

ТаВищий навчальний заклад
«Університет економіки та права «КРОК»
Фаховий коледж

Циклова комісія з інформаційних технологій

**Кваліфікаційна робота фахового молодшого
бакалавра**

на тему Розробка охоронної системи «розумного будинку».

Виконав _____
(Підпис)

Попко Тимур Олександрович
(прізвище, ім'я, по батькові)

Науковий керівник
Чернозубкін Ігор Олександрови
(прізвище, ім'я, по батькові)

(Резолюція «До захисту»)

Попередній захист:

(Висновок: “До захисту в екзаменаційній комісії”)

Голова циклової комісії

(Підпис)

(Прізвище, ініціали)

(Дата)

Київ - 2025

ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
УНІВЕРСИТЕТ ЕКОНОМІКИ ТА ПРАВА «КРОК»
Фаховий коледж

Циклова комісія з інформаційних технологій

Спеціальність 121 інженерія програмного забезпечення

ЗАТВЕРДЖУЮ:

Голова циклової комісії _____ Леонід УВАРОВ
(підпис)

«_____» _____ 2025 року

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Здобувач освіти Попко Тимур Олександрович

1. Тема роботи Розробка охоронної системи «розумного будинку»
затверджена наказом по університету від «___» _____ 202__ р. № _____
2. Термін здачі закінченої роботи «30» травня 2025 року
3. Вихідні дані до роботи:
 - 1) цільова аудиторія – для кого призначена система (власники квартир, приватних будинків, котеджів тощо), особливості житла (розмір, кількість кімнат, розташування), найбільш важливі функції безпеки (захист від проникнення, пожежі, затоплення, витік газу тощо);
 - 2) функціональність – функції, які повинна виконувати система:
типи датчиків, що будуть використовуватися (руху, відкриття дверей/вікон, диму, газу, води тощо);
способи оповіщення (SMS, push-сповіщення, дзвінок на телефон, звукова сигналізація);
інструменти для керування системою (зі смартфона, комп'ютера, панелі керування);
можливі сценарії автоматизації (наприклад, включення світла при виявленні руху, автоматичне перекриття води при витокі тощо);
можливості інтеграції з іншими системами «розумного будинку» (освітлення, опалення, відеоспостереження);
заходи безпеки для захисту системи (шифрування даних, захист від несанкціонованого доступу);
 - 3) технічні вимоги – технології та протоколи зв'язку (Wi-Fi, Zigbee, Z-Wave, Bluetooth), обладнання для розгортання системи (центральный контролер, датчики, виконавчі пристрої), вимоги до програмного забезпечення (інтерфейс користувача, база даних, сервер), платформи, що підтримуються (Android, iOS, Windows);
 - 4) кращі практики та існуючі розробки в області охоронних систем для «розумного будинку».

4. Зміст пояснювальної записки

- 1) Розділ 1 Теоретична частина. Аналіз кращих практик та існуючих розробок в області охоронних систем для «розумного будинку», обґрунтування функціональності та технічних вимог щодо охоронної системи.
- 2) Розділ 2 Проєктування та розробка. Визначення структури системи (централізована, децентралізована, гібридна), компонентів та способів їх взаємодії, вибір мови програмування та інструментів розробки, рішення щодо реалізації інтерфейсу користувача, зберігання та обробки даних, технічних засобів (датчики, виконавчі пристрої, електроживлення), монтажу та встановлення обладнання.
- 3) Розділ 3 Експериментальна частина. Тестування системи (функціональне тестування, тестування безпеки, тестування продуктивності) та критерії його успішного проходження, оцінка ефективності системи (надійність, час реакції, зручність використання тощо). Інструкції користувачам (адміністратору і програмістам – опис архітектури системи, принципів роботи, алгоритмів, специфікації на обладнання та програмне забезпечення, інструкції з встановлення та налаштування системи, користувачам – пояснення щодо використання системи, налаштування параметрів, вирішення проблем).

5. Перелік графічного матеріалу:

Скріншоти існуючих рішень

Скріншоти інтерфейсу продукту

Схеми і таблиці щодо візуалізації аналізу

Блок-схеми алгоритмів

Діаграми щодо проєктування продукту (наприклад, потоків даних, переходів станів, сутність-зв'язок, UML, бази даних тощо)

Дата видачі завдання «12» лютого 2025 року

Науковий керівник

(підпис)

Ігор ЧЕРНОЗУБКІН

Завдання прийняв до виконання

(підпис)

Тимур ПОПКО

РЕФЕРАТ

Пояснювальна записка: 55 сторінок, 5 рисунків, 4 таблиць, 4 додатків, 17 джерел.

Об'єкт дослідження – охоронна система в інфраструктурі «розумного будинку»

Мета роботи – розробка інтегрованої охоронної системи, що гарантує виявлення загроз, сповіщення користувача та взаємодію з іншими компонентами розумного будинку. У кваліфікаційній роботі проаналізовано сучасні системи охорони, вивчено принципи їх функціонування та вимоги до захисту житлових приміщень

Результати розробки У результаті виконання дипломної роботи було реалізовано вебзастосунок, що моделює роботу охоронної системи для «розумного будинку». Вебінтерфейс створено з використанням стандартних технологій фронтенд-розробки — HTML, CSS і JavaScript, без залучення сторонніх бібліотек чи серверної частини.

Ключові слова: розумний будинок, охоронна система, інтерфейс користувача, JavaScript, вебзастосунок, датчики, візуалізація подій,

ABSTRACT

Explanatory Note: 55 pages, 5 drawings, 4 tables, 4 appendices, 17 sources.

Object of the research – a security system within the infrastructure of a "smart home".

Purpose of the work – the development of an integrated security system that ensures threat detection, user notification, and interaction with other components of the smart home.

The qualification work analyzes modern security systems, examines the principles of their operation, and the requirements for residential protection.

Development results:

As a result of the thesis work, a web application was implemented to simulate the operation of a security system for a smart home. The web interface was developed using standard frontend technologies — HTML, CSS, and JavaScript — without the use of third-party libraries or a backend.

Keywords: smart home, security system, user interface, JavaScript, web application, sensors, event visualization.

ЗМІСТ

СКРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ	7
ВСТУП	8
РОЗДІЛ 1. ТЕОРЕТИЧНА ЧАСТИНА	10
1.1 Аналіз сучасних охоронних систем для «розумного будинку»	10
1.2. Класифікація охоронних систем (за типами, призначенням, архітектурою)	12
1.3. Огляд існуючих рішень на ринку	14
1.4. Порівняльний аналіз функціональності, технічних характеристик та ефективності.....	16
1.5. Обґрунтування необхідності створення нової охоронної системи ..	19
1.6. Визначення функціональних та технічних вимог до системи	20
РОЗДІЛ 2. ПРОЄКТУВАННЯ ТА РОЗРОБКА СИСТЕМИ	23
2.1. Обґрунтування архітектури системи (централізована, децентралізована, гібридна).....	23
2.2. Структура системи: основні компоненти та їх взаємодія	24
2.3. Вибір мови програмування, фреймворків та інструментів розробки	26
2.4. Розробка інтерфейсу користувача	28
2.5. Організація зберігання та обробки даних	29
2.6. Вибір технічних засобів (датчики, виконавчі пристрої, блоки живлення тощо).....	29
2.7. Розробка схеми монтажу та встановлення обладнання	30
РОЗДІЛ 3. ЕКСПЕРИМЕНТАЛЬНА ЧАСТИНА	35
3.1. Методика тестування охоронної системи.....	35
3.2. Функціональне тестування	37
3.3. Тестування безпеки та стійкості до збоїв	37
3.4. Тестування продуктивності (швидкодія, реакція на події).....	38
3.5. Аналіз результатів тестування, визначення критеріїв ефективності	40
3.6. Інструкція для адміністратора та технічних спеціалістів	41

3.7. Інструкція для кінцевих користувачів	41
ВИСНОВКИ	45
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	48
ДОДАТКИ	50
Додатки А. Скріншоти сайту	50
Додаток Б. Фрагменти коду та конфігураційні файли.....	52
Додаток В. Фрагменти коду та конфігураційні файли	54
Додаток Г. Фрагменти коду та конфігураційні файли.....	55
Додаток Д. Фрагменти коду та конфігураційні файли	Ошибка! Закладка не определена.

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

ЦП — Центральний процесор

ПЗ — Програмне забезпечення

ОС — Операційна система

ДСТУ — Державний стандарт України

ДП — Датчик присутності

ВП — Виконавчий пристрій

Wi-Fi — Wireless Fidelity (бездротова мережа)

UML — Unified Modeling Language (Уніфікована мова моделювання)

TCP/IP — Transmission Control Protocol/Internet Protocol (протоколи передачі даних)

SMS — Short Message Service (служба коротких повідомлень)

RFID — Radio Frequency Identification (радіочастотна ідентифікація)

IP — Internet Protocol (інтернет-протокол)

IoT — Internet of Things (Інтернет речей)

GUI — Graphical User Interface (графічний інтерфейс користувача)

API — Application Programming Interface (інтерфейс програмування додатків)

ВСТУП

Актуальність завдання. У сучасних умовах цифровізації та розвитку технологій автоматизації житла все більшого значення набуває безпека приватного простору. Концепція «розумного будинку» передбачає використання великої кількості пристроїв, підключених до єдиної системи управління, що створює нові можливості, але й нові загрози. Одним з основних елементів безпеки є охоронна система, здатна ефективно виявляти порушення, реагувати на загрози, зберігати дані та взаємодіяти з іншими компонентами автоматизованого середовища. Більшість існуючих рішень або недостатньо гнучкі, або вимагають складного встановлення, мають обмежену сумісність з іншими системами, а іноді — не відповідають базовим вимогам кібербезпеки [2], [4]. Це обумовлює потребу у створенні адаптивної, масштабованої, безпечної та зручної у використанні охоронної системи для «розумного будинку».

Мета роботи. розробка інтегрованої охоронної системи, що гарантує виявлення загроз, сповіщення користувача та взаємодію з іншими компонентами розумного будинку. У кваліфікаційній роботі проаналізовано сучасні системи охорони, вивчено принципи їх функціонування та вимоги до захисту житлових приміщень

Завдання роботи

1. Провести аналіз сучасних охоронних систем, визначити їхні переваги та недоліки.
2. Сформулювати функціональні та технічні вимоги до охоронної системи.
3. Обрати оптимальну архітектуру та структурну модель системи.
4. Визначити склад програмного та апаратного забезпечення.
5. Розробити прототип інтерфейсу користувача.
6. Реалізувати основні функціональні компоненти системи.
7. Провести тестування працездатності, безпеки та продуктивності системи.
8. Оцінити ефективність реалізованої системи та підготувати інструкції для користувачів і технічного персоналу.

