

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВЕТЕРИНАРНОЇ
МЕДИЦИНИ ТА БІОТЕХНОЛОГІЙ ІМ. С.З. ГЖИЦЬКОГО
ФАКУЛЬТЕТ МЕХАНІКИ, ЕНЕРГЕТИКИ ТА ІНФОРМАЦІЙНИХ
ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**

КВАЛІФІКАЦІЙНА РОБОТА

другого (магістерського) рівня вищої освіти

на тему:

«РОЗРОБКА ТА ДОСЛІДЖЕННЯ ПРОГРАМНОГО МОДУЛЯ УПРАВЛІННЯ ОХОРОННОЮ СИСТЕМОЮ РОЗУМНОГО БУДИНКУ»

Виконав: здобувач групи Іт-61
спеціальності 126 «Інформаційні системи та
технології»

Сивуляк Н. І.
(прізвище та ініціали)

Керівник: _____
Пташник В. В.
(прізвище та ініціали)

ДУБЛЯНИ-2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ПРИРОДОКОРИСТУВАННЯ
ФАКУЛЬТЕТ МЕХАНІКИ, ЕНЕРГЕТИКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Другий (магістерський) рівень вищої освіти
Спеціальність 126 «Інформаційні системи та технології»

ЗАТВЕРДЖУЮ
Завідувач кафедри

(підпис)
д.т.н., професор, Тригуба А. М.
(вч. звання, прізвище, ініціали)
“ ” 202 року

З А В Д А Н Н Я НА КВАЛІФІКАЦІЙНУ РОБОТУ

Сивуляку Назару Івановичу
(прізвище, ім'я, по батькові)

1. Тема роботи «Розробка та дослідження програмного модуля управління охоронною системою розумного будинку»

керівник роботи к. т. н., доцент., Пташник В. В.

(наук. ступінь, вч. звання, прізвище, ініціали)

затверджені наказом Львівського НУП від 28.02.2025 року № 140/к-с.

2. Строк подання студентом роботи 8 грудня 2025 року

3. Вихідні дані до роботи: технічні характеристики та експлуатаційні параметри побутових охоронних систем «розумного будинку», а також документація до використаних апаратно-програмних засобів керування і сповіщення. Паспорти, даташити й специфікації орієнтовних компонентів прототипу. Технічна документація та приклади застосування АТ-команд і DTMF-керування для модулів стандарту GSM. Науково-технічна література й нормативні вимоги щодо проєктування, експлуатації та підвищення надійності охоронної сигналізації у житлових приміщеннях.

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

Вступ

1. Аналіз сучасних систем домашньої охоронної сигналізації

2. Структурно-апаратна реалізація побутової системи охоронної сигналізації

3. Алгоритмічне та програмне забезпечення системи побутової охоронної сигналізації

4. Охорона праці та безпека в надзвичайних ситуаціях

5. Економічна ефективність

Висновки

Список використаних джерел

5. Перелік графічного матеріалу

Графічний матеріал подається у вигляді презентації

6. Консультанти розділів

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата		Відмітка про виконання
		завдання видав	завдання прийняв	
1, 2, 3, 5	Пташник В. В., к.т.н., доцент			
4	Городецький І. М., к.т.н., доцент			

7. Дата видачі завдання 3 березня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Відмітка про виконання
1	Складання інженерної характеристики охоронних систем розумного будинку	03.03.2025 – 15.04.2025	
2	Вибір принципів, методів та засобів реалізації охоронної системи розумного будинку	16.04.2025 – 31.05.2025	
3	Розробка алгоритмічного та програмного забезпечення системи побутової охоронної сигналізації та його тестування	01.06.2025 – 30.09.2025	
4	Розгляд питань з охорони праці та безпеки у надзвичайних ситуаціях	01.10.2025 – 20.10.2025	
5	Оцінка економічної ефективності прийнятих рішень	21.10.2025 – 15.11.2025	
6	Завершення оформлення розрахунково-пояснювальної записки та презентаційного матеріалу	16.11.2025 – 30.11.2025	
7	Завершення роботи в цілому. Підготовка до захисту кваліфікаційної роботи	01.06.2025 – 08.12.2025	

Здобувач

(підпис) Сивуляк Н. І.
(прізвище та ініціали)

Керівник роботи

(підпис) Пташник В. В.
(прізвище та ініціали)

УДК 681.521 / 681.518

Розробка та дослідження програмного модуля управління охоронною системою розумного будинку. Сивуляк Н. І. Кафедра інформаційних технологій – Дубляни, Львівський НУВМБ ім. С.З. Гжицького, 2025.

Кваліфікаційна робота: 69 сторінок текстової частини, 35 рисунків, 9 таблиць, 20 джерел літератури.

Мета кваліфікаційної роботи полягає у розробці та дослідженні програмного модуля керування охоронною системою «розумного будинку», який забезпечує збір даних із датчиків, виявлення тривожних подій, індикацію станів системи та дистанційне керування й оповіщення користувача через GSM-канал із підтримкою SMS-повідомлень і DTMF-команд.

Об'єктом дослідження є процеси забезпечення безпеки житлового приміщення в системі «розумного будинку», зокрема моніторинг станів охоронних датчиків, оброблення подій несанкціонованого проникнення та формування керуючих і тривожних повідомлень.

Предмет дослідження охоплює методи й програмно-апаратні засоби реалізації модуля управління охоронною сигналізацією: опитування сенсорів, оброблення тривоги, роботу інтерфейсу користувача та інтеграцію з GSM-модулем для дистанційного керування.

У кваліфікаційній роботі проаналізовано підходи до побудови охоронних систем «розумного будинку» та їхні вимоги. Запропоновано архітектуру програмного модуля на мікроконтролерній платформі, визначено склад датчиків і виконавчих елементів та описано алгоритми оброблення сигналів і формування тривоги. Реалізовано дистанційне керування й оповіщення через GSM (SMS/DTMF) і виконано тестування працездатності в типових режимах.

Ключові слова: розумний будинок, охоронна система, програмний модуль, мікроконтролер, Arduino, датчик руху, геркон, датчик розбиття скла, тривожне сповіщення, GSM-модуль, DTMF, дистанційне керування, моніторинг.

ЗМІСТ

ВСТУП.....	7
РОЗДІЛ 1 АНАЛІЗ СУЧАСНИХ СИСТЕМ ДОМАШНЬОЇ ОХОРОННОЇ СИГНАЛІЗАЦІЇ.....	9
1.1 Функціональні вимоги до побутової системи охоронної сигналізації	9
1.2 Порівняльний аналіз підходів до побудови систем охоронної сигналізації	10
1.3 Компоненти та сценарії роботи побутових охоронних систем розумного будинку	12
1.4 Огляд та порівняння побутових систем охоронної сигналізації.....	16
1.4.1 Безпроводна охоронна сигналізація MAKS PRO	16
1.4.2 Безпроводна сигналізація Kit GSM	17
1.4.3 Система безпеки Ajax StarterKit.....	18
1.4.4 Безпроводна побутова охоронна сигналізація Ajax HomeSiren	19
РОЗДІЛ 2 СТРУКТУРНО-АПАРАТНА РЕАЛІЗАЦІЯ ПОБУТОВОЇ СИСТЕМИ ОХОРОННОЇ СИГНАЛІЗАЦІЇ	20
2.1 Структурна модель системи побутової охоронної сигналізації	20
2.2 Вибір елементної бази системи охоронної сигналізації.....	23
2.2.1 Елементи модуля керування	23
2.2.2 Елементи модуля датчиків	27
2.2.3 Елементи модуля сповіщення	29
2.2.4 Елементи модуля живлення	33
2.3 Розробка електричної принципової схеми системи побутової охоронної сигналізації	33
РОЗДІЛ 3 АЛГОРИТМІЧНЕ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМИ ПОБУТОВОЇ ОХОРОННОЇ СИГНАЛІЗАЦІЇ	35
3.1 Вибір режимів роботи та розробка алгоритмів функціонування охоронної системи розумного будинку	35

3.2 Програмна реалізація модулів керування системою побутової охоронної сигналізації	39
3.3 Реалізація дистанційного керування системою за допомогою DTMF-команд	43
3.4 Дослідження експлуатаційних характеристик і надійності розробленої охоронної системи	45
РОЗДІЛ 4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ	51
4.1 Можливість виникнення статичної електрики та заходи боротьби з нею	51
4.2 Заходи з техніки безпеки при виготовленні плат, при паянні та склеюванні деталей	53
РОЗДІЛ 5 ЕКОНОМІЧНА ЕФЕКТИВНІСТЬ	58
5.1 Економічна характеристика об'єкта впровадження та аналіз ринку систем домашньої охоронної сигналізації	58
5.2 Розрахунок витрат на розробку та впровадження програмно-апаратного комплексу	60
5.3 Оцінка економічної ефективності та соціально-економічного ефекту впровадження	63
ВИСНОВКИ	67
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	68

ВСТУП

Згідно зі статистикою за 2024 рік, в Україні було зареєстровано 10 470 крадіжок зі зломом у квартирах, причому значна частина таких правопорушень залишається нерозкритою. За цих умов зростає потреба не лише у фізичних засобах захисту, а й у надійних інформаційних технологіях, здатних забезпечити безперервний моніторинг подій, оперативне оповіщення та прозору взаємодію користувача із системою безпеки. Сучасні системи сигналізації можуть ефективно протидіяти проникненню сторонніх осіб до охоронюваних приміщень завдяки використанню різних типів датчиків, розподіленої архітектури та дистанційного керування. Їхні переваги полягають у високій надійності, можливості автоматизації типових сценаріїв та здатності забезпечувати належний рівень захисту за рахунок своєчасного виявлення інцидентів.

Першочерговим завданням охоронної сигналізації є своєчасне повідомлення домовласників і, за потреби, правоохоронних органів або охоронної компанії про факт несанкціонованого проникнення чи іншу тривожну подію. Однак у межах концепції «розумного будинку» ефективність системи дедалі більше визначається якістю програмного забезпечення: коректністю алгоритмів оброблення сигналів, стійкістю до хибних спрацювань, надійністю обміну даними, веденням журналів, а також захищеністю каналів зв'язку та облікових даних. Досягти цього можливо лише шляхом обґрунтованого вибору технічних засобів, протоколів передавання, архітектурних рішень і механізмів контролю цілісності та доступності даних.

Системи охоронної сигналізації можуть відлякувати зловмисників та попереджати оточення про загрозу, зокрема через звуковий сигнал тривоги. Водночас максимальна практична ефективність досягається тоді, коли сигналізація інтегрована з централізованим пультом моніторингу охоронної компанії або з віддаленим сервісом спостереження, що забезпечує оперативну реакцію на події. Для цього програмний модуль керування має підтримувати

надійні сценарії обміну повідомленнями, гнучке налаштування зон і правил, а також механізми підтвердження доставки сповіщень, резервні канали зв'язку та контроль працездатності компонентів.

Особливо важливо, щоб охоронні системи були масштабованими, сумісними з типовими датчиками й виконавчими пристроями, а також відповідали базовим вимогам кібербезпеки (автентифікація, авторизація, захист від несанкціонованого доступу, журналювання подій). Метою кваліфікаційної роботи є розробка та дослідження програмного модуля управління охоронною системою розумного будинку для забезпечення цілодобового захисту житлових будинків. Розроблюваний модуль має реалізувати логіку опитування сенсорів, оброблення тривожних подій, формування сповіщень та інтеграцію з каналами дистанційної взаємодії, спираючись на мікропроцесорну технологію та сучасну елементну базу, з акцентом на програмно-архітектурні рішення.

Для досягнення цієї мети необхідно виконати такі завдання:

- здійснити огляд та аналіз існуючих аналогічних продуктів на ринку, визначити їхні функціональні можливості, типові архітектури та обмеження;
- розробити загальну структурну схему домашньої охоронної сигналізації з описом інформаційних потоків між датчиками, контролером, каналами зв'язку та користувацьким інтерфейсом;
- розробити принципові схеми модулів, що використовуються для керування роботою системи, та обґрунтувати вибір компонентів з позицій надійності й вартості;
- описати основні функції програмного забезпечення та алгоритми роботи модулів (оброблення подій, фільтрація хибних спрацювань, пріоритизація тривоги, журналювання);
- розробити програмне забезпечення, необхідне для коректного функціонування системи, і провести його дослідження за ключовими показниками (стабільність роботи, швидкодія, надійність сповіщень, базові аспекти безпеки).

РОЗДІЛ 1

АНАЛІЗ СУЧАСНИХ СИСТЕМ ДОМАШНЬОЇ ОХОРОННОЇ СИГНАЛІЗАЦІЇ

1.1 Функціональні вимоги до побутової системи охоронної сигналізації

Система охоронної сигналізації (СОС) – це комплекс технологій, призначених для захисту приміщень від зловмисного проникнення. Сучасні системи безпеки є високотехнологічними апаратно-програмними комплексами, які об'єднують системи відеоспостереження, охоронну та пожежну сигналізацію, системи контролю та управління доступом, інше спеціалізоване обладнання, а також забезпечують їх інтеграцію в єдину інфраструктуру.

Сучасні комп'ютерні системи охоронної сигналізації повинні відповідати таким основним вимогам:

- робота в режимі реального часу;
- автоматична активація сигналізації та надсилання сповіщень;
- повідомлення користувачів про всі спроби зловмисного проникнення;
- дистанційний моніторинг за допомогою бездротових технологій.

Ключовою вимогою є можливість автоматичної активації звукового сповіщення при виявленні вторгнення. Для цього система повинна використовувати датчики руху, датчики відкриття дверей і датчики розбиття скла. Крім того, система має бути оснащена генератором звукових сигналів. Одним із компонентів системи є пристрій на базі мікроконтролера, який опитує датчики та здійснює загальне керування системою. Для його вибору доцільно провести порівняльний аналіз наявних компонентів. Система також повинна забезпечувати дистанційний контроль стану об'єкта, тому потрібно вибрати технологію, здатну віддалено надсилати сповіщення користувачам.

1.2 Порівняльний аналіз підходів до побудови систем охоронної сигналізації

Системи охоронної сигналізації спрямовані на захист об'єктів від несприятливих впливів та факторів. Для отримання даних про стан об'єкта, що охороняється, система використовує різні типи датчиків. Усі дані від датчиків передаються на панель керування через інформаційний канал. Датчик – це пристрій, безпосередньо встановлений на об'єкті для отримання даних про його стан. Він перетворює отримані дані у форму, зручну для передавання через обраний канал зв'язку. Датчики системи охоронної сигналізації здебільшого вимірюють неелектричні величини, тому вимагають високого рівня надійності керування [2]. До найпоширеніших типів датчиків у системах охоронної сигналізації належать [3, 4]:

- інфрачервоні датчики присутності та руху;
- датчики розбиття скла;
- мікрохвильові датчики;
- датчики вібрації;
- фотоелектричні датчики;
- магнітні (герконові) датчики;
- ультразвукові датчики.

У дротовій системі охоронної сигналізації сигнал від датчика до центрального модуля передається кабелем; у бездротовій системі – радіоканалом. Гібридна система поєднує обидва типи, тому сигнал від датчика може передаватися як по радіоканалу, так і по кабелю. У минулому дротові системи були більш поширеними, оскільки технологія бездротової передачі інформації ще не була достатньо розвиненою: безпека радіоканалів була проблемною, а перебої у зв'язку траплялися часто. Сучасні бездротові технології значно підвищили свою ефективність та надійність, що створює серйозну конкуренцію дротовим рішенням. Нині бездротові системи охоронної

сигналізації пропонують високу гнучкість і масштабованість, а також є простими в установці та налаштуванні [2].

Системи охоронної сигналізації охоплюють засоби та методи забезпечення безпеки об'єктів за допомогою інтерактивних компонентів і систем пристроїв. У цій роботі як приклад розглянуто систему домашньої охоронної сигналізації. Вона являє собою мережу інтегрованих електронних пристроїв, які працюють спільно з центральною панеллю керування для запобігання крадіжкам та іншим протиправним діям. Сьогодні значна кількість будинків, підприємств та установ стикається зі спробами вторгнення, більшість яких здійснюється через вікна або зачинені двері. На рисунку 1.1 показано структуру типової системи охоронної сигналізації та її компоненти [6].

Статистичні дані свідчать, що більшості спроб несанкціонованого вторгнення зазвичай можна запобігти, просто встановивши в приміщенні охоронну сигналізацію. Злочинці, як правило, намагаються проникнути до об'єктів із слабкими заходами безпеки, а не до тих, що обладнані системами охоронної сигналізації [6]. Статистика також показує, що навіть найпростіша система сигналізації може суттєво зменшити ймовірність спроб проникнення злоумисників до захищеного об'єкта [2].

