезпеченням, яке встановлюється на пристрої IoT.

Більш конкретно:

• Backdoors: Зловмисник модифікує прошивку пристрою, вставляючи код, що дозволяє їм отримати віддалений доступ до пристрою, коли він під'єднаний до нього мережа.

• Незашифрована інформація: Зловмисники зворотним інженером складеного прошивки і

Досліджують його, щоб знайти зашифровані паролі, ключі API і відкритий ключ сертифікати. Ця інформація дозволяє їм перехопити розв'язок в пристроїв і отримати доступ до чутливих даних користувача.

• Зловмисне програмне забезпечення Firmware: Зловмисники можуть не тільки модифікувати прошивку пристрою замовлення на створення бекдорів, але також для запуску інших атак, таких як DDoS.

Атаки шифрування

Шифрування атакує цільову будь-яку форму механізму шифрування, який використовується на An Мережа IoT [12], така як:

• Атака Side Channel: Зловмисники розгортаємо цю атаку, щоб обійти шифрування в пристрої IoT. Це можливо шляхом підслуховування на бічному каналі пристрою викиди та очікування на використання ключа шифрування для доступу до пристрою.

• Атаки на основі криптоаналізу: Ці атаки припускають володіння шифротекстом або відкритий текст. Їх мета — знайти ключ шифрування, який використовується, зламавши схема шифрування системи. Приклади атак криптоаналізу на системи IoT включають атаки з відомим відкритим текстом, атаку обраним відкритим текстом, вибрану атаку шифротексту і атаку лише на шифротекст.

• Атака лише на шифротекст: У цьому метіді зловмисник може отримати доступ до шифротексту і визначити відповідний відкритий текст.

• Відома атака відкритого тексту: В цьому методі зловмисник знає відкритий текст і кілька частин шифротексту. Метою супротивника є розшифрування частини, що залишилася шифротексту, що використовує цю інформацію.

1.4. Наслідки кібератак на IoT та їх Пом`якшення

Наслідки, пов'язані з атаками, можуть бути різним: від цифрової втрати даних до фізичної шкоди. Наприклад, на перший погляд нешкідлива атака деавтентифікації не може завдати значної шкоди. Але якщо його розгорнути на пристрої з критичним значенням, наприклад, на кермі розумного автомобіля, це може становити загрозу для життя людини. Інші високосерйозні атаки на безпеку, наприклад, концепції CNI, можуть порушити доступність системи та енергетичні ресурси, спричинивши відключення системи та інші невибіркові та довгострокові пошкодження. Наслідки цих проблем безпеки можуть спричинити значні перешкоди для роботи служб. Наприклад, мережі громадського транспорту можуть стати мішенню для спричинення хаосу в періоди пікових поїздок, а атаки на електромережі можуть призвести до втрати величезної кількості енергії та можливого знеструмлення системи. Крім того, такі атаки можуть призвести до фінансових наслідків. Недавнє опитування Irdeto Global Connected Industries[1]показали, що пов’язані з IoT кібератаки можуть мати значні фінансові наслідки. Зокрема, 700 організацій у сферах транспорту, виробництва та охорони здоров’я зазнали фінансових збитків, які перевищують 300 000 доларів кожна через кібератаки, пов’язані з IoT.

У результаті, враховуючи, що найважливішим аспектом пристроїв IoT є їх взаємозв’язок,і, зрештою, підключення до Інтернету, мережеві атаки можуть вплинути на більшість пристроїв. Поряд із поєднанням тяжкості наслідків таких кібератак для IoT та їх неоднорідності, ця теза мотивована

дослідженнями мережевих атак в IoT; зокрема, захист різнорідних інтелектуальних пристроїв і виявлення таких атак.

Є кілька досліджень, які стосуються безпеки IoT. Така робота зосереджена на пом’якшенні певних елементів безпеки, таких як:

- Аутентифікація- що допомагає IoT розрізняти легітимні вихідні вузли та боротися з атаками на основі ідентифікації, такими як спуфінг.
- Управління доступом- що запобігає доступу неавторизованих користувачів до ресурсів IoT.
- Конфіденційність і чесність- який гарантує, що дані доступні для читання лише призначеному одержувачу та не були змінені.

Однак, враховуючи неоднорідність навколо IoT, такі механізми безпеки можуть бути застосовані не до всіх пристроїв, підключених до мережі. Крім того, такі рішення безпеки також можуть створювати велике обчислювальне та комунікаційне навантаження, особливо у зовнішніх пристроях Інтернету речей, таких як дешеві датчики з легкими засобами захисту. IoT не складаються з однієї технології. Скоріше це сукупність різних технологій, які працюють разом як частина надійної архітектури. Це підкреслює, що IoT є сильно неоднорідним середовищем.

Якщо говорити точніше, то в контексті IoT неоднорідність стосується впровадження широкого розмаїття апаратного забезпечення, програмного забезпечення, протоколів, платформ, політик тощо. Наприклад, не всі пристрої IoT продаються одним постачальником і створюються для однієї мети. Залежно від додатків і випадків використання пристрої IoT включають кілька різних функцій для суворого використання. Згодом пристрої IoT можна класифікувати за різними типами, беручи до уваги такі параметри, як їх розмір (наприклад, малі чи великі), їх портативність (наприклад, портативні чи стаціонарні), їх джерело живлення (наприклад, акумулятор або зовнішнє джерело) і їхні можливості обробки. (наприклад, комерційний або вбудований)[48]. Крім того, залежно від завдання, для якого вони були

розроблені, пристрої IoT використовують різні протоколи зв'язку для підключення до Інтернету, шлюзів або один з одним. Кілька найпоширеніших комунікаційних технологій, що використовуються серед пристроїв IoT, включають IEEE 802.15.4, Wi-Fi з низьким споживанням енергії, 6LoWPAN, RFID, Sigfox, LoraWAN, Bluetooth Low Energy(BLE),і Zigbee. Кожен із цих протоколів має різні атрибути, які роблять їх придатними для різних типів пристроїв. Наприклад, якщо пристрій має обмежений обсяг акумулятора, найкраще використовувати BLE, оскільки він не споживає багато енергії порівняно з іншими протоколами.. Таким чином, очевидно, що через низку різних технологій, які використовуються в інфраструктурах Інтернету речей, і обмеження обчислювальної потужності таких пристроїв, однією з найбільших проблем, які виникають у цій інфраструктурі, є застосування загальних механізмів безпеки. Тому надзвичайно важливо розробити уніфіковані механізми безпеки для різнорідних пристроїв в екосистемі IoT. Одна з найсучасніших моделей для керування різнорідними пристроями уніфікованим способомЦентри Інтернету речей. Центри Інтернету речей дозволяють керувати декількома пристроями з однієї центральної точки, що часто забезпечує додатковий контроль безпеки.

Фундаментальна ідея концентраторів IoT полягає в тому, щоб дозволити пристроям і датчикам з низькою обчислювальною потужністю зосереджуватися виключно на завданні, для виконання якого вони призначені (наприклад, вимірювання температури), без необхідності розглядати більш складні функції (наприклад, підключення до мережі, обробка даних). Ці функції виконуються ядром концентратора, шлюзом, який має значно більшу обчислювальну потужність і пам'ять у порівнянні з самими пристроями та датчиками. Центри Інтернету речей також мають можливість підключати широкий спектр різноманітних інтелектуальних пристроїв і датчиків (наприклад, термостатів, розумних замків, датчиків світла) за допомогою бездротових технологій. Існує кілька структур, які зосереджені головним

чином на усуненні неоднорідності та великих даних в IoT. Такі рамки включають. Однак такі реалізації мають обмеження, які включають обмежені можливості взаємодії між пристроями від різних виробників і неоднорідність протоколів. Таким чином, щоб задовольнити вимоги, необхідні для комунікаційного інтерфейсу, абстракції програмування та підтримки пристроїв, керованих спільнотою, Mozzami et al. реалізовано SPOT, Extensible Markup Language(XML)заснований хаб. SPOT використовує драйвери пристроїв для підтримки додаткових пристроїв. Однак ця техніка може бути дуже трудомісткою та незручною для користувача. Крім того, цей концентратор включає лише автентифікацію OAuth як механізм безпеки, а загальна ефективність безпеки концентратора не оцінюється. Саксена та ін. запропонували реалізацію шлюзу IoT, який, як очікується, працюватиме в мережах 5G, з основним акцентом на вирішенні проблеми бездротових мереж з обмеженими ресурсами. Однак цей підхід не вирішує основних проблем безпеки, і подібно до Mozzami et al., не було оцінено проти кібератак. Крім того, Gloria et al. розробив шлюз IoT, який стосується IoT.

Однак цей підхід зосереджений лише на низькорівневих вбудованих пристроях і не підтримує комерційні розумні домашні пристрої. Крім того, це рішення не зосереджено на безпеці, а механізм автентифікації, який використовується, насамперед призначено для конфігурації платформи. Крім того, щоб усунути неоднорідність і контролювати великий обсяг даних, створених IoT, Razafimandimby et al. запропонував байєсівський підхід висновку(BIA). Ця модель заснована на ієрархічній архітектурі, яка складається з простих вузлів, розумних шлюзів і центрів обробки даних. Він використовує ймовірнісні методи, щоб уникнути надсилання непотрібних даних у мережу. Хоча цей підхід успішно зменшує споживання ресурсів, він не стосується безпеки екосистеми IoT. Альшері і Сандху[58]запропонувати архітектуру, де віртуальні об’єкти використовують теми публікації та підписки (PubSub) для надання послуг користувачам через політику безпеки.

Незважаючи на те, що цей підхід успішно усуває масштабованість, неоднорідність і забезпечує безпечний механізм контролю доступу, система не надає жодних інших механізмів безпеки та не була оцінена проти ряду атак. Такі комерційні впровадження, як Samsung Smart Things, Apple HomeKit і Google Smart Home, пропонують рішення, подібні до Mozzami et al., і здатні підтримувати обмежену кількість пристроїв від різних сторонніх постачальників. Крім того, вони також можуть забезпечити маскування та ізоляцію пристрою, якщо їх використовувати в поєднанні з окремою підмережею. Однак це залежить від сумісності пристрою та концентратора, оскільки об'єднання пристроїв IoT у нову підмережу може спричинити втрату функцій і взаємодії з включеними пристроями IoT (наприклад, лампи Philips Hue мають бути на тій самій підмережі). -мережа як їхні взаємодіючі пристрої. Тому зміна налаштувань освітлення за допомогою смартфона неможлива з основної мережі). При цьому такі хаби за замовчуванням не передбачають цей механізм. Також важливо підкреслити, що часто ці концентратори не можуть взаємодіяти один з одним.

Гоцян запропонував централізовану структуру, яка використовує шлюз, який дозволяє підключати різні протоколи зв'язку для підтримки різних мереж. Тим не менш, цей підхід вимагає передових методів конфігурації та змін у фізичному обладнанні, що може бути дорогим і нелегким для розширення. Нарешті, ця структура не включає політику безпеки чи інші механізми для підвищення безпеки пристроїв IoT. Нижче наведено їх визначення:

- Аутентифікація- Хаб забезпечує механізм перевірки особи користувача (наприклад, шляхом створення облікового запису)
- Конфіденційність- Хаб забезпечує механізми захисту даних від ненавмисного, незаконного або неавторизованого доступу (наприклад, через TLS або AES).

- Управління доступом- Концентратор забезпечує механізм, який регулює, хто і коли може взаємодіяти з пристроями (наприклад, за допомогою політик контролю доступу).
- Маскування пристрою- Хаб повинен маскувати пристрої IoT, щоб зловмисникам було складніше їх знайти.
- Гетерогенність Aware- Хаб підтримує пристрої від різних виробників.
- Моніторинг поведінки зловмисників- Хаб містить механізми, які допомагають відстежувати поведінку користувачів/зловмисників (наприклад, за допомогою функцій IoT canary)

Очевидно, що попередні пропозиції, які спрямовані на вирішення неоднорідності IoT, справджуютьсяне спеціалізуються на підвищенні безпеки екосистеми. Натомість увага зосереджена на обробці великих даних, які генеруються розумними пристроями, намагаючись подолати обмеження їхньої обчислювальної потужності та масштабованості. Хоча безпека є ключовою проблемою в цих існуючих підходах, підтримувані вимоги безпеки обмежені лише частково адресовано, оскільки вони можуть забезпечувати максимум два механізми безпеки, залишаючи концентратори відкритими для зловмисників.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ВІД КІБЕРАТАК В РОЗУМНОМУ БУДИНКУ

2.1. Дослідження безпеки системи розумного будинку

Одним із найпопулярніших підходів до мережі IoT у розумному домі є зіркова топологія, коли всі розумні пристрої підключаються до центральної точки доступу.[87,133,191]. Більш конкретно, у типовому розумному домі традиційні комп'ютери та розумні пристрої отримують доступ до Інтернету, підключаючись до однієї точки доступу. Малюнок 3.1 ілюструє приклад звичайної топології мережі такої екосистеми. Цей конкретний приклад топології мережі складається з одного центрального маршрутизатора, наданого постачальником послуг Інтернету(ISP),звичайні IT-пристрої (наприклад, ноутбуки) і пристрої Інтернету речей, які підключені до точки доступу за допомогою адаптера лінії живлення через Wi-Fi або Ethernet, тоді як користувач може керувати ними за допомогою окремих мобільних/веб-додатків, які вони надають.

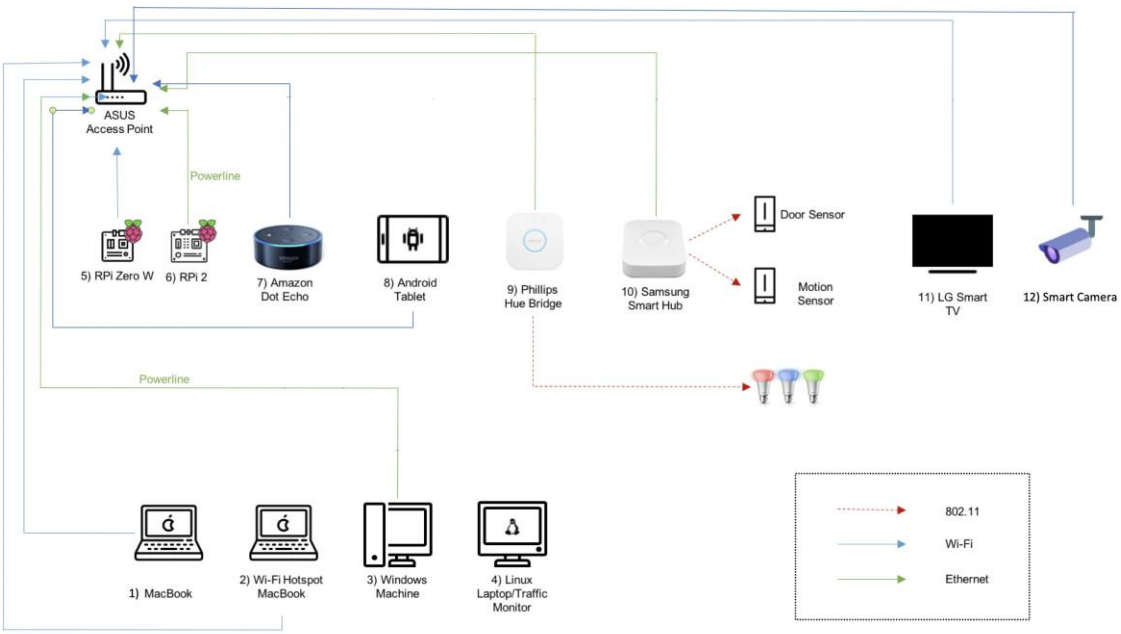

Рисунок 1.3. Традиційна домашня розумна мережа IoT

Варто підкреслити, що розумні домашні пристрої часто підтримують роботу кількох користувачів одночасно. В результаті більше ніж один користувач може контролювати та змінювати налаштування смарт-пристроїв у мережі. Спеціальні пристрої та датчики постачальників, такі як лампи Philips Hue і датчик руху Samsung Smart Things, підключаються до їхніх концентраторів керування через Zigbee або BLE. Варто зазначити, що пристрої IoT, які розглядаються в цьому документі, обмінюються даними через дротове або Wi-Fi мережеве з'єднання, а такі засоби масової інформації, як Bluetooth, ZigBee, Z-Wave і 6LowPAN, виходять за межі цієї дипломної роботи. Незважаючи на те, що це традиційна мережева конфігурація, інтелектуальні пристрої піддаються впливу будь-кого, хто може мати доступ до локальної мережі, що згодом збільшує ризики безпеки. У результаті пристрої можуть бути вразливими до різноманітних бездротових атак, таких як пасивне перехоплення, атаки MITM, DoS тощо[66].

