НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Факультет робототехніки та приладобудування

Кафедра комп'ютерно-інтегрованих технологій виробництва приладів

До захисту допущено:
Завідувач кафедри
_____ Наталія СТЕЛЬМАХ
«12» ____06____ 2026 р.

Дипломна робота

на здобуття ступеня бакалавра

за освітньо-професійною програмою «Комп'ютерно-інтегровані системи та технології в приладобудуванні»

спеціальності 151 «Автоматизація та комп'ютерно-інтегровані технології»

на тему: «Гібридна багатоквартирна IP-панель автоматичного виклику»

Виконав:
студент IV курсу, групи ПБ-22
Яріз Ростислав Анатолійович _____

Керівник:
доцент, к.т.н., доцент
Безугла Наталя Василівна _____

Рецензент:
професор, д.т.н., професор
Микитенко Володимир Іванович _____

Засвідчую, що у цьому дипломному проєкті немає запозичень з праць інших авторів без відповідних посилань.
Студент _____

Київ – 2026 року

Відомість дипломного проєкту

№ з/п	Формат	Позначення	Найменування	Кількість листів	Примітка
1	А4		Завдання на дипломний проєкт	3	
2	А4	ДПБ.ПБ-22.13.1702.ПЗ	Пояснювальна записка	64	
3	А2	ДПБ.ПБ-22.13.1702.001 СХ	Структурна схема апаратної архітектури панелі	1	
4	А2	ДПБ.ПБ-22.13.1702.002 СХ	Електрично принципова схема панелі	1	
5	А2	ДПБ.ПБ-22.13.1702.003 СХ	Схема мережевої взаємодії об'єкта керування з зовнішньою інфраструктурою	1	
6	А2	ДПБ.ПБ-22.13.1702.004 СХ	Алгоритм паралельного гібридного сповіщення	1	
7	А2	ДПБ.ПБ-22.13.1702.005 СХ	Структура бази даних	1	
8	А2	ДПБ.ПБ-22.13.1702.006 СХ	Алгоритм роботи панелі	1	
9	А2	ДПБ.ПБ-22.13.1702.007 СХ	Блок-схема алгоритму обробки RSSI (режиму «Вільні руки»)	1	
10	А2	ДПБ.ПБ-22.13.1702.008	Інтерфейс панелі керування (Web Dashboard)	1	
11	А2	ДПБ.ПБ-22.13.1702.009	Екран вхідного відеовиклику мобільного застосунку	1	

				ДРБ.ПБ-22.13.1702.ПЗ		
	ПІБ	Підп.	Дата			
Розробн.	Яріз Р. А.			Відомість дипломної роботи	Лист	Листів
Керівн.	Безугла Н.В.				1	
Консульт.					ПБФ, КПІ ім. Ігоря Сікорського	
Н/контр.						
Зав.каф.	Стельмах Н.В.					

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Факультет робототехніки та приладобудування
Кафедра комп'ютерно-інтегрованих технологій виробництва приладів

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 151 «Автоматизація та комп'ютерно-інтегровані технології»

Освітньо-професійна програма «Комп'ютерно-інтегровані системи та технології в приладобудуванні»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Наталія СТЕЛЬМАХ
«12» 06 2026 р.

ЗАВДАННЯ

на дипломну роботу студенту

Яріз Ростислав Анатолійович

1. Тема роботи «Гібридна багатоквартирна IP-панель автоматичного виклику», керівник роботи Безугла Наталя Василівна, доцент, к.т.н., затверджені наказом по університету від «26» травня 2036 р. № 1905-с

2. Термін подання студентом роботи «07» червня 2026 року.

3. Вихідні дані до роботи: технічні вимоги Апаратна сумісність із координатно-матричними системами (до 300 абонентів) та інтеграція IP-технологій. Мережеві протоколи: SIP, TCP/IP, UDP, RTSP через Ethernet 10/100 Mbps. Відеосистема: IP-камера від 2Мп та аналоговий вихід CVBS/AHD. Підсистема ідентифікації: зчитувач Mifare Desfire з апаратним шифруванням, ємнісний сканер відбитків або 3D Face ID, модуль BLE 5.0 для доступу зі смартфона. Програмний функціонал: алгоритм паралельного сповіщення, локальний веб-інтерфейс, підключення до хмарної платформи з розподілом ролей.

4. Зміст роботи: *Вступ. Розділ 1. Огляд сучасних систем контролю доступу та принцип дії гібридного пристрою. 1.1. Огляд класичних аналогових та сучасних IP-систем домофонії (через призму готових рішень). 1.2. Аналіз принципів роботи та існуючих методів інтеграції з координатно-матричними системами. 1.3. Сучасні IP-технології та хмарні рішення в системах контролю доступу. 1.4. Огляд методів ідентифікації користувачів (RFID, біометрія, BLE). Розділ 2. Теоретичне моделювання та обґрунтування концепції гібридної системи. 2.2. Опис в загальному вигляді природи технологічного об'єкту керування і процесів, що протікають в ньому. 2.3. Визначення регульованих параметрів, збурень і можливих дій керування. 2.4. Параметрична схема ОК, її фізичні величини вхідних та вихідних сигналів, збурюючих впливів. 2.5. Структурна схема системи*

керування та опис її роботи в загальному вигляді. Розділ 3. Технічне та апаратне проектування гібридної викличної панелі. 3.1. Принцип дії та архітектура запропонованої гібридної викличної панелі. 3.2. Розробка та опис електричної принципової схеми системи керування. 3.3. Апаратна реалізація мережевої інфраструктури та забезпечення стійкості з'єднання. 3.4. Спрощена апаратна архітектура для малобюджетних об'єкті. Розділ 4. Програмне забезпечення та алгоритми системи. 4.1. Архітектура програмного комплексу. 4.2. Програмна реалізація алгоритмів управління панелі. 4.3. Розробка клієнтських додатків (Web та Mobile). Висновки. Список використаних джерел.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо): *Структурна схема архітектури гібридної викличної панелі, принципова електрична схема системи керування та модуля аналогової комутації, блок-схема алгоритму паралельного виклику з логікою пріоритету першої відповіді, діаграма послідовності взаємодії застосунку з гібридною панеллю.*

6. Дата видачі завдання: 03 квітня 2026 року.

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назва етапів дипломної роботи	Строк виконання дипломної роботи	Примітки
1	Аналіз предметної області та огляд існуючих систем домофонії (аналогових координатних та сучасних IP-рішень).	17.04.2026	
2	Розробка структурної та принципової схеми системи керування	24.04.2026	
3	Апаратне проектування базової системи (обґрунтування вибору мікроконтролера, IP та аналогової камер, модулів біометрії, BLE, RFID/NFC, комутатора).	08.05.2026	
4	Проектування програмної архітектури та алгоритмів роботи (алгоритми паралельного виклику, пріоритет відповіді, інтеграція з Cloud API).	15.05.2026	
5	Розробка підсистеми безпеки та ідентифікації (апаратне шифрування AES/DES, алгоритми anti-spoofing, Bluetooth-керування).	22.05.2026	
6	Моделювання роботи системи та тестування функцій доступу (локальний веб-інтерфейс, мобільний застосунок, хмарне логування).	29.05.2026	
7	Написання та оформлення пояснювальної записки згідно з вимогами ДСТУ	07.06.2026	

Студент Яріз Ростислав ЯРІЗ

Керівник Наталя БЕЗУГЛА

Пояснювальна записка

до дипломної роботи

на тему **Гібридна багатоквартирна IP-панель автоматичного виклику**

ЗМІСТ

ВСТУП.....3
РОЗДІЛ 1. ОГЛЯД СУЧАСНИХ СИСТЕМ КОНТРОЛЮ ДОСТУПУ ТА ПРИНЦИП ДІЇ ГІБРИДНОГО ПРИСТРОЮ.....6
1.1. Огляд класичних аналогових та сучасних IP-систем домофонії (через призму готових рішень).....6
1.2. Аналіз принципів роботи та існуючих методів інтеграції з координатно-матричними системами.....8
1.3. Сучасні IP-технології та хмарні рішення в системах контролю доступу 10
1.4. Огляд методів ідентифікації користувачів (RFID, біометрія, BLE).....12
1.4.1. Технології радіочастотної ідентифікації (RFID) та стандарти шифрування MIFARE DESFire.....13
1.4.2. Біометрична ідентифікація: ємнісні сканери відбитків та криптографічний захист шаблонів.....16
1.4.3. Біометрія: Розпізнавання облич та технології Face Anti-Spoofing (FAS).....19
1.4.4. Bluetooth Low Energy (BLE) та алгоритмічний аналіз RSSI для режиму «Вільні руки».....24
РОЗДІЛ 2. ТЕОРЕТИЧНЕ МОДЕЛЮВАННЯ ТА ОБҐРУНТУВАННЯ КОНЦЕПЦІЇ ГІБРИДНОЇ СИСТЕМИ.....28
2.2. Опис в загальному вигляді природи технологічного об’єкту керування і процесів, що протікають в ньому.....28
2.3. Визначення регульованих параметрів, збурень і можливих дій керування.....29
2.4. Параметрична схема ОК, її фізичні величини вхідних та вихідних сигналів, збурюючих впливів.....31

2.5. Структурна схема системи керування та опис її роботи в загальному вигляді.....33
Розділ 3. Технічне та апаратне проектування гібридної викличної панелі.....37
3.1. Принцип дії та архітектура запропонованої гібридної викличної панелі 37
3.2. Розробка та опис електричної принципової схеми системи керування 39
3.3. Апаратна реалізація мережевої інфраструктури та забезпечення стійкості з'єднання.....46
3.4. Спрощена апаратна архітектура для малобюджетних об'єктів (до 50 абонентів).....48
Розділ 4. Програмне забезпечення та алгоритми системи.....50
4.1. Архітектура програмного комплексу.....50
4.2. Програмна реалізація алгоритмів управління панелі.....53
4.3. Розробка клієнтських додатків (Web та Mobile).....57
4.3.1. Реалізація веб-застосунку та панелі керування.....57
4.3.2. Розробка мобільного застосунку абонента.....59
Висновки.....61
Список використаних джерел:.....62

АНОТАЦІЯ

Дипломна робота на тему "Гібридна багатоквартирна IP-панель автоматичного виклику" розроблена студентом Ярізом Ростиславом Анатолієвичем під керівництвом доцента кафедри комп’ютерно-інтегрованих технологій виробництва приладів Київського політехнічного інституту імені Ігоря Сікорського, к.т.н. Безуглою Наталею Василівною.

Метою роботи є створення гібридної викличної панелі, що об'єднує аналогові координатно-матричні лінії зв'язку з сучасними IP-платформами. Це дозволяє зберегти наявну інфраструктуру абонентських трубок, додаючи можливості відеофіксації, віддаленого доступу зі смартфона, розпізнавання облич та BLE-ідентифікації.

Дипломна робота складається з пояснювальної записки (64 сторінки, 21 рисунка, 8 таблиць, 14 джерел літератури) та додатку А. Додаток містить графічний матеріал: структурну та принципову електричну схеми, схему мережевої взаємодії, алгоритми роботи системи, структуру бази даних та інтерфейси клієнтських додатків.

У чотирьох розділах записки послідовно досліджено: сучасні системи домофонії та криптографічні методи ідентифікації (MIFARE DESFire, ємнісні сканери, Face Anti-Spoofing, BLE); теоретичне моделювання об'єкта керування з визначенням параметрів і збурень; апаратне проектування панелі на базі мікроконтролера Rockchip RV1109 із розробкою мережевої інфраструктури; а також розробку архітектури ПЗ, алгоритмів паралельного виклику та клієнтських додатків (Web та Mobile).

Робота спрямована на модернізацію систем доступу багатоквартирних будинків, підвищення зручності та рівня захисту даних без повної заміни комунікацій. У висновках підтверджено готовність розробленої системи до реальної експлуатації.

Ключові слова: гібридна виклична панель, контроль доступу, координатно-матрична система, протокол SIP, BLE, розпізнавання облич, IoT.

ANNOTATION

The diploma thesis on the topic "Hybrid Multi-Apartment IP Intercom Panel" was developed by student Yariz Rostyslav Anatoliyovych under the supervision of Associate Professor of the Department of Computer-Integrated Technologies for the Production of Instruments at Igor Sikorsky Kyiv Polytechnic Institute, PhD Natalia Bezuhla.

The objective of the work is to create a hybrid intercom panel that integrates analog coordinate-matrix communication lines with modern IP platforms. This allows preserving the existing infrastructure of subscriber handsets while adding capabilities for video recording, remote access via smartphone, facial recognition, and BLE identification.

The diploma thesis consists of an explanatory note (64 pages, 21 figures, 8 tables, 14 references) and Appendix A. The appendix contains graphic materials: structural and principal electrical schematics, a network interaction diagram, system algorithms, the database structure, and client application interfaces.

The four chapters of the explanatory note sequentially explore: modern intercom systems and cryptographic identification methods (MIFARE DESFire, capacitive scanners, Face Anti-Spoofing, BLE); theoretical modeling of the control object with the definition of parameters and disturbances; hardware design of the panel based on the Rockchip RV1109 microcontroller along with the development of the network infrastructure; and the development of the software architecture, parallel calling algorithms, and client applications (Web and Mobile).

The work is aimed at modernizing access control systems in multi-apartment buildings, improving user convenience, and enhancing data protection levels without completely replacing the existing communications. The conclusions confirm the readiness of the developed system for real-world operation.

Keywords: hybrid intercom panel, access control, coordinate-matrix system, SIP protocol, BLE, facial recognition, IoT.

ВСТУП

Стрімкий розвиток інформаційних технологій, концепцій «розумного міста» (Smart City) та глобальної мережі Інтернет речей (IoT) висуває принципово нові, значно жорсткіші вимоги до архітектури систем безпеки та контролю доступу в багатоквартирному житловому секторі. Історично склалося так, що переважна більшість багатоквартирних будинків, зведених у кінці минулого та на початку поточного століття, обладнані класичними аналоговими координатно-матричними системами домофонії. Такі системи свого часу стали революційним рішенням завдяки своїй відносній дешевизні, простоті монтажу та високій енергонезалежності. Вони довели свою апаратну надійність протягом десятиліть експлуатації, оскільки базуються на фундаментальних законах електротехніки та прямій фізичній комутації ліній зв'язку. Однак в епоху цифровізації вони вичерпали свій потенціал щодо масштабування, інтеграції з мобільними пристроями, передачі відео високої чіткості та забезпечення сучасного криптографічного чи біометричного захисту.

Натомість повністю цифрові IP-системи пропонують пакетну передачу даних (TCP/IP, SIP), хмарне керування та алгоритми розпізнавання облич. Водночас повна модернізація інфраструктури будівлі — прокладання Ethernet-ліній, встановлення мережевого обладнання та заміна абонентських пристроїв — є економічно недоцільною та часто викликає соціальний спротив мешканців.

Виходячи з цього, гострою інженерною потребою є розробка гібридних викличних панелей. Такий пристрій виступає трансляційним мостом між застарілими аналоговими лініями зв'язку та сучасними IP-платформами. Це дозволяє зберегти існуючу інфраструктуру абонентських трубок, одночасно додавши можливості віддаленого відкриття зі смартфона, відеофіксації, біометрії та доступу за технологією BLE.

РОЗДІЛ 1. ОГЛЯД СУЧАСНИХ СИСТЕМ КОНТРОЛЮ ДОСТУПУ ТА ПРИНЦИП ДІЇ ГІБРИДНОГО ПРИСТРОЮ

1.1. Огляд класичних аналогових та сучасних IP-систем домофонії (через призму готових рішень)

Еволюція систем контролю та управління доступом (СКУД) у житловому секторі відображає загальний перехід від аналогової обробки сигналів до цифрових мережевих технологій. Для глибокого розуміння принципів побудови гібридного пристрою необхідно детально проаналізувати фізичні та архітектурні засади як класичних, так і сучасних підходів до проектування систем домофонії, дослідивши їхні переваги та критичні обмеження.

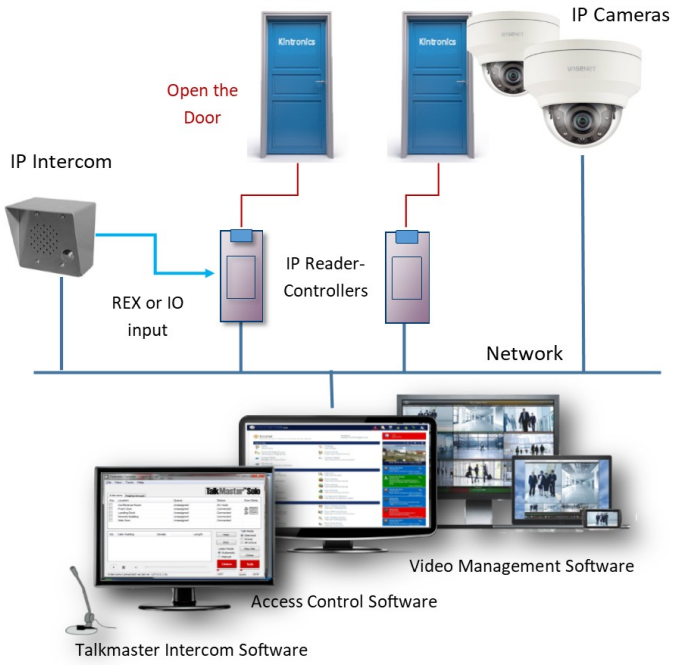


Рисунок 1.1. Схема роботи контролю доступу, покращеного за допомогою домофонів [1]

Класичні аналогові багатоабонентські домофонні системи, репрезентовані на ринку такими відомими брендами як Vizit, Cyfral, Metakom та Eltis, історично будувалися на базі координатно-матричної або, рідше,

двопровідної цифрової архітектури зв'язку. У найбільш поширених координатно-матричних системах зв'язок між викличною панеллю та абонентом встановлюється шляхом замикання відповідного електронного ключа у просторовій матриці комутатора. У такій топології один дріт магістрального кабелю відповідає за розряд «десятків» (D), а інший — за розряд «одиниць» (E) номера квартири. Фізично комутатор реалізує аналоговий мультиплексор, який з'єднує аудіотракт панелі безпосередньо з динаміком та мікрофоном обраної абонентської трубки через аналогову лінію зв'язку.

Головними інженерними перевагами аналогових систем є апаратна простота, економічність та висока відмовостійкість. Завдяки централізованому живленню абонентських пристроїв та відсутності проміжного мережевого обладнання, вони не залежать від збоїв у локальних мережах. Крім того, пряма трансляція сигналу виключає затримки (джиттер) та втрату пакетів [2].

Водночас такі системи мають фундаментальні обмеження: деградація медіаданих (зокрема відео CVBS) на значних відстанях через електромагнітні завади, низька масштабованість через жорстку кабельну архітектуру та вкрай обмежений функціонал. Вони не підтримують віддаленого адміністрування, цифрового логування чи мобільної переадресації без встановлення додаткових апаратних шлюзів.

Натомість сучасні IP-системи докорінно змінюють парадигму проектування СКУД, використовуючи стандартну інфраструктуру мереж (Ethernet, TCP/IP). Це дозволяє мультиплексувати цифровий аудіопотік, відео високої роздільної здатності та керуючі команди в єдиному каналі зв'язку.

Цифрова пакетна архітектура усуває проблему деградації сигналу від відстані. Завдяки застосуванню сучасних кодеків (H.264/H.265, G.711/Opus) система здатна транслювати відео у якості Full HD без перевантаження мережі. Оскільки кожен IP-домофон є повноцінним мережевим пристроєм

(IoT), це забезпечує легку масштабованість та глибоку інтеграцію з системами керування будівлею (BMS), відеоспостереження (NVR) та хмарними платформами.

Проте, як зазначають дослідники, впровадження повністю цифрових систем у раніше збудованих будинках стикається з серйозною проблемою так званої «останньої милі» . Необхідність прокладання нових мережевих кабелів до кожної квартири та придбання дорогих абонентських IP-моніторів замість дешевих аналогових трубок створює високий фінансовий бар'єр. Саме тому концепція гібридного пристрою, здатного на апаратному рівні працювати зі старими лініями, а на програмному рівні підтримувати стек TCP/IP, є оптимальним вектором розвитку для модернізації житлового фонду.

1.2. Аналіз принципів роботи та існуючих методів інтеграції з координатно-матричними системами

Для розробки гібридного пристрою критично важливим є розуміння принципів роботи координатно-матричних систем (КМС) та методів апаратного сполучення низьковольтних мікроконтролерів із високовольтними аналоговими лініями.

Робота КМС базується на мультиплексуванні сигналів за допомогою діодної матриці комутатора (наприклад, БК-100М, КМГ-100). Архітектура включає шини десятків (D0–D9) та одиниць (E0–E9). Кожна абонентська трубка підключається на перетині цих шин, що визначає її фізичну адресу (наприклад, кв. 45 — до D4 та E5). Послідовно ввімкнений у трубку діод забезпечує правильну полярність і запобігає перехресним перешкодам між лініями.

У стані очікування напруга на матриці відсутня, а опір лінії прямує до нескінченності. Під час виклику панель подає постійну напругу (12–15 В) на вибрані координати, активуючи звуковий генератор трубки.

