БАКАЛАВРСЬКА РОБОТА

БР. ІП - 16.00.00.000 ПЗ

Група ІП-22-4

Фуртас Олександр

2026

Івано-Франківський національний технічний університет нафти і газу

Факультет інформаційних технологій

Кафедра інженерії програмного забезпечення

Фуртас Олександр Олександрович

(прізвище, ім'я, по батькові)

УДК 004.4

(індекс)

БАКАЛАВРСЬКА РОБОТА

Проєктування програмної системи захисту приватності користувачів у середовищі IoT

(назва роботи)

Інженерія програмного забезпечення

(назва освітньої програми)

121 - Інженерія програмного забезпечення

(шифр і назва спеціальності)

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

Здобувач освітнього рівня Фуртас О.О.

(підпис, ініціали та прізвище здобувача)

Науковий керівник Романишин Тарас Любомирович, к.т.н., доцент

(підпис, прізвище, ім'я, по батькові, науковий ступінь, вчене звання керівника)

Допущено до захисту
Завідувач кафедри

доц. Бандура В.В.

(посада) (підпис) (дата) (ініціали та прізвище)

Івано-Франківськ – 2026

Івано-Франківський національний технічний університет нафти і газу

Інститут, факультет інформаційних технологій

Кафедра інженерії програмного забезпечення

Ступінь вищої освіти бакалавр

Спеціальність 121 – Інженерія програмного забезпечення

ЗАТВЕРДЖУЮ:
Зав. кафедрою **ІПЗ**
доц. В.В. Бандура
“ ____ ” _____2026 р.

ЗАВДАННЯ

НА БАКАЛАВРСЬКУ РОБОТУ СТУДЕНТОВІ

Фуртасу Олександру Олександровичу

(прізвище, ім’я, по-батькові)

1. Тема проекту (роботи) “ Проєктування програмної системи захисту приватності користувачів у середовищі IoT”

керівник проекту (роботи) Романишин Тарас Любомирович, доцент

затверджені наказом закладу вищої освіти від “ 21 ” квітня 2026р. № 179/7

2. Строк подання студентом проекту (роботи) 09 червня 2026 р.

3. Вихідні дані до проекту (роботи) Результати і матеріали отримані під час проходження переддипломної практики

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

1. Аналіз загроз конфіденційності та безпеки даних с середовищі IoT

2. Системна архітектура, алгоритмічні моделі та ризики приватності в екосистемах IoT

3. Аналіз патернів збору даних та ризиків приватності в середовищі IoT

4. Концептуальний фреймворк технічних методів мінімізації ризиків

5. Програмна реалізація прототипу системи захисту приватності користувачів у середовищі IoT

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

1. Технологічні чинники інтенсифікації розгортання IoT-систем (рис. 1.1, ст, 14)

2. Класифікація віртуальних та цифрових помічників (рис. 1.2, ст.19)

3. Архітектура функціонування VUI (рис. 1.3, ст. 22)

4. Алгоритмічна модель потоку даних у системах голосового керування (рис. 2.1, ст. 26)

5. Архітектурна діаграма типового розумного динаміка (рис. 2.2, ст.28)

6. Консультанти розділів проекту (роботи)

Розділ	**Консультант**	**Підпис, дата**	
		Завдання видав	**Завдання прийняв**

7. Дата видачі завдання **25 квітня 2026 р.**

Керівник _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	**Назва етапів дипломного проекту (роботи)**	**Строк виконання етапів проекту**	**Примітка**
1	Аналіз загроз конфіденційності та безпеки даних с середовищі IoT	04.05.2026	виконано
2	Системна архітектура, алгоритмічні моделі та ризики приватності в екосистемах IoT	15.05.2026	виконано

3	Аналіз патернів збору даних та ризиків приватності в середовищі IoT	21.05.2026	виконано
4	Концептуальний фреймворк технічних методів мінімізації ризиків	28.05.2026	виконано
5	Програмна реалізація прототипу системи захисту приватності користувачів у середовищі IoT	03.06.2026	виконано
6	Оформлення пояснювальної записки бакалаврської роботи завідувачем кафедри	09.06.2026	виконано

Студент – дипломник _____Фуртас О.О.
(підпис)

Керівник роботи _____Романишин Т.Л.
(підпис)

АНОТАЦІЯ

Бакалаврська робота містить 83 сторінки, 23 рисунки, список використаних джерел із 33 найменуваннями.

Метою роботи є проєктування та програмна реалізація системи захисту приватності користувачів у середовищі IoT шляхом аналізу ризиків конфіденційності, дослідження архітектури пристроїв та використання механізмів безпечної обробки даних.

Об'єктом дослідження є процеси збору, передачі, обробки та захисту персональних даних у середовищі Internet of Things.

Предметом дослідження є методи, алгоритми, архітектурні підходи та програмні засоби забезпечення приватності користувачів у системах розумного будинку та IoT-екосистемах.

В першому розділі визначено основні загрози конфіденційності та технологічні особливості функціонування IoT-систем і голосових інтерфейсів

В другому розділі проведений аналіз системної архітектури IoT-пристроїв дозволив виявити критичні ризики безпеки та потенційні точки витоку персональних даних.

В третьому розділі досліджено патерни збору даних та обґрунтовано ефективність сучасних методів забезпечення приватності в IoT-середовищі.

В четвертому розділі реалізовано прототип системи, призначений для моніторингу та управління захистом приватності користувачів.

Висновок: розроблено комплексний підхід до забезпечення приватності користувачів у середовищі IoT та реалізовано програмну систему, здатну підвищити рівень безпеки персональних даних у сучасних цифрових екосистемах.

КЛЮЧОВІ СЛОВА: INTERNET OF THINGS, ПРИВАТНІСТЬ, КОНФІДЕНЦІЙНІСТЬ ДАНИХ, ІНФОРМАЦІЙНА БЕЗПЕКА, РОЗУМНИЙ БУДИНОК, ГОЛОСОВІ АСИСТЕНТИ, КІБЕРБЕЗПЕКА, ЗАХИСТ ДАНИХ.

ANNOTATION

The bachelor's thesis contains 83 pages, 23 figures, a list of used sources with 33 names.

The purpose of the work is to design and programmatically implement a system for protecting user privacy in the IoT environment by analyzing privacy risks, studying device architecture and using mechanisms for secure data processing.

The object of the research is the processes of collecting, transmitting, processing and protecting personal data in the Internet of Things environment.

The subject of the research is methods, algorithms, architectural approaches and software tools for ensuring user privacy in smart home systems and IoT ecosystems.

The first section identifies the main privacy threats and technological features of the functioning of IoT systems and voice interfaces.

In the second section, an analysis of the system architecture of IoT devices allowed us to identify critical security risks and potential points of leakage of personal data.

In the third section, data collection patterns are investigated and the effectiveness of modern methods for ensuring privacy in the IoT environment is substantiated.

In the fourth section, a prototype of a system designed to monitor and manage user privacy protection is implemented.

Conclusion: a comprehensive approach to ensuring user privacy in the IoT environment has been developed and a software system has been implemented that can increase the level of security of personal data in modern digital ecosystems.

KEYWORDS: INTERNET OF THINGS, PRIVACY, DATA CONFIDENTIALITY, INFORMATION SECURITY, SMART HOME, VOICE ASSISTANTS, CYBERSECURITY, DATA PROTECTION.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

AES – Advanced Encryption Standard

CIA – Confidentiality, Integrity, Availability

dBm – decibel-milliwatt

FedAvg – Federated Averaging

IoT – Internet of Things

KPI – Key Performance Indicator

PbD – Privacy by Design

RSA – Rivest-Shamir-Adleman

Secure Multi-Party Computation – криптографічний протокол

ВСТУП

Стрімкий розвиток цифрових технологій, поширення концепції Internet of Things та активне впровадження інтелектуальних пристроїв у повсякденне життя користувачів спричинили формування нової технологічної екосистеми, у межах якої взаємодія між фізичними об’єктами, мережевою інфраструктурою та хмарними сервісами здійснюється в автоматизованому режимі. Сучасні IoT-системи активно використовуються у сфері розумного будинку, промислової автоматизації, охорони здоров’я, транспортної інфраструктури та енергетики, забезпечуючи підвищення ефективності управління, автоматизацію рутинних процесів і покращення користувацького досвіду.

У межах даної роботи проведено комплексний аналіз ризиків приватності в екосистемах розумного будинку, досліджено архітектурні та технологічні особливості IoT-пристроїв, а також реалізовано програмний прототип системи захисту приватності користувачів «IoT Safeguard». Запропонована система забезпечує централізований моніторинг IoT-мережі, аналіз потенційних загроз, управління рівнями захисту та конфігурацію механізмів безпечної обробки інформації. Результати роботи спрямовані на підвищення рівня конфіденційності та безпеки користувацьких даних у сучасних цифрових екосистемах.

Актуальність роботи

Актуальність теми обумовлена стрімким розвитком технологій Internet of Things та широким впровадженням інтелектуальних пристроїв у повсякденне життя користувачів. Сучасні IoT-системи забезпечують автоматизацію великої кількості побутових та виробничих процесів, однак їх функціонування нерозривно пов’язане зі збором, передачею та аналізом значних обсягів персональних даних. Постійне накопичення телеметричної інформації, аудіо- та відеоданих, геолокаційних показників і поведінкових

характеристик створює передумови для виникнення численних загроз конфіденційності та кібербезпеки.

Особливу небезпеку становить використання централізованих хмарних моделей обробки інформації, у межах яких персональні дані користувачів передаються до зовнішніх серверів для подальшого аналізу та зберігання. Такий підхід значно збільшує ризики витоку інформації, несанкціонованого доступу, цифрового профілювання та порушення приватності користувачів. Проблема ускладнюється тим, що значна кількість IoT-пристроїв має обмежені обчислювальні ресурси та недостатньо захищену програмно-апаратну архітектуру, що робить їх вразливими до різних типів атак.

Таким чином, розробка програмної системи захисту приватності користувачів у середовищі IoT є важливим і актуальним науково-практичним завданням, спрямованим на підвищення рівня безпеки цифрової інфраструктури, мінімізацію ризиків витоку даних та створення ефективних механізмів контролю над процесами обробки інформації.

Метою роботи є проєктування та програмна реалізація системи захисту приватності користувачів у середовищі IoT шляхом аналізу ризиків конфіденційності, дослідження архітектури пристроїв та використання механізмів безпечної обробки даних.

Об’єктом дослідження є процеси збору, передачі, обробки та захисту персональних даних у середовищі Internet of Things.

Предметом дослідження є методи, алгоритми, архітектурні підходи та програмні засоби забезпечення приватності користувачів у системах розумного будинку та IoT-екосистемах.

Завдання дослідження:

- Проаналізувати еволюцію концепції розумного будинку та особливості розвитку IoT-технологій.

- Дослідити основні загрози конфіденційності та безпеки даних у середовищі IoT.

- Виконати аналіз архітектури та принципів функціонування інтелектуальних IoT-пристроїв.

- Дослідити патерни збору даних і механізми формування поведінкових профілів користувачів.

- Розробити концептуальну модель системи захисту приватності користувачів у середовищі IoT.

- Реалізувати програмний прототип системи «IoT Safeguard» для моніторингу та управління безпекою IoT-інфраструктури.

Методи дослідження

У процесі виконання роботи використано методи системного аналізу, методи порівняльного аналізу, методи моделювання, а також методи програмної інженерії для реалізації програмного прототипу системи захисту приватності.

Наукова новизна

Наукова новизна отриманих результатів полягає у розробці комплексного підходу до забезпечення приватності користувачів у середовищі IoT, який поєднує механізми мінімізації даних, диференціальної приватності, криптографічного захисту та предиктивного аналізу ризиків. У роботі запропоновано концептуальний фреймворк оцінювання ризиків конфіденційності в екосистемах розумного будинку та розроблено ієрархічну архітектуру програмної системи.

Практичне застосування

Практичне значення роботи полягає у можливості використання розробленого програмного прототипу «IoT Safeguard» для підвищення рівня захисту приватності користувачів у системах розумного будинку та інших IoT-екосистемах. Запропоновані підходи можуть бути інтегровані у системи моніторингу безпеки, платформи управління IoT-пристроями.

Бакалаврська робота містить 83 сторінки, 33 рисунки, 3 розділи, перелік використаних джерел налічує 33 найменування.

РОЗДІЛ 1. ТЕНДЕНЦІЇ РОЗВИТКУ ТА РИЗИКИ КОНФІДЕНЦІЙНОСТІ В ЕКОСИСТЕМІ ІНТЕРНЕТУ РЕЧЕЙ

1.1. Еволюція концепції розумного будинку в контексті глобальної цифровізації

Традиційне сприйняття житла як приватного, герметичного простору, що піддається повному контролю індивіда, зазнає суттєвої трансформації під впливом стрімкої дифузії технологій Інтернету речей (IoT) [1]. Сучасне домогосподарство перестає бути автономним об'єктом, інтегруючись у глобальну цифрову мережу через систему споживчих IoT-пристроїв.

Динаміка впровадження цих технологій свідчить про експоненціальне зростання ринку. Станом на травень 2025 року загальна кількість реалізованих пристроїв з підтримкою голосового асистента Alexa перевищила 800 мільйонів одиниць. У 2025 році в США понад 80 мільйонів домогосподарств імплементували елементи розумного будинку, а згідно з прогнозними моделями, до 2028 року цей показник сягне 100 мільйонів [2]. За оцінками корпорації Oracle, до кінця 2026 року загальна кількість підключених об'єктів у світі досягне 25 мільярдів, що знаменує перехід від ери загального Інтернету до ери тотального Інтернету речей (IoT).

Інтернет речей дефініюється як мережа фізичних об'єктів, оснащених вбудованими технологіями для взаємодії один з одним та із зовнішнім середовищем [3]. Інтенсифікація розгортання IoT-систем обумовлена низкою технологічних чинників (рис. 1.1) [4]:

- Мініатюризація сенсорних мереж: підвищення енергоефективності та чутливості датчиків;

- Оптимізація обчислювальних потужностей: здешевлення хмарних систем зберігання та обробки Big Data;

- Комунікаційна доступність: поширення недорогих протоколів бездротового зв’язку (Wi-Fi 6, Zigbee, Matter).

Рисунок 1.1 - Технологічні чинники інтенсифікації розгортання IoT-систем

Мультисценарність використання IoT охоплює медичний моніторинг (телемедицина), промислову автоматизацію (Індустрія 4.0) та концепцію «розумних міст» (Smart Cities). Проте найбільш інтимний та етично складний сегмент розгортається безпосередньо у приватному житловому просторі.

Розумний будинок базується на принципі безперебійної автоматизації повсякденних процесів. Система передбачає автономну взаємодію пристроїв без прямої участі користувача: інтелектуальне ліжко ініціює алгоритм приготування кави, синхронізуючись із графіком пробудження, тоді як термостат коригує мікроклімат на основі предиктивного аналізу поведінки мешканців. Основними атрибутами таких систем є зручність, енергоефективність та адаптивність.

1.1.1. Аналіз загроз конфіденційності та безпеки даних

Незважаючи на функціональну привабливість, інтеграція IoT-пристроїв створює значні вразливості для приватності. Функціонування розумних систем тотально залежить від збору, агрегації та аналізу прецизійних даних про життєдіяльність людини.

Емпіричні дані свідчать про системні витоки конфіденційної інформації:

- геолокаційна вразливість: у 2018 році було зафіксовано розголошення точних координат користувачів пристроями Google Home та Chromecast.

- несанкціонований доступ до візуальних даних: федеральна торгова комісія (FTC) встановила факти нелегітимного перегляду співробітниками компанії Ring приватних відеозаписів із камер спостереження, встановлених у спальнях та ванних кімнатах користувачів.

Проблема посилюється відсутністю уніфікованого правового регулювання. У правовому полі США, не існує цілісної федеральної рамки, яка б чітко обмежувала обсяги збору та методи експлуатації даних із домашніх IoT-пристроїв. Наявний дискурс у політичних та технологічних колах поки що не трансформувався у дієві стандарти захисту «за замовчуванням».

Конфіденційність у контексті IoT порушується не лише внаслідок зловмисних атак, а й як легітимна частина бізнес-моделей виробників. Основна загроза полягає у контекстуальній агрегації даних.

Поодинці дані від розумної розетки (споживання електроенергії) або датчика руху здаються невинними. Однак, агрегація цих даних у хмарі дозволяє реконструювати точний розпорядок дня мешканців: час пробудження, повернення додому, періоди відсутності, кількість людей у приміщенні та навіть харчові звички (через моніторинг використання кухонних приладів). Це створює ідеальні умови для предиктивного маркетингу або психографічного маніпулювання.

Сучасні алгоритми машинного навчання здатні виявляти приховані кореляції. Наприклад, аналіз мікровібрацій, зафіксованих акселерометром

смартфона, що лежить на столі, може дозволити зловмисникам відновити текст, набраний на клавіатурі цього ж столу. У розумному домі аналіз трафіку бездротової мережі (навіть зашифрованого) може виявити, які саме пристрої активовані, що опосередковано вказує на дії користувача (наприклад, активація розумного замка вказує на вхід/вихід).

Голосові асистенти не просто фіксують команди, вони обробляють акустичні відбитки голосу. Ці дані можуть бути використані для ідентифікації користувача, аналізу його емоційного стану або навіть діагностики певних захворювань (наприклад, хвороби Паркінсона за змінами в голосі) без згоди суб'єкта.

1.1.2. Технічні вразливості на рівні пристроїв та мережі

Архітектура багатьох споживчих IoT-пристроїв часто не відповідає принципам Security by Design через обмежені обчислювальні ресурси та прагнення виробників здешевити продукцію.