Є багато причин, чому зловмисник може захотіти скомпрометувати пристрої IoT у розумному домі. По-перше, пристрої IoT, такі як розумні камери, можуть використовуватися для цілей фізичної безпеки. Тому зловмисники можуть використовувати активні атаки (наприклад, DoS), щоб викликати затемнення камери, дозволяючи узбережжю бути вільним для фізичного доступу до дому без створення цифрових доказів[151]. Такі пристрої, як розумні роботи-пилососи, які мають певну мобільність по дому, потенційно можуть надавати зловмисникам інформацію про планування будинку. Ця інформація може бути використана для подальшого планування діяльності та переміщень[20]. Крім того, інші пристрої, наприклад переносні пристрої, можуть мати доступ до конфіденційної інформації користувача, такої як імена користувачів, паролі та навіть дані кредитної картки, які можуть бути зламані. Крім того, зловмисник може викрасти пристрій IoT і згодом контролювати його. Такі атаки важко виявити, оскільки зловмисник не змінює

основні функції пристрою очевидним чином. Зокрема, зловмисник може скомпрометувати інтелектуальний замок і може вирішити розблокувати його в незвичний проміжок часу (наприклад, посеред ночі). Нарешті, зловмисник може пасивно контролювати мережевий трафік розумного будинку, щоб виконувати атаки на основі конфіденційності.

Шляхом експлуатації цих атак зловмисники можуть перехоплювати, втручатися або змінювати поведінку пристроїв IoT різними способами. Деякі з цих підходів можуть вимагати фізичного доступу до пристроїв, що може значно ускладнити запуск атак; але інші атаки, які часто є найсильнішими, можуть бути розгорнуті через Інтернет з близької або віддаленої точки. Такі атаки можуть бути спрямовані безпосередньо на конкретні пристрої IoT, тобто використовуючи пошукові системи, які індексують вразливі пристрої IoT у світі, такі як Shodan або ZoomEy. Крім того, зловмисники можуть скомпрометувати традиційний пристрій, а потім націлитися на пристрої IoT з цього моменту. У першому випадку немає гарантії, що пристрої IoT будуть проіндексовані цими пошуковими системами. Таким чином, якщо зловмисник має на увазі конкретну ціль, він може не знайти відповідних уразливих пристроїв в Інтернеті. Варто також зазначити, що враховуючи те, що тестовий стенд був розгорнутий у реальному будинку, додавання пристрою IoT до цих пошукових систем для проведення експериментів вважалося занадто ризикованим. Крім того, через обмежені можливості та обчислювальну потужність пристроїв компрометація одного конкретного IoT-пристрою суттєво обмежить діапазон/обсяг атаки зловмисника, оскільки він може не мати змоги перейти до інших уразливих IoT-пристроїв у мережі. Однак в останньому випадку, ворог зможе завдати максимальної шкоди, розгорнувши ряд атак на будь-які пристрої в розумному домі. У результаті, враховуючи високий вплив таких атак, експерименти, представлені в цьому розділі, зосереджені на відтворенні можливої поведінки атакуючої поведінки, що використовується вищезгаданими супротивниками. Згодом на основі

топології розумної домашньої мережі IoT, і можливі мережеві загрози, з якими стикається розумний дім, експериментами тут розглянемо дві моделі нападників, які використовують два можливі та реалістичні методи отримання доступу до розумної робочої мережі. Такі моделі зловмисників можуть завдати найбільшої шкоди, дозволяючи зловмиснику розгортати ряд атак, націлених на кілька пристроїв. Ці моделі базуються на тих, що представлені в інших відповідних роботах і включають найпопулярніші типи мережевих атак, до яких вразливі пристрої IoT. Згодом цей розділ зосереджений на розробці хаб-фреймворку, здатного захищати пристрої IoT від атак у рамках вищезгаданих моделей зловмисників.

Модель нападника №1. У першій моделі передбачається, що зловмисник не має фізичного доступу до пристроїв IoT, але успішно отримав пароль для центральної точки доступу в мережі розумного будинку. Цей тип зловмисника може фізично перебувати в межах бездротового діапазону розумної домашньої мережі цільового користувача. Зловмисник, який контролює бездротовий маршрутизатор, може отримати доступ до пристроїв через локальну мережу та розгорнути кілька різних атак. Такий зловмисник може мати попередні стосунки з жертвою та отримав адміністративний доступ до маршрутизатора/мережі коли вони були присутні в будинку. Метою цього зловмисника є активне розгортання атак на пристрої та мережу IoT, щоб отримати більше інформації про пристрої, зробити їх недоступними для користувачів і перехопити конфіденційні дані. Зловмисник має такі можливості:

- Просканувувати мережу.
- Пасивно прослуховувати бездротовий зв'язок.
- Розгортайте активні атаки, такі як MAC/ARP Spoofing, DoS і MITM.

Зловмисник може мати такі цілі:

- для збору інформації про підключені пристрої (тобто, які пристрої підключено, які порти відкриті).
- керувати пристроями IoT.
- перехоплювати конфіденційні дані користувача.
- зробити пристрої недоступними для цільового користувача.

Модель нападника №2. У другій моделі зловмисника вважається, що зловмисник віддалено скомпрометував пристрій (наприклад, ноутбук) і отримав доступ до основної мережі розумного будинку, використовуючи, наприклад, фішингову атаку. Для цілей наведених тут експериментів передбачається, що цей супротивник має ті самі привілеї, що й законний користувач. Метою цього зловмисника є отримання несанкціонованого доступу до пристроїв IoT та їх функцій. Зокрема, вони намагаються залишатися непоміченими, не перериваючи роботу пристрою або активно розгортаючи атаки. Їхня мета полягає в тому, щоб використовувати законні функції пристрою, щоб завдати подальшої шкоди (наприклад, розблокувати розумний замок посеред ночі). Згодом, існуючі реалізації можуть забезпечувати один або два механізми безпеки, але вищезазначені зловмисники все одно зможуть розгортати прямі атаки на концентратори, щоб зробити їх недоступними для користувача (тобто DoS), сканувати мережу для ідентифікації підключених пристроїв, виконувати MITM-атаку на перехоплювати конфіденційні дані та отримувати доступ до пристроїв.

2.2. Виявлення керованого проникнення до середовища IoT

Як правило, інтелектуальний будинок містить безліч підключених пристроїв, що належать до різних областей застосування. Зазвичай сфери застосування розбито на чотири групи: розваги, енергетика, безпека та охорона здоров'я [38]. Розваги спрямовані на максимальне покращення комфорту та зручності, надаючи індивідуальний вміст для розваг та послуги

соціального спілкування. Енергетичні програми спрямовані на забезпечення ефективного споживання енергії та управління. Домен безпеки пропонує послуги, призначені для виявлення загроз безпеці та контроль за ними. Програми охорони здоров’я зосереджені на наданні мобільних медичних послуг та підтримці фітнесу. Можливо, медична установа має найширший спектр ризиків, починаючи від підслуховування до фатального хакерства. Як приклад на рис.1 показано типову архітектуру системи інтелектуального дому.

А. Пристрої

Розумні домашні пристрої - це апаратні пристрої, що зазвичай містять датчики, виконавчі пристрої, шлюзи та інтелектуальні об'єкти. Окремі типи пристроїв:

1) датчики - вимірюють фізичну властивість середовища або фізичної особи. Датчики можуть варіювати від мобільних (наприклад, браслетів) до датчиків, які не носять (наприклад, IPкамери). Відеокамери вважаються датчиками, які порушують конфіденційність [40] разом із мікрофонами;

2) виконавчі пристрої виконують такі дії, як ввімкнення / вимкнення або затемнення ліхтарів, закриття вікон, спрацьовування сигналів тривоги тощо;

3) шлюз слугує точкою доступу до будинку, що дозволяє користувачеві або іншому об'єкту відстежувати, контролювати та управляти побутовою технікою або датчиками віддалено. Крім того, він слугує точкою агрегації для надсилання вимірюваних даних до зовнішньої мережі;

4) розумні об’єкти - це пристрої, що складаються з датчиків та / або приводів, які підключені до домашньої мережі. Прикладами цього є розумні пристрої, такі як розумні замки, які відповідають на дзвінки і забезпечують контроль за часом.

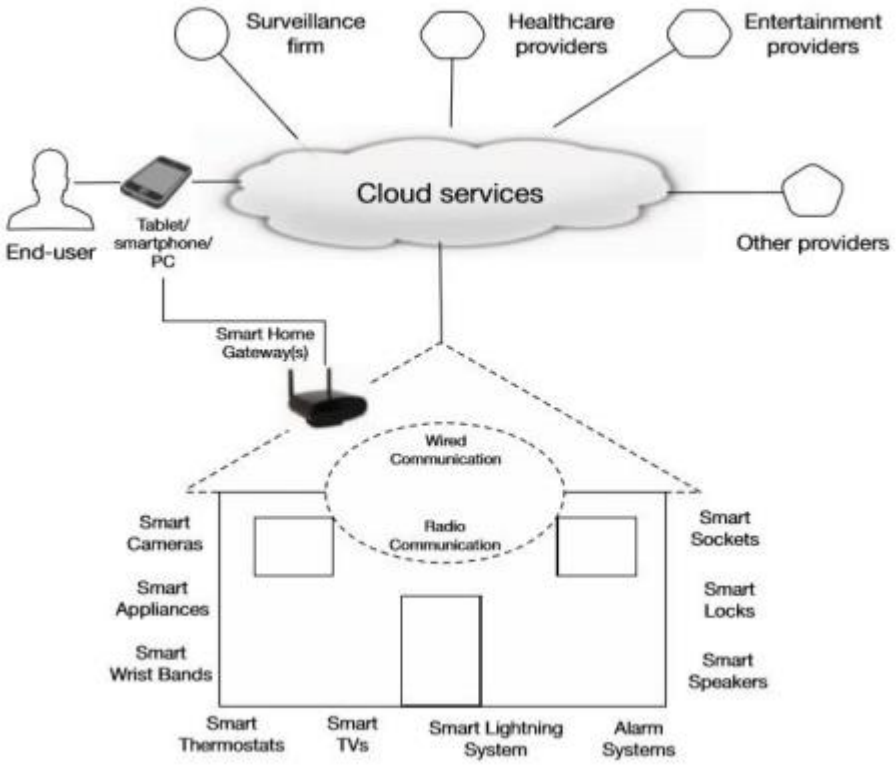

Рис. 2.2. Типова архітектура системи інтелектуального дому

Порівняно з традиційними цифровими системами більшість інтелектуальних домашніх пристроїв мають обмеження в обчислювальній потужності, пам'яті та енергії. Це призводить до того, що впроваджувати ефективні заходи безпеки та конфіденційності в розумному домашньому середовищі стає дедалі важче. Крім того, конфіденційність є складною і не завжди очевидною. Тим не менш, забезпечення конфіденційності та безпеки в будинках необхідно розглядати як пріоритетне завдання. Описано найбільш актуальні проблеми безпеки та конфіденційності, пов'язані з інтелектуальними будинками. Крім того, визначено підходи до подолання проблем на різних рівнях архітектури та запропоновано області, де потрібні подальші дослідження. Як загальне спостереження: сьогодні формуються деякі ініціативи для забезпечення безпеки та зміцнення конфіденційності користувачів. Незважаючи на це, виявлено чотири суттєві виклики, які необхідно вирішити: управління ідентифікацією, методи оцінювання ризиків,

підходи до управління інформаційними потоками та методи управління безпекою. Такі виклики посилюються в області інтелектуальних будинків, але також є загальними для інших кіберфізичних систем, де застосовуються пристрої IoT.

Системи ІД виникли як успішні методи виявлення та ідентифікації атак в мережах IoT. Завдяки розповсюдженню IoT пристроїв, їх гетерогенності, і кількості даних, які виробляються з таких технологій, IDSs стикаються з більшим масивними атаками. Щоб подолати ці обмеження, технік машинного навчання були інтегровані для підтримки IDSs в мережах IoT.

Крім того, існуюча література не має фокусу на профілювання та класифікації пристроїв. Важливою особливістю є те, що вона дозволяє ідентифікувати активи IT, а потім може допомогти при виявлення аномалій поза «нормальною» поведінкою пристрою. Крім того, такі системи не досліджують автоматизовану ідентифікацію того типу атак, який має стався, що є критичним для раннього реагування на атаки. За даними ЦКЗ та НКЦС [47], одна з головних проблем, з якими стикаються організації, полягає у виявленні типу кібер атака, що відбувається в мережі, без необхідності здійснювати в глибину врізування. В результаті це може спричинити затримку у виявленні та пом'якшенні атаки, що згодом може призвести до наслідків, починаючи від даних і фінансових втрат до фізична шкода.

Таким чином, можливість автоматичного виявлення точного типу атаки може бути значно зменшити зусилля людини, пов'язані з реагуванням на попередження, визначивши тяжкість атаки, і запуск ефективних контрзаходів.

Через причини доступності та розташування було реалізовано нове тестування IoT на основі тих же критеріїв, перелічених у попередньому розділі. Зокрема, як визначено в

Розумний будинок — це симбіоз різних пристроїв, тобто датчиків, з'єднань і додатків, які будують динамічну гетерогенну архітектуру з метою

ефективно управляючи домашніми пристроями, і надаючи додаткові послуги користувачам [43]. Навколо IDS в IoT було розроблено та впроваджено тестовий стенд, розміщений у кампусі університету, що імітує типове «мирне середовище». Причини, обговорені в розділі 3, пристрої були з'єднані в зоряній топології. Це

Конфігурація складалася з існуючих і доступних комерційних IoT пристроїв різних видів/застосування; освітлення, розваги, камери безпеки, датчики, і керування пристроєм [48]. Такі пристрої включали камеру Belkin Netcam, TP-Link NC200 Camera, TP-Link Smart Plug, Amazon Echo Dot, Lifx Lamp, I Samsung Smart Things Hub і British Gas Hive з'єднували між собою два сенсори: Рух датчик і датчик вікна/дверей. Конкретні пристрої були обрані виходячи з їх популярність, доступність, доступність і їх використання в інших відповідних і порівнянних праць.