Стан абонента визначається моніторингом падіння напруги або зміни струму в лінії. Під час зняття трубки комутується розмовний тракт, через що еквівалентний опір пристрою різко падає (до ~300 Ом для Cyfral або ~50 Ом для Vizit). Сплеск струму фіксується компаратором або АЦП панелі, яка переводить лінію в режим дуплексного аудіозв'язку. Для відкриття дверей відбувається короткочасний розрив кола (опір прямує до нескінченності) або падіння струму до порогового рівня, що детектується панеллю для формування сигналу керування реле замка.

Інтеграція сучасної IP-архітектури з аналоговою КМС потребує створення спеціалізованого модуля сполучення (шлюзу) між цифровим (SIP) та аналоговим доменами. Існують два підходи:

Використання зовнішніх цифро-аналогових адаптерів (ATA - Analog Telephone Adapters). Цей метод передбачає використання промислових SIP-шлюзів, які конвертують VoIP-сигнали в стандартні аналогові телефонні лінії (інтерфейси FXS/FXO). Однак для багатоквартирних домофонів цей підхід є неефективним та громіздким. Телефонні адаптери розраховані на стандарти класичної телефонії (напруга виклику близько 90 В змінного струму), тоді як домофонні комутатори працюють з низьковольтним постійним струмом (12-15 В) і вимагають прецизійного управління матрицею ключів. Використання зовнішніх шлюзів призводить до необхідності створення додаткових ланок узгодження рівнів сигналів, що знижує надійність системи [3].

Пряме апаратне управління комутаторами (Direct Hardware Control). Це більш сучасний та інтегрований підхід, який покладено в основу проектування спеціалізованих гібридних панелей. У такій архітектурі панель містить спеціалізований мікроконтролер (наприклад, сімейства ARM Cortex-M або AVR), який безпосередньо з'єднується з керуючими входами комутаційних блоків (таких як БК-100М). Гібридна панель оснащується багатоканальними цифро-аналоговими перетворювачами (ЦАП) для генерації аудіосигналів необхідної амплітуди та високошвидкісними АЦП для

моніторингу стану аналогової лінії. Мікроконтролер реалізує складний скінченний автомат (Finite State Machine), який програмно імітує поведінку класичної панелі: він управляє адресацією десятків і одиниць, генерує напругу виклику, детектує зняття трубки шляхом аналізу опору та розпізнає команду відкриття дверей.

Важливою проблемою є захист низьковольтних цифрових компонентів (3.3 / 5 В) від високовольтних імпульсів та зворотної ЕРС, що виникають через комутацію довгих кабельних трас та індуктивних навантажень (реле замка). Для цього застосовують гальванічну розв'язку на швидкодіючих оптопарах, TVS-діоди та самовідновлювальні запобіжники.

1.3. Сучасні IP-технології та хмарні рішення в системах контролю доступу

Перевагою гібридної системи є не лише збереження сумісності зі старим обладнанням, але й глибоке впровадження сучасних мережевих та хмарних технологій управління, що забезпечують глобальну доступність, мультимедійну комунікацію та високу експлуатаційну гнучкість. Основою для розгортання таких систем є використання відкритих стандартів Інтернету.

Протокол SIP та архітектура маршрутизації викликів. Session Initiation Protocol (SIP) — це фундаментальний протокол прикладного рівня моделі взаємодії відкритих систем (OSI), що стандартизований IETF (RFC 3261). Він призначений для ініціації, модифікації та логічного завершення інтерактивних мультимедійних сеансів зв'язку, таких як аудіо- та відеодзвінки через IP-мережі. У контексті гібридної викличної панелі протокол SIP виступає ключовим механізмом керування викликами.

Архітектура SIP-мережі є клієнт-серверною і складається з кількох логічних компонентів. Клієнтські агенти (User Agents, UA) включають саму гібридну панель (UAC - User Agent Client, що ініціює виклик) та мобільні

застосунки на смартфонах мешканців або IP-монітори всередині квартир (UAS - User Agent Server, що приймають виклик). Для забезпечення зв'язку між ними використовується централізований SIP-сервер, який зазвичай об'єднує функції Proxy-сервера (для пересилання запитів) та Registrar-сервера (для відстеження поточних IP-адрес активних користувачів) [4].

Трансляція відео (RTSP) та вирішення проблеми NAT. Для забезпечення можливості постійного моніторингу та інтеграції відеопотоку панелі в загальнобудинкову систему відеоспостереження (Network Video Recorder, NVR), використовується протокол RTSP (Real-Time Streaming Protocol). На відміну від SIP, який орієнтований на двосторонній сеанс, RTSP виконує роль пульта дистанційного керування для медіасервера панелі, дозволяючи зовнішнім системам запитувати відеопотік, контролювати його параметри та здійснювати запис 24/7. Відеодані стискаються за допомогою високоефективного кодека H.264 або H.265, що дозволяє передавати відео високої роздільної здатності (1080p) з частотою 25-30 кадрів на секунду, мінімізуючи використання смуги пропускання мережі.

Значним технічним викликом при розгортанні IP-домофонії є передача медіаданих (RTP) до мобільних смартфонів, які зазвичай знаходяться за маршрутизаторами з трансляцією мережевих адрес (NAT) або у стільникових мережах. Для вирішення проблеми прямої видимості IP-адрес (NAT Traversal) у хмарну архітектуру СКУД інтегруються сервери STUN (Session Traversal Utilities for NAT) та TURN (Traversal Using Relays around NAT). Ці технології дозволяють клієнтським пристроям дізнатися свою публічну IP-адресу або, у складних випадках симетричного NAT, ретранслювати медіа-трафік через зовнішній хмарний сервер, гарантуючи надійне встановлення відеодзвінка незалежно від конфігурації мережі користувача. Дедалі більшої популярності набуває також використання технології WebRTC, яка забезпечує встановлення одноранговых (peer-to-peer) з'єднань із мінімальними затримками

безпосередньо в середовищі веб-браузерів та мобільних застосунків, використовуючи вбудовані механізми обходу NAT (ICE-кандидати) [5].

Хмарні платформи управління (Cloud Management). Перенесення ядра управління СКУД у хмару дозволяє кардинально спростити адміністрування об'єктів. Хмарна платформа забезпечує централізоване зберігання та синхронізацію конфігураційних файлів, прошивок, бази даних користувачів та їхніх криптографічних ключів доступу. Платформи будуються на принципах рольового доступу (Role-Based Access Control, RBAC).

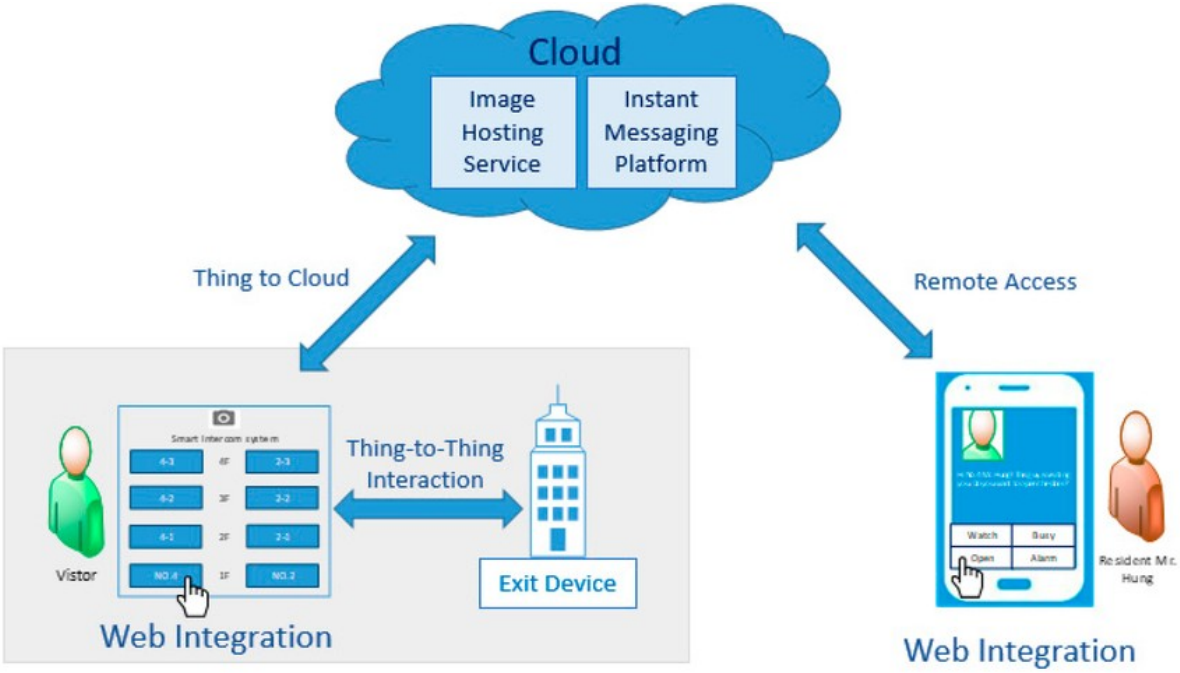


Рисунок 1.1. Принципова схема системи розумного домофона [6]

Інсталятори отримують розширені права для налаштування мережевих параметрів, конфігурації підмереж та діагностики апаратних збоїв аналогової матриці. Адміністратори житлових комплексів (ОСББ або управляючі компанії) мають доступ до веб-інтерфейсу для швидкого додавання або блокування RFID-карток мешканців, активації або деактивації мобільних застосунків, а також для перегляду структурованих журналів подій (наприклад, "Хто і коли відкрив двері"). Хмарний підхід усуває необхідність

фізичного підключення до кожної панелі для оновлення ключів, що суттєво знижує експлуатаційні витрати [6].

1.4. Огляд методів ідентифікації користувачів (RFID, біометрія, BLE)

Фундаментальною вимогою до сучасної гібридної системи контролю доступу є забезпечення безкомпромісного рівня безпеки процесу ідентифікації. Традиційні методи доступу, що використовувалися протягом останніх двох десятиліть (наприклад, безконтактні картки формату EM-Marin, що працюють на частоті 125 кГц, або контактні ключі Dallas Touch Memory), довели свою абсолютну вразливість до атак клонування. Унікальні ідентифікатори (UID) таких ключів передаються у відкритому вигляді і можуть бути зчитані та скопійовані за лічені секунди за допомогою дешевих загальнодоступних дуплікаторів. Тому розроблювана панель покладається на криптографічно захищені технології радіочастотної ідентифікації, глибокий аналіз біометричних ознак та використання безпечних радіоканалів сучасних смартфонів.

1.4.1. Технології радіочастотної ідентифікації (RFID) та стандарти шифрування MIFARE DESFire

У сегменті високобезпечної смарт-ідентифікації стандартом де-факто є технологія MIFARE DESFire (Designated Security Firewall), розроблена компанією NXP Semiconductors. Смарт-картки сімейства DESFire (покоління EV1, EV2 та EV3) працюють на частоті 13.56 МГц, повністю відповідають стандарту ISO/IEC 14443 Type A і відрізняються наявністю повноцінного мікропроцесора та апаратного криптографічного співпроцесора, що забезпечує шифрування даних безпосередньо на кристалі чипа .

Безпека передачі інформації між зчитувачем (викличною панеллю) та смарт-карткою забезпечується не просто перевіркою серійного номера, а

складним математичним протоколом триетапної взаємної автентифікації (3-pass mutual authentication) із застосуванням симетричного алгоритму AES (Advanced Encryption Standard) з довжиною ключа 128 біт. Цей протокол базується на концепції «виклик-відповідь» (challenge-response) та унеможливлює проведення атак типу «перехоплення-відтворення» (replay attack) або створення математичних клонів картки.

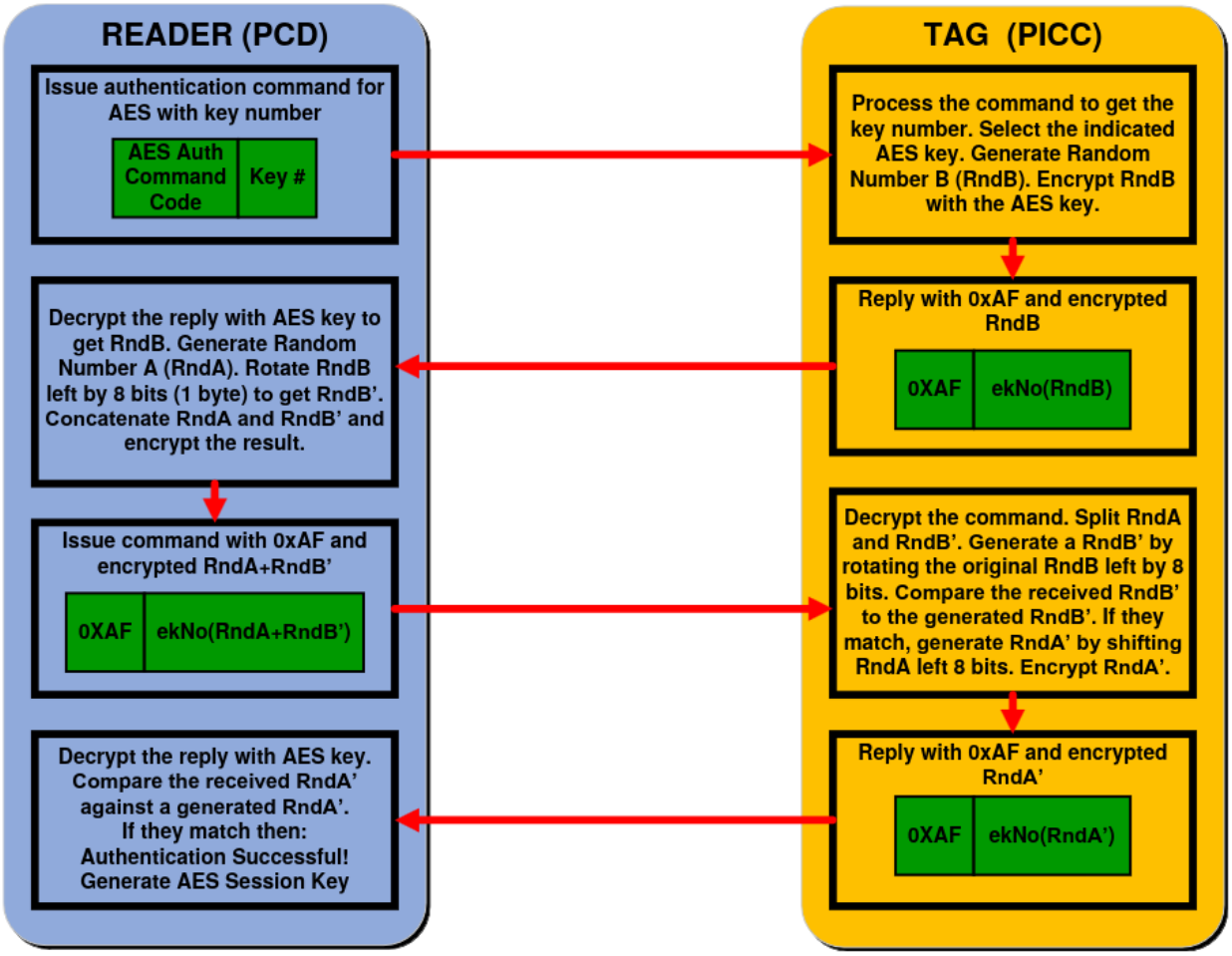


Рисунок 1.2. Послідовність автентифікації AES [7]

Механізм взаємної автентифікації AES-128 відбувається за наступним криптографічним сценарієм:

1. Зчитувач ініціює сеанс, надсилаючи картці команду на автентифікацію із зазначенням індексу системного ключа, який буде використовуватися.

2. Картка, використовуючи вбудований апаратний генератор істинних випадкових чисел (True Random Number Generator, TRNG), генерує 16-байтний випадковий блок даних, який називається RndB. Картка шифрує RndB за допомогою алгоритму AES з використанням секретного ключа, що зберігається в її захищеній пам'яті, і надсилає отриманий криптотекст зчитувачу. (Якість TRNG є критичною; будь-який дисбаланс ентропії може створити теоретичну можливість для атак).

3. Зчитувач отримує криптотекст і дешифрує його за допомогою свого примірника того ж самого секретного ключа AES, відновлюючи оригінальне значення RndB. Якщо дешифрування успішне, це доводить картці, що зчитувач володіє правильним ключем. Далі зчитувач генерує власне 16-байтне випадкове число RndA. Для продовження протоколу зчитувач виконує циклічний зсув байтів RndB вліво на одну позицію (на 8 біт), отримуючи модифіковане значення RndB'. Після цього зчитувач конкатенує RndA та RndB' у єдиний 32-байтний блок, шифрує його ключем AES і відправляє картці.

4. Картка отримує цей подвійний блок і дешифрує його. Вона вилучає RndB' і порівнює його з результатом циклічного зсуву того RndB, який вона згенерувала на початку. Якщо значення абсолютно збігаються, картка успішно автентифікує зчитувач. Збіг гарантує, що зчитувач не лише знає секретний ключ, але й бере активну участь у поточному сеансі зв'язку.

5. На останньому етапі картка виконує циклічний зсув RndA вліво на 8 біт, отримуючи RndA', шифрує його і відправляє назад до зчитувача.

6. Зчитувач дешифрує повідомлення і перевіряє правильність RndA'. За умови успішної валідації взаємну автентифікацію завершено. Після цього на базі значень RndA та RndB обидві сторони динамічно генерують унікальний тимчасовий сесійний ключ (Session Key), який буде використовуватися для

шифрування (або обчислення криптографічної контрольної суми CMAC) усіх подальших даних під час цієї транзакції.

Попри абсолютну математичну стійкість алгоритму AES-128, фізична реалізація криптопроцесорів у RFID-мітках може бути вразливою до так званих атак побічними каналами (Side-Channel Attacks, SCA). Дослідники довели можливість проведення диференціального електромагнітного аналізу (DEMA). Суть методу полягає в тому, що під час виконання операцій нелінійного перетворення (SubBytes) в алгоритмі AES або DES, кристалічний чип випромінює мікроскопічні коливання електромагнітного поля, форма та амплітуда яких прямо залежить від значень бітів секретного ключа , . Збираючи та статистично аналізуючи тисячі електромагнітних слідів (traces) під час процесу автентифікації, зловмисник може теоретично відновити секретний ключ. Однак виробники чипів DESFire останніх поколінь активно впроваджують апаратні контрзаходи проти EMA: випадкові затримки, перемішування інструкцій та паралельне виконання холостих операцій, що робить електромагнітний підпис нерозбірливим для аналізу .

1.4.2. Біометрична ідентифікація: ємнісні сканери відбитків та криптографічний захист шаблонів

Серед біометричних методів доступу відбиток пальця залишається одним з найбільш поширених завдяки балансу між точністю та зручністю. Проте традиційні оптичні сканери відбитків, які використовують систему лінз та світлочутливих елементів (CMOS/CCD) для отримання двовимірного зображення папілярних ліній, продемонстрували критичну вразливість. Їх порівняно легко ввести в оману, використовуючи двовимірні високоякісні фотографії або муляжі з силікону чи желатину.

Для вирішення проблеми стійкості до підробок у сучасній гібридній панелі використовуються ємнісні сканери відбитків пальців (Capacitive

Fingerprint Sensors). Ці датчики базуються на вимірюванні різниці електричної ємності мікроконденсаторів. Сенсор являє собою кремнієвий чип, на поверхні якого сформована двовимірна матриця, що містить десятки тисяч мікроскопічних струмопровідних пластин. Коли користувач прикладає палець до сенсора, поверхня шкіри виконує роль другої, заземленої обкладинки кожного з цих мікроконденсаторів.[17]

Фізичний принцип отримання зображення описується формулою плоского конденсатора:

$$C = \frac{\varepsilon_0 \varepsilon_r A}{d}$$

де C — електрична ємність, ε_0 — електрична стала, ε_r — відносна діелектрична проникність ізолюючого шару, A — площа пластини сенсора, а d — ефективна відстань між пластиною та шкірою.

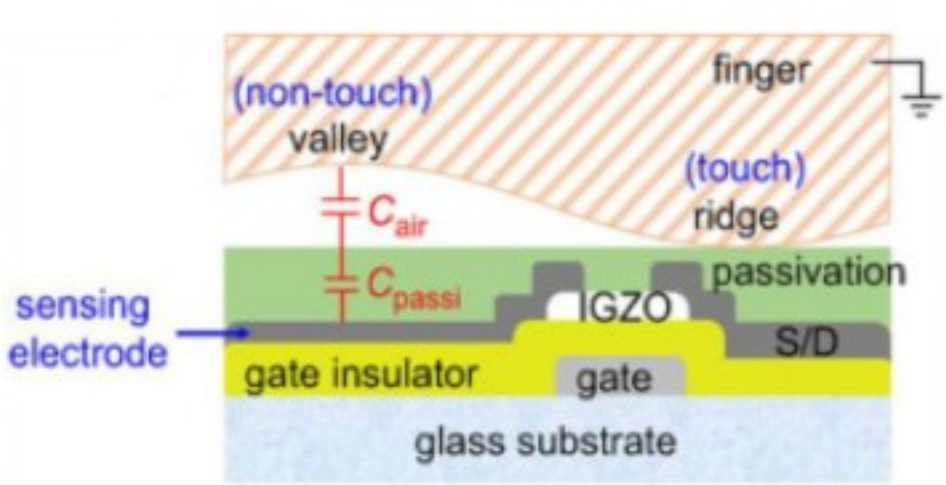


Рисунок 1.3. Принцип роботи ємнісного сенсорного датчика відбитків пальців[8]

Оскільки папілярний візерунок має рельєф, гребені (ridges) відбитка прилягають до захисного покриття сенсора практично впритул, утворюючи конденсатори з високою ємністю. Натомість западини (valleys) утворюють мікроскопічний повітряний зазор. Відносна діелектрична проникність

повітря ($\varepsilon \approx 1$) значно нижча за проникність епідермісу та захисного шару, а відстань d збільшується. Як наслідок, мікроконденсатори, розташовані під западинами, фіксують значно нижчу ємність. Електронна схема сенсора швидко почергово сканує заряди кожного мікроконденсатора, перетворюючи їх за допомогою АЦП у цифровий масив. Отриманий масив формує точне цифрове зображення відбитка пальця з 256 градаціями сірого кольору (8-bit grayscale), відтворюючи не лише поверхневий малюнок, але й структуру підшкірного шару електролітів. Оскільки для зміни ємності необхідна наявність провідного біологічного об'єкта, ємнісні сенсори володіють природною стійкістю до більшості видів неструмопровідних муляжів та надрукованих фотографій. [8]

Захист біометричних шаблонів (Biometric Template Protection).

