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.02.10.000.ДП

КОРОТНЯНА
АРТЕМА АНДРІЙОВИЧА

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 пристрою контролю доступу на територію на базі платформи Arduino

Проектний матеріал складається з пояснювальної записки на 70 сторінках та графічного (презентаційного) матеріалу на 14 аркушах (слайдах)

Дипломник _____ (Коротнян А.А.)

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 «27» червня 2025 р. Протокол ЕК № 6

Оцінка ЕК 4 (добре) / Род.

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.

"09" 06 2025 р.

ЗАВДАННЯ

на дипломний проект

Здобувачеві (здобувачці) освіти *Коротняну Артему Андрійовичу*

(прізвище, ім'я, по батькові)

1. Тема проекту *Розробка пристрою контролю доступу на територію на базі платформи Arduino*

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

2. Термін здачі закінченого проекту 16.06.2025 р.

3. Вихідні данні до проекту (роботи) *1. Системи контролю та управління доступом; 2. Класифікація СКД; 3. Мікроконтролери Arduino; 4. Середовища розробки Arduino; 5. Компоненти та типи СКД; 6. Розробити технічне завдання на проектування прострою системи контролю доступом; 7. Представити результати роботи пристрою системи контролю доступом.*

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

Теоретичні основи побудови систем контролю доступу; Поняття, принципи та класифікація систем контролю доступу; огляд можливостей платформи Arduino для реалізації пристроїв СКД; Проектування пристрою контролю доступу на базі Arduino; Розробка технічного завдання пристрою контролю доступу; Опис компонентів пристрою контролю доступу; Розробка ПЗ пристрою контролю доступу; Тестування працездатності пристрою СКД;

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

Класифікація систем контролю доступу; Переваги та недоліки мережевих СКУД; Аналіз існуючих рішень у галузі доступу на основі мікроконтролерів; Порівняльний аналіз застосунків для розробки проєкту; Особливості розробки проєкту в симуляторі Wokwi; Розробка технічного завдання пристрою контролю; Опис компонентів прострою контролю доступу; Розробка схеми пристрою доступу; Опис програмного забезпечення; Тестування працездатності пристрою керування доступом; Висновки

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. Основи побудови систем контролю доступу*	*14.05.2025*	Виконано
2.	*Поняття, принципи та класифікація СКД*	*17.05.2025*	Виконано
3.	*Аналіз існуючих рішень у галузі доступу на основі*	*20.05.2025*	Виконано
	мікроконтролерів		
4.	*Огляд можливостей платформи Arduino для реалізації*	*22.05.2025*	Виконано
	пристроїв. СКД		
5.	*Проектування пристрою контролю доступу на базі Arduino*	*01.06.2025*	Виконано
6.	*Порівняльний аналіз застосунків для розробки проєкту,*	*03.06.2025*	Виконано
	компонентний склад та типи СКУД		
7.	*Розробка технічного завдання пристрою контролю доступу*	*06.06.2025*	Виконано
8.	*Розробка схеми пристрою контролю доступу*	*10.06.2025*	Виконано
9.	*Розробка ПЗ пристрою контролю доступу*	*11.06.2025*	Виконано
10.	*Тестування працездатності пристрою керування доступом*	*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. 10 000. 00 ДП	Дипломний проект		
А4			КБ 02. 10 000. 00 ДП ПЗ	Пояснювальна записка	1	

Зм.	Арк.	№ докум.	Підпис	Дата	КБ 02. 10 000. 00 ДП		
Розробив		Коротнян А.А.			Розробка пристрою контролю доступу на територію на базі платформи Arduino	Літ.	Аркуш 3 / Аркушів 70
Перевірив		Стайкуца С.В.				НДП	
Н. Контр.		Петрашова В.І.				ВСП "ОТФК ОНТУ" гр.4КБ-02	
Затверд.		Кривченко Ю.В.					

ЗМІСТ

ВСТУП

Питання безпеки завжди супроводжують людство. Так, згідно піраміди Маслоу, безпека – це рівень поруч з базовими потребами. Безпека потрібна в особистому та корпоративному середовищі. З позиції ланки міжнародних стандартів безпека – це основа стратегії безперервності бізнесу (BCM), як головної мети компаній.

Безпека – це сукупність методів та засобів, направлених на досягнення корпоративних цілей, мінімізацію ризиків та впровадження ризик-менеджементу в компанії. Одна із складових корпоративної безпеки – технічні засоби охорони, або фізичний захист. В свою чергу, в базовий склад технічних засобів входить компонент від назвою СКУД – або системи керування управління доступом. Часто зустрічається синонімічна назва контроль доступу.

Сьогодні на ринку систем безпеки представлено чимало брендів, які пропонуються програмно-апаратні комплекси контролю доступу, які використовують різні ідентифікатори. Проте, все це закінчені рішення в рамках певної екосистеми, що дає можливість проводити експлуатацію системи, але не її детальну модернізацію та програмування. Річ йде саме про базовий рівень для отримання інженерного та програмного досвіду з мінімальним вкладанням бюджету на невеличких об’єктах невисокого режиму секретності. Тут оптимальним рішенням може стати використання платформи Arduino з використання широкого спектру представлених в лінійці компонентів. Все це дає можливість змоделювати багато рішень з точки зору безпеки, в тому числі – і з напряму контролю доступу.

Результатом дипломної роботи є розробка пристрою контролю доступу та територію на базі технології Arduino, розробка технічного завдання, вибір компонентів, написання коду, тестування працездатності в симуляторі Wokwi.

1 ОСНОВНИЙ РОЗДІЛ

1.1 Теоретичні основи побудови систем контролю доступу

1.1.1 Поняття, принципи та класифікація систем контролю доступу

Система контролю доступу (СКД) – це комплекс технічних і програмних засобів, призначених для автоматизованого обмеження або дозволу доступу осіб до певної зони, об’єкта чи ресурсу. Основною метою СКД є підвищення рівня безпеки шляхом ідентифікації користувачів та контролю за їх діями. Принципи роботи систем контролю доступу базуються на таких етапах:

1) ідентифікація;

2) аутентифікація;

3) авторизація;

4) реєстрація події.

Ідентифікація спрямована на визначення особи, яка намагається отримати доступ (за допомогою картки, пароля, біометрії тощо). Аутентифікація виконую перевірку відповідності наданої інформації збереженим даним у базі. Авторизація забезпечує ухвалення рішення про надання або заборону доступу. Реєстрація події виконує фіксацію дій користувача в системному журналі або базі даних.

Принципи роботи систем контролю доступу надано на рис. 1.1.

СКД можуть функціонувати автономно або бути частиною більших інтегрованих систем безпеки, включаючи відеоспостереження, сигналізацію, облік робочого часу тощо. Залежно від способу реалізації, системи контролю доступу класифікуються за кількома ознаками:

– за рівнем автоматизації;

– за способом ідентифікації користувача;

– за способом керування;

– за сферою використання.

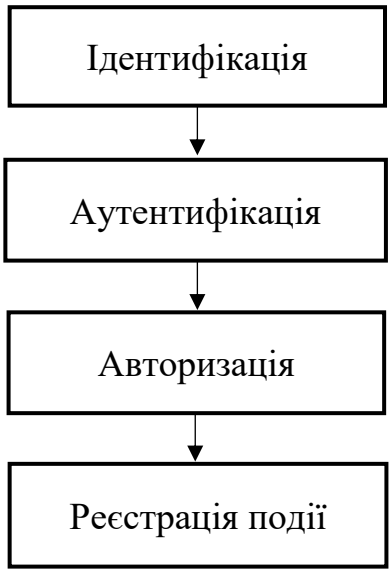


Рисунок 1.1. Принципи роботи систем контролю доступу

На рис. 1.2 надана класифікація систем керування доступом.

Рисунок 1.2. Класифікація систем керування доступом

За рівнем автоматизації розрізняють СКД: механічні (наприклад, замки з ключем); електромеханічні (керовані електричним сигналом); електронні та мікропроцесорні (на основі мікроконтролерів або комп'ютерних систем).

За способом ідентифікації користувача розрізняють наступні СКД: системи з парольним доступом (PIN-коди); системи з RFID-ідентифікацією (карти, брелоки) (рис 1.3); біометричні системи (відбитки пальців, розпізнавання обличчя); комбіновані системи (поєднання кількох методів).

Рисунок 1.3. Турнікет зі зчитувачем RFID системи контролю доступом

За способом керування розрізняють наступні СКД: автономні; мережеві.

Автономна система контролю доступу – це система, яка функціонує незалежно від зовнішніх серверів, комп'ютерів або мереж. Вона містить у собі всі необхідні елементи для забезпечення обмеженого доступу до приміщень чи територій, зберігає дані локально, а керування здійснюється безпосередньо через вбудовані компоненти або простий інтерфейс налаштування.

Основні характеристики автономних СКД:

– відсутність постійного підключення до ПК чи сервера;
– зберігання бази користувачів і паролів локально у пам'яті пристрою;
– простота налаштування і використання;
– обмежені можливості ведення журналу подій та моніторингу;
– зазвичай застосовуються в умовах малої кількості користувачів.

Приклади автономних СКД:

– електронні кодові замки з кнопковою клавіатурою;
– безконтактні RFID-системи з внутрішньою пам'яттю;
– автономні системи на базі мікроконтролерів, зокрема Arduino або ESP32.

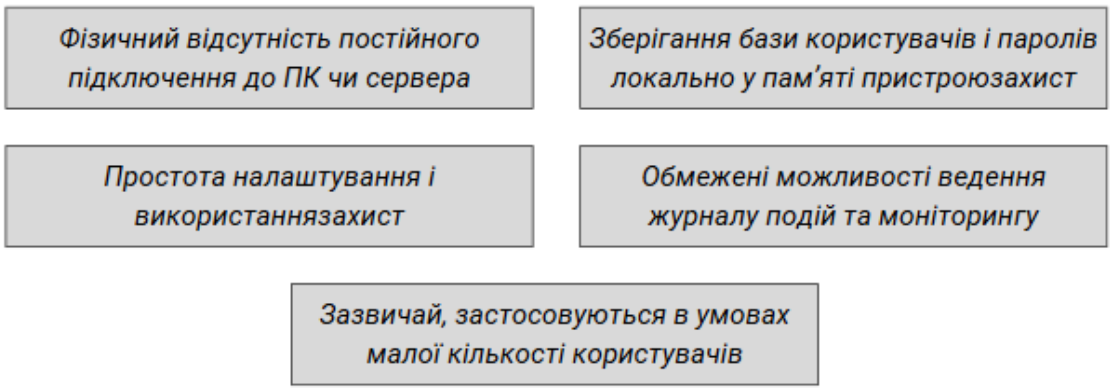


Рисунок 1.3. Основні характеристики автономних СКД

До переваг автономних СКД можна віднести:

– простота впровадження і налаштування;

– низька вартість реалізації;

– надійність за рахунок мінімальної кількості зовнішніх зв'язків;

– не вимагає інтернет-з'єднання або локальної мережі.

До недоліків автономних СКД можна віднести:

– обмежена масштабованість;

– відсутність централізованого керування та моніторингу;

– складність у веденні обліку користувачів у великих системах.

Можна відзначити наступне застосування автономних СКД:

– приватні будинки;

– гаражі, складські приміщення;

– вхідні двері в офісах без IT-інфраструктури;

– тимчасові або мобільні об'єкти (наприклад, будівельні майданчики).

У даному проєкті реалізовано саме автономну СКД. Пристрій не потребує підключення до комп'ютера чи мережі, паролі вводяться через клавіатуру, підтвердження відображається на LCD-дисплеї, а сервомотор і зумер забезпечують фізичне блокування/розблокування доступу та індикацію дій. Додатково реалізовано можливість зміни паролю без програмного перепрошивання – шляхом спеціального режиму конфігурації через клавіатуру.

Рисунок 1.4. Переваги та недоліки автономних СКД

Електронні кодові замки з кнопковою клавіатурою — це один із найпоширеніших і доступних засобів реалізації систем контролю доступу. Вони забезпечують обмеження доступу до приміщень або територій шляхом введення правильного коду (пароля) на клавіатурі.

Принцип дії електронно-кодового замку з кнопковою клавіатурою наступний. Користувач вводить на клавіатурі заздалегідь заданий цифровий або символьний код. У разі правильного введення замок активує механізм відкриття (наприклад, сервопривід, електромагнітний замок або реле). При неправильному введенні – доступ блокується, може подаватися звуковий сигнал або запускатись затримка повторного введення.

Типові функціональні можливості кодового замку:

– зміна коду користувачем або адміністратором;

– подача звукового/світлового сигналу при натисканні клавіш, введенні коду або помилці;

– захист від підбору коду (блокування після кількох неправильних спроб);

– підключення до механічних виконавчих пристроїв (сервоприводів, електрозамків);

– робота в автономному режимі без підключення до мережі або сервера.

До переваг кодового замку можна віднести:

– простота конструкції і програмування;

– низька вартість реалізації;

– відсутність потреби у фізичних ключах або RFID-картках;

– швидке оновлення коду доступу.

Недоліками кодового замку є:

– обмежена стійкість до соціальної інженерії (підгляд за кодом);

– потреба в періодичній зміні коду для підвищення безпеки4

– знос механічних кнопок при інтенсивному використанні.

Сфера використання кодового замку:

– домашні системи безпеки;

– невеликі офісні приміщення4

– побутові шафи, сейфи;

– навчальні заклади, підсобні приміщення.

У рамках цього дипломного проєкту реалізовано кодову систему доступу з 4×4 кнопковою матричною клавіатурою, де користувач вводить пароль для відкриття доступу. Також передбачено функцію зміни коду за запитом, що підвищує гнучкість і безпеку експлуатації пристрою.

Мережева система контролю доступу – це тип СКД, яка підключена до комп’ютерної мережі, і керування всіма її елементами відбувається централізовано за допомогою спеціального програмного забезпечення (рис. 1.4). Такі системи широко використовуються у великих офісах, державних установах,

підприємствах та організаціях із великою кількістю співробітників і високими вимогами до безпеки.