Значна частина IoT-пристроїв використовує застарілі або слабкі протоколи шифрування (або не використовує їх зовсім у локальній мережі). Це відкриває можливість для атак типу «Людина посередині», де зловмисник може перехоплювати дані (наприклад, паролі від Wi-Fi, відеопотоки з камер) або підміняти команди управління (наприклад, відкрити розумні двері).

Використання жорстко закодованих або слабких стандартних паролів (на кшталт "admin/1234") залишається масовим явищем. Зловмисники використовують автоматизовані сканери для пошуку таких пристроїв в Інтернеті та об'єднання їх у ботнети (наприклад, ботнет Mirai, який складався переважно з IP-камер та роутерів).

Багато бюджетних IoT-пристроїв не мають функції автоматичного оновлення прошивки. Навіть якщо вразливість виявлено, користувач часто не має можливості або знань для її усунення, що робить пристрій назавжди вразливим.

Більшість рішень розумного будинку залежать від хмарних сервісів виробника для обробки даних та дистанційного керування. Це переносить центр ризику з локального будинку на сервери компаній;

- вразливості API - API є мостом між пристроєм, мобільним додатком та хмарою. Недоліки в реалізації API можуть дозволити зловмисникам обійти автентифікацію та отримати доступ до облікових записів тисяч користувачів, зчитувати їхні дані або керувати їхніми будинками.

- інсайдерські загрози та несанкціонований доступ: згаданий інцидент з компанією Ring демонструє ризик, коли співробітники виробника або підрядники мають надмірні права доступу до приватних даних (відео/аудіо). Відсутність суворого аудиту доступу всередині компаній-виробників є критичною загрозою конфіденційності.

- взаємозалежність та ефект доміно: Сучасний розумний будинок часто є комбінацією пристроїв різних брендів, об'єднаних через платформи на кшталт Google Home, Apple HomeKit або IFTTT (If This Then That). Компрометація одного, навіть незначного сервісу, інтегрованого в екосистему, може ланцюговою реакцією призвести до компрометації всієї системи безпеки будинку.

1.1.3. Об'єкти дослідження

Для розробки комплексної основи захисту приватності в роботі виділено три найбільш репрезентативні категорії пристроїв:

- голосові асистенти: джерело ризику — постійний аудіомоніторинг та зберігання зразків голосу, що є біометричними даними.

- інтелектуальні термостати: агрегують дані про патерни присутності в домі та температурні вподобання, що дозволяє реконструювати розпорядок дня мешканців.

- розумні дверні дзвінки: здійснюють відеофіксацію не лише власника, а й третіх осіб, створюючи масиви візуальних даних про оточення.

Обрані категорії пристроїв демонструють високий рівень соціальної значущості — від інклюзивності (допомога людям з інвалідністю) до екологічної відповідальності (оптимізація енергоспоживання). Відтак, метою даного дослідження є не заперечення доцільності IoT, а розробка інтегрованої моделі захисту, що поєднує технічні інструменти (шифрування, локальна обробка даних) та політико-правові механізми регулювання.

1.2. Технологічні основи та еволюція систем віртуальних помічників

Еволюція голосових помічників є результатом тривалого прогресу в галузі обробки природної мови (NLP) та розпізнавання мовлення. Витоки цієї технології сягають першої чверті XX століття. Початковим етапом вважається поява у 1922 році іграшки «Radio Rex», що реагувала на акустичний сигнал власного імені. Подальший розвиток відбувався за наступними ключовими етапами:

- 1950-ті – 1960-ті рр.: лабораторії Bell у 1952 році представили систему «Audrey», здатну розпізнавати цифри. У 1961 році калькулятор IBM «Shoebox» розширив цей функціонал до 16 слів та 10 цифр. Важливою віхою стала розробка у MIT програми «ELIZA» (1960-ті рр.) — першого чат-бота, що імітував діалог шляхом шаблонізації та підстановки слів.

- 1970-ті – 1980-ті рр.: університет Карнегі-Меллон презентував систему «Harpy», словниковий запас якої сягав 1000 слів. Технологічний прорив стався завдяки впровадженню прихованих моделей Маркова (HMM), що дозволили перейти від простого пошуку шаблонів до ймовірнісного прогнозування звукових одиниць.

- сучасний етап (з 2011 р.): масове впровадження віртуальних асистентів розпочалося з релізу Apple Siri (2011), за яким послідували Amazon Alexa, Google Assistant та Microsoft Cortana. У 2015 році вихід Amazon Echo

інтегрував голосового помічника у форм-фактор «розумного динаміка», закріпивши його роль у побутовому середовищі.

Станом на 2025 рік глобальна кількість цифрових голосових помічників перевищила 4,6 мільярда одиниць. Прогнози вказують на те, що до кінця 2026 року загальна кількість таких пристроїв може перевищити чисельність населення планети. Сучасний етап розвитку характеризується переходом до архітектур великих мовних моделей (LLM), що дозволяє асистентам розуміти складні контексти та генерувати творчі відповіді.

Рисунок 1.2 – Класифікація віртуальних та цифрових помічників

Віртуальний або цифровий помічник визначається як програмний агент, здатний виконувати завдання на основі інтерпретації вхідних даних користувача. Для цілей систематизації доцільно виділити три основні класи систем:

1. Традиційні чат-боти (Rule-based systems) - дана категорія базується на текстових інтерфейсах та алгоритмах, заснованих на жорстких правилах.

Механізм роботи: Використання попередньо визначених дерев діалогу та пошук ключових слів.

Обмеження: Відсутність здатності до навчання та адаптації; неможливість обробки запитів поза межами запрограмованого сценарію. У разі виходу за межі алгоритму система переадресовує запит до оператора.

2. Інтелектуальні чат-боти (Conversational AI) - більш досконалі системи, що використовують методи машинного навчання (ML) та прогнозної аналітики для імітації природного людського спілкування.

Функціональні особливості: Здатність ідентифікувати намір користувача, аналізувати контекст попередніх взаємодій та надавати персоналізовані рекомендації.

Інтерфейс: Підтримка як текстового, так і голосового введення даних.

3. Голосові помічники та розумні динаміки - представляють собою вершину інтеграції штучного інтелекту, систем синтезу та розпізнавання мовлення.

Специфіка взаємодії: На відміну від чат-ботів, ці системи здатні підтримувати ітеративний діалог, уточнюючи параметри запиту до моменту отримання релевантного результату.

Апаратна інтеграція: У межах цього дослідження термін «голосовий помічник» вживається синонімічно до поняття «розумний динамік». Це підкреслює симбіоз програмного забезпечення та фізичного інтерфейсу.

Таблиця 1.1 - Порівняльна характеристика типів віртуальних асистентів

Критерій	**Традиційні чат-боти**	**Conversational AI**	**Голосові помічники**
Основа алгоритму	Дерево рішень (правила)	Машинне навчання (ML)	ML та нейронні мережі

Продовження таблиці 1.1

Контекстуальність	Відсутня	Висока	Максимальна

Спосіб введення	Текст	Текст / Голос	Переважно голос
Здатність до навчання	Ні	Так (на даних)	Так (безперервно)

Наведений розподіл дозволяє виокремити об’єкт дослідження — системи з переважно голосовим інтерфейсом, що інтегровані в домашню екосистему та володіють здатністю до предиктивного аналізу потреб користувача на основі великих масивів історичних даних.

1.3. Технологічні засади функціонування та архітектура голосових інтерфейсів користувача

Сучасні системи голосових асистентів базуються на використанні голосового інтерфейсу користувача (Voice User Interface, VUI), який забезпечує модальність взаємодії між людиною та комп’ютером за допомогою природної мови. VUI дозволяє реалізувати повний цикл двосторонньої комунікації, що включає акустичне сприйняття команд, їх семантичний аналіз, формування релевантної відповіді та її синтез у мовленнєву форму.

Архітектура функціонування VUI є комплексним процесом, який складається з кількох послідовних технологічних етапів, реалізованих за допомогою алгоритмів штучного інтелекту та обчислювальної лінгвістики:

1. Детекція акустичного тригера (Wake word detection).

Активація голосового асистента ініціюється виявленням специфічного ключового слова або фрази (наприклад, «Alexa», «Hey Siri», «Okay Google»). До моменту детекції тригера пристрій перебуває в режимі пасивного моніторингу акустичного оточення. Вхідний аудіосигнал проходить етап попередньої обробки, який включає цифрову фільтрацію фонових шумів (розмови, технічні звуки) та ехокомпенсацію за допомогою цифрових сигнальних процесорів (DSP). Лише після ідентифікації ключової фрази

система розпочинає запис корисного аудіосигналу та його передачу до хмарної інфраструктури або локального сервера для подальшого аналізу. Це забезпечує приватність користувача та запобігає помилковому виконанню команд із фонового мовлення.

Рисунок 1.3 - Архітектура функціонування VUI

2. Автоматичне розпізнавання мовлення (Automatic Speech Recognition, ASR).

Технологія ASR виконує перетворення акустичного сигналу (мовлення) у текстове представлення (Speech-to-Text, STT). Для досягнення високої точності транскрипції використовуються дві взаємодоповнюючі моделі:

- Акустична модель класифікує аудіосигнал та розбиває його на фони — мінімальні звукові одиниці мови.

- Лінгвістична модель використовує імовірнісні підходи для прогнозування найбільш вірогідної послідовності слів на основі отриманих

фонів. Це дозволяє диференціювати омофони (слова, що звучать однаково, але мають різне написання та значення, наприклад, «weather» та «whether») та коригувати помилки розпізнавання на основі контексту речення. Сучасні ASR-системи також використовують алгоритми адаптації до акцентів, тембру та інтонаційних особливостей голосу конкретного користувача.

3. Обробка природної мови (Natural Language Processing, NLP).

NLP є ядром VUI, що поєднує методи штучного інтелекту та обчислювальної лінгвістики для аналізу, розуміння та генерації мовлення. Процес NLP у VUI поділяється на два субпроцеси:

- розуміння природної мови (Natural Language Understanding, NLU): аналізує текст, отриманий від ASR, для визначення наміру (intent) користувача та виділення параметрів (slots/entities), необхідних для виконання команди (AI Base). NLU інтерпретує синтаксичну структуру, граматику та контекст. Наприклад, у фразі «встановити термостат на 21 градус», NLU ідентифікує намір (зміна температури) та параметри (об'єкт — термостат, значення — 21). Ідентифікація ключових слів дозволяє системі звертатися до відповідних прикладних програмних інтерфейсів (API).

- генерація природної мови (Natural Language Generation, NLG): відповідає за формування текстової відповіді на основі результатів виконання команди або необхідності уточнення запиту. Відповідь NLG має бути лінгвістично коректною та природною для сприйняття.

4. Менеджер діалогу та хмарна інтеграція.

Управління потоком розмови здійснюється менеджером діалогу, який координує взаємодію між NLU, NLG та зовнішніми ресурсами. Після розуміння команди система звертається до зовнішніх баз знань, хмарних сервісів або API для отримання інформації або виконання дій (Dialogue Manager). Підключення до Інтернету є критичним для більшості сучасних VUI, оскільки ресурсоємні обчислення ASR та NLP, а також доступ до динамічних даних (погода, новини) відбуваються у хмарі.

5. Синтез мовлення (Speech Synthesis).

Завершальним етапом є перетворення текстової відповіді, згенерованої NLG, в акустичний сигнал (Text-to-Speech, TTS). Сучасні TTS-системи використовують нейромережеві підходи (наприклад, WaveNet), що дозволяє генерувати високоякісне, природне мовлення з коректною просодією, інтонацією та наголосами, мінімізуючи ефект «роботизованого» голосу.

Доповнюючи технологічну архітектуру, слід виділити ключові функціональні особливості сучасних розумних динаміків, які базуються на VUI:

- персоналізація та машинне навчання. Системи VUI характеризуються здатністю до безперервного навчання на основі історичних даних взаємодії. Аналіз попередніх запитів та записаних аудіофайлів дозволяє алгоритмам адаптуватися до індивідуальних когнітивних та мовленнєвих моделей користувача, покращуючи точність розпізнавання намірів та контекстуальну релевантність відповідей.

- інтеграція в екосистему IoT. Розумні динаміки функціонують як центральні хаби для управління іншими пристроями IoT у межах розумного будинку. Завдяки підтримці стандартизованих протоколів зв'язку та API, VUI дозволяє оркеструвати роботу підключених пристроїв за допомогою єдиного голосового інтерфейсу, створюючи безперебійний користувацький досвід.

1.4 Висновки по розділу

У першому розділі було досліджено еволюцію концепції розумного будинку та визначено основні тенденції розвитку IoT-технологій у контексті глобальної цифровізації суспільства. Проведений аналіз показав, що інтеграція інтелектуальних пристроїв у повсякденне середовище користувачів супроводжується не лише підвищенням рівня автоматизації, але й суттєвим зростанням ризиків порушення конфіденційності даних.

Було встановлено, що найбільш критичними загрозами є несанкціонований доступ до персональної інформації, витоки даних через незахищені канали передачі та формування поведінкових профілів користувачів. У межах розділу також досліджено архітектурні та технологічні особливості систем віртуальних помічників і голосових інтерфейсів, які є одним із ключових джерел збору конфіденційної інформації в IoT-середовищі.

Отримані результати підтвердили необхідність розробки комплексних підходів до захисту приватності користувачів на рівні як програмного забезпечення, так і мережевої інфраструктури.

РОЗДІЛ 2. СИСТЕМНА АРХІТЕКТУРА, АЛГОРИТМІЧНІ МОДЕЛІ ТА РИЗИКИ ПРИВАТНОСТІ В ЕКОСИСТЕМАХ IoT

2.1. Апаратна архітектура та алгоритмічний потік даних у системах голосової взаємодії

Функціонування сучасних інтелектуальних асистентів базується на складній багаторівневій архітектурі, що поєднує локальну обробку сигналів та високопродуктивні хмарні обчислення. Взаємодія між цими компонентами визначає швидкість реакції системи та точність виконання команд.

Потік даних та інтеграція технологій для обробки вхідної інформації й генерації релевантних відповідей схематично представлені на рисунку 2.1.

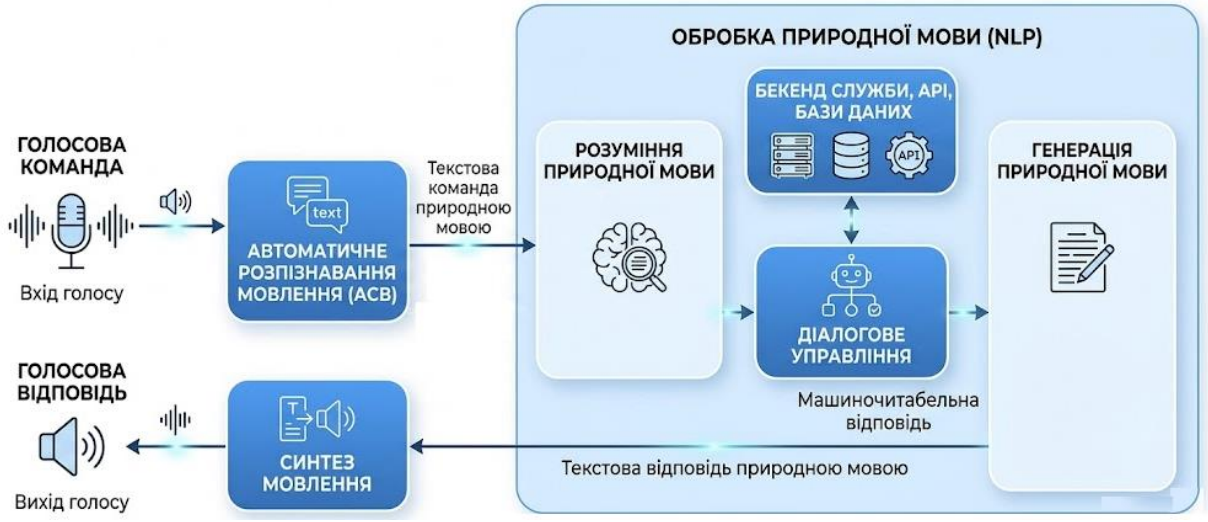

Рисунок 2.1 - Алгоритмічна модель потоку даних у системах голосового керування

Діаграма відображає послідовність трансформації акустичного сигналу в цифрові команди та зворотний процес синтезу відповіді. Стрілками вказано вектор спрямованості даних.

Нижче наведемо детальний опис ключових етапів згідно з логікою потоку даних:

1. Етап перцепції: вхід голосу та АСВ

Процес ініціюється голосовою командою. Акустичні хвилі фіксуються мікрофонами пристрою та передаються в модуль автоматичного розпізнавання мовлення (АСВ). На цьому етапі відбувається конвертація звукового сигналу в цифровий текст. Система відфільтровує шуми та, використовуючи акустичні й лінгвістичні моделі, формує текстову команду природною мовою.

2. Етап когнітивного аналізу: розуміння мови (NLU)

Текст надходить у блок обробки природної мови (NLP), де першочергову роль відіграє розуміння природної мови. Цей модуль виконує семантичний аналіз:

- визначає намір користувача (що саме потрібно зробити).

- виділяє сутності (конкретні параметри команди, наприклад, назву пісні або значення температури).

3. Етап операційного управління: Діалогове управління та бекенд

Діалогове управління виступає «диспетчером» системи. Воно приймає рішення про наступний крок на основі контексту розмови. Для виконання дії модуль звертається до бекенд служб, API та баз даних. Саме тут відбувається взаємодія з реальним світом: запит погоди, керування розумним будинком або пошук інформації в мережі. Результат виконання повертається у вигляді машиночитабельної відповіді.

