НАЦІОНАЛЬНИЙ ТРАНСПОРТНИЙ УНІВЕРСИТЕТ

ФАКУЛЬТЕТ ТРАНСПОРТНИХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра інформаційно-аналітичної діяльності та інформаційної безпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи *бакалавра*

на тему

«Захист автоматизованих інформаційних систем інтернету речей»

Виконала: студентка IV курсу, групи ІБК-IV-І
Спеціальність *122 КОМП'ЮТЕРНІ НАУКИ*
Освітньо-професійна програма «*ІНФОРМАЦІЙНА БЕЗПЕКА В КОМП'ЮТЕРИЗОВАНИХ СИСТЕМАХ*»

_____ / М.О. Бутова /
(підпис) (Ініціали Прізвище здобувача освіти)

Керівник: к.т.н.,доц. _____ / М.М. Дехтяр /
(науковий ступінь, звання) (підпис) (Ініціали Прізвище)

Нормоконтроль: к.т.н., ас. _____ / Клочан А.Є. /
(науковий ступінь, звання) (підпис) (Ініціали Прізвище)

Допущена до захисту
«___»_червня___2024_ р.

Завідувач кафедри: _____ _____ / Аль-Амморі А. Н. /
(науковий ступінь, звання) (підпис) (Ініціали Прізвище)

Рецензент: _____ _____ /_____/
(науковий ступінь, звання) (підпис) (Ініціали Прізвище)

Київ – 2024

НАЦІОНАЛЬНИЙ ТРАНСПОРТНИЙ УНІВЕРСИТЕТ

ФАКУЛЬТЕТ ТРАНСПОРТНИХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра інформаційно-аналітичної діяльності та інформаційної безпеки

Рівень вищої освіти: бакалавр

Спеціальність 122 Комп'ютерні науки

Освітня програма « *Інформаційна безпека в комп'ютеризованих системах* »

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ Аль-Амморі А. Н.
"__" __червня_____2024 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ *БАКАЛАВРА* СТУДЕНТЦІ

_____Бутовій Марії Олексіївні_____
(прізвище, ім'я, по батькові)

1. Тема роботи: «Захист автоматизованих інформаційних систем інтернету речей»

керівник роботи: к.т.н., доц., Дехтяр Марина Михайлівна
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом Національного транспортного університету
від "15" березня 2024 року № 94

2. Строк подання студентом роботи 21.06.2024 р.
3. Вихідні дані до роботи: засоби IoT та методи захисту інформації
4. Зміст пояснювальної записки (перелік питань, які потрібно розробити):

_____
.

1) Аналіз та дослідження вибраної предметної області
2) Огляд технологій для реалізації та захисту IoT
3) Визначення основних загроз для IoT та методів їх запобігання
4) Розробка додатку для реалізації системи розумних речей в приміщенні.

5. Перелік ілюстративного матеріалу/слайдів презентації (з точним зазначенням обов'язкових ілюстрацій)*:*

Застосування технологій IoT; семирівнена модель IoT; ландшафт ризиків безпеки; принципи забезпечення безпеки IoT; розумний будинок; додаток для автоматизації системи розумного будинку; захист розумного будинку .

6. Дата видачі завдання 18.03.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів виконання кваліфікаційної роботи	Строк виконання	Примітка
1	Отримання завдання	18.03.2024	виконано
2	Аналіз літературних джерел	18.03-01.04.2024	виконано
3	Підготовка та написання 1-го спеціального розділу	01.04-08.04.2024	виконано
4	Підготовка та написання 2-го спеціального розділу	09.04-16.04.2024	виконано
5	Підготовка та написання 3-го спеціального розділу	17.04-05.05.2024	виконано
6	Перший попередній захист	06.05.2024 р.	виконано
7	Написання висновків та переліку посилань	07.05.2024-01.06	виконано
8	Оформлення кваліфікаційної роботи і графічного матеріалу	03.06-10.06	виконано
9	Другий попередній захист	11.06.2024	виконано
10	Перевірка роботи на плагіат та підготовка документів до захисту	17.06-19.06.2024	виконано
11	Здача закінченої роботи	21.06.2024	виконано
12	Захист	24.06.2024	виконано

Здобувач освіти _____ М.О. Бутова_____
(підпис) (Ініціали Прізвище)

Керівник роботи,
к.т.н., доц., М.М. Дехтяр
(науковий ступінь, звання) (підпис) (Ініціали Прізвище)

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АІС ІР – автоматизовані інформаційні системи інтернету речей;

IoT – інтернет речей(Internet of Things);

IoS – інтернет сервісів(Internet of Services);

IoP – інтернет людей(Internet of People);

IoC – інтернет контенту(Internet of Content);

ІТ – Інформаційні технології(Information Technology);

WEB – Всесвітня павутина(World Wide Web);

TCP/IP – протокол керування передачею даних(Transmission Control Protocol/Internet Protocol)

IP (Internet Protocol) –набір правил, які визначають, як дані передаються через Інтернет.

LAN (Local Area Network) – це мережа комп'ютерів та інших пристроїв, які з'єднані в межах обмеженої території.

ІКТ-середовище(інформаційно-комунікаційне технологічне середовище) – сукупність технологій, які використовуються для збору, обробки, зберігання та передачі інформації.

ІБ(інформаційна безпека) – практика захисту інформації від несанкціонованого доступу, використання, розкриття, зміни або знищення.

Хакер – людина, яка використовує свої знання комп'ютерів та мереж для отримання несанкціонованого доступу до систем або даних.

ПЗ – програмне забезпечення.

ЗМІСТ

ВСТУП

Актуальність. Інтернет речей (IoT) стрімко розвивається, і кількість АІС IoT (автоматизовані інформаційні системи Інтернету речей) постійно зростає. Ці системи використовуються в різних галузях, включно з промисловістю, енергетикою, транспортом і охороною здоров'я. Системи IoT збирають, обробляють і передають великі обсяги даних, що робить їх уразливими для кібератак. Виходячи з цього, актуальним є посилення заходів безпеки та застосовувати передові методи цих систем відносно потенційних загроз, а також – сприяння впровадженню міжнародних та вітчизняних стандартів безпеки IoT в різних сферах використання.

Предмет дослідження – автоматизовані інформаційні системи Інтернету речей(АІС ІР).

Об’єктом дослідження є процес визначення уразливих для кібератак місць АІС ІР та пошук методів протидії.

Мета роботи полягає в оцінці функціональних можливостей систем інтернету речей з точки зору кіберзахисту та розробці рекомендацій щодо ефективних методів протидії кібератакам на об’єкти IoT.

Завдання дослідження. Досягнення мети досліджень потребує розв’язання таких задач:

1) дослідження історичного розвитку та сучасних напрямків і методів застосування засобів IoT;

2) аналіз проблем і загроз IoT, а також шляхи їх вирішення;

3) проектування системи взаємодії розумних речей для розумного будинку та розгляд методів захисту цієї системи.

Методологія дослідження. До основних методів, які використовуються в роботі, входять порівняння, вимірювання, абстрагування та аналіз. Порівняння дозволяє виявити подібності та відмінності між різними технологіями, загрозами, підходами до розробки. Вимірювання кількісно

оцінює характеристики технологій, загроз, ефективності роботи системи. Абстрагування дозволяє виділити суттєві аспекти досліджуваної теми та уявити певну систему IoT. Аналіз розбиває складні обширні питання на більш дрібні, керовані частини, за допомогою чого дозволяє зробити висновки по темі.

Наукова новизна дослідження полягає у тому, що в кваліфікаційній роботі пропонується застосувати комплексний підхід до аналізу та дослідження вибраної предметної області та надає огляд та порівняння різноманітних технологій для реалізації та захисту IoT.

Теоретичне та практичне значення роботи. Робота розширює теоретичну базу знань про концепцію смарт-речей та описує різні технології, загрози та методи захисту, що робить знання про IoT більш систематизованими та глибокими. Результати дослідження можуть бути використані для розробки нових та більш ефективних систем інтернету речей, а також для вдосконалення існуючих систем за рахунок кращого вибору технологій, підвищення безпеки та надійності. Запропоновані методи запобігання та захисту від загроз можуть бути втілені в життя для забезпечення безпеки та надійності систем смарт-речей.

Структура роботи. Кваліфікаційна робота містить розрахунково-пояснювальну записку, яка виконана на 96 аркушах. Розрахунково-пояснювальна записка складається з 3 основних розділів, містить 24 рисунки та 24 джерела використаної літератури.

РОЗДІЛ 1. ІСТОРІЯ ТА ТЕНДЕНЦІЇ РОЗВИТКУ IoT В СВІТІ ТА УКРАЇНІ

1.1. Сфери застосування IoT та переваги його впровадження

Інтернет речей (Internet of Things, тобто IoT) – одна з найпопулярніших наукових ідей у сучасній комп'ютерній науці, яка наразі активно впроваджується та має потенціал для значного впливу на розвиток сучасного суспільства, адже з його впровадженням багато процесів зможуть відбуватися без втручання людини.

Сама концепція являє собою цілу комунікаційну мережу об'єктів ("речей") з технологією взаємодії один з одним і з навколишнім середовищем. Крім того, вони призначені для виконання певних дій без втручання людини. Іншими словами, кожен пристрій у вашому домі, автомобілі чи ви самі можете обробляти інформацію, обмінюватися інформацією та виконувати різні дії у відповідь на цю інформацію. Середовище, в якому працюють такі пристрої, не обмежується розумним будинком, а може охоплювати ціле місто.

Інтернет речей (Internet of Things, скорочено IoT) — це глобальна мережа підключених до Інтернету речей — пристроїв, оснащених сенсорами, датчиками, засобами передавання сигналів. Зібрані дані аналізуються і на їх основі приймаються рішення. Прикладами є гаражні ворота, кавоварки та телевізори, мобільні телефони, відеокамери, датчики освітленості, датчики температури тощо.

Інтернет речей може інтегрувати реальні об'єкти у віртуальні системи для вирішення абсолютно різних завдань. Ключова ідея полягає в тому, щоб підключити всі об'єкти до мережі, збирати дані і приймати на їх основі рішення. Наприклад, відчинити двері гаража, увімкнути кавоварку чи кондиціонер, вимкнути світло. У такому середовищі створюються якісно інші

умови для бізнесу, охорони здоров'я, екологічної безпеки, а також для людини та її дому.

У такому середовищі створюються якісно інші, ніж сьогодні, умови для бізнесу, для охорони здоров’я, для забезпечення екологічної безпеки, трансформуються особисті та соціальні аспекти життя. Застосування технологій IoT успішно проявили себе у наступних напрямках:

Виробництво:

- Прогнозування поломок обладнання за допомогою датчиків вібрації та шуму.
- Оптимізація виробничих процесів в режимі реального часу на основі даних датчиків.
- Автоматизація завдань з використанням роботів та інших автономних систем.

Інфраструктура:

- Моніторинг стану мостів, будівель та інших інфраструктурних об'єктів для запобігання аваріям.
- Оптимізація дорожнього руху та громадського транспорту для зменшення заторів.
- Контроль за рівнем води та забрудненням навколишнього середовища.

Логістика:

- Відстеження товарів та вантажів протягом усього ланцюжка постачання.
- Оптимізація маршрутів доставки та зниження витрат.
- Контроль за умовами зберігання та транспортування товарів.

Транспорт:

- Розвиток автономних транспортних засобів.
- Підвищення безпеки дорожнього руху за допомогою систем ADAS.

- Оптимізація витрат на паливо та експлуатацію транспортних засобів.

Військово-оборонний комплекс:

- Розробка та використання безпілотних систем.
- Покращення ситуаційної обізнаності на полі бою.
- Підвищення точності та ефективності зброї.

Агро-сектор:

- Моніторинг стану посівів та ґрунту для оптимізації зрошення та внесення добрив.
- Відстеження худоби та контроль за її здоров'ям.
- Прогнозування врожаю та оптимізація логістики.

Торгівля, включаючи роздрібні продажі:

- Аналіз поведінки покупців та оптимізація розміщення товарів.
- Персоналізація маркетингових кампаній.
- Спрощення процесу самообслуговування для покупців.

Банківська і страхова системи:

- Виявлення шахрайства та кібератак.
- Персоналізація фінансових продуктів та послуг.
- Підвищення ефективності роботи call-центрів.

Нафто-газова промисловість і видобуток корисних копалин:

- Пошук та розвідка нових родовищ.
- Оптимізація видобутку та переробки корисних копалин.
- Контроль за викидами парникових газів.

Напрямки Smart home і Smart city:

- Енергозбереження та оптимізація використання ресурсів.
- Підвищення рівня безпеки та комфорту життя в містах.
- Покращення комунікації між жителями та міською владою.

Виробництво і реалізація продуктів харчування:

- Контроль за безпечністю продуктів харчування.

- Відстеження походження продуктів харчування.
- Оптимізація ланцюгів постачання продуктів харчування.

Сфера обслуговування:

- Персоналізація обслуговування клієнтів.
- Покращення ефективності роботи персоналу.
- Зниження витрат на обслуговування клієнтів.

Медицина:

- Віддалений моніторинг стану пацієнтів.
- Проведення операцій за допомогою роботів.
- Розробка нових методів діагностики та лікування.

IT-індустрія:

- Покращення кібербезпеки.
- Розробка нових програмних продуктів та послуг.
- Автоматизація завдань IT-адміністрування.

Рисунок 1.1 — Варіанти використання IoT

Переваги IoT для бізнесу залежать від конкретної реалізації та напрямків діяльності, але суть полягає в тому, що підприємства можуть отримувати доступ до більшої кількості даних про свої продукти, власні внутрішні системи і статус їхньої роботи. Завдяки IoT-датчикам збирається інформація з обладнання та інших компонентів виробництва, що дає глибоке розуміння його функціонування. Ці дані дозволяють формувати комплексне бачення виробничих циклів, виявляти вузькі місця, оптимізувати процеси та прогнозувати можливі проблеми. Це веде до підвищення продуктивності, зниження простоїв та покращення загальної ефективності виробництва. IoT-пристрої збирають дані в режимі реального часу, що забезпечує компанії точну та актуальну інформацію про свою діяльність. Ці дані можна використовувати для структурування та аналізу в режимі реального часу, що допомагає приймати кращі рішення, засновані на фактах. Це може призвести до покращення обслуговування клієнтів, оптимізації ланцюгів постачання та більш ефективного управління ресурсами.

Краще розуміння своїх процесів та даних завдяки IoT дозволяє компаніям оптимізувати витрати та підвищити ефективність. Це може призвести до зниження цін, покращення якості продукції та послуг, а також до більш гнучкого реагування на зміни ринку. В результаті компанії, які використовують IoT, можуть отримати значну конкурентну перевагу.

IoT-датчики можуть використовуватися для віддаленого моніторингу стану обладнання та інших компонентів інфраструктури. Це дозволяє виявляти потенційні проблеми до того, як вони призведують до збоїв або поломок, що економить час, гроші та запобігає критичним ситуаціям. Особливо це актуально для географічно віддалених об'єктів, де фізичний контроль ускладнений. IoT-камери та інші датчики можуть використовуватися для забезпечення безпеки офісів, складів та інших об'єктів. Відеоспостереження в режимі реального часу може допомогти запобігти крадіжкам, вандалізму та іншим злочинам. Крім того, дані з камер

можуть використовуватися для аналізу поведінки людей та оптимізації простору.

Аналіз даних, зібраних з IoT-пристроїв та інших джерел, може допомогти компаніям краще зрозуміти свою цільову аудиторію та їхні потреби. Це дозволяє їм корегувати свою продукцію та послуги, щоб краще відповідати очікуванням клієнтів, що може призвести до підвищення лояльності та задоволеності клієнтів. Крім того, веб-розвідка може допомогти виявити нові ринки та можливості для розширення бізнесу. IoT-пристрої можуть використовуватися для автоматизації замовлення послуги або продукту. Це може включати збір даних клієнтів, підтвердження замовлення, оновлення статусу замовлення та багато іншого. Автоматизація цих процесів може допомогти знизити витрати, покращити обслуговування клієнтів та звільнити час для співробітників, щоб вони могли зосередитися на більш складних завданнях.

1.2. Еволюція та історія розвитку інтернету речей

Інтернет – це вже існуюча річ, яка постійно змінюється і розвивається. Нові додатки та бізнеси створюються нескінченно. Крім того до розвитку Інтернету, технології змінюють його тло. Широкосмуговий зв'язок стає дешевим і повсюдним; пристрої стають потужнішими і меншими з різноманітними датчиками. Велика кількість пристроїв, що підключаються до Інтернету, призводить до появи нових прототипів. пристроїв, що підключаються, призводить до появи нового прототипу: Інтернету речей. IoT обумовлений розширенням Інтернету за рахунок додавання фізичних об'єктів, об'єднаних здатністю надавати більш розумні послуги в міру того, як стає доступним більше даних. Різні області застосування, такі як "розумна" інфраструктура, охорона здоров'я, безпека і спостереження, транспорт, роздрібна торгівля, промисловість, телекомунікації і т.д., вже сьогодні мають

телекомунікації тощо, існують проблеми, пов'язані з Інтернетом речей, особливо в таких сферах, як довіра і безпека, конфіденційність і конфіденційності даних. Таким чином, речі/об'єкти здатні розпізнавати події і зміни в своєму оточенні і діяти і реагувати автономно.

Інтернет був таким не завжди. Перші кроки в розвитку Інтернету були далекими від концепції Інтернету речей. Спочатку Інтернет був просто мережею комп'ютерів, що обмінювалися даними. З розвитком технологій з'явилися нові можливості для підключення до Інтернету різних об'єктів: від домашніх приладів до виробничого устаткування. Це призвело до зародження концепції Інтернету речей. Щоб краще зрозуміти поточний стан та потенціал IoT, важливо простежити його еволюційний шлях.

Рисунок 1.2 — Етапи еволюції інтернету

Pre-internet – це епоха до масового використання Всесвітньої мережі (WWW), яка характеризувалася ізольованими комп'ютерними мережами, обмеженим доступом та простішими протоколами зв'язку.

До настання епохи Інтернету шопінг та фінансові операції вимагали значно більше часу та зусиль. На відміну від сьогоднішнього швидкого та зручного онлайн-досвіду, коли споживачі можуть шукати товари, порівнювати ціни та робити покупки за кілька натискань, попередньо користувачі мусили витрачати багато часу на поїздки до магазинів або чекати на доставку поштою. Також, управління грошима вимагало більше ручної роботи, замість зручного онлайн-банкінгу, який дозволяє перевіряти рахунки та робити транзакції з будь-якої точки світу.

За часів до Інтернету, доступ до інформації був обмеженим. Наприклад, для отримання довідки чи знаходження інформації потрібно було звертатися до книг, енциклопедій або інших джерел, що часто були обмеженими в своєму обсязі та доступності. Зараз же, завдяки Інтернету, ми маємо необмежений доступ до величезної кількості інформації, яка оновлюється миттєво.

Крім того, спільне обмін мультимедійним контентом, таким як фотографії та відео, був складним і часом споживаючим процесом до настання Інтернету. Замість цього, сьогодні ми можемо легко ділитися своїми творами зі світом завдяки соціальним мережам та онлайн-платформам.

Pre-Internet ("доінтернетний" період) охоплює час з кінця 19 століття до початку 1990-х років, коли зароджувалися та розвивалися ранні комп'ютерні мережі, які зрештою призвели до створення сучасного Інтернету. Існували окремі комп'ютерні мережі, створені для певних цілей. Прикладами використання таких мереж були:

1) Для військових потреб – багато країн мали і досі мають власні військові мережі для забезпечення безпеки, обміну класифікованою інформацією та координації військових операцій. Створена в 1969 році, ARPANET була першою загальнонаціональною комп'ютерною мережею в США. Її використовували в основному науковці та військові для обміну інформацією та дослідження нових технологій.

2) Для наукових потреб – у наукових сферах існують закриті мережі, де проводяться дослідження та обмін конфіденційною інформацією. Ці мережі можуть використовуватися для співпраці між науковцями з різних країн або для обміну чутливими даними, такими як результати клінічних випробувань. Створена в 1981 році, CSNET була комп'ютерною мережею, яку використовували науковці в галузі комп'ютерних наук. Вона була відома своїми інноваційними дослідженнями в галузі мережевих протоколів та програмного забезпечення.

3) Для урядових потреб – багато урядів мали і мають свої власні закриті мережі для обміну конфіденційною інформацією, забезпечення комунікації між урядовими органами та забезпечення безпеки національних інформаційних ресурсів.

Ці мережі не мали зв'язку між собою і не використовували єдиного протоколу зв'язку. Доступ до комп'ютерів та мереж був обмеженим науковцями, дослідниками, військовими та деякими великими компаніями, в той час як звичайні користувачі не мали можливості використовувати ці мережі.

Використовувалися ранні протоколи зв'язку, такі як X.25, які не були настільки гнучкими та масштабованими, як TCP/IP, що використовується в сучасному Інтернеті. X.25 – це стандарт пакетної передачі даних у телефонних мережах. Він був розроблений операторами в 1970-х, і схвалений підрозділом Міжнародного союзу електрозв'язку CCITT в 1976 році. Стандарт описує протоколи трьох рівнів – фізичного, канального і пакетного. Вони відповідають першим трьом рівням мережевої моделі OSI. Одним із головних недоліків протоколу були великі затримки відгуку – у межах 0,6 сек. X.25 розробляли для передачі даних телефонними лініями. Тоді якість з'єднання була далеко не ідеальною, тому стандарт включав великий обсяг надлишкової інформації для корекції помилок. Цей факт знижував пропускну здатність.

Також не було і функціоналу для зручності користувачів, що вказувало на нерозвиненість інтернету, наприклад, не існувало гіпертексту. Гіпертекст – це нелінійна система організації тексту, яка складається з текстових блоків, пов'язаних між собою гіперпосиланнями. Це робило навігацію по мережі складною та неефективною. Користувачі мали вручну вводити адреси або переходити по ланцюжках посилань, щоб знайти потрібну інформацію.

Однак контент в основному був текстовим. Зображення та мультимедіа зустрічалися рідко. Мультимедіа – це поєднання різних способів подання інформації на одному носієві, наприклад текстової, звукової, графічної, анімації, відео.

Важливо зазначити, що pre-internet не був "порожнім простором". На той чай вже існували попередники Інтернету, такі як телетайпні мережі, BBS (дошки оголошень) та електронна пошта, які вже дозволяли людям спілкуватися та обмінюватися інформацією. Ці технології вже створювали базу для майбутнього Інтернету, відкриваючи нові можливості для взаємодії та співпраці між користувачами.

В епоху Pre-Internet відзначалися важливі події, що вплинули на подальший розвиток інтернету в цілому та призвели до появи Інтернету речей.

- 1969: Створення ARPANET, першого прототипу Інтернету.

ARPANET (Advanced Research Projects Agency Network) – це перша загальнонаціональна комп'ютерна мережа, створена в США у 1969 році. Її розробив Департамент оборони США (DOD) з метою забезпечення стійкості зв'язку в разі ядерної атаки. ARPANET стала основою для сучасного Інтернету, заклавши фундамент для багатьох його ключових технологій та протоколів.