На додаток до цих пристроїв, ноутбук був підключений до мережі IoT для розгортання різних мережевих атак. Ця призначена машина була Lenovo ThinkPad налаштована для запуску операційної системи Kali Linux [45]. Одночасно мережа для постійного запису на точку доступу було встановлено інструмент захоплення дорожнього руху мережевий трафік і збереження файлів журналу на сервері syslog.

Для того, щоб зібрати мережевий трафік, testbed був призначений для захоплення всіх пакетів в мережі. Всі вхідні і вихідні трафік від розумних пристроїв були захоплені за допомогою інструменту tcpdump [46], який постійно працював на точкі доступу. Процес збору даних був автоматизоваийа з використанням cron-завдань і скриптів bash. Мережеві пакети безперервно відзняті і збережені до Syslog Server у форматі Packet Capture (PCAP). Файли були генеровані в однохвилинних інтервалах і були доступні дистанційно через SSH для з'єднання з сервером Syslog. Щоб відповідати порівнянним дослідженням , на три тижні варто з доброякісних даних було зібрано. Протягом двох тижнів систематично запускалися напади

для створення і збирання зловмисних даних з яєчка. Загалом, оціночна загальна кількість було зібрано понад шість мільйонів доброякісних і три мільйони зловмисних пакетів.

Для того, щоб створити набір даних, що складається з доброякісного мережевого трафіку, IoT пристрої увімкнено яєчка регулярно взаємодіяли з с. Взаємодії були вирішені на основі в цільове використання пристрою, його доцільність в лабораторії та інші відповідні дослідження.

• Smart Things Hub: До офісу були прикріплені датчики дверей і руху двері, які регулярно використовувалися.

• Belkin Netcam & TP-Lik NC200: Обидві камери постійно були на і позиціонувалися в офісі.

• ТП-Link SmartPlug & Lifx Smart Lamp: Для живлення використовувався розумний штепсель розумну лампу і планувалося вимкнути вранці і вдень. Коли ж увімкнена, лампочка була інтерентувалась, щоб змінити свій колір [50].

• Apple TV: Apple TV використовувався, щоб час від часу транслювати відео з YouTube. Однак, через оточення теща і використовуючому справу в Apple TV, було непрактично взаємодіяти з пристроєм так само, як і з іншими у запорі. Згодом кількість мережного трафіку, що генерується з цього пристрій був значно менше, ніж інші пристрої на тестеї, і таким чином був у класифікаційних експериментах цей параметр не вказано.

• Hive Hub: Концентратор також був підключений до датчика дверей і руху. Двері датчики були прикріплені до настільного кресала і датчик руху зіткнувся з головним входом офісу.

• Amazon Echo Dot: The Amazon Alexa було запропоновано завершити деякі з її найбільш популярні типи взаємодій. Тому що кількість можливих взаємодій з цей пристрій не є бінарним (наприклад, "увімк./вимк."), дослідження на основі користувача [51], яке досліджувала в найпопулярніші взаємодії з нею були враховані для інформування наших рішень. Як такі, до

них входили: Перевірка погоди, пошук фактів, прослуховування щоб новини, розкажи жарти, грай музику, встановіть час і перевірте час. Однак, завдяки в обмежений вибір пристроїв, і те, що було заплановано розумну вилку Для керування лампою за допомогою власного застосунку не було підключено Echo Dot до інших пристроїв на яєчничку. При цьому Алексу не просили керуйте своїми функціями, такими як увімкнення та вимкнення лампи. Це може бути Розглядається як обмеження в рамках дослідження, оскільки ця команда є серед Alexa найпопулярніші випадки використання.

2.3. Cisco Packet Tracer 7 для створення IT-систем розумного будинку

Cisco Packet Tracer — це потужний інструмент моделювання віртуальної мережі, який використовується для навчання моделюванню комп'ютерних мереж. Інструмент розроблений Cisco для того, щоб дозволити студентам або користувачам отримувати практичні знання про мережеві технології. Cisco Packet Tracer надає користувачеві можливість проектувати та моделювати мережу за допомогою віртуальних пристроїв, такі як концентратори, маршрутизатори, комутатори тощо. У Cisco Packet Tracer симуляція працює без наявності будь-якої фізичної мережі.

Cisco Packet Tracer має дві робочі області: фізичну та логічну. Логічна область дозволяє користувачеві розміщувати та підключати пристрої віртуальної мережі, а фізична – надає графічне представлення пристроїв віртуальної мережі [56].

Перевагою цього конкретного інструменту моделювання є те, що він забезпечує середовище, де пристрої схожі на пристрої в реальному світі. Це дуже важливо, оскільки воно дає користувачеві можливість ознайомитися з приладами перед роботою з реальним обладнанням.

Інструмент також забезпечує два режими: режим реального часу та режим моделювання. У реальному часі користувач може мати чітке уявлення про те, як поводить себе реальне обладнання.

З іншого боку, режим моделювання допомагає користувачеві зрозуміти фундаментальну концепцію мережевих операцій. Цей режим дозволяє користувачеві бачити та контролювати часові інтервали, а також візуалізувати поширення даних по мережі. [53]

Cisco Packet Tracer дозволяє налаштовувати пристрої за допомогою двох способів: вкладки конфігурації або вкладки CLI (інтерфейс командного рядка). Перевага використання інтерфейсу командного рядка полягає в тому, що команди, які використовуються для налаштування обладнання практично ідентичні тим, які використовуються з реальними пристроями. Вкладка конфігурації не вимагає жодного знання команд cisco. Конфігурація здійснюється через графічний інтерфейс, зрозумілий навіть для користувача-початківця. Цей метод конфігурації також можна використовувати в ситуації, коли користувач не має достатньо часу і хоче швидко налаштувати пристрої. Ця техніка може допомогти заощадити час під час налаштування. [58]

Cisco Packet Tracer підтримує різні протоколи. На рисунку 2.3 нижче наведено списки протоколів, які підтримується програмою Cisco Packet Tracer. [58]

Layer	Protocols
Application	FTP,SMTP, POP3, HTTP, TFTP, Telnet, SSH, DNS, DHCP, NTP, SNMP,AAA, ISR VOIP, SCCP config and calls ISR command support, Call Manager Express
Transport	TCP and UDP, TCP Nagle Algorithm & IP Fragmentation, RTP
Network	BGP, IPv4, ICMP, ARP, IPv6, ICMPv6, IPSec, RIPv1/ v2/ng, Multi-Area OSPF, EIGRP, Static Routing, Route Redistribution, Multilayer Switching, L3 QoS, NAT, CBAL, Zone-based policy firewall and Intrusion Protection System on the ISR, GRE VPN, IPSec VPN
Network Access/ Interface	Interface Ethernet (802.3), 802.11, HDLC, Frame Relay, PPP, PPPoE, STP, RSTP, VTP, DTP, CDP, 802.1q, PAgP, L2 QoS, SLARP, Simple WEP, WPA, EAP

Рис. 2.3. Списки протоколів, які підтримуються в Cisco Packet Tracer

Остання версія Cisco Packet Tracer містить деякі нові функції, які дозволяють моделювати мережі з використанням технології Інтернету речей. Усі пристрої можна програмувати з використанням різних мов програмування, таких як phyton, javascript і blocky. В додаток, всі вони можуть бути підключені за допомогою дротового або бездротового зв'язку.

Cisco Packet Tracer має декілька категорій пристроїв (рис.2.4) для моделювання мережі. Користувач може обрати роутери, комутатори, концетратори, а також бездротові пристрої різних моделей. В першу чергу для побудови мережі будинку необхідні кінцеві пристрої. [60]

Рисунок 2.4. Панель категорій

Для вибору користувача доступні найрозповсюдженіші пристрої, такі як: персональні комп'ютери, ноутбуки, смартфони, сервери, телевізори, принтери, планшети і таке інше (рис.2.5).

Рисунок 2.5. Панель кінцевих приладів

Розумний будинок може містити у собі елементи мережі представлені на рисунку 2.6. Наприклад, такі пристрої як: батарея, розумне освітлення, термостат, сигналізація, розумний чайник, вентилятор, кондиціонер, камера, різні види детекторів і датчиків, тощо.

Рисунок 2.6. Панель пристроїв розумного дому

Як вже було вказано вище, технологія Інтернету речей дозволяє будувати системи не тільки побутового характеру, але ще й міського (рис. 2.7), промислового (рис.2.8) або енергоефективного (рис. 2.9). Тому у Cisco Packet Tracer можлива реалізація і таких схем.

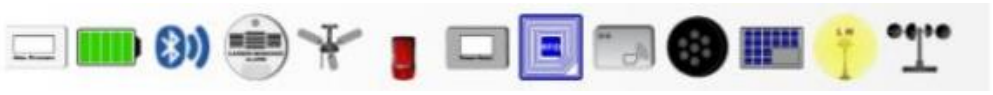

Рисунок 2.7. Панель пристроїв розумного міста

Для промислового моделювання пропонується використання наступних приладів: батареї, датчики диму, газу, розприскувачі води, нагрівальні елементи, вітряки, сонячні батареї і таке інше.

Рисунок 2.8. Панель пристроїв промислового Інтернету речей

Для проектування енергоефективних мереж пропонується використання: сонячної батареї, вольтметру, генератору вітру, датчику вітру, тощо.

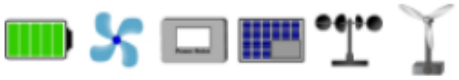

Рисунок 2.9. Панель пристроїв електроенергетичної мережі

Важливим етапом проектування мережі Інтернету речей під’єднання мікроконтролерів (рис. 2.10) (MSU або SBD), які допомагають запрограмувати розумний пристрій спрацьовувати за певним сценарієм.

Рисунок 2.10. Мікроконтролери

Cisco Packet Tracer у розрізі побудови мережі для Інтернету речей надає можливість використовувати виконуючі пристрої (рис. 2.11). Наприклад:

нагріваючий елемент, охолоджуючий елемент, теомостат, розприскувач води, гучномовець, LED дісплей, тощо.

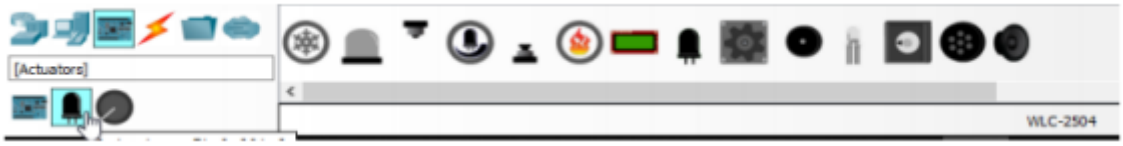

Рисунок 2.11. Виконуючі пристрої

Залежно від різних налаштувань для з’єднання використовувалися різні типи дротів. Також для мікроконтролера може бути використаний спеціальний кабелі Інтернету речей. Як видно на рисунку 2.12 нижче, Cisco Packet Tracer запропонував кілька варіантів кабельного підключення, однак важливою особливістю є опція автоматичного підключення кабелю (значок блискавки на малюнку). Вибираючи його, Cisco Packet автоматично вибирає правильний кабель для з’єднання двох мережевих інтерфейсів. З метою навчання цю опцію також можна вимкнути.

Рисунок 2.12. Панель дротів

Провівши аналіз перерахованих вище можливостей, можна дійти висновку і переконатися, що Cisco Packet Tracer наділений широким спектром можливостей для проектування розумних мереж та застосуванню технології Інтернету речей. Програма може бути використана як для навчальної мети в школі або університеті, так і для власної потреби користувача у проектуванні моделі власного житла. Cisco Packet Tracer широко розповсюджений та застосовується для моделювання мереж по всьому світу. Ця програма підходить для використання людьми різного рівня технічної обізнаності, що робить її такою популярною. Спроектована мережа дає можливість візуально

оформити та підготуватися до створення та налаштування електронної моделі розумного будинку на платі.

2.4. Методика досліджень та шляхи пошуку нових технічних рішень для розв’язання поставлених задач

Існуючі невирішені технічні проблеми та протиріччя слід досліджувати, щоб визначити основні проблеми та корінь кожної проблеми. У ході дослідження необхідно визначити, що саме є основною перешкодою, яка заважала дослідникам розв'язати певні технічні проблеми в цій галузі.

Після виявлення першопричин тих чи інших проблем та основних перешкод у боротьбі з ними слід спрямувати дослідження на пошук шляхів подолання цих проблем та основних перешкод. При застосуванні нових методів і підходів може виникнути необхідність знехтувати деякими іншими властивостями системи.

Щоб критичні та важливі властивості системи не постраждали та не погіршилися під час змін у системі, необхідно заздалегідь сформулювати рамки, за які неможливо вийти далі в процесі розробки нових рішень: певні обмеження на властивості системи, якими не можна нехтувати під час розробки та впровадження нових рішень.

Неоднорідність в системах управління «Розумним будинком» присутня на багатьох рівнях системи, від якоїсь неоднорідності позбутися не вийде; зокрема, неможливо позбавити систему необхідності знати про неоднорідність апаратного забезпечення, з яким система працює (про деталі взаємодії з пристроями кожного типу: їх інтерфейси, протоколи тощо). Позбутися такої неоднорідності можна лише запровадивши уніфікацію пристроїв в єдиний протокол взаємодії, але організаційно забезпечити використання єдиних уніфікованих інтерфейсів і протоколів різними виробниками пристроїв для

Розумного дому вкрай складно, тому ні Ви повинні створити завдання позбутися такого роду неоднорідності.

Однак системи управління розумним будинком часто також мають неоднорідність на всіх інших вищих рівнях системи, така неоднорідність породжується неоднорідністю пристроїв і призводить до паралельних і неуніфікованих способів керування цими пристроями навіть на інтерфейсах. , користувач. . ви змушені керувати різними пристроями по-різному, інтерфейс користувача буде іншим.

Цього типу гетерогенності можна уникнути, якщо ці високорівневі системи взаємодіють з гетерогенними пристроями однаково, тобто пристрої не виглядатимуть гетерогенними на цих рівнях. Щоб досягти на цих рівнях певної уніфікації пристроїв будь-якого типу в єдиній формі, можна ввести деяку абстракцію на певному рівні досить низько в системі, за якою буде прихована неоднорідність пристроїв.

Рівень системи, на якому введено таку абстракцію, буде знати про неоднорідність пристроїв, але не видаватиме зовнішнім (вищим рівням системи) деталі цієї неоднорідності шляхом уніфікації всіх цих пристроїв. для вищих рівнів системи. Введена абстракція повинна запропонувати певний уніфікований інтерфейс і протокол взаємодії з пристроєм (Smart Thing).

Такий підхід не повністю усуне неоднорідність у системі керування «Розумним будинком», але він усуне неоднорідність на вищих рівнях системи, забезпечуючи простоту системи на цих вищих рівнях, а також сприяючи розвитку. , обслуговування та розширення цих рівнів системи.