Фундаментальною проблемою використання біометрії в системах контролю доступу є невідкличність біометричних характеристик. Якщо пароль чи RFID-картку у разі компрометації можна легко замінити, то скомпрометований відбиток пальця замінити неможливо. Тому зберігання прямих цифрових знімків відбитків у базах даних панелі або хмарних серверах є грубим порушенням політик інформаційної безпеки.

Для захисту конфіденційності мешканців розроблювана система повинна застосовувати передові алгоритми незворотного біометричного хешування (Cancelable Biometrics або Bio-hashing).

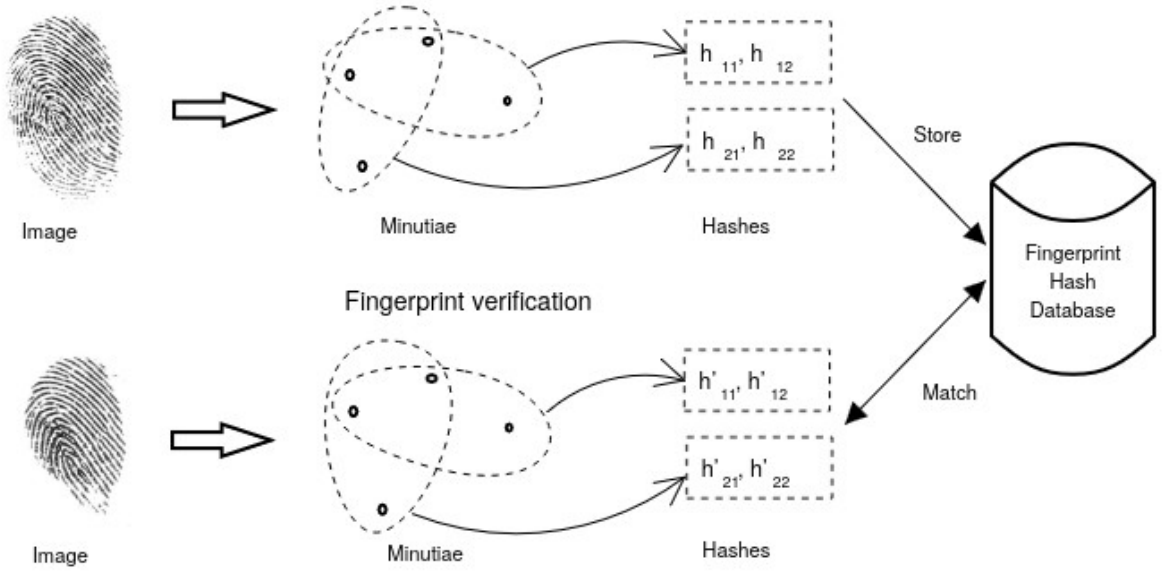


Рисунок 1.4. Застосування алгоритму хешування [9]

Процес обробки відбувається виключно у захищеній пам'яті (Secure Enclave) процесора сенсора і виглядає наступним чином:

1. Замість збереження повного зображення, алгоритм екстракції ознак виділяє набір ключових точок — мінуцій (minutiae), що характеризують закінчення папілярних ліній та їх розгалуження (біфуркації).

2. Набір координат мінуцій уявляється як багатовимірний математичний вектор. Для забезпечення безпеки до цього вектора застосовуються необоротні геометричні трансформації (наприклад, перетворення Арнольда — Arnold Cat Map), які перемішують і заплутують просторові координати мінуцій залежно від секретного криптографічного ключа користувача .

3. Модифікований набір даних проходить через симетричні хеш-функції, генеруючи фіксований бінарний хеш-код за допомогою алгоритмів криптографічного хешування, таких як SHA-256.

У процесі автентифікації відсканований палець також проходить етап екстракції та хешування. Оскільки невеликі зміщення пальця при скануванні неминучі, порівняння здійснюється не шляхом точного побітового

порівняння (як для паролів), а шляхом розрахунку евклідової відстані або відстані Геммінга між двома хеш-векторами. Якщо відстань менша за встановлений поріг (Threshold), автентифікація визнається успішною. Найголовніше: навіть у разі хакерського зламу бази даних гібридної панелі, відновити оригінальний малюнок відбитка з викраденого хеш-вектора математично неможливо. А за необхідності змінити «біометричний пароль», адміністратор може просто згенерувати новий хеш за допомогою іншого ключа трансформації для того ж самого пальця [9].

1.4.3. Біометрія: Розпізнавання облич та технології Face Anti-Spoofing (FAS)

Розпізнавання обличчя впевнено стає новим стандартом для зручного та повністю безконтактного доступу до житлових комплексів. Однак масове впровадження класичних 2D-систем розпізнавання виявило їхню критичну вразливість до атак підміни біометричних даних (Presentation Attacks, PA), які в індустрії називаються спуфінгом. Зловмисники намагаються ввести систему в оману (Spoofing) за допомогою різних інструментів (Presentation Attack Instruments, PAI): демонстрації високоякісних роздрукованих фотографій авторизованої особи, відтворення записаних відео на екранах смартфонів або планшетів високої роздільної здатності, або використання складних 3D-масок з силікону чи пластику . Дослідження показують, що звичайні алгоритми розпізнавання, засновані на виділенні контрольних точок на 2D-зображеннях (Face Landmarks), можуть бути обдурені такими методами з імовірністю понад 70% .

Для боротьби з цими загрозами сучасні гібридні панелі інтегрують багаторівневі системи визначення живості (Liveness Detection) та технології Face Anti-Spoofing (FAS). Найсучасніші дослідницькі підходи базуються на використанні багатомодальних оптичних датчиків та алгоритмів глибокого машинного навчання (Deep Learning) [10].

Багатомодальний аналіз та просторова карта глибини (Depth Map Analysis).

Найнадійнішим апаратним методом протидії є використання стереоскопічних камер, датчиків структурованого світла (Structured Light) або камер часу польоту (Time-of-Flight, ToF), що дозволяють окрім RGB-спектру захоплювати тривимірну структуру об'єкта . Камера структурованого світла проектує на обличчя людини матрицю з тисяч інфрачервоних точок, зчитуючи їх деформацію для створення високоточної 3D-карти глибини (Depth Map) у режимі реального часу. Підроблені фотографії або екрани планшетів мають абсолютно плоску геометрію, що миттєво відхиляється алгоритмами. Однак, як засвідчують новітні дослідження, навіть такі системи можуть бути атаковані за допомогою проекції підроблених тіней на плоскі фотографії (атаки типу DepthFake).

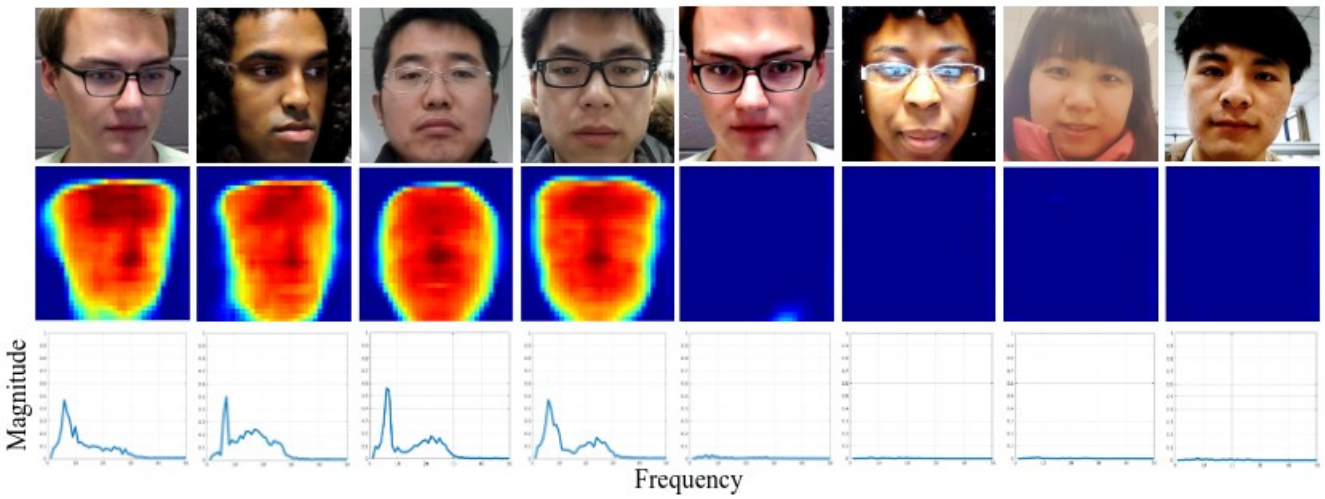


Рисунок 1.5. 8 успішних прикладів боротьби зі спуфінгом та їх розрахункові карти глибини та сигнали rPPG [11]

Щоб подолати ці недоліки, передові архітектури використовують двопотокові згорткові нейронні мережі (CNN), які навчаються одночасно на текстурних RGB-зображеннях та оціночних картах глибини . Нейромережа шукає не лише плоску геометрію, але й мікроскопічні артефакти: дефекти

друкарського растра на папері, пікселізацію матриці дисплея, або специфічне відбиття світла (відблиски) від силіконових масок у ближньому інфрачервоному діапазоні (NIR) [11].

Дистанційна фотоплетизмографія (rPPG).

Одним із найінноваційніших програмних підходів до визначення живості є метод дистанційної фотоплетизмографії (remote Photoplethysmography, rPPG) . Цей метод базується на складному спектральному аналізі відеопотоку обличчя людини. При кожному серцевому скороченні об'єм крові в капілярах підшкірного шару обличчя дещо збільшується, що призводить до мікроскопічних, непомітних для людського ока періодичних змін кольору шкіри та інтенсивності відбиття світла у червоному та зеленому каналах RGB-спектру. Алгоритми rPPG, засновані на рекурентних нейронних мережах з довгою короткостроковою пам'яттю (RNN-LSTM), здатні виділити цей ритмічний пульсуючий сигнал на фоні шумів камери. Оскільки жоден відомий вид атаки — ані фотографія, ані відеозапис з частотою кадрів, що не збігається з фазою, ані 3D-маска — не має природного серцебиття, rPPG забезпечує надзвичайно високу точність класифікації «живий об'єкт проти муляжу» [11].

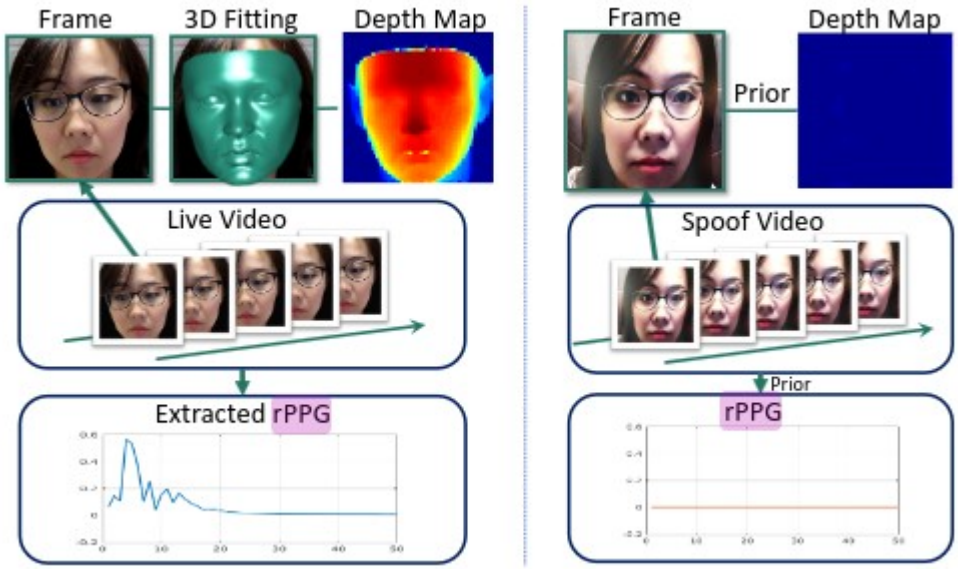


Рисунок 1.6. Приклади карт глибини наземних даних та сигналів rPPG [11]

Використання Vision Transformers (ViT).

Останнім словом у розвитку алгоритмів комп'ютерного зору для FAS є відмова від класичних згорткових мереж на користь архітектури Vision Transformers (ViT). На відміну від CNN, які фокусуються на локальних ознаках зображення за допомогою згорточних ядер, ViT застосовує механізм «уваги» (Self-Attention) для захоплення глобальних контекстуальних залежностей між віддаленими ділянками обличчя. Використання тривимірних згорток (3D CNN) у поєднанні з трансформерами дозволяє системі ефективно вловлювати як просторові (текстурні аномалії матеріалу), так і часові (динаміка міміки, моргання очей) просторово-часові залежності в режимі реального часу. Такі комплексні моделі досягають вражаючого рівня середньої помилки класифікації (ACER) менше 0.005 на складних наборах даних [12].

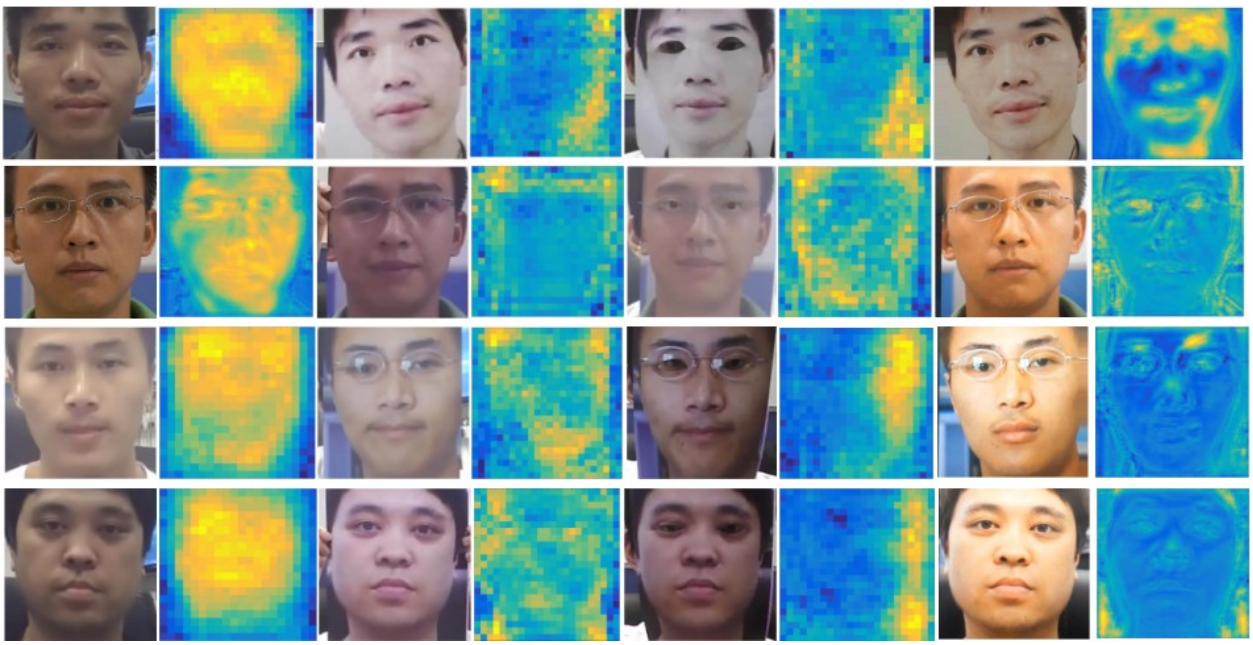


Рисунок 1.7. Оцінка глибини на тестованих CASIA-FASD об'єктах. Перші два стовпці – це живі зображення та відповідні їм карти глибини, решта шість стовпців – це три різні типи атак підробки (атаки на друк, вирізаний друк та відео) та відповідні їм карти глибини [12]

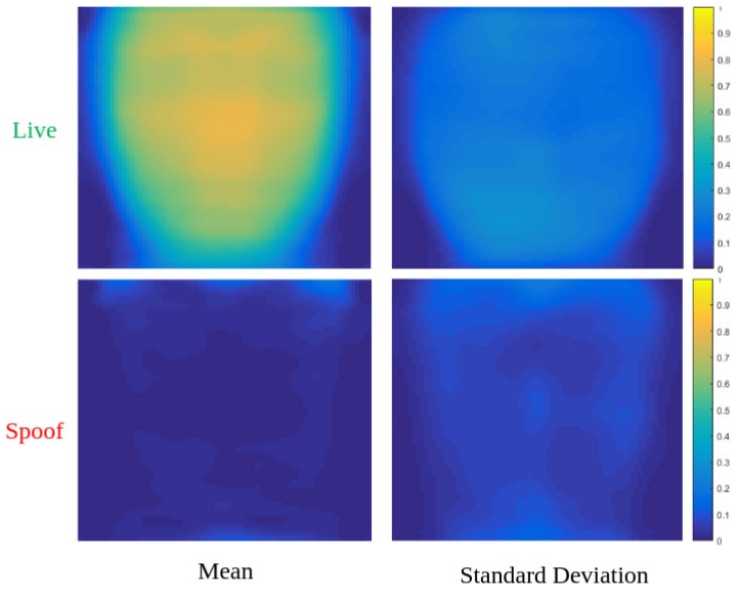


Рисунок 1.8. Середнє значення та стандартне відхилення оцінених карт глибини живих та пародійних облич для всіх тестових зразків у Reaply-Attack[12]

Аналізуючи результати на тестових об'єктах бази CASIA-FASD, можна чітко простежити фундаментальну відмінність у просторовій топології живих та підроблених облич. Для живих зразків згенерована карта глибини має виражений градієнт, що достовірно відображає тривимірну структуру людського обличчя, де виступаючі частини (наприклад, ніс та вилиці) характеризуються вищими значеннями інтенсивності. Натомість для всіх типів атак — звичайної роздруківки, вирізаного фото та відтворення з екрана пристрою — карти глибини демонструють відсутність анатомічної рельєфності. Замість тривимірної структури спостерігається рівномірний шумовий розподіл або загальна площинність, що є прямим наслідком двовимірної фізичної природи носія підробки.

1.4.4. Bluetooth Low Energy (BLE) та алгоритмічний аналіз RSSI для режиму «Вільні руки»

Інтеграція модулів бездротового зв'язку стандарту Bluetooth Low Energy (BLE 4.0 та вище, зокрема BLE 5.0) відкрила нові можливості для безконтактної ідентифікації та локального позиціонування смартфонів користувачів. На відміну від класичного Bluetooth (BR/EDR), BLE розроблений для періодичної передачі коротких пакетів даних (Advertising Packets) на частоті 2.4 ГГц з надзвичайно низьким енергоспоживанням, що дозволяє модулю смартфона бути постійно активним у фоновому режимі без значного розряду акумулятора .

У контексті систем контролю доступу BLE дозволяє реалізувати найбільш комфортний для мешканців режим доступу «Вільні руки» (Hands-free). Згідно з цим сценарієм, гібридна панель безперервно сканує ефір. Застосунок у смартфоні мешканця передає криптографічно захищений токен автентифікації. Як тільки смартфон наближається до панелі на заздалегідь визначену відстань (наприклад, 1-2 метри), система автоматично розпізнає авторизований пристрій і відчиняє замок дверей, не вимагаючи від користувача діставати телефон з кишені чи сумки.

Ключовою технічною проблемою цього процесу є точне визначення відстані (Proximity Zone Detection). Основою для вимірювання відстані в системах BLE є індикатор рівня отриманого радіосигналу (RSSI — Received Signal Strength Indicator) . Теоретично, втрата потужності радіосигналу в просторі описується логарифмічною моделлю поширення радіохвиль (логарифмічно-нормальним законом загасання), яка ґрунтується на рівнянні передачі Фрііса (Friis transmission equation):

$$P_r = \frac{P_t G_t G_r \lambda^2}{(4\pi d)^2}$$

де P_r — потужність прийнятого сигналу (RSSI в дБм), P_t — потужність передавача, G_t та G_r — коефіцієнти посилення антен, d — відстань між

пристроями, а λ — довжина хвилі. Згідно з моделлю, рівень RSSI повинен передбачувано знижуватися мірою віддалення смартфона від панелі.