- 1973: Винахід TCP/IP, ключового протоколу для сучасного Інтернету.

1973 рік став знаковим для історії Інтернету, адже саме тоді було винайдено TCP/IP (Transmission Control Protocol/Internet Protocol) – комплекс протоколів, який став основою для мережевих комунікацій в сучасному Інтернеті. До його появи різні мережі використовували різні протоколи, що ускладнювало обмін інформацією між ними. Ранні протоколи не могли гарантувати надійну доставку даних, що призводило до втрати пакетів та помилок. Також ранні протоколи не були масштабованими, що обмежувало їхню здатність підтримувати великі мережі. TCP/IP одразу вирішив цю низку проблем, з якими стикалися ранні комп'ютерні мережі, надавши набір протоколів, які могли використовуватися в будь-якій мережі, незалежно від її типу або розміру. TCP/IP гарантували надійну доставку даних, використовуючи механізми контролю помилок та повторної передачі. До того ж, TCP/IP могли підтримувати великі мережі з мільйонами користувачів. Винахід TCP/IP мав революційний вплив на розвиток Інтернету. Він дозволив створити глобальну мережу, яка могла об'єднувати комп'ютери з усього світу. TCP/IP також сприяв розробці нових Інтернет-технологій, таких як електронна пошта, Всесвітня мережа (WWW) та протокол передачі гіпертексту (HTTP). TCP/IP – це не просто протокол, а фундамент, на якому побудований сучасний Інтернет. Він відіграв ключову роль у перетворенні Інтернету з експериментальної мережі на глобальну платформу для спілкування, торгівлі та обміну інформацією.

- 1983: Створення першого інтернет-домену.

У 1983 році відбулося створення домену .com, що є одним із найважливіших подій в історії Інтернету. Домен .com є скороченням від "commercial" (комерційний) і був спроектований для використання комерційними організаціями, бізнесами та приватними користувачами. Цей домен став одним з найпопулярніших і широко використовуваних доменів у світі. Створення домену .com було частиною більшого проекту, спрямованого на створення структури для Інтернету, щоб краще організувати його рост і

розвиток. Домен .com відразу ж став символом комерційного потенціалу Інтернету, відкривши двері для бізнесів на всій планеті, щоб займатися електронною комерцією, рекламою та іншими видами діяльності в онлайні. Запровадження домену .com сприяло експоненційному зростанню Інтернету як комерційної платформи. Багато з найвідоміших та успішних компаній світу, таких як Amazon, Google, eBay та інші, використовують домен .com у своїх URL-адресах, що підкреслює його значення як символу ділового успіху в онлайн-світі.

- 1984: Розробка протоколу HTTP, який використовувався для передачі

веб-сторінок.

У 1984 році технологічний інженер Тім Бернерс-Лі в ЦЕРН (Європейська організація з ядерних досліджень) розробив протокол HTTP (Hypertext Transfer Protocol), який став фундаментальним стандартом для передачі веб-сторінок. HTTP є протоколом зв'язку між клієнтами та серверами в Інтернеті, який дозволяє запитувати та передавати ресурси, такі як веб-сторінки, з веб-серверів до веб-браузерів. Основною метою HTTP було забезпечити стандартизований спосіб доступу до веб-ресурсів та обміну даними між комп'ютерами по всьому Інтернету. Протокол HTTP сприяв поширенню та розвитку Всесвітньої павутини, оскільки він упростив взаємодію між користувачами та веб-серверами, зробивши процес отримання веб-сторінок більш ефективним та стабільним. HTTP використовується для передачі різноманітних даних, таких як текст, зображення, відео та інші мультимедійні ресурси, що робить його невід'ємною частиною веб-світу сьогодення.

В решті решт, Pre-internet був важливим етапом в історії технологій, який підготував ґрунт для революційного впливу Інтернету на наше життя. Цей етап призвів мережу та підготував людей до наступного – Internet of Content.

Інтернет контенту (IoC) – це концепція, яка описує екосистему, де цифровий контент (текст, зображення, аудіо, відео тощо) стає самостійним об'єктом з унікальною ідентифікацією та можливостями для інтеграції та взаємодії з іншими даними та сервісами. IoC прагне створити більш децентралізований та гнучкий Інтернет, де контент не обмежується веб-сайтами або платформами, а може вільно переміщатися та використовуватися в різних контекстах.

У 1989 році британський вчений Тім Бернерс-Лі розробив та представив концепцію Всесвітньої мережі (World Wide Web або WWW), яка відіграла важливу роль у тому, як ми використовуємо Інтернет сьогодні. Винайдений як спосіб обміну інформацією між вченими на ЦЕРН, WWW став ключовим кроком у розвитку Інтернету, роблячи його доступним для широкого загалу користувачів. Відмінність WWW полягала в тому, що вона впроваджувала концепцію гіпертексту, що дозволяє користувачам переходити з одного документу чи веб-сторінки на іншу за допомогою гіперпосилань. Це значно полегшило навігацію в мережі та зробило її більш інтерактивною. Ключовими компонентами WWW були: URL (Uniform Resource Locator), тобто адреса, яка ідентифікує мережевий ресурс, наприклад, веб-сторінку. URL складається з протоколу передачі, доменного імені та шляху до ресурсу. HTTP (Hypertext Transfer Protocol) – протокол передачі гіпертексту, що використовується для передачі даних між веб-серверами та веб-браузерами. HTML (Hypertext Markup Language) – мова розмітки гіпертексту, яка використовується для створення веб-сторінок. Ці компоненти разом дозволяли користувачам переглядати веб-сторінки за допомогою веб-браузерів та переходити між ними за допомогою гіперпосилань. Створення WWW революціонізувало спосіб доступу до інформації. Ця інновація стала фундаментом для розвитку онлайн-комунікацій, електронної комерції, інтернет-медіа та багато інших аспектів сучасного цифрового життя,

тому що IoC міг запропонувати набагато зручніший доступ до платформ та інформації.

По-перше, IoC не залежить від централізованих платформ або веб-сайтів. Контент може зберігатися та публікуватися в будь-якому місці Інтернету.

По-друге, IoC дозволяє контенту вільно переміщатися та використовуватися в різних контекстах. Його можна інтегрувати з іншими даними та сервісами. Кожен елемент контенту в IoC має унікальну ідентифікацію та властивості, що робить його самостійним об'єктом.

Коли до вже розвиненого Інтернету контенту додалися розвинені IT платформи та сервіси, це зіграло ключову роль у розвитку Інтернету сервісів (IoS), який являє собою екосистему, де користувачі можуть отримувати доступ до різноманітних онлайн-послуг через Інтернет. Інтернет контенту сприяв розробці нових технологій, таких як веб-сервіси, API та хмарні обчислення. Ці технології стали основою для багатьох IoS-послуг. Ці послуги можуть включати соціальні мережі, хмарне зберігання, онлайн-банкінг, електронну комерцію, потокове мовлення, онлайн-ігри та багато іншого. Інтернет контенту змінив поведінку користувачів, зробивши їх більш схильними до використання онлайн-послуг. Користувачі звикли отримувати доступ до інформації та послуг через Інтернет, що створило сприятливий ґрунт для розвитку IoS.

Інтернет сервісів має широкий спектр застосувань. IoS-послуги, такі як електронна пошта, соціальні мережі та месенджери, дозволяють людям спілкуватися та співпрацювати одне з одним онлайн. Зараз такий підхід називають «електронна комерція» (e-commerce) - це купівля та продаж товарів та послуг через Інтернет. E-commerce став одним з найважливіших секторів економіки, завдяки зручності та доступності, які він пропонує як для покупців, так і для продавців. Електронна комерція може бути класифікована на наступні категорії:

- B2C (Business-to-Consumer) – це найпоширеніший тип електронної комерції, який передбачає продаж товарів та послуг споживачам через онлайн-магазини.
- B2B (Business-to-Business) – це тип електронної комерції, який передбачає продаж товарів та послуг іншим підприємствам.
- C2C (Consumer-to-Consumer) – це тип електронної комерції, який передбачає продаж товарів та послуг між споживачами.

IoS-послуги, такі як хмарне зберігання, електронна пошта для бізнесу, інструменти для управління проектами та онлайн-бухгалтерські системи, допомагають людям та підприємствам бути більш продуктивними. Цей комплекс називають електронна продуктивність (e-productivity) - це використання інформаційних технологій для підвищення продуктивності та ефективності роботи.

З часом виникла потреба в більш складній структурі засобів для спілкування, які б могли запропонувати більше можливостей. що призвело до переходу до Інтернету людей. Цей етап розвитку, який розпочався у 1990-2000-х роках, характеризується появою та розквітом соціальних мереж, таких як SixDegrees(дозволяла користувачам створювати профілі, додавати друзів); Classmates(зосереджена на пошуку колишніх однокласників та друзів з дитинства); Friendster(використовувала мережі "шести рукостискань" для пошуку друзів та знайомств); Ці платформи дозволили користувачам створювати профілі, спілкуватися з друзями та знайомими, ділитися контентом та формувати онлайн-спільноти. Ранні соціальні мережі заклали фундамент для того, що ми знаємо як Інтернет людей сьогодні. Вони продемонстрували силу онлайн-спілкування та заклали основу для розвитку більш складних та інтерактивних платформ, які з'явилися пізніше.

Web (мережа тільки для читання) - перша версія Інтернету, яка складається з вебсторінки, створеної розробником для великої групи читачів, що дозволяє їм отримувати доступ до фактів, інформації та контенту з

джерел. Люди використовують термін «Web1» для опису ранньої форми Інтернету. Користувачі побачили перший приклад всесвітньої мережі, який продемонстрував потенціал цифрового зв'язку та обміну інформацією. Web був розроблений Тімом Бернерсом-Лі (ЦЕРН, 1990), який надав перший редактор вебсторінок та браузер (worldwideweb.app).

Користувачі могли лише пасивно споживати інформацію, представлену на веб-сторінках, створених вручну веб-розробниками. Ці сторінки не оновлювалися динамічно, а HTML 3.2 був основною мовою розмітки, яка використовувалася для їх створення. Взаємодія з веб-сайтами Web 1.0 була обмежена. Користувачі могли вводити дані у HTML-форми, які потім надсилалися електронною поштою на сервер. Вміст веб-сайтів зберігався у файловій системі сервера, а не в системі управління реляційними базами даних. Для візуалізації інформації використовувалися GIF-зображення та інші графічні елементи.

Основною метою Web 1.0 було полегшення пошуку інформації користувачами. URI/URL використовувалися для ідентифікації унікальних веб-сторінок, а HTTP (Hypertext Transfer Protocol) був основним протоколом, який використовувався для передачі даних між веб-серверами та браузерами.

Сучасні соціальні мережі використовують алгоритми машинного навчання та штучного інтелекту для персоналізації досвіду користувачів. Це означає, що кожен користувач бачить контент, який релевантний його інтересам. Тому те, що сучасні соціальні мережі зосереджені на візуальному контенті, такому як фотографії, відео та прямі трансляції не є проблемою.

Web2 (соціальні мережі) - це друге покоління Інтернету, що дає змогу створювати інтерактивні та добре продумані сайти, зручні для пошуку, і мобільні додатки, які зберігають, відображають і оновлюють дані в режимі реального часу через інтерфейси. На відміну від Web 1.0, де користувачі були переважно пасивними споживачами статичного контенту, Web 2.0 надає людям можливість створювати власний контент, ділитися ним з іншими та

взаємодіяти один з одним. Web2 з'явилася в 1995 році з народженням AJAX, Javascript та інших технологій. Сучасна версія інтернету Web2, з якою ми знайомі, визначає сучасну взаємодію з усіма платформами, включаючи Amazon, Facebook, Spotify, Discord та інші платформи і соцмережі.

Web 2.0 використовує HTML для структурування контенту веб-сторінок, CSS для форматування та стилізації, URI/URL для ідентифікації унікальних веб-сторінок, а HTTPS для безпечного шифрування даних. Javascript(мова сценаріїв) використовується для створення динамічно оновлюваного контенту, управління мультимедіа та анімації зображень. SDN використовується для централізованого управління мережевою інфраструктурою.

Популярними сьогодні стають так звані «розумні речі», або Smart речі (Smart – розумний, енергійний, кмітливий). Наприклад, гаджети, які зручно носити з собою, мають невеликі розміри і незначну масу — «розумний» годинник, фітнес-трекери, смарт-окуляри, гнучкі екрани. Smart технологія — це процес взаємодії об’єктів з оточуючим середовищем, що наділяє цю систему здатністю адаптації до нових умов, саморозвитку та самонавчання, ефективного досягнення цілей.

Ще у 1926 Нікола Тесла в інтерв’ю журналу «Collier’s» заявив, що одного разу в майбутньому радіо буде перетворено у певний «великий мозок», і, в результаті, всі речі стануть частиною єдиного цілого, а інструменти, завдяки яким це стане можливим, будуть легко поміщатися у кишені.

Базова концепція мережі розумних пристроїв була розглянута ще в 1982 році, коли з'явився перший прилад, підключений до ARPANET. Це був автомат з продажу кока-коли в Університеті Карнегі-Мелона. Машина, про яку йде мова, була холодильником. Місцеві програмісти керували автоматом з продажу кока-коли, підключивши його до Інтернету. Він міг повідомляти про

свої запаси, а також про те, чи були щойно завантажені напої холодними чи ні.

Поняття "Інтернет речей", як і сам термін, вперше з'явилося у виступі Пітера Т. Льюїса у Вашингтоні, округ Колумбія, у вересні 1985 року, який був опублікований у вересні 1985 року. У жовтні 1989 року на конференції INTEROP Джон Ромкі розробив тостер, який можна було вмикати та вимикати через Інтернет, що вважається першим гаджетом Інтернету речей. Для зв'язку тостера з комп'ютером використовувалася мережа TCP/IP.

Сучасне бачення Інтернету речей ґрунтується на статті Марка Вайзера про повсюдні обчислення 1991 року "Комп'ютер двадцять першого століття", а також на академічних форумах, таких як UbiComp і PerCom.

Кевін Ештон з Procter & Gamble, пізніше Центр автоматичної ідентифікації MIT, в 1999 році незалежно ввів термін "Інтернет речей", хоча він віддає перевагу фразі "Інтернет для речей". У той час він вважав радіочастотну ідентифікацію (RFID) критично важливою для Інтернету речей, яка дозволить комп'ютерам керувати всіма окремими речами. RFID-мітки часто прикріплюють до різних об’єктів, щоб можна було відстежувати їх місцезнаходження в режимі реального часу за допомогою високочастотних радіохвиль. Це одна з технологій, яка використовується в рішеннях з управління активами.

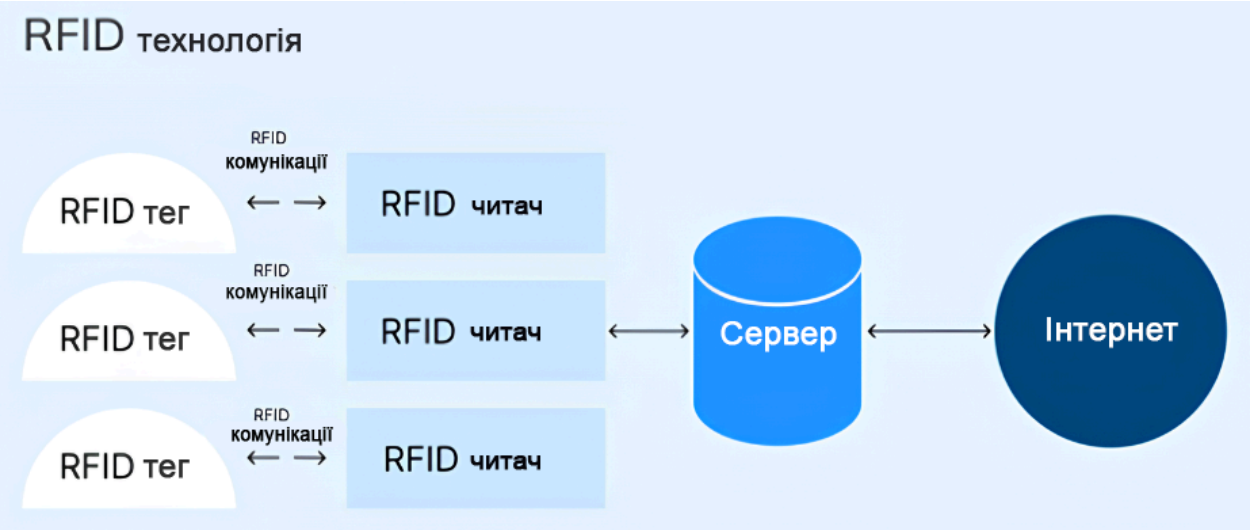

Рисунок 1.2 — Принцип роботи технології RFID

У 2005 році, коли Міжнародний союз електрозв'язку (МСЕ) Організації Об'єднаних Націй опублікував свій перший звіт, Інтернет речей вийшов на новий рівень. У 2006-2008 ЄС визнає IoT, і відбувається Перша європейська конференція IoT. А одразу після цього кількість підключених до мережі предметів перевищило кількість підключених до мережі людей. Тобто, Інтернет речей перегнав Інтернет людей. Багато експертів відзначили справжній початок ери технології IoT у 2013 році, хоча її поява не викликала у громадськості особливого інтересу. Втім, це було пов’язано з тим, що спочатку IoT стартувала як технологія міжмашинної взаємодії без людської участі (machine-to-machine, M2M) для безпроводових систем моніторингу. І лише дещо згодом до неї почали підключати все, що так чи інакше пов’язане із вбудованими обчислювальними системами (наприклад, високопродуктивні мережі – high-end networking, обладнання для цифрових вивісок, робототехніку, дрони, автомобільні комп’ютери і переносні пристрої).

Уже сьогодні «розумні будинки» дають змогу ефективно керувати всіма системами функціонування будівлі за допомогою дистанційних пультів і мобільних телефонів, оптимально витрачати тепло, воду, світло й економити на оплаті комунальних послуг тощо. Усе це створює у світі умови для нового явища – Інтернету майбутнього, який також називають Інтернет всього, або Internet of Everything(IoE), що включає в себе, крім нинішнього Інтернету людей (Internet of People, IoP), ще й Інтернет речей (Internet of Things, IoT), Інтернет контенту (Internet of Media, IoM), Інтернет сервісів (Internet of Services, IoS).

Рис. 1.2 — Інтернет майбутнього

IoT з технологічної точки зору – це, по суті, мережа мереж, що складаються з унікально ідентифікованих об’єктів (фактично «речей»), які можуть взаємодіяти між собою через IP підключення без втручання людини.

Безперечно, для активного використання цих ідей суспільству потрібний дуже швидкісний Інтернет, який може забезпечити впровадження мереж п’ятого покоління 5G. Це сприятиме зменшенню затримки під час передавання даних з датчиків, одночасній підтримці дуже великої кількості підключень, подовженню терміну придатності «розумних» пристроїв до 10 років, а також дасть підґрунтя для неймовірних швидкостей мобільної передачі даних. У той самий час украй важливим у світі «розумних» пристроїв стає питання безпеки. Експерти запевняють, що до 80 % пристроїв будуть уразливі ззовні. Для пристроїв буде потрібна абсолютна надійність мережі, адже найменший збій може призвести до травм або загибелі людей.

1.3. Сучасні тенденції розвитку IoT в світі

По мірі того, як зростає кількість підключених пристроїв наші житлові приміщення будуть наповнюватися "розумними" продуктами, за умови, що ми зможемо підтримувати і контролювати допустимий рівень захищеності, адже ризики залишаються завджи. Існування величезних мереж, які

контролюють весь навколишній світ, глобальна відкритість даних тощо можуть мати як позитивні, так і негативні наслідки. Однак технології продовжуватимуть стрімко розвиватися і поглинатимуть усі сумніви щодо їхньої доцільності та безпеки.

Очікується, що дохід світового ринку IoT у 2024 році становитиме близько 1,387 мільярда доларів США, тоді як у 2028 році прогнозований обсяг ринку становитиме близько 2,227 мільярда доларів США[1]. Це означає, що CAGR за прогнозований період з 2024 по 2028 рік становитиме понад 12,5%.

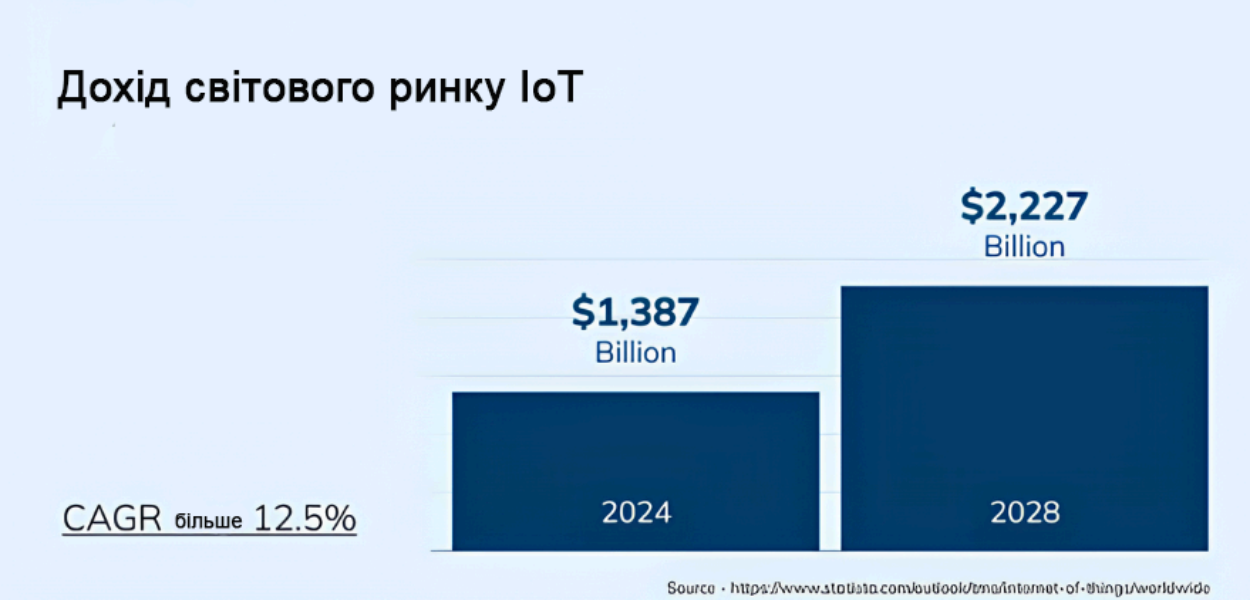

Рисунок 1.3 — Дослідження щодо світових доходів від IoT

Ці цифри виглядають вражаюче, але розглянемо, завдяки чому можливий настільки значний розвиток сфери IoT та з якими чинниками пов’язані величезні витрати.