Згідно з вимогою, щоб системи управління «Розумним будинком» могли дистанційно керувати будинком через Інтернет, класична архітектура системи передбачає наявність у домі фізичного комп’ютера – шлюзу. Уся взаємодія користувача з Smart Things (пристроїв) у домі відбувається через цей шлюз, і цей шлюз є єдиною сутністю, яка безпосередньо взаємодіє з пристроями Smart Home. Така архітектура обрана через складність і непрактичність забезпечення

кожного Smart Thing автономним доступом до мережі Інтернет, а також наявність у системі серйозного власного комп’ютера.

Цілком логічно, що ці шлюзи виступають місцем авторизації запитів до Розумного будинку в системі управління, оскільки не рекомендується робити це окремо для кожного пристрою. Це недоцільно, по-перше, через надмірну складність (як програмну, так і апаратну) цих пристроїв у такому випадку, що важко, неефективно та дорого, а по-друге, через те, що шлюз є по суті єдиною точкою доступу до будинку з назовні через Інтернет. Тому авторизацію логічно проводити на рівні шлюзу.

Тому, оскільки рекомендовано, щоб шлюз був єдиною точкою авторизації для запитів до Розумного дому, і оскільки шлюз сам по собі є комп’ютером, який міг би надати йому достатню обчислювальну потужність для виконання криптографічних операцій, можна реалізувати Шлюз є основою для забезпечення неможливості керування будинком із зовнішнього центрального сервера без відома користувача.

Треба спробувати вирішити цю проблему за допомогою асиметричної криптографії та цифрових підписів. Цифрові підписи дозволять засвідчити автора команди управління, що надсилається на шлюз, щоб шлюз, як контрольна точка Розумного будинку, міг переконатися, що команда керування надходить із надійного джерела. Такий підхід унеможливить управління будинком користувача навіть з центрального сервера.

У процесі первинного підключення будь-якого пристрою (Smart Thing) до дому за допомогою бездротових протоколів існує ризик того, що зловмисник отримає контроль над пристроєм. У існуючих системах початкова безпека з’єднання зазвичай базується лише на припущенні, що під час початкового підключення Smart Thing до дому (зокрема, шлюзу) поблизу не буде зловмисників, які активно шукатимуть пристрої. Однак цей спосіб явно не є надійним.

Зокрема, проблема полягає в тому, що важко побудувати надійну лінію довіри, щоб пристрій під час початкового підключення міг напевно знати, якому з передплатників протоколу бездротової передачі даних навколо нього можна довіряти. Таким чином, під час підключення зловмисник може видати себе за шлюз і змусити пристрій підключитися до нього та довіряти йому в майбутньому. Крім того, зловмисник також може видавати себе за пристрій, який він бере під свій контроль, і підключається до шлюзу, здійснюючи таким чином так звану атаку MITM (Man In The Middle), у цьому випадку користувач навіть не помітить, що він контролює їх Smart Thing було вилучено

Абсолютно надійний спосіб побудувати лінії довіри між шлюзом і розумною річчю під час їх початкового з’єднання – це використовувати апаратне з’єднання між шлюзом і пристроєм під час початкового з’єднання (наприклад, через кабель або штекер) – цей процес означає, що шлюз і пристрій точно фізично з'єднані і що пристрій з'єднується через бездротовий протокол саме з тим абонентом, до якого він фізично підключений в даний момент. Однак цей шлях не є економічним, оскільки він вимагає додавання нового апаратного інтерфейсу до кожної Smart Thing, який використовуватиметься виключно під час початкового підключення.

Щоб побудувати надійну лінію довіри між шлюзом і пристроєм програмно, без залучення апаратних інтерфейсів, слід зазначити, що обмін даними під час цього процесу фактично відбувається через загальнодоступні канали передачі даних, тобто іншими словами, він повинен бути припустив, що злочинці можуть читати всі передані дані. У цьому випадку жодні ключі не можуть передаватись відкрито, і також має бути певний ключ, який шлюз отримує від Smart Thing, а не через канал передачі даних через бездротовий протокол; бажано фізично записати ключ на річ, припускаючи, що зловмисник не має фізичного доступу до речі (пристрою). Підхід до ролей користувача в системах не є новим, але його використання в системах управління Розумним будинком не було помічено. Функціональність ролей надає ролі за

замовчуванням, кожна з яких має чітко визначений діапазон дозволів у системі, і конкретна роль визначається для кожного користувача, або окремий список дозволів визначається для кожного користувача окремо.

Рольовий функціонал ефективно та легко вирішує деякі потреби користувачів Розумного дому, зокрема, він дає користувачеві можливість дозволити комусь іншому частково керувати їхнім домом (наприклад, гостю можна дозволити контролювати лише техніку в кімната, або дитині можна дозволити контролювати все, крім критичної інфраструктури будинку).

Підхід до призначення ролей користувачам добре поєднується з підходом авторизації всіх запитів до Smart House з перевіркою запиту на шлюзі, оскільки надання певних прав певному користувачеві проходитиме через запит до шлюзу.

Проблема впровадження інтелектуального помічника, який надає рекомендації користувачеві з урахуванням його індивідуальних особливостей і побудови профілю комфорту користувача, полягає в складності реалізації такого інтелекту для будь-якого типу Smart Home Things, без необхідності налаштування логіки .і шлях навчання інтелекту окремо для кожного типу. Такий підхід має бути створений для навчання інтелекту для Smart Houses, який не потрібно буде розширювати для кожного нового типу Smart Things.

Щоб досягти цієї мети, необхідно створити процедуру навчання, яка не знає про функціональні характеристики та природу Smart Things. Це частково пов’язано з абстракцією, впровадження якої покликане вирішити проблему неоднорідності пристроїв: інтелект повинен тренуватися на абстрактному уявленні про розумні речі, не надаючи йому інформацію про те, які функції ці розумні речі виконують.

2.5. Забезпечення безпеки початкового з’єднання Розумної Речі зі Шлюзом Розумного Будинку

Проблема безпеки, коли Smart Thing спочатку підключається до шлюзу, полягає в тому, що зловмисник може отримати контроль над Smart Thing. Ця штука спілкується зі шлюзом за допомогою певного протоколу бездротової передачі даних у відкритому просторі, а тому небезпечна. З цієї причини дані не можуть передаватись відкрито через мережу під час початкового сполучення Smart Thing і шлюзу, а також має бути забезпечений надійний засіб довіри Smart Thing для шлюзу. Під час початкового підключення на стороні Smart Thing повинні бути створені умови, які дозволять Thing перевірити, що підключення здійснюється до Smart Home Gateway, а не те, що це атака зловмисника. Логічним вирішенням цього збою є використання шлюзом певного секретного ключа в початковому запиті до Smart Thing, який відомий Smart Thing заздалегідь і був переданий на шлюз через певний канал даних, який не є ним. основний канал передачі даних між шлюзом і предметом і точно захищений від перехоплення зловмисниками. Надійним каналом для передачі секретного ключа Річі до шлюзу явно не може бути будь-яка бездротова лінія передачі даних, оскільки проблеми вимагають, щоб початкове з’єднання Річі з Будинком було повністю чутно будь-яким радіо. хвильовий канал для передачі даних, тобто середовище передачі даних необхідно вважати повністю публічним. З цими обмеженнями існує лише два способи передачі конфіденційних даних: – фізичне апаратне з’єднання Smart Thing зі Шлюзом (за допомогою кабелів або через спеціальний апаратний інтерфейс); – користувач буде вводити певні дані в Шлюз, які фізично зчитуватиме в автономному режимі (наприклад, в тілі Smart Thing). Smart Thing зазвичай не потребує жодних апаратних інтерфейсів, окрім початкового сполучення, тому варто спробувати обійти цю помилку, не залучаючи додаткових апаратних інтерфейсів, встановлення яких безпідставно збільшить

ціну пристрою. Тому вибирається маршрут, за яким фізично офлайн користувач отримує певні дані (секрет), які він передає на шлюз через інтерфейс шлюзу по захищеному каналу. Потім шлюз повинен передати цей секрет Речі, щоб автентифікувати себе та завоювати довіру Речі. Оскільки канал передачі даних Gateway-Reach відкритий, секрет не можна передавати відкрито. Теоретично можна зробити секрет Smart Thing динамічним, але в цьому випадку Річі важко фізично показати свій секрет; наприклад, потрібно було б встановити екран на Smart Thing, що теж економічно недоцільно, тому припустимо, що секрет є статичним для всіх підключень до Thing. Таким чином, шлюз повинен знайти спосіб запевнити Smart Thing, що він знає секрет, але не транслювати цей секрет через канал даних відкрито. Щоб досягти цього, дані в першому повідомленні Gateway to the Thing повинні бути симетрично зашифровані цим секретом. Крім того, усі наступні повідомлення через канал передачі даних також мають бути зашифровані, але з іншим ключем (або ключами). Враховуючи всі ці описані вимоги, я пропоную протокол початкового підключення Smart Thing до Шлюзу, який відповідатиме вимогам і гарантуватиме необхідний рівень безпеки при передачі даних. Протокол описано на діаграмі послідовності на рис. 2.13.

Рис. 2.13. Діаграма послідовності початкового сполучення Розумної Речі»

На схемі шлюз виконує початкове з'єднання з Smart Thing і після успішного з'єднання надсилає запит до основного сервера для додавання нового Smart Thing. Стрілки на діаграмі послідовності, які супроводжуються прямокутником з двох половин, розділених горизонтально, вказують на передачу певного блоку даних, зашифрованого певним ключем (показано в поясненні внизу діаграми).

Smart Thing приймає перше початкове повідомлення та розшифровує отримані дані за допомогою симетричного ключа, який зашифровано та очікує побачити повідомлення певної структури. Якщо структура декодованого

повідомлення відповідає очікуваній структурі, авторизація шлюзу була успішно завершена, і з цим абонентом можна спілкуватися. Початкове повідомлення містить симетричний ключ шифрування, який буде використовуватися для подальшого спілкування. У відповідь на перше повідомлення від Шлюзу Розумна Річ повинна надіслати повідомлення, що містить опис структури цієї Розумної Річі, щоб Шлюз зрозумів, яка взаємодія з цією Річчю можлива і за яким протоколом.

Для додаткової безпеки та надійності під час подальшого зв’язку з Gateway-Reach можна використовувати різні ключі шифрування; змінювати їх кожне наступне повідомлення або кожні N повідомлень. Реалізація таких динамічних ключів не є складною технічною проблемою: потрібно просто надіслати нові ключі шифрування в комунікаційних повідомленнях і переконатися, що одержувач успішно отримав новий ключ і готовий працювати з ним.

Симетричні ключі шифрування слід використовувати саме тому, що калькулятор Smart Things може бути не дуже потужним: Smart Things має використовувати мікроконтролер, а не комп’ютер як калькулятор.

3 РЕАЛІЗАЦІЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В РОЗУМНОМУ БУДИНКУ

3.1. Програмний засіб для системи захисту розумного будинку

Система сигналізації - це основа системи безпеки, професійні пристрої сигналізації, яка дозволяє моментально відреагувати на вторгнення у будинок, при цьому спрацює звукова сирена, яка сповістить сусідів про вторгнення, а також система зробить сповіщення за допомогою дзвінка, СМС на мобільний телефон або в службу позавідомчої охорони [64]. До професійного обладнання для сигналізації можна підключити різного роду пристроїв, наприклад: датчики руху, датчики розбиття скла, датчики відкриття дверей, датчики затоплення, датчики газу, датчики диму, інфрачервоні бар'єри та системи відеоспостереження [65].

Практично будь-яким пристроєм, який присутній в системі та використовується, надається можливість віддаленого керування за допомогою пульта дистанційного керування, комп’ютера, планшета або смартфона: iPhone, Android, Windows Phone [66]. Також, керувати розумним будинком можна і за допомогою зручної сенсорної панелі управління [67].

Дуже важливо для забезпечення захисту використовувати правильно сконфігурованої автентифікації та шифрування передачі даних. Безпека при розробці та написання програмного коду для Інтернет речей є дуже важливою, оскільки різного роду атаки можуть загрожувати стабільності та безперервності роботи будь-якої системи, в тому числі системі розумний будинок.

При використані GSM-модуля, є ймовірність перехвату відправленого повідомлення зловмисником, тобто здійснення атаки «Людина в середині».

Процес проходження віддаленої автентифікації з використанням GSM-модуля, відбувається завдяки унікально мобільного номеру телефону. Тобто в

коді програми, записано списки номерів яким надається доступ до віддаленого управління системою, номери яких немає в списку і при отримані від них будь-яких запитів система автоматично їх відкидає, але залишається можливість підміни мобільного номеру телефону зловмисника на номер власника системи.

При використані модуля Bluetooth, захист буде здійснюватися завдяки накладання пароля на підключення до точки входу. Одним з недоліків такого методу, є можливість застосування «грубої сили - Brute», тобто метод підбору пароля по словнику.

Загальний алгоритм роботи системи по захисту розумного будинку зображено на рис. 3.1.

Рис. 3.1. Загальний алгоритм роботи програмної частини системи захисту розумного будинку

Прикладом фрагмент коду, який спрацьовує при обриві розтяжки та загорається світлодіод наведено нижче:

```
if (digitalRead(SH1))
{ //Очікування логічної 1 на 9 піні
digitalWrite(7,HIGH); //Загоряння світлодіода на 7 піні}
else { //Якщо обриву не було
digitalWrite(7,LOW); // Світлодіод вимкнутий }
```

Для управління системою з мобільного додатку, необхідно оголосити зміну, яка відповідає за надіслані дані з Bluetooth (char incomingbyte;).

Для датчика руху, необхідно вказати максимальну та мінімальну відстань виявлення загрози. При використані RFID, необхідно попереднє зчитування міток та побудова логічних дій.

Таким чином, сучасний розумний будинок є набором: датчиків, контролерів, засобів передачі даних та різного роду мікропроцесорних систем, які значно спростили життя у сьогоднішньому швидкому темпі розвитку технологій. З точки зору безпеки, розумний будинок не раз піддавався зламу та потребує більш кращого підходу до запровадження безпеки та різних протоколів обміну ключовою інформацією. Наведена програмна реалізація системи захисту розумного будинку використовує різного роду датчиків руху, дальності, RFID-міток, модуля Bluetooth, GSM та інших складових частин. Головною властивістю запропонованої реалізаціє є те, що завдяки віддаленому управлінню системою та моніторингом, буде отримане повідомлення про будь яке проникнення в будинок та запровадження автентифікації в системі. Розглянуто все можливі методи зламу системи та їх протидія.

3.2. Опис функціонування системи

Наведемо структурну схему системи інформаційної безпеки (рис. 3.2).

