Міністерство освіти і науки України

Луцький національний технічний університет
Факультет комп'ютерних та інформаційних технологій
Кафедра комп'ютерної інженерії та охоронних систем

КВАЛІФІКАЦІЙНА РОБОТА
ЗА СТУПЕНЕМ ВИЩОЇ ОСВІТИ «БАКАЛАВР»

ПРОЕКТУВАННЯ ОХОРОННОЇ СИСТЕМИ ПРИВАТНОГО БУДИНКУ

DESIGNING FOR PRIVATE HOUSE SECURITY SYSTEM

спеціальність 126 Інформаційні системи та технології
(шифр і назва спеціальності)

освітня програма «Інформаційні системи та технології охорони і безпеки»
(назва освітньої програми)

Виконав: здобувач вищої освіти
групи ІСТО-41
ІВАСИШИН Вадим Русланович
_____
(підпис)

Керівник:
к.т.н., доцент
КАЙДИК Олег Леонтійович
_____
(підпис)

Кваліфікаційну роботу
допущено до захисту
«___» _____ 2026 р.
Гарант освітньої програми:
к.т.н., доцент
ТЕРЛЕЦЬКИЙ Тарас Володимирович
_____
(підпис)

Луцьк – 2026 року

ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет: *комп'ютерних та інформаційних технологій*
Кафедра: *комп'ютерної інженерії та безпеки*
Ступінь вищої освіти: *бакалавр*
Галузь знань: *12 Інформаційні технології*
Спеціальність: *126 Інформаційні системи та технології*
Освітня програма: «*Інформаційні системи та технології охорони і безпеки*»

ЗАТВЕРДЖУЮ
Завідувач кафедри КІБ
к.т.н., доцент Терлецький Т. В.
_____
«___» _____ 2026 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ВИЩОЇ ОСВІТИ

ІВАСИШИНУ Вадиму Руслановичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи: *Проектування охоронної системи приватного будинку*

Керівник роботи: *к.т.н., доцент Кайдик Олег Леонтійович*
затверджені наказом закладу вищої освіти від «16» грудня 2026 р. № 529/01-02
2. Строк подання здобувачем вищої освіти кваліфікаційної роботи: «30» травня 2026 р.
3. Вихідні дані до роботи: *Планувальне рішення приватного будинку. ДСТУ EN 50131. ДСТУ EN 50131-1:2014. ДСТУ EN 50131-2-х. ДСТУ EN 50131-3. ДСТУ CLC/TS 50131-7. ДСТУ EN 50136-1. ДСТУ EN 54. ДСТУ IEC 60529. ДБН В.2.5-56. Системи охоронної сигналізації: AJAX FIBRA; TIRAS Orion NOVA; Satel ABAX 2 та Hikvision AX PRO.*

4. Зміст розрахунково-пояснювальної записки (перелік питань, що потрібно розробити): *Анотація. Вступ. Розділ 1. Аналітичний огляд стану предметної області (характеристика об'єкту проєктування; огляд нормативно-правової бази та стандартів; аналіз апаратних та програмних засобів реалізації; постановка завдань на кваліфікаційну роботу бакалавра). Розділ 2. Обґрунтування вибору засобів та методів реалізації (вибір базової апаратної платформи; вибір периферійного обладнання та давачів; вибір програмного забезпечення для керування та моніторингу; методика інтеграції та способи взаємодії компонентів системи; обґрунтування методів монтажу та налаштування). Розділ 3. Практична реалізація (архітектурне рішення та структурна схема системи; проєктування кабельної інфраструктури та топології підключення; інтеграція апаратного та програмного забезпечення; розробка та симуляція програмного забезпечення для інтеграції з екосистемою Ajax). Загальні висновки та рекомендації. Список використаних джерел. Додатки.*

5. Перелік графічного (ілюстративного) матеріалу: *Презентація на 11 слайдах*

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис	
		завдання видав	завдання прийняв
Розділ 1 Аналітичний огляд стану предметної області	*Кайдик О. Л.*		
Розділ 2 Обґрунтування вибору засобів та методів реалізації	*Кайдик О. Л.*		
Розділ 3 Практична реалізація	*Кайдик О. Л.*		
Загальні висновки та рекомендації	*Кайдик О. Л.*		
Нормоконтроль	*Кайдик О. Л.*		
Гарант ОП	*Терлецький Т. В.*		
Показник запозичень тексту			
Академічна доброчесність	*Кайдик О. Л.*		

7. Дата видачі завдання: «16» грудня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи бакалавра	Строк виконання етапів роботи	Примітка
1.	Обґрунтування теми	До 12.12.2025 р.	
2.	Огляд літератури із досліджуваної проблеми	До 12.12.2025 р.	
3.	Розділ 1 Аналітичний огляд стану предметної області	До 28.02.2026 р.	
4.	Розділ 2 Обґрунтування вибору засобів та методів реалізації	До 31.03.2026 р.	
5	Розділ 3 Практична реалізація	До 30.04.2026 р.	
6.	Загальні висновки та рекомендації	До 16.05.2026 р.	
7.	Формування списку використаних джерел	До 20.05.2026 р.	
8.	Формування додатків.	До 20.05.2026 р.	
9.	Формування презентації за темою кваліфікаційної роботи	До 20.05.2026 р.	
10.	Нормоконтроль	До 21.05.2026 р.	
11.	Інструментальна перевірка на академічний плагіат	До 22.05.2026 р.	
12.	Представлення кваліфікаційної роботи бакалавра до захисту	До 02.06.2026 р.	

Здобувач вищої освіти _____ (Івасишин В. Р.)
(підпис)

Керівник кваліфікаційної роботи _____ (Кайдик О. Л.)
(підпис)

АНОТАЦІЯ

Івасишин В. Р. Проектування охоронної системи приватного будинку. Рукопис.

Кваліфікаційна робота бакалавра ОП «Інформаційні системи та технології охорони і безпеки». Луцький національний технічний університет. Луцьк, 2026.

Кваліфікаційна робота бакалавра складається зі вступу, трьох розділів, загальних висновків та рекомендацій, списку використаних джерел та додатків.

У пояснювальній записці кваліфікаційної роботи акцентовано увагу на аналітичному огляді стану предметної області, нормативно-правовій базі та стандартах у сфері систем безпеки, а також проведено порівняльний аналіз архітектур сучасних охоронних систем. Обґрунтовано вибір базової апаратної платформи, периферійного обладнання, давачів та програмного забезпечення для керування й моніторингу. Описано методику інтеграції, способи взаємодії компонентів системи, а також методи їх монтажу та налаштування. У практичній частині представлено архітектурне рішення та структурну схему системи, спроєктовано кабельну інфраструктуру й топологію підключення пристроїв. Особливу увагу приділено процесам програмно-апаратної інтеграції, а також розробці та симуляції програмного забезпечення для взаємодії з екосистемою Ajax.

Ключові слова: охоронна система, централь, шина, давач, засіб виявлення, топологія підключення, монтаж, хмара, протокол, алгоритм, симуляція.

ANNOTATION

Ivasyshyn V. Designing for private house security system. Manuscript.

Bachelor’s qualification work EP «Security and safety information system and technologies». Lutsk National Technical University. Lutsk, 2026.

This bachelor’s thesis comprises an introduction, three sections, general conclusions and recommendations, a list of references, and appendices.

The explanatory note focuses on an analytical review of the industry’s state of the art, regulatory frameworks, and security system standards, providing a comparative analysis of modern security system architectures. It substantiates the selection of the core hardware platform, peripheral equipment, sensors, and management/monitoring software. Furthermore, it outlines the integration methodology, component interaction techniques, and installation and configuration methods. The practical section introduces the architectural solution and system block diagram, alongside the design of the cable infrastructure and device connection topology. Particular emphasis is placed on hardware-software integration processes, as well as the development and simulation of software designed to interface with the Ajax ecosystem.

Keywords: security system, control panel, bus, sensor, detection device, connection topology, installation, cloud, protocol, algorithm, simulation.

ЗМІСТ

ВСТУП

Вихідною точкою у розвитку дротової охоронної інженерії стало створення традиційних аналогових архітектур радіальних шлейфів, що тривалий період часу виконували функцію первинного контролю об’єктів.

На сьогоднішній день підприємства, які виготовляють таку продукцію, широко застосовують сучасні мікропроцесорні та цифрові шинні технології у своїх розробках, які дозволяють оптимально адаптувати охоронні комплекси під визначені потреби. Сфера застосування такого обладнання досить широка: від приватного житла до великих комерційних і промислових об’єктів. Ці системи є простими у керуванні та обслуговуванні, надійними і стабільними під час експлуатації завдяки хмарній інтеграції та гібридним методам зв’язку.

Перспективним вектором розвитку галузі є впровадження цифрових проприєтарних протоколів, які базувалися б на шинній топології та двосторонньому обміні даними. Цей підхід дозволить забезпечити безперервний моніторинг ліній зв’язку, дозволяючи гнучко налаштовувати параметри системи, контролювати робочу напругу та гарантувати високу точність виявлення загроз.

Об’єкт дослідження – гібридна система охоронної сигналізації на базі централі Hub Hybrid.

Предмет дослідження – процеси функціонування, топологічні аспекти проєктування кабельної інфраструктури, методики інтеграції, налаштування та програмної симуляції компонентів системи.

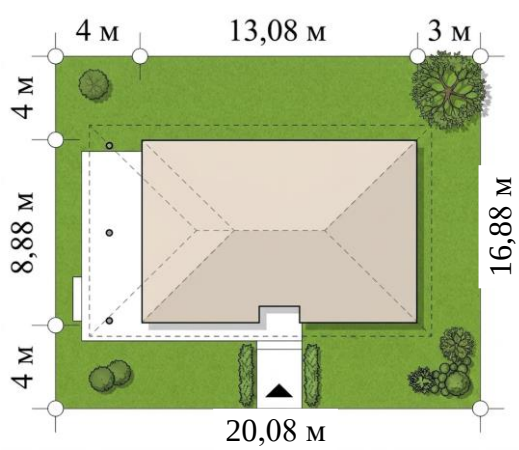
Мета кваліфікаційної роботи – проєктування та програмно-апаратна реалізація комплексної гібридної системи безпеки приватного будинку для забезпечення мінімізації ризиків несанкціонованого проникнення.

РОЗДІЛ 1
АНАЛІТИЧНИЙ ОГЛЯД СТАНУ ПРЕДМЕТНОЇ ОБЛАСТІ

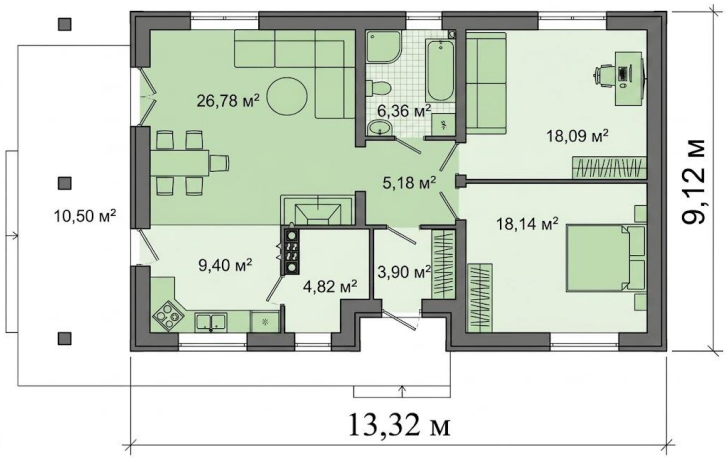
1.1 Характеристика об’єкту проєктування

Об’єктом проєктування виступає приватний будинок (рис. 1.1, а) загальною площею приблизно 121,5 м² (13,32×9,12 м), який розташовано на земельній ділянці (рис. 1.1, б) площею приблизно 340 м² (20,08×16,88 м). Планування будинку (рис. 1.1, в) включає відкриту зону вітальні-кухні, три житлові кімнати, санвузол, тамбур та простору терасу.

а)



б)



в)

Рисунок 1.1 – Приватний будинок:

а) – загальний вигляд; б) – розташування на ділянці; в) – план першого поверху

1.1.1 Аналіз вразливостей та зон ризику

Специфіка приватного сектору зумовлює підвищений рівень вразливості об’єкта, у порівнянні із багатоквартирними будинками, через наявність прибудинкової території та великої кількості шляхів потенційного проникнення.