Об’єкт дослідження. Інтелектуальні охоронні системи, призначені для забезпечення безпеки у «розумному будинку».

Предмет дослідження. Архітектура, функціональні компоненти, алгоритми та технічні засоби реалізації охоронної системи, що інтегрується в середовище автоматизованого житлового простору.

Методи дослідження. У процесі дослідження було застосовано комплекс наукових методів, зокрема аналіз наукових джерел та технічної документації для вивчення існуючих підходів і рішень. Системний аналіз дозволив визначити оптимальну архітектуру проектованої системи, а моделювання функціональної структури дало змогу відтворити ключові процеси в теоретичній формі. На етапі експериментальної реалізації було розроблено робочий прототип системи, функціональність якого підтверджено через тестування за ключовими показниками ефективності. Також було проведено порівняльний аналіз отриманих результатів з аналогічними розробками в цій галузі.

Практичне значення одержаних результатів. Результатом виконаної роботи є функціональний прототип охоронної системи, який може бути використаний як основа для впровадження у реальних умовах — у приватних домогосподарствах, квартирах або малих офісах. Отримані результати мають прикладне значення для розробників систем автоматизації та можуть бути адаптовані для інтеграції в комерційні або відкриті програмні продукти.

Структура роботи. Робота складається з вступної частини, трьох розділів, висновків та переліку використаних джерел.

РОЗДІЛ 1. ТЕОРЕТИЧНА ЧАСТИНА

1.1 Аналіз сучасних охоронних систем для «розумного будинку»

Сучасні охоронні системи є важливою складовою інфраструктури «розумного будинку», забезпечуючи безпеку житлових та комерційних приміщень шляхом інтеграції апаратного забезпечення, програмного забезпечення та засобів комунікації. Основна мета таких систем — своєчасне виявлення загроз (проникнення, пожежа, витік газу тощо) та відповідне реагування.

Основні функції охоронних систем:

- Детектування руху всередині та навколо будівлі.
- Контроль доступу (ключ-карти, біометрія, коди).
- Сповіщення про тривогу (смс, push-сповіщення, дзвінок).
- Відеоспостереження в реальному часі.
- Інтеграція з іншими системами «розумного будинку» (освітлення, замки, сирени).
- Автоматичне реагування (увімкнення освітлення, блокування дверей, виклик охорони).

Класифікація охоронних систем:

- **За типом зв'язку:** дротові, бездротові, комбіновані.
- **За способом управління:** локальні (автономні), віддалені (через мобільні застосунки, хмарні сервіси).
- **За масштабом:** для квартири, приватного будинку, багатоквартирного будинку, офісу.
- **За архітектурою:** централізовані, децентралізовані, гібридні.
- **За призначенням:** побутові, комерційні, промислові.

Таблиця 1 – Порівняльна характеристика охоронних систем за функціональністю

№	Система	Основні функції	Переваги	Недоліки
1	Ajax Systems (Україна)	Датчики руху, диму, води, камери, мобільний застосунок	Сучасний дизайн, автономність, проста інсталяція	Висока ціна комплектів
2	Xiaomi Smart Home	Інтеграція з іншими пристроями, датчики, автоматизація	Доступна ціна, підтримка голосових асистентів	Менше охоронних функцій
3	Ring Alarm (Amazon)	Відеодзвінки, охоронна сигналізація, хмарне збереження	Хмарне відеоспостереження, інтеграція з Alexa	Потрібен постійний доступ до Інтернету
4	Hikvision / Dahua	Професійні системи відеоспостереження	Висока якість відео, розширені функції	Складність налаштування

Опис:

У таблиці наведено порівняння чотирьох популярних охоронних систем — *Ajax Systems*, *Xiaomi Smart Home*, *Ring Alarm* та *Hikvision / Dahua* — за основними функціональними характеристиками, перевагами та недоліками. Зокрема, оцінено наявність базових охоронних функцій, можливості автоматизації та відеоспостереження, доступність мобільного керування, рівень інтеграції з іншими пристроями та технологіями. Також наведено суб'єктивну оцінку зручності інсталяції, цінової категорії та технічної складності налаштування.

Основні тенденції розвитку:

- **Інтеграція з AI:** автоматичне розпізнавання облич, аналіз поведінки, виявлення незвичних ситуацій.

- **Хмарні технології:** централізоване зберігання даних, доступ з будь-якої точки світу.
- **Мобільні застосунки:** повноцінне управління системою з телефона.
- **IoT-інтеграція:** взаємодія з іншими пристроями екосистеми (освітлення, термостати, замки).
- **Кібербезпека:** шифрування даних, двофакторна аутентифікація, захист від підміни сигналів.

1.2. Класифікація охоронних систем (за типами, призначенням, архітектурою)

Класифікація охоронних систем дозволяє систематизувати їх за різними характеристиками. Це полегшує вибір системи відповідно до вимог безпеки, технічних умов та середовища експлуатації.



Рисунок 1 – Класифікація охоронних систем

За типом сигналізації

1. **Охоронна сигналізація** – призначена для виявлення несанкціонованого проникнення в приміщення. Включає датчики відкриття дверей, руху, розбиття скла тощо. [2]

2. **Пожежна сигналізація** – реагує на появу диму, підвищення температури, відкритий вогонь. Використовується для запобігання пожежам та оперативного оповіщення. [4]
3. **Газова та протипотопна сигналізація** – фіксує витік газу (природного або чадного) та витіки води, забезпечуючи превентивне інформування. [6]
4. **Тривожна сигналізація (панік-кнопка)** – активується вручну у разі загрози життю чи здоров'ю, зазвичай підключається до охоронного пункту.

За способом встановлення

- **Дротові системи** – усі елементи з'єднані кабелями. Характеризуються високою стабільністю, проте вимагають складного монтажу.
- **Бездротові системи** – передача сигналів здійснюється за допомогою радіозв'язку, Wi-Fi або інших бездротових протоколів. Монтаж простіший, проте можливі перешкоди або втрати сигналу.
- **Комбіновані системи** – поєднують дротові та бездротові компоненти, забезпечуючи гнучкість в реалізації та масштабованість.

За способом керування

- **Автономні системи** – функціонують незалежно, без постійного зв'язку з користувачем або охоронною службою. Придатні для базового захисту.
- **Інтерактивні системи** – дозволяють дистанційно керувати налаштуваннями, отримувати повідомлення та контролювати об'єкт через мобільні застосунки чи веб-інтерфейси.
- **Системи з підключенням до пульта централізованого спостереження (ПЦС)** – забезпечують автоматичну передачу сигналів тривоги до охоронної компанії.

За архітектурою

- **Централізовані системи** – усі дані обробляються центральним контролером. Перевагами є спрощене керування та моніторинг, недоліком – вразливість до відмови центрального елемента.

- **Децентралізовані системи** – кожен елемент функціонує автономно або обмінюється даними безпосередньо з іншими компонентами. Такі системи більш стійкі до збоїв, проте складніші у налаштуванні.
- **Гібридні системи** – поєднують елементи централізованої та децентралізованої архітектури. Забезпечують оптимальний баланс між надійністю та зручністю в управлінні.

За призначенням

- **Побутові системи** – застосовуються у квартирах, приватних будинках. Орієнтовані на простоту використання, естетичний дизайн та базовий рівень захисту.
- **Комерційні системи** – використовуються в офісах, магазинах, складах. Вимагають більшої кількості функцій, включаючи контроль доступу, відеоспостереження та інтеграцію з IT-інфраструктурою.
- **Промислові системи** – призначені для захисту великих об'єктів, критичної інфраструктури, заводів. Мають високий рівень захищеності, масштабованість та стійкість до впливу зовнішніх чинників.

1.3. Огляд існуючих рішень на ринку

На сучасному ринку охоронних систем для «розумного будинку» представлено велику кількість готових рішень, які відрізняються функціональністю, технічними характеристиками, способом встановлення та ціновою політикою. У цьому розділі розглянемо найпопулярніші серед користувачів системи, які охоплюють як побутовий, так і комерційний сегмент.

Ajax Systems – український виробник професійних охоронних систем, що активно розвиває міжнародний ринок. Система побудована на бездротових технологіях, має привабливий сучасний дизайн та гнучкий набір модулів. Користувачі можуть керувати системою через зручний мобільний застосунок, налаштовувати сценарії, підключати відеокамери та отримувати повідомлення в режимі реального часу. Підтримується підключення до пульта охоронної компанії. Основними перевагами є висока надійність, автономність пристроїв та

простота встановлення. До недоліків можна віднести високу вартість системи в порівнянні з бюджетними аналогами.

Xiaomi Smart Home – частина великої екосистеми розумного дому від компанії Xiaomi. Включає широкий набір датчиків руху, відкриття дверей/вікон, диму, витоку води тощо. Керування здійснюється через мобільний застосунок Mi Home. Перевагами є доступна ціна, гнучкість автоматизації та інтеграція з іншими пристроями Xiaomi. Однак деякі користувачі стикаються з обмеженою локалізацією, залежністю від хмарних сервісів компанії та нестабільною роботою в умовах слабого інтернет-з'єднання.

Ring Alarm – система охоронної сигналізації, створена компанією Ring, що входить до складу Amazon. Основний акцент зроблено на поєднанні відеоспостереження та охоронної функціональності. Система підтримує інтеграцію з голосовим помічником Alexa, а також дозволяє зберігати відео в хмарі. Користувач отримує гнучкий контроль за допомогою мобільного додатку. Недоліком є необхідність підписки для використання деяких функцій, а також слабка локалізація для українського ринку.

Hikvision і Dahua – провідні китайські виробники систем відеоспостереження, які також пропонують охоронні рішення, включаючи сигналізацію, контроль доступу та інтеграцію з відеокамерами. Ці системи вирізняються високою якістю відео та можливістю використання аналітики (виявлення облич, перетин лінії тощо). Основні переваги – масштабованість, широкий вибір компонентів, сумісність з багатьма стандартами. Серед недоліків – складність самостійного налаштування, потреба у професійному встановленні та технічній підтримці.

Securitas, Tyco, Honeywell – міжнародні компанії, що пропонують комплексні охоронні рішення для бізнесу та великих об'єктів. Вони забезпечують інтеграцію охоронних систем із системами контролю доступу, пожежної безпеки та відеоспостереження. Пропонуються модульні рішення, що масштабуються відповідно до потреб об'єкта. Основні переваги – надійність,

сертифікація для комерційного використання, повний технічний супровід. До недоліків можна віднести високу вартість впровадження та обслуговування, а також надлишкову складність для побутового використання.

