

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр

(назва освітнього ступеня)

на тему: Система охорони приватного будинку на базі Arduino

Виконав(ла): студент(ка) IV курсу груп СІс-42
и

спеціальності 123 «Комп'ютерна інженерія»

(шифр і назва спеціальності)

Літвінов Л.А.
(підпис) (прізвище та ініціали)

Керівник Тиш Є.В.
(підпис) (прізвище та ініціали)

Нормоконтроль Луцик Н.С.
(підпис) (прізвище та ініціали)

Завідувач кафедри Осухівська Г.М.
(підпис) (прізвище та ініціали)

Рецензент Ясній О.П.
(підпис) (прізвище та ініціали)

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра комп'ютерних систем та мереж
(повна назва кафедри)

ЗАТВЕРДЖУЮ

Завідувач кафедри

Осухівська Г.М.

(підпис)

(прізвище та ініціали)

« _____ » _____ 2024 р.

**ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ**

на здобуття освітнього ступеня бакалавр
(назва освітнього ступеня)

за спеціальністю 123 «Комп'ютерна інженерія»
(шифр і назва спеціальності)

студенту Літвінов Любомир Анатолійович
(прізвище, ім'я, по батькові)

1. Тема роботи Система охорони приватного будинку на базі Arduino

Керівник роботи Тиш Євгенія Володимирівна, кандидат технічних наук, доцент кафедри КС
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « 26 » 04 2024 року № 4/7-468

2. Термін подання студентом завершеної роботи _____

3. Вихідні дані до роботи Технічне завдання

4. Зміст роботи (перелік питань, які потрібно розробити)

1. Аналіз технічного завдання

2. Проектна частина

3. Практична частина

3. Практична частина

4. Безпека життєдіяльності, основи охорони праці

Висновки. Список використаних джерел

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

АНОТАЦІЯ

Система охорони приватного будинку на базі Arduino // Кваліфікаційна робота бакалавра // Літвінов Любомир Анатолійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра комп'ютерних систем та мереж, група Сіс-42 // Тернопіль, 2024 // с. – 54, рис. – 23, табл. – 1, аркушів А1 – 4, бібліогр. – 19.

Ключові слова: система охорони, Arduino, мікроконтролер, програмне забезпечення.

Кваліфікаційна робота зосереджена на створенні системи для моніторингу безпеки приватного будинку за допомогою технології віддаленого спостереження. Під час огляду та аналізу сучасних комп'ютеризованих засобів охорони приватних будинків виявлено, що одним із найбільш перспективних напрямків є розробка системи на основі програмно-апаратних модулів arduino для віддаленого спостереження. Розроблено структурну схему системи для охорони приватних будинків з виведенням інформації на телефон за допомогою telegram-бота. Створено принципову електричну схему охоронного пристрою. Описано алгоритм роботи системи та розроблено відповідне програмне забезпечення.

ANNOTATION

Security System for a Private House Based on Arduino // Bachelor's Qualification Work // Lubomyr Anatoliyovych Litvinov // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Computer Systems and Networks, Group CIS-42 // Ternopil, 2024 // p. – 54, fig. – 23, tables – 1, A1 sheets – 4, bibliography – 19.

Keywords: security system, Arduino, microcontroller, software.

The qualification work focuses on the development of a system for monitoring the security of a private house using remote surveillance technology. A review and analysis of modern computerized means for securing private houses revealed that one of the most promising directions is the development of a system based on software-hardware modules arduino for remote surveillance. A structural diagram of the system for securing private houses with information output to a phone via a Telegram bot has been developed. The circuit diagram of the security device has been created. The system's operation algorithm is described, and the corresponding software has been developed.

ЗМІСТ

СПИСОК СКОРОЧЕНЬ.....	7
ВСТУП.....	8
РОЗДІЛ 1 АНАЛІЗ ТЕХНІЧНОГО ЗАВДАННЯ.....	10
1.1 Аналіз вимог до системи охорони у приватному будинку.....	10
1.2 Аналіз можливих рішень поставленого завдання.....	12
1.3 Огляд існуючих систем охорони приватних будинків.....	13
1.3.1 Система ajax starterKit.....	13
1.3.2 Система охорони CoVi security HS-800	16
1.3.3 Система безпеки Kerui Alarm G18.....	19
РОЗДІЛ 2 ПРОЕКТНА ЧАСТИНА	20
2.1 Розробка узагальненої структури системи для охорони приватного будинку.....	20
2.2 Обґрунтування вибору апаратного забезпечення системи охорони приватного будинку.....	22
2.2.1 Вибір елементної бази	22
2.2.2 Датчик руху та датчик відкриття дверей.....	27
2.2.3 Wi-Fi модуль.....	29
2.2.4 Telegram-бот	30
2.2.5 Модуль з мікросхемою годинника реального часу DS1307	31
2.2.6 LCD-дисплей	33
2.3 Обґрунтування вибору програмних засобів для системи охорони.....	37
2.3.1 Середовище розробки Arduino.....	37
2.3.2 Робота з telegram-ботом.....	37
РОЗДІЛ 3 ПРАКТИЧНА ЧАСТИНА	39
3.1 Розробка алгоритмів роботи системи охорони приватного будинку.....	39

					КС КРБ 123.22-320.00.00 ПЗ						
Змн.	Арк.	№ докум.	Підпис	Дата	Система охорони приватного будинку на базі Arduino						
Розроб.		Літвінов Л.А.							Літ.	Арк.	Акрушів
Перевір.		Тиш С.В							5		
Реценз.		Ясній О.П.							ТНТУ, каф. КС, Сіс-42		
Н. контр.		Луцик Н.С									
Затверд.		Осухівська Г.М									

3.2 Створення інтерфейсу користувача.....	40
3.3 Тестування системи охорони приватного будинку.....	43
РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ	47
4.1 Вплив електромагнітних полів на людину та заходи щодо зменшення їх впливу жителів будинку.....	47
4.2 Вимоги пожежної безпеки при гасінні електроустановок.....	49
ВИСНОВКИ.....	52
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	53
Додаток А Технічне завдання	55
Додаток Б Лістинг програми	65

					КС КРБ 123. 22-320.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		6

СПИСОК СКОРОЧЕНЬ

АПК – апаратно-програмний комплекс

АЦП – аналого-цифровий перетворювач

БЖ – блок живлення

БУ – блок управління

МК – мікроконтролер

ПДМ – програма дистанційного моніторингу

ТЗ – технічне завдання

					КС КРБ 123. 22-320.00.00 ПЗ	Арк.
						7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Сучасні системи охорони не є окремим приладом або пристроєм. Це ретельно спроектований комплекс систем і технічних засобів, які запобігають несанкціонованому проникненню зловмисників на приватну власність та своєчасно сповіщають про це власника. Вони включають в себе різноманітні компоненти, такі як камери відеоспостереження, датчики руху, сигналізації, системи контролю доступу, а також програмне забезпечення для моніторингу та управління. Завдяки інтеграції цих елементів забезпечується високий рівень безпеки, що дозволяє не лише виявляти потенційні загрози, а й оперативно реагувати на них. Крім того, сучасні технології дозволяють віддалено контролювати систему охорони через мобільні додатки, що надає власникам можливість постійно бути в курсі стану своєї власності та оперативно приймати необхідні заходи для її захисту.

Однак, не кожен може дозволити собі придбання таких систем через їх високу вартість. Тому ця робота присвячена розробці охоронної системи на базі Arduino, яка буде менш затратною порівняно з уже доступними на ринку аналогами. Використання Arduino дає змогу створити гнучку та настроювану систему, яка може бути адаптована під конкретні потреби користувача. Крім того, завдяки відкритій платформі Arduino, така система може бути легко вдосконалена та розширена з додаванням нових компонентів, як-от додаткових датчиків або камер. У цій роботі буде детально розглянуто процес розробки та налаштування охоронної системи, включаючи апаратну частину, програмне забезпечення та способи інтеграції з існуючими технологіями для забезпечення максимального рівня безпеки за мінімальних витрат.

Ключовими елементами такої системи стануть прості у використанні і доступні компоненти, як-от плати Arduino, датчики руху, модулі для бездротового зв'язку та сирени. Програмне забезпечення буде розроблено таким чином, щоб забезпечити простоту у використанні та можливість віддаленого контролю через інтернет. Це дозволить власникам мати повний контроль над

					КС КРБ 123. 22-320.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		8

своєю системою охорони незалежно від їхнього місцезнаходження. В результаті, така система стане доступним рішенням для широкого кола користувачів, забезпечуючи при цьому високий рівень безпеки їхньої приватної власності.

Система буде модульною, що дозволить легко додавати або змінювати компоненти в залежності від потреб користувача. Наприклад, до базової конфігурації можна буде додати датчики відкриття дверей та вікон, інфрачервоні датчики для виявлення тепла, а також інші пристрої для підвищення рівня безпеки. Програмне забезпечення на базі Arduino буде розроблено з відкритим кодом, що дозволить ентузіастам і розробникам вносити власні покращення та адаптувати систему під свої специфічні вимоги.

Крім того, в роботі буде розглянуто аспекти енергоефективності, що дозволить зменшити споживання електроенергії системою охорони, а також використання альтернативних джерел живлення, таких як сонячні батареї. Це зробить систему більш автономною та надійною в умовах можливих перебоїв з електропостачанням.

Таким чином, ця робота не лише пропонує економічно вигідне рішення для охорони приватного будинку, але й надає можливість користувачам створювати та налаштовувати власні системи безпеки, що відповідають їхнім індивідуальним потребам та вимогам.

					КС КРБ 123. 22-320.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		9

РОЗДІЛ 1 АНАЛІЗ ТЕХНІЧНОГО ЗАВДАННЯ

У цьому розділі кваліфікаційної роботи проведено аналіз вимог до системи охорони приватного будинку. Під час критичного огляду існуючих систем було виявлено різноманітні підходи та технології, які використовуються в цій сфері. Зокрема, розглянуто рішення на базі традиційних систем безпеки, які пропонуються на ринку спеціалізованими компаніями. Визначено, що хоча такі системи можуть бути ефективними, вони часто характеризуються високою вартістю та обмеженими можливостями розширення.

Зокрема, були виявлені такі переваги, як висока надійність та професійний рівень захисту. Проте, недоліками таких систем є їхня висока вартість, складність установки та обмежені можливості інтеграції з іншими пристроями та системами.

Крім того, було проаналізовано можливість створення власної системи на базі платформи Arduino. Виявлено, що використання Arduino дозволяє розробити гнучку та економічно вигідну систему, яка може бути адаптована до конкретних потреб користувача. Такий підхід дозволяє зменшити витрати на систему охорони, а також надає можливість легко розширювати функціональність системи у майбутньому.

1.1 Аналіз вимог до системи охорони у приватному будинку

Розглянемо та проаналізуємо технічне завдання для кваліфікаційної роботи. Умовою є розробка системи безпеки приватного будинку, яка повинна виконувати такі функції:

- Моніторинг датчика руху та датчика відкриття дверей.
- Передача даних через Telegram-бот.

Змн.	Арк.	№ докум.	Підпис	Дата	КС КРБ 123.22-320.00.00 ПЗ			
Розроб.		Літвінов Л.А.			Аналіз технічного завдання	Літ.	Арк.	Акрушів
Перевір.		Тиш С.В.					10	
Реценз.		Ясній О.П.				ТНТУ, каф. КС, Сіс-42		
Н. контр.		Луцик Н.С.						
Затверд.		Осухівська Г.М.						

- Надсилання інформації на локальний комп'ютер.
- Автоматичне активація сигналізації в разі виявлення неправомірного доступу.
- Можливість віддаленого керування системою через telegram-бот

Очевидно, для ефективного виконання своїх завдань структура системи повинна включати датчик відкриття, який надійно повідомлятиме про відкриття дверей або вікон. Крім того, важливо використовувати додаткові датчики, такі як датчик вібрації та руху, які активуються у разі спроби проникнення через розбиття скла або несанкціонованого руху на території об'єкта. Це дозволить забезпечити більш високий рівень захисту приватної власності шляхом реагування на різноманітні загрози та потенційні небезпеки.

Згідно з умовою, однією з ключових складових системи є пристрій, розроблений на основі мікроконтролера, що забезпечує збір даних з датчиків та управління різними аспектами роботи системи. Вибір конкретної моделі мікроконтролера буде здійснено в результаті аналізу елементної бази, де будуть враховані такі критерії, як продуктивність, енергоефективність, вартість та можливості розширення функціоналу в майбутньому. Це дозволить забезпечити оптимальну сумісність із потребами системи та максимальну ефективність її роботи.

Згідно з технічним завданням, система має забезпечити можливість віддаленого спостереження за контрольованим об'єктом. Для цього необхідно детально проаналізувати технології, що можуть бути використані для передачі даних до ядра системи. Це може включати оцінку ефективності бездротових технологій, таких як Wi-Fi або Bluetooth, або розгляд можливостей використання мережових з'єднань, наприклад, Інтернету через мобільний зв'язок або Ethernet. Важливо також врахувати аспекти безпеки та надійності передачі даних, а також можливості реалізації більшості функцій віддаленого спостереження.

Важною вимогою до технічного завдання є розробка програмного забезпечення, яке забезпечить збір даних про стан системи охорони приватного будинку та своєчасну обробку. Програмне забезпечення для мікроконтролера

					КС КРБ 123. 22-320.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		11

має працювати ефективно для втілення всіх можливостей системи.