Зони ризику зовнішнього периметра та території:

– фронтальна зона – основний в’їзд та вхід на ділянку є точками найвищої активності, які потребують контролю доступу та відеофіксації;

– відступи від меж ділянки – наявність вільних проходів навколо будинку (3-4 м) дозволяє зловмиснику приховано пересуватися вздовж фасадів (особлива увага приділяється «вузьким» зонам, де огляд обмежується парканом або рослинністю);

– ландшафтні загрози – зелені насадження на ділянці створюють «сліпі зони» для камер та можуть провокувати хибні спрацювання давачів руху, викликані коливанням гілок або руху тварин.

До зон ризику будівлі варто віднести:

– вхідні двері – основний вхід через тамбур (3,9 м²) та засклена група виходу на терасу (10,5 м²) з вітальні (26,78 м²) – у нашому випадку тераса є найбільш критичною точкою, враховуючи її велику площу скління та низьку видимість з боку вулиці;

– віконні проєми (прорізи) – шість віконних блоків розподілено за усім периметром – у нашому випадку найбільш вразливими є кутові кімнати (18,14 м² та 18,09 м²), вікна яких виходять на різні сторони будинку;

– внутрішній простір – центральний хол (5,18 м²) є стратегічним вузлом, оскільки з’єднує усі приміщення будинку – у нашому випадку контроль цієї зони дозволить фіксувати будь-яке переміщення, за умови коли основний периметр було подолано.

1.1.2 Класифікація потенційних загроз

Для забезпечення комплексної безпеки проектована система захисту повинна протидіяти наступним категоріям загроз:

– несанкціоноване проникнення та крадіжка – спроби подолання огорожі, взламування замків хвіртки або вхідних дверей, розбиття скла або підважування віконних рам;

– вандалізм – навмисне пошкодження фасадів, зовнішніх блоків інженерних систем (кондиціонерів, лічильників) або елементів огорожі;

– пожежна небезпека – виникнення загорянь, особливу увагу слід звернути на зону кухні (9,4 м²) через експлуатацію нагрівальних приладів;

– техногенні та побутові аварії – ризик витоку води у санвузлі (6,36 м²) та на кухні, що може призвести до значних матеріальних збитків.

1.1.3 Визначення ступеня ризику згідно з нормативними документами

Відповідно до вимог ДСТУ EN 50131-1 [1], об’єкт проектування класифікується за ступенем безпеки – Grade 2, а це передбачає захист від зловмисників із обмеженими знаннями про охоронні системи, які можуть використовувати базовий набір інструментів. У такому випадку охоронна система повинна гарантувати:

– сповіщення про проникнення через усі основні шляхи;

– автономну роботу під час відключення основного джерела живлення;

– високу надійність каналів зв’язку.

За екологічними умовами експлуатації (відповідно до ДСТУ CLC/TS 50131-7 [2]) компоненти системи поділяються на:

– внутрішні (клас II) – для встановлення всередині приміщень із можливим коливанням температури;

– зовнішні (клас IV) – для обладнання, яке монтується на відкритому повітрі (таке обладнання повинно мати ступінь захисту нижче IP65 та працювати в широкому температурному діапазоні, зазвичай від -25 до +60°C).

1.2 Огляд нормативно-правової бази та стандартів

Проектування системи охоронної сигналізації для приватного будинку повинне базуватись на комплексі національних та міжнародних стандартів, які

регламентують вимоги до надійності обладнання, якості монтажу та алгоритмів реагування. Лише дотримання цих норм гарантує не лише технічну надійність системи, а й правову легітимність її експлуатації.

1.2.1 Базові стандарти

ДСТУ EN 50131 є основоположною серією стандартів, які визначають «правила гри» на ринку безпеки України.

ДСТУ EN 50131-1:2014 – встановлює загальні вимоги, які висуваються до систем. Оскільки об’єкт класифіковано як Grade 2, то стандарт вимагає, щоб кожен пристрій системи мав захист від несанкціонованого доступу та зміг передати сигнал тривоги під час подавлення радіоканалу або обриву кабеля.

ДСТУ EN 50131-2-х – група стандартів, яка визначає вимоги, які висуваються до конкретних типів давачів. Наприклад, частина 2-2 [3] відноситься до пасивних ІЧ-давачів руху, а частина 2-4 [4] – комбінованих.

ДСТУ EN 50131-3 [5] – регламентує вимоги до контрольних панелей. Для приватного будинку стандарт вимагає наявності журналу подій, до якого не повинен мати доступ звичайний користувач.

1.2.2 Стандарти проектування та експлуатації

ДСТУ CLC/TS 50131-7 – це основний документ проєктувальника. Цей документ визначає етапність проектування: від первинного обстеження об’єкта до фінального тестування. Саме він висуває вимогу до високої надійності пристроїв, забезпечуючи їх стабільну роботу за агресивних умов НС.

ДСТУ EN 50136-1 [6] – визначає вимоги до систем передавання тривожних сповіщень. Оскільки будинок є автономним об’єктом, стандарт рекомендує дублювати канали зв’язку (Ethernet + GSM/4G).

1.2.3 Пожежна та екологічна безпека

Враховуючи виділену, в зоні кухні, загрозу пожежі та ризики підтоплення, слід врахувати:

– ДСТУ EN 54 [7] – серія стандартів для систем пожежної сигналізації, що визначає типи димових та теплових сповіщувачів, які використовуються для житлового сектору;

– ДСТУ IEC 60529 [8] – важливий для зовнішнього обладнання нормативний документ, оскільки вимагає їх захист не нижче IP65, що запобігає потраплянню у них пилу та води.

1.2.4 Галузеві будівельні норми

ДБН В.2.5-56 [9] – враховуючи те, що приватний будинок не завжди підлягає обов'язковій державній пожежній експертизі, ці норми здатні сформувати чіткі рекомендації щодо розміщення давачів охоронної сигналізації в кімнатах різного призначення.

Розглянута нормативна база дозволяє сформувати проектне рішення, яке стане не лише технічно ефективним для захисту конкретних вразливостей, але й юридично обґрунтованим під час сертифікації системи або укладання договору з охоронною компанією.

1.3 Порівняльний аналіз архітектур охоронних систем

1.3.1 Типи систем охоронної сигналізації

Система охоронної сигналізації (СОС) являє собою комплекс технічних засобів (ТЗ), які призначені для виявлення та запобігання несанкціонованому проникненню в охоронну зону.

Основними функціями СОС прийнято вважати:

– здійснення цілодобового моніторингу охоронної зони;

– негайне сповіщення про наявність ознак порушення;

– збирання, обробка, передача та зберігання даних про проникнення на охоронний об'єкт.

На практиці існують наступні типи охоронної сигналізації: автономна, індивідуальна та пультова.

Принцип роботи автономної сигналізації [10] базується на психологічному впливі на порушника шляхом подачі звукового сигналу тривоги та привернення уваги інших людей, які перебувають не далеко від охоронного об'єкта. Основу цієї системи становлять технічні засоби

сповіщення/оповіщення, що забезпечує незалежний моніторинг цього об’єкту. За наявності загрози сповіщувач передає сигнал на увімкнення оповіщувача, який й формує гучний сигнал тривоги.

Цей тип сигналізації широко використовується в квартирах, магазинах, офісах, готелях, ресторанах та бізнес-центрах.

До основних переваг автономної сигналізації слід віднести: доступність; низька вартість та простий монтаж.

Недоліками цієї системи прийнято вважати: легко вивести з ладу (вкрай нестійка до перешкод радіоканалу) та ненадійна (може не відразу, або ж зовсім, привернути увагу оточуючих).

Індивідуальна сигналізація [10] є аналогічною до автономної, за винятком того, що до її складу входить засіб мобільного зв’язку, який виконує функції приймання-передачі сигналу. Це, у випадку виникнення загрози, дозволяє не лише активувати звуковий сигнал тривоги, але й передати сигнал оповіщення на гаджет.

Даний тип сигналізації широкого використовується в офісах, компаніях та квартирах.

До основних переваг індивідуальних систем сигналізації відносять: середню вартість; гнучке налаштування (віддалене управління) та простий монтаж;

Основними їх недоліками є: обов’язкова наявність мобільної мережі та функціонування системи із перешкодами за умови низьких температур.

Пультова система охоронної сигналізації [11] – це продовження індивідуальної, тому що використовує технологію мобільного зв’язку для передачі даних. На відміну від індивідуальних, відноситься до типу активних систем, тобто система призначена для запобігання та усунення загрози. Як правило це розробка охоронних агентств, та у разі небезпеки сигнал передається на центральний пульт охорони, для затримання порушника.

Цей тип сигналізації використовують для найрізноманітніших об’єктах, серед яких: торгові центри, банки, музеї, ресторани, ювелірні крамниці тощо.

До основних переваг пультової системи охоронної сигналізації відносять: високу надійність та ефективність й щомісячне технічне обслуговування.

Недоліками системи прийнято вважати: високу вартість обладнання та щомісячну абонентську плату.

1.3.2 Архітектура охоронних систем

Сучасна інженерія безпеки пропонує три фундаментальні підходи до побудови систем захисту приватних об’єктів [12], кожен з яких базується на специфічних методах передачі даних та енергозабезпечення компонентів.

Провідну охоронну сигналізацію прийнято вважати найбільш стабільною та надійною формою захисту, де взаємодія між сповіщувачами та центральним приймально-контрольним приладом (ПКП) відбувається через кабельні лінії. У такій системі електричний сигнал проходить по замкненому контуру, а будь-яка зміна опору або розрив ланцюга миттєво реєструється як тривожна подія.

Основною перевагою цієї архітектури є її повна незалежність від радіоперешкод, атмосферних умов та спроб дистанційного подавлення робочого сигналу. Окрім цього вона здатна живити усі давачі системи, що усуває потребу в регулярному обслуговуванні індивідуальних елементів живлення. З точки зору довгострокової експлуатації або в умовах, де доступ до давачів обмежено, це робить її ідеальною. Однак складність інсталяції, що супроводжується необхідністю штробіння стін та прокладання великої кількості кабелів, робить її впровадження доцільним лише на етапі будівництва, оскільки монтаж у вже відремонтованих приміщеннях може завдати значних естетичних та фінансових збитків.

Паралельно з розвитком цифрових технологій широкого розповсюдження набула безпровідна або радіоканальна сигналізація, яка радикально змінила підхід до монтажу та масштабування систем безпеки. У цій архітектурі зв’язок між пристроями відбувається за допомогою зашифрованих радіопакетів на спеціально виділених частотах. Відсутність потреби у прокладанні кабелів дозволяє розгорнути повноцінну систему захисту в приватному будинку за лічені години, не пошкоджуючи оздоблення стін та стель. Безпровідні давачі є

повністю автономними пристроями, які живляться від вбудованих елементів живлення, термін служби яких сягає від п’яти до семи років. Гнучкість такої системи є її найсильнішою стороною: користувач може легко змінити місце розташування давача або додати нові пристрої до системи за допомогою мобільного додатка. Проте, безпровідна архітектура вимагає використання складних протоколів захисту від інтелектуального злому та постійного моніторингу стану радіоефіру. Питання дальності сигналу в умовах залізобетонних перекриттів або товстих цегляних стін стає критичним, що іноді змушує використовувати додаткові ретранслятори для покриття усієї території ділянки.

Третім та найбільш збалансованим варіантом є гібридна архітектура, яка виступає інтегратором переваг обох попередніх типів. Гібридні централі зазвичай обладнують роз’ємами для фізичних ліній зв’язку та радіомодулями високої потужності для бездротової комунікації. Це дозволяє інженерам-проєктувальникам підходити до кожного об’єкта індивідуально, обираючи оптимальний спосіб підключення для конкретної зони захисту. Слід відзначити, що гібридна модель дозволяє забезпечити найвищий рівень живучості системи, оскільки вихід з ладу одного каналу зв’язку не паралізує роботу усієї мережі. Вона дозволяє поступово модернізувати застарілі кабельні системи шляхом додавання сучасних радіоканальних модулів, що робить її найбільш перспективною для складних приватних домоволодінь із розвиненою прибудинковою територією.

Порівняльний аналіз архітектурних рішень подано в таблиці 1.1.

