МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: 123 «Комп'ютерна інженерія»

Освітньо-професійна програма: «Безпека комп'ютерних систем і мереж»

Група: 4КБ-02

Дипломний проект

здобувача освіти денної форми навчання
КБ.02.13.000.ДП

ПЕРВУХІНА
МАКСИМА ЮРІЙОВИЧА

м. Одеса
2025 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: **123 «Комп'ютерна інженерія»**

Освітньо-професійна програма: «**Безпека комп'ютерних систем і мереж»**

Група: **4КБ-02**

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проекту на тему:

Розробка системи безпеки приватного середовища на платформі Arduino

Проектний матеріал складається з пояснювальної записки на 69 сторінках та графічного (презентаційного) матеріалу на 16 аркушах (слайдах)

Дипломник _____ (Первухін М.Ю.)

Керівник _____ (Стайкуца С.В.)

Консультанти:

з економічного розділу _____ (Канський М.Ю.)

з розділу охорони праці та техніки безпеки _____ (Чорновол Н.І.)

з нормоконтролю _____ (Петрашова В.І.)

старший консультант _____ (Кривченко Ю.В.)

До захисту допущений

Голова циклової комісії _____ (Кривченко Ю.В.)

Завідувач відділення _____ (Краснокутська К.Г.)

Захист «26» червня 2025 р. Протокол ЕК № 5

Оцінка ЕК 4 (добре) / 80 б.

Секретар ЕК _____

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Відділення *комп'ютерних систем* Комісія *КТ та ПІ*

Спеціальність *123 «Комп'ютерна інженерія»*

Освітньо-професійна програма *«Безпека комп'ютерних систем і мереж»*

ЗАТВЕРДЖУЮ:

Заст. дир. з НВР _____

Беркань І.В.

"19" 05 2025 р.

ЗАВДАННЯ

на дипломний проект

Здобувачеві (здобувачці) освіти *Первухіну Максиму Юрійовичу*

(прізвище, ім'я, по батькові)

1. Тема проекту *Розробка системи безпеки приватного середовища на платформі Arduino*

затверджена наказом по коледжу від "14" листопада 2025 р. № 246

2. Термін здачі закінченого проекту _____

3. Вихідні данні до проекту (роботи) *1. Передбачити відповідність засобів охоронної сигналізації до законодавства України; 2. Моделі плати мікроконтролерів Arduino: Arduino Uno; Arduino Mega; Arduino Nano; Arduino Nano; 3. Кількість компонентів в складі безпеки на платформі Arduino - 5; 4. Розробку системи безпеки приватного середовища виконати у симуляторі Tincercad; 5. Розробити електричну та принципіальну схеми системи безпеки приватного середовища.*

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

Аналіз видів загроз та методів захисту приватних середовищ; Огляд існуючих рішень для забезпечення безпеки на основі Arduino; Вибір компонентів та апаратної частини системи; Аналіз принципів та алгоритмів функціонування системи; Розробка технічного завдання на розробку приватного приміщення; Розробка електричної та принципіальної схем системи безпеки приватного середовища; Розробка програмного забезпечення

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

Ефективність технічних засобів охорони об'єктів; Компоненти системи безпеки приватних середовищ; Щодо мети спостереження; Загрози приватних середовищ; Огляд існуючих рішень для забезпечення безпеки на основі Arduino; Проектування та реалізація системи безпеки на платформі Arduino; Вибір компонентів та апаратної частини системи; Схема електрична принципіальна системи безпеки приватного середовища; Алгоритм дій при роботі з Arduino IDE; Зображення макету схеми системи безпеки приватного середовища у симуляторі Tincercad

6. Консультанти по проекту (роботі), із зазначенням розділів проекту, що їх стосується

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
Основний розділ	*Стайкуца С.В.*		
Економічний розділ	*Канський М.Ю.*		
Розділ охорони праці	*Чорновол Н.І.*		
Нормоконтроль	*Петрашова В.І.*		
Старший консультант	*Кривченко Ю.В.*		

7. Дата видачі завдання 28.04.25р.

Керівник *Стайкуца С.В.* _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/р	Назва етапів дипломного проекту (роботи)	Термін виконання етапів дипломного проекту (роботи)	Відмітка про виконання
1.	*Вступ. Постановка задачі проектування*	*14.05.2025*	Виконано
2.	*Огляд видів загроз та методи захисту середовищ*	*17.05.2025*	Виконано
3.	*Огляд рішень для забезпечення безпеки на основі*	*21.05.2025*	Виконано
	Arduino		
4.	*Аналіз актуальних технологій та інструментів*	*24.05.2025*	Виконано
	для побудови систем безпеки		
5.	*Вибір компонентів та апаратної частини системи*	*02.06.2025*	Виконано
6.	*Аналіз принципів та алгоритмів функціонування*	*04.06.2025*	Виконано
	системи		
7.	*Розробка технічного завдання*	*09.06.2025*	Виконано
8.	*Розробка електричної та принципіальної схем системи*	*10.06.2025*	Виконано
	безпеки приватного середовища		
9.	*Розробка програмного забезпечення*	*11.06.2025*	Виконано
10.	*Аналіз результатів тестування системи безпеки*	*13.06.2025*	Виконано
11.	*Виконання економічних розрахунків*	*14.06.2025*	Виконано
12.	*Розробка заходів з охорони праці. Графічна частина*	*16.06.2025*	Виконано

Дипломник _____
(підпис)

Керівник _____
(підпис)

Формат	Зона	Поз.	Позначення	Назва	Кіл.	Примітка
				Документація		
			КБ 02. 13 000. 00 ДП	Дипломний проект		
А4			КБ 02. 13 000. 00 ДП ПЗ	Пояснювальна записка	1	

Зм.	Арк.	№ докум.	Підпис	Дата	КБ 02. 13 000. 00 ДП		
Розробив		Первухін М.Ю.		18.05	Розробка системи безпеки приватного середовища на платформі Arduino	Літ.	Аркуш 3 / Аркушів 69
Перевірив		Стайкуца С.В.		18.06		Н Д П	
Н. Контр.		Петрашова В.І.		18.06.25		ВСП "ОТФК ОНТУ" гр.4КБ-02	
Затверд.		Кривченко Ю.В.		20.06			

ЗМІСТ

ВСТУП

У сучасному світі питання безпеки приватного середовища стає все більш актуальним. Приватне середовище, до якого відносяться як житлові приміщення, так і офісні простори, вимагає ефективних рішень для забезпечення його захисту від різноманітних загроз, таких як несанкціоноване проникнення, пожежі, витоки газу та інших аварійних ситуацій. Зі швидким розвитком технологій та зростаючим використанням автоматизованих систем, безпека приватних середовищ потребує новітніх інноваційних рішень.

Одним із перспективних підходів до створення ефективних систем безпеки є використання мікроконтролерів, зокрема платформи Arduino, що дозволяє створювати доступні та гнучкі рішення для моніторингу та управління безпекою. Arduino є відмінною базою для розробки низько вартісних, але надійних пристроїв, здатних виконувати завдання, пов'язані з контролем доступу, виявленням руху, пожежною безпекою та іншими аспектами.

Метою даної дипломної роботи є розробка системи безпеки приватного середовища з використанням платформи Arduino на основі датчиків руху з інфрачервоним випромінюванням.

У рамках цієї роботи буде здійснено проектування та реалізацію пристрою управління, що поєднує в собі різноманітні датчики для моніторингу навколишнього середовища та забезпечення захисту. Система повинна реагувати на різні загрози, такі як проникнення в приміщення, зміни в температурі чи рівні газу, і оперативно сповіщати власника про потенційну небезпеку.

Розробка такої системи є не лише практично важливим проектом для забезпечення безпеки, але й демонстрацією можливостей сучасних технологій для створення доступних та ефективних рішень у сфері захисту приватного середовища.

1 ОСНОВНИЙ РОЗДІЛ

1.1 Теоретичні основи безпеки приватного середовища

1.1.1 Поняття системи безпеки та її роль у приватних середовищах

Система безпеки – це сукупність організаційних, технічних та програмних заходів, спрямованих на захист об'єктів від різноманітних загроз, що можуть виникнути внаслідок людської діяльності чи природних катастроф. Її основною метою є забезпечення безпеки людей, майна та інформації, а також створення належних умов для нормальної життєдіяльності та діяльності в приватному середовищі. У контексті приватних середовищ, таких як житлові приміщення чи офіси, система безпеки повинна забезпечити захист від вторгнень, несанкціонованого доступу, а також інших загроз, таких як пожежі, витоки газу або стихійні лиха.

Приватне середовище, як правило, має специфічні вимоги до безпеки, оскільки в ньому знаходяться персональні дані, цінні матеріальні ресурси, а також проживають або працюють люди, що робить такі об'єкти особливо вразливими. Рішення для забезпечення безпеки повинні бути ефективними, але водночас доступними та простими у використанні, що робить технології на основі мікроконтролерів, таких як платформа Arduino, особливо привабливими для створення недорогих та надійних систем безпеки.

Системи безпеки для приватних середовищ, в основному, виконують такі основні функції:

1) контроль доступу;

2) спостереження;

3) виявлення загроз;

4) сповіщення.

Контроль доступу – це сукупність організаційних і технічних заходів, спрямованих на обмеження доступу до приватного середовища для

неавторизованих осіб. Це один із ключових елементів у системі безпеки, що забезпечує захист фізичного простору, матеріальних цінностей та конфіденційної інформації.

У контексті приватного підприємства або житлового приміщення контроль доступу виконує наступні функції:

– ідентифікація користувача (впізнавання особи за допомогою певного параметру, наприклад, коду, RFID-мітки або біометричних даних);

– аутентифікація – перевірка відповідності пред'явленого параметра даним, збереженим у системі;

– прийняття рішення – дозвіл або заборона на доступ до приміщення;

– реєстрація подій – фіксація усіх спроб входу та виходу, як успішних, так і відхилених.

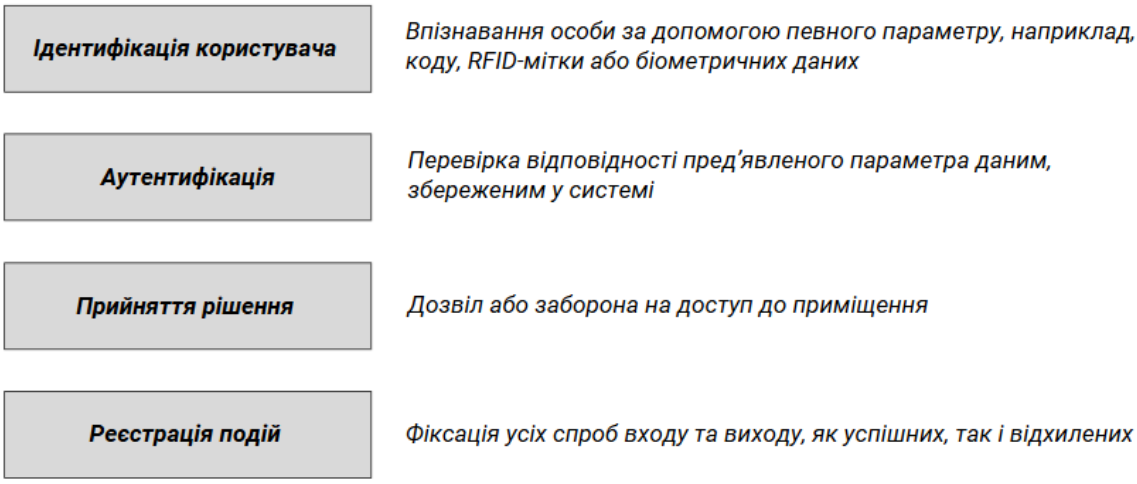


Рисунок 1.1. Основні функції контролю доступу

У практиці приватного середовища використовуються наступні типи систем контролю доступу:

– електронні замки з PIN-кодом або карткою – це найпростіші системи, які дозволяють відкривати двері за допомогою введення цифрового коду або піднесення картки;

– RFID-системи широко використовуються в офісах, складах та будинках; надають доступ лише тим, у кого є авторизований RFID-ключ.

– біометричні системи (відбитки пальців, розпізнавання обличчя, сканування сітківки) забезпечують високий рівень безпеки та індивідуальність доступу;

– інтелектуальні домофони та відеоспостереження дозволяють перевірити особу відвідувача перед відкриттям дверей.

Система контролю доступу може бути інтегрована з охоронною сигналізацією. Наприклад, якщо спроба входу була неавторизованою, автоматично активується сирена або сповіщення власника через GSM-модуль чи мобільний застосунок.

Забезпечення ефективного контролю доступу є важливим етапом у загальній архітектурі безпеки приватного середовища, оскільки дозволяє не лише захищати фізичний простір, але й створювати умови для відповідальності та аудиту подій доступу.

Системи спостереження є ключовим елементом у забезпеченні безпеки приватних середовищ, як житлових, так і комерційних. Їх основне завдання полягає у виявленні, фіксації та попередженні несанкціонованого доступу, підозрілої активності або загроз у режимі реального часу.

Мета спостереження представлена на рис. 1.2

Рисунок 1.2. Мета спостереження

Компоненти систем відеоспостереження для приватних середовищ:

– відеокамери – внутрішні та зовнішні, стаціонарні або поворотні, з функцією нічного бачення;

– центральний блок (реєстратор або мікроконтролер) забезпечує обробку та зберігання відеопотоку;

– модуль зберігання даних – це карта пам’яті, жорсткий диск, хмарне сховище;

– дисплей або веб-інтерфейс призначено для перегляду в реальному часі або архівного запису;

– мережеве підключення призначено для віддаленого спостереження через Wi-Fi або Ethernet.

У системах на базі Arduino, реалізація базових функцій спостереження можлива шляхом підключення:

– PIR-датчиків руху призначено для визначення руху в приміщенні;

– Камери типу OV7670 або модулів ESP32-CAM призначені для знімання фото або відео;

– SD-карт або Wi-Fi модулів призначені для збереження або передавання даних;

– LCD-дисплеїв або мобільного застосунку призначені для локального або дистанційного моніторингу.

Системи спостереження також можуть включати функції автоматичного сповіщення (наприклад, через GSM або Telegram-бот), що дозволяє оперативно реагувати на інциденти.

Важливим аспектом є етичне та правове використання систем відеоспостереження. У приватному середовищі необхідно інформувати осіб про наявність спостереження та дотримуватися норм захисту персональних даних.

Таким чином, спостереження приватних середовищ є невіддільною складовою комплексної системи безпеки, що підвищує її ефективність і забезпечує спокій власника об’єкта.

Приватні середовища – це приміщення чи території, доступ до яких має бути обмеженим для сторонніх осіб. До таких середовищ належать квартири, будинки, офіси, приміщення приватних підприємств, складські зони тощо. Забезпечення їхньої безпеки потребує своєчасного виявлення загроз, які можуть призвести до порушення конфіденційності, втрати майна або нанесення шкоди користувачам.

Основні загрози для приватного середовища умовно поділяють на фізичні та технічні:

– фізичні загрози – це несанкціонований доступ (вторгнення через двері або вікна), вандалізм, крадіжка, проникнення вночі, пошкодження майна, тощо;

– технічні загрози – це маніпуляції з елементами системи безпеки (відключення живлення, перехоплення сигналів), підміна пристроїв або датчиків, перешкоди у роботі бездротових модулів.

Для виявлення загроз використовуються такі типи сенсорів:

– датчики руху (PIR) дозволяють виявити присутність людини у приміщенні за змінами інфрачервоного випромінювання;

– магнітоконтактні датчики (геркони) – реагують на відкривання/закривання дверей або вікон;

– вібродатчики фіксують вібрацію або удари по вікнах чи інших поверхнях;

– звукові сенсори дозволяють реагувати на розбиття скла або інші нетипові звуки;

– газові, димові та температурні датчики допомагають виявити пожежу, витік газу або інші потенційно небезпечні події.

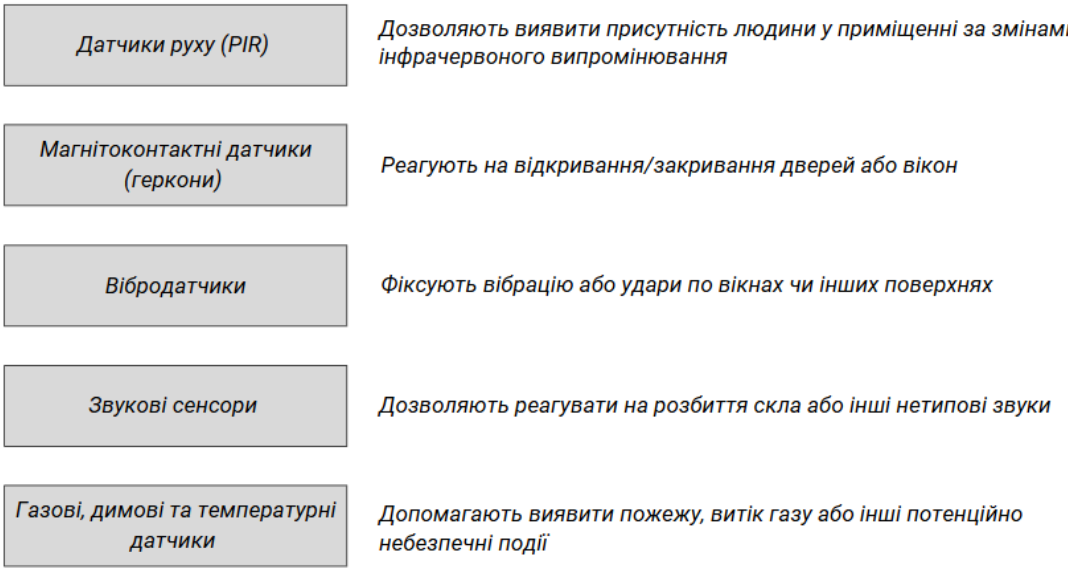


Рисунок 1.3. Типи сенсорів в фокусі виявлення загроз

Ефективне виявлення загроз базується на комбінації різних типів сенсорів, розміщених у ключових точках приміщення, таких як:

– вхідні двері;

– вікна (особливо на першому поверсі);

– коридори, що з'єднують приміщення;

– кімнати з цінним майном або інформацією (кабінет директора, бухгалтерія, серверна тощо).