Одним з важливих завдань пристрою є забезпечення можливості контролю та управління доступом до системи. Тому потрібно розглянути методи взаємодії користувача з системою прямо на об'єкті. Це може включати розробку інтерфейсу користувача через сенсорний екран або кнопочний пульт, що забезпечить зручність та простоту використання системи для кінцевого користувача. У даному випадку таким пристроєм буде локальний комп'ютер.

При відключенні електроживлення важливо забезпечити можливість доступу до інформації про налаштування параметрів та режимів роботи системи охорони будинку. Це можна забезпечити шляхом збереження важливих даних в енергонезалежній пам'яті. Додатково, система може бути оснащена незалежним або резервним джерелом живлення, що забезпечить неперервне функціонування та збереження важливої інформації, навіть у випадку відключення основного джерела живлення.

1.2 Аналіз можливих рішень поставленого завдання

Системи безпеки можна встановлювати в різноманітних типах будівель: квартирах, заміських оселях, громадських і адміністративних приміщеннях, а також у промислових і складських об'єктах, або будь-якому місці, де існує потенційна загроза проникнення.

Типова система охорони включає три основні компоненти: сенсори, такі як датчики руху, датчики відкриття дверей чи вікон, а також вібраційні датчики і так далі, сирени для сповіщення про вторгнення, а також модуль керування, що відповідає за управління всією системою.

Сенсори відкриття зазвичай встановлюються на вікнах та зовнішніх дверях з метою виявлення будь-яких невинних відкриттів. Сенсори руху зазвичай розташовуються всередині приміщення так, щоб охоплювати всю його площу та реагувати на будь-який рух. Сенсори вібрації, встановлені на вікнах, призначені для виявлення спроб проникнення шляхом розбиття скла.

					КС КРБ 123. 22-320.00.00 ПЗ	Арк.
						12
Змн.	Арк.	№ докум.	Підпис	Дата		

Завдяки універсальності платформи Arduino, система може моніторити кілька приміщень одночасно. Через компактний розмір, датчики легко монтувати, що робить їх ідеальними для використання в різних типах приміщень.

Модуль керування призначений для живлення всіх підключених до нього сенсорів, а також для їх управління та генерації звукового сигналу у разі виявлення порушення. Звукове сповіщення активується, якщо система реєструє активацію одного або кількох датчиків. Додатково передбачено можливість відправлення повідомлення на мобільний телефон або інші пристрої.

Розроблена автоматизована система призначена для автоматичного сповіщення у разі виявлення порушень. Після активації датчика безпеки система автоматично активує звуковий сигнал та надсилає повідомлення користувачеві. Вимкнення сигналу тривоги можливе як локально, так і дистанційно за допомогою введення користувачем коду безпеки.

1.3 Огляд існуючих систем охорони приватних будинків

На сьогоднішній день існує багато варіантів систем захисту приватних будинків, доступних на ринку. Розглянемо та проаналізуємо деякі з них, щоб з'ясувати їх переваги та недоліки.

1.3.1 Система Ajax StarterKit

Ajax StarterKit - це сучасна система охорони, яка ідеально підходить для приватних будинків. Вона включає в себе всі необхідні компоненти для ефективного моніторингу та захисту вашого житла.

Стартовий набір Ajax містить:

- Центральну одиницю (Hub): це мозок системи, який забезпечує безперебійну роботу всіх компонентів. Вона має вбудований GSM та Ethernet зв'язок, що забезпечує надійний зв'язок з центральними службами моніторингу та вашим смартфоном через мобільний додаток.

					КС КРБ 123. 22-320.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		13

- Датчики руху: ці датчики активуються при русі в зоні їх дії та надсилають сигнали до центральної одиниці, спрацьовуючи тривогу.

- Датчики відкриття: вони встановлюються на дверях та вікнах і спрацьовують, коли двері чи вікна відчиняються, надсилаючи сигнал про можливе проникнення.

- Брелоки: набір включає кілька брелоків, які дозволяють зручно ввімкнути та вимкнути систему з безпечної відстані.

Ця система також підтримує можливість розширення, дозволяючи додавати додаткові датчики або пристрої для посилення безпеки вашого будинку за потреби. Завдяки простому встановленню та зручному використанню, Ajax StarterKit є надійним партнером у забезпеченні безпеки житла.

Особливості системи Ajax StarterKit (рис. 1.1) полягають у її високій ефективності, надійності та зручності використання:

- Бездротовий зв'язок: Система Ajax працює на бездротовій технології, що робить її встановлення простим та ефективним, а також уникне непотрібних кабелів, які можуть порушити естетику вашого будинку.

- Надійність зв'язку: Центральна одиниця Hub має вбудований GSM та Ethernet зв'язок, що забезпечує стійкий та надійний зв'язок з вами та центральною системою моніторингу навіть у випадку відключення інтернету.

- Зручний мобільний додаток: Додаток Ajax дозволяє вам контролювати систему з будь-якої точки світу через ваш смартфон. Ви можете вмикати або вимикати систему, переглядати статус тривог та отримувати повідомлення про події в режимі реального часу.

- Широкі можливості розширення: Ajax StarterKit може бути легко розширений за потреби. Є можливість додавати додаткові датчики руху, датчики відкриття, камери спостереження та інші пристрої для збільшення обсягу моніторингу та безпеки вашого будинку.

- Безпечність і конфіденційність: Ajax забезпечує високий рівень захисту ваших персональних даних та конфіденційності інформації про ваш будинок, що робить його надійним і безпечним засобом захисту.

					КС КРБ 123. 22-320.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		14

Завдяки цим особливостям, Ajax StarterKit є ідеальним вибором для тих, хто цінує простоту, надійність та ефективність у системі безпеки свого приватного будинку.



Рисунок 1.1 – Охоронна система Ajax StarterKit

Дана система орієнтована на приватний сектор та звичайних людей, що робить її досить доступною та зрозумілою для широкого кола користувачів. Незалежно від того, чи є ви досвідченим користувачем технологій, або ви розпочинаєте знайомство з системами безпеки, Ajax StarterKit надає простий та інтуїтивно зрозумілий інтерфейс, який дозволяє швидко налаштувати та керувати вашою системою. Багатофункціональний мобільний додаток, надійний бездротовий зв'язок та можливість розширення роблять цю систему ідеальним вибором для будь-якого, хто прагне забезпечити безпеку свого будинку з мінімальними зусиллями.

					КС КРБ 123. 22-320.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		15

1.3.2 Система охорони CoVi security HS-800

CoVi Security HS-800 - це інноваційна система безпеки, спеціально розроблена для надійного захисту приватних будинків. Оснащена передовими технологіями та функціями, вона забезпечує високий рівень безпеки та комфорту для користувачів.

Основні характеристики системи CoVi Security HS-800 включають:

- Бездротовий зв'язок: Система працює на основі бездротових технологій, що спрощує її встановлення та забезпечує надійний зв'язок між компонентами.
- Мобільний додаток: Вбудований мобільний додаток дозволяє користувачам зручно керувати системою з будь-якої точки світу через смартфон або планшет. Ви можете отримувати повідомлення про тривоги, переглядати відеозаписи та керувати налаштуваннями за допомогою цього додатку.
- Датчики руху та відкриття: Високочутливі датчики руху та датчики відкриття дверей та вікон надійно захищають ваш будинок від несанкціонованого доступу.
- Камери відеоспостереження: Система підтримує підключення камер відеоспостереження, що дозволяє вам в реальному часі спостерігати за подіями, які відбуваються в вашому будинку, та зберігати записи на сервері.
- Автономне живлення: Забезпечена автономним живленням, система продовжує працювати навіть при відключенні електропостачання.

CoVi Security HS-800 - це надійний та ефективний спосіб забезпечити безпеку вашого будинку. Із цією системою ви можете бути впевнені, що ваше майно та ваша родина захищені від будь-яких потенційних загроз.

Також система безпеки CoVi Security HS-800 (рис. 1.2) має численні переваги, які роблять її привабливим вибором для користувачів:

- Надійність: CoVi Security HS-800 використовує передові технології, які гарантують надійний захист приватного будинку. Високочутливі датчики та надійний бездротовий зв'язок забезпечують швидке виявлення потенційних загроз та надсилання тривог до користувача.

					КС КРБ 123. 22-320.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		16

- Зручність у використанні: Інтуїтивний і простий у використанні мобільний додаток дозволяє зручно керувати системою з будь-якої точки світу. Користувач може отримувати повідомлення про тривоги, переглядати відеозаписи та налаштовувати параметри системи зі свого смартфона або планшета.

- Висока ефективність: Система CoVi Security HS-800 забезпечує ефективний захист будинку завдяки високочутливим датчикам руху та відкриття, а також можливості підключення камер відеоспостереження.

- Гнучкість та розширюваність: Система дозволяє гнучко налаштовувати параметри та розширювати функціонал за потребою. Ви можете додавати додаткові датчики, камери та інші пристрої для більш повного захисту вашого будинку.

- Автономне живлення: Вбудований джерело живлення дозволяє системі продовжувати працювати навіть при відключенні електропостачання, що робить її надійним засобом захисту в умовах екстремальних ситуацій.



Рисунок 1.2 – Охоронна система CoVi security HS-800

					КС КРБ 123. 22-320.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		17

Загалом, система CoVi Security HS-800 - це надійний, зручний та ефективний засіб для захисту вашого будинку та майна від потенційних загроз.

1.3.3 Система безпеки Kerui Alarm G18

Система безпеки Kerui Alarm G18 є інтегрованим комплексом засобів та пристроїв, що спрямовані на захист приватних будинків, офісних приміщень, а також інших об'єктів від несанкціонованого доступу. Та включає в себе компоненти, що працюють спільно для забезпечення повноцінної безпеки.

Основні компоненти системи включають в себе центральну контрольную панель, датчики руху та відкриття, дистанційні пульти, сирени та індикатори оповіщення. Контрольна панель є головним елементом системи, вона приймає сигнали від датчиків і відповідно реагує на потенційні загрози. Датчики руху та відкриття розташовуються в стратегічних місцях для виявлення будь-яких недозволених рухів або відкриття дверей та вікон.

Дистанційні пульти дозволяють користувачам зручно активувати та вимикати систему, а також надсилати тривоги у випадку екстрених ситуацій. Сирени та індикатори оповіщення відповідають за висвітлення або відтворення сигналів тривоги для привернення уваги інших осіб у навколишньому середовищі.

Однією з важливих особливостей системи Kerui Alarm G18 (рис. 1.3) є її гнучкість та розширюваність. Вона може бути легко налаштована для використання в різних умовах та об'єктах, а також підвищена за допомогою додаткових компонентів, які можуть бути додані до системи за потреби користувача.

					КС КРБ 123. 22-320.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		19



Рисунок 1.3 – Охоронна система Kerui Alarm G18

					КС КРБ 123. 22-320.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		19

РОЗДІЛ 2 ПРОЕКТНА ЧАСТИНА

2.1 Розробка узагальненої структури системи для охорони приватного будинку

На початковому етапі проектування системи безпеки для приватного будинку була розроблена узагальнена структурна схема, яка наглядно відображає основні функціональні компоненти системи та зв'язки між ними. Ця структурна схема служить для узагальненого опису призначення системи та її функціональних елементів, а також для визначення їх взаємозв'язків. Вона використовується для загального ознайомлення з принципом роботи системи та показує, як вона взаємодіє з різними компонентами.

Компоненти, які використовуються у розробці пристрою, уявлені у спрощеному вигляді за допомогою умовно-графічних позначень, зазвичай у формі прямокутників різної форми. У внутрішній частині цих прямокутників, які представляють функціональні блоки системи, зазначені найменування, які коротко описують призначення кожного конкретного елемента. Такий підхід дозволяє зручно узагальнити та візуалізувати різні компоненти пристрою для кращого розуміння його структури та функціональності.

Вибір компонентів, які включені до структурної схеми, був проведений на основі сучасних, ефективних та модернізованих мікроелектронних елементів, з урахуванням завдань, що були визначені для проектованої системи в технічному завданні. Загальна структура системи охорони приватного будинку наведена на рис. 2.1.

Змн.	Арк.	№ докум.	Підпис	Дата	КС КРБ 123.22-320.00.00 ПЗ			
Розроб.		Літвінов Л.А.			Проектна частина	Літ.	Арк.	Акрушів
Перевір.		Тиш С.В.					20	
Реценз.		Ясній О.П.				ТНТУ, каф. КС, СІс-42		
Н. контр.		Луцик Н.С.						
Затверд.		Осухівська Г.М.						