На початку історія IoT була відзначена розробкою рішень для промислового сектора та розумних міст. Прогнозне технічне обслуговування і досі є одним з найбільш перспективних варіантів використання IoT у промисловості. Системи Інтернету речей, що працюють на основі інструментів штучного інтелекту, можуть не тільки накопичувати дані, пов’язані з технічним станом машин, але й аналізувати їх і виявляти будь-які

ознаки майбутніх проблем. У разі виявлення незвичайних моделей системи IoT надсилають повідомлення операторам, які можуть вжити необхідних заходів. В результаті можна уникнути серйозних збитків, викликаних несподіваними збоями обладнання та простоями.

Серед інших варіантів використання IoT ми повинні згадати відстеження активів, управління ланцюгом поставок, управління запасами, віддалений моніторинг виробництва та використання цифрових близнюків. Останнє рішення дозволяє користувачам створювати віртуальні моделі різних фізичних об’єктів і процесів на основі даних у реальному часі, отриманих від датчиків. Ці віртуальні моделі можуть повністю імітувати реальну продуктивність і поведінку об’єктів, допомагаючи компаніям-розробникам Інтернету речей експериментувати з різними змінами та інноваціями без серйозних фінансових ризиків.

Щодо технологій розумного міста, то це, як правило, масштабні рішення, які об’єднують різноманітні модулі, наприклад, призначені для відстеження трафіку в реальному часі, моніторингу води чи організації розумної парковки. Такі системи можуть допомогти зробити міста безпечнішими завдяки введенню розумного освітлення та інтелектуальних продуктів спостереження. Ми ще не бачили масового впровадження технології розумних міст у всьому світі, оскільки такі проекти вимагають значних інвестицій в інфраструктуру, впровадження та обслуговування. Тим не менш, з довгострокової перспективи ми можемо очікувати значного прогресу в цій сфері, оскільки соціальні переваги таких систем очевидні, від зниження споживання ресурсів до загального підвищення якості життя.

Одним із факторів, який відіграє вирішальну роль у ефективності систем IoT, є швидкість передачі даних та їх обробки. Це одна з проблем, яку сьогодні намагаються вирішити розробники. Стандарт підключення 5G став величезним поштовхом у покращенні якості всіх процесів, пов’язаних з даними. Переваги цієї бездротової технології для IoT:

- Значно вища швидкість передачі даних у порівнянні з 4G;
- Підключення з низькою затримкою;
- Розширені функції енергозбереження для підключених пристроїв, встановлених у приміщенні;
- Покращене покриття всередині приміщень, що дуже важливо для рішень, які використовуються в підвалах, паркінгах тощо; і
- Кращий мобільний широкосмуговий доступ.

Ще один актуальний тренд у розвитку IoT – це так звані периферійні обчислення. Ця стратегія передбачає обробку даних поблизу місця, де вони були зібрані та використовуватимуться. Іншими словами, такий підхід дозволяє не надсилати дані на хмарну платформу для обробки та передачі назад. В результаті обробка даних займає менше часу, а рівень захисту даних вищий.

Одним із найперспективніших варіантів використання є віддалений моніторинг пацієнтів, який можна здійснювати 24/7 без збільшення навантаження на медичних працівників. Завдяки спеціальним медичним приладам можна безперервно відслідковувати зміни в життєво важливих органах пацієнта та в разі потреби вживати відповідних заходів. Існують подібні (але часто спрощені) пристрої, призначені для фітнесу та спорту. Такі пристрої також можуть вимірювати життєві показники та інші важливі фактори під час змагань і тренувань.

Іншим важливим випадком використання IoT для галузі охорони здоров’я є відстеження активів лікарень. Мітки RFID, розміщені на різних предметах і частинах обладнання, полегшують моніторинг їх розташування в режимі реального часу.

Хоча досягнення в індустрії IoT сьогодні можуть виглядати досить вражаючими, очевидно, що вони ще не на завершальній точці розвитку. Пов’язані технології продовжують рухатися вперед, і однією з

найважливіших тенденцій у розвитку IoT є поєднання його зі списком нових технологій.

- IoT та ШІ. Алгоритми штучного інтелекту та машинного навчання вже досить широко застосовуються в рішеннях IoT, але очікується, що в майбутньому це значно збільшиться. У той час як IoT відповідає за збір даних, AI і ML можуть обробляти інформацію, виявляти тенденції, знаходити будь-які відхилення від традиційних моделей і робити прогнози. Усе це важливо не лише для бізнес-планування, але й у багатьох сценаріях реального життя, включаючи системи розумного будинку чи автономне водіння.
- IoT та AR/VR. AR і VR часто асоціюються з індустрією розваг. Однак дует IoT і AR/VR може вийти набагато далі. IoT може відповідати за збір найважливіших даних у режимі реального часу, тоді як пристрої AR і VR можуть демонструвати їх користувачам за допомогою розумних окулярів або спеціальних наголовних дисплеїв. Ці технології можуть значно сприяти розвитку виробництва, управління складами та охорони здоров’я (особливо, коли ми говоримо про складні операції, які вимагають найвищої точності).
- IoT і блокчейн. Очікується, що ця технологія покращить захист і передачу даних у системах IoT. Блокчейн-мережі покладаються на надійні реєстри, які можуть забезпечити цілісність і автентичність даних, що зберігаються в них. Саме для поєднання технологій IoT та блокчейну наразі розвивається всесвітня павутина Web3. Різниця між Web3 та Web2 полягає в управлінні даними та програмами. Web3 децентралізує володіння та зберігання даних на серверах, розташованих у її децентралізованій мережі. Крім того, Web3 відкриває більше можливостей для підключення, оскільки все більше пристроїв Інтернету речей (IoT) можуть отримувати доступ до різних децентралізованих додатків на блокчейнах. І блокчейн, і IoT прагнуть до децентралізації. Блокчейн замінює централізовані органи влади розподіленою мережею, а IoT дає можливість пристроям взаємодіяти один з

одним без посередників. Блокчейн забезпечує прозорість транзакцій, а IoT може збирати та ділитися даними в режимі реального часу. Також блокчейн пропонує стійкість до несанкціонованого доступу та шахрайства, а IoT може використовувати блокчейн для автентифікації пристроїв та захисту даних.

1.4 Інтернет речей в Україні

Враховуючи обставини, здається , що Україна не може бути лідером в сфері інтернет технологій. Втім виявилося, не все настільки погано: інтернет речей в Україні продовжує розвиватися і бути одним з головних лідерів Європи у цій сфері.

У напряму екологічної безпеки в Києві розгорнута мережа сенсорів якості повітря. У застосунку «Київ цифровий» можна подивитися якість повітря в конкретному місці, де перебуває користувач. Ця історія також реалізована на базі інтернету речей. Мережа містить 46 сенсорів, які знімають багато показників. Частина з них доступна користувачам «Києва цифрового», а повний великий набір цих показників – спеціалістам управління екології та іншим зацікавленим особам. Окремо реалізовано контроль викидів шкідливих речовин: у Києві є підприємства, які використовують у своїй роботі хлор та аміак.

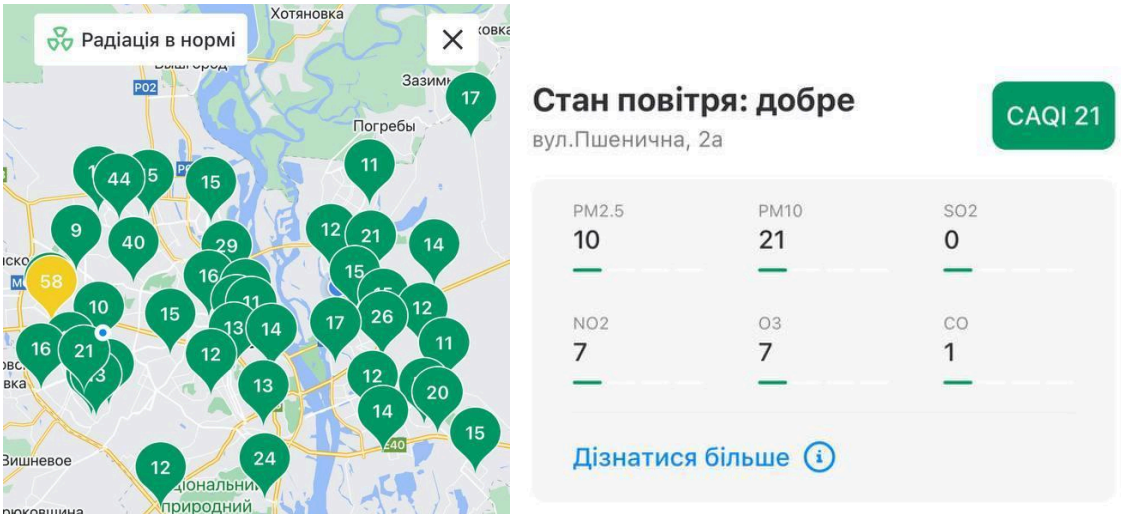

Рисунок 1.4 — Приклад показань в додатку «Київ Цифровий»

Масштабування деяких проектів, що запустили до повномасштабного вторгнення, поки тимчасово зупинили. Наприклад, наразі контроль вивозу сміття, наповнення сміттєвих баків реалізовано в дуже обмеженому вигляді. Ще один цікавий напрям – розробку систем контролю мікроклімату в приміщеннях, наприклад у школах та університетах, планують відновити при першій можливості.

Розвиток IoT дуже важливий, тому що це один з основних важелів розвитку цифрової економіки у світі. Співробітники «Vodafone Україна» кажуть, що IoT – саме той напрям, з яким ми пов'язуємо своє стратегічне майбутнє. Наприклад, можна згадати розумний кар'єр на Єристівському кар'єрі в Полтавській області. IoT там використовується для віддаленого управління буровими установками, екскаваторами та іншою промисловою технікою. Ще одне цікаве рішення було впроваджене для Дунайського пароплавства, у якому IoT моніторить переміщення суден і вантажів по Дунаю в режимі реального часу.

Багато проектів реалізовано для енергетиків, банків і фінансових компаній. Сьогодні вендінгові машини з продажу напоїв і снеків, банкомати, POS-термінали, приміром «Нової Пошти», використовують IoT-рішення. Також цікавим рішенням є цифрова шахта «Ювілейна». Там на глибині 500 метрів під землею провели Wi-Fi та розгорнули купу датчиків і сенсорів. Вони дозволяють бачити, де перебувають шахтарі, у якому вони там стані, чи немає викидів тощо.

Яскравим прикладом, що показує актуальність розвитку IoT на сьогодні в Україні є те, що міністр цифрової трансформації Олександр Борняков у своєму пості на Facebook обговорив концепцію самодостатньої екосистеми для економіки України з використанням технологій Iот та Web 3, що дозволить зробити економічні процедури, наприклад, сплату податків, більш прозорою та такою, що не буде потребувати присутності людини в цьому процесі. CEO WhiteBIT, Володимир Носов, підтримав його, підкресливши

важливість наступних аспектів: чіткого і зрозумілого законодавства для розвиваючогося інтернету, підвищення загальної криптограмотності серед українців та звичайно, наша якнайшвидша перемога у війні.

Інтернет Бойових Речей (IoBT/Mil-IoT) є важливим напрямком розвитку військової технології, що базується на адаптації концепцій Інтернету Речей (IoT) для потреб військових цілей. Ця інновація спрямована на забезпечення зв'язку та інтеграції військових засобів, солдатів та інших активів з метою підвищення ситуаційної обізнаності, точності цілевказівок та ефективності бойових операцій. Одним із ключових аспектів IoBT є здатність об'єднувати передові технології, такі як штучний інтелект, машинне навчання, робототехніка та сенсорні мережі, для створення взаємопов'язаної, інтегрованої оборонної системи. Це дозволяє збирати, аналізувати та передавати дані в реальному часі, що сприяє прийняттю обґрунтованих стратегічних та тактичних рішень у бойових умовах. IoBT відкриває нові можливості для військових командувань, забезпечуючи підвищену ефективність ведення бойових операцій, зменшення ризику для військових осіб та підвищення загальної безпеки. Інтеграція цих передових технологій дозволяє створювати автоматизовані системи моніторингу, реагування та координації, що сприяють підвищенню ефективності та точності військових операцій. У світлі постійного розвитку технологій та зростаючих вимог до військової сфери, IoBT відіграє ключову роль у модернізації та удосконаленні військових стратегій та тактик. Ця інновація сприяє підвищенню бойової готовності, забезпечуючи військовим підрозділам доступ до передових технологій та засобів для успішного виконання завдань у сучасному бойовому середовищі.

РОЗДІЛ 2. ДОСЛІДЖЕННЯ ЗАСОБІВ ТА МЕТОДІВ РОБОТИ IoT ТА АНАЛІЗ ЗАГРОЗ БЕЗПЕКИ

2.1. Екосистема IoT

Інтернет речей (IoT) – це мережа фізичних пристроїв, оснащених датчиками, програмним забезпеченням та підключенням до Інтернету, які можуть збирати та обмінюватися даними. Екосистема IoT складається з багатьох компонентів, які працюють разом, щоб забезпечити безперебійну роботу IoT-пристроїв. Основними компонентами екосистеми IoT є датчики та виконавчі механізми, системи зв'язку з датчиками, локальні обчислювальні мережі, агрегатори, маршрутизатори, шлюзи та пограничні пристрої, глобальна обчислювальна мережа, хмара, сервіси аналізу даних і безпека.

Датчики та виконавчі механізми включають вбудовані системи, що збирають дані або виконують дії, операційні системи реального часу для управління роботою датчиків, джерела безперебійного живлення для забезпечення автономності, а також мікро-електромеханічні системи (МЕМС) для мініатюризації та підвищення точності. Системи зв'язку з датчиками складаються з безпровідних мереж з радіусом дії від 0 до 100 метрів, низькошвидкісних малопотужних каналів передачі даних та спеціальних протоколів, відмінних від IP. Локальні обчислювальні мережі (LAN) базуються на протоколі IP для швидкого обміну даними, таких як Wi-Fi мережі 802.11, і використовують пірингові або зіркоподібні топології.

Агрегатори, маршрутизатори, шлюзи та пограничні пристрої включають постачальників вбудованих систем, виробників модулів, таких як IoT-модулі та пасивні компоненти, виробників мережевого обладнання, стільникових та бездротових систем, а також постачальників програмного забезпечення для міжплатформного використання, туманних обчислень, аналітики, безпеки та сертифікації. Глобальна обчислювальна мережа

представлена операторами стільникового, супутникового зв'язку та LPWAN, які використовують транспортні протоколи Інтернету, такі як MQTT, CoAP та HTTP.

Сервіси аналізу даних обробляють величезні обсяги даних з IoT-пристроїв, здійснюють комплексну обробку подій, аналітику, машинне навчання та видобуток знань з даних для прийняття кращих рішень, а хмара включає інфраструктуру, платформи та послуги для цих потреб IoT. Безпека охоплює захист всіх компонентів IoT: датчиків, процесорів, мереж, протоколів, забезпечення безпеки, достовірності та цілісності даних, а також мінімізацію ризику кібератак.

Одним з найважливіших аспектів розвитку IoT є стандартизація. Відсутність єдиних стандартів може призвести до проблем з сумісністю різних пристроїв та платформ. Для забезпечення інтеграції та взаємодії різних компонентів IoT необхідні стандарти, які визначають загальні правила для підключення, обміну даними та безпеки. Організації, наприклад такі як Інститут інженерів з електротехніки та електроніки (IEEE) та Національний інститут стандартів і технологій(NIST), працюють над створенням таких стандартів.

Рисунок 2.1 — Екосистема IoT

2.2. Стандарти сумісності та еталонні моделі IoT

Останнім часом продовжують виникати сукупності різнорідних рішень, які можуть перевершити розгортання «ідеальних» сценаріїв, де всі IoT-пристрої та системи взаємодіють за допомогою спільних протоколів і рішень IoT на основі стандартів. Це відноситься до багатьох нових технологій на етапі створення.

Наприклад, відзначають, що дві характеристики мережевих IoT-пристроїв, що викликають найбільші проблеми, - це наявність пристроїв з низьким енергоспоживанням (розрахованих на роботу протягом великого часу без підзарядки) і частий обмін даними по мережах з втратою пакетів. Для цих умов стандартні протоколи Інтернету є неоптимальними. Дисбаланс має місце між величезною кількістю пристроїв, що генерують дані з екстримальною швидкістю в різних місцях, і використанням мережевих технологій та хмарних систем, які зберігають величезні обсяги даних в обмеженій кількості локацій при відносно низькій швидкості оновлення

даних. Над вирішенням цих питань працює кілька організацій і стандартизаційних форумів, прагнучі розширити або адаптувати протоколи Інтернету для пристроїв IoT. Основними організаціями та стандартизаційними форумами, що працюють над вирішенням цих питань, прагнуть розширити або адаптувати протоколи Інтернету для пристроїв IoT, є:

– Міжнародний союз електрозв’язку (International Telecommunication Union, ITU): 193 країни і понад 700 членів по секторам і асоціаціям (науково-промислових підприємств, державних і приватних операторів зв'язку, радіомовних компаній, регіональних і міжнародних організацій).

– Всесвітній форум IoT (IoT World Forum, IWF): IBM, Intel, Cisco, Samsung.

– Національний інститут стандартів і технології Міністерства торгівлі США.

– Консорціум індустріального Інтернету (Industrial Internet Consortium,IIC): SAP, IBM, Intel, Fujitsu, General Electric, Oracle.

Ці групи також працюють над питаннями формальної архітектури Інтернету речей, щоб створити єдину структуру та класифікувати необхідні функції відповідно до їх розташування у стеку протоколів. Хоча існуючі стандарти та інтернет зробили можливим IoT, навряд чи найближчим часом з'явиться новий пакет стандартів, який доповнить або змінить існуючі стандарти Інтернету речей. Але, враховуючи масштабність Інтернету речей, має сенс створити архітектуру, яка визначає ключові компоненти та їх взаємозв'язки. Архітектура IoT пропонує ряд значних переваг, як для адміністраторів мереж та IT-менеджерів, так і для розробників. Вона може слугувати контрольним списком для оцінки функціональності та повноти пропозицій від різних постачальників IoT-рішень, орієнтиром для розробників для розуміння необхідних функцій в IoT та їх взаємодії, а також

основою для стандартизації для сприяння сумісності різних IoT-систем, що знижує витрати на розробку та експлуатацію.

Еталонна модель IoT від Міжнародного союзу електрозв’язку (МСЕ-Т) описана в Рекомендації Y.2060 [3]. На відміну від більшості інших еталонних моделей, модель МСЕ-Т деталізує фактичні фізичні компоненти екосистеми IoT. Це важливо, оскільки дозволяє зосередити увагу на елементах екосистеми IoT, які мають бути з'єднані, інтегровані, керовані і надані додаткам. Детальна специфікація екосистеми описує вимоги до можливостей IoT. Важливо зазначити, що IoT не є просто мережею фізичних речей. Це мережа пристроїв, з'єднаних фізичними речами, разом з прикладними платформами, такими як комп'ютери, планшети і смартфони, які взаємодіють з цими пристроями. Розгляд моделі МСЕ-Т слід почати з визначення пристроїв:

o Мережа зв'язку (Communication Network) – інфраструктурна мережа, що з'єднує пристрої та додатки, така як мережа на основі стека протоколів IP або Інтернет.

o Річ (Thing) – предмет фізичного світу (фізичні речі) або інформаційного світу (віртуальні речі), який може бути ідентифікований та інтегрований в мережі зв'язку.

o Пристрій (Device) – елемент обладнання, який володіє обов'язковими можливостями зв'язку та додатковими можливостями вимірювання, спрацьовування, а також введення, зберігання і обробки даних.

o Пристрій переносу даних (Data-carrying Device) – пристрій переносу даних підключається до фізичної речі і непрямим чином з'єднує цю фізичну річ з мережами зв'язку. Прикладами можуть служити активні мітки RFID.

o Пристрій збору даних (Data-capturing Device) – під пристроєм збору даних розуміється пристрій, що зчитує / записуючий пристрій, що має можливість взаємодії з фізичними речами. Взаємодія може здійснюватися

непрямим чином за допомогою пристроїв перенесення даних або безпосередньо за допомогою носіїв даних, підключених до фізичних речей.

o Носій даних (Data Carrier) – безбатарейний об'єкт перенесення даних, підключений до фізичної речі і має можливість надавати інформацію придатному для цього пристрою збору даних. Ця категорія включає штрихкоди і QR-коди, наклеєні на фізичні речі.

o Сенсорний пристрій (Sensing Device) – пристрій, який може виявляти або вимірювати інформацію, що відноситься до навколишнього середовища, і перетворювати її в цифрові електричні сигнали.

o Виконавчий пристрій (Actuating Device) – пристрій, який може перетворювати цифрові електричні сигнали, що надходять від інформаційних мереж, в дії.

o Пристрій загального призначення (General Device) – пристрій загального призначення володіє вбудованими можливостями обробки і зв'язку і може обмінюватися даними з мережами зв'язку з використанням дротових або бездротових технологій. Пристрої загального призначення включають обладнання та прилади, які стосуються різних галузей застосування IoT, наприклад, верстати, побутові електроприлади і смартфони.

o Шлюз (Gateway) – елемент IoT, що з'єднує пристрої з мережами зв'язку. Він виконує необхідну трансляцію між протоколами, що використовуються в мережах зв'язку і в пристроях.

Унікальною особливістю IoT є наявність великої кількості фізичних речей і пристроїв, які відрізняються від традиційних обчислювальних пристроїв та пристроїв обробки даних. Модель IoT розглядає цю систему як мережу пристроїв, тісно пов'язаних з фізичними об'єктами. Сенсори та виконавчі пристрої взаємодіють з фізичними об'єктами у навколишньому середовищі. Пристрої збору даних зчитують або записують інформацію на фізичні об'єкти через взаємодію з пристроями перенесення даних або носіями даних, які тим чи іншим чином підключені або пов'язані з цими об'єктами.

Ця модель чітко розрізняє пристрої перенесення даних та носії даних. Наприклад, RFID-мітка є пристроєм перенесення даних, тоді як носій даних - це елемент, прикріплений до фізичного об'єкта для ідентифікації або передачі інформації. Технології, що використовуються для взаємодії між пристроями збору даних і пристроями перенесення даних або носіями даних, включають радіочастотне, інфрачервоне, оптичне та гальванічне збудження.

● Радіочастотні: Радіочастотні ідентифікаційні (RFID) мітки або радіопозначки використовуються для автоматичної ідентифікації та збору даних.

● Оптичні: Штрих-коди і QR-коди є прикладами ідентифікаційних носіїв даних, які зчитуються оптично.

● Інфрачервоні: Інфрачервоні мітки можуть використовуватися в збройних силах, лікарнях та інших середовищах, де необхідно відстежувати розташування і переміщення персоналу. Це можуть бути нашивки на військовій формі, що відбивають світло, або мітки, що працюють від батарейок і випромінюють ідентифікуючу інформацію.

