Міністерство освіти і науки України
Київський столичний університет імені Бориса Грінченка
Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка

«Допущено до захисту»
Завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
кандидат технічних наук, доцент
Складанний П.М.

_____
(підпис)
« ___ » _____ 2025 р.

КВАЛІФІКАЦІЙНА РОБОТА
на здобуття другого (магістерського)
рівня вищої освіти

Спеціальність 125 Кібербезпека та захист інформації

Тема роботи:
РОЗРОБКА ТА ОБҐРУНТУВАННЯ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ СИСТЕМИ «РОЗУМНИЙ ДІМ»

Виконав
студент групи КБм-1-24-1.4.д
Михайло Камінський
_____
(підпис)

Науковий керівник
к. в. н., доцент
(науковий ступінь, наукове звання)
Андрій Аносов
_____
(підпис)

Київ – 2025

Київський столичний університет імені Бориса Грінченка
Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка

Освітньо-кваліфікаційних рівень – магістр
Спеціальність 125 Кібербезпека та захист інформації
Освітня програма 125.00.01 Безпека інформаційних і комунікаційних систем

«Затверджую»
Завідувач кафедри інформаційної та
кібернетичної безпеки імені
професора Володимира Бурячка
кандидат технічних наук, доцент
Складанний П.М.

_____
(підпис)
« ___ » _____ 20__ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
Камінському Михайлу Костянтиновичу
(прізвище, ім'я, по батькові)

1. Тема роботи: Розробка та обґрунтування методів та засобів захисту інформації системи «Розумний Дім»;

   керівник: Аносов Андрій Олександрович,

   затверджені наказом ректора від «___»____ 20___ року №__.
2. Термін подання студентом роботи «___»_____ 20___ р.
3. Вихідні дані до роботи:
   3.1 науково-технічна та нормативна література з теми дослідження;
   3.2 методи: системний аналіз, порівняльний аналіз;
4. Зміст текстової частини роботи (перелік питань, які потрібно розробити):
   4.1 Проаналізувати сучасні моделі систем «Розумний Дім» та їх системи захисту інформації;
   4.2 Описати та проаналізувати статистику ризиків для системи РД;
   4.3 Розробити та обґрунтувати методи захисту системи «Розумний Дім»;
   4.4 На основі розробленого методу проаналізувати вектор розвитку систем РД.
5. Перелік графічного матеріалу:
   5.1 Презентація доповіді, виконана в Microsoft PowerPoint.
6. Дата видачі завдання «___»_____ 20___ р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів підготовки роботи	Термін виконання	Примітка
1.	Уточнення постановки завдання		
2.	Аналіз літератури		
3.	Обґрунтування вибору рішення		
4.	Збір даних		
5.	Виконання та оформлення розділу 1.		
6.	Виконання та оформлення розділу 2.		
7.	Виконання та оформлення розділу 3.		
8.	Вступ, висновки, реферат		
9.	Апробація роботи на науково-методичному семінарі та/або науково-технічній конференції		
10.	Оформлення та друк текстової частини роботи		
11.	Оформлення презентацій		
12.	Отримання рецензій		
13.	Попередній захист роботи		
14.	Захист в ЕК		

Студент _____ Михайло Камінський
(підпис) (прізвище, ім’я, по батькові)

Науковий керівник _____ Андрій Аносов
(підпис) (прізвище, ім’я, по батькові)

РЕФЕРАТ

Кваліфікаційна робота присвячена створенні системи захисту інформаційної безпеки для системи «розумний дім» та обґрунтуванню методів та засобів захисту інформації в ній.

Робота складається зі вступу, 3 розділів, що містять 38 рисунків та таблиць, висновків та списку використаних джерел, що містить 14 найменувань. Загальний обсяг роботи становить 83 сторінки, а також перелік умовних скорочень та список використаних джерел.

Об'єктом дослідження в роботі є процес забезпечення безпеки систем «розумного дому», що застосовуються в житлових будинках та квартирах.

Предметом дослідження є методи проектування системи інформаційної безпеки технології «розумний дім».

Метою роботи є розробка системи захисту інформації у системі «розумний дім» на основі аналізу можливих загроз, обґрунтування її методів роботи, а також аналіз майбутніх концепцій на основі сучасних прикладів систем.

Для досягнення поставленої мети у роботі:

проведено аналіз існуючих підходів дослідження та структуризації джерел загроз та недоліків систем інформаційної безпеки, та аналіз підходів до створення систем «розумного дому»;

досліджено особливості роботи при побудові системи інформаційної безпеки, побудови системи «розумного дому», та особливості підбору підсистем та їх аналіз для забезпечення максимального рівня безпеки;

обґрунтовано обрану модель інформаційної безпеки, низку обраних підсистем, загальну побудовану систему, та актуальність подібних систем в можливому майбутньому процесі уніфікації подібних технологій.

Наукова новизна одержаних результатів полягає в тому, що в роботі запропоновано приклад уніфікованого варіанту побудови системи «розумного дому», що є бюджетним та практичним вибором при побудові системи, використано метод оцінки джерел загроз на підставі відповідних українських та європейських стандартів, створено список найочікуваніших загроз із найвищим пріоритетом та на їх базі обрано найкращі варіанти протидії визначеним загрозам з урахуванням недоліків системи.

Галузь застосування. Запропоновані підходи можуть бути використані для створення прикладу уніфікованої системи «розумного дому» для майбутнього, загального використання.

Ключові слова: БЕЗПЕКА, ЗАГРОЗА, ІНФОРМАЦІЯ, ІНФОРМАЦІНА БЕЗПЕКА, РОЗУМНИЙ ДІМ, ОБ'ЄКТ БЕЗПЕКИ, СИСТЕМА ЗАХИСТУ.

ЗМІСТ

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ІБ – Інформаційна безпека

РД – Розумний дім

NIST – (The National Institute of Standards and Technology) Національний інститут стандартів і технології

ISO – (International Organization for Standardization) Міжнародна організація зі стандартизації

ДСТУ - Державні стандарти України

Wi-Fi – (Wireless Fidelity) Бездротова вірність

LED – (Light-emitting diode) Світлодіод

IoT – (Internet of Things) Інтернет речей

MQTT – (Message Queue Telemetry Transport) Протокол передачі телеметрії в черзі повідомлень

IP – (Internet Protocol) Інтернет протокол

USB – (Universal Serial Bus) Універсальна послідовна шина

ШІ – (Artificial intelligence, AI) Штучний інтелект

ЗЗІ – Засоби захисту інформації

ВСТУП

Питання автоматизації та спрощення життя багато століть стояло перед науковцями та простими людьми, винайти технології та процеси щоб покращити та спростити собі життя завжди було важливою та цікавою ідеєю. Починаючи з давніх віків люди завжди знаходили спосіб замінити робочу силу примітивними механізмами, інструментами та тваринною силою чим значно спрощували своє складне життя.

Багато чого змінилося у 19 та 20 столітті, науковий прогрес, технічні революції та політичні зміни до підходів людського життя дали широкий вплив на розвиток технологій у цій сфері, а також, що э не менш важливим, поштовхом для науковців та письменників-фантастів, що надихаючись історичними здобутками своїх співвітчизників почали уявляти життя майбутніх поколінь. Так, одними з найвідоміших письменників-фантастів Жюлем Верном, Айзеком Азімовим, Гербертом Уеллсом, Рейєм Брэдбері та іншими, вже у 20 столітті були сформовані повністю готові та чіткі бачення на життя майбутніх людей – роботи-пилососи, «розумні» холодильники, «розумні» годинники, автономні електричні прилади що допомагають у кулінарії та прибиранні, та багато іншого – концепція замінити людську роботу на працю роботів в їх очах читалася дуже чітко, люди горіли бажаннями підкорити електрику та приборкати її для своїх певних потреб.

Вражаюча точність описаних у той час роботів що допомагають по господарству, являючись без применшення частиною родини, технології літаючих машин на ядерному паливі та багато іншого показують що люди на будь якому етапі мріють про покращення та спрощення рівня свого життя.

Актуальність теми. За даними джерела [1] кількість встановлених систем «розумний дім» (далі РД) у 2018 році, тільки у США було 40,3 мільйона – це на пристойні 20,4% більше, ніж у 2017 році, що означає, що ринок «розумних будинків» оцінюється в 19,827 мільйонів доларів і, як повідомляється, дорівнює 32% від загальної кількості будинків у США. До 2022 року ця частка зросла аж до 53,1% будинків. Типовий американський фанат «розумного будинку» витрачає

146,54 доларів на рік на домашню техніку. Не відстають від тенденцій Китай, Велика Британія, Південна Корея та Індія – у цих країнах відсоток людей із системами РД сягнув 62,4 мільйона, 5,3 мільйона, 4 мільйони, 2,2 мільйона підключених будинків відповідно.

Виходячи із стрімкого збільшення клієнтів в країнах по всьому світу кожна з країн так чи інакше намагається покривати ринок за рахунок власних розробок, випускаючи уніфіковану техніку від одного виробника, для синхронізації пристроїв в одній домашній системі, додатки, а також ПО. Незважаючи на власне виробництво, навіть країни-лідери в технологіях допускають похибки із забезпечення інформаційної безпеки таких систем та окремих вузлів пристроїв.

Виходячи із дослідження [2] – середній рівень атак на пристрої в домашній мережі — приблизно 10 спроб атаки на мережу дому щодня, ботнетні кампанії та масові зараження маршрутизаторів і смарт-пристроїв залишаються повсюдною загрозою — окремі кампанії заражали тисячі роутерів протягом кількох днів (приклад — зараження Asus-роутерів однією з шкідливих кампаній), також зросла загальна кількість спроб фішингу/шкідливих файлів та банківських троянів значно зросла у 2024—2025 роках; наприклад, Kaspersky зафіксував сотні мільйонів блокованих фішингових спроб у 2024 і велике зростання атак на мобільні пристрої у 2024–2025. Ці тренди означають підвищений ризик вторгнень до домашньої мережі через скомпрометовані телефони або облікові записи.

Більшість побутових користувачів та працівники бізнесу зіштовхуються з низкою проблемних питань, зокрема:

1) неможливість ранньої ідентифікації ризику для системи і окремих пристроїв;
2) відсутність аналітичного відділу у даній сфері;
3) сумнівні або «сірі» виробники;
4) відсутність оновлень прошивки, або недбале ставлення користувачів до оновлень;
5) відсутність шифрування трафіку, та недостатній контроль доступу.

Вище перелічене підтверджує актуальність даного дослідження.

Мета роботи полягає у аналізі існуючих моделей захисту інформації у системах РД, проведення аналізу вразливостей цих систем та складання системи-концепту захисту даних на основі отриманої інформації. Для досягнення цієї мети в роботі необхідно вирішити такі **завдання:**

1) проаналізувати сучасні моделі систем РД та їх системи захисту інформації;
2) описати та проаналізувати статистику ризиків для системи РД;
3) розробити та обґрунтувати методи захисту системи РД;
4) на основі розробленого методу проаналізувати вектор розвитку систем РД.

Виходячи з цього**, об'єктом дослідження є** системи «розумного будинку» що застосовуються в житлових будинках та квартирах. **Предметом дослідження –** методи проектування системи інформаційної безпеки технології «розумний дім».

Методи дослідження. Для вирішення задачі було обрано методи оцінки загроз за стандартами ISO/IEC 27005:2022 та ДСТУ ISO/IEC 27002, та створення системи РД за останніми дослідженнями Національного інституту стандартів і технології NIST.

Наукова новизна одержаних результатів. Наукова новизна полягає у створенні теоретичної системи, що в майбутньому дозволить уніфікувати та привести до однорідного бачення систем ІБ та функціонування систем РД.

Теоретичне та практичне значення полягає в обґрунтуванні наявних джерел небезпеки для систем РД, розробки нових систем із огляду на масове виробництво та їх інтеграція з системами побутових користувачів.

Галузь застосування – результати роботи можуть бути використані для впровадження додаткових методів захисту або для створення нових систем захисту інформації для побутових споживачів та бізнесів різних рівнів, а також як матеріал для використання у навчальному процесі.

Апробація результатів дипломної роботи. Основні положення роботи викладалися:

У тезах «Збірнику тез конференції «Безпека інформаційно-комунікаційних систем - 2025»»

https://fitm.kubg.edu.ua/informatsiya/naukova-diialnist/konferentsii-fakultetu/2646-bezpeka-informatsiino-komunikatsiinykh-system.html

РОЗДІЛ 1. АНАЛІЗ ТЕМИ ТА ІСНУЮЧИХ МОДЕЛЕЙ СИСТЕМ «РОЗУМНОГО ДОМУ»

1.1 Визначення терміну технології «розумного дому»

Технологія «розумний дім» – під цим терміном прийнято розуміти сукупність підключених до загальної мережі пристроїв, що виконують певні дії з мінімальним втручанням з боку людини. Концепція «розумного дому» полягає в автоматизації та інтелектуалізації управління інженерними системами житлового або комерційного приміщення, що дозволяє підвищити комфорт проживання, забезпечити безпеку та оптимізувати витрати ресурсів. Сучасні системи РД здатні самостійно приймати рішення на основі даних від датчиків, аналізувати поведінку користувачів та адаптуватися до їхніх потреб без постійного ручного втручання.

Ідея створення РД в наближеному до сьогоднішнього розуміння цього терміну з'явилася в кінці 20 століття. Один з перших таких будинків був описаний в журналі "Popular Mechanics" в 1950 році. Термін «розумний дім» був введений в 1984 році американською Асоціацією житлово-будівельних компаній і до 2000 року ідея «розумних домів» була досить поширена в Європі і, особливо, в США.

Справжній переворот у технологіях домашньої автоматизації відбувся з появою смартфонів та масовим поширенням бездротових технологій зв'язку. Це зробило системи «розумного дому» значно доступнішими, простішими у встановленні та дешевшими. Кількість необхідних проводів скоротилася до мінімуму, а керування системами стало можливим через мобільні додатки з будь-якої точки світу. Поява голосових асистентів додатково спростила взаємодію користувачів з «розумними» системами, дозволяючи керувати будинком за допомогою голосових команд.

Технологія РД використовується для різних цілей, можна виділити основні з них [15-21]:

— тепло та енергозбереження – системи автоматично регулюють опалення, кондиціонування, освітлення та роботу електроприладів залежно від присутності людей, часу доби та зовнішніх умов, що дозволяє значно знизити споживання електроенергії, газу та води;

— підвищення комфорту – автоматизація повсякденних завдань, створення персоналізованих сценаріїв для різних ситуацій (прокидання, відхід з дому, повернення додому, відпочинок), можливість дистанційного контролю та управління всіма системами будинку через єдиний інтерфейс;
— забезпечення безпеки – інтеграція систем відеоспостереження, охоронної сигналізації, контролю доступу, датчиків протечки води, диму, газу та вогню з можливістю миттєвого сповіщення власника про будь-які інциденти та автоматичного реагування на загрози.

Різні підприємства застосовують технологію РД в основному для енергозбереження та безпеки, оскільки це дозволяє суттєво знизити операційні витрати на утримання будівель та підвищити рівень захисту обладнання, товарів та конфіденційної інформації. Комерційні об'єкти, офісні центри, готелі та торгові комплекси активно впроваджують системи автоматизації для оптимізації витрат та створення комфортних умов для співробітників та відвідувачів.

У житлових приміщеннях системи «розумного дому» можуть використовуватися для всіх вищезазначених цілей одночасно, створюючи комплексне рішення для управління всіма аспектами життєдіяльності помешкання. Сучасні РД здатні інтегрувати десятки різних підсистем та пристроїв, забезпечуючи їх злагоджену роботу та взаємодію. Користувачі можуть поступово розширювати функціональність своєї системи, додаючи нові пристрої та можливості відповідно до потреб та бюджету.

Компанії виробники систем «розумного будинку» пропонують різні варіації систем: готові рішення "під ключ" і системи, які налаштовуються під вимоги конкретного клієнта. Готові рішення включають стандартний набір обладнання та функцій, які покривають базові потреби більшості користувачів. Вони характеризуються швидкістю впровадження, прогнозованою вартістю та простотою експлуатації. Індивідуальні системи проектуються з нуля під конкретний об'єкт, враховуючи його архітектурні особливості, специфічні вимоги замовника та майбутні плани розширення функціональності.