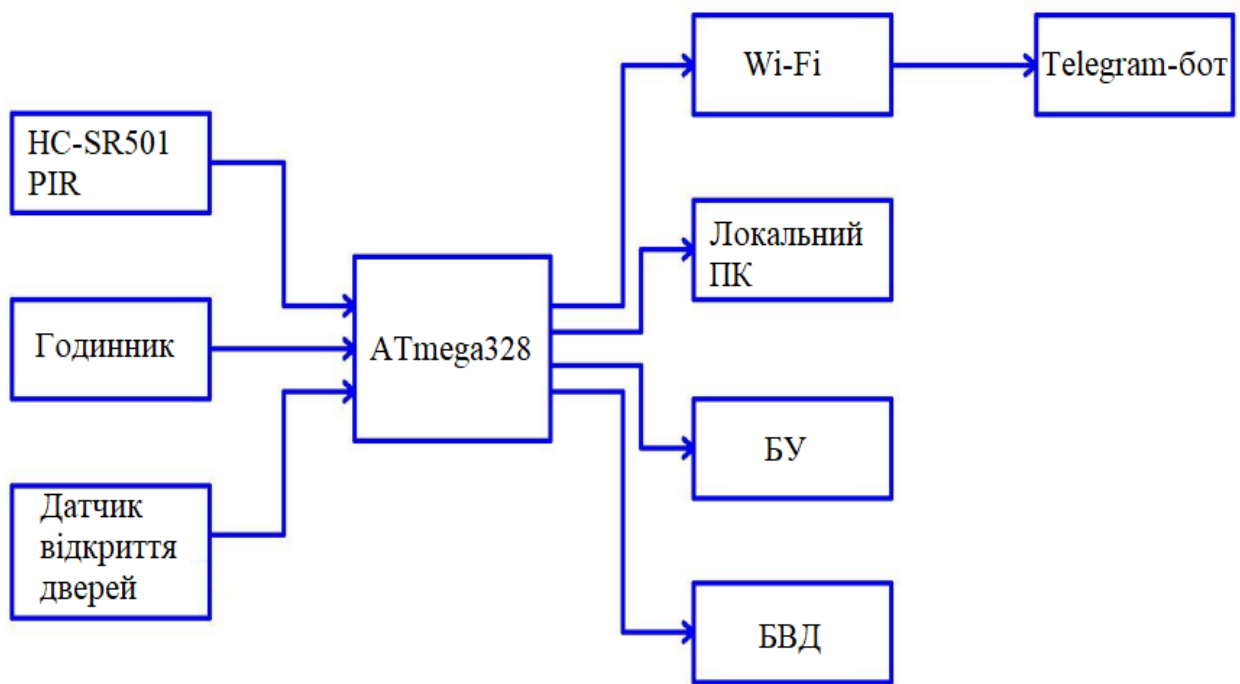


Рисунок 2.1 – Структурна схема системи охорони будинку

Призначення функціональних блоків структурної схеми:

- HC-SR501 PIR – піроелектричний інфрачервоний датчик руху, він виявляє будь-який рух та передає дані в мікроконтролер.
- Датчик відкриття дверей – це датчик, що спрацьовує при відкритті дверей та при виявленні даної дії передає сигнал на мікроконтролер.
- Годинник – годинник реального часу DS1307, передає дані, а саме теперішні дату та час в мікроконтролер.
- ATmega328 – мікроконтролер, який є основою плати Arduino UNO R3 та на основі якого здійснюються всі операції в даній системі.
- Wi-Fi – модуль, який використовується для передачі інформації на телефон користувача, а саме у telegram-бот.
- БВД – блок виводу даних, являє собою LCD-дисплей на який виводиться інформація і чотири світлодіоди: 1 – RGB світлодіод, індикатор проникнення, 2 – RGB світлодіод, індикатор стану системи, зелений активний стан, червоний пасивний стан, 3 – світлодіод зеленого кольору, індикатор живлення і 4 – світлодіод червоного кольору, індикатор помилки.

- БУ – блок управління, який складається із клавіатури та 2 кнопок, перша кнопка служить для ввімкнення або вимкнення живлення, друга для зміни стану системи з активного на пасивний, або навпаки, клавіатура служить для введення коду доступу;

- Telegram-бот – це система, що перенаправляє дані та дозволяє керувати охоронною системою через телефон користувача;

- Локальний ПК – це комп'ютер, що підключений до системи, який дозволяє безпосередньо керувати та змінювати її параметри.

2.2 Обґрунтування вибору апаратного забезпечення комп'ютеризованої системи для моніторингу водопостачання

2.2.1 Вибір елементної бази

Відповідно до технічного завдання, комп'ютеризована система для моніторингу водопостачання розробляється на основі мікроконтролерної платформи Arduino Uno. Ця платформа забезпечує необхідну гнучкість та надійність для виконання різноманітних функцій системи, включаючи збір, обробку та передачу даних про стан водопостачання. Arduino Uno дозволяє легко інтегрувати різноманітні датчики та виконавчі пристрої, що робить її ідеальною для побудови ефективною та масштабованою системи моніторингу.

В якості головного керуючого елемента в проєктованій системі використовується восьмирозрядний мікроконтролер фірми ATMEL – Atmega328P. Платформа Arduino Uno включає чотирнадцять цифрових входів/виходів загального призначення (шість з яких можуть використовуватися як виходи ШІМ), шість аналогових входних виводів, кнопку перезавантаження, кварцовий резонатор з частотою 16 МГц, роз'єм USB, роз'єм для підключення зовнішнього джерела живлення і роз'єм ICSP.

Для початку роботи необхідно підключити платформу до ПК за допомогою USB-кабелю або подати живлення через акумуляторну батарею чи адаптер AC/DC.

					КС КРБ 123. 22-320.00.00 ПЗ	Арк.
						22
Змн.	Арк.	№ докум.	Підпис	Дата		

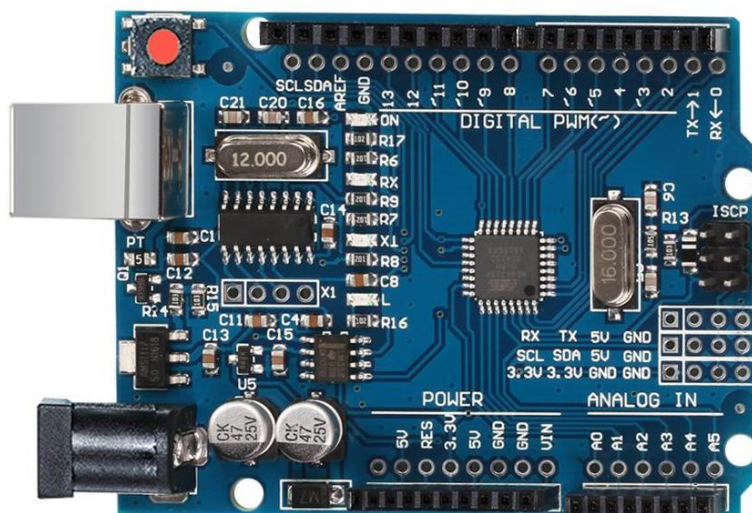


Рисунок 2.3 – Зовнішній вигляд плати Arduino Uno

Платформа Arduino Uno може живитися від зовнішнього джерела постійного струму в діапазоні від 6 В до 20 В. Однак, якщо напруга живлення падає нижче 7 В, вихідний контакт 5 В може видавати напругу менше 5 В, що може призвести до нестабільної роботи платформи. При підключенні до напруги живлення понад 12 В стабілізатор напруги може перегріватися, що може пошкодити плату. Тому виробники рекомендують використовувати оптимальний діапазон напруги від 7 В до 12 В для забезпечення стабільної та безпечної роботи платформи.

Кожен із чотирнадцяти цифрових виводів Arduino Uno можна налаштувати для використання як вхід або вихід, використовуючи функції `pinMode()`, `digitalRead()` та `digitalWrite()`. Виводи працюють при напрузі 5 В. Кожен вивід може бути підключений до навантажувального резистора номіналом 20-50 кОм (який за замовчуванням відключений) і здатний пропускати струм до 40 мА. Крім того, ці виводи можуть бути використані для підключення різних датчиків і виконавчих пристроїв, що робить платформу Arduino Uno гнучкою та універсальною.

Розміри друкованої плати Arduino Uno складають 5,3 см у ширину та 6,9 см у довжину. USB-роз'єм та роз'єм для підключення зовнішнього блоку живлення виступають за ці габарити.

					КС КРБ 123. 22-320.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		24

Технічний опис контролера ATmega328P:

- Висока продуктивність, низька потужність.
- Прогресивна RISC-архітектура.
- Набір команд, що включає 131 інструкцію.
- 32 8-бітних робочих реєстри загального призначення.
- Повністю статичні операції.
- До 20 MIPS пропускної здатності при частоті 20 МГц.
- Високопродуктивні енергонезалежні сегменти пам'яті.
- Система самопрограмованої флеш-пам'яті об'ємом 4/8/16/32 Кбайт.
- 256/512/512/1К байт EEPROM (ATmega48P/88P/168P/328P).
- 512/1К/1К/2К байт внутрішня SRAM (ATmega48P/88P/168P/328P).
- Кількість циклів стирання/запису: 100,000 EEPROM / 10,000 Flash.
- Тривалість зберігання даних: 100 років при температурі 25 °С / 20 років при 85 °С.

Периферійні особливості:

- Два 8-розрядних таймери/лічильники з режимом порівняння та роздільним прескалером.
 - Один 16-розрядний таймер/лічильник з режимом порівняння та окремим попереднім дільником.
 - Шестиканальний ШІМ.
 - Восьмиканальний 10-бітний АЦП в TQFP і QFN/МФ пакеті.
 - Шести-канальний 10-бітний АЦП в PDIP пакеті.
 - Програмований сторожовий таймер з окремим вбудованим генератором.
 - Програмований послідовний інтерфейс USART.
 - Аналоговий вбудований компаратор.
 - Послідовний інтерфейс SPI Master/Slave.
- #### Особливості мікроконтролера:
- Внутрішній калібрований генератор.
 - Скидання після включення живлення.

					КС КРБ 123. 22-320.00.00 ПЗ	Арк.
						25
Змн.	Арк.	№ докум.	Підпис	Дата		

- Режими сну: зниження енергоспоживання, при відключенні живлення, у режимі очікування.

- Зовнішні та внутрішні джерела переривань.
- 23 програмованих входи/виходи.

Робоча напруга:

- 1,8 В - 5,5 В для АТmega48P/88P/168PV.
- 2,7 В - 5,5 В для АТmega48P/88P/168P.
- 1,8 В - 5,5 В для АТМЕГА328P.

Діапазон робочих температур:

- Від -40 °С до 85 °С.
- Активний режим: 0,3 мА.
- Режим відключення живлення: 0,1 мкА.
- Режим економії енергії: 0,8 мкА (включаючи 32 кГц RTC).

На рис. 2.4 зображено позначення виводів контролера АТmega328P.

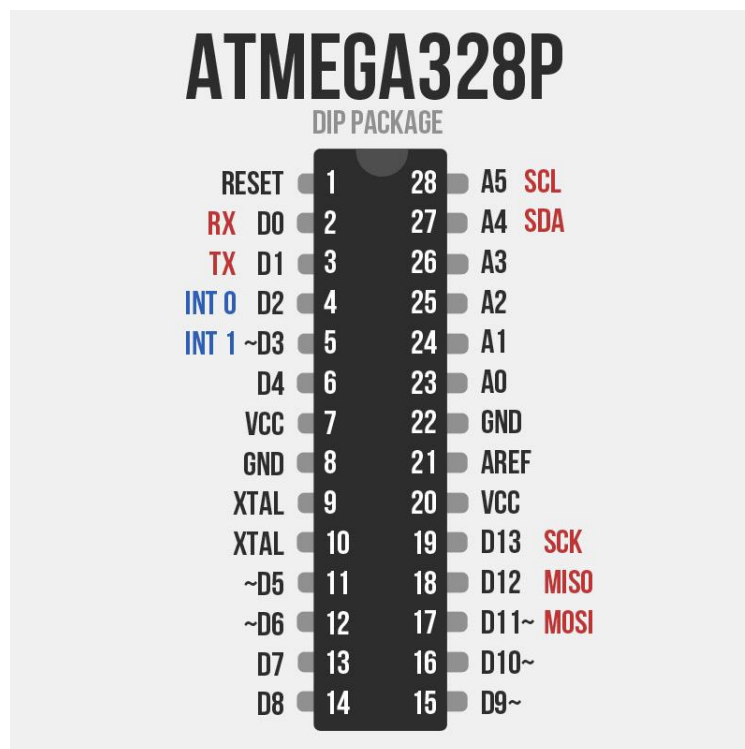


Рисунок 2.4 – Позначення виводів контролера АТmega328P

2.2.2 Датчик руху та датчик відкриття дверей

Для виявлення руху у даній системі використовується піроелектричний інфрачервоний датчик руху HC-SR501(рис. 2.5, рис. 2.6).

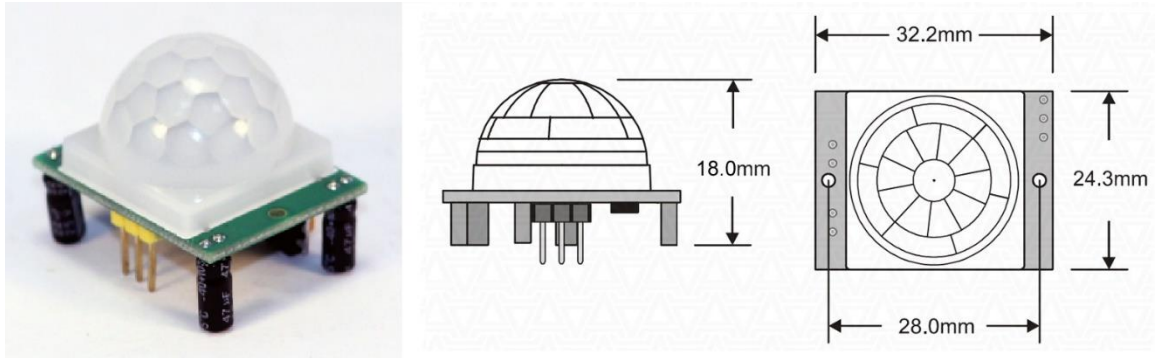


Рисунок 2.5 – Зовнішній вигляд та габарити датчика руху HC-SR501

Основні характеристики HC-SR501 вказано в табл. 2.1.