Коли сучасна охоронна система отримує сигнал, який може свідчити про вторгнення або спробу проникнення, вона зазвичай подає дуже гучний сигнал тривоги та/або надсилає сповіщення власнику будинку (якщо така функція передбачена конструкцією системи). З огляду на зростання рівня злочинності, захист будівель та майна за допомогою сучасних пристроїв охоронної сигналізації має вирішальне значення. Вартість таких пристроїв залежить від їхньої конструкції та застосовуваних технологій [6].

Охоронні пристрої, що використовують радіоканали для передавання інформації з датчиків про дії злоумисників, є ефективнішими за інші типи пристроїв. Застосування сучасних технологій дає змогу суттєво підвищити стійкість радіоканалів до перешкод і збільшити дальність передавання інформації [7].

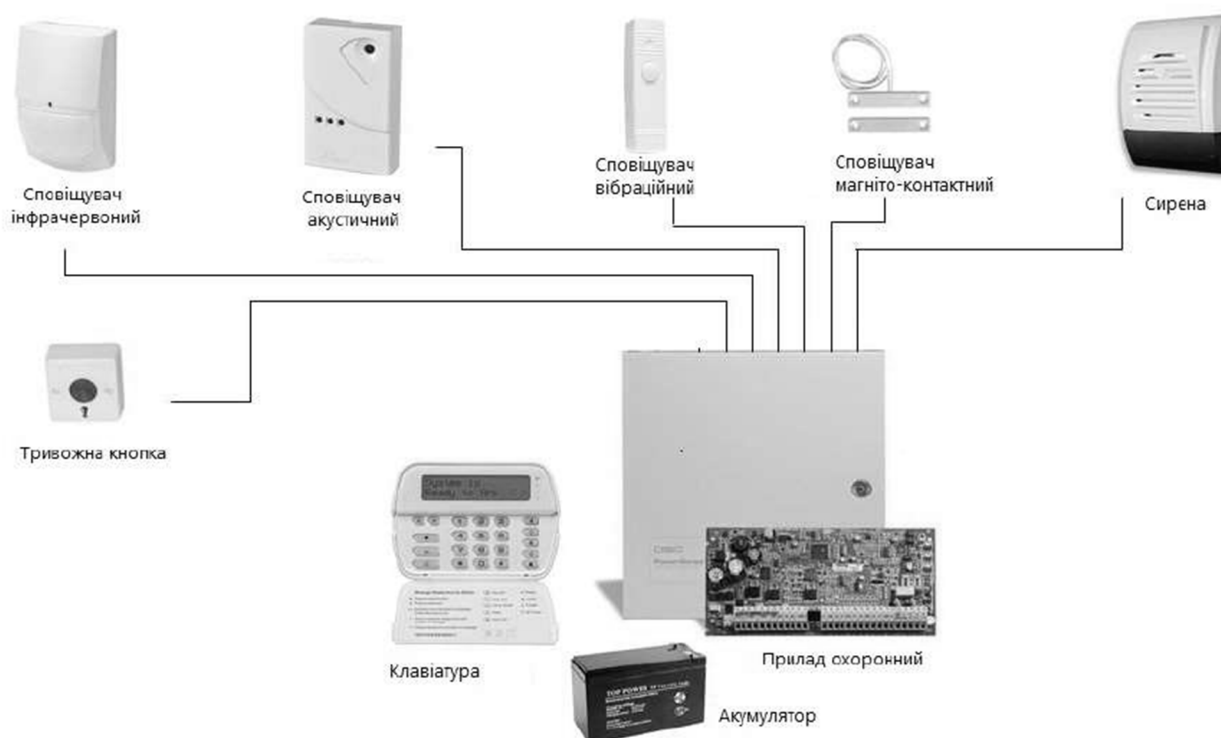


Рисунок 1.1 – Типова функціональна структура системи охоронної сигналізації

1.3 Компоненти та сценарії роботи побутових охоронних систем розумного будинку

Побутові системи охоронної сигналізації в «розумному будинку» поєднують апаратні засоби виявлення подій і програмні механізми їх оброблення та реагування. Типова архітектура включає набір сенсорів (руху, відкриття дверей/вікон, диму, газу), а також підсистеми відеоспостереження. Центральний контролер (або програмний центр керування) збирає телеметрію, виконує первинну фільтрацію, визначає стан системи (охорона/часткова охорона/пауза), формує події тривоги та запускає сценарії реагування. Для користувача ключовими є віддалене керування через мобільний застосунок/вебінтерфейс і оперативні сповіщення в режимі реального часу. Практика впровадження показує, що ефективність таких рішень суттєво залежить не лише від «заліза», а

й від логіки програмного модуля: коректної обробки станів, фільтрації, правил підтвердження тривоги та надійної доставки повідомлень. Використання хмарних сервісів розширює можливості моніторингу та керування, але підвищує вимоги до захисту облікових записів, автентифікації, шифрування та регулярних оновлень ПЗ як складників протидії кіберзагрозам.

У більшості комплексних систем важливу роль відіграють камери та засоби зберігання відеоданих. Навіть якщо прийняття рішення частково покладається на людину (службу охорони або власника), відеоархів і можливість подальшого аналізу є критичними для верифікації інциденту та ідентифікації порушника. Поширеним підходом є не безперервний запис, а алгоритмічний режим: камера активується після спрацювання датчика руху чи контактного датчика, виконує запис протягом визначеного часу та передає відео в реальному часі або серію кадрів. Така схема зменшує обсяг даних і водночас накладає вимоги на програмний модуль щодо коректного керування подіями, таймерами та пріоритезацією сповіщень.

Аудіоканали застосовуються рідше та переважно як допоміжні до відеоспостереження. Вони можуть підвищувати інформативність інциденту, однак потребують додаткових механізмів фільтрації й зниження хибних спрацювань, що особливо важливо в умовах високого фонового шуму.

Розвиток охоронних рішень сьогодні тісно пов'язаний з еволюцією «розумного дому»: від ранніх прототипів автоматизації до масового поширення мікроконтролерних платформ і мобільних інтерфейсів керування, що істотно підвищило зручність і функціональність таких систем [4]. Інтеграція з іншими підсистемами будинку (освітлення, клімат, енергозбереження) дає змогу реалізовувати комбіновані сценарії, але водночас ускладнює архітектуру та підвищує вимоги до узгодженості логіки між підсистемами. Концепція безпеки стала частиною цієї інтеграції: автономні охоронні рішення поступово об'єднувалися в єдину інфраструктуру завдяки спільним датчикам і контролерам [5]. На рис. 1.2 наведено різновиди та приклади сучасних систем безпеки розумного будинку.



Рисунок 1.2 – Різновиди обладнання сучасних систем безпеки розумного будинку

Сенсорна база істотно впливає на чутливість і надійність охоронної системи, однак на практиці немає потреби задіювати всі доступні датчики. Доцільним є розміщення обмеженої кількості сенсорів у найвразливіших зонах або в точках, які неможливо обійти. Датчики руху залишаються базовим інструментом виявлення присутності; вони фіксують зміни параметрів середовища у контрольованій зоні та формують сигнали логіки безпеки [6]. Попри різноманітність реалізацій, у побутових умовах переважають оптичні й акустичні підходи, а їх універсальність дозволяє використовувати ті самі сенсори як для автоматизації освітлення, так і для виявлення вторгнення. Контактні датчики (двері/вікна) мають просту конструкцію та надійно фіксують зміну стану проходу; в інтегрованих системах вони також можуть обслуговувати сценарії автоматизації (зупинка механізму закривання, контроль «вікно зачинене» тощо). За потреби застосовують і спеціалізовані сенсори (інфрачервоні бар'єри, тиску, нахилу), але їх використання зазвичай зумовлене конкретними умовами об'єкта.

З погляду комплектації, для квартир типовими є датчики руху у зоні входу та датчики відкривання/закривання дверей; додатково може використовуватися тривожна кнопка для ручного виклику допомоги (рис. 1.3). У «розумному будинку» роль тривожної кнопки може виконувати будь-який елемент керування, включно з голосовими командами, що потребує від програмного модуля підтримки різних каналів ініціації тривоги та політик безпечного підтвердження події. Підвищення рівня безпеки (наприклад, додавання відеоаналітики або аналізу звуку) розширює можливості системи, але збільшує складність і ризик відмови, тому програмний модуль має забезпечувати режим деградації без втрати критичних можливостей оповіщення.

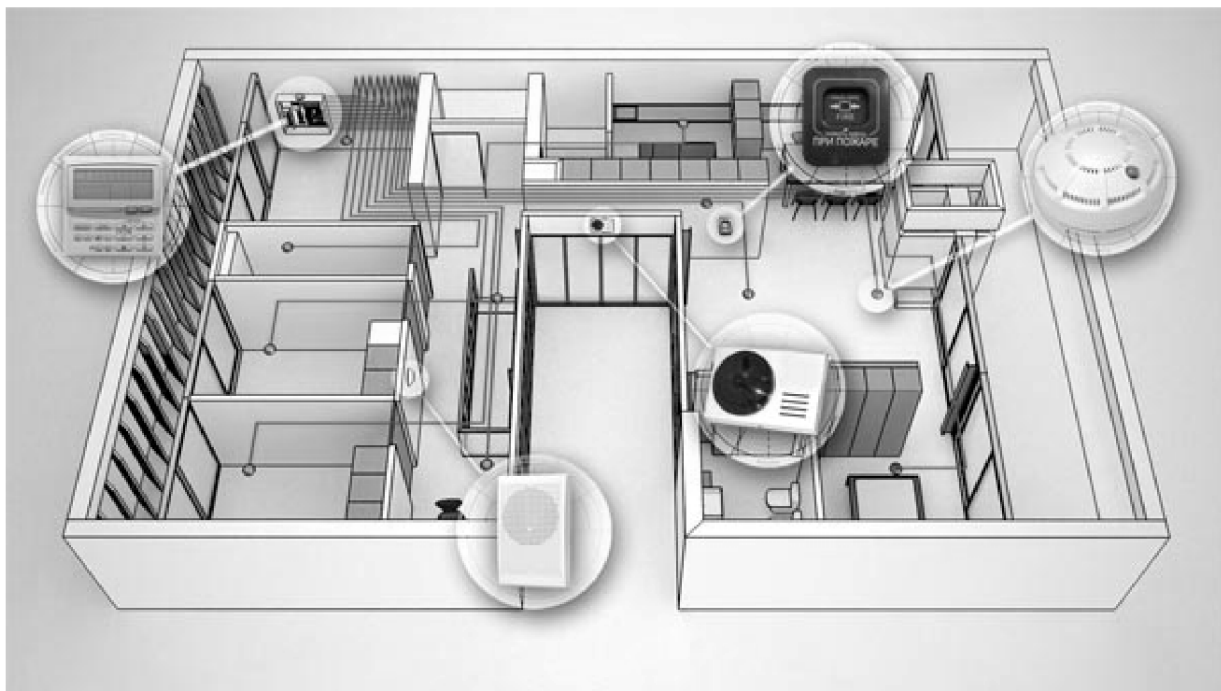


Рисунок 1.3 – Комплектація комплексної системи охоронної сигналізації

Активація/деактивація охорони може здійснюватися традиційно (кодова панель, замки), через брелок/передавач або мобільний телефон. Водночас віддалене керування створює типові ризики (втрата пристрою, компрометація облікового запису, шкідливе програмне забезпечення), тому сучасні рішення доповнюються механізмами блокування доступу, резервними каналами керування та централізованим зберіганням подій і записів.

1.4 Огляд та порівняння побутових систем охоронної сигналізації

Наразі на українському ринку представлено велику кількість систем домашньої охоронної сигналізації. Коротко розглянемо системи сигналізації від провідних виробників і проаналізуємо їхні функції та основні характеристики [2].

1.4.1 Безпроводна охоронна сигналізація MAKS PRO

MAKS PRO – це система, призначена для захисту критично важливих об'єктів (рис. 1.4). Вона може працювати автономно або у взаємодії з пультом охорони. Керування налаштуваннями та повний контроль над системою можуть здійснюватися з мобільних пристроїв під керуванням iOS та Android [8].

Ключовою особливістю MAKS PRO є здатність автоматично переходити в режим енергозбереження під час живлення від акумулятора у разі відключення електроенергії. Повідомлення передаються через кілька каналів зв'язку: GSM/GPRS та Ethernet. Система MAKS PRO є масштабованою та розрахована на підключення великої кількості пристроїв. Вона може працювати з до двохсот різними пристроями, такими як датчики, брелоки, клавіатури, детектори тощо.



Рисунок 1.4 – Безпроводна охоронна сигналізація MAKS PRO

1.4.2 Безпроводна сигналізація Kit GSM

Kit GSM – це бездротова GSM-система сигналізації, яка після виявлення вторгнення може негайно подати сигнал тривоги, здійснити голосовий дзвінок та надіслати текстове повідомлення на вказаний номер телефону (рис. 1.5).

Система виготовлена компанією ATIS і підтримує два способи керування: за допомогою брелока або смартфона [9].

Ця система використовує GSM-інтерфейс як основний канал зв'язку. Вбудований літєвий акумулятор забезпечує безперебійну роботу всіх компонентів у разі відключення електроживлення. РК-екран виконує роль інтерфейсу користувача, на якому відображається важлива інформація про стан системи.

Передавання тривожних повідомлень і службових даних здійснюється через мобільну мережу з використанням стандартних протоколів обміну, що забезпечує віддалений доступ до системи. Конструкція передбачає можливість налаштування параметрів зв'язку та інформування користувача про події й поточні режими роботи.



Рисунок 1.5 – Бездротова GSM-система охоронної сигналізації Kit GSM

1.4.3 Система безпеки Ajax StarterKit

StarterKit – це охоронна система, призначена для запобігання проникненню злоумисників у будинок через двері та вікна (рис. 1.6). Система використовує технології Ethernet та GSM для надсилання сигналів тривоги на пульт охорони та смартфон користувача. Керування системою здійснюється через мобільний застосунок [10].



Рисунок 1.6 – Стартовий комплект охоронної системи Ajax StarterKit

Система працює, опитуючи чутливі датчики, які контролюють стан дверей і вікон та виявляють активність у приміщеннях. Центральний блок StarterKit відповідає за надсилання тривожних повідомлень.

Основні компоненти системи можуть бути розширені шляхом підключення додаткових датчиків для виявлення затоплення та пожежі. Крім того, StarterKit можна інтегрувати з відеокамерами та засобами автоматизації.

Оброблення сигналів від сенсорів виконується за заданими правилами, що дає змогу зменшити кількість хибних спрацювань і своєчасно формувати події тривоги. У разі інциденту система може активувати попередньо налаштовані сценарії реагування та забезпечувати інформування користувача про зміни стану в реальному часі.

1.4.4 Безпроводна побутова охоронна сигналізація Ajax HomeSiren

HomeSiren – це бездротова система домашньої сигналізації, яка подає сигнал тривоги під час спрацювання датчика. Її встановлюють у приміщенні для відлякування зломисників або попередження про небезпеку [1].

Система дає змогу користувачам обирати гучність і тривалість звукового сигналу під час спрацювання датчика. За потреби сигналізацію можна підключити до зовнішнього світлодіодного індикатора, який розміщують поза межами приміщення для контролю стану системи безпеки (рис. 1.7).



Рисунок 1.7 – Модуль-сирена у складі побутової безпроводної сигналізація Ajax HomeSiren

На завершення, на підставі проведеної оцінки та аналізу систем безпеки можна зробити висновок, що більшість розглянутих пристроїв подають звукові та візуальні сигнали тривоги під час спрацювання датчиків. Окремі моделі вищого класу також дають змогу користувачам отримувати SMS-сповіщення на смартфон.

Отже, можна вважати, що розробка домашньої системи сигналізації на основі технології GSM є одним із найефективніших способів досягнення поставленої мети.

РОЗДІЛ 2

СТРУКТУРНО-АПАРАТНА РЕАЛІЗАЦІЯ ПОБУТОВОЇ СИСТЕМИ ОХОРОННОЇ СИГНАЛІЗАЦІЇ

2.1 Структурна модель системи побутової охоронної сигналізації

Під час розробки системи охоронної сигналізації було застосовано принцип модульного проєктування, за яким систему поділено на кілька модулів, кожен з яких відповідає за виконання певної функції. Загальна структура та функціональна схема домашньої системи охоронної сигналізації наведені на рис. 2.1.