Також на ринку представлені окремі «розумні» продукти (в основному

випускаються виробниками техніки), які користувач може самостійно об'єднати в систему РД. Такий підхід дає максимальну гнучкість та можливість поступового нарощування функціональності системи. Користувачі можуть почати з простих пристроїв, таких як «розумні» лампочки або розетки, та поступово додавати більш складні компоненти – термостати, камери, датчики, системи контролю доступу тощо. Багато виробників пропонують екосистеми пристроїв, які легко інтегруються між собою, що спрощує процес створення власної системи «розумного дому».

Системи «розумний дім» не мають єдиної методології опису. Як компанії, так і дослідники технології РД, мають різні підходи до опису системи «розумного будинку», що відображає складність та багатогранність цієї технології. Це зумовлено різноманітністю стандартів зв'язку, протоколів передачі даних, архітектурних рішень та способів інтеграції компонентів. Відсутність єдиного стандарту одночасно є і перевагою, оскільки стимулює конкуренцію та інновації, і недоліком, ускладнюючи сумісність пристроїв різних виробників.

Найбільш частіше зустрічається підхід – поділ системи РД на різні підсистеми за функціональним призначенням. Це дозволяє структурувати опис системи, спростити процес проектування та полегшити розуміння взаємозв'язків між компонентами. Кожна підсистема відповідає за конкретну функцію або групу функцій, але при цьому всі підсистеми тісно інтегровані та можуть обмінюватися даними для забезпечення узгодженої роботи всієї системи. Узагальнений та детальний приклад підсистеми «розумного будинку» представлено на схемах 1.1 та 1.2:

Схема 1.1 Узагальнений опис підсистем «розумного будинку»

Як ми бачимо із блок-схеми основні вузли робочих елементів справді базуються на системах електроживлення, вентиляція та опалення та системах освітлення що підкреслює їх важливість для звичайного користувача.

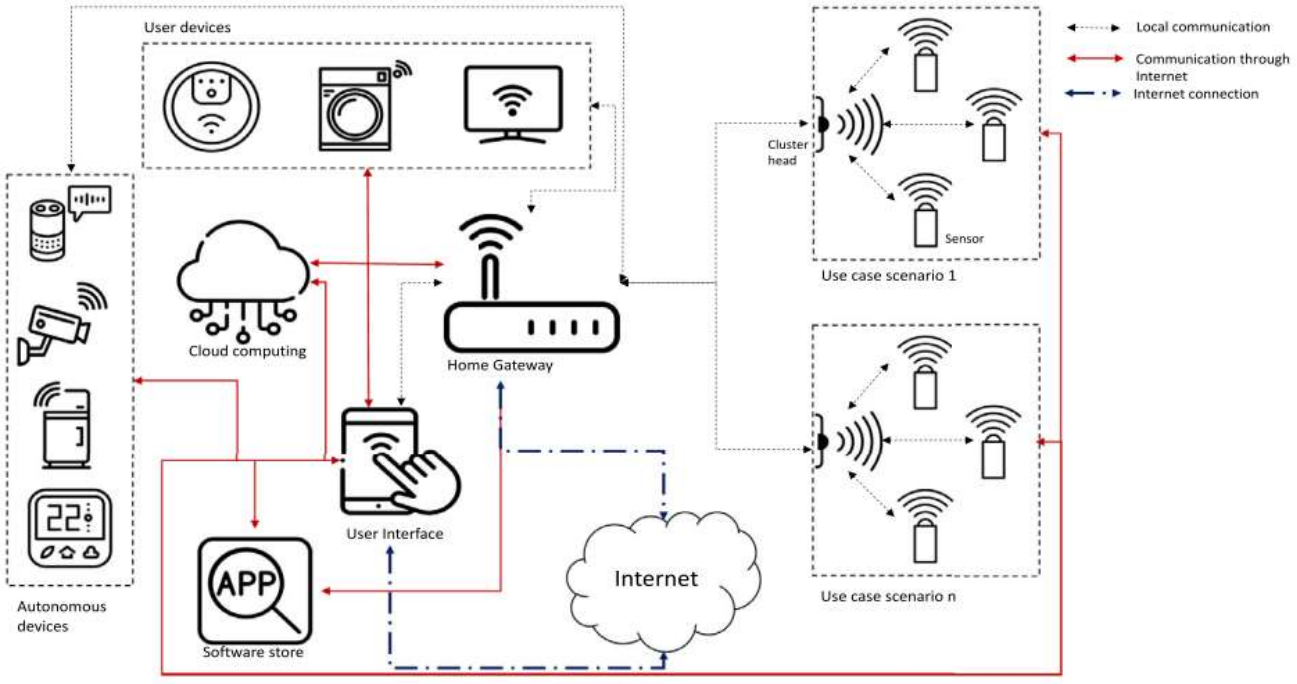

Схема 1.2 Детальний приклад підсистеми «розумного будинку»

На схемі продемонстровані основні частини системи РД, їх можливі шляхи під’єднання та керування.

1.2 Визначення та опис основних підсистем-модулів системи «розумного дому»

Як вже визначалось раніше – під системою РД мають на увазі приміщення в офісних та житлових будівлях, квартирах, будинках з єдиною автоматизованою системою управління і моніторингу всіх підсистем життєзабезпечення і безпеки. До таких основних підсистем можна віднести:

– управління освітленням. До таких можемо віднести «розумний» димер – модуль, що встановлюється замість стандартного вимикача і дозволяє дистанційно вмикати/вимикати світло та регулювати його яскравість (димування), або ж «розумну» LED-лампу – лампа з вбудованим модулем зв'язку (наприклад, Wi-Fi або Zigbee), що керується безпосередньо через контролер, дозволяючи змінювати колір (RGB) та температуру світла;

Рис. 1.2.1 Приклад «розумної» LED-лампи

– управління опаленням і гарячим водопостачанням. До таких підсистем відносяться «розумні» термостати - центральні пристрої для збору даних про температуру та вологість і відправки команд керування на котел, також з можливістю створювати автономні, програмовані графіки. Термостатичний клапан на радіатор – пристрій, що монтується на радіатор опалення і дозволяє дистанційно регулювати та контролювати температуру окремої кімнати;

Рис. 1.2.2 Приклад «розумного» терморегулятору для газового котла

– управління електричними мережами для подачі електроенергії і вторинними джерелами електроживлення. До них відносяться «розумний» автомат – модуль, що встановлюється в електро-щиток та дозволяє дистанційно вмикати/вимикати живлення окремих ліній або груп приладів, а також моніторити споживання, та система керування додаткових систем живлення – модуль, що моніторить стан акумуляторів або генератора та автоматично перемикає живлення на резервне джерело при зникненні основної електроенергії;

Рис. 1.2.3 Приклад «розумного» автоматичного автомата

– система інтернет-доступу (локальна обчислювальна мережа), обладнання

доступу. Прикладом підсистеми є Mesh-маршрутизатор - сучасна система Wi-Fi, яка забезпечує безшовне покриття Інтернетом великої площі, що критично важливо для стабільної роботи всіх IoT-пристроїв;

Рис. 1.2.4 приклад Mesh-маршрутизатора

– система охоронно-пожежної сигналізації. Прикладами є комбіновані датчики диму та чадного газу, та сирени. Ці пристрої можуть працювати як і в парі, так і окремо – реагуючи на різні фактори небезпеки гучним звуковим оповіщенням та світловою індикацією, що активується контролером при отриманні сигналу тривоги від будь-якого датчика;

Рис. 1.2.5 Приклад датчиків диму та чадного газу разом із сиреною

– система відеоспостереження. Найбільш розповсюджена підсистема систем РД, представлена «розумними» PTZ-камерами або відео-реєстраторами – пристроями

що дозволяють дистанційно керувати кутом огляду, нахилом і оптичним збільшенням, а також зберігання та обробки відео-потоків з усіх камер системи;

Рис. 1.2.6 Приклад набору камер спостереження із відео-реєстратором

– система контролю і управління доступом в приміщення. Представлені на ринку біометричними зчитувачами або електромагнітними замками – пристроями що використовують різні біометричні дані верифікованих користувачів (відбиток пальця, голос, сітківку ока) та фізично блокує/розблоковує прохід;

Рис. 1.2.7 Приклад систем біометричного зчитування даних. В даному випадку відбитку пальця та обличчя

– система кондиціонування і вентиляції. Пристрої що вимірюють рівень вуглекислого газу, летких органічних сполук та пилу, автоматично активуючи вентиляцію та прилади зволоження повітря, представлені «розумними» кондиціонерами або ж датчиками якості повітря.

Рис. 1.2.8 Приклад системи «розумної» вентиляції

1.3 Захист інформаційної безпеки у системах «розумного» дому

Система «розумного» будинку є об'єктом інформатизації, схильним до загроз інформаційній безпеці. Загрози інформаційній безпеці системи залежать від методів побудови системи, використовуваних технологій і оброблюваних інформаційних потоків, тому не існує єдиної методології способу захисту інформаційної безпеки.

Специфіка загроз для систем «розумного» дому полягає в тому, що вони об'єднують фізичний та цифровий світи. Успішна кібератака може призвести не лише до витоку конфіденційної інформації, але й до реальних фізичних наслідків – несанкціонованого відкриття дверей, вимкнення систем безпеки, маніпуляції з системами опалення або освітлення. Крім того, пристрої IoT часто мають обмежені обчислювальні ресурси, що ускладнює впровадження складних механізмів захисту безпосередньо на рівні пристроїв.

Багато систем «розумного» будинку мають вбудований компонент захисту інформаційної безпеки. Найчастіше він представлений програмами що підтримують роботу головного модуля системи РД – модулю що об'єднує всі інші підсистеми, забезпечує зв'язок між ними, передачу інформації, тощо. Цей центральний модуль, часто називаний хабом або шлюзом, відповідає за аутентифікацію пристроїв, шифрування даних та контроль доступу до системи. Деякі виробники інтегрують функції захисту безпосередньо в прошивку пристроїв, забезпечуючи базовий рівень безпеки на апаратному рівні.

Альтернативним підходом є окремий, автономний прилад із окремим застосунком або мобільним додатком, який виконує функції брандмауера або системи виявлення вторгнень спеціально для IoT-пристроїв. Такі рішення працюють як проміжна ланка між «розумними» пристроями та зовнішньою мережею, моніторячи весь трафік та блокуючи підозрілу активність. Вони можуть виявляти аномалії в поведінці пристроїв, несанкціоновані спроби підключення та потенційні вразливості в мережі.

І все ж таки, на жаль, дані варіанти вирішення проблеми не завжди гарантують високий рівень захисту. Проблема полягає в тому, що багато

вбудованих механізмів безпеки мають обмежену функціональність через необхідність економії обчислювальних ресурсів та енергії. Крім того, виробники часто не випускають своєчасні оновлення безпеки для старіших моделей пристроїв, залишаючи їх вразливими до нових типів атак. Навіть системи з вбудованим захистом можуть мати критичні вразливості через помилки в програмному коді або недосконалість архітектури безпеки.

У деяких системах компонент інформаційної безпеки може навіть бути відсутнім, особливо в бюджетних рішеннях або пристроях від малих виробників. Такі системи розраховані на те, що користувач самостійно забезпечить захист через налаштування домашнього роутера або використання додаткових засобів безпеки. Це створює значні ризики, оскільки більшість кінцевих користувачів не мають достатніх знань для правильного налаштування захисту.

З цієї причини деякі компанії почали виробництво додаткових засобів із захисту інформаційної безпеки «розумного будинку». Ці спеціалізовані рішення включають апаратні брандмауери для IoT, системи моніторингу мережевої активності, засоби шифрування трафіку та платформи для централізованого управління безпекою всіх підключених пристроїв. Такі продукти розраховані на користувачів, які серйозно ставляться до питань безпеки та готові інвестувати додаткові кошти в захист своєї системи «розумного дому».

Але, якщо компанія є виробником «розумних» пристроїв, то в більшості випадків засіб захисту, який розроблюється, здатен працювати тільки з «розумними пристроями» цієї компанії. Це створює проблему фрагментації ринку та ускладнює захист гетерогенних систем, де використовуються пристрої від різних виробників. Користувачі змушені або обирати екосистему одного виробника, обмежуючи свій вибір, або використовувати кілька різних систем захисту, що значно ускладнює управління безпекою.

У 2014 році спілкою незалежних компаній що базуються на визначенні та наданні характеристики щодо інформаційної безпеки систем (в тому числі і систем «розумних-будинків») було проведено тестування декількох загальнодоступних систем. Метою дослідження було виявлення реального стану безпеки комерційних

систем «розумного дому» та визначення основних векторів атак, яким вони схильні.

Компанії досліджували:

— наявність шифрованого зв'язку між елементами РД – перевірялося, чи використовується криптографічний захист для передачі даних між пристроями та центральним контролером, а також між системою та хмарними сервісами;
— використання активної аутентифікації – аналізувалися механізми перевірки ідентичності користувачів та пристроїв, надійність паролів за замовчуванням, наявність багатофакторної автентифікації;
— можливість зовнішньої маніпуляції – тестувалася стійкість системи до атак типу "людина посередині", можливість перехоплення та підміни команд, вразливість до віддаленої експлуатації;
— рівень захищеності віддаленого доступу – оцінювалася безпека мобільних додатків, веб-інтерфейсів та API, через які користувачі керують системою з-поза домашньої мережі.

Результати тестування семи систем РД показали тривожну картину стану безпеки на ринку «розумних домів»:

— лише три системи забезпечують достатній рівень інформаційної безпеки, використовуючи шифрування, надійну аутентифікацію та захист від найпоширеніших типів атак;
— дві системи недостатньо захищені і можуть бути схильні до внутрішніх атак з боку зловмисників, які мають фізичний доступ до локальної мережі або можуть перехопити незахищений трафік;
— дві системи мають дуже слабкий інформаційний захист і можуть бути схильні як до внутрішніх, так і до зовнішніх атак, включаючи віддалене проникнення через Інтернет без необхідності фізичної присутності поблизу об'єкта.

Проведене тестування доводить, що навіть користувачам готових рішень не слід забувати про інформаційний захист і при необхідності використовувати

додаткові засоби захисту. Рекомендується регулярно оновлювати програмне забезпечення всіх пристроїв, змінювати паролі за замовчуванням на надійні унікальні комбінації, використовувати сегментацію мережі для ізоляції IoT-пристроїв від основної домашньої мережі, вмикати всі доступні функції безпеки в налаштуваннях системи.

Виробникам РД потрібно випускати продукти з більш високим рівнем захисту, впроваджуючи безпеку на етапі проектування, а не як додаткову функцію. Необхідно забезпечувати регулярні оновлення безпеки протягом усього життєвого циклу продукту, використовувати сучасні криптографічні стандарти, проводити незалежні аудити безпеки та дотримуватися міжнародних стандартів у галузі кібер-безпеки IoT-пристроїв.

1.4. Існуючі рішення захисту інформації системах «розумного дому»

Як було зазначено, компанії, які є одночасно виробниками «розумних» пристроїв та засобів захисту, найчастіше пропонують монолітні рішення, які забезпечують високий рівень сумісності, але обмежують вибір споживача лише пристроями їхньої екосистеми. На противагу цьому, інші компанії зосереджуються на розробці універсальних засобів захисту інформації (ЗЗІ), прагнучи покрити весь ринок різнорідних пристроїв IoT.

Універсальні ЗЗІ зазвичай реалізуються або як програмне забезпечення, інтегроване в прошивку роутера, або як окремий апаратний пристрій (шлюз безпеки), що фізично функціонує між роутером та локальною мережею, створюючи єдину точку контролю. Ці системи працюють, створюючи та постійно оновлюючи профіль нормальної мережевої поведінки для кожного IoT-пристрою. ЗЗІ використовує машинне навчання для виявлення аномалій: якщо «розумний» пристрій починає сканувати внутрішню мережу або намагається встановити з'єднання із зовнішніми IP-адресами, відомими як шкідливі, ЗЗІ миттєво ідентифікує це як компрометацію.