4. Етап синтезу відповіді: NLG та вихід голосу

Машиночитабельні дані передаються в модуль генерації природної мови, який трансформує сухі факти у граматично правильну та природну для людини текстову відповідь.

Завершальним кроком є синтез мовлення (TTS), де текст перетворюється на аудіосигнал. Користувач отримує Голосову відповідь через динамік пристрою, що завершує комунікативний цикл.

Ключова особливість схеми полягає в тому, що вона демонструє перехід від «сирих» даних (звук) до абстрактних концепцій і назад до фізичного втілення (мова), що є фундаментальним принципом сучасного Conversational AI.

Конструктивні особливості та системна ієрархія пристроїв деталізовані в архітектурній схемі на рисунку 2.2.

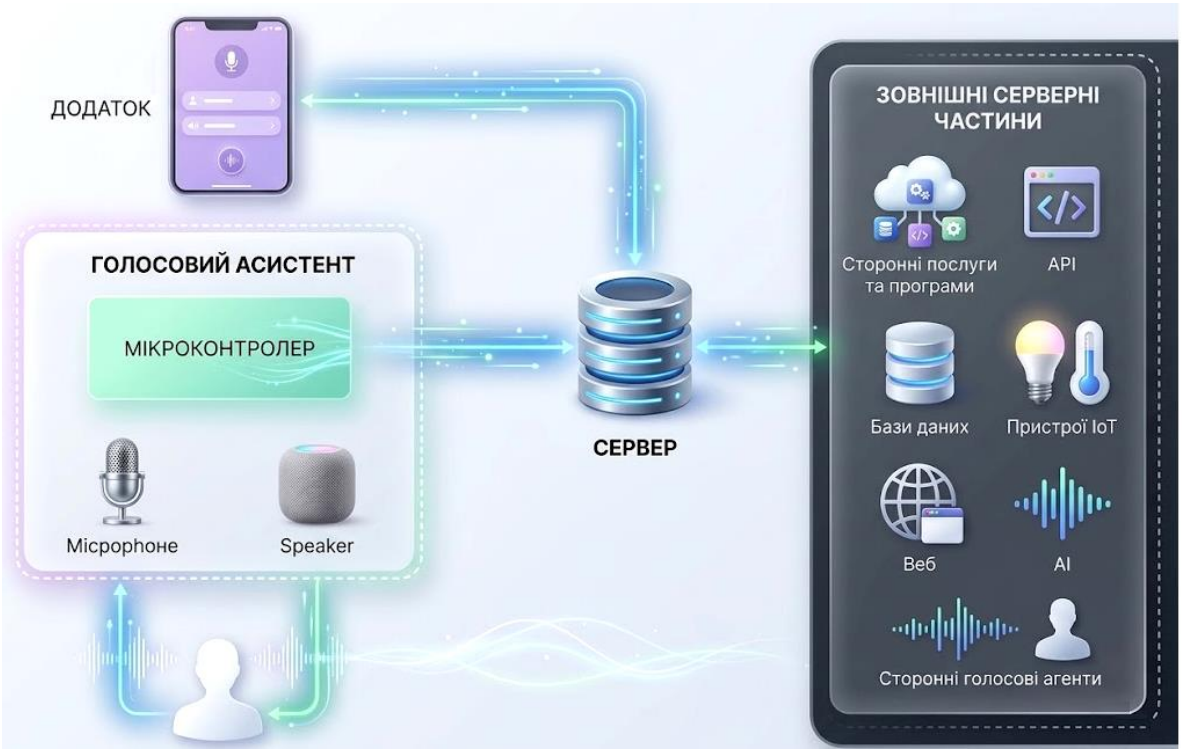

Рисунок 2.2 - Архітектурна діаграма типового розумного динаміка

Рисунок 2.2 ілюструє взаємозв'язок між апаратною частиною та серверною інфраструктурою. Як свідчать дані, наведені на рисунку 2.2 термінальний пристрій (розумний динамік) базується на мікроконтролері, що включає центральний процесор та локальний модуль пам'яті. Периферійна система складається з масиву мікрофонів для акустичної фіксації та динаміка для відтворення вихідного сигналу. Сучасні моделі можуть додатково оснащуватися сенсорними дисплеями для візуалізації інформації.

Процес взаємодії ініціюється локально: мікрофон записує звук, який проходить первинну стадію «очищення» та нормалізації. Оскільки локальні

обчислювальні потужності термінальних пристроїв обмежені, складні аналітичні операції переносяться у хмару.

Після локальної обробки цифровий запис передається на віддалений хмарний сервер. Тут реалізуються найбільш ресурсомісткі процеси:

- транскрипція та семантичний аналіз - використання технологій ASR (автоматичне розпізнавання мовлення) та NLP (обробка природної мови) для інтерпретації наміру користувача.

- зберігання даних - аудіозаписи архівуються в хмарних сховищах для подальшого навчання моделей машинного навчання.

- виконавчий менеджмент: Сервер ініціює програмні розширення, звертаючись до зовнішніх баз даних, API та веб-ресурсів (новинні агрегатори, метеослужби, IoT-платформи розумного будинку).

Генерація відповіді відбувається шляхом зворотного перетворення результату операції в природну мову за допомогою синтезу мовлення, після чого стиснений аудіопакет повертається на локальний пристрій для відтворення.

Додатковим рівнем управління виступає супутній мобільний або веб-додаток. Він виконує роль адміністративного інтерфейсу для конфігурації системи та може використовуватися як альтернативний канал комунікації. Зокрема, пристрій може підтримувати мультимодальне керування, коли параметри відтворення (наприклад, гучність або вибір контенту) регулюються паралельно через голосові команди та графічний інтерфейс смартфона.

2.2. Детермінанти конфіденційності та ризики безпеки в екосистемі інтелектуальних асистентів

Специфіка функціонування голосових помічників, що базується на постійному акустичному моніторингу, актуалізує критичні питання захисту приватності. Оскільки пристрій перебуває в стані очікування ключового слова

(«wake word»), він фактично здійснює безперервне прослуховування фонового середовища.

Ключові проблеми конфіденційності:

1. Обсяг та характер записів. Питання стосується частки аудіоінформації, яка обробляється та зберігається у періоди, коли користувач не звертається безпосередньо до асистента (ризик хибнопозитивних спрацювань).

2. Доступ третіх сторін. Існує невизначеність щодо суб'єктів, які мають право доступу до хмарних архівів записів, та цілей використання цих даних (маркетинговий аналіз, навчання ШІ або державний нагляд).

3. Вразливість до кіберзагроз: Несанкціонований доступ (злам) до голосового помічника дозволяє зловмисникам здійснювати дистанційне шпигунство всередині приватного приміщення.

4. Ескалація ризиків через інтеграцію. Оскільки асистенти часто інтегровані з критичними сервісами (інтернет-банкінг, системи безпеки, медичні реєстри), компрометація одного пристрою може призвести до системного витоку конфіденційної інформації або втрати контролю над іншими елементами Інтернету речей (IoT).

Таким чином, забезпечення безпеки в системах VUI вимагає впровадження методів локальної обробки даних та прозорих протоколів шифрування для мінімізації ризиків несанкціонованого втручання в приватну сферу.

2.3. Особливості керування базовими та програмними термостатами

Термостат визначається як контрольно-регулюючий пристрій, призначений для підтримки заданого температурного режиму в окремому приміщенні або групі приміщень шляхом керування виконавчим

обладнанням. У сучасному житловому будівництві системи терморегуляції класифікуються за рівнем технологічної складності та ступенем автоматизації процесів прийняття рішень.

Найпростіші (базові) термостати функціонують на основі механізмів зворотного зв'язку, що дозволяють підтримувати константне значення температури. Прилад детектує відхилення фактичних показників середовища від заданих користувачем і активує відповідні компоненти системи опалення, вентиляції та кондиціонування (HVAC), забезпечуючи циклічне нагрівання або охолодження повітря.

Програмні термостати представляють наступний етап розвитку, дозволяючи користувачеві встановлювати часові графіки роботи системи ОВК. Функціонування таких пристроїв ґрунтується на концепції температурного зниження: система утримує температуру під час активності мешканців та переходить у режим енергозбереження в період сну.

Проте критичним недоліком програмних систем є їхня статичність. Вони не здатні адаптуватися до непередбачуваних змін у графіку присутності людей. Як зазначають в [10], якщо мешканець повертається додому раніше встановленого графіка, система не змінить режим роботи автоматично, що вимагає ручного втручання для відновлення комфортних умов.

Інтеграція модулів бездротового зв'язку (Wi-Fi) трансформувала термостати в елементи мережевої інфраструктури. Користувачі отримали можливість дистанційної моніторингу та корекції налаштувань через цифрові інтерфейси (мобільні додатки), що забезпечує гнучкість управління незалежно від фізичного місцезнаходження суб'єкта.

Реактивні термостати, на відміну від програмних аналогів, оснащені сенсорною базою для детекції фактичної присутності мешканців. Це дозволяє системі ОВК реагувати на заповненість приміщень у реальному часі. Проте ефективність таких рішень обмежена інерційністю системи: нездатність до

миттєвої реакції на динамічні зміни в патернах присутності знижує потенціал енергозбереження.

Вершиною технологічного розвитку в даному сегменті є розумні термостати. Їхньою визначальною характеристикою є автономність та здатність до предиктивного моделювання. Окрім функцій дистанційного керування та реактивної детекції, ці пристрої володіють механізмами машинного навчання.

Основні функціональні переваги інтелектуальних термостатів включають:

- автономна оптимізація: пристрій самостійно координує роботу підсистем обігріву та охолодження для досягнення максимальної енергоефективності в різних зонах будинку.

- динамічне навчання: на основі агрегації даних про патерни присутності, тривалість перебування в приміщеннях та індивідуальні температурні уподобання, термостат формує адаптивну модель поведінки мешканців.

- предиктивне регулювання: система прогнозує необхідність зміни температурного режиму до моменту фактичного настання події, враховуючи час, необхідний для нагрівання/охолодження дому до цільового значення.

Таким чином, сучасний розумний термостат перетворюється з пасивного регулятора на активний агент управління мікрокліматом, який мінімізує енерговитрати, одночасно підвищуючи рівень комфорту за рахунок мінімізації необхідності мануального керування.

2.4. Функціонально-технологічна архітектура старт-систем терморегуляції

Інтелектуальні (розумні) термостати представляють собою еволюційний етап розвитку систем автоматизації житла, забезпечуючи більш швидке, точне

та цілеспрямоване коригування роботи систем опалення, вентиляції та кондиціонування (HVAC) порівняно з традиційними аналогами. Ключовою відмінністю таких пристроїв є здатність максимізувати енергоефективність без зниження рівня споживчого комфорту завдяки синергії сенсорних технологій та алгоритмів предиктивного аналізу.

Рисунок 2.3 – Функціональні елементи класифікації розумних термостатів

До основних функціональних елементів та технологічних рішень, що визначають інтелектуальність сучасних термостатів, належать:

1. Мультимодальне сенсорне детектування. Пристрої інтегрують технології виявлення екологічних змінних, включаючи температуру, вологість, рівень освітлення, концентрацію вуглекислого газу та акустичні сигнали. Особливе значення мають датчики руху, що надають дані про наявність мешканців у реальному часі, дозволяючи системі пріоритизувати економію енергії у порожніх приміщеннях. Використання дистанційних сенсорів у різних кімнатах нівелює похибки, спричинені особливостями

ізоляції або інсоляції окремих зон, забезпечуючи локальне коригування мікроклімату саме там, де знаходиться користувач. Сучасні системи дозволяють диференціювати типи руху, ігноруючи транзитні переміщення повз двері для уникнення хибних спрацювань.

2. Механізми глибокого зниження температури (Deep setbacks). На відміну від стандартних режимів, глибоке зниження температури дозволяє системі суттєво відхилятися від цільових показників у періоди тривалої відсутності мешканців. Рішення про ступінь зниження (або підвищення у спекотний період) приймається на основі прогнозних моделей повернення користувача, що забезпечує значну економію ресурсів.

3. Інтелектуальне планування та предиктивне нагрівання/охолодження. Розумне планування базується на аналізі поточних сенсорних даних, історичних патернів перебування людей та технічних характеристик потужності системи HVAC. Система обчислює оптимальний час для початку підготовки приміщення, варіюючи потужність та ефективність: за низької терміновості використовується режим високої ефективності, а при неочікуваному прибутті мешканців система переходить у режим максимальної потужності для швидкої компенсації температурної різниці. Прикладом реалізації таких функцій є технології Time-to-Temp та Early-On у пристроях Google Nest.

4. Геопросторовий моніторинг (Geofencing). Технологія передбачає створення віртуального периметра навколо об'єкта за допомогою GPS-сигналів смартфона користувача. Це дозволяє системі автоматично перемикатися між енергозберігаючим та комфортним режимами ще до фактичного входу людини в будинок. Точність геолокації (в межах 100–200 метрів) залежить від щільності покриття мережі та використання Wi-Fi або мобільних даних.

5. Дистанційний доступ та інтерактивна аналітика. Підключення до Wi-Fi забезпечує користувачу можливість моніторингу та корекції налаштувань

через мобільні або веб-додатки з будь-якої точки світу. Крім прямого керування, пристрої надають розгорнуту аналітику енергоспоживання та персоналізовані рекомендації щодо оптимізації витрат.

6. Участь у програмах реагування на попит (Demand-response). Завдяки дистанційному доступу розумні термостати стають елементами балансування енергомереж. Комунальні компанії можуть дистанційно коригувати налаштування пристроїв зареєстрованих споживачів у пікові періоди навантаження в обмін на знижені тарифи або інші стимули.

7. Машинне навчання та поведінковий аналіз. Пристрої безперервно акумулюють дані про температурні уподобання та графіки руху мешканців всередині будинку. Аналіз цих масивів дозволяє навчати моделі, які з часом повністю автоматизують процес управління кліматом, прогнозуючи потреби користувача без необхідності мануального програмування.

8. Системна IoT-інтеграція. Термостати інтегруються в загальну екосистему розумного будинку, що дозволяє реалізовувати голосове керування через інтелектуальні динаміки або використовувати розумне освітлення як додатковий індикатор присутності людей для більш точного коригування мікроклімату.

2.5. Архітектурна модель та апаратне забезпечення інтелектуальних систем терморегуляції

Системна архітектура сучасного розумного термостата являє собою інтегроване середовище, що поєднує обчислювальні модулі, сенсорні мережі та виконавчі інтерфейси. На рисунку 2.4 ілюструється типова архітектурна діаграма такої системи, що відображає ієрархію компонентів та напрямки інформаційних потоків.

Основним вузлом обробки даних у термостаті є мікроконтролер, який інтегрує центральний процесор, локальну пам'ять пристрою та системні

таймери. Ці компоненти забезпечують виконання програмних алгоритмів, обробку вхідних сигналів від сенсорів та генерацію команд для виконавчого обладнання. На відміну від традиційних пристроїв, локальна пам'ять розумного термостата використовується для тимчасової фіксації патернів поведінки до моменту їх синхронізації з сервером.

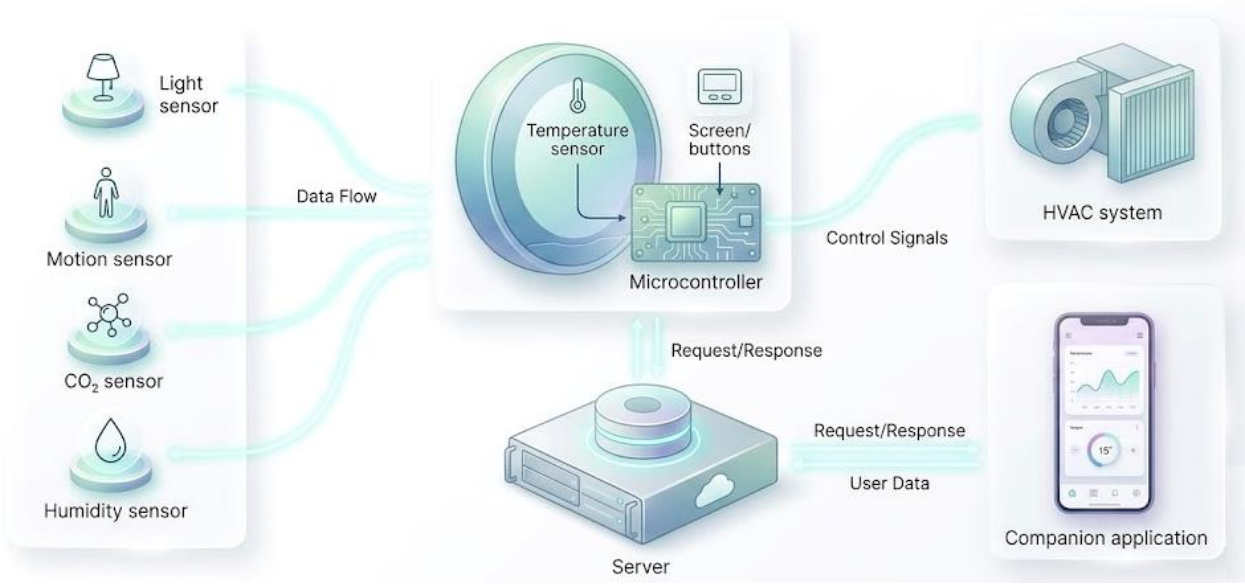

Рисунок 2.4 - Архітектурна діаграма типової системи розумного термостата. Стрілки вказують напрямок потоку даних.