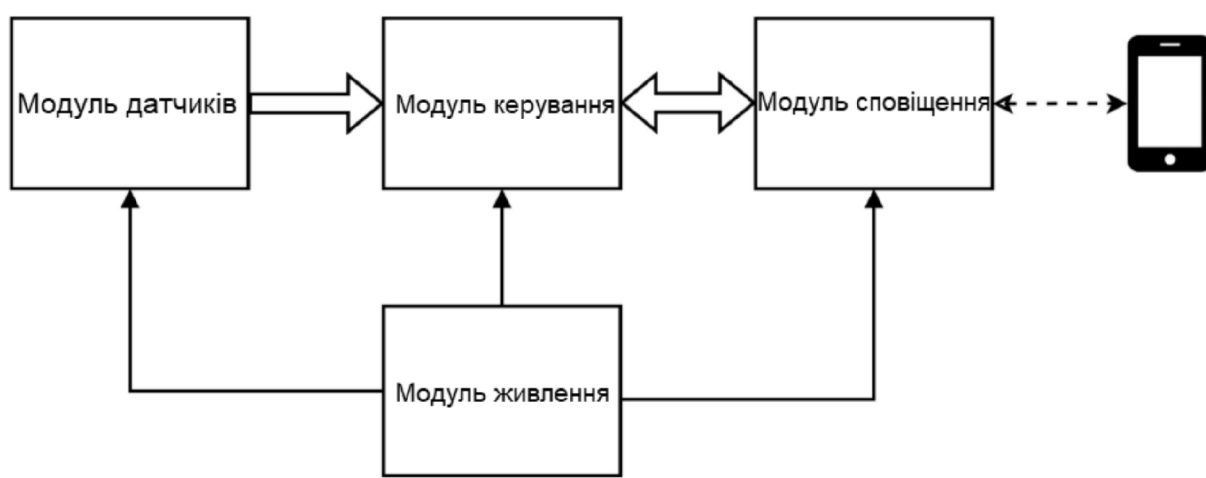


Рисунок 2.1 – Загальна структурно-функціональна модель розробленої побутової системи сигналізації

Система складається з чотирьох модулів:

- модуль датчиків;
- модуль керування;
- модуль сповіщення;
- модуль живлення.

Оскільки метою охоронної системи є моніторинг умов у приміщенні, будемо використовувати датчики об'єднані в окремий модуль. А для обробки отриманих від них даних розробимо модуль керування.

Для автономної роботи системи потрібні акумуляторна батарея, відповідний перетворювач та схема заряджання. Усі ці компоненти можуть бути об'єднані в одному конструктивному елементі – модулі живлення. Для ефективного реагування та оповіщення про зловмисні дії доцільно виділити окремий модуль сповіщення. Детальна структурна схема домашньої охоронної сигналізації наведена на рис. 2.2.



Рисунок 2.2 – Деталізована структурна схема модулів системи охоронної сигналізації

Модуль датчиків призначено для отримання інформації про стан приміщення та передавання відповідної інформації до модуля керування. Модуль включає такі датчики:

- датчик відкриття дверей;
- датчик розбиття скла;
- інфрачервоний датчик руху.

Цей набір датчиків надає модулю керування вичерпну інформацію про стан контрольованого приміщення та спроби несанкціонованого проникнення. Датчики можуть житися від різних джерел, тому їх встановлення не потребує окремого зовнішнього джерела живлення.

Датчик відкриття дверей визначає зміну стану дверей із закритого на відкритий. Двері є однією з основних точок входу для зломисників, тому датчики, що контролюють їхній стан, належать до найважливіших компонентів системи охоронної сигналізації.

Датчик руху контролює стан приміщення. Виявивши джерело інфрачервоного випромінювання, він негайно активується та надсилає відповідний сигнал до блока керування.

Датчик розбиття скла контролює стан вікон, які також можуть бути шляхом несанкціонованого проникнення. У разі розбиття віконного скла датчик фіксує акустичні коливання та надсилає відповідний сигнал до блока керування.

Таким чином, завдяки вибору відповідних датчиків можна контролювати всі основні маршрути проникнення зломисників та фіксувати їхню активність у приміщенні.

Модуль керування містить такі функціональні компоненти:

- плата керування на базі мікроконтролера;
- матрична клавіатура;
- контролер I²C;
- РК-дисплей.

Плата керування на базі мікроконтролера забезпечує взаємодію між усіма її складовими. Матрична клавіатура разом із РК-дисплеєм формує інтерфейс користувача для введення паролів, які використовуються для постановки та зняття системи з охорони, а також для зміни паролів. У системі застосовується дванадцятиклавішна клавіатура, організована у вигляді матриці 3×4 з клавішами на перетинах. Контролер I²C дає змогу зменшити кількість провідників, що підключають РК-дисплей.

Модуль сповіщення містить такі компоненти:

- GSM-модуль;
- п'єзоелектричний динамік;
- світлодіод.

GSM-модуль передає дані до віддаленого центру моніторингу та надсилає сповіщення власнику будинку на смартфон. П'єзоелектричний динамік подає звуковий сигнал під час спрацювання сигналізації. Світлодіодний індикатор відображає поточний стан сигналізації.

2.2 Вибір елементної бази системи охоронної сигналізації

2.2.1 Елементи модуля керування

Як основний елемент модуля керування розробленою системою було обрано плату розробки Arduino Uno. Такий вибір зумовлено її низькою вартістю та наявністю великої кількості додаткових модулів і програмних бібліотек. Зовнішній вигляд цього модуля показано на рис. 2.3.

Платформа Arduino Uno має шість аналогових вхідних контактів і чотирнадцять цифрових контактів загального призначення (шість із них можна використовувати для генерації ШІМ), а також інтерфейси USB та ICSP для програмування мікроконтролера та взаємодії із зовнішніми пристроями. Плата

Arduino Uno може житися кількома способами: через USB або від зовнішнього джерела живлення. З огляду на те, що цю платформу планується використовувати в системі сигналізації (яка, згідно зі специфікаціями, повинна мати можливість автономної роботи), живлення здійснюватиметься від зовнішнього акумулятора.

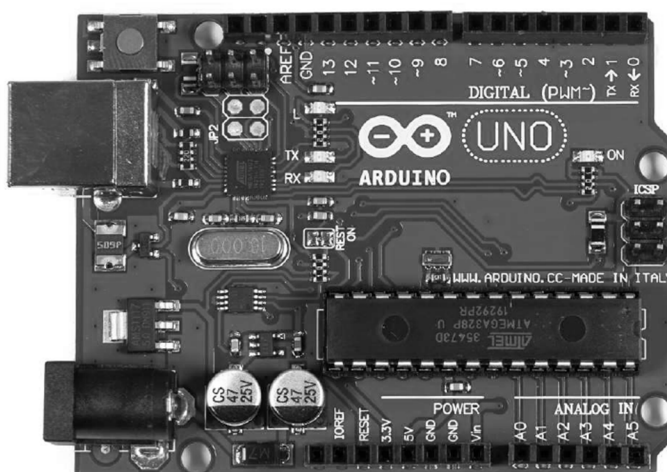


Рисунок 2.3 – Плата керування Arduino Uno

Платформа Arduino Uno побудована на базі 8-бітного мікроконтролера ATmega328P, його розпіновку наведено на рис. 2.4.

(PCINT14/RESET) PC6	1	28	PC5 (ADC5/SCL/PCINT13)
(PCINT16/RXD) PD0	2	27	PC4 (ADC4/SDA/PCINT12)
(PCINT17/TXD) PD1	3	26	PC3 (ADC3/PCINT11)
(PCINT18/INT0) PD2	4	25	PC2 (ADC2/PCINT10)
(PCINT19/OC2B/INT1) PD3	5	24	PC1 (ADC1/PCINT9)
(PCINT20/XCK/T0) PD4	6	23	PC0 (ADC0/PCINT8)
VCC	7	22	GND
GND	8	21	AREF
(PCINT6/XTAL1/TOSC1) PB6	9	20	AVCC
(PCINT7/XTAL2/TOSC2) PB7	10	19	PB5 (SCK/PCINT5)
(PCINT21/OC0B/T1) PD5	11	18	PB4 (MISO/PCINT4)
(PCINT22/OC0A/AIN0) PD6	12	17	PB3 (MOSI/OC2A/PCINT3)
(PCINT23/AIN1) PD7	13	16	PB2 (SS/OC1B/PCINT2)
(PCINT0/CLKO/ICP1) PB0	14	15	PB1 (OC1A/PCINT1)

Рисунок 2.4 – Розташування та призначення виводів мікроконтролера ATmega328P

ATmega328P – це мікроконтролер, що використовує розширену RISC-архітектуру, яка характеризується високою продуктивністю та високою щільністю коду. Він має 32 КБ флеш-пам'яті, з яких 500 байт відведено для зберігання завантажувача. Крім того, ATmega328P містить 1 КБ EEPROM та 2 КБ SRAM. Мікроконтролер працює на тактовій частоті 16 МГц, яка формується вбудованим кварцовим генератором.

Мікроконтролер ATmega328P має вбудований 10-бітний АЦП, що є однією з ключових причин вибору саме цієї моделі. Він також підтримує інтерфейси I2C, SPI та UART.

РК-екран у системі безпеки використовується для відображення стану датчиків і взаємодії з користувачем під час введення пароля при постановці приміщення під охорону та зняття його з охорони. Зовнішній вигляд екрана показано на рис. 2.5.

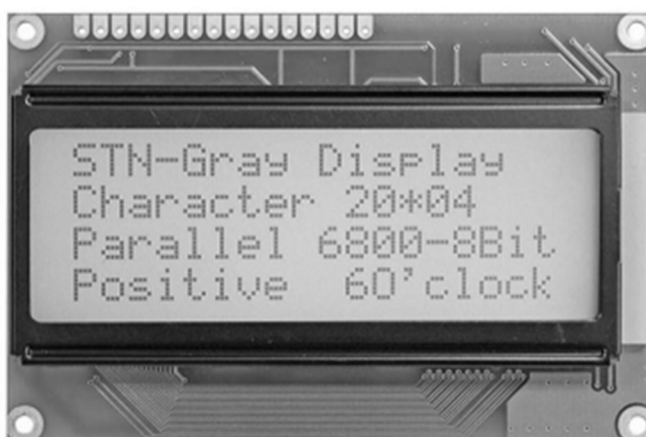


Рисунок 2.5 – РК-дисплей для індикації стану системи охоронної сигналізації

Контролер HD44780 відповідає за роботу дисплея та отримує дані від платформи Arduino через модуль I²C, призначений для економії виводів мікроконтролера та спрощення процесу передавання інформації на РК-екран у роботі використовується модуль I²C на базі мікросхеми контролера введення/виведення PCF8574T. Зовнішній вигляд модуля I²C показано на рис. 2.6.

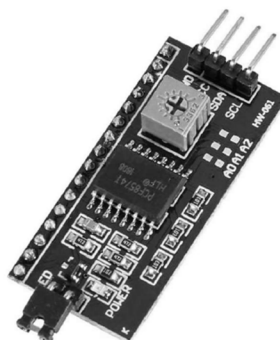


Рисунок 2.6 – Модуль інтерфейсу I²C для підключення РК-індикатора

Виходи SDA та SCL підключаються до відповідних входів мікроконтролера Arduino. Цими лініями інформація передається до контролера I²C і, зрештою, на РК-дисплей.

Клавіатура в цій системі призначена для введення пароля доступу під час зняття приміщення з охорони. Крім того, її можна використовувати для зміни системних налаштувань, зокрема оновлення пароля доступу. Для цих завдань доцільно застосувати модуль, що містить 12 мембранних клавiш. Клавіатура виконана у вигляді матриці 3×4, де клавiші розташовані на перетинах рядків і стовпців. На рис. 2.7 наведено зовнішній вигляд дванадцятиклавiшної мембранної клавіатури.

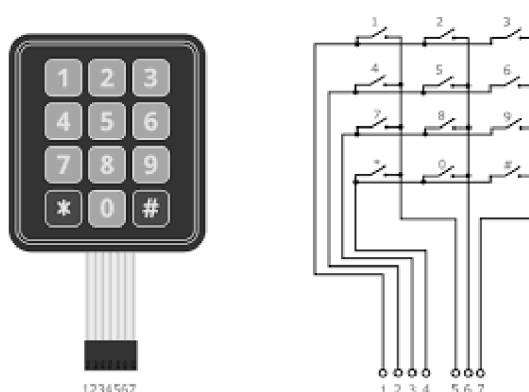


Рисунок 2.7 – Матрична мембранна клавіатура 3×4 для введення пароля

Виводи модуля клавіатури підключені до порту мікроконтролера: три з них (5-7) використовуються для сканування, а чотири (1-4) – для опитування стану клавiш.

2.2.2 Елементи модуля датчиків

Для виявлення несанкціонованого вторгнення в цій системі безпеки використовується піроелектричний інфрачервоний (PIR) датчик руху на базі модуля HC-SR501. Цей датчик здатний виявляти рух людей у навколишньому середовищі в межах своєї зони чутливості. Принцип його роботи полягає у вимірюванні кількості інфрачервоного випромінювання, що випромінюється живими організмами. Крім того, датчик може реагувати й на інші об'єкти, які генерують тепло. Зовнішній вигляд датчика руху показано на рис. 2.8.

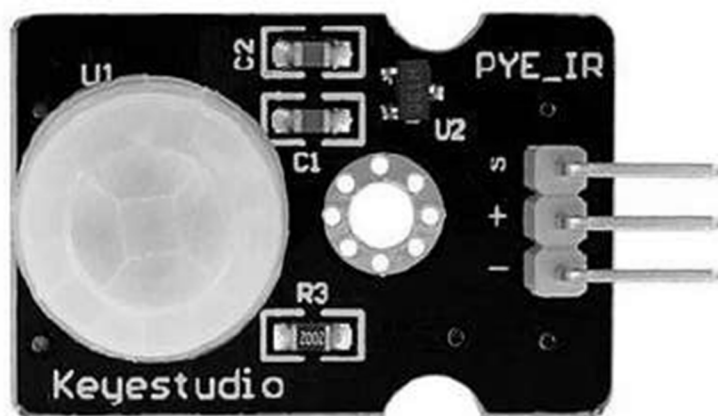


Рисунок 2.8 – Модуль PIR-датчика руху HC-SR501

Цей сенсор оснащено лінзою Френеля, яка фокусує інфрачервоне випромінювання на піроелектричний датчик. Датчик вважається пасивним, оскільки виявляє рух без потреби у додатковому джерелі енергії, використовуючи лише енергію, що випромінюється самим об'єктом.

Сенсорний елемент складається з двох чутливих компонентів. Мікросхема, що керує модулем, реєструє зміни сигналів від цих двох компонентів і, на основі характеру цих змін, виявляє рухомі об'єкти, які випромінюють інфрачервоне випромінювання. Цей модуль має невеликі розміри, простий у використанні, є дуже надійним і споживає мало енергії. Основні технічні параметри модуля датчика руху наведено в табл. 2.1.

Таблиця 2.1 – Основні технічні характеристики PIR-датчика руху HC-SR501

Характеристика	Діапазон значень
Сила струму споживання, мкА	50
Напруга живлення, В	4,5-20
Напруга логічного рівня, В	3,3

Це робить його придатним для використання у пристроях, що живляться від автономного джерела живлення. Чутливість модуля зменшується зі збільшенням відстані, тому важливо уникати розміщення поблизу джерел тепла та сильного світла, яке потрапляє на поверхню лінзи датчика.

Ще одним елементом блоку датчиків охоронної системи розумного будинку є датчик відкриття дверей. Це геркон, яким керують за допомогою магнітного поля. Зовнішній вигляд датчика відкриття дверей МС-38 показано на рис. 2.9.



Рисунок 2.9 – Герконовий датчик відкриття дверей МС-38

Датчик має номінальну потужність 10 Вт і допускає максимальний струм 500 мА. Геркон МС-38 характеризується відстанню спрацьовування до 18 мм із похибкою близько 6 мм. Цей датчик є нормально замкнутим, тобто його контакти замкнені за наявності магнітного поля.

Коли двері зачинені й магніт розташований поруч із датчиком, контакти замкнені, а коли двері відчиняються, магніт віддаляється, і контакти розмикаються.