Крім того, універсальні засоби здійснюють глибоку інспекцію пакетів, аналізуючи зміст трафіку (де це можливо без порушення криптографії), щоб виявити використання вразливих протоколів або передачу конфіденційних даних у незашифрованому вигляді. Системи також забезпечують географічну та чорну фільтрацію, постійно порівнюючи зовнішні IP-адреси, з якими намагаються зв'язатися IoT-пристрої, зі світовими базами даних загроз і автоматично блокуючи трафік, що прямує до відомих командних центрів зловмисників. Оскільки багато виробників IoT-пристроїв не забезпечують регулярні оновлення, універсальні ЗЗІ можуть виконувати функцію віртуального патчування. Система виявляє вразливість у пристрої та фільтрує трафік, блокуючи спроби її експлуатації ще до того, як пакет дійде до вразливого гаджета, а у разі підозри на компрометацію, пристрій може бути автоматично ізольований (поміщений у карантин) у спеціальний мережевий мікросегмент. Таким чином, універсальні ЗЗІ пропонують

адаптивний, багаторівневий захист, критично важливий для домашніх мереж, що складаються з різнорідних пристроїв.

Один з поширених методів роботи на ринку пристроїв додаткового інформаційного захисту РД – підключення до роутера і моніторинг потоку інформації між підключеними до Wi-Fi пристроями, ось декілька варіантів:

— Dojo, розроблене невеликою ізраїльською компанією Dojo-Labs;

— Bitdefender Box, розробка румунської компаніїї Bitdefender;

— різноманітна спеціалізована продукція Cisco, підходить більше для бізнес-варіанту або для заможніх споживачів. Виробляється багатонаціональною американською компанією "Cisco Systems, Inc." (Cisco).

1.4.1. Dojo (BullGuard / Dojo Labs)

Dojo (BullGuard / Dojo Labs) — «камінчик»/шлюз, що підключається до маршрутизатора, аналізує метадані трафіку й повідомляє про аномалії. Він має мобільний додаток і можливість відключати скомпрометовані пристрої одразу після його виявлення.

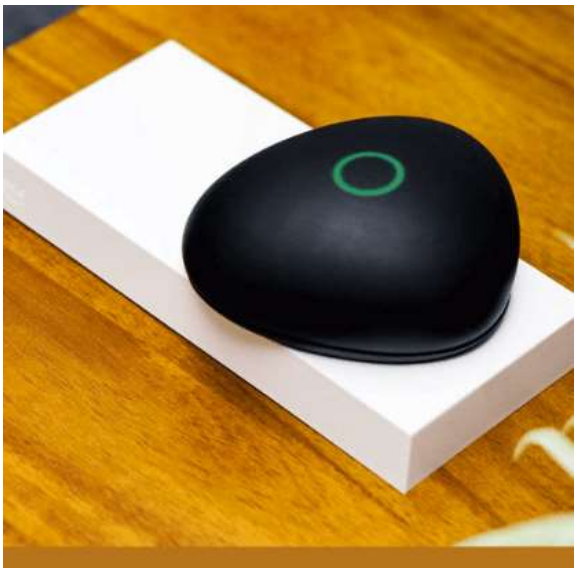

Рис. 1.4.1.1. Зображення шлюзу Dojo

Біла коробка Dojo підключається до маршрутизатора Wi-Fi і відстежує весь мережевий трафік в режимі реального часу та виявляє аномалії та загрози. "Digital

pet rock" має систему світлодіодів, що вказують на стан безпеки. Це єдина функція цього компонента, крім дизайну. Управління Dojo здійснюється за допомогою додатку для смартфону "Dojo App". Усі сповіщення з’являються у програмі, яка дозволяє користувачеві знати про проблеми, перш ніж вони вплинуть на його конфіденційність або безпеку.

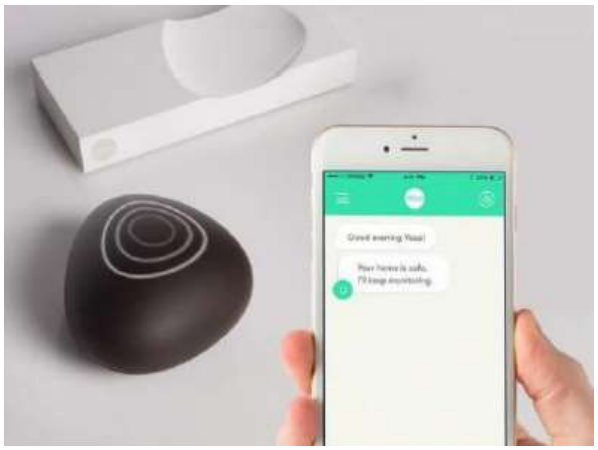

Рис. 1.4.1.2. Зображення мобільного додатку Dojo

1.4.2. Bitdefender Box

Bitdefender Box розроблена великою румунською компанією Bitdefender, що спеціалізується на антивірусних продуктах. На офіційному веб-сайті є три варіанти продуктів для різних рівнів захисту та ряду підключених пристроїв. Bitdefender BOX постійно сканує, виявляє та висвітлює недоліки мережевої безпеки. Він шукає приховані бекдори та погано захищені порти управління. Продукт працює як два попередні пристрої: коробчастий пристрій, модем, додаток для смартфона та хмарне сховище даних.

Рис. 1.4.2.1 Зображення Bitdefender Box

1.4.3. Продукція Cisco

Cisco є справжнім мастодонтом цифрової безпеки, світовим лідером у галузі мережевих технологій та захисту інформації. Її рішення охоплюють усі рівні — від корпоративних датацентрів до повних систем РД, забезпечуючи виявлення загроз, моніторинг трафіку й контроль доступу до мережевих ресурсів. Продукція є дуже різноманітною – від варіантів для бюджетної системи РД до систем що охоплюють великі бізнес центри.

Cisco Firepower 1010 NGFW Appliance Desktop – це брандмауер нового покоління (Next-Generation Firewall), який забезпечує глибоку інспекцію мережевого трафіку, виявлення атак і контроль над підключеними пристроями. Firepower 1010 дозволяє сегментувати домашню або корпоративну мережу, блокувати підозрілі з’єднання, а також створює безпечний простір для роботи IoT-пристроїв у системах РД.

Рис. 1.4.3.1 Зображення Cisco Firepower 1010 NGFW

Cisco ASA5525-K9 Adaptive Security Appliance – апаратний фаєрвол серії ASA, що поєднує функції фільтрації трафіку, VPN-захисту та виявлення вторгнень. Пристрій забезпечує стабільний контроль за обміном даними між внутрішньою мережею та інтернетом, запобігаючи несанкціонованому доступу. Підходить для середовищ, де важлива безперервність зв’язку та високий рівень інформаційної безпеки, зокрема для систем «розумного дому».

Рис. 1.4.3.2 Зображення Cisco ASA5525-K9 Adaptive Security Appliance

Ці пристрої є брандмауерами з розширеною функцією моніторингу з'єднань, що забезпечує прозорість та обізнаність у контексті програми. Серії мають простий дизайн, що є типовим для таких пристроїв. Головною перевагою цих серій є висока ефективність захисту інформації, підтверджена тестами. Це високотехнологічний продукт із відповідною ціною. Такі пристрої розроблені також можуть використовуватись для малих та великих підприємств і вимагати досить складних умов монтажу та обслуговування та, як наслідок, висококваліфікованого персоналу.

1.5. Основні недоліки існуючих моделей та основні проблеми роботи

Перелічені системи цифрової безпеки та їх аналоги все ж не гарантують повної безпеки. Це зумовлено низкою факторів, пов’язаних як із технічними обмеженнями самих пристроїв, так і з поведінкою користувачів чи недостатньою стандартизацією ринку.

Загалом, дослідники з джерел [4,5,6] вказують, що системи IoT-захисту для систем РД стикаються з низкою ключових недоліків та експлуатаційних проблем, які обмежують їхню ефективність і створюють додаткові ризики для безпеки користувачів, а саме:

- велика площа атаки - через кількість різних пристроїв (розетки, лампи, камери, термостати, хаби) у «розумному домі» збільшується число точок «входу» для зловмисників;
- слабка аутентифікація, заводські/типові паролі - багато пристроїв постачаються з паролями за замовчуванням або можливістю налаштування слабких паролів.
- незадовільне шифрування або його відсутність - локальні протоколи, обмін між пристроями або між пристроєм і мобільним додатком можуть бути незашифровані чи недостатньо захищені;
- проблеми з оновленнями й життєвим циклом пристроїв - виробники можуть припинити підтримку пристрою, оновлення можуть виходити повільно або взагалі відсутні, що підвищує ризик залишитись із вразливим пристроєм.
- сумісність, стандартизація, інтеграція різних пристроїв - множинність виробників, різні протоколи, відсутність єдиних стандартів — усе це ускладнює безпечне інтегрування систем;
- приватність і збори даних - пристрої часто збирають дані про користувача/середовище (камера, мікрофон, сенсори). Якщо захист слабкий — можливий витік чи профілювання.

Також багато проблем, особливо при використанні невпевненими

приватними користувачами, або ж некваліфікованим персоналом бізнесів, спричиняють проблеми через неправильну експлуатацію:

— невідповідне розділення мережі (network segmentation) - часто IoT-пристрої "сидять" в тій же мережі, що ПК чи телефони, і при компрометації одного пристрою можливість переходу на інші велика;
— недостатня увага користувача / слабка експлуатація - багато користувачів не змінюють паролі, не перевіряють оновлення, не відслідковують підозрілі пристрої;
— застаріле або невідоме ПО/компоненти в пристроях - деякі пристрої містять бібліотеки або компоненти з відомими вразливостями, але оновлення не приходять;
— виробник/сервіс-залежність/завершення підтримки - якщо виробник припиняє вироби або сервіс, пристрій може бути лишений оновлень і стає ризиковим.
— банальна складність для користувача - налаштуванні безпеки, VPN, сегментації, регулярних оновлень - потрібно певне знання або готовність інвестувати час.

На основі проведених досліджень [7] що опирались на міжнародні сертифікати оцінки ризиків, таких як ISO/IEC 27005:2022 та NIST Special Publication 800-30 Revision 1, можна зібрати таблицю основних ризиків для систем інформаційної безпеки в системах РД та розрахувати коефіцієнти їх загрози загальній системі.

Таблиця 1.5.1

Розрахунок коефіцієнту основних ризиків для систем безпеки в системах РД

№	Категорія Ризику	Конкретна Загроза (Вектор Атаки)	Рівень Впливу (Impact)	Рівень Ймовірності (Likelihood)	Загальний Рівень Ризику (Risk Score)
1	Вразливість Пристроїв	Використання стандартних або слабких паролів	3	3	9

2	Вразливість Пристроїв	Несвоєчасне оновлення ПЗ	3	3	9
3	Мережева Безпека	Атака "Людина-посередник" (Man-in-the-Middle, MitM) у локальній мережі	3	2	6
4	Мережева Безпека	Перехоплення незашифрованого трафіку	2	3	6
5	Конфіденційність	Несанкціонований збір та витік персональних даних (PII) із хмарного сховища	3	2	6
6	Конфіденційність	Аналіз поведінки та звичок на основі даних сенсорів (Стеження)	3	2	6
7	Шкідливе ПЗ	Включення пристрою (камери/роутера) до Ботнету (наприклад, Mirai)	2	3	6
8	Шкідливе ПЗ	Програма-вимагач (Ransomware) з блокуванням доступу до системи	3	1	3
9	Фізична Безпека	Дистанційне розблокування «розумного» замка через вразливість системи	3	2	6
10	Аутентифікація/Авторизація	Злом облікового запису користувача через фішинг	3	3	9

Де, шкала рівню впливу 1–3позначає рівень впливу на систему:

1 – низький

2 – середній

3 – високий

Шкала ймовірності впливу на систему позначає ймовірність впливу на систему:

1 – низький

2 – середній

3 – високий

загальний рівень ризику (Risk Score) - обчислюється як добуток:

Рівень Ризику = Рівень Впливу x Рівень Ймовірності

Максимальний бал: 9 (Критичний ризик)

Мінімальний бал: 1 (Низький ризик)

Проведений якісний аналіз ризиків із застосуванням матриці дозволяє ідентифікувати ключові загрози для існуючих моделей систем безпеки РД. Виходячи із вищезгаданих стандартів, критичний рівень ризику (Risk Score 9) був присвоєний загрозам, пов'язаним із використанням стандартних або слабких паролів, несвоєчасному оновленню ПЗ або злому облікового запису користувача. Це обумовлено поширеністю проблем через людський фактор та недбалість в кібер-безпеці IoT.

До зони середнього ризику (Risk Score 6) увійшли загрози, які прямо стосуються фізичної безпеки – перехоплення інформації, візуальне стеження за системами безпеки, розсилання шкідливих листів та злам електричних замків системи.

РОЗДІЛ 2 АНАЛІЗ ІНФОРМАЦІЙНОГО ЗАБЗЕПЕЧЕННЯ СИСТЕМ «РОЗУМНОГО ДОМУ». ФАКТОРИ ВРАЗЛИВОСТЕЙ ТЕХНОЛОГІЇ. ПОБУДОВА СТРУКТУРОВАНОЇ МОДЕЛІ ЗАХИСТУ СИСТЕМИ «РОЗУМНОГО ДОМУ»

2.1 Аналіз інформаційного забезпечення та опис підсистем «розумного дому»

Відсутність єдиної методології побудови системи захисту системи РД підштовхує до створення власного підходу побудови цієї структури. Умовно розділивши завдання, можна відокремити 4 окремих етапи:

— опис обраної моделі системи РД;

— опис основних методів класифікації джерел загроз системам ІБ;

— аналіз можливих джерел загроз для обраної системи ІБ та методи боротьби із ними;

— аналіз отриманих результатів та опис перспективних рішень.

Для проведення детального аналізу інформаційного забезпечення та розробки плану безпеки було обрано гібридну, багаторівневу модель системи РД. Ця модель відображає сучасні тенденції інтеграції, поєднуючи локальні мережі пристроїв із централізованим хмарним управлінням. Метою аналізу є виявлення критичних вузлів, шляхів передачі даних та вразливостей на кожному з рівнів архітектури.

Обрана архітектура складається з трьох ключових рівнів: периферійного (сенсори та датчики), керуючого (контролери та шлюз) та хмарного (сервери та мобільний додаток). Зв'язок між пристроями здійснюється за допомогою різних протоколів – Zigbee та Z-Wave для низького енергоспоживання на периферії, та Wi-Fi/Ethernet для високошвидкісних пристроїв, таких як IP-камери та центральний шлюз. Саме ці вузли мережі є основними об'єктами аналізу, оскільки вони створює множинні точки входу для потенційних кібератак.