Порівняльний аналіз цих архітектур через призму вартості, надійності та зручності використання демонструє чітку сегментацію їх застосування. Як бачимо, провідні системи виграють у вартості самого обладнання, але значно програють у вартості та тривалості монтажних робіт. Безпровідні рішення, навпаки, мають вищу ціну за одиницю виробу, проте мінімізують витрати на інсталяцію та дозволяють уникнути витрат на відновлення інтер’єру. З точки зору надійності за стандартом Grade 2, усі три типи архітектур можуть

відповідати високим вимогам, якщо вони використовують сертифіковане обладнання. Проте, провідна та гібридна системи мають природну перевагу у захисті від активних радіоперешкод.

Таблиця 1.1 – Порівняльний аналіз архітектур охоронних систем

Критерій порівняння	Провідна	Безпровідна	Гібридна
Надійність зв'язку	Найвища	Висока	Найвища
Складність інсталяції	Висока	Низька	Середня
Автономність	Залежить від АКБ централі	Кожен давач автономний	Максимальна гнучкість
Вартість реалізації	Висока робота / Дешеве обладнання	Дороге обладнання / Дешева робота	Вище середнього
Відповідність Grade 2	Повна	Повна	Повна

На сьогодні провідні системи дедалі більше інтегруються з цифровими шинами даних, перетворюючись на адресні інтелектуальні мережі, де кожен кабель передає не просто сигнал тривоги, а деталізовану діагностичну інформацію про стан пристрою. Безпровідні технології рухаються у бік енергоефективності та використання меш-мереж, де кожен давач здатен виступати ретранслятором для іншого, збільшуючи загальну стійкість системи. Гібридний підхід об'єднує ці інновації, дозволяючи власнику приватного будинку отримати систему, яка не лише буде реагувати на проникнення, але й попередить про витік газу, води або виникнення пожежі, використовуючи найкращий для кожної із задачі фізичний принцип передачі даних.

Зрештою, вибір архітектури охоронної сигналізації визначається балансом між бюджетом проєкту, стадією готовності об'єкта та індивідуальними вимогами до рівня безпеки, де кожне рішення є обґрунтованим кроком до створення захищеного життєвого простору.

1.4 Аналіз апаратних та програмних засобів реалізації

Сучасний ринок засобів безпеки пропонує широкий спектр апаратно-програмних комплексів, ефективність яких визначається не лише фізичними характеристиками окремих пристроїв, а й глибиною їх системної інтеграції.

Будь-який аналіз апаратного забезпечення слід розпочинати із центрального ПКП, який виступає інтелектуальним ядром усієї системи. Для об’єкта класу Grade 2 централь повинна підтримувати багатоканальність зв’язку, що гарантує, у випадку навмисного пошкодження кабельних мереж або використання засобів радіоелектронної боротьби, доставку тривожного сигналу. Ще одним важливим аспектом апаратної реалізації є архітектура живлення: до складу сучасних контролерів входять інтелектуальні контролери заряду резервних акумуляторів, що дозволяє системі підтримувати працездатність від 16 до 30 годин в автономному режимі.

Периферійне обладнання, до складу якого входять сповіщувачі, які працюють за різними фізичними явищами, формує перший ешелон захисту. Варто зауважити, що їх аналіз, в контексті проектування системи охоронної сигналізації приватного будинку, це є критично важливим.

На сьогодні, програмне забезпечення (ПЗ) систем безпеки прийнято розділяти на три рівні: вбудоване мікропрограмне забезпечення, хмарні сервіси та клієнтські застосунки. ПЗ першого рівня, зазвичай, базується на операційній системі реального часу, яка виключає можливість підвисання або збоїв при обробці критичних завдань. Хмарні технології дозволяють здійснювати постійний моніторинг стану системи з будь-якої точки світу, забезпечуючи її власника необхідною інформацією. Клієнтське програмне забезпечення дозволило трансформувати охоронну систему в повноцінний інструмент керування життєвим простором. Користувач отримує можливість не лише ставити будинок під охорону, а й керувати сценаріями її автоматизації. З точки зору інсталятора такі програмні засоби дозволяють отримати необхідні інструменти для дистанційної діагностики, що значно знижує вартість технічного обслуговування системи протягом усього періоду її експлуатації.

З наведеного бачимо, що ефективність функціонування системи безпеки сучасного приватного будинку визначається принципами синергії апаратного та програмного забезпечення. У свою чергу апаратна частина відповідає за фізичне виявлення загроз та первинну обробку сигналів, тоді як програмна

оболонка забезпечує логіку взаємодії компонентів, зручність керування для користувача та канали передачі тривожних сповіщень.

На сьогодні ринок систем безпеки в Україні об’єднано навколо таких ключових гравців як Ajax Systems, TIRAS Technologies, Satel та Hikvision. При цьому, кожен з них пропонує вій унікальний підхід до архітектури апаратних та програмних засобів реалізації системи охоронної сигналізації.

Ajax Systems – це інноваційна мобільна екосистема (рис. 1.2), яка використовує запатентовані радіопротоколи «Jeweller» та «Wings». Аналіз технології Fibra дозволяє констатувати появу якісно нового цифрового стандарту в галузі дротових систем безпеки.

Рисунок 1.2 – Система охоронної сигналізації AJAX FIBRA [13]

З апаратної точки зору ключовою інновацією є використання стандартного чотирижильного кабелю для передачі даних на екстремальні відстані до 2000 метрів, що досягається завдяки високій енергоефективності компонентів та унікальній шинній архітектурі. Апаратна база Fibra споживає мінімальну кількість енергії, що дозволяє системі з 30 пристроїв підтримувати повну працездатність протягом 60 годин від одного резервного акумулятора ємністю 7 А·год. Це в рази перевищує показники класичних аналогових систем і гарантує безперебійний захист об’єкта в умовах тривалої відсутності електропостачання. Важливою апаратною можливістю є підтримка фотопідтвердження тривог за провідниками (дротами), що раніше було

прерогативою виключно радіоканальних пристроїв. Система антисаботажу реалізована на фізичному рівні через контроль цілісності лінії та захист від підміни пристроїв, що робить дротове з'єднання стійким до спроб професійного втручання.

З програмної точки зору Fibra повністю успадкувала інтелектуальну екосистему Ajax, що базується на операційній системі реального часу «Malevich» та хмарній інфраструктурі. Програмна логіка дозволяє системі миттєво ідентифікувати кожен підключений пристрій, незалежно від його місця в топології шини, та надає можливість віддаленого налаштування всіх параметрів датчиків через мобільний або десктопний застосунок. Це усуває необхідність фізичного доступу до кожної точки монтажу для зміни чутливості або тестування зон, що радикально спрощує обслуговування. Програмні алгоритми забезпечують миттєву доставку сповіщень (до 0,15 с) та інтелектуальну верифікацію подій, де кожен пакет даних шифрується за пропрієтарним протоколом, унеможливлюючи перехоплення або програмне взломування.

Серія охоронних централей Orion NOVA (рис. 1.3) від TIRAS Technologies – це універсальна платформа, яка поєднує в собі високу інформативність дротових систем та гнучкість бездротових технологій, забезпечуючи, при цьому, надійний захист об'єктів будь-якої складності. Аналіз ПКП Orion NOVA дозволяє стверджувати, що цей пристрій є флагманським рішенням професійного рівня, де технологічна синергія забезпечує найвищий рівень відмовостійкості.

З апаратної точки зору ПКП вирізняється модульною архітектурою, яка дозволяє масштабувати систему з базових 16 до 128 зон детектування, що робить його придатним як для приватного житла, так і для масштабних комерційних об'єктів. Відповідність стандарту ДСТУ EN 50131-1:2014 на рівні Grade 3 свідчить про наявність «просунутих» схемотехнічних рішень для захисту від професійного саботажу, включаючи моніторинг цілісності шлейфів та стійкість до інтелектуальних атак на апаратному рівні. Комунікаційна

складова приладу базується на принципі багатоканального резервування: вбудований 2G-модуль із підтримкою двох SIM-карт у поєднанні з опціональними інтерфейсами Ethernet або Wi-Fi реалізує категорію передачі даних DP4, що є найвищим показником надійності доставки тривожних сповіщень. Апаратний функціонал розширено за рахунок наявності силових та сигнальних виходів (реле та транзисторні ключі), що дозволяє інтегрувати систему з інженерними мережами будівлі.

Рисунок 1.3 – Комплект охоронної системи TIRAS Orion NOVA X [14]

На програмному рівні Orion NOVA працює під управлінням вбудованої операційної системи, яка підтримує автоматичне оновлення прошивки та реалізує складні алгоритми контролю завад у GSM-каналі. Програмна екосистема TIRAS забезпечує безшовну взаємодію між «залізом» та користувачем через хмарний сервіс та мобільний додаток «Control NOVA II». Це ПЗ дозволяє здійснювати не лише віддалений моніторинг, а й повну конфігурацію системи без необхідності фізичного підключення до плати централі. Гібридний характер системи, що підтримує роботу з бездротовими компонентами серії «X», реалізований через інтелектуальні програмні шлюзи, які гарантують стабільність радіообміну та криптографічний захист сигналів.

Двостороння бездротова система ABAX 2 (рис. 1.4) від Satel – це професійне радіоканальне рішення, яке базується на вдосконаленому протоколі передачі даних і забезпечує високу надійність зв’язку на рівні дротових систем.

Аналіз цієї системи дозволяє визначити її як високотехнологічну платформу, яка базується на принципах двостороннього радіозв’язку й енергоефективності.

Рисунок 1.4 – Охоронна сигналізація Satel ABAX 2 [15]

З апаратної точки зору ABAX 2 є складним технічним комплексом, який включає до свого складу контролери, світлозвукові сповіщувачі, а також широкий спектр давачів: від стандартних детекторів руху та розбиття скла до комбінованих пристроїв та давачів диму. Ключовою апаратною інновацією є використання чотирьох каналів у діапазоні частот 868 МГц, що забезпечує стабільність зв’язку та високу завадостійкість за рахунок постійного моніторингу рівня сигналу. Кожен елемент системи має власне автономне живлення, а використання енергозберігаючих алгоритмів дозволяє пристроям працювати тривалий час без заміни джерел енергії, що у поєднанні із відсутністю кабельних ліній радикально спрощує монтаж та зберігає естетичність інтер’єру. Апаратна частина також включає вбудовані механізми захисту від саботажу, такі як тамперні контакти та невеликі габарити пристроїв, що робить їх непомітними для зловмисників.

З програмної точки зору система характеризується гнучкою логікою налаштування та розширеними можливостями керування через хмарні сервіси та мобільні застосунки. Програмне забезпечення контролера забезпечує миттєву обробку тривожних подій та їх передачу користувачеві або на пульт централізованого спостереження за допомогою GSM-каналу, використовуючи

різні формати сповіщень. Інтелектуальна складова софту Satel дозволяє реалізувати функції «розумного будинку». Програмна архітектура підтримує легке розширення системи шляхом додавання нових компонентів за декілька хвилин, а також забезпечує дистанційну діагностику та контроль за станом кожного датчика.

Бездротова охоронна система Hikvision AX PRO [16] базується на використанні пропрієтарних радіопротоколів «Tri-X» та «Cam-X», які дозволяють забезпечити надійну передачу даних на великі відстані та миттєву відеоверифікацію тривожних подій. Аналіз цієї інтелектуальної системи дозволяє класифікувати її як конвергентне рішення, що об’єднує класичну охоронну сигналізацію з передовими технологіями відеоаналітики.

Рисунок 1.5 – Охоронна система Hikvision AX PRO [16]

З апаратної точки зору архітектура системи базується на центральному хабі, який підтримує підключення до 210 периферійних пристроїв (давачів). Ключовою інновацією є використання технології подвійного радіочастотного сигналу з протоколами Tri-X та Cam-X, які працюють на частоті 868 МГц. Перший протокол забезпечує стабільну передачу подій та команд на відстані до 2000 метрів, тоді як другий спеціально виділений для передачі графічних даних, що дозволяє реалізувати функцію фотоверифікації тривог через давачі PIRCAM. Апаратна стійкість системи підсилюється механізмом частотного хоппінгу між 50 каналами для уникнення навмисних завад та часовим розділенням сигналів, що запобігає виникненню перешкод у радіоефірі. Комунікаційна складова хаба включає повний набір інтерфейсів. Важливою

особливістю є інтеграція RFID-зчитувачів безпосередньо в органи керування, що розширює способи авторизації користувачів.