Таблиця 2.1 – Основні характеристики датчика HC-SR501

Напруга живлення	DC 4.5V- 20V
Дистанція виявлення	3 - 7м(можна налаштувати)
Кут виявлення	до 120°-140°
Тривалість імпульсу при виявленні	5 - 200сек(можна налаштувати)

Опис виводів:

- Vcc – вивід живлення, 3.3V.
- P0.4 –вивід для обміну даними.
- GND – спільний вивід (земля).

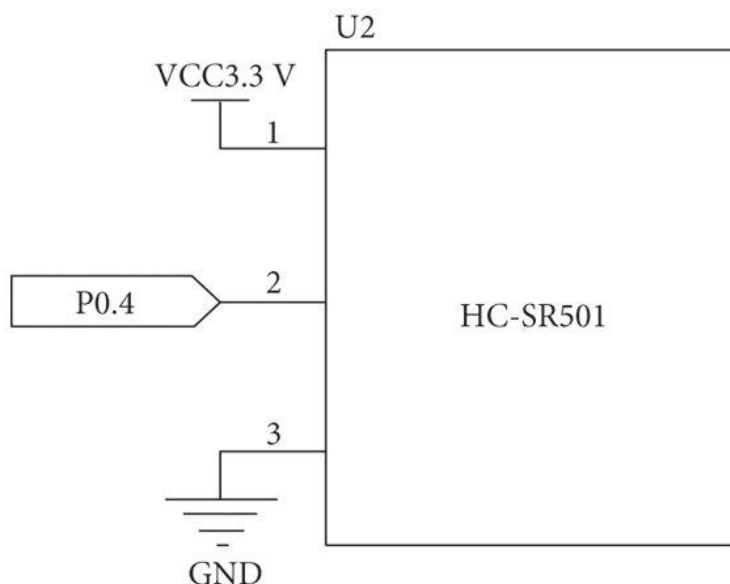


Рисунок 2.6 – Умовне графічне позначення HC-SR501

Датчик відкриття по суті є датчиком згинання, розміщеним у зручному корпусі для використання. Він встановлюється таким чином, що одна частина кріпиться до дверей, а інша – до стіни. Коли двері відкриваються, датчик згинається, що дозволяє виявити факт відкриття дверей та передати відповідний сигнал до системи. Цей механізм забезпечує ефективний контроль над доступом до приміщення, попереджаючи про несанкціоноване проникнення.

У даному випадку був використаний датчик згину Flex Sensor 2.2 (рис. 2.7). без додаткового корпусу. Цей датчик дозволяє легко інтегрувати його в систему та використовувати для виявлення відкриття дверей або вікон.



Рисунок 2.7 – Зовнішній вигляд датчика згину Flex Sensor 2.2

					КС КРБ 123. 22-320.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		28

На рис. 2.8 зображено умовне позначення датчика згину Flex Sensor 2.2.

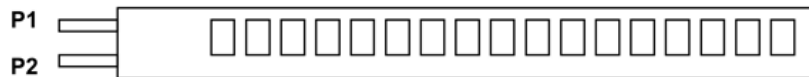


Рисунок 2.8 – Умовне позначення датчика згину Flex Sensor 2.2

2.2.3 Wi-Fi модуль

Для передачі даних користувачу, використовується Wi-Fi модуль для Arduino, який забезпечує зручне підключення пристрою до локальної мережі або інтернету. Цей модуль дозволяє системі на базі Arduino, обмінюватися даними з будь-якої точки світу, через Інтернет-з'єднання. На рис. 2.9 зображено зовнішній вигляд Wi-Fi модуля.

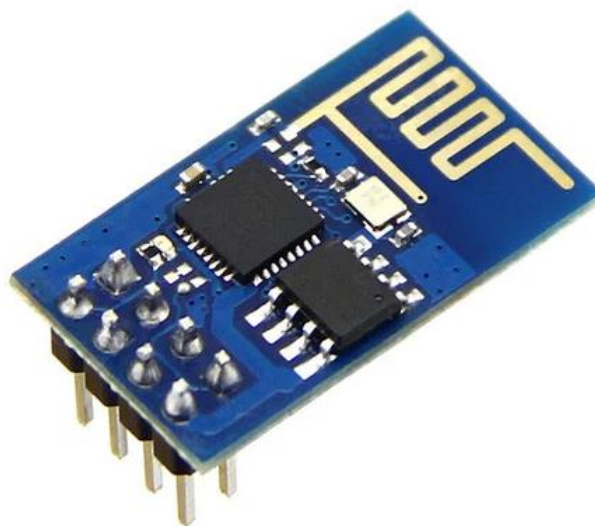


Рисунок 2.9 – Зовнішній вигляд Wi-Fi модуля

На рис. 2.10 зображено позначення Wi-Fi модуля на схемі електричній принциповій.

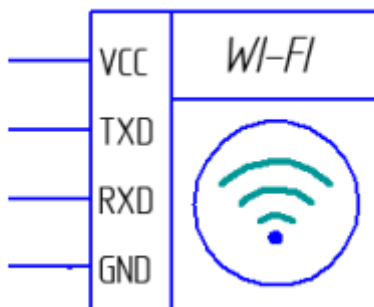


Рисунок 2.10 – Умовне позначення Wi-Fi модуля

Wi-Fi модуль базується на чіпі WIZnet W5100, який володіє внутрішнім буфером об'ємом 16 кбайт. Цей модуль підтримує швидкості передачі даних 10/100 Мбіт/с. Щоб працювати з Wi-Fi модулем програмно, необхідно підключити бібліотеку Arduino Ethernet, яка автоматично встановлюється разом з середовищем розробки Arduino IDE.

Також на платі є слот для карти пам'яті microSD, на яку можна записувати та зчитувати інформацію. Для роботи з цією картою також потрібна відповідна бібліотека.

2.2.4 Telegram-бот

Для зручного отримання даних користувачем і контролю над системою буде використано Telegram-бот. Цей метод є простішим у порівнянні зі створенням власного додатка або веб-сайту, що зробить систему більш доступною за вартістю. Telegram-боти дозволяють отримувати сповіщення в реальному часі, керувати налаштуваннями системи, а також взаємодіяти з іншими компонентами системи через зручний інтерфейс мобільного додатка.

У даній роботі не було доцільно створювати бота з нуля, тому було використано готове рішення - бот-конструктор BotFather, який дозволяє швидко і легко створювати інші боти. BotFather надає широкі можливості для Налаштування та управління ботами, включаючи генерацію токенів доступу,

налаштування команд та опису бота, а також інтеграцію з іншими сервісами.

Основні переваги використання Telegram-бота в системі охорони:

- Миттєві сповіщення: Користувач отримує повідомлення про спрацьовування датчиків або інші важливі події в режимі реального часу.
- Віддалене керування: Користувач може керувати системою охорони, змінювати налаштування та отримувати інформацію про стан системи з будь-якої точки світу.
- Простота інтеграції: Використання готового бот-конструктора значно спрощує процес створення та налаштування бота, що зменшує час та витрати на розробку.
- Безпека: Всі повідомлення в Telegram захищені шифруванням, що забезпечує високий рівень конфіденційності та безпеки даних.
- Кросплатформеність: Telegram-додаток доступний на різних платформах, включаючи Android, iOS, Windows, MacOS та Linux, що забезпечує зручний доступ до системи охорони для користувачів з різними пристроями.

Використання Telegram-бота як інтерфейсу для системи охорони дозволяє забезпечити високу функціональність та зручність використання, одночасно знижуючи загальну вартість системи та час її розробки.

2.2.5 Модуль з мікросхемою годинника реального часу DS1307

Мікросхема DS1307 (рис. 2.11) годинника реального часу з послідовним інтерфейсом, це малопотужний двійково-десятковий годинник-календар, який також містить незалежну статичну пам'ять об'ємом 56 байт. Передача даних та адрес здійснюється послідовно по шині з двома провідниками. Годинник-календар відраховує рік, місяць, дату, день, години, хвилини та секунди. Остання дата кожного місяця змінюється автоматично для місяців з кількістю днів менше 31, враховуючи корекцію високосного року. Годинник може функціонувати як у двадцяти чотирьох годинному, так і в дванадцяти годинному режимах.

Модуль DS1307 має вбудовану схему контролю живлення, яка виявляє перебої у подачі вхідної напруги і автоматично перемикається на живлення від

					КС КРБ 123. 22-320.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		31

акумуляторної батареї. Це дозволяє зберігати точний час навіть у випадку втрати основного джерела живлення, забезпечуючи безперервну роботу системи.

Особливості DS1307:

- Низьке енергоспоживання: Мікросхема споживає дуже мало енергії, що робить її ідеальною для використання в енергоефективних системах.
- Послідовний інтерфейс I2C: Простий у використанні інтерфейс для передачі даних і адрес, що забезпечує легку інтеграцію з іншими компонентами.
- Автоматичне коригування дати: Автоматична зміна останньої дати кожного місяця з урахуванням високосних років.
- Гнучкі режими роботи: Підтримка як 24-годинного, так і 12-годинного режимів роботи з індикатором АМ/РМ.
- Резервне живлення: Вбудована схема контролу живлення дозволяє мікросхемі автоматично перемикатися на живлення від акумулятора у разі перебоїв з основним живленням, забезпечуючи безперервну роботу годинника.

Ця мікросхема є надійним і простим у використанні рішенням для даного проєкту, де необхідно точно відстежувати час і дату, незалежно від наявності основного джерела живлення.

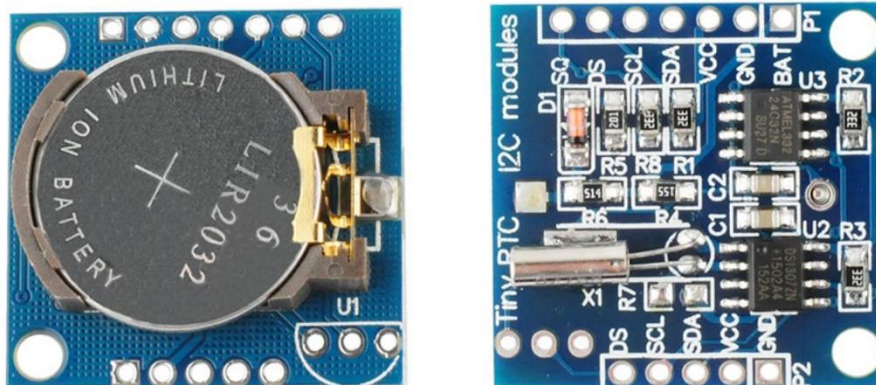


Рисунок 2.11 – Зовнішній вигляд мікросхеми годинника реального часу DS1307

На рис. 2.12 зображено умовне позначення годинника реального часу.

Змн.	Арк.	№ докум.	Підпис	Дата

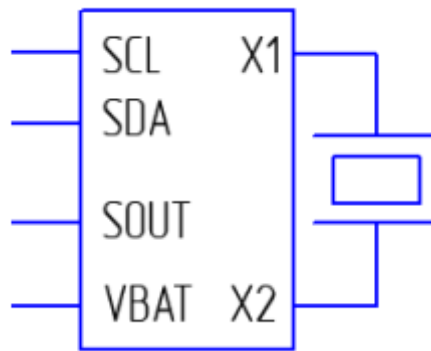


Рисунок 2.12 – Умовне позначення мікросхеми годинника реального часу
DS1307

2.2.6 LCD-дисплей

Для відображення текстової та цифрової інформації в системі використовується LCD-дисплей на базі контролера HD44780(рис. 2.13). Дисплей має роздільну здатність 16x2.

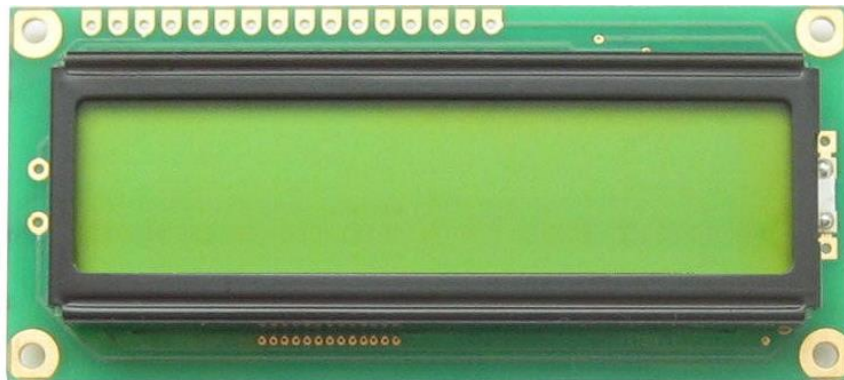


Рисунок 2.13 – Зовнішній вигляд LCD-дисплею HD44780

На рис. 2.14 зображено умовне позначення LCD-дисплею HD44780.



Рисунок 2.14 – Умовне позначення LCD-дисплею HD44780

Для оптимізації використання виводів контролера та полегшення процесу виведення інформації на дисплей застосовується модуль I2C на базі контролера вводу/виводу PCF8574 (рис. 2.15), який функціонує як "розширювач портів". Це дозволяє підключити дисплей до контролера з використанням лише кількох виводів, значно спрощуючи підключення.