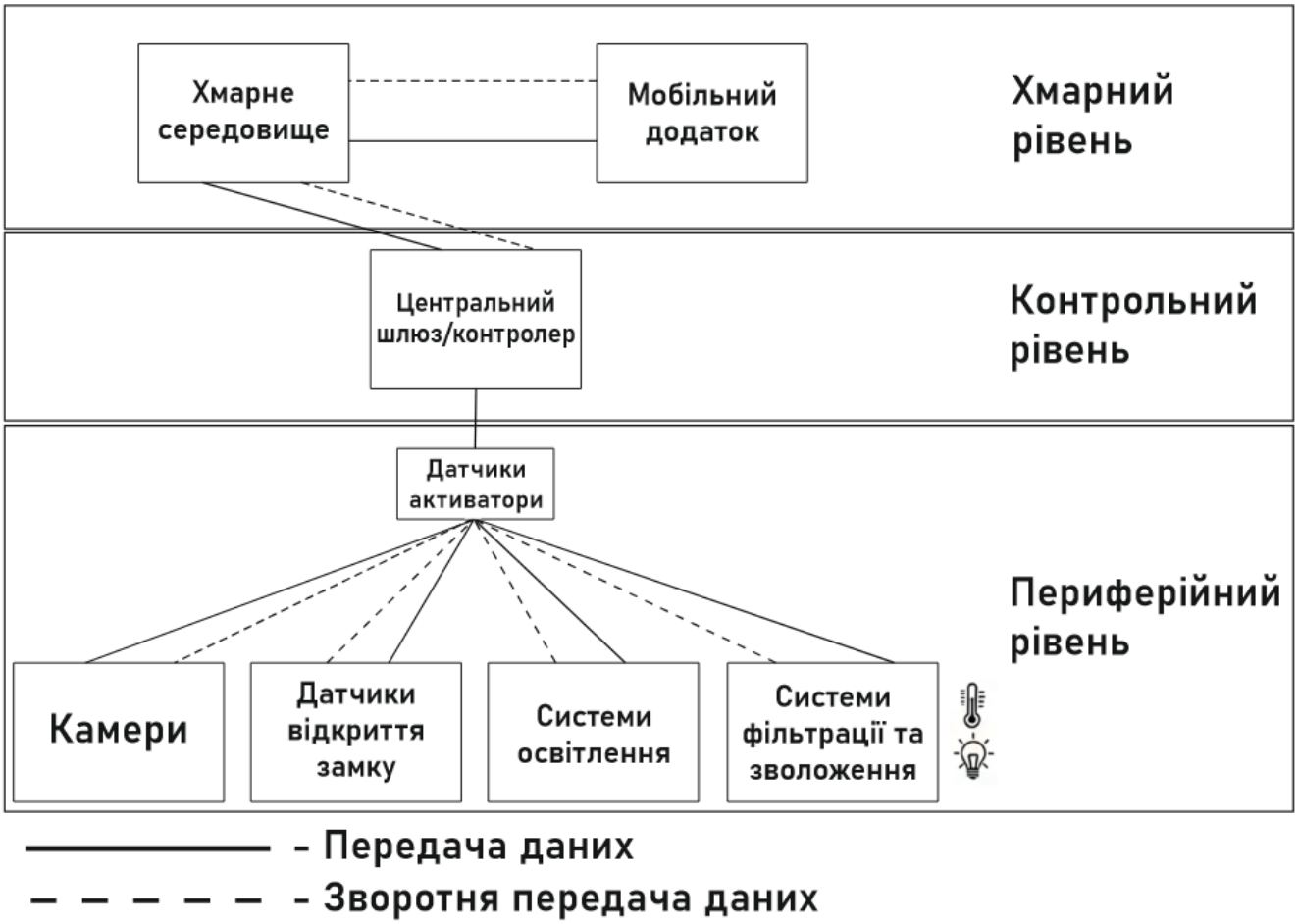

Рис. 2.1.1 Схематичне зображення обраної системи РД

Обрана схема представлена таким чином не просто так, вона в повному обсязі відображає актуальні схеми існуючих моделей РД «під ключ» із повним діапазоном доступних зручностей для користувача – огляд території із камер для зовнішньої та внутрішньої безпеки, датчики відкриття дверей будинку та інших будівель – для безпеки від проникнення зловмисників, системи освітлення – для контролю освітлення приміщень та прибудинкових територій, та системи фільтрації та зволоження – для підтримання комфортних температур та вологості у приміщені та кімнатах. Датчики що знаходяться в кожній підсистемі та самі по собі окремо, виконують роль активаторів підсистем та «тригером» спрацьовування для передачі інформації на центральний шлюз що обробляє дані в режимі реального часу та передає інформацію із фіксацією показників, даних, та часу фіксації із подальшою передачею інформації до мобільного додатку користувача для негайного реагування.

Робота будь-якої підсистеми системи РД здійснюється за трирівневою архітектурою: периферійний – контрольний – хмарний. Процес завжди починається з тригера на периферійному або зовнішньому рівні. Розберемо кожну підсистему із її описом роботи окремо, для більш детального опису принципу роботи:

Наприклад, у підсистемі контролю доступу, датчик відкриття замку фіксує зміну стану і через локальний, низько-енергетичний протокол надсилає зашифрований пакет даних на центральний шлюз/контролер. Шлюз ідентифікує подію, оцінює її пріоритет та виконує локальну логіку - наприклад, активує сценарій "Ласкаво просимо" у системі освітлення, регулюючи яскравість. Ця локальна обробка є критично важливою для безпеки та комфорту, оскільки гарантує швидку реакцію та незалежність від зовнішнього інтернет-з'єднання. Після локальної реакції, контрольний рівень ініціює зв'язок із хмарним середовищем для віддаленого сповіщення та управління. Центральний шлюз встановлює захищене з'єднання (TLS/HTTPS) із хмарним сервером виробника і надсилає деталізовану інформацію про подію (наприклад, «Двері відкриті»). Хмарний сервер, своєю чергою, генерує Push-сповіщення, яке доставляється на мобільний додаток користувача.

У системі відеоспостереження, запит на перегляд потокового відео, ініційований користувачем у додатку, також проходить цей шлях: додаток – хмара – IP-камера. Камера, у відповідь, починає передачу високошвидкісного, але зашифрованого відео-потоку.

У випадку керування станом мікроклімату (наприклад, системи фільтрації та зволоження повітря), потік може ініціюватися зворотним чином або автоматично. Системи фільтрації та зволоження повітря можуть працювати в автоматичному режимі. В цьому випадку, датчик якості повітря надсилає дані про високий рівень CO2 або низьку вологість на контролер. Контролер запускає сценарій, активуючи відповідну підсистему (наприклад, «розумний» зволожувач).

Зворотний зв'язок є невід'ємною частиною архітектури та забезпечує

надійність системи. Після виконання команди (наприклад, увімкнення освітлення або зволожувача), підсистема надсилає пакет підтвердження про успішне виконання на центральний шлюз. Цей статус синхронізується через хмару і відображається в мобільному додатку, підтверджуючи користувачеві, що дія відбулася. З іншого боку, ЗЗ також включає коригувальні дії користувача, які передаються від додатку через хмару до контролера (наприклад, вручну вимкнути примусову вентиляцію).

В основі об'єднання системи буде використовуватись локальна мережа Wi-Fi (за стандартом IEEE 802.11) – це є найпоширенішим варіантом для побутових систем за рахунок простоти використання. На відміну від дротових систем, Wi-Fi виступає транспортним шаром для центрального шлюзу/контролера та для високошвидкісних пристроїв, таких як «розумні» IP-камери. Якщо камера фіксує рух, вона використовує Wi-Fi для встановлення прямого з'єднання з маршрутизатором і починає передачу відео-потоку. Це вимагає високої пропускної здатності, яку забезпечує саме Wi-Fi. Водночас, сам центральний шлюз використовує Wi-Fi або Ethernet для виходу в Інтернет та зв'язку з хмарним середовищем. Таким чином, Wi-Fi є мостом між локальною мережею РД і глобальною мережею, забезпечуючи передачу як масивних даних (відео), так і службової інформації.

Незважаючи на домінування Wi-Fi як транспортного засобу, безпосередній обмін даними між низько-енергетичними пристроями (датчики, освітлення, замки) та шлюзом здійснюється за допомогою інших протоколів, що працюють поверх Wi-Fi або паралельно з ним.

Для підсистем датчиків відкриття/замку та систем освітлення часто використовуються Zigbee або Z-Wave. Ці протоколи мають мале енергоспоживання, що важливо для роботи від батарей, та будують надійну Mesh-мережу, де кожен пристрій може передавати сигнал іншому. Наприклад, датчик відкриття надсилає пакет про зміну статусу через Zigbee на шлюз. З іншого боку, комунікація між центральним шлюзом і хмарним середовищем для обміну статусами (наприклад, стан системи фільтрації повітря) часто використовує легкий

протокол MQTT (Message Queuing Telemetry Transport). MQTT ідеально підходить для швидкої та надійної передачі невеликих пакетів даних (температура, вологість, стан ON/OFF), мінімізуючи навантаження на мережу та хмарні сервери.

Критичним елементом є безпека та зворотний зв'язок на всіх рівнях. Кожна команда, ініційована користувачем через мобільний додаток (наприклад, змінити налаштування системи фільтрації), також використовує MQTT протокол, що гарантує шифрування даних. Цей захищений канал необхідний для запобігання перехопленню команд керування та облікових даних. Зворотний зв'язок також використовує ці протоколи: після того, як команда досягає «розумного» замка і виконується, зашифрований пакет підтвердження (статус "Заблоковано") передається через Zigbee/Z-Wave на шлюз, а потім через MQTT на хмарний сервер, звідки оновлюється інформація в мобільному додатку. Таким чином, Wi-Fi служить магістраллю, тоді як Zigbee, Z-Wave та MQTT, формують багаторівневу мову системи, забезпечуючи її функціональність, енергоефективність та захист даних.

Якщо мережа Wi-Fi в сьогоденні стала відома та впізнавана, а підсистеми системи РД вже були описані, то про зв’язки Zigbee, MQTT та Z-Wave я згадую вперше. Тут потрібно зробити відступ та розкрити ці поняття, описати їх принцип роботи та обґрунтувати свій вибір саме цими моделями протоколів.

2.1.1 Опис протоколу з’єднання підсистеми Zigbee

Zigbee – специфікація мережевих протоколів верхнього рівня – рівня додатків APS та мережевого рівня NWK, – які використовують сервіси нижніх рівнів – рівня управління доступом до середовища MAC та фізичного рівня PHY, регламентованих стандартом IEEE 802.15.4. Zigbee та IEEE 802.15.4 описують бездротові персональні мережі (WPAN).

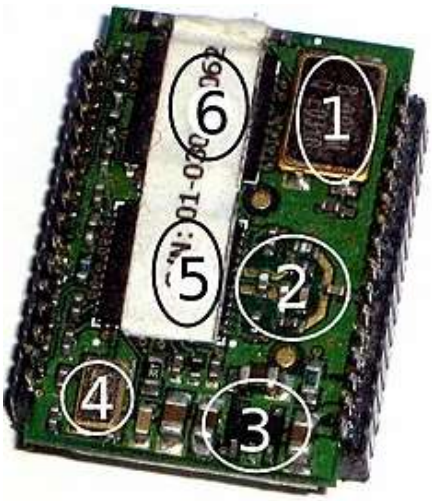

Рис. 2.1.1.1 Плата модулю Zigbee

Специфікація Zigbee орієнтована на програми, що вимагають гарантованої безпечної передачі даних при відносно невеликих швидкостях та можливості тривалої роботи мережевих пристроїв від автономних джерел живлення (батарей).

Основна особливість технології Zigbee полягає в тому, що вона при малому енергоспоживання підтримує не тільки прості топології мережі («точка-точка», «дерево» і «зірка»), але і осередок (Mesh), що самоорганізується і самовідновлюється, з ретрансляцією і маршрутизацією повідомлень. Крім того, специфікація Zigbee містить можливість вибору алгоритму маршрутизації залежно від вимог програми та стану мережі, механізм стандартизації додатків – профілі додатків, бібліотека стандартних кластерів, кінцеві точки, прив'язки, гнучкий механізм безпеки, а також забезпечує простоту розгортання, обслуговування та модернізації.

Основними областями застосування технології Zigbee є бездротові сенсорні мережі та автоматизація житла, медичне обладнання, системи промислового моніторингу та управління, а також побутова електроніка та «периферія» персональних комп'ютерів.

Здатність до самоорганізації та самовідновлення, пориста (Mesh-) топологія, захищеність, висока стійкість до перешкод, низьке енергоспоживання і відсутність необхідності отримання частотного дозволу роблять Zigbee-мережа підходящою основою для бездротової інфраструктури систем позиціонування в режимі реального часу (RTLS).

У межах такої мережі функціонують три основні типи пристроїв: координатор, роутери та кінцеві вузли. Координатор відповідає за формування мережі та керування адресним простором, роутери виконують роль проміжних ретрансляторів сигналу, а кінцеві пристрої - це датчики, контролери або виконавчі механізми, які безпосередньо виконують дії.

Передача даних у системі відбувається у кілька етапів. Наприклад, коли датчик фіксує певну подію, він надсилає сигнал через Zigbee-мережу до центрального шлюзу. Шлюз перетворює сигнал у формат, сумісний з інтернет-протоколами, і відправляє його у хмарне середовище. Там дані обробляються, після чого користувач отримує відповідне сповіщення у мобільному додатку. У разі потреби користувач може через той самий додаток передати зворотну команду - вона проходить через хмару, шлюз і Zigbee-мережу назад до потрібного пристрою, який виконує дію. Саме таким чином, Zigbee забезпечує взаємодію між сенсорами, контролерами та хмарними сервісами, формуючи автономну, надійну та масштабовану систему керування системою РД.

2.1.2 Опис протоколу з’єднання підсистеми Z-Wave

Z-Wave є запатентованим бездротовим протоколом зв'язку, розроблений датською компанією Zensys для домашньої автоматизації, зокрема для контролю та управління в житлових та комерційних об'єктах. Технологія використовує малопотужні та мініатюрні радіочастотні модулі, які вбудовуються в побутову електроніку та різні пристрої, такі як освітлювальні прилади, опалювальні прилади, пристрої контролю доступу, розважальні системи та побутову техніку.

Рис. 2.1.2.1 Плата модулю Z-Wave

Z-Wave – це бездротова радіотехнологія з низьким енергоспоживанням, розроблена спеціально для дистанційного керування. На відміну від Wi-Fi та інших стандартів IEEE 802.11 передачі даних, призначених в основному для великих потоків інформації, Z-Wave працює в діапазоні частот до 1 ГГц і оптимізована для передачі простих керуючих команд з малими затримками (наприклад, включити/вимкнути, змінити гучність, яскравість і т. д.). Вибір низького радіочастотного діапазону для Z-Wave обумовлений малою кількістю потенційних джерел перешкод (на відміну від завантаженого діапазону 2,4 ГГц, в якому доводиться вдаватися до заходів, що зменшують можливі перешкоди від різних побутових бездротових пристроїв, що працюють — Wi-Fi або Bluetooth). Z-Wave призначений для створення недорогої та енергоефективної споживчої електроніки, у тому числі пристроїв на батарейках, таких як пульти дистанційного керування, датчики диму, температури, вологості, руху та інших датчиків безпеки.

В основі рішення Z-Wave лежить мережа (Mesh-мережа), в якій кожен вузол або пристрій може приймати і передавати керуючі сигнали іншим пристроям мережі, використовуючи проміжні сусідні вузли. У системі Z-Wave пристрої розподіляються на дві основні категорії: контролери та слейви – керовані пристрої. Головний контролер є центральним шлюзом, який ініціює мережу, керує нею та маршрутизує дані. Слейви — це всі інші пристрої. Слейви, які постійно підключені до електромережі (наприклад, «розумні» димери, «розумні» розетки), виконують

функцію репітерів, активно підтримуючи Mesh-мережу. Слейви, які працюють від батарей (наприклад, датчики температури, «розумні» замки), більшу частину часу перебувають у стані глибокого сну для збереження енергії.

Передача даних починається, коли слейв (наприклад, датчик відчинення замку) реєструє подію і пробуджується для надсилання пакета даних на головний контролер. Унікальною особливістю Z-Wave є те, що кожен пакет даних містить ідентифікатор джерела та кінцевого пункту призначення, а також інформацію про шлях передачі. Якщо прямий зв'язок неможливий, мережа Z-Wave автоматично обирає оптимальний маршрут через доступні репітери. Усі дані, що передаються в мережі, захищені за допомогою AES-128-бітного шифрування для забезпечення цілісності та конфіденційності інформації. Зворотний зв'язок відбувається, коли контролер надсилає команду слейву (наприклад, "заблокувати замок"), а слейв після виконання дії відправляє пакет підтвердження про зміну свого статусу назад до головного контролера.

Станом на 2018 рік Z-Wave підтримується більш ніж 700 виробниками по всьому світу та покриває широкий спектр споживчих та комерційних продуктів у США, Європі та Азії. Нижні шари протоколу, MAC та PHY, і повністю сумісні, відповідно однією з найголовніших рисою Z-Wave є те, що всі ці продукти сумісні між собою. Сумісність підтверджується процесом сертифікації Z-Wave чи Z-Wave Plus.