З програмної точки зору AX PRO функціонує в межах глобальної екосистеми Hikvision, використовуючи два основні програмні продукти: Hik-Connect для кінцевих користувачів та Hik-ProConnect для професійних інсталяторів. Програмне середовище дозволяє здійснювати точне налаштування сценаріїв автоматизації та зв’язків між давачами та камерами відеоспостереження, реалізуючи функцію IVaaS (Intrusion Verification as a Service [17]). Це дає змогу отримувати не лише статичні фото, а й короткі відеоролики під час спрацювання тривоги для миттєвої оцінки ситуації. Програмна логіка системи підтримує оновлення OTA (Over-The-Air [18]), автоматично актуалізуючи прошивки компонентів через хмарні ресурси без втручання користувача. Високий ступінь автоматизації програмних алгоритмів дозволяє системі самостійно контролювати стан батарей периферійних пристроїв, забезпечуючи їх автономну роботу до 5 років, та здійснювати моніторинг радіоефіру в режимі реального часу для виявлення спроб саботажу.

Як бачимо кожна система має свій унікальний підхід до фізичної передачі сигналу та визначає швидкість її реакції. Зведена інформація про основні характеристики розглянутих вище систем охоронної сигналізації подано в таблиці 1.2.

Таблиця 1.2 – Зведена таблиця порівняльних характеристик

Критерій	Система охоронної сигналізації			
	AJAX FIBRA	TIRAS Orion NOVA	Satel ABAX 2	Hikvision AX PRO
Тип системи	Дротова (цифрова шина)	Гібридна (Grade 3)	Бездротова (професійна)	Бездротова (відеоцентрична)
Максимальна кількість зон/пристроїв	До 100	До 128	До 48 (залежить від ПКП)	До 210
Дальність зв’язку	2000 м (провідник)	1000 м (провідник) / 3000 м (радіо)	2000 м (радіо)	2000 м (радіо)
Відео-верифікація	Так (через хмару)	Обмежена	Через додаткові модулі	Бортова (PIRCAM / IVaaS)
Резервування	Ethernet, GSM (2G/4G)	Ethernet, 2G (2 SIM), Wi-Fi	Ethernet, GSM, PSTN	Ethernet, Wi-Fi, 4G (2 SIM)

1.5 Постановка завдань на кваліфікаційну роботу бакалавра

Ефективність сучасних систем захисту житлових об’єктів напряму залежить від детального аналізу архітектурних особливостей будівлі, виявлення потенційних шляхів несанкційонованого проникнення та правильного вибору технологічного стеку. Проєктування комплексу безпеки для приватного будинку вимагає синергії між надійною апаратною інфраструктурою та гнучким програмним забезпеченням, що дозволяє забезпечити стабільне його функціонування в умовах динамічних експлуатаційних навантажень.

Для досягнення поставленої мети та розв’язання описаної науково-технічної проблеми необхідно виконати такі завдання:

– проаналізувати архітектурно-планувальне рішення приватного будинку як об’єкта проєктування, змоделювати потенційні загрози та визначити найбільш вразливі зони периметра й внутрішнього простору.

– провести порівняльний аналіз сучасних дротових/бездротових технологій безпеки з точки зору доцільності впровадження адресно-цифрового шинного протоколу.

– розрахувати та спроєктувати топологію кабельної мережі ліній та виконати перевірочні інженерні розрахунки.

– здійснити програмно-апаратну інтеграцію централі та периферійних засобів виявлення.

– розробити програмні алгоритми збору телеметрії (моніторинг напруги, стану зв'язку) та обробки сигналів тривоги з об’єкта для інтеграції з пультами централізованого спостереження або сторонніми сервісами.

РОЗДІЛ 2
ОБҐРУНТУВАННЯ ВИБОРУ ЗАСОБІВ ТА МЕТОДІВ РЕАЛІЗАЦІЇ

2.1 Вибір базової апаратної платформи

Методика вибору оптимальної апаратної платформи для охоронної системи приватного будинку базується на детальному аналізі специфіки вразливостей кожної із зон та порівнянні технічних можливостей наявних охоронних систем.

Специфіка вразливості вхідної групи (рис. 2.1, а), яка складається із тамбура (3,9 м²) та заскленого виходу на терасу (10,5 м²), полягає у високій ймовірності силового взламування або розбиття великих скляних поверхонь, які часто мають низьку видимість з боку вулиці, що робить цю зону найбільш критичною точкою проникнення.

Специфіка вразливості віконних проємів (рис. 2.1, б) обумовлена їх рівномірним розподілом за периметром 13,32×9,12 м, де кутові кімнати (18,14 м² та 18,09 м²) стають найбільш незахищеними через наявність декількох векторів потенційного доступу (рис. 2.1, б), що вимагає від системи надійного адресного детектування.

Центральний хол (5,18 м²), як стратегічний транзитний вузол (рис. 2.1, в), характеризується також вразливістю: якщо основний периметр буде подолано, саме контроль цієї зони буде останнім рубежем для фіксування переміщення зловмисника між спальнями (18,14 м² та 18,09 м²), санвузлом (6,36 м²) й вітальнею (26,78 м^2).

Методика вибору платформи включає у себе оцінку критерія за типом зв’язку (табл. 2.1): Ajax FIBRA пропонує революційну дротову цифрову технологію, яка ідеально підходить для надійного захисту тераси та вікон без необхідності заміни елементів живлення, тоді як Satel ABAX 2 забезпечить професійну двосторонню радіопередачу із високою завадостійкістю, що є важливим для складного планування з багатьма перестінками.

Рисунок 2.1 – План першого поверху приватного будинку:
а) – вхідна група; б) – віконні проєми; в) – центральний хол

Таблиця 2.1 – Порівняльний аналіз вибору платформи

Платформа	Пріоритетний тип зв’язку	Оптимальний сценарій використання
Ajax FIBRA	Цифрова дротова шина	Приватні будинки (ремонт), висока автономність
Tiras Orion NOVA	Гібридний (Grade 3)	Банки, ТРЦ, великі офіси, державні установи
Satel ABAX 2	Завадостійкий радіоканал	Складні радіоумови, професійний монтаж
Hikvision AX PRO	Радіоканал з відеоверифікацією	Котеджі, малий бізнес з акцентом на відео

Під час вибору системи за критерієм верифікації, то Hikvision AX PRO демонструє перевагу у зоні тераси завдяки вбудованій відеоаналітиці та фотофіксації тривог, що дозволить миттєво відрізнити реальну загрозу від помилкового спрацювання. Tiras Orion NOVA виступає як найбільш

збалансоване за ціною та надійністю рішення для українського ринку, пропонуючи строгу відповідність Grade 3 та можливість побудувати гібридну систему, де критичні зони (вхід та тераса) будуть захищені провідниками, а хол та спальні – безпровідними модулями серії X.

Обґрунтування вибору системи охоронної сигналізації потребує формування порівняльної таблиці де повинні відображатися їх ключові технічні параметри, які впливають на надійність, масштабованість та функціональність об’єкта. В таблиці 2.2 подано розгорнуту матрицю, за якою аргументують свій вибір на користь тієї чи іншої платформи (залежить від пріоритетів проєкту).

Таблиця 2.2 – Порівняльна таблиця програмно-апаратних комплексів безпеки

Критерій	Система охоронної сигналізації			
	Ajax FIBRA	Tiras Orion NOVA	Satel ABAX 2	Hikvision AX PRO
Технологічна основа	Цифрова провідникова шина	Гібридна (провідники + радіо)	Професійний радіоканал	Бездротова (відеоцентрична)
Рівень безпеки (Grade)	Grade 2	Grade 3	Grade 2	Grade 2
Максимальна кількість пристроїв	100	128	48 (залежить від ПКП)	210
Дальність зв’язку	2000 м (кабель)	1000 м (кабель)	2000 м (радіо)	2000 м (радіо)
Автономність (від АКБ)	До 60 годин	До 24 годин	Залежить від ПКП	До 12 годин
Відеоверифікація	Так (серія фото)	Обмежена (сторонні)	Через модулі інтеграції	Вбудована (фото/відео)
Канали зв’язку	Ethernet, Wi-Fi, 4G	Ethernet, Wi-Fi, 2G (2 SIM)	GSM, IP, PSTN	Ethernet, Wi-Fi, 4G (2 SIM)
Налаштування системи	Мобільний додаток (PRO)	ПЗ «Tiras-1» / клавіатура	ПЗ DLOADX (через PC)	Hik-ProConnect / Web
Складність монтажу	Середня (потребує кабеля)	Висока (професійна)	Середня	Низька (Plug & Play)
Відеоверифікація	Так (серія фото)	Обмежена (сторонні)	Через модулі інтеграції	Вбудована (фото/відео)

Застосовуючи, до об’єкта проєктування, методику експертних оцінок [19] бачимо (табл. 2.3), що найвищий бал в Ajax FIBRA (рис. 2.2), оскільки її здатність працювати на довгих лініях дозволяє легко охопити увесь периметр

будинку, а програмна підтримка миттєвих сповіщень та фотопідтверджень нівелює ризики, пов’язані із вразливістю великої площі скління.

Таблиця 2.3 – Експертна оцінка порівняльних характеристик систем

Ваговий коефіцієнт (W_i)	Система охоронної сигналізації			
	Ajax FIBRA	Tiras Orion NOVA	Satel ABAX 2	Hikvision AX PRO
Надійність (0,25)	9	10	9	8
Гібридність (0,20)	9	10	8	9
Автономність (0,15)	10	8	7	8
Програмне забезпечення (0,20)	10	7	8	9
Відеоверифікація (0,10)	8	7	6	10
Монтаж (0,10)	7	7	9	10
Інтегральний бал	9,05	8,45	7,95	8,75

Рисунок 2.2 – Модуль для інтеграції сторонніх пристроїв у систему Ajax Superior MultiTransmitter Fibra [20]

Як бачимо, ця методика дозволяє трансформувати архітектурні недоліки будинку (велика кількість вікон та відкрита тераса) у вимоги, які висуваються до апаратної потужності та швидкодії вибраної платформи, забезпечуючи, при цьому, цілісну та інтелектуальну систему захисту.

2.2 Вибір периферійного обладнання та давачів

Для забезпечення максимальної безпеки об’єкта проектування необхідно передбачити три рубежа охорони, які дозволять послідовно виявляти загрози, починаючи від підступів до будівлі та завершуючи внутрішнім простором. Такий підхід мінімізує час перебування зловмисника всередині непоміченим та дозволяє задіяти відповідні сценарії реагування на ранніх стадіях.

Першим і критично важливим ешелоном захисту приватного будинку є зовнішній периметр (тераса площею 10,50 м²), який є суттєвою зоною ризику. Тераса, як правило, є найбільш доступною та має найменшу природну протидію перешкоді. На відміну від внутрішніх приміщень, тут зловмисник може перебувати довший час, готуючись до подальшого взламування.

Для захисту цієї зони найбільш вдалим та обґрунтованим вибором виступають зовнішні комбіновані сповіщувачі руху [21-23]. Ці пристрої використовують одночасно пасивний інфрачервоний та мікрохвильовий сенсори (рис. 2.3). Таке поєднання є ключовим для зовнішнього застосування, оскільки ІЧ-сенсор може сформувати помилковий сигнал від нагрітих сонцем предметів або тварин, а НВЧ-сенсор реагує на будь-який рух, але не розрізняє об’єкти. Спільне спрацювання обох сенсорів гарантує високу точність виявлення людини та мінімізує кількість помилкових тривог від птахів, вітру або змін температури. Оптимальним буде монтаж сповіщувача типу «штора» або з вузькою діаграмою спрямованості для перекриття фасаду тераси. Такий давач створює невидиму стіну, реагуючи лише на її перетин, і дозволяє виявити загрозу ще до того, як зловмисник почне пошкоджувати вікно або двері.

а) б)

Рисунок 2.3 – ІЧ давач руху з додатковим мікрохвильовим сенсором Ajax MotionProtect Plus Jeweller [24]:

а) – вигляд загальний; б) – параметри виявлення

Другий рубіж охорони захищає найбільш вразливі точки входу – віконні проєми та вхідні двері. Цей ешелон захисту повинен виявляти як спроби

відкриття, так і руйнування будівельних конструкцій. Для захисту від відкриття на усі стулки вікон та полотна вхідних дверей встановлюють магнітоконтактні сповіщувачі [21-23], більш відомі як геркони (рис. 2.4). Це найпростіший, найнадійніший та найекономічніший спосіб контролю цілісності периметра. Принцип їх роботи базується на розмиканні контактів під час віддалення магніту від давача. Їх неможливо обійти, не пошкодивши саме вікно. Додатковою перевагою є можливість налаштування системи на взяття об'єкта під охорону із відкритими на «мікровентиляцію» вікнами, що забезпечує комфорт та безпеку одночасно.