Можна визначити наступні основні характеристики мережевих СКД:

– централізоване управління з одного або декількох ПК через мережу Ethernet, Wi-Fi або інші канали зв’язку;

– єдина база даних користувачів, яка зберігається на сервері;

– журнали подій – це можливість фіксування всіх подій доступу (хто, коли, куди зайшов або не зміг зайти);

– гнучке налаштування прав доступу, розкладів, зон і груп;

– інтеграція з іншими системами безпеки: відеоспостереження, охоронна сигналізація, пожежна безпека.

Журнали подій – це функціональний компонент сучасних систем контролю доступу (СКД), який дозволяє реєструвати всі дії, пов’язані з отриманням або відмовою в доступі. Журнал подій може містити наступну інформацію:

– ідентифікатор користувача (код, PIN, RFID, тощо);

– дата та точний час спроби доступу;

– місце доступу (наприклад, вхід у головний офіс, серверну тощо);

– результат (успішний доступ / відмова в доступі);

– тип події (введено невірний код, змінено пароль, система перезавантажена, тощо).

Особливо важливим є ведення журналів подій:

– аудит безпеки: аналіз, хто і коли здійснював спробу доступу;

– розслідування інцидентів: у разі порушення безпеки дає змогу встановити винуватців;

– контроль персоналу: допомагає відстежувати робочий час і присутність працівників;

– тестування пристрою: спрощує налагодження та пошук помилок під час розробки системи.

Журнал подій може бути реалізовано наступним шляхом:

– виведення інформації на дисплей при кожній спробі доступу;

– зберігання подій у внутрішній пам’яті (EEPROM);

– виведення журналу через послідовний порт (Serial Monitor) на комп’ютер або модуль реєстрації на SD-карту.

У базовій конфігурації реалізовано відображення подій на LCD-дисплеї (наприклад, «Access Granted», «Wrong Code», «Code Changed»), а також можна легко розширити функціонал для логування дій у зовнішню пам’ять або базу даних через модуль ESP8266 чи Ethernet Shield.

Переваги мережевих СКД наступні:

– масштабованість – легко додавати нові точки контролю;

– аналітика та звітність – ведення історії доступу та звітів про користувачів;

– дистанційне управління – зміну налаштувань можна здійснювати з будь-якої точки доступу до системи;

– безпечність – підтримка сучасних методів авторизації (біометрія, багатофакторна аутентифікація).

Недоліки мережевих СКД наступні:

– складність у налаштуванні та обслуговуванні;

– вища вартість обладнання та впровадження;

– залежність від мережевої інфраструктури – у разі її відмови можуть виникнути проблеми з доступом.

Приклади мережевих СКД:

– системи на базі контролерів з Ethernet або Wi-Fi модулями (наприклад, на ESP32);

– корпоративні рішення від відомих виробників: Hikvision, ZKTeco, Honeywell, Parsec, etc;

– кастомізовані системи на базі Raspberry Pi або промислових контролерів.

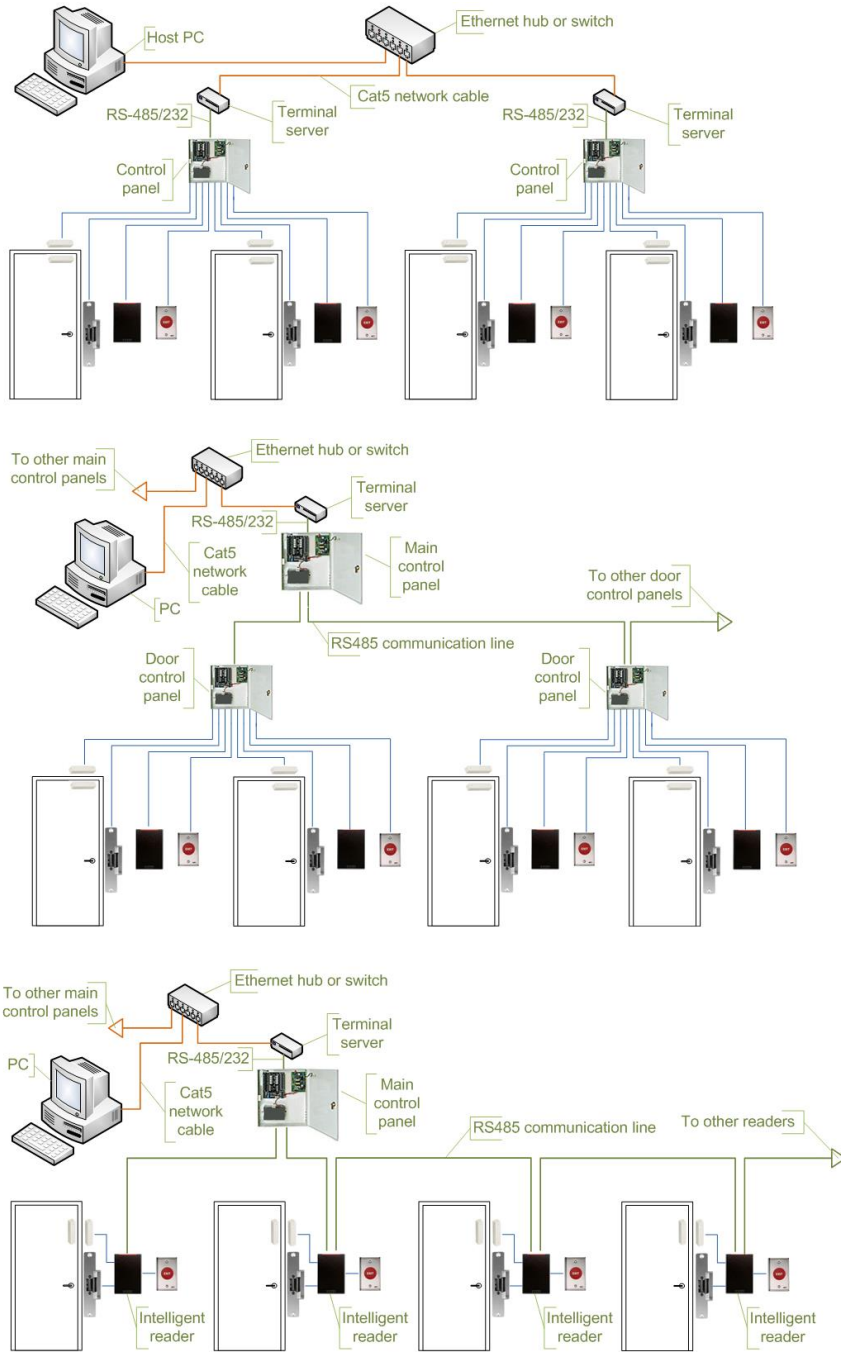


Рисунок 1.5. Приклад СКД офісу з використанням RFID системи

В табл. 1.1 представлено порівняльні характеристики автономних та мережевих СКД.

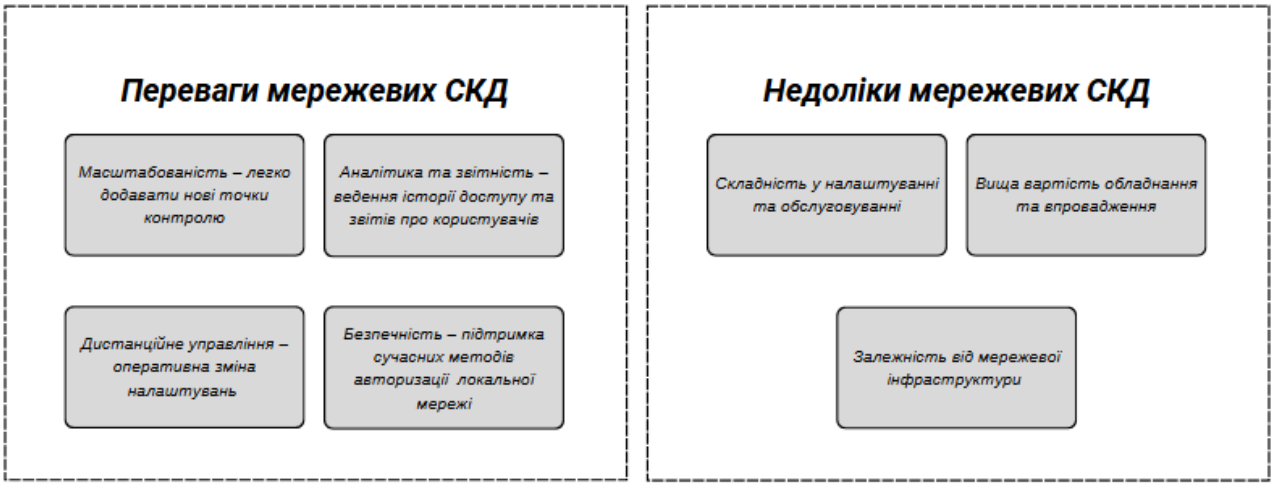


Рисунок 1.6. Переваги та недоліки мережевих СКД

Застосування мережевих СКД:

– високозахищені об’єкти з великою кількістю працівників;

– офіси з потребою у детальному контролі переміщень;

– системи доступу в бізнес-центрах і на підприємствах;

Платформи із централізованим управлінням через хмарні сервіси

– Системи контролю доступу (СКД) можуть класифікуватися не лише за архітектурою (автономні, мережеві), а й за сферою застосування (рис. 1.5), що визначає їхні функціональні особливості, рівень захисту, масштаб та інтерфейси взаємодії з користувачем. Основні сфери використання СКД включають:

1) СКД для житлових об’єктів;

2) СКД для офісів та адміністративних приміщень;

3) СКД для промислових та виробничих об'єктів;

4) СКД для об'єктів критичної інфраструктури;

5) СКД для закладів освіти та охорони здоров’я;

6) СКД для транспорту та паркінгів;

7) СКД для готелів і хостелів.

СКД для житлових об’єктів:

– застосовуються у приватних будинках, квартирах, багатоквартирних будинках;

– зазвичай автономні або з мінімальною мережею4

– контроль доступу реалізується за допомогою PIN-коду, ключа, RFID або біометричних засобів;

– часто інтегруються з системами сигналізації та відеоспостереження.

СКД для офісів та адміністративних приміщень:

– забезпечують контроль доступу співробітників до різних зон;

– можуть бути як автономними, так і мережевими з централізованим керуванням;

– підтримують інтеграцію з обліком робочого часу, розкладом доступу та віддаленим адмініструванням;

– важливими є масштабованість, журналювання подій та резервне живлення.

3. СКД для промислових та виробничих об'єктів:

– високий рівень безпеки, захист від несанкціонованого доступу;

– часто інтегруються з іншими системами автоматизації та промисловими протоколами (Modbus, Profibus тощо);

– використовують багаторівневу авторизацію: карти, біометрія, коди;

– можуть обмежувати доступ до обладнання, технологічних зон або небезпечних ділянок.

4. СКД для об'єктів критичної інфраструктури:

– енергетичні підприємства, водозабезпечення, зв'язок, державні установи;

– потребують найвищого рівня надійності, захисту і контролю;

– широко використовують біометричну автентифікацію, шифрування каналів зв’язку, подвійний контроль доступу;

– часто інтегруються з державними системами безпеки.

5. СКД для закладів освіти та охорони здоров’я:

– метою обмеження є доступ до приміщень навчального закладу або медичного центру;

– забезпечення безпеки учнів, студентів, пацієнтів і персоналу;

– можуть використовуватися для фіксації часу приходу/виходу працівників;

– у дитсадках та школах – часто оснащені функцією повідомлення батьків про вхід/вихід дитини.

6. СКД для транспорту та паркінгів:

– автоматизоване керування шлагбаумами, воротами, зонами для транспорту;

– зчитувачі номерних знаків, RFID-мітки, мобільні застосунки;

– інтеграція з білінговими та навігаційними системами.

7. СКД для готелів і хостелів:

– карткові системи, мобільні додатки, NFC-ключі;

– прив’язка прав доступу до конкретного періоду перебування;

– інтеграція з програмами керування номерним фондом.

Таблиця 1.1. Порівняльні характеристики автономних та мережевих СКД

Критерій	Автономна СКД	Мережева СКД
Підключення до мережі	Не потрібне	Обов’язкове
Керування користувачами	Локально	Централізовано
Масштабованість	Обмежена	Висока
Журнал подій	Відсутній або мінімальний	Детальний, на сервері
Вартість	Низька	Вища
Обслуговування	Просте	Складніше, потребує IT-підтримки
Типи об’єктів застосування	Будинок, гараж, невеликий офіс	Заводи, великі офіси, держустанови

Таким чином, класифікація СКД за сферою використання дозволяє правильно вибрати архітектуру, технології та компоненти при створенні

конкретного проєкту. У рамках дипломного проєкту реалізується автономна система контролю доступу для обмеження входу на певну територію, яка за функціональністю може бути адаптована до житлових об'єктів або малих офісів. Таким чином, системи контролю доступу є гнучкими інструментами безпеки, які можуть бути адаптовані до різних умов, завдань і бюджетів. Сучасні тенденції у цій галузі передбачають активне використання мікроконтролерних платформ, таких як Arduino, для створення доступних, функціональних та масштабованих рішень.

Рисунок 1.7. Термінал реєстрації робочого часу

1.1.2 Аналіз існуючих рішень у галузі доступу на основі мікроконтролерів

Останніми роками мікроконтролерні платформи, зокрема Arduino, ESP8266/ESP32, Raspberry Pi та інші, широко використовуються для створення недорогих і гнучких систем контролю доступу. Їх популярність зумовлена простотою програмування, відкритим програмним середовищем та великою кількістю сумісних модулів.

Найпоширеніші рішення на основі мікроконтролерів можна класифікувати за способом ідентифікації користувача:

1) RFID-системи на базі Arduino;

2) системи з клавіатурним вводом PIN-коду;
3) біометричні системи (відбитки пальців);
4) Bluetooth- або Wi-Fi-контроль доступу;
5) комбіновані системи.