2.1.3 Опис протоколу з’єднання підсистеми MQTT

MQTT (Message Queuing Telemetry Transport) є надлегким протоколом обміну повідомленнями, який був спеціально розроблений для використання в умовах обмеженої пропускної здатності мережі, низької потужності та високої затримки. Завдяки цим характеристикам він став ідеальним рішенням для Інтернету Речей (IoT) та систем телеметрії, включно з системами РД. Протокол працює поверх TCP/IP і використовує архітектурну модель "публікація/підписка" (Publish/Subscribe), що кардинально відрізняється від традиційної моделі "Клієнт-Сервер".

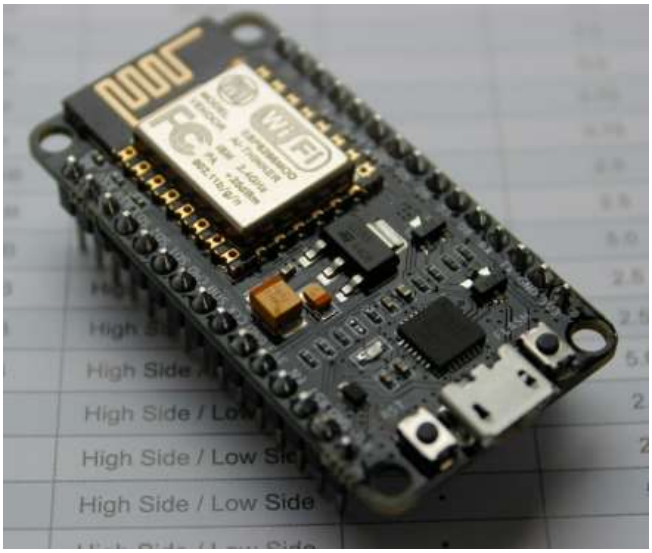

Рис. 2.1.3.1 Плата ESP8266, із вбудованим протоколом MQTT

Центральним елементом архітектури MQTT є Брокер (Broker) - сервер, який виконує функцію комунікаційного центру. На відміну від прямого спілкування, пристрої не звертаються один до одного. Натомість, Видавці (Publisher) - це клієнти (наприклад центральний шлюз), які створюють дані та публікують їх у Брокера на певному тематичному шляху, що називається Топіком (наприклад, home/living_room/temperature). Підписники (Subscriber) - це інші клієнти (наприклад, Мобільний додаток або актуатор), які заздалегідь підписуються на певний Топік і отримують всі повідомлення, опубліковані в цьому шляху. Брокер відповідає за маршрутизацію: він приймає повідомлення від Видавця та миттєво доставляє його всім Підписникам цього Топіку.

Для забезпечення гнучкості та надійності, MQTT пропонує 2 рівні якості обслуговування (QoS). QoS 0 (At most once) забезпечує максимальну швидкість без гарантії доставки, тоді як QoS 1 (Exactly once) гарантує, що повідомлення буде доставлено рівно один раз, що необхідно для критичних команд, як-от оновлення прошивки або команд безпеки. Для використання в професійних і комерційних системах «розумного дому» MQTT-з'єднання завжди повинно бути захищене за допомогою TLS/SSL (Transport Layer Security) для шифрування даних, а клієнти мають проходити автентифікацію перед підключенням до Брокера, забезпечуючи таким чином необхідну безпеку інформаційних потоків.

Принцип роботи протоколу у обраній системі ґрунтується на ролі

центрального шлюзу як Видавця (Publisher) та хмарного сервера як Брокера (Broker). Коли шлюз обробляє дані від локальних пристроїв (Zigbee/Z-Wave), наприклад, отримує статус «заблоковано» від «розумного» замка, він перетворює ці дані на повідомлення MQTT і публікує їх на певному тематичному шляху — Топіку (наприклад, home/security/lock_status). Хмарний брокер приймає це повідомлення і миттєво маршрутизує його всім Підписникам (Subscribers) цього топіка, яким виступає мобільний додаток користувача та механізми хмарного сховища. Таким чином, MQTT гарантує, що дані від датчиків потрапляють до користувача в режимі реального часу, використовуючи при цьому мінімальний інтернет-трафік.

Протокол MQTT також критично важливий для забезпечення зворотного каналу керування. Якщо користувач у мобільному додатку (який також виступає Видавцем) ініціює команду (наприклад, "Увімкнути світло"), ця команда публікується на спеціальному топіку команд (наприклад, home/lighting/command). Центральний шлюз є постійним підписником цього топіка, він миттєво отримує команду від хмарного брокера і перетворює її на відповідний локальний протокол.

Підсумуємо. У проектованій моделі будуть використовуватись 3 протоколи: Zigbee та Z-Wave є взаємодоповнюючими для локальної мережі – Z-Wave забезпечує надійність там, де вона критична (безпека/електро-замки), а Zigbee - економічність та масштабованість (датчики освітлення/вологості). MQTT є зв'язуючою ланкою, що трансформує дані, зібрані локальними протоколами, у ефективний формат для передачі через інтернет, забезпечуючи надійний віддалений моніторинг через хмарний сервіс у мобільному додатку.

Задля кращого розуміння та обґрунтування вибору саме цих систем можемо представити їх у таблиці, вказавши їх переваги та недоліки у порівнянні з іншими протоколами передачі даних.

Таблиця 2.1.3.2

Порівняльна характеристика протоколів передачі даних у системі РД

Протокол	Переваги (в порівнянні з Wi-Fi, Bluetooth, HTTP)	Недоліки (в порівнянні з Wi-Fi, Bluetooth, HTTP)	Роль у Загальній системі РД
Zigbee	Низьке енергоспоживання (на відміну від Wi-Fi) — критично для роботи від батарей. Mesh-архітектура (на відміну від Bluetooth) що передбачає самовідновлення та розширення покриття.	Потребує Центрального шлюзу (на відміну від деяких пристроїв Wi-Fi), які можуть підключатися напряму. Низька пропускна здатність у порівнянні з Wi-Fi, що не підходить для передачі відео.	Горизонтальний зв'язок від пристрою до шлюзу, створює Mesh-мережу на 2.4 ГГц. Використовується для енергоефективних датчиків та спрацьовування освітлення, вентиляції.
Z-Wave	Краща стійкість до перешкод (на відміну від Wi-Fi), оскільки використовує незавантажений спектр. Має кращу проникаючу здатність через стіни.	Має низьку швидкість передачі даних. Обмежена кількість вузлів у мережі (на відміну від потенційно необмеженого Wi-Fi).	Горизонтальний зв'язок від пристрою до шлюзу. Створює Mesh-мережу на низьких частотах (868/908 МГц). Використовується для критичних пристроїв, як електронні замки, через надійність сигналу.
MQTT	Надзвичайна легкість з мінімумом трафіку, порівняно з HTTPS/REST —	Немає вбудованої підтримки сесій та складних транзакцій (на відміну від	Вертикальний зв'язок від шлюзу до хмарного середовища та додатку. Шлюз є

	ідеально для моніторингу статусу. Модель «Публікація/Підписка» (на відміну від REST) забезпечує миттєву доставка до багатьох підписників, що усуває необхідність опитуванні щодо оновлень.	HTTP/REST). Потребує постійного брокера (на відміну від HTTP-запитів).	видавцем, хмара/додаток — підписником. Використовується для ефективної, захищеної передачі телеметрії та команд.

2.2 Основні методи класифікації загроз системам інформаційної безпеки

У пункті 1.5 ми вже говорили про важливість встановлення модулів безпеки при створенні системи ІБ в системах РД, та аналізували основні можливі загрози для систем інформаційної безпеки. Тепер настав час проаналізувати категорії ризиків та фактори що можуть становити небезпеку взагалі для повної системи РД.

Основні категорії ризиків в інформаційній безпеці (ІБ), згідно ISO/IEC 27001:2022 [8], ДСТУ ISO/IEC 27002 [9], класифікуються за різними ознаками, але найчастіше їх характеризують за тріадою CIA – системо аналізу в трьох головних секторах: сектору конфіденційності, сектору цілісності, та сектору доступності. На їх основі запроваджуються правила та пункти для інформування адміністраторів, користувачів та операторів щодо використання захисної продукції для гарантування інформаційної безпеки в межах організацій:

Ризики порушення конфіденційності (Confidentiality) – загроза, що інформація стане відомою тим, хто не має повноважень доступу (несанкціоноване розкриття). До таких ризиків можна віднести витік персональних даних, комерційної таємниці, промислове шпигунство, перехоплення даних.

Ризики порушення цілісності (Integrity) – загроза несанкціонованої або випадкової зміни чи знищення інформації. Порушення цілісності означає, що інформація більше не є точною та повною. З прикладів можна навести зміну фінансових даних, зараження системи вірусами, навмисне або випадкове видалення критичних файлів, некоректне оновлення бази даних.

Ризики порушення доступності (Availability) – це загроза, при якій інформаційний актив (система, мережа, дані) буде недоступний для використання уповноваженими користувачами, коли це необхідно – DDoS-атаки (відмова в обслуговуванні), збої обладнання, відключення електроенергії, стихійні лиха, блокування даних шифрувальниками-вимагачами (ransomware).

Рис. 2.2.1 Зображення моделі Тріади CIA

Модель тріади CIA використовується переважно у бізнес процесах, підприємствах та організаціях із масштабним обсягом даних та великим штатом користувачів, але в нашому випадку створення системи для персонального користування ми скористаємось більш корисної та гнучкою системою оцінки ризиків – аналіз ризику за джерелом загрози. Розрізняють 3 види ризиків за джерелом небезпеки:

1. Антропогенні джерела небезпеки охоплюють суб'єктів (людей), чиї навмисні або ненавмисні дії можуть призвести до порушення інформаційної безпеки. Ця категорія є однією з найбільш значущих і становить високий інтерес для користувачі системи, оскільки людську поведінку часто можна оцінити, прогнозувати та розробити відповідні організаційні методики протидії.

Будь-який суб'єкт, незалежно від наявності повноважень, що взаємодіє зі стандартними інструментами захищеного об'єкта, розглядається як потенційне антропогенне джерело загроз. Суб'єкти, чиї дії призводять до інцидентів ІБ, поділяються на дві основні групи: зовнішні [I.A.] та внутрішні [I.B.].

Зовнішні джерела [I.A.] можуть бути випадковими або невипадковими та характеризуються різним рівнем кваліфікації. До цієї групи належать:

— [I.A.1] організовані злочинні угруповання;

— [I.A.2] потенційні зловмисники та несанкціоновані особи (хакери);

— [I.A.3] несумлінні ділові партнери;
— [I.A.4] технічний персонал, що надає інформаційні послуги (постачальники, аутсорсери);
— [I.A.5] інженерний персонал сторонніх організацій, що здійснюють нагляд або моніторинг;
— [I.A.6] представники правоохоронних та силових органів.

Внутрішні суб'єкти [I.B.] зазвичай є висококваліфікованими спеціалістами, які мають глибокі знання в галузі розробки та експлуатації програмно-технічного забезпечення. Вони ознайомлені з особливостями робочих завдань, внутрішньою структурою, ключовим функціоналом та принципами роботи ІБ, а також вміють використовувати мережеве та персональне обладнання. До них належать:

— [I.B.1] ключовий штат організації (користувачі системи та розробники ПЗ);
— [I.B.2] співробітники служб, відповідальних за захист інформації;
— [I.B.3] допоміжний (обслуговуючий) персонал організації;
— [I.B.4] інженерно-технічний персонал, що забезпечує життєдіяльність та експлуатацію систем (наприклад, системні адміністратори).

2. Техногенна група джерел загроз ІБ включає чинники, які виникають у результаті технічної діяльності людини, але чиї наслідки є неконтрольованими. Ці непередбачувані небезпеки вимагають підвищеної уваги з огляду на актуальні прогнози експертів. Передбачається значне зростання кількості технічних катастроф у сучасних умовах, що часто пов'язано з фізичним або моральним старінням використовуваного обладнання, а також з обмеженістю чи відсутністю необхідних ресурсів для його своєчасного оновлення чи заміни.

Технічні засоби, що можуть стати потенційним джерелом загроз інформаційній безпеці, поділяються на зовнішні [II.A.] та внутрішні [II.B.].

Зовнішні Технічні Джерела Загроз [II.A.] – це елементи інфраструктури, що не належать безпосередньо до захищеного об'єкта, але впливають на його функціонування:

— [II.A.1] засоби комунікації (мережі зв'язку);

— [II.A.2] міські (комунальні) інженерні мережі (наприклад, системи водопостачання та каналізації);
— [II.A.3] транспортна інфраструктура.

Внутрішні Технічні Джерела Загроз [II.B.] – це аспекти програмно-технічного середовища, що використовуються безпосередньо в установі:

— [II.B.1] дефекти або неналежна якість технічного забезпечення, призначеного для обробки інформації (апаратне забезпечення);
— [II.B.2] дефекти або неналежна якість програмного забезпечення, яке використовується для інформаційної обробки (ПЗ);
— [II.B.3] допоміжні технічні засоби (наприклад, системи охорони, сигналізації чи телефонії);
— [II.B.4] інші технічні пристрої та обладнання, що експлуатуються в межах організації.

3. Стихійні джерела загроз ІБ [III.A.] – ця категорія джерел поєднує обставини, що становлять форс-мажор, тобто такі об’єктивні та абсолютні обставини які поширюються та стосуються всіх. Форс-мажор у законодавстві та на практиці включає стихійні лиха чи інші непередбачувані обставини або події, яким практично неможливо запобігти на сучасному рівні людських знань та можливостей. Такі джерела небезпек є повністю непередбачуваними, і тому завжди слід застосовувати заходи захисту. Природні або стихійні джерела ймовірних загроз ІБ розуміються в першу чергу як стихійні лиха:

— [III.A.1] пожежі;
— [III.A.2] землетруси;
— [III.A.3] повені;
— [III.A.4] урагани;
— [III.A.5] різні непередбачувані обставини;
— [III.A.6] явища, які не можливо пояснити;
— [III.A.7] інші форс-мажорні обставини.

2.2.1 Класифікація вразливостей безпеки

Окрім поняття загрози безпеки що прямо впливає на безпеку системі ІБ, існує поняття вразливості безпеки системи. Різниця між ними кардинальна – загроза (в першу чергу мається на увазі зовнішня) є силою або дією що має намір нашкодити системі використовуючи її слабкість, в той же час вразливість безпеки має на увазі внутрішні недоліки системи, або її прогалини. Сама по собі вона не завдає шкоди, але створює можливість для безпосередньої атаки на систему.

Вразливості які є властивими об'єкту інформатизації, невіддільні від нього через недоліки операційного процесу, властивостей архітектури систем, обмінну протоколів та інтерфейсів, програмно-апаратної платформи, умов роботи та розташування. Джерела загроз доволі часто можуть використовувати вразливі місця для порушення ІБ та отримання неправомірної вигоди (заподіяння шкоди власнику або користувачу інформації). Для кожної загрози можна зіставити різні вразливості. Усунення або значне ослаблення вразливостей впливає на здатність реалізовувати загрози інформаційної безпеки. Вразливі місця інформаційної безпеки можуть бути:

— [A] об'єктивні;

— [B] суб'єктивні;

— [C] випадкові.

Об'єктивні вразливості [A] як правило залежать від особливостей конструкції та технічних характеристик обладнання, що використовується на об'єкті, що охороняється. Повністю усунути ці вразливості неможливо, але їх можна значно послабити технічними та інженерними методами відбору загроз інформаційній безпеці. До них належать:

Технічні [A.I], ті, що стосуються технічних засобів які випромінюють:

— [A.I.a] електромагнітні технічні засоби (побічне випромінювання елементів технічних засобів, кабельних ліній, випромінювання на частотах генераторів та підсилювачів);

— [A.I.b] електричні технічні засоби (слабкості, що виникають через наведення електромагнітного випромінювання на кабельних лініях і провідниках,

інфільтрацію сигналів через ланцюги живлення та заземлення, а також через нерівномірне споживання струму джерелами живлення).