Інтелектуальні алгоритми виявлення, вбудовані у мікроконтролери, дозволяють аналізувати сигнали від датчиків, уникати помилкових спрацювань і визначати характер загрози. У разі виявлення порушення система виконує заздалегідь запрограмовані дії – подає звукову та/або світлову сигналізацію, активує сповіщення користувача, записує інформацію на SD-карту або передає її через мережу.

Таким чином, виявлення загроз є ключовим етапом забезпечення безпеки приватного середовища і має базуватися на багатокомпонентному підході з використанням як апаратних, так і програмних засобів.

Сповіщення – це важливий елемент системи безпеки приватного середовища, який забезпечує негайну реакцію на виявлену загрозу. Завдяки системі сповіщення власник або відповідальні особи можуть оперативно дізнатися про проникнення, підозрілу активність або інші критичні події.

Мета системи сповіщення приватного середовища:

– миттєве інформування про спрацювання охоронних датчиків;

– залучення уваги до потенційної загрози (наприклад, шляхом гучного звуку);

– підвищення ефективності реагування на інциденти;

– попередження зловмисників про наявність системи охорони.

Види сповіщення приватного середовища:

1) акустичне сповіщення реалізується за допомогою сирен, зумерів або динаміків. Використовується для залучення уваги та відлякування зловмисника;

2) світлове сповіщення забезпечується за рахунок використання світлодіодів або миготливих ламп для візуального сигналу про спрацювання певного датчика;

3) Мобільне/дистанційне сповіщення реалізується за рахунок відправки SMS, push-повідомлень або повідомлень через месенджери (наприклад, Telegram або Viber);

4) Мережева інтеграція – це передача сигналу на віддалений сервер або охоронний пульт.

Реалізація в Arduino-системах:

– акустичне сповіщення можна реалізувати через зумери (buzzer) або сирени, які підключаються до цифрових виходів мікроконтролера;

– світлові сигнали забезпечують світлодіоди, що вказують на конкретний спрацювавший датчик;

– для мобільного оповіщення використовуються GSM-модулі (наприклад, SIM800L) або Wi-Fi модулі (ESP8266, ESP32), які дозволяють надсилати SMS або повідомлення у хмарні сервіси;

– додатково, через інтернет або Bluetooth, система може передавати дані у мобільний застосунок або вебінтерфейс.

Розглянемо приклад сценарію сповіщення при загрозу. При виявленні руху в кімнаті директора, система активує світлодіод індикації, запускає сирену, а GSM-модуль надсилає SMS власнику:

"Тривога! Виявлено рух у кімнаті директора о 03:14."

Важливі аспекти:

– затримка на активацію сповіщення для виключення помилкових спрацювань;

– можливість віддаленого вимкнення або підтвердження сповіщення;

– програмне обмеження кількості повідомлень, щоб уникнути спаму.

Таким чином, система сповіщення є критично важливою для ефективного функціонування охоронного комплексу в приватному середовищі, дозволяючи вчасно реагувати на потенційні загрози та мінімізувати можливі наслідки.

Складові системи безпеки для приватних середовищ надано на рис. 1.4.

Оскільки загрози безпеці приватних середовищ можуть бути різноманітними і не завжди передбачуваними, системи безпеки повинні мати

здатність реагувати на широке коло потенційних інцидентів. Використання датчиків різного призначення – від руху до температури та вологості – дозволяє створити універсальні рішення, які можуть бути налаштовані для конкретних умов.

Рисунок 1.4. Складові системи безпеки для приватних середовищ

Технології, що застосовуються для побудови таких систем, мають на меті забезпечити простоту використання та доступність, а також інтеграцію з іншими смарт-пристроями в домі чи офісі. Платформа Arduino, завдяки своїй відкритій архітектурі та широкому вибору доступних компонентів, є чудовим інструментом для розробки таких систем. Вона дозволяє створювати як прості, так і складні системи безпеки з можливістю налаштування та масштабування, що є важливим аспектом для приватних середовищ.

1.1.2 Відповідність засобів охоронної сигналізації до законодавства України

Приватні середовища, такі як житлові приміщення, офіси та інші приватні об'єкти, постійно піддаються різним загрозам, які можуть загрожувати безпеці людей, майна та інформації. Ці загрози можуть бути як фізичними, так і інформаційними, а їх вплив може мати різні наслідки — від незначних збитків до серйозних аварій або навіть людських жертв. Для того щоб ефективно забезпечити безпеку, важливо розуміти основні типи загроз та методи їх захисту.

Види загроз приватних середовищ можуть бути наступними:

– фізичні загрози;

– техногенні загрози;

– інформаційні загрози.

На рис. 1.5 надано ризики виникнення можливих загроз для приватних середовищ.

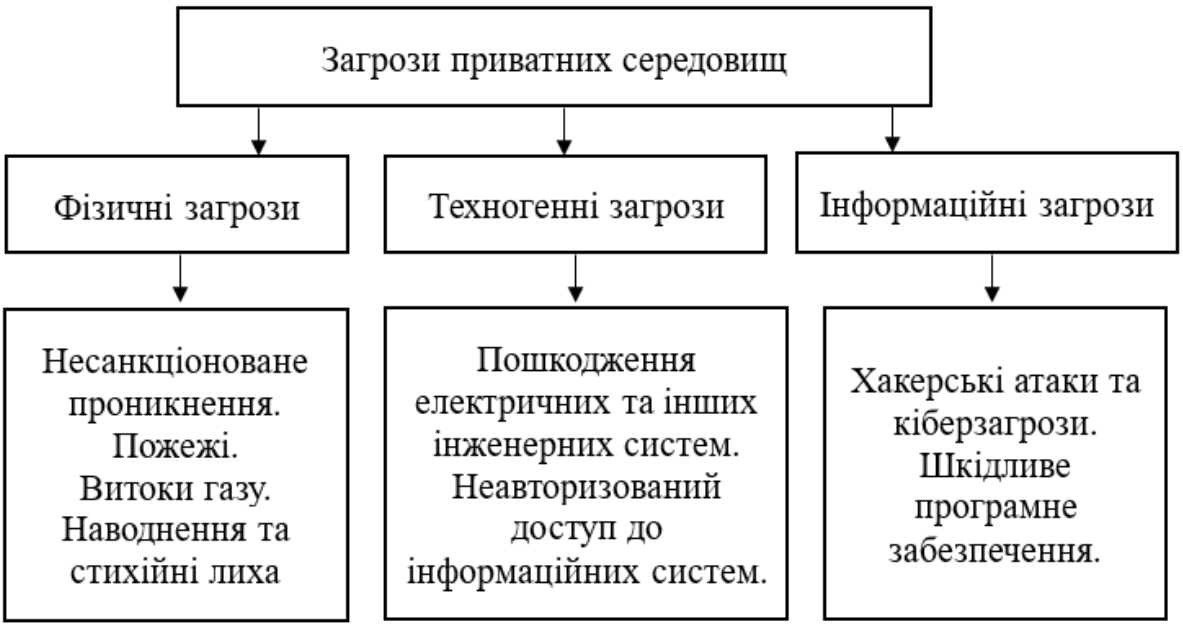


Рисунок 1.5. Загрози приватних середовищ

Фізичні загрози включають: несанкціоноване проникнення; пожежі; витоки газу; наводнення та стихійні лиха.

Несанкціоноване проникнення це одна з найбільш поширених загроз, яка передбачає незаконний доступ до приватного простору з метою крадіжки майна або нанесення шкоди. Часто застосовуються методи обману або насильства для проникнення в приміщення.

Пожежі можуть виникати внаслідок короткого замикання електропроводки, неправильно експлуатованих побутових приладів, а також унаслідок людських помилок або навмисних підпалів. Пожежа може мати катастрофічні наслідки, якщо не буде своєчасно виявлена.

Газові витоки можуть стати причиною вибухів або отруєння. Це особливо актуально для будинків, де використовуються газові прилади для опалення чи приготування їжі.

Природні катастрофи, такі як затоплення, землетруси чи бурі, також можуть становити загрозу для приватних об'єктів.

До техногенних загроз можна віднести пошкодження електричних та інших інженерних систем; неавторизований доступ до інформаційних систем.

Пошкодження електричних та інших інженерних систем призводять до аварії в електропостачанні або водопостачанні. Це може призвести до серйозних проблем в функціонуванні приватного середовища, особливо коли йдеться про тривале відключення електрики чи води.

Неавторизований доступ до інформаційних систем: зі збільшенням використання цифрових технологій зростає загроза несанкціонованого доступу до особистої інформації, паролів, банківських даних та інших чутливих відомостей.

Джерелом інформаційних загроз може бути хакерські атаки та кіберзагрози; шкідливе програмне забезпечення. Зі зростанням числа підключених пристроїв та використанням Інтернету важливою загрозою є атаки на комп'ютери та мережі, спрямовані на крадіжку персональних даних або завдання шкоди програмному забезпеченню. Шкідливі програми можуть потрапити в пристрої користувачів, крадучи або пошкоджуючи дані, а також створюючи загрози для приватності та конфіденційності.

Методи захисту приватних середовищ включає наступне:

– фізичний захист;

– техногенний захист;

– інформаційний захист.

Фізичний захист включає: системи контролю доступу; сигналізації та відеоспостереження; датчики пожежі та газу;

Системи контролю доступу призначені для запобігання несанкціонованому проникненню, що потребує встановлення електронних замків, біометричних систем або інших механізмів контролю доступу, що дозволяє обмежити або контролювати вхід в приміщення.

Системи сигналізації реагують на вторгнення, виявляючи рух або відкриття дверей/вікон, та сповіщають власника або охоронну службу. Відеокамери забезпечують постійний моніторинг та фіксацію подій.

Системи виявлення пожежі та витоків газу здатні своєчасно реагувати на зміни в середовищі та сповіщати про небезпеку. Для зниження ризику їх встановлюють на базі датчиків температури, диму або концентрації газу.

Техногенний захист базується на використанні охоронних інженерних систем та резервних джерел живлення.

Системи моніторингу електропостачання, водопостачання та інших інженерних мереж дозволяють оперативно виявляти проблеми та запобігати серйозним аваріям. Для забезпечення безперервної роботи важливих систем (наприклад, пожежних сигналізацій) використовуються джерела безперебійного живлення (ДБЖ) або генератори.

Інформаційний захист базується на використанні засобів кібербезпеки; антивірусного програмного забезпечення. Для захисту від несанкціонованого доступу до інформаційних систем використовуються різноманітні методи шифрування даних, встановлення міжмережевих екранів, антишпигунські програми та інші засоби для забезпечення цілісності та конфіденційності даних.

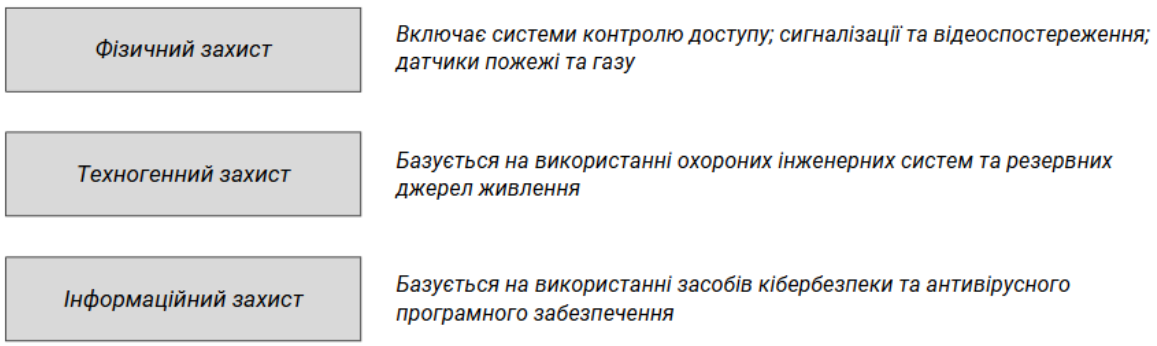


Рисунок 1.6. Методи захисту приватних середовищ

Антивірусне програмне забезпечення передбачає регулярне оновлення антивірусних програм допомагає виявляти та блокувати шкідливі програми, що можуть пошкодити або викрасти важливу інформацію.

Застосування комплексного підходу до захисту приватних середовищ дозволяє знизити рівень ризиків і ефективно запобігати загрозам. Вибір методів захисту залежить від конкретних умов, у яких працює система, та типу загроз, які необхідно мінімізувати. Системи безпеки, побудовані на платформі Arduino, є доступними та гнучкими рішеннями для реалізації багатьох з цих методів захисту, що дозволяє власникам приватних середовищ створювати ефективні і персоналізовані системи безпеки.

1.1.3 Огляд існуючих рішень для забезпечення безпеки на основі Arduino

Платформа Arduino є популярною основою для створення різноманітних пристроїв та систем, включаючи рішення для забезпечення безпеки приватних середовищ. Вона дозволяє розробляти доступні, гнучкі та ефективні системи, що можуть бути адаптовані до специфічних потреб користувача. Завдяки широкому вибору датчиків, модулів та можливості програмування, Arduino стає перспективним інструментом для створення різних елементів безпеки, таких як системи відеоспостереження, контроль доступу, охорона від пожеж та витоків газу.

У цьому підрозділі розглянемо основні існуючі рішення для забезпечення безпеки, які можна реалізувати на платформі Arduino, а також їх особливості, переваги та недоліки. Технічні складові забезпечення безпеки на основі платформи Arduino надано на рис. 1.7.

Розглянемо системи відеоспостереження на базі Arduino. Одним з основних аспектів забезпечення безпеки є відеоспостереження. Для цього використовуються камери та модулі, які можна підключити до платформи Arduino. Прості камери, такі як OV7670, можуть бути використані для зйомки та передачі зображення на мікроконтролер для подальшої обробки. Зокрема, Arduino може здійснювати запис відео або фото для документування подій, а також для виявлення руху за допомогою датчиків руху, що дозволяє знижувати рівень фальшивих спрацьовувань.

Рисунок 1.7. Технічні складові забезпечення безпеки на основі платформи Arduino

На рис. 1.8 надано вигляд модуля відеокамери VGA OV7670 SCCB I2C IIC для платформи Arduino.

Рисунок 1.8. Відеокамера VGA OV7670 SCCB I2C IIC платформи Arduino

Можна відзначити наступні переваги цього модуля: простота реалізації та доступність компонентів; можливість інтеграції з іншими системами безпеки; низька вартість рішення для базових потреб.

Недоліками є обмежена потужність обробки зображень на самій платформі Arduino, а також потреба в додаткових модулях для підключення до Інтернету для віддаленого доступу.

В системах сигналізації та детекції руху для забезпечення безпеки приватного середовища використовуються датчики руху, які можуть спрацьовувати при виявленні несанкціонованого доступу в приміщення. На базі Arduino існують рішення, що використовують різноманітні датчики руху, зокрема інфрачервоні датчики PIR (Passive Infrared Sensors), ультразвукові датчики або радарні сенсори.

До переваг цих датчиків можна віднести: швидка реакція на рух; легкість інтеграції з іншими компонентами системи, такими як сирени, замки або мобільні додатки для сповіщення користувача; низька енергоспоживаність, що є важливим для автономних систем.

До недоліків можна віднести: погане виявлення руху через бар'єри або обмежену зону покриття; можливість хибних спрацьовувань через зміну температури або незначні рухи.

Системи контролю доступу є важливою частиною безпеки приватних об'єктів, забезпечуючи можливість лише авторизованим особам входити в приміщення. На платформі Arduino можна реалізувати різноманітні системи контролю доступу, що використовують RFID (радіочастотні ідентифікаційні картки), біометричні сканери або цифрові клавіатури для введення паролів.

До їх переваг слід віднести: високий рівень безпеки при використанні RFID або біометричних даних; можливість додавання множинних методів автентифікації для підвищення надійності системи; можливість інтеграції з мобільними додатками для віддаленого контролю.

Недоліки цих систем контролю доступу є: необхідність у забезпеченні надійного живлення та резервних джерел для безперебійної роботи; потенційні проблеми з сумісністю біометричних пристроїв з платформою Arduino.

Важливим є системи виявлення пожежі та витоків газу призначені для забезпечення безпеки приватного середовища. Для цього на платформі Arduino використовуються спеціалізовані датчики, такі як датчики вуглекислого газу (MQ-7, MQ-9) та датчики диму (MQ-2). Ці датчики можуть спрацьовувати при

виявленні підвищених рівнів газу або диму в повітрі, що є ознакою пожежі або витоку газу.

Переваги таких систем є: можливість оперативно виявити загрози на ранніх етапах; висока точність виявлення шкідливих газів і диму; можливість інтеграції з іншими системами, такими як сповіщення на мобільний телефон або автоматичне відключення газових приладів.

До недоліків слід віднести необхідність регулярного технічного обслуговування датчиків та можливість хибних спрацьовувань через високі рівні пилу або інших аномальних факторів. Вигляд модулів виявлення диму, метану, зрідженого газу MQ-2 MQ-7, MQ-9, MQ-135 надано на рис. 1.9.