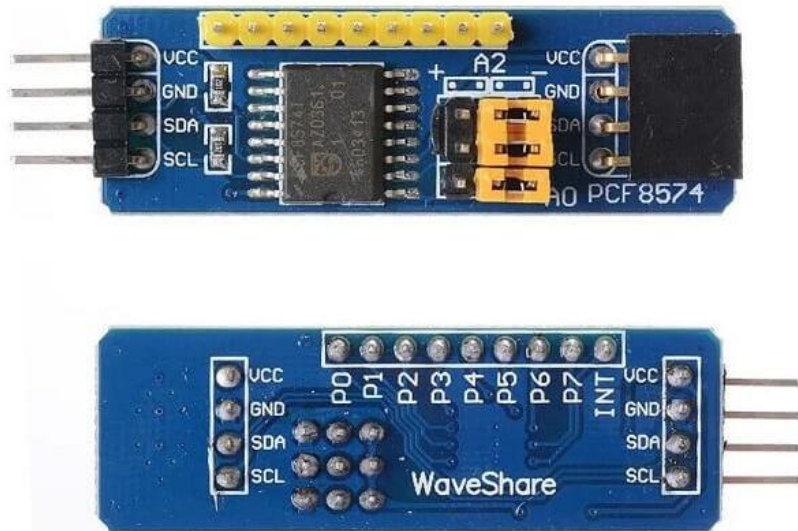


Рисунок 2.15 – Зовнішній вигляд модуля I2C на базі PCF8574

На рис. 2.16 зображено умовне позначення модуля I2C на базі PCF8574.

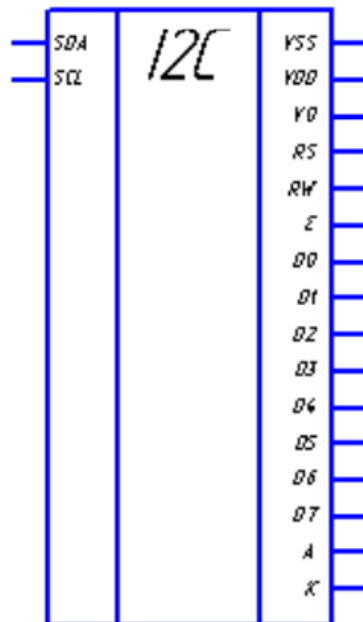


Рисунок 2.16 – Умовне позначення модуля I2C

Передача інформації для виводу на LCD-дисплей здійснюється через шину I2C, конкретно через виводи "SDA" та "SCL". На схемі підключення LCD-дисплею до мікросхеми PCF8574, зображеній на рис. 2.17, видно, що виводи "SDA" та "SCL" мікросхеми PCF8574 підключаються до відповідних виводів контролера.

Основні характеристики мікросхеми PCF8574 включають:

- Робочий режим живлення від 2,5 до 6 В, що дозволяє широкий діапазон напруги живлення.
- Низький струм спокою до максимуму 10 мА, що забезпечує економію енергії.
- Інтерфейс I2C для підключення до контролера, що розширює паралельний порт.
- Вихід переривання з відкритим стоком, що дозволяє використовувати його для взаємодії з іншими пристроями.
- Дистанційний 8-бітний розширювач введення-виведення для I2C-шини, що спрощує керування з великою кількістю пристроїв.
- Сумісність з більшістю мікроконтролерів, що робить його універсальним рішенням для різних аплікацій.

- Виходи з регістром-клямкою з високими характеристиками по струму для прямої передачі сигналу на світлодіоди.
- Можливість адресації до 3 виведень апаратних адрес для використання з до 8 пристроями (до 16 пристроїв при використанні PCF8574A).
- Підтримка різних корпусів, таких як DIP16, компактний SO16 і SSOP20, що дозволяє легко інтегрувати мікросхему в різні типи систем.

Ці характеристики роблять PCF8574 ідеальним вибором для використання як розширювача портів для LCD-дисплеїв у системах з обмеженим числом виводів контролера.

На рис. 2.17 зображено схему підключення LCD-дисплею модуля I2C на базі PCF8574.

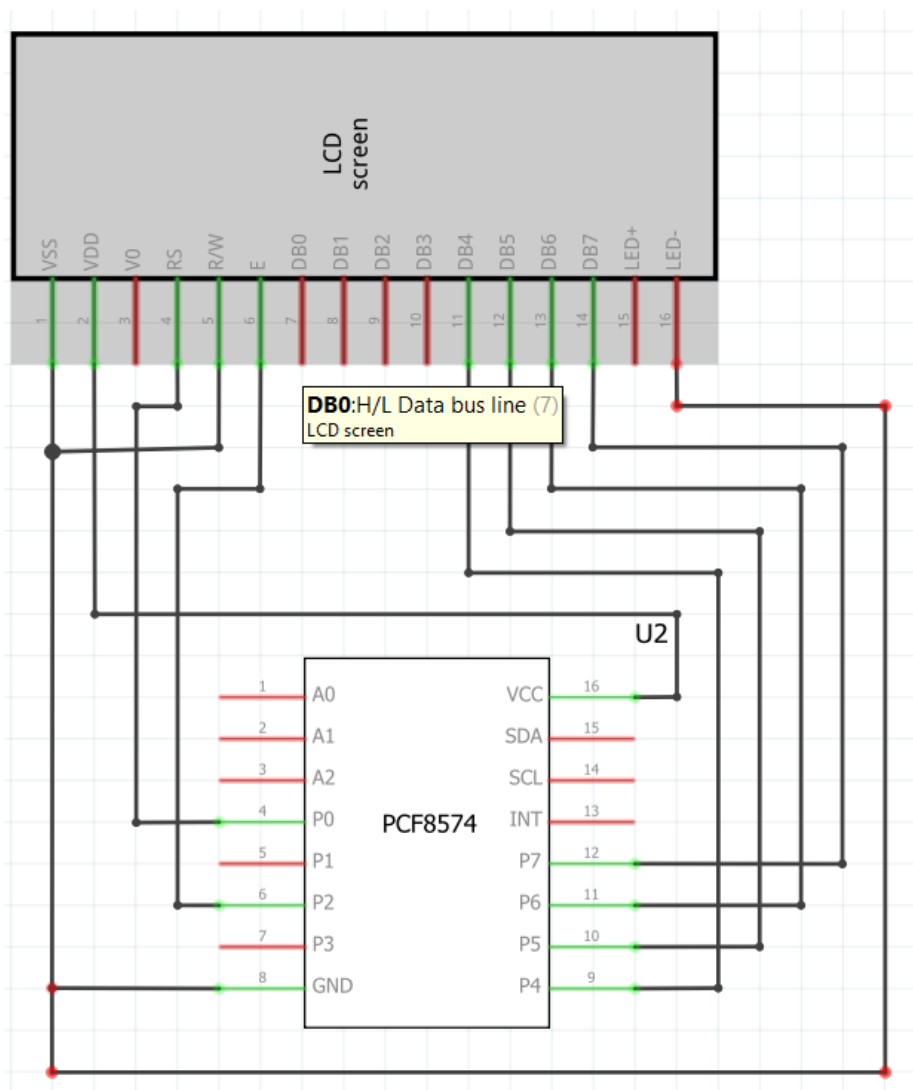


Рисунок 2.17 – Схема підключення LCD-дисплею до мікросхеми PCF8574

2.3 Обґрунтування вибору програмних засобів для системи охорони

2.3.1 Середовище розробки Arduino

Для розробки програмного забезпечення для мікроконтролерів Arduino інтегроване середовище розробки (IDE) Arduino є вельми корисним і популярним інструментом. Його кросплатформенний характер означає, що можна використовувати його на будь-якій операційній системі: Windows, macOS або Linux, що робить його доступним для широкого кола розробників.

Arduino IDE пропонує простий інтерфейс, що дозволяє швидко та легко створювати програмний код. Вона містить в собі всі необхідні інструменти для розробки прошивки мікроконтролерів Arduino, включаючи текстовий редактор для написання коду, компілятор для перетворення програмного коду у машинний код, а також інтерфейс для завантаження цього коду на мікроконтролер.

Однією з ключових переваг Arduino IDE є широкий вибір бібліотек і прикладів коду, що дозволяє швидко і ефективно інтегрувати різноманітні пристрої і сенсори у проекти. Також є можливість створювати власні бібліотеки та розширювати функціональні можливості проекту, що робить Arduino IDE відмінним вибором для даного проекту.

2.3.2 Робота з telegram-ботом

Для ефективної передачі даних про безпеку будинку до користувача використовуються спеціалізовані додатки, що ідуть у комплекті із системами, які існують на ринку. Ці додатки призначені спеціально для інтеграції з цими системами і забезпечують швидкий доступ до інформації про стан безпеки. Хоча веб-сайти також можуть використовуватися, цей метод вважається менш ефективним і застарілим у сучасних умовах.

Оскільки дана система має обмежений бюджет, жоден із зазначених методів не підходить для використання у цьому проекті була використовується

					КС КРБ 123. 22-320.00.00 ПЗ	Арк.
						37
Змн.	Арк.	№ докум.	Підпис	Дата		

передача даних через telegram-бота. Цей підхід є зручним і економічно доцільним, оскільки не потребує розробки бота з нуля. Для створення бота використовується інструмент під назвою BotFather.

					КС КРБ 123. 22-320.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		38

РОЗДІЛ 3 ПРАКТИЧНА ЧАСТИНА

3.1 Розробка алгоритмів роботи системи охорони приватного будинку

Для забезпечення коректної роботи системи охорони, вона повинна функціонувати за чітко визначеним алгоритмом. Алгоритм – це набір інструкцій, які визначають порядок дій, необхідних для досягнення бажаного результату.

Таким чином, для розробки програми охорони будинку було створено наступний алгоритм:

Ініціалізація системи:

- Підключення до датчиків.
- Оголошення змінних.
- ініціалізація COM-порту, LCD дисплею, портів вводу-виводу, Wi-Fi модулю.
- Підключення до Telegram API для надсилання повідомлень.
- Перевірка на відповідь Telegram-бота, при відсутності відповіді, запустити світлодіод помилки.
- Перевірка натискання кнопки для переведення системи у пасивний режим, при натисканні змінити змінну P на 1.

Режим роботи системи:

- Перевірка чи змінна $P = 1$.
- Якщо так: вимкнути сповіщення при спрацюванні датчиків, увімкнути другий RGB світлодіод у червоний режим, вимкнути перший RGB світлодіод.
- Якщо ні: перевести систему сповіщення в активний режим, увімкнути перший RGB світлодіод, увімкнути другий RGB світлодіод у зелений режим

Змн.	Арк.	№ докум.	Підпис	Дата	КС КРБ 123.22-320.00.00 ПЗ			
Розроб.		Літвінов Л.А.			Практична частина	Літ.	Арк.	Акрушів
Перевір.		Тиш С.В.					39	
Реценз.		Ямній О.П.				ТНТУ, каф. КС, СІс-42		
Н. контр.		Луцик Н.С.						
Затверд.		Осухівська Г.М.						

Фіксація змінної P:

- Фіксувати змінну P, доки не буде введено вірний пароль через клавіатуру.

Зчитування сигналу з клавіатури:

- При введенні даних, записати їх у змінні K, E, Y, S.
- Увімкнути LCD-дисплей.
- Вивести змінні K, E, Y, S на LCD-дисплей.

Порівняння введених змінних з системним паролем:

- Якщо введений код вірний, вивести на LCD-дисплей підтвердження вводу та зчитувати дані з кнопки стану системи до внесення даних у змінну P, після знову зафіксувати змінну.

- Якщо код невірний, вивести на LCD-дисплей повідомлення про невірний код

Зчитування даних з сенсорів:

- Занести дані у змінні (0 - відсутність даних, 1 - наявність).
- Перевірка змінних зі зчитаними даними.
- Якщо усі змінні рівні нулю, повернутись до зчитування даних.
- Якщо будь-яка змінна рівна 1, запустити сирену, відправити користувачеві повідомлення через Telegram та очікувати введення паролю з клавіатури або команди від Telegram-бота.

Команда від Telegram-бота:

- При отриманні команди "тихо" від Telegram-бота, внести число 1 у змінну P.

3.2 Створення інтерфейсу користувача

Оскільки взаємодія користувача із системою здійснюватиметься через Telegram-бота, інтерфейс користувача буде заснований на програмі Telegram.

					КС КРБ 123. 22-320.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		40

Для створення такого бота необхідно виконати наступні кроки:

- Відкрити Telegram та знайти бота під назвою BotFather (рис. 3.1).
- Використати команду `/newbot` для створення нового бота.
- Слідувати інструкціям BotFather, щоб надати новому боту назву та ім'я користувача. Назва може бути будь-якою, проте ім'я користувача має бути унікальним і закінчуватись на "bot". У нашому випадку це буде TsecuritysisBot.

- Використати команду `/setcommands` для налаштування команд, на які бот буде реагувати. Наприклад, `/start` почати роботу, `/on` ввімкнути охоронну систему, `/off` вимкнути охоронну систему, `/mute` - вимкнути систему оповіщення.

- Використати команду `/token` для отримання API токена, необхідного для зв'язку системи з ботом. У даному випадку отриманий токен виглядає так: 6425220751:AAEdPK19E8GtL6q8BgT-T5pgxTnkvTf6kYU.

- За допомогою команди `/setdescription` налаштувати повідомлення, які бот буде надсилати у відповідь на команди та у випадку проникнення.

					КС КРБ 123. 22-320.00.00 ПЗ	Арк.
						41
Змн.	Арк.	№ докум.	Підпис	Дата		

Про бота



BotFather

бот



BotFather — єдиний бот, який керуватиме всіма. Використовуйте його для створення нових облікових записів ботів і керування існуючими ботами.