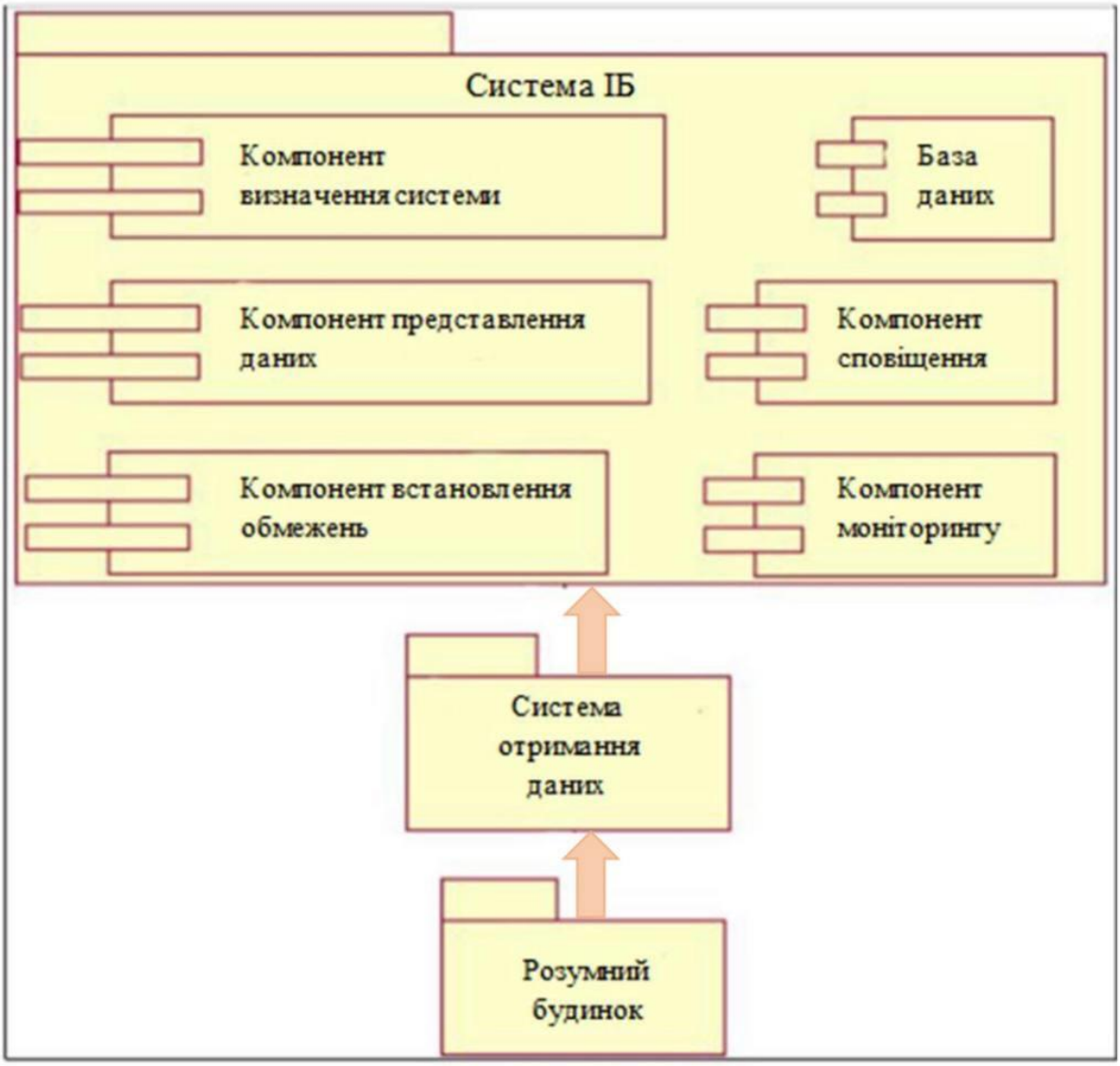

Рис. 3.2. Структурна схема інформаційної безпеки розумного будинку

Розглянемо детальніше вибрані елементи системи:

- компонент визначення системи необхідний для визначення складу системи DM на основі отриманих даних;

- компонент представлення даних використовується для відображення даних, отриманих системою інформаційної безпеки користувачу;

- компонент встановлення обмежень необхідний для автоматичного визначення обмежень для зчитування елементів системи РБ з отриманих даних;

- база даних використовується для зберігання даних про склад системи РБ, класифікації загроз інформаційної безпеки та даних, яку вона використовує;

- компонент моніторингу контролює стан системи РБ шляхом перевірки вхідних даних та виявлення розбіжностей;

- компонент сповіщення служить для інформування користувача про виявлені загрози або підозрілі дії.

Цей алгоритм виконується системою ІБ щодо складу системи РБ і встановлення обмежень шляхом додавання користувачем вручну кожного елемента системи РБ.

3.3. Алгоритмічне забезпечення

Для розроблення системи оцінки загроз у кіберфізичній системі було розроблено діаграми діяльності щодо визначення складу системи та алгоритму моніторингу даних.

Для відображення алгоритму визначення користувачем складу системи РБ було побудовано діаграму діяльності (рис. 3.3).

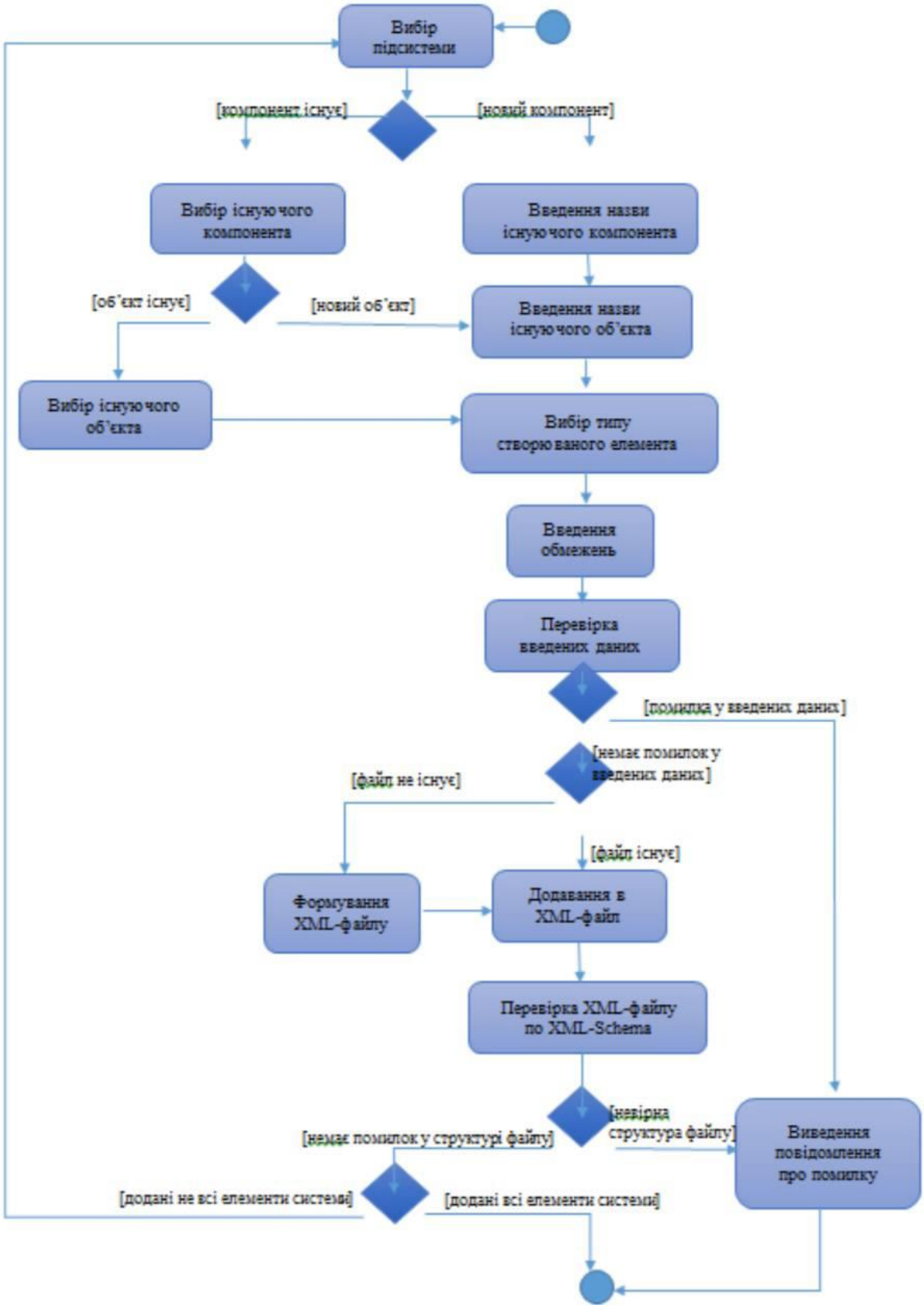

Рис. 3.3. Алгоритм визначення користувачем складу системи РБ

Для автоматичного визначення складу системи РБ было розроблено алгоритм, який виконується системою інформаційної безпеки, що входить до складу розумного будинку, і встановлює обмеження шляхом отримання «ідеального» стану системи. Для відображення алгоритму было побудовано

діаграму діяльності (рис. 3.4).

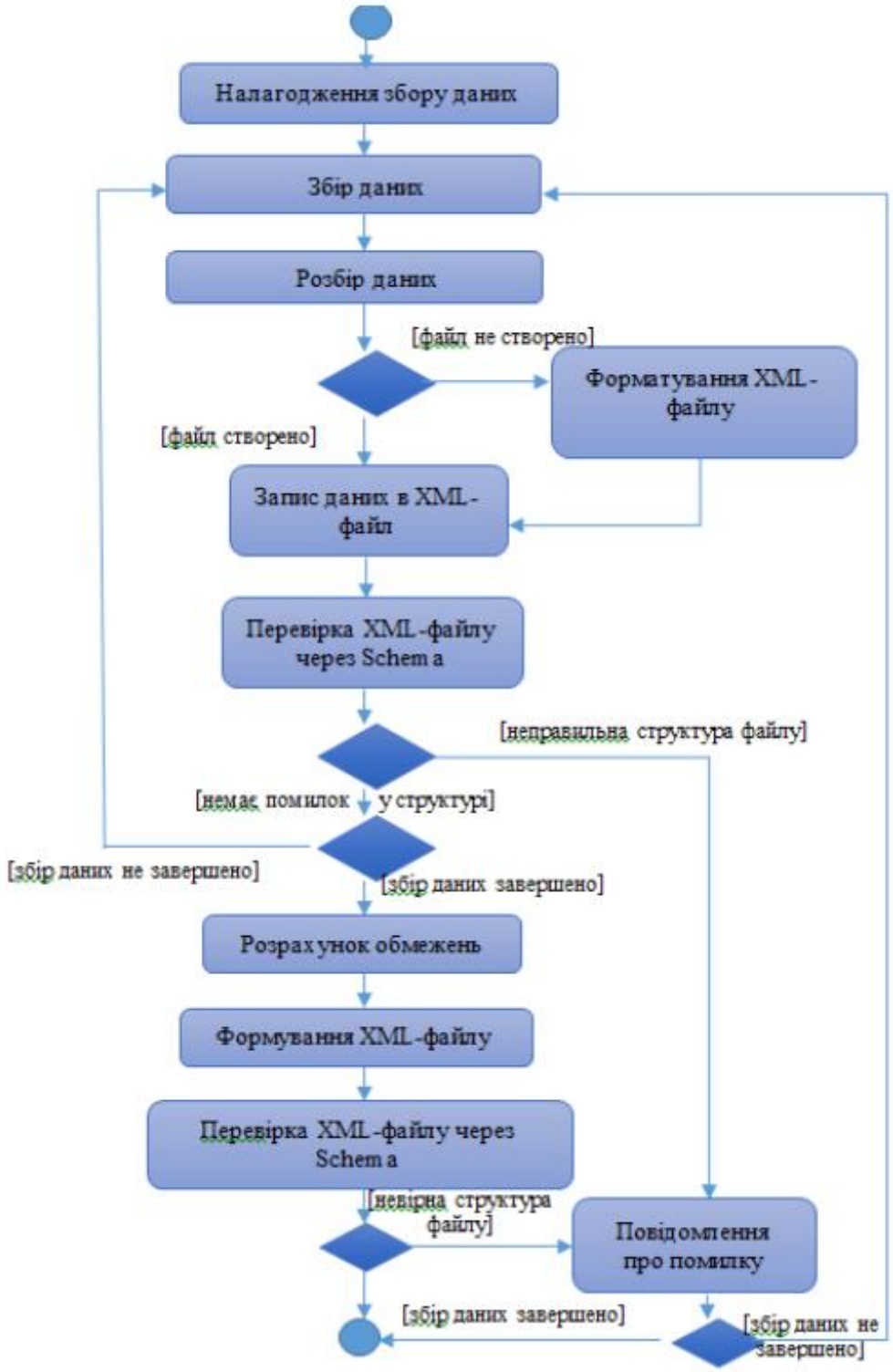

Рис. 3.4. Алгоритм автоматичного визначення складу системи РБ

Алгоритм моніторингу стану системи РБ полягає у перевірці всіх отриманих даних із системи РИБ у режимі реального часу. Для відображення алгоритму було побудовано діаграму діяльності (рис. 3.5).

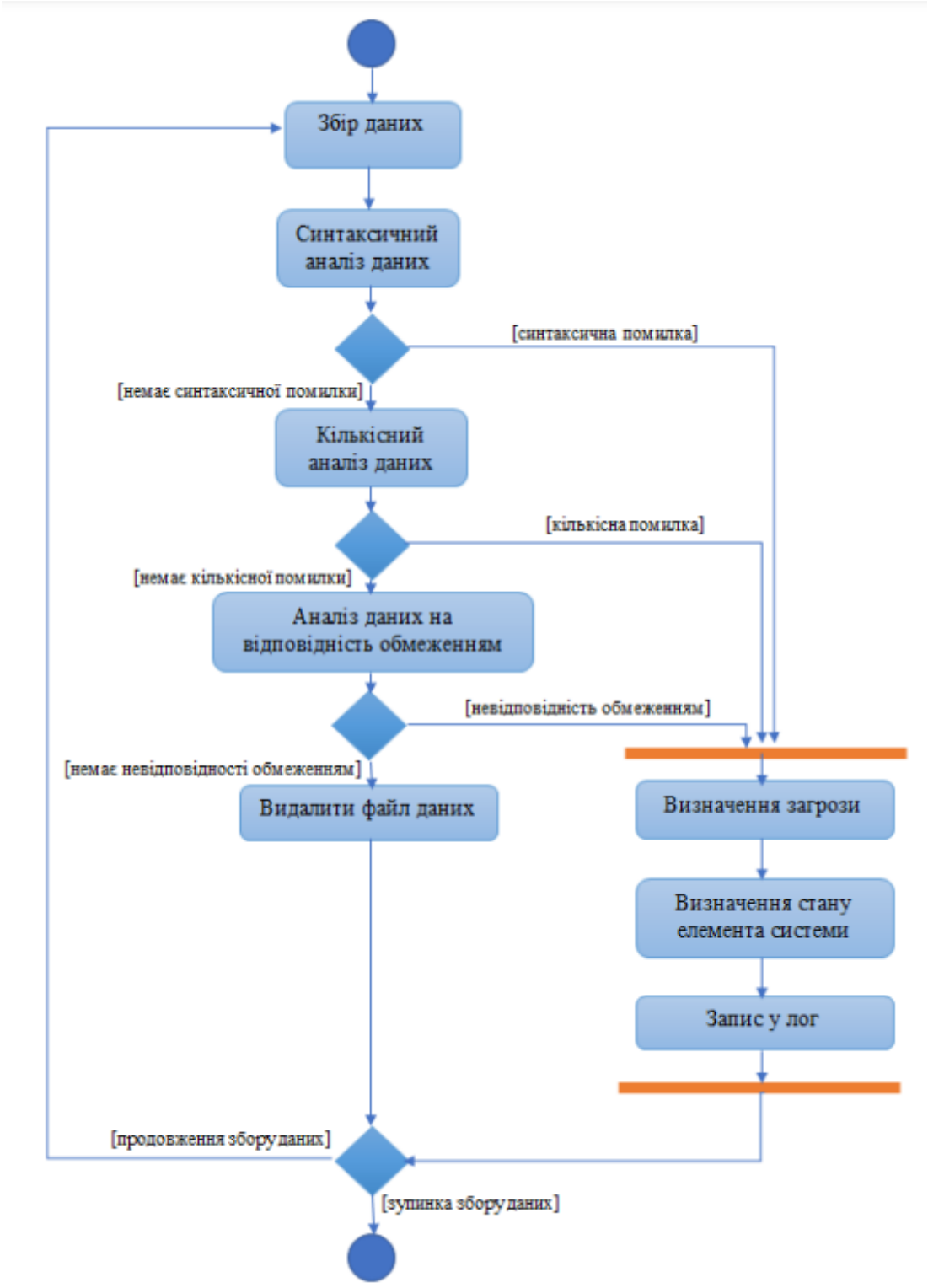

Рис. 3.5. Алгоритм моніторингу стану системи РБ

У проектованій системі інформаційної безпеки для опису даних про склад системи «Розумний будинок» та для опису загроз інформаційної безпеки було обрано формат XML. Для опису структури файлів XML була використана мова XML Schema.