Рисунок 1.9. Модулі виявлення диму, метану, зрідженого газу: MQ-2, MQ-7, MQ-9, MQ-135 платформи Arduino

Arduino має великий потенціал для інтеграції з Інтернетом речей, що дозволяє створювати системи безпеки з можливістю віддаленого доступу та моніторингу. Модулі Wi-Fi, такі як ESP8266 або ESP32, дозволяють підключити систему до Інтернету і налаштувати віддалений моніторинг через веб-інтерфейс або мобільний додаток. Це дозволяє користувачам отримувати сповіщення про події в реальному часі та контролювати стан системи безпеки з будь-якої точки світу. До переваг такої інтеграції слід віднести: можливість віддаленого

моніторингу та управління; широкий вибір готових платформ і додатків для інтеграції; гнучкість у налаштуванні та масштабуванні системи.

Недоліка інтеграції є потреба в стабільному інтернет-з'єднанні для коректної роботи, а також ризики безпеки, пов'язані з підключенням до Інтернету та необхідністю захисту від кіберзагроз.

Отже, існуючі рішення для забезпечення безпеки на основі Arduino пропонують широкий спектр можливостей для реалізації різноманітних функцій, від контролю доступу до виявлення загроз, таких як пожежі та витоки газу. З переваг можна виділити низьку вартість, гнучкість та можливість персоналізації систем під конкретні потреби користувачів. Однак існують і обмеження, такі як обмеженість ресурсів для обробки складних даних, необхідність у додаткових модулях для забезпечення високої надійності та можливість хибних спрацьовувань датчиків. Усе це вказує на необхідність комплексного підходу до розробки та налаштування таких систем для досягнення максимальної ефективності.

1.1.4 Аналіз актуальних технологій та інструментів для побудови систем безпеки

Сучасні технології для забезпечення безпеки приватних середовищ постійно розвиваються, дозволяючи створювати більш ефективні, надійні та гнучкі системи захисту. Вони охоплюють широкий спектр інструментів, від базових датчиків до складних систем з інтеграцією з Інтернетом речей (IoT), а також використання штучного інтелекту (AI) для покращення функцій виявлення та реагування на загрози. У цьому розділі розглянемо основні технології та інструменти, що застосовуються для побудови сучасних систем безпеки, зокрема в контексті використання мікроконтролерів та платформи Arduino. Технології та інструменти для побудови систем безпеки надано на рис. 1.10.

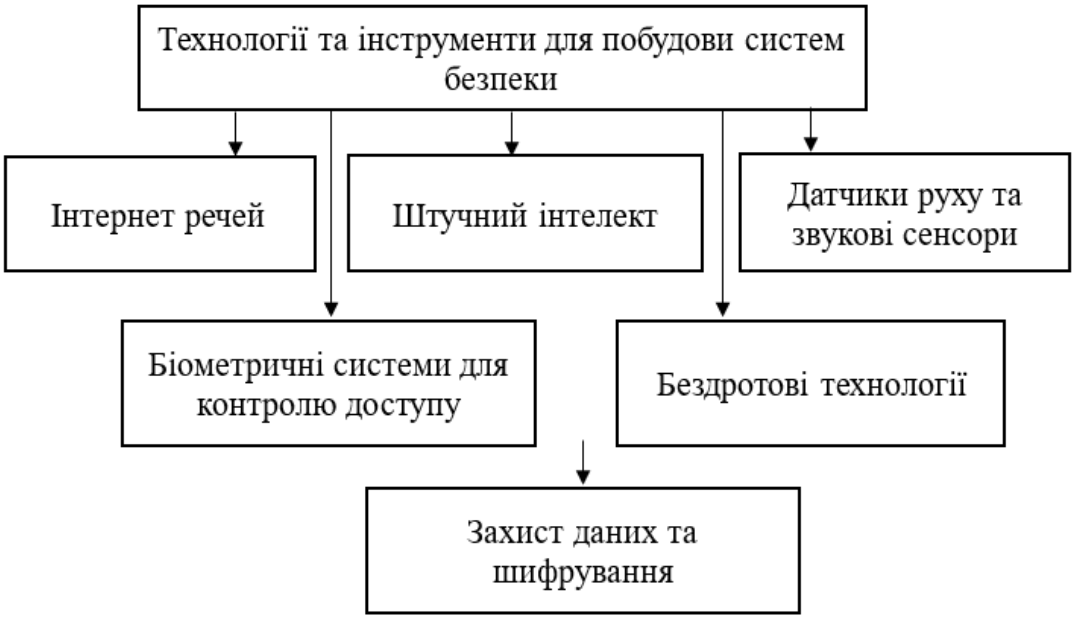


Рисунок 1.10. Технології та інструменти для побудови систем безпеки

Однією з найактуальніших технологій для побудови сучасних систем безпеки є Інтернет речей (IoT). IoT дозволяє інтегрувати фізичні пристрої та датчики з Інтернетом, що надає можливість віддаленого моніторингу та управління системами безпеки. Наприклад, за допомогою модулів Wi-Fi або Bluetooth, таких як ESP8266 або ESP32, можна створювати системи безпеки, які передають дані через Інтернет на мобільні додатки чи сервери для подальшого аналізу та прийняття рішень.

До переваг технології IoT слід віднести: віддалений доступ до системи та моніторинг в реальному часі; широкий вибір компонентів для різних завдань; можливість інтеграції з іншими пристроями IoT для створення розумних домів.

Недоліками цієї технології є: необхідність у стабільному Інтернет-з'єднанні; питання безпеки при підключенні до Інтернету та ризик кіберзагроз.

Штучний інтелект (AI) також є потужним інструментом для покращення функціональності систем безпеки. Завдяки використанню алгоритмів машинного навчання, AI може допомогти в автоматичному виявленні аномалій у даних, таких як рух чи зміни в оточуючому середовищі. Системи на базі AI здатні до навчання і підлаштування до нових умов, знижуючи кількість хибних спрацьовувань і підвищуючи точність виявлення загроз.

Перевагами AI є: можливість автоматичного виявлення аномалій; підвищення точності виявлення загроз; зменшення потреби в ручному втручанні та налаштуваннях.

Недоліки AI є висока складність у розробці та налаштуванні, що потребує значних обчислювальних ресурсів. Це також може бути обмеженням для простих систем на платформі Arduino.

Датчики руху є основними компонентами більшості систем сигналізації для приватних середовищ. Вони можуть бути реалізовані на основі інфрачервоних датчиків PIR, ультразвукових датчиків або радарних сенсорів, які виявляють рух в охоронюваній зоні. Крім того, звукові сенсори можуть використовуватися для виявлення несанкціонованих звуків або шуму, що дозволяє виявити вторгнення чи інші небезпечні події.

До їх переваг можна віднести: швидка реакція на рух або звук; легкість інтеграції в систему безпеки; доступність компонентів.

Проте до недоліків можна віднести можливість хибних спрацьовувань, наприклад, через зміни температури або незначні коливання в приміщенні.

Біометрія є потужним інструментом для створення високонадійних систем контролю доступу. Використання біометричних даних, таких як відбитки пальців, розпізнавання обличчя чи сітківки ока, дозволяє забезпечити високу точність і надійність автентифікації користувачів. Для розробки таких систем на базі Arduino часто використовуються спеціалізовані модулі, наприклад, для зчитування відбитків пальців або камери для розпізнавання осіб.

Перевагами біометричного контролю доступу є: висока надійність і безпека; зручність для користувачів (немає потреби запам'ятовувати паролі чи носити карти доступу).

До недоліків такої системи доступу можна віднести високу вартість обладнання, а також проблеми з точністю при низьких якостях зображень або неправильних умовах (наприклад, зчитування відбитків пальців).

Бездротові технології, такі як Wi-Fi, Bluetooth, ZigBee та LoRa, забезпечують бездротове підключення компонентів системи безпеки, що дає

можливість забезпечити більшу гнучкість у розміщенні датчиків і модулів. Використання бездротових технологій дозволяє уникнути складних монтажних робіт і знижує витрати на прокладання проводки. Перевагами бездротових технологій для інтеграції систем безпеки є: легкість у монтажі та налаштуванні; можливість установки датчиків у важкодоступних місцях; гнучкість у розширенні та масштабуванні системи. До їх недоліків можна віднести можливі проблеми з надійністю бездротових з'єднань в умовах перешкод або великої відстані, а також вища вартість обладнання порівняно з проводовими системами.

Для забезпечення конфіденційності та захисту даних, що передаються в рамках систем безпеки, використовуються технології шифрування. Це може включати використання алгоритмів шифрування даних, таких як AES (Advanced Encryption Standard) або RSA для захисту інформації при передачі по мережах або зберіганні на пристроях. Платформи Arduino підтримують інтеграцію з криптографічними модулями для шифрування даних. До їх переваг можна віднести: захист від несанкціонованого доступу до чутливої інформації; підвищення безпеки при використанні віддаленого доступу через Інтернет. Недолікам такої системи захисту є підвищена складність реалізації та аисоке навантаження на ресурси мікроконтролера при використанні складних алгоритмів шифрування.

Отже, сучасні технології для побудови систем безпеки, включаючи IoT, штучний інтелект, біометричні системи, бездротові технології та шифрування, значно покращують ефективність і надійність таких систем. Платформа Arduino є потужним інструментом для створення доступних та ефективних рішень, що використовують ці технології. Однак важливо враховувати обмеження ресурсів та потребу в правильному налаштуванні для досягнення оптимальної роботи системи безпеки.

1.2 Проектування та реалізація системи безпеки на платформі Arduino

1.2.1 Вибір компонентів та апаратної частини системи

При розробці системи безпеки на платформі Arduino важливо правильно обрати компоненти, які забезпечать надійність, ефективність і функціональність системи. У цьому розділі розглядаються ключові компоненти, що складають апаратну частину системи безпеки приватного середовища, а також фактори, які слід враховувати при їх виборі.

Основним компонентом системи є мікроконтролер Arduino, який керує усіма процесами в системі та забезпечує взаємодію між датчиками, виконавчими механізмами та користувачем. Для розробки системи безпеки оптимальними є такі моделі плати мікроконтролерів Arduino: Arduino Uno; Arduino Mega; Arduino Nano; Arduino Nano.

Плата мікроконтролера Arduino Uno є один з найпоширеніших мікроконтролерів, що має достатню кількість цифрових та аналогових входів для підключення базових датчиків і виконавчих механізмів. На рис. 1.11 представлено зовнішній вигляд плати мікроконтролера Arduino UNO R3 (ATmega328P). Ця плата має 14 цифрових пінів і 6 аналогових.

Плата мікроконтролера Arduino Mega має більшу кількість портів і пам'яті, що дозволяє використовувати більш складні конфігурації з великою кількістю датчиків та модулів. На рис. 1.12 надано зовнішній вид плата мікроконтролера Arduino Nano V3.0 (ATmega328P), яка має 56 цифрових пінів і 16 аналогових.

Плата мікроконтролера Arduino Nano це компактна версія Arduino Uno, ідеальна для встановлення в обмежених просторах. На рис. 1.13 представлена плата мікроконтролера Arduino Nano V3.0 (ATmega328P), яка має 14 цифрових пінів і 6 аналогових.

Плата мікроконтролера Arduino Pro Mini 3.3V (ATMega328) представлені на рис. 1.14, які мають 14 цифрових та 8 аналогових пінів.

Плата мікроконтролера мережного інтернету модуля Arduino (Ethernet Shield W5100 UNo R3) представлена на рис. 1.15. Це плата має контролер: Ethernet: W5100, мають 14 цифрових та 6 аналогових пінів.

Рисунок 1.11. Плата мікроконтролера Arduino UNO R3 (ATmega328P)

Рисунок 1.12. Плата мікроконтролера Arduino Mega 2560

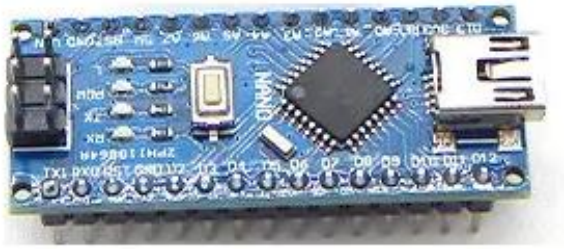


Рисунок 1.13. Плата мікроконтролера Arduino Nano V3.0 (ATmega328P)

Рисунок 1.14. Плата мікроконтролера Arduino Pro Mini 3.3V (ATMega328)

Рисунок 1.15. Плата мікроконтролера мережного інтернету модуля Arduino (Ethernet Shield W5100 UNo R3)

До переваги вибору Arduino можна віднести: легкість у використанні завдяки доступному програмуванню; велика кількість бібліотек і готових рішень для інтеграції різних датчиків та виконавчих пристроїв; широка спільнота та підтримка, що дозволяє швидко знаходити рішення для розробки.

Одними з основних елементів системи безпеки є датчики руху. Вони дозволяють виявити наявність людини в охоронюваній зоні. Найпоширенішими типами датчиків є: інфрачервоні датчики PIR та ультразвукові датчики.

Інфрачервоні датчики PIR (Passive InfraRed) виявляють зміну теплового випромінювання в зоні детекції. Це дозволяє виявляти рух людей або тварин. Ультразвукові датчики вимірюють відстань до об'єкта за допомогою ультразвукових хвиль, що дозволяє визначати рух у конкретній зоні. На рис. 1.16 та 1.17 представлено плати інфрачервоного датчику обходу перешкод Arduino. Як правили, таки датчики можуть виявляти порушника на відстані 3-7 метрів. Також в таких датчиках є можливість регулювати чутливість рівня інфрачервоного

випромінювання. Це доцільно в тих випадках, коли потрібно зробити щоб датчик не реагував на домашніх тварин в помешканні, яке охороняється.

До переваг PIR датчиків можна віднести простий спосіб підключення та налаштування та низька вартість. Недоліками є можливість хибних спрацьовувань через зміну температури чи інші чинники. На рис. 1.18 представлено передній та задній вид плати ультразвукового датчику відстані для Arduino. Це датчик дозволяє вимірювати відстань до суб'єкта, який наближається до датчика.

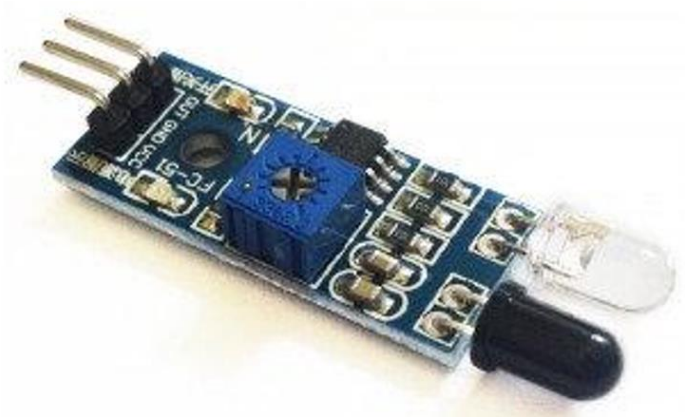


Рисунок 1.16. Плата інфрачервоного датчику обходу перешкод Arduino

Рисунок 1.17. Плата інфрачервоного датчику руху для ARDUINO HC-SR501

Рисунок 1.18. Плата ультразвукового датчику відстані для Arduino

Для контролю доступу до приміщення використовуються магнітні датчики відкриття. Вони складаються з двох частин: магніту та сенсора, який фіксує, коли двері або вікно відкриваються. Ці датчики надзвичайно прості у використанні та інтеграції з Arduino. Для них характерно є легкість монтажу, надійність у роботі та висока чутливість до змін положення. На рис. 1.19. представлено зовнішній вид герконів. Також на вікна встановлюється модуль датчика вібрації. Модуль датчик вібрації для Arduino на LM393 представлено на рис. 1.20. На рис. 1.21 представлено зовнішній вид модулю датчика нахилу і вібрації SW-18010P. Чутливість цих датчиків можна регулювати за допомогою зміни оперу змінного резистора.

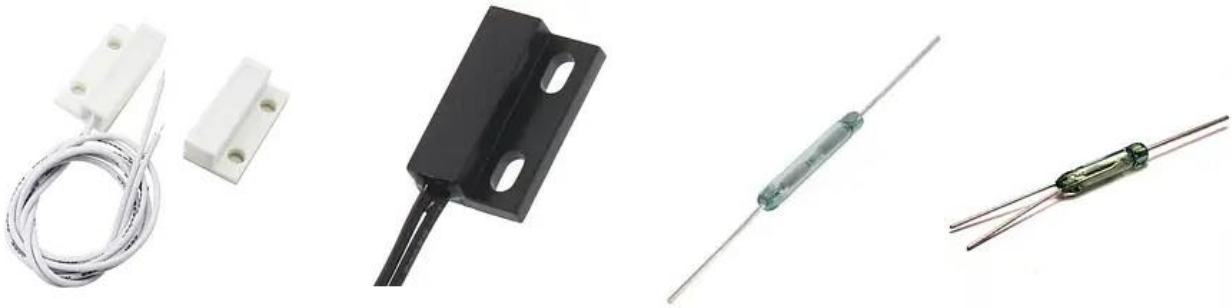


Рисунок 1.19. Зовнішній вид герконів

Рисунок 1.20. Модуль датчик вібрації для Arduino на LM393

Рисунок 1.21. Модуль датчика нахилу і вібрації SW-18010P

Для покращення моніторингу можна інтегрувати камера для відеоспостереження. Для невеликих систем на платформі Arduino використовуються камери з можливістю підключення через модуль камер OV7670 або більш складні модулі, що підтримують відео потокове передавання. Для допомогою такої камери є можливість побудови системи для візуального спостереження, що підвищує рівень безпеки через відеоінформацію. На рис. 1.22 надано зовнішній вигляд модуля VGA камери OV7670.

Рисунок 1.22. Модуль VGA камери OV7670

До недоліків слід віднести високу вартість камер високої роздільної здатності та потребу в додаткових ресурсах для обробки відео.