Ефективність термостата безпосередньо залежить від точності та різноманітності вхідних даних:

- Інтегровані сенсори: Кожен пристрій оснащений вбудованим датчиком температури для моніторингу поточних показників середовища безпосередньо в місці монтажу.

- Зовнішні сенсорні модулі: Для створення комплексної моделі мікроклімату термостат може отримувати дані від віддалених датчиків вологості, концентрації CO_2 та освітленості.

- Детекція присутності: Ключову роль у реалізації енергоефективних сценаріїв відіграють датчики руху:

- Пасивні інфрачервоні (PIR): виявляють рух шляхом фіксації теплового випромінювання об'єктів.

- Мікрохвильові: використовують метод ехолокації, випромінюючи хвилі та фіксуючи зміну відстані до об'єктів.

- Подвійні (Dual-tech): комбінують PIR та мікрохвильову технології для мінімізації хибних спрацювань; активація відбувається лише за умови підтвердження руху обома сенсорами.

Взаємодія з термостатом реалізується через два основні канали:

- локальний інтерфейс: Вбудований дисплей, кнопки або сенсорні панелі, що дозволяють здійснювати мануальне регулювання та базове налаштування графіків. Наявність USB-порту в деяких моделях забезпечує можливість офлайн-діагностики або завантаження попередньо сконфігурованих профілів роботи.

- дистанційний інтерфейс: Мобільні або веб-додатки, що взаємодіють із термостатом через сервер. Ці інтерфейси забезпечують візуалізацію аналітичних даних, отримання сповіщень та віддалене керування параметрами системи ОВК (HVAC).

Мікроконтролер виступає активним регулятором системи HVAC. У разі виникнення дельти між поточною температурою та цільовим значенням (встановленим користувачем або визначеним алгоритмами машинного навчання), пристрій ініціює відповідний цикл обігріву або охолодження.

Усі зібрані дані — від температурних показників до графіків активності мешканців — передаються для зберігання у базу даних на локальному або віддаленому (хмарному) сервері. Хмарна інфраструктура дозволяє проводити складні обчислення, необхідні для прогнозування поведінки користувачів, та забезпечує синхронізацію налаштувань між різними інтерфейсами. Архітектурні відмінності між локальними та хмарними методами обробки даних у контексті безпеки будуть детально розглянуті у наступних розділах.

2.6. Технологічний аналіз та класифікація інтелектуальних систем контролю доступу на прикладі розумних дверних дзвінків

У сучасній архітектурі екосистем «розумного будинку» системи безпеки посідають пріоритетне місце, забезпечуючи користувачам можливість дистанційного моніторингу об’єктів у режимі реального часу. Комплексна безпека домогосподарства реалізується через інтеграцію різноманітних IoT-пристроїв, серед яких виділяються внутрішні та зовнішні камери відеоспостереження, інтелектуальні замки, адаптивне освітлення, а також спеціалізовані системи сигналізації. Розумні дверні дзвінки (Smart Doorbells) наразі є одним із найбільш затребуваних сегментів споживчої електроніки в категорії домашньої безпеки.

З технічної точки зору, розумний дверний дзвінок (або відеодзвінок) визначається як мережевий пристрій, що сповіщає власника про присутність відвідувача біля входу через активацію фізичної кнопки або спрацювання сенсорів наближення. За способом енергозабезпечення та монтажу пристрої класифікуються на дві основні категорії:

- дротові системи з живленням від мережі: Інтегруються безпосередньо в електричну мережу будівлі аналогічно до традиційних систем дзвінків. Основною перевагою є безперебійне енергопостачання, що усуває необхідність регулярної заміни акумуляторів і гарантує працездатність пристрою за умови стабільності електромережі.

- автономні бездротові системи: Функціонують на базі вбудованих акумуляторних батарей, що звільняє від необхідності прокладання кабелів. Це забезпечує високу гнучкість при виборі місця монтажу для досягнення оптимального кута огляду камери. Проте такі системи вимагають періодичної підзарядки або заміни елементів живлення, оскільки за їх розрядження пристрій повністю втрачає функціональність.

Для цілей даного дослідження технічне розмежування між дротовими та автономними пристроями не вважається принциповим, оскільки ключові інтелектуальні функції та алгоритми обробки даних є ідентичними для обох типів конструкцій.

Рисунок 2.5 – Технологічний стек розумного дверного дзвінка

Статус «інтелектуального» пристрою дверний дзвінок отримує завдяки синергії апаратних компонентів та програмних алгоритмів. Високий рівень безпеки та зручності експлуатації забезпечується наступним технологічним стеком:

1. Відеофіксація та моніторинг у реальному часі

Пристрої оснащуються камерами високої роздільної здатності, що дозволяють ідентифікувати об'єкт без фізичного контакту. Камери активуються за сигналом натискання кнопки або спрацювання датчиків руху. Сучасні системи надають функцію "Live View", що дозволяє ініціювати трансляцію в будь-який момент через супутній додаток. Обов'язковою умовою є наявність інфрачервоного підсвічування (нічного бачення) для отримання чіткого зображення в умовах низької освітленості.

2. Детекція руху та мультимодальне сенсування

Датчики руху дозволяють фіксувати активність біля входу навіть за відсутності прямої взаємодії відвідувача з пристроєм. Просунуті моделі підтримують налаштування «зон руху», що дозволяє ігнорувати активність на тротуарах або дорогах, фокусуючись лише на підходах до будинку.

- PIR-сенсори (Passive Infrared): Найпоширеніший тип датчиків, що реагує на теплові зміни. На відкритому просторі вони можуть давати хибні спрацювання через вітер або тварин.

- Мультимодальний підхід: Комбінування PIR-сенсорів із датчиками температури, освітленості та вологості дозволяє значно знизити рівень помилкових тривог.

3. Двосторонній аудіозв’язок

Наявність інтегрованих мікрофонів та динаміків забезпечує повнодуплексний зв’язок. Це дозволяє власнику дистанційно комунікувати з кур’єрами або відвідувачами, створюючи ефект присутності навіть за фізичної відсутності вдома.

4. Хмарна інфраструктура та зберігання даних

Для забезпечення можливості ретроспективного аналізу подій (наприклад, у разі вчинення правопорушень) аудіо- та відеоматеріали автоматично завантажуються в хмарне сховище через Wi-Fi з’єднання. Користувачі отримують доступ до «часової шкали подій», що структурує всі зафіксовані епізоди активності.

5. Глибокий аналіз відеопотоку та біометрична ідентифікація

Найбільш складним аспектом функціонування є інтелектуальна аналітика відео, яка включає розрізнення об’єктів (люди, тварини, транспорт, пакунки).

- Розпізнавання облич: Використовуються глибокі нейронні мережі для аналізу рис обличчя та їх порівняння з базою «знайомих» суб’єктів. Система

пропонує користувачеві маркувати відвідувачів, що дозволяє надалі отримувати персоналізовані сповіщення (наприклад, «Ваша дитина вдома»).

- Детекція життєздатності: Важливий компонент безпеки, що запобігає спробам обману системи за допомогою фотографій або масок. Може бути активним (вимагає від відвідувача виконання дії) або пасивним (аналіз текстур і мікрорухів шкіри алгоритмами глибинного навчання).

6. Системна інтеграція та інтероперабельність

Розумні дверні дзвінки виступають частиною гетерогенної мережі IoT. Інтеграція з розумними замками дозволяє реалізувати сценарій дистанційного відкриття дверей після візуального підтвердження особи. Також можлива автоматизація через голосові команди (Smart Speakers) або використання освітлення як візуального індикатора присутності відвідувача. Постійне машинне навчання на основі історичних даних дозволяє системі з часом адаптуватися до специфіки середовища та зменшувати кількість хибних тривог.

2.7. Системна архітектура та логіка функціонування інтелектуальних дверних дзвінків та ризики порушення приватності

Процес функціонування сучасної системи інтелектуального дверного дзвінка базується на складній багаторівневій архітектурі, що поєднує периферійні обчислення та централізовану хмарну обробку даних. Типова структурна схема такої системи представлена на рисунку 2.6, де відображено основні вузли та вектори інформаційного обміну.

Апаратна частина пристрою базується на мікроконтролері, який інтегрує центральний процесор, локальні модулі пам'яті та інтерфейси введення-виведення. Основне завдання мікроконтролера полягає в управлінні апаратними ресурсами та виконанні програмних інструкцій у реальному часі. До складу периферійних модулів входять:

- фізичний інтерфейс взаємодії - механічна або сенсорна кнопка виклику.

- мультимедійні модулі - інтегрований масив мікрофонів та динамік для реалізації двостороннього аудіозв'язку, а також оптичний сенсор (камера) для фото- та відеофіксації.

- логіка активації - пристрій переходить у активний режим або при фізичному натисканні кнопки, або за сигналом від детектора руху, що ініціює запис події та передачу метаданих.

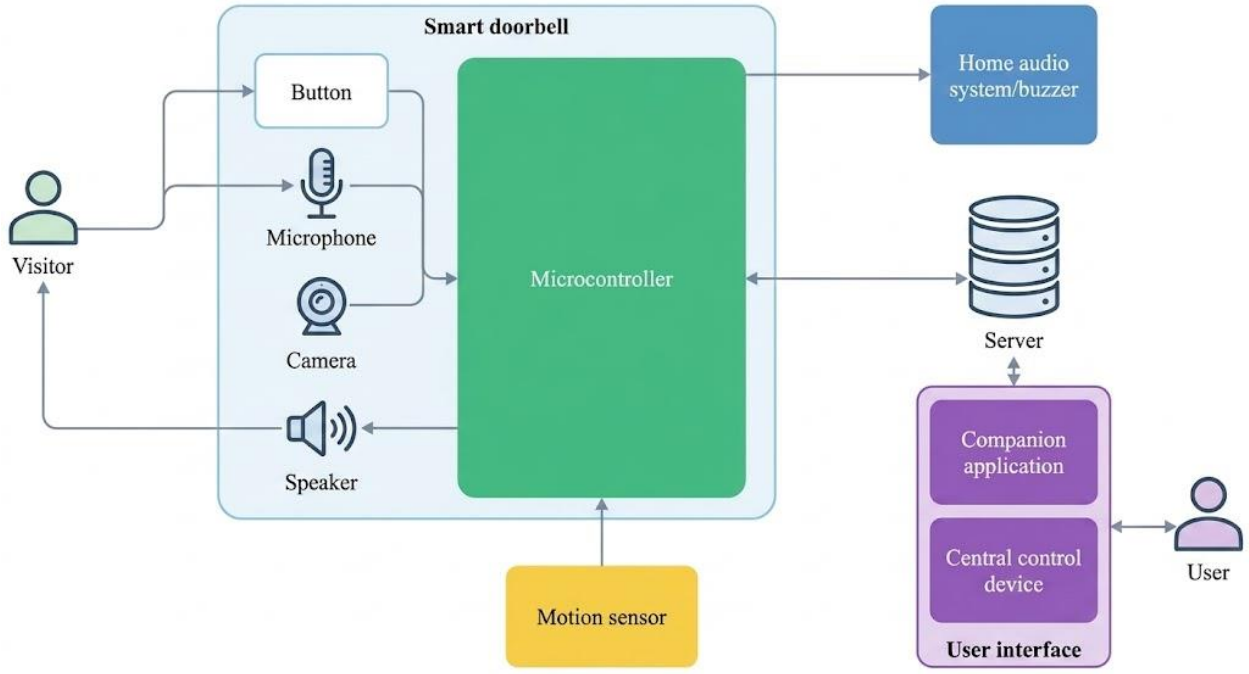

Рисунок 2.6 - Архітектурна діаграма типової системи інтелектуального дверного дзвінка

Зібрані медіадані та супровідні метадані передаються на сервер для подальшої інспекції. Виділяють два основні підходи до обробки відеопотоку: локальний та серверний. Використання зовнішніх серверів є технологічно виправданим, оскільки дозволяє застосовувати ресурсоємні алгоритми глибинного навчання для аналізу відео, які перевищують обчислювальні можливості стандартних мікроконтролерів. Серверна інфраструктура може бути реалізована як локально, так і за допомогою хмарних сервісів. Хмарні

рішення є найбільш поширеними завдяки їхній здатності масштабувати сховища для великих обсягів відеоданих.

Взаємодія кінцевого споживача з системою реалізується через супутні мобільні або веб-додатки. Після завершення серверної обробки система надсилає пуш-повідомлення або візуальні сповіщення на пристрій користувача. Основний функціонал інтерфейсу включає:

- моніторинг: перегляд прямих трансляцій та архівних записів безпосередньо з хмарного сховища.

- комунікація: передача аудіосигналу зі смартфона користувача через сервер до динаміка дверного дзвінка.

- навчання системи: маркування ідентифікованих облич для підвищення точності майбутнього розпізнавання.

Додатково система може комплектуватися внутрішньою станцією керування («базовим блоком»), оснащеною дисплеєм та аудіосистемою для використання всередині приміщення.

Інтелектуальні дверні дзвінки виступають інтегрованим елементом ширшої системи безпеки. Через серверні запити пристрій може взаємодіяти з розумними замками, освітленням та акустичними системами сповіщення, формуючи єдиний контур безпеки житла.

Широке впровадження систем відеофіксації доступу актуалізує низку проблем у сфері конфіденційності, що обумовлено специфікою експлуатації камер та мікрофонів у напівпублічному просторі.

Ключові вектори загроз приватності:

- несанкціонований доступ (злам): існує критичний ризик компрометації пристрою, що дозволяє зловмисникам вести дистанційне стеження за власниками будинку або перехожими.

- масштабний збір даних: постійна фіксація аудіо- та відеоматеріалів створює масиви даних, щодо яких виникають питання про терміни зберігання, методи використання та протоколи доступу третіх осіб.

- проблема відсутності згоди: Оскільки камери розташовані на зовнішньому фасаді будівлі, вони неминуче фіксують дії випадкових перехожих або сусідів. На відміну від мешканців будинку, ці суб'єкти не надавали згоди на обробку своїх біометричних даних, що створює правову колізію між правом на безпеку власника та правом на приватність оточуючих.

Рисунок 2.7 - Ключові вектори загроз приватності систем відео фіксації доступу

Враховуючи вищезазначене, інтелектуальні дверні дзвінки потребують не лише технічного вдосконалення, а й чіткого законодавчого регулювання щодо меж відеоспостереження та захисту зібраної персональної інформації.

2.8 Висновки по розділу

У другому розділі було виконано аналіз системної архітектури IoT-пристроїв, алгоритмічних моделей їх функціонування та основних ризиків

конфіденційності в екосистемах інтелектуальних асистентів. Дослідження показало, що сучасні IoT-системи характеризуються складною багаторівневою структурою обробки даних, у межах якої значна частина інформації передається до зовнішніх хмарних сервісів. Було встановлено, що інтелектуальні термостати та розумні дверні дзвінки здатні акумулювати значний обсяг персональних і поведінкових даних користувачів, що створює додаткові ризики для приватності.

Проведений аналіз дозволив ідентифікувати критичні точки потенційного витоку інформації, пов’язані з мережевою взаємодією, механізмами автентифікації та недостатнім рівнем локального захисту даних. У результаті було обґрунтовано необхідність використання багаторівневих механізмів захисту та адаптивних моделей контролю безпеки в IoT-інфраструктурі.

РОЗДІЛ 3. АНАЛІЗ ПАТЕРНІВ ЗБОРУ ДАНИХ ТА РИЗИКІВ ПРИВАТНОСТІ В СЕРЕДОВИЩІ IoT

У цьому розділі проводиться детальне дослідження проблем конфіденційності, притаманних експлуатації інтелектуальних голосових помічників, розумних термостатів та дверних відеодзвінків. Хоча кожна категорія пристроїв має специфічні вразливості, більшість виявлених проблем є репрезентативними для сегмента споживчого Інтернету речей (IoT) у цілому. Спершу здійснюється системний аналіз типів даних, що акумулюються кожним класом пристроїв, після чого розглядаються етико-правові та технічні проблеми приватності, які виникають у процесі обробки та використання цієї інформації.

3.1. Детермінація та джерела збору даних

Функціональна цілісність голосових асистентів, інтелектуальних термостатів та систем відеоспостереження базується на безперервному отриманні даних від користувачів та параметрів навколишнього середовища. Ці пристрої виступають у ролі активних «генераторів даних»: для реалізації заявлених автономних функцій вони потребують обробки колосальних масивів інформації. За оцінками International Data Corporation (IDC), до 2026 року пристрої IoT щорічно генеруватимуть майже 80 зеттабайт даних (1 зеттабайт = 10^{12} Гб).

Агрегація даних у розумних будинках здійснюється через три основні вектори:

1. Прямі вхідні дані: інформація, отримана під час безпосередньої взаємодії користувача з апаратною частиною (камери, сенсорні панелі).

2. Конфігураційні дані: параметри, що вводяться під час налаштування та реєстрації пристрою.

3. Синхронізовані дані: інформація з інтегрованих облікових записів, сторонніх додатків та периферійних пристроїв.

Нижче наведено розгорнутий опис специфічних типів даних для кожної з досліджуваних категорій пристроїв.

Рисунок 3.1 – Вектори агрегації даних в розумних будинках

3.1.1. Інтелектуальні голосові помічники

Голосові асистенти спеціалізуються на зборі акустичної інформації. Вони здійснюють перманентне зберігання голосових записів команд користувача та їхніх текстових транскрипцій. Окрім безпосереднього змісту запитів, системи екстрагують поведінкові інсайти з патернів взаємодії, аналізують типи сервісних запитів та подальшу активність у сторонніх екосистемах.

До переліку даних, що збираються під час взаємодії, належать:

- Медіаактивність: вподобання щодо музичного контенту, телевізійних шоу та підкастів.