При визначенні складу системи РБ користувачем самостійно шляхом визначення кожного елемента системи формується XML-файл опису системи РБ. Графічне представлення схеми опису складу системи РБ зображено на рисунку 3.6.

При автоматичному способі визначення складу системи РБ спочатку формується файл з «ідеальним» станом системи, потім розраховуються обмеження елементів системи, і формується файл з описом складу системи РБ. Графічне представлення файлу, що описує структуру «ідеального» стану системи РБ зображено на рисунку 3.7.

Графічне зображення схеми опису загроз ІБ системи РБ показано на рисунку 3.8.

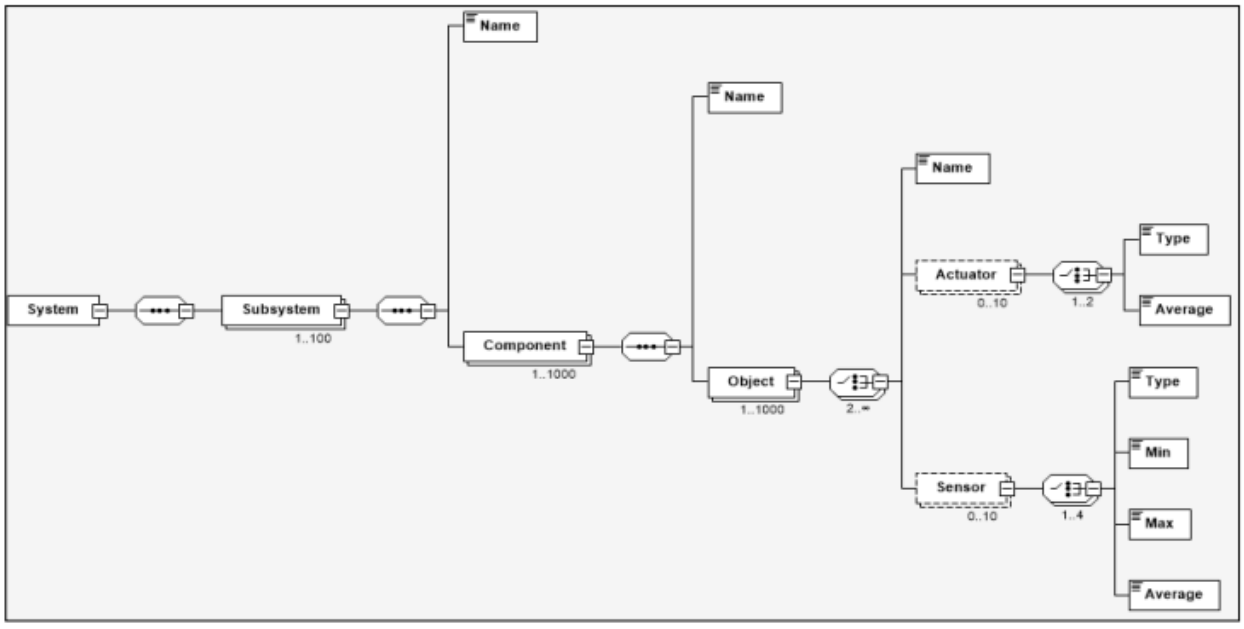

Рис. 3.6. Графічне зображення схеми опису складу системи «Розумний дім»

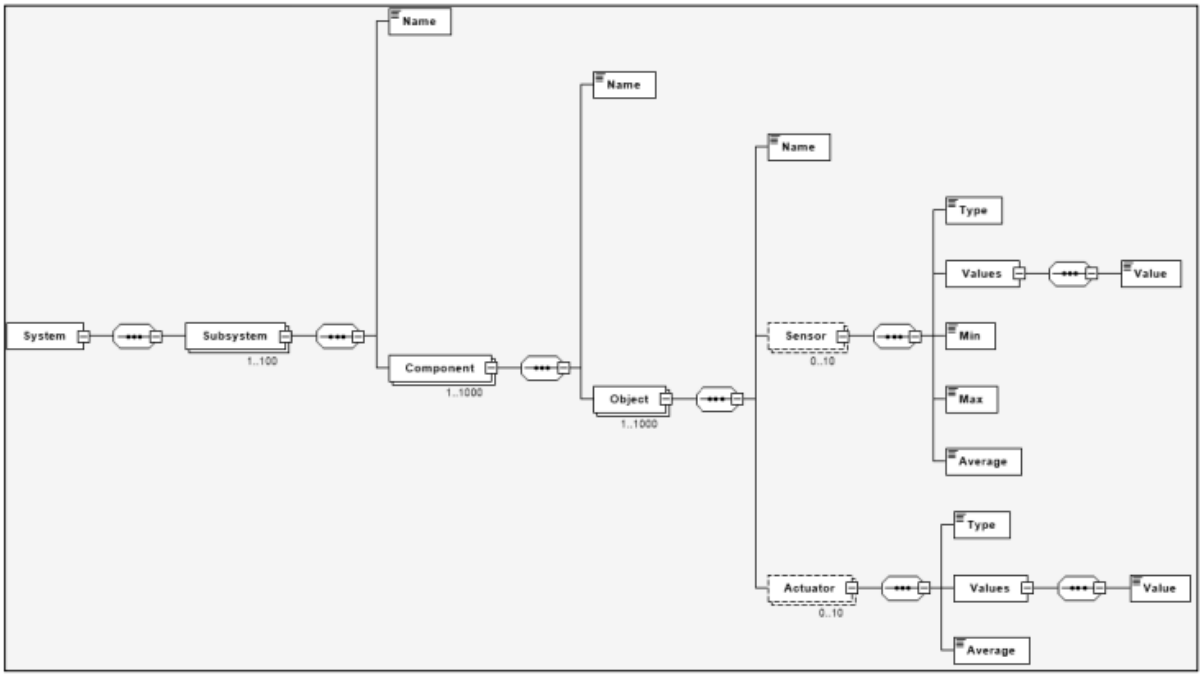

Рис. 3.7. Графічне зображення схеми опису «ідеального» стану системи

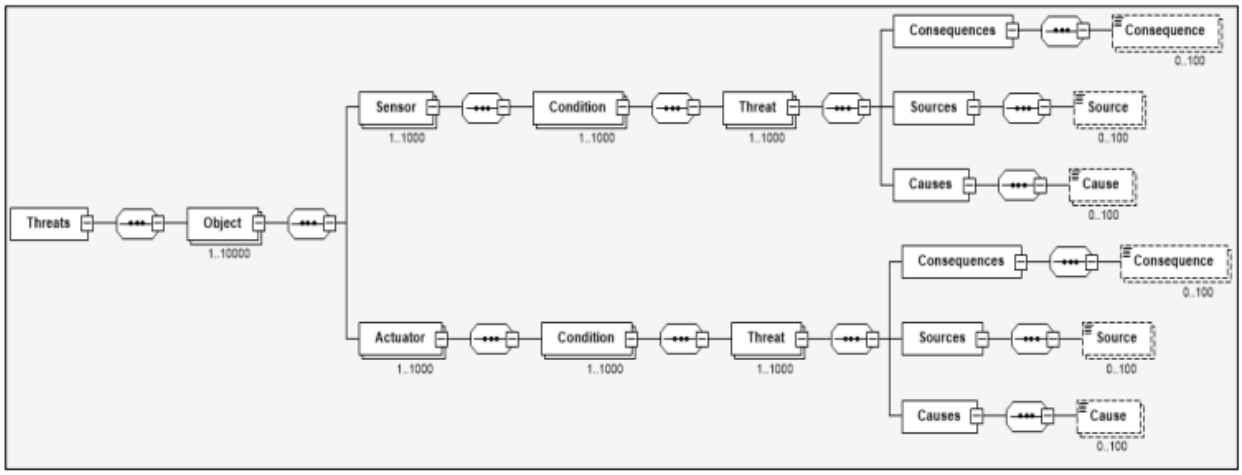

Рис. 3.8. Графічне представлення схеми опису загроз системи «Розумний будинок»

3.4. Розробка системи інформаційної безпеки

До компонентів системи інформаційної безпеки «Розумного будинку», що розробляється, доданий компонент генерування даних. Цей компонент використовує файл-зразок, що визначає склад системи НБ і значення

показників об'єктів управління. Значення показників файлу-зразка використовуються при генерації випадкових значень у файлах, що генеруються. Файли генеруються у окремому потоці програми. Лістинг 1 демонструє потік генерування файлів (кожні дві секунди) з даними та запуску їх моніторингу. Приклад вмісту файла-зразка зображено на рисунку 3.9.

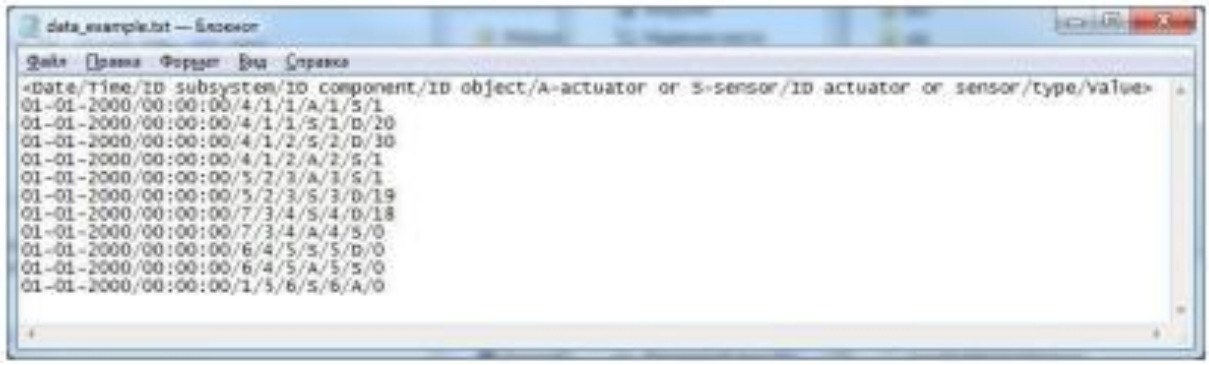

Рис. 3.9. Приклад файлу зразка

При запуску програми необхідно визначити склад системи РБ, після чого будуть доступні кнопки управління моніторингом. Інтерфейс основного вікна для визначення складу системи представлений на рисунку 3.10.

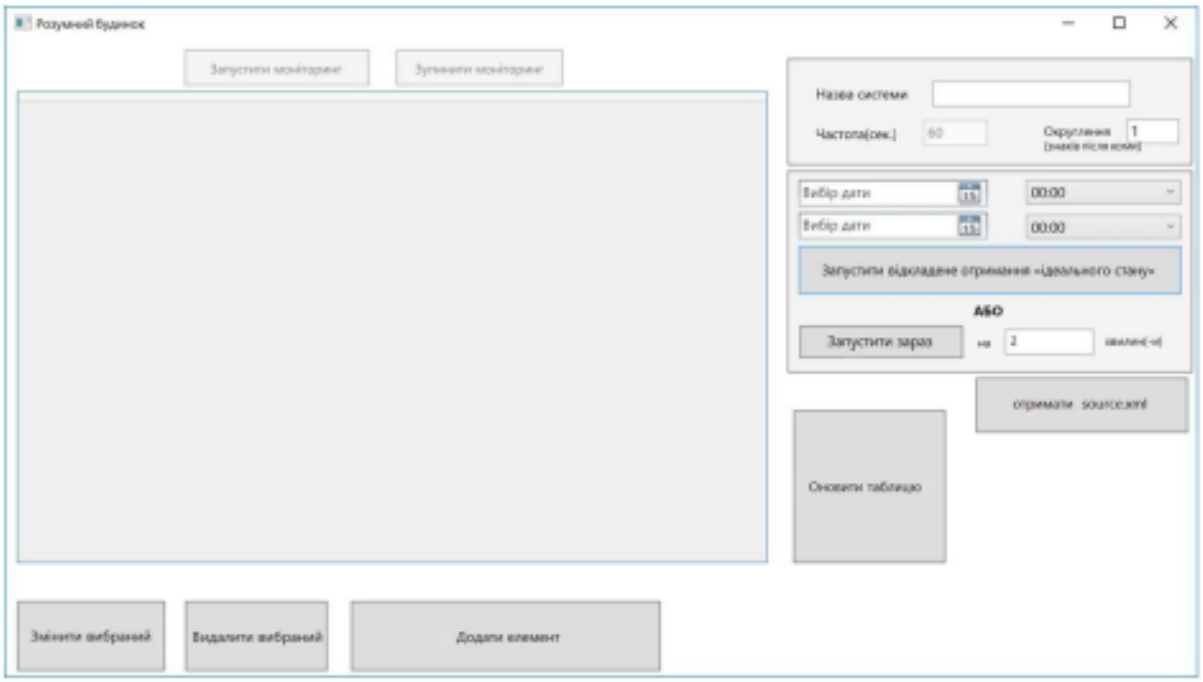

Рис. 3.10. Інтерфейс основного вікна визначення складу системи

Для автоматичного отримання складу системи РБ необхідно в правій частині основного вікна визначити налаштування отримання «ідеального стану»:

- вказати назву системи РБ;
- визначити частоту збору даних (частота генерування файлів з даними);
- вказати ступнь закруглення значень показань (за замовчуванням встановлено заокруглення до одного знака після коми);
- позначити дату та час початку та закінчення відкладеного збору даних, або визначити час закінчення для збору даних у поточний час.

Лістинг 2, який демонструє фрагмент коду, що додає елементи «датчик» або «виконавчий механізм», і дані елементів XML-файлу «ідеального стану системи».

Для самостійного визначення користувачем складу системи РБ необхідно на основному вікні вибрати кнопку «Додати елемент», після чого відкриється вікно для додавання/редагування елемента. Інтерфейс вікна додавання

Елемента представлений на рисунку 3.11.