Для забезпечення безперервної роботи системи безпеки необхідно обрати надійне джерело живлення для всіх компонентів. Зазвичай для живлення Arduino використовується адаптер 5V, а для безперебійного живлення можуть бути встановлені акумулятори або батареї для забезпечення функціонування системи при відключенні електрики. Перевагами вибору стабільних джерел живлення **є**

збереження працездатності системи в умовах перебоїв з електропостачанням та довготривала робота без необхідності заміни батареї.

Для інтеграції системи з віддаленими пристроями або додатками можуть бути використані різні модулі зв'язку, такі як: Wi-Fi модуль ESP8266 або ESP32; Bluetooth модуль HC-05/HC-06; RFID модулі.

Wi-Fi модуль ESP8266 або ESP32 забезпечує можливість підключення до Інтернету, відправлення даних на сервер або мобільний додаток. Bluetooth модуль HC-05/HC-06 дозволяє організувати бездротове підключення через смартфон або інші пристрої Bluetooth. RFID модулі — для контролю доступу з використанням карток або брелоків. Перевагами таких модулей є можливість віддаленого моніторингу і управління системою через Інтернет або мобільний додаток, а також підключення до інших пристроїв для розширення функцій системи.

Для реалізації фізичного впливу в системі безпеки можуть бути використані актуатори – це механізми, що виконують певні дії у відповідь на сигнал з мікроконтролера. Це можуть бути сервомотори і реле. Сервомотори призначені для відкриття або закриття дверей, вікон. Реле призначені для вмикання або вимикання інших пристроїв, таких як сирена чи світлові індикатори. Перевагами є можливість автоматичного виконання фізичних дій у разі спрацьовування датчиків. Недоліками є висока енергетична витрата для деяких механізмів, а також необхідність додаткового контролю та налаштування для забезпечення точності виконання.

Для підвищення рівня безпеки приватного середовища можуть бути інтегровані датчики температури та вологості, такі як DHT11 або DHT22. Вони дозволяють відслідковувати параметри навколишнього середовища, що може бути важливим для виявлення пожеж, протікань води та інших аномалій.

Таким чином, вибір компонентів для системи безпеки на платформі Arduino є критичним етапом, що визначає ефективність і надійність усієї системи. Правильний підбір датчиків, мікроконтролера, виконавчих механізмів та засобів зв'язку дозволить створити гнучку та масштабовану систему, що

відповідає вимогам безпеки для приватних середовищ. Оскільки Arduino має широкий вибір сумісних компонентів, розробник може адаптувати систему під конкретні потреби та умови експлуатації.

1.2.2 Аналіз принципів та алгоритмів функціонування системи

У даному розділі описано принципи функціонування системи безпеки на платформі Arduino, а також основні алгоритми, що використовуються для забезпечення надійного контролю та реагування на різні загрози в приватному середовищі.

Система безпеки приватного середовища, розроблена на основі платформи Arduino, складається з кількох основних компонентів, які взаємодіють між собою для забезпечення належного рівня безпеки. Ось основні етапи її роботи: моніторинг середовища; аналіз та обробка сигналів; оповіщення та реагування; контроль доступу; збір і передача даних.

При моніторингу середовища система постійно відслідковує фізичні параметри навколишнього середовища за допомогою різних датчиків, таких як датчики руху (PIR), магнітні датчики для контролю дверей і вікон, датчики температури і вологості тощо. Датчики руху (PIR) фіксують наявність руху в зоні дії, що дозволяє виявити несанкціоновану активність. Магнітні датчики використовуються для контролю стану дверей і вікон, відслідковуючи їх відкриття чи закриття. Датчики температури та вологості дозволяють виявити можливі загрози, наприклад, у разі пожежі або витоку води.

При аналізу та обробки сигналів зібрані сигнали від датчиків передаються на мікроконтролер Arduino, який обробляє отриману інформацію. Якщо значення датчиків виходять за задані межі (наприклад, рух в охоронюваній зоні або відкрите вікно), система розпізнає це як загрозу.

Оповіщення та реагування відбувається у разі виявлення загрози, система може активувати різні оповіщення, наприклад, через звукову сигналізацію (сирену) або індикацію через світлодіоди (LED). Також можлива інтеграція з мобільними додатками або відправка повідомлень через Інтернет (Wi-Fi або Bluetooth), щоб користувач отримав повідомлення про спрацювання системи.

Контроль доступу відбувається для додаткового рівня захисту. Система може використовувати модулі для контролю доступу, наприклад, RFID або Bluetooth для розпізнавання карток чи пристроїв. Якщо зчитується несанкціонований RFID-картка або відсутнє з'єднання через Bluetooth, система може автоматично активувати сигналізацію або блокувати доступ.

Для збору і передачі даних система може здійснювати передавання даних про стан безпеки через Інтернет за допомогою модуля Wi-Fi, що дозволяє користувачу віддалено моніторити стан системи через мобільний додаток або веб-інтерфейс.

Алгоритм роботи системи безпеки можна поділити на кілька етапів: ініціалізація системи; постійний моніторинг; аналіз даних; реагування на загрозу; аналіз результатів та відновлення роботи.

При ініціалізації системи відбувається: підключення всіх датчиків до мікроконтролера Arduino; налаштування початкових параметрів для кожного датчика: допустимий діапазон для датчиків температури, руху, магнітних датчиків для дверей/вікон; ініціалізація виконавчих пристроїв (сирена, світлодіоди) та модулів зв'язку (Wi-Fi, Bluetooth).

Постійний моніторинг передбачає, що система постійно зчитує значення з датчиків. Якщо датчик руху PIR зафіксував зміни, то відбувається активація певного алгоритму. При цьому магнітні датчики перевіряють стан дверей/вікон, датчики температури та вологості перевіряють, чи не перевищують параметри небезпечні пороги.

Аналіз даних передбачає наступне: якщо значення датчиків перевищують задані пороги (наприклад, рух в охоронюваній зоні або температура понад 30°C), система розпізнає це як загрозу. В разі виявлення загрози система переходить до наступного етапу – реагування.

Реагування на загрозу має наступні етапи. Перший етап реакції: активація сирени або світлодіодної сигналізації. Другий етап реакції: якщо система підключена до Wi-Fi або Bluetooth, вона надсилає повідомлення користувачеві на мобільний пристрій або комп'ютер через спеціальний додаток або смс. У разі

виявлення несанкціонованого доступу через RFID або Bluetooth відбувається блокування доступу та активація сигналізації.

Аналіз результатів та відновлення роботи передбачає наступне: після виявлення загрози система продовжує моніторинг середовища; в разі необхідності система може скинути всі показники і перейти до початкового стану для повторної перевірки середовища.

1.3 Тестування та оцінка ефективності системи

1.3.1 Технічне завдання на розробку приватного приміщення

На рис. 1.23 надано план розташування кімнат приватного приміщення офісу для якої потрібно розробити систему охоронної сигналізації. Офіс складається з наступних кімнат:

1) кімната директора – 20 кв. м, яке має одне вікно та двері;

2) кімната секретаря – 10 кв. м, одне вікно та двері;

3) кімната бухгалтерії – 20 кв. м, яке має одне вікно та двері;

4) кімната відділу збуту та постачання – 20 кв. м, яке має одне вікно та двері;

5) хол – 20 кв. м, вхідні двері;

Офіс має 5 вікон, 4 внутрішніх дверей і одна зовнішня.

Для спрощення системи охоронної сигналізації пропонується використати для датчик руху для наступних приміщень:

1) туалет;

2) відділ бухгалтерії;

3) кімната секретаря;

4) кімната директора;

5) відділ збуту та постачання.

Для вхідної двері холу запропоновано використати геркон.

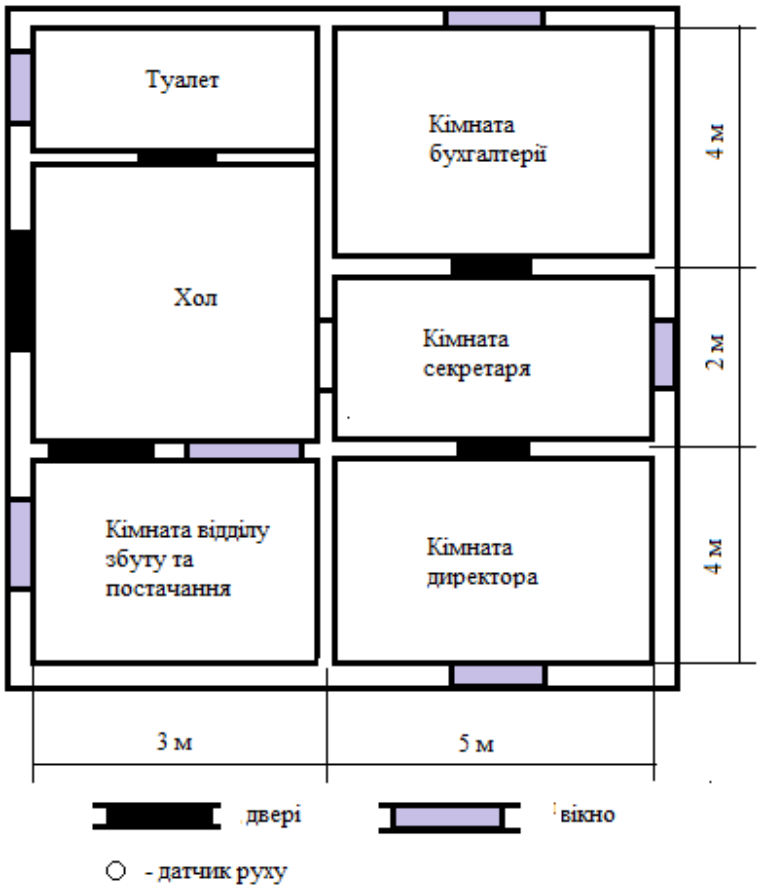


Рисунок 1.23. План розташування кімнат приватного приміщення

1.3.2 Розташування датчиків охоронної сигналізації в приміщеннях офісу

Отже, для завдання проєкту буде використано:

1) датчики руху – 6 шт;

2) геркон – 1 шт;

2) для охоронного пульта кількість світлодіодів – 6 шт;

5) динамік – 1 шт;

6) пристрій живлення ~220 В – 9В.

Розроблена система охоронної сигналізації призначена для контролю доступу та виявлення несанкціонованого проникнення до окремих приміщень приватного підприємства. В основі системи лежить мікроконтролер Arduino Mega, до якого підключено набір датчиків, індикаторів та сигнальних пристроїв.

Система охорони покликана здійснювати моніторинг переміщення у визначених приміщеннях підприємства, а також відстежувати відкриття вхідних

дверей. У випадку виявлення руху або відкриття дверей, система вмикає світлову індикацію на охоронному пульті та активує звукову сирену для попередження про вторгнення.

На охоронному пульті розташовано 6 світлодіодів, кожен з яких відповідає за одну з контрольованих зон. При спрацюванні відповідного датчика світлодіод загоряється, сигналізуючи про рух або відкриття.

Для привернення уваги в разі тривоги використовується звуковий динамік (сирена). При спрацюванні будь-якого з датчиків система активує сирену до моменту скидання або відключення сигналізації.

Система живиться від джерела змінного струму ~220 В через адаптер, який понижує напругу до 9 В, сумісної з Arduino Mega. Такий спосіб живлення дозволяє забезпечити стабільну роботу всієї системи в умовах офісного середовища.

На рис. 1.24 представлено план розташування кімнат приватного приміщення із сигналізацією.

Принцип роботи системи безпеки приватного середовища наступний:

1) після подачі живлення мікроконтролер переходить у режим охорони;

2) мікроконтролер плати Arduino постійно опитує датчики:

– якщо датчик неактивний, відповідний світлодіод вимкнений;

– якщо зафіксовано рух або відкриття дверей, вмикається відповідний світлодіод, активується сирена;

– система може бути розширена додатковими функціями: кнопкою скидання тривоги, екраном, віддаленим повідомленням через GSM або Wi-Fi тощо.

1.3.3 Розробка електричної та принципіальної схем системи безпеки приватного середовища

На рис 1.25 представлена схема електрична принципіальна системи безпеки приватного середовища.

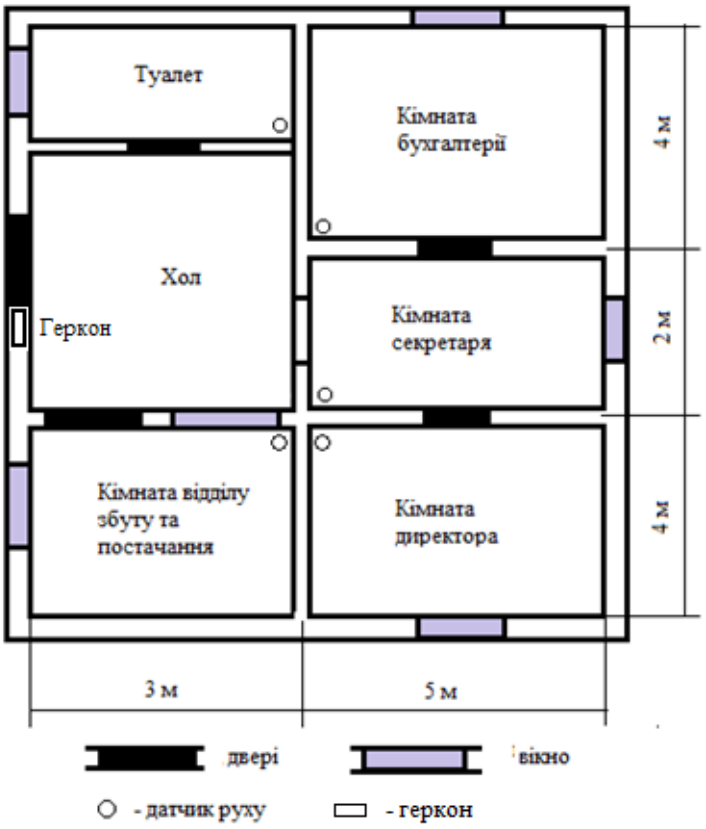


Рисунок 1.24. План розташування кімнат приватного приміщення із сигналізацією

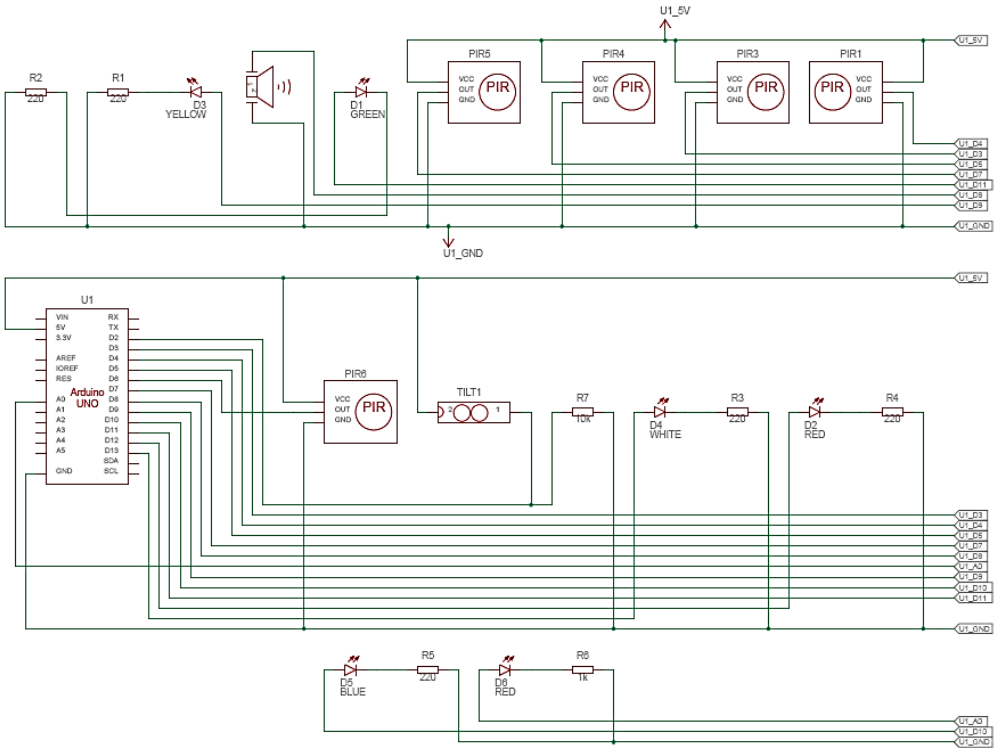


Рисунок 1.25. Схема електрична принципіальна системи безпеки приватного середовища

Розглянемо обґрунтування вибору плати мікроконтролера Arduino Uno. Arduino Uno – одна з найпоширеніших і найзручніших для початківців мікроконтролерних платформ. Вона має відкриту архітектуру, просту IDE (середовище розробки) та велику кількість прикладів, що значно спрощує процес розробки охоронної системи навіть без поглиблених знань у галузі електроніки та програмування.

Arduino Uno має: 14 цифрових пінів (0–13) – з них 6 можна використовувати як PWM-виходи; 6 аналогових входів (A0–A5), які також можна використовувати як цифрові. Цього цілком достатньо для реалізації базової охоронної системи, яка включає: датчики руху (до 6); герконові датчики (до 2–3); світлодіоди індикації (до 6); сирену або зумер.

Arduino Uno підтримує велику кількість охоронних сенсорів: PIR-датчики руху; геркони; вібродатчики; ультразвукові датчики. Це дозволяє створити гнучку та масштабовану охоронну систему. Arduino Uno працює від: USB (5 В), зовнішнього адаптера 7–12 В, що дозволяє живити її від стандартного блоку живлення або мобільного джерела (наприклад, акумулятора), що важливо для охоронної системи. Arduino Uno має апаратний послідовний порт (UART), що дозволяє зручно підключати: GSM/GPRS модулі (наприклад, SIM800L), Bluetooth-модулі (наприклад, HC-05), RFID-рідери (через SPI/I2C).

