**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.02.07.000.ДП**

## *КОБИЛЯНА ВЛАДИСЛАВА ВОЛОДИМИРОВИЧА*

**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 програмно-апаратних рішень для системи безпеки із використанням платформи Arduino

Проектний матеріал складається з пояснювальної записки на 73 сторінках та графічного (презентаційного) матеріалу на 13 аркушах (слайдах)

Дипломник _____ ( Кобилян В.В.)

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 «30» червня 2025 р. Протокол ЕК № 8

Оцінка ЕК 4 (добре) / 75 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 *Кобиляну Владиславу Володимировичу*

(прізвище, ім'я, по батькові)

1. Тема проекту *Розробка програмно-апаратних рішень для системи безпеки із використанням платформи Arduino*

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

2. Термін здачі закінченого проекту _____

3. Вихідні данні до проекту (роботи) *1. Мікроконтролери 2. Комплексні системи безпеки; 3.Розробка систем безпеки на базі мікроконтроллерів; 4.Мікроконтролерні платформи розробки; 5. Платформа Arduino; 6. Розробити технічне завдання на проектування системи безпеки; 7. Демонстрацію роботи системи представити в середовищі Tinkercad.*

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

*Аналіз сучасних підходів до розробки систем безпеки на базі мікроконтролерів; Призначення та вимоги до сучасних систем безпеки; Організація контролю доступу в системах безпеки; Проектування архітектури системи безпеки на базі Arduino; Можливості платформи Arduino в контексті безпеки; Вибір симуляторів для проєктування системи безпеки на основі Arduino; Реалізація, тестування та аналіз ефективності системи в Tinkercad*

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

*Призначення та вимоги сучасних систем безпеки; Вимоги до сучасних систем безпеки; Аналіз, фіксація зміни фізичних параметрів середовища в системах безпеки; Саботаж в системах безпеки підприємства; Можливості платформи Arduino в контексті безпеки; Додаткові можливості платформи Arduino; Вибір симуляторів для проектування системи безпеки на основі Arduino; Розробка схеми пристрою контролю доступу; Схема електрична принципіальна системи безпеки; Тестування та демонстрація системи.*

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 _____

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. Аналіз сучасних підходів до розробки систем* | *14.05.2025* | Виконано |
| | *безпеки на базі мікроконтролерів* | | |
| *2.* | *Призначення та вимоги до сучасних систем безпеки* | *17.05.2025* | Виконано |
| *3.* | *Саботаж в системах безпеки підприємства* | *20.05.2025* | Виконано |
| *4.* | *Проектування архітектури системи безпеки на базі* | *22.05.2025* | Виконано |
| | *Arduino, можливості платформи в контексті безпеки* | | |
| *5.* | *Вибір симуляторів для проєктування системи безпеки* | *01.06.2025* | Виконано |
| *6.* | *Аналіз існуючих рішень і підходів до створення охоронних* | *03.06.2025* | Виконано |
| | *систем.* | | |
| *7.* | *Постановка задачі проектування системи* | *06.06.2025* | Виконано |
| *8.* | *Розробка схеми підключення компонентів* | *10.06.2025* | Виконано |
| *9.* | *Розробка програмного забезпечення системи* | *11.06.2025* | Виконано |
| *10.* | *Тестування та демонстрація системи в Tinkercad* | *12.06.2025* | Виконано |
| *11.* | *Виконання економічних розрахунків* | *13.06.2025* | Виконано |
| *12.* | *Розробка заходів з охорони праці* | *14.06.2025* | Виконано |
| *13.* | *Виконання графічної частини проекту* | *16.06.2025* | Виконано |

Дипломник _____
(підпис)

Керівник _____
(підпис)

| Формат | Зона | Поз. | Позначення | Назва | Кіл. | Примітка |
|---|---|---|---|---|---|---|
| | | | | Документація | | |
| | | | КБ 02. 07 000. 00 ДП | Дипломний проект | | |
| А4 | | | КБ 02. 07 000. 00 ДП ПЗ | Пояснювальна записка | 1 | |

| Зм. | Арк. | № докум. | Підпис | Дата | КБ 02. 07 000. 00 ДП | | | |
|---|---|---|---|---|---|---|---|---|
| Розробив | | Кобилян В.В. | | 18.06 | Розробка програмно-апаратних рішень для системи безпеки із використанням Arduino | Літ. | Аркуш | Аркушів |
| Перевірив | | Стайкуца С.В. | | 18.06 | | Н Д П | 3 | 72 |
| Н. Контр. | | Петрашова В.І. | | 18.06.25 | | ВСП "ОТФК ОНТУ" гр.4КБ-02 | | |
| Затверд. | | Кривченко Ю.В. | | 18.06 | | | | |

# ЗМІСТ

# ВСТУП

У сучасному світі питання забезпечення безпеки об'єктів різного призначення. Зростаючий рівень злочинності, техногенні загрози, потреба в моніторингу й контролі доступу вимагають створення ефективних, доступних та гнучких систем охорони. У зв’язку з цим дедалі більше уваги приділяється розробці автоматизованих програмно-апаратних рішень, які здатні забезпечити своєчасне виявлення загроз і реагування на них. Одним із перспективних підходів є застосування мікроконтролерних платформ, таких як Arduino, що дозволяє створювати функціональні прототипи охоронних систем із мінімальними витратами.

Ця дипломна робота присвячена розробці системи безпеки з використанням платформи Arduino, яка поєднує апаратні компоненти та програмне забезпечення для моніторингу подій і реагування на них.

Мета роботи – розробити та реалізувати програмно-апаратне рішення для забезпечення охорони приміщення на основі мікроконтролера Arduino.

Завдання дослідження - провести аналіз сучасних систем безпеки та технічних засобів контролю, обґрунтувати вибір апаратної платформи та допоміжних модулів, спроєктувати архітектуру охоронної системи, розробити програмне забезпечення для управління системою, протестувати функціональність розробленого рішення.

Об'єкт дослідження – системи технічного захисту об'єктів на основі мікроконтролерів.

Предмет дослідження – методи й засоби реалізації охоронних функцій із використанням апаратних компонентів та програмних засобів платформи Arduino.

Практична цінність полягає у створенні доступного прототипу охоронної системи, що може бути використаний як основа для впровадження в приватних або малих комерційних об’єктах, а також для навчальних цілей у галузі мікроконтролерної техніки та інформаційної безпеки.

# 1 ОСНОВНИЙ РОЗДІЛ

## 1.1 Аналіз сучасних підходів до розробки систем безпеки на базі мікроконтролерів

### 1.1.1 Призначення та вимоги до сучасних систем безпеки

Сучасні системи безпеки призначені для виявлення, запобігання та реагування на несанкціоновані дії, які можуть загрожувати майну, здоров'ю або інформаційній цілісності. Такі системи активно застосовуються в житлових будинках, офісах, виробничих приміщеннях, навчальних закладах тощо.

Основне призначення систем безпеки полягає в:

– виявленні порушень: фіксація вторгнення, пожежі, витоку газу, зміни температури або вологості тощо;

– повідомленні про загрозу: передача інформації користувачу або службі охорони через світлову, звукову або дистанційну сигналізацію (SMS, мобільний додаток, інтернет);

– автоматизованому реагуванні: увімкнення сирени, замикання дверей, відключення електроживлення, активація камер спостереження;

– контролі доступу: обмеження доступу до приміщень або зон лише для авторизованих осіб.

Основні складові призначення систем безпеки представлено на рис. 1.1.


Рисунок 1.1. Основні складові призначення системи безпеки

Виявлення порушень у контексті систем безпеки означає фіксацію будь-яких аномальних або несанкціонованих дій, які можуть становити загрозу для охоронюваного об’єкта. Це перший та найважливіший етап у роботі охоронної системи, адже саме від своєчасного і точного виявлення залежить ефективність усієї системи.

Основними аспектами виявлення порушень є:

1) виявлення фізичної присутності або руху;

2) фіксація зміни фізичних параметрів середовища;

3) контроль доступу;

4) реєстрація спроб саботажу;

5) моніторинг активності у визначених зонах.

Основні аспекти виявлення порушень системи безпеки представлено на рис. 1.2.

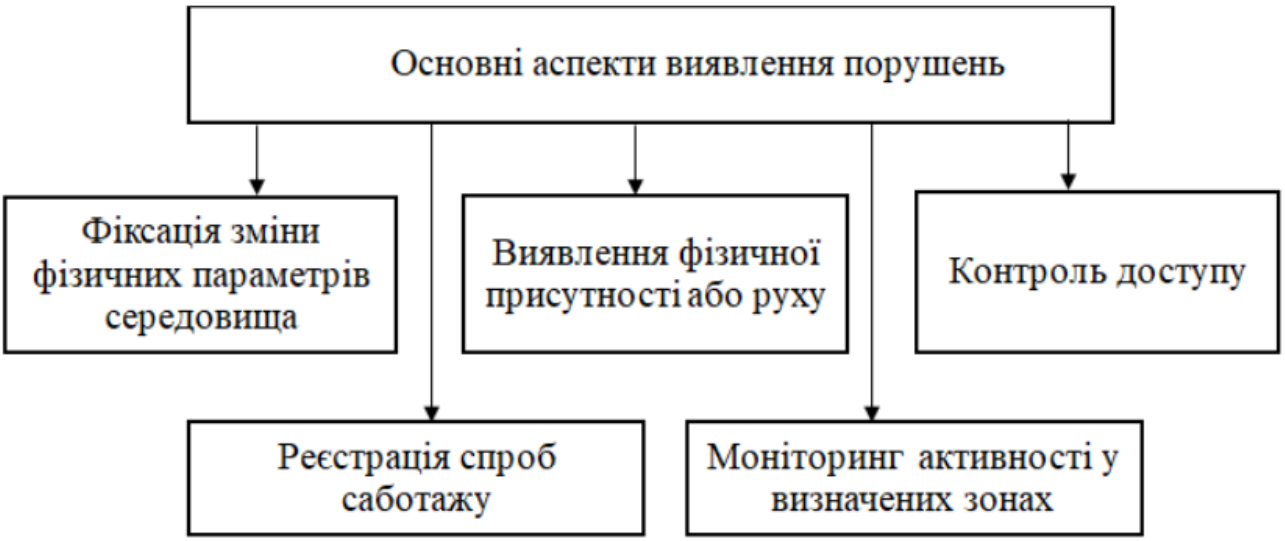



Рисунок 1.2. Основні аспекти виявлення порушень системи безпеки

Виявлення фізичної присутності або руху відбувається за допомогою: датчиків руху (PIR-сенсори); інфрачервоних або ультразвукових сенсорів; датчиків відкриття дверей або вікон (магнітні сенсори).

Фіксація зміни фізичних параметрів середовища відбувається за допомогою наступних фізичних явищ:

1) зміна температури (термодатчики);

2) наявність диму або полум’я (пожежні сенсори);

3) витік газу (газові сенсори);

4) підвищення вологості.

Контроль доступу призначено для виявлення спроби несанкціонованого входу за допомогою клавіатури, RFID, біометричних даних тощо. Реєстрація спроб саботажу це фіксація факту виявлення зняття кришки пристрою, відключення живлення, спроба знищити або обійти датчики. Моніторинг активності у визначених зонах призначено для виявлення присутності у забороненій зоні в певний час (ночі, неробочий час). Отже, виявлення порушень полягає у неперервному спостереженні за середовищем з метою своєчасної фіксації загрозливої події, яка запускає подальші дії системи – сигналізацію, запис, повідомлення, блокування доступу тощо.

До вимог, які висуваються до сучасних систем безпеки, належать:

1) надійність;

2) масштабованість;

3) інтерактивність;

4) автономність;

5) швидкість реагування;

6) інтеграція;

7) енергоефективність.

Основні вимоги до сучасних системи безпеки представлено на рис. 1.3.

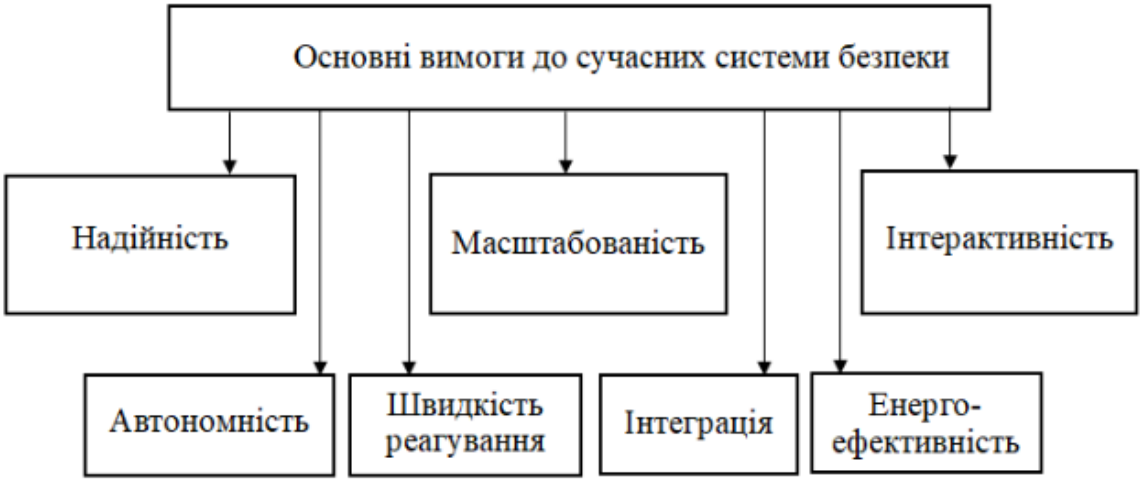



Рисунок 1.3. Вимоги до сучасних системи безпеки

Надійність забезпечується завдяки стабільної роботі в різних умовах, здатність виявляти реальні загрози та мінімізувати хибні спрацьовування.

Масштабованість – це можливість розширення системи шляхом додавання нових датчиків або функцій без істотної модифікації основного обладнання.

Інтерактивність – це наявність зручного інтерфейсу для керування, налаштування та моніторингу (мобільний додаток, веб-інтерфейс, пульт керування).

Автономність – це здатність працювати у разі відключення основного живлення, наприклад, завдяки резервному акумулятору.

Швидкість реагування – це мінімальна затримка між виявленням події та виконанням відповідної дії (сповіщення, блокування тощо).

Інтеграція – це підтримка взаємодії з іншими системами: відеоспостереження, системи «розумного дому», пожежна сигналізація.

Енергоефективність важлива для автономних або портативних систем, особливо при живленні від акумуляторів.

У контексті технологічного розвитку зростає роль програмно-апаратних рішень, які базуються на відкритих платформах, зокрема Arduino, що забезпечують низьку вартість, простоту реалізації та можливість адаптації під конкретні потреби користувача. В умовах обмеженого бюджету такі рішення є особливо актуальними для малих підприємств, приватних домоволодінь та навчальних закладів.

### 1.1.2 Організація контролю доступу в системах безпеки

Контроль доступу – це один із ключових елементів системи безпеки, що забезпечує керування правом входу до приміщення або об’єкта. Його основне завдання – дозволити доступ лише авторизованим особам та запобігти проникненню сторонніх.

Призначення контролю доступу наступне:

1) ідентифікація особи, яка полягає в перевірки, хто саме намагається отримати доступ;

2) аутентифікація побудована на підтвердженні, що ця особа має право на вхід;

3) реєстрація подій необхідно для збереження інформації про всі спроби доступу (час, успішність, ідентифікатор користувача);

4) управління виконавчими пристроями побудовано на відкриванні дверей, включення сигналізації, запуск світла тощо.

Основні способи реалізації контролю доступу в системах на базі Arduino:

1) кодовий доступ;

2) RFID-картки або брелоки;

3) біометричні сенсори;

4) Bluetooth або Wi-Fi;

5) картки NFC або QR-коди.

Кодовий доступ (кнопкова клавіатура) – це коли користувач вводить PIN-код на клавіатурі. Мікроконтролер плати Arduino перевіряє правильність введеного коду й відкриває доступ при збігу.

RFID-картки або брелоки використовують зчитувач RFID (наприклад, RC522) зчитує унікальний ідентифікатор картки. При цьому пристрій порівнює його з базою дозволених ID й надає/забороняє доступ.

Біометричні сенсори (відбитки пальців, обличчя) забезпечують доступ лише після ідентифікації біометричних даних. Приклад сенсора є R307 для зчитування відбитків пальців.

Використання Bluetooth або Wi-Fi забезпечує авторизацію за допомогою смартфона, що дає змогу відкрити двері через мобільний додаток, SMS або веб-інтерфейс.

Картки NFC або QR-коди забезпечують авторизацію шляхом зчитування коду за допомогою сумісного модуля або камери (у складніших системах).

Вимоги до системи контролю доступу наступні:

1) надійність і захищеність від підбору коду або підробки ідентифікатора;

2) журналювання подій: фіксація, хто, коли та з якою спробою заходив;

3) можливість віддаленого керування (через інтернет або SMS);

4) резервне живлення на випадок знеструмлення;

5) гнучкість у додаванні/видаленні користувачів.

У системі безпеки можна реалізувати наступний сценарій:

– при спробі доступу користувач підносить RFID-картку до зчитувача;

– Arduino перевіряє її в EEPROM або на SD-карті;

– якщо картка авторизована – активується реле для відкривання дверей, і вмикається зелений світлодіод;

– якщо ні, то спрацьовує сигналізація або надсилається повідомлення адміністратору.

Таким чином, контроль доступу є важливим функціональним блоком, який забезпечує безпечне, контрольоване та протокольоване використання охоронюваних приміщень або ресурсів. У системах на основі Arduino його реалізація є гнучкою, доступною та придатною для масштабування.

### 1.1.3 Аналіз фіксація зміни фізичних параметрів середовища в системах безпеки

Фіксація зміни фізичних параметрів середовища – це один із ключових напрямів роботи сучасних систем безпеки, який полягає в постійному контролі таких параметрів, як температура, вологість, наявність диму, газу або вогню. Виявлення аномальних значень дає змогу своєчасно попередити аварійні ситуації, техногенні загрози або інші небезпеки.

Основні приклади контролю фізичних параметрів середовища:

1) температура;

2) вологість повітря;

3) дим і полум’я;

4) газ;

5) тиск, освітлення, шум.

Фізичні параметри для контролю середовища системи безпеки представлено на рис. 1.4.