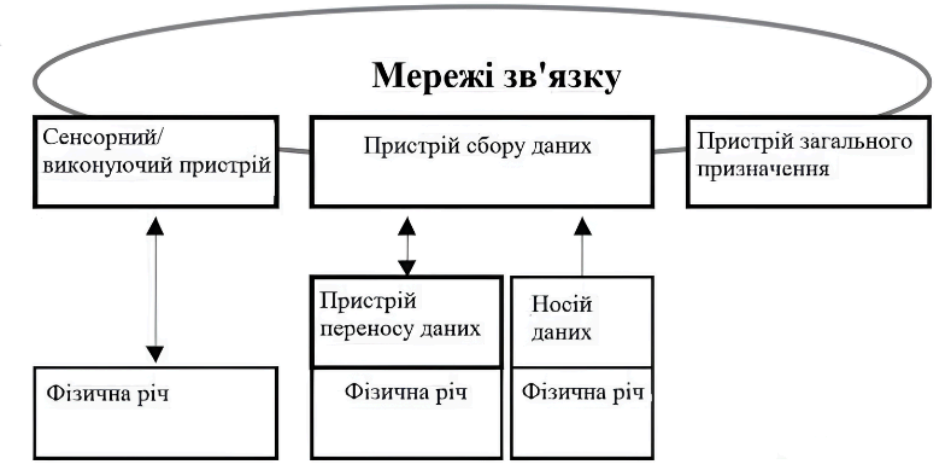

Рисунок 2.2 — Принцип взаємодії пристроїв

«Розумні» пристрої підтримують широкий спектр бездротових і дротових технологій передачі даних і мережевих протоколів. Крім того, можливості обробки даних у таких пристроїв, як правило, обмежені.

Рекомендація Y.2067 [6] закріплює вимоги до шлюзів IoT, які діляться на три категорії:

1) Шлюз підтримує різні технології доступу до пристроїв, дозволяючи пристроїв обмінюватися даними один з одним і з мережею Інтернет або корпоративною мережею, що містить додатки IoT. Такі схеми доступу включають Bluetooth і Wi-Fi.

2) Шлюз підтримує необхідні мережеві технології як для локальних, так і для глобальних мереж. Ці технології можуть включати в себе Ethernet і Wi-Fi на території організації, а також стільниковий зв'язок, Ethernet, DSL і кабельний доступ до Інтернету глобальним корпоративним мережам.

3) Шлюз підтримує взаємодію з додатками, управління мережею і функції безпеки, забезпечуючи ефективну комунікацію між IoT-пристроями, локальними мережами та хмарними сервісами, а також виконуючи роль посередника для обробки, фільтрації та передачі даних, шифрування та автентифікації для захисту інформації.

Рисунок 2.3 — Рівні передачі даних IoT

Еталонна модель Інтернету речей (IoT) від Міжнародного союзу електрозв'язку (МСЕ-Т) являє собою чотирирівневу структуру, доповнену горизонтальними функціями управління та безпеки. На рівні пристрою реалізуються фізичні та канальні функції відповідно до моделі OSI. Рівень мережі забезпечує дві ключові функціональні групи: взаємодію пристроїв та шлюзів, а також транспорт інформації служб і додатків IoT, включаючи дані управління та контролю, що відповідає мережевому та транспортному рівням OSI.

Рівень підтримки послуг і додатків надає загальні та спеціалізовані можливості, що використовуються додатками IoT. Загальні можливості, такі як обробка даних та управління базами даних, можуть бути використані різними додатками, тоді як спеціалізовані можливості розроблені для задоволення потреб конкретних підмножин додатків. Рівень додатку включає всі додатки, що взаємодіють з IoT-пристроями.

Наскрізні функції управління охоплюють традиційні аспекти управління мережею, такі як обробка несправностей, конфігурація, облік, моніторинг продуктивності та безпека. Функції безпеки забезпечують загальні механізми захисту, незалежні від конкретних додатків. В рекомендації приклади загальних можливостей забезпечення безпеки включають:

- На рівні програми: авторизацію, автентифікацію, захист конфіденційності і цілісності даних програми, захист недоторканності приватного життя, аудит безпеки і антивірусний захист;
- На рівні мережі: авторизацію, автентифікацію, конфіденційність даних про використання та даних сигналізації, а також захист цілісності даних сигналізації;
- На рівні пристрою: автентифікацію, авторизацію, перевірку цілісності пристрою, управління доступом, захист конфіденційності і цілісності даних.

Комітет з архітектури Всесвітнього форуму з Інтернету речей (IoT), до складу якого входять лідери індустрії, включаючи IBM, Intel та Cisco, опублікував еталонну модель IoT у жовтні 2014 року. Ця модель є загальною структурою, розробленою для прискорення розгортання IoT рішень. Вона покликана стимулювати співпрацю та сприяти створенню повторюваних моделей впровадження. Еталонна модель є важливим доповненням до моделі MCE-T. Документи MCE-T зосереджуються на рівнях пристрою та шлюзу, описуючи верхні рівні лише загалом. У рекомендації Y.2060 опис рівня додатків вміщується лише в одну фразу. Основна увага рекомендацій серії Y.206x приділяється визначенню концепції для підтримки розробки стандартів взаємодії з пристроями IoT. Всесвітній форум з Інтернету речей (IWF) стурбований більш масштабними питаннями розробки додатків, проміжного програмного забезпечення та функцій підтримки для корпоративного Інтернету речей. Запропонована семирівнева модель зображена на рисунку 2.4.

Рисунок 2.4 — Еталонна модель від Всесвітнього форуму IoT

1. Рівень фізичних пристроїв та контролерів включає фізичні пристрої, сенсори, та контролери, які збирають і генерують дані. Серед інших можливостей ці пристрої можуть вміти здійснювати аналого-цифрове і

цифро-аналогове перетворення, генерацію даних, а також підтримувати дистанційний опитування і / або дистанційне керування.

2. На рівні підключення забезпечується передача даних від пристроїв до інших компонентів системи IoT. Він включає в себе різноманітні мережеві протоколи і технології підключення, такі як Wi-Fi, Bluetooth, Zigbee, 4G/5G та інші.

3. Рівень периферійних обчислень (Edge Computing обробляє дані безпосередньо на пристроях або на близько розташованих серверах (на "краю" мережі) перед передачею даних до хмарних або центральних обчислювальних ресурсів. Це дозволяє зменшити затримки та знизити навантаження на мережу.

4. На рівні накопичення даних (Data Accumulation) дані, зібрані з пристроїв, агрегуються і зберігаються для подальшої обробки і аналізу. Дані, що надійшли з різних пристроїв, профільтровані і оброблені рівнем периферійних обчислень, поміщаються в сховище, де будуть доступні для більш високих рівнів. Рівень забезпечує зберігання та управління великими обсягами даних.

5. Рівень абстракції (Data Abstraction) відповідає за організацію, перетворення та узагальнення даних, що дозволяє зробити їх доступними для аналізу та використання додатками. Він включає механізми управління даними, які забезпечують інтеграцію та стандартизацію даних. Також цей рівень відповідає за захист даних шляхом відповідної автентифікації і авторизації і комбінування даних з різних джерел.

6. На рівні додатків знаходяться різноманітні додатки, які використовують оброблені дані для надання користувачам корисної інформації та функціональності. Це можуть бути мобільні додатки, веб-додатки або програмне забезпечення для управління IoT пристроями. Як правило, додатки взаємодіють з рівнем 5 і з даними в спокої, тому їм не обов'язково функціонувати на швидкостях мережі.

7. Рівень взаємодій і процесів відповідає за інтеграцію IoT додатків з бізнес-процесами і забезпечення співпраці між різними системами та користувачами. Він дозволяє створювати нові бізнес-моделі і процеси на основі даних IoT.

Всесвітній форум з Інтернету речей (IWF) вважає еталонну модель IoT базовою структурою, яка спрямована на стандартизацію концепцій та термінології, пов'язаних з IoT. Найважливіше те, що ця модель визначає необхідний функціонал та питання, які потрібно вирішити для повної реалізації потенціалу IoT у галузі. Модель корисна як для постачальників, що розробляють функціональні компоненти всередині цієї структури, так і для замовників, оскільки допомагає їм формулювати свої вимоги та оцінювати пропозиції постачальників.

2.3 Особливості захисту безпеки архітектурних рівнів

Компанія Cisco Systems, яка відіграла ключову роль у розробці еталонної моделі Всесвітнього форуму IoT, створила фреймворк безпеки IoT, що став важливим доповненням до цієї моделі. На рисунку 2.5 представлено середовище безпеки, яке пов'язане з логічною структурою IoT.

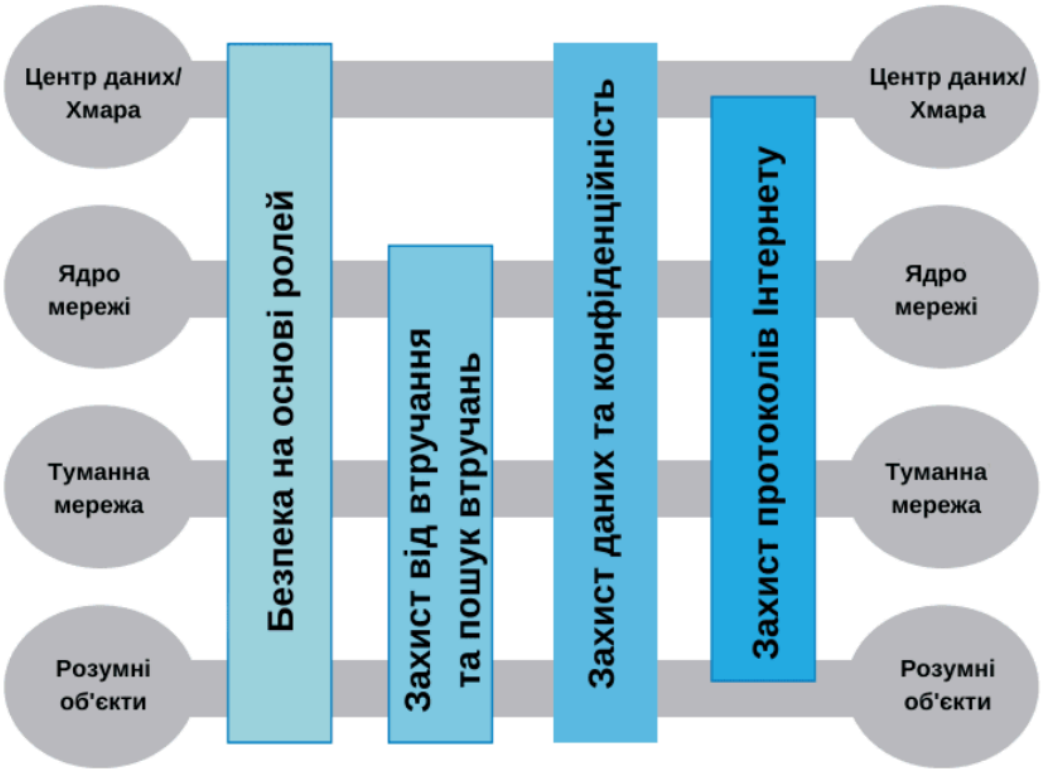

Рисунок 2.5 — Середовище безпеки IoT

На рисунку 2.5 показано конкретні функціональні області безпеки, які охоплюють чотири рівні моделі IoT. У документі Cisco пропонується концепція безпеки IoT, що визначає компоненти функцій безпеки для IoT, які охоплюють всі рівні моделі, як зображено на рисунку 2.6. Основні компоненти безпеки включають:

1. Аутентифікація: цей компонент охоплює елементи, які ініціюють доступ, ідентифікуючи IoT пристрої. На відміну від звичайних корпоративних мережевих пристроїв, де аутентифікація може здійснюватися за допомогою даних людини (наприклад, ім'я/пароль або бейдж), кінцеві IoT пристрої повинні використовувати методи аутентифікації, що не вимагають людського втручання. До таких методів належать радіочастотні мітки, сертифікати x.509 або MAC-адреси.

2. Авторизація: управляє доступом до пристроїв через мережеву структуру, включаючи контроль доступу. Працюючи разом з аутентифікацією, цей компонент забезпечує необхідні параметри для обміну інформацією між

пристроями та між пристроями і прикладними платформами, підтримуючи роботу IoT служб.

3. Мережева політика охоплює всі елементи, що здійснюють маршрутизацію та транспортування трафіку з кінцевих пристроїв через інфраструктуру, включаючи контрольний, управлінський та даний трафік.

4. Аналітика безпеки, включаючи видимість і контроль: включає функції для централізованого управління IoT пристроями, зокрема видимість пристроїв, що дозволяє центральним функціям управління бути в курсі про парк розподілених пристроїв, їх ідентичність і атрибути. На основі такої видимості виникає здатність здійснювати контроль, включаючи конфігурацію, патчі, оновлення та контрзаходи для припинення загроз.

Важливим елементом цієї концепції є довірчі відносини. Вони означають здатність двох учасників обміну бути впевненими в ідентичності та правах доступу один одного. Аутентифікаційний компонент забезпечує базовий рівень довіри, який доповнюється авторизаційним компонентом.

У документі Cisco наведено приклад, де автомобіль встановлює довірчі відносини з іншою машиною того ж виробника. Ці довірчі відносини дозволяють обмінюватися лише відомостями про безпеку. Однак, при встановленні довірчих відносин між автомобілем і дилерською мережею, машина може передавати і отримувати додаткову інформацію, таку як показання одометра та результати останнього техобслуговування. Таким чином, розширення довірчих відносин на інші системи підвищує ефективність і зручність обслуговування.

Рисунок 2.6 — Безпечний фреймворк IoT

1. Захист безпеки IoT на рівні фізичних пристроїв та контролерів

Рівень фізичних пристроїв та контролерів є фундаментом Інтернету речей (IoT), оскільки він об'єднує сенсори, виконавчі механізми, мікроконтролери та інші пристрої, що безпосередньо взаємодіють з оточенням. Ці пристрої збирають дані про температуру, вологість, рух, освітлення, а також виконують дії, такі як відкриття/закриття дверей чи вмикання/вимикання світла.

Однак, цей рівень є вразливим до різних загроз. Зловмисники можуть отримати фізичний доступ до пристроїв, щоб змінити їх прошивку, викрасти дані або вивести їх з ладу. Також можлива підробка даних, що передаються сенсорами, для викликання неправильної реакції системи. Атаки типу "відмова в обслуговуванні" можуть зробити пристрої недоступними або перевантажити їх роботу, а незахищені інтерфейси, такі як JTAG або UART, можуть бути використані для несанкціонованого доступу.

Для забезпечення безпеки на цьому рівні застосовуються різні заходи. Аутентифікація та ідентифікація пристроїв здійснюється за допомогою апаратних ідентифікаторів (TPM, чипи безпеки), цифрових сертифікатів X.509 та протоколів аутентифікації (EAP-TLS, IEEE 802.1X). Шифрування

даних, що передаються, забезпечується легковаговими алгоритмами (AES-128, ChaCha20), а також надійним зберіганням та управлінням криптографічними ключами. Захист каналу зв'язку здійснюється за допомогою протоколів TLS або DTLS.

Фізична безпека пристроїв забезпечується використанням антивандальних корпусів, датчиків втручання та розміщенням пристроїв у безпечних місцях. Безпечне оновлення прошивки включає перевірку цифрового підпису оновлення, використання захищеного каналу для передачі та можливість відкату до попередньої версії у разі проблем.

2. Захист безпеки рівня підключення

Рівень підключення слугує критично важливим інтерфейсом між окремими пристроями та розгалуженою мережевою інфраструктурою. Оскільки це перша лінія оборони від зовнішніх загроз, надійна безпека на цьому рівні є запорукою цілісності всієї цифрової екосистеми. Ключовими стратегіями забезпечення безпеки є використання безпечних комунікаційних протоколів, захист бездротових мереж, мережевий моніторинг та виявлення/попередження вторгнень, сегментація мережі, контроль доступу до мережі та захист кінцевих точок.

Безпечні комунікаційні протоколи, такі як TLS, DTLS, SSH та IPsec, шифрують дані та аутентифікують пакети, захищаючи їх від несанкціонованого доступу та підробки. Захист бездротових мереж включає використання WPA3, приховування SSID та фільтрацію MAC-адрес, що ускладнює виявлення та підключення до мережі неавторизованих пристроїв. Мережевий моніторинг та системи виявлення/попередження вторгнень (IDS/IPS) постійно аналізують трафік, виявляючи та блокуючи підозрілу активність.

Сегментація мережі обмежує поширення загроз, ізолюючи уражені сегменти. Контроль доступу до мережі (NAC) перевіряє відповідність пристроїв політикам безпеки перед наданням доступу. Захист кінцевих точок

включає використання антивірусного та антишпигунського програмного забезпечення, персональних файрволів та регулярне оновлення програмного забезпечення для виправлення вразливостей.

3. Захист безпеки на рівні периферійних обчислень

Рівень периферійних обчислень, що включає вузли обробки даних ближче до місця їх збору, дозволяє зменшити навантаження на централізовані сервери та затримку передачі даних. Однак, для захисту цих вузлів від кібератак необхідні комплексні заходи безпеки. Сегментація мережі за допомогою VLAN або брандмауерів ізолює різні частини системи, обмежуючи вплив атак. Строгий контроль доступу на основі RBAC або ACL запобігає несанкціонованому доступу до даних. Встановлення антивірусного програмного забезпечення та систем виявлення вторгнень допомагає виявляти та блокувати зловмисне ПЗ. Шифрування даних за допомогою SSL/TLS забезпечує конфіденційність та цілісність даних, що передаються. Фізичний захист вузлів від несанкціонованого доступу та пошкоджень також є важливим. Регулярний моніторинг активності та аудит журналів подій допомагають виявляти підозрілу активність. Своєчасне оновлення програмного забезпечення та прошивки закриває відомі вразливості. Загартовування пристроїв шляхом відключення непотрібних служб та портів, налаштування брандмауера та використання інших методів зменшує потенційну "поверхню атаки" периферійних вузлів.

4. Захист безпеки на рівні накопичення даних

Рівень накопичення даних, де зберігаються великі обсяги інформації, зібраної пристроями Інтернету речей (IoT), вимагає особливої уваги до безпеки. Застосування надійних алгоритмів шифрування, таких як AES-256, для зберігання даних у стані спокою гарантує їх конфіденційність та цілісність, навіть якщо зловмисник отримає доступ до сховища. Регулярне створення резервних копій даних та їх зберігання в окремому, захищеному місці дозволяє відновити інформацію у випадку її втрати або пошкодження.

Контроль доступу до даних за допомогою ролей та політик доступу, таких як RBAC, обмежує коло осіб, які мають право доступу, та операції, які вони можуть виконувати. Сегментація сховищ залежно від типу та чутливості даних дозволяє застосовувати різні політики безпеки та обмежувати потенційний вплив атаки. Ведення журналів доступу до даних та їх регулярний аналіз допомагають виявляти підозрілу активність та потенційні загрози. Встановлення та регулярне оновлення антивірусного програмного забезпечення на серверах та інших пристроях захищає від шкідливих програм. Якщо дані зберігаються на локальних серверах, важливо забезпечити їх фізичний захист. Використання хмарних сервісів може надати додаткові можливості для захисту даних, такі як географічне розподілення, автоматичне резервне копіювання та вбудовані засоби безпеки.

5. Захист безпеки рівня абстракції

Рівень абстракції, що забезпечує доступ до даних і ресурсів IoT-системи через інтерфейси прикладного програмування (API) та сервіси, також вимагає особливої уваги до безпеки. Для захисту API необхідно використовувати надійні механізми аутентифікації та авторизації, такі як OAuth 2.0 та JWT, щоб підтвердити особу користувачів та визначити їх права доступу. Застосування політик контролю доступу на основі ролей (RBAC) або списків контролю доступу (ACL) обмежує доступ до API лише авторизованим користувачам та додаткам. Шифрування даних за допомогою протоколів, таких як HTTPS, захищає дані від несанкціонованого перехоплення та модифікації. Ретельна перевірка всіх вхідних даних запобігає атакам типу "введення SQL-коду" та іншим вразливостям. Ведення детальних журналів усіх запитів до API та постійний моніторинг активності дозволяють відстежувати дії користувачів та виявляти підозрілі дії. Для захисту від DoS-атак необхідно встановити обмеження на кількість запитів, використовувати кешування відповідей та розподіляти навантаження між кількома серверами.

6. Захист безпеки рівня додатків

Рівень додатків відіграє центральну роль в екосистемі Інтернету речей (IoT), забезпечуючи взаємодію користувачів з різноманітними розумними пристроями та надаючи послуги на основі отриманих даних. Ці додатки можуть бути мобільними, веб- або десктопними, і вони дозволяють користувачам моніторити, налаштовувати та керувати IoT-пристроями, такими як датчики, камери, термостати, побутова техніка та інші.

Для забезпечення ефективного та безпечного управління IoT-пристроями використовуються різні способи взаємодії. Мобільні додатки є найпоширенішим способом, забезпечуючи зручність та доступність з будь-якого місця. Веб-інтерфейси дозволяють керувати пристроями через браузер, що зручно для складніших налаштувань та детального моніторингу. Голосові помічники, такі як Google Assistant або Apple Siri, спрощують взаємодію з IoT-пристроями за допомогою голосових команд. Інтерфейси прикладного програмування (API) надають розробникам можливість створювати власні додатки та сервіси для керування IoT, а використання сценаріїв та правил автоматизації дозволяє пристроям взаємодіяти між собою та виконувати дії без втручання користувача.

Однак, з розширенням можливостей керування зростають і потенційні ризики безпеки. Тому захист додатків та способів керування IoT-пристроями є невід'ємною частиною забезпечення безпеки всієї системи. Застосування методологій безпечної розробки програмного забезпечення (SDL), регулярне тестування на проникнення та своєчасне оновлення програмного забезпечення допомагають виявити та усунути вразливості в додатках.

Для захисту облікових записів користувачів важливо використовувати багатофакторну аутентифікацію (MFA), надійні паролі та обмеження кількості спроб входу. Шифрування даних під час передачі та зберігання, контроль доступу на основі ролей та мінімізація обсягів даних є ключовими заходами для забезпечення конфіденційності.

Для запобігання несанкціонованому доступу та зловмисним діям необхідно застосовувати валідацію вхідних даних, захист від XSS (міжсайтовий скриптинг) та CSRF (підробка міжсайтових запитів), а також механізми захисту від DoS-атак (відмова в обслуговуванні).

Безпека оновлень також є важливим аспектом. Регулярне оновлення прошивки пристроїв та програмного забезпечення додатків дозволяє усунути відомі вразливості та захистити від нових загроз. Постійний моніторинг активності додатків та пристроїв, а також детальне логування подій дозволяють швидко виявляти та реагувати на підозрілу активність.

Комплексний підхід до безпеки на рівні додатків забезпечує надійний захист від кіберзагроз, гарантуючи конфіденційність, цілісність даних та безперебійну роботу всієї IoT-екосистеми.