Отже, плата мікроконтролера Arduino Uno є оптимальним вибором для побудови недорогих, надійних і простих в реалізації систем охоронної сигналізації. Вона забезпечує достатній функціонал, має велику спільноту підтримки, дозволяє реалізувати усі необхідні функції системи без ускладнення апаратної частини.

У схемі використовується Arduino Uno (U1), який керує усіма елементами системи: піни D2–D13, A0–A5 використовуються як цифрові входи/виходи для підключення датчиків і світлодіодів. Живлення подається на Arduino через VCC (5V) та GND. У схемі передбачено 6 PIR-датчиків руху: PIR1 → PIR6. Кожен датчик підключений до Arduino: вихід з датчика – до цифрового входу Arduino. Живлення кожного PIR подається з шини 5V (U1_5V) та GND (U1_GND). Їх

призначення є виявлення руху в окремих зонах охоронюваного приміщення. Датчик нахилу (TILT1) (використовується в якості геркону) може реагувати на зміну положення (наприклад, відкриття дверей, підняття корпусу). Він підключений до одного з цифрових входів Arduino.

Світлодіоди використовуються для візуального інформування про спрацювання: LED1 (WHITE) – через R3, LED2 (RED) – через R4, LED3 (BLUE) – через R5, LED4 (RED) – через R6, LED5 (WHITE) – через R7, LED6 (GREEN) – через R8, LED7 (YELLOW) – через R1. Кожен світлодіод підключений до цифрового виходу Arduino через токообмежувальні резистори (220–330 Ом).

Зумер підключений через піни та елемент керування (ймовірно, транзистор або реле), позначений як сигнал. Він служить для звукового сповіщення про тривогу. Живиться від 5V, управляється з одного з цифрових виходів Arduino.

Таблиця 1.1. Перелік елементів схеми системи безпеки приватного середовища

Найменування на схемі	Кількість елементів	Назва елементу
U1	1	Arduino Uno R3
PIR1, PIR3, PIR4, PIR5, PIR6	5	PIR Sensor
PIEZO1	1	Piezo
R1, R2, R3, R4, R5	5	220 Ω Resistor
D1,	1	Green LED
D2, D6	2	Red LED
D3	1	Yellow LED
D4	1	White LED
D5	1	Blue LED
R6	1	1 kΩ Resistor
Meter1	1	Voltage Multimeter
TILT1	1	Tilt Sensor
R7	1	10 kΩ Resistor

Вся схема живиться від 5V джерела, підключеного до шини живлення (U1_5V). Спільна земля (U1_GND) об’єднує всі елементи. Arduino може бути підключений до комп’ютера або іншого модуля для передачі інформації (наприклад, серійна передача через TX/RX).

Загальне призначення системи – це модульна охоронна сигналізація, яка: реагує на рух у приміщеннях (через PIR-датчики), може фіксувати зміну положення (датчик нахилу), дає світлову і звукову індикацію при тривозі, побудована на простій і надійній платформі Arduino Uno.

Перелік елементів схеми системи безпеки приватного середовища представлено в табл. 3.1.

Зображення макету схеми системи безпеки приватного середовища у симуляторі Tincercad представлено на рис. 3.4.

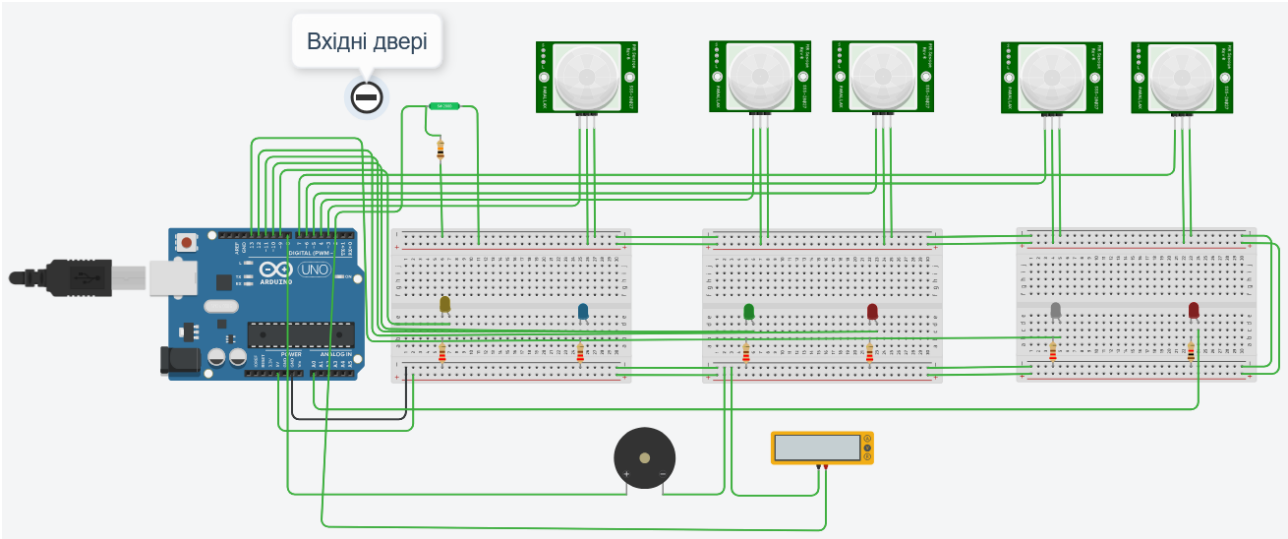


Рисунок 1.26. Зображення макету схеми системи безпеки приватного середовища у симуляторі Tincercad

1.3.4 Розробка програмного забезпечення

Програма реалізує логіку роботи охоронної сигналізації для 6 приміщень підприємства та вхідних дверей. Система реагує на спрацювання датчиків руху та геркона, активує відповідні світлодіоди для візуальної індикації, а також запускає сирену й зумер у разі тривоги.

Список елементів та підключення наступні: 6 датчиків руху підключені до цифрових входів 2–7 (один не використовується у цьому варіанті); 1 герконовий датчик підключено до піну 2 (перевизначено як buttonState1); 6 світлодіодів підключено до пінів 9, 10, 11, 12, 13, A0; сирена (динамік) підключена до піну 8; зумер підключений до піну A1.

Логіка роботи програми наступна. Setup-функція: встановлює пінові режими: датчики: INPUT; світлодіоди, сирена та зумер: OUTPUT; ініціалізує серійне з'єднання для відлагодження через монітор порту.

Loop-функція забезпечує зчитування станів датчиків: датчики руху та геркон зчитуються через digitalRead(); у разі спрацювання (значення HIGH) відповідному світлодіоду подається живлення, а в серійну консоль виводиться повідомлення, наприклад: Toilet. або Entrance door.

Формування сигналу тривоги: якщо хоча б один датчик активний, встановлюється прапор alarm = true, Реакція на тривогу: у випадку alarm = true активується сирена (tone(sirenPin, 1200, 200) – короткий звуковий імпульс) і зумер (призначений, але в коді фактично не активується, можна додати tone(buzzerPin, ...)). Якщо всі датчики неактивні, то сирена та зумер вимикаються.

Затримка delay(500) призначена для запобігання надто частому оновленню станів.

Особливості та примітки наступні:

– Пін 2 одночасно використовувався для sensor1Pin (закоментовано) та buttonState1. У даній реалізації використовується як герконовий датчик дверей;

– один з датчиків руху (sensor1Pin) не використовується — потенційно його можна активувати (наприклад, для ще однієї зони);

– для зумера бажано використовувати tone() або digitalWrite() як для сирени, наразі він не звучить, бо відповідні рядки закоментовані.

Потенційне розширення функціоналу наступні:

– додати кнопку зняття з охорони;

– реалізувати передачу SMS / повідомлення на телефон;

– зберігати події в EEPROM або на SD-карті;

– використати екран (LCD / OLED) для відображення стану системи.

Програмне забезпечення системи безпеки приватного середовища, яке розроблено у симуляторі Tincercad має наступний вид:

```
// Піни підключення датчиків//const int sensor1Pin = 2;
const int sensor2Pin = 3;
const int sensor3Pin = 4;
const int sensor4Pin = 5;
const int sensor5Pin = 6;
const int sensor6Pin = 7;
const int buttonState1 = 2; // геркон - двері

// Піни підключення світлодіодів
const int led1Pin = 9;
const int led2Pin = 10;
const int led3Pin = 11;
const int led4Pin = 12;
const int led5Pin = 13;
const int led6Pin = A0; // аналоговий пін використовується як цифровий


// Пін підключення сирени
const int sirenPin = 8;

// Пін підключення зумера
const int buzzerPin = A1; // аналоговий пін використовується як цифровий

void setup() {
  // Налаштування пінів датчиків як входів
  // pinMode(sensor1Pin, INPUT);
```

```
  pinMode(sensor2Pin, INPUT);
  pinMode(sensor3Pin, INPUT);
  pinMode(sensor4Pin, INPUT);
  pinMode(sensor5Pin, INPUT);
  pinMode(sensor6Pin, INPUT);

  // Налаштування пінів світлодіодів як виходів
  pinMode(led1Pin, OUTPUT);
  pinMode(led2Pin, OUTPUT);
  pinMode(led3Pin, OUTPUT);
  pinMode(led4Pin, OUTPUT);
  pinMode(led5Pin, OUTPUT);
  pinMode(led6Pin, OUTPUT);
  pinMode(buttonState1,INPUT);

  // Налаштування піну сирени як вихід
  pinMode(sirenPin, OUTPUT);

  // Налаштування піну зумера як вихід
  pinMode(buzzerPin, OUTPUT);

  // Ініціалізація серійного зв'язку для налагодження монітору
  Serial.begin(9600);
}

void loop() {
  // Змінні для зберігання стану датчиків
 // bool sensor1State = digitalRead(sensor1Pin);
  bool sensor2State = digitalRead(sensor2Pin);
  bool sensor3State = digitalRead(sensor3Pin);
```

```
bool sensor4State = digitalRead(sensor4Pin);
bool sensor5State = digitalRead(sensor5Pin);
bool sensor6State = digitalRead(sensor6Pin);
bool sensor7State = digitalRead(buttonState1);

// Змінна для індикації спрацювання хоча б одного датчика
bool alarm = false;

// Перевірка стану кожного датчика та індикація світлодіодом

if (sensor2State == HIGH) {
  digitalWrite(led2Pin, HIGH);
  alarm = true;
  Serial.println("Toilet.");
} else {
  digitalWrite(led2Pin, LOW);
}

if (sensor3State == HIGH) {
  digitalWrite(led3Pin, HIGH);
  alarm = true;
  Serial.println("Accounting.");
} else {
  digitalWrite(led3Pin, LOW);
}

if (sensor4State == HIGH) {
  digitalWrite(led4Pin, HIGH);
  alarm = true;
  Serial.println("Secretary.");
```

```
} else {
  digitalWrite(led4Pin, LOW);
}

if (sensor5State == HIGH) {
  digitalWrite(led5Pin, HIGH);
  alarm = true;
  Serial.println("Director.");
} else {
  digitalWrite(led5Pin, LOW);
}

if (sensor6State == HIGH) {
  digitalWrite(led6Pin, HIGH);
  alarm = true;
  Serial.println("Sales and Supply.");
} else {
  digitalWrite(led6Pin, LOW);
}

 // Аналіз стану датчика
if (sensor7State == HIGH)
{
  digitalWrite(led1Pin, HIGH);
  alarm = true;
  Serial.println("Entrance door.");
}
else
{
  // turn LED off
```

```
  digitalWrite(led1Pin, LOW);
 }
 delay(10);
 // Якщо хоча б один датчик спрацював, включаємо сирену і зумер
 if (alarm) {
  tone(sirenPin, 1200,200);
   //digitalWrite(sirenPin, HIGH);
  //digitalWrite(buzzerPin, HIGH);
   Serial.println("Motion detected! Siren and buzzer are on.");
 } else {
   digitalWrite(sirenPin, LOW);
   digitalWrite(buzzerPin, LOW);
 }

 // Затримка для стабільності роботи
 delay(500);
}
```

Посилання на проєкт в симуляторі Tinkercad: https://www.tinkercad.com/things/80SnGBP5QXh-control-666-pir/editel?returnTo=https%3A%2F%2Fwww.tinkercad.com%2Fdashboardhttps://www.tinkercad.com/things/ks8zlD01vwX-frantic-pir4-4/editel?returnTo=%2Fthings%2Fks8zlD01vwX-frantic-pir4-4&sharecode=GUAznW4jZY1vAJUU2UV7XsdM1DlICSre5XVd2kVjdmk

1.3.5 Аналіз результатів тестування системи безпеки

У цьому підпункті проводиться аналіз працездатності розробленої системи безпеки на основі мікроконтролера Arduino Uno в умовах реального або імітованого використання. Метою тестування було перевірити функціональність

усіх компонентів системи, швидкість реагування на події, стабільність роботи та надійність взаємодії між датчиками та мікроконтролером.

Розглянемо перевірку реагування PIR-датчиків. У процесі тестування кожен з шести інфрачервоних датчиків руху (PIR1–PIR6) демонстрував коректну роботу:

– виявлення руху в межах заявленого радіусу (до 5–7 метрів);

– час затримки між фіксацією руху і передачею сигналу до Arduino складав менше 1 секунди;

– система правильно відображала активацію кожного окремого датчика за допомогою відповідного світлодіоду.

На рис. 1.27 надано приклад тестування датчику руху приміщення «Туалет» у симуляторі Tincercad.

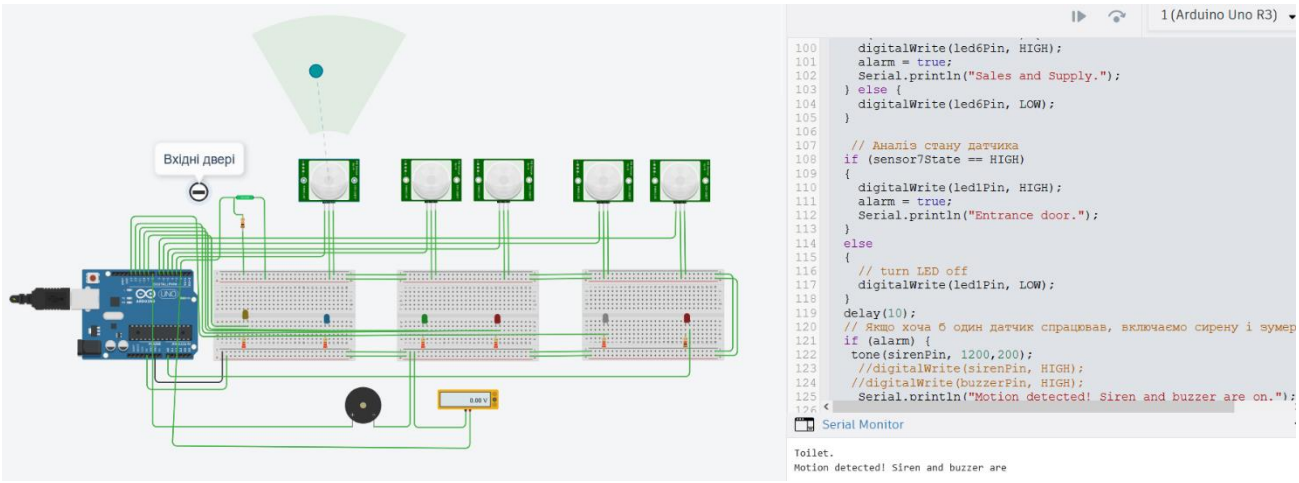


Рисунок 1.27. Тестування датчику руху приміщення «Туалет» у симуляторі Tincercad

Розглянемо роботу датчика нахилу (геркона). Датчик нахилу (TILT1) також функціонував відповідно до очікувань: при нахилі або зміні положення системи відбувалося спрацювання тривоги. Надійність спрацювання склала 100% у межах 10 тестових спроб. На рис. 1.28 представлено тестування датчику нахилу (геркону) вхідної двері приватного приміщення у симуляторі Tincercad.

Система індикації працює стабільно: світлодіоди загоряються відповідно до зони активації (колірна диференціація забезпечує зручність ідентифікації);

зумер вмикається при спрацюванні будь-якого датчика, подаючи гучний сигнал тривоги; час реагування на тривогу не перевищував 0,5 секунди з моменту фіксації події

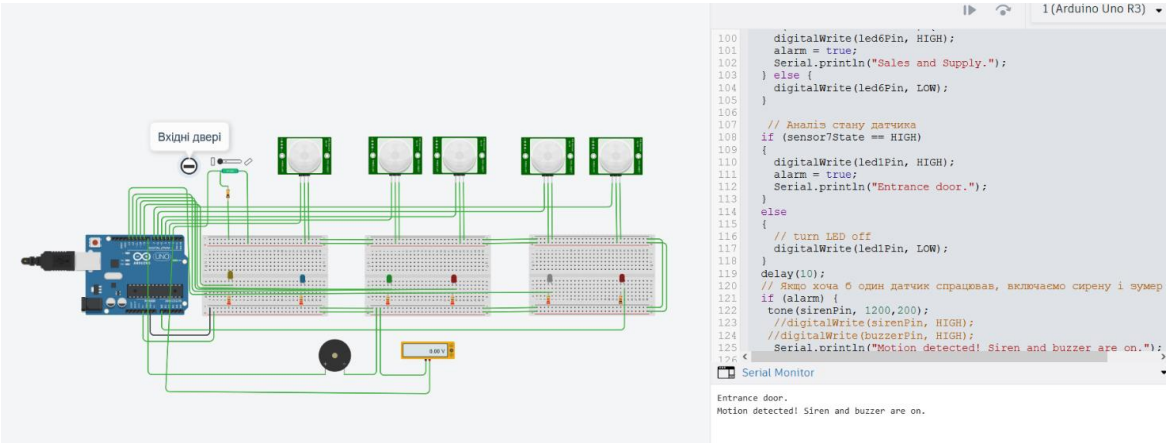


Рисунок 1.28. Тестування датчику нахилу (геркону) вхідної двері приватного приміщення у симуляторі Tincercad

Результати тестування підтвердили, що система безпеки: працює стабільно та точно; реагує оперативно на потенційні загрози; дає зрозумілу індикацію тривожних подій; може бути використана як в автономному, так і в інтегрованому режимі з іншими захисними системами. Отже, система відповідає вимогам до базової охоронної сигналізації для житлових або офісних приміщень.