— [A.I.c] звукові технічні засоби (недоліки, пов'язані з акустичними та вібро-акустичними каналами (наприклад, через мікрофонний ефект або структурні вібрації)).

Вразливості, що активуються (закладні елементи) [A.II]:

— [A.II.a] апаратні закладки (пристрої, що можуть бути таємно встановлені у телефонних лініях, електромережі, приміщеннях чи безпосередньо у технічних засобах);

— [A.II.b] програмні закладки (вразливості, пов'язані зі шкідливим програмним забезпеченням, технологічними (прихованими) виходами з програм, а також із використанням нелегальних копій ПЗ).

Вразливості, зумовлені характеристиками елементів [A.III]:

— [A.III.a] елементи з електроакустичними перетвореннями (компоненти, здатні перетворювати електричний сигнал на звук і навпаки (наприклад, гучномовці, мікрофони, трансформатори, індуктори тощо));

— [A.III.b] елементи, чутливі до електромагнітних полів (компоненти, на роботу яких впливають зовнішні поля (наприклад, магнітні середовища, певні мікросхеми або нелінійні елементи, чутливі до високочастотного (ВЧ) накладання)).

Вразливості, зумовлені характеристиками об’єкта, що охороняється [A.IV]:

— [A.IV.a] розташування об’єкта (недоліки, пов'язані з відсутністю контрольованої зони, прямою видимістю віддалених об'єктів або рухомих елементів, а також наявністю поверхонь, що відбивають вібрації);

— [A.IV.b] організація каналів обміну інформацією (вразливості, пов'язані з вибором технологій передачі даних, таких як використання радіоканалів, глобальних інформаційних мереж або орендованих каналів зв’язку).

Суб'єктивні вразливості [B] виникають внаслідок людського фактору, зокрема через помилки та порушення режимів роботи.

Помилками [B.I] можна вважати:

- [B.I.a] помилки у підготовці та використанні програмного забезпечення (ПЗ) (включають недоліки, допущені під час розробки алгоритмів та ПЗ, помилки при інсталяції та завантаженні ПЗ, а також огріхи, що виникають при експлуатації ПЗ та введенні даних);
- [B.I.b] помилки під час керування складними системами (недоліки, що виникають при використанні можливостей самонавчання систем, під час налаштовування служб універсальних систем, а також при організації керування потоком обміну інформацією);
- [B.I.c] помилки при експлуатації технічних засобів (недоліки, пов'язані з некоректними діями під час ввімкнення/вимкнення обладнання, неправильного використання технічних засобів захисту або неналежного поводження із засобами обміну інформацією).

Порушенням режимів [B.II] вважаються:

- [B.II.a] порушення режимів охорони та захисту (недотримання правил, що регулюють доступ до об'єкта керування та окремих технічних засобів);
- [B.II.b] порушення режимів роботи технічних засобів (невиконання вимог щодо енергопостачання або життєзабезпечення обладнання);
- [B.II.c] порушення правил користування інформацією (недотримання процедур обробки та обміну даними, а також правил зберігання та утилізації носіїв інформації).

Випадкові вразливості [C] зазвичай залежать від довкілля та непередбачуваних умов. Ці фактори важко спрогнозувати, а їхнє усунення можливе лише шляхом застосування сукупності організаційних та інженерних заходів, спрямованих на запобігання загрозам інформаційній безпеці, до таких вразливостей відносять збої або відмови, ушкодження систем, та підсистем комунікацій.

До першої категорії збоїв та відмов [C.I] належать:

- [C.I.a] збої та несправності технічних засобів (несправності, що стосуються

засобів обробки інформації (наприклад, комп'ютерів), обладнання, що забезпечує їхню ефективність, а також засобів захисту та контролю доступу).

— [C.I.b] застаріння та вихід з ладу носіїв інформації (фізичний знос або поломка знімних носіїв, жорстких дисків, елементів мікросхем, а також кабелів та сполучних ліній);
— [C.I.c] збої програмного забезпечення (несправності або помилки в роботі операційних систем (ОС), систем керування базами даних (СКБД), прикладних програм, утиліт та антивірусного ПЗ);
— [C.I.d] відключення електроенергії (втрата живлення для обладнання для обробки інформації та допоміжного обладнання).

До другої категорії – ушкоджень [C.II], належать:

— [C.II.a] ушкодження комунікацій життєзабезпечення (порушення роботи основних інженерних систем, таких як електрика, водопостачання, газ, теплопостачання, каналізація, а також кондиціонування та вентиляція);
— [C.II.b] ушкодження огороджувальних конструкцій (недоліки, пов'язані з пошкодженням зовнішніх територіальних огорож, стін та стель будівель, а також конструкцій, що захищають технологічне обладнання).

На розумінні визначень та класифікації загроз безпеки системи та вразливостей системи ІБ будується основна робота створення такої системи. Своєчасний аналіз ризиків, підбір компонентів та підсистем загальної системи дозволяє мінімізувати ризик виявлення проблем, а у разі їх виникнення – оперативного рішення цієї проблеми. Тепер, знаючи класифікацію та різницю між цими поняттями, я можу перейти до безпосереднього створення системи захисту ІБ та опису конкретних компонентів із обґрунтуванням вибору кожного компоненту.

2.3 Аналіз ризиків виникнення загроз інформаційної безпеки та вразливостей системи в обраній системі «розумного дому»

Провівши в минулому пункті аналіз джерел походження ризиків та класифікацію вразливостей безпеки ми можемо чітко визначити і зрозуміти потенційних ініціаторів атак для нашої системи ІБ. Це особливо важливо для системи РД пересічного громадянина що має систему у своєму приватному будинку, де фокус загроз зміщується на цільові зовнішні атаки та внутрішні помилки користувачів. Водночас, класифікація вразливостей системи дозволяє нам ідентифікувати, чи криється слабкість у самій архітектурі, чи вона спричинена людським фактором що є ключовим ризиком для користувачів.

Таблиця 2.3.1

Аналіз ризиків виникнення загроз у системі ІБ в системі РД

Класифікація	Опис загрози та об’єкт атаки	Причина виникнення	Рівень вплив у (Impact)	Рівень ймовірності (Likelihood)	Загальний рівень ризику (Risk)
[I.A.1]	Цільова атака на замок/відео	Фізичне підслуховування трафіку Z-Wave з метою Replay-атаки для несанкціонованого доступу до майна.	3	2	6
[I.A.2]	Сканування та злом центрального шлюзу	Віддалений пошук інформації у прошивці шлюзу, що дає повний контроль.	3	2	6

[I.A.3]	Компрометація через сторонніх людей	Стороння людина отримує доступ до логіну/пароля в процесі тимчасового спільного використання системи.	2	2	4
[I.A.2]	Фішинг-атака на члена сім'ї	Зловмисник через фішинг отримує облікові дані для мобільного додатку (доступ до MQTT-сесії) з метою віддаленого саботажу.	3	2	6
[I.B.1]	Несанкціонована зміна конфігурації	Дитина або інший член сім'ї випадково чи навмисно деактивує ключові датчики замку через мобільний додаток.	3	3	9
[I.B.1]	Нецільове використання підсистемою	Власник залишив роботу підсистеми у віддаленому режимі керування, що дозволяє зловмиснику маніпулювати приладом з метою саботажу.	3	3	9

[ІІІ.А.1]	Збій в роботі «розумної» IP-камери	Вихід з ладу накопичувача або перегрів камери, що призводить до втрати відеоспостереження.	2	3	6
[ІІІ.А.2]	Помилкове спрацювання датчика	Технічний дефект датчика відкриття/замку або вплив зовнішніх факторів, що призводить до помилкової тривоги.	1	3	3
[ІІІ.А.3]	Критичний збій центрального шлюзу	Помилка в роботі операційної системи шлюзу, що призводить до неможливості обробки команд Zigbee/Z-Wave.	3	2	6
[ІІІ.А.1]	Конфлікт локальних протоколів (Zigbee/Wi-Fi)	Інтерференція сигналів Zigbee та Wi-Fi (працюють на 2.4 ГГц), що призводить до неможливості спрацювання датчика руху.	2	2	4

Таблиця 2.3.2

Аналіз виникнення уразливостей у системі ІБ в системі РД

Класифікація	Вразливість системи та об'єкт	Приклади прояву вразливості	Рівень впливу (Impact)	Рівень ймовірності (Likelihood)	Загальний рівень ризику (Risk)
[A] Об'єктивні	Слабка криптографічна стійкість (Z-Wave/Zigbee)	Використання старих стандартів безпеки (наприклад, Z-Wave S0 замість S2) у кінцевих пристроях.	3	2	6
[A] Об'єктивні	Відсутність сегментації мережі	Усі пристрої РД знаходяться в одній мережі з корпоративними/особистими пристроями власника.	3	3	9
[B] Суб'єктивні	Неправильна конфігурація MQTT-брокера	Використання QoS 0 для критичних команд, публікація даних на неавторизованих топіках.	2	2	4
[B] Суб'єктивні	Ігнорування оновлень ПЗ	Власник або адміністратор свідомо не встановлює оновлення прошивки центрального шлюзу чи камер з виправленнями CVE.	3	2	6

[C] Випадкові	Збій електроживлення	Відключення основного живлення, що призводить до зупинки системи фільтрації та виведення з ладу роутера/шлюзу без UPS.	2	2	4
[C] Випадкові	Фізичний збій накопичувача	Вихід з ладу HDD/SSD на локальному сховищі відео або на шлюзі, що призводить до втрати архівів та логів.	2	1	2
[C] Випадкові	Стихійні явища та лиха	Фізичне пошкодження підсистем безпеки, особливо зовнішніх, через погодні умови або стихійні явища	2	2	4

В даному випадку я також використовую систему оцінку та вимірювання загального рівня ризику що і в таблиці 1.5.1:
Де, шкала рівню впливу 1–3 позначає рівень впливу на систему:

1 – низький

2 – середній

3 – високий

Шкала ймовірності впливу на систему позначає ймовірність впливу на систему:

1 – низький

2 – середній

3 – високий

загальний рівень ризику (Risk Score) - обчислюється як добуток:

Рівень Ризику = Рівень Впливу x Рівень Ймовірності

Максимальний бал: 9 (Критичний ризик)

Мінімальний бал: 1 (Низький ризик)

Із першої таблиці можна зробити висновок що основний ймовірний вектор розвитку небезпеки йде від несанкціонованої зміни конфігурації налаштувань або параметрів системи та нецільового користування системою – людським фактором що є найбільш небезпечний при побудові системи ІБ. Водночас, середнім рівнем загальної загрози виступають зовнішні загрози пов’язані зі зловмисниками та збоями роботи самої системи. Це пояснюється великою шкодою системі, що може призвести до виводу з ладу окремої підсистеми, або ж до повної втрати контролю всієї системи. Проте такі атаки мають середній рівень ймовірності, це пояснюється тим що порушник повинен мати достатній рівень кваліфікації для злому системи безпеки, а також повної бездіяльності з боку користувача, що впринципі є неможливим з урахуванням постійного моніторингу системи через мобільний додаток.

До загроз із найнижчим показником небезпеки було прийнято рішення включити варіант потенційного ризику із помилковим спрацьовуванням датчику підсистем. Враховуючи загальний рівень побудови системи РД, новітні протоколи передачі та аналізу даних, шанс цього є мінімальним, до того ж не принесе відчутної шкоди для користувача.

Таблиця виникнення вразливостей також була розрахована за таким самим принципом. Згідно неї найвищий рівень ризику має отримати відсутність сегментації мережі, що є найбільш вірогідною вразливістю, з урахуванням можливої недостатньої компетенції користувача, або працівника компанії що буде створювати систему, та рівню шкоди яку може принести дана загроза.

До помірних вразливостей із середнім рівнем небезпеки було додано майже усі інші вразливості, а саме слабку криптографію, невірне налаштування протоколу передачі даних між хмарою та шлюзом, ігнорування оновлень ПЗ підсистем, збої в електроживленні (в тому числі і резервних), а також погодні умов та стихійні явища, що можуть нанести шкоду підсистемам безпеки (особливо зовнішнім, що

знаходяться поза межами будинку). Це пояснюється в першу чергу невисокою ймовірністю вразливості, будь яка система в першу чергу після монтажу буде перевірятися та запускатися в тестовому режимі, де можна буде побачити усі можливі конфлікти підсистем, або проблеми під час її створення, по друге усі підсистеми повинні монтуватися з умовою погодних умов даної місцевості, а також повинні бути забезпеченими фізичним захистом від стихійних лих. По третє, дані вразливості фізично не зможуть нанести критичної шкоди для системи, її збій буде короткочасним і швидко з’ясується, а також виправиться.

До найнижчих вразливостей залишилось віднести лише фізичне пошкодження накопичувача. Це неможливо без прямого, фізичного втручання, а також не принесе великої шкоди, оскільки при необхідності камери все одно будуть функціонувати в автономному режимі, просто без збереження записів відео.

Отже, підводячи підсумок, після проведення роботи на цьому етапі і визначившись із переліком загроз та вразливостей, ми також визначили список найбільш актуальних загроз. На основі цього я і планую вибудовувати основну архітектуру системи покрокового розписуючи систему безпеки як і кожної підсистеми, так і загальної системи ІБ в системі РД.

2.4 Створення системи інформаційної безпеки на основі джерел ризиків із найвищим пріоритетом

Почнемо обґрунтування із описом вибраних протоколів з’єднання системи. Не будемо відходити від запропонованих прикладів із пунктів 2.1.1-2.1.3, тому розберемо самі ці, робочі та дієві варіанти:

Для критичних підсистем (замки, датчики відкриття) обираємо Z-Wave із найновішим стандартом Security 2 (S2). S2 використовує потужне криптографічне хешування Elliptic Curve Diffie-Hellman для генерації ключів, що усуває вразливості старих протоколів. Це гарантує, що пристрої автоматично обмінюються ключами лише після автентифікації на хабі через PIN-код/QR-код, що є прямим контрзаходом проти Replay-атак та слабкої криптографії.

Для енергоефективних та менш критичних пристроїв (датчиків руху та освітлення) обираємо Zigbee з підтримкою Pro Security Mode. Цей режим забезпечує наскрізне симетричне шифрування AES-128 від кінцевого пристрою до шлюзу. Додатково Zigbee Pro підтримує Mesh-маршрутизацію з повторною автентифікацією кожного вузла, що захищає від підслуховування трафіку та вивчення режиму дня власника навіть при розширеній мережі.

Для вертикального зв'язку головного шлюзу із хмарним середовищем використовуємо MQTT поверх TLS/SSL. Це не тільки шифрує трафік від зовнішнього перехоплення, але й забезпечує клієнтську автентифікацію. Це означає, що центральний шлюз повинен мати унікальний сертифікат, щоб підключитися та публікувати дані, що запобігає маніпуляціям даними з неавторизованого джерела.

Підсумовуючи обґрунтування протоколів зведемо всю інформацію до таблиці.

Таблиця 2.4.1

Обґрунтування обраних методів протоколів з’єднань підсистем

Протокол Зв'язку	Ключовий метод безпеки та обґрунтування вибору
Z-Wave S2	Використання ECDH-хешування для захищеної генерації ключів та наскрізне шифрування, що захищає критичні вузли від Replay-атак та слабкої криптографії.
Zigbee Pro	Шифрування AES-128 та механізм повторної автентифікації вузлів у Mesh-мережі, що захищає від підслуховування трафіку та конфліктів у системі.
MQTT + TLS/SSL	Шифрування каналу та двостороння клієнтська автентифікація за сертифікатами, що гарантує захист від компрометації сесії та перехоплення керуючих команд.

Обираючи конкретні приклади периферійних підсистем РД, основний наголос будемо роботи на мережевий захист від зовнішнього злому та атак, та фізичний захист від фізичної шкоди та зовнішніх чинників:

Із різноманітності камер спостереження на ринку, обираємо Ubiquiti UniFi Protect G5 Bullet.