Для контролю температури використовуються цифрові або аналогові датчики температури (наприклад, DS18B20, LM35). Надлишкове підвищення температури може свідчити про перегрів обладнання або пожежу. Проте, різке зниження може бути критичним для об’єктів, чутливих до холоду.

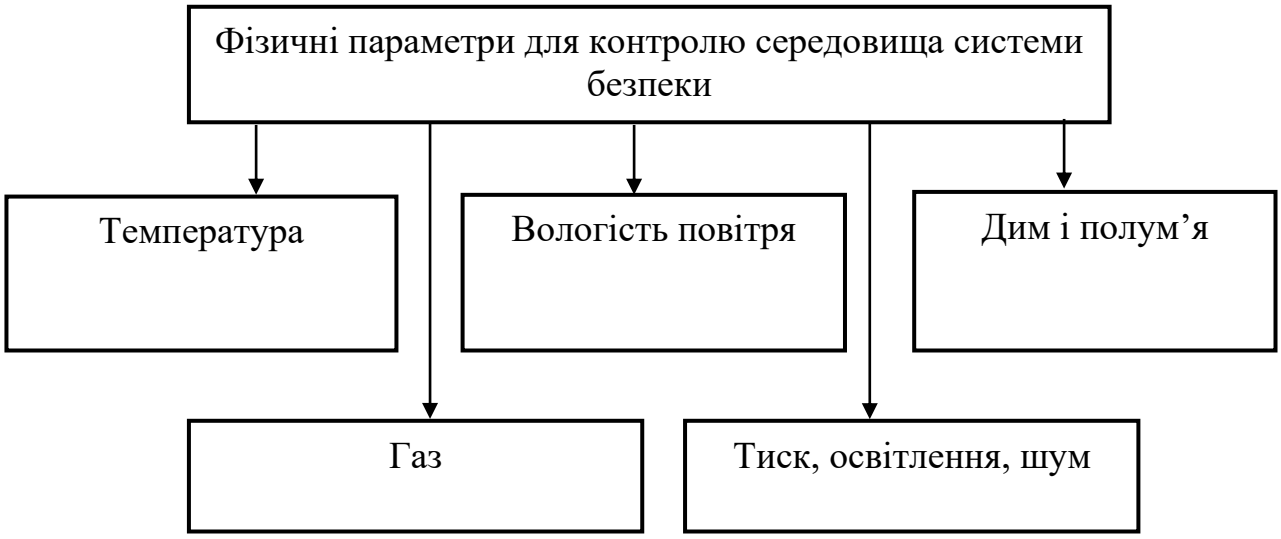



Рисунок 1.4. Фізичні параметри для контролю середовища системи безпеки

Зовнішній вигляд модуля з датчиком температури LM35 представлено на рис. 1.5.

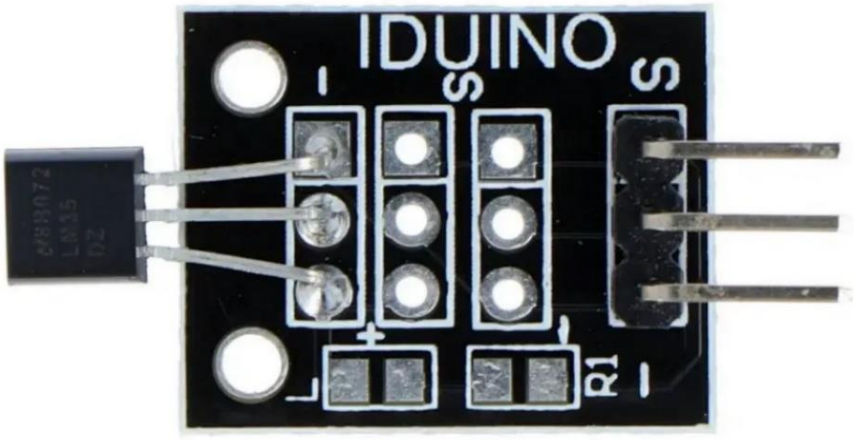



Рисунок 1.5. Зовнішній вигляд модуля з датчиком температури LM35

Вологість повітря вимірюється датчиками вологості (наприклад, DHT11, DHT22), що дозволяє відстежувати підвищену вологість, яка може спричинити плісняву, корозію або загрозу короткого замикання.

Зовнішній вигляд модуля датчика температури і вологості DHT11 надано на рис. 1.6.

Димові датчики (наприклад, MQ-2, MQ-135) реагують на мікрочастинки, що виділяються при горінні. Датчики полум'я фіксують інфрачервоне випромінювання, характерне для відкритого вогню.

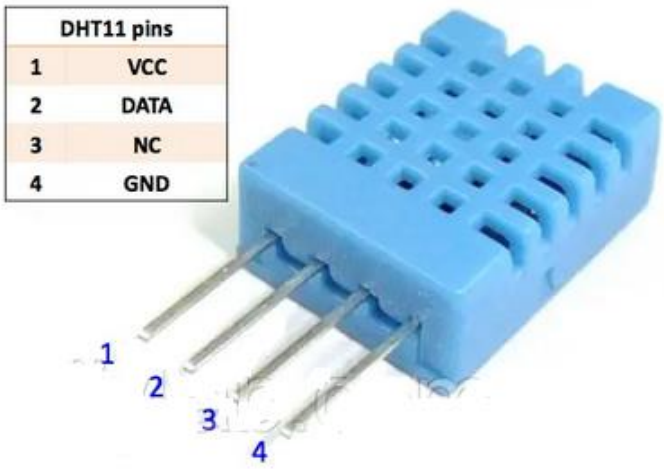



Рисунок 1.6. Зовнішній вигляд модуля датчика температури і вологості DHT11

Зовнішній вигляд модуля датчика якості повітря MQ-135 надано на рис. 1.7.

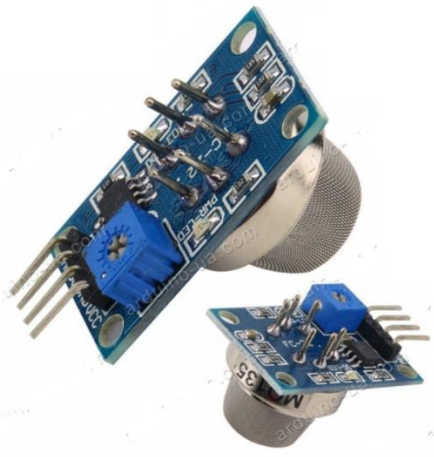


Рисунок 1.7. Зовнішній вигляд модуля датчика якості повітря MQ-135

Газ – це вибухонебезпечні або отруйні речовини. Для їх фіксації використовуються газові сенсори для виявлення:

– витоку побутового газу (метану, пропану);

– вуглекислого газу ($CO_2$);

– чадного газу (CO);

– токсичних домішок у повітрі.

У спеціалізованих системах можливий контроль додаткових параметрів, як-от:

– рівень освітлення (фоторезистори або цифрові сенсори світла);

– зміна звукового фону (мікрофони для фіксації вибухів, розбиття скла тощо);

– атмосферний тиск (для виявлення відкриття/закриття герметичних приміщень).

Зовнішній вигляд фоторезистора GL55 для контролю рівня освітлення надано на рис. 1.7.

Рисунок 1.8. Зовнішній вигляд фоторезистора GL55

Призначення механізму виявлення аварійної ситуації виконує наступні функції:

1) автоматичне виявлення аварійної ситуації без участі людини;

2) забезпечення безпеки на ранньому етапі розвитку інциденту (наприклад, ще до займання відкритого полум’я);

3) інформування користувача або відповідних служб через сигналізацію, SMS, push-сповіщення тощо.

У програмно-апаратних системах на базі Arduino для фіксації змін фізичних параметрів часто використовують комбінації кількох сенсорів, що дозволяє створити багаторівневу систему контролю середовища з підвищеною точністю й надійністю.

### 1.1.4 Саботаж в системах безпеки підприємства

Реєстрація спроб саботажу в системах безпеки полягає у виявленні та фіксації навмисних дій, спрямованих на виведення з ладу, пошкодження або обхід охоронної системи. Це важлива функція, яка дозволяє не лише виявити факт порушення, а й запобігти атаці на саму систему безпеки.

Розрізняють наступні види саботажу у системі безпеки:

1) спроба фізичного пошкодження елементів системи;

2) втручання в логіку роботи системи;

3) електронне або радіочастотне втручання.

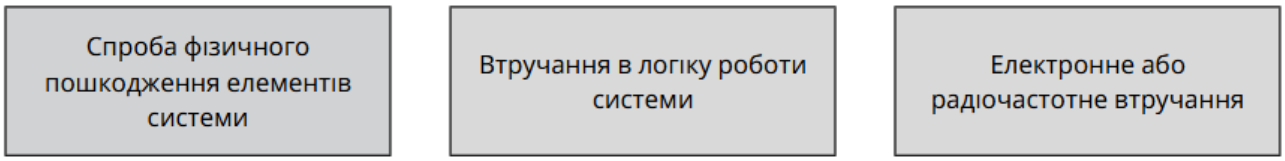



Рисунок 1.9. Види саботажу у системі безпеки

Спроба фізичного пошкодження елементів системи припускає зняття корпусу пристрою (датчика, контролера), перерізання або коротке замикання проводів, вимикання живлення або спроба знеструмити систему.

Втручання в логіку роботи системи передбачає підміну або копіювання RFID-картки, неправильне багаторазове введення пароля (Brute-force), спроба змінити прошивку або підключити зовнішні пристрої.

Електронне або радіочастотне втручання передбачає глушіння сигналів між пристроями (наприклад, між датчиком і контролером), передачу фальшивих команд через інтерфейс зв’язку.

Arduino-система може реєструвати саботаж наступним чином:

1) тампер-контакт;

2) контроль живлення;

3) лічильник помилкових спроб доступу;

4) захист програмного забезпечення;

5) сигналізація при відключенні датчиків.


Рисунок 1.10. Можливості реєстрації саботажу системою на базі Arduino

Тампер-контакт встановлюється у корпусі пристрою або датчика. При відкритті корпусу (наприклад, зняття кришки) звучить сигнал про втручання.

Контроль живлення призначено для виявлення зникнення живлення або напруги нижче критичного рівня. Перехід на резервне живлення відбувається шляхом сповіщення користувача.

Лічильник помилкових спроб доступу побудовано на контролі кількості неправильних введення коду або зчитувань RFID-карт. Після певної кількості спроб відбувається блокування доступу або тривога.

Захист програмного забезпечення відбувається шляхом реалізації перевірки цілісності прошивки. При цьому потрібна заборона на перепрошивання без апаратного дозволу (наприклад, кнопки всередині корпусу).

Сигналізація при відключенні датчиків вимагає наступне: плата мікроконтролера Arduino опитує критичні компоненти, наприклад, датчики дверей, руху тощо. Якщо датчик не відповідає, то фіксується подія як спроба саботажу.

Реакція системи на саботаж може бути такою:

1) увімкнення сирени або світлового індикатора;

2) надсилання повідомлення власнику (SMS, push, email);

3) блокування подальших дій до ручної перевірки;

4) активізація резервних або дублюючих засобів безпеки.

Таким чином, реєстрація спроб саботажу є необхідним компонентом комплексного захисту, що дозволяє не лише охороняти об'єкт, а й захищати саму систему охорони від навмисного впливу. Arduino, з відповідним набором датчиків і логікою програмування, цілком здатна реалізувати базові механізми антисаботажного контролю.

## 1.2 Проектування архітектури системи безпеки на базі Arduino

### 1.2.1 Огляд мікроконтролерних платформ для реалізації охоронних систем

Сучасні охоронні системи дедалі частіше реалізуються на основі мікроконтролерних платформ, що забезпечують високу гнучкість, масштабованість та можливість інтеграції з різноманітними сенсорами й засобами сповіщення. Правильний вибір платформи є ключовим етапом у проєктуванні ефективної та надійної системи безпеки.

Основні вимоги до мікроконтролера для охоронної системи:

- підтримка великої кількості цифрових і аналогових входів/виходів;
- наявність інтерфейсів для зв’язку (UART, I2C, SPI);
- підтримка бездротових модулів (Wi-Fi, GSM, Bluetooth);
- низьке енергоспоживання (для автономної роботи);
- достатній об’єм пам’яті для зберігання коду та даних;
- доступність компонентів і спільноти підтримки.

Розглянемо популярні мікроконтролерні платформи.

Arduino – одна з найпоширеніших платформ для навчальних і прикладних проєктів з безпеки. Переваги цієї платформи є:

- простота у використанні та програмуванні (мова Arduino/C++);
- велика спільнота та документація;

– широкий вибір моделей (Uno, Mega, Nano, Leonardo);

– підтримка великої кількості датчиків, модулів та дисплеїв.

Arduino Mega 2560 є особливо придатною для охоронних систем завдяки великій кількості пінів (54 цифрові, 16 аналогових) та збільшеному об’єму пам’яті.

ESP8266 / ESP32 – ці мікроконтролери з вбудованим Wi-Fi-модулем, які ідеально підходять для реалізації розумних систем безпеки з доступом через інтернет.

ESP8266 – бюджетне рішення з Wi-Fi, достатнє для простих завдань. ESP32 – потужніший контролер, має два ядра, більше пінів і підтримує Bluetooth.

Їх перевагами є:

– бездротове керування через Wi-Fi;

– можливість відправлення повідомлень (через MQTT, Telegram, email тощо);

– підтримка OTA (оновлення прошивки через інтернет).

Raspberry Pi – це повноцінний одноплатний комп’ютер, що дозволяє реалізувати складні охоронні системи з відеоспостереженням, базами даних, веб-інтерфейсами тощо.

Перевагою цієї платформи є:

– підтримка операційної системи Linux;

– USB, HDMI, Ethernet, Wi-Fi, Bluetooth;

– можливість запуску серверів, ведення логів, запису відео.

До недоліків можна віднести високу вартість, складність програмування, надмірна потужність для простих систем.

STM32 (STMicroelectronics) – це професійна серія 32-бітних контролерів з низьким енергоспоживанням і великою продуктивністю. Підходить для промислових систем безпеки. До її переваг можна віднести:

– висока швидкодія;

– підтримка реального часу (RTOS);

– великий вибір моделей.

До її недоліків можна віднести необхідність досвіду роботи з низькорівневим програмуванням (наприклад, у середовищі STM32CubeIDE).

Таблиця 1.1. Порівняльна характеристика платформ

| Плат-форма | Склад-ність | Комуні-кації | Па-м'ять | Під-тримка Wi-Fi | Вартість | Ідеально для |
|---|---|---|---|---|---|---|
| Arduino Uno | Низька | UART, I2C, SPI | 32 KB | Ні (через модуль) | Низька | Початкові системи |
| Arduino Mega | Низька | UART, I2C, SPI | 256 KB | Ні | Середня | Багатосенсорні системи |
| ESP8266 | Середня | UART, I2C, SPI | 1 MB | Так | Низька | IoT-системи безпеки |
| ESP32 | Середня | UART, I2C, SPI, BT | 4 MB | Так | Середня | Смарт-охорона, моб. керування |
| Raspberry Pi | Висока | USB, Ethernet, BT | > 1 GB | Так | Висока | Відеоспостереження, сервери |

Таким чином, для більшості побутових або навчальних проєктів на тему охоронних систем оптимальним вибором є Arduino Mega або ESP32, які поєднують простоту, доступність і гнучкість. У випадках, коли потрібне розширене мережеве керування або обробка складних даних, доцільно використовувати ESP32 або Raspberry Pi. Вибір платформи має ґрунтуватися на вимогах проєкту, наявних ресурсах та рівні підготовки розробника.

### 1.2.2 Можливості платформи Arduino в контексті безпеки

Платформа Arduino завоювала широке визнання серед розробників систем безпеки завдяки простоті у використанні, доступності апаратного забезпечення та великій спільноті користувачів. У контексті побудови охоронних систем Arduino надає необхідні інструменти для контролю доступу, моніторингу середовища, виявлення порушень і оперативного сповіщення про загрози.

Розглянемо основні можливості Arduino, які корисні для системи безпеки:

1) обробка сигналів від сенсорів;

2) управління виконавчими пристроями;

3) інтерфейси зв’язку та комунікації;

4) можливість реалізації контролю доступу;

5) реєстрація подій та логування;

6) гнучке програмування і оновлення логіки.

Можливості Arduino для розробки системи безпеки представлено на рис. 2.1.


Рисунок 1.11. Можливості Arduino для розробки системи безпеки

Arduino дозволяє зчитувати інформацію з великої кількості аналогових та цифрових датчиків:

- датчики руху (PIR);
- магнітні контакти для дверей/вікон;
- сенсори температури, диму, газу, вологи;
- датчики вібрації, шуму, освітлення тощо.

Завдяки простим функціям digitalRead() та analogRead() мікроконтролер може швидко реагувати на зміну фізичних параметрів середовища.

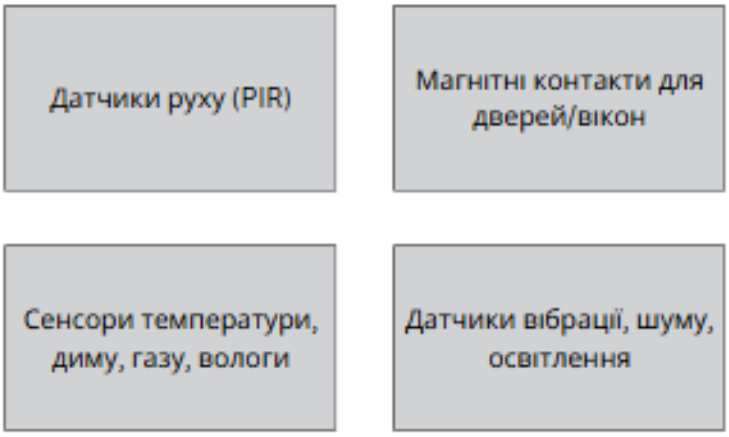



Рисунок 1.12. Можливості Arduino щодо зчитування інформації з датчиків

Управління виконавчими пристроями на основі Arduino дозволяє керувати такими елементами безпеки, як:

– електромеханічні замки (через реле або транзисторні ключі),

– звукові та світлові сигнали тривоги,

– сирени, сигнальні лампи, мотори (наприклад, для автоматичних штор чи бар'єрів).