Рисунок 2.7 — «Тріада» інформаційної безпеки

7. Рівень взаємодій і процесів

Рівень взаємодій і процесів охоплює бізнес-процеси та взаємодію між різними компонентами IoT-системи, включаючи пристрої, шлюзи, хмарні

сервіси, додатки та користувачів. Безпека на цьому рівні зосереджується на захисті від загроз, пов'язаних з бізнес-логікою, неправильною конфігурацією системи, людськими помилками та іншими факторами, що можуть вплинути на цілісність та доступність системи. Заходи безпеки на цьому рівні включають управління ризиками, яке передбачає систематичний аналіз потенційних загроз та вразливостей IoT-системи, оцінку їх ймовірності та потенційного впливу, а також впровадження відповідних заходів безпеки для зниження ризиків до прийнятного рівня з постійним моніторингом та переглядом ефективності вжитих заходів. Важливим аспектом є розробка та впровадження чітких політик безпеки, які охоплюють усі аспекти IoT-системи, включаючи правила доступу, використання пристроїв, обробку даних, реагування на інциденти та інші важливі аспекти. Необхідно забезпечити, щоб усі співробітники та користувачі системи були ознайомлені з цими політиками та дотримувалися їх, а також регулярно переглядати та оновлювати політики з урахуванням змін у системі, нових загроз та вимог законодавства. Аудит та відповідність є невід'ємною частиною забезпечення безпеки, тому необхідно проводити регулярні аудити безпеки для оцінки ефективності вжитих заходів, виявлення потенційних вразливостей та перевірки відповідності системи вимогам безпеки і законодавства, а також своєчасно усувати виявлені недоліки і вразливості, готувати звіти про результати аудиту та вжиті заходи для керівництва або інших зацікавлених сторін.

2.4 Сучасні проблеми безпеки та захист автоматизованих систем IoT від інформаційних загроз

Коли ми розмірковуємо про середовище Інтернету речей, захист від зовнішніх загроз і вразливостей повинен розглядатися так само важливим, як і в звичайному ІКТ-середовищі. Причиною цього є величезна кількість

пристроїв і середовищ Інтернету речей, які можуть бути використані для створення бот-мереж або для будь-якої іншої ворожої діяльності .

Конфіденційність та безпека даних є ключовими питаннями на сьогоднішній день при розгляді пристроїв Інтернету речей на організаційному рівні або у приватному користуванні. Масштабна крадіжка інформації про особисту ідентичність або її конфіденційних даних з установи чи організації –це завжди є значним ризиком. Для забезпечення належного рівня захисту екосистем IoT, бізнес-організації повинні проводити аналіз ризиків. Однією з частин аналізу ризиків є впровадження відповідних запобіжних заходів. Крім того, необхідно визначити політику управління безпекою та впровадити її у внутрішні процеси.

У той час як IoT все більше і більше входить в повсякденне життя, ризики безпеки, пов'язані з IoT, зростають і швидко змінюються. У сучасному світі «завжди увімкнених» технологій і недостатньої обізнаності користувачів у питаннях безпеки користувачів, кібератаки – це вже не питання «якщо», а «коли». Кіберзлочинці працюють над новими методами, щоб проникнути крізь систему безпеки авторитетних організацій, отримуючи доступ до всього – від IP-адреси до індивідуальної інформації про клієнтів. Вони роблять це для того, щоб завдати шкоди, порушити конфіденційність даних і викрасти інтелектуальну власність. З кожним днем атаки зловмисників стають все більш витонченими, а захист чи усунення наслідків від атак все важче. Через цей постійний розвиток не можливо точно сказати, які загрози з'являться наступного року, через п'ять років або через 10 років. Можна лише сказати, що ці загрози будуть ще більш небезпечними, ніж ті, що існують сьогодні (див. рис. 2.8) [7].

Рисунок 2.7 — Ландшафт ризиків ІБ систем IoT

Забезпечити ефективну кібербезпеку стає дедалі складніше. Традиційний організаційний периметр розмивається, а існуючі засоби захисту зазнають все більшого тиску. Точкові рішення, зокрема антивірусне програмне забезпечення, IDS, IPS, виправлення та шифрування, залишаються ключовим засобом боротьби з відомими на сьогоднішній день атаками; однак з часом вони стають менш ефективними, оскільки зловмисники знаходять нові способи обходу контролю. Як і всі атаки, інциденти, пов'язані з Інтернетом речей, непередбачувані і потенційно можуть завдати величезної шкоди.

Наприклад, під час DDoS-атаки ботнету Mirai користувачі не змінили стандартні паролі сотень тисяч старих веб-камер, відеореєстраторів і роутерів. Озброївшись шкідливим кодом, хакери націлилися на застарілі версії ядра Linux на пристроях, а потім Dyn з використанням ботнету пристроїв Інтернету речей наводнили трафіком сервери компанії Dyn, Inc. –одного з найбільших DNS-провайдерів. Системи перевантажилися і вийшли з ладу, що призвело до падіння численних веб-сайтів, включаючи Etsy,

GitHub, Netflix, Shopify, SoundCloud, Spotify, Twitter і навіть сайт відомого експерта з питань безпеки Брайана Кребса. Після успішного зараження вразливого IoT-гаджета ботнет автоматично шукав в інтернеті інші вразливі пристрої. Щоразу, коли він знаходив такий пристрій, шкідливе програмне забезпечення використовувало стандартне ім'я та пароль для входу в систему, інсталяції та повторення процесу. Багато з цих пристроїв мали проблеми із застарілою прошивкою або слабкі паролі за замовчуванням, що робило їх постійно вразливими і легкими для злому. Цей злом відбувся в жовтні 2016 року і досі залишається найбільшою DDoS-атакою з усіх коли-небудь здійснених.

Пристрої Інтернету речей мають величезний потенціал в галузі медицини. Однак, ставки дуже високі, коли мова йде про кібербезпеку. Це яскраво проілюстрував інцидент у 2017 році, коли FDA оголосило, що виявило серйозну вразливість в імплантованих кардіостимуляторах, вироблених компанією St. Jude Medical. В даному випадку вразливість полягала в передавачі, який кардіостимулятори використовували для зв'язку із зовнішніми службами. Ці кардіостимулятори передавали інформацію про стан пацієнта його лікарям, що значно полегшувало моніторинг кожного пацієнта. Отримавши доступ до передавача кардіостимулятора, зловмисники могли змінювати його роботу, розряджати батарею і навіть завдавати потенційно смертельних ударів струмом.

Компанія TRENDnet рекламувала свої камери SecurView як ідеальні для широкого спектру використання. Вони могли слугувати не лише камерами домашньої безпеки, але й подвійними радіонянями. А головне, вони повинні були бути безпечними. Але, як виявилося, будь-хто, хто зміг знайти IP-адресу одного з цих пристроїв, міг легко переглянути його. У деяких випадках зловмисники також могли перехоплювати аудіо. Пізніше FTC оголосила, що протягом певного періоду часу TRENDnet передавав реєстраційні дані користувачів через Інтернет без будь-якого шифрування у

вигляді чистого тексту, який можна було прочитати. Цей інцидент демонструє, що не варто сприймати безпеку як належне. Якщо пристрій нібито захищений, це не означає, що він не витікає ваші особисті дані. Найкращий спосіб запобігти подібним випадкам - провести тест на проникнення або встановити VPN на домашньому роутері. Він зашифрує всі ваші інтернет-комунікації, тому жоден хакер не зможе їх прочитати.

Також знаковою була атака, вперше продемонстрована в липні 2015 року командою з IBM. Команді вдалося отримати доступ до бортового програмного забезпечення позашляховика Jeep і використати вразливість у механізмі оновлення прошивки. Дослідники отримали повний контроль над автомобілем і змогли прискорювати і сповільнювати його рух, а також повертати кермо і змушувати автомобіль з'їжджати з дороги. Оскільки все більше людей починають користуватися електромобілями і переходять на безпілотні технології, стає все більш важливо, щоб ці транспортні засоби були максимально безпечними.

Гучні прогалини в безпеці, подібні до згаданих вище, лише посилюють потенціал катастрофи, коли безпекою нехтують.

Проблема кібербезпеки, пов'язана із захистом IoT, є складною і масштабною через те, що пристрої IoT розгорнуті на широкій поверхні, що піддається атаці, і містять численні вектори загроз, такі як аутентифікація і авторизація, програмне забезпечення та авторизація, загрози для пристроїв, загрози для засобів керування, загрози хмарі, мережеві загрози та вразливості на рівні операційної системи. Проблема ускладнюється тим, що багато пристроїв Інтернету речей не є частиною запланованої процедури виправлення помилок або оновлення ПЗ.

Найслабшою ланкою в ланцюжку підключених до Інтернету речей є сам

пристрій. Наприклад, хакери можуть знайти вразливість пристрою і змінити його ідентифікатор, щоб отримати доступ до мережі. Заразивши один

пристрій і отримавши доступ до мережі, зловмисник може розпочати масштабний злом. Оскільки пристрої Інтернету речей можуть випускатися з уразливими місцями в системі безпеки і погано налаштованими або незашифрованими мережами Wi-Fi, пристрої схильні до атак типу «людина посередині». Сценарії включають зловмисників, які таємно передають і змінюють зв'язок між зловмисником і жертвою, коли жертва вважає, що вони безпосередньо спілкуються через приватне з'єднання. Насправді, вся комунікація може контролюватися і змінюватися зловмисником.

Деякі системи IoT страждають від синдрому ізоляції вбудованих пристроїв: іноді використовуються слабкі протоколи і практики, оскільки деякі технології IoT були розроблені для закритого, не підключеного до Інтернету використання з власницьким кодом і без ретельного тестування програмного забезпечення. Зручність використання та сумісність є важливими факторами для виробників IoT. Видається розумним уникати помилок минулого та підняти безпеку і конфіденційність до рівня основних принципів проектування. Існує відносно небагато стандартів або передових практик, якими можна керуватися при розробці та тестування технологій Інтернету речей. На рис. 2.8 представлено загальні принципи кібербезпеки IoT у всіх стеках .

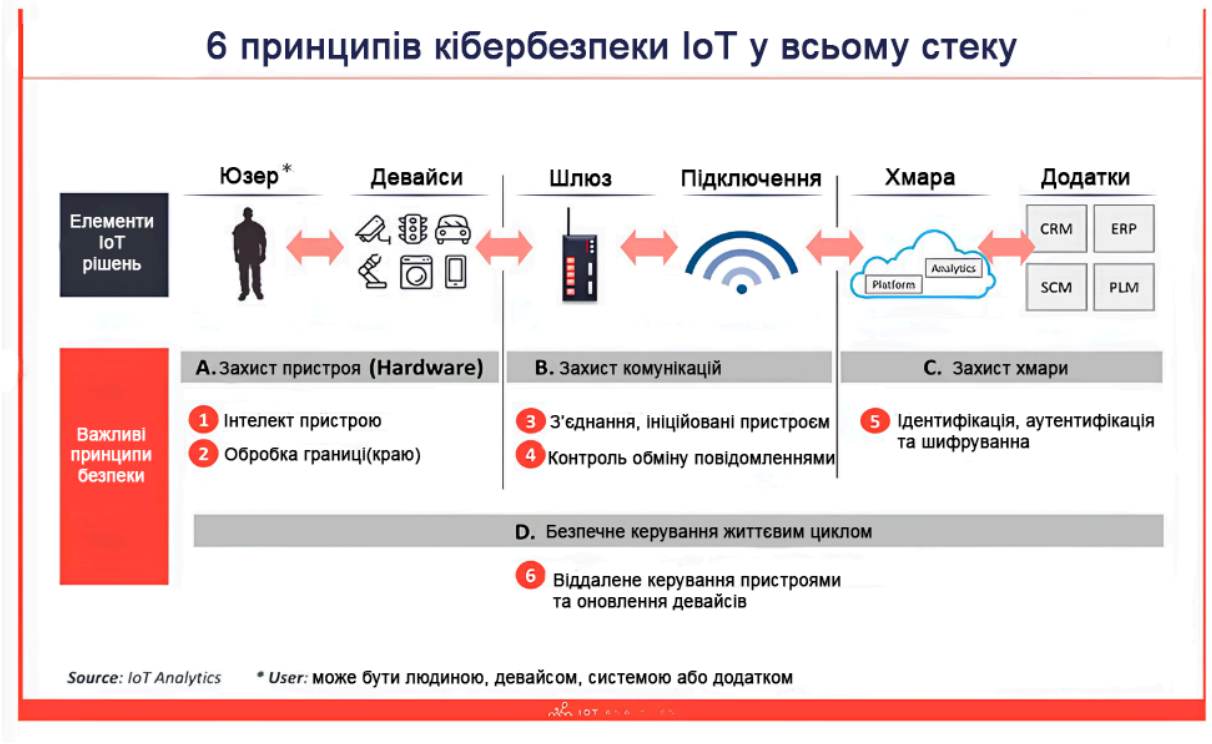

Рисунок 2.8 — Принципи кібербезпеки у всьому стеці IoT

Для порівняння, персональні комп’ютери вперше використовували антивірусне програмне забезпечення у 1980-х роках. Однак в контексті Інтернету речей (IoT) виникають суттєві проблеми з безпекою. Основна з них полягає в тому, що більшість пристроїв IoT були розроблені без належного врахування аспектів безпеки. Виробники часто зосереджуються на забезпеченні функціональності та зниженні витрат на виробництво, виходчи з цього, багато пристроїв IoT мають обмежені обчислювальні ресурси, пам'ять та енергоспоживання, а багато розробників не мають достатнього досвіду в галузі кібербезпеки IoT. Це значно ускладнює можливість встановлення будь-якого програмного забезпечення для забезпечення безпеки безпосередньо на самих пристроях IoT, що створює значні ризики для користувачів і систем, у яких ці пристрої використовуються. Щоб швидко захопити ринок пристроїв IoT, постачальники постачають дешеві рішення, які не підтримуються і розробник не випускає жодних виправлень програмного забезпечення чи оновлень безпеки. Відповідно до нещодавнього звіту Фонду безпеки Інтернету речей (IoTSF), чотири з п’яти постачальників

пристроїв виявились невдалими в базових практиках кібербезпеки. Проаналізувавши сотні популярних виробників продуктів IoT, організація виявила, що лише приблизно кожен п’ятий надає користувачам можливість повідомляти постачальникам про вразливі місця безпеки, щоб продукт можна було виправити. [9]

Незахищені мережі також відіграли ключову роль у тому, що системи були відкритими для загроз. Відповідно до звіту Unit 42 IoT Threat Report, 98% усього трафіку пристроїв IoT є незашифрованим . Це дозволило зловмисникам збирати особисту, а також конфіденційну інформацію та використовувати ці дані для отримання прибутку в темній мережі [10]. Загрози продовжують розвиватися, націлюючись на пристрої IoT, використовуючи нові складні та обхідні методи, такі як одноранговий командний і контрольний зв’язок і черв’якові функції для саморозповсюдження.

Також спостерігається перехід від основного втручання зловмисників до запуску ботнетів для проведення DDoS-атак через пристрої IoT до зловмисного програмного забезпечення, що поширюється мережею через функції, схожі на черв’яків, що дозволяє зловмисникам запускати шкідливий код для здійснення різноманітних нових атак.

Трьома провідними категоріями загроз безпеці Інтернету речей є експлойти, такі як віддалене виконання коду та ін’єкція команд, зловмисне програмне забезпечення, таке як ботнети та трояни, а також пов’язані з користувачем уразливості, такі як слабкі паролі та фішинг. Кожен пристрій IoT у мережі є потенційною точкою входу для хакерів. Термін «поверхня атаки» часто використовується для позначення загальної кількості точок входу для несанкціонованого доступу до системи, включаючи всі пристрої IoT, мережеві підключення та програмне забезпечення.

Хоча за останні роки пристрої IoT покращилися, їх потенційні вразливості більш-менш залишилися незмінними. Незважаючи на те, що

політики та учасники індустрії прагнуть закрити прогалини в безпеці нових пристроїв, застарілі системи залишаються такими ж вразливими, як і раніше. Приблизно 57% усіх пристроїв Інтернету речей уразливі до атак середнього або високого ступеня тяжкості, що робить їх легкою мішенню для зловмисників. Зламавши перший пристрій, зловмисник часто використовує його як спосіб зламати інші системи в мережі.

Експлойти є однією з найпоширеніших загроз для пристроїв IoT. Зазвичай вони являють собою частину коду, написану для пошкодження або викрадення даних із системи. Як показано на рис. 2.9, 41% атак є використанням уразливостей пристроїв IoT, причому найбільший компонент цієї категорії походить від сканування пристроїв, підключених до мережі.

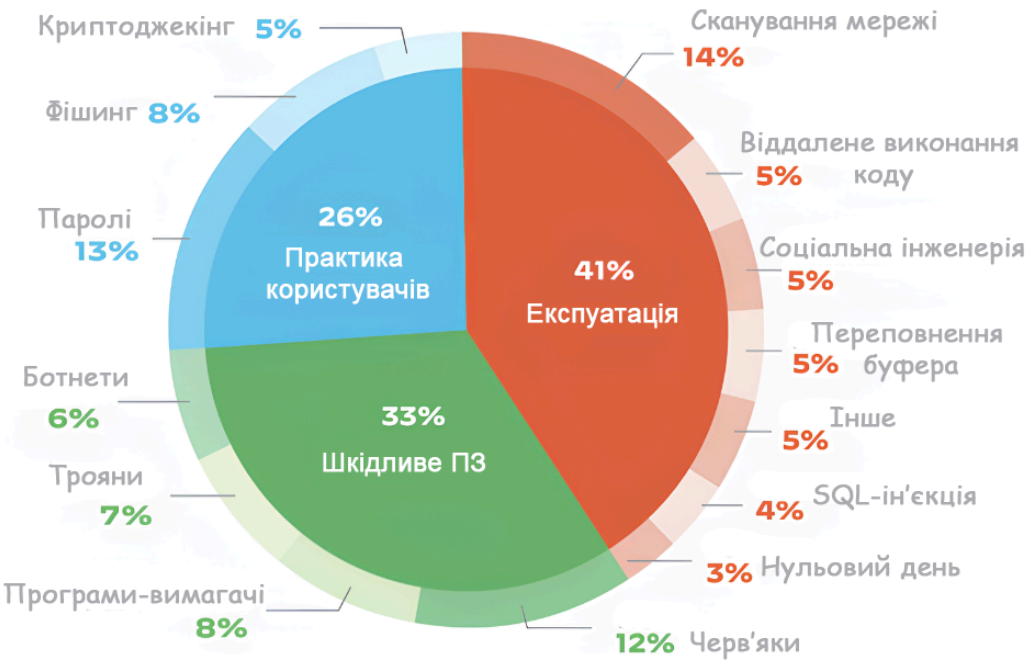

Рисунок 2.9 — Поширення кіберзагроз на пристрої IoT

- Сканування мережі (14%)**:** процес пошуку вразливих IoT-пристроїв у мережі, який може бути використаний зловмисниками для подальших атак.

- Паролі (13%)**:** використання слабких або вгаданих паролів є поширеною проблемою, яка може дозволити зловмисникам легко отримати доступ до IoT-пристроїв.

- Черв'яки (12%)**:** тип шкідливого ПЗ, який може самостійно поширюватися через мережу, заражаючи велику кількість пристроїв.
- Фішинг (8%)**:** спроби обманом змусити користувачів розкрити конфіденційну інформацію, таку як паролі або дані кредитних карт, зазвичай через підроблені електронні листи або веб-сайти.
- Програми-вимагачі (8%)**:** тип шкідливого ПЗ, який блокує доступ до пристрою або даних і вимагає викуп за відновлення доступу.
- Трояни (7%)**:** тип шкідливого ПЗ, який маскується під легітимне програмне забезпечення, але виконує шкідливі дії.
- Ботнети (6%)**:** мережі заражених пристроїв, які можуть бути використані для проведення DDoS-атак, розсилки спаму або інших шкідливих дій.
- Соціальна інженерія (5%)**:** маніпуляція людьми з метою отримання конфіденційної інформації або доступу до систем.
- Віддалене виконання коду (5%)**:** вразливість, яка дозволяє зловмисникам виконувати довільний код на віддаленому пристрої.
- Переповнення буфера (5%)**:** вразливість, яка виникає, коли програма записує дані за межі виділеного буфера пам'яті.
- SQL-ін'єкція (4%)**:** тип атаки, при якій зловмисник вставляє шкідливий SQL-код у запит до бази даних.
- Нульовий день (3%)**:** вразливість, про яку не знають розробники програмного забезпечення або постачальники пристроїв, і для якої немає виправлення.
- Криптоджекінг (5%)**:** несанкціоноване використання обчислювальних ресурсів пристрою для майнінгу криптовалюти.

Безпека Інтернету речей розроблена для подолання вразливостей пристроїв IoT за допомогою таких методів, як відокремлені мережі, контроль доступу та моніторинг поведінки. Ці методи захищають від різних ризиків безпеці, включаючи, найчастіше, крадіжку інформації та зловмисне

програмне забезпечення. Але незважаючи на те, що останнім часом число атак IoT подвоїлося, витрати на безпеку ще не встигають за зростанням уразливостей. Раніше Gartner підрахував, що понад 25% виявлених корпоративних атак стосуватимуться IoT, але на IoT припадатиме лише 10% бюджетів IT-безпеки. Глобальні витрати на безпеку IoT досягли лише 6 мільярдів доларів у 2023 році.

Проблема безпеки Інтернету речей пов'язана не лише з великою кількістю пристроїв, які необхідно захистити. Існує також фундаментальна проблема безпеки, яка випливає з того, як виготовляються пристрої IoT. Велика кількість продуктів Інтернету речей – це просто повсякденний пристрій із встановленим комп'ютерним чіпом, тому захистити їх так само, як за допомогою персонального комп'ютера, практично неможливо.

Лідери безпеки в організаціях виходять за межі застарілих мережевих рішень і впроваджують підходи, які усувають недоліки безпеки на кожному етапі життєвого циклу IoT. Ключові моменти та процеси, які використовуються для захисту пристроїв Інтернету речей, включають:

● Видимість. Першим кроком у забезпеченні безпеки IoT є визначення точної кількості пристроїв IoT у мережі. Ведення детальної актуальної інвентаризації всіх підключених пристроїв дозволяє визначити профіль ризику кожного пристрою та його поведінку з рештою мережі.

● Сегментація мережі. Чим більше сегментована ваша мережа на локальні підмережі, тим меншою буде ваша поверхня для атаки. Розділивши вашу мережу на дві або більше частин, хакерам буде важче загрожувати всій вашій мережі, скомпрометувавши лише один пристрій.

● Аутентифікація. Більшість пристроїв IoT постачаються зі слабкими попередньо встановленими паролями, які можна легко знайти в Інтернеті. Перше, що слід зробити, коли ви підключаєте пристрій IoT до мережі, це змінити пароль на більш складний.

● Оновлення мікропрограми. На відміну від IT-систем, більшість пристроїв Інтернету речей (IoT) не розроблені з можливістю виправляти недоліки безпеки за допомогою регулярних оновлень. Таким чином, важливо співпрацювати з постачальником пристрою IoT, щоб розробити стратегію оновлення мікропрограми та усунути вразливі місця безпеки, перш ніж виникнуть проблеми.