RFID-системи на базі Arduino є одним із найпопулярніших підходів є використання RFID-модулів (наприклад, RC522) для зчитування карток або брелоків, що містять унікальний ідентифікаційний номер. Ці системи зазвичай складаються з: мікроконтролера (Arduino Uno/Nano/Pro Mini); RFID-зчитувача; електронного замка (наприклад, соленоїдного); джерела живлення та індикаторів (світлодіоди, дисплеї). Такі рішення прості у реалізації, мають середній рівень безпеки і підходять для побутових або навчальних цілей.

Системи керування доступом з клавіатурним вводом PIN-коду (рис. 1.8) є одним популярним варіантом є використання матриць клавіатур 4×4 або 3×4, що дозволяють вводити цифровий пароль. Arduino зчитує введений код, порівнює його з еталонним, і у разі збігу відкриває доступ.

Недоліком таких систем є ризик компрометації пароля, однак їх можна посилити шляхом додавання екрану, двофакторної аутентифікації або змінних кодів.

Рисунок 1.8. СКД з клавіатурним вводом PIN-коду

Біометричні системи (відбитки пальців) завдяки доступності модулів типу R305 або GT-521F дають можливість реалізувати ідентифікацію за відбитками пальців. Такі модулі працюють у парі з Arduino і дозволяють зберігати та порівнювати біометричні шаблони. Біометричні системи забезпечують вищий рівень безпеки, але є дорожчими і чутливішими до умов експлуатації (забруднення, волога тощо). Біометрична СКД на основі біометрії відбитки пальців надана на рис. 1.9.

Рисунок 1.9. Біометрична СКД на основі біометрії відбитки пальців

Bluetooth- або Wi-Fi-контроль доступу можливо реалізувати на основі модулів HC-05/HC-06 (Bluetooth) або ESP8266/ESP32 (Wi-Fi), які керується зі смартфона. Наприклад, користувач натискає кнопку в мобільному застосунку, що надсилає команду на Arduino, який у свою чергу керує електрозамком.

Такі рішення зручні для сучасних користувачів і можуть бути інтегровані з хмарними базами даних, проте потребують захисту від мережевих атак.

Найбільш захищеними є комбіновані рішення, які поєднують декілька методів ідентифікації: наприклад, RFID + PIN-код або біометрія + мобільний доступ. Це дозволяє значно підвищити рівень захисту. На рис. 1.10 надана система контролю доступу з електромеханічним замком на основі RFID карток

та Wi-Fi. Система RFID використовується доступу до приміщення працівниками офісу, а Wi-Fi забезпечує відкривання вхідної двері за допомогою смартфона.

Рисунок 1.10. Bluetooth модуль HC-06 для реалізації СКД

Рисунок 1.11. Комплект контролю доступу з електромеханічним замком та Wi-Fi викличною панеллю SEVEN KD-7841

Загалом, аналіз ринку показує, що системи контролю доступу на основі мікроконтролерів мають високий потенціал завдяки своїй доступності, масштабованості та можливості адаптації до конкретних потреб. Arduino виступає ідеальною платформою для реалізації подібних проектів у навчальному середовищі та для побутового використання.

Рисунок 1.12. Система контролю доступу з електромеханічним замком на основі RFID карток та Wi-Fi

1.1.3 Огляд можливостей платформи Arduino для реалізації подібних пристроїв

Платформа Arduino є однією з найпопулярніших середовищ для розробки прототипів електронних пристроїв завдяки своїй відкритості, простоті використання та широкому асортименту сумісних модулів. Arduino дозволяє створювати – доступні та функціональні системи контролю доступу без необхідності глибоких знань у галузі електроніки чи програмування.

Можна визначити основні переваги Arduino:

– простота програмування;

– велика спільнота;

– гнучкість та масштабованість;

– модульність;

– доступність.

Простота програмування пояснюється використанням мови програмування, схожа на C/C++, а середовище Arduino IDE має інтуїтивно зрозумілий інтерфейс (рис. 1.11). Велика спільнота – це численні приклади, бібліотеки та форуми значно спрощують розробку. Гнучкість та масштабованість – це підтримка великої кількості модулів: RFID-зчитувачі, клавіатури, екрани, модулі зв'язку, датчики тощо. Модульність – це можливість швидкого збирання пристрою за допомогою готових компонентів без складного монтажу. Доступність – це плати Arduino та модулі мають відносно низьку вартість, що важливо для навчальних проєктів і малобюджетних рішень.

Рисунок 1.13. Інтерфейс середовища Arduino IDE

Для створення програмного забезпечення можна використати Arduino IDE (Integrated Development Environment) – офіційне середовище розробки для мікроконтролерів на базі платформи Arduino. Ця середа є кросплатформною, підтримує операційні системи Windows, Linux та macOS, а також має відкритий вихідний код.

Визначимо наступні можливості Arduino IDE:

– написання коду мовою програмування C/C++ із використанням специфічних бібліотек Arduino;

– просте завантаження скетчів (програм) до мікроконтролера через USB;

– наявність вбудованого монітора порту для перевірки передавання даних через UART;

– величезна база бібліотек та прикладів, що значно спрощує розробку;

– підтримка великої кількості апаратних платформ (Arduino Uno, Mega, Nano, ESP8266, ESP32 та інші);

– можливість використання розширень та інтеграції з онлайн-сервісами (наприклад, Arduino Cloud, Wokwi);

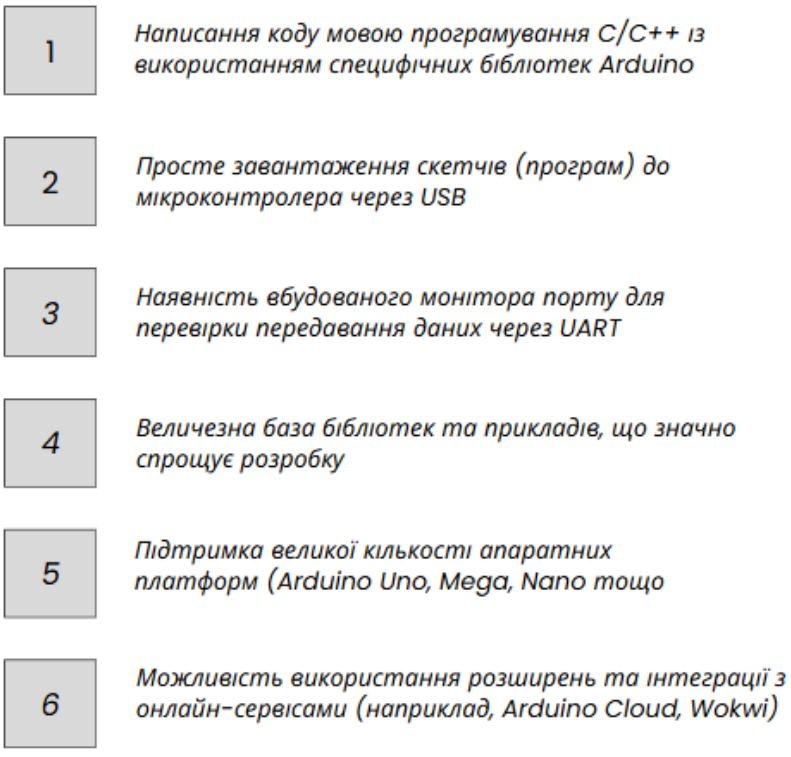


Рисунок 1.14. Можливості Arduino IDE

Альтернативи Arduino IDE: хоча Arduino IDE є найпопулярнішим середовищем, для – складніших проєктів можна використовувати інші інструменти:

– PlatformIO – розширене середовище для Visual Studio Code з підтримкою автодоповнення, налагодження та роботи з багатьма платформами.

– Wokwi – онлайн-симулятор для тестування Arduino-проєктів без фізичних компонентів. Дозволяє створювати схеми, писати код та запускати програму віртуально, що було особливо корисним під час розробки та тестування пристрою.

Таким чином, платформа Arduino IDE у поєднанні з симулятором Wokwi надало зручне середовище для розробки, налагодження та перевірки пристрою контролю доступу. Простота інтерфейсу, велика база бібліотек та активна спільнота розробників зробили Arduino ідеальним вибором для реалізації даного проєкту.

Можна визначити наступні моделі плат мікроконтролерів Arduino для розробки системи контролю доступу: Arduino Uno; Arduino Nano; Arduino Mega; Arduino Leonardo; ESP8266/ESP32. Arduino Uno – це класична плата з достатньою кількістю входів/виходів для більшості завдань. Arduino Nano – це компактна версія, зручна для вбудованих рішень. Arduino Mega має більше портів вводу/виводу, що підходить для систем керування доступом з великою кількістю пристроїв. Arduino Leonardo може емулювати клавіатуру або мишу, що корисно при роботі з ПК. Пристрої ESP8266/ESP32 сумісні з Arduino IDE, забезпечують вбудований Wi-Fi та Bluetooth для реалізації бездротових функцій.

Розглянемо модулі та периферія для систем контролю доступу:

– RC522 – це ефективний RFID-зчитувач;

– 4×4 Keypad – це клавіатура для введення PIN-коду;

– R305 або GT-521F – це біометричні сканери відбитків пальців;

– Relay Module – це керування електрозамками;

– LCD/OLED дисплеї – це відображення повідомлень користувачу;

– Bluetooth HC-05/HC-06 або Wi-Fi ESP8266/ESP32 – це реалізація бездротового зв’язку;

– датчики руху, кнопки, сигналізація, сирени – це додаткові пристрої безпеки СКД.

Таким чином, платформа Arduino дозволяє ефективно реалізувати повнофункціональні системи контролю доступу як у навчальних, так і в практичних проєктах. Його гнучкість і розширюваність роблять платформу ідеальним вибором для створення прототипу пристрою контролю доступу з можливістю подальшої модернізації або масштабування.

1.2 Проектування пристрою контролю доступу на базі Arduino

1.2.1 Порівняльний аналіз застосунків для розробки проєкту

Для розробки пристроїв на основі мікроконтролерів Arduino існує кілька популярних середовищ, які забезпечують проєктування, моделювання та налагодження електронних схем. У цьому підпункті проведено порівняльний аналіз найпоширеніших рішень для реалізації проєкту системи контролю доступу.

Інтегроване середовище Arduino IDE призначено для **с**творення, компіляція та завантаження програмного коду на фізичну плату Arduino та має широкий вибір бібліотек, а також підтримує різні моделі плат Arduino. Проте, недоліком такого середовища є **н**е підтримка процесу моделювання, тобто - потрібен реальний пристрій для тестування та підходить тільки для фінального етапу, коли вже зібрано фізичну схему.

Симулятор Wokwi є онлайн-симулятором Arduino, який дозволяє моделювати електронні схеми та виконувати код без фізичних пристроїв. Це основна його перевага. Крім цього цей симулятор працює в браузері та підтримує різні пристрої, наприклад, LCD, клавіатуру, сервомотор, зумери та

інші компоненти. Цей симулятор дозволяє візуально перевірити логіку роботи. Також він дозволяє зберігати та поширювати проєкти.

До його недоліків можна віднести: обмежена підтримка нестандартних або складних компонентів; не враховує фізичні обмеження (наприклад, шуми чи затримки реальних схем). Отже симулятор Wokwi підходить для початкового етапу розробки, тестування алгоритмів, демонстрацій та дистанційного навчання.

Симулятор Tinkercad Circuits використовує **о**нлайн-платформу для 3D-моделювання та симуляції електронних схем (підтримується Arduino). До його переваг слід віднести: простий інтерфейс; візуальна побудова схеми; інтеграція з кодом Arduino; вбудований монітор. Проте, до його недоліків слід віднести: обмежений набір компонентів; менш точне моделювання, ніж у Wokwi; не підтримує складні бібліотеки та великі проєкти.

Таблиця 1.2. Порівняльні показники ПЗ для розробки проєктів

Характеристика	Arduino IDE	Wokwi Simulator	Tinkercad Circuits
Тип середовища	Десктопна програма	Онлайн-симулятор	Онлайн-симулятор
Підтримка моделювання	Ні	Так	Так
Підтримка бібліотек	Повна	Обмежена	Обмежена
Підтримка складних схем	Так	Так	Ні
Потрібне обладнання	Так	Ні	Ні
Простота використання	Висока	Висока	Дуже висока
Освітнє застосування	Середнє	Високе	Високе

Отже, для розробки пристрою контролю доступу найбільш ефективним є поєднання середовищ:

- Wokwi – для моделювання схеми та перевірки алгоритму роботи (етап розробки і тестування);
- Arduino IDE – для прошивки та роботи з фізичною платою (етап впровадження);
- Tinkercad – як альтернативний варіант для початкового навчання або створення спрощених моделей.

Цей підхід забезпечує зручність, гнучкість і ефективність у всіх етапах реалізації проєкту.

1.2.2 Особливості розробки проєкту в симуляторі Wokwi

Для моделювання та тестування пристрою контролю доступу було використано онлайн-симулятор Wokwi (https://wokwi.com/) (рис. 2.1), який дозволяє створювати віртуальні схеми, писати код і виконувати симуляцію роботи Arduino-проєктів у браузері без необхідності використання фізичних компонентів.

Етапи створення проєкту в симуляторі Wokwi:

1. Реєстрація та створення нового проєкту.
2. Після реєстрації на сайті Wokwi створено новий проєкт типу Arduino Uno.
3. Додавання компонентів до схеми.
4. У графічному редакторі Wokwi були додані основні елементи системи:

– плата Arduino Uno;
– клавіатура 4×4;
– LCD-дисплей 16×2 з інтерфейсом I2C;
– сервопривід SG90;
– П’єзоелектричний зумер;
– кнопка для зміни пароля;

5. З'єднання компонентів: проведено віртуальне з’єднання елементів згідно зі схемою, яка відповідає реальному апаратному монтажу. Використано відповідні пін-коди для підключення клавіатури, дисплея, сервомотора та зумера.