Однак на практиці, у закритих приміщеннях, під'їздах чи біля вхідних груп будинків, ідеальна модель не працює через явище сильного багатопроменевого поширення (Multipath Fading). Радіохвилі багаторазово відбиваються від металевих дверей, залізобетонних стін та підлоги, утворюючи конструктивну та деструктивну інтерференцію в точці прийому. Більше того, людське тіло складається переважно з води, яка сильно поглинає радіочастоти 2.4 ГГц (тілесна абсорбція). Якщо смартфон знаходиться в задній кишені брюк, сигнал буде значно слабшим, ніж якщо він знаходиться в руках. Це спричиняє хаотичні та глибокі флуктуації виміряного RSSI (шум сигналу). Якщо алгоритм покладатиметься лише на миттєве значення RSSI, це неминуче призведе до хибних спрацьовувань замка (коли людина знаходиться ще за 5-10 метрів від дверей, але сигнал випадково посилився інтерференцією), або навпаки, до відмови у доступі перед самими дверима.

Для вирішення проблеми стабілізації RSSI та точного визначення зони доступу, мікроконтролер гібридної панелі використовує складні алгоритми математичної фільтрації часових рядів:

Корекція просторового зміщення (Offset Correction) та Фільтр ковзного середнього (MAF).

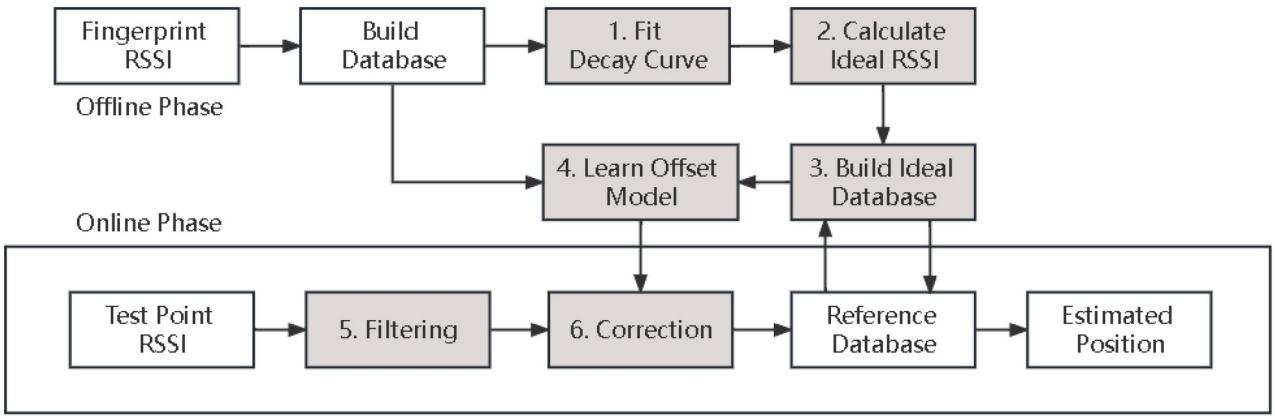


Рисунок 1.9. Схема робочого процесу методу корекції зміщення RSSI [13]

Сирі значення RSSI спочатку пропускаються через фільтр ковзного середнього (Moving Average) для придушення випадкових флуктуацій сигналу в реальному часі. Далі відфільтровані дані проходять через спеціальну модель корекції, побудовану на базі машинного навчання (SVR), яка перетворює реальний спотворений сигнал на «ідеальний». Ця модель ефективно компенсує постійні помилки середовища (поглинання меблями, нерегулярні відбиття від стін), які неможливо усунути звичайними фільтрами, спираючись на попередньо розраховану еталонну логарифмічну криву загасання (LNSM). Це дозволяє суттєво підвищити якість вхідних даних ще на етапі попередньої обробки, не дозволяючи алгоритму позиціонування хибно ідентифікувати координати [13].

Алгоритми частотно-часових вікон (Time Window based detection).

Для підвищення надійності режиму «Вільні руки», детектор доступу використовує евристичний підхід часових вікон . Детектування наближення об'єкта до критичної зони (наприклад, ближче 1 метра) фіксується і підтверджується лише тоді, коли відфільтрований рівень RSSI не просто перевищує заданий поріг ($RSSI_{Threshold}$), а стабільно утримується вище цього порогу протягом заданого часового проміжку Δ (наприклад, 1.5 - 2 секунди) зі стабільною частотою отримання пакетів. Це дозволяє системі розрізнити цілеспрямований рух людини безпосередньо до дверей від простого проходження повз будівлю на межі радіусу дії сигналу.

Захист самого каналу передачі даних BLE забезпечується механізмами стандарту Bluetooth 5.0, що включає криптографічне зв'язування пристроїв (Bonding) з використанням протоколу узгодження ключів на еліптичних кривих (Elliptic Curve Diffie-Hellman, ECDH). Дані шифруються симетричним алгоритмом AES-CCM на канальному рівні. Такий захист унеможливлює перехоплення MAC-адреси або автентифікаційного токена смартфона та їхнє подальше використання для підробки цифрової ідентичності [14].

РОЗДІЛ 2. ТЕОРЕТИЧНЕ МОДЕЛЮВАННЯ ТА ОБҐРУНТУВАННЯ КОНЦЕПЦІЇ ГІБРИДНОЇ СИСТЕМИ.

2.1. Опис в загальному вигляді природи технологічного об’єкту керування і процесів, що протікають в ньому

Об’єктом керування є система фізичного доступу до багатоквартирного будинку та її комунікаційна інфраструктура. Розроблювана гібридна панель виклику виконує роль системного контролера, який аналізує вхідні дані, формує керуючі впливи на замикаючі пристрої вхідної групи та координує інформаційні потоки між абонентами.

Функціонування об'єкта охоплює чотири ключові технологічні процеси. Першим є процес ідентифікації та переведення вхідної групи у стан «Відчинено». Для його реалізації передбачено алгоритмічну обробку сигналів від безконтактних міток доступу, пеленгацію мобільних пристроїв (режим «Вільні руки», радіус 0,5–3 м) та розпізнавання біометричних векторів (до 0,5 с із обов'язковим застосуванням алгоритмів Anti-spoofing). Альтернативні контури відкриття реалізовано через Cloud API або локальну кодопанель.

Другим критичним процесом є двостороння маршрутизація викликів (паралельне сповіщення).

Третій і четвертий процеси — це розподіл медіапотоків та системне логування подій. Відеоінформація транслюється двома незалежними потоками: у цифрову IP-мережу (від 2 Мп Full HD, кут огляду від 110°) та як аналоговий сигнал (CVBS/AHD) для локальних реєстраційних пристроїв. Будь-яка зміна стану об'єкта миттєво фіксується: логуються ідентифікатори ключів, факти проходу та помилкові спроби авторизації. Це доповнюється автоматичною фотофіксацією відвідувача та синхронізацією даних із хмарною системою керування.

Динаміка об'єкта описується дискретно-подієвою моделлю, де вхідними збуреннями є випадкові запити на доступ або зв'язок. Основне

завдання керування, яке я вирішувала у цьому розділі, полягає у мінімізації часу реакції системи на події, забезпеченні надійної координатної комутації та гарантуванні безперебійного контролю фізичного периметра об'єкта.

2.2. Визначення регульованих параметрів, збурень і можливих дій керування

Визначимо регульовані параметри системи контролю доступу (де об'єктом керування є стан дверей та комунікаційних каналів):

- Стан виконавчого механізму (електромеханічного або магнітного замка дверей) – відкрито або закрито.
- Стан каналів зв'язку – встановлення аудіо/відео з'єднання між викличною панеллю та конкретним абонентом.
- Маршрутизація виклику – паралельне направлення сигналу на аналогову трубку в квартирі та PUSH-повідомлення у хмарний мобільний застосунок.
- Режим роботи модуля бездротового зв'язку Bluetooth (BLE) – активний або пасивний («Вільні руки») із заданою дистанцією спрацьовування від 0,5 до 3 метрів.
- Стан інформаційного дисплея панелі – відображення номера квартири та поточних статусів (Виклик, Розмова, Відкрито).

Також визначимо можливі збурення, які впливають на об'єкт керування. Їх можна розділити на штатні (інформаційні впливи) та нештатні (спроби обходу безпеки або фізичний вплив):

- Введення гостем номера квартири на клавіатурі панелі.
- Наближення мешканця зі смартфоном (з увімкненим Bluetooth) у радіус дії панелі.
- Фізичний дотик до біометричного датчика відбитків пальців або потрапляння обличчя в поле зору 3D-модуля (Face ID).

- Прикладання карти чи брелока стандарту Mifare Desfire.
- Надходження команди «Дистанційне відкриття» з мобільного застосунку через Cloud API.
- Невдалі спроби вводу персонального цифрового коду.
- Спроба несанкціонованого доступу шляхом використання фотографій чи відео замість реального обличчя.
- Спроба підбору паролів та копіювання ключів.
- Вплив екстремальних температур навколишнього середовища (від -40°C до +50°C) та спроби вандалізму.

2.3. Параметрична схема ОК, її фізичні величини вхідних та вихідних сигналів, збурюючих впливів

Складемо параметричну схему системи керування (де гібридна багатоквартирна IP-панель виклику виступає керуючим пристроєм) та вкажемо фізичні величини вхідних та вихідних сигналів, а також збурюючих впливів, з якими працює система.

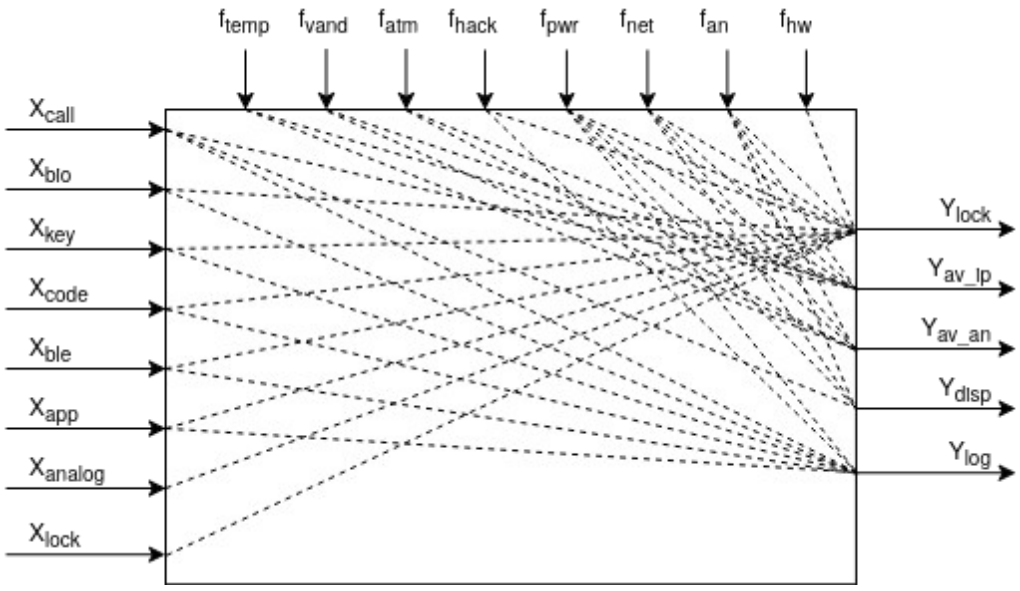


Рисунок 2.1. Параметрична схема системи керування

Керувальні впливи (Вхідні сигнали):

- X_{call} – виклик абонента шляхом введення номера квартири на панелі.
- X_{bio} – біометричні дані, отримані через дотик до ємнісного сканера відбитків пальців або 3D-модуля розпізнавання обличчя.
- X_{key} – зашифровані дані ідентифікації при прикладанні карти або брелока формату Mifare Desfire до зчитувача.
- X_{code} – персональний цифровий код, введений користувачем на клавіатурі.
- X_{ble} – ідентифікаційні дані смартфона, отримані через модуль Bluetooth (BLE) у радіусі від 0.5 до 10 метрів.
- X_{app} – команда дистанційного відкриття дверей, що надходить із мобільного застосунку через Cloud API.
- X_{analog} – керівний електричний сигнал на відкриття від аналогової трубки чи стороннього відеодомофона.

Збурення:

- f_{temp} – температурний вплив навколишнього середовища, який панель повинна витримувати в межах від -40°C до +50°C.
- f_{vand} – механічні (вандальні) впливи на корпус пристрою, від яких захищає антивандальна конструкція (клас IK08/IK09).
- f_{atm} – атмосферні впливи, такі як волога та пил (клас захисту IP65).
- f_{hack} – спроби несанкціонованого доступу, включаючи використання фотографій чи відео замість реального обличчя (захищається технологією Anti-spoofing), підбір паролів та спроби копіювання ключів (блокується алгоритмами AES/DES).
- f_{pwr} — Відсутність або нестабільність напруги живлення. Це критичне збурення, що виникає при аварійних відключеннях основної мережі живлення, що може призвести до повного вимкнення пристрою або переходу в режим обмеженої функціональності.

- f_{net} — Втрата інтернет-з'єднання або затримки в мережі. Впливає на роботу IP-технологій, зокрема на можливість відправки PUSH-повідомлень у мобільний застосунок та зв'язок із хмарою.
- f_{an} — Несправність аналогової лінії або комутатора. Коротке замикання або обрив в координатно-матричній системі (до 300 трубок), що унеможливлює виклик мешканця через класичну трубку.
- f_{hw} — Апаратне забруднення або вихід з ладу сенсорів. Наприклад, забруднення поверхні ємнісного сканера відбитків пальців або об'єктива камери, що знижує точність біометричної ідентифікації.

Вихідні параметри (Реакція системи):

- Y_{lock} – вихідний керуючий сигнал на спрацювання електромеханічного або магнітного замка дверей (відкриття).
- Y_{av_ip} – вихідний цифровий відеопотік з роздільною здатністю не менше 2Мп (Full HD) та аудіосигнал, що передаються по мережі Ethernet за протоколами SIP, TCP/IP, RTSP.
- Y_{av_an} – вихідний аналоговий відеосигнал (CVBS/AHD) та аудіосигнал для паралельного підключення до старих моніторів, аналогових трубок або сторонніх відеореєстраторів.
- Y_{disp} – вихідна інформація для користувача на вбудованому дисплеї (відображення номера квартири та статусів: Виклик, Розмова, Відкрито).
- Y_{log} – вихідні пакети даних журналу подій (відкриття ключем, через додаток, невдалі спроби) та фотофіксація відвідувачів, які відправляються на хмарну платформу (Cloud Management).

Математично залежність вихідних параметрів від вхідних впливів та збурень у загальному вигляді можна описати наступними функціями:

$$Y_{lock} = F\ (X_{lock}, X_{bio}, X_{key}, X_{code}, X_{ble}, X_{app}, X_{analog}, f_{hack}, f_{pwr}, f_{net}, f_{an}, f_{hw})$$

$$Y_{av\_ip} = F\ (X_{call}, f_{temp}, f_{atm}, f_{vand}, f_{pwr}, f_{net}, f_{an})$$

$Y_{av\_an} = F(X_{call}, f_{temp}, f_{atm}, f_{vand}, f_{pwr}, f_{net}, f_{an})$

$Y_{disp} = F(X_{call}, Y_{lock}, f_{pwr}, f_{net}, f_{an})$

$Y_{log} = F(X_{call}, X_{bio}, X_{key}, X_{code}, X_{ble}, X_{app}, f_{hack}, f_{pwr})$

2.4. Структурна схема системи керування та опис її роботи в загальному вигляді

Для кращого розуміння принципів функціонування розроблюваної гібридної IP-панелі складемо структурну схему системи керування.

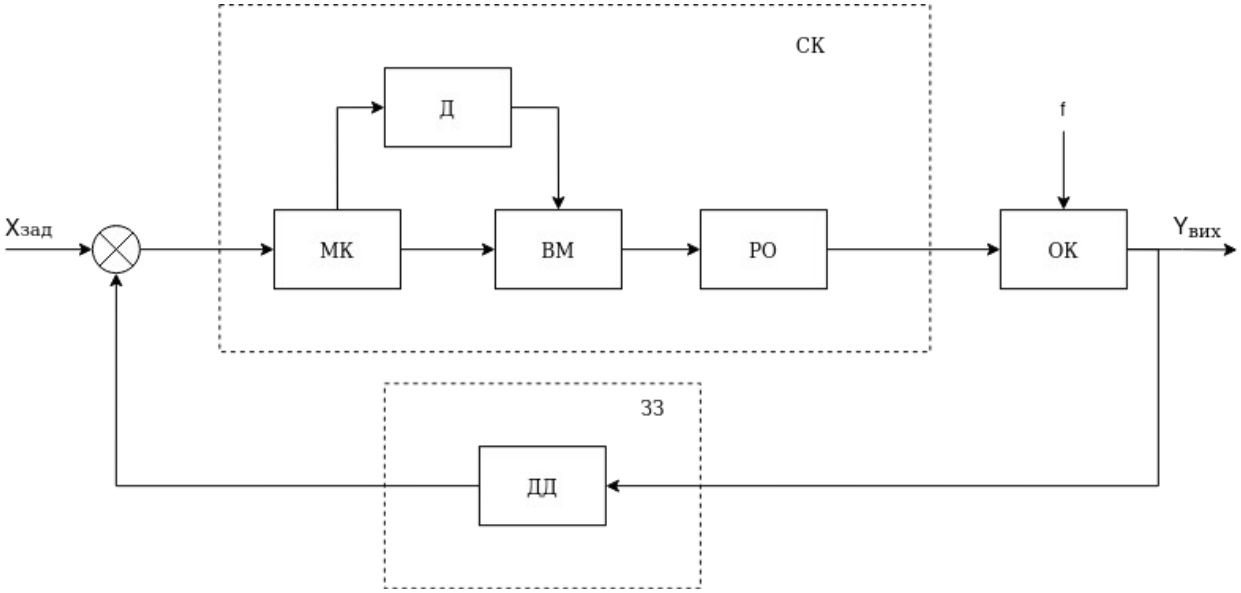


Рисунок 2.2. Структурна схема системи керування гібридної панелі виклику

Розшифрування елементів структурної схеми:

- Хзад (Задані параметри) – еталонні дані, закладені в систему: база зареєстрованих зашифрованих ключів Mifare, біометричних хешів (до 1000 шаблонів), PIN-кодів мешканців, а також налаштування маршрутизації мережі.
- Увих (Вихідні параметри) – кінцевий стан системи: фізичний стан дверей (відкрито/закрито) або стан інформаційного каналу (аудіо/відеозв'язок встановлено/розірвано).

- МК (Мікроконтролер) – основний обчислювальний центр панелі, який приймає рішення на основі закладених алгоритмів.
- ВМ (Виконавчий механізм) – внутрішні вузли, що реалізують рішення МК: мережевий модуль (для відправки PUSH-повідомлень), інтегрований комутатор (для аналогових трубок) та реле керування замком.
- РО (Регулювальний орган) – фізичні пристрої, що безпосередньо змінюють стан об'єкта: електромеханічний/електромагнітний замок або динамік панелі.
- ОК (Об’єкт керування) – контрольно-пропускний пункт (двері під'їзду) та система комунікації з абонентами.
- Д (Дисплей) – екран панелі для індикації статусів.
- ДД (Множина датчиків) – пристрої збору інформації: зчитувач ключів, ємнісний сканер відбитків, 3D-модуль Face ID, модуль Bluetooth, IP та аналогова камери.
- ЗЗ (Зворотний зв'язок) – контур передачі інформації про фактичний стан Yвих назад до системи.
- f (Збурення) – зовнішні нештатні фактори (екстремальні температури, вандалізм, спроби підбору паролів).

На етапі ініціалізації адміністратор вносить до системи задані параметри (Хзад) через веб-інтерфейс або хмарну платформу, формуючи базу ідентифікаторів та рівні доступу для мешканців.

Функціональний цикл починається, коли множина датчиків (ДД) фіксує зовнішній вплив: відвідувач вводить номер квартири, або мешканець ініціює авторизацію (дотик до сканера, зчитування обличчя, прикладання брелока чи наближення зі смартфоном по Bluetooth). Зібрані дані передаються до мікроконтролера (МК). МК аналізує ці дані, перетворюючи біометрію у зашифрований математичний хеш, та порівнює їх із заданими параметрами

(Хзад), паралельно перевіряючи алгоритми Anti-spoofing для уникнення збурень. Під час обробки МК передає сигнал на дисплей (Д), щоб відобразити користувачу поточний статус («Виклик», «Розмова»).

Якщо ідентифікація успішна або абонент прийняв виклик (першим зняв аналогову трубку чи відповів у смартфоні), мікроконтролер подає відповідний сигнал на виконавчий механізм (ВМ). Виконавчий механізм активує регулювальний орган (РО) — наприклад, подає струм на відкриття замка або з'єднує аудіоканал.

Внаслідок цих дій об'єкт керування (ОК) змінює свій стан (Yвих) — двері розблоковуються. Лінія зворотного зв'язку (ЗЗ) отримує цей вихідний сигнал (через датчик стану дверей) і передає інформацію назад до МК, який здійснює фінальне логування: записує подію в архів (хто і коли відкривав двері) та змінює статус на дисплеї на «Відкрито». Після цього цикл завершується.

РОЗДІЛ 3. ТЕХНІЧНЕ ТА АПАРАТНЕ ПРОЕКТУВАННЯ ГІБРИДНОЇ ВИКЛИЧНОЇ ПАНЕЛІ.