● Постійний моніторинг. Впровадивши рішення для моніторингу в реальному часі, яке постійно аналізує поведінку всіх пристроїв Інтернету речей (IoT), з'являється можливість швидко реагувати на загрози безпеці.

Зростання кількості постачальників, які пропонують рішення безпеки IoT, свідчить про зміни в галузі – організації нарешті серйозно ставляться до безпеки IoT . З цією метою у сертифікованому звіті про безпеку PSA за 2023 рік зазначено, що 9 із 10 опитаних організацій поставили безпеку в трійку головних бізнес-пріоритетів, тоді як 83% респондентів шукають конкретні облікові дані безпеки, купуючи продукти IoT. Сьогодні рішення безпеки IoT включають такі можливості, як шифрування, брандмауери, виявлення та реагування кінцевих точок (EDR), керування ідентифікацією та доступом (IAM), а також інструменти сегментації мережі.

До постачальників рішень безпеки Інтернету речей відносяться:

Microsoft Defender для IoT пропонує уніфікований захист і захист від загроз для всіх пристроїв Інтернету речей (IoT), операційних технологій (OT) і систем промислового керування (ICS) із мережевим виявленням і реагуванням без агентів (NDR).

Palo Alto Networks використовує підхід повного життєвого циклу до захисту пристроїв IoT. Їх структура безпеки IoT включає виявлення кінцевих точок і реагування (EDR), доступ до мережі з нульовою довірою (ZTNA), управління вразливістю, управління активами та контроль доступу до мережі (NAC).

Fortinet займається безпекою Інтернету речей за допомогою служби FortiGuard IoT Service, яка поєднує в собі брандмауер і службу контролю доступу до мережі в рішення програмного забезпечення як послуги (SaaS), відомого як FortiNAC.

РОЗДІЛ 3. РОЗРОБКА ВЕБ-ДОДАТКУ ДЛЯ РЕАЛІЗАЦІЇ ЗАХИЩЕНОЇ СИСТЕМИ РОЗУМНОГО БУДИНКУ

3.1. Елементи та принципи функціонування розумного будинку

Інтернет речей являє собою складну систему взаємопов'язаних датчиків та виконавчих пристроїв, вбудованих у фізичні об'єкти, що забезпечує передачу даних через дротові та бездротові мережі. Активний розвиток IoT охоплює широкий спектр сфер, включаючи інтелектуальні мережі, логістику, моніторинг навколишнього середовища та безпеки, транспорт, промисловість, фінанси, оборону, охорону здоров'я, сільське господарство та розумні будинки.

Розумні будинки, як підмножина IoT, характеризуються наявністю комунікаційної мережі, що об'єднує ключові датчики та виконавчі механізми, забезпечуючи дистанційний доступ, моніторинг та управління. Відмінними рисами розумних будинків є обмежений розмір мережі, невелика кількість користувачів (члени сім'ї), використання різних типів мережевого підключення (3G, 4G, Wi-Fi), локальне управління даними, застосування бездротових технологій (RFID, WSN) та помірні вимоги до пропускної здатності.

Розумний дім, також відомий як сукупність технологій автоматизації пристроїв в будинку, спрямований на підвищення комфорту, зручності, безпеки, автономності та економічності житла. Завдяки численним перевагам, домашня автоматизація набуває все більшої популярності. Зростаюча різноманітність інтелектуальних датчиків, програмних рішень, підключених пристроїв та хмарних сервісів створюється з метою забезпечення можливості працювати в різних формах та форматах у наших житлових та робочих середовищах. Це охоплює квартири, офісні будівлі, виробничі приміщення та інші місця, спрямовані на дії, які повинні бути вкрай потужними та

оснащеними передовими технологіями. Навіть звичайні об'єкти стають цифровими, взаємопов'язаними між собою на місцевому рівні. Це дозволяє систематично наділяти наші оточення відповідними та правильними інтелектуальними можливостями шляхом додавання функціональних модулів всередині та інтеграції з віддаленим програмним забезпеченням.

Система домашньої автоматизації складається з чотирьох основних компонентів. Перший – це інтерфейс користувача, наприклад, комп'ютер або телефон, за допомогою якого віддаються команди системі керування. Другий компонент – це режим передачі даних, який може бути Ethernet (дротовий), Bluetooth та Wi-Fi (бездротовий). Третій – центральний контролер, який є апаратним інтерфейсом, що зв'язується з користувацьким інтерфейсом, керуючи електронними пристроями. Останній компонент – це різні електронні пристрої, такі як кондиціонер, лампа або обігрівач, які сумісні з режимом передачі і підключені до центральної системи управління. Принцип роботи розумного будинку полягає в автоматизації всіх аспектів житлової споруди, включаючи освітлення, кондиціонування, систему безпеки, електроенергію, опалення, водопостачання та водовідведення та інші системи.

Таким чином, «розумний будинок» складається з програмного і апаратного забезпечення, датчиків і проводової / безпроводової мережі. У загальному випадку, «розумний будинок» надає його власнику такі переваги:

1) зниження споживання ресурсів (газ, вода, електроенергія);

2) високий рівень комфорту;

3) забезпечення необхідної взаємодії всіх систем об'єкта нерухомості, що автоматизуються, задання різних режимів роботи;

4) підвищення оперативності, простоти і зручності управління;

5) зниження ймовірності виникнення аварійних ситуацій.

Розумні датчики – це невеликі, але потужні пристрої, які відіграють ключову роль у створенні сучасного розумного будинку. Вони здатні збирати

різноманітну інформацію про навколишнє середовище та передавати її на центральний контролер або смартфон. Зростаючий список відомих рішень для автоматизації включає в себе:

● Елементи безпеки та спостереження: датчики безпеки для вікон, дверей, руху, розбиття скла та диму. Можуть надавати найважливішу інформацію про безпеку будинків. IP-захищені камери безпеки та спостереження дуже важливі для забезпечення тісної, нерозбитної та непроникної безпеки. Системи виявлення та попередження вторгнення є іншими відомими модулями безпеки.

● Системи опалення, кондиціонування повітря, системи вентиляції, освітлення та системи відтінків. Комфорт стає вирішальним чинником у будинках нового покоління. Забезпечується зв'язок між різними домашніми пристроями, включаючи світлові вимикачі, настінні сенсорні панелі тощо.

● Обчислювальні та комунікаційні пристрої. В даний час в домашніх умовах використовується широкий спектр обчислювальних машин, починаючи від персональних комп'ютерів (ПК), ноутбуків / ноутбуків / планшетів, маршрутизаторів Wi-Fi та шлюзів, носіїв та смартфонів.

● Розваги, освіта та системи масової інформації. Розумні датчики у сфері розваг відстежують рухи тіла, фізіологічні параметри та дотики, щоб зробити ігри та віртуальну реальність більш захоплюючими. Вони також розпізнають обличчя та жести, відкриваючи нові можливості для інтерактивних додатків. В освіті датчики відстежують присутність, увагу та взаємодію учнів з матеріалами, допомагаючи персоналізувати навчання. У системах масової інформації вони вимірюють параметри середовища, відстежують аудиторію та її реакції, допомагаючи оптимізувати контент та підвищити його ефективність.

● Домашня мережа. Всі побутові пристрої інтегруються в єдину цифрову екосистему, обмінюючись даними через бездротові протоколи. Це дозволяє віддалено контролювати та керувати домашніми пристроями через

Інтернет. Автомобільні системи також інтегруються в домашню мережу, забезпечуючи двосторонню взаємодію. Це дозволяє дистанційно спостерігати, управляти та обслуговувати домашні пристрої. Автомобільні мультимедіа, навігаційні та інформаційно-розважальні системи, системи керування паркуванням тощо, також підключаються до домашніх систем безпосередньо або через проміжне програмне забезпечення на базі коробки для взаємодії та взаємодії в реальному часі.

● Домашній контроль доступу. Електронні замки стають невід'ємною частиною системи безпеки, забезпечуючи контроль доступу до житла.

● Об'єкти комфорту та настрою. Побутові предмети, такі як освітлення, меблі та побутова техніка, об'єднані в мережу, створюють адаптивне середовище, що реагує на потреби користувача.

● Системи охорони здоров'я. Медичні пристрої, роботи та інші технології інтегруються в домашню мережу, забезпечуючи моніторинг здоров'я та профілактику захворювань.

● Кухонна техніка. "Розумна" кухонна техніка, включаючи кавоварки, духовки, холодильники та посудомийні машини, стає ключовим елементом розумного будинку, оптимізуючи процеси приготування їжі та зберігання продуктів.

Рисунок 3.1 — Різновиди розумних датчиків

У майбутньому нас оточуватиме все більш технологічно насичене середовище, де побутові пристрої, сенсори та інтелектуальні системи взаємодіятимуть, збираючи дані, контролюючи параметри та забезпечуючи комфорт і безпеку користувачів. Розумний будинок, як ключовий елемент цього середовища, являє собою інтегровану систему, що оптимізує використання ресурсів, підвищує безпеку та створює індивідуальний комфорт для мешканців.

Центральний процесор, "мозок" розумного будинку, аналізує дані з різноманітних сенсорів та пристроїв, автоматично реагуючи на зміни в навколишньому середовищі та виконуючи задані алгоритми. Це дозволяє уникнути необхідності ручного керування кожним пристроєм окремо, забезпечуючи інтуїтивну та ефективну взаємодію з розумним будинком.

Систему можна розділити на кілька основних компонентів: автоматизація, ручне управління, мультимедіа та безпека. Автоматизація у цьому контексті передбачає налаштування функціонування системи залежно від часу доби, рівня освітленості, руху, температури, макросів і сценаріїв.

Ручне управління також має велике значення і включає віддалене управління за допомогою телефону, комп'ютера, веб-додатка, бездротове управління електронікою, а також інтеграцію універсального пульта для всіх пристроїв, що зменшує кількість необхідних пультів. Мультимедіа охоплює бездротову передачу аудіо та відео, а також функції спостереження. Безпека, яка є одним з найважливіших аспектів при виборі системи "розумного будинку", включає можливість встановлення охоронної сигналізації, світлової та звукової сигналізації, імітації присутності господарів, функції "паніка" та інші заходи безпеки.

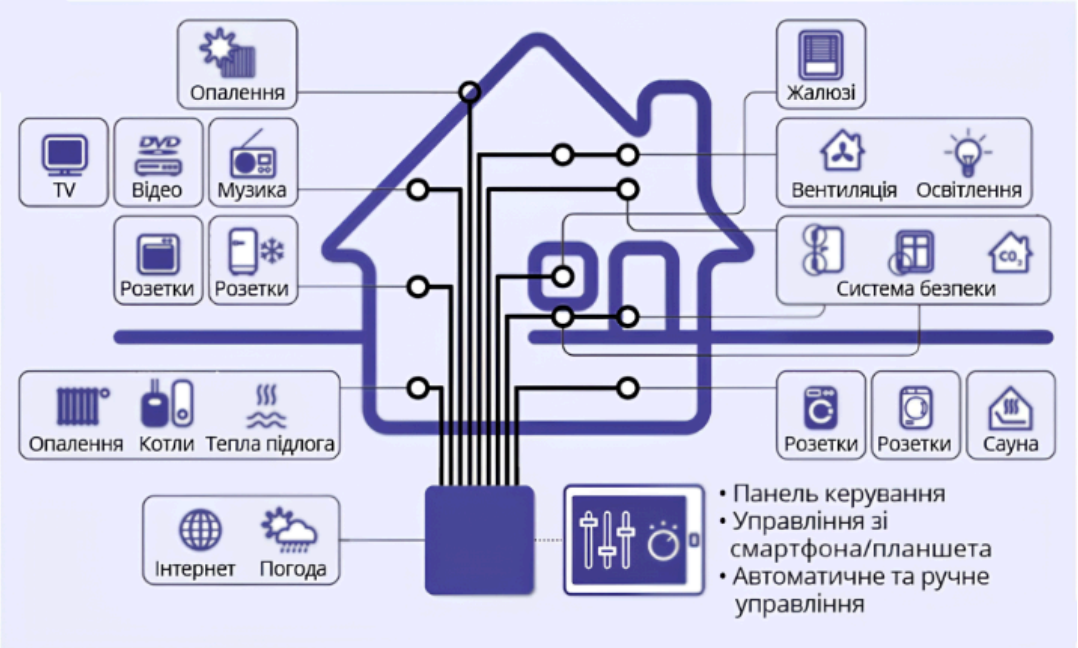

Рисунок 3.2 — Компоненти «розумного будинку»

"Розумний будинок" – це інтегрована система автоматизації, що контролює та координує роботу різноманітних домашніх пристроїв та систем. Завдяки здатності розпізнавати типові ситуації та реагувати на них, система забезпечує оптимальне використання ресурсів та створює максимально комфортні умови для мешканців.

"Розумний будинок" не лише керує окремими приладами, а й оптимізує їхню спільну роботу, що призводить до синергетичного ефекту. Це означає, що ефективність всієї системи перевищує суму ефективності

окремих її компонентів. Це сприяє створенню максимально комфортних умов проживання людей при максимально економному споживанні ресурсів.

Розумний будинок, незважаючи на свою технологічну просунутість, залишається вразливим до відключень електроенергії. Це особливо актуально для України, де блекаути стали частиною реальності через пошкодження енергетичної інфраструктури. Однак, існують різні підходи та технології, що дозволяють забезпечити базову функціональність розумного будинку навіть за відсутності централізованого електропостачання. Збереження функціональності розумного будинку під час блекаутів є критично важливим завданням. Системи сигналізації та відеоспостереження повинні залишатися активними, щоб забезпечити захист житла від несанкціонованого доступу та злому. Для цього важливо використовувати резервні джерела живлення, такі як акумуляторні батареї або генератори. Розумні замки та інші системи контролю доступу повинні функціонувати навіть під час відключення електроенергії, забезпечуючи безпечний вхід та вихід з приміщення. Автоматичне ввімкнення аварійного освітлення у разі відключення електроенергії допоможе уникнути травм та забезпечить безпеку пересування. Альтернативні джерела опалення, такі як газові котли, твердопаливні котли або каміни, допоможуть підтримувати комфортну температуру в приміщенні

Джерела безперебійного живлення (ДБЖ) здатні забезпечити роботу критично важливих систем протягом певного часу. Їх можна використовувати для живлення роутера, центрального хабу розумного будинку, сигналізації та деяких інших пристроїв. Для підключення пристроїв до ДБЖ достатньо під'єднати їх до відповідних розеток на пристрої. Деякі розумні пристрої, такі як датчики та камери, можуть мати вбудовані акумулятори, що дозволяють їм працювати автономно протягом певного часу.

Генератори є потужнішими джерелами живлення, здатними забезпечити роботу більшості приладів у будинку протягом тривалого часу. Для підключення пристроїв до генератора необхідно вимкнути основне живлення будинку та під'єднати прилади до генератора за допомогою подовжувачів або спеціальних кабелів. Важливо дотримуватися інструкцій виробника та не перевищувати допустиме навантаження генератора.

Інтеграція сонячних панелей або інших відновлюваних джерел енергії дозволяє забезпечити роботу розумного будинку навіть за тривалих відключень електроенергії. У разі відсутності електроенергії, резервні системи опалення, такі як газові котли або каміни, можуть підтримувати комфортну температуру в будинку. Інвертор підключається до домашньої електромережі або до акумуляторної батареї для зберігання надлишкової енергії. За допомогою спеціальних контролерів та програмного забезпечення, сонячна система інтегрується з системою розумного будинку. Це дозволяє автоматично керувати розподілом енергії, пріоритезуючи живлення критично важливих пристроїв під час відключень електроенергії.

Під час блекаутів в Україні багато власників розумних будинків використовували різні стратегії для підтримки функціональності своїх систем. Наприклад, деякі встановили потужні ДБЖ, які забезпечували роботу основних систем протягом кількох годин. Це дозволяло підтримувати зв'язок через інтернет, забезпечувати роботу сигналізації та навіть деяких побутових приладів. Інші власники розумних будинків інвестували в сонячні панелі та системи зберігання енергії. Це дозволило їм не лише забезпечити електроенергією будинок під час блекаутів, а й продавати надлишки енергії в мережу, коли вона працювала. Також деякі українці використовували розумні розетки та вимикачі, які дозволяли віддалено керувати електроприладами та вимикати їх, коли вони не використовувалися. Це допомагало економити заряд акумуляторів та продовжувати роботу найважливіших систем.

3.2. Забезпечення інформаційної безпеки розумного будинку

Інтернет речей (IoT), що поєднує мережеві комплекси та системи, алгоритми штучного інтелекту та хмарні обчислення, створює значні виклики для безпеки інформаційних програм та баз даних. Основними аспектами безпеки IoT є безпека зв'язку, захист пристроїв, контроль пристроїв та контроль взаємодії в мережі.

Звіт Cisco за 2023 рік [14] підкреслює, що спеціалісти із захисту швидкими темпами впроваджують IoT-пристрої, проте звертають мало уваги на безпеку цих систем. Незахищені та неконтрольовані IoT-пристрої надають зловмисникам можливість проникати в мережі. Так, дослідники загроз із компанії Cisco виявили 224 нових вразливостей в продуктах, які не належать Cisco: з них 74 уразливості IoT-пристроям. Звіт про IoT за 2019 рік компанії Gemalto свідчить, що найбільшою проблемою є захист даних, обсяги яких зростають: тільки 60% організацій визнають шифрування цих даних, тоді як 40% залишають їх уразливими, а 48% компаній не можуть виявити, який пристрій IoT має порушення. В ході проведеного компанією HP дослідження виявлено, що приблизно в 70% проаналізованих пристроїв не шифрується бездротової трафік. Веб-інтрефейс 60% пристроїв експерти HP порахували небезпечним через небезпечну організацію доступу і високих ризиків міжсайтового скриптинга. У більшості пристроїв передбачені паролі недостатньо стійкі. Приблизно 90% пристроїв збирають ту чи іншу персональну інформацію про власника без його відома. Всього ж фахівці HP нарахували близько 25 різних вразливостей в кожному з досліджених пристроїв (телевізорів, дверних замків, побутових ваг, домашніх охоронних систем, електророзеток) і їх мобільних і хмарних компонентах.

Слабкі місця IoT:

– перехід на IPv6;

– живлення датчиків;

– стандартизація архітектури і протоколів, сертифікація пристроїв.

– інформаційна безпека;

– стандартні облікові записи від виробника, слабка аутентифікація;

– відсутність підтримки з боку виробника для усунення вразливостей

– важко або неможливо оновити ПЗ і ОС;

– використання текстових протоколів і непотрібних відкритих портів;

– використовуючи слабкість одного гаджета, хакеру легко потрапити у всю мережу;

– використання незахищених мобільних технологій;

– використання незахищеною хмарної інфраструктури;

– використання небезпечного ПЗ.

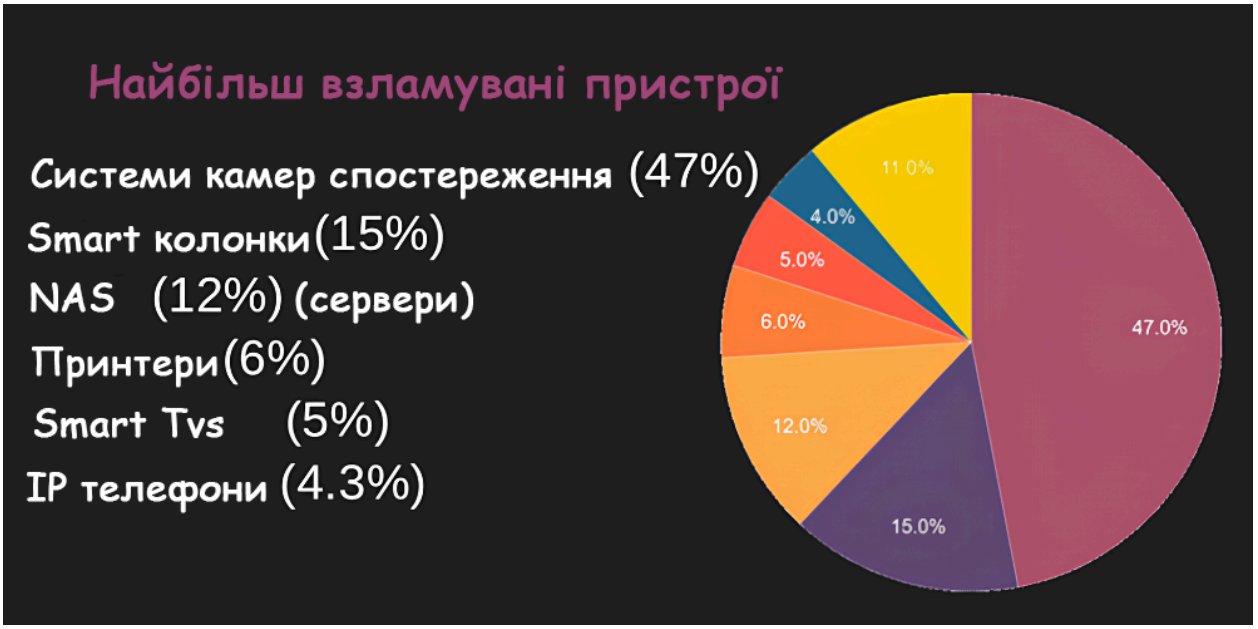

Рисунок 3.3 — Найбільш вразливі пристрої розумного будинку

Система розумного будинку складається з пристроїв, які генерують, обробляють та обмінюються величезною кількістю критично важливих для безпеки даних, а також конфіденційної інформації, і, отже, є привабливими для різних кібератак. Існують різні дослідження щодо безпеки та

конфіденційності IoT та розумного будинку [15]. Важливим для таких систем є створення мереж малого радіуса дії, здатних тримати зв'язок основного процесора з багатьма пристроями і надійно передавати дані, економно витрачаючи живлення IoT пристроїв.

Основними складовими безпеки інформації, інформаційної системи або технології є такі категорії: доступність, цілісність, конфіденційність. У загальному розумінні, доступність інформації технологій розумного будинку означає можливість власникам (або самим підсистемам розумного будинку) виконувати дозволені операції та/або своєчасно обмінюватися інформацією між пристроями. Наприклад, відкрити або закрити двері, перевірити температуру для вмикання або вимикання кондиціонера. Цілісність інформації забезпечується повною і достовірною інформацією про стан всіх пристроїв розумного будинку, наприклад, система знає, як діяти при виявленні витоку газу. Конфіденційність інформації в розумному будинку означає, що витік приватної інформації не є можливим.