Опис

@BotFather

Ім'я користувача



Сповіщення



НАПИСАТИ



З поширених посилання



Поскаржитися



Зупинити й заблокувати бота

Рисунок 3.1 – Обліковий запис BotFather у telegram

Для зручного користування бот має відповідати на команди користувача наступним чином:

- Команда `/start`: "Вітаю! Бот активовано. Використовуйте наступні команди для керування охоронною системою: `/on`, `/off`, `/mute`."
- Команда `/on`: "Охоронну систему запущено. Всі сенсори працюють нормально."
- Команда `/off`: "Охоронну систему вимкнено. Усі сенсори в режимі очікування та не фіксують даних."
- Команда `/mute`: "Система оповіщення вимкнена. Ви більше не отримуватимете сповіщення про проникнення."
- Повідомлення у випадку проникнення: "Увага! Виявлено проникнення у захищену зону! У разі потреби зв'яжіться з правоохоронцями!"

					КС КРБ 123. 22-320.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		42

3.3 Тестування системи охорони приватного будинку

Ця система призначена для охорони приватного будинку, виявлення будь-яких спроб проникнення та інформування власника про події. Сповіщення здійснюється як локально, у будинку, за допомогою звукових сигналів, так і віддалено через Telegram-бота. Крім того, система підтримує два режими керування: віддалений через Telegram-бота та безпосередній через локальну систему контролю.

На рис. 3.2 зображено модель зовнішнього вигляду панелі контролю системи безпеки.

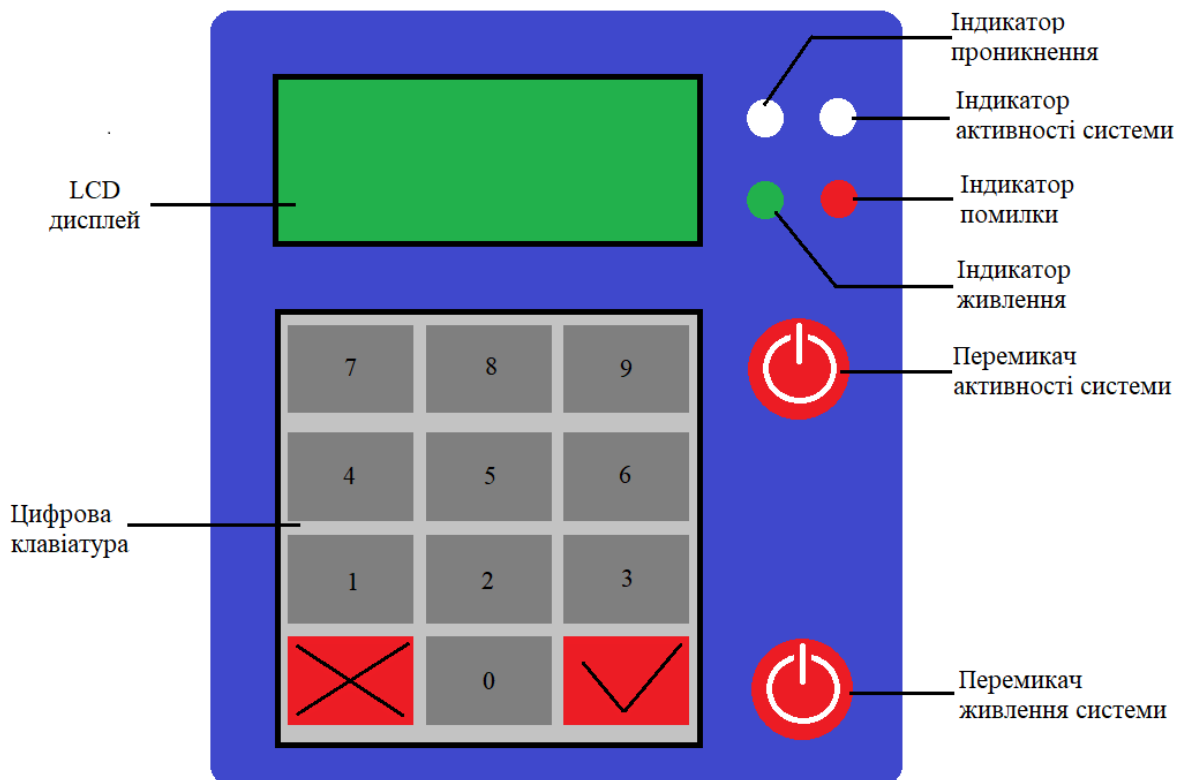


Рисунок 3.2 – Модель зовнішнього вигляду панелі керування

Для повного тестування системи необхідно перевірити функціонування кожного з її аспектів. Це включає перевірку виявлення проникнень, локального звукового оповіщення, віддалених сповіщень через Telegram-бота, а також обох режимів керування – віддаленого та прямого через локальну систему контролю.

Пристрій зчитує сигнали з таких датчиків:

- Датчик руху.
- Датчик згинання (відкриття дверей, вікон).

Для індикації результатів роботи і стану системи, а також для кращої взаємодії між користувачем та пристроєм, використовуються такі компоненти:

- LCD-дисплей для відображення даних.
- RGB-світлодіод «Індикатор стану системи», який змінює свій колір залежно від режиму системи.
- RGB-світлодіод «Індикатор проникнення», який змінює свій колір залежно від того, чи виявлено проникнення одним з сенсорів.
- Світлодіод зеленого кольору «Індикатор живлення» для індикації стану живлення.
- Світлодіод червоного кольору «Індикатор помилки» для індикації системної чи апаратної помилки.
- Кнопка ввімкнення/вимкнення системи.
- Кнопка зміни режиму роботи системи.
- Клавіатура для доступу до системи.
- Годинник реального часу для забезпечення точного часу в системі.

Ці компоненти забезпечують зручність використання, надійність роботи та інформативність для користувача.

Після серії ретельних тестувань було встановлено, що система працює правильно та надійно. Повідомлення до Telegram-бота надходять миттєво, забезпечуючи оперативне інформування власника про стан системи та можливі загрози. Віддалені команди, надіслані через Telegram-бота, виконуються без затримок, що дозволяє ефективно керувати системою з будь-якої відстані.

На рис. 3.3 зображено приклад роботи сповіщення та керування системою через telegram-бота.

					КС КРБ 123. 22-320.00.00 ПЗ	Арк.
						44
Змн.	Арк.	№ докум.	Підпис	Дата		

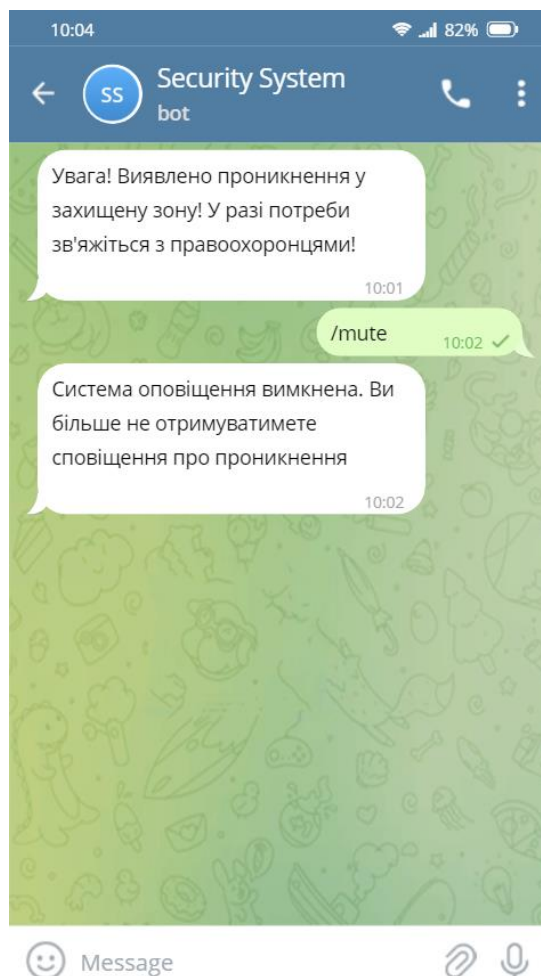


Рисунок 3.3 – Приклад роботи з системою через telegram-бот

Система демонструє високу чутливість та точність у виявленні руху та відкриття дверей або вікон. Індикація на LCD-дисплеї та через RGB-світлодіоди чітко відображає поточний стан системи, а також реагує на будь-які зміни режиму роботи або виявлені проникнення. Крім того, зелені та червоні світлодіоди надають візуальну інформацію про стан живлення та можливі системні помилки, що сприяє швидкому виявленню та усуненню проблем. Кнопки ввімкнення/вимкнення та зміни режиму роботи працюють відмінно, забезпечуючи користувачеві зручність у керуванні системою.

При увімкненні пристрою до джерела живлення активується зелений світлодіод "Індикатор живлення".

У режимі очікування пристрій не збирає дані з датчиків, і світяться зелений світлодіод "Індикатор живлення" та червоний світлодіод стану системи.

					КС КРБ 123. 22-320.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		45

Коли режим роботи змінено на активний, система переходить у цей режим і реагує на будь-які спроби проникнення. У цьому режимі світлодіод проникнення та світлодіод стану системи світяться зеленим кольором. Якщо один із датчиків спрацьовує, спрацьовує тривога, а світлодіод проникнення змінює свій колір на червоний.

					КС КРБ 123. 22-320.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		46

РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

Оскільки у кваліфікаційній роботі розглядається питання створення системи безпеки приватного будинку, то у даному розділі доцільно розглянути наступні питання: вплив електромагнітних полів на людину та заходи щодо зменшення їх впливу на мешканців будинку; вимоги пожежної безпеки при гасінні електроустановок

4.1 Вплив електромагнітних полів на людину та заходи щодо зменшення їх впливу жителів будинку

Розвиток електроніки, радіо- та комп'ютерної техніки значно підвищив рівень електромагнітного забруднення природного середовища. Джерела електромагнітних полів (ЕМП) можуть мати як природне, так і антропогенне походження.

Антропогенні джерела включають потужні радіотелевізійні станції, радіолокаційні системи, мобільні зв'язкові станції, комп'ютери з недосконалою екрануванням, високовольтні лінії електрозв'язку, електротранспорт, електростанції та підстанції, промислові установки для високочастотного нагріву, мікрохвильові печі, телевізори, електроплити, праски, холодильники та будь-які інші пристрої, що підключені до електромережі.

Електромагнітні випромінювання, спричинені діяльністю людини, розглядаються як один з видів енергетичних забруднень через їх негативний вплив на здоров'я людини, інші живі організми та екологічні системи. ЕМП передаються у вигляді електромагнітних хвиль, які характеризуються довжиною хвилі, частотою коливань та швидкістю поширення. Напруженість

					КС КРБ 123.22-320.00.00 ПЗ			
<i>Змн.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>	Безпека життєдіяльності, основи охорони праці	<i>Літ.</i>	<i>Арк.</i>	<i>Акрушів</i>
<i>Розроб.</i>	Літвінов Л.А.						47	
<i>Перевір.</i>	Тиш Є.В.							
<i>Консульт.</i>	Пилипець М.І.							
<i>Н. контр.</i>	Луцик Н.С							
<i>Затверд.</i>	Осυχівська Г.М					ТНТУ, каф. КС, СІс-42		

електромагнітного поля вимірюється в одиницях Вольт на метр (В/м) і служить основним показником забруднення.

Розвиток електроніки, радіо- та комп'ютерної техніки призвів до значного зростання електромагнітного забруднення природного середовища. Інтенсивність електромагнітного поля в будь-якій точці простору залежить від потужності джерела випромінювання та відстані до нього. У приміщеннях розподіл поля впливає наявність металевих предметів, що є провідниками, а також діелектриків, що знаходяться у полях.

Зараз рівень інтенсивності електромагнітних полів суттєво зросли через збільшення кількості джерел та їх потужності. У деяких районах цей рівень перевищує санітарні норми на порядки, що має негативний вплив на здоров'я людей, які працюють біля таких джерел випромінювання, а також на мешканців, які проживають поруч.

Електромагнітні поля впливають на організм людини залежно від діапазону частот, інтенсивності впливу, тривалості опромінення, характеру випромінювання та інших факторів. Вони можуть спричиняти різні біологічні реакції, включаючи зміни в роботі нервової системи, серцево-судинної системи, ендокринної системи, порушення функцій внутрішніх органів, а також можуть впливати на клітинний рівень.

Також електромагнітні випромінювання можуть викликати теплові ефекти, спричинюючи підвищення температури тіла і навіть нагрівання тканин. Це може призводити до шкідливих наслідків, таких як недуги та погіршення фізичного стану людини.

Для запобігання впливу електромагнітного випромінювання на здоров'я людини і зменшення ризику захворювань розроблені санітарні норми та правила експлуатації радіотехнічних і електротехнічних об'єктів, які ґрунтуються на медикобіологічних дослідженнях. Ці норми регламентують умови експлуатації з метою захисту населення від шкідливого впливу електромагнітних випромінювань.

					КС КРБ 123. 22-320.00.00 ПЗ	Арк.
						48
Змн.	Арк.	№ докум.	Підпис	Дата		

Для захисту від дії електромагнітних опромінювань застосовуються різні технічні і організаційні заходи:

- Зменшення випромінювання біля джерела: цей захід досягається збільшенням відстані між джерелом випромінювання та робочим місцем, а також зменшенням потужності випромінювання генератора.
- Екранування джерел випромінювання: встановлення екранів навколо джерела випромінювання для зниження рівня електромагнітного поля.
- Організаційні заходи: проведення регулярного дозиметричного контролю інтенсивності електромагнітних випромінювань (не рідше одного разу на 6 місяців), а також медичні огляди (не рідше одного разу на рік) для контролю впливу на організм.
- Застосування засобів індивідуального захисту: це включає в себе використання переносних парасольок, комбінезонів і халатів з металізованої тканини, які здатні захищати організм за принципом заземленого сітчастого екрану.
- Використання захисних екранів: захисні кожухи, екрани та козирки, що встановлюються на шляху випромінювання, виготовлені з радіопоглинаючих матеріалів для максимальної ефективності захисту.