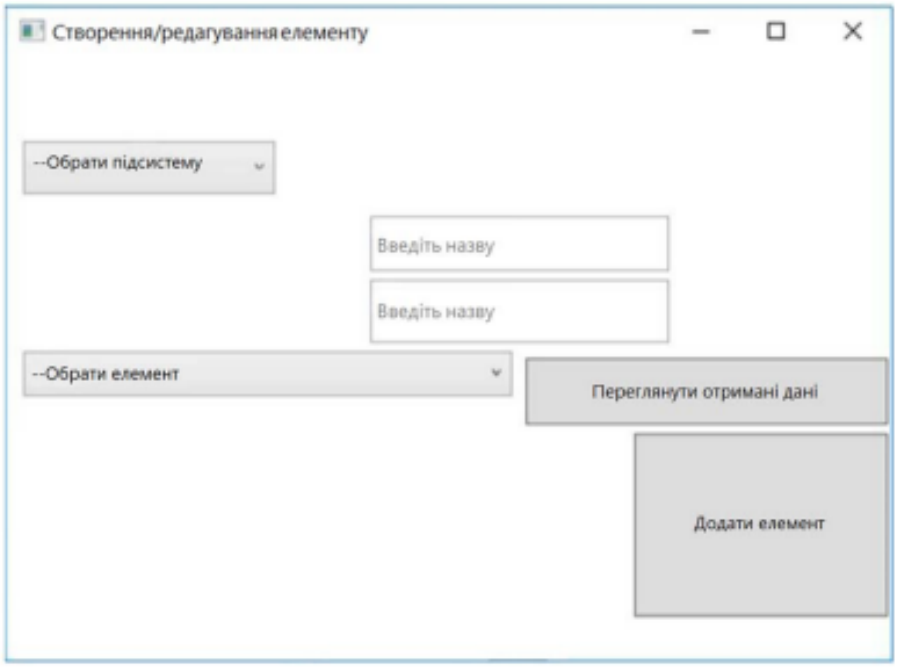

Рис. 3.11. Інтерфейс вікна додавання елемента

Користувачеві необхідно вибрати зі списку підсистему, ввести назви для компонента підсистеми та об'єкта управління (або вибрати з існуючих, якщо вони були додані раніше), вибрати створюваний елемент. Після вибору елемента, стануть доступні список для визначення типу елемента, текстові поля для визначення обмежень. Приклад заповненої форми створення датчика елемента управління лампочки представлений на рисунку 3.12.

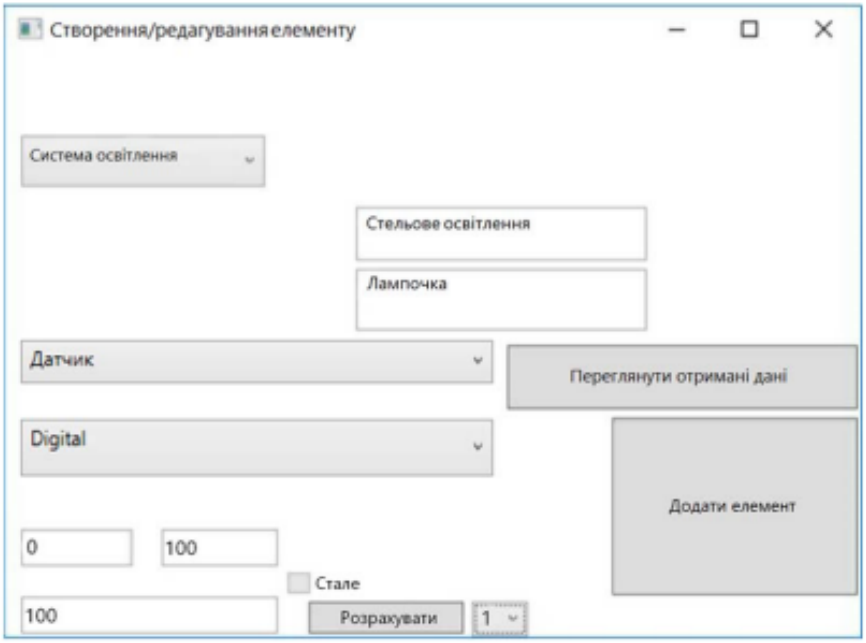

Рисунок 3.12. Інтерфейс заповненого вікна додавання елемента

Після визначення складу системи у таблиці на основному вікні програми з'являться дані про елементи. Дані в таблиці можна сортувати за спаданням та зростанням будь-якого стовпця. Приклад заповненої таблиці з даними представлено на рисунку 3.13.

SubsystemName	SubsystemID	ComponentName	ComponentID	ObjectName	ObjectID	Average	Min	Max	ID	Type	Name	State
Система освітлення	4	Стельове освітлення	1	Лампочка	1	83	--	--	1	Switch	Actuator	green
Система освітлення	4	Стельове освітлення	1	Лампочка	1	24,5	11	38	1	Digital	Sensor	green
Система освітлення	4	Стельове освітлення	1	Лампочка	2	33,7	5	54	2	Digital	Sensor	green
Система освітлення	4	Стельове освітлення	1	Лампочка	2	83	--	--	2	Switch	Actuator	green
Система опалення	5	Опалення житлових кімнат	2	Батарея	3	16,2	7	28	3	Digital	Sensor	green
Система опалення	5	Опалення житлових кімнат	2	Батарея	3	83	--	--	3	Switch	Actuator	green
Система кондиціонування	7	Спільне кондиціонування	3	Кондиціонер	4	18,2	1	30	4	Digital	Sensor	green
Система кондиціонування	7	Спільне кондиціонування	3	Кондиціонер	4	16	--	--	4	Switch	Actuator	green
Система вентиляції	6	Вентиляція вікон	4	Вікно	5	0	0	30	5	Digital	Sensor	green
Система вентиляції	6	Вентиляція вікон	4	Вікно	5	16	--	--	5	Switch	Actuator	green
Система керування і зв'язку	1	Сервер	5	Системний блок	6	1	0	1	6	Analog	Sensor	green

Рис. 3.13. Екранна форма таблиці з даними

Лістинг 3 демонструє метод заповнення таблиці даними з XML-файлу зі складом системи.

Такі дані елементів як назва та обмеження можна змінювати, для цього необхідно виконати подвійне натискання на потрібній комірці або вибрати

рядок у таблиці та натиснути кнопку «Змінити вибраний». У першому варіанті відкриється вікно для редагування конкретного значення даних елемента (рис. 3.14), у другому відкриється заповнене даними елемента вікно додавання/редагування елемента, описане раніше.

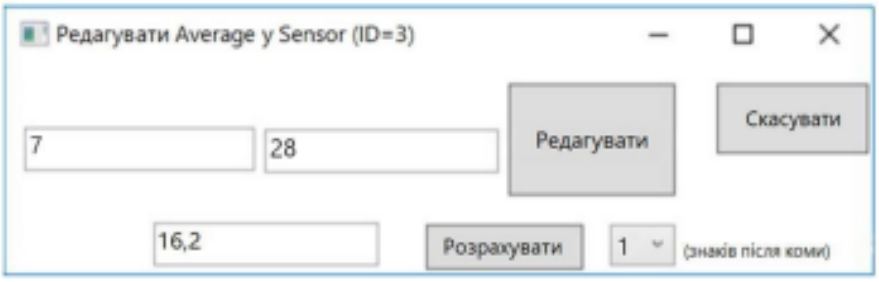

Рис. 3.14. Приклад редагування осередку таблиці

Для запуску моніторингу стану системи РБ на головному вікні потрібно вибрати кнопку «Запустити моніторинг». За потреби моніторинг стану РБ можна залишити, вибравши кнопку «Зупинити моніторинг». При виявленні погроз та невідповідності показань датчика або виконавчого механізму об'єктів керування, у таблиці з даними змінюється значення елемента в стовпці «State» (статус) і рядок елемента підсвічується кольором. Приклад зовнішнього вигляду таблиці з даними, у яких виявлено загрози, представлено на рисунку 3.15.

SubsystemName	SubsystemID	ComponentName	ComponentID	ObjectName	ObjectID	Average	Min	Max	ID	Type	Name	State
Система освітлення	4	Стельове освітлення	1	Лампочка	1	83	--	--	1	Switch	Actuator	green
Система освітлення	4	Стельове освітлення	1	Лампочка	1	24,5	11	38	1	Digital	Sensor	red
Система освітлення	4	Стельове освітлення	1	Лампочка	2	33,7	5	54	2	Digital	Sensor	Red
Система освітлення	4	Стельове освітлення	1	Лампочка	2	83	--	--	2	Switch	Actuator	green
Система опалення	5	Опалення житлових кімнат	2	Батарея	3	16,2	7	28	3	Digital	Sensor	red
Система опалення	5	Опалення житлових кімнат	2	Батарея	3	83	--	--	3	Switch	Actuator	green
Система кондиціонування	7	Спільне кондиціонування	3	Кондиціонер	4	18,2	1	30	4	Digital	Sensor	red
Система кондиціонування	7	Спільне кондиціонування	3	Кондиціонер	4	16	--	--	4	Switch	Actuator	green
Система вентиляції	6	Вентиляція вікон	4	Вікно	5	0	0	30	5	Digital	Sensor	red
Система вентиляції	6	Вентиляція вікон	4	Вікно	5	16	--	--	5	Switch	Actuator	green
Система керування і зв'язку	1	Сервер	5	Системний блок	6	1	0	1	6	Analog	Sensor	red

Рис. 3.15. Приклад таблиці виявленими загрозами

У методі перевірки даних при виявленні помилок визначається їхній вигляд. Список описаних помилок показаний на рис. 3.16.

№ помилки	Вид помилки
1	Помилка у форматі дати
2	Помилка у форматі часу
3	Помилка у форматі ID підсистеми
4	Помилка у форматі ID компонента
5	Помилка у форматі ID об'єкта
6	Помилка у вигляді виду елемента
7	Помилка у форматі ID елемента
8	Помилка у форматі типу елемента
9	Помилка у форматі значення елемента
33	Не знайдено підсистему із заданим ID
44	Не знайдено компонент із заданим ID
55	Не знайдено об'єкт із заданим ID
771	Не знайдено датчик із заданим ID
772	Не знайдено виконавчий механізм із заданим ID
8810	У датчика із заданим ID не вказано тип
881	Невірний тип датчика
8820	У виконавчого механізму із заданим ID не вказано тип
882	Невірний тип виконавчого механізму
99	Дані сенсора не відповідають обмеженням
100	Неправильна кількість елементів даних
103	У вхідному масиві відсутні дані щодо підсистеми
104	У вхідному масиві відсутні дані щодо компоненту
105	У вхідному масиві відсутні дані щодо об'єкту
1071	У вхідному масиві відсутні дані щодо датчика
1072	У вхідному масиві відсутні дані про виконавчий механізм

Рис. 3.16. Список помилок

Подвійне натискання на статус елемента відкриває вікно з детальною інформацією про можливу загрозу. Приклад відомостей про загрозу, виявлену в датчику розтину корпусу сервера системи управління, представлений на рисунку 3.17.

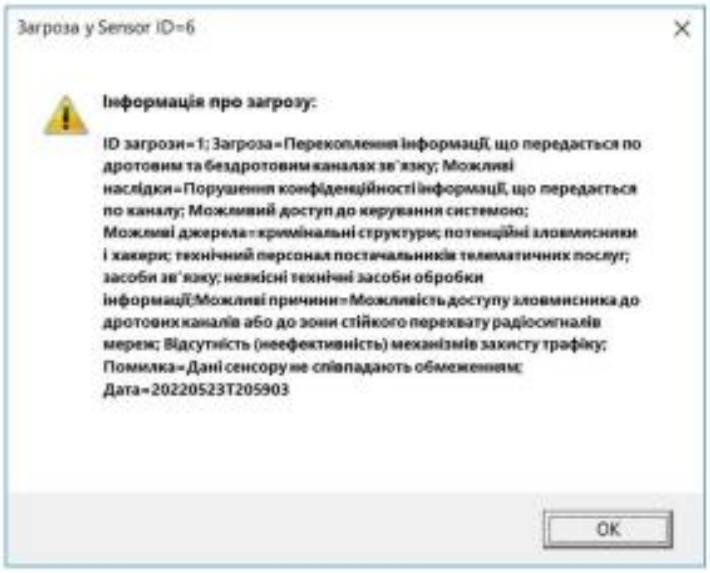

Рис. 3.17. Вікно відомостей про можливі загрози

За відсутності даних про загрозу система ІБ надає користувачеві дані про помилку та дату її виявлення. Приклад відомостей про невідому загрозу, виявлену в датчику відкриття вікна, представлений на рисунку 3.18.

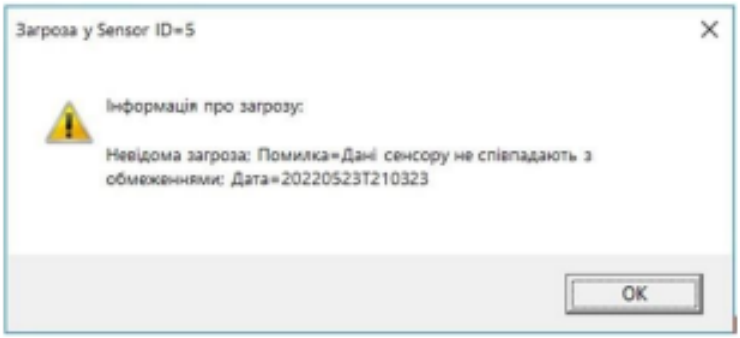

Рис. 3.18. Вікно відомостей про невідому загрозу

В результаті виконання кваліфікаційної бакалаврської роботи було розроблено застосунок, необхідний для оцінки загроз та аналізу безпеки системи «Розумного будинку». Застосунок визначає склад системи «Розумного будинку» та встановлює ліміти для відображення об'єктів керування користувачами, забезпечує моніторинг даних системи РБ та формує повідомлення про стан системи РБ, у випадку виявлення загроз інформує користувача повідомленням.

ВИСНОВКИ

Таким чином було проаналізовано IoT, який надає широкий спектр можливостей споживачам та організаціям різних галузей, наприклад: медицина, логістика тощо. У зв‘язку з популяризацією IoT, розробники отримують нові задачі з гарантування безпеки IoT-додатків, оскільки останні мають доступ до великої кількості конфіденційних даних.

Також розроблено систему захисту розумного будинку, яка базується на основі двох апаратнопрограмних платформ: Arduino Uno та Arduino Nano. До скаладу системи також входять різного роду модулі, а саме: Bluetooth, RFID, GSM, датчики руху та відстані.

Виконано дослідження Інтернет речей, яке показало велику проблему в забезпечені безпеки. Яскравим прикладом технології IoT є розумний будинок – система, яка повністю аналізує та оптимізує процес управління житловим простором. Важливим аспектом як IoT, так і розумного будинку є захист даних. Так як практично, будь який пристрій може бути зламаний.

Рекомендовано в подальшій роботі використовувати складні паролі для Bluetooth. Для захисту інформації, яка зберігається на пристроях та в момент її передачі, використовувати строгу автентифікацію, шифрування і безпечне управління ключами шифрування. Одним з можливих способів підвищення стійкості Інтернет речей і в тому ж числі розумного будинку є створення не тільки стійкого програмного забезпечення, а й перенесення частини цієї задачі на апаратне забезпечення.