Платформа Arduino має підтримку різноманітних інтерфейсів, що дає змогу інтегрувати систему в більші охоронні комплекси або IoT-середовище:

– UART – для з’єднання з GSM-модулями, GPS або Bluetooth;

– SPI, I2C – для зв’язку з датчиками, екранами, зовнішніми модулями пам’яті;

– Ethernet або Wi-Fi (через ESP8266/ESP32) – для надсилання сповіщень, керування через інтернет.

Можливість реалізації контролю доступу на основі платформи Arduino дозволяє організувати наступне:

– кодові замки з клавіатурою (матриці 4x4);

– RFID-ідентифікацію користувачів (зчитувач RC522);

– біометричні системи (модулі зчитування відбитків пальців);

– керування з телефону (Bluetooth, GSM, Wi-Fi).

Такі можливості дозволяють створити гнучку систему керування правами доступу.

Реєстрація подій та логування на основі Arduino дозволяє наступне:

– зберігати події на SD-карту;

– вести локальний журнал доступу;

– надсилати звіти на віддалений сервер або смартфон користувача.

Це забезпечує прозорість роботи системи та можливість аудиту після інцидентів.

Гнучке програмування і оновлення логіки на основі платформі Arduino дозволяє реалізовувати наступне:

– модульне програмування;

– застосування таймерів, інтервалів та обробки переривань;

– створення складних сценаріїв реагування (наприклад, активація кількох рівнів тривоги в залежності від ситуації).

Таблиця 1.2 Переваги платформи Arduino

| Перевага | Пояснення |
|---|---|
| Низька вартість | Arduino Uno або Mega коштує значно менше, ніж комерційні охоронні панелі |
| Модульність | Можна легко додавати нові датчики та функціонал |
| Низьке енергоспоживання | Актуально для автономних систем на акумуляторі або батарейках |
| Велика база прикладів і бібліотек | Швидка розробка завдяки відкритому коду |

Таким чином, платформа Arduino надає широкі можливості для створення ефективних, масштабованих і бюджетних охоронних систем. Завдяки простоті інтеграції з різноманітними сенсорами та модулями, вона є оптимальним вибором для реалізації індивідуальних та навчальних проєктів у сфері безпеки, а також для моделювання прототипів комерційних систем.


Рисунок 1.13. Додаткові можливості платформи Arduino

### 1.2.3 Вибір симуляторів для проєктування системи безпеки на основі Arduino

На початкових етапах розробки систем безпеки доцільним є використання середовищ симуляції, які дозволяють протестувати логіку роботи пристроїв, взаємодію компонентів і поведінку системи без потреби в реальному апаратному забезпеченні. Для Arduino існує кілька потужних онлайн- та офлайн-симуляторів, які значно спрощують процес проєктування, налагодження й демонстрації роботи системи.

Основні критерії вибору симулятора:

– підтримка мікроконтролерів Arduino (Uno, Mega, Nano тощо);

– наявність базових компонентів безпеки (датчики, реле, сирени, LCD, GSM, клавіатури);

– підтримка написання, компіляції та запуску коду;

– можливість симуляції взаємодії з оточенням;

– зручний інтерфейс, доступність, підтримка української/англійської мови;

– можливість збереження та демонстрації проєктів.

Розглянемо огляд популярних симуляторів:

Wokwi Arduino Simulator має наступні переваги:

– підтримує Arduino Uno, Mega, Nano, ESP32;

– велика бібліотека компонентів: PIR-датчики, RFID-модулі, дисплеї, Wi-Fi, клавіатури;

– симуляція реального середовища (затримки, переривання, анімація);

– підтримка компіляції реального Arduino-коду;

– зручне середовище для роботи з проектами;

– можливість ділитися симуляціями через посилання.

Недоліками Wokwi Arduino Simulator є наступне:

– не всі бібліотеки сумісні (але постійно оновлюється);

– деякі компоненти платні (преміум-функції).

Wokwi є найбільш рекомендованим для проєктування охоронних систем через простоту, реалістичність та підтримку складних конфігурацій.

Tinkercad Circuits має наступні переваги:

– інтуїтивно зрозумілий інтерфейс;

– візуальне складання схеми з компонентів;

– підтримка Arduino Uno;

– можливість симуляції коду без додаткового ПЗ;

– гарна платформа для навчання.

Недоліками Tinkercad Circuits є наступне:

– обмежена кількість компонентів;

– не підтримує Arduino Mega або ESP32;

– слабкі можливості роботи з периферійними модулями безпеки.

Tinkercad підходить для базових проєктів, навчання школярів і початківців, однак має обмеження для складних охоронних систем.

Proteus (offline) є платний, який має наступні переваги:

– професійний симулятор з підтримкою електричних схем і мікроконтролерів;

– детальна налагоджувальна інформація;

– підтримка більшості моделей Arduino;

– можливість поєднання з аналоговими схемами сигналізації.

Можна визначити наступні недоліки симулятора Proteus:

– складне налаштування;

– потребує встановлення ліцензованого ПЗ;

– важкий для новачків.

Симулятор Proteus – це промисловий стандарт, проте не підходить для швидкого онлайн-прототипування. Порівняльні характеристики симуляторів наведено в табл. 2.3.

Таблиця 1.3. Порівняльні характеристики симуляторів

| Симулятор | Підтримка Arduino Mega | Онлайн | Рівень складності | Компоненти для безпеки | Найкраще підходить для |
|---|---|---|---|---|---|
| Wokwi | Так | так | Середній | Так | Проєктування реальних систем |
| Tinkercad | лише Uno | так | Легкий | Обмежено | Навчання, демонстрації |
| Proteus | Так | ні | Високий | так | Промислові рішення |

Таким чином, для великих проєктів охоронної системи безпеки доцільним є використання Arduino Mega. Для такого мікроконтролера оптимальним вибором є Wokwi – онлайн-симулятор, який забезпечує симуляцію роботи компонентів безпеки, дозволяє налагоджувати та тестувати Arduino-код без фізичного пристрою. Його можливості особливо корисні на етапі проектування та верифікації логіки роботи майбутньої системи.

Для невеликих проєктів системи безпеки, там де кількість пінів управління обмежена, доцільним є обрання плати мікроконтролера Arduino Uno або Nano. Розроблення системи безпеки на основі плати мікроконтролера Arduino Uno згідно табл. 2.3 можна виконати за допомогою симулятора Tinkercad, який має кращі демонстраційні можливості у порівнянні з симулятором Wokwi.


Рисунок 1.14. Основні критерії вибору симулятора

### 1.2.4 Аналіз існуючих рішень і підходів до створення охоронних систем

Сучасні охоронні системи представлені широким спектром рішень — від комерційних централізованих охоронно-пожежних комплексів до модульних або DIY-систем, що будуються на основі мікроконтролерів. У цьому підрозділі розглянемо ключові типи реалізації охоронних систем, їхні особливості, переваги та недоліки, а також сучасні тенденції у цій сфері.

Комерційні охоронні системи (готові рішення) – це такі системи розробляються спеціалізованими компаніями (наприклад, Ajax, Satel, Hikvision, Dahua) і мають комплексну архітектуру: центральний блок, датчики руху/диму/розбиття, клавіатура, модулі GSM/Wi-Fi, сирени.

До їх переваг можна віднести наступне:

– висока надійність та сертифікація;

– професійна технічна підтримка;

– готовність до підключення до охоронних компаній;

– автономність, акумулятори, шифрування сигналів.

Недоліками можна вважати:

– висока вартість;

– закритий код і складність модифікації;

– залежність від конкретного виробника та сервісного обслуговування.

Системи на основі мікроконтролерів (DIY-підхід) – ці системи створюються користувачами або розробниками з використанням відкритих платформ, зокрема Arduino, ESP8266/ESP32, Raspberry Pi.

Перевагами їх є наступне:

– гнучкість і адаптованість під потреби користувача;

– низька вартість реалізації;

– відкритий код — можливість доопрацювання;

– швидке створення прототипу або навчального проєкту.

До недоліків можна віднести:

– обмежена надійність без відповідного рівня тестування;

– потреба в програмуванні й налаштуванні;

– відсутність сертифікації та офіційної техпідтримки.

Розглянемо основні типові приклади таких систем:

– Arduino-системи з датчиками руху, магнітними контактами та GSM-модулями;

– ESP32-системи з Wi-Fi доступом і Telegram-сповіщенням;

– Raspberry Pi-сервери з IP-камерами та веб-інтерфейсом.

Інтегровані системи безпеки з IoT-компонентами – це більш просунуті варіанти, які поєднують класичні функції охорони з інтернет-технологіями та мобільним керуванням:

– доступ через смартфон (веб або мобільний застосунок);

– отримання push-сповіщень про події;

– хмарне зберігання логів чи відео;

– інтеграція з голосовими асистентами (Google Home, Alexa).

Ці системи створюються як на основі мікроконтролерів, так і на платформі розумного будинку (Home Assistant, OpenHAB, Domoticz).

Сучасні підходи до побудови охоронних систем представлені в табл. 2.4.

Таблиця 1.4. Сучасні підходи до побудови охоронних систем

| Підхід | Характеристика |
|---|---|
| Модульність | Система легко масштабується додаванням нових сенсорів або функцій. |
| Безпровідність | Використання Wi-Fi, ZigBee, LoRa, GSM дозволяє зменшити кількість проводів. |
| Хмарні сервіси | Дистанційний моніторинг та керування з будь-якої точки світу. |
| Автономність | Наявність резервного живлення, збереження роботи при відключенні інтернету. |
| Кіберзахист | Шифрування даних, автентифікація користувачів, контроль доступу. |

Таким чином, існуючі охоронні системи охоплюють широкий спектр рішень – від промислових комплексів до індивідуальних, відкритих і експериментальних платформ. Попри те, що комерційні системи пропонують високу надійність, Arduino-платформи надають великі можливості для створення адаптованих, бюджетних і ефективних охоронних рішень, особливо у навчальних і побутових проєктах. Завдяки відкритій архітектурі та підтримці великої кількості модулів, Arduino залишається оптимальним вибором для розробників, що прагнуть створити індивідуальні системи безпеки з гнучкою логікою реагування.

## 1.3 Реалізація, тестування та аналіз ефективності системи

### 1.3.1 Постановка задачі проектування системи

Метою цього проєкту є розробка програмно-апаратної охоронної системи на базі платформи Arduino Uno із використанням компонентів, доступних у симуляторі Tinkercad Circuits. Система повинна забезпечувати моніторинг стану середовища, контроль доступу, виявлення порушень, візуальне та звукове інформування про загрози, а також гнучку логіку реагування.

Метою даного етапу є формування чітких вимог до розробки багаторівневої охоронної системи на базі платформи Arduino з урахуванням типових загроз для

приватних середовищ (квартира, офіс, складське приміщення тощо). Передбачається створення інтегрованого рішення, здатного виявляти проникнення, фіксувати наявність небезпечних факторів середовища та інформувати про них користувача шляхом світлової та звукової індикації.

Завдання проектування полягає у розробці функціональної, надійної, недороговартісної та легко модифікованої системи, яка повинна виконувати такі функції:

1) Моніторинг якості повітря з використанням газового сенсора для виявлення надмірної концентрації газу або шкідливих речовин;
2) Виявлення руху в контрольованій зоні за допомогою інфрачервоного (PIR) датчика;
3) Контроль несанкціонованого відкривання дверей або вікон через магнітоконтактний датчик (геркон);
4) Реагування на загрози шляхом активації звукової сигналізації (пасивний бузер) і світлової індикації (світлодіод);
5) Протоколювання подій через серійний монітор з метою налагодження та демонстрації роботи системи в режимі реального часу;
6) Можливість подальшої модернізації, наприклад, додавання GSM-модуля, Wi-Fi-комунікації або віддаленого керування.

Система повинна бути змодельована та протестована у середовищі Tinkercad, що дозволяє створити віртуальний прототип, протестувати логіку роботи, проаналізувати реакцію на типові події та перевірити відповідність розробки поставленим вимогам.

Виявлення фізичного проникнення відбувається за допомогою:

– магнітоконтактних датчиків, що реагують на відкривання дверей або вікон;

– PIR-датчиків руху (опціонально, за потреби моделювання сценаріїв з присутністю людини).

Контроль параметрів середовища, а саме:

– використання датчика якості повітря (MQ-135) для виявлення перевищення допустимих рівнів газів або забруднень.

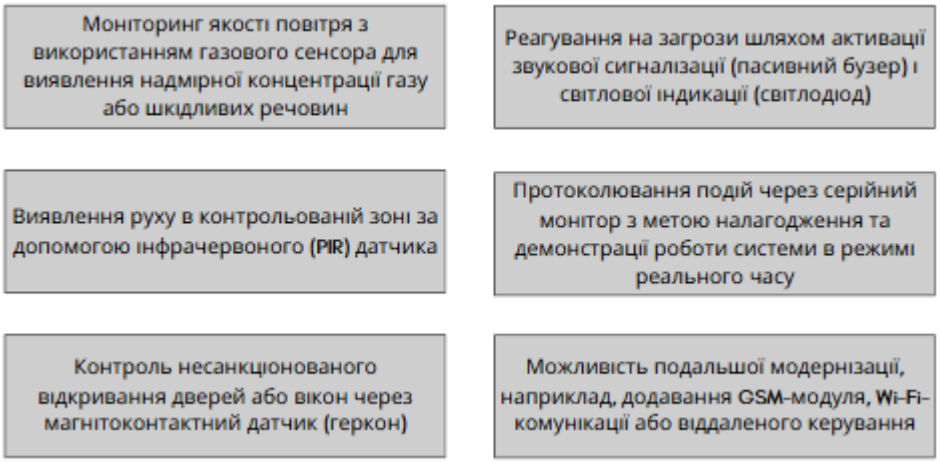



Рисунок 1.15. Формування технічного завдання. Опис базових функцій системи

Індикація стану системи:

– світлова сигналізація – червоний (тривога), зелений (норма), жовтий (режим очікування);

– звукова сигналізація – активація базера або сирени при тривозі.

Програмне керування логікою роботи системи:

– умовна активація тривоги залежно від поєднання показників датчиків;

– затримки, таймери, режими збройно/роззброєно (опціонально – кнопка чи перемикач).

Інтерактивність:

– використання кнопок для керування режимами;

– виведення повідомлень на LCD-дисплей (наприклад, “Увімкнено охорону”, “Двері відчинено”, “Газ виявлено”).

Розглянемо умови реалізації в симуляторі Tinkercad Circuits, який дозволяє:

– Проєктувати електронні схеми без потреби у фізичних компонентах, що значно спрощує процес тестування рішень на базі Arduino;

– Емулювати роботу датчиків та пристроїв (газові сенсори, PIR-датчики, світлодіоди, бузери тощо) з можливістю спостереження за значеннями у режимі реального часу;

– Завантажувати та налагоджувати код Arduino у вбудованому середовищі, що підтримує мову програмування Arduino C/C++;

– Візуально аналізувати поведінку системи, завдяки інтерактивному виведенню значень через віртуальний серійний монітор та індикатори;

– Експериментувати з різними сценаріями реагування охоронної системи на зміни в середовищі, зміну станів датчиків, появу небезпеки.

Таким чином, Tinkercad Circuits є ефективним інструментом для моделювання, відлагодження та демонстрації роботи системи безпеки, не вдаючись до складної апаратної реалізації на початкових етапах проєкту.

Таблиця 1.5. Орієнтовний склад компонентів у симуляторі Tinkercad

| № з/п | Назва компонента | Кількість | Призначення |
|---|---|---|---|
| 1 | Arduino Uno R3 | 1 | Центральний контролер для керування всіма елементами системи |
| 2 | Газовий сенсор (Gas Sensor) | 1 | Виявлення наявності шкідливих або вибухонебезпечних газів |
| 3 | Датчик руху (PIR Sensor) | 1 | Виявлення руху в контрольованій зоні |
| 4 | Магнітоконтактний датчик (геркон) | 1 | Фіксація відкривання дверей або вікон |
| 5 | Світлодіод (LED) | 1–2 | Візуальна індикація тривожної події |
| 6 | Пасивний бузер (Buzzer) | 1 | Звукова сигналізація при спрацюванні системи |
| 7 | Резистори (220–330 Ом) | 2–3 | Обмеження струму для світлодіодів |
| 8 | Макетна плата (Breadboard) | 1 | Збирання схеми без пайки |
| 9 | З’єднувальні дроти (Jumper Wires) | 15–20 | Підключення елементів між собою та до Arduino |
| 10 | Віртуальний серійний монітор | - | Виведення діагностичних повідомлень і показників датчиків |

### 1.3.2 Розробка схеми підключення компонентів

На основі сформульованих вимог до багаторівневої системи безпеки та обраного переліку електронних компонентів у середовищі Tinkercad Circuits була розроблена схема підключення, що дозволяє забезпечити виявлення кількох типів загроз та реакцію системи на них.

До складу системи входять такі основні елементи:

– Газовий сенсор (Gas Sensor – підключений до аналогового входу A0);

– PIR-датчик руху – цифровий вхід (наприклад, D7);

– Магнітоконтактний датчик (геркон) – цифровий вхід (наприклад, D6);

– Світлодіод (LED) – для індикації загрози (наприклад, D12);

– Бузер (Buzzer) – для звукової сигналізації (наприклад, D11);

– Живлення – використовується стандартне джерело +5В з Arduino та загальна «земля» (GND).

Підключення сенсорів здійснюється відповідно до рекомендацій виробників та схемотехнічних стандартів Arduino. Зокрема:

– Газовий сенсор MQ-2 чи аналогічний виводить аналоговий сигнал, що зчитується через analogRead();

– PIR-датчик працює за цифровим принципом: при виявленні руху подає логічну "1";

– Магнітоконтактний датчик (геркон) при замкненому положенні може формувати логічну "0" або "1" залежно від типу підключення (pull-up або pull-down резистора);

– Бузер та світлодіод керуються логічними сигналами на відповідні пін-коди.

Розглянемо особливості використання та фізичні принципи дії датчика PIR.

PIR-датчик (Passive InfraRed sensor) – це сенсор, який виявляє рух за рахунок зміни інфрачервоного (теплового) випромінювання у навколишньому середовищі. Основним принципом його роботи є фіксація різниці температур,

що виникає при переміщенні теплих об’єктів (наприклад, людського тіла) в межах поля зору сенсора.