3.1. Принцип дії та архітектура запропонованої гібридної викличної панелі

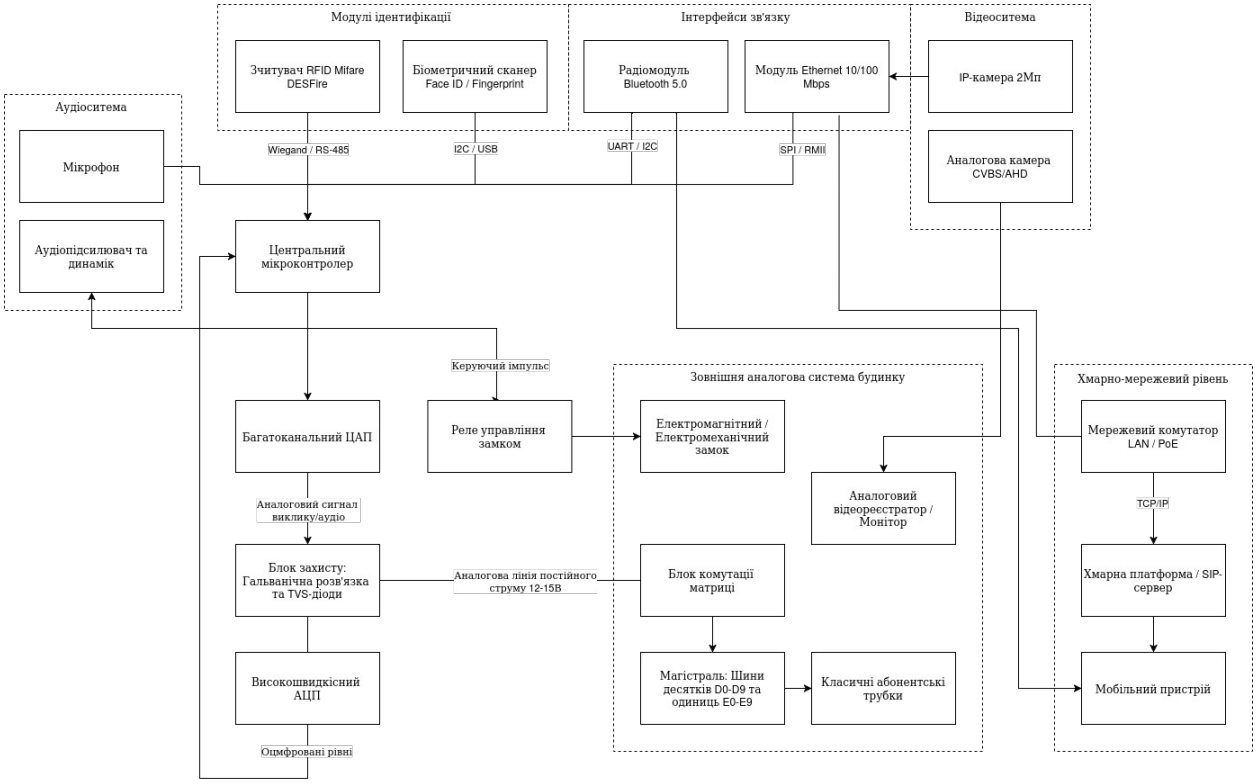


Рисунок 3.1. Структурна схема апаратної архітектури панелі

Основним обчислювальним ядром архітектури виступає центральний мікроконтролер, який виконує функції маршрутизації сигналів та керування периферійними пристроями. Локальна аудіосистема панелі, що складається з мікрофона та аудіопідсилювача з динаміком, безпосередньо підключена до контролера для забезпечення двостороннього зв'язку. Для підсистеми ідентифікації я передбачила використання зчитувача RFID стандарту Mifare DESFire, що взаємодіє з ядром через шини Wiegand або RS-485, та біометричного сканера Face ID / Fingerprint, який підключається за допомогою інтерфейсів I2C або USB.

Інтерфейси зв'язку апаратно представлені двома основними вузлами. Радіомодуль Bluetooth 5.0, підключений через UART/I2C, забезпечує пряму локальну взаємодію з мобільними пристроями абонентів. Модуль Ethernet 10/100 Mbps, що використовує шини SPI/RMII, фізично з'єднує панель із хмарно-мережевим рівнем через зовнішній мережевий комутатор LAN/PoE. Пакетна передача даних здійснюється протоколами стека TCP/IP до хмарної платформи (SIP-сервера) з подальшою маршрутизацією на мобільні пристрої користувачів. Відеосистема пристрою фізично розділена на два незалежні тракти: цифрова IP-камера (2 Мп) інтегрована для роботи з мережевим рівнем, тоді як аналогова камера постійно транслює сигнал стандарту CVBS/AHD для прямого підключення до зовнішньої аналогової системи будинку (відеореєстратора або монітора).

Апаратне сполучення мікроконтролера з високовольтними класичними абонентськими трубками я реалізувала через спеціалізований тракт перетворення. Процесор формує цифровий код, який багатоканальний ЦАП конвертує в аналоговий сигнал виклику та аудіо. Для захисту цифрової електроніки я запровадила блок гальванічної розв'язки та TVS-діодів, звідки по аналоговій лінії постійного струму напругою 12-15В сигнал надходить до блоку комутації матриці. Цей блок керує магістраллю шин десятків (D0-D9) та одиниць (E0-E9), встановлюючи фізичне з'єднання з трубками. Зворотний моніторинг стану лінії здійснюється шляхом передачі оцифрованих рівнів з блоку захисту через високошвидкісний АЦП назад до мікроконтролера.

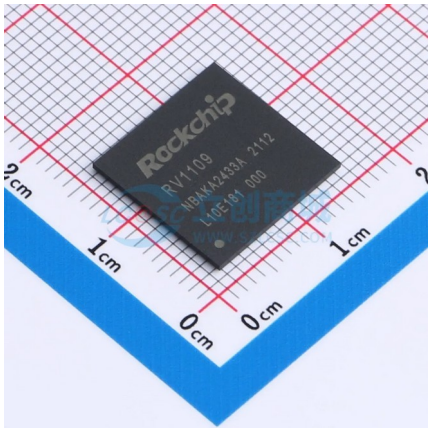
Керування виконавчими механізмами зовнішньої системи будинку здійснюється подачею керуючого імпульсу від центрального мікроконтролера на реле управління замком, яке комутує ланцюг живлення електромагнітного або електромеханічного замка.

3.2. Розробка та опис електричної принципової схеми системи керування

Для практичної реалізації розробленої архітектури здійснений підбір елементної бази. Головними критеріями вибору є забезпечення високої обчислювальної потужності для обробки медіаданих та алгоритмів, сумісність із застарілими аналоговими лініями (Vizit, Cyfral), економічна доцільність для масового впровадження та доступність компонентів на ринку.

Центральний процесор Rockchip RV1109. Обраний для локального виконання алгоритмів комп'ютерного зору. Вбудований NPU на 1.2 TOPS забезпечує роботу Face Liveness Detection та розпізнавання облич до 0.5 с. Двопотоковий кодек H.264/H.265 реалізує одночасне стиснення Full HD відео (RTSP) та низькобітрейтного потоку (SIP), мінімізуючи тепловиділення в герметичному корпусі.

Таблиця 3.1. Характеристики Rockchip RV1109

Назва елемента та маркування	Основні технічні характеристики	Зовнішній вигляд
Rockchip RV1109 Центральний SoC	Dual Core ARM Cortex-A7 (1.0 GHz), RISC-V MCU, NPU 1.2 TOPS, H.264/H.265 HW кодек.	

Цифрова IP-камера Sony IMX307. Використовує технологію зворотного підсвічування Starvis для високої чутливості за низької освітленості. Забезпечує чіткість текстур у ближньому інфрачервоному діапазоні (NIR) для

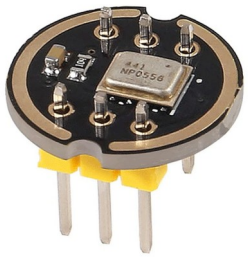
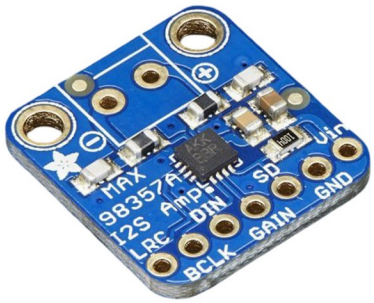
коректної роботи 3D CNN у задачах Face Anti-Spoofing. Підключення через інтерфейс MIPI CSI усуває затримки кадрів та джиттер.

Таблиця 3.2. Характеристики Sony IMX307

Назва елемента та маркування	Основні технічні характеристики	Зовнішній вигляд
Sony IMX307 Цифрова IP-камера	Матриця 1/2.8" CMOS, 2 Мп (Full HD), технологія Starvis, інтерфейс MIPI CSI, підтримка NIR..	

MEMS-мікрофон INMP441 та аудіопідсилювач MAX98357A. Забезпечують повністю цифрову топологію звукового тракту. Всеспрямований мікрофон із 24-бітним АЦП та підсилювач класу D підключені по шині I2S безпосередньо до процесора, що виключає аналогові фільтри й операційні підсилювачі. Це нівелює електромагнітні завади від замка і комутатора, гарантуючи роботу алгоритмів ехоприглушення (AEC) при VoIP-зв'язку.

Таблиця 3.3. Характеристики INMP441 та MAX98357A

Назва елемента та маркування	Основні технічні характеристики	Зовнішній вигляд
INMP441 MEMS-мікрофон	Всеспрямований цифровий мікрофон, вбудований 24-бітний АЦП, інтерфейс I2S, SNR 61 dBA.	
MAX98357A Аудіопідсилювач	Підсилювач класу D, вбудований ЦАП, інтерфейс I2S, потужність до 3.2 Вт (навантаження 4 Ом).	

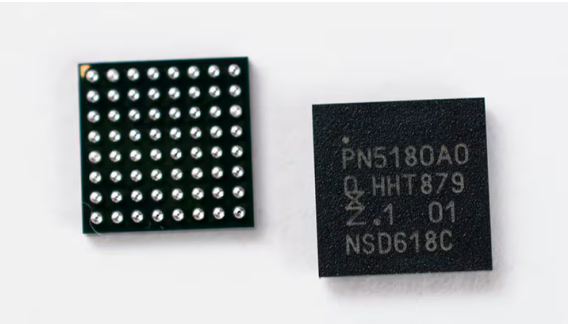
Ethernet PHY трансивер LAN8720A. Обраний через компактний корпус QFN-24 та інтерфейс RMII, що економить виводи процесора. Підтримує узгодження рівнів сигналів у лініях "витої пари" до 100 м при живленні по PoE (IEEE 802.3af). Сумісність із Keep-Alive запитами на рівні ядра Linux RV1109 дозволяє миттєво діагностувати обрив зв'язку для переходу в автономний режим.

Таблиця 3.4. Характеристики LAN8720A Ethernet PHY

Назва елемента та маркування	Основні технічні характеристики	Зовнішній вигляд
LAN8720A Ethernet PHY трансивер	Швидкість 10/100 Mbps Fast Ethernet, інтерфейс RMII, сумісність із PoE (IEEE 802.3af).	

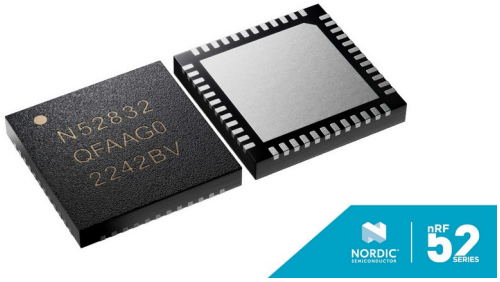
RFID/NFC зчитувач NXP PN5180. Володіє підвищеною вихідною потужністю та системою динамічного контролю (DPC) для зчитування міток через антивандальний корпус. Необхідний для апаратної триетапної взаємної автентифікації смарт-карт MIFARE DESFire за криптоалгоритмом AES-128. Швидкісний інтерфейс SPI унеможливлює атаки типу "перехоплення-відтворення".

Таблиця 3.5. Характеристики NXP PN5180

Назва елемента та маркування	Основні технічні характеристики	Зовнішній вигляд
NXP PN5180	Високопродуктивний зчитувач 13.56 MHz, апаратна підтримка MIFARE DESFire EV2, інтерфейс SPI.	

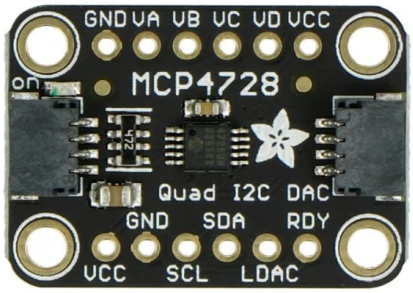
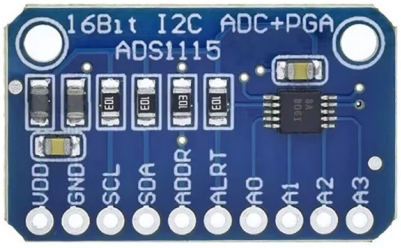
Радіомодуль BLE Nordic nRF52832. Оснащений виділеним ядром ARM Cortex-M4F, що дозволяє делегувати фільтрацію (MAF) та стабілізацію (SVR) сигналів RSSI від смартфонів на периферійний чіп без навантаження ЦП. Стандарт Bluetooth 5.0 забезпечує пеленгацію пристроїв у радіусі до 10 метрів для функції «Вільні руки».

Таблиця 3.6. Характеристики Nordic nRF52832

Назва елемента та маркування	Основні технічні характеристики	Зовнішній вигляд
Nordic nRF52832 Радіомодуль BLE	Ядро ARM Cortex-M4F, підтримка Bluetooth 5.0 Low Energy, інтерфейси UART/I2C.	

ЦАП MCP4728 та АЦП ADS1115 (Контур аналогового мосту). Виконують функцію трансляційного мосту з координатно-матричними системами (Vizit, Cyfral). Чотириканальний 12-бітний ЦАП MCP4728 із вбудованою EEPROM генерує прецизійні рівні викличної напруги під конкретні профілі. 16-бітний АЦП ADS1115 із програмованим підсилювачем квантує напругу в лінії, фіксуючи падіння опору до ~50 або ~300 Ом для точного визначення підняття трубки чи натискання кнопки відкриття.

Таблиця 3.7. Характеристики MCP4728 та ADS1115

Назва елемента та маркування	Основні технічні характеристики	Зовнішній вигляд
MCP4728 Цифро-аналоговий перетворювач	4-канальний 12-бітний ЦАП, інтерфейс I2C, вбудована енергонезалежна пам'ять EEPROM.	
ADS1115 Аналого-цифровий перетворювач	4-канальний 16-бітний прецизійний АЦП, інтерфейс I2C, вбудований підсилювач (PGA).	

Силове реле Omron G5Q-14 та елементи захисту PC817 / SMAJ15CA. Реле комутує струми до 10А, ізолюючи індуктивні навантаження електромагнітного/електромеханічного замка від плати. Оптопари PC817 забезпечують гальванічну розв'язку цифрової частини від зворотної ЕРС довгих ліній, а двоспрямовані TVS-діоди SMAJ15CA з пікосекундним часом спрацьовування обмежують імпульси перенапруги.

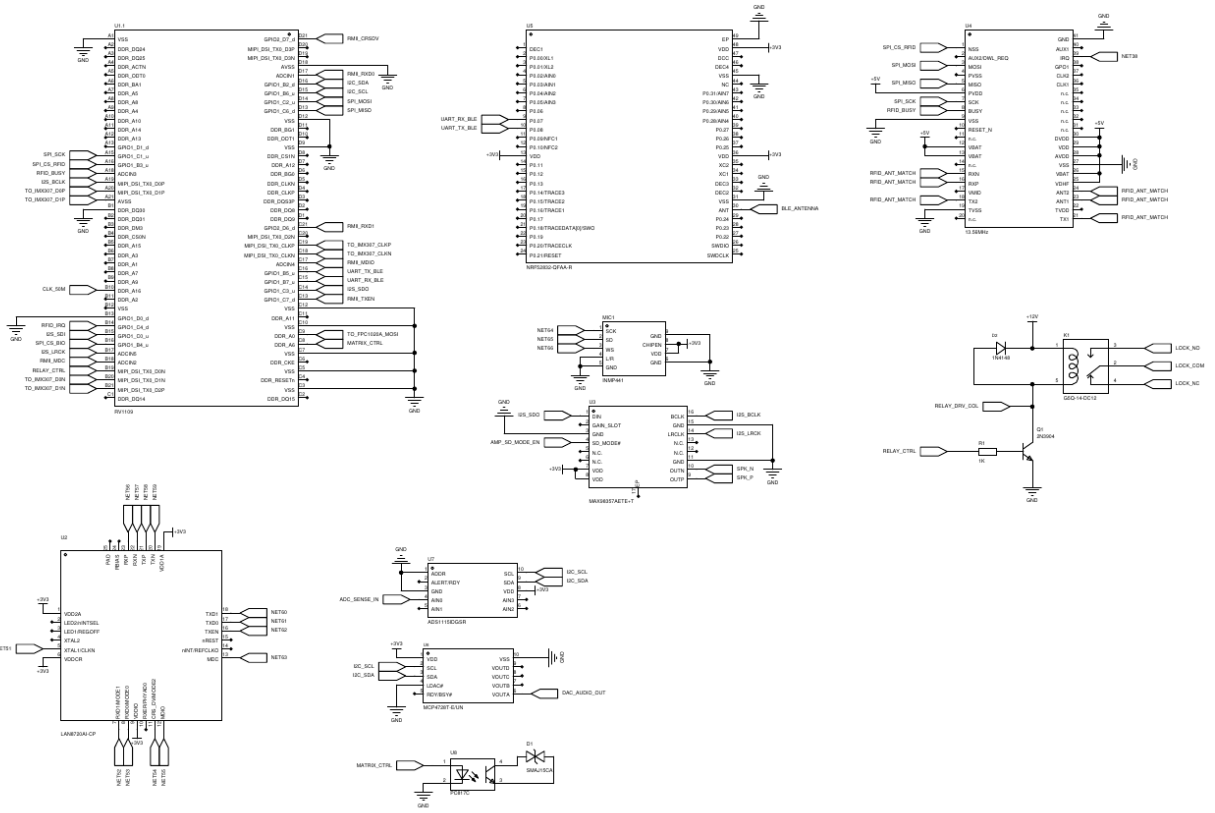


Рисунок 3.2. Електрично принципова схема панелі

Апаратна архітектура системи базується на обчислювальному ядрі Rockchip RV1109, до якого по високошвидкісній диференційній шині MIPI CSI підключено матрицю цифрової камери Sony IMX307. Аудіотракт реалізовано повністю у цифровому домені: захоплення звуку виконується MEMS-мікрофоном INMP441, а відтворення — підсилювачем класу D MAX98357A, які синхронізуються з процесором через єдину шину I2S. Мережева інфраструктура побудована на трансивері фізичного рівня LAN8720A, що взаємодіє з центральним контролером по зменшеному інтерфейсу RMII та забезпечує підключення до Ethernet із підтримкою стандарту живлення PoE. Підсистема безконтактної ідентифікації об'єднує RFID-зчитувач NXP PN5180, керований по шині SPI, та радіомодуль BLE Nordic nRF52832, що сполучається з системою через інтерфейс UART для реалізації локального позиціонування.

Критичний вузол сполучення низьковольтної логіки з високовольтною аналоговою координатною матрицею реалізовано через контур перетворення та захисту. Генерація викличних і звукових сигналів для класичних абонентських трубок здійснюється за допомогою 12-бітного ЦАП MCP4728, тоді як зворотний моніторинг стану лінії (визначення зняття трубки за зміною еквівалентного опору) виконується прецизійним АЦП ADS1115; обидві мікросхеми працюють на спільній шині I2C. Для унеможливлення пошкодження цифрових компонентів від зворотної ЕРС та імпульсних завад магістралі застосовано роздільний захист: цифрові керуючі сигнали матриці гальванічно ізольовано оптопарами PC817C, а аналогові виводи ЦАП та АЦП зашунтовано швидкодіючими двоспрямованими TVS-діодами SMAJ15CA відносно ізольованої землі. Силове керування замком виконується через електромеханічне реле Omron G5Q-14, котушка якого комутується транзисторним ключем із обов'язковим встановленням паралельного зворотного діода 1N4148 для придушення небезпечних індуктивних викидів напруги під час розмикання кола.

3.3. Апаратна реалізація мережевої інфраструктури та забезпечення стійкості з'єднання

Для повноцінної інтеграції гібридної викличної панелі з хмарними сервісами (Cloud Management), SIP-телефонією та мобільними застосунками користувачів було спроектовано надійну мережеву інфраструктуру. Оскільки пристрій виконує роль трансляційного моста між аналоговою координатно-матричною магістраллю та цифровим середовищем, забезпечення безперебійного мережевого обміну даними є критичною умовою його функціонування.

На апаратному рівні підключення до локальної мережі будівлі (LAN) реалізовано на базі інтегрального фізичного трансивера (PHY) LAN8720A-CP-TR. Даний мікросхемний модуль забезпечує роботу стандарту Fast

Ethernet зі швидкістю 10/100 Мбіт/с. Зв'язок між трансивером та центральним мікропроцесором (SoC) Rockchip RV1109 здійснюється за допомогою високошвидкісної синхронної шини RMII (Reduced Media Independent Interface). Фізичне підключення панелі до комутаційного обладнання багатоквартирного будинку виконується через стандартний роз'єм RJ-45. З метою мінімізації кількості кабельних трас та спрощення монтажу, апаратна частина підтримує технологію PoE (Power over Ethernet). Це дозволяє отримувати як інформаційний сигнал, так і напругу живлення по єдиному кабелю типу «вита пара» безпосередньо від центрального мережевого комутатора (PoE Switch), який підключений до джерела безперебійного живлення.