Для забезпечення безпеки даних в RFID, буде застосовано захист даних, які збережених в пам'яті від несанкціонованого доступу, а також забезпечення цілісності даних та автентифікація.

У ході магістерської роботи було отримано проект робочої інтелектуальної домашньої мережі «Smart House» у симуляторі Cisco Packet Tracer 7. Для проектування системи було використано бездротовий та

дротовий зв’язок. Перевірено, що усі з’єднані пристрої доступні для керування та моніторингу через веб-інтерфейс кінцевих пристроїв, а саме: смартфону та планшету. Також налаштована внутрішня мережа Wi-Fi для планшета, та стільниковий зв’язок для смартфону. Реалізована можливість реєструвати нових користувачів в системі «розумного будинку» та конфігурувати нові правила взаємодії пристроїв віддалено, або безпосередньо знаходячись у будинку.

За результатами проведеного дослідження запропоновано кіберфізичну систему в основі якої, закладено метод колективної комунікації в кластерній структурі мережі. Запропонований метод забезпечує ефективний обмін даними для обробки виданих запитів, оскільки він утворює енергоефективні кластери, що формуються на основі властивостей речей.

Розглянуто концепцію та принципи та функціонування автоматизованої системи розумного будинку. Проведено порівняльний аналіз переваг та недоліків існуючих рішень в області вирішення проблему забезпечення енергоменеджменту у середовищі розумного будинку.

ПЕРЕЛІК ПОСИЛАНЬ

1. Smart house Розумний дім [Електронний ресурс]. – Режим доступу: URL http://buchuk.domen.uz.ua/index.php?id=smatr-house – Назва з екрану

2. Розумний дім [Електронний ресурс]. – Режим доступу: URL http://sutem.com.ua/pages/7smartbus.html – Назва з екрану

3. Центральні елементи розумного будинку [Електронний ресурс]. – Режим доступу: URL http://sutem.com.ua/021%20inels.phpНазва з екрану

4. Система розумний будинок [Електронний ресурс]. – Режим доступу: URL http://ittel.com.ua/proektuvannya-inzhenernix-merezh/sistema-rozumnij-budinok/ - Назва з екрану

5. Савченко К. В., Войтович О. П. Структурна схема системи захисту розумного будинку // Матеріали конференції XLVI Науково – технічна конференція факультету інформаційних технологій та комп'ютерної інженерії(2017) [Електронний ресурс]–Режим доступу: https://conferences.vntu.edu.ua/index.php/all – fitki/all – fitki – 2017/paper/view/2736 – Назва з екрану

6. Вишньовський В. В., Войтович О. П. Структурна схема системи захисту розумного будинку // Матеріали конференції XLVI Науково – технічна конференція факультету інформаційних технологій та комп'ютерної інженерії(2017) [Електронний ресурс]–Режим доступу: https://conferences.vntu.edu.ua/index.php/all-fitki/all fitki2017/paper/view/2639/2009 – Назва з екрану

7. Конфігурація системи розумний дім [Електронний ресурс]. – Режим доступу до ресурсу: http://amperasmart.ru/article/

8. Розумний будинок — з чого він складається та чи потрібен вам [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://nachasi.com/2018/06/25/smart-house-faq/

9. Як працює система «розумного будинку» CLAP, яку встановлять у 20 тис. Квартир "Укрбуду" [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: http://abcnews.com.ua/ru/markets/kak-rabotaet-sistema-umnogo-domaclap-kotoruiu-ustanoviat-v-20-tys-kvartir-ukrbuda

10. Євтух Б.В. «Система управління розумним домом. Підсистема забезпечення безпеки», [Електронний ресурс] /Євтух. – 2015. – Режим доступу до ресурсу: http://cad.kpi.ua/attachments/093_2015_%D0%B5%D0%B2%D1%82%D1%83%D1%85.pdf

11. Amazon Echo article // Wikipedia URL: https://en.wikipedia.org/wiki/Amazon_Echo (дата звернення: 20.04.2018).

12. Zhang, Y.; Wang, L.; Sun, W.; Green, R.; Alam, M. Distributed Intrusion Detection System in a Multi-Layer Network Architecture of Smart Grids. IEEE Trans. Smart Grid 2011, 2, 796–808.

13. Lugo-Cordero, H.; Guha, R.; Ortiz-Rivera, E. An Adaptive Cognition System for Smart Grids with Context Awareness and Fault Tolerance. IEEE Trans. Smart Grid 2014, 5, 1246–1253.

14. Li, Z.; Liang, Q. Performance Analysis of Multiuser Selection Scheme in Dynamic Home Area Networks for Smart Grid Communications. IEEE Trans. Smart Grid 2013, 4, 13–20.

15. ZigBee Alliance, “Zigbee Specification,” 2006

16. Bluetooth SIG, “Bluetooth core specification version 4.0,” Specification of the Bluetooth System, 2010.

17. E. Mackensen, M. Lai, and T. M. Wendt, “Performance analysis of an Bluetooth Low Energy sensor system,” in 2012 IEEE 1st International Symposium on Wireless Systems (IDAACS-SWS), Sept 2012, pp. 62–66.

18. E. Perahia and M. X. Gong, “Gigabit wireless LANs: an overview of IEEE 802.11 ac and 802.11 ad,” ACM SIGMOBILE Mobile Computing and Communications Review, vol. 15, no. 3, pp. 23–33, 2011.

19. Płaczek, B.; Bernaś, M. Uncertainty-based information extraction in wireless sensor networks for control applications. Ad Hoc Netw. 2014, 14, 106–117.

20. Yick, J.; Biswanath M.; Dipak, G. Wireless sensor network survey. Comput. Netw. 2018, 52, 2292–2330.

21. Akyildiz, I. F.; Su, W.; Sankarasubramaniam, Y.; Cayirci, E. Wireless sensor networks: a survey. Comput. Netw. 2002, 38, 393–422.

22. Xu, R.; Donald, W. Survey of clustering algorithms. IEEE Trans. Neural Netw. 2005, 16, 645–678.

23. Pantazis, N. A.; Stefanos, A. N.; Dimitrios, D. V. Energy-efficient routing protocols in wireless sensor networks: A survey. IEEE Commun. Surveys Tutor. 2013, 15, 551–591.

24. Liu, X. A survey on clustering routing protocols in wireless sensor networks. Sensors 2012, 12, 11113–11153.

25. De Silva, L.C.; Morikawa, C.; Petra, I.M. State of the art of smart homes. Eng. Appl. Artif. Intell. 2012, 25, 1313–1321.

26. Zhang, D.; Shah, N.; Papageorgiou, L.G. Efficient energy consumption and operation management in a smart building with microgrid. Energy Convers. Manag. 2013, 74, 209–222.

27. Pedrasa, M.; Spooner, T.; MacGill, I. Coordinated Scheduling of Residential Distributed Energy Resources to Optimize Smart Home Energy Services. IEEE Trans. Smart Grid 2010, 1, 134–143.

28. United States Department of Commerce, National Telecommunications and Information Administration, United States Department of Commerce. URL: http://www.its.bldrdoc.gov

29. Gu, H.; Diao, Y.; Liu, W.; Zhang, X. The design of smart home platform based on Cloud Computing. In Proceeding of the International Conference on the Design of Smart Home Platform Based on Cloud Computing, Harbin, China, 12–14 August 2011.

30. Płaczek, B.; Bernaś, M. Uncertainty-based information extraction in wireless sensor networks for control applications. Ad Hoc Netw. 2014, 14, 106–117.

31. Saponara, S.; Bacchillone, T. Network Architecture, Security Issues, and Hardware Implementation of a Home Area Network for Smart Grid. J. Comput. Netw. Commun. 2012

32. Gonzalez-Tablas, A.; Ferreres, A.I.; Ramos Alvarez, B.; Garnacho, A. Guaranteeing the Authenticity of Location Information. IEEE Pervasive Comput. 2008, 7, 72–80.

33. Xing, F.; Wang, W. Analyzing Resilience to Node Misbehaviors in Wireless Multi-Hop Networks. In Proceedings of the IEEE Wireless Communications and Networking Conference, WCNC 2007, Kowloon, Hong Kong, China, 11–15 March 2007.

34. Liu, X. A survey on clustering routing protocols in wireless sensor networks. Sensors 2012, 12, 11113–11153.

35. Solis, I.; Obraczka, K. Isolines: Energy-efficient mapping in sensor networks. In Proceedings of the 10th IEEE Symposium on Computers and Communications (ISCC'05), Murcia, Spain, 27–30 June 2005.

36. Erramilli, V.; Malta, I.; Bestavros, A. On the interaction between data aggregation and topology control in wireless sensor networks. In Proceedings of the 2004 First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, Santa Clara, CA, USA, 4–7 October 2004

37. Ding, M.; Cheng, X.; Xue, G. Aggregation tree construction in sensor networks. In Proceedings of the 2003 IEEE 58th Vehicular Technology Conference, Orlando, USA, 6–9 October 2003.

38. Luo, H.; Luo, J.; Liu, Y. Energy efficient routing with adaptive data fusion in sensor networks. In Proceedings of the 2005 joint workshop on Foundations of mobile computing, Cologne, Germany, 2 September 2005

39. Wang, P.; Yao, C.; Zheng, Z.; Sun, G.; Song, L. Joint Task Assignment, Transmission, and Computing Resource Allocation in Multilayer Mobile Edge Computing Systems. IEEE IoT J. 2018, 6, 2872–2884.

40. Welcome page OpenHUB // OpenHUB URL: https://www.openhab.org/ (дата звернення: 20.04.2018).

41. Welcome page Jeedom // Jeedom URL: https://www.jeedom.com/site/en/index.html (дата звернення: 20.04.2018).

42. Ren, J.; He, Y.; Huang, G.; Yu, G.; Cai, Y.; Zhang, Z. An edgecomputing based architecture for mobile augmented reality. IEEE Netw. 2019, 33, 162–169.

43. Heinzelman, W.R.; Chandrakasan, A.; Balakrishnan, H. Energy-efficient communication protocol for wireless microsensor networks. In Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, Maui, HI, USA, 4–7 January 2000.

44. Hoan-Suk Choi, Jun-Young Lee, Na-Ri Yang, Woo-Seop Rhee, “User-centric Service Environment for Context Aware Service Mash-up” // 2014 IEEE World Forum on Internet of Things (WF-IoT) URL: https://www.researchgate.net/profile/Hoan_Suk_Choi/publication/269309102_User-cen tric_service_environment_for_context_aware_service_mash-up/links/5718ed4208ae986 b8b7b2bde.pdf (дата звернення: 26.05.2018).

45. Younis, O.; Sonia, F. HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks. IEEE Trans. Mobile Comput. 2004, 3, 366–379.

46. Cherchi, R.; Colistra, G.; Pilloni, V.; Atzori, L. Energy consumption management in Smart Homes: An M-Bus communication system. In Proceedings of the 2014 International Conference on Telecommunications and Multimedia (TEMU), Heraklion, Greece, 28–30 July 2014

47. Hu, Q.; Li, F. Hardware Design of Smart Home Energy Management System with Dynamic Price Response. IEEE Trans. Smart Grid 2013, 4, 1878–1887.

48. Jo, H.; Kim, S.; Joo, S. Smart heating and air conditioning scheduling method incorporating customer convenience for home energy management system. IEEE Trans. Consum. Electron. 2013, 59, 316–322.

49. Peruzzini, M.; Germani, M.; Papetti, A.; Capitanelli, A. Smart Home Information Management System for Energy-Efficient Networks. In Collaborative Systems for Reindustrialization; Springer: Berlin, Germany; Heidelberg, Germany; Dresden, Germany, 2013; Volume 408, pp. 393–401.

50. Han, D.M.; Lim, J.H. Smart home energy management system using IEEE 802.15.4 and ZigBee. IEEE Trans. Consum. Electron. 2010, 56, 1403–1410.

51. Han, D.M.; Lim, J.H. Design and implementation of smart home energy management systems based on ZigBee. IEEE Trans. Consum. Electron. 2010, 56, 1417–1425.

52. R. Want, “An introduction to RFID technology,” IEEE Pervasive Computing, vol. 5, no. 1, pp. 25–33, Jan 2006.

53. Wilson C, Hargreaves T, Hauxwell-Baldwin R. Smart homes and their users: a systematic analysis and key challenges [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://link.springer.com/article/10.1007/s00779-014-0813-0

54. L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A Survey,” Computer Networks, vol. 54, no. 15, pp. 2787–2805, 2010.

55. M. Friedli, L. Kaufmann, F. Paganini, and R. Kyburz, “Energy Efficiency of the Internet of Things - Technology and Energy Assessment Report,” International Energy Agency, vol. 1, 2016

56. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, 2013.

57. J. Yick, B. Mukherjee, and D. Ghosal, “Wireless sensor network survey,” Computer networks, vol. 52, no. 12, pp. 2292–2330, 2008.

58. G. Bag, Z. Pang, M. E. Johansson, X. Min, and S. Zhu, “Engineering friendly tool to estimate battery life of a wireless sensor node,” Journal of Industrial Information Integration, vol. 4, pp. 8–14, 2016.

59. Ninja Block. URL: https://www.ninjablocks.com

60. SmartThings. URL: https://www.smartthings.com

61. Google, NEST. URL: https://www.nest.com

62. L.-J. Kau, B.-L. Dai, C.-S. Chen, and S.-H. Chen, “A cloud networkbased power management technology for smart home systems,” in 2012 IEEE International Conference on Systems, Man, and Cybernetics (SMC). IEEE, 2012, pp. 2527–2532.

63. B. Martinez, M. Monton, I. Vilajosana, and J. D. Prades, “The Power of Mod- ´ els: Modeling Power Consumption for IoT Devices,” IEEE Sensors Journal, vol. 15, no. 10, pp. 5777–5789, Oct 2015.

64. V. Konstantakos, A. Chatzigeorgiou, S. Nikolaidis, and T. Laopoulos, “Energy Consumption Estimation in Embedded Systems,” IEEE Transactions on Instrumentation and Measurement, vol. 57, no. 4, pp. 797–804, April 2008.

65. H. Jayakumar, K. Lee, W. S. Lee, A. Raha, Y. Kim, and V. Raghunathan, “Powering the Internet of Things,” in 2014 IEEE/ACM International Symposium on Low Power Electronics and Design (ISLPED), Aug 2014, pp. 375–380.

66. Q. Wang, M. Hempstead, and W. Yang, “A Realistic Power Consumption Model for Wireless Sensor Network Devices,” in 2006 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks, vol. 1, Sept 2006, pp. 286–295.

67. F. Kaup, P. Gottschling, and D. Hausheer, “PowerPi: Measuring and modeling the power consumption of the Raspberry Pi,” in 39th Annual IEEE Conference on Local Computer Networks, Sept 2014, pp. 236–243

68. K. Hinton, F. Jalali, and A. Matin, “Energy Consumption Modelling of Optical Networks,” Photonic Network Communications, vol. 30, no. 1, pp. 4–16, 2015

69. G. P. Conservation, “ITU-T G-Series Recommendations-Supplement 45 (G. sup45),” ITU-T, May, 2009.

70. Clas Olson, “WT450H Temperature Sensor/Hygrometer,”. URL: http://www.clasohlson.com/uk/Temperature-Sensor-Hygrometer/36-1797#moreinfo.