- Комерційна активність: історія замовлень продуктів харчування, предметів одягу, програмного забезпечення та медикаментів через голосовий інтерфейс.

- Пошукова активність: звички веб-перегляду та тематика запитів, наданих помічнику.

- Приватна комунікація: зміст електронних листів, текстових повідомлень та інших форм зв'язку, включаючи фрагменти вербальних діалогів.

Фактично, будь-яка операція, що здійснюється за посередництвом пристрою, підлягає протоколюванню та аналізу. Крім того, пристрої можуть акумулювати біометричну інформацію, зокрема унікальні «голосові профілі» для ідентифікації конкретних мешканців. Системи також фіксують метадані записів: часові мітки, точну геолокацію та ідентифікатор активного мовця.

Процес налаштування пристрою ініціює збір ідентифікаційних даних (ім'я, вік, контакти), платіжної інформації та мережевих параметрів (IP-адреси, облікові дані Wi-Fi, діагностичні звіти). Важливим аспектом є збереження назв пристроїв у межах мережі (наприклад, «Alexa на кухні»), що дає змогу реконструювати структуру приміщень. Синхронізація з екосистемами (наприклад, Google Nest) надає помічнику доступ до всієї історії пошуку, файлів у хмарних сховищах, контактних листів та календарних планів користувача.

3.1.2. Розумні термостати

Основним джерелом даних для інтелектуальних термостатів є телеметрія від вбудованих та зовнішніх сенсорних мереж, а також мануальні налаштування користувача.

Екологічні дані, що підлягають моніторингу, включають:

- Внутрішню температуру та відносну вологість повітря.

- Рівень інсоляції (навколишнього світла).

- Концентрацію вуглекислого газу, задимленість та інші показники безпеки.

Датчики руху відіграють критичну роль у зборі даних про присутність людей та їхні цикли сну. Система фіксує графіки відбуття та прибуття мешканців, періоди активності та відпочинку. Використання датчиків у декількох кімнатах дозволяє аналізувати інтенсивність експлуатації окремих зон будинку.

Користувацькі вподобання фіксуються через кожне коригування температури в додатку або на пристрої. Кожна зміна супроводжується метаданими про точний час та місце операції. Ці масиви даних використовуються для навчання предиктивних моделей. Деякі виробники (наприклад, Google Nest) також можуть вимагати інформацію про план будинку для оптимізації регіонального енергоспоживання.

На етапі конфігурації збираються дані про HVAC-систему (опалення, вентиляція, кондиціонування), системні журнали та інформація про мережу. При активації геолокації термостат отримує можливість відстежувати переміщення користувача поза межами дому за допомогою GPS-сигналів смартфона. Хоча взаємодія мешканців із термостатом є менш інтенсивною, ніж із голосовим асистентом, обсяг поведінкових даних, які він збирає, залишається надзвичайно високим.

3.1.3. Розумні дверні дзвінки

Інтелектуальні дверні дзвінки агрегують інформацію з відеокамер, мікрофонів та датчиків наближення. Основна увага приділяється протоколюванню активності біля входу та медіафіксації подій.

Система реєструє:

- Кожен факт активації дзвінка.
- Фото- та відеоматеріали, згенеровані пристроєм.
- Акустичне тло в зоні дії пристрою.

Відеодані є найбільш репрезентативним джерелом інформації. Вони охоплюють не лише відвідувачів, а й сторонніх осіб та тварин у зоні досяжності сенсорів. Зокрема, пристрої Ring можуть виявляти рух у радіусі до 155 градусів по горизонталі, фіксуючи перехожих на вулиці, які не мають наміру взаємодіяти з домом. Мікрофони здатні записувати приватні розмови на відстані до 20 футів (~6 метрів).

Додаткові дані, що збираються через супутні додатки, включають:

- GPS-координати (за умови активації геолокації).

- Результати розпізнавання облич: імена, присвоєні користувачем, та відповідні біометричні відбитки.

- Аналітику взаємодії з контентом (наприклад, масштабування зображення на відеозаписі).

Платформи на кшталт Ring Neighbors збирають публікації користувачів про підозрілу активність, коментарі та метадані взаємодії з правоохоронними органами. Іноді компанії додатково пропонують створення «профілів екстреної реакції», де зберігаються такі чутливі атрибути, як вік, стать та гендерна ідентичність користувача.

3.2. Аналіз загроз конфіденційності та механізмів виведення похідних даних в екосистемі розумного будинку

Фундаментальною основою більшості проблем конфіденційності, що виникають внаслідок експлуатації інтелектуальних побутових пристроїв, є їхня тотальна залежність від безперервної генерації та обробки масивів великих даних. Традиційно житловий простір сприймається суб’єктом як іманентно приватна сфера, захищена від зовнішнього спостереження. Проте інтеграція IoT-технологій (Internet of Things), оснащених широким спектром сенсорів та підключених до глобальної мережі, фактично трансформує інтимні

аспекти життєдіяльності людини на структуровану інформацію, доступну для аналізу зовнішніми акторами.

Ключові занепокоєння щодо приватності в середовищі розумного будинку можна класифікувати за такими детермінантами:

- Семантичне наповнення даних: виявлення ступеня розкриття інформації, яку користувач прагне залишити в межах приватної сфери.

- Суб'єкти доступу: ідентифікація кола осіб та організацій (виробників, агрегаторів, правоохоронних органів), що мають фактичний або потенційний доступ до масивів даних.

- Телеологічний аспект: аналіз цілей, з якими використовується зібрана інформація (таргетування реклами, предиктивне моделювання).

- Ризики віктимізації: оцінка можливості використання даних проти суб'єкта (шантаж, дискримінація, фінансові втрати).

- Технічна цілісність: вразливість пристроїв до несанкціонованого втручання (хакінгу) з метою дистанційного спостереження.

Джерелом зазначених проблем є як комерційні стратегії компаній, спрямовані на монетизацію біхевіоральних даних, так і недостатній рівень кібербезпеки на етапах передачі та зберігання інформації. Оскільки ці загрози є спільними для різних категорій пристроїв, доцільно розглянути їх у межах єдиної аналітичної моделі.

Критичним аспектом порушення приватності є не лише первинний збір інформації, а й можливість її кореляції з даними третіх сторін. Процес аналітичного виведення дозволяє на основі фрагментарних відомостей реконструювати цілісну картину життя користувача, розкриваючи факти, які суб'єкт не мав наміру оприлюднювати. Оскільки дані генеруються безпосередньо в приватному просторі, отримані висновки мають високий ступінь персоналізації та достовірності.

Нижче наведено деталізовану типізацію висновків, які можуть бути сформовані на основі експлуатації конкретних пристроїв:

1. Голосові асистенти

Завдяки обробці природної мови та аналізу акустичних параметрів, ці пристрої дозволяють екстраполювати дані щодо:

- Фізіологічних характеристик: приблизний зріст, вага та загальний соматичний стан на основі тембральних особливостей голосу.

- Біхевіоральних та дієтологічних звичок: стиль життя (веганство) та харчові обмеження на основі аналізу замовлень та пошуку рецептур.

- Соціально-демографічного профілю: стать, раса, релігійна приналежність та сексуальна орієнтація.

- Медичного статусу: діагнози та стан здоров’я на основі аналізу медичної кореспонденції та специфічних пошукових запитів.

- Психографічних рис: особливості особистості та емоційний стан.

Яскравим прикладом предиктивного аналізу є виявлення вагітності користувача на основі запитів про вітаміни та симптоматику першого триместру. Подальша зміна характеру запитів (наприклад, пошук алкогольної продукції) дозволяє системі зробити висновок про зміну фізіологічного статусу. Крім того, метадані (часові мітки) у поєднанні з назвами пристроїв дозволяють точно мапувати щоденні ритуали: час прийняття душу або приготування їжі, що фактично веде до повної деанонімізації розпорядку дня.

2. Розумні термостати (Smart Thermostats)

Інтелектуальні системи клімат-контролю, попри обмежену функціональність, є потужним джерелом інформації про:

- Архітектоніку житла: детальне планування будинку на основі розташування датчиків та термостатів.

- Патерни активності та патології сну: аналіз руху в нічний час дозволяє виявити наявність інсомнії або інших розладів у мешканців.

- Професійну діяльність: за допомогою геолокації визначається місце регулярного перебування суб’єкта в робочий час, що дозволяє класифікувати його соціально-економічний статус.

- Фізіологічну сензитивність: кореляція внутрішніх температурних налаштувань із зовнішніми метеорологічними даними розкриває індивідуальну чутливість мешканців до тепла або холоду.

- Матеріальне становище: дані про енергоспоживання та рахунки за комунальні послуги слугують індикатором фінансового добробуту.

3. Розумні дверні дзвінки (Smart Doorbells)

Дана категорія пристроїв розширює сферу спостереження на напівпублічний простір, збираючи дані про третіх осіб:

- Поведінковий моніторинг оточення: на основі відеофіксації та розпізнавання облич система може реконструювати графік пересування сусідів (наприклад, регулярні пробіжки).

- Культурна та релігійна ідентифікація: аналіз візуальних атрибутів дозволяє зробити висновки про конфесійну приналежність власника.

- Семантичний аналіз розмов: фіксація та інтерпретація діалогів із відвідувачами надає інформацію, аналогічну тій, що збирають голосові асистенти.

Наведені приклади демонструють, що розумні домашні пристрої функціонують як інструменти глибокого профілювання, де поєднання первинних даних із алгоритмами машинного навчання призводить до ерозії приватності, часто без усвідомленої згоди суб’єкта. Подальший аналіз у роботі буде зосереджений на механізмах правового та технічного захисту від зазначених загроз.

3.3. Технічні стратегії та методи забезпечення конфіденційності в системах розумного будинку

Після детальної класифікації та верифікації фундаментальних проблем приватності, що виникають внаслідок експлуатації інтелектуальних побутових пристроїв, критично важливим є розгляд комплексу технічних

рішень, спрямованих на нейтралізацію зазначених ризиків. У даному розділі пропонується концептуальна рамкова основа технічних методів захисту, які згруповані за трьома стратегічними векторами:

1. Мінімізація та оптимізація обсягів збору даних;

2. Посилення протоколів захисту даних з метою нівелювання ризиків, пов'язаних із їх передачею, обробкою та запобіганням несанкціонованому доступу;

3. Підвищення системної стійкості (безпеки) самих пристроїв.

Структурування технічних пропозицій здійснюється у відповідності до раніше визначеної класифікації проблем конфіденційності. Це дозволяє сформувати цілісну рамкову основу, де кожна вразливість корелює з конкретним технологічним рішенням. Слід зауважити, що запропоновані методи можуть мати комплексний характер і вирішувати одночасно кілька видів ризиків. Як було обґрунтовано в попередніх розділах, першопричиною більшості загроз приватності є генерація та експлуатація надлишкових масивів інформації. Повну відмову від збору даних слід вважати нераціональною, оскільки це унеможливлює функціонування інтелектуальних систем за їх прямим призначенням.

Проте суттєве зменшення обсягів інформації, що передається на зовнішні сервери компаній-виробників, без критичної втрати точності роботи пристрою, дозволяє радикально знизити імовірність порушення конфіденційності. У цьому контексті під «зібраними даними» ми розуміємо виключно інформацію, що виходить за межі локального периметра пристрою користувача. Для реалізації цієї стратегії доцільно впровадити наступні методологічні підходи.

3.3.1. Принцип мінімізації даних

Мінімізація даних — це фундаментальна практика проектування систем, яка передбачає обмеження збору інформації виключно тими обсягами, що є критично необхідними для виконання конкретної транзакції або функції.

Ця методологія базується на принципі гранулярності доступу до даних залежно від складності запиту. Наприклад, технологія Siri від компанії Apple реалізує цей принцип через адаптивний підхід до геолокації («Improving Siri»):

- При запиті загального характеру (наприклад, щодо результатів спортивних подій) система використовує лише агреговані, низькодеталізовані дані про місцезнаходження.

- Прецизійні координати залучаються виключно в ситуаціях, що вимагають високої точності (наприклад, розрахунок дистанції до конкретного географічного об'єкта).

Аналогічний підхід має застосовуватися в усіх аспектах взаємодії з VUI (голосовими інтерфейсами). Так, функція «читання вголос» на персональному комп'ютері не повинна ініціювати передачу всього масиву текстових повідомлень на хмарний сервер; інтелектуальний агент має віддавати команду локальному модулю синтезу мовлення, зберігаючи зміст повідомлення всередині локальної пам'яті пристрою.

3.3.2. Використання синтетичних даних

Розвиток генеративного штучного інтелекту відкриває перспективи використання синтетичних наборів даних як ефективного інструменту захисту ідентичності. Моделі ШІ здатні аналізувати реальні ідентифіковані масиви інформації для генерації штучних точок даних, які є статистично ідентичними реальним, проте позбавлені будь-якого зв'язку з конкретними фізичними особами (Hern, “‘Anonymised’ data”).

Впровадження цієї технології дозволяє компаніям навчати свої алгоритми на синтетичних копіях, що зберігають усі необхідні патерни поведінки без ризику деанонімізації користувачів. Реальні персональні дані

при такому підході використовуються лише короткочасно для навчання генеративної моделі, після чого підлягають гарантованому знищенню. Це дозволяє радикально зменшити обсяг «чутливої» інформації, що зберігається в довгостроковій перспективі.

3.3.3. Технологія федеративного навчання

Однією з головних дилем у проектуванні приватних IoT-систем є необхідність навчання алгоритмів на великих масивах даних для забезпечення високої якості персоналізації. Традиційна модель передбачає агрегацію даних тисяч користувачів на центральному сервері, що створює значні ризики масових витоків інформації.

Рішенням цієї проблеми є федеративне навчання — метод децентралізованого машинного навчання, що дозволяє пристроям вдосконалювати свої моделі локально, без передачі сирих даних на зовнішні сервери.

Механізм функціонування федеративного навчання передбачає наступні етапи:

- Локальна копія моделі навчається безпосередньо на пристрої користувача, використовуючи локальні дані (наприклад, зразки голосу).

- Замість самих даних у хмару або на центральний сервер надсилаються лише оновлені параметри моделі (градієнти/ваги).

- На сервері відбувається агрегація цих параметрів від багатьох користувачів у «головну модель», яка згодом розсилається назад на всі пристрої.

Apple та Google активно впроваджують цей підхід для вдосконалення голосових асистентів. Зокрема, розпізнавання фрази-тригера («Hey Siri» або «Hey Google») вимагає ідентифікації специфічного голосу власника, щоб уникнути хибних спрацювань на пристроях сторонніх осіб. Завдяки федеративному навчанню ці складні моделі розпізнавання стають точнішими

з кожною взаємодією, проте самі записи голосу ніколи не залишають пам'яті смартфона чи розумного динаміка, що нівелює ризики їх несанкціонованого використання.

3.4. Синтез технологічних можливостей та викликів конфіденційності в середовищі IoT

Дослідження систем домашньої автоматизації на прикладі голосових помічників, розумних термостатів та дверних відеодзвінків дозволяє виявити фундаментальні принципи функціонування споживчого Інтернету речей. Ключові технологічні компоненти, такі як автоматичне розпізнавання мовлення, обробка природної мови, предиктивне виявлення руху, геозонування та біометрична аналітика відеопотоку, у поєднанні з хмарними обчисленнями та високошвидкісним бездротовим зв'язком, забезпечують якісно новий рівень побутового комфорту та енергоефективності.

Проте функціонування зазначених алгоритмів нерозривно пов'язане з генерацією та обробкою критичних обсягів персональної інформації. Дані перебувають у стані постійної циркуляції між фізичними датчиками, мікроконтролерами, віддаленими хмарними серверами та додатками сторонніх розробників. Ця безперервна передача даних створює розгалужену цифрову архітектуру, де кожна ланка ланцюга є потенційним джерелом витоку конфіденційної інформації.

3.4.1. Таксономія та критичний аналіз загроз конфіденційності

Інтелектуальні домашні пристрої виступають інструментами тотального збору даних, що охоплюють акустичні, візуальні та поведінкові аспекти життя суб'єкта. Агрегація інформації здійснюється через мультимодальні джерела: камери, мікрофони, сенсорні мережі, історію взаємодій та інтегровані облікові записи сторонніх сервісів.

На основі аналізу зібраних масивів даних виділено наступні категорії ризиків:

- аналітичне виведення (Data Inference): можливість формування детальних психологічних та біографічних профілів на основі кореляції фрагментарних даних із зовнішніми джерелами.

- інвазивний маркетинг: використання гіперлокальних та поведінкових даних для створення агресивної таргетованої реклами.

- несанкціонована дифузія даних: поширення конфіденційної інформації третім сторонам та суб'єктам, згода на взаємодію з якими не була явно виражена користувачем.

- державний нагляд та дискримінація: потенційна можливість використання домашніх мереж IoT для тотального моніторингу та соціального інжинірингу.

- кіберзлочинність: вразливість централізованих баз даних до зламів, що робить користувачів об'єктами шантажу, переслідування або фізичних крадіжок.

- ерозія права власності на дані: поступова втрата користувачем контролю над власною цифровою ідентичністю після етапу первинного збору даних.

3.4.2. Концептуальний фреймворк технічних методів мінімізації ризиків

Встановлено, що забезпечення приватності та функціонування розумних пристроїв не є взаємовиключними поняттями. Впровадження принципів Privacy by Design (PbD) дозволяє інтегрувати захисні механізми безпосередньо в архітектуру системи.