Рисунок 2.4 – Давач відчинення з герконом Ajax DoorProtect Jeweller [25]

Для захисту від проникнення через розбите скло, без відкриття стулки вікна, доцільно застосовувати акустичні сповіщувачі розбиття скла [21-23]. Ці давачі (рис. 2.5) є звуковими та реагують на специфічний звуковий спектр, який складається із двох послідовних компонентів: звуку удару та звуку руйнування кристалічної решітки скла. Такий складний алгоритм обробки звуку дозволяє відрізнити реальне розбиття від випадкового падіння металевих предметів або інших побутових шумів. Встановлюються такі пристрої на стелі або стіни навпроти вікон. В кімнатах із великою площею скління, до прикладу вітальня (26,78 м²), один такий давач може ефективно захистити декілька вікон одночасно, що робить їх вибір економічно виправданим.

Третій рубіж охорони є резервним і захищає внутрішній простір. Він необхідний у тому випадку, якщо зловмисник все ж таки зміг проникнути всередину будівлі непоміченим, обійшовши перші два ешелони (наприклад,

через дах, підвал або якщо він був всередині до ввімкнення охорони). У ключових точках будинку, таких як вітальня (26,78 м²) та центральний хол (5,18 м²), які є загальною ланкою між усіма приміщеннями, встановлюють внутрішні пасивні інфрачервоні сповіщувачі руху [21-23]. Ці давачі (рис. 2.6) реагують на зміну теплового фону при русі людини. Оптимальним є вибір моделей з імунітетом до тварин, щоб уникнути помилкових спрацювань, якщо у будинку є домашні улюбленці. Встановлюються вони в кутах кімнат для максимального перекриття площі, направляючи промені перпендикулярно до найбільш ймовірного маршруту руху, де вони найбільш чутливі.

Рисунок 2.5 – Давач розбиття скла з мікрофоном Ajax GlassProtect Jeweller [26]

Рисунок 2.6 – ІЧ давач руху Ajax Superior MotionProtect Fibra [27]

Наступним етапом обґрунтування вибору периферійного обладнання та давачів є специфікація вибору, яка подається у формі матриці обґрунтування. Цю матрицю подано в таблиці 2.4 у вигляді структурованого інструменту, який дозволяє аргументувати прийняття проєктних рішень шляхом прямого зіставлення технічних характеристик обладнання із конкретними експлуатаційними вимогами об’єкта. Такий підхід забезпечує об’єктивність

вибору, де кожен компонент периферії або центральна панель оцінюється через призму техніко-економічної доцільності, мінімізації ризиків хибних спрацювань та відповідності нормативним стандартам, створюючи надійне підґрунтя для подальшої технічної реалізації проєкту.

Таблиця 2.4 – Специфікація вибору

Тип обладнання	Місце встановлення	Обґрунтування вибору
Пасивний інфрачервоний + мікрохвильовий (PIR + MW (Dual))	Кухня та вітальня	Висока імовірність теплових завад (плита, камін).
Давач розбиття скла (GlassProtect)	Вікна	Необхідність захисту від розбиття без штроблення рам.
Давач відкриття дверей (DoorProtect)	Вхідна група	Виявлення первинного проникнення (статус «Відкрито»).
Пасивний інфрачервоний давач руху (PIRCAM)	Хол / Вхід	Візуальна верифікація тривоги для зменшення хибних виїздів ДСО.
Вулична сирена (Outdoor Siren)	Фасад будинку	Психологічний вплив на злочинця та інформування сусідів.

Розрахунок надійності периферійного обладнання охоронної системи є критичним етапом проектування, який дозволяє математично спрогнозувати стабільність функціонування усієї мережі сповіщувачів протягом заданого експлуатаційного періоду. Методологічно цей процес базується на визначенні ймовірності безвідмовної роботи кожного окремого пристрою за допомогою експоненціального закону надійності, де ключовим показником є інтенсивність відмов, що зазвичай вказується виробником у технічній документації.

Оскільки периферійні пристрої, такі як датчики руху, магнітоконтактні сповіщувачі та сирени, утворюють послідовну, з точки зору надійності, структуру, вихід із ладу будь-якого критичного елемента призводить до часткової або повної втрати функціональності відповідної зони захисту.

Математична модель розрахунку загальної надійності системи $P_c(t)$ являє собою добуток ймовірностей безвідмовної роботи усіх її компонентів (2.1):

$$P_c(t) = P_1(t) \cdot P_2(t) \cdot \ldots \cdot P_n(t), \quad (2.1)$$

де $P_i(t)$ – ймовірність того, що і-й давач не відмовить протягом певного часу t.

Для сучасного професійного обладнання рівнів Grade 2 та Grade 3 показник інтенсивності відмов є надзвичайно низьким, що забезпечує індивідуальну надійність кожного пристрою на рівні 0,99 і вище. Проте під час проектування розгалужених систем для приватних будинків великої площі, де кількість периферійних одиниць може сягати 20-30 пристроїв, загальна ймовірність безвідмовної роботи системи природно знижується, що обґрунтовує необхідність регулярного технічного обслуговування та програмного моніторингу стану елементів живлення та каналів зв’язку.

Окрім цього, розрахунок повинен враховувати середній час відновлення системи після відмови, який у сучасних комплексах мінімізується завдяки функціям самодіагностування та миттєвого сповіщення про втрату зв’язку з периферійним пристроєм.

2.3 Вибір програмного забезпечення для керування та моніторингу

Вибір програмного забезпечення для системи охоронної сигналізації на базі Ajax Superior MultiTransmitter Fibra визначає не лише зручність користування, а й відповідність комплексу строгим міжнародним стандартам безпеки. Обґрунтування вибору операційної системи (ОС) централі базується на використанні пропрієтарної ОС «Malevich», яка належить до класу систем реального часу (RTOS). На відміну від універсальних ОС, Malevich працює за принципом циклічного опитування пристроїв та детермінованого розподілу ресурсів, що гарантує миттєву обробку тривожного сигналу навіть у моменти пікового навантаження. В лінійці «Superior» додатково оптимізовано програмне ядро, що дозволяє підтримувати алгоритми Grade 3 та здійснювати глибокий моніторинг стану ліній системи, які підключаються через MultiTransmitter Fibra, розрізняючи, при цьому, типи несправностей та спроби саботажу сторонніх давачів із високою точністю.

Аргументація використання мобільних застосунків для кінцевого користувача та інсталятора (Ajax та Ajax PRO) полягає в забезпеченні повної

прозорості та інтерактивності гібридної системи. Через застосунок реалізується унікальна можливість програмного налаштування MultiTransmitter: вибір типу опору резисторів, регулювання затримок та моніторинг напруги живлення в реальному часі. Це дозволяє власнику об’єкта не лише отримувати детальні push-сповіщення з фотоверифікацією, а й дистанційно діагностувати стан провідникових давачів, які інтегровано у загальну систему. Це радикально підвищує зручність експлуатації та знижує витрати на виклик сервісної служби.

Вибір методів передачі даних та обґрунтування протоколів шифрування базується на синергії цифрового протоколу Fibra та багатоканальності централі. Fibra використовує пакетну передачу даних із обов’язковим підтвердженням від хаба, що унеможливлює втрату повідомлення. Усі дані шифруються за алгоритмом із плаваючим ключем, що виключає можливість ретрансляції сигналу або програмного взламування. Програмна логіка Superior MultiTransmitter Fibra передбачає постійну автентифікацію кожного підключеного пристрою, а шифрований обмін даними між хабом та хмарою Ajax Cloud забезпечує захист від DDoS-атак та спроб підміни обладнання.

Використання резервних каналів зв’язку (Ethernet та 4G) у поєднанні з криптографічним захистом гарантує доставку критично важливої інформації протягом надмалого часу, забезпечуючи найвищий рівень кібербезпеки приватного будинку.

2.4 Методика інтеграції та способи взаємодії компонентів системи

Методика інтеграції та способи взаємодії компонентів системи базуються на створенні єдиного інформаційного середовища, де кожен елемент системи працює в синергії з іншими для мінімізації часу реакції на загрозу.

Опис топології підключення для дротових сегментів системи Ajax Fibra передбачає використання шинної структури, де пристрої підключаються послідовно до чотирижильного кабелю. Це дозволяє реалізувати як лінійну, так і кільцеву топологію.

Кільцеве підключення – це пріоритетний метод інтеграції, оскільки воно забезпечує фізичне резервування: у разі обриву кабелю в будь-якій точці система миттєво розбиває лінію на два незалежні промені, зберігаючи повну працездатність усіх давачів. Для інтеграції застарілих дротових зон використовують модуль MultiTransmitter Fibra, який перетворює аналогові сигнали інших сповіщувачів у цифровий формат протоколу Fibra, дозволяючи програмно керувати живленням та режимами роботи кожного пристрою.

Методи інтеграції підсистеми відеоспостереження до загального контуру безпеки реалізують через хмарні та прямі протоколи передачі даних. Використання протоколу RTSP (Real Time Streaming Protocol [28]) дозволяє отримувати живий потік із будь-якої IP-камери безпосередньо в мобільний застосунок охоронної системи, забезпечуючи високу швидкість трансляції. Найбільш ефективним є метод P2P (Peer-to-Peer [29]), який використовують для глибокої інтеграції камер Hikvision або Dahua. Цей спосіб дозволяє не лише переглядати відео, а й реалізувати функцію відеоверифікації тривог: під час спрацювання визначеного давача система охоронної сигналізації автоматично підтягує відеозапис із прив’язаної до цієї зони камери. Це створює єдиний контекст події, де текстове сповіщення підкріплюється візуальним доказом, що критично важливо для ідентифікації або відхилення хибних викликів.

Сценарії автоматизації розглядають як засоби підвищення ефективності охорони, що дозволяє системі перейти від пасивного інформування до активної протидії. Програмна логіка взаємодії дозволяє налаштовувати алгоритм дій, який активовується за певної події, працюючи на випередження. Сценарії за розкладом або за зміною режиму охорони не лише підвищують безпеку, але й оптимізують енергоспоживання.

2.5 Обґрунтування методів монтажу та налаштування

Обґрунтування методів монтажу та налаштування системи Ajax Fibra базується на забезпеченні фізичної цілісності ліній зв’язку та відповідності

програмних параметрів давачів реальним умовам об’єкта. Вибір витратних матеріалів розпочинається із підбору кабельної продукції: для системи Fibra стандартом є чотирижильна мідна вита пара (U/UTP Cat 5e) або спеціалізований сигнальний кабель (Alarm Cable) поперечним перетином не менше 0,22 мм². Використання саме мідних провідників, а не обмідненого алюмінію (CCA), є критичним для мінімізації опору лінії на великих відстанях та стабільного живлення периферії. Монтаж кабелю здійснюють всередині гофрованих ПВХ-труб або в штробах під шаром штукатурки для захисту від випадкових механічних пошкоджень, а інсталювання самих пристроїв – на капітальні конструкції за допомогою комплектних кріплень «SmartBracket», які мають вбудовані тампери для виявлення відриву пристрою від поверхні.

Методика тестування зон виявлення та калібрування чутливості давачів після завершення монтажних робіт реалізується через системне тестування у застосунку Ajax PRO. Першим етапом є «Тест рівня сигналу Fibra», який перевіряє стабільність обміну пакетами даних. Далі проводиться «Тест зони виявлення», під час якого інсталятор фізично переміщується у приміщенні, фіксуючи моменти спрацювання давача. Калібрування чутливості виконується програмно для кожної зони окремо, що дозволяє досягти балансу між швидкістю виявлення порушника та відсутністю хибних тривог.