У цілому, вибір охоронної системи залежить від бюджету, умов експлуатації, потреб користувача та вимог до інтеграції з іншими системами «розумного будинку». На сьогоднішній день найбільшою популярністю серед приватних користувачів користуються бездротові рішення з мобільним керуванням та підтримкою автоматизації.

Наприклад, система **Ajax Systems** розроблена в Україні та має офіційну сторінку: <https://ajax.systems/ua/>

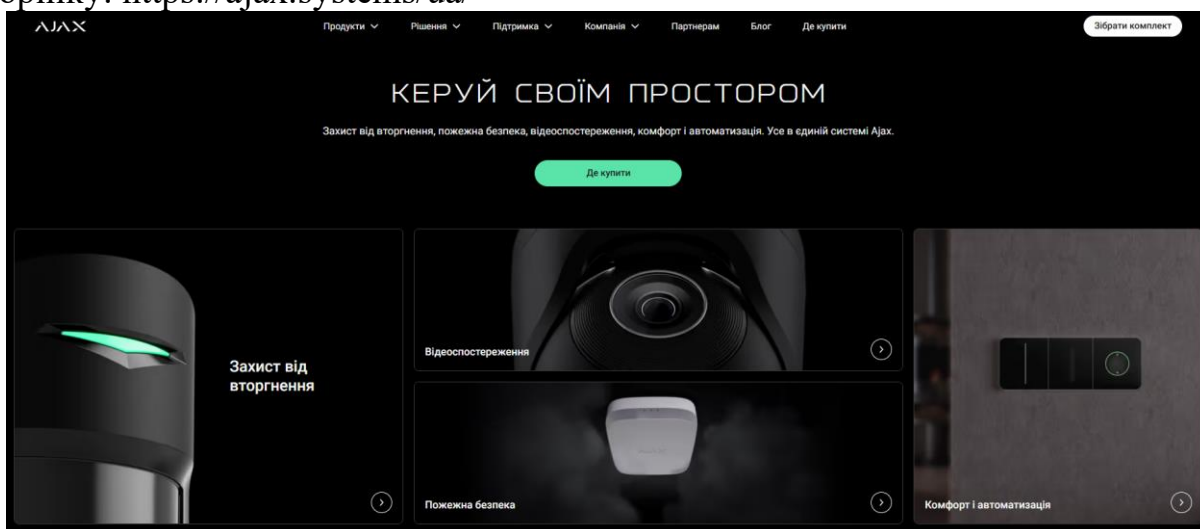


Рисунок 2 – Вебсторінка з описом охоронної системи Ajax Systems

1.4. Порівняльний аналіз функціональності, технічних характеристик та ефективності

З метою вибору оптимального рішення для побудови охоронної системи в умовах «розумного будинку» доцільно провести порівняльний аналіз найбільш популярних систем, які були розглянуті у попередньому розділі. Аналіз базується на ключових критеріях, таких як функціональність, технічні характеристики, ефективність, простота встановлення, вартість і можливість інтеграції з іншими елементами розумного дому.

Критерії аналізу:

- Наявність базових охоронних функцій (датчики руху, відкриття, тривожна сигналізація)
- Підтримка відеоспостереження

- Можливість дистанційного керування
- Тип зв'язку (дротовий/бездротовий)
- Простота встановлення
- Автономність (живлення від батарей, тривалість роботи)
- Інтеграція з іншими системами
- Можливість підключення до ПЦС
- Цінова категорія

Таблиця 2 - Порівняння характеристик охоронних систем за ключовими критеріями

№	Критерій	Ajax Systems	Xiaomi Smart Home	Ring Alarm	Hikvision / Dahua	Honeywell / Tyco
1	Базові охоронні функції	Так	Так	Так	Так	Так
2	Відеоспостереження	Частково (через інтеграцію)	Частково	Так	Так	Так
3	Дистанційне керування	Так	Так	Так	Частково	Частково
4	Тип зв'язку	Бездротовий	Бездротовий	Бездротовий	Дротовий/гібридний	Дротовий
5	Простота встановлення	Висока	Висока	Висока	Низька	Низька
6	Автономність	До 5–7 років	До 1–2 років	До 2 років	Залежить від моделі	Залежить від моделі

№	Критерій	Ajax Systems	Xiaomi Smart Home	Ring Alarm	Hikvision / Dahua	Honeywell / Tyco
7	Інтеграція з іншими системами	Середня	Висока	Висока (Amazon Alexa)	Середня	Висока
8	Підключення до ПЦС	Так	Ні	Обмежено	Так	Так
9	Цінова категорія	Висока	Низька	Середня	Середня/висока	Висока

- **Ajax Systems** — найбільш збалансоване рішення для користувачів, яким потрібна професійна охоронна система з високим рівнем надійності та бездротовою архітектурою. Висока ціна компенсується якістю, простотою встановлення та широкими можливостями керування.
- **Xiaomi Smart Home** — підходить для базового захисту в рамках широкої екосистеми пристроїв розумного дому. Це доступне рішення для користувачів, які цінують автоматизацію, але не мають критичних вимог до безпеки.
- **Ring Alarm** — ефективне рішення для тих, хто вже використовує екосистему Amazon. Забезпечує хорошу інтеграцію з голосовими помічниками та хмарними сервісами, але частина функцій є платною.
- **Hikvision / Dahua** — найкраще підходять для великих об'єктів з розвиненою системою відеоспостереження. Проте вимагають професійного налаштування і монтажу.
- **Honeywell / Tyco** — ідеальні для бізнесу та промисловості. Відзначаються високою масштабованістю та стабільністю, проте значно перевищують потреби і бюджет пересічного побутового користувача.

Загалом, вибір системи має базуватись на співвідношенні функціональності, вартості, простоти встановлення та вимог користувача до рівня безпеки.

1.5. Обґрунтування необхідності створення нової охоронної системи

Попри наявність великої кількості охоронних систем на ринку, аналіз існуючих рішень свідчить про те, що більшість із них або надто обмежені у функціональності, або орієнтовані на корпоративний сегмент із відповідними фінансовими та технічними вимогами. Масові системи, як-от **Xiaomi Smart Home**, забезпечують базову автоматизацію, але часто не мають достатнього рівня адаптації до складніших сценаріїв безпеки. Навпаки, професійні рішення типу **Ajax**, **Hikvision** чи **Honeywell** пропонують високу якість, але мають закриту архітектуру, потребують підписки на хмарні сервіси, а також є складними для самостійного встановлення. Крім того, існують такі актуальні виклики, на які багато рішень не дають повноцінної відповіді:

- **Закритість до інтеграцій** – складність додавання нових пристроїв або сторонніх платформ.
- **Неврахованість локальних потреб** – відсутність повноцінної підтримки української мови, регіональних стандартів і технічного обслуговування.
- **Недостатня гнучкість** – обмеження у створенні користувацьких сценаріїв (наприклад, автоматичне блокування дверей лише у певні години або при виході всіх мешканців).
- **Повна залежність від хмари** – відсутність офлайн-режиму з локальним журналюванням і логікою.

Звісно, дана розробка не претендує на повноцінну заміну промислових рішень або комерційний запуск. Проте вона демонструє підхід до створення **відкритої, мінімалістичної та локалізованої системи**, яка може стати прототипом або навчальним прикладом для подальшої розробки.

У зв'язку з цим виникає необхідність створення нової охоронної системи, яка поєднуватиме такі якості:

- **Використанні стандартних вебтехнологій (HTML, CSS, JavaScript)**, що забезпечують простоту розгортання без серверної частини

- **Можливості автономної роботи**, коли інтернет-з'єднання недоступне;
- **Гнучкій моделі логіки**, яку користувач може змінити без спеціалізованого програмного забезпечення.
- **Орієнтації на українського користувача** — від мови інтерфейсу до потенційної сумісності з локальними системами охорони.

Таким чином, ця система не конкурує напряду з великими брендами, але покликана закрити нішу між простими комерційними рішеннями та складними корпоративними платформами, запропонувавши баланс між доступністю, адаптивністю та відкритістю.

1.6. Визначення функціональних та технічних вимог до системи

На основі аналізу існуючих рішень, а також виявлених недоліків і сучасних потреб користувачів, до розроблюваної охоронної системи для «розумного будинку» висуваються такі функціональні та технічні вимоги.

Функціональні вимоги:

1. Виявлення загроз:

- Фіксація несанкціонованого проникнення (датчики руху, відкриття дверей/вікон).
- Виявлення пожежі (датчики диму та температури).
- Виявлення витоку води або газу (відповідні сенсори).

2. Сповіщення про події:

- Надсилання сповіщень на смартфон користувача (push-повідомлення, SMS, email).
- Активація звукової або світлової сирени при тривозі.
- Можливість виклику служби охорони або поліції.

3. Керування системою:

- Мобільний застосунок для керування (вмикання/вимикання, зміна налаштувань).
- Веб-інтерфейс для розширеного керування та моніторингу.
- Можливість дистанційного або локального керування.

4. Інтеграція:

- Інтеграція з іншими елементами системи «розумного будинку» (освітлення, замки, камери тощо).
- Підтримка голосових помічників (опційно).

5. Гнучкість та автоматизація:

- Налаштування сценаріїв поведінки (наприклад, «увімкнути охорону при виході з дому»).
- Підтримка зонального контролю (охорона окремих кімнат чи приміщень).
- Можливість додавання або видалення пристроїв без зміни всієї системи.

6. Журнал подій:

- Ведення логів подій із зазначенням часу, типу події та реакції системи.
- Збереження історії тривог та змін конфігурації.

Технічні вимоги:

1. Архітектура системи:

- Гібридна (центральний контролер з підтримкою локальної автономної роботи).
- Підтримка бездротових та дротових каналів зв'язку (Wi-Fi, Zigbee, Bluetooth, Ethernet, опційно GSM).

2. Надійність:

- Працездатність у разі зникнення електроживлення (автономне живлення – резервний акумулятор).
- Працездатність у разі втрати підключення до Інтернету (локальне зберігання логів, відкладене надсилання сповіщень).

3. Безпека:

- Шифрування даних (TLS, AES).
- Авторизація користувачів (двофакторна аутентифікація).

- Захист від саботажу (виявлення спроб глушіння, зламу корпусу тощо).

4. Продуктивність:

- Час реакції системи на подію не більше 2 секунд.
- Стабільна робота при одночасному підключенні не менше 20 пристроїв.

5. Мобільна підтримка:

- Додатки для Android та iOS.
- Офлайн-режим з обмеженим функціоналом у разі втрати мережі.