У цій системі як датчик розбиття скла використовується акустичний модуль KY-037. Цей модуль можна налаштувати для реагування на певні типи звукових сигналів. Зовнішній вигляд датчика KY-037 показано на рис. 2.10.

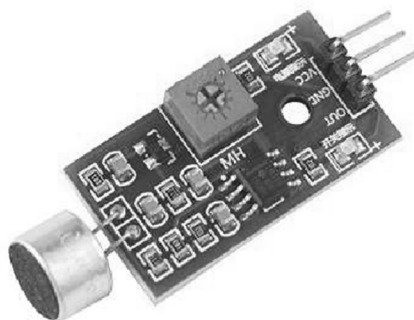


Рисунок 2.10 – Модуль KY-037 для виявлення звуку розбитого скла

Датчик KY-037 працює за принципом виявлення впливу звукових хвиль на діафрагму мікрофона, що змушує її коливатися. Ці коливання змінюють ємність конденсатора, унаслідок чого змінюється напруга на виході звукового датчика відповідно до характеристик звукового сигналу.

Модуль KY-037 призначений для виявлення сильних звукових сигналів, зокрема звуку розбитого скла. За умови правильного налаштування він практично не реагує на тихіші шуми, такі як звичайна розмова людей.

2.2.3 Елементи модуля сповіщення

Для надсилання користувачам повідомлень про надзвичайні ситуації на об'єктах, що охороняються, було обрано GSM-модуль SIM800L, зовнішній вигляд якого показано на рис. 2.11. Цей модуль функціонує майже так само, як мобільний телефон. За допомогою SIM800L можна здійснювати та приймати дзвінки, надсилати текстові повідомлення та підключатися до Інтернету з використанням таких протоколів, як TCP/IP та GPRS. Крім того, модуль підтримує чотиридіапазонні мережі GSM і базується на мікросхемі SimCom SIM800L.



Рисунок 2.11 – GSM-модуль SimCom SIM800L

Модуль SIM800L має вбудовану антену, однак для покращення якості сигналу можна підключити зовнішню антену. На нижній частині плати модуля розташовано роз'єм для встановлення SIM-картки. Обмін даними з мікроконтролером здійснюється через інтерфейс UART із максимальною швидкістю передавання даних 11520 біт/с. Призначення виводів GSM-модуля SIM800L наведено на рисунку 2.12.

Підключення до послідовного порту мікроконтролера має певні особливості: лінію RXD не можна під'єднувати безпосередньо до GSM-модуля, оскільки цифровий вихід мікроконтролера ATmega328 має логічний рівень 5 В, тоді як модуль SIM800L працює при напрузі 3,3 В. Тому рекомендується використовувати схему подільника напруги для зниження її рівня. Вона складається з двох резисторів номіналом 5 кОм та 10 кОм.

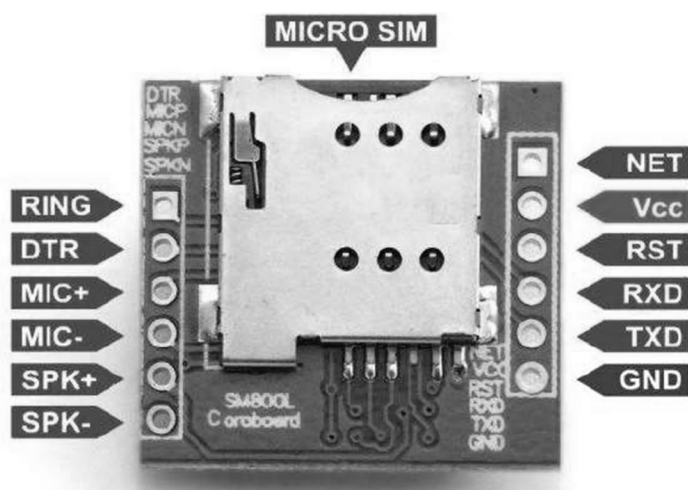


Рисунок 2.12 – Позначення виводів GSM-модуля SimCom SIM800L

Перед запуском GSM-модуля необхідно вставити SIM-картку у відповідний роз'єм на платі та підключити антену. Модуль має максимальне споживання струму до 2 А, тому його неможливо живити безпосередньо від мікроконтролера. Він розрахований на живлення в діапазоні напруг від 3,3 В до 4,4 В, тож може працювати від звичайного літієвого акумулятора.

У розробленій системі для формування звукового сповіщення під час активації датчика було обрано п'єзоелектричний модуль. Він перетворює команди, отримані від мікроконтролера, на звуковий сигнал. Зовнішній вигляд п'єзоелектричного модуля показано на рис. 2.13.

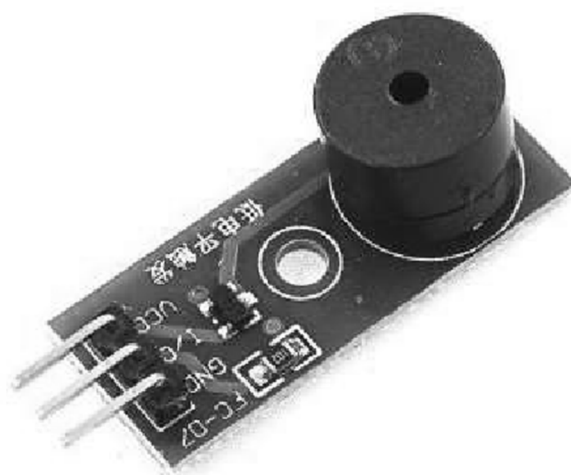


Рисунок 2.13 – П'єзоелектричний звуковий модуль для формування сигналу тривоги

П'єзоелектричний вібратор являє собою металеву пластину, покриту електропровідним керамічним шаром. Принцип його роботи ґрунтується на п'єзоелектричному ефекті: під час проходження електричного струму металева пластина деформується. Якщо до неї прикласти змінну напругу, виникають механічні коливання, які створюють звуковий сигнал потрібної частоти. Для цього в конструкцію п'єзоелектричного вібратора вбудовано генератор звукової частоти. Основні параметри п'єзоелектричного вібратора наведено в табл. 2.2.

Таблиця 2.2 – Основні характеристики п'єзоелектричного звукового модуля

Характеристика	Діапазон значень
Випромінювана частота, Гц	2300
Сила струму споживання, мА	до 30
Напруга живлення, В	5

Релейні модулі є ключовими компонентами охоронної систем «розумного будинку», які дають змогу керувати потужними зовнішніми пристроями, зокрема елементами звукової та світлової індикації. Вони є невід'ємною частиною системи, забезпечуючи зручне та ефективне керування побутовими та інженерними пристроями.

Релейний модуль складається з електромагнітного реле, яке здійснює підключення або відключення живлення навантаження. Він призначений для приймання та оброблення сигналів низького струму, зокрема таких, що генеруються мікроконтролером. Модуль зазвичай має кілька релейних виходів, що дає змогу одночасно керувати різними пристроями. На рис. 2.14 показано зовнішній вигляд такого релейного модуля.

Релейний модуль працює на основі створення електромагнітного поля для перемикавання контактів реле. Коли на котушку реле подається сигнал низького струму, електромагніт змушує контакти перемикатися, підключаючи або відключаючи потужний пристрій, під'єднаний до реле.



Рисунок 2.14 – Релейний модуль для підключення периферійного обладнання

2.2.4 Елементи модуля живлення

Згідно з технічними характеристиками, система охоронної сигналізації повинна мати можливість автономної роботи та живитися від батареї. Тому в розробленій системі передбачено пристрій для заряджання акумулятора. Для цієї мети обрано модуль на базі мікросхеми TP4056 (рис. 2.15). Процес заряджання батареї подібний до заряджання смартфона: після завершення заряджання загоряється світлодіодний індикатор. Модуль може живитися через роз'єм microUSB або через відповідні контактні площадки, до яких можна припаяти дроти.



Рисунок 2.15 – Зарядний модуль TP4056 для літієвого акумулятора системи

2.3 Розробка електричної принципової схеми системи побутової охоронної сигналізації

На рисунку 2.16 наведено електричну схему домашньої системи охоронної сигналізації, розроблену в програмі EasyEDA.

Схема може живитися від двох джерел: стандартного джерела живлення через роз'єм DC1 або від модуля керування зарядом/розрядом U7 акумулятора B1. Оскільки GSM-модуль SIM800L працює за напруги 3,3 В, до складу схеми введено стабілізатор напруги LM390IT, позначений як U4.

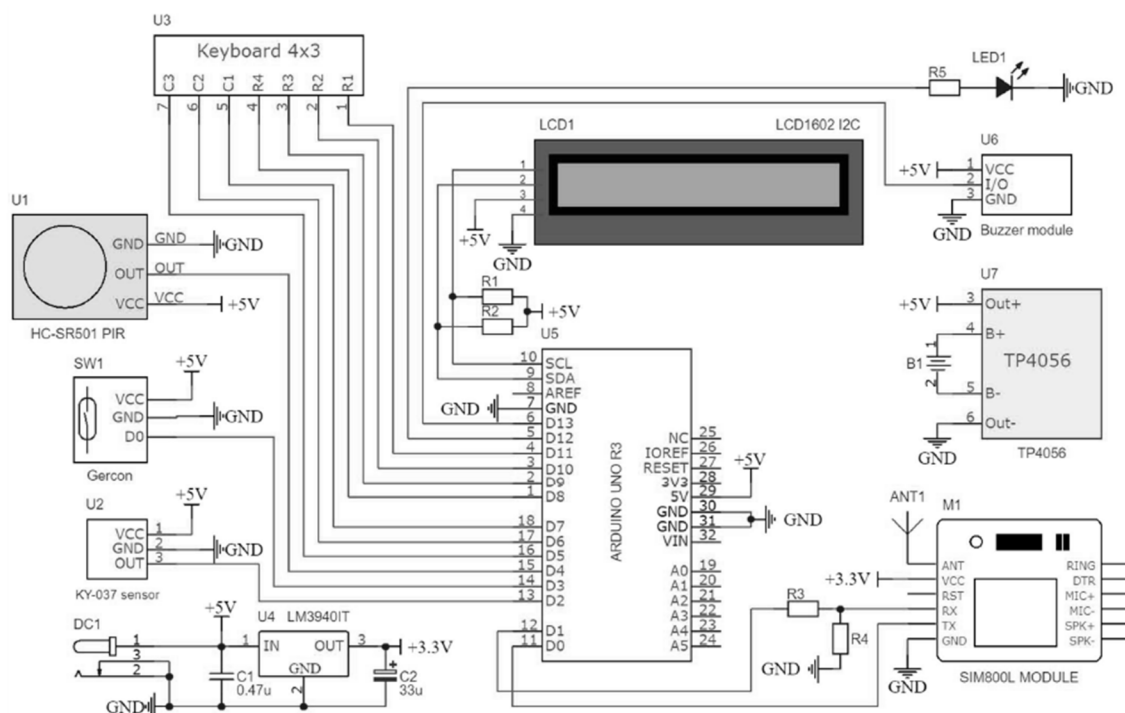


Рисунок 2.16 – Принципова електрична схема охоронної системи розумного будинку

Виходи датчика руху (U1), датчика відкриття дверей (SW1) та датчика розбиття скла (U2) підключені до цифрових входів платформи Arduino Uno, позначених на схемі як U5. Модуль матричної клавіатури U3 має сім контактів: три для підключення стовпців клавіатури до входів мікроконтролера та чотири для підключення її рядків.

ПК-дисплей LCD1 інтегрований із модулем I²C та обмінюється даними з мікроконтролером через контакти SDA і SCL. Резистори R1 та R2 номіналом 10 кОм підтягують ці лінії до рівня +5 В, що забезпечує коректну роботу інтерфейсу I²C.

GSM-модуль M1 обмінюється даними з мікроконтролером платформи Arduino через інтерфейс UART. Оскільки напруги живлення модулів U5 та M1 різняться, резистори R3 і R4 утворюють дільник напруги для узгодження рівнів їхніх логічних сигналів. Антена ANT1 підключена до GSM-модуля M1 для покращення якості приймання та передавання радіосигналу.

РОЗДІЛ 3

АЛГОРИТМІЧНЕ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМИ ПОБУТОВОЇ ОХОРОННОЇ СИГНАЛІЗАЦІЇ

3.1 Вибір режимів роботи та розробка алгоритмів функціонування охоронної системи розумного будинку

Після активації системи управління охоронно розумного будинку розпочинається аналіз сигналів, що надходять до блока керування (який підключає авторизований пристрій та датчики). Мікроконтролер порівнює покази датчиків із пороговими значеннями, що відповідають нормальному стану та були задані під час конфігурації перед першим використанням системи. Якщо стан будь-якого датчика змінюється, блок керування негайно фіксує подію та формує сигнал для активації пристрою сповіщення. У цій системі пристрій сповіщення реалізовано у вигляді світлових та звукових сигналів. Крім того, GSM-модуль надсилає текстове повідомлення та/або здійснює телефонний дзвінок домовласнику, а за потреби – встановлює зв'язок з охоронною компанією, підключеною до системи сигналізації.

Щоб деактивувати систему безпеки, необхідно ввести відповідний пароль. Після цього користувач може зайти до будинку та змінити режим роботи системи. У цьому режимі датчики продовжують функціонувати, проте блок керування не реагує на зміни їхнього стану.

Програмне забезпечення мікроконтролера складається з двох основних частин. Перша частина виконується один раз одразу після ввімкнення мікроконтролера та використовується для налаштування цифрових виходів і послідовного порту. Друга частина виконується циклічно протягом усього часу роботи мікроконтролера. Блок-схеми алгоритму роботи системи управління охороною розумного будинку наведено на рисунках 3.1 та 3.2.

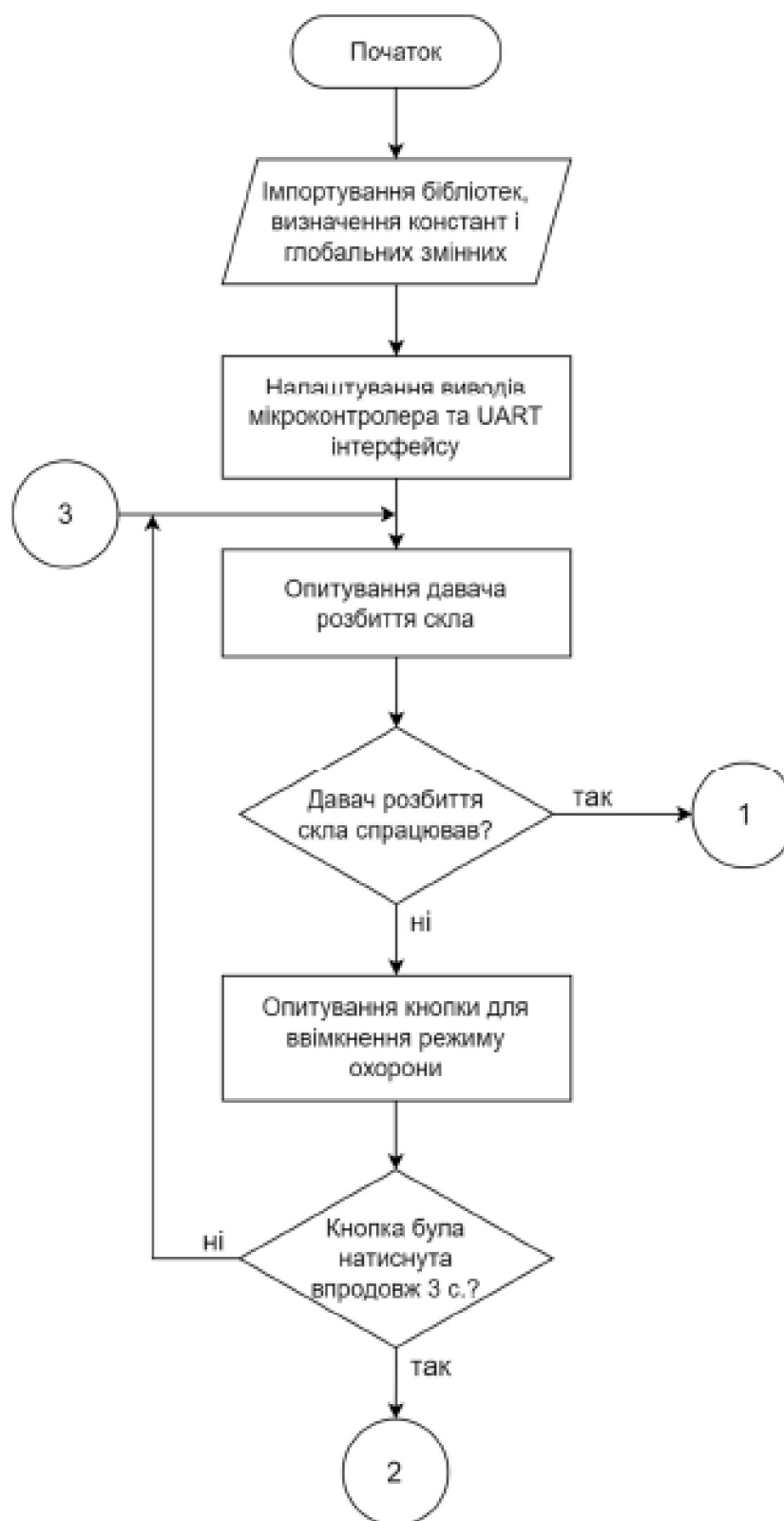


Рисунок 3.1 – Алгоритм функціонування програмного модуля управління охоронною системою розумного будинку (частина 1)