Фізичні особливості PIR-датчик наступні:

1. Інфрачервоні промені:
   - PIR-датчик не випромінює сигнал, а лише приймає пасивне інфрачервоне випромінювання від об’єктів.
   - у центральній частині міститься піроелектричний елемент, який чутливий до ІЧ-випромінювання в діапазоні ~8–14 мкм.
2. Френелевська лінза:
   - більшість PIR-датчиків обладнані спеціальною сегментованою лінзою, яка концентрує інфрачервоне випромінювання з різних напрямків на чутливу зону.
   - це дозволяє розширити зону огляду та підвищити чутливість до руху.
3. Три основні виводи:
   - VCC – підключення живлення (зазвичай 5 В або 3.3 В).
   - GND – заземлення.
   - OUT – цифровий вихід. При виявленні руху видає високий рівень сигналу (HIGH).
4. Регульовані параметри (на деяких модулях):
   - затримка спрацьовування (Delay Time) — час, протягом якого вихід залишається активним після виявлення руху.
   - чутливість (Sensitivity) — відстань, на якій датчик може виявляти рух.

Особливості використання PIR-датчик наступні:

1. Обмеження на навколишнє середовище:
   - PIR-датчик чутливий до температурних змін, тому не рекомендується розміщувати його біля нагрівальних приладів, вікон або в місцях з прямим сонячним світлом.

– не виявляє об’єкти без теплового випромінювання (наприклад, неживі предмети).

2. Область покриття:

– стандартний кут огляду становить близько 120° при дальності до 6–7 метрів.

– для надійного спрацювання об’єкт повинен рухатися поперек поля зору, а не прямо до датчика.

3. Стабілізація після увімкнення:

– датчик потребує кілька секунд (5–60 с) для прогріву після подачі живлення, протягом яких може випадково спрацьовувати.

4. Низьке енергоспоживання:

– PIR-датчики є енергоефективними, що робить їх придатними для автономних охоронних систем на базі батарейного живлення.

Принцип роботи PIR-датчика представлена на рис. 3.1.

Таблиця 1.6. Технічні характеристики PIR-датчика

| Параметр | Значення |
|---|---|
| Робоча напруга | 4.5 – 20 В |
| Робочий струм | 50 – 60 мкА |
| Тип виходу | Цифровий (HIGH/LOW) |
| Вихідна напруга (HIGH) | Близько 3.3 В – 5 В |
| Відстань виявлення | 3 – 7 метрів (регулюється) |
| Кут огляду | ≈ 120° (по горизонталі) |
| Затримка спрацювання | 0.3 – 600 сек (регулюється) |
| Час встановлення після запуску | ≈ 30 – 60 секунд |
| Робоча температура | -15°C до +70°C |

Варто додати програмну затримку для уникнення помилкових спрацьовувань одразу після старту мікроконтролера, особливо в охоронних системах.

Газовий датчик серії MQ є напівпровідниковим сенсором, який виявляє присутність певних газів у повітрі (наприклад, метан, пропан, чадний газ, дим, аміак, вуглекислий газ тощо). Основний сенсорний елемент — чутлива нагрівна спіраль з оксидом олова ($SnO_2$).


Рисунок 1.16. Принцип роботи PIR-датчика

Принцип роботу датчику газу наступний:

1) нагрівання сенсора: всередині датчика розташована маленька спіраль нагрівання (Heater Coil), яка нагріває оксид олова до робочої температури (~200-400°C);

2) хімічна реакція з газами: на поверхні оксиду олова в присутності повітря утворюється шар кисню, що зв’язує вільні електрони. Коли у повітрі

з’являється газ, який датчик може виявляти, він взаємодіє з цим шаром кисню, змінюючи провідність матеріалу;

3) зміна опору: у результаті взаємодії з газами електричний опір сенсорного елемента змінюється. Ця зміна вимірюється у вигляді аналогової напруги;

4) зчитування Arduino: мікроконтролер зчитує зміну напруги через аналоговий вхід (analogRead()) і визначає рівень забруднення повітря чи наявність газу.

В табл. 1.7 наведено характеристики датчика газу.

Таблиця 1.7. Характеристики датчика газу

| Параметр | Значення |
|---|---|
| Робоча напруга | 5 В |
| Нагрівальний елемент | Спіраль з високим опором |
| Вихідний сигнал | Аналоговий |
| Час прогріву (перед вимірюванням) | 1–2 хв. (оптимально до 24 годин) |
| Газ, що виявляється | $CO_2$, $NH_3$, NOx, спирти, бензол, дим |
| Чутливість | Висока, але потребує калібрування |

Поради при використанні наступні:

1) після включення сенсор потребує часу на прогрів (до 60 секунд для базового використання, до кількох годин для точного калібрування);

2) показник на аналоговому виході може залежати від вологості та температури;

3) для кращої точності можна порівнювати значення з порогом (наприклад: if (gasLevel > 600)).

Принцип роботи магнітоконтактного датчика (геркона)

Геркон (від нім. "Hermetisch verschlossener Kontakt") — це електромеханічний сенсор, який замикає або розмикає електричний ланцюг у присутності магнітного поля. Його широко застосовують у системах охоронної сигналізації, особливо для контролю відкриття/закриття дверей і вікон.

Конструкція геркона складається з наступних елементів:

1. Герметична скляна трубка, всередині якої знаходяться:

– два тонкі металеві контакти, виготовлені з феромагнітного матеріалу;

– трубка наповнена інертним газом або вакуумом для запобігання окисленню;

2. У комплекті з герконом зазвичай використовується постійний магніт, що розміщується на рухомій частині (наприклад, на дверях).

Принцип роботи геркону полягає в наступному:

– у нормальному стані (без магніту): контакти розімкнуті – струм не проходить;

– коли магніт наближається: виникає магнітне поле, яке притягує контакти один до одного – вони замикаються, і струм може протікати;

– коли магніт віддаляється: магнітне поле зникає, і контакти знову розмикаються.

В табл. 1.8 представлені режими роботи геркона.

Таблиця 1.8. Режими роботи геркона

| Тип геркона | Робоча логіка |
|---|---|
| Нормально розімкнутий | Замикається при наближенні магніту |
| Нормально замкнутий | Розмикається при наближенні магніту (рідше) |

Приклад використання з Arduino:

– один контакт геркона підключають до входу цифрового піну (наприклад, pin 2), інший — до GND.

– у коді використовується digitalRead() для зчитування стану:

```
const int reedPin = 2;
void setup() {
  pinMode(reedPin, INPUT_PULLUP);  // Активація внутрішнього підтягування
  Serial.begin(9600);
}
```

```
void loop() {
  int state = digitalRead(reedPin);
  if (state == LOW) {
    Serial.println("Двері зачинені");
  } else {
    Serial.println("Двері відкриті!");
  }
  delay(500);
}
```

Переваги геркона полягає в наступному:

- низьке енергоспоживання;
- надійність і простота;
- висока чутливість до магнітного поля;
- ізоляція контактів від навколишнього середовища;

Геркон застосовується в наступних сферах:

- охоронні системи (вікна, двері, сейфи).
- контроль положення.
- побутова електроніка та техніка безпеки.

Принцип роботи базера (buzzer) полягає в наступному.

Базер – це електроакустичний пристрій, призначений для створення звукових сигналів. У проектах на основі Arduino зазвичай використовуються п’єзоелектричні базери (piezo buzzers) або електромагнітні.

В табл. 1.9 представлені типи базерів.

Таблиця 1.9. Типи базерів

| Тип базера | Особливості |
|---|---|
| Активний базер | Має вбудований генератор. Видає звук при подачі живлення (HIGH) на пін. |
| Пасивний базер | Потребує генерування частоти мікроконтролером (tone()). |

У симуляторі Tinkercad Circuits зазвичай доступний пасивний базер.

Принцип дії п’єзо-базера:

1) усередині базера знаходиться п’єзоелемент;

2) при подачі змінного струму або імпульсів (генерація частоти), п’єзоелемент починає коливатися.

3) ці коливання створюють звукову хвилю – ми чуємо писк або тон.

Схема підключення (приклад):

– Один пін базера підключається до цифрового піну Arduino (наприклад, 11);

– Інший — до GND.

У разі пасивного базера використовують функцію:

- tone(11, 1000);  // Генерація тону 1000 Гц;
- delay(300);
- noTone(11);  // Зупинка звуку

Приклад використання:

```
const int buzzerPin = 11;
void setup() {
  pinMode(buzzerPin, OUTPUT);
}

void loop() {
  tone(buzzerPin, 2000);  // Генеруємо 2000 Гц
  delay(500);             // 0.5 секунди
  noTone(buzzerPin);
  delay(500);
}
```

Застосування базера в наступних сферах:

- охоронні системи (сигнал тривоги);
- звукові повідомлення про помилку;
- звукове підтвердження натискання кнопки;
- таймери й годинники.

На рис. 1.17 представлено умовну схему підключення компонентів системи в середовищі Tinkercad. Схема враховує правильність електроживлення та дозволяє проводити тестування в інтерактивному режимі.

Примітка: У віртуальному середовищі можлива симуляція значень, наприклад, зміни рівня газу або появи руху, шляхом ручного керування інтерфейсом симулятора.

Розглянемо використані інструменти в симуляторі Tinkercad Circuits.

Для реалізації системи безпеки було використано програмне середовище Tinkercad Circuits, яке дозволяє моделювати роботу електронних схем та програмного забезпечення для мікроконтролерів. У процесі розробки системи були застосовані такі основні компоненти:

1. Arduino Uno
   - центральний контролер системи;
   - має 14 цифрових входів/виходів (з них 6 можуть працювати як PWM) та 6 аналогових входів;
   - програмується через Arduino IDE за допомогою мови, подібної до C++.
2. Газовий сенсор (Gas Sensor)
   - датчик у симуляторі Tinkercad має 6 виводів, але функціонально використовується як аналоговий пристрій;
   - підключається одним з виходів до аналогового входу Arduino (наприклад, A0);
   - реєструє рівень забруднення повітря або наявність газу;
   - у Tinkercad можна вручну задати рівень газу під час симуляції (через повзунок).
3. PIR-датчик руху (Passive Infrared Sensor):
   - використовується для виявлення руху людини в зоні контролю;
   - має три виводи: VCC (живлення), GND (заземлення) і OUT (цифровий вихід);
   - при виявленні руху OUT переходить у HIGH;

4. Магнітоконтактний датчик (геркон):
   - складається з двох частин: одна частина кріпиться до рухомого елементу (двері, вікно), інша – до рами;
   - у нормальному стані (двері зачинені) ланцюг замкнений. При відкритті – розмикається;
   - підключається до цифрового входу Arduino з підтягуванням до живлення (INPUT_PULLUP).
5. Світлодіоди (LED):
   - використовуються для індикації різних станів системи (газ, рух, проникнення);
   - підключаються через токообмежувальний резистор (220–330 Ом) до цифрових виходів Arduino.
6. Пасивний бузер (Passive Buzzer):
   - призначений для звукового оповіщення;
   - працює у парі з функцією tone() для генерації звукових сигналів різної частоти;
   - підключається до цифрового виходу Arduino (наприклад, D11).
7. Серійний монітор (Serial Monitor)
   - інструмент у середовищі Arduino IDE для виведення повідомлень та налагодження роботи системи;
   - дозволяє виводити показники датчиків та діагностичні повідомлення в режимі реального часу.

Цей набір компонентів дозволяє моделювати роботу базової багаторівневої охоронної системи в умовах симуляції, максимально наближеній до реального середовища. Якщо потрібно, можу допомогти оформити це як табличку або включити інші датчики (дим, ультразвук, світло).

На рис. 3.2 надана схема підключення компонентів системи безпеки та завантажений програмний код в середовище Tinkercad.

Схема електрична принципіальна системи безпеки надана на рис. 3.3.

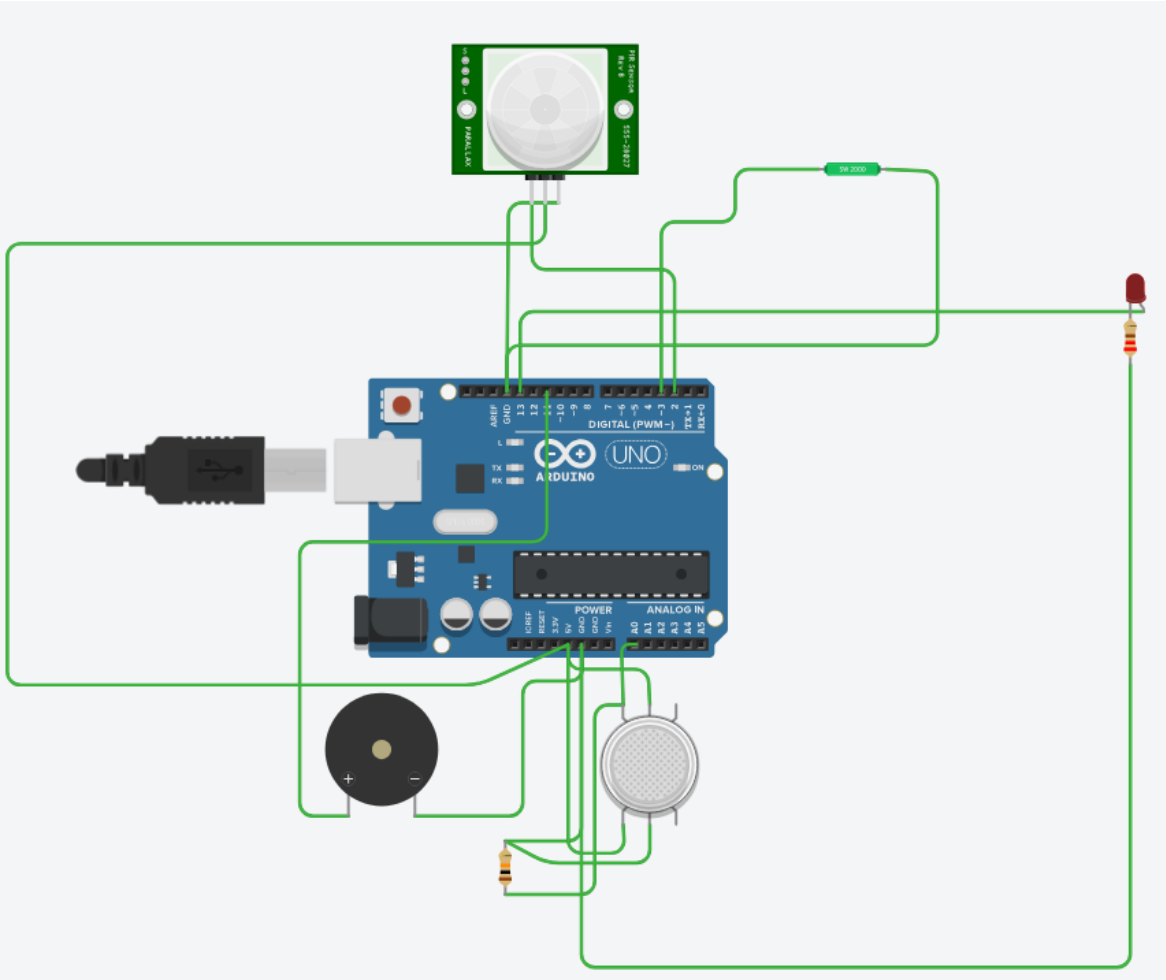



Рисунок 1.17. Умовна схема підключення компонентів системи безпеки в середовищі Tinkercad

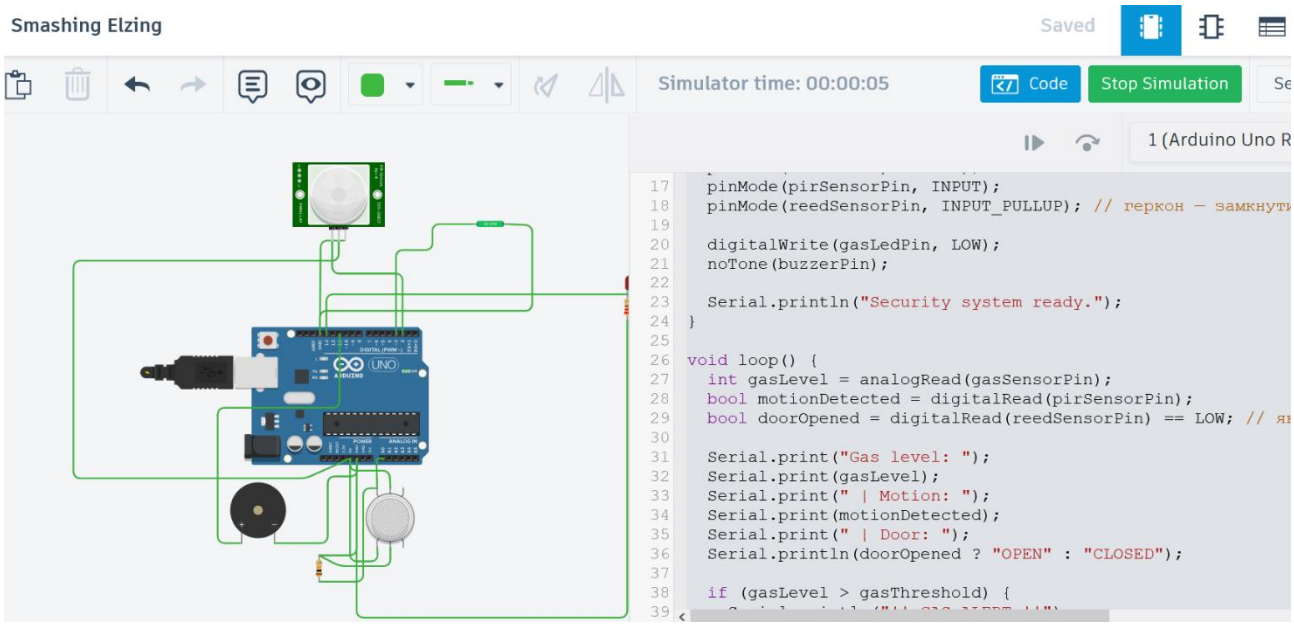



Рисунок 1.18. Схема підключення компонентів системи безпеки та програмний код в середовищі Tinkercad

Схема електрична принципіальна системи безпеки представлена на рис. 1.19.