Запропоновані стратегії захисту класифіковано за трьома основними напрямами:

1. Оптимізація та редукція збору інформації

Метою цих методів є збереження точності прогнозних моделей при радикальному зменшенні обсягу переданих даних:

- Мінімізація даних: впровадження суворих лімітів на збір лише тієї інформації, що є іманентно необхідною для поточної операції.

- Генерація синтетичних даних: використання штучних наборів даних для навчання моделей, що дозволяє уникнути зберігання реальних біометричних або поведінкових відбитків користувачів.

- Федеративне навчання: децентралізований підхід, за якого навчання моделей відбувається локально на пристроях користувачів, а на центральний сервер передаються лише оновлені параметри (ваги) моделі, а не вихідні дані.

Рисунок 3.2 – Стратегії концептуального фреймворку мінімізації ризиків в середовищі IoT

2. Посилення безпеки обробки та зберігання масивів даних

Ці заходи спрямовані на захист інформації в процесі її життєвого циклу:

- Криптографічний захист: використання наскрізного шифрування (E2EE) та перспективних методів шифрування даних безпосередньо під час їхньої обробки.

- Диференціальна приватність: математичний метод додавання статистичного «шуму» до наборів даних, що унеможливлює ідентифікацію конкретного суб'єкта навіть за умови доступу до бази даних.

- Периферійні обчислення: перенесення процесів аналізу та зберігання інформації з хмарних серверів безпосередньо на локальний пристрій користувача.

3. Підвищення апаратної та системної стійкості

Забезпечення автономності пристроїв є ключовим фактором безпеки:

- Офлайн-обробка: реалізація критичних функцій (наприклад, розпізнавання ключових слів голосовим асистентом) без підключення до мережі Інтернет для зменшення поверхні кібератак.

- гібридні системи захисту: комбінування асиметричного шифрування з використанням симетричних ключів, що зберігаються в апаратно захищених модулях безпосередньо на пристрої.

Комплексне впровадження зазначених методів дозволяє створити захищену екосистему, де технологічний прогрес не стає інструментом порушення базових прав людини на приватність.

3.5 Висновки по розділу

У третьому розділі здійснено комплексний аналіз патернів збору даних та ризиків порушення приватності у середовищі Internet of Things. У ході дослідження було визначено основні джерела формування даних у системах розумного будинку та встановлено, що навіть непрямі телеметричні показники можуть використовуватись для формування детальних поведінкових профілів користувачів.

Аналіз загроз конфіденційності підтвердив, що сучасні IoT-системи потребують впровадження спеціалізованих механізмів мінімізації ризиків, спрямованих на обмеження обсягів збору та передачі персональної інформації. У межах розділу було досліджено принцип мінімізації даних, використання синтетичних даних та технологію федеративного навчання як перспективні підходи до забезпечення приватності.

На основі проведеного аналізу сформовано концептуальний фреймворк технічних методів захисту, який поєднує криптографічні механізми, локальну обробку даних та технології диференціальної приватності.

РОЗДІЛ 4. ПРОГРАМНА РЕАЛІЗАЦІЯ ПРОТОТИПУ СИСТЕМИ ЗАХИСТУ ПРИВАТНОСТІ КОРИСТУВАЧІВ У СЕРЕДОВИЩІ IoT

4.1. Розробка ієрархічної архітектури системи

На рисунку 4.1 подано багаторівневу ієрархічну архітектуру програмно-апаратної системи «IoT Safeguard», призначеної для комплексного забезпечення конфіденційності, цілісності та доступності даних у середовищі Інтернету речей (IoT). Структура системи побудована за принципом потокової обробки інформації в напрямку від джерел (сенсорів) до термінальних вузлів (хмарних сервісів), з послідовним застосуванням механізмів захисту та аналізу.

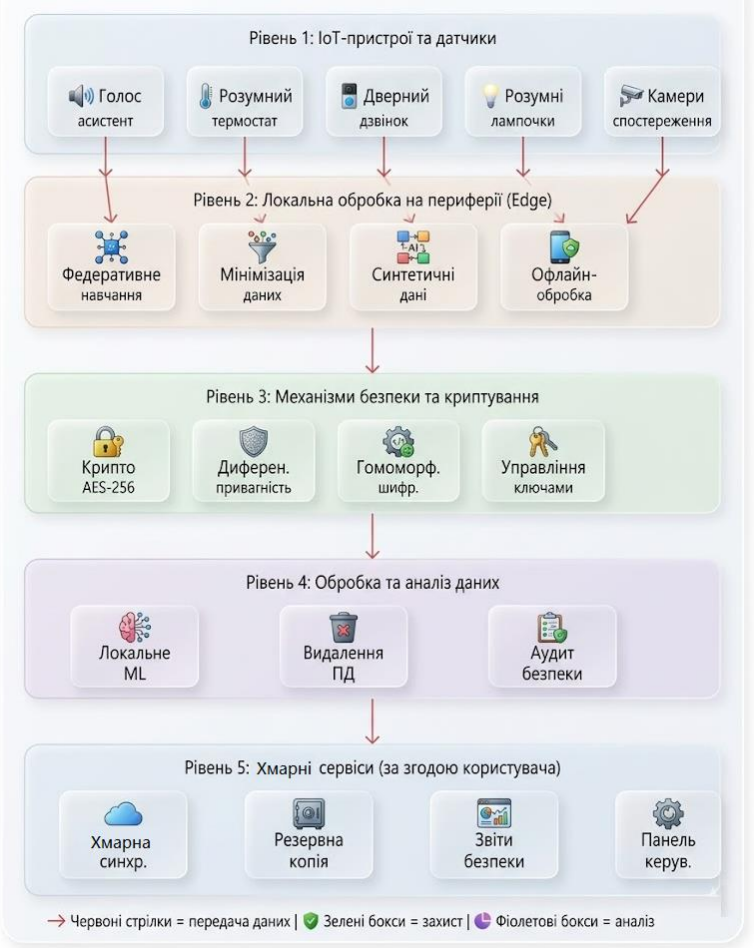

Рисунок 4.1 - Багаторівнева ієрархічна архітектура

Відповідно до легенди схеми, функціональні компоненти диференційовані за колірним кодуванням: зелений колір ідентифікує механізми активного захисту та безпеки; фіолетовий — аналітичні інструменти; червоні вектори вказують на напрямок передачі даних між рівнями.

Архітектура системи дихотомізується на п'ять функціональних рівнів:

Рівень 1. IoT-пристрої та датчики (Рівень генерації первинних даних)

Цей рівень є фізичним базисом системи, де розташовані гетерогенні пристрої IoT (мультимедійні, побутові, безпекові сенсори тощо). Вони виступають ініціаторами інформаційних потоків. Потоки даних з голосових асистентів, смарт-термостатів, відеодзвінків, смарт-лампочок та камер спостереження транзитуються на наступний етап для первинної обробки.

Рівень 2. Локальна обробка на периферії (Edge) (Рівень превентивного захисту)

Реалізує парадигму периферійних обчислень з метою мінімізації латентності та зниження обсягів передачі даних у зовнішні мережі. Тут застосовуються методи федеративного навчання для розподіленого тренування моделей ML без деанонімізації вихідних даних, алгоритми мінімізації даних (агрегація, фільтрація надлишкової інформації) та генерації синтетичних даних для моделювання без ризику витоку реальних ПД. Також передбачено механізм офлайн-обробки для автономної роботи пристроїв.

Рівень 3. Механізми безпеки та криптування (Криптографічний рівень)

Це центральний рівень технічного захисту інформації (всі блоки зелені). На ньому реалізовано симетричне шифрування за стандартом AES-256, методи диференційної приватності для додавання статистичного шуму до наборів даних, та перспективне гомоморфне шифрування, що дозволяє виконувати математичні операції над зашифрованими даними без їх декриптування. Функціонування цього рівня забезпечується системою управління ключами.

Рівень 4. Обробка та аналіз даних (Аналітичний рівень)

Призначений для семантичної обробки та аудиту вже захищеної інформації. Тут функціонують моделі локального машинного навчання для прийняття автономних рішень, процеси гарантованого видалення персональних даних (ПД) згідно з регламентами (наприклад, GDPR) та інструменти аудиту безпеки для моніторингу цілісності самої системи захисту.

Рівень 5: Хмарні сервіси (Термінальний рівень)

Цей рівень є факультативним і задіюється виключно на підставі преференцій та явної згоди користувача. Він забезпечує розширений функціонал: хмарну синхронізацію для доступу до даних з будь-якої точки, резервне копіювання для відновлення після збоїв, генерацію звітів безпеки та надає панель керування (GUI/Dashboard) для адміністрування системи.

Загалом, представлена архітектура демонструє ешелонований підхід до захисту IoT-інфраструктури, поєднуючи сучасні криптографічні методи, периферійні обчислення та локальну аналітику для створення довіреного середовища обробки даних.

4.2. Архітектура та функціональні можливості користувацького інтерфейсу системи «IoT Safeguard»

Програмна реалізація концептуального фреймворку захисту відображена у графічному інтерфейсі головної сторінки, що представлений на рисунку 4.2. Інтерфейс спроектований із дотриманням принципів ергономіки та візуалізації великих масивів даних, що дозволяє користувачеві здійснювати оперативний моніторинг стану безпеки домашньої мережі IoT.

Верхня панель навігації містить:

- Логотип та назву системи
- Меню розділів (Головна, Аналіз загроз, Пристрої, Захист, Профіль)
- Статус захисту системи в реальному часі

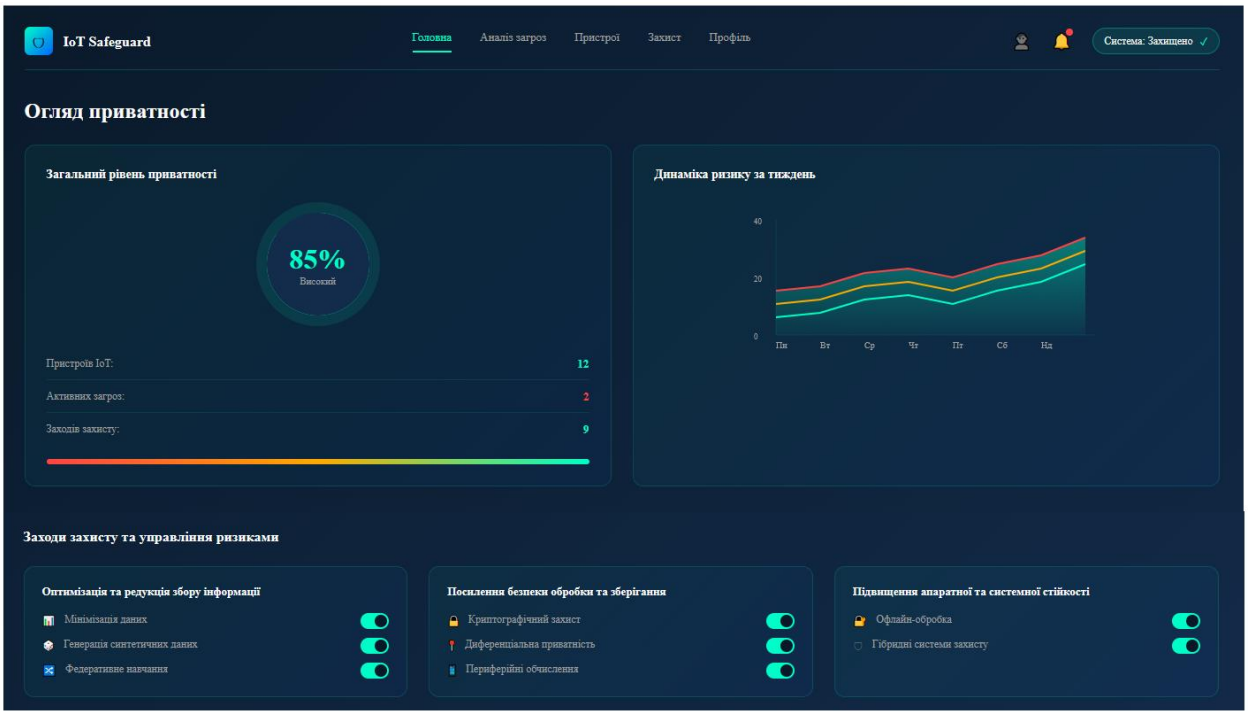

Рисунок 4.2 - Користувацький інтерфейс головної сторінки системи управління приватністю «IoT Safeguard».

4.2.1. Аналітична панель «Огляд приватності»

Верхній сегмент інтерфейсу присвячений візуалізації ключових показників ефективності (KPI) системи безпеки. Він розділений на два основні інформаційні блоки:

- Моніторинг загального рівня захищеності: ліва панель містить кільцеву діаграму, що відображає інтегральний показник «Загального рівня приватності», який наразі становить 85%, що класифікується системою як «Високий». Нижче наведені кількісні метрики поточної інфраструктури: загальна кількість підключених IoT-пристроїв (12), зафіксовані активні загрози (2) та активовані заходи захисту (9).

- Часова динаміка ризиків: права панель представляє лінійний графік «Динаміки ризику за тиждень», що відображає коливання рівня загроз у часовому розрізі. Використання мультилінійного графіка дозволяє

диференціювати різні вектори атак або категорії вразливостей, забезпечуючи предиктивний аналіз безпекового середовища.

4.2.2. Панель управління «Заходи захисту та управління ризиками»

Нижній сегмент інтерфейсу забезпечує контроль над технічними методами мінімізації ризиків. Функціональні елементи згруповані у три логічні кластери, кожен з яких оснащений індивідуальними перемикачами для активації відповідних протоколів:

- Оптимізація та редукція збору інформації: включає інструменти для мінімізації даних, генерації синтетичних наборів та активації федеративного навчання, що дозволяє навчати моделі без передачі вихідних даних на сервер.

- Посилення безпеки обробки та зберігання: надає можливість управління захистом, впровадження методів диференціальної приватності та переведення обчислень у периферійний режим.

- Підвищення апаратної та системної стійкості: дозволяє перемикати пристрої в режим офлайн-обробки для критичних функцій та активувати гібридні системи захисту, що поєднують різні рівні шифрування та апаратної ізоляції ключових вузлів.

Дизайн інтерфейсу виконано у темній кольоровій гамі, що мінімізує зорове навантаження та акцентує увагу на критичних елементах (індикаторах загроз та статусі захисту). Стан системи дублюється у верхньому правому куті статусним повідомленням «Система: Захищено», що підтверджує цілісність усіх активних периметрів безпеки.

4.3. Модуль моніторингу та управління вузлами IoT-мережі. Інтерфейс вкладки «Пристрої»

Вкладка «Пристрої» в системі «IoT Safeguard» є централізованою консоллю для адміністрування інвентаризаційного переліку підключеного

обладнання. Інтерфейс забезпечує багаторівневий моніторинг стану кожного вузла мережі, поєднуючи технічну телеметрію з показниками безпеки та конфіденційності (рис. 4.3).

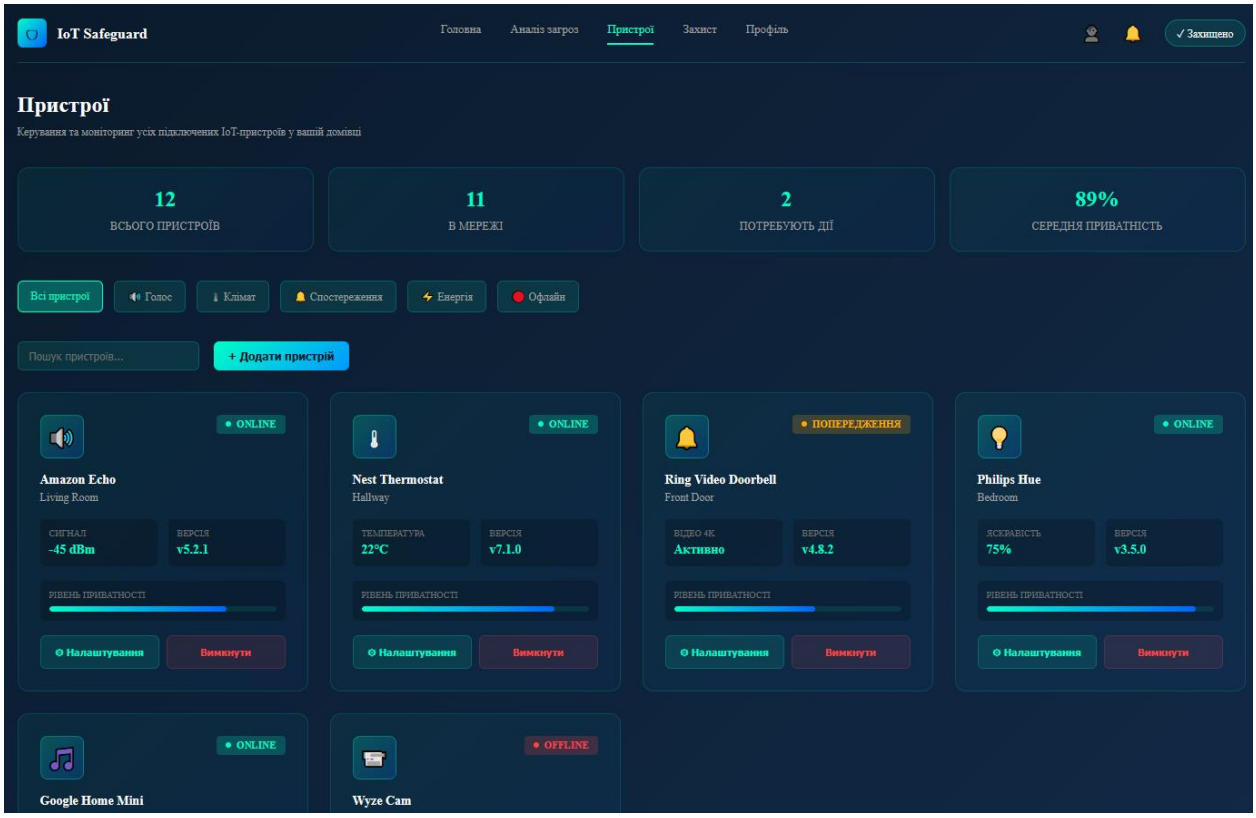

Рисунок 4.3 - Інтерфейс вкладки «Пристрої»

4.3.1. Агреговані статистичні метрики

Верхня панель вкладки представляє зведені дані про стан екосистеми у форматі чотирьох інформаційних блоків:

- Інвентаризаційний кількісний показник: зафіксовано 12 пристроїв у межах домашньої мережі.