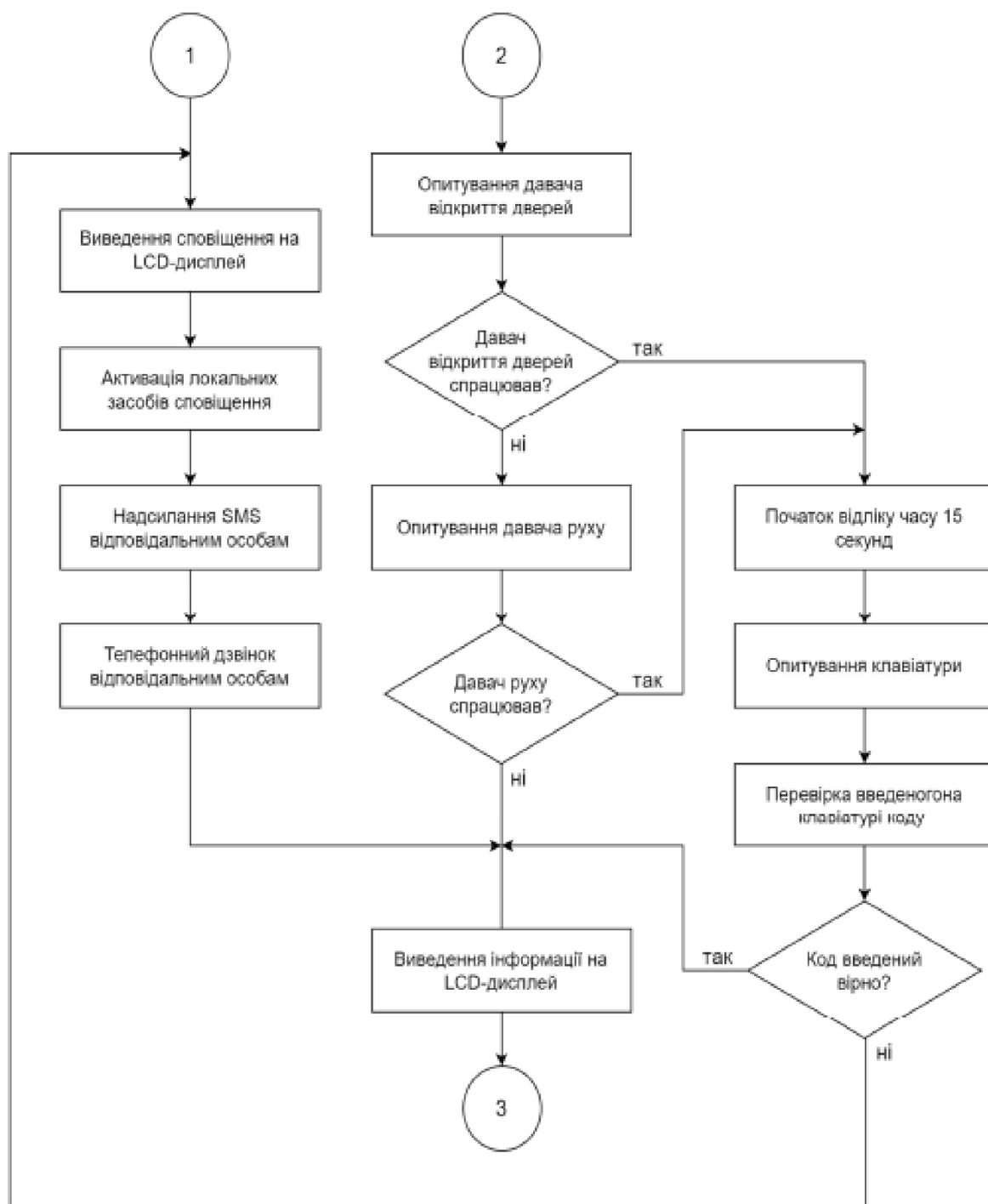


Рисунок 3.2 – Алгоритм функціонування програмного модуля управління охоронною системою розумного будинку (частина 2)

Спочатку програма імпортує необхідні бібліотеки та ініціалізує режими роботи виводів мікроконтролера. Блок-схема алгоритму програми містить кілька перевірок, три з яких пов'язані з опитуванням та аналізом показів датчиків, а дві – зі зчитуванням стану кнопок і клавіатури.

Для досягнення модульності та підвищення зручності супроводу програму поділено на такі частини:

- модуль опитування вхідних сигналів;
- модуль зміни стану системи;
- модуль обробки стану.

Залежно від завдання система управління охоронною системою розумного будинку може працювати в чотирьох режимах:

- режим очікування коли стан датчиків ігнорується, приміщення використовується у звичайному режимі;
- режим безпеки у якому усі датчики активні, а приміщення перебуває під охороною;
- режим тривоги у який система переходить якщо спрацює датчик руху або датчик відкриття дверей, легітимний користувач має 15 секунд для введення пароля;
- режим тригера у якому активується сповіщення.

Основна програма виконується у циклі, спочатку зчитуючи значення на всіх виводах мікроконтролера, до яких підключені датчики. До них належать як цифрові входи, так і входи, що використовуються для зчитування стану клавіатури. Після запису всіх даних у відповідні змінні програма переходить до етапу їх обробки, зокрема до обробки натискань на клавіатурі та стану кнопок. Одна з дванадцяти клавіш клавіатури використовується для перемикання режиму роботи системи з режиму «Очікування» в режим «Безпека». Для перемикання режимів необхідно натиснути й утримувати цю кнопку протягом 3 секунд, після чого залишити приміщення протягом 15 секунд. У цей час мікроконтролер не реагує на зміни стану датчиків, надаючи користувачу можливість вийти з кімнати та запобігаючи хибному спрацюванню сигналізації.

Спочатку програма перевіряє датчик розбиття скла. Якщо від цього датчика надходить сигнал, система переходить у режим «Тригер». Далі

аналізуються дані від датчика руху та датчика відкриття дверей. У разі спрацювання будь-якого з цих датчиків система переходить у режим «Тривога».

Окремий розділ програмного забезпечення використовується для налагодження. Він передає значення змінних через послідовний порт, фіксуючи показання датчиків та інформацію про поточний стан системи. Це дає змогу динамічно відстежувати зміну режимів роботи.

Наступний розділ коду реалізує модуль обробки режимів системи. Він виконує операції, що відповідають кожному режиму роботи, на основі заданих умов. Оскільки у «режимі захисту» п'єзоелектричний модуль і світлодіод не повинні бути увімкнені, на їхні виводи подається низький логічний рівень. У «режимі тривоги» запускається таймер зворотного відліку. Якщо правильний код не буде введено протягом заданого часу, система переходить у режим «Тригер». У цьому режимі на вивід, підключений до пристрою сповіщення, подається високий логічний рівень. За допомогою стандартної бібліотеки формується команда для надсилання SMS-повідомлення із заздалегідь визначеним текстом та здійснення виклику на вказаний номер користувача. Після виконання цієї частини коду потік керування повертається на початок циклу. Таким чином, система домашньої сигналізації безперервно контролює стан приміщення.

3.2 Програмна реалізація модулів керування системою побутової охоронної сигналізації

У цьому розділі описано функціональні можливості програмного забезпечення та програмний код, який виконується мікроконтролером для реалізації всіх функцій домашньої системи охоронної сигналізації.

Для використання клавіатури на початку програми задаються константи для обробки натискань клавіш (рис. 3.3).

```
// Піни Arduino, підключені до рядків матричної клавіатури 4x3
const int Row[] = {11, 10, 9, 8}; // виводи рядків

// Піни Arduino, підключені до стовпців клавіатури
const int Col[] = {7, 6, 5}; // виводи стовпців

// Таблиця відповідності натиснутої комбінації (рядок-стовпець) символу на клавіатурі
const char k3x4[3][4] = { // символи на клавіатурі
    {'1', '2', '3'},
    {'4', '5', '6'},
    {'7', '8', '9'},
    {'*', '0', '#'}
};
```

Рисунок 3.3 – Фрагмент коду з оголошенням констант для обробки натискань клавiш мембранної клавіатури

У функції `setup()` виводи мікроконтролера, підключені до рядків клавіатури, налаштовуються як цифрові виходи з високим рівнем, а виводи, підключені до стовпців клавіатури, – як цифрові входи з підтягуванням до логічної «1» (рис. 3.4).

```
// Налаштування ліній клавіатури: рядки робимо виходами й ставимо в HIGH
for (int i = 0; i <= 3; i++) {
    pinMode(Row[i], OUTPUT); // Виводи рядків як виходи
    digitalWrite(Row[i], HIGH); // Початковий стан рядків - логічна 1
}

// Налаштування стовпців клавіатури як входів з підтяжкою до VCC
for (int i = 0; i <= 2; i++)
    pinMode(Col[i], INPUT_PULLUP); // Виводи стовпців як входи з внутрішньою підтяжкою

Serial.begin(9600); // Запускаємо послідовний порт для діагностики
Serial.println("begin"); // Повідомлення про старт роботи програми
```

Рисунок 3.4 – Програмна ініціалізація виводів мікроконтролера для підключення клавіатури

У функції `loop()` на виводи рядків послідовно подається низький рівень напруги в циклі з періодом 50 мс, а виводи стовпців опитуються у вкладеному циклі. Якщо на виході стовпця фіксується логічний «0», вважається, що замкнулися *i*-й рядок і *j*-й стовпець, тобто натиснуто кнопку `k3x4(i, j)`.

Розглянемо програмну реалізацію виведення даних на РК-дисплей (рис. 3.5). На початку підключається бібліотека `LiquidCrystal_I2C`, яка забезпечує роботу з LCD-модулем за двопровідною шиною та спрощує підключення. Далі створюється об'єкт `lcd` із зазначенням I²C-адреси `0x3F` і параметрів екрана `16×2`, що відповідає 16 символам у двох рядках. Під час виконання функції `lcd.begin()` здійснюється запуск і підготовка дисплея до відображення тексту, а команда `lcd.backlight()` вмикає підсвічування для кращої видимості. Командою `lcd.print("Alarms")` на першому рядку виводиться заголовок, який інформує користувача про режим або призначення екрана. Далі `lcd.setCursor(0, 1)` переводить курсор на початок другого рядка, після чого друк пробілів фактично очищує або підготовлює цей рядок для подальшого динамічного виведення даних. Таким чином формується початковий стан інтерфейсу відображення, який буде оновлюватися в процесі роботи системи.

```
// Підключаємо бібліотеку для роботи з LCD по інтерфейсу I2C
#include <LiquidCrystal_I2C.h>

// Створюємо об'єкт lcd з I2C-адресою 0x3F, розміром 16 символів у 2 рядках
LiquidCrystal_I2C lcd(0x3F, 16, 2);

// Ініціалізація LCD-дисплея та виведення початкового тексту
lcd.begin();           // Запуск роботи LCD-модуля
lcd.backlight();       // Увімкнення підсвічування дисплея
lcd.print("Alarms");   // Виводимо напис у першому рядку
lcd.setCursor(0, 1);   // Переміщуємо курсор на початок другого рядка
lcd.print(" ");        // Очищуємо / заповнюємо другий рядок для подальшого тексту
```

Рисунок 3.5 – Ініціалізація РК-дисплея в програмі мікроконтролера

Оскільки GSM-модуль SIM800 обмінюється даними за допомогою протоколу UART, у програмі підключається бібліотека `SoftwareSerial`, яка дозволяє реалізувати додатковий послідовний порт на вибраних цифрових виводах мікроконтролера (рис. 3.6). Далі оголошується об'єкт `SIM800serial` із зазначенням ліній RX/TX, після чого в `setup()` ініціалізується апаратний порт `Serial` для діагностики та контролю запуску системи через монітор порту. Окремо

запускається програмний послідовний порт для модема зі швидкістю 9600 бод і надсилається тестова AT-команда, що використовується для перевірки готовності модуля до приймання команд. Такий підхід забезпечує паралельну роботу: відображення службових повідомлень на ПК та обмін керуючими командами з GSM-модулем.

```
// Підключаємо бібліотеку програмного послідовного порту
#include <SoftwareSerial.h>

// Оплошуємо програмний послідовний порт для модема SIM800 (RX, TX)
SoftwareSerial SIM800serial(0, 1);

void setup() {
    Serial.begin(9600);           // Ініціалізація апаратного порту для зв'язку з ПК
    Serial.println("Alarm!");     // Повідомлення в монітор порту про запуск системи

    SIM800serial.begin(9600);     // Запуск програмного порту для модема SIM800
    SIM800serial.println("AT");   // Надсилання тестової AT-команди модему
}
```

Рисунок 3.6 – Фрагмент коду налаштування програмного UART для роботи з GSM-модулем

У функції loop() для надсилання та отримання даних використовуються функції available() та write() (рис. 3.7).

```
// Прозорий міст між апаратним портом Serial і модемом SIM800

if (Serial.available()) {        // Якщо з боку ПК є вхідні дані
    SIM800serial.write(Serial.read()); // Передаємо байт у модем SIM800
}

if (SIM800serial.available()) {  // Якщо модем SIM800 щось відправив
    Serial.write(SIM800serial.read()); // Виводимо байт у Serial (на ПК/монітор порту)
}
```

Рисунок 3.7 – Процес передавання й приймання даних через UART-інтерфейс

На рис. 3.8 показано реалізацію функції sms(text, phone), призначеної для надсилання SMS-повідомлення через GSM-модуль SIM800 за допомогою AT-команд. На початку роботи функції виводиться службове повідомлення в монітор порту, що дозволяє контролювати запуск процедури відправлення. Далі

модему передається команда AT+CMGS із номером одержувача, після чого виконується затримка для переходу SIM800 у режим введення тексту повідомлення. Текст SMS передається командою SIM800serial.print(text), а завершення введення ініціюється надсиланням символу Ctrl+Z (код 26), який є стандартним завершувачем повідомлення для SIM800. Після короткої паузи очікується підтвердження від модема, і в журнал виводиться повідомлення про завершення операції. Додаткова затримка наприкінці використовується для стабілізації обміну та уникнення конфліктів при наступних командах до GSM-модуля.

```
// Функція надсилання SMS-повідомлення через модем SIM800
void sms(String text, String phone)
{
    Serial.println("SMS send started");
    SIM800serial.println("AT+CMGS=\"" + phone + "\"");
    delay(1000);
    SIM800serial.print(text);
    delay(300);
    SIM800serial.print((char)26);
    delay(300);
    Serial.println("SMS send finish");
    delay(3000);
}

// Повідомляємо в порт про початок відправлення
// Надсилаємо AT-команду з номером одержувача
// Чекаємо, поки модем перейде в режим введення тексту
// Передаємо текст SMS
// Невелика пауза перед завершенням
// Надсилаємо Ctrl+Z (код 26) для завершення SMS
// Чекаємо підтвердження від модема
// Логуюємо завершення відправлення
// Пауза перед наступними операціями з модемом
```

Рисунок 3.8 – Функція надсилання SMS-повідомлень за допомогою модуля SIM800L

3.3 Реалізація дистанційного керування системою за допомогою DTMF-команд

Для набору телефонних номерів використовуються двотональні багаточастотні сигнали (DTMF). Вони генерують багаточастотні двотональні аналогові сигнали, які забезпечують автоматизовану телефонну сигналізацію між пристроями. Зокрема, такі сигнали можна використовувати для керування з'єднаннями між аналоговими пристроями (наприклад, між АТС та телефонним апаратом).