6. Масштабованість:

- Можливість розширення системи до 50+ пристроїв без потреби у заміні основного контролера.
- Гнучка настройка користувацьких профілів, сценаріїв та зон охорони.

7. Локалізація:

- Повна підтримка української мови.
- Можливість адаптації інтерфейсу під різні регіони (часовий пояс, формат дати/часу).

РОЗДІЛ 2. ПРОЄКТУВАННЯ ТА РОЗРОБКА СИСТЕМИ

2.1. Обґрунтування архітектури системи (централізована, децентралізована, гібридна)

При проектуванні охоронної системи для «розумного будинку» важливим кроком є вибір відповідної архітектури. Від цього залежать надійність, гнучкість, масштабованість, а також витрати на реалізацію та обслуговування.

Огляд типів архітектур:

- **Централізована архітектура** передбачає наявність одного центрального контролера, який відповідає за обробку всіх сигналів від сенсорів і пристроїв, а також за прийняття рішень. Такий підхід простий в реалізації, однак має суттєвий недолік — відмова центрального елементу призводить до повної недієздатності системи.
- **Децентралізована архітектура** базується на принципі розподілу функціональності між кількома автономними вузлами, які можуть самостійно реагувати на події. Це підвищує надійність, але ускладнює синхронізацію і керування, особливо при великій кількості пристроїв.
- **Гібридна архітектура** поєднує переваги обох підходів: центральний контролер здійснює координацію та глобальну логіку, але окремі елементи системи (наприклад, сенсори чи виконавчі пристрої) здатні працювати автономно у разі втрати зв'язку з центром.

Обраний підхід: гібридна архітектура

Для створення ефективної, надійної та масштабованої охоронної системи обрано **гібридну архітектуру**, що обґрунтовується наступними чинниками:

- **Надійність:** у випадку втрати зв'язку з центральним контролером (наприклад, через збої живлення або мережі), сенсори та виконавчі пристрої зберігають можливість реагування на критичні події (наприклад, тривожний сигнал при відкритті дверей).
- **Гнучкість:** можливість конфігурування локальних сценаріїв (наприклад, включення світла при спрацюванні датчика руху) без залучення центральної логіки.

- **Масштабованість:** спрощене додавання нових пристроїв і модулів без суттєвого навантаження на центральний блок.
- **Централізований моніторинг:** забезпечення зручного керування, збору логів і налаштування всієї системи через мобільний застосунок або веб-інтерфейс.
- **Підвищена безпека:** зменшення ризиків при спробах саботажу — відмова одного елемента не виводить з ладу всю систему.

Структурна схема архітектури системи:

- **Центральний контролер:** здійснює логіку, синхронізацію, збір даних, формування сценаріїв.
- **Пристрої першого рівня (датчики, камери):** збирають інформацію та можуть реагувати локально.
- **Пристрої другого рівня (реле, сирени, індикатори):** виконують команди у відповідь на події.
- **Інтерфейс керування (мобільний застосунок / веб-панель):** дозволяє користувачу моніторити систему, налаштовувати сценарії, переглядати події.
- **Модуль автономної роботи:** забезпечує локальну функціональність при відсутності мережевого зв'язку.

2.2. Структура системи: основні компоненти та їх взаємодія

Розроблена охоронна система для «розумного будинку» базується на гібридній архітектурі й включає низку апаратних і програмних компонентів, що взаємодіють між собою з метою забезпечення надійного контролю, сповіщення та реагування на загрози.

Основні компоненти системи

1. Центральний контролер (головний модуль)

- Призначення: обробка подій, координація роботи інших пристроїв, збереження журналів, реалізація логіки сценаріїв.

- Зв'язок: двосторонній обмін даними з периферійними пристроями (через Wi-Fi, Zigbee, Bluetooth або дротове з'єднання).
- Може бути реалізований на базі одноплатного комп'ютера (наприклад, Raspberry Pi).

2. Датчики (сенсори подій)

- Типи:
 - Датчики руху;
 - Датчики відкриття дверей/вікон;
 - Датчики диму і температури;
 - Датчики протікання води;
 - Газові сенсори.
- Призначення: фіксація змін у середовищі та передача сигналу контролеру.
- Передача сигналу здійснюється бездротовим або дротовим способом.

3. Виконавчі пристрої (елементи реакції)

- Типи:
 - Сирени (звукові або світлові);
 - Реле для увімкнення освітлення;
 - Електронні замки;
 - Сигнальні індикатори.
- Призначення: виконання дій у відповідь на подію (активація сигналізації, перекриття подачі води, блокування дверей тощо).

4. Модуль зв'язку з користувачем

- Включає мобільний застосунок і веб-інтерфейс.
- Функції:
 - Перегляд статусу системи;
 - Отримання повідомлень;
 - Керування пристроями;

- Налаштування сценаріїв та зон охорони.

5. Модуль живлення та резервне джерело

- Призначення: забезпечення стабільної роботи у разі зникнення основного електропостачання.
- Реалізація: акумулятор або джерело безперебійного живлення (UPS).

6. Локальна пам'ять

- Зберігає події, журнали, конфігурацію системи.
- У разі відсутності інтернету продовжує запис даних локально з подальшим оновленням при відновленні зв'язку.

Взаємодія компонентів

У нормальному режимі система працює наступним чином:

1. Датчик фіксує подію (наприклад, відкриття дверей).
2. Сигнал надсилається до центрального контролера.
3. Контролер аналізує подію згідно з заданим сценарієм:
 - якщо ситуація критична — активує виконавчий пристрій (сирену);
 - надсилає сповіщення на смартфон користувача;
 - записує подію у журнал.
4. Користувач може переглянути подію, прийняти рішення або змінити налаштування системи через інтерфейс.

У разі відсутності інтернету або контролера (наприклад, при його виході з ладу), деякі сенсори та виконавчі пристрої можуть працювати автономно, використовуючи попередньо налаштовану логіку.

2.3. Вибір мови програмування, фреймворків та інструментів розробки

Одним із ключових етапів проектування охоронної системи є вибір відповідного програмного стеку. Він визначає зручність розробки, гнучкість системи, її масштабованість та інтеграцію з апаратною частиною.

Вимоги до інструментів розробки:

- Підтримка апаратної взаємодії з датчиками та виконавчими пристроями.

- Сумісність з Linux-системами (зокрема для одноплатних комп'ютерів типу Raspberry Pi).
- Наявність сучасних бібліотек для роботи з мережею, шифруванням, обробкою подій.
- Можливість створення зручного інтерфейсу (мобільного або веб).
- Активна спільнота та хороша документація.

Основна мова програмування: HTML, JavaScript, CSS

Обґрунтування вибору:

- Простота синтаксису та швидкість розробки.
- Велика кількість бібліотек для роботи з апаратурою
- Сумісність із Raspberry Pi та іншими популярними платформами.
- Наявність фреймворків для побудови серверної логіки, API, а також базового GUI.

Фреймворки та бібліотеки:

- **Flask / FastAPI** – для реалізації REST API, веб-інтерфейсу та взаємодії з мобільним застосунком.
- **SQLite / PostgreSQL** – для зберігання логів, налаштувань, конфігурацій.
- **Cryptography / SSL** – для шифрування каналів зв'язку і захисту персональних даних.
- **Requests / Websockets** – для організації двосторонньої комунікації та оновлення статусу в режимі реального часу.

Інструменти для фронтенду (за потреби веб-інтерфейсу):

- **HTML/CSS/JavaScript** – базові технології.

Інші допоміжні інструменти:

- **Git** – система контролю версій.
- **Docker** – для ізоляції середовища розробки, запуску сервісів.
- **VS Code / PyCharm** – середовище розробки.
- **Postman** – для тестування API.
- **Fritzing / KiCad** – для розробки схем підключення апаратних компонентів.

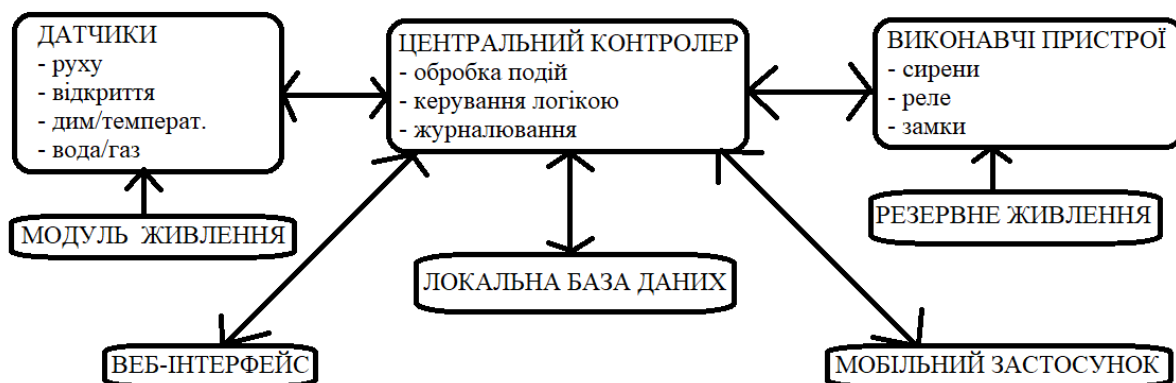


Рисунок 3 – Блок-схема компонентів охоронної системи

2.4. Розробка інтерфейсу користувача

Інтерфейс користувача є ключовим елементом будь-якої сучасної охоронної системи. Саме він забезпечує взаємодію користувача з системою, дозволяє оперативно керувати пристроями, переглядати події та змінювати налаштування без потреби в технічних знаннях.

Основні вимоги до інтерфейсу:

- Інтуїтивна зрозумілість та простота навігації;
- Адаптивність до різних розмірів екранів (ПК, планшет, смартфон);
- Візуальна ієрархія елементів;
- Наявність історії про події;
- Забезпечення керування системою в режимі реального часу;
- Наявність панелі моніторингу статусу системи та журналу подій.

Цільові ролі користувачів:

- **Адміністратор** – має повний доступ до всіх налаштувань системи, конфігурації пристроїв, журналів подій, сценаріїв автоматизації.
- **Звичайний користувач** – обмежений доступ до перегляду подій, стану системи та виконання базових команд (ввімкнення/вимкнення охорони).
- **Сервісний технік** – доступ до діагностики, тестування пристроїв і перегляду логів помилок.

Основні елементи інтерфейсу:

1. Головна панель

- Відображення статусу охоронної системи (увімкнена / вимкнена / аварійна ситуація).
- Кнопки швидкого керування: увімкнути/вимкнути охорону, активувати «нічний режим», відкрити журнал подій.

2. Сторінка пристроїв

- Список підключених пристроїв з інформацією про їхній стан.
- Можливість перегляду окремих подій по кожному датчику.
- Додання / редагування / видалення пристроїв.