6. Розробка та завантаження програмного коду: у вбудованому редакторі коду написано скетч, що реалізує логіку:

– введення та перевірку пароля;

– управління сервоприводом у разі правильного введення;

– подачу звукового сигналу на зумер;

– зміну пароля при натисканні спеціальної кнопки (наприклад, «A»).

7. Тестування логіки роботи: за допомогою інтерфейсу Wokwi проведено моделювання сценаріїв:

– введення правильного та неправильного пароля;

– відкриття та закриття замка;

– зміна пароля;

– індикація дій на дисплеї;

– звукове супроводження подій.

Можна визначити наступні переваги використання симулятора Wokwi:

– можливість швидко перевірити працездатність схеми без фізичних компонентів;

– зручне налаштування та повторне використання проєкту;

– швидке внесення змін у схему та код;

– візуалізація всіх дій у режимі реального часу.

Рисунок 1.15. Етапи створення проекту в симуляторі Wokwi

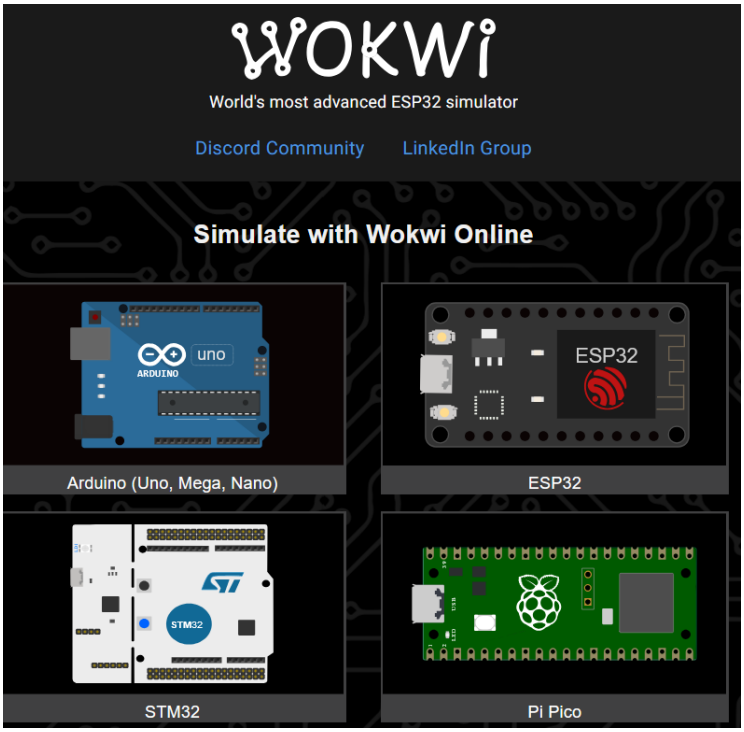


Рисунок 1.16. Інтерфейс середи проєктування симулятора Wokwi

На рис. 1.17 наведено середа симулятора Wokwi для вибору компонентів для проєкту.

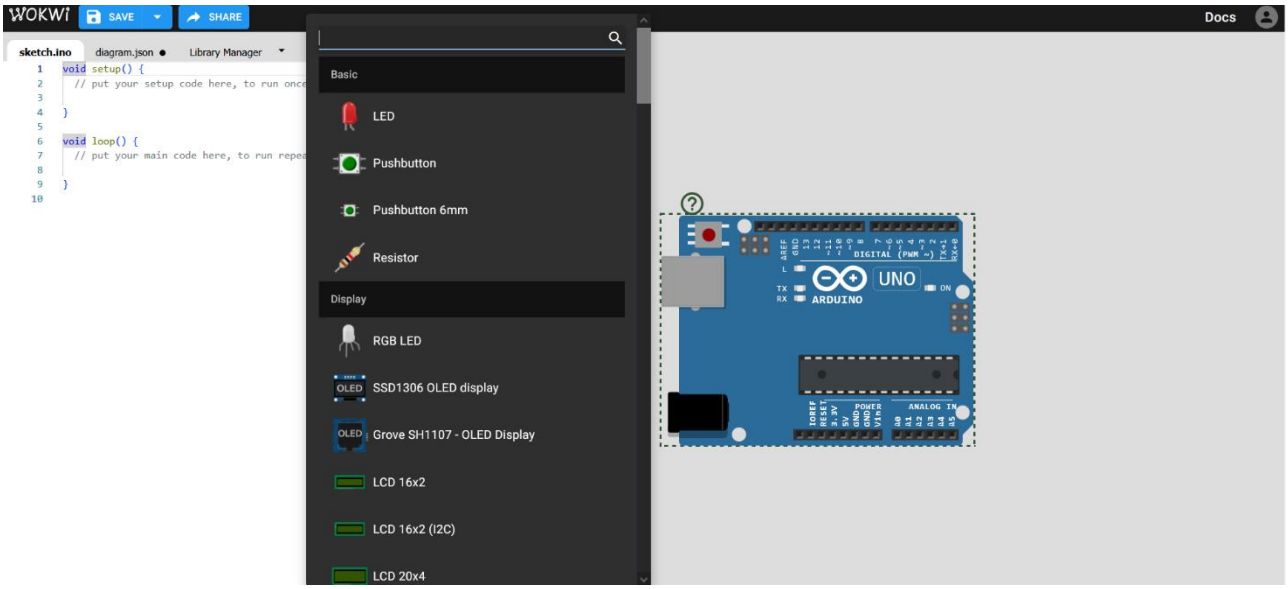


Рисунок 1.17. Вибір компонентів для проєкту в симуляторі Wokwi

Таким чином, використання симулятора Wokwi на етапі розробки значно прискорило процес тестування та налагодження пристрою. Створена модель повністю імітує роботу реального пристрою, що дало змогу переконатися у правильності реалізованих рішень до етапу фізичної збірки.

1.3 Розробка системи пристрою контролю доступу на територію

1.3.1 Розробка технічного завдання пристрою контролю доступу

Метою проєкту є розроблення функціонального макету пристрою контролю доступу до приміщення або обмеженої території, що працює на базі мікроконтролера Arduino з використанням клавіатури, дисплея, сервопривода та звукової сигналізації. Система повинна забезпечувати ідентифікацію користувача за кодом та можливість зміни пароля без програмування.

Система повинна виконувати наступні функції:

1) Прийом введеного пароля з 4-клавішної цифрової клавіатури.

2) Відображення інформації на LCD-дисплеї 16x2 (інструкції, статус доступу, введення пароля).

3) Управління сервоприводом для моделювання відкриття/закриття замка.

4) Відтворення звукових сигналів через зумер:

- позитивний сигнал при успішному вході;
- негативний сигнал при помилці.

5) Реалізація режиму зміни пароля за запитом користувача (натискання клавіші 'A'):

- введення старого пароля;
- введення нового пароля;
- підтвердження успішної зміни.

6) Затримка перед автоматичним закриттям замка після успішного відкриття.

7) Захист від несанкціонованого доступу (після декількох помилок — звукова сигналізація або тимчасове блокування, якщо потрібно).

Технічні вимоги до пристрою системи керування доступом надано в табл. 3.1.

Вимоги до програмного забезпечення наступне:

1) програма повинна бути написана в середовищі Arduino IDE;

2) повинна включати модулі: введення з клавіатури; виведення на дисплей;

3) управління сервоприводом;

4) обробка логіки зміни пароля;

5) генерація звукових сигналів.

В табл. 3.1 представлені технічні вимоги до системи контролю доступом підприємства.

Таблиця 1.3. Технічні вимоги до системи контролю доступом підприємства

Компонент схеми проєкта	Назва компонента
Мікроконтролер	Arduino Uno або Arduino Mega
Клавіатура	4x4 матрична клавіатура
Дисплей	LCD 16x2 з інтерфейсом I2C
Привід	Сервомотор типу SG90 або аналог
Звуковий пристрій	П’єзоелектричний зумер
Енергоживлення	220В - 9В постійного струму
Програмування	Arduino IDE, мова C++
Середовище для моделювання	Wokwi (віртуальна симуляція)

Розглянемо додаткові умови до розробляємого проєкту:

1) можливість запуску та тестування у симуляторі Wokwi;
2) опціонально: додати EEPROM для збереження пароля після вимкнення живлення.

Очікуваний результат віл реалізації проєкту:

1) функціонуючий пристрій або віртуальна модель;
2) програмний код;
3) електрична схема підключення компонентів;
4) текстова документація проєкту.

1.3.2 Опис компонентів пристрою контролю доступу

Для вашого проекту Arduino Uno цілком підходить, оскільки він має достатньо можливостей для роботи з клавіатурою, дисплеєм, сервоприводом та звуковим сигналом. Ось кілька факторів, які можна взяти до уваги при виборі між Arduino Uno та Arduino Mega.

Плата мікроконтролера Arduino Uno має 14 цифрових пінів (6 з яких можуть бути використані для PWM) і 6 аналогових пінів. Пам'ять складає 32 KB флеш-пам'яті для зберігання програми та 2 KB SRAM для зберігання змінних. Ресурсів плати достатньо для проекту з клавіатурою 4x4, LCD дисплеєм,

сервоприводом і п’єзо-біпером. Застосування цього мікроконтролеру дозволяє легше налаштувати та розробляти для маленьких проектів. На рис. 3.1 надано зовнішній вид плати мікроконтролера Arduino Uno.

Рисунок 1.18. Вигляд плати мікроконтролера Arduino Uno

Звуковий пристрій на основі п’єзоелектричного зумеру – це простий електронний пристрій, який створює звуковий сигнал при подачі керуючого сигналу з мікроконтролера. Він використовується для звукового супроводу дій користувача в системі контролю доступу. Розглянемо його основні характеристиками. Він може бути активним або пасивним. Його робоча напруга складає в межах 3–5 В. Робоча частота може бути в межах 1–5 кГц та залежить від частоти керуючого сигналу. Для підключення використовуються 2 виводи (VCC і GND) та керується через ШІМ-сигнал або просто HIGH/LOW. На рис. 3.2 представлено зображення цього зумера.

Зумер покращує зручність користування пристроєм, забезпечуючи аудіозворотній зв'язок, що особливо важливо в умовах низької видимості або для користувачів з вадами зору.

Функціональне призначення його наступне:

1) сигнал про успішне введення пароля (короткий позитивний сигнал);
2) сигнал про помилку (низький тривалий або подвійний сигнал);
3) звуковий супровід при натисканні клавіш або зміні пароля.

Рисунок 1.19. Вигляд зумера

Сервомотор SG90 є компактним і легким приводом, який широко використовується в проєктах на основі Arduino для імітації механічних замків або рухомих частин пристроїв. Основні характеристики сервомотор SG90 наступні: тип з обмеженим кутом повороту; кут обертання 0–180°; напруга живлення складає 4.8–6 В; споживання струму приблизно 500 мА при навантаженні; інтерфейс має 3 дроти (живлення +5В, GND, сигнальний). Сервомотор використовується для механічного відкривання та закривання доступу (наприклад, імітації замка або засувки) після успішного введення пароля. Положення сервопривода змінюється залежно від результату перевірки коду – відкриття при правильному паролі та повернення у вихідне положення після затримки. Зовнішній вид сервомотору SG90 надано на рис. 3.3.

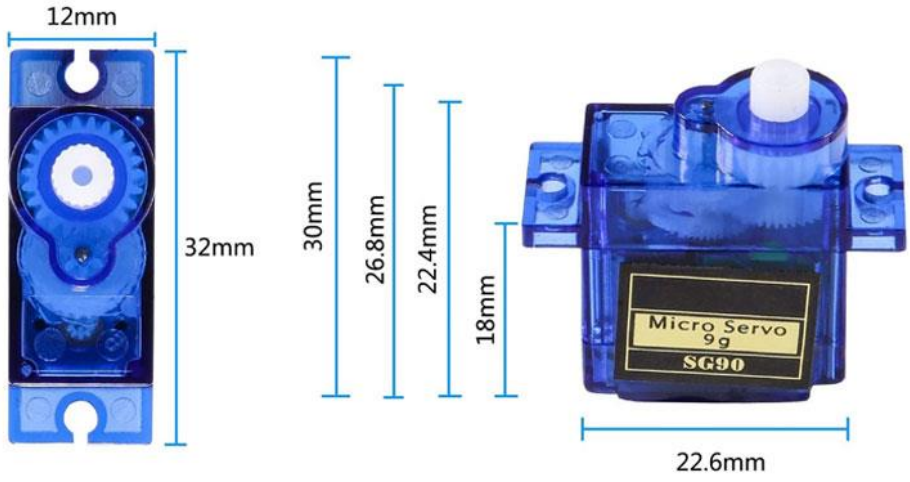


Рисунок 1.20. Зовнішній вид сервомотору SG90

Матрична клавіатура 4x4 складається з 16 кнопок, розміщених у вигляді 4 рядків і 4 стовпців. Кожне натискання кнопки замикає відповідну пару рядок-

стовпець, дозволяючи мікроконтролеру визначити, яка клавіша була натиснута. Основні характеристики наступні: кількість клавіш: 16 (0–9, A–D, *, #); інтерфейс: 8 виводів (4 рядки + 4 стовпці); напруга живлення: 3.3–5 В. Перевагами матричної клавіатури наступні компактність, надійність, просте підключення. Клавіатура використовується для введення пароля користувачем та ініціації зміни пароля через кнопку ‘A’. На рис. 3.4 надано зовнішній вид матричної клавіатури.

Дисплей LCD 16x2 з інтерфейсом I2C – це рідкокристалічний дисплей, здатний виводити до 16 символів у двох рядках. У поєднанні з I2C-модулем (адаптером для двопровідного з'єднання) він забезпечує просте та ефективне підключення до мікроконтролера Arduino з мінімальною кількістю проводів.

Основні характеристики дисплею наступні: формат відображення: 16 символів × 2 рядки; напруга живлення: 5 В; інтерфейс з Arduino: I2C (2 дроти – SDA і SCL); адреса I2C: 0x27 або 0x3F; підсвічування: наявне (регулюється або вимикається); контрастність: налаштовується потенціометром.