Сигнали DTMF також застосовуються, коли користувачі вручну вводять команди в різних системах, зокрема в голосових автовідповідачах. Команди DTMF широко використовуються на телевізійних каналах та комерційних радіостанціях, а також у системах охоронної сигналізації та розумного дому.

У розробленій системі команди DTMF використовуються для дистанційного керування сигналізацією через модуль SIM800L. Якщо номери збережені в пам'яті SIM-картки, їхні власники вважаються користувачами, які мають право вмикати та вимикати систему сигналізації. Номер з іменем ADMIN вважається номером адміністратора. Якщо в пам'яті SIM-картки немає запису ADMIN, перший користувач, який зателефонує на нову SIM-картку, автоматично отримує права адміністратора, а його номер зберігається в телефонній книзі.

Лише адміністратор може надсилати SMS-повідомлення та команди DTMF. У розробленій охоронній системі використовуються команди DTMF, наведені на рис. 3.9.

```
// Перелік команд, що приходять від користувача у вигляді DTMF-кодів
// Кожне значення відповідає окремій дії охоронної системи
enum
{
    GUARD_ON = 1,      // 1# - встановлення системи на охорону
    GUARD_OFF,         // 2# - зняття системи з охорони
    GPRS_ON_OFF,       // 3# - увімкнути/вимкнути GPRS-з'єднання
    SMS_ON_OFF,        // 4# - увімкнути/вимкнути надсилання SMS
    TEL_ON_OFF,        // 5# - увімкнути/вимкнути дзвінок при тривозі
    GET_INFO,          // 6# - зібрати та відправити всі дані датчиків
    EMAIL_ADMIN_PHONE, // 7# - надіслати на e-mail номер адміністратора
    EMAIL_PHONE_BOOK,  // 8# - надіслати на e-mail телефонну книгу
    ADMIN_NUMBER_DEL,  // 9# - зробити поточний адміністраторський номер звичайним
    SM_CLEAR,          // 10# - видалити всі номери з SIM-карти
    MODEM_RESET,       // 11# - перезавантажити модем/модуль зв'язку
    BAT_CHARGE,        // 12# - показати інформацію про рівень заряду батареї
    CONNECT_ON_OFF     // 13# - інвертувати прапорець постійного з'єднання CONNECT_ALWAYS
};
```

Рисунок 3.9 – Перелік DTMF-команд для дистанційного керування системою сигналізації

GSM-модуль налаштовано на автоматичну відповідь на вхідні дзвінки з номера керування. Ця функція використовується для виконання DTMF-команд. Дзвінки з інших номерів будуть автоматично розірвані. Адміністратор може надсилати DTMF-команди. Якщо команду прийнято, система розірве поточний дзвінок. Звіт про виконання команди буде надіслано на вказану адресу електронної пошти. Після цього потрібно ввести будь-які цифри та символ #, щоб вказати, що введення команди завершено. Нарешті, модуль завершить поточний дзвінок і почне виконувати отриману команду.

3.4 Дослідження експлуатаційних характеристик і надійності розробленої охоронної системи

Для оцінки працездатності запропонованої системи виконано прикладне дослідження для кількісної оцінки імовірності виявлення вторгнень, частоти хибних спрацювань, часової затримки реагування та доставки сповіщень, надійності віддаленого керування.

Мета проведеного дослідження – експериментально визначити, наскільки стабільно система виявляє типові загрози (рух у зоні контролю, відчинення дверей, звук «розбиття скла») та як швидко/надійно формує локальне й віддалене сповіщення через SIM800L.

Дослідження проводилось в наступних умовах: система встановлювалась у приміщенні розміром 4×5 м з одними дверима. Датчик руху було спрямовано на зону проходу; геркон МС-38 закріплено на дверному полотні; датчик КУ-037 – поблизу вікна. Окремо фіксуються три типи фонових впливів: протяги/коливання температури, побутові шуми (розмова, телевізор), випадкові вібрації (удари по столу тощо). Ефект розбиття вікна імітувався шляхом відтворення відповідної звукової доріжки за допомогою професійного мультимедійного обладнання.

Ключовими метриками дослідження є:

- ймовірність виявлення $PD = TP/(TP+FN)$, де TP – кількість коректних спрацювань на подію, FN – пропуски події;
- частота хибних спрацювань $FPR = FP/(FP+TN)$ або у практичному вигляді «спрацювань за годину» у режимі «Безпека», де FP – кількість хибних спрацювань, TN – кількість коректних пропусків;
- час реакції T_{alarm} – час від моменту події (фіксованого спостерігачем) до переходу системи у режим «Тривога/Тригер»;
- затримка сповіщення T_{sms} – час від старту відправлення SMS (момент AT+CMGS у журналі) до фактичного отримання повідомлення на телефоні;
- надійність віддалених команд S_{dtmf} – частка успішно розпізнаних і виконаних DTMF-команд.

Спочатку проведено серію експериментальних досліджень, покликаних встановити особливості роботи елементів, що входять до складу модуля датчиків. У табл. 3.1 подано результати експериментального вивчення спрацювання датчика руху. Тригером для його спрацювання слугував контрольних проходів людини в полі зору датчика на відстані 1-7 метрів від самого датчика. У кожній точці виконано по 100 контрольних проходів, при цьому апаратна часова затримка виставлена на мінімум. Графічне представлення отриманих результатів відображено на рис. 3.10.

Таблиця 3.1 – Показники виявлення подій датчиком руху залежно від відстані

Відстань, м	Кількість спроб	Виявлено (TP)	Пропущено (FN)	Ймовірність виявлення, %
1	100	99	1	99.0
2	100	98	2	98.0
3	100	96	4	96.0
4	100	92	8	92.0
5	100	86	14	86.0
6	100	75	25	75.0
7	100	60	40	60.0

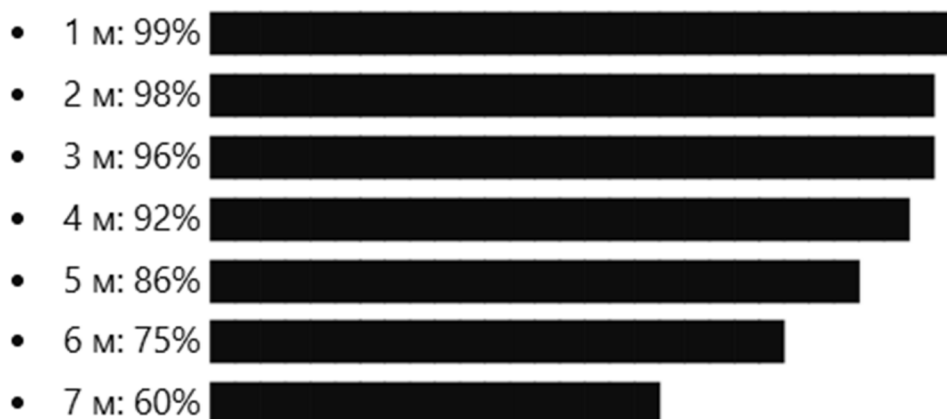


Рисунок 3.10 – Залежність спрацювання датчика руху від відстані до перешкоди

Аналіз результатів дослідження показав закономірне зниження P_D зі зростанням відстані. Практично це означає, що під час монтажу бажано орієнтувати датчик руху на ключові проходи на дистанції до 4–5 м, а у більших приміщеннях застосовувати інше розміщення або додатковий датчик.

Геркон МС-38 має відстань спрацювання до 18 мм, для експериментальної перевірки цього показника виконано 100 циклів «відкриття/закриття» та 200 контрольних перевірок у стані «двері зачинені». Результати експериментального дослідження подано у табл. 3.2

Таблиця 3.2 – Перевірка межі спрацювання датчика відчинення дверей МС-38

Показник	Значення
Кількість подій «відчинення»	100
Виявлено (TP)	100
Пропущено (FN)	0
Контрольних перевірок «без події»	200
Хибних спрацювань (FP)	0

Отже герконовий датчик у більшості випадків демонструє дуже високу відтворюваність і є «еталонним» для оцінки швидкості переходів системи у режим «Тривога».

Наступним етапом дослідження став аналіз впливу порогу чутливості на спрацювання датчика розбиття вікна. Для кожного порогу виконано 50 «позитивних» подій (імітація характерного звуку) і 200 «негативних» епізодів фонового шуму. Результати дослідження подано у табл. 3.3. А на рис. 3.11 зображено ROC-подібну криву, що відображає залежність TPR від FPR і відображено оптимальний поріг чутливості.

Таблиця 3.3 – Вплив порогу чутливості KY-037 на якість виявлення «розбиття скла»

Поріг (норм.)	TP	FN	FP	TN	TPR, %	FPR, %
0.30	49	1	44	156	98.0	22.0
0.40	48	2	30	170	96.0	15.0
0.50	46	4	18	182	92.0	9.0
0.60	43	7	10	190	86.0	5.0
0.70	36	14	4	196	72.0	2.0
0.80	28	22	2	198	56.0	1.0

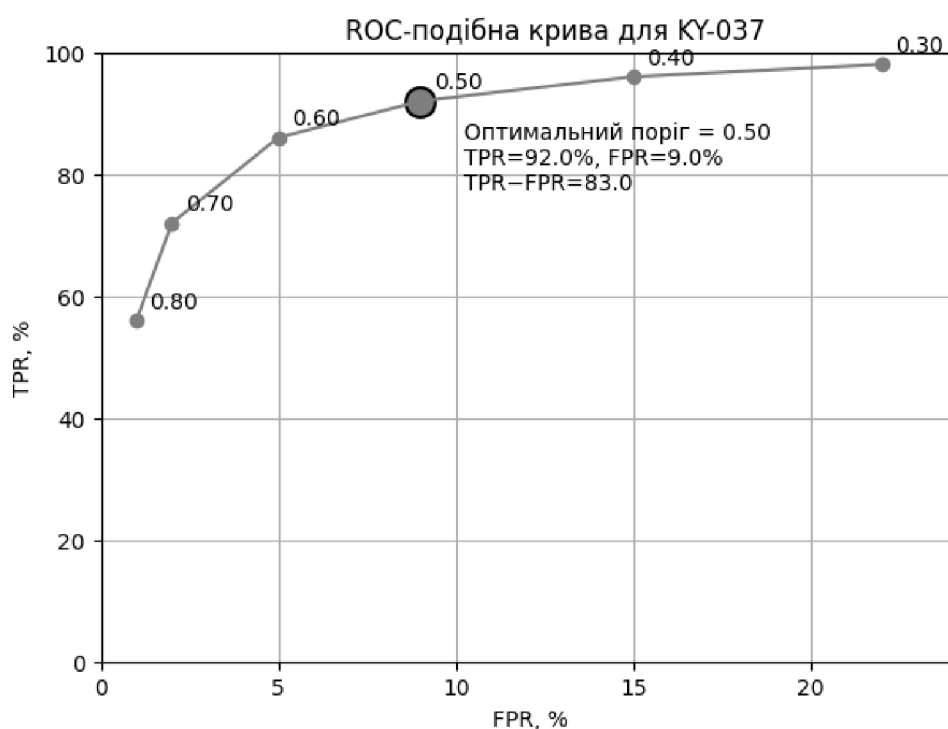


Рисунок 3.11 – ROC-подібна крива залежності TPR від FPR для різних порогів чутливості датчика KY-037

З отриманих результатів видно типовий компроміс: при низькому порозі майже немає пропусків, але багато хибних тривог; при високому – хибних мало, але зростає кількість пропусків. Для житлового середовища часто доцільний середній поріг (наприклад, 0.55–0.65) з додатковою програмною фільтрацією (коротке «підтвердження» події або аналіз повторюваності імпульсів), щоб зменшити FP без різкого падіння TPR .

Також проведено оцінювання часових характеристик каналу сповіщення через GSM-модуль SIM800L, а саме затримки доставки SMS-повідомлення залежно від якості приймання мережі оператора lifecell. Випробування виконувалися у межах одного приміщення, де змінювалися умови приймання сигналу за рахунок різного розміщення пристрою відносно вікна та конструктивних перешкод у кімнаті. Передавачем виступала розроблена охоронна система з підключеним SIM800L, приймачем – мобільний телефон, на який надходили тестові SMS. Надсилання повідомлень здійснювалося стандартним способом через AT-команди GSM-модуля, а моменти ініціювання відправлення фіксувалися у середовищі Arduino IDE через Serial Monitor: у момент формування події «тривога» та запуску процедури надсилання виводилась часова мітка/позначка, що використовувалася як початок відліку. Момент отримання SMS визначався за фактом появи повідомлення на телефоні, після чого різниця між часом ініціювання відправлення (за Serial Monitor) і часом отримання фіксувалася як затримка доставки T_{sms} . Результати дослідження подано у табл. 3.4.

Для порівняння було сформовано три режими якості зв'язку: висока якість приймання (пристрій у зоні найкращого прийому в кімнаті, як правило ближче до вікна), середня якість (розміщення у центральній частині кімнати) та низька якість (розміщення у зоні з найгіршим прийомом, у куті кімнати, ближче до капітальних стін). У кожному режимі виконувалася серія однакових відправлень SMS однакового змісту; між спробами витримувався інтервал, достатній для завершення попередньої операції та стабілізації роботи мережі. За результатами серій вимірювань для кожного режиму обчислювалися статистичні показники,

наведені в табл. 3.4: середнє значення, медіана, 95-й перцентиль (P95), а також мінімальне і максимальне значення затримки. Такий підхід дозволив оцінити не лише типову швидкодію сповіщення через lifecell у кімнатних умовах, а й характерні «гірші випадки», що є критичними для охоронних систем, де важлива гарантована доставка тривожного повідомлення у прийнятний час.

Таблиця 3.4 – Затримка доставки SMS залежно від якості GSM-зв'язку (SIM800L)

Якість сигналу	n	Середнє, с	Медіана, с	P95, с	Мін, с	Макс, с
Висока (антена, стабільний GSM)	30	10.8	9.8	16.9	5.0	18.2
Середня (кімната, 2–3 поділки)	30	18.5	18.5	27.0	6.4	31.1
Низька (підвал/кут, 0–1 поділка)	30	29.0	27.1	47.3	11.6	50.2

Затримка доставки SMS у GSM-мережі істотно залежить від умов приймання. Тому при інсталяції системи потрібно забезпечити достатній рівень сигналу (розміщення антени, уникнення екранування, стабільне живлення), а для критичних випадків – дублювання каналу сповіщення (наприклад, дзвінок + SMS).

На підставі наведених вимірювань можна стверджувати, що підсумовується, що розроблений модуль управління охоронною системою розумного будинку:

1. Достатньо високу ймовірність виявлення для типових сценаріїв «рух/двері», за умови коректного розміщення датчиків.
2. Найбільш «чутливим» до налаштувань є акустичний канал KY-037, тому він потребує підбору порогу та/або програмної фільтрації.
3. Час доставки SMS змінюється в широких межах і визначається умовами GSM-мережі та інсталяції, що узгоджується з вимогами до живлення SIM800L.

РОЗДІЛ 4

ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Можливість виникнення статичної електрики та заходи боротьби з нею

Статична електрика – це сукупність явищ, які пов'язані з виникненням та накопиченням вільного електричного заряду на ізольованих провідниках чи в об'ємі або на поверхні діелектриків. Підвищений рівень статичної електрики входить в категорію фізичних шкідливих і небезпечних виробничих факторів.

Суть електризації полягає в тому, що діелектрики за певних умов стають електрично зарядженими. При цьому заряди не зникають і не виникають, а переходять з одного електризованого тіла на інше, переміщуються в межах одного й того ж тіла чи накопичуються на поверхнях їх стикання. Статична електрика може появлятися на тілах і внаслідок індукції, тобто завдяки взаємодії на відстані.

Наслідки, які спричинені електризацією, демонструють необхідність здійснення заходів щодо попередження шкідливої і небезпечної дії статичної електрики на організм людини.

У випадку якщо напруженість електричного поля більша за електричну міцність середовища (повітря), то починається розряд статичної електрики. Питомий електричний опір ($\text{Ом}\cdot\text{м}$) є головною причиною, яка характеризує спроможність різних матеріалів проводити електричний струм, а також спричинює їх здатність до електризації.

Умовно прийнято, що при значенні питомого електричного опору матеріалів і речовин порядку менше $10 \text{ Ом}\cdot\text{м}$ заряди не накопичуються і небезпеки не становлять. Якщо ж опір високий і швидкість відриву поверхні велика, то заряди зберігаються. Величина зарядів визначається швидкістю

розділення поверхонь і природою матеріалу, тобто інтенсивністю технологічного процесу.