Камера Ubiquiti працює на закритому протоколі та забезпечує локальне зберігання відео (на Network Video Recorder - NVR) без використання зовнішніх публічних хмарних сервісів. Це прямий контрзахід проти загрози компрометації конфіденційності через зовнішній хмарний злом. Камера має закриту систему оновлень FOTA, що нівелює ризик ігнорування оновлень.

Рис. 2.4.2 Приклад камери Ubiquiti UniFi Protect G5 Bullet

Вибір камер спостереження для систем РД на ринку дуже великий, вибір саме на цей варіант впав також через бюджетність варіанту, гарним відгукам користувачів та простоту встановлення та підключення.

Датчиків відкриття замків на ринку також багато, представлені моделі добре співпрацюють в пару із іншими підсистемами, але вибір впав саме на Fibaro Door/Window Sensor 2 (Z-Wave S2).

Використання датчика з підтримкою Z-Wave S2 гарантує, що повідомлення про відкриття замку/дверей не можуть бути перехоплені, дешифровані або використані для Replay-атаки. Датчик фізично захищений від зовнішнього втручання та має вбудований захист від несанкціонованого відкриття корпусу.

Рис. 2.4.3 Приклад датчику Fibaro Door/Window Sensor 2 (Z-Wave S2)

Датчик також є максимально бюджетним варіантом, має багато гарних відгуків, швидке та просте монтування та підключення.

Прикладів систем освітлення, особливо із приходом до українського ринку китайських компаній-виробників, стало дуже багато. Багато з них представляють собою автономні пристрої що добре комунікують з іншими підсистемами, надійно поєднують усі «розумні» лампочки в єдину мережу, мають компактний розмір та зручне налаштування. Із них обираємо надійний варіант Philips Hue (Zigbee 3.0) із «розумними» лампами Philips Hue E27 White.

Рис. 2.4.4 Приклад лампочки Philips Hue E27 White

Рис. 2.4.5 Приклад пристрою Philips Hue (Zigbee 3.0)

Система Hue використовує bridge (міст) як єдину точку виходу в інтернет. Це означає, що лампи (які працюють на Zigbee) ізольовані від прямого зовнішнього доступу. Це контрзахід проти відсутності сегментації, оскільки злом лампи не дасть хакеру доступ до основної мережі.

Системою фільтрації та зволоження повітря виступає система Dyson Pure Cool із датчиком Zooz Ambient Sensor що під’єднанні до «розумної» розетки Z-Wave S2. Система є гарним аналогом багатьох інших варіантів представлених на ринку. Проста система підключення, автономність та бюджетність, робить її чудовим рішенням для приватного користування в системі РД.

Рис. 2.4.6 Приклад «розумної» розетки Z-Wave S2

Рис. 2.4.7 Приклад зволожувача Dyson Pure Cool

Рис. 2.4.8 Приклад сенсору Zooz Ambient Sensor

Щоб запобігти зовнішнім атакам на IoT-інтерфейс, пристрої мікроклімату підключаються через «розумну» розетку (Z-Wave S2). Таким чином, управління здійснюється не через потенційно вразливий Wi-Fi чи хмару виробника фільтра, а через захищений локальний протокол, що контролюється шлюзом.

На перший погляд може здатися що підключення цієї підсистеми складна та довга операція, проте головна мета такого рішення — ізоляція. По перше таким чином ми уникаємо підключення вразливого, комерційного Wi-Fi інтерфейсу очищувача/зволожувача до мережі., а по друге це захищає підсистему від зовнішніх атак та маніпуляцій даними, оскільки команда «ввімкнути/вимкнути» йде через перевірений криптографічний канал.

Підбиваючи підсумки вибори саме цих варіантів підключених підсистем, створимо таблицю із коротким описом обґрунтування обраних варіантів.

Таблиця 2.4.9

Приклади підсистем для використання їх у обраній системі РД з обґрунтуванням вибору

Підсистема	Ключовий метод безпеки та обґрунтування вибору

Камери спостереження	Локальне (NVR) зберігання та закритий протокол. Захист від компрометації конфіденційності через хмару.
Датчики замку/відкриття	Використання Z-Wave S2 із криптографією ECDH. Захист від Replay-атак на критичному вузлі.
Системи Освітлення	Ізоляція ламп від інтернету через шлюз. Контрзахід проти відсутності сегментації.
Системи Фільтрації	Керування через захищену Z-Wave розетку та моніторинг через Z-Wave датчик Zooz Ambient Sensor. Ізоляція від зовнішніх атак на менш захищений IoT-пристрій.

Із широкого вибору шлюзів я обрав модель Ubiquiti UniFi Dream Machine Pro (UDM Pro). UDM Pro — це високопродуктивний мережевий пристрій, який поєднує в собі маршрутизатор корпоративного класу, мережевий комутатор, відео-реєстратор (NVR) та контролер для всіх пристроїв.

Рис. 2.4.10 Приклад шлюзу Ubiquiti UniFi Dream Machine Pro

Хоч UDM Pro і не має вбудованих радіо-модулів Z-Wave/Zigbee, він фізично дозволяє підключити їх як додаткові компоненти – Z-Wave S2 та Zigbee 3.0 підключаються до UDM Pro непрямо. Необхідно додати невеликий USB-радіо-модуль (наприклад, Z-Wave Z-Stick та Zigbee USB-стик) до UDM Pro або до окремого мікрокомп'ютера, який буде підключений до UDM Pro через LAN-порт. На цьому мікрокомп'ютері встановлюється програмний контролер

(наприклад, Home Assistant) для управління Z-Wave/Zigbee.

Також ще одним плюсом використання UDM Pro стає те, що він має вбудовану функцію хмарного середовища, за допомогою додатку UniFi Cloud Access. Це спеціальна служба від Ubiquiti, яка працює через UDM Pro та дозволяє користувачу віддалено підключатися до пристрою через інтернет за допомогою мобільного додатка UniFi Protect.

Тепер час обрати мобільний додаток за допомогою якого користувач буде дізнаватися статус підсистем та керувати ними. Так як обраний мною шлюз вже має готовий варіант додатку – UniFi Protect, використовувати його буде гарною ідеєю. Даний варіант має свої плюси. По перше додаток дуже гнучкий та має багато варіантів використання інструментарію, починаючи із перегляду відео-потоку онлайн, доступу до архіву відеозаписів, отримання вчасного сповіщення про рух, та керування камерами для зміни кута нахилу та зйомки. По друге, компанія надає фізичну гарантію від злому. Виробник заявляє що додаток забезпечує прямий, максимально захищений доступ до критично важливих мережевих налаштувань та локального відео. Єдиний мінус цього рішення, що цей додаток дозволяє керувати виключно підсистемами що належать до серії моделей компанії UniFi, отже в нашому випадку тільки камерами.

Рис. 2.4.11 Приклад мобільного додатку UniFi Protect

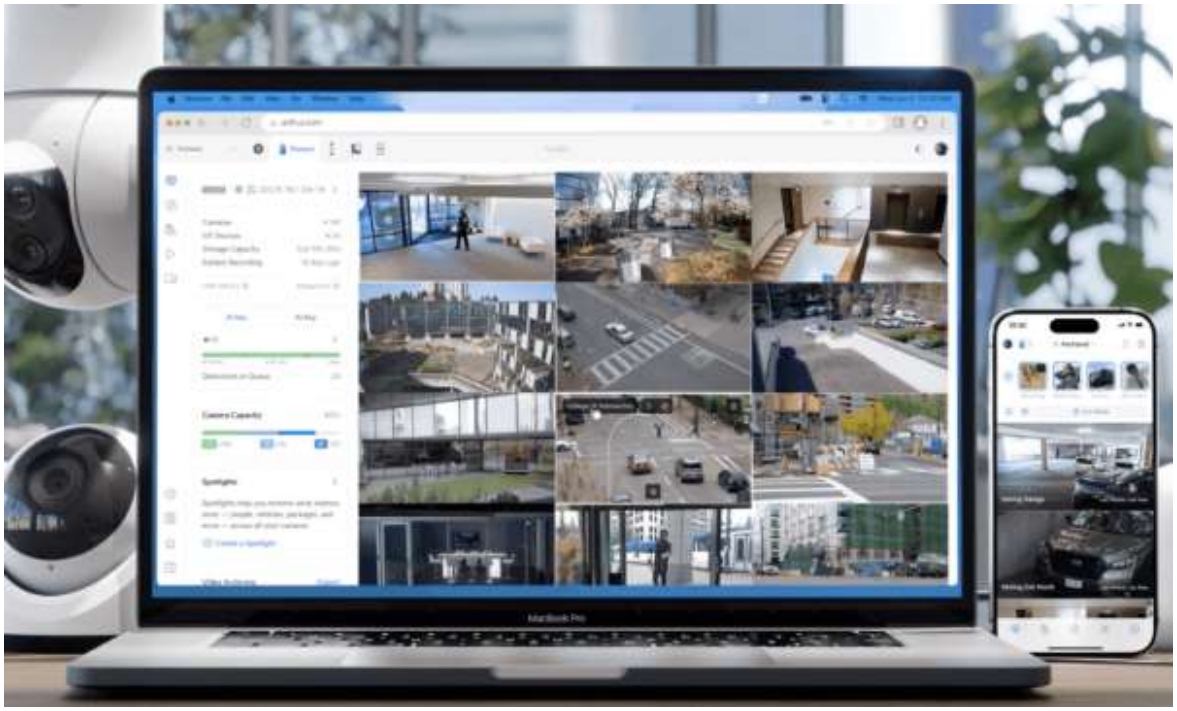

Рис. 2.4.12 Безпосередній вигляд роботи мобільного додатку UniFi

Для інших підсистем що обслуговуються єдиними протоколами зв’язку – ZigBee та Z-Wave, я також готовий надати приклад мобільного додатку – Home Assistant Companion.

Вибір саме на цей додаток впав не просто так. По перше він безкоштовний, що в умовах постановки задачі створення бюджетної системи безпеки є ваговим фактором, по друге, він чудово і легко об’єднує підсистеми в одну систему що працюють на протоколах ZigBee та Z-Wave – якраз ті що я і використовую, по третє він має легкий візуал, що зменшує «рівень входження» в програму навіть для недосвідченого користувача, має зрозумілий дизайн, що повинно забезпечити деяку безпеку від людського фактору джерел загроз, а також підтримує біометричну аутентифікацію (Face ID/Touch ID) для входу, що в повинно зменшити вірогідність несанкціонованого доступу до додатку зі сторони умовного порушника.

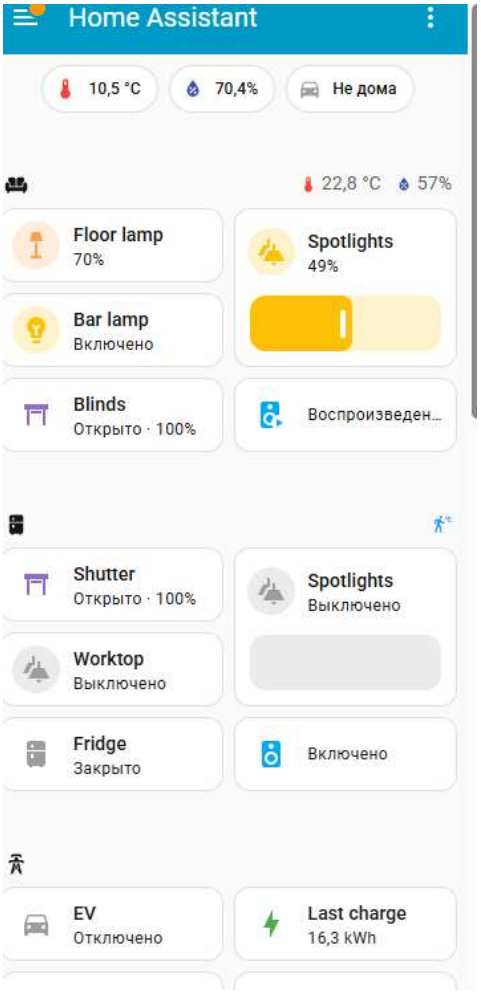

Рис. 2.4.13 Приклад мобільного додатку Home Assistant Companion

Використовуючи усі вище описані приклади підсистем, в кінцевому варіанті наша обрана система РД буде виглядати наступним чином:

Рис. 2.4.14 Схематичний план системи РД із обраними варіантами підсистем

Для прикладу роботи системи розберемо сценарій спрацьовування датчику руху камер – розберемо за якою послідовністю піде передача сигналу, яким чином відреагує шлюз, та які міри безпеки ми зможемо прийняти.

Камера UniFi G5 Bullet виявляє рух у зоні моніторингу, і розцінює її як потенційну загрозу згідно з її внутрішнім алгоритмом. Після цього вона миттєво ініціює запис події та надсилає сигнал про виявлення небезпеки до UDM Pro через захищений Ethernet/TCP/IP канал. UDM Pro, як шлюз-комутатор, отримує сигнал про рух, та починає збереження на своєму локальному жорсткому диску, як відео-реєстратор, та надсилає запит про сповіщення до мобільного додатку через локальну мережу Wi-Fi або через службу UniFi Cloud Access. Отримуючи повідомлення користувач повинен пройти аутентифікацію в мобільному додатку за допомогою (Face ID/Touch ID). Після успішної аутентифікації, додаток UniFi Protect встановлює захищене з'єднання із UDM Pro, після чого користувач може миттєво переглянути запис подій що безпосередньо транслюється з локального

диска на мобільний пристрій.

2.5 Висновок до побудованої системи інформаційної безпеки. Підсумки щодо протидії визначеним джерелам загроз

У висновку дана система ІБ демонструє, що ми ефективно вирішуємо найбільш критичні джерела загроз та вразливості що ідентифіковані на попередніх етапах (нагадую, що ми зосередилися на нейтралізації зовнішніх цільових атак та ризиків, пов'язаних із внутрішніми порушниками), а також створюємо систему РД бюджетною, доступною для невпевнених користувачів системами, та із постійною підтримкою на українському рівні.

Найочевидніша загроза - це зовнішня цільова атака, яка прагне експлуатувати слабку криптографію або незахищені порти. Ми вирішуємо це на двох рівнях. По-перше, на рівні низько-потужних протоколів, використання Z-Wave S2 та Zigbee 3.0 не просто шифрує трафік, а застосовує передові методи, такі як хешування для обміну ключами в Z-Wave. Це усуває цілий клас атак, відомих як Replay-атаки, де зловмисник міг би записати команду "відкрито" та відтворити її пізніше. По-друге, на рівні мережевого периметра, UDM Pro діє як інтелектуальний шлюз. Його вбудовані системи IDS/IPS (системи виявлення та запобігання вторгненням) активно сканують вхідний і вихідний трафік. Якщо зовнішній зловмисник намагається зісканувати порти чи використовувати відомі вразливості для зламу центрального шлюзу, UDM Pro автоматично виявляє та блокує такі спроби, захищаючи найкритичніший вузол мережі.

Дві найбільш суттєві вразливості - відсутність мережевої сегментації та компрометація конфіденційності відео-потоку - усуваються завдяки інтегрованій платформі UniFi. UDM Pro є ключем до вирішення вразливості сегментації: він дозволяє апаратно розділити мережу на окремі VLAN. Це означає, що IoT-пристрої (наприклад, лампи), які мають нижчий рівень захисту, ізолюються від мережі особистих пристроїв (комп'ютерів, телефонів). Таким чином, якщо зловмиснику вдається отримати контроль над одним Zigbee-пристроєм, цей

доступ обмежується лише тим сегментом мережі, що запобігає поширенню атаки на фінансові дані або особисту інформацію власника. Що стосується відеоспостереження, використання UDM Pro як локального NVR є найсильнішим контрзаходом. Відео-потік не передається на сторонні сервери, а зберігається лише на локальному жорсткому диску, усуваючи будь-яку можливість компрометації конфіденційності через зовнішній хмарний злом. Віддалений доступ забезпечується лише через захищене UniFi Cloud Access реле, яке не зберігає дані на хмарних серверах компанії.