Рисунок 1.21.Зовнішній вид матричної клавіатури

Функціональне призначення дисплею наступні:

1) виведення підказок для користувача (наприклад, “Введіть пароль”, “Пароль прийнято”, “Невірний пароль”);

2) індикація режиму (звичайний, зміна пароля тощо);

3) підтвердження виконання операцій у реальному часі.

Переваги використання інтерфейсу I2C наступні: зменшення кількості підключень з 6–8 до 2; збереження цифрових входів/виходів Arduino для інших компонентів; простота програмування за допомогою бібліотек LiquidCrystal_I2C. Дисплей значно покращує взаємодію користувача з пристроєм, забезпечуючи візуальний інтерфейс та зворотний зв'язок у процесі контролю доступу. На рис. 3.5 представлено зовнішній вигляд дисплею LCD 16x2 з інтерфейсом I2C.

Рисунок 1.22.Зовнішній вигляд дисплею LCD 16x2 з інтерфейсом I2C

1.3.3 Розробка схеми пристрою контролю доступу

Система контролю доступу на базі Arduino Uno реалізована з використанням кількох основних компонентів: матричної клавіатури 4x4, LCD-дисплея 16x2 з інтерфейсом I2C, сервомотора SG90, п’єзоелектричного зумера та джерела живлення 9 В. Центральним елементом схеми є плата Arduino Uno, яка керує усіма модулями системи. Вона приймає дані з клавіатури, обробляє

введену інформацію, керує індикацією на дисплеї, положенням сервоприводу та звуковою сигналізацією.

Клавіатура 4x4 підключена до цифрових входів Arduino (наприклад, D2–D9). Ця клавіатура служить для введення пароля. Кожна клавіша формує замикання певного рядка й стовпця матриці, що зчитується програмою.

LCD-дисплей 16x2 з інтерфейсом I2C підключається до виводів A4 (SDA) і A5 (SCL) Arduino. Він використовується для виведення підказок, повідомлень про статус введеного пароля та підтвердження зміни режиму (наприклад, “Пароль змінено”).

Сервомотор SG90 підключений до виводу D10 Arduino. Він виконує функцію відкриття або блокування доступу (наприклад, поворотом "замка"). При правильному введенні пароля сервомотор обертається на заданий кут, відкриваючи доступ.

П’єзоелектричний зумер підключений до виводу D11, зумер сигналізує про дії користувача: короткий звуковий сигнал – це підтвердження натискання клавіші; довгий або подвійний сигнал – це помилка або неправильний пароль; серія коротких сигналів – це успішна авторизація.

Для автономної роботи пристрій живиться від зовнішнього блоку живлення 9 В, 1 А, підключеного до стандартного роз’єму живлення Arduino. Вбудований стабілізатор напруги Arduino забезпечує напругу 5 В для всіх компонентів.

Загальна логіка роботи схеми контролю наступна:

1) користувач вводить пароль з клавіатури;

2) на дисплеї з’являється відповідне повідомлення;

3) якщо пароль правильний, то сервопривід відкриває доступ і подається звуковий сигнал;

4) якщо пароль неправильний, то виводиться помилка, подається інший звуковий сигнал;

5) натиснення спеціальної клавіші (наприклад, "A") дозволяє увійти в режим зміни пароля;

6) система дозволяє зберегти новий пароль до енергонезалежної пам’яті (EEPROM).

Усі підключення повинні бути виконані згідно з документацією на компоненти, а лінії живлення бажано продублювати фільтрами або конденсаторами для стабільної роботи сервомотора.

Розглянемо схема підключення компонентів до плати Arduino Uno для проєкту системи контролю доступу на основі клавіатури, дисплея, сервомотора та зумера.

Клавіатура 4x4 (матриця 4 рядки × 4 стовпці) підключається до цифрових входів D2–D9 згідно табл. 1.4.

Схема підключення LCD дисплея 16x2 з інтерфейсом I2C до пінів плати мікроконтролера Arduino Uno надана в табл. 1.5.

Таблиця 1.4. Схема підключення клавіатури 4x4 до пінів Arduino Uno

Контакт клавіатури	Пін Arduino Uno
Row 1 (R1)	D2
Row 2 (R2)	D3
Row 3 (R3)	D4
Row 4 (R4)	D5
Column 1 (C1)	D6
Column 2 (C2)	D7
Column 3 (C3)	D8
Column 4 (C4)	D9

Таблиця 1.5. Схема підключення LCD дисплея 16x2 з інтерфейсом I2C

Контакт дисплея	Пін Arduino Uno
VCC	5V
GND	GND
SDA	A4
SCL	A5

Підключення сервомотору SG90 до пінів плати мікроконтролера Arduino Uno надано в табл. 1.6.

Таблиця 1.6. Схема підключення сервомотору SG90

Контакт сервоприводу	Пін Arduino Uno
GND	GND
VCC (5V)	5V
Signal	D10

Слід відзначити, що якщо сервопривід працює нестабільно, потрібно живіть його окремо від Arduino через стабілізатор на 5 В.

П’єзоелектричний зумер підключається до пінів D2 та GND.

Блок живлення 9 В 1 А підключається до роз’єму DC power на Arduino Uno або через контакт Vin + GND, якщо використовуєте джерело без роз’єму.

Підсумок використовуваних пінів Arduino Uno наведено в табл. 1.7.

Таблиця 1.7.Загальна схема підключення компонентів пристрою керування доступу

Компонент	Використані піни
Клавіатура	D2–D9
LCD (I2C)	A4 (SDA), A5 (SCL)
Сервомотор	D10
Зумер	D11
Вільні піни	D0, D1, D12, D13, A0–A3

На рис. 1.23 представлена схема пристрою контролю доступу, яка була спроєктована в симуляторі Wokwi.

Алгоритм роботи пристрою контролю доступу наступний:

1. Спочатку виконується початкове налаштування, яке полягає в наступному:

– встановлюється початковий пароль (наприклад, "1234");

– ініціалізується: LCD-дисплей; клавіатура; сервопривід у закритому стані; біпер

– на дисплеї виводиться: "Введіть пароль:".

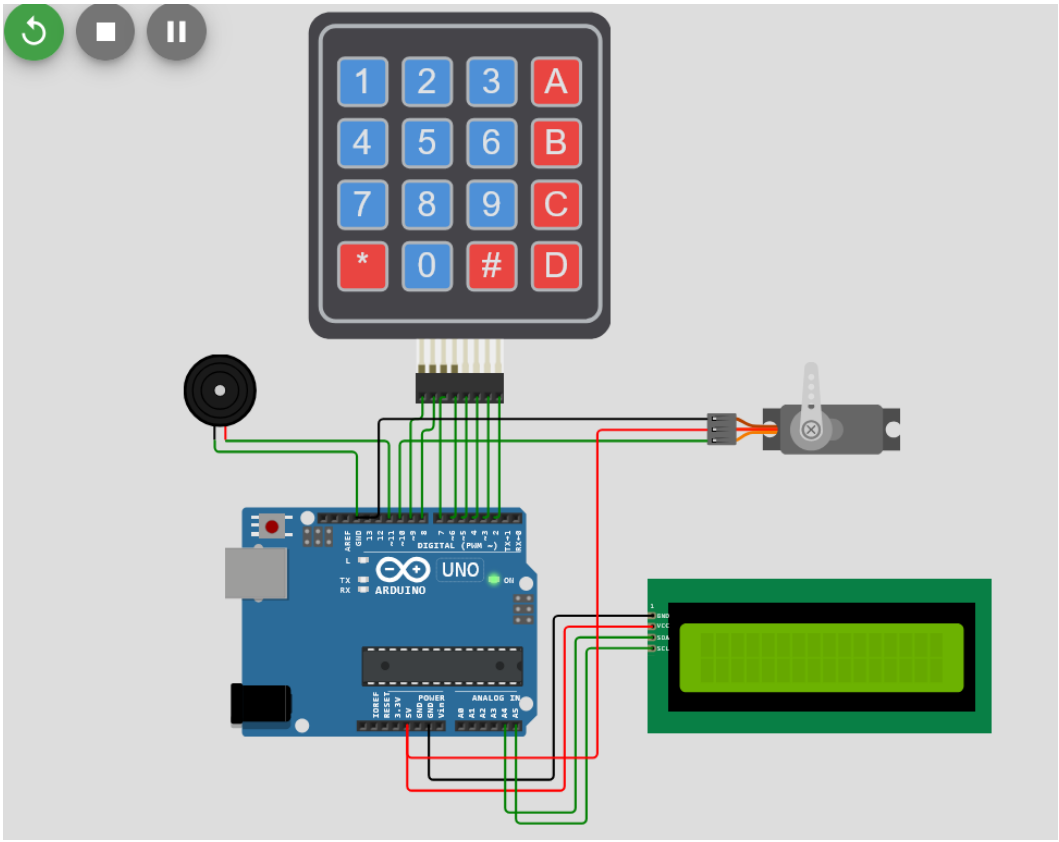


Рисунок 1.23. Схема пристрою контролю доступу, яка була спроєктована в симуляторі Wokwi

2. Далі водиться пароль користувачем:

- користувач вводить 4 цифри з клавіатури;
- після кожного введення на екрані відображається *;
- після введення 4 цифр:
  - Якщо пароль вірний:
    - На дисплеї – "Пароль вірний";
    - Звучить сигнал успіху;
    - Сервопривід повертається у відкриту позицію (наприклад, 90°);
    - Через 5 секунд – закривається назад (0°);
    - Знову виводиться "Введіть пароль";
  - Якщо пароль невірний:
    - На дисплеї — "Невірний пароль";
    - Звучить сигнал помилки;
    - Знову запитується пароль.

3. Зміна пароля (натискання A) полягає в наступному:

- Якщо користувач натискає клавішу A:
    1. На дисплеї з’являється: "Старий пароль:"
    2. Користувач вводить чинний пароль:
        - Якщо вірно:
            - На дисплеї – "Новий пароль:"
            - Користувач вводить новий 4-значний пароль
            - На дисплеї – "Пароль змінено"
            - Сигнал успіху
        - Якщо невірно:
            - Повідомлення: "Доступ заборонено"
            - Сигнал помилки
            - Повернення до режиму введення

Безпека системи керування доступом полягає в наступному:

– Пароль зберігається в оперативній пам’яті (не EEPROM), тож втрачається після перезавантаження, якщо не реалізовано збереження.

– Можна реалізувати додаткову перевірку на довжину, обмеження спроб, блокування пристрою тощо.

1.3.4 Розробка програмного забезпечення пристрою контролю доступу

Програмне забезпечення (ПЗ) для пристрою контролю доступу реалізовано на мові програмування C++ із використанням середовища Arduino IDE. Основне завдання ПЗ — забезпечити взаємодію між користувачем і системою: введення пароля, перевірка коректності, відкриття доступу, подання звукових та візуальних сигналів, а також можливість зміни пароля.

Структура програми наступна. Програма умовно поділяється на такі основні блоки:

1. Ініціалізація компонентів:
    - підключення бібліотек (Keypad, LiquidCrystal_I2C, Servo).
    - визначення пінів для клавіатури, дисплея, зумера, сервомотора.

- ініціалізація LCD-дисплея, встановлення кута сервомотора у вихідне положення (закрито).

2. Головний цикл (loop) виконує:
   - зчитування натискань клавіш.
   - формування введеного пароля.
   - перевірку правильності введення.
   - управління сервоприводом і зумером.
   - виведення інформації на дисплей.
3. Режим зміни пароля:
   - активація по натисканню спеціальної клавіші (наприклад, A).
   - перевірка старого пароля.
   - прийом нового пароля, його підтвердження.
   - запис нового пароля у змінну EEPROM (або оперативну пам’ять, залежно від реалізації).
4. Функціональні підпрограми (функції):
   - checkPassword() — перевіряє правильність введеного пароля.
   - unlockDoor() — активує сервомотор і відкриває доступ.
   - lockDoor() — повертає сервопривід у вихідне положення.
   - beepSuccess(), beepError() — подають звукові сигнали.

Особливості програмного забезпечення полягають в наступному: дозволяє легко змінювати довжину пароля, пін-коди, повідомлення на дисплеї; не зберігає пароль у відкритому вигляді у виводах дисплея; реалізований інтуїтивно зрозумілий режим зміни пароля без потреби перепрошивати контролер; можливість доповнення іншими модулями (зчитувач RFID, GSM, Bluetooth тощо).

Приклад логіки роботи пристрою:

1. Користувач вводить пароль;
2. Якщо пароль правильний: доступ відкривається (сервомотор повертається); лунає короткий сигнал; на дисплеї повідомлення «Доступ надано»;

3. Якщо пароль неправильний: лунає подвійний сигнал помилки; виводиться повідомлення «Невірний код»;
4. При натисканні A користувач входить у режим зміни пароля.