Ці заходи є важливими для забезпечення безпеки людей, які працюють з радіоелектронними пристроями, а також для мешканців, які проживають неподалік від потужних джерел електромагнітного випромінювання.

4.2 Вимоги пожежної безпеки при гасінні електроустановок

Пожежна безпека в приміщенні, де використовуються електроустановки, забезпечується за допомогою комплексу організаційно-технічних заходів і інших заходів для попередження пожеж. Ці заходи спрямовані на забезпечення безпеки людей, зниження можливих матеріальних збитків, мінімізацію негативних екологічних наслідків, створення умов для швидкого виклику пожежних підрозділів і успішного гасіння пожеж, а також для евакуації людей, документів

					КС КРБ 123. 22-320.00.00 ПЗ	Арк.
						49
Змн.	Арк.	№ докум.	Підпис	Дата		

і матеріальних цінностей з зони виникнення та можливого розповсюдження пожежі.

Система безпеки приватного будинку передбачає встановлення блоків живлення для забезпечення необхідної напруги. Однак при неналежному нагляді такі електроустановки можуть стати потенційними джерелами загоряння.

Під час пожежної небезпеки гасіння електроустановок можна поділити на дві категорії:

- гасіння електроустановок, які залишаються під напругою.
- гасіння електроустановок, що відключені від мережі.

У всіх електроустановках необхідно встановити належне заземлення з гнучкого мідного голого проводу з перерізом не менше 25 мм², який з'єднується з заземленими конструкціями.

Для забезпечення безпеки людей та пожежників, які беруть участь у гасінні пожеж електроустановок під напругою, застосовуються індивідуальні ізолюючі електрозахисні засоби, такі як діелектричні рукавиці, боти, калоші та килими. Кількість заземлень і індивідуальних ізолюючих захисних засобів, а також місця їх зберігання, визначаються керівниками проектів з розрахунку подачі вогнегасних засобів на електроустановки, які перебувають під напругою. Випробування електрозахисних засобів здійснюється в установленому порядку.

При виникненні пожежі на електроустановці, особа, яка першою виявила загоряння, повинна негайно викликати пожежників для запобігання подальшого поширення вогню. Гасіння електроустановок під напругою з використанням ручних стволів має відповідати наступним умовам:

- Ефективні методи подачі вогнегасних речовин в зону горіння.
- Дотримання безпечних відстаней від електрообладнання, яке знаходиться під напругою, до пожежників, що використовують ручні пожежні стволи.
- Використання ізолюючих електрозахисних засобів під час гасіння без відключення електропостачання.
- Забезпечення надійного заземлення стволів і пожежних автомобілів.

					КС КРБ 123. 22-320.00.00 ПЗ	Арк.
						50
Змн.	Арк.	№ докум.	Підпис	Дата		

Для гасіння пожеж на електроустановках під напругою доцільно використовувати розпилені струмені води, інертні гази, порошкові суміші або комбіновані методи, які включають розпилену воду з порошком. Використання пін та розчинів піноутворювача при гасінні заборонене через їхню підвищену електропровідність.

Під час гасіння пожежі на електроустановках під напругою необхідно використовувати тільки такі методи та засоби, які забезпечують безпечність для пожежників і ефективне пригнічення пожежі. Компактні струмені води можна використовувати до напруги 110 кВ лише тоді, коли неможливо наблизитися з розпиленою водою, з урахуванням безпечної відстані до електрообладнання.

Для забезпечення гасіння пожеж електроустановок, що перебувають під напругою, можна використовувати воду з міських систем водопостачання, а також з природних і штучних водойм, забезпечуючи безпечне забирання води через спеціалізовані пірси на пожежних автомобілях.

Під час гасіння пожеж на електроустановках з напругою до 220 кВ включно, час, який пожежники проводять на робочих позиціях, не є обмеженим. Для заземлення ручних пожежних стволів і насосів пожежних автомобілів у таких ситуаціях використовуються гнучкі мідні проводи з перерізом не менше 12 мм², оснащені спеціальними струбцинами для підключення до заземлених конструкцій, таких як гідранти, металеві опори ліній електропередачі, труби свердловин і шурфи. Місця для заземлення визначаються спеціалістами. Ручні пожежні стволи і насоси пожежних автомобілів повинні бути заземлені окремо. При подачі води з внутрішнього водопроводу заземлюються лише пожежні стволи. З метою електробезпеки персонал і пожежники, які безпосередньо беруть участь у гасінні пожеж на електроустановках під напругою, повинні використовувати індивідуальні ізолюючі електрозахисні засоби, такі як діелектричні рукавиці та боти. Автомобілі пожежних частин мають бути обладнані відповідною кількістю індивідуальних ізолюючих засобів захисту для членів бойової обслуги, які безпосередньо займаються гасінням пожежі.

					КС КРБ 123. 22-320.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		51

ВИСНОВКИ

У кваліфікаційній роботі бакалавра було вирішено актуальне завдання з розробки системи безпеки для приватного будинку на базі Arduino. Під час виконання роботи були отримані наступні практичні результати:

- Проведений огляд і аналіз сучасних систем безпеки підтвердив, що одним з найбільш перспективних напрямків є створення системи з використанням технології віддаленого спостереження у вигляді програмно-апаратних модулів.

- Розроблена структурна схема системи безпеки приватного будинку, що забезпечує контроль доступу до приміщення, активацію звукового сигналу при виявленні порушника, а також передачу повідомлень про проникнення користувачеві через інтернет-технології, що дозволяє здійснювати сповіщення в будь-якому місці та часі.

- Розроблена електрична принципова схема системи безпеки приватного будинку.

- Описано алгоритм роботи розробленої системи та написано відповідне програмне забезпечення для його реалізації.

Отримані практичні результати дозволили показати ефективність розробленої системи, зокрема:

- Проведено тестування розробленої системи безпеки приватного будинку для перевірки її надійності та стабільності в різних умовах експлуатації.

- Виявлено і вирішено потенційні проблеми із забезпеченням безперебійної роботи системи, включаючи заходи щодо забезпечення захисту від несанкціонованого доступу і втручання.

- Виконано порівняльний аналіз розробленої системи з існуючими аналогами, що підтвердив її конкурентоспроможність і переваги.

Ці результати підкріплюють практичну цінність та потенціал застосування розробленої системи в реальних умовах експлуатації приватних будинків.

					КС КРБ 123. 22-320.00.00 ПЗ	Арк.
						52
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Безпека в приватному будинку: сучасні системи та заходи для захисту вашого житла. URL: <https://dewpoint.com.ua/uk/bezpeka-v-privatnomu-budinku-suchasni-sistemi-ta-zahodi-dlya-zahistu-vashogo-zhitla/>(дата звернення: 05.06.2024).

2.Способи захисту свого будинку та майна. URL: <https://vencon.ua/ua/articles/ohranyaemaya-territoriya-sposoby-zashchity-svoego-doma-i-imushchestva>(дата звернення: 06.06.2024).

3.АТmega328 URL: <https://en.wikipedia.org/wiki/ATmega328>(дата звернення: 10.06.2024).

4.Пушкар М.С., Проценко С.М. Проектування систем автоматизації: навчальний посібник. Дніпропетровськ: видання Національного гірничого університету, 2013. 182 с.

5.Терещенко Т.О., Тодоренко В.А., Батрак Л.М., Ямненко Ю.С. Мікропроцесорні пристрої: навчальний посібник. Київ: видання Київського політехнічного інституту імені Ігоря Сікорського, 2017. 186 с.

6. Шаповал І.В., Лебедев Д.Ю. Алгоритм роботи пристрою AES шифратора. Київ: видання Київського політехнічного інституту імені Ігоря Сікорського, 2016. 87 с.

7. Кужильний О.В., Лебедев Д.Ю. GSM-сигналізація на базі датчика руху. Київ: видання Київського політехнічного інституту імені Ігоря Сікорського, 2017. 48 с.

8.Овчарук Є.С., Осухівська Г.М. Аналіз передавання даних в комп'ютеризованій системі обліку електроенергії. Матеріали VI науково-технічної конференції «Інформаційні моделі, системи та технології». 2018. с. 45.

9. Кривонос О. М., Кузьменко Є. В., Кривонос М. П., Кузьменко С. В. Fritzing - спеціалізоване прикладне програмне забезпечення для моделювання електронних пристроїв на основі платформи arduino. Житомир: видання житомирського державного університету імені Івана Франка. 2020. с. 31.

					КС КРБ 123. 22-320.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		53

10.Луцків А., Судомир В. Потокова модель даних при функційному програмуванні мікроконтролерів. Збірник тез доповідей VIII Міжнародної науково-технічної конференції молодих учених та студентів. 2019. С. 96-97.

11. Паламар А. М. Комп'ютерна система для моніторингу параметрів джерел безперебійного живлення на основі технології Internet of Things. Матеріали IV Міжнародної науково-технічної конференції «Теоретичні та прикладні аспекти радіотехніки, приладобудування і комп'ютерних технологій», Тернопіль. 2019. С. 208–209.

12. Паламар М. І., Паламар А. М. Система керування і моніторингу пристроїв гарантованого електроживлення. Праці II Міжнародної науково-технічної конференції «Світлотехніка й електротехніка: історія, проблеми й перспективи», Тернопіль. 2005. С. 135–139.

13. Дем'янчук Н.Р., Лупенко С.А., Луцків А.М., Осухівська Г.М. Ймовірнісні характеристики та імітація циклічного випадкового процесу, утвореного на базі адитивної моделі. Науковий вісник НЛТУ України. 2011. С. 322-331.

14. Білостоцький Т., Осухівська Г. М. Математичне моделювання передачі даних в комп'ютерних мережах. Матеріали II науково-технічної конференції «Інформаційні моделі, системи та технології», 2012. С.36.

15. Осухівська Г.М., Лобур Т.Б., Білостоцький Т.О. Дослідження та моделювання інтернет-трафіку комп'ютерної мережі. Збірник тез доповідей XVI наукової конференції ТНТУ ім. І. Пулюя, 2012, с. 58.

16. Зеркалов Д.В. Безпека життєдіяльності. Навчальний посібник. К.: Основа. 2011. 189 с.

17. Толок А.О. Крюковська О.А. Безпека життєдіяльності: Навчальний посібник. 2011. 89 с.

18. Яремко З. М. Безпека життєдіяльності: Навчальний посібник. 2005. 42 с.

19. Осухівська Г.М. Тиш Є.В. Луцик Н.С. Паламар А.М. Методичні вказівки до виконання кваліфікаційних робіт. Тернопіль. 2022. С. 5-24

					КС КРБ 123. 22-320.00.00 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		54

Додаток А
Технічне завдання

1 Загальні відомості

1.1 Повна назва та її умовне позначення

Повна назва теми кваліфікаційної роботи бакалавра: «Система охорони приватного будинку на базі arduino».

Умовне позначення дипломного проекту: КС КРБ 123. 22-320.00.00.

1.2 Виконавець

Студент групи СІс-42, факультету комп'ютерно-інформаційних систем і програмної інженерії, кафедри комп'ютерних систем та мереж, Тернопільського національного технічного університету імені Івана Пулюя, Літвінов Любомир Анатолійович.

1.3 Підстава для виконання роботи

Підставою для виконання кваліфікаційної роботи бакалавра є наказ по університету № 4/7-468 від «26» квітня 2024 року.

1.4 Планові терміни початку та завершення роботи

Плановий термін початку виконання кваліфікаційної роботи бакалавра – 26.04.2024 р.

Плановий термін завершення виконання кваліфікаційної роботи бакалавра – 24.06.2024 р.

1.5 Порядок оформлення та пред'явлення результатів роботи

Оформлення технічної документації до кваліфікаційної роботи бакалавра здійснюється згідно діючих вимог вітчизняних та міжнародних стандартів. Технічна документація до кваліфікаційної роботи бакалавра включає в себе текст пояснювальної записки та креслення, які максимально інформативно та стисло відображають основні результати розробки комп'ютеризованої системи для моніторингу водопостачання. Основними регламентними документами при оформленні та пред'явленні результатів проектування є групи діючих стандартів ДСТУ, ГОСТ, ISO та ЄСКД, ЕСПД. Пред'явлення результатів кваліфікаційної роботи бакалавра відбувається шляхом захисту дипломного проекту на відповідному засіданні ДЕК, ілюстрацією основних досягнень за допомогою графічного матеріалу.

2 Призначення і цілі створення системи

2.1 Призначення системи

Ця система призначена для забезпечення безпеки приватних майнових об'єктів, зокрема, будинків.

2.2 Мета створення системи

Метою створення системи є:

- забезпечення безпеки майна;
- виведення даних про безпеку на локальному комп'ютері;
- виведення даних про безпеку через telegram-бота;
- керування роботою датчиків та компонентів системи через telegram-бота;
- автоматичне сповіщення власника майна.

2.3 Характеристика об'єкту

Система проектується для моніторингу безпеки будинку, що включає в себе: – розробку структурної схеми; – розробку схеми електричної принципової; – розробку алгоритму роботи та програмного забезпечення для мікроконтролера.

3 Вимоги до системи

3.1 Вимоги до системи в цілому

Система безпеки приватного будинку повинна забезпечити:

1. Спраювання сигналу тривоги при неавторизованому проникненні;
2. Сповіщення користувача про проникнення;
3. Дистанційний моніторинг усіх датчиків системи;
4. Відображення результатів вимірювань на локальному комп'ютері;
5. Безвідмовну роботу при температурі повітря навколишнього середовища від $-10\text{ }^{\circ}\text{C}$ до $+40\text{ }^{\circ}\text{C}$, при відносній вологості повітря до 90 %.