Розряди статичної електрики є одними з ймовірних імпульсів вибухів і спалахування, що пов'язано, в першу чергу, із використанням сильно електризуючих матеріалів і речовин (пил органічного походження, горючі рідини). Електризація рідин приводить до вибухів і спалахування в три рази частіше, ніж електризація дрібнодисперсних речовин, оскільки мінімальна енергія загорання пилово-вітрянних сумішей в десятки чи навіть сотні разів менша. При протіканні рідин значення величини заряду залежить від діаметра труб, швидкості протікання, шорсткості стінок, діелектричної сталої і її забрудненості.

Статична електрика може бути усунена: відведенням зарядів від працівників у виробництвах, в яких існує небезпека спалахування горючих сумішей розрядом з людини; шляхом нанесення на діелектричне устаткування електропровідних покриттів; заміною горючих середовищ негорючими (для промивання трубопроводів, ємностей, наприклад замість гасу, бензину слід застосовувати пожежобезпечні розчинники з підтриманням концентрації горючих речовин за межами вибуховості); зволоженням навколишнього середовища, якщо це дозволяється за умовами технологічного процесу. Якщо це неможливо, то можна використовувати місцеве зволоження, шляхом спрямовування на поверхні розпилюючого струменя, з яких потрібно відвести статичні заряди; забезпеченням проявів заряду в тих місцях, в яких немає вибухонебезпечного горючого і середовища; збільшенням поверхневої і об'ємної провідності діелектриків, які застосовують для зберігання і транспортування рідин; іонізацією повітря радіоактивними, високовольтними, індукційними та комбінованими нейтралізаторами. Вибір кожного типу нейтралізатора здійснюється з врахуванням заземлення обладнання; характеристик іонізаторів і середовища; зміною технологічного процесу з метою усунення причин, які сприяють появі електризації. Заземлення обладнання – один з обов'язкових і важливих заходів щодо захисту від статичної електрики.

Пристрої, машини, апарати, які можуть стати джерелами появи зарядів статичної електрики, повинні бути заземленими не менше ніж у двох місцях незалежно від заземлення усього технологічного кола.

Звичайні заземлюючі пристрої для захисту від розрядів статичної електрики об'єднують із заземлюючими приладами для електрообладнання. Заземлення повинно бути виконане лише шляхом паралельного приєднання захисного обладнання. Допустиме значення опору заземленого пристрою у вигляді малих струмів витрат для захисту від статичної електрики повинно не перевищувати 100 Ом.

Гнучкі трубопроводи для перекачування рідин, які здатні генерувати заряди (гас, бензин, спирт тощо), повинні мати металеве заземлене оплетення, а вихідні штуцери мають бути з'єднані із заземленим металевим оплетенням і повинні бути виготовлені із кольорових металів.

Серед інших заходів, які направлені на заземлення небезпечних проявів розрядів статичної електрики, варто відмітити такі, як заміна плоских пасів текстурними (клиновими); зміна швидкості переміщення рідких і твердих матеріалів; недопущення розприскування рідин при їх розливанні в ємності завдяки опусканню завантажувальних труб на відстань не більше двадцяти сантиметрів від днища приймальної посудини.

4.2 Заходи з техніки безпеки при виготовленні плат, при паянні та склеюванні деталей

Друкована (печатна) плата – це пластина, яка виготовлена з діелектрика (гетинакс, текстоліт тощо), на якій сформований принаймні один провідний малюнок. Електронні компоненти монтуються на друковану плату і з'єднуються своїми виводами з елементами провідного малюнка шляхом паяння, або, значно рідше – зварювання, внаслідок чого збирається електронний пристрій (або

змонтована друкована плата). Зазвичай друкована плата проєктується індивідуально залежно від типів корпусів деталей і електронної схеми. Для їх розробки використовують спеціальне програмне забезпечення.

Однією з стадій розробки системи побутової охоронної сигналізації є виготовлення друкованої плати та монтаж електронних елементів на її поверхню у відповідності до спроектованої електричної схеми.

Сучасна технологія виготовлення друкованих плат містить з велику кількість різних хімічних, фотохімічних і механічних операцій. Більшість речовин і матеріалів, які застосовуються при виготовленні друкованих плат, є небезпечними для життя і здоров'я людини. Шкідливі речовини і їх пари можуть проникати в організм людини через кишково-шлунковий тракт, шкіру і органи дихання.

Вдихання хімічних речовин в будь-якому стані (пил, пари, чи газ) спричиняє ураження верхніх дихальних шляхів і загально-токсичний ефект при всмоктуванні речовин в кров. У кишково-шлунковий тракт шкідливі речовини попадають при курінні, вживанні води і їжі на ділянках виготовлення друкованих плат.

Нагрівання розчинів призводить до виділення краплин рідини і інтенсивного пароутворення, які тягнуть за собою частинки розчину, а це спричиняє забруднення атмосфери виробничих приміщень. Крім цього, під час різних операцій утворюються і поступають в атмосферу проміжні речовини, які можна віднести до першого класу небезпеки. Так, хлоровані вуглеводні (тетрахлоретилен, трихлоретилен) при взаємодії з сонячним світлом чи відкритими джерелами полум'я утворюють нову речовину – надзвичайно небезпечний газ фосген, а при реагентному способі очищення відпрацьованих вод від сполук ціану може утворюватися хлорціан.

Попадання кислоти в лужний ціанистий електроліт, змішування ціанистих і кислих стоків вентиляційних вихлопів може спричинити утворення ціаністого водню. Процеси хімічного фрезерування, електрохімічної обробки, травлення і знежирення супроводжуються виділенням парів лугів, кислот і

потраплянням їх в повітря зони дихання. Багато шкідливих речовин надходить в організм через шкіру, особливо небезпечними є розчинники, луги, концентровані кислоти і хромові композиції.

У відділах приготування електролітів завжди має місце висока концентрація парів токсичних речовин і пилу, особливо під час: змішування сипучих компонентів, дозуванні при приготуванні розчинів, обробки матеріалів і під час транспортних операцій.

При ціаністому срібленні і мідненні утворюється ціаністий водень, який потрапляє в атмосферу, в цьому випадку відчувається запах мигдалю. Поява у повітрі шкідливих речовин над ваннами є результатом виносу дрібних краплинок електроліту бульбашками газів (кисню і водню), які виділяються на електродах під час електролітичного процесу та випаровування розчинів. Ціаністий водень утворюється внаслідок контакту ціаністого розчину з вуглекислотою. Біля ванн окисдування утворюються пари лугів; біля ванн кадміювання – оксиди кадмію; біля ванн декапірування – пари соляної кислоти; при очистці свинцевих анодів – пил свинцю; при хромуванні – хромовий ангідрид; при нікелюванні – пари сполучення нікелю.

Однією з умов дотримання безпеки праці є забезпечення здійснення етапів виробництва відповідно до технологічної послідовності окремих операцій, передбачаючи механізацію і автоматизацію процесів, а також централізацію приготування електролітів. Пульти операторів автоматичних ліній з програмним управлінням повинні бути віддалені від ванн на певну відстань, що виключає вплив на працівників небезпечних виробничих факторів.

При неможливості автоматизації процесів має бути забезпечена комплексна механізація окремих етапів – підготовчих, транспортних, фінішних, зокрема завантаження друкованих плат у ванни і їх вивантаження. Використання ручних робіт допускається при відсутності в технологічному процесі речовин 1-го і 2-го класів небезпеки і з застосуванням індивідуального і колективного захисту робітників. Особливу увагу необхідно звернути на

заміну токсичних речовин нетоксичними чи менш токсичними, заміну небезпечних операцій менш шкідливими. Так, використання інгібіторів і присадок дозволяє зменшити витрати на вентиляцію, а також значно знизити виділення парів кислоти з поверхні травильних і гальванічних ванн (дзеркало ванни покривається піною).

При склеюванні та паянні деталей, виконанні монтажних робіт системи охоронної сигналізації, присутні певні шкідливі фактори. Тому усі робочі місця мають бути обладнані витяжною вентиляцією, а працівники використовувати засоби індивідуального захисту шкіри, очей і органів дихання. Повітря має бути чистим, потрібної вологості і температури. Отже, використання вентиляції потрібне для зменшення або ліквідації задимленості повітря та покращення виробничого процесу і підвищення вищої якості продукції.

Усе це робить вентиляцію одним з найефективніших засобів оздоровлення, підвищення продуктивності праці і безпеки та покращення якості продукції при монтажних роботах. За способом переміщення повітря вентиляція може бути механічною, природною і змішаною. Природний обмін повітря у робочому приміщенні здійснюється через двері, кватирки, вікна, ґратки на підлозі та у стінах. При механічній вентиляції повітря видаляється або подається системою вентиляційних каналів за допомогою вентиляторів [3].

У приміщеннях де виконуються монтажні роботи, використовують механічну і природню вентиляцію. За місцем дії вентиляція може бути і загальнообмінною, принцип дії якої базується на розрідженні речовин, які виділяються, свіжим повітрям до певної температури і концентрації. У приміщеннях, в яких можливе різке надходження у повітря великої кількості шкідливої пари, пилу, газів, передбачається аварійна вентиляція. Для ефективної роботи системи вентиляції кількість повітря, яке надходить повинна відповідати кількості видаленого повітря, або різниця між ними повинна бути мінімальною. Витяжні і припливні системи у приміщенні розміщені так, що свіже повітря подається у ті частини, в яких кількість шкідливих речовин мінімальна (або

відсутня зовсім), а видаляється там, де їх видалення є мінімальним; приплив повітря відбувається у робочі зони, а витяжка з верхньої зони приміщення.

Система вентиляції не викликає ні перегріву ні переохолодження працівників і не створює шуму на робочих місцях, який би міг перевищувати допустимі норми. Система вентиляції також повинна бути пожежо- і вибухонебезпечною, надійною, простою в експлуатації і економічною.

Вентиляція забезпечує потрібний обмін повітря завдяки різниці густини теплого повітря, яке знаходиться всередині приміщення і холоднішого повітря зовні, а також внаслідок вітрових потоків. Природна вентиляція може бути організованою і неорганізованою. У першому випадку повітря видаляється і надходить через щілини і пори кватирок, вікон і зовнішніх огорож.

Організована вентиляція здійснюється дефлекторами і аерацією. Аерація – це організований і регулюючий природний обмін повітря. Дефлектори являють собою спеціальні пасажі, що використовують енергію вітру і встановлюються на витяжних повітровідводах.

Штучна вентиляція підтримує постійний обмін повітря незалежно від зовнішніх метеорологічних умов, завдяки механічним і повітроводам вентиляторам. Повітря, яке надходить до приміщення, у випадку необхідності охолоджується або підігрівається, осушується або зволожується. Забезпечується очищення повітря, яке виводиться в атмосферу.

Місцева вентиляція забезпечує вентиляцію безпосередньо біля робочого місця працівника, вловлює шкідливі речовини під час їх виділення і запобігає потраплянню шкідливих речовин у повітря приміщень. Місцева вентиляція за способом обміну повітря також поділяється на витяжну та припливну.

Під час розробки системи побутової охоронної сигналізації необхідно дотримуватись правил техніки безпеки при виготовленні друкованих плат та паянні електронних компонентів, які описані в цьому розділі.

РОЗДІЛ 5

ЕКОНОМІЧНА ЕФЕКТИВНІСТЬ

5.1 Економічна характеристика об'єкта впровадження та аналіз ринку систем домашньої охоронної сигналізації

Об'єктом впровадження розробленого програмного модуля є побутова система охоронної сигналізації для квартири або приватного будинку, побудована на базі мікроконтролера Arduino Uno, датчиків руху, відкриття дверей, розбиття скла та GSM-модуля SIM800L. Відповідно до технічного завдання, така система забезпечує контроль основних маршрутів проникнення зломисників (двері, вікна, внутрішній простір приміщення), подає світлові й звукові сигнали тривоги, а також надсилає SMS-повідомлення чи здійснює виклики на смартфон власника. У порівнянні з традиційними дротовими системами, розроблене рішення відрізняється гнучкістю, можливістю модернізації програмної частини та низькою собівартістю апаратної бази.

Ринок систем побутової охоронної сигналізації в Україні є насиченим, на ньому представлені як прості автономні сигналізації, так і комплексні рішення класу «розумний дім». До найбільш відомих рішень належать безпроводні комплекси MAKS PRO, Kit GSM, Ajax StarterKit і допоміжні модулі типу Ajax HomeSiren. Зазвичай такі системи включають центральний блок, набір датчиків, сирену та інтерфейси GSM/Ethernet для зв'язку з користувачем або пультом охоронної компанії.

З урахуванням інформації, наведеної у розділі 1, можна узагальнити основні техніко-економічні характеристики типових систем, що є аналогами розробленого комплексу (табл. 5.1).

Таблиця 5.1 – Порівняльна характеристика типових систем домашньої охоронної сигналізації

Система	Тип зв'язку	Кількість підключених пристроїв	Наявність GSM / мобільного застосунку	Орієнтовна складність монтажу	Орієнтовна ціна комплекту*
MAKS PRO	GSM/GPRS, Ethernet	До 200 пристроїв	Є / є	Висока	Висока
Kit GSM (ATIS)	GSM	Невелика кількість датчиків	Є / частково через GSM-керування	Середня	Середня
Ajax StarterKit	Радіоканал, GSM, Ethernet	Розширюється додатковими датчиками	Є / повноцінний мобільний застосунок	Низька–середня	Висока
Ajax HomeSiren	Радіоканал	Працює як елемент системи Ajax	Немає / налаштування через хаб	Низька	Низька–середня

*Примітка: цінові оцінки наведено якісно (низька/середня/висока) для ілюстрації ринкової ніші.

Проаналізовані рішення демонструють високий рівень функціональності, однак мають декілька обмежень. По-перше, користувач фактично прив'язаний до конкретної платформи виробника та його екосистеми. По-друге, вартість комплексів середнього і високого класу є відчутною для пересічного домогосподарства. По-третє, можливості гнучкої модифікації алгоритмів охорони, інтеграції з іншими саморобними або академічними проєктами часто є обмеженими.

Розроблений у кваліфікаційній роботі програмний модуль управління охоронною системою розумного будинку орієнтований на відкриту апаратну платформу Arduino Uno та доступні датчики HC-SR501, MC-38, KY-037, GSM-модуль SIM800L тощо. Це дозволяє істотно знизити собівартість системи, адаптувати її до специфічних умов конкретного об'єкта, а також використовувати в навчальних та наукових цілях. Завдяки вбудованій підтримці DTMF-команд і SMS-керування користувач отримує можливість дистанційно змінювати режими роботи сигналізації без додаткових ліцензійних платежів за програмне забезпечення.

Таким чином, з економічної точки зору об'єкт впровадження можна охарактеризувати як низьковитратний, гнучкий та масштабований програмно-апаратний комплекс для домашньої безпеки, який займає нішу між простими автономними сигналізаціями та дорогими пропрієтарними системами «розумного дому».

5.2 Розрахунок витрат на розробку та впровадження програмно-апаратного комплексу

До витрат, пов'язаних з реалізацією проєкту «Розробка та дослідження програмного модуля управління охоронною системою розумного будинку», належать одноразові витрати на розробку програмного забезпечення та прототипу, а також змінні витрати на виготовлення кожного комплексу системи для окремого об'єкта.

Одноразові витрати на розробку включають оплату праці розробника (або невеликої команди), нарахування на заробітну плату, витрати на електроенергію, амортизацію комп'ютерної техніки та інші накладні витрати. Для розрахунку приймемо умовні, але реалістичні значення. Безпосередня розробка програмного

модуля, налагодження прототипу та проведення експериментів тривали 3 місяці при місячній заробітній платі фахівця 30 000 грн.