Програмне забезпечення схеми керування доступом має наступний вид:

```
#include <Keypad.h>
#include <Wire.h>
#include <LiquidCrystal_I2C.h>
#include <Servo.h>

LiquidCrystal_I2C lcd(0x27, 16, 2);

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

String password = "1234"; // Початковий пароль
String input = "";
bool changingPassword = false;
bool confirmOld = false;

Servo lockServo;
```

```
const int servoPin = 10;
const int buzzerPin = 11;

void setup() {
  lcd.init();
  lcd.backlight();
  lcd.setCursor(0, 0);
  lcd.print("Access system");
  delay(2000);
  lcd.clear();

  pinMode(buzzerPin, OUTPUT);
  lockServo.attach(servoPin);
  lockServo.write(0); // Закритий стан
}

void loop() {
  char key = keypad.getKey();
  if (key) {
    tone(buzzerPin, 2000, 100); // Короткий сигнал при кожному натисканні

    if (key == 'A') {
      lcd.clear();
      lcd.print("Change password");
      tone(buzzerPin, 3000, 150);
      delay(1000);
      lcd.clear();
      lcd.print("Enter the old one:");
      input = "";
      changingPassword = true;
```

```
  confirmOld = true;
  return;
 }

 if (key == '#') {
  if (!changingPassword) {
   if (input == password) {
    lcd.clear();
    lcd.print("Access allowed");
    tone(buzzerPin, 1000, 100);
    delay(100);
    tone(buzzerPin, 2000, 100);
    lockServo.write(90); // Відкриваємо замок
    delay(3000);
    lockServo.write(0); // Закриваємо
   } else {
    lcd.clear();
    lcd.print("Access denied");
    tone(buzzerPin, 500, 600); // Помилка
   }
   delay(2000);
   lcd.clear();
   input = "";
  } else {
   if (confirmOld) {
    if (input == password) {
     lcd.clear();
     lcd.print("New password:");
     tone(buzzerPin, 1500, 200);
     input = "";
```

```
        confirmOld = false;
      } else {
        lcd.clear();
        lcd.print("Password is incorrect.");
        tone(buzzerPin, 400, 600);
        delay(2000);
        lcd.clear();
        changingPassword = false;
        input = "";
      }
    } else {
      password = input;
      lcd.clear();
      lcd.print("Password changed");
      tone(buzzerPin, 1800, 100);
      delay(100);
      tone(buzzerPin, 2200, 100);
      delay(2000);
      lcd.clear();
      changingPassword = false;
      input = "";
    }
  }
} else if (key == '*') {
  input = "";
  lcd.clear();
  lcd.print("Скинуто");
  tone(buzzerPin, 2500, 150);
  delay(1000);
  lcd.clear();
```

```
    } else {
      if (input.length() < 10) {
        input += key;
        lcd.setCursor(0, 0);
        lcd.print("Entered: ");
        lcd.print(input);
      }
    }
  }
}
```

Проєкт представлений за наступним посиланням: https://wokwi.com/projects/431482494751180801

1.3.5 Тестування працездатності пристрою керування доступом

Після завершення етапів розробки апаратної частини та програмного забезпечення системи контролю доступу було проведено тестування пристрою з метою перевірки його функціональності, стабільності та відповідності технічним вимогам. Мета тестування полягає в наступному: перевірка правильності роботи клавіатури для введення пароля; перевірка виведення повідомлень на LCD-дисплей; оцінка реакції сервомотора при правильному та неправильному паролі; перевірка роботи зумера як індикатора дій користувача; тестування функції зміни пароля.

Розглянемо методику тестування:

1. Первинне увімкнення пристрою: перевірено, що при подачі живлення на дисплеї з’являється привітальне повідомлення та запрошення ввести пароль;
2. Введення вірного пароля: введено пароль за замовчуванням 1234 (рис. 3.8):

   – сервомотор повернувся у положення «доступ відкрито» (рис. 3.8);

   – зумер коротким сигналом підтвердив успішне введення;

   – дисплей показав повідомлення про відкриття доступу.

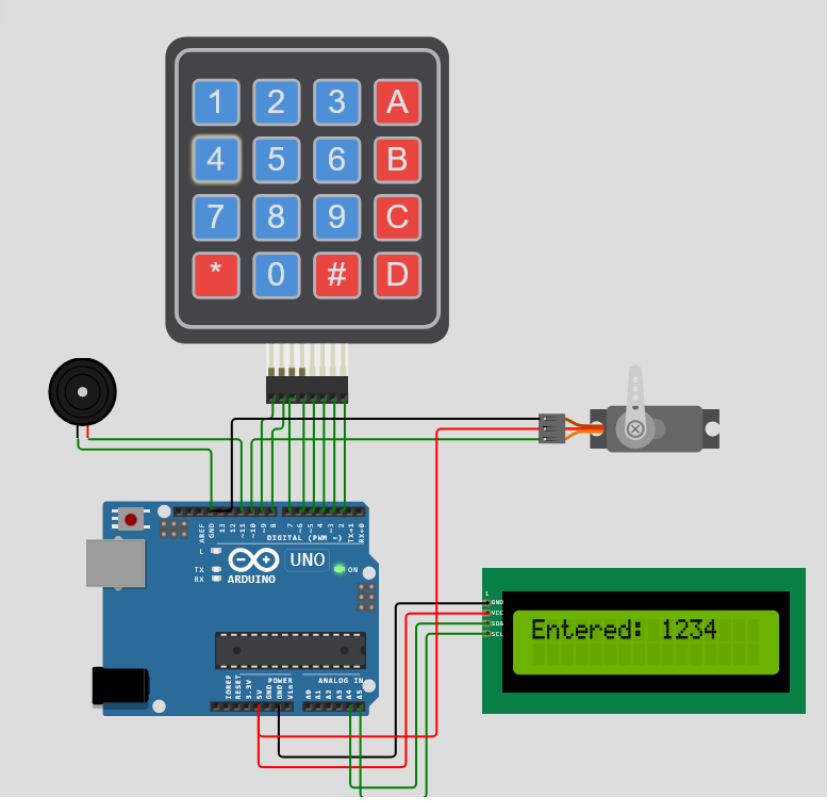


Рисунок 1.24. Введення вірного пароля за замовчуванням 1234

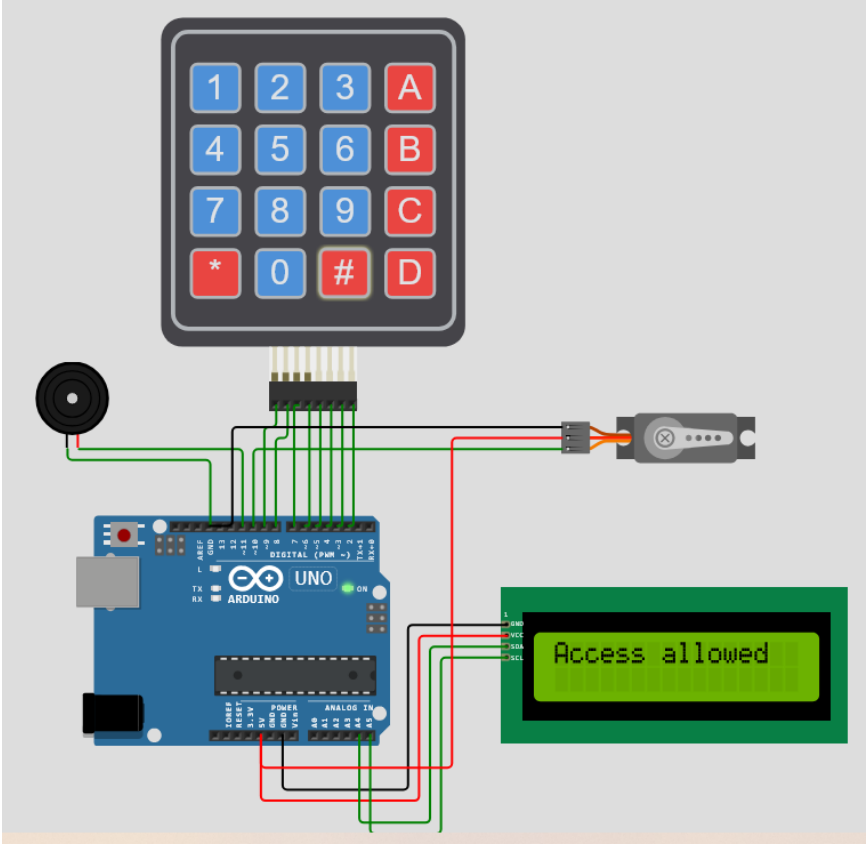


Рисунок 1.25. Сервомотор повернувся у положення «Доступ відкрито»

3. Введення неправильного пароля. Було кілька спроб введення неправильного пароля:

– сервомотор залишився у закритому положенні;

– зумер видав кілька коротких сигналів;

– на дисплеї з’явилося попередження про помилку.

4. Зміна пароля:

– натиснута спеціальна клавіша (наприклад, A) для входу в режим зміни пароля (рис. 2.10);

– система запитала старий пароль;

– після правильного введення старого пароля запропоновано ввести новий (рис. 2.10). Новий пароль був збережений, повторна авторизація проходила вже з новим паролем.

1. Робота сервомотора: перевірено, що після відкриття доступу сервопривід автоматично повертається у вихідне положення через встановлений інтервал часу.

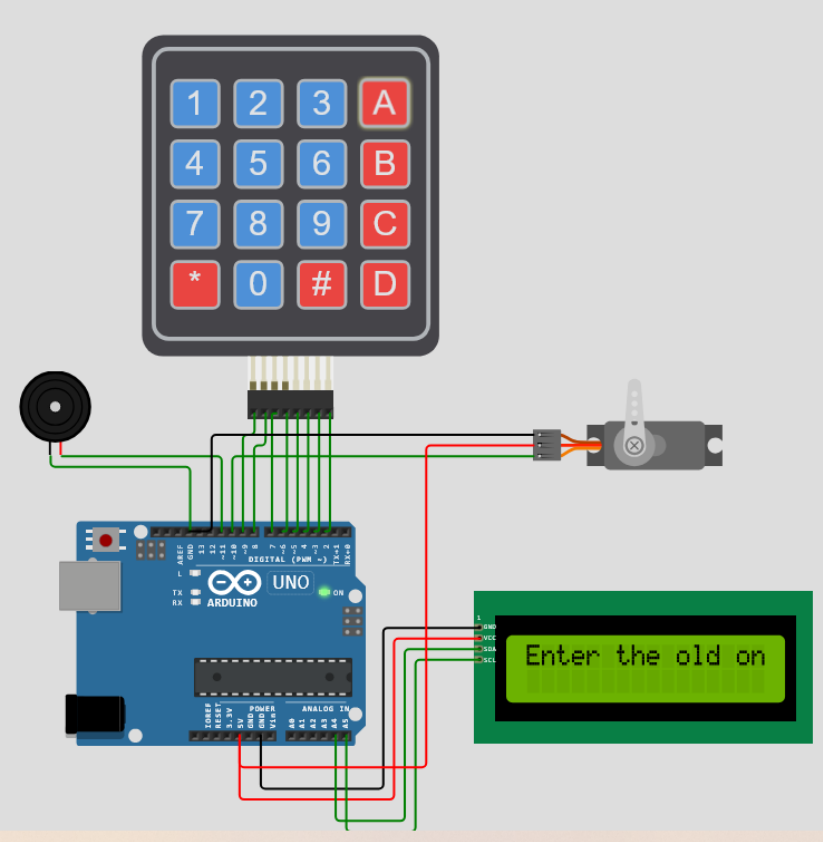


Рисунок 1.26. Режим зміни пароля – натиснута спеціальна клавіша A

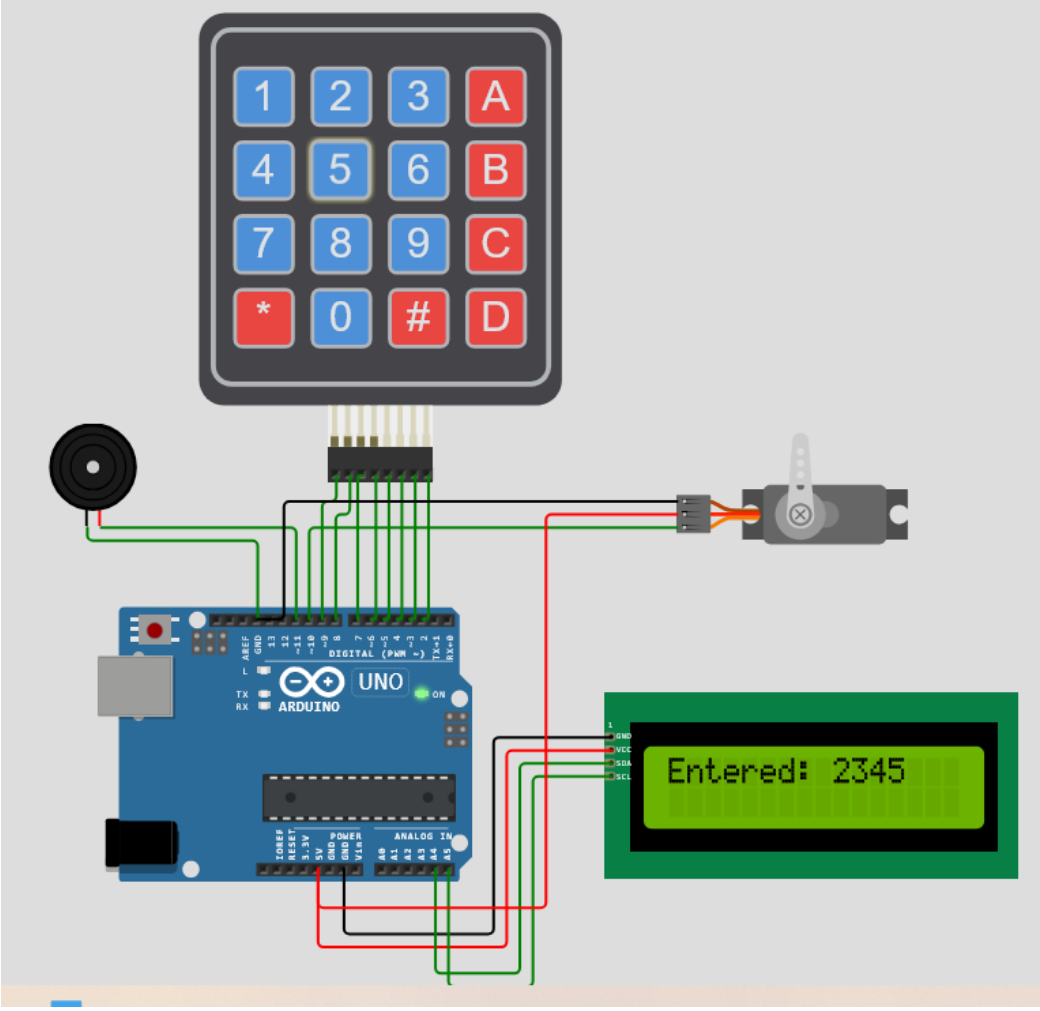


Рисунок 1.27.Зміна старого пароля 1234 на новий 2345

Таким чином, можна зробити висновок, що усі компоненти пристрою працюють відповідно до заданих функцій. Реакція на введення, сигнали зумера та положення сервомотора коректно відповідають на дії користувача. Система забезпечує базовий рівень доступу з можливістю зміни пароля.