3.1.1 Вимоги до структури та функціонування системи

Структура системи охорони будинку включає в себе:

- Мікроконтролер на базі Arduino, який відповідає за загальне керування функціонуванням системи.;
- датчики руху та відкриття дверей чи вікон;
- персональний комп'ютер.

Основні функціональні вимоги характеризуються наступними критеріями:

- швидкість реагування;
- надійність;
- захищеність;
- зручність монтажу та модернізації;
- контрольованість.

3.1.2 Вимоги до способів та засобів зв'язку між компонентами системи

Обмін даними між компонентами системи охорони повинен здійснюватися з використанням безпроводних технологій передачі.

3.1.3 Вимоги до режимів функціонування системи

Система повинна функціонувати в двох режимах роботи: активний та пасивний. Активний режим передбачає забезпечення безпеки від проникнення та сповіщення про зловмисника, користувача. Пасивний режим передбачає припинення роботи сенсорів та сповіщення про події, користувача.

3.1.4 Перспективи розвитку та модернізації системи

Передбачаються перспективи розвитку системи, які охоплюють можливість масштабування та розширення функціоналу. Наприклад, це може включати додавання нових датчиків для розширення області охоплення, інтеграцію з додатковими пристроями для підвищення безпеки, а також розробку додаткових програмних модулів для розширення можливостей системи управління та моніторингу.

3.1.5 Вимоги до надійності системи

Система повинна бути захищена від фізичних чи механічних пошкоджень на рівні апаратного та програмного забезпечення. Надійність системи повинна забезпечувати відновлюваність функціонування у випадку збою апаратного чи програмного забезпечення. Ймовірність безвідмовної роботи системи повинна складати не менше 99,6 %.

3.1.6 Вимоги до функцій та задач, які виконує система

Функції та задачі, які повинна виконувати система, передбачають:

- автоматичне ввімкнення тривоги при втявленні зловмисника;
- сповіщення користувача про проникнення;
- дистанційний моніторинг стану системи за допомогою бездротових технологій передачі даних;
- відображення результатів вимірювань на локальному комп'ютері.

3.1.7 Вимоги до апаратного забезпечення

Вимоги до елементної бази розробки:

- режими роботи і умови експлуатації вибраних елементів повинні відповідати вказаним в ТЗ;
- вибрана елементна база має забезпечувати необхідні режими роботи системи;
- Елементна база повинна бути універсальною, легко доступною і економічно вигідною. Також необхідно враховувати можливість заміни обраних елементів на аналогічні.

Вимоги до мікроконтролера:

- мікроконтролер має підтримувати RISC архітектуру команд;
- мікроконтролер повинен містити необхідний набір вбудованих периферійних пристроїв (таймери, АЦП і т.п.) та потрібну кількість керованих портів введення /виведення.

4 Вимоги до документації

Документація повинна відповідати вимогам ЄСКД та ДСТУ. Комплект конструкторської документації повинен складатись з:

- пояснювальної записки;
- графічного матеріалу:
 1. функціональна схема системи;
 2. структурна схема пристрою;
 3. схема електрична принципова;
 4. схема розміщення елементів на друкованій платі;
 5. перелік елементів до електричної схеми;
 6. блок-схема алгоритму роботи програми.

*Примітка: В комплект конструкторської документації можуть вноситися зміни та доповнення в процесі розробки.

5 Техніко-економічні показники

Собівартість розробки системи повинна становити не більше 20000 грн.

Термін експлуатації системи повинен бути не менший 10 років.

*Примітка: собівартість системи може змінюватись під час розрахунку в процесі розробки.

Таблиця 1 – Стадії та етапи виконання КРБ

№ етапу	Назва етапу виконання КРБ	Термін виконання
1	Розробка та затвердження технічного завдання	01.02-09.02
2	Аналіз технічного завдання та обґрунтування можливих рішень	05.02.-11.02
3	Розробка структурної та функціональної схеми	02.05-10.05
4	Розробка схеми електричної принципової, вибір елементної бази	11.05-01.06
5	Розробка програмного забезпечення для проєктованої системи	02.06-09.06
6	Опрацювання питань розділу «Безпека життєдіяльності, основи охорони праці»	10.06-15.06
7	Оформлення пояснювальної записки дипломного проєкту	16.06-18.06
8	Оформлення графічної частини	19.06-20.06
9	Попередній захист кваліфікаційної роботи бакалавра	14.06
10	Захист кваліфікаційної роботи бакалавра	24.06-28.06

7 Додаткові умови виконання кваліфікаційної роботи бакалавра

Під час виконання дипломного проєкту в дане технічне завдання можуть вноситися зміни та доповнення.

Додаток Б

Лістинг програми для мікроконтролера, що керує системою охорони приватного будинку

```
#include <Wire.h>
#include <RTClib.h>
#include <WiFiEsp.h>
#include <WiFiEspClient.h>
#include <WiFiEspUdp.h>
#include <WiFiEspServer.h>
#include <SoftwareSerial.h>
#include <ArduinoJson.h>
#include <LiquidCrystal_I2C.h>
#include <Keypad.h>

#define ESP8266_BAUD 9600
#define PIR_PIN 2
#define FLEX_SENSOR_PIN A0
#define SIREN_PIN 3
#define POWER_BUTTON_PIN 4
#define MODE_BUTTON_PIN 5
#define GREEN_LED_PIN 12
#define RED_LED_PIN 13
#define SYSTEM_STATUS_LED_RED_PIN 6
#define SYSTEM_STATUS_LED_GREEN_PIN 7
#define ALARM_STATUS_LED_RED_PIN 8
#define ALARM_STATUS_LED_GREEN_PIN 9

const char* ssid = "SSID";
const char* password = "password";
const char* telegramBotToken = "bot_token";
const char* chatId = " chat_id";

RTC_DS1307 rtc;
SoftwareSerial espSerial(10, 11); // RX, TX
```

```

WiFiEspClient client;
LiquidCrystal_I2C lcd(0x27, 16, 2);

const byte ROWS = 4;
const byte COLS = 4;
char keys[ROWS][COLS] = {
    {'1', '2', '3', 'A'},
    {'4', '5', '6', 'B'},
    {'7', '8', '9', 'C'},
    {'*', '0', '#', 'D'}
};

byte rowPins[ROWS] = {9, 8, 7, 6};
byte colPins[COLS] = {5, 4, 3, 2};
Keypad keypad = Keypad(makeKeymap(keys), rowPins, colPins, ROWS,
COLS);

bool systemActive = true; // Стан системи (активна/пасивна)
bool notificationsMuted = false; // Приглушення сповіщень
bool powerOn = true; // Живлення увімкнене
String accessCode = "1234"; // Код доступу
String inputCode = ""; // Введений код
bool passwordEntered = false; // Флаг, що показує, що пароль введено
правильно

void setup() {
    Serial.begin(9600);
    espSerial.begin(ESP8266_BAUD);
    WiFi.init(&espSerial);

    pinMode(GREEN_LED_PIN, OUTPUT);
    pinMode(RED_LED_PIN, OUTPUT);
    pinMode(SYSTEM_STATUS_LED_RED_PIN, OUTPUT);
    pinMode(SYSTEM_STATUS_LED_GREEN_PIN, OUTPUT);
    pinMode(ALARM_STATUS_LED_RED_PIN, OUTPUT);
    pinMode(ALARM_STATUS_LED_GREEN_PIN, OUTPUT);
}

```

```
lcd.begin();
lcd.backlight();
lcd.print("Запуск системи");

if (WiFi.status() == WL_NO_SHIELD) {
    lcd.print("Немає WiFi модуля");
    while (true);
}

WiFi.begin(ssid, password);
while (WiFi.status() != WL_CONNECTED) {
    delay(500);
    lcd.print(".");
}
lcd.clear();
lcd.print("WiFi підключено");

rtc.begin();
pinMode(PIR_PIN, INPUT);
pinMode(FLEX_SENSOR_PIN, INPUT);
pinMode(SIREN_PIN, OUTPUT);
pinMode(POWER_BUTTON_PIN, INPUT_PULLUP);
pinMode(MODE_BUTTON_PIN, INPUT_PULLUP);

if (!rtc.isrunning()) {
    lcd.print("RTC не працює");
    rtc.adjust(DateTime(F(__DATE__), F(__TIME__)));
}
}

void loop() {
    static unsigned long lastCheckTime = 0;
    unsigned long currentMillis = millis();

    // Вмикаємо зелену LED в залежності від стану живлення
    digitalWrite(GREEN_LED_PIN, powerOn ? HIGH : LOW);
```

```

    digitalWrite(RED_LED_PIN, powerOn ? LOW : HIGH); // Червона LED
протилежа зелени для стану живлення

    // Вмикаємо LED статусу системи (ЧЕРВОНИЙ = пасивна, ЗЕЛЕНИЙ =
активна)
    digitalWrite(SYSTEM_STATUS_LED_RED_PIN, systemActive ? LOW :
HIGH);
    digitalWrite(SYSTEM_STATUS_LED_GREEN_PIN, systemActive ? HIGH :
LOW);

    // Вмикаємо LED статусу тривоги (ЧЕРВОНИЙ = тривога активна,
ЗЕЛЕНИЙ = нормальний режим)
    digitalWrite(ALARM_STATUS_LED_RED_PIN, digitalRead(SIREN_PIN) ==
HIGH ? HIGH : LOW);
    digitalWrite(ALARM_STATUS_LED_GREEN_PIN, digitalRead(SIREN_PIN) ==
HIGH ? LOW : HIGH);

    if (digitalRead(POWER_BUTTON_PIN) == LOW) {
        powerOn = !powerOn;
        lcd.clear();
        if (powerOn) {
            lcd.print("Живлення УВИМКН.");
        } else {
            lcd.print("Живлення ВИМКН.");
        }
        delay(500);
    }

    // Перевіряємо натискання кнопки MODE тільки після введення пароля
    if (passwordEntered && digitalRead(MODE_BUTTON_PIN) == LOW) {
        systemActive = !systemActive;
        lcd.clear();
        if (systemActive) {
            lcd.print("Система АКТИВНА");
        } else {
            lcd.print("Система ПАСИВНА");
        }
    }

```

```

        delay(500);
    }

    char key = keypad.getKey();
    if (key) {
        lcd.clear();
        lcd.print(key);
        if (key == '#') {
            if (inputCode == accessCode) {
                lcd.print("Доступ Дозволено");
                passwordEntered = true; // Встановлюємо прапорець, що
                пароль введено правильно
                // Виконуємо додаткові дії після доступу дозволено
            } else {
                lcd.print("Доступ Заборонено");
            }
            inputCode = "";
        } else if (key == '*') {
            inputCode = "";
            lcd.print("Код Очищено");
        } else {
            inputCode += key;
        }
        delay(500);
        lcd.clear();
    }

    if (currentMillis - lastCheckTime >= 1000) {
        lastCheckTime = currentMillis;
        DateTime now = rtc.now();
        checkForCommands();
        if (powerOn && systemActive && (digitalRead(PIR_PIN) == HIGH
|| analogRead(FLEX_SENSOR_PIN) > threshold)) {
            triggerAlarm(now);
        }
    }
}

```

```

void triggerAlarm(DateTime timestamp) {
    digitalWrite(SIREN_PIN, HIGH);
    lcd.clear();
    lcd.print("Тривога спрацювала");
    if (!notificationsMuted) {
        String message = "Тривога спрацювала о: " +
timestamp.timestamp();
        sendMessageToTelegram(message);
    }
    delay(5000); // Тривожна сигналізація тривалість
    digitalWrite(SIREN_PIN, LOW);
    lcd.clear();
}

void checkForCommands() {
    if (client.connect("api.telegram.org", 80)) {
        client.print("GET /bot");
        client.print(telegramBotToken);
        client.print("/getUpdates HTTP/1.1\r\n");
        client.print("Host: api.telegram.org\r\n");
        client.print("Connection: close\r\n\r\n");

        while (client.connected()) {
            String line = client.readStringUntil('\n');
            if (line == "\r") {
                break;
            }
        }

        String response = client.readString();
        client.stop();

        StaticJsonDocument<2000> doc;
        deserializeJson(doc, response);

        JsonArray updates = doc["result"].as<JsonArray>();

```

```

    for (JsonObject update : updates) {
        String messageText =
update["message"]["text"].as<String>();
        if (messageText == "off") {
            systemActive = false;
            sendMessageToTelegram("Система тепер пасивна.");
        } else if (messageText == "on") {
            systemActive = true;
            sendMessageToTelegram("Система тепер активна.");
        } else if (messageText == "mute") {
            notificationsMuted = true;
            sendMessageToTelegram("Сповідження приглушено.");
        }
    }
}
}
}

```

```

void sendMessageToTelegram(String message) {
    if (client.connect("api.telegram.org", 80)) {
        client.print("POST /bot");
        client.print(telegramBotToken);
        client.print("/sendMessage HTTP/1.1\r\n");
        client.print("Host: api.telegram.org\r\n");
        client.print("Content-Type: application/x-www-form-
urlencoded\r\n");
        client.print("Content-Length: ");
        client.print(message.length() + 10 + String(chatId).length());
        client.print("\r\n\r\n");
        client.print("chat_id=");
        client.print(chatId);
        client.print("&text=");
        client.print(message);
        client.print("\r\n");
        client.stop();
    }
}
}

```