- Статус підключення: 11 одиниць обладнання перебувають у стані активного з'єднання («В мережі»).

- Оперативне реагування: ідентифіковано 2 вузли, що потребують уваги адміністратора («Потребують дії»).

- Середній індекс конфіденційності: інтегральний показник захищеності всієї мережі становить 89%, що корелює з раніше описаним загальним рівнем приватності.

4.3.2. Система фільтрації та управління інфраструктурою

Для оптимізації взаємодії з гетерогенним середовищем IoT впроваджено систему тегів та категорій:

- Класифікація пристроїв: швидкий доступ за функціональним призначенням — «Голос» (Amazon Echo), «Клімат» (Nest Thermostat), «Спостереження» (Ring Video Doorbell), «Енергія» (Philips Hue) та «Офлайн».

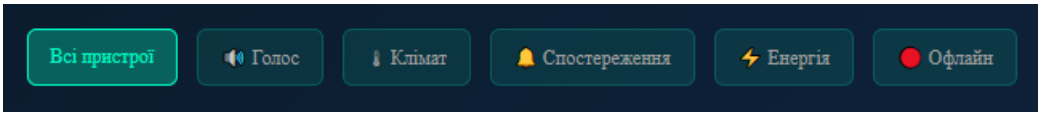

Рисунок 4.4 – Меню швидкого доступу до пристроїв

Інструменти пошуку та масштабування: передбачено поле для контекстного пошуку пристроїв за назвою та кнопку «Додати пристрій» для розширення мережі.

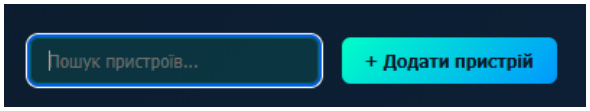

Рисунок 4.5 – Меню пошуку і додавання нового пристрою

4.3.3. Деталізація термінальних пристроїв

Графічна візуалізація окремих вузлів реалізована через інтерактивні картки, що містять вичерпну технічну та безпекову інформацію:

- Ідентифікація та локація: вказано тип пристрою, його комерційну назву та місцезнаходження в будівлі (наприклад, Living Room, Hallway, Front Door).

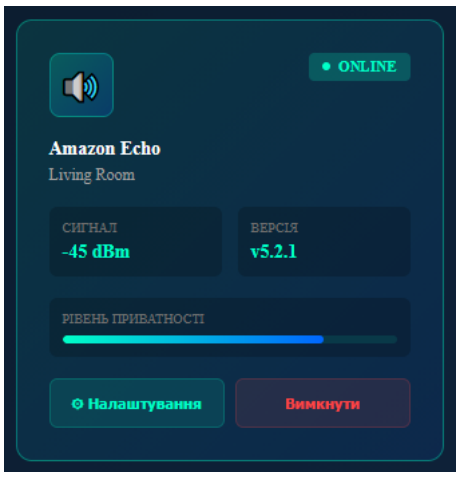

Рисунок 4.6 – Інформація про пристрій

Після натискання кнопки “Налаштування” відкривається детальна інформація про пристрій (рис. 4.7).

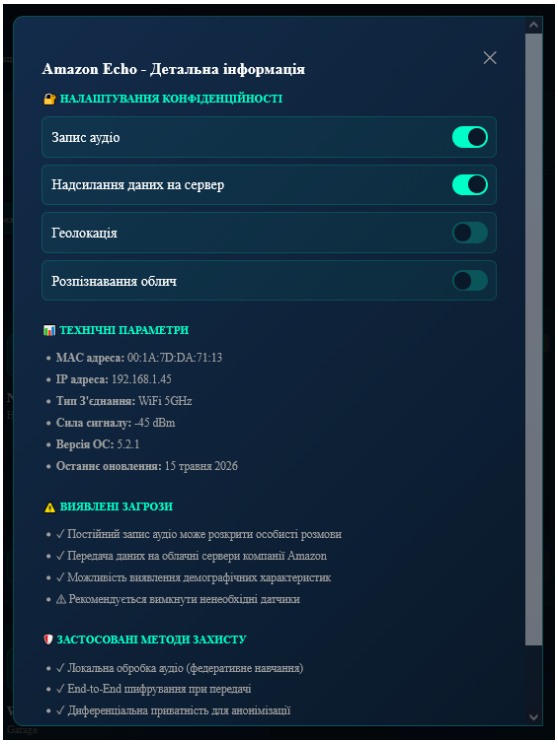

Рисунок 4.7 – Детальна інформація про пристрій

Верхній сегмент інтерфейсу — «Налаштування конфіденційності» — реалізує принцип контролю за потоками чутливої інформації в реальному часі.

Користувачеві доступні чотири логічні перемикачі, що визначають активність сенсорних модулів:

- Запис аудіо та надсилання даних на сервер: перебувають у стані ON, що свідчить про активний режим збору вербальної інформації та її транзит до хмарної інфраструктури.

- Геолокація та Розпізнавання облич: деактивовані (OFF), що мінімізує обсяг ідентифікаційних даних, які виходять за межі локальної мережі.

Блок «Технічні параметри» містить набір унікальних ідентифікаторів та метрик мережевої активності, що необхідні для верифікації справжності пристрою:

- Мережеві адреси: MAC та IP для точної адресації в локальному сегменті.

- Фізичний рівень зв’язку: тип з’єднання (WiFi 5GHz) та сила сигналу, що свідчить про високу якість каналу передачі.

- Програмна ревізія: версія ОС (5.2.1) та часова мітка останнього оновлення (15 травня 2026), що дозволяє контролювати актуальність патчів безпеки.

Нижня частина вікна розділена на два аналітичні блоки, що корелюють із раніше описаним теоретичним фреймворком:

- виявлені загрози: автоматизована система аудиту ідентифікує критичні вектори ризику, такі як ризик деанонімізації приватних розмов через постійний запис аудіо та потенційну можливість виявлення демографічних характеристик суб’єкта. Важливим елементом є рекомендація щодо відключення нежиттєво необхідних датчиків.

- застосовані методи захисту: візуальне підтвердження активації технологій, описаних у попередньому розділі. Зокрема, підтверджено використання федеративного навчання для локальної обробки акустичних сигналів, наявність End-to-End шифрування та застосування диференціальної приватності для анонімізації даних перед їх відправкою на сервери Amazon.

Статус безпеки: кольорові бейджі сигналізують про поточний стан — ONLINE (зелений), ПОПЕРЕДЖЕННЯ (жовтий, наприклад, для Ring Video Doorbell) або OFFLINE (червоний).

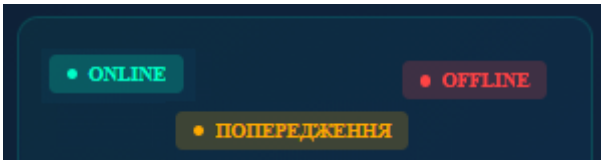

Рисунок 4.8 – Статуси пристроїв

Технічна телеметрія: відображення специфічних для кожного типу даних:

- Amazon Echo: рівень сигналу Wi-Fi (-45 dBm).
- Nest Thermostat: поточна температура (22°C).
- Ring Video Doorbell: статус відеопотоку 4K (Активно).
- Philips Hue: рівень яскравості (75%).

Програмна підтримка: відображення поточної версії прошивки для контролю цілісності та вчасного оновлення (наприклад, v5.2.1, v7.1.0).

Візуалізація індексу приватності: кожна картка містить індивідуальну шкалу «Рівень приватності», що дозволяє оцінити ступінь ризику для кожного окремого пристрою.

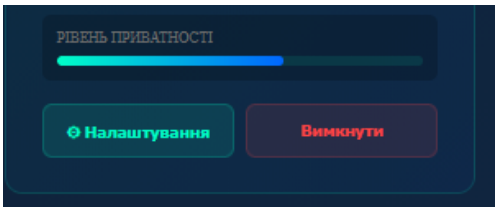

Рисунок 4.9 – Відображення рівня приватності

Нижня частина кожної картки містить органи управління («Налаштування» та «Вимкнути»), що забезпечують можливість швидкого

переведення вузла в режим офлайн-обробки або повного деактивування в разі компрометації.

4.4. Конфігураційна панель прецизійного управління механізмами захисту. Інтерфейс вкладки «Захист»

Інтерфейс вкладки «Захист», представлений на рисунку 4.10, є командним центром для детермінації політик безпеки та управління криптографічними параметрами екосистеми «IoT Safeguard».

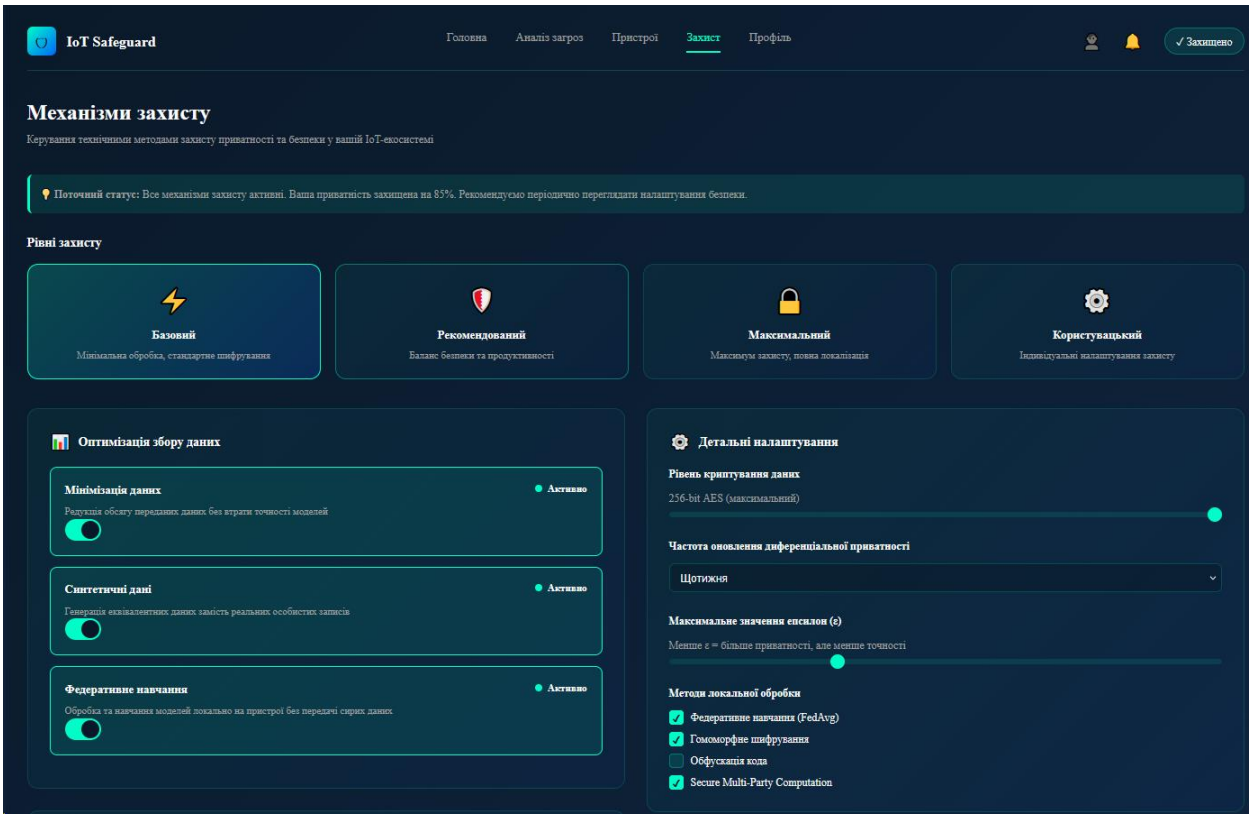

Рисунок 4.10 - Інтерфейс вкладки «Механізми захисту» з вибором рівнів безпеки та детальними налаштуваннями алгоритмів

4.4.1. Моніторинг статусу та вибір рівнів інтенсивності захисту

Верхній сегмент інтерфейсу містить інформаційний банер поточного стану системи, що вказує на активацію всіх захисних вузлів та підтверджує інтегральний рівень приватності у 85%.

Нижче розташовано блок «Рівні захисту», що пропонує чотири пресетні архітектури безпеки:

- Базовий: фокусується на стандартному шифруванні з мінімальним впливом на обчислювальні ресурси.

- Рекомендований: забезпечує оптимальний баланс між конфіденційністю та продуктивністю системи.

- Максимальний: передбачає повну локалізацію обробки даних та найвищий ступінь анонімізації.

- Користувацький: дозволяє здійснювати індивідуальну конфігурацію кожного технічного параметра.

Рисунок 4.11 – Градація рівнів захисту

4.4.2. Модуль оптимізації збору та трансформації даних

Ліва панель управління реалізує стратегії редукції збору інформації:

- Мінімізація даних: активна функція редукції обсягу транзитованих пакетів без деградації точності аналітичних моделей.

- Синтетичні дані: активний процес генерації штучних еквівалентів замість зберігання автентичних персональних записів.

- Федеративне навчання: активний режим локального навчання моделей безпосередньо на кінцевих пристроях, що виключає передачу «сирих» даних на центральні сервери.

4.4.3. Прецизійні налаштування криптографії та диференціальної приватності

Права панель «Детальні налаштування» забезпечує доступ до низькорівневих параметрів захисту даних:

- Криптографічний сектор: встановлено максимальний рівень шифрування за стандартом 256-bit AES.

- Управління диференціальною приватністю: передбачено можливість встановлення частоти оновлення алгоритмів (щотижня) та регулювання значення епсилон (ε). Згідно з математичною моделлю, менше значення ε гарантує вищий рівень приватності за рахунок внесення більшого обсягу статистичного шуму, що може впливати на прецизійність аналітики.

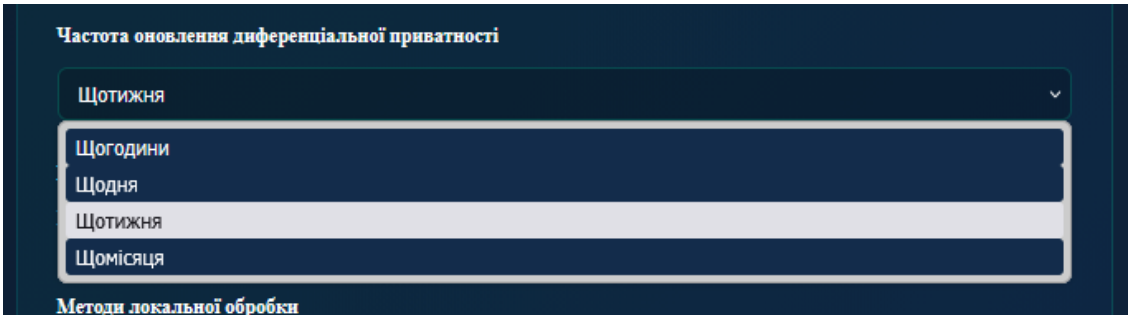

Рисунок 4.12 – Вибір частоти оновлення алгоритмів приватності

- Методи локальної обробки: чек-лист активованих технологій, що включає FedAvg (алгоритм федеративного навчання), Гомоморфне шифрування та Secure Multi-Party Computation.

Нижній сегмент вкладки «Захист» системи «IoT Safeguard» фокусується на операційному моніторингу безпеки та управлінні життєвим циклом критичних даних (рис. 4.13). Ця частина інтерфейсу забезпечує прозорість фонових процесів захисту та надає інструменти для глибокої конфігурації криптографічних протоколів.

У верхній частині даного блоку розташовані модулі контролю за поточною обробкою даних:

- Посилення безпеки обробки: Підтверджує активний статус (Активно) двох ключових механізмів:

1. Імплементація наскрізного шифрування за стандартом AES-256, що гарантує цілісність інформації як під час транзиту, так і в стані спокою.

2. Диференціальна приватність: Механізм анонімізації шляхом внесення контрольованого статистичного шуму, що запобігає деанонімізації індивідуальних характеристик користувача у великих вибірках.