Фонд основної заробітної плати за період розробки становитиме:

$$З_{\text{осн}} = 30\,000 * 3 = 90\,000 \text{ грн.} \quad (5.1)$$

Нарахування на заробітну плату (ЄСВ та інші обов'язкові платежі) приймемо на рівні 22 %:

$$З_{\text{нар}} = 0,22 * 90\,000 = 19\,800 \text{ грн.} \quad (5.2)$$

Для врахування витрат на амортизацію обладнання, електроенергію, послуги Інтернету, витратні матеріали та інші накладні витрати введемо коефіцієнт 0,1 від суми фонду оплати праці та нарахувань:

$$В_{\text{накл}} = 0,1 * (З_{\text{осн}} + З_{\text{нар}}) = 0,1 * 109\,800 \approx 10\,980 \text{ грн.} \quad (5.3)$$

Тоді загальна сума одноразових витрат на розробку програмного модуля та прототипу становитиме:

$$К_{\text{розр}} = З_{\text{осн}} + З_{\text{нар}} + В_{\text{накл}} \approx 90\,000 + 19\,800 + 10\,980 \approx 120\,000 \text{ грн.} \quad (5.4)$$

Змінні витрати на виготовлення одного комплекту системи складаються з вартості апаратних компонентів, витрат на монтаж і налагодження. На основі запропонованої структури системи (розділ 2) сформовано перелік основних компонентів (табл. 5.2).

До вартості елементної бази додамо витрати на монтаж і налагодження одного комплекту системи. Приймемо, що робота монтажника (1 день) оцінюється у 500 грн. Тоді змінні витрати на одну систему становитимуть:

$$V = 1\,940 + 500 = 2\,440 \text{ грн.} \quad (5.5)$$

Під час серійного впровадження потрібно врахувати розподіл одноразових витрат на розробку між певною кількістю реалізованих систем. Нехай планується встановити $N = 30$ комплектів розробленої системи. Тоді частка витрат на розробку, що припадає на один комплект, дорівнюватиме:

$$K_{\text{розр}}^{(1)} = \frac{K_{\text{розр}}}{N} = \frac{120\,000}{30} = 4\,000 \text{ грн.} \quad (5.6)$$

Таблиця 5.2 – Вартість апаратних компонентів одного комплекту системи

№ з/п	Найменування компонента	Кількість, шт.	Орієнтовна ціна за одиницю, грн	Сума, грн
1	Плата Arduino Uno	1	350	350
2	Датчик руху PIR HC-SR501	1	80	80
3	Датчик відкриття дверей MC-38	1	40	40
4	Акустичний датчик розбиття скла KY-037	1	80	80
5	GSM-модуль SIM800L	1	250	250
6	РК-дисплей 16×2 з модулем I2C	1	200	200
7	Мембранна клавіатура 3×4	1	60	60
8	Модуль заряджання акумулятора TP4056	1	50	50
9	П'єзоелектричний динамік	1	30	30
10	Літій-іонний акумулятор з тримачем	1	200	200
11	Блок живлення 5 В, 2 А	1	150	150
12	Корпус, дроти, роз'єми, монтажні матеріали	1 комплект	300	300
13	Дрібні витрати (плата, кріплення, запасні елементи)	1 комплект	150	150
	Разом			1 940

Повна собівартість одного комплекту при такому обсязі впровадження становить:

$$C_{\text{комп}} = V + K_{\text{розр}}^{(1)} = 2\,440 + 4\,000 = 6\,440 \text{ грн.} \quad (5.7)$$

Для формування ціни продажу системи врахуємо бажану рентабельність. Якщо прийняти рівень прибутку 25 % від собівартості, розрахункова ціна складе:

$$\text{Ц} = \text{C}_{\text{комп}} * (1 + 0,25) = 6\,440 * 1,25 \approx 8\,050 \text{ грн.} \quad (5.8)$$

Для подальших розрахунків зручно округлити ціну до 8 000 грн за комплект системи з установкою.

5.3 Оцінка економічної ефективності та соціально-економічного ефекту впровадження

Економічний ефект проєкту можна оцінювати з двох позицій: з точки зору розробника/інтегратора системи та з точки зору кінцевого користувача (власника квартири або будинку). Для розробника ключовим показником є окупність одноразових витрат на розробку програмного модуля і прототипу, для користувача – зниження витрат на охорону помешкання та зменшення ризику матеріальних збитків від крадіжок.

З погляду розробника, величина прибутку від продажу одного комплекту системи визначається різницею між ціною продажу та змінними витратами:

$$\text{П}_1 = \text{Ц} - \text{V} = 8\,000 - 2\,440 = 5\,560 \text{ грн.} \quad (5.9)$$

Тоді необхідний обсяг реалізації для повного відшкодування одноразових витрат на розробку (точка беззбитковості) визначається за формулою:

$$N_0 = \frac{\text{K}_{\text{розр}}}{\text{П}_1} = \frac{120\,000}{5\,560} \approx 21,6. \quad (5.10)$$

Отже, для виходу проєкту «в нуль» потрібно реалізувати не менше 22 комплектів системи. При плановому обсязі 30 комплектів сумарний прибуток розробника становитиме

$$\text{П}_{\Sigma} = \text{П}_1 * N - \text{K}_{\text{розр}} = 5\,560 * 30 - 120\,000 = 46\,800 \text{ грн.} \quad (5.11)$$

Це свідчить про наявність економічної доцільності комерційного тиражування розробленого програмного модуля в складі системи охоронної сигналізації.

З точки зору кінцевого користувача, доцільно порівняти витрати на використання розробленої системи з альтернативним варіантом – підключенням до традиційної пультової охорони, де застосовується комерційний комплект сигналізації та щомісячна абонентська плата. Для спрощення приймемо такі умовні дані.

Варіант 1 – традиційна пультова охорона:

- вартість обладнання та монтажу комерційної системи: 5 000 грн;
- щомісячна абонентська плата: 500 грн (6 000 грн/рік).

Варіант 2 – розроблена система з GSM-сповіщенням:

- вартість обладнання та монтажу: 8 000 грн;
- витрати на мобільний зв'язок (SIM-картка для GSM-модуля): 100 грн/місяць (1 200 грн/рік);
- витрати на електроенергію незначні й у подальших розрахунках не враховуються.

Порівняємо сумарні витрати користувача протягом трьох років експлуатації системи (табл. 5.3).

Таблиця 5.3 – Порівняння витрат користувача для двох варіантів охорони помешкання

Показник	Варіант 1 – пультова охорона	Варіант 2 – розроблена система
Початкові витрати, грн	5 000	8 000
Річні експлуатаційні витрати, грн	6 000	1 200
Сумарні витрати за 1-й рік, грн	11 000	9 200
Сумарні витрати за 2 роки, грн	17 000	10 400
Сумарні витрати за 3 роки, грн	23 000	11 600

Як видно з таблиці, уже в перший рік експлуатації витрати користувача на розроблену систему менші на:

$$\Delta_1 = 11\,000 - 9\,200 = 1\,800 \text{ грн}, \quad (5.12)$$

а в подальшому розрив між варіантами збільшується. За три роки економія користувача становитиме:

$$\Delta_3 = 23\,000 - 11\,600 = 11\,400 \text{ грн}. \quad (5.13)$$

Графічно залежність сумарних витрат від тривалості експлуатації зручно подати у вигляді лінійного графіка (рисунок 5.1), на якому по осі абсцис відкладається час, років, а по осі ординат – накопичені витрати за кожним із варіантів.

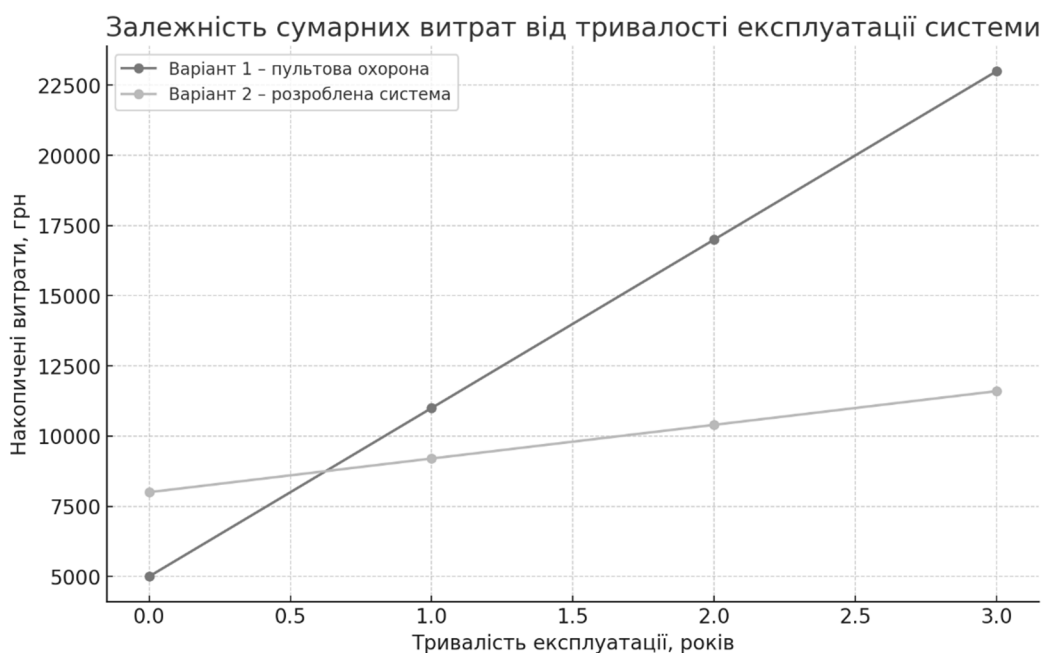


Рисунок 5.1 – Залежність сумарних витрат на забезпечення охорони помешкання від тривалості експлуатації системи

На графіку крива для традиційної пультової охорони починається нижче (через нижчі початкові витрати), проте має більший нахил через значні щорічні платежі. Крива для розробленої системи стартує з вищого початкового значення, але зростає повільніше. У момент перетину кривих (приблизно між першим і другим роком експлуатації) реалізується «точка економічної рівноцінності» для користувача, після чого використання розробленого програмно-апаратного

комплексу стає економічно вигіднішим. Чим довший період експлуатації, тим більшою є накопичена економія коштів на користь запропонованого рішення.

Крім суто фінансових показників, важливим є соціально-економічний ефект від впровадження системи. Розроблена охоронна сигналізація підвищує рівень безпеки житла, зменшує імовірність матеріальних збитків від крадіжок, забезпечує психологічний комфорт мешканців. Можливість гнучкого налаштування алгоритмів у мікроконтролері, введення та зміни паролів через клавіатуру, використання DTMF-команд і SMS-інтерфейсу дозволяє адаптувати систему під потреби різних категорій користувачів, у тому числі людей похилого віку. Потенційна інтеграція з іншими підсистемами «розумного будинку» (освітлення, клімат-контроль, протипожежна сигналізація) сприяє підвищенню енергоефективності та загального рівня комфорту проживання.

Отже, на основі проведених розрахунків і порівняльного аналізу можна зробити висновок, що впровадження розробленого програмного модуля управління охоронною системою розумного будинку є економічно доцільним як для розробника, так і для кінцевого користувача. Проєкт забезпечує прийнятний термін окупності, значну економію експлуатаційних витрат у порівнянні з традиційними варіантами охорони, а також формує додатковий соціально-економічний ефект за рахунок підвищення безпеки та якості життя мешканців.

ВИСНОВКИ

Розроблено та експериментально перевірено роботу програмного модуля управління охоронною системою «розумного будинку», який забезпечує збір даних із датчиків, виявлення тривожних подій, індикацію станів, а також дистанційне керування й оповіщення користувача через GSM-канал із підтримкою SMS-повідомлень і DTMF-команд.

Опрацьовано функціональні вимоги до побутових систем охоронної сигналізації та виконано порівняльний аналіз підходів і рішень, що дозволило обґрунтувати ключові функції для проєктованої системи (оперативне виявлення вторгнення, мінімізація хибних спрацювань, зручний користувацький інтерфейс і гарантоване віддалене сповіщення).

Сформовано структурно-апаратну основу рішення та підібрано елементну базу прототипу. Реалізований комплект включає плату Arduino Uno, датчик руху PIR HC-SR501, датчик відкриття дверей MC-38, акустичний датчик «розбиття скла» KY-037, GSM-модуль SIM800L тощо. Сукупна вартість апаратних компонентів одного комплекту оцінена на рівні 1940 грн, що підтверджує придатність рішення для бюджетного сегмента та подальшого тиражування.

Реалізовано алгоритмічне та програмне забезпечення системи, включно з режимами роботи, обробленням подій, формуванням тривоги, індикацією та сценаріями дистанційної взаємодії через SIM800L (SMS/DTMF). Підтверджено доцільність компромісу між чутливістю та стійкістю до хибних спрацювань для акустичного датчика KY-037, для житлових умов доцільним є середній поріг порядку 0.55–0.65 з додатковою програмною фільтрацією події.

Середня затримка доставки SMS у створених умовах становила 10.8 с за високої якості сигналу, 18.5 с за середньої та 29.0 с за низької; при цьому 95-й перцентиль досягав 16.9 с, 27.0 с і 47.3 с відповідно, що є важливим для оцінювання «гірших випадків» у тривожних сценаріях.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Жураковський Б. Ю., Зенів І. О. Технології інтернету речей. – Київ : КПІ ім. Ігоря Сікорського, 2021. – 271 с.
2. Пулеко І. В., Єфіменко А. А. Архітектура та технології Інтернету речей. – Житомир : Державний університет «Житомирська політехніка», 2022. – 234 с.
3. Сторчак К. П., Тушич А. М., Срібна І. М., Яковенко Н. Д., Кравець Д. В. Технології Інтернет речей. – Київ : Державний університет телекомунікацій, 2021. – 68 с.
4. Крижановський В. Г., Сергієнко С. П. До практичної реалізації пристроїв Інтернету речей (IoT). – Вінниця : ДонНУ ім. Василя Стуса, 2019. – 61 с.
5. Кулічок А. М. Розумний дім. – Вінниця : Універсум-Вінниця, 2005. – 300 с.
6. Макєєв С., Віровець С. Сучасна апаратура та обладнання систем «розумний будинок» // Вісник НТУ «ХПІ». Серія : Проблеми удосконалювання електричних машин і апаратів. Теорія і практика. – 2020. – Т. 4, № 2. – С. 16–20.
7. Кукунін С. Розробка цілісної методології організації систем типу «розумний будинок» в рамках парадигми «інтернету речей» // Computer-integrated technologies: education, science, production. – 2020. – № 38. – С. 40–45.
8. Маслова М. «Розумний будинок» : бібліографічний покажчик. – Запоріжжя : Запорізька обласна універсальна наукова бібліотека, 2021. – 76 с.
9. Денисюк В. О., Цирульник С. Мікропроцесорні системи управління. – Вінниця : ТВОРИ, 2021. – 204 с.
10. Татарчук Д. Д., Діденко Ю. В. Мікропроцесори та мікроконтролери : курс лекцій. – Київ : КПІ ім. Ігоря Сікорського, 2020. – 238 с.

11. Козбур І. Р., Марущак П. О., Медвідь В. Р., Савків В. Б., Пісьціо В. П. Проектування мікропроцесорних систем керування. – Тернопіль : Вид-во ТНТУ ім. І. Пулюя, 2022. – 324 с.
12. Грищук Ю. С. Мікроконтролери : архітектура, програмування та застосування в електромеханіці. – Харків : НТУ «ХПІ», 2019. – 384 с.
13. Кушнір А. П., Чалий Д. О. Системи пожежної та охоронної сигналізації. – Львів : Сполом, 2022. – 298 с.
14. Дерев'янка О. А., Бондаренко С. М., Христич В. В., Антошкін О. А. Системи пожежної та охоронної сигналізації : текст лекцій. – Харків : УЦЗУ, 2008. – 144 с.
15. Кріса І. Я., Воробйов О. І. Системи пожежної сигналізації. – Львів : Сполом, 2013. – 138 с.
16. Живило Є. О., Головка Г. В., Шефер О. В. Системи технічного захисту інформації. Ч. 1 / за ред. Є. О. Живило. – Полтава : Нац. ун-т «Полтавська політехніка ім. Ю. Кондратюка», 2023. – 155 с.
17. Богуш В. М., Бровко В. Д., Кобус О. С., Козюра В. Д. Технічний захист інформації. – Київ : Ліра-К, 2022. – 508 с.
18. Ластівка Г. І., Шпатар П. М. (уклад.). Технічний захист інформації в інформаційних та телекомунікаційних системах. – Чернівці : Чернівецький нац. ун-т ім. Ю. Федьковича, 2018. – 252 с.
19. Fedko A. O., Zelenova I. Y., Tiahunova M. Y. Development and modeling of a smart home system with increased reliability based on Arduino // Problems of Modeling and Design Automation. – 2019. – Vol. 21, No. 1. – P. 23–32.
20. Ajax Systems. Розумний будинок Ajax : система комплексної безпеки приватних об'єктів [Електронний ресурс]. – Режим доступу : <https://ajax.systems>.