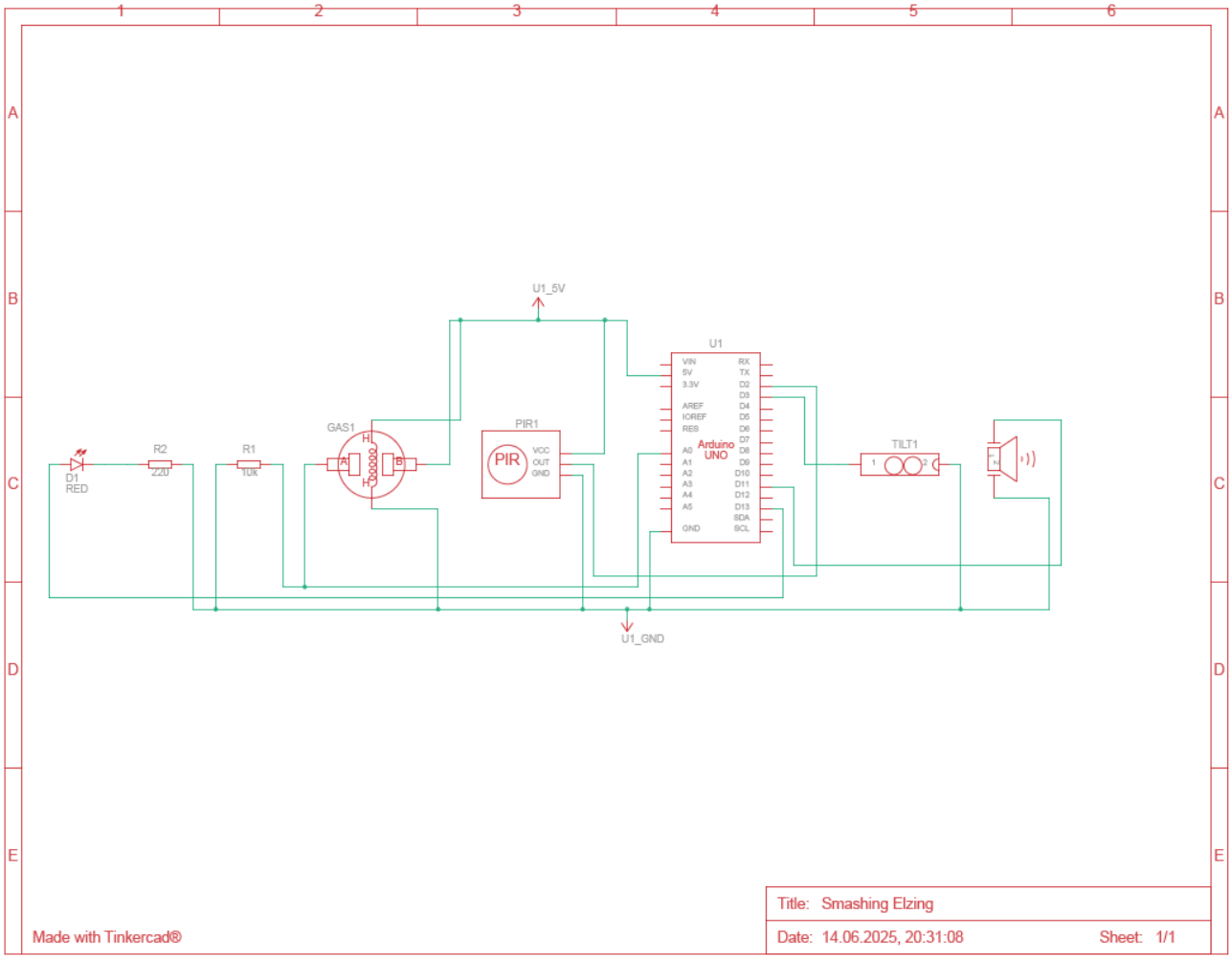



Рисунок 1.19. Схема електрична принципіальна системи безпеки

Логіка роботи схеми полягає в наступному:

1. Після подачі живлення система ініціалізується та переходить у режим очікування. Основним керуючим елементом є мікроконтролер Arduino Uno, який опитує стан усіх підключених сенсорів і керує виконавчими елементами (світлодіодом та бузером):

2. Газовий сенсор (Gas Sensor): постійно зчитує аналоговий сигнал, що відображає рівень газу в повітрі. У разі перевищення заданого порогу (наприклад, 600 одиниць) система активує тривогу: вмикає світлодіодну та звукову індикацію;

3. PIR-датчик руху: контролює наявність руху в зоні дії. При фіксації руху передає сигнал на цифровий вхід Arduino, що також спричиняє активацію тривоги;

4. Магнітоконтактний датчик: використовується для контролю відкриття/закриття дверей або вікон. При розмиканні контактів (наприклад, при відкритті дверей) на вхід Arduino надходить сигнал, що також запускає тривожну реакцію системи;

5. Сигнальні пристрої:

– світлодіод (LED): засвічується у випадку виявлення загрози (газ, рух або саботаж);

– бузер: видає звуковий сигнал, який сповіщає про небезпеку або несанкціоноване проникнення.

Таким чином, система працює за принципом моніторингу середовища в реальному часі та оперативного реагування на будь-які потенційні загрози. Реалізація в середовищі Tinkercad дозволяє візуалізувати, протестувати та змінити конфігурацію системи без потреби у фізичних компонентах.

Компоненти системи та принципи їх підключення представлені в табл. 1.10.

Таблиця 1.10. Компоненти системи та принципи їх підключення

| № з/п | Назва компонента | Тип підключення | Пін на Arduino |
|---|---|---|---|
| 1 | Газовий сенсор (Gas Sensor) | Аналоговий вхід | A0 |
| 2 | PIR-датчик руху | Цифровий вхід | D7 |
| 3 | Магнітоконтактний датчик | Цифровий вхід | D6 |
| 4 | Світлодіод (LED) | Цифровий вихід | D12 |
| 5 | П'єзобузер (Buzzer) | Цифровий вихід (PWM) | D11 |
| 6 | Плата Arduino Uno | Живлення та керування | — |
| 7 | Резистори 220–10 кОм | Підтягуючі/обмежувальні | — |

### 1.3.3 Розробка програмного забезпечення системи

Програмне забезпечення системи безпеки, реалізованої на базі Arduino, відповідає за зчитування сигналів з датчиків, аналіз отриманої інформації та керування виконавчими пристроями (світлодіодом і бузером). Код написано мовою програмування C++ з використанням середовища Arduino IDE.

Основні функції програмного забезпечення:

1) Ініціалізація компонентів – у функції setup() налаштовуються режими роботи виводів Arduino, а також ініціюється серійний порт для виведення діагностичних повідомлень;

2) Моніторинг газового сенсора – щосекунди зчитується аналогове значення з піну A0. Якщо рівень газу перевищує порогове значення, активується тривожна сигналізація;

3) Обробка сигналу від PIR-датчика руху – цифровий пін опитується в режимі digitalRead(). При виявленні руху вмикається сигналізація;

4) Контроль магнітоконтактного датчика – якщо контакти розімкнуті (двері або вікно відкрито), система також переходить у тривожний режим;

5) Управління світловою та звуковою індикацією – у разі виявлення загрози вмикається світлодіод та звучить сигнал з пасивного бузера, використовуючи функції digitalWrite() та tone().

Нижче наведено фрагмент програмного коду, реалізованого для системи:

```
// === Pins ===
const int gasSensorPin = A0;
const int gasLedPin = 13;         // Червоний LED — газ
const int buzzerPin = 11;         // Пасивний бузер

const int pirSensorPin = 2;       // PIR датчик руху
const int reedSensorPin = 3;      // Магнітоконтактний датчик (геркон)

// === Пороги ===
const int gasThreshold = 600;
```

```
void setup() {
  Serial.begin(9600);

  pinMode(gasLedPin, OUTPUT);
  pinMode(buzzerPin, OUTPUT);
  pinMode(pirSensorPin, INPUT);
  pinMode(reedSensorPin, INPUT_PULLUP); // геркон — замкнутий у нормі

  digitalWrite(gasLedPin, LOW);
  noTone(buzzerPin);

  Serial.println("Security system ready.");
}

void loop() {
  int gasLevel = analogRead(gasSensorPin);
  bool motionDetected = digitalRead(pirSensorPin);
  bool doorOpened = digitalRead(reedSensorPin) == LOW; // якщо геркон розімкнутий → відчинено

  Serial.print("Gas level: ");
  Serial.print(gasLevel);
  Serial.print(" | Motion: ");
  Serial.print(motionDetected);
  Serial.print(" | Door: ");
  Serial.println(doorOpened ? "OPEN" : "CLOSED");

  if (gasLevel > gasThreshold) {
    Serial.println("!! GAS ALERT !!");
```

```
    digitalWrite(gasLedPin, HIGH);
    triggerAlarm(1000);
  }
  else if (motionDetected || doorOpened) {
    Serial.println("!! INTRUSION ALERT !!");
    digitalWrite(gasLedPin, HIGH);
    triggerAlarm(2000);
  }
  else {
    digitalWrite(gasLedPin, LOW);
    noTone(buzzerPin);
  }

  delay(500);
}

void triggerAlarm(int frequency) {
  for (int i = 0; i < 3; i++) {
    tone(buzzerPin, frequency);
    delay(300);
    noTone(buzzerPin);
    delay(200);
  }
}
```

Такий підхід дозволяє системі надійно працювати у режимі реального часу, реагувати на зміни в середовищі та своєчасно сигналізувати про потенційну загрозу. Простота логіки та відкритий код дають змогу легко масштабувати або змінювати функціональність системи відповідно до потреб користувача.

Пояснення до програмного коду системи безпеки.

Код реалізує логіку багаторівневої охоронної системи, яка включає в себе газовий датчик, інфрачервоний датчик руху (PIR), магнітоконтактний датчик, звукову сигналізацію (buzzer) та світлову індикацію (LED).

Оголошення змінних:

```
const int gasSensorPin = A0;
const int pirSensorPin = 2;
const int contactSensorPin = 3;
const int buzzerPin = 11;
const int ledPin = 13;
```

– gasSensorPin – аналоговий пін для підключення газового датчика.

– pirSensorPin – цифровий пін, до якого підключено PIR-датчик руху.

– contactSensorPin – цифровий пін з підтяжкою до VCC для магнітоконтактного датчика (типово замкнений контакт).

– buzzerPin – пін для керування пасивним бузером.

– ledPin – пін для керування світлодіодом (індикація тривоги).

Функція setup():

```
void setup() {
  Serial.begin(9600);
  pinMode(pirSensorPin, INPUT);
  pinMode(contactSensorPin, INPUT_PULLUP);
  pinMode(buzzerPin, OUTPUT);
  pinMode(ledPin, OUTPUT);
  digitalWrite(ledPin, LOW);
}
```

– ініціалізується серійний порт зі швидкістю 9600 бод;

– PIR-датчик налаштовано як вхід;

– магнітоконтактний датчик підключено з внутрішнім підтягуванням до живлення (технологія INPUT_PULLUP), що дозволяє уникнути використання зовнішніх резисторів;

– Світлодіод і бузер налаштовані як виходи;

Основна логіка у функції loop():

```
int gasLevel = analogRead(gasSensorPin);
bool pirState = digitalRead(pirSensorPin);
bool doorOpen = digitalRead(contactSensorPin) == LOW;
```

– зчитується поточне значення рівня газу;

– зчитується стан PIR-датчика (1 – є рух, 0 – немає);

– зчитується стан магнітоконтактного датчика. Якщо контакт розімкнутий, digitalRead() поверне LOW, що означає відкриття дверей або вікна.

```
Serial.print("Gas: ");
Serial.print(gasLevel);
Serial.print(" | PIR: ");
Serial.print(pirState);
Serial.print(" | Door: ");
Serial.println(doorOpen);
```

– виводяться поточні значення сенсорів у монітор порту для спостереження;

```
if (gasLevel > 600 || pirState == HIGH || doorOpen) {
  digitalWrite(ledPin, HIGH);
  tone(buzzerPin, 1000);
  delay(500);
  noTone(buzzerPin);
  delay(200);
} else {
  digitalWrite(ledPin, LOW);
  noTone(buzzerPin);
}
```

– якщо виявлено будь-яку з подій (газ, рух або відкриття дверей/вікна) – вмикається світлодіод і лунає звуковий сигнал із бузера;

– у режимі очікування LED та бузер вимикаються.

– delay(500);

– затримка між циклами для стабільної роботи.

– цей код забезпечує просту, але ефективну охоронну систему, яка дозволяє:

– виявляти витік газу;

– виявляти несанкціонований рух у приміщенні;

– фіксувати спроби відчинення дверей або вікна;

– реагувати сигналізацією на загрозу;

– виводити діагностичну інформацію через серійний порт.

Такий підхід добре підходить для симуляції в Tinkercad та реальної реалізації у домашніх або офісних умовах

### 1.3.4 Тестування та демонстрація системи в Tinkercad

Для перевірки працездатності розробленої багаторівневої системи безпеки було використано онлайн-симулятор Tinkercad Circuits, який дозволяє моделювати роботу електронних компонентів і мікроконтролерів Arduino у реальному часі. Розроблений проєкт представлено за посиланням: https://www.tinkercad.com/things/5NN9SIzJc0c-smashing-elzing/editel?returnTo=https%3A%2F%2Fwww.tinkercad.com%2Fdashboard&sharecode=AgmRmB_bmRE9wCz40v8G_kJ3bM6hnenP_jE6m7mad38.

У процесі тестування були виконані наступні дії:

– перевірка коректності з’єднань компонентів: було змодельовано підключення газового сенсора, PIR-датчика руху, магнітоконтактного датчика, світлодіодів індикації та бузера відповідно до розробленої схеми;

– відпрацювання логіки реагування на події: за допомогою віртуальних входів було емуляційно створено сигнали, що імітують появу газу, рух у приміщенні та відкриття дверей/вікон. Система коректно виявляла ці події та активувала звукову та світлову сигналізацію;

– моніторинг через серійний порт: значення з датчиків виводилися у серійний монітор, що дало змогу відслідковувати стан сенсорів у режимі реального часу та впевнитися у коректності обробки даних;

– оцінка швидкості реагування: система реагувала на зміни станів датчиків із затримкою, що не перевищувала 1 секунди, що є достатнім для своєчасного сповіщення про загрозу.

– візуальна індикація: світлодіодні індикатори чітко відображали стан тривоги, що сприяло простому сприйняттю інформації користувачем.

За результатами тестування в Tinkercad було підтверджено працездатність системи у заданих умовах. Модель може бути використана як базова платформа для подальшого вдосконалення з додаванням бездротових модулів, віддаленого моніторингу або інтеграції з мобільними додатками.

На рис. 3.5 надано процес тестування датчика газу схеми системи безпеки в симуляторі Tinkercad. Бачимо, що після натискання кнопки Star Simulation відбувається ініціалізація проєкту. Далі активізуємо датчик Gas Sensor, що призведе до появи хмарного затемнення.

Далі хмарне затемнення наводимо на датчик Gas Sensor, що призведе до його спрацьовування. На рис. 3.6 надано цей процес. Після цього звучить звуковий сигнал від динаміка і починає світитися червоний світлодіод.

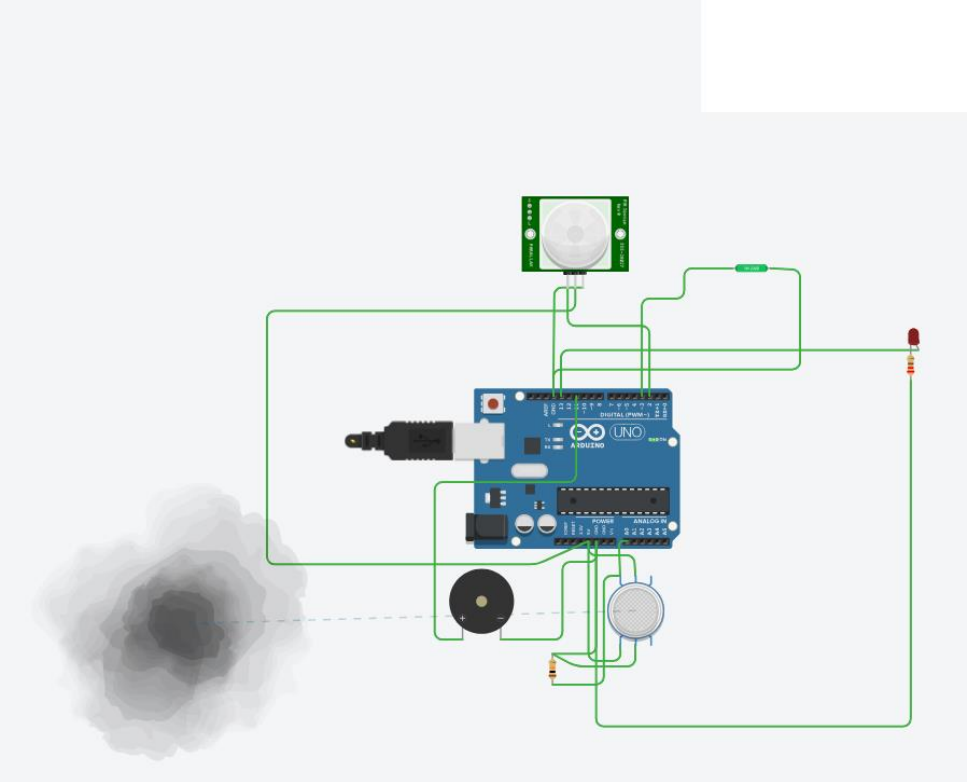


Рисунок 1.20. Процес тестування датчика газу схеми системи безпеки

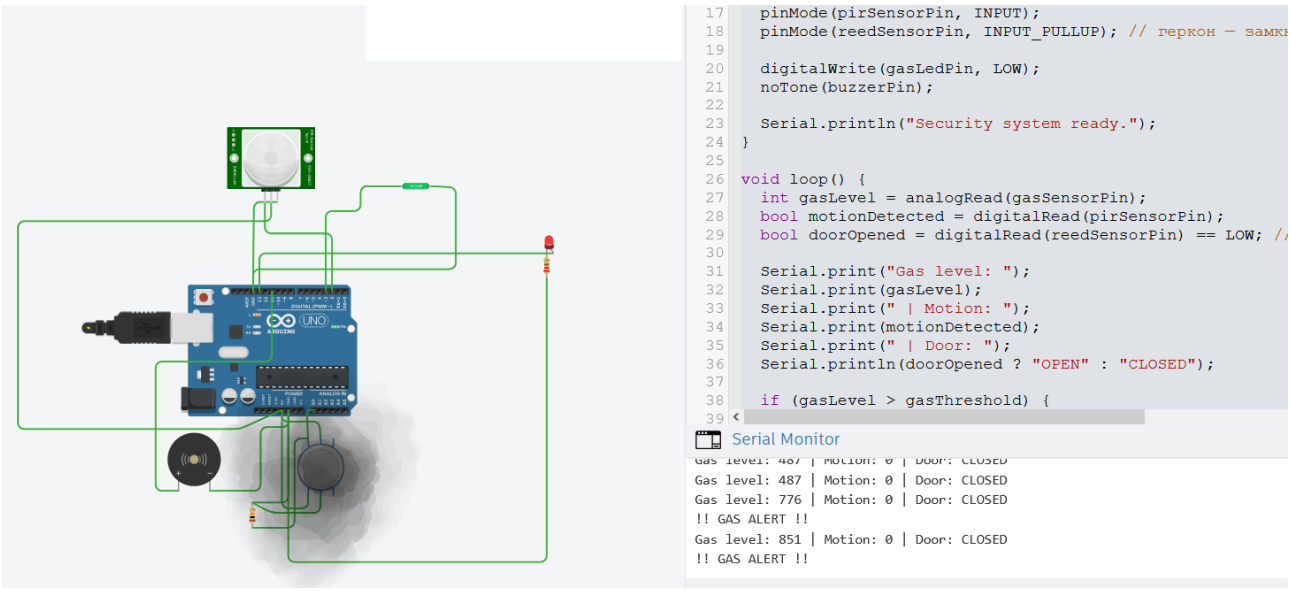



Рисунок 1.21.Процес перевірки датчика газу за допомогою темної хмари

На рис. 1.22 надано процес активізації датчика PIR.