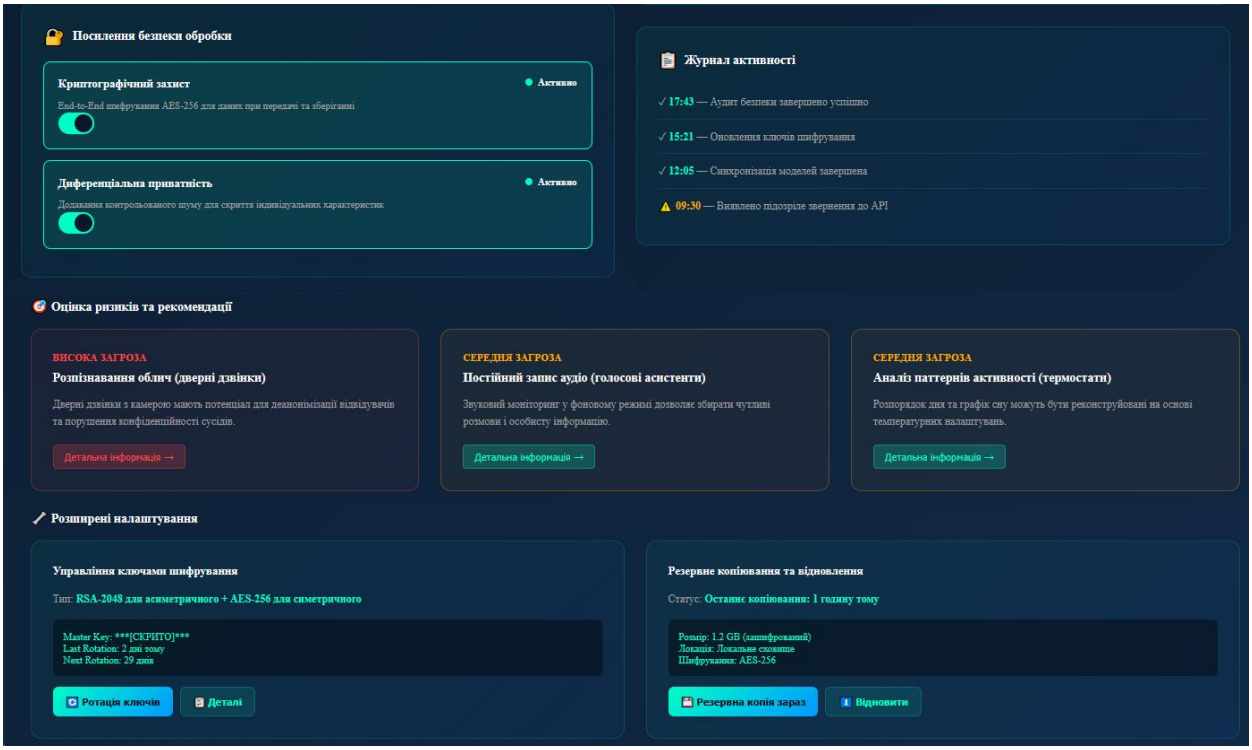

Рисунок 4.13 – Нижня частина вкладки «Механізми захисту»

- Журнал активності: виконує роль системного лога, що фіксує події безпеки в хронологічному порядку. Зокрема, відображено успішне завершення аудиту, оновлення ключів та синхронізацію моделей. Важливою є наявність попередження про виявлення підозрілого звернення до API, що свідчить про роботу вбудованої системи виявлення вторгнень.

4.4.4. Предиктивна оцінка ризиків та рекомендації

Центральний блок «Оцінка ризиків та рекомендації» трансформує загрози у прикладну площину для конкретної екосистеми:

- Висока загроза — розпізнавання облич (дверні дзвінки): Система попереджає про критичний потенціал деанонімізації суб'єктів у напівпублічному просторі, що може призвести до правових колізій із сусідами.

- Середня загроза — Постійний запис аудіо (голосові асистенти): Акцентує увагу на ризику фонового моніторингу чутливих розмов.

- Середня загроза — Аналіз патернів активності (термостати): Повідомляє про можливість реконструкції розпорядку дня та графіків сну на основі телеметрії температурних налаштувань.

Кожен блок оснащений кнопкою «Детальна інформація», що веде до розширеного опису методів пом'якшення для конкретного ризику.

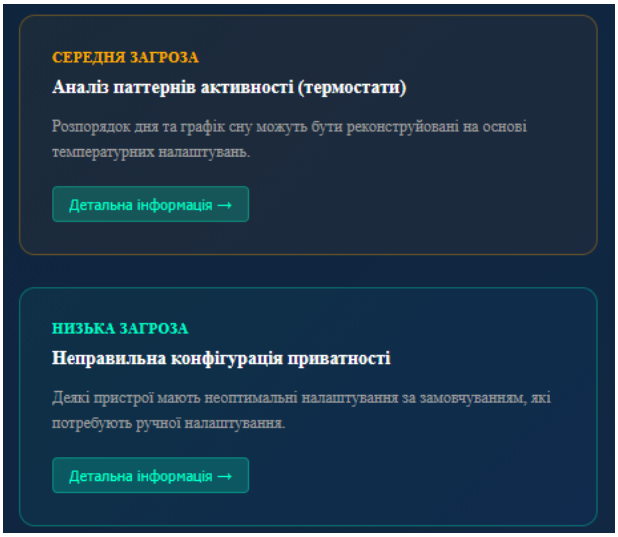

Рисунок 4.14 – Опис видів загроз

4.4.5. Розширені налаштування та управління криптографічним ядром

Нижній сегмент інтерфейсу надає доступ до низькорівневих параметрів безпеки:

- Управління ключами шифрування: Демонструє використання гібридної моделі — асиметричного алгоритму RSA-2048 для обміну ключами та симетричного AES-256 для шифрування контенту. Система відображає статус ротації майстер-ключа (Last Rotation: 2 дні тому), забезпечуючи принцип «досконалої прямої секретності» (Perfect Forward Secrecy). Майстер-ключ за замовчуванням прихований з міркувань безпеки.

- Резервне копіювання та відновлення: Забезпечує доступність даних — третій стовп тріади CIA. Вказано обсяг зашифрованого архіву (1.2 GB), його локацію в захищеному сховищі та статус останньої ітерації копіювання.

Даний інтерфейс успішно поєднує високорівневу аналітику загроз із інструментами прямого технічного впливу, дозволяючи оператору підтримувати заданий рівень приватності або підвищувати його шляхом додаткової ротації ключів чи активації суворіших режимів офлайн-обробки.

4.5 Висновки по розділу

У четвертому розділі було реалізовано програмний прототип системи захисту приватності користувачів «IoT Safeguard», призначений для моніторингу та управління безпекою IoT-інфраструктури. Розроблена система базується на ієрархічній архітектурі та забезпечує централізоване управління вузлами мережі, параметрами конфіденційності та механізмами захисту даних. У процесі реалізації було створено функціональні модулі аналітики ризиків, управління пристроями, конфігурації криптографічних параметрів і контролю рівнів захисту. Особливу увагу приділено реалізації інструментів предиктивної оцінки ризиків та адаптивного налаштування механізмів диференціальної приватності, що дозволяє підвищити ефективність захисту інформації у динамічному середовищі IoT. Результати програмної реалізації підтвердили можливість створення комплексної системи захисту приватності, здатної забезпечити підвищений рівень безпеки користувацьких даних у сучасних екосистемах розумного будинку.

ВИСНОВКИ

В бакалаврській роботі виконано проектування та розробку прототипу програмної системи захисту приватності користувачів в екосистемі розумного будинку.

У межах першого розділу було досліджено еволюцію концепції розумного будинку в умовах глобальної цифровізації та визначено основні тенденції розвитку IoT-екосистем. Встановлено, що сучасні системи автоматизації побутового середовища характеризуються високим рівнем інтеграції хмарних сервісів, сенсорних мереж та алгоритмів машинного навчання, що забезпечує значне підвищення функціональності, однак водночас створює нові вектори кіберзагроз. Проведений аналіз загроз конфіденційності дозволив систематизувати ключові ризики, серед яких особливу небезпеку становлять несанкціонований доступ до персональних даних, витоки інформації через незахищені канали передачі, віддалене перехоплення аудіо- та відеопотоків, а також формування поведінкових профілів користувачів на основі зібраних телеметричних даних. Окрему увагу було приділено технічним вразливостям на рівні пристроїв та мережевої інфраструктури, включаючи використання слабких механізмів автентифікації, застарілих протоколів шифрування та недостатній рівень сегментації мережі.

У другому розділі було проведено комплексний аналіз системної архітектури IoT-пристроїв та алгоритмічних моделей їх функціонування. Досліджено апаратні та програмні компоненти систем голосової взаємодії, визначено характерні алгоритмічні потоки даних та ідентифіковано критичні точки потенційного витоку інформації. На основі аналізу детермінант конфіденційності встановлено, що ризики безпеки в екосистемах інтелектуальних асистентів формуються не лише на рівні програмного забезпечення, але й на рівні фізичних сенсорів, мережевих шлюзів та механізмів інтеграції з зовнішніми сервісами.

У третьому розділі виконано детальний аналіз патернів збору даних та ризиків приватності у середовищі IoT. Досліджено основні джерела формування даних у системах розумного будинку, а також проаналізовано механізми виведення похідної інформації на основі непрямих телеметричних показників. Встановлено, що навіть обмежений набір технічних метаданих може використовуватись для визначення режиму життя користувачів, їхніх звичок, графіків присутності у приміщенні та поведінкових характеристик. Проведений аналіз підтвердив, що проблема приватності у середовищі IoT виходить за межі безпосереднього захисту даних і включає необхідність запобігання алгоритмічному профілюванню та вторинному використанню інформації.

У четвертому розділі було здійснено програмну реалізацію прототипу системи захисту приватності користувачів «IoT Safeguard». Розроблена система базується на ієрархічній архітектурі та включає модулі моніторингу IoT-мережі, управління вузлами інфраструктури, аналізу ризиків та конфігурації механізмів захисту. Реалізований програмний комплекс забезпечує централізований контроль над рівнем конфіденційності в середовищі розумного будинку та дозволяє користувачам здійснювати гнучке управління параметрами збору, передачі та обробки даних.

У межах програмної реалізації було створено аналітичну панель, яка забезпечує візуалізацію ключових показників безпеки та оцінку поточного рівня ризиків. Також реалізовано модуль управління захисними механізмами, що дозволяє здійснювати налаштування рівнів інтенсивності захисту, контролювати параметри криптографічного ядра та конфігурувати механізми диференціальної приватності. Особливу увагу приділено модулю предиктивної оцінки ризиків, який забезпечує аналіз потенційних загроз і формування рекомендацій щодо оптимізації політик безпеки.

ПЕРЕЛІК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Alrawais A., Alhothaily A., Hu C., Cheng X. Fog Computing for the Internet of Things: Security and Privacy Issues // IEEE Internet Computing. – Los Alamitos : IEEE Computer Society, 2017. – Vol. 21, No. 2. – P. 34–42.
2. Atzori L., Iera A., Morabito G. The Internet of Things: A Survey // Computer Networks. – Amsterdam : Elsevier, 2010. – Vol. 54, No. 15. – P. 2787–2805.
3. Sicari S., Rizzardi A., Grieco L. A., Coen-Porisini A. Security, Privacy and Trust in Internet of Things: The Road Ahead // Computer Networks. – Amsterdam : Elsevier, 2015. – Vol. 76. – P. 146–164.
4. Roman R., Zhou J., Lopez J. On the Features and Challenges of Security and Privacy in Distributed Internet of Things // Computer Networks. – Amsterdam : Elsevier, 2013. – Vol. 57, No. 10. – P. 2266–2279.
5. Weber R. H. Internet of Things – New Security and Privacy Challenges // Computer Law & Security Review. – Oxford : Elsevier, 2010. – Vol. 26, No. 1. – P. 23–30.
6. Perera C., Zaslavsky A., Christen P., Georgakopoulos D. Context Aware Computing for The Internet of Things: A Survey // IEEE Communications Surveys & Tutorials. – New York : IEEE, 2014. – Vol. 16, No. 1. – P. 414–454.
7. Miorandi D., Sicari S., De Pellegrini F., Chlamtac I. Internet of Things: Vision, Applications and Research Challenges // Ad Hoc Networks. – Amsterdam : Elsevier, 2012. – Vol. 10, No. 7. – P. 1497–1516.
8. Ziegeldorf J. H., Morchon O. G., Wehrle K. Privacy in the Internet of Things: Threats and Challenges // Security and Communication Networks. – Hoboken : Wiley, 2014. – Vol. 7, No. 12. – P. 2728–2742.
9. Fernandes E., Jung J., Prakash A. Security Analysis of Emerging Smart Home Applications // Proceedings of the 2016 IEEE Symposium on Security and Privacy. – San Jose : IEEE, 2016. – P. 636–654.

10. Apthorpe N., Reisman D., Feamster N. A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic // Workshop on Data and Algorithmic Transparency. – New York : ACM, 2017. – P. 1–6.

11. Abomhara M., Køien G. M. Security and Privacy in the Internet of Things: Current Status and Open Issues // Proceedings of the International Conference on Privacy and Security in Mobile Systems. – Barcelona : IEEE, 2014. – P. 1–8.

12. Diro A. A., Chilamkurti N. Distributed Attack Detection Scheme Using Deep Learning Approach for Internet of Things // Future Generation Computer Systems. – Amsterdam : Elsevier, 2018. – Vol. 82. – P. 761–768.

13. Lin J., Yu W., Zhang N., Yang X., Zhang H., Zhao W. A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications // IEEE Internet of Things Journal. – New York : IEEE, 2017. – Vol. 4, No. 5. – P. 1125–1142.

14. Gubbi J., Buyya R., Marusic S., Palaniswami M. Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions // Future Generation Computer Systems. – Amsterdam : Elsevier, 2013. – Vol. 29, No. 7. – P. 1645–1660.

15. Rose K., Eldridge S., Chapin L. The Internet of Things: An Overview // The Internet Society. – Reston : ISOC, 2015. – P. 1–50.

16. Zanella A., Bui N., Castellani A., Vangelista L., Zorzi M. Internet of Things for Smart Cities // IEEE Internet of Things Journal. – New York : IEEE, 2014. – Vol. 1, No. 1. – P. 22–32.

17. Conti M., Dehghantanha A., Franke K., Watson S. Internet of Things Security and Forensics: Challenges and Opportunities // Future Generation Computer Systems. – Amsterdam : Elsevier, 2018. – Vol. 78. – P. 544–546.

18. Riahi Sfar A., Natalizio E., Challal Y., Chtourou Z. A Roadmap for Security Challenges in the Internet of Things // Digital Communications and Networks. – Beijing : Elsevier, 2018. – Vol. 4, No. 2. – P. 118–137.

19. Xu L. D., He W., Li S. Internet of Things in Industries: A Survey // IEEE Transactions on Industrial Informatics. – New York : IEEE, 2014. – Vol. 10, No. 4. – P. 2233–2243.

20. Da Xu L., He W., Li S. Internet of Things in Industries: A Survey // IEEE Transactions on Industrial Informatics. – New York : IEEE, 2014. – Vol. 10, No. 4. – P. 2233–2243.

21. Shwartz L., Mathur A. Privacy-Aware Smart Homes: A Survey of Data Protection Mechanisms // Journal of Network and Computer Applications. – London : Elsevier, 2020. – Vol. 161. – P. 102635.

22. Bugeja J., Jacobsson A., Davidsson P. On Privacy and Security Challenges in Smart Connected Homes // Proceedings of the European Intelligence and Security Informatics Conference. – Uppsala : IEEE, 2016. – P. 172–175.

23. Dorri A., Kanhere S. S., Jurdak R. Blockchain in Internet of Things: Challenges and Solutions // arXiv Preprint arXiv:1608.05187. – Ithaca : Cornell University, 2016. – P. 1–14.

24. Nguyen G. T., Reddi V. J. Deep Reinforcement Learning for Cyber Security // IEEE Transactions on Neural Networks and Learning Systems. – New York : IEEE, 2021. – Vol. 32, No. 5. – P. 1557–1570.

25. McMahan B., Moore E., Ramage D., Hampson S., Arcas B. Communication-Efficient Learning of Deep Networks from Decentralized Data // Proceedings of the 20th International Conference on Artificial Intelligence and Statistics. – Fort Lauderdale : PMLR, 2017. – P. 1273–1282.

26. Dwork C. Differential Privacy // Proceedings of the 33rd International Colloquium on Automata, Languages and Programming. – Venice : Springer, 2006. – P. 1–12.

27. Dwork C., Roth A. The Algorithmic Foundations of Differential Privacy // Foundations and Trends in Theoretical Computer Science. – Hanover : Now Publishers, 2014. – Vol. 9, No. 3–4. – P. 211–407.

28. Kairouz P., McMahan H. B., Avent B. et al. Advances and Open Problems in Federated Learning // Foundations and Trends in Machine Learning. – Boston : Now Publishers, 2021. – Vol. 14, No. 1–2. – P. 1–210.

29. Bonawitz K., Eichner H., Grieskamp W. et al. Towards Federated Learning at Scale: System Design // Proceedings of the 2nd SysML Conference. – Palo Alto : SysML, 2019. – P. 1–15.

30. Haddadi H., Hui P., Brown I. Mobile Data Consumption: Privacy Risks and Mitigation Strategies // IEEE Internet Computing. – Los Alamitos : IEEE Computer Society, 2012. – Vol. 16, No. 3. – P. 62–68.

31. Alaba F. A., Othman M., Hashem I. A. T., Alotaibi F. Internet of Things Security: A Survey // Journal of Network and Computer Applications. – London : Elsevier, 2017. – Vol. 88. – P. 10–28.

32. Khan M. A., Salah K. IoT Security: Review, Blockchain Solutions, and Open Challenges // Future Generation Computer Systems. – Amsterdam : Elsevier, 2018. – Vol. 82. – P. 395–411.

33. Ammar M., Russello G., Crispo B. Internet of Things: A Survey on the Security of IoT Frameworks // Journal of Information Security and Applications. – Amsterdam : Elsevier, 2018. – Vol. 38. – P. 8–27.

БІБЛІОГРАФІЧНА ДОВІДКА

Тема бакалаврської роботи: “ Проєктування програмної системи захисту приватності користувачів у середовищі IoT ”

Обсяг пояснювальної записки: 83 аркуші.

Дата закінчення роботи: 9 червня 2026 р.

Підпис студента _____