2 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою даної дипломної роботи є розробка системи безпеки приватного середовища з використанням платформи Arduino на основі датчиків руху з інфрачервоним випромінюванням. Даний вид проекту відноситься до науково-дослідницької розробки. Оцінка якості розробленого проекту включає визначення трудомісткості і вартості його створення. Перелік етапів і робіт, що виконуються при проведенні НДР, приведений в таблиці 2.1.

Таблиця 2.1. Розподіл робіт по етапах і видах виконавців

Етап проведення НДР	Вигляд робіт	Посада виконавця
Розробка технічного завдання	1.Складання і затвердження ТЗ для НДР по розробці «Розробка системи безпеки приватного середовища на платформі Arduino»	Дипломник, керівник
Вибір напряму дослідження	1. Пошук джерел. Аналіз інформації: Систематизація даних 2. Формулювання можливих напрямів вирішення завдань, поставлених в технічному завданні НДР і їх порівняння. 3. Розробка плану проведення досліджень для подальшої розробки.	Дипломник керівник
Теоретичні і експериментальні дослідження	1. Огляд теоретичних основ безпеки приватного середовища. 2. Проектування та реалізація системи безпеки на платформі Arduino 3. Тестування та оцінка ефективності системи	Дипломник керівник консультанти
Узагальнення і оцінка результатів	1. Узагальнення результатів попередніх етапів. 2. Оцінка повноти вирішення завдань. 3. Складання і оформлення звіту.	Дипломник керівник консультант

В умовах відсутності нормативної бази тривалість виконання окремих робіт розраховується на основі вірогідних оцінок робіт, що задаються виконавцями.

Таблиця 2.2.Очікувана трудомісткість робіт.

Склад роботи	Очікуваний час виконання (дні)
1. Складання і затвердження ТЗ для НДР по розробці «Модернізація проєкту муніципальної мережі на базі технології оптичного зв'язку»	1
2. Збір і вивчення науково – технічної літератури, технічної документації і інших матеріалів.	4
3. Формулювання можливих напрямів вирішення завдань, поставлених в технічному завданні НДР і їх порівняльна оцінка.	2
4. Розробка плану проведення досліджень для подальшої розробки.	3
5. Огляд теоретичних основ безпеки приватного середовища.	4
6. Проектування та реалізація системи безпеки на платформі Arduino	4
7 . Тестування та оцінка ефективності системи	4
8. Узагальнення і оцінка результатів досліджень.	4
Всього:	26

Враховуючи, що науково-технічна продукція значною мірою є результатом інтелектуальної праці**,** розрахунок її собівартості та ціни виконання науково-дослідної роботи (НДР) включає такі основні статті витрат: витрати на матеріали, основна і додаткова заробітна плата, відрахування до єдиного соціального фонду страхування, витрати на роботи сторонніх організацій, інші витрати

1. Витрати на матеріали – 400 грн.

2. Основна заробітна плата це прямі виплати фахівцям, які безпосередньо залучені до виконання НДР. Основна заробітна плата визначається на основі трьох ключових показників**:** кількості виконавців**,** трудомісткості їхніх завдань **та** середньої заробітної плати за робочий день**.** При цьому, Закон України «Про Державний бюджет України на 2025 рік» (стаття 8) встановлює мінімальну місячну зарплату в розмірі 8000 грн та мінімальну погодинну ставку в 48 грн **з** 1 січня 2025 року. Середня зарплата за один робочий день для кожного виконавця визначена по формулі:

Зден= п.т.с. * 8;

де п.т.с – погодинна тарифна ставка, грн..;

8 – тривалість робочого дня,год.

Витрати на основну заробітну плату НДР, що включаються в собівартість, приведені в таблиці 2.3.

Таблиця 2.3 Витрати на основну заробітну плату.

Виконавець	Погодинна тарифна ставка, грн	Денна ставка, грн	Трудомісткість робочих днів	Сума основної зарплати,грн
Дипломник	48,00	364	26	8528,00
Керівник	120,00	960	1	960,00
Консультант по економіч. частині.	100,00	800	0,25	200,00
Консультант по охороні праці	100,00	800	0,25	200,00
Нормоконтроль	100,00	800	0,25	200,00
Всього (Зо)				10088,00

3. Додаткова заробітна плата: Виплати, пов'язані з оплатою відпусток, лікарняних, премій тощо. У наукових закладах додаткова заробітна плата складає 10-12% від основної заробітної плати.

Зд=0,12* Зо = 0,12* 10088,00= 1210,56 грн

4. Відрахування до Єдиного соціального фонду страхування: Обов'язкові платежі, що нараховуються на фонд заробітної плати відповідно до чинного законодавства.

Зєсв=0,22*(Зо+Зд)=0,22*(10088,00+ 1210,56) = 2485,68 грн..

5.До накладних витрат відносять витрати на управління і господарське обслуговування, що відноситься до всіх виконуваних НДР. У наукових закладах накладні витрати складають 40 -120% від основної і додаткової заробітної плати.

Рнакл= (З0+Зд)*0,5 = (10088,00+ 1210,56) * 0,6 = 6779,14 грн.

Ці складові формують повну картину фінансових витрат, пов'язаних зі створенням нової науково-технічної продукції. На підставі отриманих даних по окремих статтях витрат складена калькуляція планової собівартості в цілому НДР за формою, приведеною в таблиці 2.4.

Таблиця 2.4 Калькуляція планової собівартості

Статті витрат	Сума, грн.
1. Матеріали	400,00
2. Основна заробітна плата	10088,00
3. Додаткова заробітна плата	1210,56
4. Відрахування до єдиного соціального внеску	2485,68
5. Накладні витрати	6779,14
Планова собівартість (Спл)	20 963,37

Плановий прибуток визначений по формулі:

Ппл = 0,1*Спл=0,1*20 963,37= 20 96,34 грн

Де 0,1 – норматив, який враховує граничний рівень рентабельності, встановлений чинним законодавством для науково-технічної продукції.

Договірна ціна визначається по формулі:

Цндр = Спл + Ппл= 20 963,37 + 20 96,34 = 23059,71 грн.

Ціну реалізації встановлюємо з урахуванням ПДВ

Цр = Цндр + ПДВ= 23059,71 + 23059,71 * 0,2 = 27671,65 грн.

3 РОЗДІЛ З ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ

Організація здорового та безпечного робочого середовища покладається на керівництво підприємств, установ і організацій. Адміністрація зобов'язана впроваджувати сучасні заходи з охорони праці, що сприяють запобіганню нещасних випадків і створенню оптимальних санітарно-гігієнічних умов, які, у свою чергу, знижують ризик виникнення професійних захворювань. Умови, в яких працює співробітник, безпосередньо впливають на його здоров'я, працездатність і всебічний особистісний розвиток.

Темою мого дипломного проекту є «Розробка системи безпеки приватного середовища на платформі Arduino». У сучасних умовах цифровізації та автоматизації особливу увагу слід приділяти питанням охорони праці при розробці електронних систем безпеки. Використання платформи Arduino потребує суворого дотримання норм електробезпеки та правил роботи з низьковольтним обладнанням. Також важливим є правильне проектування та використання сенсорних систем задля уникнення ризиків для користувача при експлуатації пристрою.

3.1 Аналіз шкідливих та ризикових факторів

При проведенні паяльних робіт співробітники піддаються впливу низки шкідливих та небезпечних чинників, що виникають при використанні спеціалізованих інструментів. Серед основних факторів ризику слід відзначити:

- роботу з комп'ютерною та електротехнічною апаратурою,
- недостатню освітленість робочої зони,
- психоемоційні навантаження,
- високий рівень шуму,
- недостатню вентиляцію приміщення,
- порушення правил пожежної безпеки тощо.

3.2 Гігієнічні вимоги до виробничого середовища

Для безперебійного, безпечного та якісного виконання паяльних робіт необхідно суворо дотримуватись правил техніки безпеки та організувати робоче

місце оптимальним чином. Це означає, що всі інструменти та матеріали для паяння мають бути систематизовано розміщені, а роботи виконувати у заздалегідь підготовлених зонах, де мінімізовано вплив зовнішніх факторів.

Параметри мікроклімату робочої зони повинні відповідати вимогам санітарних норм мікроклімату виробничих приміщень (ДСН 3.3.6.042-99).

Рівень шуму має не перевищувати встановлених норм щодо виробничого шуму, ультразвуку та інфразвуку (ДСН 3.3.6.037-99).

Допустимі показники вібрації на робочих місцях зумовлені державними санітарними нормами загальної та локальної виробничої вібрації (ДСН 3.3.6.039-99).

Вимоги до рівнів електромагнітних полів визначені державними санітарними нормативами і правилами, затвердженими наказом МОЗ України від 18.12.2002 № 476.

3.3 Вимоги до організації робочого місця працівника

Згідно зі ст. 13 Закону України «Про охорону праці» (від 14.10.1992 р. № 2694-XII), роботодавець зобов'язаний забезпечити створення належних умов праці в кожному структурному підрозділі відповідно до чинних нормативно-правових актів та організувати лабораторні дослідження робочого середовища.

Паяння використовується для з'єднання заготовок зі сталі, кольорових металів і їх сплавів, а також для створення з'єднань із зазначених матеріалів. Найчастіше ця технологія застосовується в електромонтажних роботах, монтажі контрольно-вимірювальних приладів, виробництві радіо- та електроприладів, створенні теплових обмінників, а також у технологічних процесах, де використовують вироби з армованих пластин з твердих сплавів.

У виробничих приміщеннях концентрація шкідливих речовин не повинна перевищувати гранично допустимих значень, визначених відповідними стандартами (наприклад, ГОСТ 12.1.005-88 «Система стандартів безпеки праці. Загальні санітарно-гігієнічні вимоги до повітря робочої зони»).

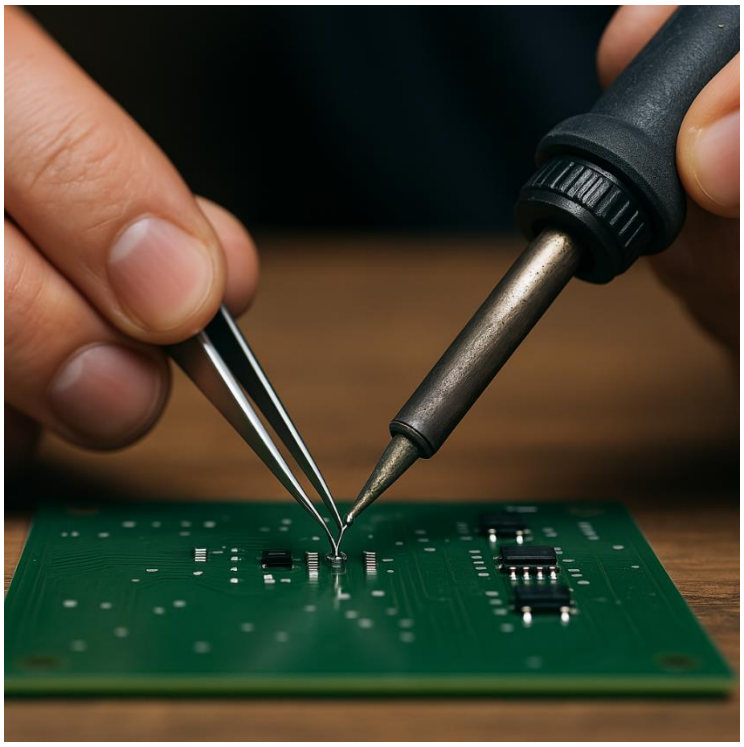


Рисунок 3.1. Процес паяння пристрою

Працівники, залучені до паяльних робіт, повинні мати забезпечення засобами індивідуального захисту, а також профілактичними засобами у вигляді захисних кремів, паст чи спеціального лікувально-профілактичного харчування.

Роботодавець повинен організувати:

Організувати проведення попередніх медичних оглядів (при прийнятті на роботу) та регулярних періодичних оглядів відповідно до затвердженого порядку МОЗ України (наказ від 21.05.2007 № 246).

Провести атестацію робочих місць за умовами праці відповідно до встановлених норм (відповідно до постанови Кабінету Міністрів України від 01.08.1992 № 442).

У разі необхідності розробити і впровадити заходи з мінімізації шкідливого впливу виробничих чинників на здоров’я співробітників.

3.4 Електробезпека

Обладнання, таке як персональні комп'ютери, периферійні пристрої, апаратура управління, контрольно-вимірювальні прилади та освітлювальні засоби, а також електропроводи і кабелі, мають відповідати класифікаційним

вимогам за зоною застосування та бути обладнаними захисними елементами для запобігання коротким замиканням та іншим аварійним ситуаціям.

Лінія електропостачання для ПК і периферії повинна формувати окрему групову мережу з трьома провідниками: фазовим, робочим нульовим та захисним нульовим. При цьому нульовий захисний провід використовується виключно для заземлення апаратів, а його функціональність не може дублювати робочий нульовий провід. Він прокладається окремо від робочої лінії від групового розподільника до електроживильних розеток, причому недопустиме підключення обох провідників до одного контактного затискача.

Основними причинами травмування електричним струмом є:

- прямий контакт з відкритими проводами,
- взаємодія з внутрішніми компонентами комп'ютера,
- використання несправного обладнання,
- відмова засобів захисту, з якими контактує користувач,
- непередбачене виникнення напруги через пошкодження ізоляції.

Для ефективного запобігання ураження струмом необхідно:

- суворо дотримуватись інструкцій з виконання робіт і правил експлуатації обладнання,
- забезпечувати недоступність частин пристроїв, що працюють під високою напругою, для оператора,
- використовувати високоякісні ізоляційні матеріали, товщина яких відповідає вимогам безпеки,
- підключати електроживлення через спеціально обладнані розетки з функцією занулення,
- розраховувати споживану потужність для запобігання перевантаженням,
- здійснювати надійне заземлення всіх металевих корпусів, доступних для оператора.

3.5 Пожежна безпека

Виробничі приміщення, технологічні установки та будівлі повинні бути обладнані першоджерельними засобами пожежогасіння, до яких належать:

- вогнегасники,
- контейнери з піском,
- негорючі покривала з теплоізоляційного матеріалу,
- високоміцні тканинні вироби тощо.

Ці засоби повинні відповідати нормативним вимогам, затвердженим документами з технологічного проектування та Правилами пожежної безпеки в Україні (НАПБ А.О1.001-2014). Вогнегасники слід встановлювати в легкодоступних, добре помітних місцях (наприклад, в коридорах, біля входів та виходів або у зонах підвищеного ризику виникнення пожежі), захищаючи їх від прямого сонячного випромінювання та впливу опалювальних приладів. Розміщення вогнегасників має забезпечувати їхнє повне відкриття, причому вони встановлюються не вище 1,5 м від підлоги та на безпечній відстані від дверей.

Рисунок 3.2. Засоби пожежогасіння

Також засоби пожежогасіння (рис.3.2) не повинні заважати евакуації персоналу. Виробничі приміщення повинні забезпечуватись запасними виходами, а двері до них мають бути позначені зрозумілими освітленими написами, наприклад, «Запасний вихід». План евакуації повинен бути розміщений у видному місці біля основного виходу.

ВИСНОВКИ

У ході виконання дипломної роботи було реалізовано повний цикл розробки багаторівневої системи безпеки приміщення з використанням мікроконтролера Arduino Uno. Основною метою роботи було створення функціональної, недороговартісної та надійної системи охорони, здатної реагувати на різні типи загроз у реальному часі.

У результаті виконано наступне:

1) проаналізовано сучасні підходи до побудови систем безпеки, що дало змогу обґрунтовано обрати компоненти та архітектуру майбутньої системи;

2) розроблено структурну та принципову електричну схему, яка включає інфрачервоні датчики руху (PIR), датчик нахилу, світлодіодні індикатори, звукову сигналізацію та блок керування на базі Arduino Uno;

3) реалізовано програмне забезпечення мікроконтролера, що забезпечує обробку сигналів від сенсорів, керування індикацією та подачею звукового сигналу при виявленні порушення;

4) проведено моделювання та тестування системи, які засвідчили її стабільну роботу, високу чутливість сенсорів та швидке реагування на події (менше 1 секунди);

5) обґрунтовано вибір Arduino Uno, як оптимальної платформи з достатньою кількістю входів/виходів, підтримкою сенсорів та доступним середовищем розробки.

Система показала хороші результати при тестуванні в умовах, наближених до реальних, і може бути використана для охорони житлових, офісних чи складських приміщень. Простота конструкції, доступність компонентів і відкритість платформи Arduino створюють потенціал для подальшого розвитку системи, наприклад, із додаванням бездротового зв’язку (Wi-Fi, GSM), інтеграцією з мобільними додатками або віддаленим моніторингом.

Отже, поставлені в роботі завдання виконано повністю, а мета досягнута.

ПЕРЕЛІК ВИКОРИСТАНИХ ІНФОРМАЦІЙНИХ ДЖЕРЕЛ

1 Сучасні телекомунікації: мережі, технології, безпека, економіка, регулювання, Довгий С.О., Воробієнко П.П., Гуляєв К.Д., за загальною редакцією члена-кореспондента НАН України Довгого С.О., Київ “АзимутУкраїна”, 607 стор., 2013 р.