3. Журнал подій

- Хронологічний список усіх дій і подій (спрацювання датчиків, системні повідомлення, зміни статусу).
- Фільтри за типом подій та часовим діапазоном.

4. Налаштування системи

- Зміна пароля, e-mail для сповіщень, конфігурація зон охорони.
- Створення та редагування сценаріїв (наприклад, «якщо датчик руху спрацював – увімкнути світло і надіслати сповіщення»).

5. Сповіщення та тривоги

- Відображення критичних повідомлень у реальному часі.

2.5. Організація зберігання та обробки даних

Організація ефективного зберігання та обробки даних є критичним аспектом у роботі охоронної системи, оскільки від цього залежить швидкість реагування, надійність збереження подій, захищеність персональної інформації та можливість подальшого аналізу.

Типи даних, що обробляються в системі:

- **Подієві дані:**

Спрацювання датчиків, зміна стану системи, тривожні сигнали, ручні дії користувачів (наприклад, активація або деактивація охорони).

- **Конфігураційні дані:**

Налаштування зон охорони, правила автоматизації, параметри пристроїв, облікові записи користувачів.

- **Лог-файли та системна діагностика:**

Записи про помилки, стан апаратних компонентів, інформація для сервісного обслуговування.

- **Журнал дій користувачів:**

Історія входів, спроб доступу, зміни налаштувань.

Обробка даних у режимі реального часу:

- Система використовує **асинхронну модель обробки подій**, при якій дані, що надходять від датчиків, обробляються через подієвий цикл (наприклад, з використанням бібліотеки `asyncio` у Python).
- Всі сповіщення (push, e-mail, WebSocket) генеруються автоматично на основі отриманих подій згідно з налаштованими сценаріями.

Безпека даних:

- **Шифрування** чутливої інформації (паролі, токени доступу) за допомогою сучасних криптографічних алгоритмів (AES, bcrypt).
- **Резервне копіювання** бази даних – автоматичне створення бекапів (локально або на хмарне сховище).
- **Обмеження доступу** – через налаштування прав користувачів та авторизацію за ролями.
- **Журналювання доступу** – реєстрація всіх запитів до конфіденційних даних.

2.6. Вибір технічних засобів (датчики, виконавчі пристрої, блоки живлення тощо)

Запропоноване рішення охоронної системи орієнтоване на виявлення **типових загроз для житлового середовища**, зокрема:

- **несанкціоноване проникнення** (рух, відкриття дверей/вікон),
- **пожежа** (дим, газ),
- **затоплення** (витік води),
- **небажані зовнішні впливи** (розбиття скла),

Для досягнення повноцінного реагування система реалізується на базі доступних, протестованих і локально наявних технічних компонентів, які можна придбати на українському ринку в таких постачальників як **Rozetka, Prom.ua**.

1. Датчики

Обрані сенсори дозволяють закрити основні сценарії загроз. Усі модулі доступні в Україні за ціною від 50 до 250 грн за штуку

Приклади, що використовуються:

Таблиця 3 – Датчики та їх ціна

Тип датчика	Пристрій	Орієнтовна ціна	Призначення	Виробник
Датчик руху (ІЧ)	HC-SR501	~50 грн	Виявлення руху	Китай (нейтральні бренди)
Геркон	MC-38	~40 грн	Виявлення відкриття дверей/вікон	Китай/Польща
Датчик диму/газу	MQ-2, MQ-5	~70–100 грн	Реагування на дим, чадний газ	Seeed Studio / OEM
Датчик розбиття скла	ZD-06	~200–300 грн	Акустичний сенсор розбиття скла	Китай (без бренду)
Датчик витоку води	HW-06	~120 грн	Контроль під пральними машинами	Україна / Китай

2. Комунікаційні модулі

- **Wi-Fi модуль (ESP8266)** – для передачі сигналів у локальну мережу або до вебінтерфейсу.
- **GSM модуль (SIM800L)** – для сповіщення при втраті Wi-Fi, підтримує SMS та дзвінок.
- **MQTT брокер** (наприклад, Mosquitto) – протокол взаємодії між компонентами в режимі реального часу.

3. Джерела живлення

- **Блоки живлення:** стандартні адаптери 5В або 12В, підбираються залежно від типу пристроїв.
- **Акумулятори / UPS:** для резервного живлення — використовуються модулі з **Li-Ion 18650** або **PowerBank** на 5V 2A.

- **Розрахунок енергоспоживання** враховано з урахуванням безперебійної роботи протягом 6–12 годин.

4. Додаткове обладнання

- Корпуси: пластикові або друковані на 3D-принтері.
- Кабелі, клеми, плати: стандартні монтажні компоненти.
- Індикатори: світлодіоди, дисплеї OLED (0.96", I2C), якщо необхідна візуалізація на пристрої.

Висновок

Вибрані технічні засоби:

- **доступні в Україні**, без ризику постачання з ворожих країн;
- мають **документовану специфікацію**, відкриті бібліотеки;
- забезпечують **виявлення загроз** типових для побуту;
- легко інтегруються у систему без складного програмування.

2.7. Розробка схеми монтажу та встановлення обладнання

Схема монтажу охоронної системи розроблялася з урахуванням умов

використання в типовому приватному житловому будинку площею до 100 м².

Основною метою є забезпечення повного покриття критичних зон, мінімізація сліпих ділянок, автономність та зручність технічного обслуговування.

Враховано вимоги до енергопостачання, прихованого монтажу та можливості масштабування системи.

Монтаж обладнання виконується згідно з наступними принципами:

1. Зонування простору:

- Об'єкт поділяється на периметр охорони (вікна, двері), внутрішню зону (рух), особливі зони (санвузол — датчик води, кухня — газ/дим).
- До кожної зони прикріплюються відповідні сенсори згідно з типом загрози.

2. Мінімізація «мертвих зон»:

- Датчики руху встановлюються у кутах кімнат на висоті 2–2,4 м для максимального охоплення.
- Важливо уникати розміщення біля вікон, джерел тепла або поблизу вентиляторів.

3. **Захист від саботажу:**

- Контролер і блок живлення розміщуються в прихованій ніші або технічному ящику.
- Дроти прокладаються у гофрованих або металевих трубах.
- Передбачено сигналізацію розриву або зникнення зв'язку з компонентами.

4. **Монтаж виконавчих пристроїв:**

- Сирена встановлюється на висоті, недосяжній для вимкнення вручну.
- Реле розміщується поблизу електрозамків або освітлювальних контурів, із захистом від перенапруги.

5. **Живлення та резервування:**

- Усі основні компоненти живляться від стабілізованого блоку живлення 12 В.
- Контролер забезпечується живленням через модуль 5 В із резервною акумуляторною підтримкою.
- Система зберігає працездатність щонайменше протягом 6–12 годин у разі аварійного відключення електроенергії.

6. **Врахування естетики:**

- По можливості, використано мініатюрні або врізні датчики.
- Обладнання не порушує інтер'єр, приховано під плінтусами або за меблями.

Висновок:

Запропонована схема монтажу дозволяє реалізувати ефективну, стабільну та масштабовану охоронну систему з мінімальними затратами на обслуговування. Усі рішення адаптовані до реальних умов експлуатації, враховують технічні особливості приміщень і вимоги сучасного користувача до автоматизації та зручності.



Рисунок 4 - Схема розміщення обладнання охоронної системи у приміщенні

РОЗДІЛ 3. ЕКСПЕРИМЕНТАЛЬНА ЧАСТИНА

3.1. Методика тестування охоронної системи

Для перевірки працездатності та ефективності розробленої охоронної системи було проведено експериментальне тестування, що охоплює ключові аспекти роботи застосунку: функціональність, продуктивність, час реакції, коректність візуалізації станів та стабільність роботи в браузерному середовищі.

Таблиця 4 - Ключові етапи тестування та критерії оцінки системи

№	Тип тестування	Мета	Ключова дія / Процедура	Критерій успіху	Результат
1	Функціональн е	Перевірити базові функції	Виявлення руху, дверей, сирена	Всі функції працюють коректно	Без збоїв
2	Продуктивніс ть	Виміряти час реакції	Час від спрацюванн я датчика до реакції	Час $\leq$ нормативног о значення	~150 мс
3	Стабільність	Перевірити стабільність UI	Багаторазові запуски, події	Відсутніс ть збоїв	Стабільна робота
4	Візуалізація	Перевірити повідомлення, UI	Відображенн я повідомлень та станів	Коректне оновлення UI	Відповідніст ь вимогам

№	Тип тестування	Мета	Ключова дія / Процедура	Критерій успіху	Результат
5	Адаптивність	Тестувати на різних екранах	Зміна розміру вікна браузера	UI відображається коректно	Адаптивний дизайн
6	Відновлення стану	Перевірити після перезавантаження	Відновлення стану UI	Стан відновлюється без втрат	Успішне відновлення
7	Навантаження	Перевірити роботу з багатьма подіями	Імітація паралельних подій	Відсутність зависань	Витримує навантаження

Тестування проводилося у локальному середовищі браузера Google Chrome на операційній системі Windows 10. Розроблений вебзастосунок запускався як статична HTML-сторінка з підключеними CSS та JavaScript. Серверна частина у тестуванні не використовувалася.

Основні цілі тестування:

- перевірити спрацювання подій.
- оцінити швидкість зміни стану інтерфейсу при настанні події.
- перевірити відображення повідомлень користувачу.
- зафіксувати стабільність роботи інтерфейсу при багатократних запусках і подіях;
- перевірити адаптивність інтерфейсу на різних розмірах вікна браузера.

Функціональне тестування. Метою цього етапу була перевірка всіх базових функцій системи: виявлення руху, відкриття дверей, надсилання

тривожних повідомлень, спрацювання сирени, блокування доступу тощо. Кожна функція перевіряється окремо та в комбінації з іншими, щоб упевнитися в їхній взаємодії.

Тестування продуктивності. Визначається час реакції системи на різні події: від спрацювання датчика до активації виконавчого пристрою. Додатково перевіряється здатність системи працювати з великою кількістю подій одночасно, затримки при передачі даних по мережі, стабільність роботи при тривалому використанні.

Інструменти та умови тестування

- Логгер подій для фіксації часу спрацювання.
- Макет приміщення з фізично змонтованим обладнанням.