Існує широкий спектр джерел загроз інформаційній безпеці розумного будинку та можливих наслідків таких дій. До них належать антропогенні фактори (хакерські атаки на основний сервер, перехоплення інформації, крадіжка пристроїв, наявність порушників серед персоналу), технічні фактори (перебої в електроживленні, помилки програмного забезпечення, поломка апаратури системи) та стихійні лиха. Дослідження поділяють вразливості інформаційній безпеці розумного будинку на дві категорії: надмірні привілеї (excessive privilege) і незахищений обмін повідомленнями (insecure messaging) [16]. Надмірні привілеї означають злом системи безпеки, коли мобільний додаток отримує доступ або права на операції, які йому не потрібні для роботи. Коли шкідливі програми (malware) отримують необмежений доступ до SMS APIs або логів, це може призвести до витоку особистої інформації (PII), включаючи пінкод або паролі. Вважається, що розумні будинки вразливі до атак, здійснених через смартфони користувачів,

навіть якщо домашній шлюз контролює обмін пакетами вдома та поза ним. Вчені виявили серйозні недоліки безпеки у численних пристроях розумного дому: наприклад, підключені до Інтернету смарт-лампочки та комутатори живлення можуть бути легко скомпрометовані через слабкий контроль аутентифікації. Цифрові фотографії, кадри, камери та динаміки передають дані у відкритому тексті, що легко перехопити, ставлячи під загрозу конфіденційність користувача. Цю вразливість легко використати зловмисником. Виділяють п’ять областей, пов’язаних з безпекою IoT:

1) локальність недовіри (LAN Mistruct) — якщо пристрій здійснює автентифікацію в мережі один раз, то надалі йому довіряють;

2) екологічна недовіра (Environment) — IoT довіряє фізичному середовищу, в межах якого воно розміщене;

3) додаткові привілеї (App Over-privilege);

4) слабка автентифікація або її відсутність (No/Weak Authentication);

5) недоліки реалізації (Implementation Flaws) — витік приватної інформації, не шифрування даних.

В ідеалі, розумний дім повинен забезпечувати гарантовану безпеку його мешканцям. Технології розумного дому дозволяють оперативно реагувати на аварійні ситуації та запобігати їм, здійснювати контроль доступу на територію та в житло тощо. У статті [17] проведено аналіз підходів до забезпечення безпеки розумного будинку:

1) підходи, пов’язані з фізичною особою:

- автентифікація;

- контроль доступу;

2) підходи, пов’язані з архітектурою програмного та апаратного забезпечення:

- вбудована система безпеки в пристрій;

- атестація пристроїв;

- система виявлення вторгнень;

- інформаційний потік.

У дослідженні «Privacy Preserving Data Analytics for Smart Homes» [17] запропоновано архітектурний метод з трьома модулями для захисту конфіденційності даних у розумних будинках. Модуль збору даних збирає дані з датчиків і надсилає їх до модуля приймача даних, який перетворює та зберігає їх у двох різних наборах. Модуль результатів контролює доступ до оброблених даних, забезпечуючи конфіденційність. Він складається з чотирьох підмодулів:

1) Контроль доступу автентифікація, авторизація та визначення рівня конфіденційності для спільної інформації.

2) Ретривер ідентифікаторів запитує словник ідентифікаторів для створення списку даних, до яких кінцевий користувач має доступ.

3) Трансформатор узагальнює особисті значення та створює набір даних з хешованими, фактичними та узагальненими значеннями.

4) Процесор результатів запускає завдання на ідентифікованому сховищі та замінює хешовані значення відповідними узагальненими значеннями.

Цей метод гарантує доступ до даних лише справжньому користувачеві та запобігає зв’язуванню різних даних одного користувача. Проте, він не забезпечує конфіденційність, коли дані необхідно розкрити постачальнику послуг.

У інших дослідженнях було виявлено, що багато пристроїв IoT не мають базових гарантій безпеки. Було запропононовано метод захисту цих пристроїв шляхом обмеження доступу на рівні мережі. Під час підключення нового пристрою IoT до мережі користувач, адміністратор або Інтернет-провайдер можуть запитувати захисні заходи у постачальника SaaS. Це рішення не вимагає змін від виробників пристроїв, зменшує навантаження на кінцевих користувачів і забезпечує безпеку як послугу, яку надає Інтернет-провайдер або спеціалізований постачальник у хмарі. Однак, цей

метод залишається вразливим до атак, здійснених через смартфони користувачів.

Технологія Blockchain, впроваджена програмістом Satoshi Nakamoto у 2008 році, стала вирішенням проблеми забезпечення довіри між сторонами без залучення зовнішніх гарантів, таких як банки. Blockchain — це структурована база даних, де кожен блок пов’язаний з попереднім і містить набір записів (інформації). Кожен новий блок додається в кінець ланцюга та має унікальний цифровий підпис — хеш, який змінюється при зміні навіть одного символу в тексті, що унеможливлює внесення правок у блок або додавання блоку між іншими. Завдяки загальнодоступності, розподіленості та достовірності, Blockchain є перспективною технологією для забезпечення безпеки інформаційних систем розумного будинку. Наразі пропонується використання комбінації IPFS та алгоритму шифрування для надійного зберігання інформації IoT. Інформація зберігається в IPFS, а хеш-значення шифрується та зберігається в Blockchain. Авторизовані користувачі можуть отримати хеш-значення через смарт-контракт, який підтверджує дозвіл. Проте, прийняття Blockchain у контексті IoT супроводжується кількома суттєвими проблемами: високий попит на ресурси, довга затримка на підтвердження транзакцій та низька масштабованість.

Загальний алгоритм забезпечення захисту системи "Розумний будинок" націлено на виявлення, запобігання та реагування на потенційні загрози, що можуть виникнути у зв'язку з використанням IoT-пристроїв у домашньому середовищі. Зокрема, він враховує такі ключові аспекти:

1. Фізична безпека. Крім внутрішньої безпеки, мережі необхідний захист від зовнішніх загроз. Датчики повинні бути розміщені таким чином, щоб зловмисники не мали до них прямого фізичного доступу та вони були непомітними для них.

2. Сертифікація пристроїв та перевірка справжності. Крім відповідності стандартам, необхідно забезпечити сертифікацію складових

мережі сертифікаційними центрами. Це дозволяє перевіряти пристрої, що підключаються до мережі, на відповідність вимогам безпеки та запобігає проникненню шкідливих пристроїв.

3. Стандартизація. Мережі IoT здебільшого бездротові, що ускладнює забезпечення їхньої безпеки порівняно з традиційними дротовими мережами через різноманітність нових протоколів і стандартів для радіочастот та радіозв'язку. Пристрої та система в цілому мають відповідати стандартам безпеки, щоб уникнути вразливостей до злочинних дій.

4. Аутентифікація. Пристрої IoT повинні бути автентичними користувачами мережі. Методи аутентифікації варіюються від статичних паролів до двофакторної аутентифікації, біометрії та цифрових сертифікатів. Унікальною особливістю IoT є те, що пристрої повинні розпізнавати один одного, що зменшує ризик проникнення несанкціонованих пристроїв у систему.

5. Шифрування. Шифрування необхідне для запобігання несанкціонованому доступу до даних. Хоча забезпечення шифрування у різноманітних пристроях IoT є складним завданням, воно повинно бути частиною загального процесу управління безпекою. Сучасні дослідження розробили чіпи для шифрування на еліптичних кривих, які можуть використовуватися в IoT-пристроях.

6. Захист інтерфейсу. Більшість виробників надають доступ до пристроїв через програмний інтерфейс (API). Забезпечення безпеки API вимагає аутентифікації та авторизації пристроїв для обміну даними. Лише авторизовані пристрої, розробники та програми можуть здійснювати зв'язок між захищеними пристроями.

7. Механізми доставки. Потрібні постійні оновлення та патчі для подолання мінливих тактик хакерів. Це вимагає знань у патчах, які виправляють вразливості в програмному забезпеченні у режимі реального часу.

8. Аналітика безпеки та прогнозування загроз. Необхідно не лише стежити за даними, пов'язаними з безпекою, але й використовувати їх для прогнозування майбутніх загроз. Це доповнює традиційні методи, що виявляють аномальні дії, які виходять за рамки встановлених політик.

9. Контроль доступу. Якщо будь-який компонент скомпрометовано, контроль доступу гарантує, що вторгнення матиме мінімальний вплив на інші частини системи. Механізми контролю доступу на базі пристроїв подібні до мережевих систем, обмежуючи скомпрометовану інформацію лише тими областями мережі, де вона авторизована.

3.3. Опис та огляд функціональних можливостей та структури додатку для реалізації захищеної автоматизованої системи розумного будинку

Технології «розумних» квартир пройшли довгий шлях, щоб стати доступними зручностями для звичайних людей. Сьогодні перевагами «розумних» квартир можуть скористатися всі – від мешканців до менеджерів з управління нерухомістю. До 2027 року кількість активних домогосподарств на ринку «розумних» квартир, ймовірно, перевищить 672 мільйони користувачів [24]. Ці цифри доводять, що для багатоквартирних будинків технології «розумного будинку», безсумнівно, стануть стандартними зручностями, а не предметами розкоші, і попит на них буде постійно зростати.

Отже, технологія розумного будинку – це не лише розумні пристрої, а новий спосіб життя з відчуттям контролю над усім, що відбувається вдома. Перш за все, рішення для розумних квартир покликані полегшити життя мешканців, дати їм більше часу на речі, які дійсно мають значення, і допомогти їм позбутися рутини, яку можна автоматизувати завдяки передовим технологіям. Завдяки розумним пристроям можна не лише значно скоротити витрати на електроенергію завдяки саморегульованим елементам,

таким як термостати та розумне освітлення, але й замінити додатковий персонал, який обслуговує нерухомість, наприклад, охоронців і швейцарів, на автоматизовані системи. При будівництві «розумних» квартир дизайнери приділяють особливу увагу питанням безпеки. Є можливість встановити сучасну систему безпеки з розумними датчиками і камерами, щоб гарантувати, що ніхто не матиме можливості порушити спокій будинку. Екологічність віднедавна стала новим стандартом для побутової техніки. Звичайні прилади, такі як світильники та холодильники, тепер виробляються з мінімальним споживанням енергії. Інші системи, такі як датчики протікання, можуть вберегти будинок від неприємних аварій та надмірного споживання води.

Пристрої для розумного дому можуть бути такими ж численними, як і традиційні прилади, які використовують для полегшення життя. Розумні пристрої охоплюють майже всі аспекти вашого життя в багатоквартирному будинку, але існує кілька основних, які зазвичай встановлюються першими. Розумні вимикачі та терморегулятори – це одні з найпростіших і найпоширеніших зручностей у розумному домі. Вони дозволяють забути про ручне регулювання температури та освітлення, оскільки всі налаштування можна контролювати одним натисканням кнопки і автоматизувати відповідно до ваших уподобань і розкладу. Розумні системи освітлення не лише дозволяють створювати необхідні налаштування, але й можуть використовувати датчики руху для автоматичного вмикання і вимикання світла при вході або виході з кімнати. Крім того, ці пристрої є більш енергоефективними.

Розумні замки поступово замінюють традиційні фізичні ключі, пропонуючи значно більше переваг, ніж просто відмикання дверей за допомогою смартфона. Вони дозволяють контролювати доступ до інших приміщень, таких як спортзали, і надавати доступ конкретним людям.

Розумні камери є невід'ємною частиною будь-якого розумного будинку для квартир. Вони забезпечують цілодобовий контроль над усім, що відбувається як всередині, так і зовні вашого помешкання. Ці пристрої дозволяють вам завжди мати доступ до своїх кімнат, відстежувати переміщення дітей або домашніх тварин, а також бачити кожного відвідувача вашого будинку. У разі небажаних гостей, є можливість швидко відреагувати на ситуацію та заблокувати доступ.

Виявлення протікань і загазованості є надзвичайно важливим аспектом безпеки будинку. У більшості випадків люди виявляють витоки занадто пізно, коли уникнути шкідливих наслідків вже неможливо. Спеціальні рішення для розумних квартир дозволяють уникнути таких ситуацій завдяки датчикам, які сповіщають на смартфон про перші ознаки аварії. Це дає змогу негайно вжити заходів для вирішення проблеми.

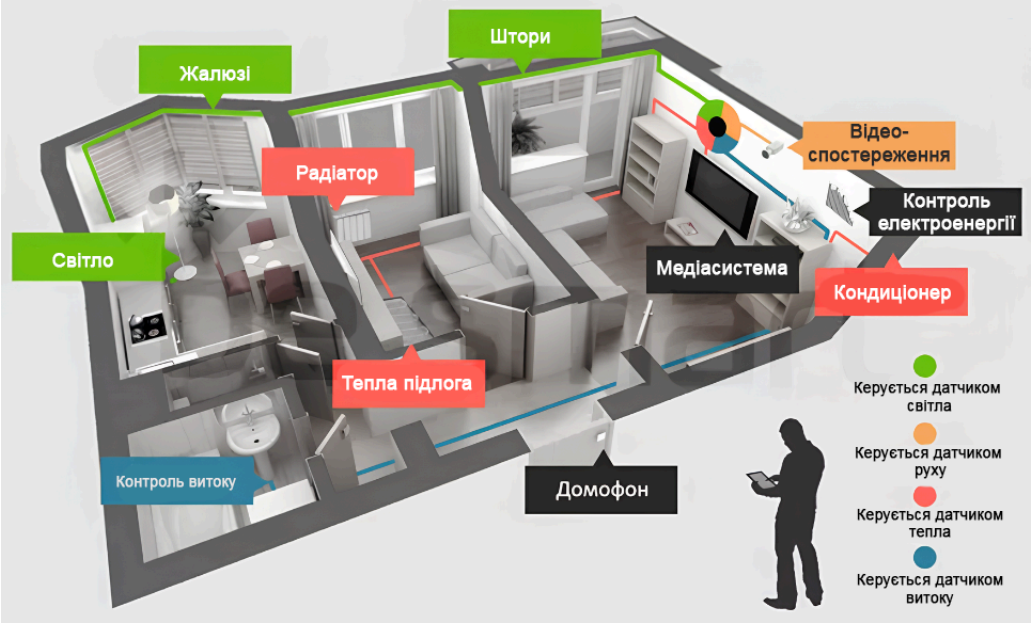

Рисунок 3.4 — Проект розумної квартири

Важливою складовою систем розумного будинку або квартири є правильна розстановка та інтеграція IoT-пристроїв, що забезпечують контроль та управління різними аспектами життєдіяльності. Розробка веб-додатку для планування та керування розумним будинком дозволить

мешканцям і планувальникам з легкістю організовувати і контролювати свої пристрої, створюючи індивідуальні сценарії використання та покращуючи загальну функціональність житла. Такий веб-додаток пропонує численні переваги для мешканців та планувальників розумного будинку:

1. Реєстрація пристроїв та приміщень: завдяки вкладці "Реєстрація приладів" користувачі можуть додавати та всі необхідні IoT-пристрої. Кожен пристрій представлений у вигляді картки з фотографією, назвою моделі, актуальною ціною та описом, що дозволяє швидко ідентифікувати його. Вкладка "Реєстрація квартир" дозволяє користувачам вносити дані про приміщення, включаючи їх розміри та розташування.

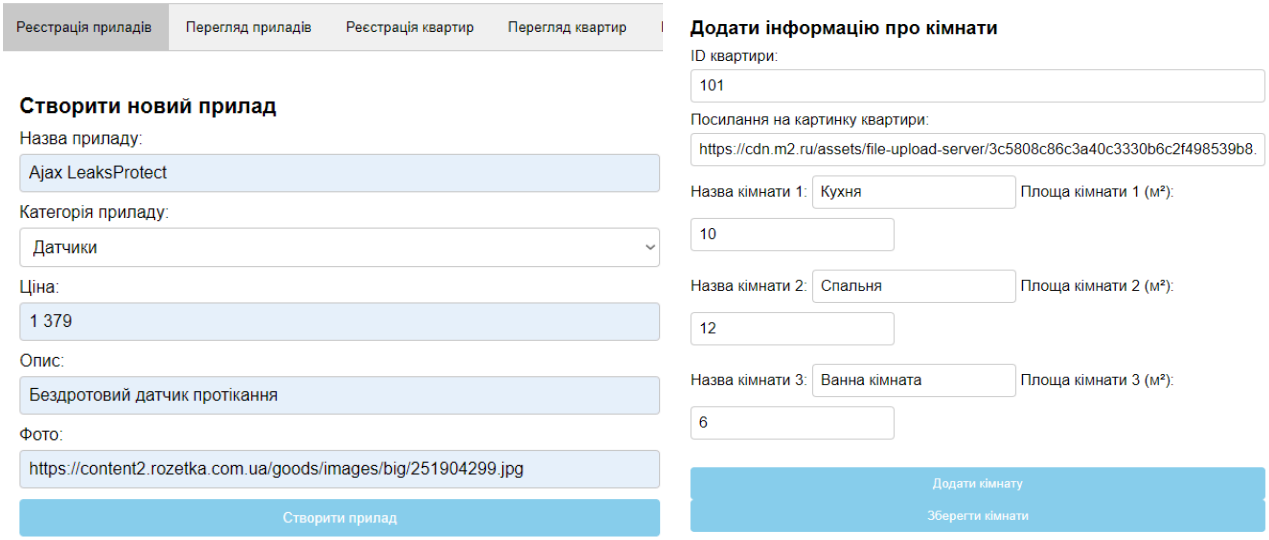

Рисунок 3.5 — Реєстрація розумних пристроїв та приміщень у додатку

2. Оптимальна розстановка обладнання: вкладка «Перегляд пристроїв» надає можливость перегляду карток пристроїв з фотографією та назвою моделі. Вкладка «Перегляд квартир» показує перелік кімнат із зазначенням їх розмірів (наприклад, спальня 1, спальня 2, вітальня, коридор, передпокій, ванна, кладовка) та фото плану квартири.

Фрагмент коду, що відповідає за реєстрацію та виведення списку всіх пристроїв:

```
// Виводимо кожен пристрій
        devices.forEach((device, index) => {
            const deviceItem = document.createElement('div');
```

```
        deviceItem.classList.add('device-item');
        deviceItem.innerHTML = `
            <div class="device-image">
                <img src="${device.photo}" alt="${device.deviceName}">
            </div>
            <div class="device-info">
                <p>Назва: ${device.deviceName}</p>
                <p>Категорія: ${device.deviceCategory}</p>
                <p>Ціна: ${device.price}</p>
                <p>Опис: ${device.description}</p>
            </div>
        `;
        devicesContainer.appendChild(deviceItem);
    });
```

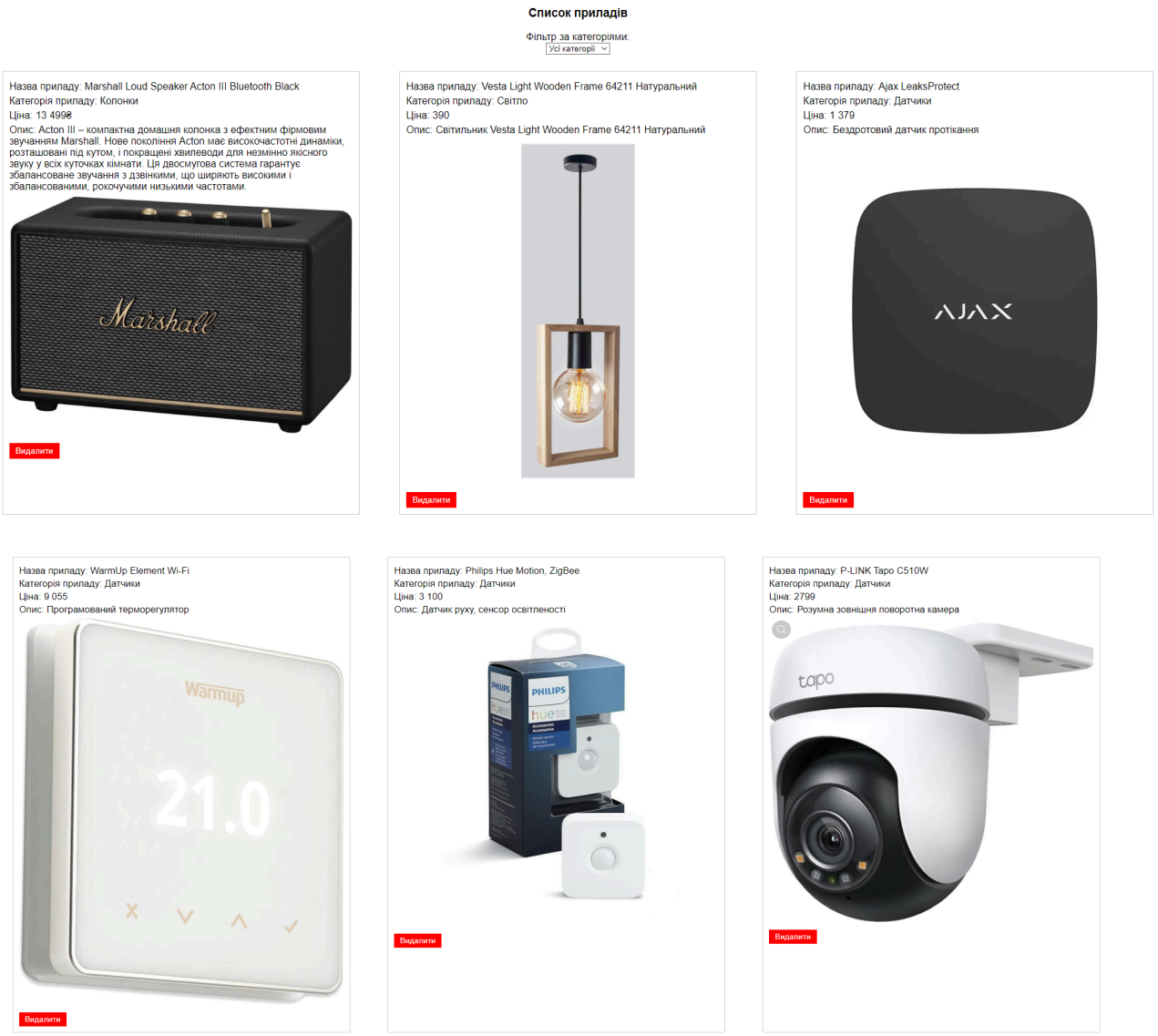

Рисунок 3.6 — Перегляд розумних пристроїв у додатку

Фрагмент коду, що відповідає за реєстрацію та виведення списку всіх квартир, їх планів та кімнат:

```
// Виводимо кожну квартиру
        apartments.forEach(apartment => {
            const apartmentItem = document.createElement('div');
            apartmentItem.classList.add('apartment-item');
    // Додаємо ідентифікатор квартири та зображення квартири
    const apartmentInfo = document.createElement('div');
    apartmentInfo.classList.add('apartment-info');
    apartmentInfo.innerHTML = `
        <img src="${apartment.image}" alt="Квартира №${apartment.id}">
        <p>ID квартири: ${apartment.id}</p>
    `;
    apartmentItem.appendChild(apartmentInfo);
    // Виводимо кожну кімнату квартири
    apartment.rooms.forEach(room => {
        const roomItem = document.createElement('div');
        roomItem.classList.add('room-item');
        roomItem.innerHTML = `
            <p>Назва кімнати: ${room.roomName}</p>
            <p>Площа кімнати: ${room.roomArea} м²</p>
        `;
        apartmentItem.appendChild(roomItem);
    });
```

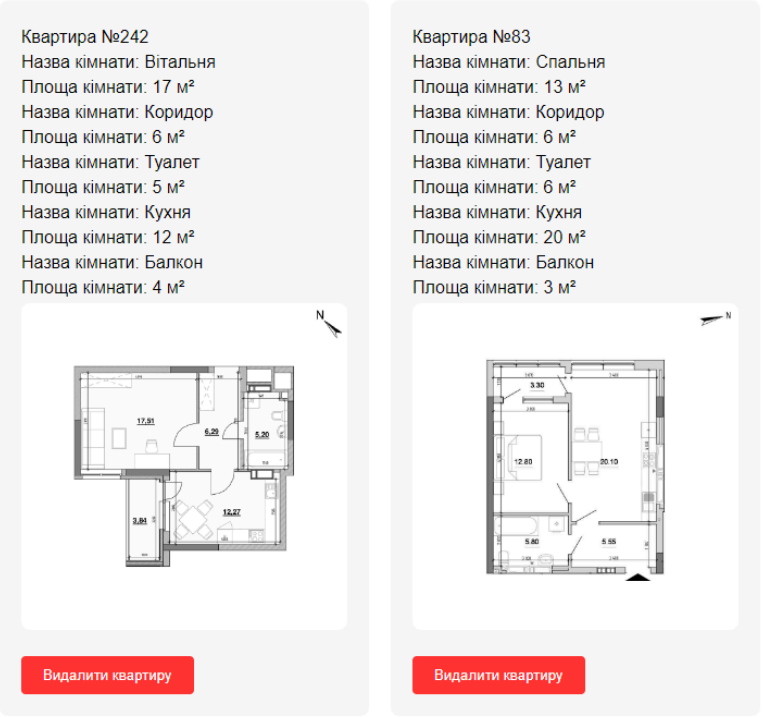

Рисунок 3.7 — Перегляд квартир у додатку

3. Створення індивідуальних сценаріїв: вкладка "Підбір приладів" дозволяє об'єднувати кілька пристроїв у групи або працювати з окремими пристроями, призначаючи їх до певних кімнат обраної квартири. Це дає змогу створювати різноманітні сценарії для автоматизації повсякденних завдань та оптимізувати вибір пристроїв по певним ознакам, таким як вартість, розміри і т.д., що підвищує зручність користування розумним будинком.