Дотримання нормативних вимог ДСТУ CLC/TS 50131-7 під час інсталяції пристроїв системи охоронної сигналізації є обов’язковим для професійних систем безпеки. Відповідно до встановлених норм, сповіщувачі руху встановлюються на висоті 2,4 м (уникнення «сліпих зон»). Центральна панель монтується в прихованому місці із обмеженням доступом, але з дотриманням умов вентиляції та стабільного покриття мережі. Ще однією вимогою стандарту є те, щоб кабельні мережі не проходили паралельно із силовими лініями (min 0,2-0,5 м) це дозволяє уникнути наведення електромагнітних перешкод, які спотворюють цифровий сигнал Fibra. Кінцева перевірка включає у себе обов’язкове тестування системи на відклик під час імітування саботажу, що підтверджує готовність об’єкта до встановлення під охорону.

РОЗДІЛ 3
ПРАКТИЧНА РЕАЛІЗАЦІЯ

3.1 Архітектурне рішення та структурна схема системи

Для забезпечення комплексної безпеки приватного будинку запроєктовано ешелоновану (багаторівневу) систему охоронної сигналізації. Основним принципом побудови такої системи є послідовне створення рубежів захисту, що дозволяє виявити загрозу на ранніх стадіях та мінімізувати ризики хибних спрацювань.

Архітектура системи базується на професійній дротовій адресній технології Ajax Fibra. Вибір цієї технології обґрунтовано наступними інженерно-технічними чинниками:

– шинна топологія підключення (дозволяє з’єднувати пристрої послідовно в лінії (шини), суттєво оптимізує витрати кабельної продукції сигнального типу);

– повна адресність пристроїв (кожен сповіщувач має у системі унікальний ідентифікатор, що забезпечує точну локалізацію події в інтерфейсі моніторингового пульта);

– висока завадостійкість та захист (передача даних у лініях Fibra відбувається за допомогою власного зашифрованого протоколу з автентифікацією для захисту від підміни пристроїв (спуфінгу) та постійним моніторингом цілісності лінії);

– енергонезалежність (живлення периферійних пристроїв реалізовано безпосередньо від шини з ультранизьким споживанням, що забезпечує тривалу автономну роботу системи від резервного акумулятора централі).

3.1.1 Специфікація та просторовий розподіл засобів виявлення

Відповідно до експлікації приміщень та визначених зон ризику (рис. 2.1), об’єкт проєктування розділено на три рубежі охоронного захисту.

Перший рубіж – периметральний захист – охоплює віконні проєми (контроль розбиття скла) та вхідну групу (контроль відкриття дверей).

Другий рубіж – об’ємний захист – охоплює житлові кімнати, спальні та зони загального користування (контроль просторового переміщення).

Третій рубіж – транзитні пастки – контролює внутрішній коридор, як критичний вузол логістики всередині будинку.

Для детального аналізу ешелонованої оборони об’єкта проєктування розроблено експлікацію периферійних пристроїв Ajax Fibra за функціональними зонами їх захисту

Таблиця 3.1 – Експлікація обладнання системи сигналізації за зонами захисту

Назва приміщення (зони)	Площа, $м^2$	Рубіж захисту	Тип та модель обладнання Ajax / Кількість	Специфіка та логіка монтажу
Вхідна група (Тамбур)	4,82	–	Central Hub Hybrid (2G/4G) / 1 KeyPad Fibra / 1 DoorProtect Fibra / 1	Централь монтують приховано у захищеному місці із оптимальним рівнем GSM-сигналу. Клавіатура керування – біля дверей на висоті 1,5 м. Магнітоконтактний давач – на полотно вхідних дверей.
Вітальня	26,78	I та II	CombiProtect Fibra / 1	Монтується в кутку навпроти віконних конструкцій.
Кухня	9,40	I та II	CombiProtect Fibra / 1	Монтується в кутку навпроти віконних конструкцій.
Спальня 1	18,09	II	MotionProtect Fibra / 1	Оптична вісь давача спрямовується на віконний проєм та зону дверей.
Спальня 2	18,14	II	MotionProtect Fibra / 1	Оптична вісь давача спрямовується на віконний проєм та зону дверей.
Коридор	5,18	III	MotionProtect Fibra / 1	Оптична вісь давача руху формує «пастку» фіксуючи порушника, якщо той подолав/оминув перший рубіж охорони без активації вхідної групи.

Слід врахувати, що лінійка Fibra орієнтована на стаціонарні охоронні сповіщувачі та давачі протікання води LeaksProtect, які інтегруються через бездротовий протокол Jeweller, що є технічно доцільним для уникнення прокладання кабелів по підлозі у вологих зонах.

3.1.2 Структурна схема системи та топологія кабельних ліній

Структурна схема комплексу безпеки побудована за радіально-шинною архітектурою. Основним елементом системи є гібридна централь Hub Hybrid Fibra, яка координує роботу пристроїв, обробляє сигнали, які надходять від сповіщувачів та здійснює передачу тривожних сповіщень.

Для оптимізації кабельних трас та підвищення живучості системи, дротову топологію об’єкта проєктування розподілено на дві незалежні шини:

– «Шина №1» (периметр та керування) – підключається до виходу «Line 1» централі, а кабель проходить транзитом через пристрої вхідної групи та загальних кімнат:

Central Hub Hybrid → KeyPad Fibra (Тамбур) → DoorProtect Fibra (Тамбур) →
→ CombiProtect Fibra (Кухня) → CombiProtect Fibra (Вітальня);

– «Шина №2» (внутрішній простір) – підключається до виходу «Line 2» централі та охоплює виключно об’ємні сповіщувачі внутрішньої зони:

Central Hub Hybrid → MotionProtect Fibra (Коридор) →
→ MotionProtect Fibra (Спальня 1) → MotionProtect Fibra (Спальня 2).

Запропонований розподіл дозволяє фізично розмежувати зони постійного контролю (Шина №1) та зони гнучкого відключення (Шина №2).

3.1.3 Організація каналів зв’язку та алгоритм функціонування

Для забезпечення високого коефіцієнта готовності ($к_г$) та відмовостійкості системи технічних засобів охорони, у проєкті, на базі централі Hub Hybrid Fibra реалізовано технологію мультиканального дублювання зв’язку (Quad-stream). Інформаційний обмін між об’єктом, хмарним сервером моніторингу та пультом централізованого спостереження (ПЦС) здійснюється через три незалежні фізичні та логічні канали:

– основний канал (дротовий) – Ethernet (10/100 Base-T) через локальну мережу об’єкта до широкосмугового інтернет-провайдера (забезпечує мінімальний пінг (до 0,15 с) та постійний обмін тестовими пакетами);

– резервний канал №1 (бездротовий) – мобільний зв’язок GSM/передача даних стандарту 4G (LTE) через першу SIM-карту основного оператора;

– резервний канал №2 (бездротовий) – мобільний зв’язок GSM/передача даних стандарту 2G/3G через другу SIM-карту альтернативного оператора

Логіка моніторингу каналів базується на постійному опитуванні хмари Ajax Cloud (період опитування 36 с). У випадку зникнення зв’язку за основним каналом (Ethernet), хаб автоматично (<1 с) перемикається на мобільну мережу 4G/3G/2G. Якщо сервер Ajax Cloud фіксує повну втрату зв’язку (3-5 хв) з хабом за усіма каналами, то генерує сповіщення «Втрачено зв’язок», що запобігає спробам саботажу шляхом глушіння.

Передача тривожних сповіщень на ПЦС здійснюється за міжнародним текстовим протоколом SIA (DC-09) [30] або Contact ID [31], що гарантує повну сумісність із сучасним ПЦС-софтом.

Функціонування системи охоронної сигналізації приватного будинку базується на циклічному опитуванні периферійних пристроїв та виконанні алгоритму обробки подій за пріоритетністю. Обрана система працює у трьох, основних, макрорежимах:

– режим «Знято з охорони» (Disarmed) – активні лише давачі 24/7;

– режим «Повна охорона» (Armed) – активні усі зони першого, другого та третього рубежів захисту;

– режим «Часткова/Нічна охорона» (Stay Mode) – активний перший рубіж (об’ємні давачі руху в спальнях і коридорі ігноруються).

Нижче, у вигляді блок-схеми алгоритму обробки подій, наведено розроблену візуалізацію логіки роботи системи охоронної сигналізації приватного будинку на базі гібридної централі Hub Hybrid Fibra.

3.2 Проєктування кабельної інфраструктури та топології підключення

Дротова система охоронної сигналізації Ajax Fibra використовує адресну шинну архітектуру. Для забезпечення максимальної надійності, живучості системи та оптимізації кабельних трас необхідно користуватись:

– топологією «Промінь/Line» – підключення лінійних груп сповіщувачів (периферійні пристрої підключаються до лінії один за одним, при цьому останній пристрій в лінії глушать термінуючим резистором);

– топологією «Кільце/Ring» – підключення об’єктів, до яких висуваються підвищені вимоги до безпеки (у випадку обриву лінії кільце розпадається на два робочих сегменти («Промені»), а система продовжує працювати в штатному режимі, сигналізуючи про аварію).

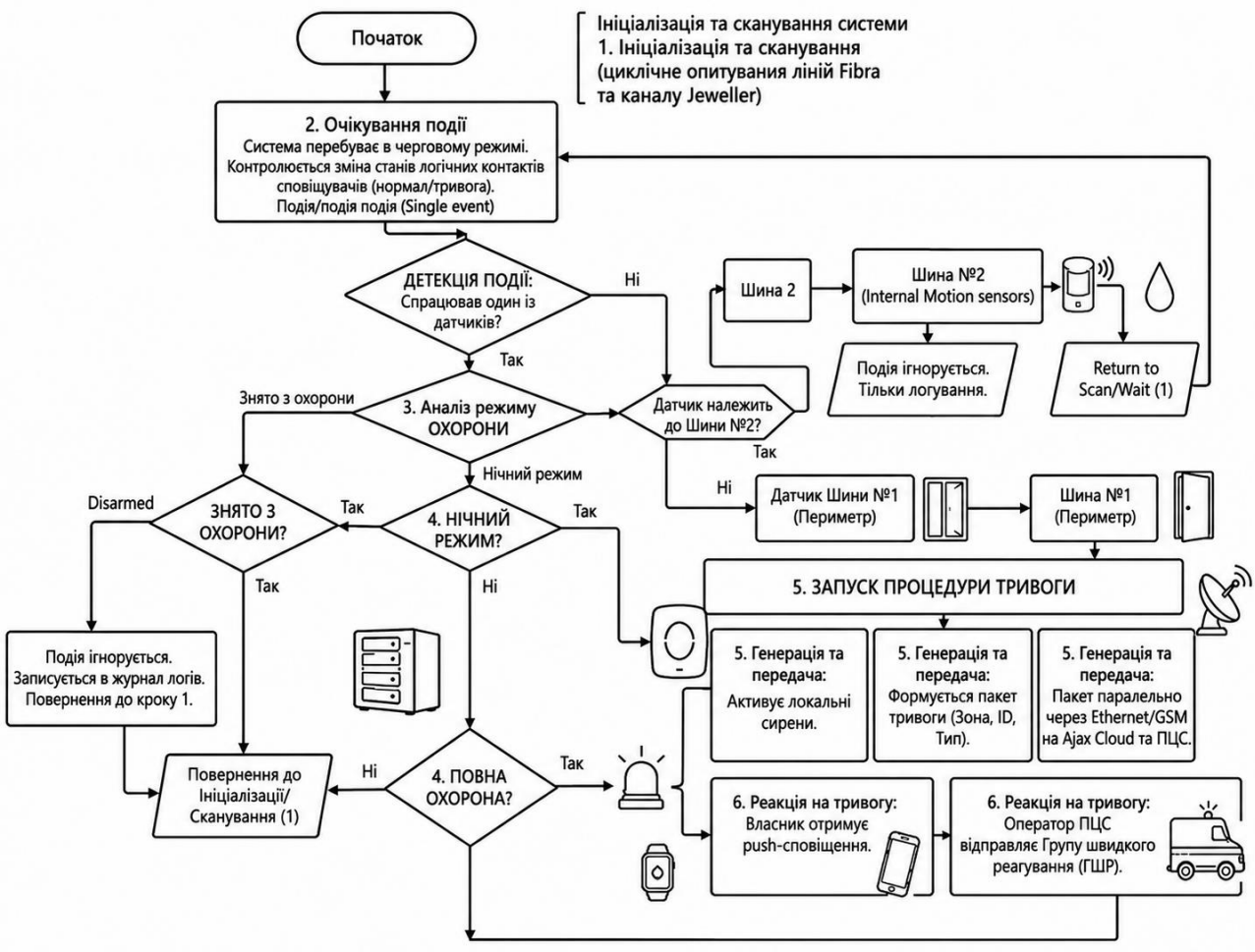


Рисунок 3.1 – Алгоритм роботи системи Ajax Fibra

Вимоги, які висуваються до кабельної продукції:

– тип кабелю: сигнальний кабель або вита пара (U/UTP Cat.5e);

– матеріал провідника: виключно мідь, використання обмідненого алюмінію або сталі не рекомендовано через високий питомий опір;

– рекомендований поперечний перетин жил кабеля: від 0,22 до 0,50 мм².