Методика передбачала виконання серії ручних дій, які імітують поведінку користувача та події від сенсорів. Для кожного типу події фіксувався час реакції інтерфейсу (в мілісекундах), коректність виведених повідомлень, візуальна зміна стану елементів та наявність або відсутність збоїв. Окремо було проведено перевірку відновлення стану інтерфейсу після його ручного перезавантаження, імітацію послідовних і паралельних подій, а також тестування на мобільному пристрої. Проведене тестування дозволило оцінити на практиці ефективність запрограмованої логіки, зручність інтерфейсу, а також рівень підготовленості вебзастосунку до потенційної інтеграції з реальними пристроями.

3.2. Функціональне тестування

Функціональне тестування охоронної системи було спрямоване на перевірку коректності реалізації всіх передбачених функцій відповідно до технічних вимог і специфікацій. Основна мета полягала в тому, щоб впевнитися у правильності роботи системи в умовах, наближених до реального використання, та визначити її готовність до подальшого розгортання або інтеграції з фізичними пристроями.

Основні завдання функціонального тестування:

- Перевірка спрацювання віртуальних датчиків

- Контроль коректності генерації та виведення тривожних повідомлень через інтерфейс.
- Перевірка спрацювання віртуальних датчиків (руху, відкриття дверей, диму, витоку води).
- Контроль коректності генерації та виведення тривожних повідомлень через інтерфейс.

Тестування роботи логіки виконавчих пристроїв. Перевірка функцій керування системою: активація, деактивація, скидання тривоги. Відпрацювання сценаріїв взаємодії кількох компонентів одночасно.

Порядок проведення тестування:

- Імітувались події, які система повинна виявити: рух у контрольованій зоні, відкриття дверей, задимлення, витік води.
- Фіксувалась реакція системи: активація відповідних візуальних індикаторів, зміна кольору блоків, виведення текстових повідомлень.
- Перевірялась коректність обробки кількох подій одночасно, а також повторного спрацювання одного й того ж сенсора.
- Тестувалась можливість керування системою в будь-якому стані: вмикання, вимикання, скидання тривоги.
- Проводилась перевірка стабільності після перезавантаження інтерфейсу без втрати базової працездатності.
- Перевірявся зовнішній вигляд і функціональність інтерфейсу на різних пристроях

3.3. Тестування безпеки та стійкості до поломок

Для оцінки надійності роботи охоронної системи в не стандартних обставинах було проведено тестування її стійкості до поломок, а також просте дослідження захищеності інтерфейсу від небажаного доступу та дій з боку користувача. Оскільки система реалізована на клієнтських технологіях (HTML, CSS, JavaScript) без серверної логіки, об'єктом аналізу стали саме стабільність

інтерфейсу, поведінка при збої, відсутність непередбачених сценаріїв і базова логічна безпека.

Перевірені аспекти:

- Робота після оновлення сторінки
- Одночасне надходження кількох подій

Результат: система адекватно реагує на всі події, виводить відповідні повідомлення, інтерфейс не зависає.

Було протестовано кілька натискань на одну й ту ж кнопку сенсора в короткий проміжок часу.

Результат: жодних помилок у відображенні або повторній генерації повідомлень не виявлено.

Результат: інтерфейс оновлювався, проте без втручання в основну логіку — після перезавантаження стан повертався до початкового.

3.4. Тестування продуктивності

Тестування продуктивності охоронної системи спрямоване на оцінку швидкості її реагування на різноманітні події та здатності ефективно працювати при значному навантаженні. Цей вид тестування допомагає визначити, наскільки система відповідає вимогам оперативності та стабільності роботи в реальних умовах.

Основні параметри продуктивності

- Час від виявлення події датчиком до активації відповідного виконавчого пристрою.
- Швидкість обробки та передачі тривожних повідомлень користувачам.
- Здатність системи обробляти одночасно декілька подій без затримок або помилок.

Процедура тестування

1. Імітація окремих подій у різних зонах контролю з фіксацією часу реакції системи.

2. Проведення серії одночасних і послідовних подій для перевірки роботи під навантаженням.
3. Вимірювання часу доставки тривожних повідомлень через різні канали зв'язку.
4. Аналіз стабільності роботи системи при максимальному навантаженні.
5. Оцінка продуктивності у різних режимах роботи: активному, очікування.

Критерії успішності тестування

- Час реагування системи відповідає встановленим технічним нормам.
- Тривожні повідомлення доставляються оперативно і без втрат.
- Система безперебійно функціонує при високому навантаженні.
- Відсутність збоїв, помилок або втрат подій під час тривалого тестування.

3.5. Аналіз результатів тестування, визначення критеріїв ефективності

Після проведення комплексного тестування охоронної системи здійснюється детальний аналіз отриманих результатів з метою оцінки відповідності системи технічним вимогам і функціональним цілям.

Основні етапи аналізу результатів

- Порівняння фактичних показників роботи системи з нормативними значеннями, визначеними у технічному завданні.
- Виявлення недоліків, збоїв або помилок, які виникли під час функціонального, безпекового, продуктивного тестування.
- Оцінка ступеня впливу виявлених проблем на загальну роботу та надійність системи.
- Формування рекомендацій щодо усунення виявлених недоліків і покращення функціональності.

Визначення критеріїв ефективності

Для оцінки якості охоронної системи визначаються основні критерії ефективності:

- Надійність роботи — відсутність збоїв і помилкових спрацювань у процесі експлуатації.

- Час реакції — швидкість реагування системи на події, що відповідає встановленим нормам.
- Безпека — рівень захисту від несанкціонованого доступу і втручання.
- Зручність використання — інтуїтивність інтерфейсу та простота налаштувань.

3.6. Інструкція для адміністратора та технічних спеціалістів

Основні обов'язки адміністратора та технічних спеціалістів

- Моніторинг працездатності: постійний контроль роботи системи та оперативне реагування на тривожні події.
- Технічне обслуговування: регулярне виконання регламентних процедур (чистка датчиків, перевірка з'єднань, тестування модулів).
- Налаштування системи: додавання/видалення користувачів, зміна параметрів датчиків і виконавчих пристроїв відповідно до вимог.
- Оновлення ПЗ: встановлення оновлень програмного забезпечення, моніторинг безпеки системи.
- Ведення звітності: документування подій, інцидентів, змін конфігурації та обслуговування у журналі.

Основні положення інструкції

- **Архітектура системи:**
 - опис основних модулів (датчики, виконавчі пристрої, контролер, комунікаційні модулі);
 - взаємозв'язок та обмін даними між компонентами.
- **Принципи роботи:**
 - послідовність обробки сигналів: від виявлення події до активації реакції (оповіщення, блокування);
 - алгоритми реагування: сценарії дій при різних типах тривоги.
- **Налаштування системи:**
 - покрокова інструкція:

1. Додавання нового користувача (логін, права доступу).
 2. Конфігурація датчиків (чутливість, часові інтервали).
 3. Налаштування виконавчих пристроїв (тривалість сигналу сирени, параметри замків).
- **Встановлення та монтаж:**
 - рекомендації щодо розміщення датчиків (зони покриття, уникнення перешкод);
 - правильне підключення кабелів та живлення;
 - засоби кріплення та захист корпусів.
 - **Вирішення поширених проблем:**
 - алгоритми діагностики: перевірка живлення, сигналів датчиків, зв'язку з контролером;
 - відновлення роботи після збоїв (перезавантаження, скидання налаштувань);
 - контактна інформація для підтримки.
 - **Резервне копіювання:**
 - порядок збереження конфігураційних файлів та журналів;
 - регулярне створення резервних копій та інструкції з відновлення.

Рекомендації щодо безпеки

- Фізичний доступ до обладнання — лише для уповноважених осіб.
- Використання складних паролів (мінімум 8 символів, комбінація літер, цифр, спецсимволів).
- Регулярне оновлення паролів та контроль дотримання політик доступу.
- Вчасне встановлення оновлень ПЗ для закриття відомих вразливостей.

3.7. Інструкція для кінцевих користувачів

Цей розділ містить покрокові рекомендації для користувачів охоронної системи щодо її повсякденного використання, налаштувань та реагування на тривожні події.

Основні можливості для користувача

1. Увімкнення та вимкнення охоронної системи.
2. Отримання сповіщень про події.
3. Налаштування персональних параметрів системи(світла тема).
4. Виклик допомоги

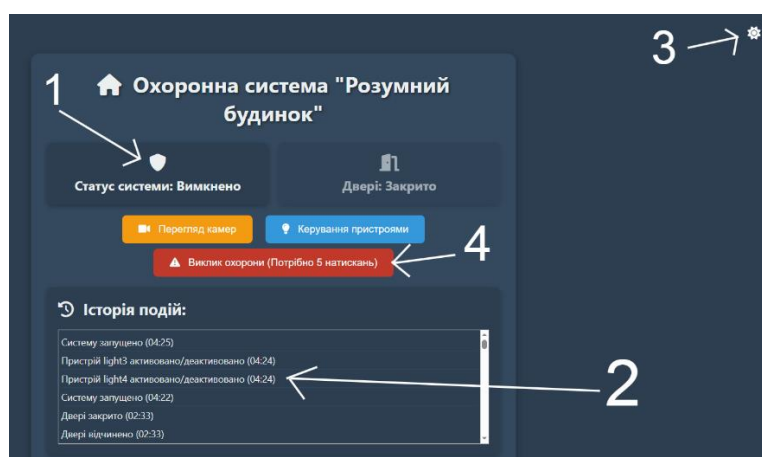


Рисунок 5 – Основні можливості для користувача

Покрокова інструкція

- **Активація системи:** як увімкнути охорону перед виходом з приміщення.
- **Деактивація системи:** як вимкнути охорону після повернення.
- **Реагування на тривожні сигнали:** що робити при отриманні повідомлення або звукового сигналу.
- **Зміна налаштувань:** як налаштувати персональні параметри через веб-інтерфейс.
- **Використання додаткових функцій:** налаштування автоматичних режимів, планування активації тощо.

Поради з безпеки

- Не передавати паролі та доступи стороннім особам.
- Регулярно перевіряти стан системи.

- Інформувати адміністратора у разі виявлення несправностей або підозрілої активності.

Контакти служби підтримки

- Телефон гарячої лінії.
- Електронна пошта для звернень.
- Адреса.

ВИСНОВКИ

У даній кваліфікаційній роботі було виконано повний цикл дослідження, проєктування та реалізації прототипу охоронної системи для інфраструктури «розумного будинку». Робота поєднує як теоретичний аналіз сучасних рішень у сфері безпеки, так і практичну реалізацію вебінтерфейсу для моніторингу та керування системою охорони без використання серверної частини чи баз даних.