Обробка мережевого трафіку базується на апаратній підтримці стека протоколів TCP/IP ядром операційної системи Linux, що функціонує на базі процесора RV1109. Передача мультимедійних даних розділена на два незалежні логічні канали. Формування відеопотоку з 2-мегапіксельної IP-камери у якості Full HD (1080p) кодується апаратним кодеком H.264/H.265 та транслюється за протоколом RTSP (Real-Time Streaming Protocol) для запису на зовнішні мережеві відеореєстратори (NVR) системи безпеки будинку. Одночасно з цим, для реалізації алгоритму паралельного виклику на мобільні пристрої абонентів, використовується протокол ініціації сеансів SIP у зв'язці з RTP (Real-time Transport Protocol) для передачі голосу та відео з мінімальними затримками (UDP-трафік). Керуючі команди, зокрема дистанційне відкриття замка через застосунок користувача (Cloud API) та синхронізація бази ключів Mifare Desfire і біометричних хешів, здійснюються зашифрованими TCP-пакетами.

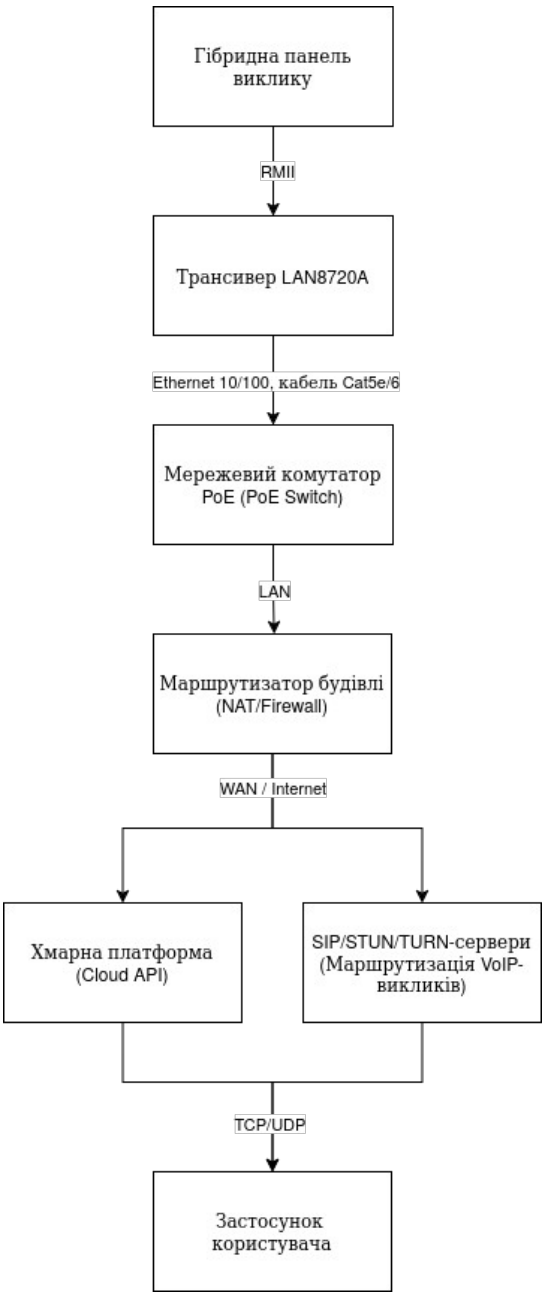


Рисунок 3.3. Схема мережевої взаємодії об'єкта керування з зовнішньою інфраструктурою

Забезпечення стійкості з'єднання та відмовостійкості системи (Fault Tolerance) реалізовано на декількох рівнях. Для запобігання апаратному та програмному зависанню мережевого стека використано апаратний сторожовий таймер (Watchdog Timer). У випадку відсутності відгуку від

мережевого інтерфейсу протягом критичного інтервалу часу, мікроконтролер примусово перезавантажує трансивер LAN8720A та переініціалізує з'єднання.

На рівні програмної логіки впроваджено алгоритми постійного моніторингу доступності шлюзу (Keep-Alive запити). У разі втрати зв'язку із зовнішнім інтернет-каналом панель автоматично переходить у локальний автономний режим. У цьому стані повністю зберігається працездатність алгоритмів ідентифікації: локально обробляються біометричні дані, зчитуються RFID-мітки та функціонує модуль BLE для режиму «Вільні руки». Всі події проходу, спроби несанкціонованого доступу та фотофіксації відвідувачів буферизуються у незалежній Flash-пам'яті пристрою. При відновленні мережевого з'єднання мікроконтролер автоматично виконує фонову синхронізацію накопиченого журналу подій із хмарною базою даних та повторно реєструє пристрій на SIP-сервері, не перериваючи процесу обслуговування абонентів через аналогові координатні лінії.

3.4. Спрощена апаратна архітектура для малобюджетних об'єктів (до 50 абонентів)

Головним завданням під час розробки цієї версії було максимальне здешевлення апаратної частини за рахунок використання інтегрованих мікроконтролерів та відмови від надлишкових обчислювальних модулів, зі збереженням базового функціоналу ідентифікації та зв'язку.

Замість високопродуктивного процесора Rockchip RV1109, який використовується в основній версії для апаратної обробки нейромереж та відео високої роздільної здатності, можна застосувати енергоефективний мікроконтролер архітектури ESP32. Цей чип має вбудовані апаратні контролери Bluetooth (BLE) та Wi-Fi, що дозволить виключити з електричної схеми окремі трансивери (NRF52832 та LAN8720A). Комутаційна матриця була масштабована з розрахунку на 5 шин десятків (D0-D4) та 10 шин

одиниць (E0-E9), що значно зменшило кількість необхідних твердотільних реле та спростило топологію друкованої плати.

Для ідентифікації користувачів лишився зчитувач карток RFID та модуль BLE для безконтактного доступу зі смартфона, однак варто повністю вилучити складний 3D-модуль розпізнавання обличчя та ємнісний сканер відбитків пальців, оскільки їхня робота вимагає значних обчислювальних ресурсів та здорожчує конструкцію. Відеосистема також зазнала оптимізації: замість двох незалежних камер (IP та аналогової) використаний єдиний бюджетний модуль камери з роздільною здатністю 1 Мп, який передає цифровий потік безпосередньо через апаратні ресурси мікроконтролера.

Таблиця 3.8. Порівняння змін спрощеної версії

Функціональний вузол	Базова архітектура (до 300 абонентів)	Спрощена архітектура (до 50 абонентів)
Обчислювальне ядро	Rockchip RV1109	ESP32-S3
Відеосистема	IP (2 Мп) + Аналогова (AHD) + 3D Face ID	Одиночний базовий CMOS-сенсор (OV2640)
Радіомодуль BLE	Дискретний NRF52832	Вбудований у мікроконтролер
Комутаційна матриця	Повна (до D9/E9), зовнішні АЦП/ЦАП	Зменшена (до D4/E9), вбудовані АЦП/ЦАП

Таке інженерне спрощення апаратної архітектури дозволило знизити собівартість компонентної бази та витрати на виробництво. Завдяки оптимізації компонентної бази, собівартість пристрою знижується орієнтовно на 40–50%.

РОЗДІЛ 4. ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ТА АЛГОРИТМИ СИСТЕМИ

4.1. Архітектура програмного комплексу

Програмний комплекс гібридної системи контролю доступу побудовано за розподіленою клієнт-серверною архітектурою, яка забезпечує одночасну взаємодію цифрових мережевих протоколів та локальних апаратних інтерфейсів керування. Головним обчислювальним вузлом є локальний сервер, розгорнутий на базі ОС Linux безпосередньо на мікропроцесорі викличної панелі. Цей системний демон виконує роль граничного шлюзу (Edge Device), завданням якого є безперервне захоплення медіапотоку з камери та мікрофона, а також інкапсуляція низькорівневих апаратних переривань від зчитувачів у стандартизовані мережеві запити.

Взаємодія між компонентами системи розділена на два паралельні логічні маршрути, що гарантує сумісність із застарілим обладнанням. Перший маршрут відповідає за програмне керування зовнішньою аналоговою координатно-матричною магістраллю. Локальний сервер ініціює виклик, передаючи цифрові інструкції по шині I2C на мікроконтролер комутатора, який генерує необхідну напругу для абонентської трубки, що детально відображено на рисунку 4.2, де описано алгоритм паралельного гібридного сповіщення. Другий маршрут забезпечує функціонування сучасного цифрового зв'язку: сервер упаковує медіадані у протоколи SIP та RTSP і транслює їх на хмарний бекенд для подальшої маршрутизації.

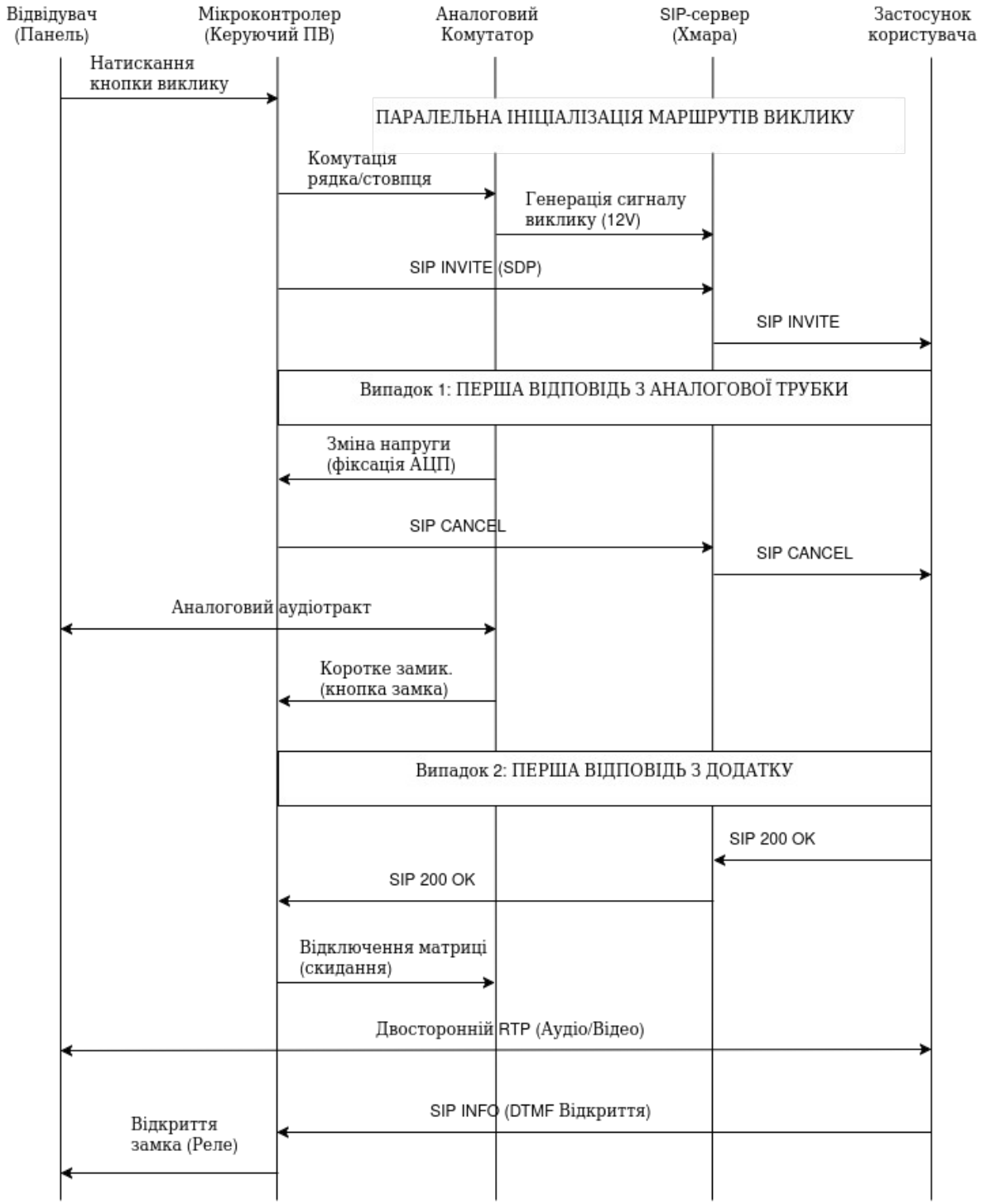


Рисунок 4.1. Алгоритм паралельного гібридного сповіщення

Веб-клієнт та мобільний застосунок абонента є тонкими клієнтами, які не мають прямого мережевого доступу до апаратних ресурсів викличної панелі. Уся комунікація, включаючи передачу відеопотоку та відправку керуючих команд (наприклад, сигналу на відкриття дверей), здійснюється

виключно через захищений REST API та WebSocket-з'єднання хмарного сервера. Це архітектурне рішення усуває необхідність відкриття портів на локальному маршрутизаторі будівлі та унеможливлює несанкціоноване відкриття замка шляхом прямих мережевих атак на IP-адресу панелі.

Для централізованого зберігання конфігурацій, керування правами доступу та ведення журналів подій спроектована реляційна база даних, розгорнуту на серверному боці. База даних нормалізована до третьої нормальної форми для усунення надмірності та підтримання цілісності даних при частих транзакціях (додавання/видалення користувачів через веб-дашборд).

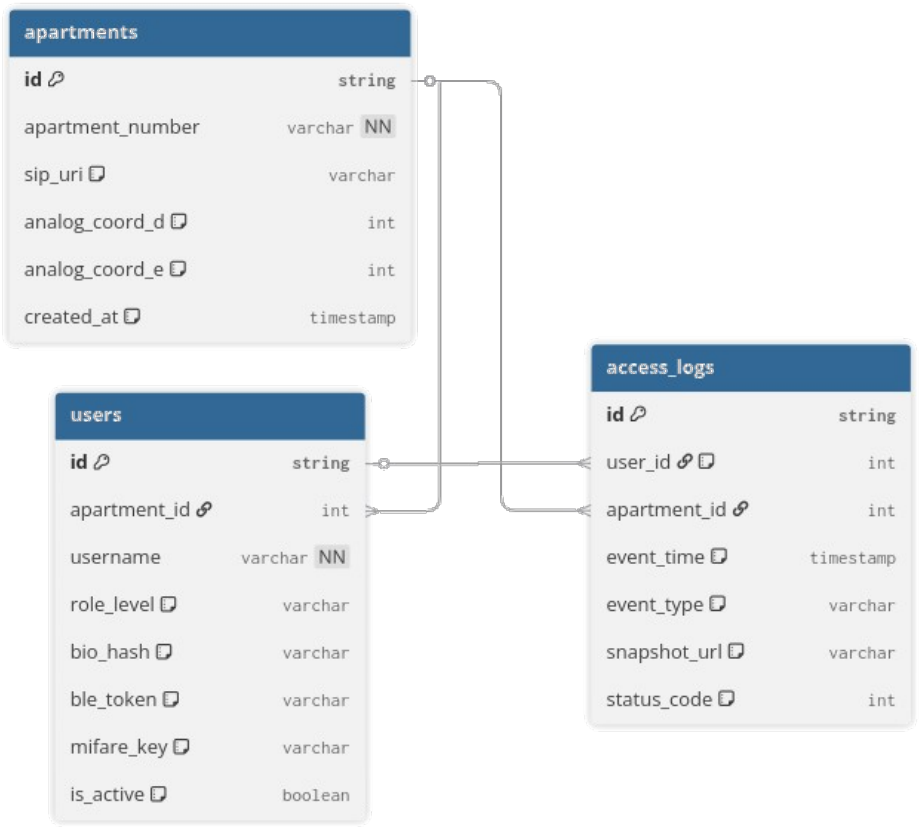


Рисунок 4.2. Структура бази даних

Таблиця apartments зберігає конфігурацію зв'язку: фізичний номер, цифрову SIP-адресу для IP-викликів та апаратні координати (шини десятків D та одиниць E) для аналогової комутації.

Таблиця users керує авторизацією, маючи зв'язок «один-до-багатьох» із квартирами. Відповідно до концепції Privacy-by-Design, біометричні дані (Face ID/Fingerprint) зберігаються виключно як незворотні математичні хеші. Для радіоідентифікації використовуються захищені токени BLE та криптографічні ключі Mifare DESFire.

Таблиця access_logs акумулює телеметрію, фіксуючи мітки часу, тип події (успіх/відмова), ініціатора та посилання на фотофіксацію відвідувача у хмарному сховищі. Ця структура гарантує мінімальний час відгуку (до 0.5 с) при ідентифікації та цілісність даних для панелі адміністратора.

4.2. Програмна реалізація алгоритмів управління панелі

Головний потік програми ініціює асинхронний цикл обробки подій, що здійснює паралельне опитування дескрипторів файлів апаратних інтерфейсів (драйверів системних шин SPI, I2C, UART) та мережевих сокетів за допомогою системних викликів ядра. Після завершення етапу низькорівневої ініціалізації пристрою та конфігурації периферійних модулів, програма переходить у стан очікування апаратних переривань. Усі вхідні події класифікуються на два базові типи: запити на авторизацію доступу (вхід мешканця за біометрією або RFID-міткою) та запити на встановлення сеансу зв’язку (введення гостем номера квартири на клавіатурі).

Загальну послідовність програмних переходів, розгалуження логіки за типами подій та фіксацію результатів у системному журналі відображено за допомогою блок-схеми загального алгоритму роботи панелі.

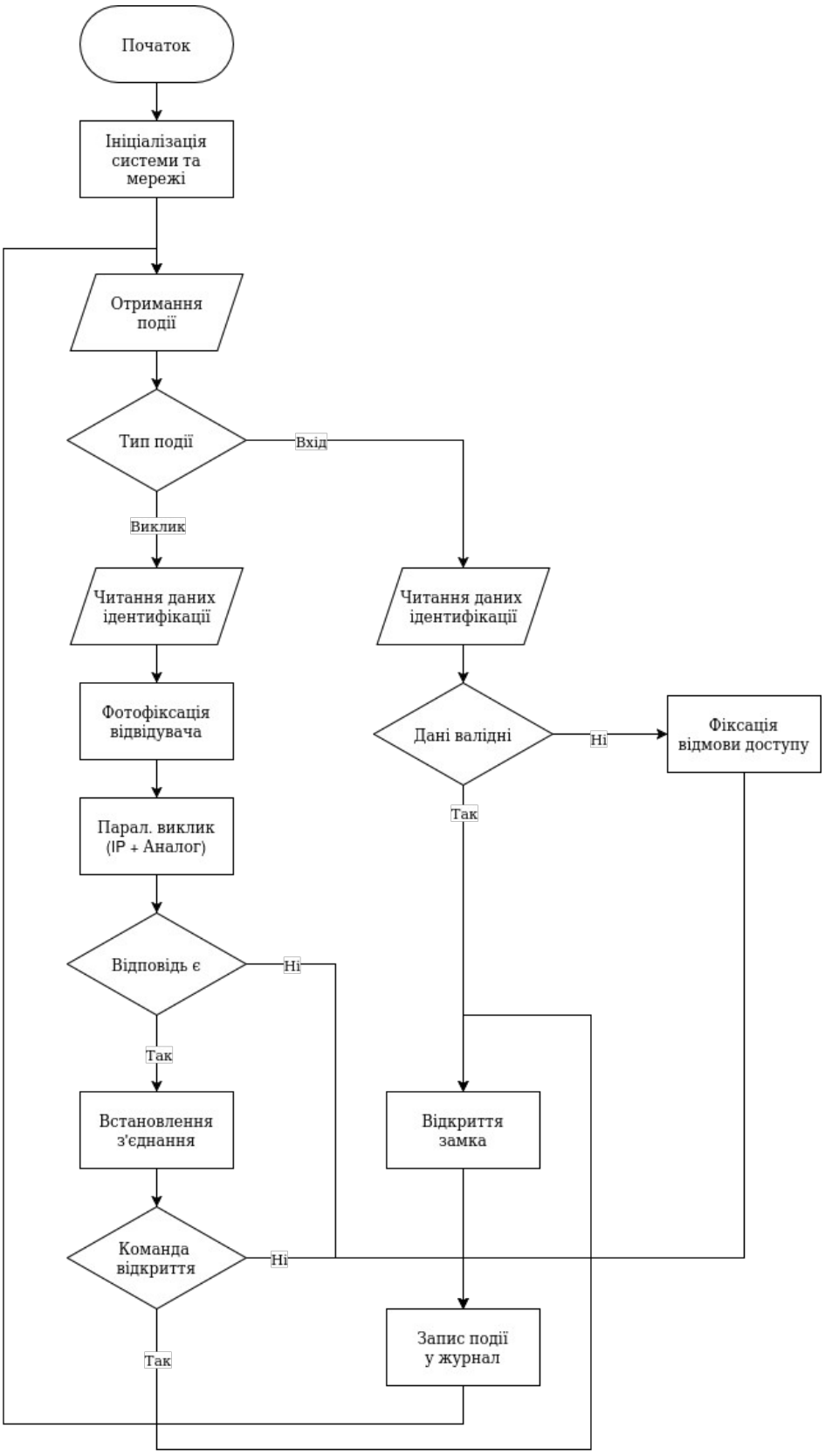


Рисунок 4.3. Алгоритм роботи панелі

При детектуванні події виклику програмний модуль обробки запускає два паралельні неблокуючі потоки виконання (threads) для реалізації алгоритму гібридного сповіщення. Перший робочий потік відповідає за комунікацію з координатно-матричним аналоговим доменом: через інтерфейсну бібліотеку шини I2C надсилається пакет інструкцій на чотириканальний ЦАП MCP4728 для генерації прецизійної аналогової напруги виклику у вибраний сегмент десятків та одиниць. Одночасно з цим запускається фонова задача циклічного опитування 16-бітного АЦП ADS1115 із заданою частотою дискретизації, що необхідно для фіксування падіння еквівалентного опору лінії при знятті абонентської трубки. Другий паралельний потік ініціює сесію цифрового зв'язку, використовуючи низькорівневі методи SIP-стека. Програмно формується сигнальний пакет `SIP INVITE` із параметрами SDP та надсилається на хмарний сервер для подальшої генерації PUSH-повідомлення у мобільний застосунок користувача.