2 Богуш В.М., Юдін О.К. Інформаційна безпека держави. Навчальний посібник – К.: «МК-Прес», - 2005. – 432 с.

3 Шон Харрис. CISSP Посібник для підготовки до іспиту / Шон Харрис // П’ята редакція, 2019. - 875 с.

4 Бабій, М. В., В. А. Бабій, and А. О. Мартинчук. "Інтелектуальні системи безпеки руху." *Матеріали V Міжнародної науково-практичної конференції «Підвищення надійності і ефективності машин, процесів і систем». Кропивницький: ЦНТУ* (2023): 156.

5 Kumar, N. Sathish, et al. "IOT based smart garbage alert system using Arduino UNO." *2016 IEEE region 10 conference (TENCON)*. IEEE, 2016.

6 Taneja, Kriti, and Sanmeet Bhatia. "Automatic irrigation system using Arduino UNO." *2017 International Conference on Intelligent Computing and Control Systems (ICICCS)*. IEEE, 2017.

7 Access control systems. [Електроний ресурс]. – Режим доступу: https://isbc.com/app_area/humans-id/access-control/.

8 Среда разработки Arduino. [Електроний ресурс]. – Режим доступу: http://arduino.ru/Arduino_environment.

9 Getting Started with Arduino UNO. [Електроний ресурс]. – Режим доступу: https://www.arduino.cc/en/Guide/ArduinoUno.

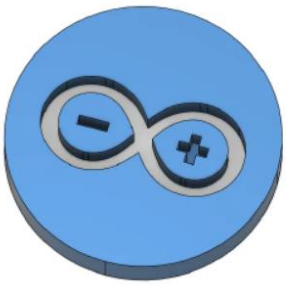
10Language Reference. [Електроний ресурс]. – Режим доступу: https://www.arduino.cc/reference/en.

ДОДАТОК А. Слайди мультимедійної презентації

ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ

РОЗРОБКА СИСТЕМИ БЕЗПЕКИ ПРИВАТНОГО СЕРЕДОВИЩА НА ПЛАТФОРМІ ARDUINO

ДИПЛОМНИЙ ПРОЕКТ



Керівник:
к.ф.н., доцент каф. КБ та ТЗІ ДУІТЗ Стайкуца С.В.

Виконав:
студент групи 4КБ-02 Первухін М.Ю.

2025

Ефективність технічних засобів охорони об’єктів

Технічні засоби безпеки

– це пристрої, програми та системи, призначені для забезпечення безпеки на об'єкті, будівлі або території.

Продуктивність	Мінімальний вплив на продуктивність	Низька кількість помилок
Простота використання	Автоматизація	Висока точність
Моніторинг та звітність	Скалабельність	Оптимізація ресурсів

Компоненти системи безпеки приватних середовищ

Складові системи безпеки для приватних середовищ

3

Щодо мети спостереження

Ідентифікація користувача	*Впізнавання особи за допомогою певного параметру, наприклад, коду, RFID-мітки або біометричних даних*
Аутентифікація	*Перевірка відповідності пред'явленого параметра даним, збереженим у системі*
Прийняття рішення	*Дозвіл або заборона на доступ до приміщення*
Реєстрація подій	*Фіксація усіх спроб входу та виходу, як успішних, так і відхилених*

Основні функції контролю доступу

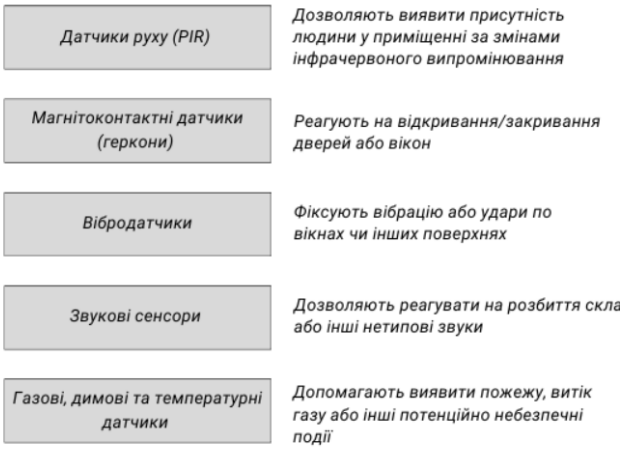
Підвищення рівня безпеки об'єкта за рахунок постійного моніторингу	*Створення відеодоказів у разі інцидентів (порушення, крадіжки, вандалізм)*
Забезпечення контролю за роботою персоналу або технічного обладнання	*Інтеграція з іншими охоронними системами*

Мета спостереження

4

Загрози приватних середовищ

Загрози приватних середовищ



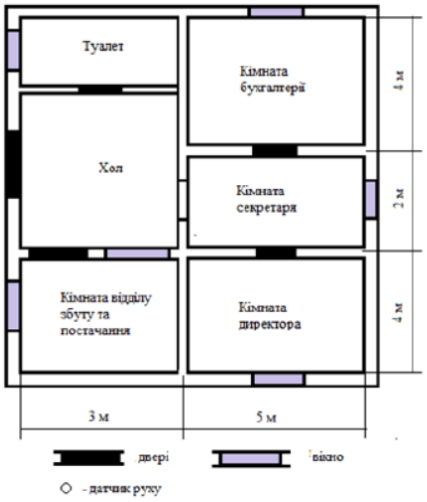
Типи сенсорів в фокусі виявлення загроз

Огляд існуючих рішень для забезпечення безпеки на основі Arduino

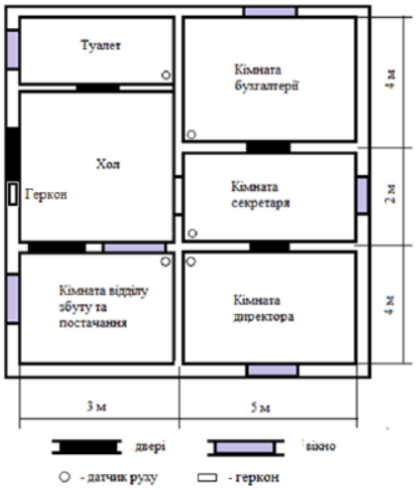
Технічні складові забезпечення безпеки на основі платформи Arduino

Відеокамера VGA OV7670

Модулі виявлення диму, метану та зрідженого газу



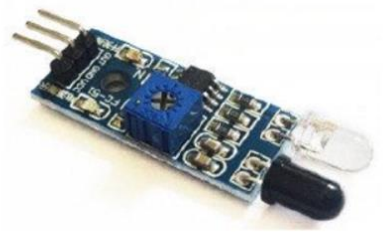
План розташування кімнат приватного приміщення



План розташування кімнат приватного приміщення із сигналізацією

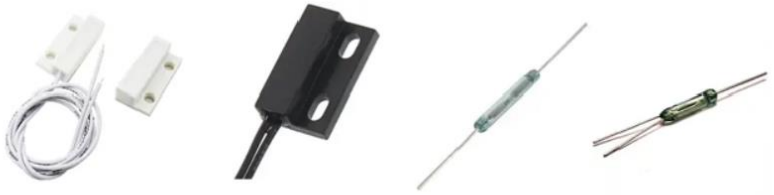
Загальні характеристики плати ArduinoUno:

a)мікроконтролер: ATmega328;
b)робоча напруга: 5В;
c)вхідна напруга (рекомендована) - 6-9В;
d)цифрових входів/виходів: 14
(з яких 6 можуть бути використані як ШІМ);
e)аналогових входів – 6;
f)сила струму на входах/виходах: 40 мА;
g)сила струму для 3.3В виходу: 50 мА;
h)пам'ять: 32 кБ з яких 2кб використовується бутлоадер;
i)SRAM: 2 кБ;
j)EEPROM: 1 кБ.
k)частота: 16 МГц
l)USB інтерфейс: CH340



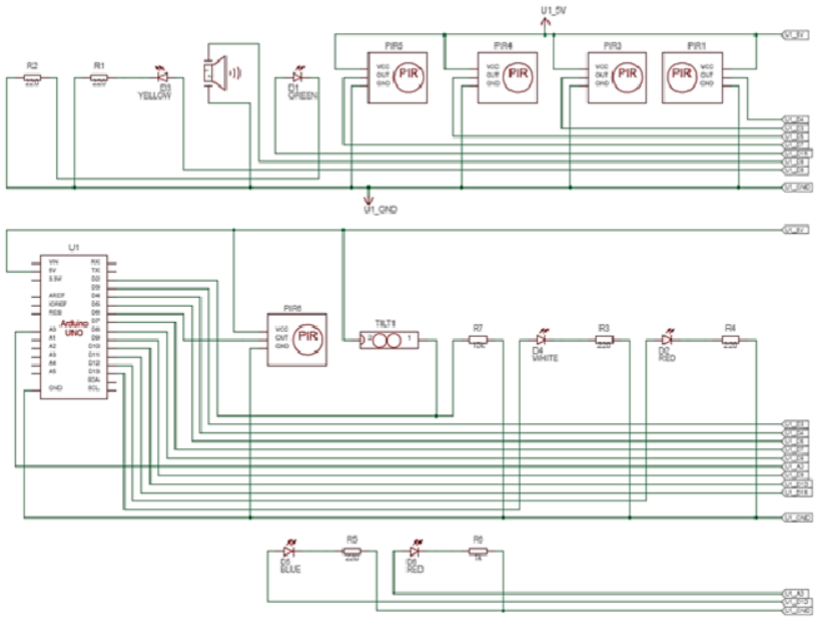
Плата інфрачервоного датчику обходу перешкод Arduino

Плата інфрачервоного датчику руху для ARDUINO HC-SR501



Зовнішній вид герконів

Схема електрична принципіальна системи безпеки приватного середовища



Алгоритм дій при роботі з Arduino IDE

Найменування на схемі	Кількість елементів	Назва елементу
U1	1	Arduino Uno R3
PIR1, PIR3, PIR4, PIR5, PIR6	5	PIR Sensor
PIEZO1	1	Piezo
R1, R2, R3, R4, R5	5	220 Ω Resistor
D1,	1	Green LED
D2, D6	2	Red LED
D3	1	Yellow LED
D4	1	White LED
D5	1	Blue LED
R6	1	1 kΩ Resistor
Meter1	1	Voltage Multimeter
TILT1	1	Tilt Sensor
R7	1	10 kΩ Resistor

Перелік елементів схеми системи безпеки приватного середовища

Загальне призначення системи – це модульна охоронна сигналізація, яка: реагує на рух у приміщеннях (через PIR-датчики), може фіксувати зміну положення (датчик нахилу), дає світлову і звукову індикацію при тривозі, побудована на простій і надійній платформі Arduino Uno

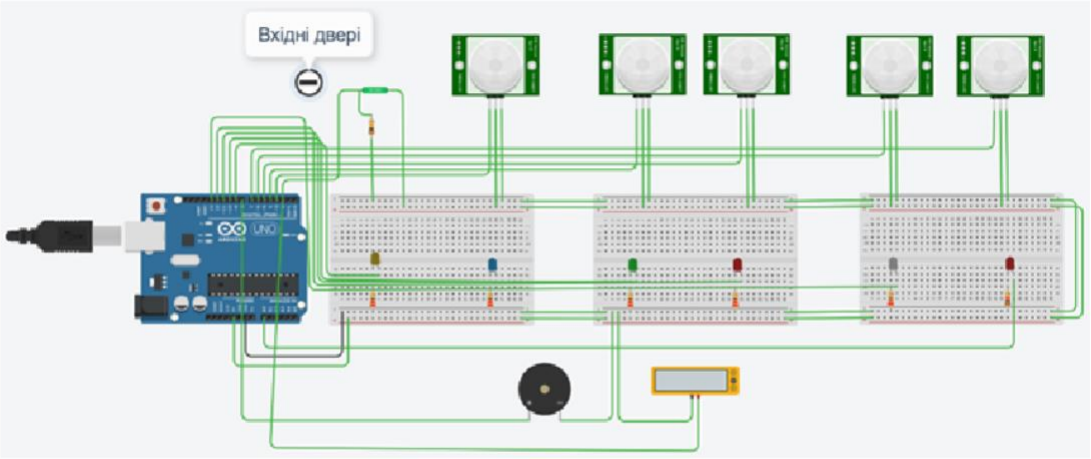
Розробка програмного забезпечення

Програма реалізує логіку роботи охоронної сигналізації для 6 приміщень підприємства та вхідних дверей. Система реагує на спрацювання датчиків руху та геркона, активує відповідні світлодіоди для візуальної індикації, а також запускає сирену й зумер у разі тривоги.

Setup-функція	*Встановлює пінові режими: датчики: INPUT; світлодіоди, сирена та зумер: OUTPUT; ініціалізує серійне з'єднання для відлагодження через монітор порту*
Loop-функція	*Забезпечує зчитування станів датчиків: датчики руху та геркон зчитуються через digitalRead(); у разі спрацювання (значення HIGH) відповідному світлодіоду подається живлення, а в серійну консоль виводиться повідомлення, наприклад: Toilet. або Entrance door*
Формування сигналу тривоги	*Якщо хоча б один датчик активний, встановлюється прапор alarm = true, Реакція на тривогу: у випадку alarm = true активується сирена (tone(sirenPin, 1200, 200) – короткий звуковий імпульс) і зумер (призначений, але в коді фактично не активується, можна додати tone(buzzerPin, ...)). Якщо всі датчики неактивні, то сирена та зумер вимикаються.*
Затримка delay(500)	*Призначена для запобігання надто частому оновленню станів*

Логіка роботи програми

Зображення макету схеми системи безпеки приватного середовища у симуляторі Tincercad

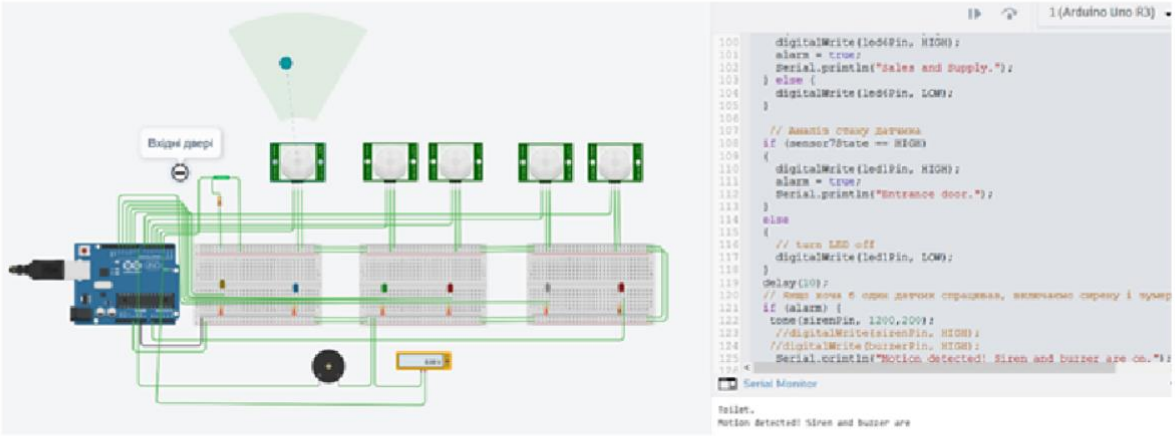


Tinkercad, оснований на веб-платформі, пропонує симулятор Arduino, що дозволяє вам розробляти, тестувати і навіть взаємодіяти з вашими проектами Arduino без необхідності використання фізичного обладнання

Загальні блоки ПЗ щодо забезпечення системи безпеки приватного середовища

Піни підключення датчиків	*Піни підключення світлодіодів*	*Пін підключення сирен*
1	2	3
Пін підключення зумера	*Налаштування пінів датчиків як входів*	*Налаштування пінів світлодіодів як виходів*
4	5	6
Налаштування піну сирени як вихід	*Налаштування піну зумера як вихід*	*Ініціалізація серійного зв'язку*
7	8	9
Змінні для зберігання стану датчиків	*Змінна для індикації спрацювання хоча б одного датчика*	*Перевірка стану кожного датчика та індикація світлодіодом*
10	11	12

Тестування датчику руху приміщення «Туалет» у симуляторі Tincercad



Висновки

В роботі проведено розробку розробка системи безпеки приватного середовища на платформі Arduino.

Результати досліджень, виконаних в роботі дозволили встановити, що:

1) платформа Arduino має інтегровану середу для розробки та програмування на мові C++;

2) платформа Arduino має широкий вибір різних мікроконтролерів та датчиків для створення системи безпеки приватного середовища;

3) для завдання розробки схеми та програмного забезпечення можна використовувати як апаратні рішення, так і симулятори (наприклад, Tinkercad Arduino Simulator);

4) застосування симулятору дало змогу перевірити правильність написання коду програми та працездатність роботи схеми електричної принципіальної системи охоронної сигналізації та реалізувати ТЗ на розробку рішення

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

РЕЦЕНЗІЯ

на дипломний проект здобувача (здобувачки) освіти
відділення комп'ютерних систем

Первухіна Максима Юрійовича

(прізвище, ім`я та по батькові)

Спеціальність *123 «Комп'ютерна інженерія»*

Освітня програма *«Безпека комп'ютерних систем і мереж»*

Керівник дипломного проекту (роботи) *Стайкуца Сергій Володимирович*

(прізвище, ім`я та по батькові)

Тема дипломного проекту (роботи) *Розробка системи безпеки приватного середовища на платформі Arduino*

Обсяг розрахунково-пояснювальної записки *84* сторінок

Обсяг графічної (презентаційної) частини *16* аркушів (слайдів)

ХАРАКТЕРИСТИКА ДИПЛОМНОГО ПРОЕКТУ (РОБОТИ)

а) заключення про ступінь відповідності виконаного дипломного проекту завданню

Представлений на рецензію дипломний проект відповідає затвердженій темі та виконаний відповідно технічному завданню. Дипломний проект присвячений темі розробки системи безпеки приватного середовища та складається з пояснювальної записки та мультимедійної презентації, що містить приклади роботи програми.