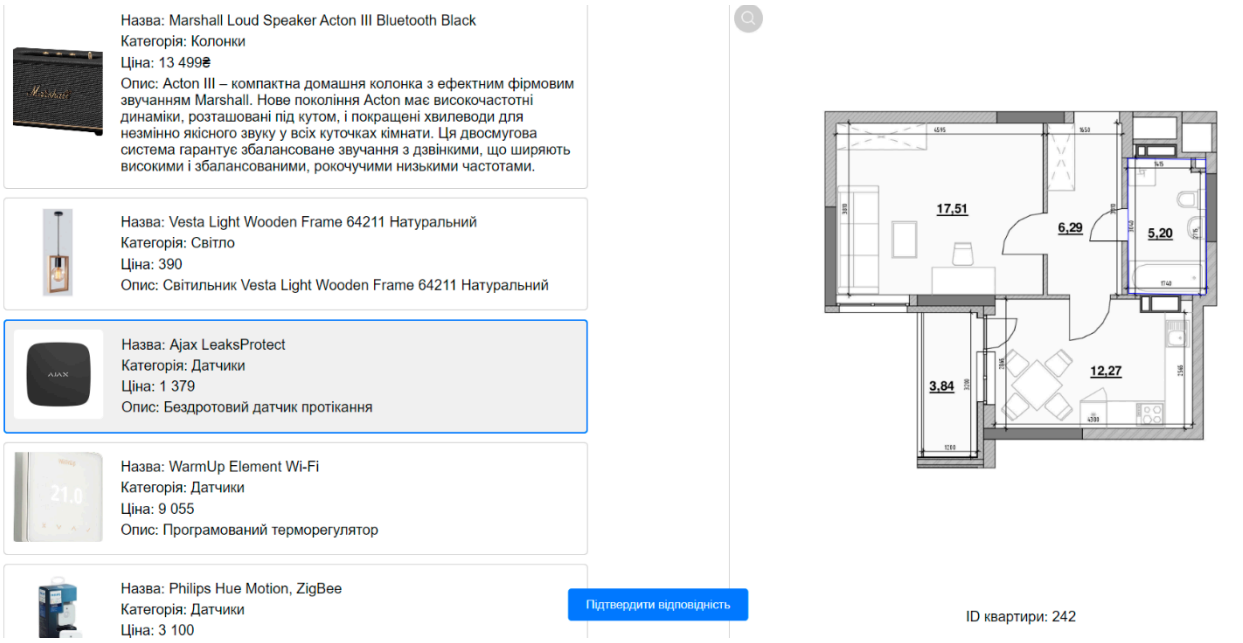

Рисунок 3.8 — Підбір пристроїв до кімнат у додатку

4. Візуалізація та організація простору: вкладка "Підібрані пристрої" надає можливість візуалізувати розміщення пристроїв у кімнатах. Кожна кімната представлена у вигляді блоку з її назвою та списком пристроїв, що знаходяться в ній. Це полегшує планування та дозволяє легко знаходити та контролювати необхідні пристрої.

Фрагмент коду, що відповідає за підбір пристроїв до обраних кімнат в квартирах:

```
saveDataToAcceptedOffers(confirmedMatches);
selectedDevices.forEach(device => {
   device.classList.remove('selected');
});
```

```
        selectedRooms.forEach(room => {
            room.classList.remove('selected');
        });
            showNotification('Підтверджено відповідність пристроїв та кімнат');
```

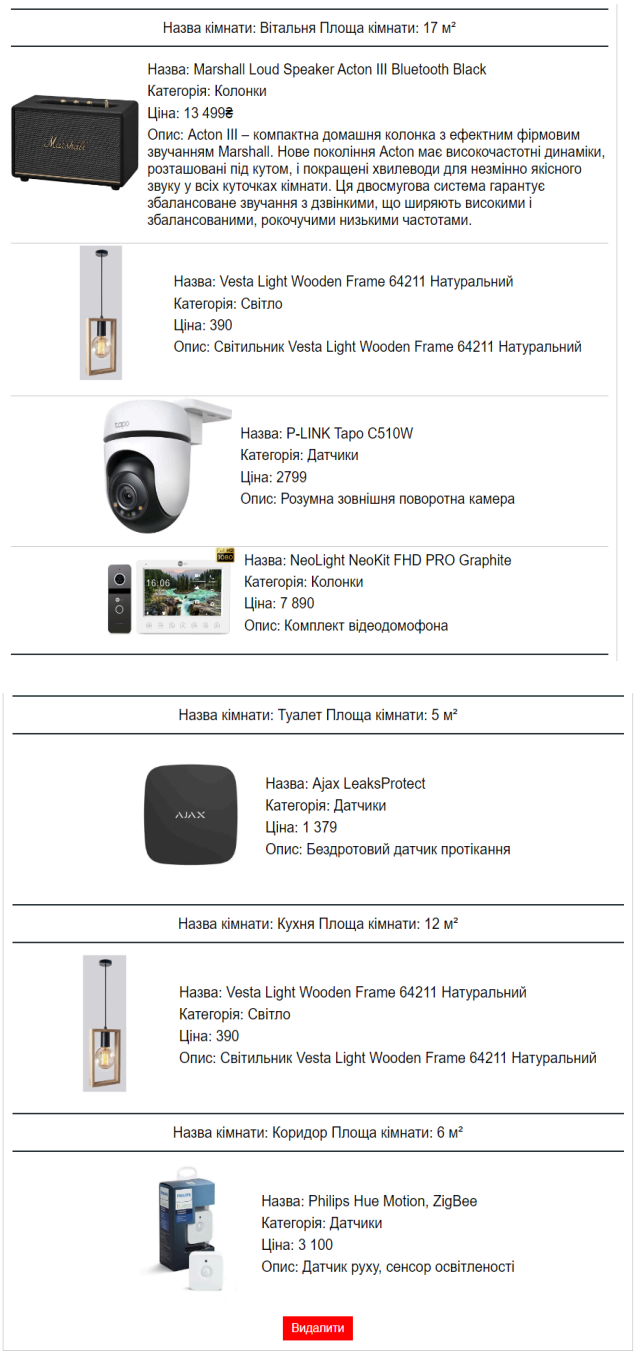

Рисунок 3.9 — Підібрані пристрої для кімнат розумної квартири

Розроблений додаток може модифікуватися та містити інтерактивний план приміщень, де користувачі зможуть віртуально розміщувати IoT-пристрої, враховуючи їх функціональність та зони покриття. Крім того,

веб-додаток може забезпечити зручний інтерфейс для налаштування автоматичних сценаріїв, що дозволить створювати індивідуальні режими роботи розумного будинку залежно від часу доби, присутності мешканців або зовнішніх умов. Інтеграція з хмарними сервісами та голосовими помічниками розширить можливості веб-додатку, надаючи користувачам доступ до даних про споживання енергії, історії подій та віддаленого керування розумним будинком з будь-якого місця.

ВИСНОВКИ

У даній кваліфікаційній роботі було розглянуто автоматизовані інформаційних систем IoT, інформаційні загрози для них та методи захисту. Були поставлені наступні завдання: дослідження історичного розвитку та сучасних напрямків і методів застосування технологій IoT; аналіз проблем і загроз інформаційній безпеці IoT, а також шляхи їх вирішення; проектування системи взаємодії розумних речей для розумного будинку та розгляд методів захисту систем розумного будинку.

У першому розділі було розглянуто історію розвитку інтернету речей, починаючи з перших кроків у розвитку інтернету до появи терміну IoT та його розвитку в Україні і світі. Було описано переваги впровадження IoT в різних сферах життя, а також проблеми, з якими стикаються розробники під час впровадження.

У другому розділі було проаналізовано екосистему IoT, стандарти сумісності та еталонні моделі, описані різними організаціями, такими як Міжнародний союз електрозв'язку (ITU), Всесвітній форум IoT (IWF), Національний інститут стандартів і технологій (NIST). Були досліджені засоби та методи роботи IoT, проаналізовано основні загрози безпеки на кожному з рівнів екосистеми IoT та запропоновані методи захисту від кіберзлочинців.

У третьому розділі були описані елементи та принципи функціонування розумного будинку, розглянуто переваги та недоліки технологій розумного будинку, а також детально описаний процес розробки додатку для реалізації захищеної автоматизованої системи розумного будинку, який дозволяє користувачам додавати та контролювати розумні пристрої в будинку.

Висновки з кваліфікаційної роботи свідчать про важливість вивчення та застосування методів захисту систем IoT. Застосування правильних підходів та методик може значно знизити ризики вразливості систем, запобігти

конкретним загрозам та забезпечити розробників і користувачі методиками захисту при виникненні небезпечної ситуації для ПЗ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Alda M. Internet of Things - Worldwide [Електронний ресурс] / Meredith Alda // Statista. – 2024. – Режим доступу до ресурсу: https://www.statista.com/outlook/tmo/internet-of-things/worldwide.

2. Підгайна Є. Інтернет речей і N-надцать несподіваних варіантів його застосування під час війни: кейси «розумного» Києва, ДТЕК та «Vodafone Україна» [Електронний ресурс] / Євгенія Підгайна // Mind. – 2024. – Режим доступу до ресурсу: https://mind.ua/publications/20266478-internet-rechej-i-n-nadcat-nespodivanih-variantiv-jogo-zastosuvannya-pid-chas-vijni-kejsi-rozumnogo.

3. THE HISTORY OF IOT: HOW THIS TECHNOLOGY IS EVOLVING [Електронний ресурс] // Cogniteq. – 2024. – Режим доступу до ресурсу: https://www.cogniteq.com/blog/history-iot-how-technology-evolving.

4. Rui Aguiar. The 9th IEEE World Forum on Internet of Things [Електронний ресурс] / Rui Aguiar, Adam Drobot // IEEE. – 2023. – Режим доступу до ресурсу: https://wfiot2023.iot.ieee.org.

5. Cisco Security at Cisco Live 2024: Innovating at Scale [Електронний ресурс] // Cisco. – 2024. – Режим доступу до ресурсу: https://blogs.cisco.com/news/cisco-security-at-cisco-live-2024-innovating-at-scale.

6. ITU-T Recommendations Y.4101/Y.2067 [Електронний ресурс] / ITU-T. Study Group 20 // ITU-T. 2017 *(2023)* – Режим доступу до ресурсу: https://handle.itu.int/11.1002/1000/13384.

7. IoT 2023 in review: The 10 most relevant IoT developments of the year [Електронний ресурс] // IoT Analytics. – 2023. – Режим доступу до ресурсу: https://iot-analytics.com/iot-2023-in-review/.

8. National Institute of Standards and Technology. Framework for Cyber-Physical Systems [Електронний ресурс] / 12. National Institute of Standards and Technology // (2024). – 2017. – Режим доступу до ресурсу: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-201.pdf.

9. IoT Security Foundation. Consumer IoT sector – basic cybersecurity hygiene practice still not happening [Електронний ресурс] / IoT Security Foundation. – 2021. – Режим доступу до ресурсу: https://iotsecurityfoundation.org/consumer-iot-sector-basic-hygiene-practice-still-not-happening/.

10. UNIT 42. 2020 Unit 42 IoT Threat Report [Електронний ресурс] / UNIT 42. – 2020. – Режим доступу до ресурсу: https://unit42.paloaltonetworks.com/iot-threat-report-2020/.

11. PSA. PSA Certified 2023 Security Report [Електронний ресурс] / PSA. – 2023. – Режим доступу до ресурсу: https://report.psacertified.org.

12. National Institute of Standards and Technology. TERNET OF THINGS (IOT) [Електронний ресурс] / NIST. – 2024. – Режим доступу до ресурсу: https://www.nist.gov/internet-things-iot.

13. S. Fan, L. Song, and C. Sang, “Research on Privacy Protection in IoT System Based on Blockchain,” in InternationalConference on Smart Blockchain, SmartBlock [Електронний ресурс] / S. Fan, L. Song, C. Sang // Easychair. – 2019. Smart Blockchain – Режим доступу до ресурсу: https:easychair.org/publications/preprint_download/Vg7v

14. Cisco Industrial IoT Solutions [Електронний ресурс] // Cisco. – 2023. – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/solutions/internet-of-things/overview.html.

15. V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, “Asurvey on IoT Security: Application Areas, Security Threats, and SolutionArchitectures,” IEEE Access, vol. 7, pp. 82721–82743, Jun. 2019

16. N. A. Khan, M. Altaf, and F. A. Khan, “Selective encryption of JPEG images with chaotic based novel S-box,” Multimedia Tools and Apps, Springer, vol. 80, no. 6, pp. 9639–9656 – 2021.

17. Аль-Амморі А.Н., Іщенко Р.М., Дехтяр М.М. Електронний документообіг та захист інформації: конспект лекцій. Київ: НТУ, 2021. – 58 с.

18. N. Zhang, S. Demetriou, X. Mi, W. Diao, K. Yuan, P. Zong, F. Qian, X. Wang, K.Chen, Y. Tian, C. A.Gunter, K. Zhang, P. Tague and Y. Lin.Understanding IoT Security Through the Data Crystal Ball: Where We Are Now and Where We Are Going to Be. – 2017. – Режим доступу до ресурсу: https://arxiv.org/pdf/1703.09809.pdf

19. A. Dean and M. O. Agyeman, “A study of the advances in IoT security,”in Proc. 2nd Int. Symp. on Computer Science and Intelligent Control, pp.1–6 – 2019.

20. Hurrah, Nasir N and Parah, Shabir A and Sheikh, Javaid A and Al-Turjman, Fadi and Muhammad, Khan, “Secure data transmission frame-work for confidentiality in IoTs,” Ad Hoc Netw., Elsevier, vol. 95, pp. 1–20 – 2019.

21. Ferrag, Mohamed Amine and Maglaras, Leandros and Derhab, Abde-louahid, “Authentication and authorization for mobile IoT devices using biofeatures: Recent advances and future trends,” Security and Communication Networks, Hindawi, vol. 2019, pp. 1–21 – 2019.

22. A. Tewari and B. Gupta, “Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework,” Future Generation Computer Systems, Elsevier, vol. 108, pp. 909–920 – 2020.

23. A. C. Jose and R. Malekian, “Improving smart home security: Integrating logical sensing into smart home,” IEEE Sensors J., vol. 17, no. 13, pp. 4269–4286, – 2019.

24. Smart Apartment Technology: The Gateway to Elevated and Effortless Living [Електронний ресурс] // RoomBanker. – 2024. – Режим

доступу до ресурсу: https://www.roombanker.com/blog/smart-apartment-technology/.

Systems, Elsevier, vol. 108, pp. 909–920, 2020

- cation Networks, Hindawi, vol. 2019, pp. 1–21, 201
- Springer, vol. 80, no. 6, pp. 9639–9656, 2021.

ДОДАТКИ

Додаток А — Фрагменти коду додатку для автоматизації розумної квартири

```
// Отримуємо дані про користувача з локального сховища
   const userDataString = localStorage.getItem('usersData');
   if (userDataString) {
      // Перетворимо рядок JSON на об'єкт
      const userData = JSON.parse(userDataString);

      // Відображаємо дані про користувача в інтерфейсі
      document.getElementById("username").textContent = `Логін: ${userData.username}`;
      document.getElementById("userRole").textContent = `Роль: ${decodeURIComponent(userData.role)}`;
   }
   // За замовчуванням відкриваємо першу вкладку
   document.getElementById("Tab1").style.display = "block";
   document.getElementById("Tab5").style.display = "none";
   // Відображаємо офери під час завантаження сторінки
   showOffers();
   showRooms();
   showDevices()
   showRoomsWithDevices()
   showAcceptedOffersInfo();
});
// setInterval(() => {
//     showOffers();
//     showPersonnel();
```

```
//    showAcceptedOffers();
// }, 20000);
function openTab(evt, tabName) {
   var i, tabcontent, tablinks;
   tabcontent = document.getElementsByClassName("tabcontent");
   for (i = 0; i < tabcontent.length; i++) {
      tabcontent[i].style.display = "none";
   }
   tablinks = document.getElementsByClassName("tablinks");
   for (i = 0; i < tablinks.length; i++) {
      tablinks[i].className = tablinks[i].className.replace(" active", "");
   }
   document.getElementById(tabName).style.display = "flex";
   evt.currentTarget.className += " active";
}
function showNotification(message) {
   const notification = document.getElementById('notification');
   const notificationMessage = document.getElementById('notification-message');
   // Встановлюємо текст повідомлення
   notificationMessage.textContent = message;
   // Показуємо повідомлення
   notification.classList.remove('hide');
   // Через 5 секунд приховуємо повідомлення
   setTimeout(() => {
      hideNotification();
   }, 5000);
}
// Функція приховування повідомлення
function hideNotification() {
   const notification = document.getElementById('notification');
   notification.classList.add('hide');
}
         // Виводимо кожну квартиру
         apartments.forEach((apartment, index) => {
            const apartmentItem = document.createElement('div');
            apartmentItem.classList.add('apartment-item');
            const roomsContent = apartment.rooms.map(room => `
                  <p>Назва кімнати: ${room.roomName}</p>
                  <p>Площа кімнати: ${room.roomArea} м²</p>
               `).join('');
            const content = `
                  <div class="apartment-info">
                     <p>Квартира №${apartment.id}</p>
                     ${roomsContent}
                     <img class="zoomable-image" src="${apartment.image}" alt="Картинка квартири">
                  </div>
                  <button class="delete-button" onclick="deleteApartment(${index})">Видалити квартиру</button>
               `;
            apartmentItem.innerHTML = content;
            apartmentsList.appendChild(apartmentItem);
         });
function showDevices() {
   // Отримуємо дані про пристрої з файлу devices.json
   fetch('https://api.github.com/repos/butovamia/diplom/contents/offers.json')
      .then(response => {
         if (!response.ok) {
            throw new Error('Помилка при отриманні даних із сервера');
         }
         return response.json();
      })
      .then(data => {
```

```
            const devicesString = atob(data.content);
            const decodedDevicesString = decodeURIComponent(devicesString);
            let devices;
            try {
                devices = JSON.parse(decodedDevicesString);
                if (!Array.isArray(devices)) {
                    devices = [devices];
                }
            } catch (error) {
                devices = [];
            }
            // Очищаємо список пристроїв
            const devicesContainer = document.getElementById('devicesContainer');
            devicesContainer.innerHTML = '';
            // Виводимо кожен пристрій
            devices.forEach((device, index) => {
                const deviceItem = document.createElement('div');
                deviceItem.classList.add('device-item');
                deviceItem.innerHTML = `
                    <div class="device-image">
                        <img src="${device.photo}" alt="${device.deviceName}">
                    </div>
                    <div class="device-info">
                        <p>Назва: ${device.deviceName}</p>
                        <p>Категорія: ${device.deviceCategory}</p>
                        <p>Ціна: ${device.price}</p>
                        <p>Опис: ${device.description}</p>
                    </div>
                `;
                devicesContainer.appendChild(deviceItem);
            });
        })
        .catch(error => {
            console.error('Помилка при отриманні даних про пристрої:', error);
        });
}
function showRoomsWithDevices() {
    // Отримуємо дані про квартири із файлу apartments.json
    fetch('https://api.github.com/repos/butovamia/diplom/contents/employees.json')
        .then(response => {
            if (!response.ok) {
                throw new Error('Помилка при отриманні даних із сервера');
            }
            return response.json();
        })
        .then(data => {
            const apartmentsString = atob(data.content);
            const decodedApartmentsString = decodeURIComponent(apartmentsString);
            let apartments;
            try {
                apartments = JSON.parse(decodedApartmentsString);

                if (!Array.isArray(apartments)) {
                    apartments = [apartments];
                }
            } catch (error) {
                apartments = [];
            }
            // Очищаємо список квартир та пристроїв
            const roomsWithDevices = document.getElementById('roomsWithDevices');
            roomsWithDevices.innerHTML = '';
```

```
            // Виводимо кожну квартиру
            apartments.forEach(apartment => {
                const apartmentItem = document.createElement('div');
                apartmentItem.classList.add('apartment-item');
                // Додаємо ідентифікатор квартири та зображення квартири
                const apartmentInfo = document.createElement('div');
                apartmentInfo.classList.add('apartment-info');
                apartmentInfo.innerHTML = `
                    <img src="${apartment.image}" alt="Квартира №${apartment.id}">
                    <p>ID квартири: ${apartment.id}</p>
                `;
                apartmentItem.appendChild(apartmentInfo);
                // Виводимо кожну кімнату квартири
                apartment.rooms.forEach(room => {
                    const roomItem = document.createElement('div');
                    roomItem.classList.add('room-item');
                    roomItem.innerHTML = `
                        <p>Назва кімнати: ${room.roomName}</p>
                        <p>Площа кімнати: ${room.roomArea} м²</p>
                    `;
                    apartmentItem.appendChild(roomItem);
                });
                roomsWithDevices.appendChild(apartmentItem);
            });
        })
        .catch(error => {
            console.error('Помилка при отриманні даних про квартири:', error);
        });
}
```