Для запобігання виникненню стану гонки потоків та конфліктів медіапотоків, у коді реалізовано логіку строгого пріоритету першої відповіді за допомогою міжпотокових прапорців синхронізації. Якщо АЦП ADS1115 реєструє зміну напруги, яка свідчить про підняття механічної трубки в квартирі, перший потік виставляє прапорець перехоплення виклику. Мережевий потік негайно зчитує цей статус і надсилає команду `SIP CANCEL` для коректного завершення цифрової сесії на смартфонах. У протилежному випадку, коли з мережевого сокета першим надходить пакет `SIP 200 OK` від мобільного клієнта, програма віддає команду на блоки комутації матриці для негайного розмикання ключів, знеструмлюючи аналогову лінію для унеможливлення ретрансляції голосу та виникнення ехо-ефектів.

Реалізація безконтактного доступу за технологією Bluetooth Low Energy покладається на програмний модуль обробки радіосигналу. Периферійний

контролер Nordic nRF52832 через UART-інтерфейс передає у головний процес масив даних, що містить значення індикатора рівня отриманого сигналу (RSSI) від мобільних пристроїв.

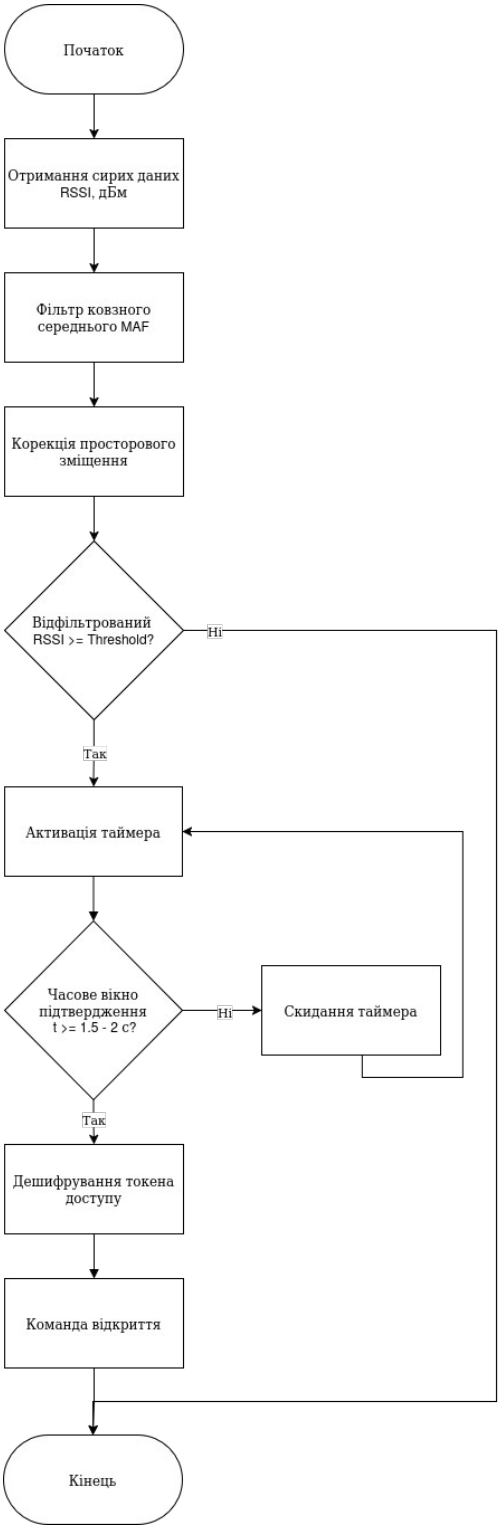


Рисунок 4.4. Блок-схема алгоритму обробки RSSI (режиму «Вільні руки»)

Спочатку сирі дані пропускаються через програмний фільтр ковзного середнього (Moving Average Filter, MAF) зі змінним розміром вікна для придушення випадкових флуктуацій

Відфільтрований вектор подається на вхід інтегрованої моделі просторової корекції зміщення (Offset Correction), яка компенсує деструктивну інтерференцію від стін та залізобетонних конструкцій. Наступний логічний блок коду реалізує евристичне часове вікно підтвердження: команда на запуск процедури дешифрування токена доступу формується лише тоді, коли обчислений рівень сигналу стабільно утримується вище встановленого порогу $RSSI_{Threshold}$ протягом заданого інтервалу часу Δt = 1.5 - 2 секунд. Після успішної часової валідації викликаються криптографічні функції для перевірки цифрового підпису та розшифрування токена за алгоритмом AES-CCM, що завершується відправкою керуючого імпульсу на силові транзисторні ключі реле замка.

4.3. Розробка клієнтських додатків (Web та Mobile)

Для взаємодії користувачів з апаратно-серверною частиною системи мною було спроектовано та реалізовано два типи клієнтських додатків: веб-панель керування (Web Dashboard) для адміністрування та мобільний застосунок для кінцевих абонентів. Клієнтська архітектура побудована за принципом ізоляції інтерфейсів від бізнес-логіки бекенду, де взаємодія відбувається виключно через стандартизовані API.

4.3.1. Реалізація веб-застосунку та панелі керування

Програмна реалізація фронтенд-частини виконана у вигляді Single Page Application (SPA), що дозволяє динамічно оновлювати інтерфейс без перезавантаження сторінок. Архітектура веб-додатка спирається на компонентний підхід із застосуванням глобального менеджера станів. Це забезпечує реактивну синхронізацію даних між компонентами інтерфейсу під

час додавання або видалення ключів доступу та редагування профілів користувачів. Сесійна аутентифікація адміністраторів базується на передачі токенів стандарту JWT (JSON Web Tokens) у заголовках кожного HTTP-запиту, що гарантує захист ендпоінтів.

Критичним вузлом веб-клієнта є реалізація модуля прийому викликів. Замість класичного поллінгу (HTTP Long Polling), для миттєвого отримання сигналів виклику з панелі реалізовано підключення через захищений протокол WebSocket. При надходженні сигналу веб-клієнт ініціалізує об'єкт RTCPeerConnection для встановлення однорангового з'єднання. Сигнальний обмін SDP-пакетами та збір ICE-кандидатів для проходження NAT виконуються безпосередньо через відкритий WebSocket-канал. Після успішного узгодження параметрів, вхідний відеопотік прив'язується до HTML-тегу <video> для відтворення з використанням апаратного декодування браузера.

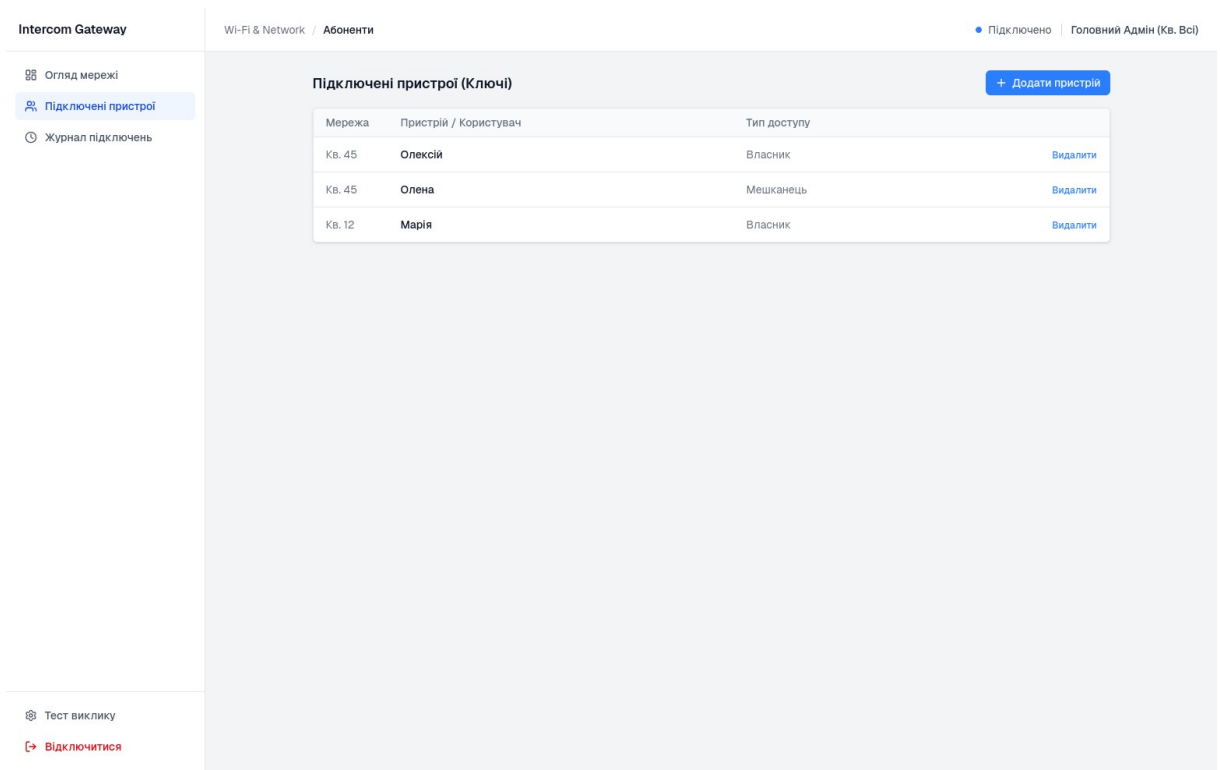


Рисунок 4.5. Інтерфейс панелі керування (Web Dashboard) під час налаштування параметрів доступу квартири.

4.3.2. Розробка мобільного застосунку абонента

Мобільний клієнт розроблено з використанням кросплатформового фреймворку для створення єдиної кодової бази під операційні системи iOS та Android. Головним інженерним викликом при розробці мобільного ПЗ стала необхідність гарантованої доставки виклику на пристрій, що перебуває у стані глибокого сну (Doze mode). Для цього відбувається обробка високопріоритетних PUSH-повідомлень на рівні системних служб. Отримавши такий push-payload, додаток взаємодіє з нативними API (наприклад, ConnectionService для Android або CallKit для iOS), що дозволяє вивести екран виклику поверх заблокованого смартфона та коректно перехопити аудіофокус системи (Audio Focus).

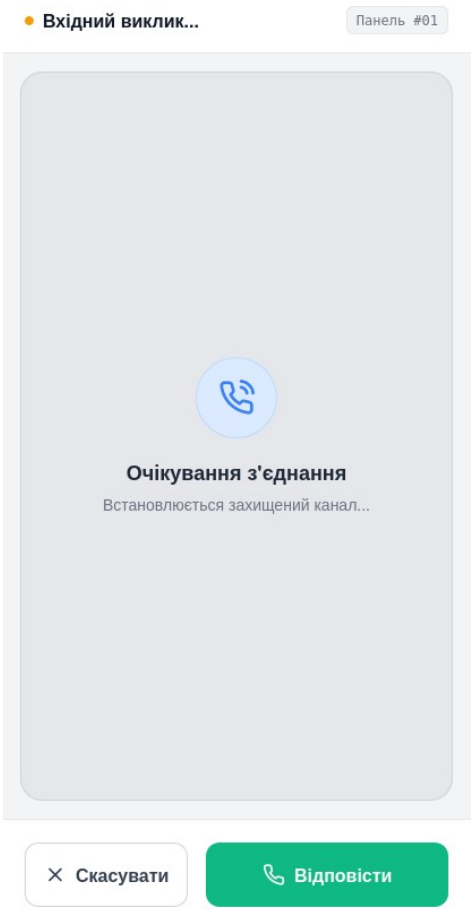


Рисунок 4.6. Екран вхідного відеовиклику мобільного застосунку з інтегрованими елементами управління замком.

Для забезпечення режиму безконтактного відкриття «Вільні руки» на клієнтському боці реалізовано ізольований фоновий процес. Цей сервіс використовує бібліотеки Bluetooth Low Energy для безперервного сканування пакетів в ефірі. Алгоритм на мобільному пристрої фільтрує MAC-адреси, виділяє пакети, що належать викличній панелі, і здійснює первинну фільтрацію стрибків RSSI. При входженні в радіус спрацювання, мобільний додаток автоматично ініціює BLE-з'єднання і передає зашифрований токен авторизації, усуваючи необхідність ручної взаємодії користувача з інтерфейсом смартфона.

ВИСНОВКИ

У дипломній роботі було розроблено гібридну викличну панель, яка забезпечує інтеграцію застарілих координатно-матричних систем домофонії з сучасними мережевими та хмарними технологіями. Це дозволяє модернізувати інфраструктуру багатоквартирних будинків без необхідності заміни існуючих аналогових абонентських ліній.

На основі теоретичного моделювання розроблено апаратну архітектуру, базовим обчислювальним ядром якої обрано процесор Rockchip RV1109. Для апаратного сполучення з високовольтними аналоговими трубками спроектовано трансляційний міст на базі багатоканального ЦАП та прецизійного АЦП із застосуванням гальванічної розв'язки для захисту цифрової електроніки.

Реалізовано підтримку смарт-карт MIFARE DESFire із взаємною автентифікацією за алгоритмом AES-128, впроваджено ємнісне сканування відбитків пальців із захистом шаблонів методом незворотного біометричного хешування. Систему розпізнавання облич посилено технологіями 3D-картування глибини та дистанційної фотоплетизмографії (rPPG) для протидії атакам типу "спуфінг". Також розроблено алгоритм фільтрації та просторової корекції зміщення RSSI для модуля BLE, що забезпечує стабільну роботу режиму «Вільні руки».

У програмній частині реалізовано розподілену клієнт-серверну архітектуру з підтримкою паралельного гібридного сповіщення через протокол SIP та аналоговий сигнал. Розроблено веб-панель адміністрування та кросплатформний мобільний застосунок абонента, що взаємодіють із системою через захищений Cloud API та WebSocket, забезпечуючи надійний віддалений контроль доступу та трансляцію медіаданих. Комплекс розроблених апаратних і програмних рішень формує повноцінну систему контролю доступу, готову до впровадження у реальних умовах експлуатації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Access Control Enhanced With Intercoms (https://kintronics.com/access-control-enhanced-with-intercoms/)

2. Comparative analysis of traditional telephone and voice-over-Internet protocol (VoIP) systems (https://www.researchgate.net/publication/4075122_Comparative_analysis_of_traditional_telephone_and_voice-over-Internet_protocol_VoIP_systems)

3. Design and implementation of analog telephone on IPPBX network interconnection (https://www.researchgate.net/publication/338850232_Design_and_implementation_of_analog_telephone_on_IPPBX_network_interconnection)

4. A DISTRIBUTED IP-BASED TELECOMMUNICATION SYSTEM USING SIP (https://arxiv.org/abs/1312.2625)

5. Implementation and Analysis of Real-Time Streaming Protocols (https://www.researchgate.net/publication/316944787_Implementation_and_Analysis_of_Real-Time_Streaming_Protocols)

6. Design and Implementation of a Smart Intercom System through Web Services on Web of Things (https://www.researchgate.net/publication/365399604_Design_and_Implementation_of_a_Smart_Intercom_System_through_Web_Services_on_Web_of_Things)

7. Side-Channel Analysis of Cryptographic RFIDs with Analog Demodulation (https://www.langer-emv.de/fileadmin/2011_Side-Channel%20Analysis%20of%20Cryptographic%20RFIDswith%20Analog%20Demodulation.pdf)

8. A Review of Fingerprint Sensors: Mechanism, Characteristics, and Applications (https://pmc.ncbi.nlm.nih.gov/articles/PMC10305017/)

9. Symmetric Hash Functions for Fingerprint Minutiae (https://www.acsu.buffalo.edu/~tulyakov/papers/tulyakov_ICAPR05_fingerprint_hash.pdf)

10.DepthFake: A vulnerability of 3D face authentication systems based on structured light (https://gangw.cs.illinois.edu/class/cs562/papers/3d-spoof-sp23.pdf)

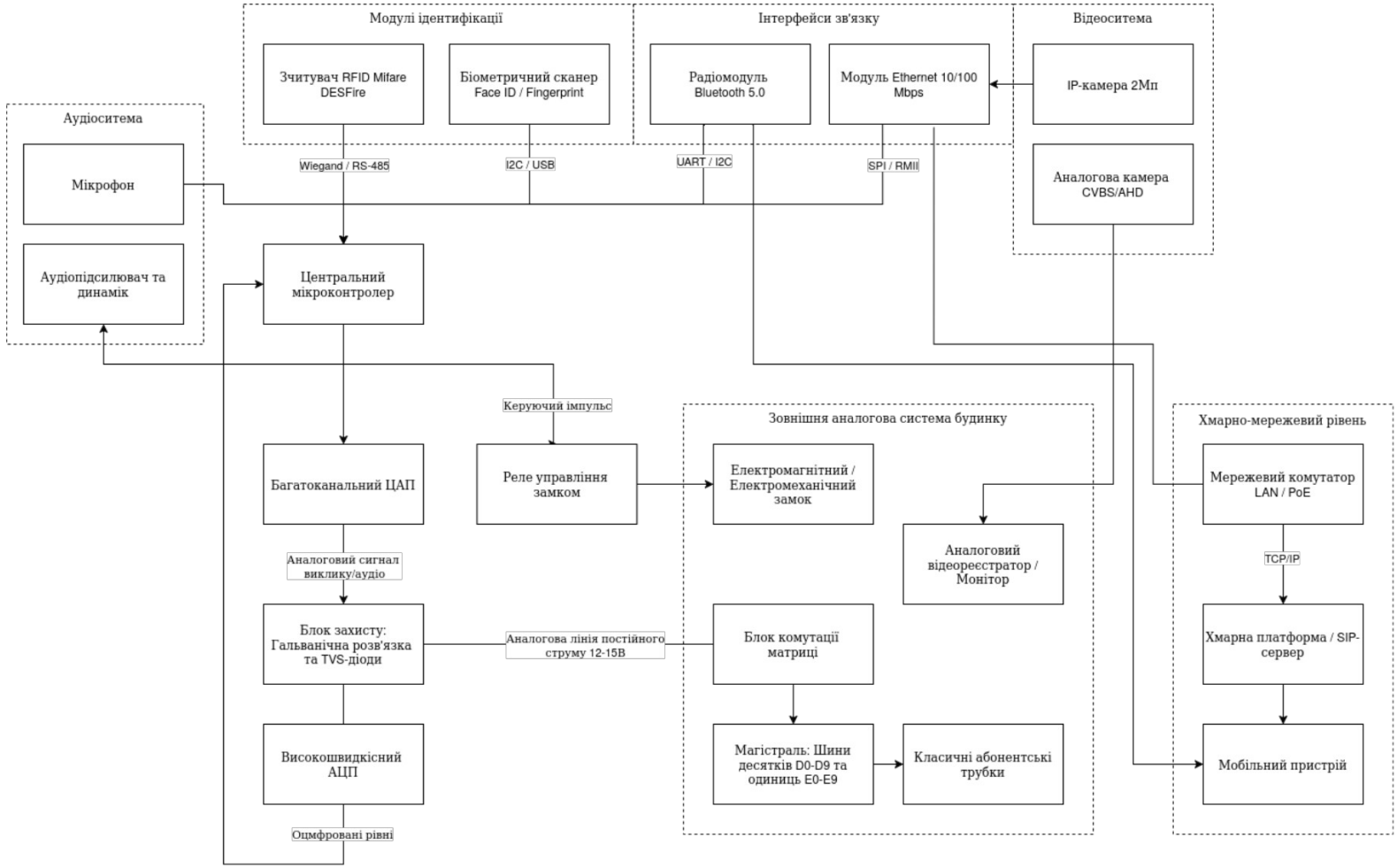
11.Learning Deep Models for Face Anti-Spoofing: Binary or Auxiliary Supervision (https://openaccess.thecvf.com/content_cvpr_2018/CameraReady/0615.pdf)

12.Face anti-spoofing using patch and depth-based CNNs (http://cvlab.cse.msu.edu/pdfs/FaceAntiSpoofingUsingPatchandDepthBasedCNNs.pdf)

13.Enhanced Position Estimation via RSSI Offset Correction in BLE Fingerprinting-Based Indoor Positioning (https://www.mdpi.com/1999-5903/17/10/440)

14.Accurate Indoor Proximity Zone Detection Based on Time Window and Frequency with Bluetooth Low Energy (https://www.researchgate.net/publication/282500792_Accurate_Indoor_Proximity_Zone_Detection_Based_on_Time_Window_and_Frequency_with_Bluetooth_Low_Energy)

Додаток А



Зм.	Лист	№ докум.	Підп.	Дата
Розроб.		Яріз Р.А.		
Пров.		Безугла Н.В.		
Т. контр.				
Н. контр.				
Упв.				