б) характеристика виконання кожного розділу дипломного проекту

Пояснювальна записка складається з основного розділу (аналізу предметної області, складання ТЗ, проектування рішення, реалізації та тестування), економічного розділу, розділу охорони праці та додатків. Перелічені розділи поетапно охоплюють розробку, виконані докладно та обґрунтовано. Розділ охорони праці містить загальну інформацію та вимоги до організації робочого місця. Економічний розділ проекту містить розрахунок ціни програмного продукту нормативним методом.

в) оцінка якості виконання пояснювальної записки та графічної частини дипломного проекту

Графічна частина складається з 16 слайдів мультимедійної презентації, виконаної у програмному продукті MS PowerPoint, які містять ілюстративні схеми, скріншоти роботи програмного застосунку, передбачені технічним завданням. Пояснювальна записка виконана акуратно та у відповідності до норм. Якість виконання графічної частини проекту та пояснювальної записки добра, розробку виконано у повному обсязі.

г) перелік позитивних якостей дипломного проекту *Реалізовано програмно-апаратне рішення в рамках екосистеми Arduino з використанням компонентів напряму безпеки.*

Детально розглянуто етапи життєвого розробки рішення для захисту приватного середовища, а саме – проектування, реалізація та тестування.

д) основні недоліки дипломного проекту

Треба було розглянути більш розширений спектр компонентів екосистеми Arduino. Є лише базові функції локального реагування. Передача тривог через SMS чи push не реалізована. Обмежене опрацювання безпеки зберігання і шифрування даних. Паролі, якщо використовуються, зберігаються у відкритому вигляді. Відсутні хешування або захист EEPROM.

Оцінка розрахункової частини *Добре*

Оцінка графічної частини *Відмінно*

Загальна оцінка *Добре*

Прізвище, ім'я, по батькові рецензента *к.т.н. Шибаєва Наталя Олегівна*

Місце роботи і посада рецензента *Національний університет «Одеська політехніка», доцент кафедри інформаційних технологій*

Підпис:

«23» 06 2025 р.

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

ВІДГУК

керівника на дипломний проект здобувача (здобувачки) освіти

відділення комп'ютерних систем

Первухіна Максима Юрійовича

(прізвище, ім`я та по батькові)

Спеціальність: *123 "Комп'ютерна інженерія"*

Освітня програма: *«Безпека комп'ютерних систем і мереж»*

Тема дипломного проекту: Розробка системи безпеки приватного середовища на платформі Arduino

ХАРАКТЕРИСТИКА ДИПЛОМНОГО ПРОЕКТУ

а) обсяг і якість виконання проекту (графічного матеріалу і розрахунково-пояснювальної записки) *Дипломний проект виконано відповідно технічному завданню. Пояснювальна записка містить __ сторінки. У пояснювальній записці розглянуто проблематику розробки систем безпеки приватного середовища на платформі Arduino із вибором компонентного складу. Графічна частина складається з слайдів мультимедійної презентації, які також містять креслення, передбачені технічним завданням. Якість виконання пояснювальної записки та графічної частини добра, розробку виконано в повному обсязі.*

б) самостійність роботи над проектом: *Протягом всього строку дипломного проектування та переддипломної практики здобувач освіти Первухін М.Ю. виконував всі етапи розробки проекту, без порушення термінів. Роботу студент виконував в більшій мірі самостійно, з оглядом на рекомендації керівника та отримуючи зворотній зв'язок.*

в) теоретична підготовка випускника (випускниці): *Здобувач освіти Первухін М.Ю. під час роботи над дипломним проектом проаналізував достатню кількість літературних джерел та матеріалів за даною тематикою.*

Вважаю, що теоретична підготовка дипломника якісна і він готовий до захисту дипломного проекту.

г) вміння розв'язувати виробничі та конструкторські питання _____

Під час дипломного проектування здобувач освіти Первухін М.Ю. приймав рішення щодо вибору обладнання, аналізував вимоги на етапах проектування, розробляв проектні рішення, обґрунтовував вибір платформи розробки, мови програмування та алгоритмів реалізації розробленого проекту.

Оцінка розрахункової частини *Добре*

Оцінка графічної частини *Відмінно*

Загальна оцінка *Добре*

Прізвище, ім'я, по батькові керівника дипломного проекту

Стайкуца Сергій Володимирович

Місце роботи і посада керівника дипломного проекту

"Державний університет інтелектуальних технологій і зв'язку", доцент кафедри кібербезпеки та технічного захисту інформації, помічник декана факультету інформаційних технологій та кібербезпеки

Підпис _____

«____»_____2025 р.

ДОЗВІЛ
НА РОЗМІЩЕННЯ
ВИПУСКНОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ
(ДИПЛОМНОГО ПРОЕКТУ)
В ЕЛЕКТРОННОМУ РЕПОЗИТАРІЇ ВСП «ОТФК ОНТУ»

Ми, що нижче підписалися,

Первухін Максим Юрійович
здобувач освіти гр. 4КБ-02, та

Стайкуца Сергій Володимирович,
керівник дипломного проекту,

не заперечуємо щодо розміщення електронного варіанту пояснювальної записки до дипломного проекту фахового молодшого бакалавра на тему:

«Розробка системи безпеки приватного середовища на платформі Arduino» (автор роботи – Первухін М.Ю., керівник роботи – Стайкуца С.В.)

виконаного у ВСП «Одеський технічний фаховий коледж Одеського національного технологічного університету» в 2025 році, у повному обсязі в електронному репозитарії ВСП «ОТФК ОНТУ» для вільного доступу через мережу Інтернет.

Несемо відповідальність за ідентичність електронного та друкованого варіантів випускної кваліфікаційної роботи і даємо згоду на обробку персональних даних.

Виконавець _____ / Первухін М.Ю. /

Керівник _____ / Стайкуца С.В. /

«17» червня 2025 р.

ДОВІДКА

циклової комісії КТ та ПІ
про допуск до захисту дипломного проєкту
здобувача (здобувачки) освіти IV курсу
відділення комп'ютерних систем групи 4КБ-02

Первухіна Максима Юрійовича

на тему *Розробка системи безпеки приватного середовища на платформі Arduino*

Висновок відповідальної особи за проведення нормоконтролю:

пояснювальна записка до дипломного проєкту виконана з некритичними порушеннями ДСТУ та оформлена відповідно до вимог Положення про дипломне проєктування

(підпис)	*20.06.2025* (дата)	*Петрашова В.І.* (П.І.Б.)

Висновок відповідальної особи за перевірку роботи на наявність академічного плагіату *згідно звіту про перевірку від 18.06.2025 р. значення коефіцієнту подібності в роботі становить 15,51%, коефіцієнт цитування – 1,35%.*

(підпис)	*20.06.2025* (дата)	*Краснокутська К.Г.* (П.І.Б.)

Попередня експертиза (малий захист) дипломного проєкту

здобувача (здобувачки) освіти *Первухіна М.Ю.* (П.І.Б.)

проведена «*20*» *червня* 2025 р.

Висновки *Пояснювальна записка до дипломного проєкту виконана у повному обсязі. Випускна кваліфікаційна робота (дипломний проєкт) відповідає вимогам Положення про дипломне проєктування та рекомендована до захисту.*

Голова ЦК КТ та ПІ _____ (підпис) *Кривченко Ю.В.* (П.І.Б.)

StrikePlagiarism.com

Дата звіту 6/18/2025
Дата редагування 6/18/2025

Документ прийнятий

Звіт подібності

метадані

Назва організації
Odesa Technical Professional College of Odesa National University of Technology
Заголовок
Розробка системи безпеки приватного середовища на платформі Arduino
Автор Науковий керівник / Експерт
Первухін Максим ЮрійовичСтайкуца Сергій Володимирович
підрозділ
Відокремлений структурний підрозділ "Одеський технічний фаховий коледж Одеського національного технологічного університету"

Обсяг знайдених подібностей

Коефіцієнт подібності визначає, який відсоток тексту по відношенню до загального обсягу тексту було знайдено в різних джерелах. Зверніть увагу, що високі значення коефіцієнта не автоматично означають плагіат. Звіт має аналізувати компетентна / уповноважена особа.

КП 1

КЦ

25	11194	92009
Довжина фрази для коефіцієнта подібності 2	Кількість слів	Кількість символів

Тривога

У цьому розділі ви знайдете інформацію щодо текстових спотворень. Ці спотворення в тексті можуть говорити про МОЖЛИВІ маніпуляції в тексті. Спотворення в тексті можуть мати навмисний характер, але частіше характер технічних помилок при конвертації документа та його збереженні, тому ми рекомендуємо вам підходити до аналізу цього модуля відповідально. У разі виникнення запитань, просимо звертатися до нашої служби підтримки.

Заміна букв	ß	0
Інтервали	A→	0
Мікропробіли	·	6
Білі знаки	ß	1
Парафрази (SmartMarks)	a	55

Подібності за списком джерел

Нижче наведений список джерел. В цьому списку є джерела із різних баз даних. Колір тексту означає в якому джерелі він був знайдений. Ці джерела і значення Коефіцієнту Подібності не відображають прямого плагіату. Необхідно відкрити кожне джерело і проаналізувати зміст і правильність оформлення джерела.

10 найдовших фраз — Колір тексту

ПОРЯДКОВИЙ НОМЕР	НАЗВА ТА АДРЕСА ДЖЕРЕЛА URL (НАЗВА БАЗИ)	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	https://card-file.ontu.edu.ua/bitstreams/341a820e-d025-42f3-b7dc-27e831d6c66f/download	49 0.44 %
2	https://card-file.ontu.edu.ua/bitstreams/62baa43e-b968-4993-bb54-8cf8761a89b2/download	48 0.43 %
3	https://card-file.ontu.edu.ua/bitstreams/9908b7a9-6b3e-46f5-a46e-84d83787cfd4/download	40 0.36 %
4	https://card-file.ontu.edu.ua/bitstreams/549ee9fe-7574-4ae5-b500-9fe2711f33e6/download	40 0.36 %
5	https://card-file.ontu.edu.ua/bitstreams/6cf43324-8f08-4031-ba42-f80b18efbbc8/download	38 0.34 %

6	https://card-file.ontu.edu.ua/server/api/core/bitstreams/fc8a1853-39fc-4671-8807-2fd27ddb0779/content	38 0.34 %
7	https://card-file.ontu.edu.ua/server/api/core/bitstreams/44c16132-5f53-48e2-b6c0-61e9a2f0fd75/content	37 0.33 %
8	https://card-file.ontu.edu.ua/server/api/core/bitstreams/8da72e29-656f-4ee4-9b22-716dedf53ff5/content	37 0.33 %
9	https://card-file.ontu.edu.ua/bitstreams/6cf43324-8f08-4031-ba42-f80b18efbbc8/download	37 0.33 %
10	https://card-file.ontu.edu.ua/bitstreams/341a820e-d025-42f3-b7dc-27e831d6c66f/download	37 0.33 %

з домашньої бази даних (1.30 %)

ПОРЯДКОВИЙ НОМЕР	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	Моделювання системи охоронної сигналізації з використанням симулятору TinkerCAD [redacted] 6/17/2025 **Odesa Technical Professional College of Odesa National University of Technology (Відокремлений структурний підрозділ "Одеський технічний фаховий коледж Одеського національного технологічного університету")**	**76 (6) 0.68 %**
2	Модернізація системи відеоспостереження на основі механізмів інтелектуальної безпеки [redacted] 6/17/2025 **Odesa Technical Professional College of Odesa National University of Technology (Відокремлений структурний підрозділ "Одеський технічний фаховий коледж Одеського національного технологічного університету")**	**57 (5) 0.51 %**
3	Розробка web-застосунку для аутентифікації користувачів з використанням методів криптографії [redacted] 6/17/2025 Odesa Technical Professional College of Odesa National University of Technology (Відокремлений структурний підрозділ "Одеський технічний фаховий коледж Одеського національного технологічного університету")	12 (2) 0.11 %

з програми обміну базами даних (0.00 %)

ПОРЯДКОВИЙ НОМЕР	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)

з Інтернету (14.21 %)

ПОРЯДКОВИЙ НОМЕР	ДЖЕРЕЛО URL	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	**https://card-file.ontu.edu.ua/bitstreams/1dff552d-7200-49b8-ae1d-ba76a1335685/download**	**377 (34) 3.37 %**
2	**https://card-file.ontu.edu.ua/server/api/core/bitstreams/44c16132-5f53-48e2-b6c0-61e9a2f0fd75/content**	**242 (20) 2.16 %**
3	**https://card-file.ontu.edu.ua/bitstreams/341a820e-d025-42f3-b7dc-27e831d6c66f/download**	**116 (4) 1.04 %**
4	**https://card-file.ontu.edu.ua/bitstreams/62baa43e-b968-4993-bb54-8cf8761a89b2/download**	**104 (5) 0.93 %**
5	**https://card-file.ontu.edu.ua/bitstreams/6cf43324-8f08-4031-ba42-f80b18efbbc8/download**	**75 (2) 0.67 %**
6	**https://arduinogetstarted.com/faq/how-to-blink-multiple-led**	**50 (2) 0.45 %**
7	**https://card-file.ontu.edu.ua/bitstreams/549ee9fe-7574-4ae5-b500-9fe2711f33e6/download**	**45 (2) 0.40 %**
8	**https://card-file.ontu.edu.ua/bitstreams/b1c4b329-c3e8-4b5a-a1fc-ae232ec677bd/download**	**43 (3) 0.38 %**
9	https://card-file.ontu.edu.ua/bitstreams/035f6436-20b4-4ee6-8e99-bede670e308b/download	42 (4) 0.38 %
10	https://card-file.ontu.edu.ua/bitstreams/53ed22ad-8700-4162-b97a-082a1ad472d6/download	42 (4) 0.38 %
11	**https://card-file.ontu.edu.ua/server/api/core/bitstreams/8da72e29-656f-4ee4-9b22-716dedf53ff5/content**	**42 (2) 0.38 %**

12	**https://card-file.ontu.edu.ua/bitstreams/9908b7a9-6b3e-46f5-a46e-84d83787cfd4/download**	**40 (1) 0.36 %**
13	**https://card-file.ontu.edu.ua/server/api/core/bitstreams/fc8a1853-39fc-4671-8807-2fd27ddb0779/content**	**38 (1) 0.34 %**
14	**https://wokwi.com/projects/374480002658418689**	**31 (1) 0.28 %**
15	**https://card-file.ontu.edu.ua/bitstreams/c58b0ff5-46e0-49f8-8cbe-65c32256665d/download**	**30 (1) 0.27 %**
16	https://forum.arduino.cc/t/help-with-sequential-led-push-button-and-potentiometer/947264	28 (5) 0.25 %
17	https://card-file.ontu.edu.ua/server/api/core/bitstreams/4bb7255e-46d4-4349-9726-9698476da02d/content	26 (3) 0.23 %
18	https://card-file.ontu.edu.ua/bitstreams/29489599-0581-4ce6-8890-c3b13d9f2e0e/download	26 (2) 0.23 %
19	https://card-file.ontu.edu.ua/server/api/core/bitstreams/a05c07c5-bf65-4cb0-bdfa-e28694707551/content	23 (2) 0.21 %
20	https://card-file.ontu.edu.ua/bitstreams/bbaf3f38-16a8-4070-bead-5562769b7c71/download	23 (1) 0.21 %
21	https://link.springer.com/chapter/10.1007/978-3-031-37117-2_3	23 (2) 0.21 %
22	https://card-file.ontu.edu.ua/bitstreams/aed610a6-43ef-47e0-9066-e85c89456f3e/download	21 (2) 0.19 %
23	https://card-file.ontu.edu.ua/bitstreams/82a6d375-2b69-4233-b80f-fbfd149b7747/download	21 (2) 0.19 %
24	https://elartu.tntu.edu.ua/bitstream/lib/46148/2/Bachelor_Thesis_Fil_2024.pdf	18 (2) 0.16 %
25	https://card-file.ontu.edu.ua/bitstreams/34a6756b-592f-4b77-a805-183aa03a6a26/download	17 (1) 0.15 %
26	http://uadoc.zavantag.com/text/18266/index-1.html	15 (1) 0.13 %
27	http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0121-750X2019000300224&lng=en&tlng=es	9 (1) 0.08 %
28	https://card-file.ontu.edu.ua/bitstreams/5240e379-7721-49f0-8ee8-27140b0b473a/download	7 (1) 0.06 %
29	https://card-file.ontu.edu.ua/bitstreams/72fa1396-889f-4082-af7d-898b6ac28dd4/download	7 (1) 0.06 %
30	https://card-file.ontu.edu.ua/server/api/core/bitstreams/a141b658-5fa7-4f90-b0bd-7f0ccaed21e5/content	5 (1) 0.04 %
31	https://card-file.ontu.edu.ua/server/api/core/bitstreams/6eb6bf1c-5813-45e6-93c5-25539b4709d3/content	5 (1) 0.04 %

Список прийнятих фрагментів (немає прийнятих фрагментів)

ПОРЯДКОВИЙ НОМЕР	ЗМІСТ	КІЛЬКІСТЬ ОДНАКОВИХ СЛІВ (ФРАГМЕНТІВ)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: 123 «Комп'ютерна інженерія» Освітньо-професійна програма: **«Безпека** комп'ютерних **систем і мереж»**
Група: 4 КБ- 02

Дипломний проект
здобувача освіти денної форми навчання
КБ. 02.13.000.ДП

ПЕРВУХІНА
МАКСИМА **ЮРІЙОВИЧА м.** Одеса
2025 р. **МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»**

Спеціальність: 123 «Комп'ютерна інженерія»
Освітньо-професійна програма: **«Безпека** комп'ютерних **систем і мереж»**