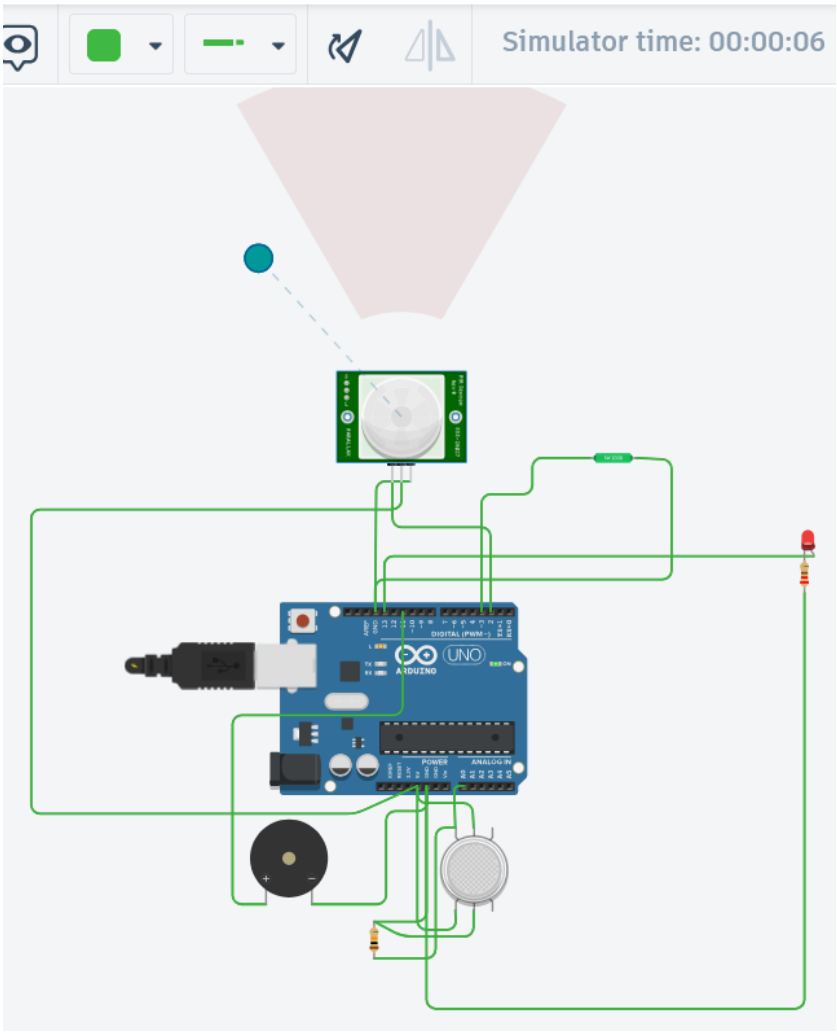



Рисунок 1.22. Процес активізації датчика PIR

Сценарії для тестування системи безпеки в Tinkercad представлені в табл. 3.7.

Таблиці 1.11. Сценарії для тестування системи безпеки в Tinkercad

| № | Сценарій тестування | Вхідні умови | Очікувана поведінка системи | Результат (факт) |
|---|---|---|---|---|
| 1 | Виявлення витоку газу | Значення газового датчика перевищує поріг (>600) | Увімкнення LED газової тривоги та активація звукового сигналу | Відповідає очікуванням |
| 2 | Виявлення руху за допомогою PIR-датчика | Поява сигналу HIGH на вході PIR-датчика | Увімкнення LED тривоги і звукового сигналу | Відповідає очікуванням |
| 3 | Відкриття дверей/вікон (магнітоконтактний датчик) | Розмикання контакту, LOW на вході датчика | Увімкнення LED тривоги та звукової сигналізації | Відповідає очікуванням |
| 4 | Відсутність загроз | Нормальні значення датчиків (газ <600, PIR LOW, контакт замкнений) | Вимкнений LED і відсутність звукової сигналізації | Відповідає очікуванням |
| 5 | Швидкість реагування системи | Імітація швидкої зміни станів датчиків | Сигналізація активується без затримок, не пропускає події | Відповідає очікуванням |

Використані інструменти в симуляторі

– для розробки та тестування системи безпеки у середовищі Tinkercad Circuits було використано такі основні компоненти та інструменти:

– мікроконтролер Arduino Uno – виконує роль центрального керуючого пристрою, обробляє сигнали з датчиків та керує виконавчими пристроями;

– газовий сенсор (Gas Sensor) – відповідає за виявлення підвищеного рівня газу у приміщенні;

– PIR-датчик руху – фіксує рух в зоні спостереження для виявлення несанкціонованого проникнення.;

– магнітоконтактний датчик – реагує на відкриття дверей або вікон, контролюючи стан закриття;

– світлодіоди (LED) – слугують індикаторами станів системи: тривога газу, руху або доступу;

– пасивний бузер (Passive Buzzer) – забезпечує звукову сигналізацію у разі виявлення загроз;

– серійний монітор Arduino IDE – використовується для виводу інформації про стан системи та параметри датчиків у процесі налагодження.

Всі компоненти були зібрані у віртуальну схему в Tinkercad, що дало змогу моделювати їх поведінку в режимі реального часу без необхідності фізичного монтажу.

# 2 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою даних розрахунків є обчислення вартості виконання науково-дослідної розробки «Розробка програмно-апаратних рішень для системи безпеки із використанням платформи Arduino»

Цей проєкт є науково-дослідницькою розробкою. Щоб оцінити його якість, ми визначаємо трудомісткість та вартість створення. Повний перелік етапів і робіт, що виконуються під час цієї НДР, представлено в таблиці 2.1.

Таблиця 2.1. Розподіл робіт по етапах і видах виконавців.

| Етап проведення НДР | Вигляд робіт | Посада виконавця |
|---|---|---|
| Розробка технічного завдання (ТЗ) | 1.Складання і затвердження ТЗ для НДР по розробці «Модернізація системи відеоспостереження на основі механізмів інтелектуальної безпеки» | Дипломник, керівник |
| Вибір напряму дослідження | 1. Збір і вивчення науково-технічної літератури.<br>2. Формулювання можливих напрямів вирішення завдань, поставлених в технічному завданні НДР і їх порівняння.<br>3. Розробка плану проведення досліджень для подальшої розробки. | Дипломник керівник |
| Теоретичні і експериментальні дослідження | 1. Етапи розвитку систем спостереження<br>2. Дослідження екосистеми СОТ<br>3. Типи даних в системах спостереження<br>4. Алгоритми отримання інформації в СОТ<br>5. Аналіз застосування систем інтелектуального відеоспостереження<br>6. Модернізація системи відеоспостереження в фокусі інтелектуальних технологій | Дипломник керівник консультанти |

Продовження таблиці 2.1. Розподіл робіт по етапах і видах виконавців

| Етап проведення НДР | Вигляд робіт | Посада виконавця |
|---|---|---|
| Узагальнення і оцінка результатів досліджень | 1. Узагальнення результатів попередніх етапів.<br>2. Оцінка повноти вирішення завдань.<br>3. Складання і оформлення звіту. Розгляд результатів проведеною НДР і прийняття | Дипломник керівник консультанти |

За відсутності належної нормативної бази, тривалість виконання окремих робіт визначається на основі ймовірнісних оцінок, наданих самими виконавцями**.**

Таблиця 2.2.Очікувана трудомісткість робіт.

| Вигляд роботи | Час виконання (дні) |
|---|---|
| 1. Складання і затвердження ТЗ для НДР «Моделювання імпульсного ДБЖ на базі мікроконтролерної системи» | 1 |
| 2. Збір і вивчення науково – технічної літератури, технічної документації і інших матеріалів. | 2 |
| 3. Формулювання можливих напрямів вирішення завдань, поставлених в технічному завданні НДР і їх порівняльна оцінка. | 2 |
| 4. Розробка плану проведення досліджень для подальшої розробки. | 2 |
| 5. Аналіз сучасних підходів до розробки систем безпеки на базі мікроконтролерів | 3 |
| 6. Проектування архітектури системи безпеки на базі arduino | 2 |
| 7. Реалізація, тестування та аналіз ефективності розробленої системи | 2 |
| 8.Узагальнення результатів Оцінка повноти вирішення поставлених завдань | 3 |
| Всього: | 23 |

Через значну роль інтелектуальної праці у створенні науково-технічної продукції, собівартість і ціна виконання науково-дослідних робіт (НДР) формуються з таких основних статей витрат: витрати на матеріали, основна і додаткова заробітна плата, відрахування до єдиного соціального фонду страхування, витрати на роботи, що виконуються сторонніми організаціями.

1) Витрати на матеріали складають – друк роботи 280 грн.

2) До витрат «Основна заробітна плата» відносяться оплата праці виконавців, безпосередньо притягнених до її виконання. Для розрахунку основної заробітної плати враховується чисельність виконавців за категоріями, обсяг виконаної ними роботи та середня денна оплата їхньої праці**.** Важливо зазначити, що відповідно до статті 8 Закону України «Про Державний бюджет України на 2025 рік», з 1 січня 2025 року мінімальна зарплата становить 8000 гривень на місяць**,** а мінімальна погодинна ставка — 48 гривень 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, 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 | 384,00 | 24 | 9312,00 |
| Керівник | 100,00 | 800,00 | 1 | 800,00 |
| Консультант по економіч. розр. | 80,00 | 640,00 | 0,25 | 160,00 |
| Консультант по охороні праці | 80,00 | 640,00 | 0,25 | 160,00 |
| Нормоконтроль | 80,00 | 640,00 | 0,25 | 160,00 |
| Всього (Зо) | | | | 10592,00 |

3) Додаткова заробітна плата розраховується як відсоток від основної заробітної плати**.** У наукових установах цей показник зазвичай становить 10-12% від суми основної заробітної плати..

Зд=10% *Зо =10592,00* 0.1 = 1059,20 грн

4) До собівартості науково-дослідних робіт (НДР) включаються всі податки, збори та інші обов'язкові платежі, передбачені чинною системою оподаткування

Зєсв=0,22*(Зо+Зд) = 0,22 *(10592,00+1059,20) = 2 563,26 грн

5) Накладні витрати включають усі управлінські та господарські витрати, пов’язані з виконанням науково-дослідних робіт (НДР) у межах діяльності установи. У наукових установах ці витрати зазвичай коливаються в межах від 40% до 120% від сукупної суми основної та додаткової заробітної плат

Рнакл= (Зо+Зд)*0,4 = (10592,00+1059,20)*0,6 = 6 990,72 грн

На основі зібраних даних щодо кожної статті витрат, планова собівартість всієї НДР представлена у формі калькуляції, згідно з таблицею 2.4**.**

Таблиця 2.4 Калькуляція планової собівартості.

| Статті витрат | Сума, грн. |
|---|---|
| 1. Матеріали | 280,00 |
| 2. Основна заробітна плата | 10592,00 |
| 3. Додаткова заробітна плата | 1059,20 |
| 4. Відрахування до єдиного соціального внеску | 2 563,26 |
| 5. Накладні витрати | 6 990,72 |
| Планова собівартість (Спл) | 21 485,18 |

Плановий прибуток визначений по формулі:

Ппл = 0,1*Спл = 0,1 * 21 485,18= 21 48,52 грн

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

Договірна ціна визначається по формулі

Цнір = Спл + Ппл = 21 485,18+21 48,52 = 23 633,69грн.

Ціну реалізації встановлюємо з урахуванням ПДВ

Цр = Цнір + ПДВ = 23 633,69+23 633,69* 0,2= 28 360,43грн.

# 3 РОЗДІЛ ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ

У сучасному світі питання забезпечення безпеки об’єктів різного призначення – житлових приміщень, офісів, складів, навчальних закладів — набуває особливої актуальності. Підвищення рівня злочинності, зростання техногенних загроз та потреба постійного моніторингу й контролю доступу стимулюють розробку ефективних, доступних і гнучких систем охорони. Актуальність дослідження зумовлена необхідністю впровадження сучасних рішень, що дозволяють своєчасно виявляти загрози та оперативно реагувати на них, мінімізуючи шкоду для людей та майна.

Одним із перспективних підходів у розробці охоронних систем є використання мікроконтролерних платформ, таких як Arduino. Завдяки відкритій архітектурі, широкому асортименту сумісних модулів (датчики руху, газу, диму, температури, GSM, RFID тощо), простоті програмування та активній спільноті розробників, Arduino дає можливість створити функціональні прототипи охоронних систем з мінімальними витратами.

Метою даної дипломної роботи є розробка та реалізація програмно-апаратного рішення для забезпечення охорони приміщень на базі мікроконтролера Arduino. Пропонована система поєднує апаратні компоненти (датчики, виконавчі пристрої) та програмне забезпечення для моніторингу подій і оперативного реагування на них. Підготовлений прототип здатний виконувати базові функції безпеки, такі як виявлення вторгнення, фіксація подій, передача сповіщень та контроль доступу, що створює можливості для подальшого вдосконалення систем охоронних технологій.

## 3.1 Аналіз небезпечних та шкідливих чинників, що впливають на працівника

Для установлення можливого впливу на здоров’я користувачів ВДТ виробничих чинників має значення ряд якісних характеристик робочого середовища. Це середовище у приміщеннях (офісах) в основному характеризується такими фізичними параметрами, як температура, вологість та

електричний опір підлоги. Фізико-хімічні показники включають інформацію про вміст у повітрі іонів та різноманітних забруднювачів, а також деякі інші якісні характеристики середовища

## 3.2 Розробка заходів з охорони праці

Виробничі приміщення

Будівлі та приміщення, де розміщені робочі місця програмістів повинні відповідати вимогам СНіП 2.09.02-85 «Производственные здания» та ДСанПіН 3.3.2.007 «Державні санітарні правила і норми роботи з ВДТ ЕОМ» Вони мають бути не нижче другого ступеня вогнестійкості. Для всіх приміщень повинно бути визначено клас зони згідно з НПАОП 40.1-1.01-97. Відповідне позначення повинно бути нанесено на вхідних дверях кожного приміщення.

Не дозволяється розташування приміщень з робочими місцями операторів ПК у підвалах і цокольних поверхах. Площа приміщення із розрахунку на одне робоче місце має бути не менше 6,0 кв.м, а об'єм – не менше 20,0 куб.м.

Для внутрішнього оздоблення приміщень з ПК слід використовувати дифузно-відбивні матеріали з коефіцієнтом відбитті для стелі 0,7 – 0,8, для стін 0,5 – 0,6. Покриття підлоги повинне бути матовим, поверхня рівною, не слизькою, з антистатичними властивостями.

Віконні прорізи приміщень для роботи з ПК мають бути обладнані регульованими пристроями (жалюзі, завіски, зовнішні козирки).

Забороняється для оздоблення інтер'єру приміщень з ПК застосовувати полімерні матеріали, що виділяють у повітря шкідливі хімічні речовини. Приміщення можуть обладнуватись шафами для зберігання документів, полицями, стелажами.

У приміщеннях слід щоденно робити вологе прибирання. Вони мають бути оснащені аптечками першої медичної допомоги.

При приміщеннях з ВДТ мають бути обладнані побутові приміщення для відпочинку під час роботи, кімната психологічного розвантаження, де слід передбачити встановлення пристроїв для приготування й роздачі тонізуючих напоїв, а також місця для занять фізичною культурою ( СНиП 2.09.04 – 87).

Мікроклімат робочої зони працівників, вентиляція

Висока температура повітря негативно позначається на функціональному стані людини. Хоч генерація теплоти дисплеєм досягає критичного рівня тільки у саму теплу пору року, необхідно створювати комфортні теплові умови постійно.

Оптимальні та допустимі мікрокліматичні параметри у приміщеннях повинні враховувати специфіку технологічного процесу при використанні комп'ютерів. Згідно з діючими у нашій країні нормативними документами (ДСанПіН 3.3.2-007-98 у холодні періоди року температура повітря, швидкість його руху та відносна вологість повітря повинні відповідно складати: 22-24$^0$С; 0,1 м/с; 40-60%. Температура повітря може коливатись у межах від 21 до 25$^0$С при збереженні інших параметрів мікроклімату.

В теплі періоди року температура повітря, його рухливість та відносна вологість повинні відповідно становити: 23-25$^0$С; 0,1-0,2 м/с; 40-60 %.

Оптимальним рівнем аероіонізації у зоні дихання користувача вважається вміст легких аерофонів обох знаків від 150 до 5000 у 1 см$^3$ повітря.

Нормалізуючий вплив на склад повітря робочої зони справляють примусова вентиляція, захисні екрани (оснащені заземленням) та застосування іонізаторів.

Освітлення робочого місця, шум, вібрація

Освітлення у приміщеннях з ВДТ має бути змішаним – природним та штучним. Природне освітлення повинно здійснюватися у вигляді бічного освітлення та відповідати нормам ДБН В.2.5-28-2006 «Природне і штучне освітлення».