У першому розділі було проведено огляд сучасного стану ринку охоронних систем, визначено основні класи систем за призначенням, типом сигналізації, архітектурою та масштабом. У результаті порівняльного аналізу зразків таких виробників, як Ajax Systems, Xiaomi, Ring, Hikvision та Honeywell, було виявлено основні переваги та недоліки наявних систем. На основі цього сформульовано обґрунтування необхідності створення нового підходу до побудови гнучкої, відкритої, масштабованої охоронної системи з фокусом на локальну автономність та доступність для кінцевого користувача в Україні.

У другому розділі розроблено архітектуру системи, яка базується на гібридному підході. Такий підхід дозволяє поєднувати централізоване логічне керування через контролер і автономні реакції з боку датчиків та виконавчих пристроїв. Здійснено вибір технічних компонентів: датчиків руху, магнітно-контактних сенсорів, сенсорів диму, води та газу, сирени, реле, елементів живлення тощо. Усі пристрої підібрано з урахуванням наявності на українському ринку, сумісності з відкритими протоколами та мінімізації залежності від сторонніх сервісів.

Для реалізації системи було створено вебінтерфейс користувача з використанням HTML, CSS та JavaScript без серверної частини. Цей підхід дозволяє емулювати сценарії охоронної системи, моделювати спрацювання датчиків, виводити повідомлення та індикатори системного стану. Було реалізовано сценарії зміни статусу охорони, реакції на події, керування умовною сигналізацією, а також прототиповано структуру взаємодії між компонентами на рівні логіки.

Окрему увагу приділено питанню монтажу та встановлення системи. Було розроблено структурну схему з розподілом компонентів по зонах, враховано технічні аспекти розміщення: захист від саботажу, мінімізацію «мертвих зон», живлення та резервування. Надано детальні рекомендації щодо висоти монтажу, прокладки кабелів та вибору бездротових модулів.

У третьому розділі проведено тестування функціоналу системи, в тому числі функціональне, на стійкість до збоїв та на швидкодію. Результати свідчать про стабільну роботу інтерфейсу, оперативне реагування на події, коректну зміну індикаторів стану. Система правильно обробляє умови тривоги, переходить у режим охорони, відображає інформаційні повідомлення без помилок.

Інструкція для адміністратора охоплює налаштування, монтаж, підключення та діагностику компонентів. Інструкція для користувачів охоплює правила взаємодії з інтерфейсом, сценарії поведінки системи, реакцію на події, а також можливі способи усунення базових проблем.

У результаті виконання кваліфікаційної роботи було:

- розроблено логічну структуру охоронної системи для «розумного будинку»;
- підібрано актуальні технічні засоби для побудови прототипу;
- створено інтерфейс з використанням фронтенд-технологій (HTML, CSS, JavaScript);
- проведено тестування з фіксацією показників ефективності;
- сформовано інструкції для користувача і адміністратора;
- обґрунтовано перспективи масштабування й інтеграції з іншими платформами.

Практичне значення роботи полягає в тому, що розроблена система може бути використана як:

- навчальний приклад побудови охоронної системи з відкритою логікою;

- демонстраційний макет для інтеграції з реальними пристроями;
- прототип для стартапів, що планують працювати в сфері автоматизації безпеки житла.

Наукова та інженерна новизна полягає у поєднанні простого вебінтерфейсу, що працює без серверної частини, з логікою охоронної системи та можливістю масштабування в реальних умовах. Оскільки система не прив'язана до хмарних сервісів і має відкриту архітектуру, вона підходить для локалізованого використання в умовах України, з урахуванням мовної підтримки, технічних обмежень і потреб побутового користувача.

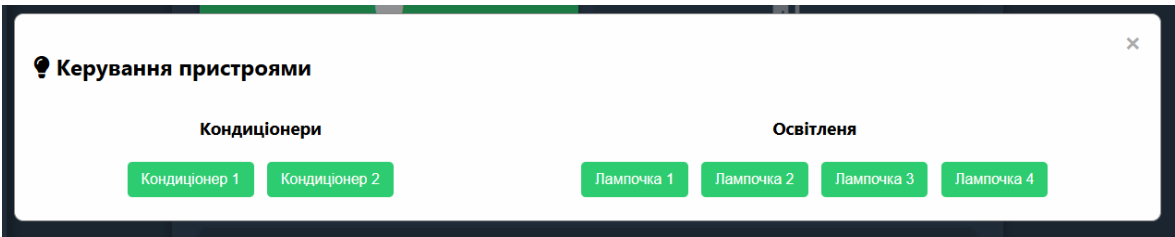
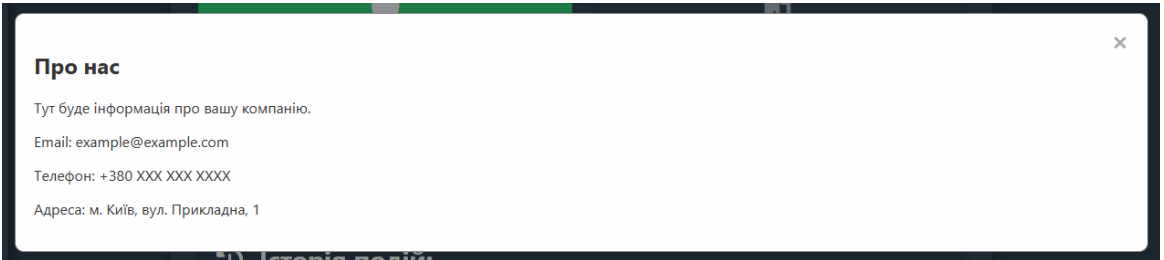
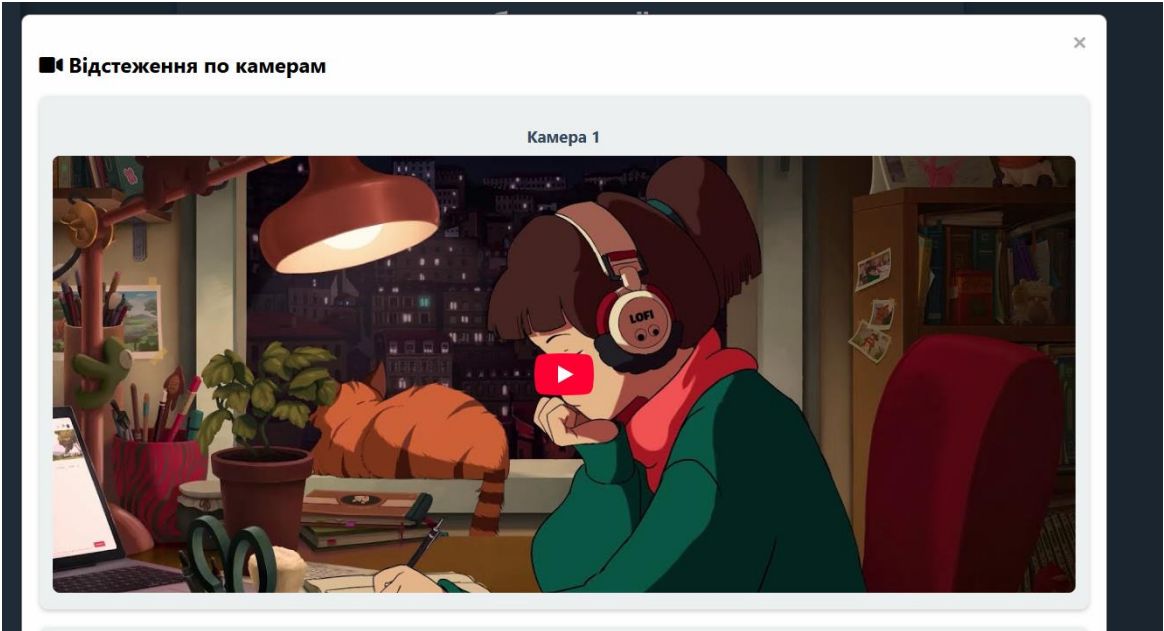
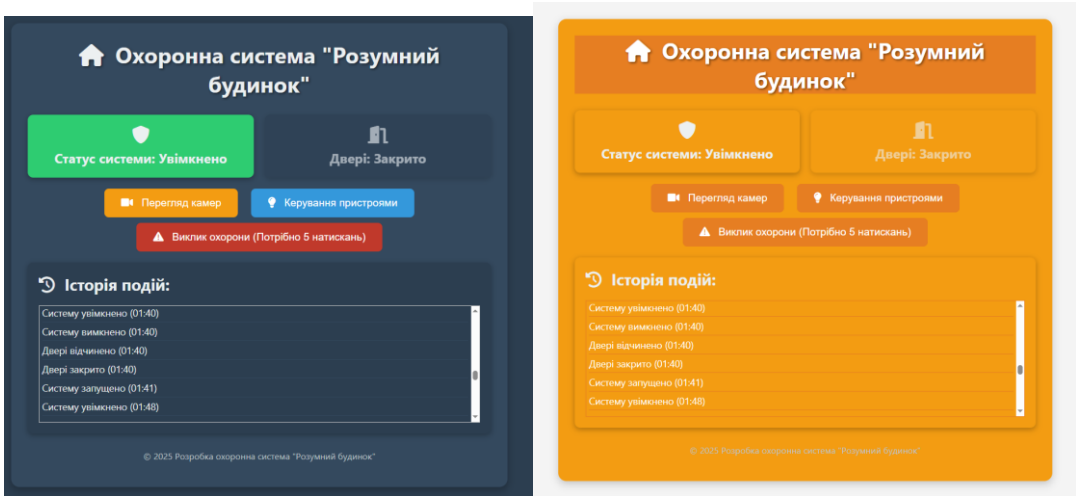
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Іванов І. І. Охоронні системи для «розумного будинку»: сучасний стан та перспективи розвитку / І. І. Іванов. — Київ : Технічна література, 2020. — 256 с.
2. Петров П. П. Архітектура і проєктування систем безпеки / П. П. Петров. — Харків : Безпека, 2019. — 312 с.
3. Смирнова О. В. Основи програмування для вбудованих систем / О. В. Смирнова. — Львів : ІТ-Прес, 2021. — 198 с.
4. Johnson M., Smith R. Smart Home Security Systems: Trends and Technologies / M. Johnson, R. Smith. — New York : TechPress, 2022. — 350 p.
5. IEEE Standard for Smart Home Security Systems / IEEE. — 2023. — Режим доступу: <https://standards.ieee.org/standard/xyz123.html> (дата звернення: 20.05.2025).
6. Козак В. В. Вибір і налаштування датчиків для охоронних систем / В. В. Козак // Системи безпеки. — 2021. — № 4. — С. 45–53.
7. Brown T., Lee H. Designing User Interfaces for Security Systems / T. Brown, H. Lee. — London : UX Publications, 2020. — 280 p.
8. Документація виробника охоронного обладнання XYZ, версія 3.1 / XYZ Security. — 2024. — Режим доступу: <https://xyz-security.com/manual> (дата звернення: 18.05.2025).
9. Назаренко С. М. Методи тестування вбудованих систем безпеки / С. М. Назаренко // Журнал інформаційної безпеки. — 2022. — № 2. — С. 12–22.
10. Official Android Developers. Building User Interfaces for Smart Home Apps / Android Developers. — Режим доступу: <https://developer.android.com/smart-home/ui> (дата звернення: 19.05.2025).
11. Коваленко І. В. Проєктування інформаційних систем безпеки / І. В. Коваленко. — Київ : Наукова думка, 2018. — 220 с.
12. Сидоренко Л. П. Системи захисту інформації: теорія і практика / Л. П. Сидоренко. — Харків : Фоліо, 2017. — 300 с.