2 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою даних розрахунків є обчислення вартості виконання науково-дослідної розробки «Розробка пристрою контролю доступу на територію на базі платформи Arduino».

Даний вид проекту відноситься до науково-дослідницької розробки. Оцінка якості розробленого проекту включає визначення трудомісткості і вартості його створення. Перелік етапів і робіт, що виконуються при проведенні НДР, приведений в таблиці 2.1.

Таблиця 2.1. Розподіл робіт по етапах і видах виконавців

Етап проведення НДР	Вигляд робіт	Посада виконавця
Розробка технічного завдання	1.Складання і затвердження ТЗ для НДР «Проектування комп'ютерно-телекомунікаційної мережі підприємства з мобільними об'єктами»	Дипломник, керівник
Вибір напряму дослідження	1. Збір і вивчення науково-технічної літератури, 2. Формулювання можливих напрямів вирішення завдань, поставлених в технічному завданні НДР і їх порівняльна оцінка. 3. Розробка плану проведення досліджень для подальшої розробки.	Дипломник керівник
Теоретичні і експериментальні дослідження	1. Аналіз існуючих рішень у галузі доступу на основі мікроконтролерів 2. Огляд можливостей платформи Arduino для реалізації подібних пристроїв 3. Проєктування пристрою контролю доступу на базі Arduino 4. Розробка системи пристрою контролю доступу на територію.	Теоретичні і експериментальні дослідження

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. 2. Оцінка повноти вирішення поставлених завдань. 3. Складання і оформлення звіту. Розгляд результатів НДР і прийняття результатів в цілому.	Дипломник керівник консультант

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

Таблиця 2.2.Очікувана трудомісткість робіт

Вигляд роботи	Очікуваний час виконання (дні)
1. Складання і затвердження ТЗ для НДР по розробці «Розробка пристрою контролю доступу на територію на базі платформи Arduino»	1
2. Збір і вивчення технічної літератури та документації	4
3. Формулювання можливих напрямів вирішення завдань, поставлених в технічному завданні НДР і їх порівняльна оцінка.	2
4. Розробка плану проведення досліджень для подальшої розробки.	3
5. Аналіз існуючих рішень у галузі доступу на основі мікроконтролерів	4
6. Огляд можливостей платформи Arduino для реалізації подібних пристроїв	4
7 . Проєктування пристрою контролю доступу на базі Arduino	4
8. Розробка системи пристрою контролю доступу на територію.	4
Всього:	26

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

1. Витрати на матеріали – 310 грн.

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

$$Зден = п.т.с. * 8;$$

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

8 – тривалість робочого дня,год.

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

Таблиця 2.3 Витрати на основну заробітну плату.

Виконавець	Погодинна тарифна ставка, грн	Денна ставка, грн	Трудомісткість робочих днів	Сума основної зарплати,грн
Дипломник	48,00	364	26	8528,00
Керівник	100,00	800	1	800,00
Консультант по економіч. частині.	100,00	800	0,25	200,00
Консультант по охороні праці	100,00	800	0,25	200,00
Нормоконтроль	100,00	800	0,25	200,00
Всього (Зо)				9928,00

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

Зд=0,12* Зо = 0,12* 9928,00= 1191,36 грн

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

Зєсв=0,22*(Зо+Зд)=0,22*(9928,00+ 1191,36) = 2446,26 грн..

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

Рнакл= (З0+Зд)*0,5 = (9928,00+ 1191,36) * 0,5 = 5559,68 грн.

Ці складові формують повну картину фінансових витрат, пов'язаних зі створенням нової науково-технічної продукції. На підставі отриманих даних по окремих статтях витрат складена калькуляція планової собівартості.

Таблиця 2.4Калькуляція планової собівартості

Статті витрат	Сума, грн.
1. Матеріали	310,00
2. Основна заробітна плата	9928,00
3. Додаткова заробітна плата	1191,36
4. Відрахування до єдиного соціального внеску	2446,26
5. Накладні витрати	5559,68
Планова собівартість (Спл)	19435,30

Плановий прибуток визначений по формулі:

Ппл = 0,1*Спл=0,1*19435,30= 1943,50грн

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

Договірна ціна визначається по формулі:

Цндр = Спл + Ппл= 19435,30+ 1943,50= 21378,80 грн.

Ціну реалізації встановлюємо з урахуванням ПДВ

Цр = Цндр + ПДВ= 21378,80 + 21378,80 * 0,2 = 25654,60 грн.

3 РОЗДІЛ ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ

Охорона праці – це система правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних і лікувально-профілактичних заходів, спрямованих на створення безпечних умов праці та запобігання професійним ризикам.

Основні принципи охорони праці:

Правове регулювання – дотримання законодавчих норм та стандартів безпеки.

Гігієна праці – забезпечення комфортних умов робочого середовища (освітлення, температура, вентиляція).

Технічна безпека – запобігання аварійним ситуаціям через контроль стану обладнання.

Психологічна безпека – запобігання стресу та вигоранню, підтримка комфортного психологічного клімату.

Основні фактори ризику на робочому місці:

Фізичні – вплив шуму, вібрацій, температури, освітлення.

Хімічні – контакти з токсичними речовинами.

Біологічні – ризик інфекцій або небезпечного біологічного середовища.

Психологічні – нервове напруження, перевтома, стрес.

Засоби забезпечення охорони праці:

Ергономіка робочого місця – правильне розташування обладнання, якісні меблі та освітлення.

Захист працівників – використання спецодягу, засобів індивідуального захисту.

Навчання та інструктаж – регулярні тренінги з техніки безпеки.

Сучасний розвиток технічного та технологічного стану виробництва передбачає постійну автоматизацію та оптимізацію виробничих процесів. Сьогодні, напевно, важко уявити компанію, господарська діяльність в якій здійснювалась би без використання комп’ютерної техніки. Через масовий характер робіт, що виконуються працівниками за допомогою комп’ютера,

законодавством України чітко врегульовано норми та вимоги до використання комп'ютерної техніки на підприємстві, безпосередньо й охорона праці при роботі з комп'ютером.

3.1 Аналіз небезпечних і шкідливих факторів

Під час роботи з комп'ютером людина зазнає впливу низки негативних факторів, які можуть суттєво вплинути на її здоров'я. Сучасні дослідження підтверджують прямий зв'язок між тривалим використанням ПК і виникненням багатьох захворювань. Серед них – поступове погіршення зору, наліт біль у спині та ділянці шиї, а також дискомфорт у кистях, ліктях і плечових суглобах. Крім того, постійна робота за комп'ютером часто асоціюється з порушенням сну та виникненням хронічних головних болей.

До основних ознак синдрому комп'ютерного зору належать швидка втома очей, двоїння (диплопія), труднощі у сприйнятті кольорів і часте сльозоточивість. Окрім цього, надмірне використання комп'ютерних технологій може призвести до розвитку синдрому інтернет-залежності, який характеризується сильною психологічною залежністю від онлайн-середовища і втратою контролю над особистою діяльністю при тривалій роботі за ПК.

3.2 Гігієнічні вимоги до виробничого середовища

Санітарно-гігієнічні вимоги для співробітників організацій, які використовують комп'ютери та оргтехніку, регламентуються документом ДСанПіН 3.3.2-007-98 «Державні санітарні правила і норми. Гігієнічні вимоги до організації роботи з візуальними дисплейними терміналами електронно-обчислювальних машин». Цей норматив встановлює стандарти як для виробничих приміщень, де використовуються ПК, так і для організації й обладнання робочих місць. Зокрема, забороняється розміщувати робочі місця з ПЕОМ у підвальних приміщеннях та на цокольних поверхах. Для забезпечення комфортних умов, кожне робоче місце має мати площу не менше 6,0 м², а об'єм приміщення – не менше 20,0 м³. Також передбачено, що відстань між робочими місцями в одному ряду має становити щонайменше 2,5 м, а між рядами – не

менше 1,2 м. Для створення сприятливого мікроклімату стіни приміщень повинні фарбуватись у пастельні тони з коефіцієнтом відбиття світла у межах 0,5–0,6.

Таблиця 3.1. Санітарно-гігієнічні вимоги для програмістів

Параметри	Значення
Приводне та штучне освітлення	300-500 люкс
Рівень шуму	Не більше 65 дБ
Площа на один ПК	Не менш 6 $м^2$
Об'єм на один ПК	Не менш 20 $м^2$
Крісло Повітрообмін	Підйомно-поворотні з регулюванням висоти нахилу спинки Нормальний (провітрювання, вентиляція, кондиціонування)
Мікроклімат (оптимальні параметри)	Вологість 40-60% t^0 повітря зимою: +18 - +20^0 С; t^0 повітря влітку: +23 - +25С
Відстань до екрану монітора	50 – 70 см
Неперервний час роботи за ПК	Не більше 2-х годин, обов'язкові перерви
Спеціальні заходи	Комплексні вправи для м'язів тіла і очей, психологічне розвантаження

Освітлення

Приміщення, в яких встановлені персональні комп'ютери, повинні мати природне та штучне освітлення відповідно до ДБН В.2.5-28:2018 «Природне і штучне освітлення». Природне освітлення має здійснюватися через світлові прорізи, орієнтовані переважно на північ чи північний схід і забезпечувати коефіцієнт природною освітленості (КПО) не нижче ніж 1,5%. Штучне освітлення в приміщеннях з робочими місцями має здійснюватися системою загального рівномірного освітлення. У разі переважної роботи з документами, допускається застосування системи комбінованого освітлення. Зазначення освітленості на поверхні робочого столу в зоні розміщення документів має становити 300-500лк.

Вимоги до організації робочого місця працівника

Робоче місце – це спеціально відведена зона для виконання трудових функцій співробітника, яка оснащена усіма необхідними засобами для реалізації його посадових обов'язків. Організація робочого місця оператора комп'ютерного набору починається з обладнання його відповідною меблями, спеціалізованим

обладнанням та канцелярськими приладами. Базовий комплект меблів має включати:

- Канцелярський стіл з рухомою тумбою,
- Комп’ютерне крісло,
- Допоміжний стіл або підставку для оргтехніки,
- Шафу для зберігання документів,
- Сейф для зберігання документів, бланків, штампів та печаток,
- Стілець для відвідувачів.

Робоче сидіння або комп’ютерне крісло повинно складатися з сидіння, спинки та, за потребою, знімних чи стаціонарних підлокітників.

Основні характеристики сидіння:

- Ширина та глибина сидіння мають бути не менше 400 мм,
- Висота сидіння регулюється в межах 400–500 мм,
- Кут нахилу сидіння повинен варіюватися від 15° вперед до 5° назад,

Мікроклімат

Приміщення для роботи з персональними комп’ютерами повинні бути оснащені системами опалення, кондиціонування повітря або припливно-витяжною вентиляцією, що дозволяє забезпечити оптимальний мікроклімат для комфортної та безпечної роботи. В робочих зонах слід підтримувати задані нормативами параметри температури, відносної вологості та рухливості повітря згідно з вимогами ГОСТ 12.1.005-88 та СН 4088-86, як це ілюстровано у Таблиці 3.2.

Таблиця 3.2. Параметри мікроклімату в залежності від категорії робіт

Пора року	**Категорія робіт**	**Температура повітря (°C)**	**Відносна вологість (%)**	**Швидкість руху повітря (м/с)**
Холодна	Легка-1а	22 – 24	40 – 60	0,1
	Легка-1б	21 – 23	40 – 60	0,1
Тепла	Легка-1а	23 – 25	40 – 60	0,1
	Легка-1б	22 – 24	40 – 60	0,2

Крім того, санітарно-гігієнічні норми вимагають, щоб рівні позитивних і негативних іонів у повітрі відповідали стандартам, встановленим нормами № 2152-80. Детальні значення наведено в таблиці 3.3.

Таблиця 3.3. Рівні позитивних і негативних іонів у повітрі

Рівень	**Кількість іонів в 1 см³ повітря**
Мінімально необхідні	n^+: 400, n^-: 600
Оптимальні	n^+: 1500–3000, n^-: 3000–5000
Максимально допустимі	n^+: 50000, n^-: 50000

Забезпечення таких умов сприяє підвищенню рівня комфорту, зниженню ризиків для здоров’я користувачів і створенню сприятливого середовища для виконання робочих завдань.

3.3 Пожежна безпека

Пожежна безпека виробничих, складських і офісних будівель та приміщень — це система заходів, спрямована на збереження життя та здоров’я людей у разі аварійних ситуацій.

На робочих місцях для гасіння пожеж використовують вуглекислотні і порошкові вогнегасники. Вуглекислотні вогнегасники, такі як модель ВВК-5, випускаються у ручному форматі, а порошкові — в різних модифікаціях, наприклад, ВП-2, ВП-5, ВП-10 та інші. Ці пристрої повинні бути розміщені на вертикальних перегородках або стінах з використанням спеціальних кронштейнів, або встановлені в пожежних шафах. Крім того, механізми запуску і двері пожежних шаф обов’язково обладнуються захисними пломбами (див. рис. 3.1).

Рисунок 3.1. Пожежна шафа

ВИСНОВКИ

У ході виконання дипломної роботи було спроєктовано, розроблено та протестовано пристрій контролю доступу на базі апаратної платформи Arduino Uno. Основною метою проєкту було створення надійного, доступного та функціонального рішення для обмеження фізичного доступу до об’єктів за допомогою введення пароля через матричну клавіатуру.