При природному освітленні слід передбачити наявність сонцезахисних засобів, що знижують перепади яскравостей між природним світлом та свіченням екрана ВДТ. З цією метою можна використовувати плівки з металізованим покриттям або жалюзі з вертикальними лам елями, що регулюються.

Штучне освітлення у приміщеннях з ВДТ треба здійснювати у вигляді

комбінованої системи освітлення з використовуванням люмінесцентних джерел світла у світильниках загального освітлення. На робочих місцях має бути забезпечена рівномірна освітленість за допомогою переважно відбитого або розсіяного світлорозподілу. Світлових відблисків з клавіатури, екрана та від інших частин ВДТ у напрямку очей користувача не повинно бути.

Деякі ВДТ є потенційними джерелами цілого ряду звуків, що містять як коливання, які можна почути, так і коливання ультразвукового діапазону. Цей шум справляє негативний вплив на стан користувача, особливо при тривалому впливі.. У користувача, діяльність якого пов'язана з переробкою інформації це виражається у знижені розумової працездатності, зростає кількість помилок, розвиток зорового втомлення, зміні відчуття кольорів, появі головного болю, послаблення уваги. Нормованим параметром шуму на робочих місцях є рівень 50 дБ. Основними заходами боротьби з шумом є усунення або ослаблення причин шуму в самому його джерелі у процесі проектування, використання засобів звукопоглинання, раціональне планування виробничих приміщень.

Електробезпека

Причинами ураження працівника електрострумом можуть бути:

– Випадковий дотик до струмоведучих частин, у результаті ведення робіт поблизу або на цих частинах;

– Випадковий дотик до струмоведучих частин, у результаті ведення робіт поблизу або на цих частинах;

– Несправність захисних засобів, якими потерпілий доторкався до струмоведучих частин;

Помилкове прийняття устаткування, що перебуває під Електробезпека.

Значення сили струму, що проходить через організм людини, залежить від напруги, під якою перебуває людина й від опору ділянки тіла, до якого прикладена ця напруга. Джерелом живлячої напруги є мережа змінного струму з напругою 229В, на яку поширюється ГОСТ 25861-83.

Організація робочого місця користувача ПК

Обладнання і організація робочого місця з ВДТ мають забезпечувати

відповідність конструкцій всіх елементів робочого місця та їх взаємного розташування, ергономічним вимогам, з урахуванням характеру і особливостей трудової діяльності ( ДСанПіН 3.3.2.-007-98).

Конструкція робочого місця й взаємне розташування всіх його елементів відповідають антропометричним, фізіологічним і психологічним вимогам, а також характеру роботи. Конструкція робочих меблів дає можливість забезпечувати можливість індивідуального регулювання їх відповідно до потреб працівника для підтримки зручної пози. Робочий стіл повинен бути пофарбований матовою фарбою. Дисплей розташований так, що його верхній край перебуває на рівні очей, на відстані близько 70 см, що укладається в припустимі рамки від 60 до 90 см. Частота мерехтіння екрана дорівнює 100 Гц, що відповідає умові більше 70 Гц.

## 3.3 Пожежна безпека

Пожежна безпека приміщень, що мають електричні мережі, регламентується ГОСТ 12.1.033-81, ГОСТ 12.1.004-85. Робота оператора ЕОМ повинна вестися в приміщенні, що відповідає категорії Д пожежної безпеки.

Пожежна безпека забезпечується:

-системою запобігання пожежі;

-системою протипожежного захисту;

- організаційно-технічними заходами.

Протипожежний захист приміщення забезпечується застосуванням установки автоматичної пожежної сигналізації, наявністю засобів пожежогасіння, організацією своєчасної евакуації людей.

Для ліквідації невеликих осередків пожеж, а також для гасіння пожеж у початковій стадії їх розвитку силами персоналу об’єктів, застосовуються первинні засобі пожежогасіння. Це вогнегасники (вуглекислотні та порошкові), пожежний інвентар (покривала з негорючого полотна, ящики з піском, бочки з водою), пожежний інвентар.

# ВИСНОВКИ

У процесі виконання дипломної роботи було досліджено сучасні вимоги до систем безпеки, а також проведено огляд мікроконтролерних платформ для їх реалізації. Платформа Arduino обрана як ефективний та доступний інструмент для створення програмно-апаратних рішень у цій сфері.

У результаті виконано наступне:

1. Розроблено та реалізовано прототип охоронної системи, яка включає датчики якості повітря (MQ-135), магнітоконтактні датчики, звукову та світлову індикацію, а також інтерфейс користувача на базі LCD дисплея. Для моделювання та тестування системи використано середовище Tinkercad, що дозволило ефективно перевірити коректність роботи системи без необхідності використання фізичного обладнання.

2. Запропонована система забезпечує контроль стану об’єкта, виявлення потенційних загроз (відкриття дверей, підвищення рівня шкідливих газів), та своєчасне оповіщення користувача за допомогою звукової та світлової сигналізації.

3. Розроблене програмне забезпечення реалізує логіку активації та деактивації режимів охорони, а також адекватно реагує на різні типи подій, що свідчить про надійність і гнучкість системи.

Запропонований підхід може бути використаний як основа для подальшого розвитку більш складних систем безпеки з розширеним набором датчиків і можливістю інтеграції в мережі «розумного дому». Додатково підхід може бути запропоновано до використання в навчальному процесі з метою розвитку інженерної обізнаності та створення і програмування діючих систем безпеки

Отримані результати свідчать про доцільність використання платформи Arduino для створення доступних і ефективних систем безпеки як у приватних, так і в комерційних цілях

# ПЕРЕЛІК ВИКОРИСТАНИХ ІНФОРМАЦІЙНИХ ДЖЕРЕЛ

1 Програмування мікроконтролерів AVR : [навчальний посібник] / С. М. Цирульник, О. Д. Азаров, Л. В. Крупельницький, Т. І. Трояновська. – Вінниця : ВНТУ, 2018. – 111 с. – Режим доступу: https://pdf.lib.vntu.edu.ua/books/IRVC/2021/Tsirulnik_2018_111.pdf

2 Класифікація та аналіз загроз інформаційній безпеці в ключових системах інформаційної інфраструктури/ Ю. Васильєв// ДержНДІ Спецзв'язку. 2015. С. 58-60.

3 Основи мікропроцесорної техніки/ В. С. Баран, Г. Г. Власюк, Ю. О. Оникієнко, О. І. Смоленська. КПІ ім. Ігоря Сікорського. Київ: КПІ ім. Ігоря Сікорського, 2019. 140 с.

4 Характеристика та загальні вимоги до системи контролю і управління доступом/ М.О. Омельченко// Сучаснийзахист інформації. 2020. No4 (44). С.46-50.

5 Аналіз та класифікація систем контролю та управління доступом на підприємстві/ О.К. Юдін, О.М. Весельська// Наукоємні технології. 2018. No 2 (38). С. 220-225.

6 Офіційна документація Arduino [Електронний ресурс]. – Режим доступу: https://www.arduino.cc/reference/en/ (дата звернення: 10.06.2025).

7 Tinkercad Circuits – Documentation & Help Center [Електронний ресурс]. – Режим доступу: https://www.tinkercad.com/learn/circuits (дата звернення: 10.06.2025).

8 Datasheet MQ-135 Gas Sensor [Електронний ресурс]. – Режим доступу: https://www.datasheetq.com/MQ-135-doc (дата звернення: 10.06.2025).

9 Petzoldt M. Arduino Project Handbook. Vol. 1: 25 Practical Projects to Get You Started. – No Starch Press, 2020. – 272 p.

10 Системи контролю доступу ASSA ABLOY Global Solutions: [Електронний ресурс] – Режим доступу: https://www.assaabloyglobalsolutions.com/en/products

# ДОДАТОК А. Слайди мультимедійної презентації

ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ
ОДЕСЬКОГО НАЦІОНАЛЬНОГО ТЕХНОЛОГІЧНОГО УНІВЕРСИТЕТУ

## РОЗРОБКА ПРОГРАМНО-АПАРАТНИХ РІШЕНЬ ДЛЯ СИСТЕМИ БЕЗПЕКИ ІЗ ВИКОРИСТАННЯМ ПЛАТФОРМИ ARDUINO

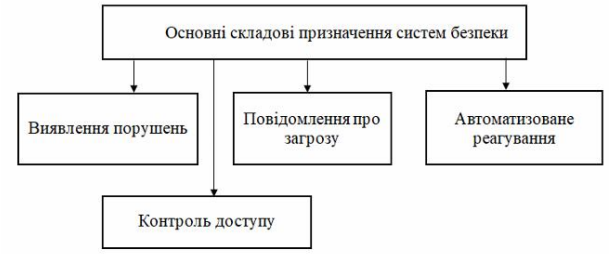
ДИПЛОМНИЙ ПРОЕКТ

**Керівник:**
Стайкуца С.В.

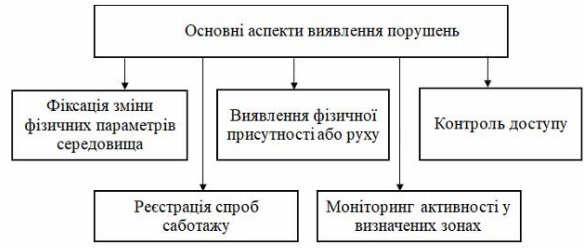
**Виконав:**
Кобилян В.В.

2025

Призначення та вимоги до сучасних систем безпеки

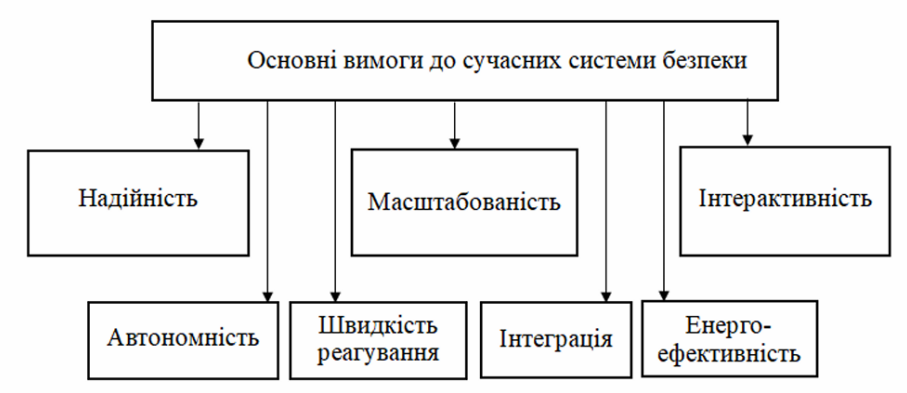



Основні складові призначення системи безпеки




Основні аспекти виявлення порушень системи безпеки

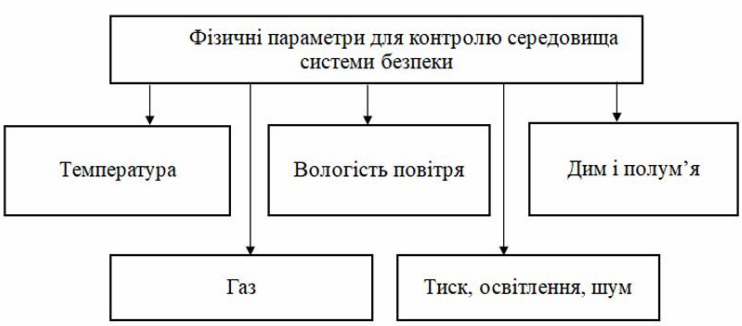
Вимоги до сучасних системи безпеки



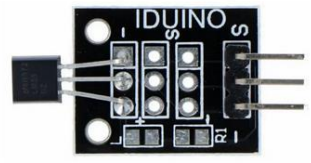

У контексті технологічного розвитку зростає роль програмно-апаратних рішень, які базуються на відкритих платформах, зокрема Arduino, що забезпечують низьку вартість, простоту реалізації та можливість адаптації під конкретні потреби користувача. В умовах обмеженого бюджету такі рішення є особливо актуальними для малих підприємств, приватних домоволодінь та навчальних закладів



Аналіз фіксація зміни фізичних параметрів середовища в системах безпеки



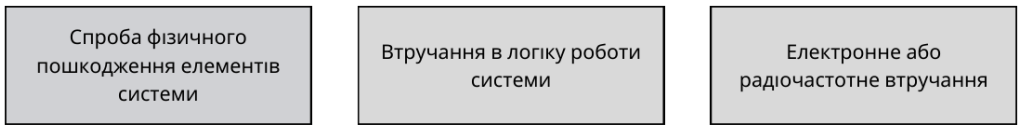

Фізичні параметри для контролю середовища системи безпеки




Зовнішній вигляд модуля з датчиком температури LM35

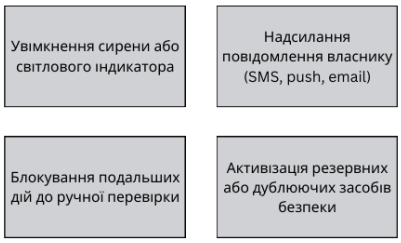
Зовнішній вигляд модуля датчика якості повітря MQ-135

Саботаж в системах безпеки підприємства




Види саботажу у системі безпеки

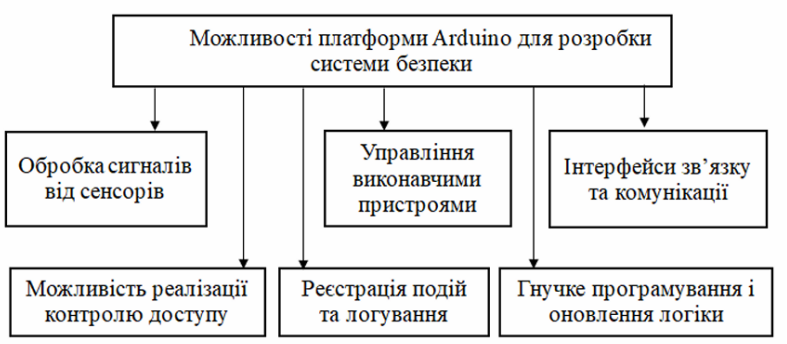

Можливості реєстрації саботажу системою на базі Arduino



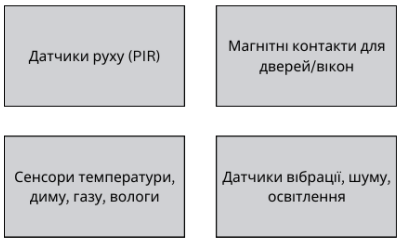

Реакція системи на саботаж



Можливості платформи Arduino в контексті безпеки




Можливості Arduino для розробки системи безпеки




Можливості Arduino щодо зчитування інформації з датчиків

Додаткові можливості платформи Arduino




Вибір симуляторів для проєктування системи безпеки на основі Arduino


Основні критерії вибору симулятора

Порівняльні характеристики симуляторів

| Симулятор | Підтримка Arduino Mega | Рівень складності | Компоненти для безпеки | Найкраще підходить для |
|---|---|---|---|---|
| *Wokwi* | *Так* | *Середній* | *Так* | *Проєктування реальних систем* |
| *Tinkercad* | *лише Uno* | *Легкий* | *Обмежено* | *Навчання, демонстрації* |
| *Proteus* | *Так* | *Високий* | *так* | *Промислові рішення* |

Вибір симуляторів для проєктування системи безпеки на основі Arduino

| | |
|---|---|
| Моніторинг якості повітря з використанням газового сенсора для виявлення надмірної концентрації газу або шкідливих речовин | Реагування на загрози шляхом активації звукової сигналізації (пасивний бузер) і світлової індикації (світлодіод) |
| Виявлення руху в контрольованій зоні за допомогою інфрачервоного (PIR) датчика | Протоколювання подій через серійний монітор з метою налагодження та демонстрації роботи системи в режимі реального часу |
| Контроль несанкціонованого відкривання дверей або вікон через магнітоконтактний датчик (геркон) | Можливість подальшої модернізації, наприклад, додавання GSM-модуля, Wi-Fi-комунікації або віддаленого керування |

Формування технічного завдання.
Опис базових функцій системи

| № з/п | Назва компонента | Кількість | Призначення |
|---|---|---|---|
| 1 | Arduino Uno R3 | 1 | Центральний контролер для керування всіма елементами системи |
| 2 | Газовий сенсор (Gas Sensor) | 1 | Виявлення наявності шкідливих або вибухонебезпечних газів |
| 3 | Датчик руху (PIR Sensor) | 1 | Виявлення руху в контрольованій зоні |
| 4 | Магнітоконтактний датчик (геркон) | 1 | Фіксація відкривання дверей або вікон |
| 5 | Світлодіод (LED) | 1–2 | Візуальна індикація тривожної події |
| 6 | Пасивний бузер (Buzzer) | 1 | Звукова сигналізація при спрацюванні системи |
| 7 | Резистори (220–330 Ом) | 2–3 | Обмеження струму для світлодіодів |
| 8 | Макетна плата (Breadboard) | 1 | Збирання схеми без пайки |
| 9 | З'єднувальні дроти (Jumper Wires) | 15–20 | Підключення елементів між собою та до Arduino |
| 10 | Віртуальний серійний монітор | - | Виведення діагностичних повідомлень і показників датчиків |