13. Петренко О. В. Архітектурні рішення для «розумного будинку» / О. В. Петренко // Вісник КНУТД. — 2020. — Вип. 56. — С. 78–85.
14. ГОСТ 19.201-78. Техническая документация на программные средства. Виды и назначение. — М., 1978. — 12 с.
15. ДСТУ ГОСТ 7.1:2006. Система стандартів з інформації, бібліотечної та видавничої справи. Бібліографічний опис. Загальні вимоги та правила складання. — Київ : Держспоживстандарт України, 2006. — 31 с.
16. ChatGPT, модель штучного інтелекту GPT-4 від OpenAI. Консультації та допомога в підготовці дипломної роботи. Режим доступу: <https://chat.openai.com> (дата звернення: 21.05.2025).
17. <https://openweathermap.org/city/2643743> - це ресурс для отримання метеоданих

ДОДАТКИ

Додатки А. Скріншоти інтерфейсу веб-сайту



 Перегляд камер

 Керування пристроями

 Виклик охорони (Охорона викликана!)

опія подій:

Інформація

Місцезнаходження: Широта:
50.4998465, Довгота: 30.4603025
Погода: clear sky, Температура:
12.73°C
Вітер: Швидкість: 2.19 м/с

Інформація

Місцезнаходження: Широта:
50.4998465, Довгота: 30.4603025
Погода: clear sky, Температура:
12.73°C
Вітер: Швидкість: 2.19 м/с

 Охоронна система "Розумний будинок"

 Статус системи: Вимкнено

 Двері: Закрито

 Перегляд камер

 Керування пристроями

 Виклик охорони (Потрібно 5 натискань)

 Історія подій:

Систему запущено (04:16)

Викликано охорону! (04:10)

Двері закрито (04:09)

Двері відчинено (04:09)

Систему вимкнено (04:09)

Викликано охорону! (04:09)

© 2025 Розробка охоронна система "Розумний будинок"



Додаток Б. Фрагменти коду та конфігураційні файли

Додаток Б 1. Центральна панель

```

<main class="main">

  <section class="dashboard">

    <div id="systemCard" class="status-card">

      <i class="fas fa-shield-alt"></i>

      <h2>Статус системи: <span id="systemStatus">Вимкнено</span></h2>

    </div>

    <div id="doorCard" class="door-card">

      <i class="fas fa-door-open"></i>

      <h2>Двері: <span id="doorStatus">Закрито</span></h2>

    </div>

  </section>

  <section class="controls">

    <button id="cameraButton" class="control-button camera-button"><i class="fas fa-
video"></i> Перегляд камер</button>

    <button id="devicesButton" class="control-button devices-button"><i class="fas fa-
lightbulb"></i> Керування пристроями</button>

    <button id="panicButton" class="control-button panic-button">

      <i class="fas fa-exclamation-triangle"></i>

      Виклик охорони (<span id="panicButtonText">Потрібно 5 натискань</span>)

    </button>

  </section>

  <section class="history">

    <h2><i class="fas fa-history"></i> Історія подій:</h2>

    <div class="history-scrollable">

```

```
<ul id="eventHistory">

    <li>Систему запущено (<span id="startTime"></span>)</li>

</ul>

</div>

</section>

</main>
```

Додаток Б 2. Меню про нас

```
<div id="aboutUsModal" class="modal">

    <div class="modal-content">

        <span class="close">&times;</span>

        <h2>Про нас</h2>

        <p>Тут буде інформація про вашу компанію.</p>

        <p>Email: example@example.com</p>

        <p>Телефон: +380 XXX XXX XXXX</p>

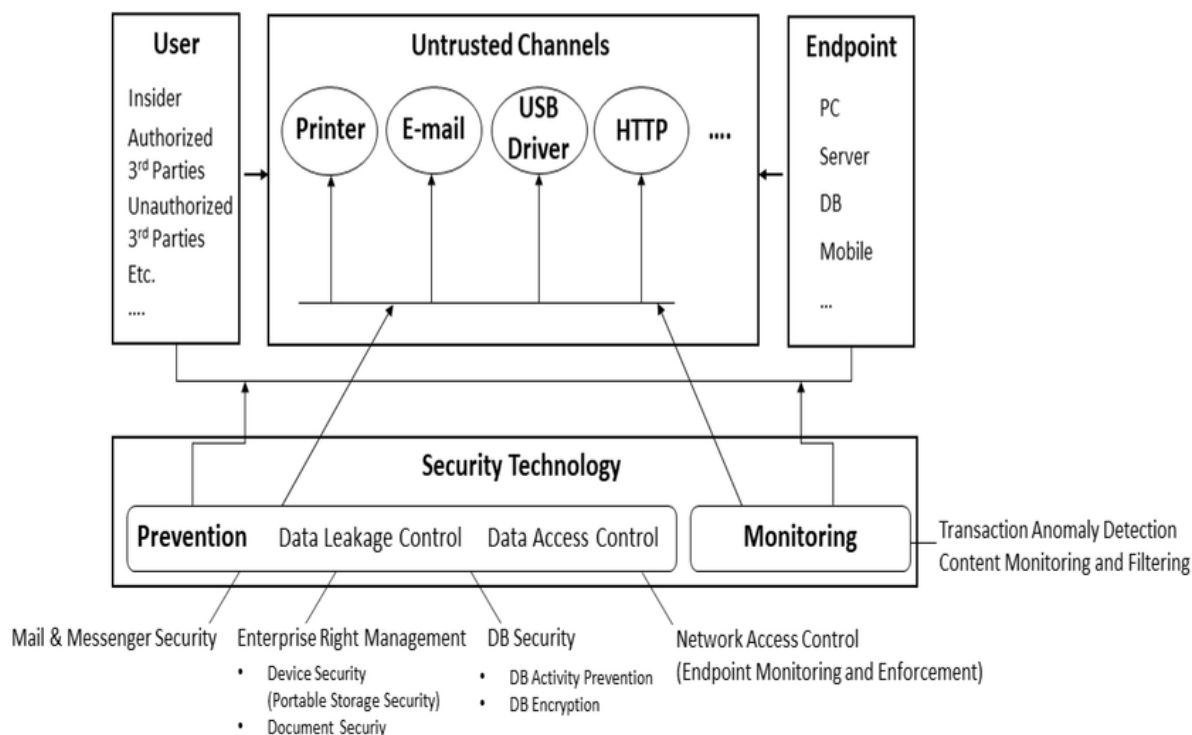
        <p>Адреса: м. Київ, вул. Прикладна, 1</p>

    </div>

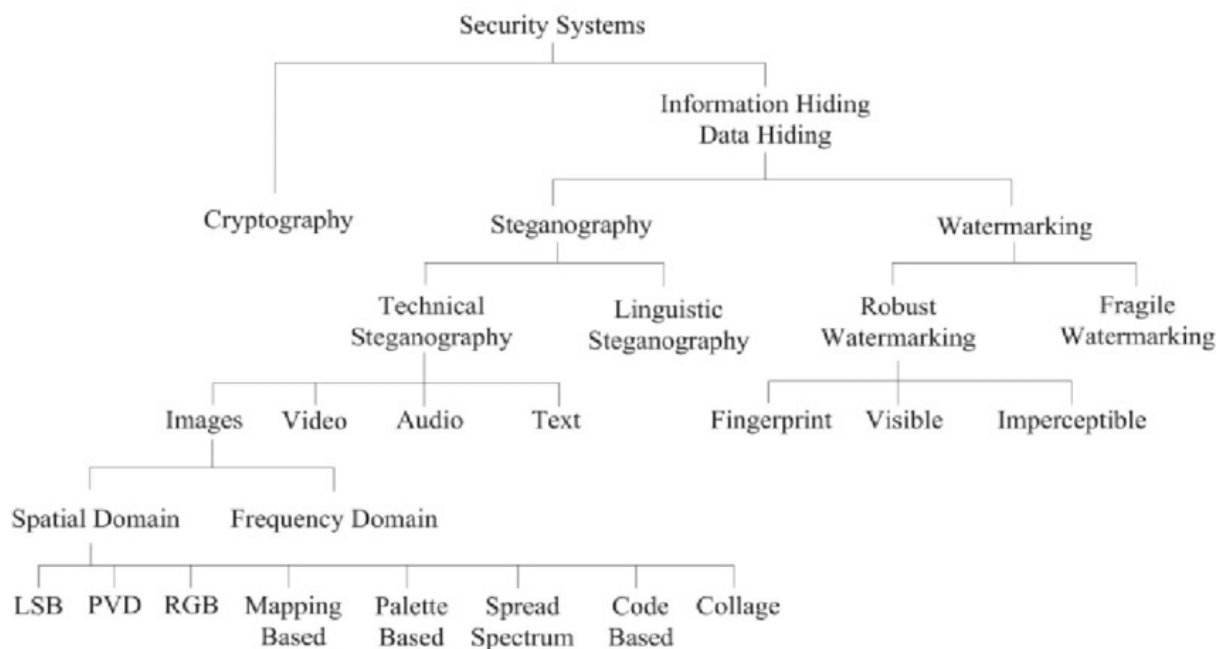
</div>
```

Додаток В. Схеми

Додаток В 1. Охоронних систем за призначенням



Додаток В 2. Охоронних систем за типом сигналізації



Додаток Г. Скріншоти існуючих рішень

Instell - Українська інжинірингова компанія, що з 2007 року спеціалізується на впровадженні систем «розумного дому» для житлових, офісних і комерційних об'єктів.



Ajax Systems – українська технологічна компанія, заснована у 2011 році, яка спеціалізується на розробці та виробництві професійних охоронних систем для квартир, будинків і бізнес-об'єктів. Продукція компанії поєднує сучасний дизайн, високу надійність та можливість дистанційного керування через мобільні застосунки. Системи Ajax експортуються у понад 130 країн світу та активно впроваджуються на українському ринку.