Система людського фактору, що була оцінена як високо-потенційне джерело загроз також була підсилена підсистемами для зменшення шансів відтворення та зниження ризиків від шкоди. Ми усуваємо це через приватне та доступне управління. По-перше, для доступу до керування IoT (Home Assistant Companion) та відео (UniFi Protect) обов'язково застосовується біометрична аутентифікація. Це не просто вимагає пароля, але й підтверджує особу власника через відбиток пальця чи сканування обличчя, що ефективно запобігає випадковим або зловмисним змінам критичних налаштувань, таких як деактивація сигналізації. По-друге, UDM Pro інтегрує всі мережеві та відео-функції в єдину консоль управління. Це значно спрощує підтримку та оновлення ПЗ, що є критичним для усунення технічних вразливостей. Замість того, щоб оновлювати роутер, NVR та комутатор окремо, власник керує одним пристроєм, що знижує ймовірність ігнорування оновлень, і, відповідно, ризик експлуатації відомих вразливостей.

Обрана архітектура системи саме з трьох-рівневою структурою демонструє високу актуальність та є стратегічною моделлю для подальшого розвитку ринку IoT у житловому секторі, подібні дослідження вже проводилися в 2021 році [10] компанією NIST. Актуальність визначається кількома ключовими факторами, що відображають сучасні тренди та виклики:

— зі збільшенням кількості підключених пристроїв у будинку вектор атаки розширюється постійно. Системи, що покладаються на стандартну Wi-Fi мережу без сегментації, швидко застарівають, в той час як представлена

модель, яка використовує UDM Pro для апаратної ізоляції, є прямим відображенням майбутнього стандарту ІБ, де мережева сегментація буде обов'язковою вимогою, а не опцією;

— уніфікація підсистем управління, та перехід від "зоопарку" розрізнених додатків до єдиної платформи управління (Home Assistant) та мережевого шлюзу з UDM Pro є ключовим трендом. Ця уніфікація не лише спрощує користувацький досвід, але й мінімізує ризик людського фактору та помилок конфігурації, оскільки оновлення та моніторинг стають більш простими та централізованими;

— локальна обробка даних та зберігання на фізичних носіях шлюзів. У світі, де приватність даних стає найвищою цінністю, архітектура, яка зберігає критичні дані локально та використовує локальний MQTT-брокер, стає базовою вимогою. Це прямий контрзахід проти компрометації конфіденційності та масового витоку даних з хмарних сервісів;

— майбутня стандартизація методів безпеки пропонує використання промислових стандартів шифрування, як Z-Wave S2, що є необхідною умовою для інтеграції систем у більш широку екосистему, наприклад, в екосистему «розумних» міст. Таким чином, системи, які поєднують надійні протоколи, мережеву інфраструктуру корпоративного класу та відкриту, локально-орієнтовану автоматизацію, є не просто актуальними, а є прообразом майбутнього стандарту загальної, безпечної системи РД із прообразом системи «розумного міста».

РОЗДІЛ 3 АНАЛІЗ ЕФЕКТИВНОСТІ ПЕРСПЕКТИВНИХ РІШЕНЬ В СИСТЕМАХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА «РОЗУМНОГО ДОМУ»

3.1 Аналіз майбутніх перспективних рішень інформаційної безпеки

Розвиток систем інформаційної безпеки у контексті «розумного дому» сьогодні визначається необхідністю переходу від традиційних, статичних методів захисту до адаптивних та крипто-графічно стійких архітектур. З огляду на стрімке зростання кількості підключених пристроїв, що розширює потенційний вектор атаки, стратегічною ціллю стає впровадження інноваційних рішень, здатних забезпечити довгостроковий захист даних та цілісність системи.

Штучний інтелект та машинне навчання займають центральне місце в цій еволюції. Вони дозволяють системам ІБ переходити до автономного аналізу поведінки, що є значно ефективнішим за сигнатурний захист. ШІ-керовані системи безпеки здатні постійно моніторити трафік та профілі використання кожного IoT-пристрою, виявляючи навіть мінімальні відхилення від норми – так звані аномалії поведінки мережі. Наприклад, якщо «розумний» термостат раптово починає генерувати великий обсяг мережевого трафіку до зовнішнього IP-адресу, система ШІ, інтегрована в центральний шлюз, може автоматично ініціювати його ізоляцію, блокуючи потенційну загрозу до її поширення. Такий підхід забезпечує своєчасну реакцію на інциденти без постійного втручання користувача.

Ключовим архітектурним зрушенням є повсюдне впровадження концепції «Нульової довіри» (Zero Trust). Традиційна модель, де всі пристрої всередині домашньої мережі автоматично вважаються довіреними, доводить свою неспроможність перед сучасними загрозами. Модель Zero Trust вимагає автентифікації та авторизації кожного запиту на доступ чи комунікацію, незалежно від того, чи надходить він від зовнішнього сервера, чи від сусіднього «розумного» пристрою. У контексті РД, це реалізується через сегментацію мережі, де кожен пристрій або їхня група (наприклад, всі пристрої на протоколі Zigbee)

функціонують у власній ізольованій зоні. Це гарантує, що компрометація одного пристрою не надасть зловмиснику плацдарм для контролю над усією системою.

Для забезпечення довгострокової криптографічної стійкості критично важливим стає перехід до пост-квантової криптографії (PQC). З огляду на прогрес у квантових обчисленнях, існує реальна загроза для чинних асиметричних алгоритмів шифрування, що захищають конфіденційні історичні дані (відео-архіви, дані про режим дня). Впровадження нових, стійких до квантових атак алгоритмів, рекомендованих NIST (наприклад, CRYSTALS-Kyber), у прошивки IoT-пристроїв та центральних шлюзів, є необхідною умовою для захисту особистої інформації протягом десятиліть.

Одночасно відбувається трансформація механізмів контролю доступу через розвиток біометричної автентифікації. Сучасні системи відходять від простих паролів на користь складних біометричних параметрів (розпізнавання обличчя, сканування відбитків пальців), інтегруючи їх не лише у фізичні замки, а й у мобільні додатки для керування. Це не тільки значно підвищує рівень безпеки, оскільки біометричні дані неможливо втратити або передати, але й дозволяє системі персоналізувати налаштування (освітлення, клімат) на основі ідентифікації конкретного користувача.

3.2 Аналіз майбутніх перспективних рішень «розумного дому»

Системи «розумного дому» еволюціонують від простих систем дистанційного керування до складних, інтелектуальних екосистем, що поглиблюють свій функціонал та інтегруються в міську інфраструктуру. Основною рушійною силою цього розвитку також є подальша інтеграція штучного інтелекту та досягнення повної автономії.

Інтелектуальні системи безпеки, підсилені ШІ, значно розширюють свій функціонал. Сучасні ШІ-камери вийшли за межі простого запису, ставши активними аналізаторами зображень у реальному часі. Вони здатні не лише розпізнавати обличчя та відрізняти людей від тварин, але й визначати аномалії в поведінці (наприклад, залишена посилка або рух у незвичний час). Це призводить до критичного зменшення хибних спрацювань та дозволяє системі надсилати сповіщення лише про справді важливі інциденти. Домофони та «розумні» дверні дзвінки стають невід'ємною частиною РД, пропонуючи, наприклад, функцію виявлення посилок, що є важливим елементом безпеки майна.

Управління системами трансформується завдяки голосовим асистентам та «розумним хабам», які виступають центральним елементом екосистеми. Сучасні інтерфейси дозволяють керувати освітленням, клімат-контролем та безпекою за допомогою природної мови, а також інтегрують розпізнавання жестів та персоналізацію налаштувань на основі ідентифікації користувача. Це підвищує зручність використання, але вимагає від розробників постійного посилення безпеки голосових команд та їхньої автентифікації, щоб уникнути несанкціонованого доступу.

Перспективи розвитку тісно пов'язані з подальшою інтеграцією штучного інтелекту, машинного навчання та блокчейн-технологій. Майбутні системи будуть здатні автоматично виявляти та нейтралізувати загрози, адаптуватися до нових типів атак та забезпечувати персоналізований рівень безпеки. Розвиток єдиних стандартів безпеки для IoT-пристроїв та посилення регуляторних вимог до виробників також сприятиме підвищенню загального рівня захищеності систем РД, забезпечуючи їхню надійну інтеграцію у повсякденне життя.

Незважаючи на всі переваги, системи РД стикаються з системними викликами в галузі інформаційної безпеки. Багато пристроїв продовжують мати вразливості, пов'язані зі слабкими паролями за замовчуванням та нерегулярним оновленням мікро-програмного забезпечення. Основні загрози включають атаки типу «людина посередині», розподілені атаки відмови в обслуговуванні (DDoS), що можуть вивести з ладу всю систему, та експлуатацію вразливостей. Це передбачає не лише використання надійних паролів та дво-факторної автентифікації, а й обов'язкову сегментацію домашньої мережі для ізоляції IoT-пристроїв від основної мережі (практика, що буде нормою у майбутньому). Важливим елементом є також освіта користувачів щодо основних принципів кібер-безпеки, словом, для забезпечення належного рівня безпеки необхідний комплексний підхід до створення системи який аналізував та демонстрував в цьому дослідженні.

ВИСНОВКИ

Проведена робота була присвячене комплексному аналізу та розробці архітектури інформаційної безпеки для систем «розумного дому». У рамках роботи було досягнуто поставленої мети та виконано всі ключові завдання, починаючи з надання чітких визначень системи РД та системи ІБ у контексті домашньої автоматизації, що стало основою для подальшого аналізу. Було здійснено ґрунтовний аналіз існуючих рішень РД, що дозволило ідентифікувати переваги та, найважливіше, критичні недоліки найбільш поширених комерційних платформ, особливо у сфері безпеки та приватності даних. Центральною частиною дослідження стало проведення детального аналізу джерел загроз та вразливостей, специфічних для мереж IoT, у результаті чого було виявлено, що найбільшу загрозу становили та становлять зовнішні порушники безпеки, людський фактор при використанні системи, та технічна невідповідність компонентів разом із особливостями монтажу при встановлення , які стали пріоритетними цілями для нейтралізації.

На основі отриманих даних було створено приклад системи РД, яка є максимально універсальною та масштабованою, включаючи критичні підсистеми: керування доступом, відеоспостереження, освітлення та мікроклімат. Ключовим результатом роботи стала розробка відповідної архітектури ІБ на її основі. Ця архітектура базується на апаратній ізоляції периметра через використання шлюзу корпоративного класу Ubiquiti UniFi Dream Machine Pro (UDM Pro) для реалізації мережевої сегментації (VLAN), що стало прямим контрзаходом проти, ізолюючи IoT-пристрої від основної мережі. Також впроваджені протоколи Z-Wave S2 та Zigbee 3.0 для забезпечення наскрізного шифрування та захисту від Replay-атак, а суверенітет даних забезпечено локальним зберіганням відео-потоку на NVR всередині UDM Pro, що усуває ризик через хмарні вразливості.

Підбиваючи загальні підсумки проведеної роботи можна сказати що структура РД не є універсальною та , що найгірше, не має уніфікованої системи створення системи ІБ, і не скоро буде мати. Тому кожну систему слід розробляти

та аналізувати виходячи зі своїх технічних та фінансових можливостей, побажань та рівню професійної обізнаності. Попри це, систему що представив я при написанні цієї роботи є дієвим та цілком реальним варіантом, вона підтверджує, що ефективна безпека РД досягається не за рахунок одного пристрою, а шляхом комплексної, багатошарової оборони, яка поєднує корпоративні стандарти ІБ із гнучкими IoT-протоколами. Ця модель є не лише відповіддю на поточні загрози, але й фундаментальним кроком до створення надійних, масштабованих та етично відповідальних систем РД майбутнього, що відповідають загальним світовим трендам безпеки – Edge AI та Нульової Довіри. Таким чином, всі завдання, поставлені в роботі, були успішно виконані, а запропонована архітектура може бути рекомендована для практичного впровадження.

Оформлення результатів цього дослідження здійснювалося згідно з методичними рекомендаціями кафедри [22].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. «У всьому світі тенденції «розумного дому»» Бер 31, 2023
https://hitech.mediadoma.com/uk/u-vsomu-sviti-tendencii-rozumnogo-budinku/
2. « Netgear (з підсумками Bitdefender)»
https://www.netgear.com/hub/network/2024-iot-threat-report/
3. «ENISA—ThreatLandscape2023»
https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf
4. Top IT, OT, and IoT Security Challenges and Best Practices October 8, 2025
https://www.balbix.com/insights/addressing-iot-security-challenges
5. Security Awareness in Smart Homes: Protect Your IoT Devices 2024-12-12
https://keepnetlabs.com/blog/security-awareness-in-smart-homes-protect-your-io-t-devices
6. Software Update Practices on Smart Home IoT Devices Aug 2022
https://arxiv.org/abs/2208.14367
7. Security and privacy issues for an IoT based smart home May 2017
https://www.researchgate.net/publication/318562742_Security_and_privacy_issues_for_an_IoT_based_smart_home
8. ISO/IEC 27005:2022 , 2022 (Edition 3, 2022)
https://www.iso.org/standard/27001
9. ДСТУ ISO/IEC 27002 17.08.2023
https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=104399
10.NIST SP 800-213, November 2021
https://csrc.nist.gov/pubs/sp/800/213/final
11.ISO/IEC 27005:2022
https://www.iso.org/standard/80585.html
12.NIST SP 800-30 Rev. 1, September 2012
https://csrc.nist.gov/pubs/sp/800/30/r1/final
13.Аналіз ринку «розумного дому» в Україні. 2021 рік Лютий 2021 року

https://pro-consulting.ua/ua/issledovanie-rynka/analiz-rynka-umnogo-v-ukraine-2021-god

14. Z-Wave Alliance Announces Release of 2024B Specification Updates and New Accelerator Membership Level February 6, 2025 https://z-wavealliance.org/news_p/z-wave-alliance-announces-release-of-2024b-specification-updates-and-new-accelerator-membership-level/

15. Довженко, Н., Іваніченко, Є., Складанний, П., & Аушева, Н. (2024). Інтеграція безпеки та відмовостійкості сенсорних мереж на основі аналізу енергоспоживання та трафіку. Кібербезпека: освіта, наука, техніка, 1(25), 390–400. https://doi.org/10.28925/2663-4023.2024.25.390400

16. Довженко, Н., Іваніченко, Є., Костюк, Ю., & Петришин, Л. (2025). Методика виявлення та локалізації кіберзагроз у хмарних середовищах з інтегрованими IoT-компонентами на основі графових моделей. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(29), 762–776. https://doi.org/10.28925/2663-4023.2025.29.938

17. Олійник, Я., Платоненко, А., Черевик , В., Ворохоб, М., & Шевчук, Ю. (2025). Методи захисту інформації в технологіях IoT. Кібербезпека: освіта, наука, техніка, 3(27), 100–108. https://doi.org/10.28925/2663-4023.2025.27.705

18. Костюк, Ю., Бебешко, Б., Гулак, Г., Складанний, П., Рзаєва, С., & Хорольська, К. (2024). Забезпечення кібербезпеки та швидкодії передачі даних у безпровідних мережах. Безпека інформації, 30(3), 365–375. https://doi.org/10.18372/2225-5036.30.20357

19. Крючкова, Л., & Леонтюк, Н. (2024). Програмно-апаратна реалізація алгоритму швидкої оцінки потужності Wi-Fi сигналу в точках простору урбанізованого приміщення. Кібербезпека: освіта, наука, техніка, 4(24), 241–256. https://doi.org/10.28925/2663-4023.2024.24.241256

20. V. Dudykevych, et al., Platform for the Security of Cyber-Physical Systems and the IoT in the Intellectualization of Society, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 449–457.

21. B. Zhurakovskyi, et al., Secured Remote Update Protocol in IoT Data Exchange

System, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 67–76

22. Жданова, Ю. Д., Складанний, П. М., & Шевченко, С. М. (2023). Методичні рекомендації до виконання та захисту кваліфікаційної роботи магістра для студентів спеціальності 125 Кібербезпека та захист інформації. https://elibrary.kubg.edu.ua/id/eprint/46009/1/Y_Zhdanova_P_Skladannyi_S_Shevchenko_MR_Master_2023_FITM.pdf