Орієнтовний склад компонентів у симуляторі Tinkercad



*Розробка схеми пристрою контролю доступу*

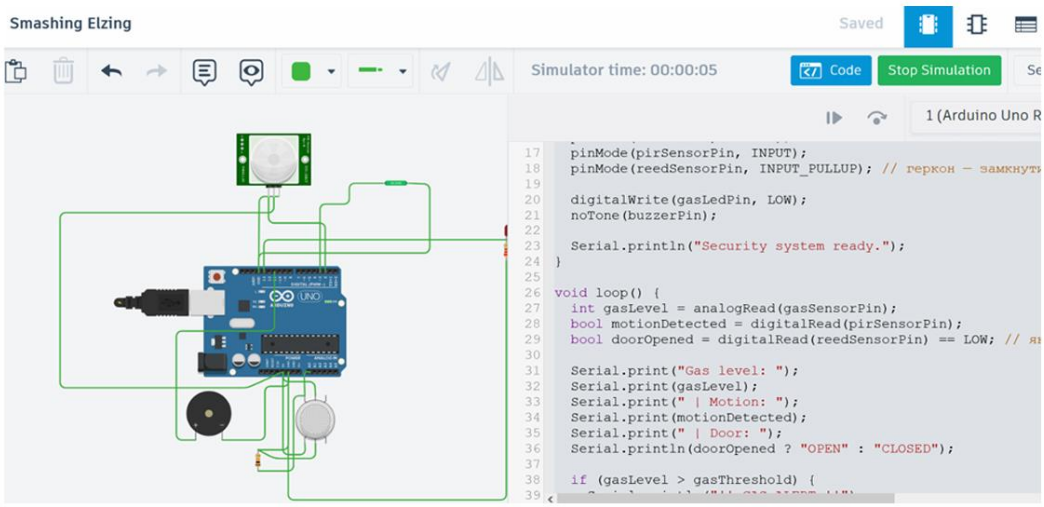
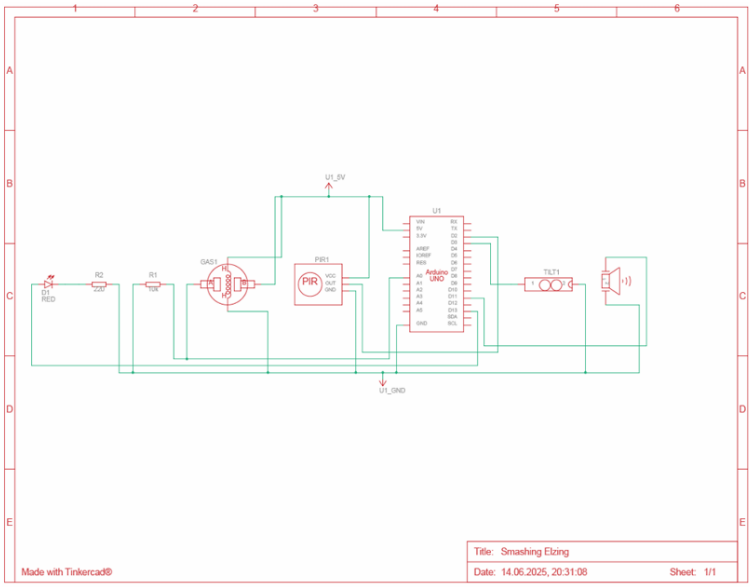



Схема підключення компонентів системи безпеки та програмний код в середовищі Tinkercad

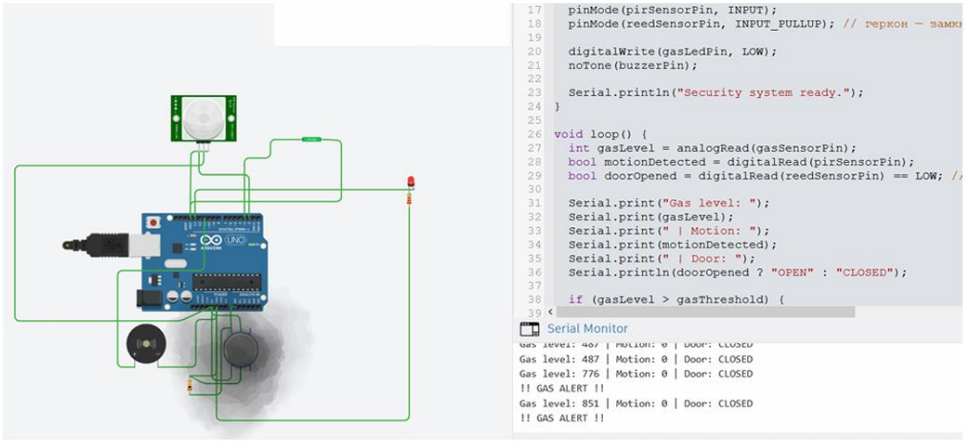
*Схема електрична принципіальна системи безпеки*




11

*Тестування та демонстрація системи*

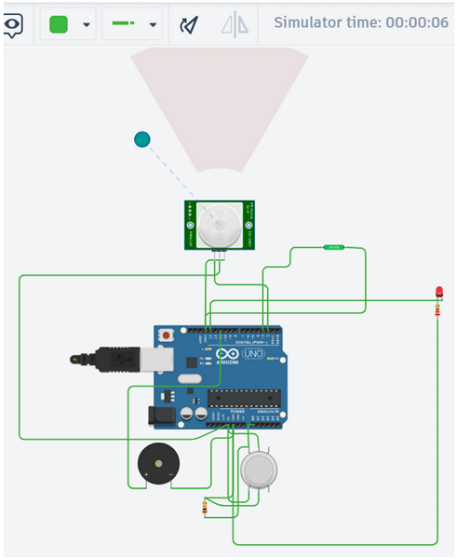
Для перевірки працездатності розробленої багаторівневої системи безпеки було використано онлайн-симулятор Tinkercad Circuits, який дозволяє моделювати роботу електронних компонентів і мікроконтролерів Arduino у реальному часі.




Процес перевірки датчика газу за допомогою темної хмари

12

*Тестування та демонстрація системи*




Процес активізації датчика PIR

| № | Сценарій тестування | Вхідні умови | Очікувана поведінка системи | Результат (факт) |
|---|---|---|---|---|
| 1 | Виявлення витоку газу | Значення газового датчика перевищує поріг (>600) | Увімкнення LED газової тривоги та активація звукового сигналу | Відповідає очікуванням |
| 2 | Виявлення руху за допомогою PIR-датчика | Поява сигналу HIGH на вході PIR-датчика | Увімкнення LED тривоги і звукового сигналу | Відповідає очікуванням |
| 3 | Відкриття дверей/вікон (магніто-контактний датчик) | Розмикання контакту, LOW на вході датчика | Увімкнення LED тривоги та звукової сигналізації | Відповідає очікуванням |
| 4 | Відсутність загроз | Нормальні значення датчиків (газ <600, PIR LOW, контакт замкнений) | Вимкнений LED і відсутність звукової сигналізації | Відповідає очікуванням |
| 5 | Швидкість реагування системи | Імітація швидкої зміни станів датчиків | Сигналізація активується без затримок, не пропускає події | Відповідає очікуванням |

Сценарії для тестування системи безпеки в Tinkercad



# ДЯКУЮ ЗА УВАГУ!

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

# РЕЦЕНЗІЯ

на дипломний проект здобувача (здобувачки) освіти

відділення комп'ютерних систем

*Кобиляна Владислава Володимировича*

(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 програмно-апаратних рішень для системи безпеки із використанням платформи Arduino*

Обсяг розрахунково-пояснювальної записки *73* сторінок

Обсяг графічної (презентаційної) частини *13* 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 програмно-апаратного пристрою на базі універсальної платформи Arduino та складається з пояснювальної записки та мультимедійної презентації, що містить логіку роботи.*

б) характеристика виконання кожного розділу дипломного проекту

*Пояснювальна записка складається з основного розділу), економічного розділу, розділу охорони праці та додатків. Перелічені розділи поетапно охоплюють розробку, виконані докладно та обґрунтовано. Розділ охорони праці містить загальну інформацію, аналіз небезпечних та шкідливих чинників та результати розробки заходів з охорони праці. Економічний розділ проекту містить розрахунок вартості виконання науково-дослідної розробки в напрямку реалізації проекту.*

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

*Графічна частина складається з 13 слайдів мультимедійної презентації. 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 *Представлено реалізацію рішення в рамках екосистеми Arduino як сучасної платформи розробки.*

*Послідовно та системно проведено реалізацію за всіма етапами життєвого циклу розробки з тестуванням в напрямках охоронної сигналізації та протипожежного захисту*

д) основні недоліки дипломного проекту

*Треба було більш детально опрацювати протипожежний захист та долучити більше елементного складу. Було б доцільним додати до рішення більшу кількість охоронних датчиків. Апаратна база має базовий склад. Обмежена відмовостійкість. Немає механізмів резервного живлення, апаратного watchdog або self-test після збою.*

Оцінка розрахункової частини *Добре*

Оцінка графічної частини *Добре*

Загальна оцінка *Добре*

Прізвище, ім'я, по батькові рецензента *к.т.н. Рудніченко Микола Дмитрович*

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

Підпис:

«27» 06 2025 р.

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

# ВІДГУК

керівника на дипломний проект здобувача (здобувачки) освіти

відділення комп'ютерних систем

*Кобиляну Владиславу Володимировичу*

(прізвище, ім`я та по батькові)

Спеціальність: *123 "Комп'ютерна інженерія"*

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

Тема дипломного проекту: *Розробка програмно-апаратних рішень для системи безпеки із використанням платформи 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 73 сторінки. У пояснювальній записці розглянуто напрям розробки програмно-апаратного пристрою на базі універсальної платформи Arduino, як програмно-апаратної платформи. Графічна частина складається з 13 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 Кобилян В.В. 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 Кобилян В.В. під час роботи над дипломним проектом проаналізував достатню кількість літературних джерел та матеріалів за напрямом роботи.*

*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 Кобилян В.В. 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

«18» 06 2025 р.

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

Ми, що нижче підписалися,

***Кобилян Владислав Володимирович***
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 програмно-апаратних рішень для системи безпеки із використанням платформи Arduino» (автор роботи – Кобилян В.В., 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 _____ / Кобилян В.В. /

Керівник _____ / Стайкуца С.В. /

«20» 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

*Кобиляна Владислава Володимировича*

на тему *Розробка програмно-апаратних рішень для системи безпеки із використанням платформи 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) | *21.06.2025* (дата) | *Петрашова В.І.* (П.І.Б.) |
|---|---|---|

Висновок відповідальної особи за перевірку роботи на наявність академічного плагіату *згідно звіту про перевірку від 20.06.2025 р. значення коефіцієнту подібності в роботі становить 22,82%, коефіцієнт цитування – 1,14%.*

| (підпис) | *21.06.2025* (дата) | *Краснокутська К.Г.* (П.І.Б.) |
|---|---|---|

**Попередня експертиза (малий захист) дипломного проєкту**

здобувача (здобувачки) освіти *Кобиляна В.В.* (П.І.Б.)

проведена «*21*» *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 6/20/2025
Дата редагування 6/20/2025

Документ прийнятий

# Звіт подібності

## метадані

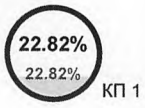
Назва організації
**Odesa Technical Professional College of Odesa National University of Technology**
Заголовок
**Розробка програмно-апаратних рішень для системи безпеки із використанням платформи Arduino**

Автор
**Кобилян Владислав Володимирович**
Науковий керівник / Експерт
**Стайкуца 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.





| 25 | 11602 | 97392 |
|---|---|---|
| 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 | · | 0 |
| Білі знаки | ß | 1 |
| Парафрази (SmartMarks) | a | 43 |

## 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/bbed74c8-2ea7-44c5-8d00-0fe3fd9790ee/download | 243 2.09 % |
| 2 | https://card-file.ontu.edu.ua/bitstreams/bbed74c8-2ea7-44c5-8d00-0fe3fd9790ee/download | 229 1.97 % |
| 3 | https://card-file.ontu.edu.ua/bitstreams/bbed74c8-2ea7-44c5-8d00-0fe3fd9790ee/download | 189 1.63 % |
| 4 | https://card-file.ontu.edu.ua/bitstreams/bbed74c8-2ea7-44c5-8d00-0fe3fd9790ee/download | 105 0.91 % |
| 5 | https://card-file.ontu.edu.ua/bitstreams/1dff552d-7200-49b8-ae1d-ba76a1335685/download | 100 0.86 % |

| | | |
|---|---|---|
| 6 | https://card-file.ontu.edu.ua/server/api/core/bitstreams/ead3fa83-2e3d-4cd7-bfbd-1d5ed04c1ce4/content | 57 0.49 % |
| 7 | https://card-file.ontu.edu.ua/bitstreams/62baa43e-b968-4993-bb54-8cf8761a89b2/download | 52 0.45 % |
| 8 | https://card-file.ontu.edu.ua/bitstreams/6cf43324-8f08-4031-ba42-f80b18efbbc8/download | 51 0.44 % |
| 9 | Малік_Система управління доступом користувачів за допомогою нейромереж [redacted] 6/7/2025 Khmelnytskyi National University (Кафедра комп'ютерної інженерії та інформаційних систем) | 50 0.43 % |
| 10 | https://card-file.ontu.edu.ua/bitstreams/c1f3e592-1123-419d-b14a-4c28662f0f1e/download | 48 0.41 % |

## з домашньої бази даних (0.29 %)

| ПОРЯДКОВИЙ НОМЕР | ЗАГОЛОВОК | КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ) |
|---|---|---|
| 1 | Розробка анімованої веб-вікторини до 95-річчя ВСП "ОТФК ОНТУ" [redacted] 6/19/2025 Odesa Technical Professional College of Odesa National University of Technology (Відокремлений структурний підрозділ "Одеський технічний фаховий коледж Одеського національного технологічного університету") | 34 (3) 0.29 % |

## з програми обміну базами даних (1.00 %)

| ПОРЯДКОВИЙ НОМЕР | ЗАГОЛОВОК | КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ) |
|---|---|---|
| **1** | Малік_Система управління доступом користувачів за допомогою нейромереж [redacted] 6/7/2025 **Khmelnytskyi National University (Кафедра комп'ютерної інженерії та інформаційних систем)** | **106 (4) 0.91 %** |
| 2 | КПІ_2024_Програмування_КР_3_012_Малюка [redacted] 7/11/2024 Ukrainian national aviation university (Ukrainian national aviation university) | 10 (1) 0.09 % |

## з Інтернету (21.52 %)

| ПОРЯДКОВИЙ НОМЕР | ДЖЕРЕЛО URL | КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ) |
|---|---|---|
| **1** | **https://card-file.ontu.edu.ua/bitstreams/bbed74c8-2ea7-44c5-8d00-0fe3fd9790ee/download** | **917 (11) 7.90 %** |
| **2** | **https://card-file.ontu.edu.ua/bitstreams/1dff552d-7200-49b8-ae1d-ba76a1335685/download** | **312 (22) 2.69 %** |
| **3** | **https://card-file.ontu.edu.ua/bitstreams/53ed22ad-8700-4162-b97a-082a1ad472d6/download** | **181 (13) 1.56 %** |
| **4** | **https://card-file.ontu.edu.ua/bitstreams/62baa43e-b968-4993-bb54-8cf8761a89b2/download** | **161 (9) 1.39 %** |
| 5 | https://card-file.ontu.edu.ua/bitstreams/035f6436-20b4-4ee6-8e99-bede670e308b/download | 152 (15) 1.31 % |
| **6** | **https://card-file.ontu.edu.ua/server/api/core/bitstreams/a05c07c5-bf65-4cb0-bdfa-e28694707551/content** | **146 (6) 1.26 %** |
| 7 | https://card-file.ontu.edu.ua/bitstreams/aed610a6-43ef-47e0-9066-e85c89456f3e/download | 99 (10) 0.85 % |
| **8** | **https://card-file.ontu.edu.ua/bitstreams/6cf43324-8f08-4031-ba42-f80b18efbbc8/download** | **82 (2) 0.71 %** |
| **9** | **https://card-file.ontu.edu.ua/server/api/core/bitstreams/ead3fa83-2e3d-4cd7-bfbd-1d5ed04c1ce4/content** | **57 (1) 0.49 %** |
| **10** | **https://card-file.ontu.edu.ua/bitstreams/c1f3e592-1123-419d-b14a-4c28662f0f1e/download** | **48 (1) 0.41 %** |
| 11 | https://card-file.ontu.edu.ua/server/api/core/bitstreams/44c16132-5f53-48e2-b6c0-61e9a2f0fd75/content | 45 (4) 0.39 % |

| | | |
|---|---|---|
| 12 | https://card-file.ontu.edu.ua/bitstreams/29489599-0581-4ce6-8890-c3b13d9f2e0e/download | 42 (4) 0.36 % |
| **13** | **https://card-file.ontu.edu.ua/server/api/core/bitstreams/8da72e29-656f-4ee4-9b22-716dedf53ff5/content** | **37 (1) 0.32 %** |
| **14** | **https://card-file.ontu.edu.ua/bitstreams/158e44b0-583e-4b2d-b758-6b86979e33bb/download** | **36 (2) 0.31 %** |
| 15 | https://card-file.ontu.edu.ua/bitstreams/549ee9fe-7574-4ae5-b500-9fe2711f33e6/download | 31 (3) 0.27 % |
| **16** | **https://card-file.ontu.edu.ua/server/api/core/bitstreams/6eb6bf1c-5813-45e6-93c5-25539b4709d3/content** | **29 (1) 0.25 %** |
| 17 | https://card-file.ontu.edu.ua/bitstreams/82a6d375-2b69-4233-b80f-fbfd149b7747/download | 28 (2) 0.24 % |
| 18 | https://card-file.ontu.edu.ua/bitstreams/21173711-5b67-4b87-b17f-6302c25e7a31/download | 21 (2) 0.18 % |
| 19 | https://card-file.ontu.edu.ua/server/api/core/bitstreams/21ac499a-a9e9-4137-810c-5f21a0318048/content | 19 (2) 0.16 % |
| 20 | https://card-file.ontu.edu.ua/bitstreams/341a820e-d025-42f3-b7dc-27e831d6c66f/download | 12 (1) 0.10 % |
| 21 | https://ethicalhacking.freeflarum.com/d/721-auto-della-polizia-con-arduino | 12 (1) 0.10 % |
| 22 | http://reposit.nupp.edu.ua/bitstream/PoltNTU/10251/1/402-%D0%A2%D0%9A%20%D0%9A%D0%BE%D0%B1%D0%B8%D0%BB%D0%B8%D0%BD%D1%81%D1%8C%D0%BA%D0%B8%D0%B9.docx | 11 (1) 0.09 % |
| 23 | https://card-file.ontu.edu.ua/server/api/core/bitstreams/4bb7255e-46d4-4349-9726-9698476da02d/content | 10 (1) 0.09 % |
| 24 | https://card-file.ontu.edu.ua/bitstreams/34a6756b-592f-4b77-a805-183aa03a6a26/download | 9 (1) 0.08 % |

## 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:** 4КБ- 02

Дипломний **проект здобувача освіти денної форми навчання КБ.** 02.07.000.ДП

КОБИЛЯНА
ВЛАДИСЛАВА
ВОЛОДИМИРОВИЧА

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: 4 КБ-02

ПОЯСНЮВАЛЬНА ЗАПИСКА
до дипломного проекту **на тему:** _____
_____ **Проектний матеріал складається з пояснювальної записки на** _____ **сторінках та графічного (презентаційного) матеріалу на** _____ **аркушах (слайдах)** Дипломник_____ ( Кобилян В.В.) Керівник _____ ( Стайкуца С. В.)