ДРБ.ПБ-22.13.1702.001 СХ

Структурна схема апаратної архітектури панелі

Літ.	Маса	Масштаб
Аркуш	Аркушів	

ПБФ, КПІ ім. Ігоря Сікорського

Копировал

Формат А2

Перв. примен.

Справ. №

Подп. и дата

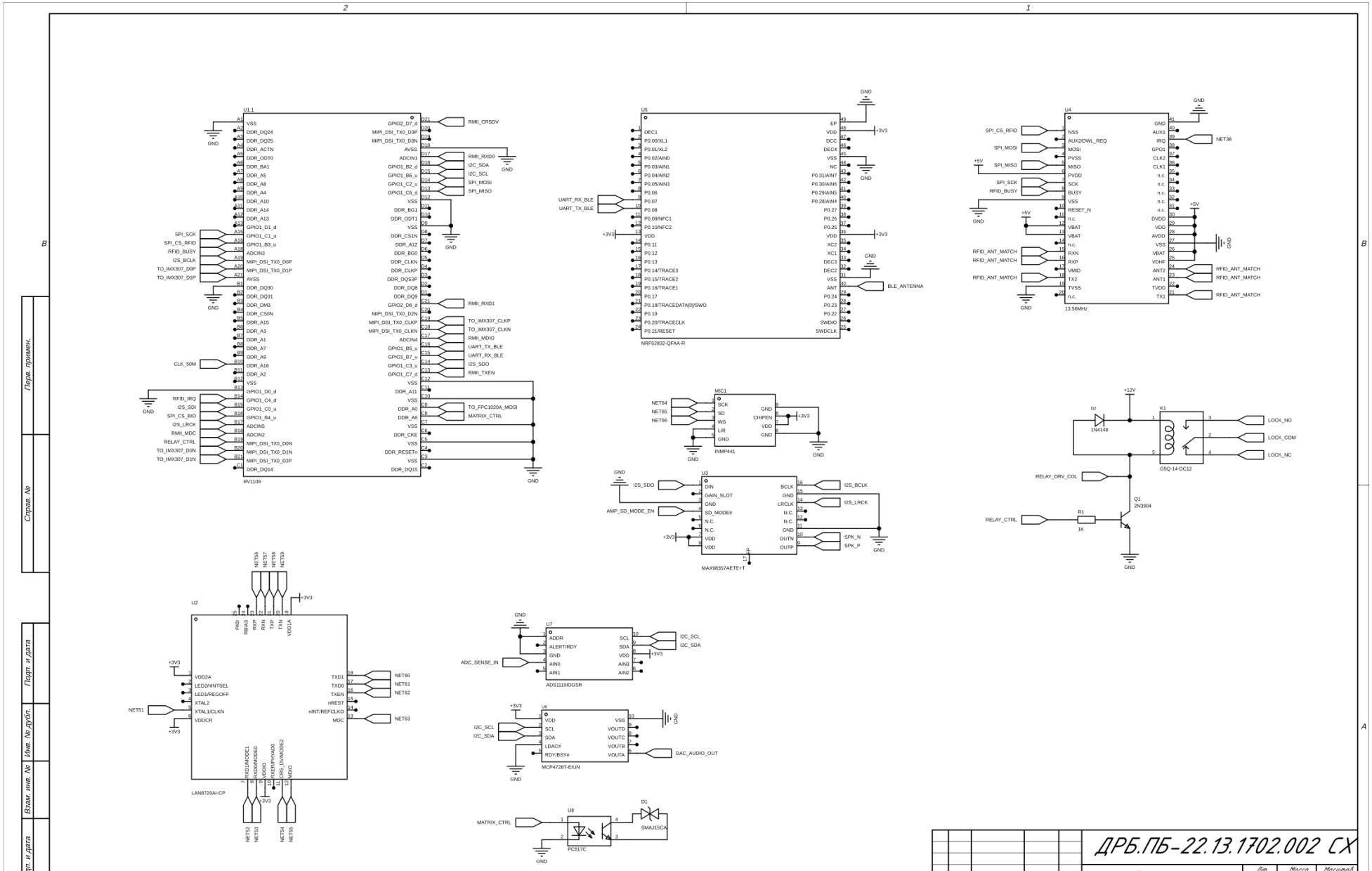
Инв. № дубл.

Взам. инв. №

Подп. и дата

Инв. № подл.

Файл: шаблонрамки



Зм.	Лист	№ докум.	Підп.	Дата	
Розроб.		Яріз Р.А.			
Пров.		Безугла Н.В.			
Т. контр.					
Н. контр.					
Утв.					

ДРБ.ПБ-22.13.1702.002 СХ

Електрична принципова схема панелі

Літ.	Маса	Масштаб
Аркуш	Аркушів	

ПБФ, КПІ ім. Ігоря Сікорського

Копировал

Формат А2

Перв. примен.

Справ. №

Подп. и дата

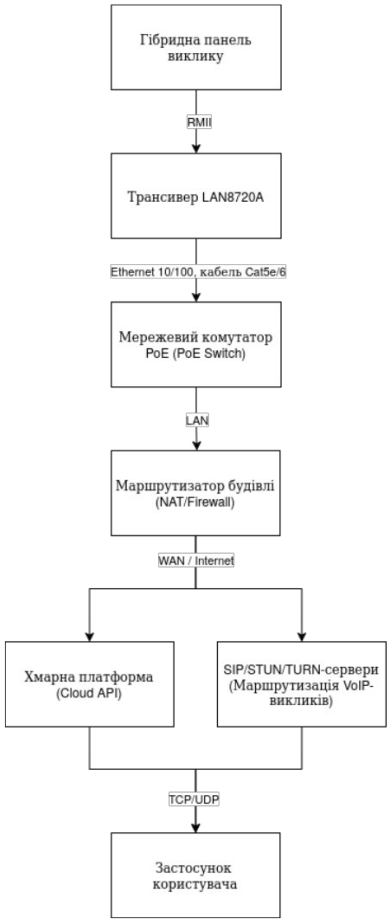
Инв. № дубл.

Взам. инв. №

Подп. и дата

Инв. № подл.

Файл: шаблонрамки



						ДРБ.ПБ-22.13.1702.003 СХ		
Зм.	Лист	№ докум.	Підп.	Дата	Схема мережевої взаємодії об'єкта керування з зовнішньою інфраструктурою	Літ.	Маса	Масштаб
Розроб.		Яріз Р.А.						
Пров.		Безугла Н.В.				Аркуш	Аркушів	
Т. контр.						ПБФ, КПІ ім. Ігоря Сікорського		
Н. контр.								
Затв.								

Копировал

Формат А2

Перев. примен.

Справ. №

Подп. и дата

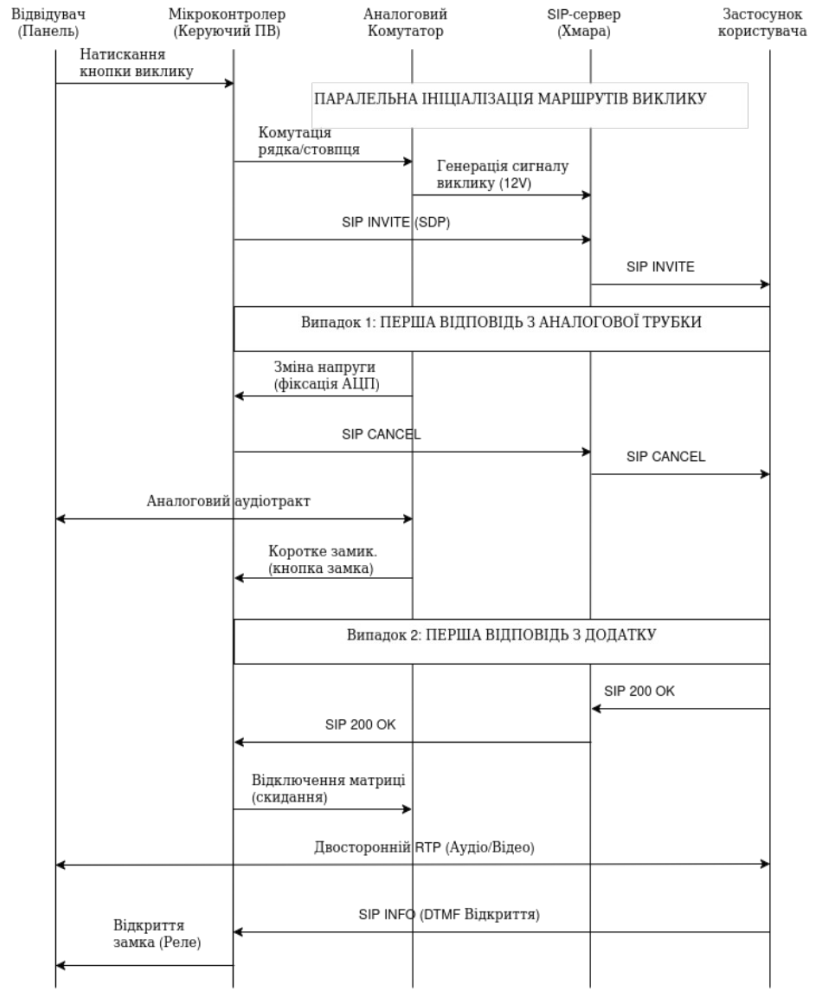
Инв. № дубл.

Взам. инв. №

Подп. и дата

Инв. № подл.

Файл: шаблонами



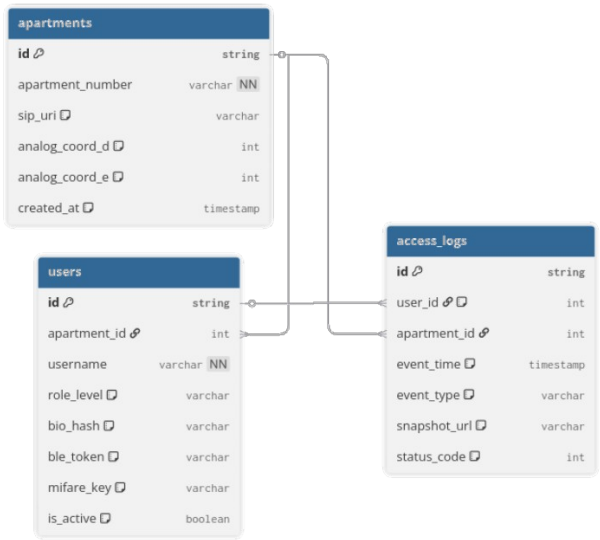
Зм.	Лист	№ докум.	Підп.	Дата	ДРБ.ПБ-22.13.1702.003 СХ
Розроб.		Яріз Р.А.			Алгоритм паралельного гібридного сповіщення
Пров.		Безугла Н.В.			
Т. контр.					
Н. контр.					ПБФ, КПІ ім. Ігоря Сікорського
Утв.					

Літ. | Маса | Масштаб
Аркуш | Аркушів

Перв. примен. | Справ. № | Підп. и дата | Инв. № дубл. | Взам. инв. № | Подп. и дата | Инв. № подл.

Копировал | Формат А2

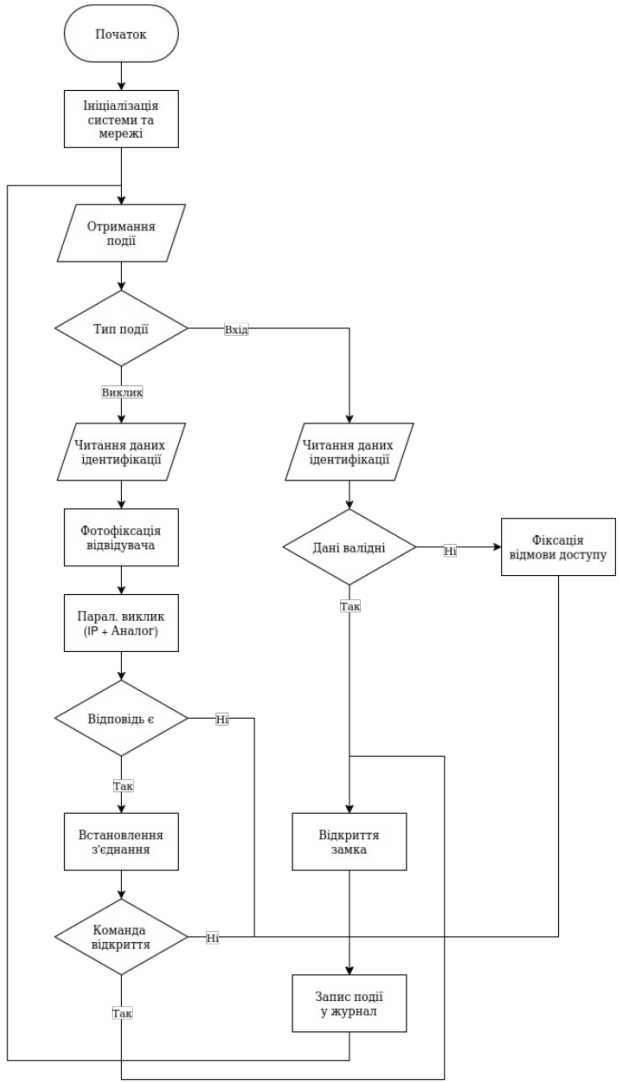
Файл: шаблонрамки



Зм.	Лист	№ докум.	Підп.	Дата	ДРБ.ПБ-22.13.1702.005 СХ		
Розроб.		Ярів Р.А.			Структура бази даних	Літ.	Маса	Масштаб
Пров.		Безугла Н.В.						
Т. контр.						Аркуш	Аркушів	
Н. контр.						ПБФ, КПІ ім. Ігоря Сікорського		
Затв.								

Перев. примен. | Справ. № | Підп. и дата | Инв. № дубл. | Взам. инв. № | Подп. и дата | Инв. № подл.

Копировал | Формат А2 | Файл: шаблонрамки



Зм.	Лист	№ докум.	Підп.	Дата	ДРБ.ПБ-22.13.1702.006 СХ
Розроб.		Ярієв Р.А.			Алгоритм роботи панелі
Пров.		Безугла Н.В.			
Т. контр.					
Н. контр.					ПБФ, КПІ ім. Ігоря Сікорського
Затв.					

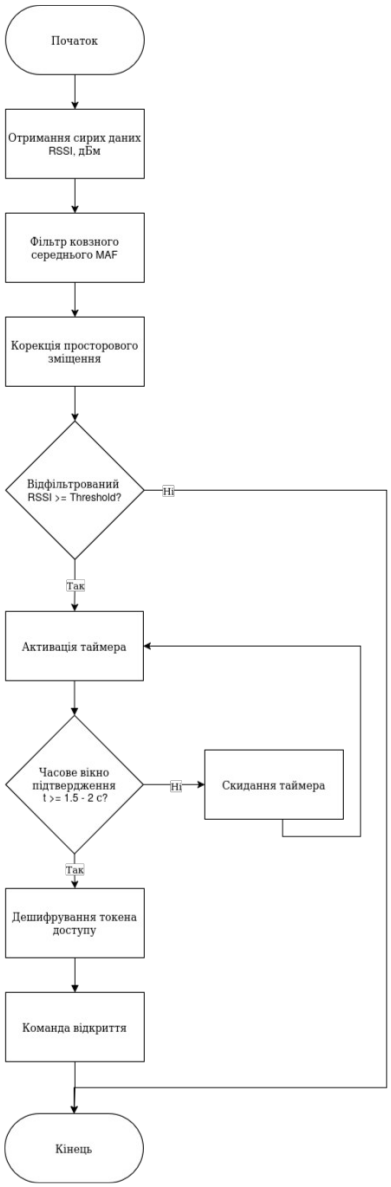
Лит. | Маса | Масштаб

Аркуш | Аркушів

Копировал | Формат А2

Перев. примен. | Справ. № | Подп. и дата | Инв. № дубл. | Взам. инв. № | Подп. и дата | Инв. № подл.

Файл: шаблонами



Зм.	Лист	№ докум.	Підп.	Дата
Розроб.		Яріз Р.А.		
Пров.		Безугла Н.В.		
Т. контр.				
Н. контр.				
Утв.				

ДРБ.ПБ-22.13.1702.007 СХ

Блок-схема алгоритму обробки RSSI (режиму «Вільні руки»)

Літ.	Маса	Масштаб
Аркуш	Аркушів	

ПБФ, КПІ ім. Ігоря Сікорського

Копировал

Формат А2

Перев. примен.

Справ. №

Подп. и дата

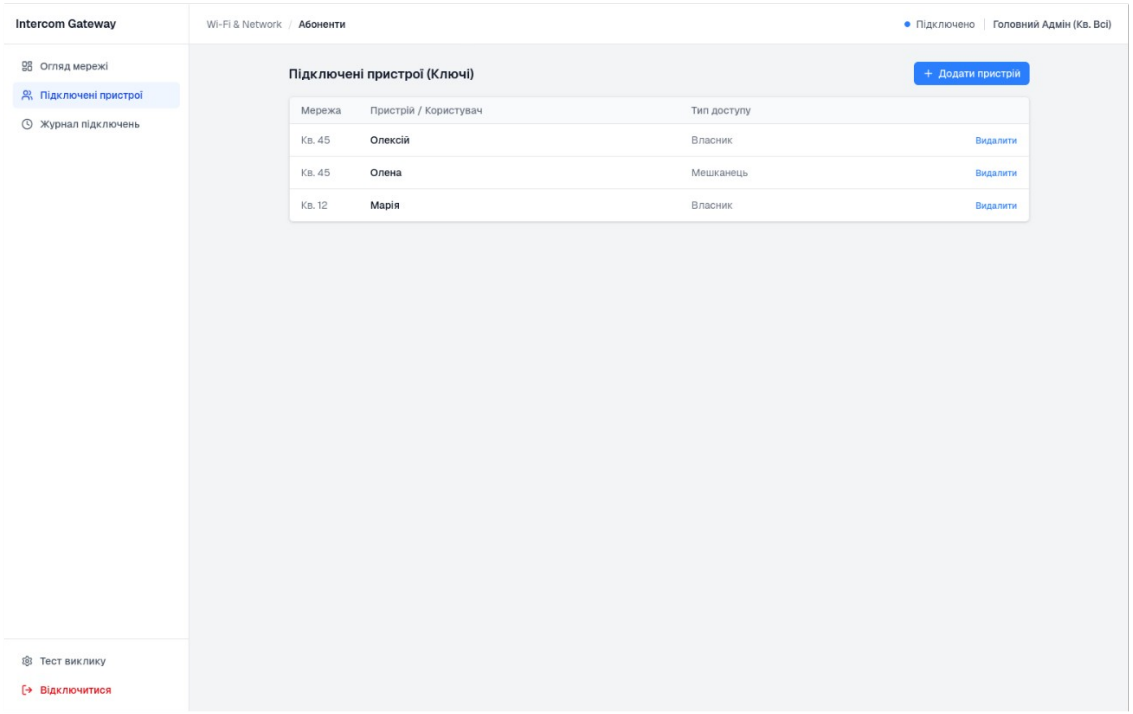
Инв. № дубл.

Взам. инв. №

Подп. и дата

Инв. № подл.

Файл: шаблон рамки

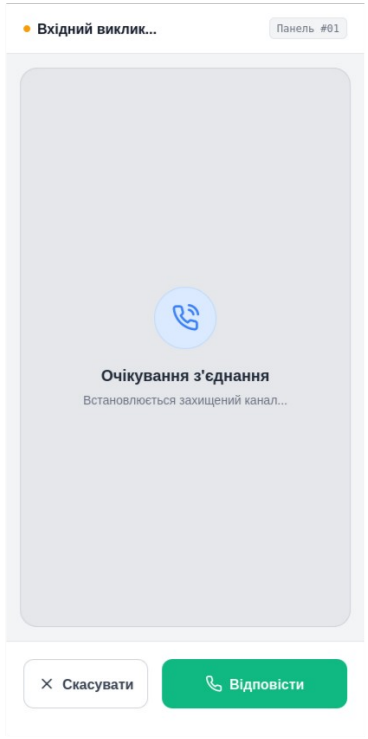


Зм.	Лист	№ докум.	Підп.	Дата	ДРБ.ПБ-22.13.1702.008		
Розроб.		Яріз Р.А.			Інтерфейс панелі керування (Web Dashboard)	Літ.	Масса / Масштаб
Пров.		Безугла Н.В.					
Т. контр.						Аркуш	Аркушів
Н. контр.					ПБФ, КПІ ім. Ігоря Сікорського		
Утв.							

Перв. примен. | Справ. № | Подп. и дата | Инв. № дубл. | Взам. инв. № | Подп. и дата | Инв. № подл.

Копировал | Формат А2

Файл: шаблонрамки



Зм.	Лист	№ докум.	Підп.	Дата	ДРБ.ПБ-22.13.1702.009 СХ		
Розроб.		Яріз Р.А.			Екран вхідного відеовиклику мобільного застосунку	Літ.	Маса	Масштаб
Пров.		Безугла Н.В.						
Т. контр.						Аркуш	Аркушів	
Н. контр.					ПБФ, КПІ ім. Ігоря Сікорського			
Утв.								

Перев. примен. | Справ. № | Подп. и дата | Инв. № дубл. | Взам. инв. № | Подп. и дата | Инв. № подл.

Копировал | Формат А2

Файл: шаблон рамки