3.2.1 Розрахунок довжини ліній та падіння напруги

Основною умовою стабільної роботи пристроїв Fibra є забезпечення номінальної напруги живлення. Максимальне падіння напруги на лінії (за вихідної напруги з Hub Hybrid ~24 В) не повинно знижувати напругу на найвіддаленішому пристрої нижче 8 В (3.1):

$$U_з=24-Uп \geq 8 \text{ В}, \quad (3.1)$$

де $U_п$ – падіння напруги, яке встановлюють із виразу (3.2):

$$U_п=I_з \cdot R, \quad (3.2)$$

де $I_з$ – сумарний струм споживання усіх пристроїв на лінії в режимі тривоги;

R – опір кабелю, який встановлюють з (3.3):

$$R=2\rho \cdot (L/S), \quad (3.3)$$

де ρ – питомий опір міді (0,0175 Ом·мм^2/м);

L – довжина лінії;

S – площа поперечного перетину жили (для Cat.5e (24 AWG) S≈0,205 мм^2).

Паспортні дані компонентів Ajax Fibra, необхідні для розрахунку сумарного струму споживання шини сигналізації зведено в таблиці 3.2.

Таблиця 3.2 – Технічна характеристика пристроїв Ajax Fibra

Назва пристрою	Тип пристрою	Максимальне споживання струму
MotionProtect Fibra	Сповіщувач руху	7 мА
DoorProtect Fibra	Сповіщувач відкриття	7 мА
GlassProtect Fibra	Сповіщувач розбиття скла	7 мА
CombiProtect Fibra	Сповіщувач руху та розбиття	7 мА
KeyPad Fibra	Клавіатура керування	15 мА
HomeSiren Fibra	Кімнатна сирена	30 мА
StreetSiren Fibra	Вулична сирена	100 мА
MultiTransmitter Fibra	Модуль інтеграції (18 зон)	120 мА

3.2.2 Планування кабельних ліній та підключення пристроїв

Для оптимізації монтажних робіт та забезпечення живучості системи розроблено схему трасування кабельних ліній (табл. 3.3).

Таблиця 3.3 – Архітектура ліній Fibra на об’єкті проєктування

Порт	Топологія	Тип кабелю	Довжина (м)	Підключені пристрої (послідовно)
Лінія 1	Промінь	Сигнальний 4×0,22	120	DoorProtect (вхід) → → MotionProtect (коридор) → KeyPad
Лінія 2	Промінь	U/UTP Cat.5e (мідь)	250	4×MotionProtect (4 кімнати) → → HomeSiren
Лінія 3	Кільце	U/UTP Cat.5e (порти 3-4)	400	6×CombiProtect (периметр 1-го поверху)
Лінія 4	Промінь	Сигнальний 4×0,50	80	StreetSiren (вулична сирена)

3.3.3 Розрахунок навантаженої лінії

Для розрахунку навантаженої лінії приймемо лінію №1 довжиною 120 м.

З таблиці 3.3 бачимо, що кабелем виступає сигнальний кабель 4×0,22, який виготовлено з міді (S=0,22 мм^2). Для живлення використовуються дві жили (одна на «+», одна на «-»). Довжина лінії – 120 метрів.

До лінії підключено один сповіщувач відкриття DoorProtect Fibra (7 мА), один сповіщувач руху MotionProtect Fibra (7 мА) та клавіатура керування KeyPad Fibra (15 мА).

Розрахуємо сумарний струм на лінії:

$$I_з = 7 + 7 + 15 = 29 \text{ мА} = 0,029 \text{ А}.$$

Розрахуємо опір лінії:

$$R = 2 \times 0,0175 \times (120 / 0,22) = 19,09 \text{ Ом}.$$

Встановлюємо падіння напруги на лінії:

$$U_п = 0,029 \times 19,09 \approx 0,55 \text{ В}.$$

Визначаємо кінцеве значення напруги:

$$U_з = 24 – 0,55 = 23,45 \text{ В}.$$

Як бачимо, 23,45 В > 8 В – лінія спроєктована правильно, падіння напруги знаходиться в межах норми й пристрої працюватимуть стабільно.

Для перевірки працездатності та забезпечення стабільного живлення усіх периферійних пристроїв проведено електричний розрахунок кабельних трас. Зведені результати обчислень для кожної шини наведено в таблиці 3.4.

Таблиця 3.4 – Зведена таблиця розрахунків ліній об’єкта

Порт	Сумарний струм (мА)	Опір на лінії (Ом)	Напруга падіння (В)	Очікувана напруга (В)
Лінія 1	7+7+15=29	19,09	0,55	23,45
Лінія 2	(4×7)+30=58	42,68	2,48	21,52
Лінія 3	6×7=42	68,29	2,87	21,13
Лінія 4	100	5,38	0,54	23,46

Відповідно до розрахункових даних, очікувана напруга на кінцевих пристроях усіх ліній задовольняє мінімальні технічні вимоги обладнання.

3.3.4 Правила монтажу та кабель-менеджменту

Для захисту системи від наводок, саботажу та механічних пошкоджень, монтаж кабельної інфраструктури виконують з дотриманням наступних правил:

– сумісне прокладання – забороняється прокладати слабкострумові кабелі Fibra в одному лотку або штробі разом із силовими кабелями 220/380 В; мінімальна відстань паралельного прокладання – 0,5 м; під час перетину кабелів кут повинен становити 90°;

– захист ліній – всередині приміщень кабель прокладається в ПВХ-трубах, гофротрубах або кабельних каналах (коробах), які стійкі до горіння; на вулиці кабель прокладається виключно в підземні комунікації або в УФ-захищених трубах;

– з’єднання кабелів – усі з’єднання ліній повинні виконуватись в монтажних коробках методом паяння або шляхом клемування (скрутки кабелів категорично заборонені);

– маркування – кожна лінія Fibra біля централі та в розподільчих коробах повинна мати бирку з маркуванням (наприклад: «Fibra Line 1 – Сектор А»).

Для забезпечення фізичного захисту кабельних трас та монтажу периферійного обладнання призначено необхідну номенклатуру та обсяги матеріалів (табл. 3.5).

Таблиця 3.5 – Специфікація кабельної продукції та монтажних матеріалів

Найменування матеріалу	Одиниця вимірювання	Кількість	Примітка
Кабель сигнальний з екраном ОК 4×0,22S-Cu	м	350	Для коротких ліній та давачів
Кабель мережевий U/UTP-cat5E 4×2×0,51 ЗЗКМ	м	500	Для магістральних ліній та кільця
Труба гофрована Ø16 мм з протяжкою 750N/5см, ПВХ	м	400	Для прокладання за гіпсокартоном
Короб пластиковий серії STEP 15×10/2 м	м	150	Для відкритого прокладання
Розподільча коробка NEOMAX NX1045	шт	12	Для розгалужень та комутації

3.3 Інтеграція апаратного та програмного забезпечення

Інтеграція апаратного та програмного забезпечення централі Ajax Hub Hybrid (Fibra) – це комплекс заходів, які дозволяють поєднати фізичну кабельну інфраструктуру, адресні цифрові пристрої та хмарну екосистему в єдину відмовостійку систему безпеки. На відміну від традиційних шлейфових систем, технологія Fibra базується на шинній топології, де кожен апаратний компонент (HardWare) інтегрується на програмному рівні (SoftWare) як окремий цифровий вузол із власною логічною адресою.

Нижче подано базову взаємодію компонентів системи на фізичному, логічному та хмарному рівнях, яка реалізується у три послідовні етапи.

Етап 1: апаратна інтеграція (HW Integration). На цьому етапі формується фізичне середовище для передачі даних та живлення пристроїв.

1. Топологія та прокладання кабелю. Для інтеграції пристроїв Fibra використовують чотирижильний кабель (мідний U/UTP cat.5e). Дві жили відповідають за живлення (+12 В, GND), а інші дві – за передачу даних (A, B).

2. Підключення до централі. Кабельні лінії зачищаються та затискаються у клемних колодках централі відповідно до маркування: «+» – живлення +12 в, «-» – заземлення/загальний); «A» – лінія даних «A»; «B» – лінія даних «B».

3. Забезпечення резервного живлення та каналів зв’язку. У корпус централі встановлюють свинцево-кислотний акумулятор 12 В (на 4/7/9 А·год).

Підключається основний канал зв’язку (Ethernet) та резервні (дві SIM-карти 2G/3G/4G залежно від покоління хаба).

Етап 2: програмно-апаратна синхронізація (FirmWare & Cloud). Цей етап зв’язує фізично підключені пристрої із програмним ядром централі ОС «Malevich» та хмарою Ajax Cloud:

[Пристрої Fibra] ← (Протокол Fibra) → [Hub Hybrid (OS Malevich)] ←

← (Протокол Cloud Connect) → [Ajax Cloud] ↔ [Застосунок PRO].

1. Ініціалізація централі. У застосунку Ajax PRO Tool створюється обліковий запис компанії/інсталятора. Хаб зчитує конфігурацію мережі через DHCP (або налаштовується статичний IP) й встановлює шифроване з’єднання з сервером Ajax Cloud за пропрієтарним протоколом Cloud Connect. Прив’язка хаба до об’єкта відбувається через сканування QR-коду (апаратний ID вноситься в базу даних хмари).

2. Сканування та адресація шин (Bus Scanning). Це є ключовим моментом інтеграції SW та HW. Кожен пристрій Fibra володіє унікальним заводським ID (чип-ідентифікатор). Інсталятор запускає «Сканування шин» через інтерфейс застосунку. ОС «Malevich» надсилає широкомовний запит по черзі на кожну з восьми ліній. Пристрої на лінії відповідають, передаючи свої ID та типи. Програма формує карту фізичного розташування пристроїв на шині.

3. Програмне призначення та логічна адресація. Ідентифікація за допомогою LED – поєднання віртуального пристрою у застосунку із реальним давачем, використовують функція «Миготіння». Централь надсилає команду конкретному ID, і світлодіод давача починає миготіти. Логічна прив’язка – пристрою присвоюють назву, він додається у відповідну охоронну групу (зону).

Етап 3: тестування та валідація інтеграції. Після того, як софт «побачив» залізо, необхідно провести програмні тести фізичних параметрів лінії через утиліти Ajax PRO.

1. Тест живлення шин (Bus Power Test). Програма програмно імітує максимальне навантаження (вмикає підсвітку клавіатури, сирени, давачів). Спеціальні давачі струму на платі централі заміряють падіння напруги. Якщо

напруга на кінці лінії падає нижче критичних 7 В, то софт видає попередження про необхідність перероблення топології або зменшення кількості пристроїв.

2. Тест рівня сигналу Fibra. Тут перевіряють якість цифрового сигналу та кількість втрачених пакетів даних між хабом і кінцевими пристроями. Нормою є стабільний рівень сигналу у 2-3 поділки.

3. Тест зони виявлення. Інсталятор фізично тестує кожен давач. У застосунку в реальному часі відображається графік спрацювання, що підтверджує правильність інтеграції логічної зони та фізичного сенсора.

3.4 Розробка та симуляція програмного забезпечення для інтеграції з екосистемою Ajax

Оскільки екосистема Ajax є закритою (Proprietary Software), то сторонні розробники не мають прямого доступу до вихідного коду самої операційної системи реального часу ОС «Malevich», яка функціонує безпосередньо на централі. Така архітектурна ізоляція є базовою вимогою безпеки для запобігання несанкціонованому втручанню у прошивку пристрою.

Проте, взаємодія з централями Ajax на програмному рівні успішно реалізується через два основні інтерфейси:

– Ajax Cloud API (Enterprise API) – дозволяє сторонньому ПЗ, серверам моніторингових компаній або системам «розумного будинку» здійснювати керування хабом, змінювати режими охорони та запитувати телеметрію;

– прямі протоколи моніторингу (SIA-DC09) – використовуються для миттєвої передачі подій та тривог безпосередньо від хаба на ПЦС.

Нижче наведено практичні приклади програмних рішень, які ілюструють інтеграцію верхнього рівня з апаратним комплексом Hub Hybrid.

3.4.1 Програмна реалізація сервера обробки подій (SIA-DC09)

Для отримання тривог від дротових пристроїв ліній Fibpa у режимі реального часу, ПЗ взаємодіє із Ajax Hub Hybrid за допомогою веб-хуків (Webhooks) або через пряме сокет-з’єднання.

У лістингу (Додаток А) подано програмний код обробника подій на мові Python. Він реалізує локальний сервер, який приймає та декодує тривоги і статуси від централі Ajax за міжнародним стандартом SIA-DC09.

3.4.2 Організація періодичного опитування стану давачів через REST API

Оскільки Ajax Hub Hybrid самостійно здійснює низькорівневе опитування давачів Fibra по фізичній шині, то зовнішнє прикладне програмне забезпечення не взаємодіє з кожним давачем. Замість цього софт робить періодичні запити до Ajax Cloud API за допомогою протоколу HTTP REST (через JSON-запити) або отримує потокові дані через WebSockets.

У тому випадку коли програма запитує стан хаба, хмарний сервер повертає структуру даних, де для пристроїв ліній Fibra критично важливими є параметри живлення (вольтаж) та якість зв’язку. Приклад такої відповіді наведено у структурі JSON (Додаток Б).

Для аналізу таких даних розроблено сервіс опитування (polling-скрипт). У лістингу (Додаток В) наведено приклад коду, який імітує роботу служби автоматичного моніторингу: програма кожні 10 секунд звертається до інтерфейсу API, оцінює стабільність підключення пристроїв Fibra, рівень сигналу та загрозу падіння напруги на шині.

3.4.3 Високорівнева симуляція процесів сканування та адресації шин

Оскільки низькорівневі процедури фізичного опитування цифрової шини виконуються мікроконтролером централі під управлінням ОС «Malevich» безпосередньо, то розробники позбавлені доступу до керування драйверами шини.

Для проектування сумісних рішень та розуміння архітектури обміну даними, цей процес було відтворено у вигляді високорівневої програмної симуляції. У лістингу (Додаток Г)Х.3 представлено симулятор, який відображає внутрішню логіку роботи хаба під час сканування ліній: відправку широкомовного запиту (Broadcast), збір унікальних апаратних ID (чип-ідентифікаторів) та динамічне формування логічної карти адрес системи.

ЗАГАЛЬНІ ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ

У кваліфікаційній роботі бакалавра вирішено актуальну науково-технічну проблему проєктування, розробки та програмно-апаратної інтеграції сучасної адресно-цифрової системи безпеки для приватного житлового будинку. На основі опрацьованого матеріалу, інженерних розрахунків та програмних симуляцій отримано наступні висновки:

– за результатами аналізу архітектурно-планувального рішення об’єкта було детально вивчено геометрію будинку та змодельовано потенційні вектори загроз. Встановлено, що найбільш вразливими зонами є віконні та дверні проєми й зона основного входу. Відповідно до цього було розроблено стратегію ешелонованого захисту, яка поєднує давачі контролю периметра з давачами об’ємного виявлення (руху) всередині приміщень.

– на основі порівняльного аналізу сучасних засобів безпеки обґрунтовано, що для захисту приватного будинку найбільш доцільним є використання адресно-цифрового шинного протоколу на базі Ajax Fibra. Цей підхід дозволяє поєднати надійність фізичного кабельного з’єднання із високою інформативністю радіоканальних систем, забезпечуючи при цьому індивідуальну ідентифікацію кожного пристрою в мережі.

– у ході інженерного проєктування було розраховано оптимальну топологію кабельної мережі ліній Fibra. Застосування комбінації топологій «Промінь» для віддалених точок та «Кільце» для критично важливих зон дозволило досягти апаратного дублювання ліній. Проведені перевірочні розрахунки падіння напруги за максимального пікового навантаження підтвердили, що рівень напруги на кінцевих точках ліній не падає нижче критичної межі у 10,5 В, що гарантує стабільність живлення системи.

– реалізовано програмно-апаратну інтеграцію централі Hub Hybrid із периферійними засобами виявлення. Застосування спеціалізованого програмного забезпечення дозволяє автоматично сканувати цифрові шини, ідентифіковувати апаратні ID пристроїв й здійснювати логічне структурування

за віртуальними охоронними зонами, що спрощує адміністрування та підвищує точність локалізації тривог.

– розроблено програмні алгоритми верхнього рівня на мові Python. Створено симулятор сканування шин для верифікації карти об’єкта, а також серверний обробник подій за міжнародним стандартом SIA-DC09 (TCP/IP). Це підтверджує повну програмну сумісність спроєктованої системи з пультами централізованого спостереження та сторонніми сервісами автоматизації, забезпечуючи необхідну швидкість передачі сповіщень про тривогу.

Для підвищення ефективності, довговічності та відмовостійкості розробленої системи безпеки під час її практичної експлуатації рекомендується:

– кабельна інфраструктура: під час фізичного монтажу ліній Fibra використовувати виключно мідний чотирижильний кабель, оскільки він має високий опір і не спотворює результат розрахунків падіння напруги; сигнальні кабелі необхідно прокладати на відстані не менше 0,2 м від силових ліній електропередач;

– резервування живлення: здійснювати планову перевірку та тестування ємності встановленого у централь свинцево-кислотного акумулятора 12 В (щонайменше один раз на шість місяців) з метою гарантування нормативних 60 годин автономної роботи системи у разі знеструмлення об’єкта;

– інтеграція з пультами централізованого спостереження: попри наявність, для користувача, зручного мобільного застосунку рекомендовано підключати (протокол SIA-DC09) таку систему до ліцензованого пульта професійної охорони;

– канали зв’язку: доцільно використовувати мультислотовий режим передачі даних, що унеможливить глушіння або формування технічних збоїв.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ДСТУ EN 50131-1:2014. Системи тривожної сигналізації. Системи охоронної сигналізації. Частина 1. Загальні вимоги (EN 50131-1:2006, EN 50131-1:2006/A1:2009, EN 50131-1:2006/IS2:2010, IDT). [Чинний від 2016-01-01]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2015. 70 с.

2. ДСТУ CLC/TS 50131-7:2014. Системи тривожної сигналізації. Системи охоронної сигналізації. Частина 7. Правила застосування (CLC/TS 50131-7:2010, IDT). [Чинний від 2016-01-01]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2015. 58 с.

3. ДСТУ EN 50131-2-2:2019. Системи тривожної сигналізації. Системи охоронної сигналізації. Частина 2-2. Сповіщувачі охоронні пасивні інфрачервоні (EN 50131-2-2:2017, IDT). [Чинний від 2019-06-13]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2019. 36 с.

4. ДСТУ EN 50131-2-4:2022, Системи тривожної сигналізації. Системи охоронної сигналізації. Частина 2-4. Вимоги до комбінованих пасивних інфрачервоних та мікрохвильових сповіщувачів (EN 50131-2-4:2020, IDT). [Чинний від 2022-12-28]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2022. 40 с.

5. ДСТУ EN 50131-3:2014. Системи тривожної сигналізації. Системи охоронної сигналізації. Частина 3. Прилади приймально-контрольні (EN 50131-3:2009, IDT). [Чинний від 2014-12-30]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2014. 40 с.

6. ДСТУ EN 50136-1:2014. Системи тривожної сигналізації. Системи передавання тривожних сповіщень та устаткування. Частина 1. Загальні вимоги до систем передавання тривожних сповіщень (EN 50136-1:2012/A1:2018, IDT). Зміна № 1:2019. [Чинний від 2019-06-13]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2014. 56 с.

7. ДСТУ EN 54-1:2022. Системи виявлення пожежі та пожежної сигналізації. Частина 1: Вступ (EN 54-1:2021, IDT). [Чинний від 2022-12-28]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2022. 38 с.

8. ДСТУ IEC 60529:2019. Ступені захисту, забезпечувані корпусами (IP-код) (IEC 60529:2013, IDT). [Чинний від 2019-12-23]. Вид. офіц. Київ : ДП «УкрНДНЦ», 2019. 38 с.

9. ДБН В.2.5-56:2014. Системи протипожежного захисту. Зі Зміною № 1. [Чинний від 2014-11-13]. Вид. офіц. Київ : ДП «Укрархбудінформ», 2014. 211 с.

10. Дерев'янко О. А., Антошкін О. А., Бондаренко С. М., Христич В. В. Системи пожежної та охоронної сигналізації. URL: https://surl.li/gxygay (дата звернення: 10.01.2026).

11. Що таке пультова охорона та як вона працює. URL: https://surl.li/jawmgx (дата звернення: 10.01.2026).

12. Система охоронної сигналізації для приватного будинку. Рекомендації щодо вибору. URL: https://surl.li/jbmdpb (дата звернення: 20.01.2026).

13. FIBRA – AJAX. URL: https://surl.li/spiqgo (дата звернення: 20.01.2026).

14. Комплект бездротової охоронної системи Tiras Orion NOVA X. URL: https://surl.li/tmddqv (дата звернення: 20.01.2026).

15. Система сигналізації Satel – з чого вона складається і яку модель вибрати? URL: https://surl.li/xozybo (дата звернення: 20.01.2026).

16. Бездротова охоронна система AX PRO від Hikvision. URL: https://surl.li/kumgyq (дата звернення: 20.01.2026).

17. Intruder Verification as a Service. URL: https://surl.li/cveirl (дата звернення: 20.01.2026).

18. What is Over-the-Air (OTA) in IoT? URL: https://surl.li/hboxan (дата звернення: 20.01.2026).

19. Грабовецький Б. Є. Методи експертних оцінок: теорія, методологія, напрямки використання. URL: https://surl.li/xfyxir (дата звернення: 20.01.2026).

20. Дротовий модуль для інтеграції сторонніх пристроїв у систему Ajax Superior MultiTransmitter Fibra. URL: https://surl.li/ohlmcv (дата звернення: 20.01.2026).

21. Датчики охоронної системи – робимо правильний вибір. URL: https://surl.li/vglqnu (дата звернення: 20.01.2026).

22. Види охоронних датчиків у системі безпеки: як вони працюють? URL: https://surl.lu/ekjbwb (дата звернення: 20.01.2026).

23. Огляд сучасних датчиків сигналізації: безпека вашого об’єкта. URL: https://surl.li/eyicmb (дата звернення: 20.01.2026).

24. Бездротовий ІЧ датчик руху з додатковим мікрохвильовим сенсором K-діапазону MotionProtect Plus Jeweller. URL: https://surl.li/axyvvl (дата звернення: 20.01.2026).

25 Бездротовий датчик відчинення з герконом DoorProtect Jeweller. URL: https://ajax.systems/ua/products/doorprotect/ (дата звернення: 20.01.2026).

26. Бездротовий датчик розбиття скла з мікрофоном GlassProtect Jeweller. URL: https://ajax.systems/ua/products/glassprotect/ (дата звернення: 20.01.2026).

27. Дротовий ІЧ датчик руху Superior MotionProtect Fibra. URL: https://surli.cc/bzcwni (дата звернення: 20.01.2026).

28. Real Time Streaming Protocol (RTSP). URL: https://surl.li/dvyoxi (дата звернення: 20.01.2026).

29. What Are Peer-to-Peer (P2P) Networks? URL: https://surl.li/vymonu (дата звернення: 20.01.2026).

30. SIA DC-09. URL: https://fortsense.net/blog/glossary/sia-dc09 (дата звернення: 20.01.2026).

31. Ademco® Contact ID Protocol. URL: https://surl.li/bqgwth (дата звернення: 20.01.2026).

32. Терлецький Т. В., Кайдик О. Л. Кваліфікаційна робота : методичні вказівки до виконання кваліфікаційної роботи бакалавра для здобувачів першого (бакалаврського) рівня вищої освіти освітньої програми «Інформаційні системи та технології охорони і безпеки» галузі знань 12 Інформаційні технології спеціальності 126 Інформаційні системи та технології денної та заочної форм навчання. Луцьк: ЛНТУ, 2025. 53 с.