У результаті виконання роботи було отримано:

1) Проведено аналіз сучасних систем контролю доступу, зокрема рішень на основі мікроконтролерів;

2) Обґрунтовано вибір платформи Arduino завдяки її відкритості, підтримці великої кількості периферії та простоті програмування;

3) Визначено технічні вимоги до пристрою та обрано відповідні компоненти: клавіатура 4×4, LCD-дисплей 16×2 з інтерфейсом I2C, сервомотор SG90, п’єзоелектричний зумер;

4) Розроблено електричну схему пристрою, програмне забезпечення з можливістю перевірки пароля та його зміни користувачем;

5) Проведено моделювання та тестування системи в середовищі Wokwi, яке підтвердило правильність логіки та працездатність усіх компонентів;

Пристрій може бути використаний як основа для розгортання більш складних систем безпеки, з можливістю інтеграції додаткових модулів – RFID, Bluetooth, GSM, датчиків руху тощо. Створений програмно-апаратний комплекс демонструє приклад ефективного використання мікроконтролерів у реальних задачах автоматизації доступу та підвищення фізичної безпеки об’єктів.

Отримані знання та практичний досвід у сфері проєктування вбудованих систем і систем контролю доступу можуть бути використані для подальших досліджень або впровадження в прикладні проєкти.

ПЕРЕЛІК ВИКОРИСТАНИХ ІНФОРМАЦІЙНИХ ДЖЕРЕЛ

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

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

3 Безсонова, А. О., & Василенко, О. Д. (2023). Застосування систем контролю доступу для різних типів підприємств.

4 Лапіна, Т. И., Лапін, Д. В., & Петрик, Е. А. (2013). Підхід до класифікації цифрових сигналів у системах контролю доступу. Інформаційно-вимірювальні та керуючі системи, 11(9), 058-064.

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

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

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

8 Arduino Create. [Електроний ресурс]. – Режим доступу: https://www.arduino.cc/en/main/create.

9 Asparuhova, K., Shehova, D., Asenov, S., Kanevski, H., & Parushev, A. (2024, September). Using WOKWI Simulator to Support Engineering Student Learning in Microcontrollers and Sensors. In *2024 XXXIII International Scientific Conference Electronics (ET)* (pp. 1-4). IEEE.

10 Яковенко,Т.К. (2024). Датчики руху на основі мікроконтролера Arduino в інтелектуальних системах безпеки.

ДОДАТОК А. Слайди мультимедійної презентації

ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ

РОЗРОБКА СИСТЕМИ БЕЗПЕКИ ПРИВАТНОГО СЕРЕДОВИЩА НА ПЛАТФОРМІ ARDUINO

ДИПЛОМНИЙ ПРОЕКТ

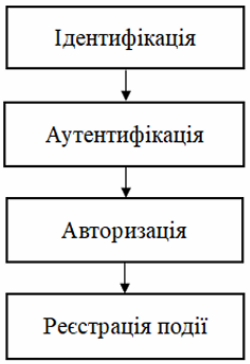
Керівник:
Стайкуца С.В.

Виконав:
Коротнян А.А.

Одеса - 2025

Класифікація систем контролю доступу

Система контролю доступу (СКД) – це комплекс технічних і програмних засобів, призначених для автоматизованого обмеження або дозволу доступу осіб до певної зони, об'єкта чи ресурсу.
Основною мета СКД – підвищення рівня безпеки шляхом ідентифікації користувачів та контролю за їх діями



Основні функції контролю доступу

Класифікація систем контроля доступу за базовими ознаками

Класифікація систем контролю доступу

Класифікація систем керування доступом

Основні характеристики автономних СКД

Переваги та недоліки мережевих СКУД

Мережева система контролю доступу – це тип СКД, яка підключена до комп'ютерної мережі, і керування всіма її елементами відбувається централізовано за допомогою спеціального програмного забезпечення

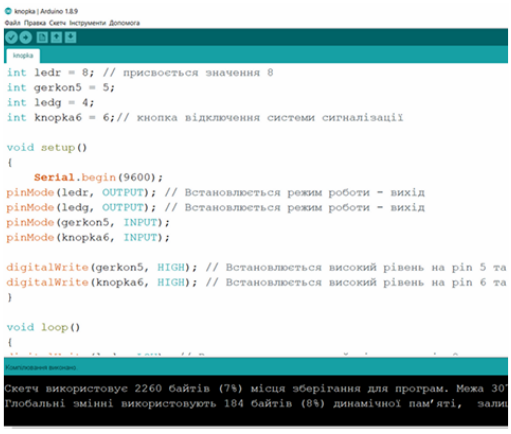
- *RFID-системи на базі Arduino*
- *Системи з клавіатурним вводом PIN-коду*
- *Біометричні системи (відбитки пальців)*
- *Bluetooth- або Wi-Fi-контроль доступу*
- *Комбіновані системи*

Найпоширеніші рішення на основі мікроконтролерів

Біометрична СКД на основі біометрії відбитки пальців

Bluetooth модуль HC-06 для реалізації СКД

Платформа Arduino є однією з найпопулярніших середовищ для розробки прототипів електронних пристроїв завдяки своїй відкритості, простоті використання та широкому асортименту сумісних модулів.



Інтерфейс середовища Arduino IDE

1. *Написання коду мовою програмування C/C++ із використанням специфічних бібліотек Arduino*
2. *Просте завантаження скетчів (програм) до мікроконтролера через USB*
3. *Наявність вбудованого монітора порту для перевірки передавання даних через UART*
4. *Величезна база бібліотек та прикладів, що значно спрощує розробку*
5. *Підтримка великої кількості апаратних платформ (Arduino Uno, Mega, Nano тощо*
6. *Можливість використання розширень та інтеграції з онлайн-сервісами (наприклад, Arduino Cloud, Wokwi)*

Можливості Arduino IDE

Порівняльний аналіз застосунків для розробки проєкту

Характеристика	Arduino IDE	Wokwi Simulator	Tinkercad Circuits
Тип середовища	Десктопна програма	Онлайн-симулятор	Онлайн-симулятор
Підтримка моделювання	Ні	Так	Так
Підтримка бібліотек	Повна	Обмежена	Обмежена
Підтримка складних схем	Так	Так	Ні
Потрібне обладнання	Так	Ні	Ні
Простота використання	Висока	Висока	Дуже висока
Освітнє застосування	Середнє	Високе	Високе

Порівняльні показники програмного забезпечення для розробки проєктів

Wokwi – для моделювання схеми та перевірки алгоритму роботи (етап розробки і тестування)

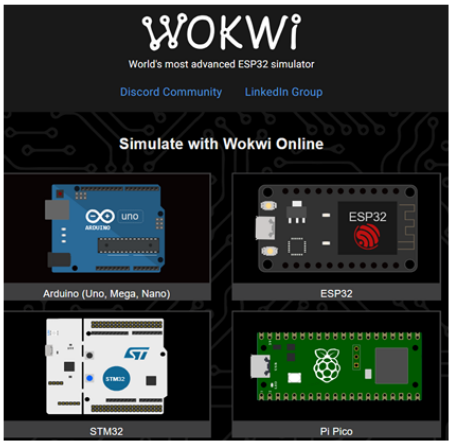
Arduino IDE – для прошивки та роботи з фізичною платою (етап впровадження)

Tinkercad – як альтернативний варіант для початкового навчання або створення спрощених моделей

Особливості розробки проєкту в симуляторі Wokwi

1. РЕЄСТРАЦІЯ ТА СТВОРЕННЯ НОВОГО ПРОЄКТУ
2. СТВОРЕННЯ ПРОЄКТУ ТИПУ ARDUINO UNO
3. ДОДАВАННЯ КОМПОНЕНТІВ ДО СХЕМИ
4. ДОДАВАННЯ ЕЕЛМЕНТІВ В ГРАФІЧНОМУ РЕДАКТОРІ WOKWI
5. З'ЄДНАННЯ КОМПОНЕНТІВ
6. РОЗРОБКА ТА ЗАВАНТАЖЕННЯ ПРОГРАМНОГО КОДУ
7. ТЕСТУВАННЯ ЛОГІКИ РОБОТИ

Етапи створення проєкту в симуляторі Wokwi



Інтерфейс середовища проєктування симулятора Wokwi

Розробка технічного завдання пристрою контролю доступу

Метою проєкту є розроблення функціонального макету пристрою контролю доступу до приміщення або обмеженої території, що працює на базі мікроконтролера Arduino з використанням клавіатури, дисплея, сервопривода та звукової сигналізації

1. *Прийом введеного пароля з 4-клавішної цифрової клавіатури*
2. *Відображення інформації на LCD-дисплеї 16x2*
3. *Управління сервоприводом для моделювання відкриття/закриття замка*
4. *Відтворення звукових сигналів через зумер*
5. *Реалізація режиму зміни пароля за запитом користувача*
6. *Затримка перед автоматичним закриттям замка після успішного відкриття*
7. *Захист від несанкціонованого доступу*

Задачі до функціоналу системи доступу

1. *Програма повинна бути написана в середовищі Arduino IDE*
2. *ПЗ повинно включати модулі: введення з клавіатури; виведення на дисплей*
3. *Управління сервоприводом*
4. *Обробка логіки зміни пароля*
5. *Генерація звукових сигналів*

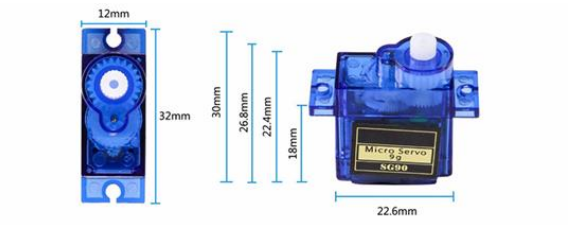
Вимоги до програмного забезпечення

Опис компонентів пристрою контролю доступу

Компонент схеми проєкта	Назва компонента
Мікроконтролер	Arduino Uno або Arduino Mega
Клавіатура	4x4 матрична клавіатура
Дисплей	LCD 16x2 з інтерфейсом I2C
Привід	Сервомотор типу SG90 або аналог
Звуковий пристрій	П'єзоелектричний зумер
Енергоживлення	220В - 9В постійного струму
Програмування	Arduino IDE, мова C++
Середовище для моделювання	Wokwi (віртуальна симуляція)

Технічні вимоги до системи контролю доступом підприємства

Вигляд плати мікроконтролера Arduino Uno



Зовнішній вид сервомотору SG90

Зовнішній вид матричної клавіатури

Розробка схеми пристрою контролю доступу

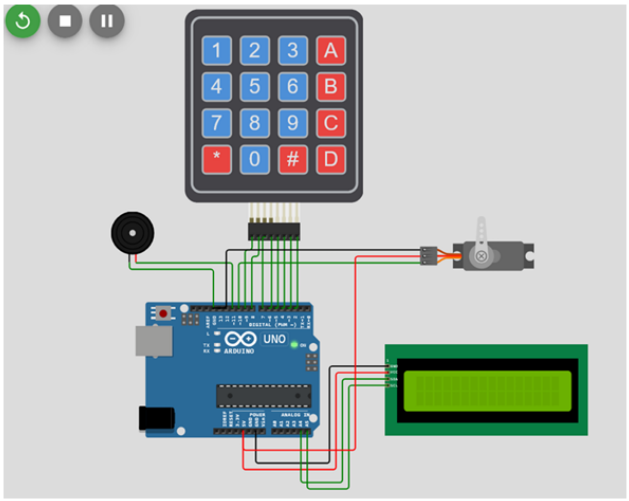


Схема пристрою контролю доступу, яка була спроєктована в симуляторі Wokwi

Загальна логіка роботи схеми контролю наступна:
1) Користувач вводить пароль з клавіатури;
2) На дисплеї з'являється відповідне повідомлення;
3) Якщо пароль правильний, то сервопривід відкриває доступ і подається звуковий сигнал;
4) Якщо пароль неправильний, то виводиться помилка, подається інший звуковий сигнал;
5) Натиснення спеціальної клавіші (наприклад, "A") дозволяє увійти в режим зміни пароля;
6) Система дозволяє зберегти новий пароль до енергонезалежної пам'яті (EEPROM).

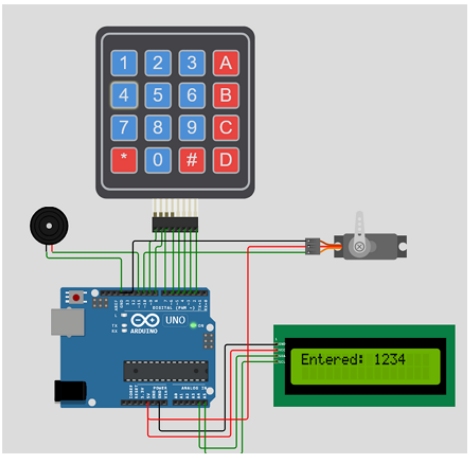
Опис програмного забезпечення

Програмне забезпечення (ПЗ) для пристрою контролю доступу реалізовано на мові програмування C++ із використанням середовища Arduino IDE. Основне завдання ПЗ — забезпечити взаємодію між користувачем і системою: введення пароля, перевірка коректності, відкриття доступу, подання звукових та візуальних сигналів, а також можливість зміни пароля

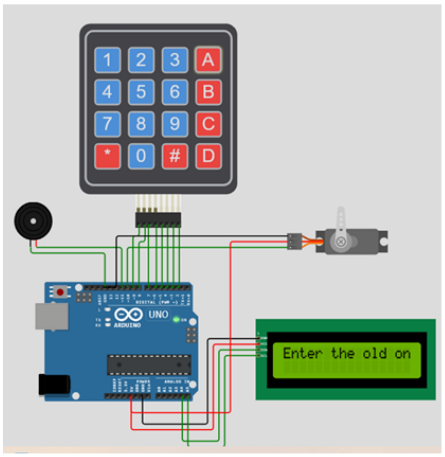
Ініціалізація компонентів	*Підключення бібліотек (Keypad, LiquidCrystal_I2C, Servo), визначення пінів для клавіатури, дисплея, зумера, сервомотора та ініціалізація LCD-дисплея, встановлення кута сервомотора у вихідне положення (закрито).*
Головний цикл (loop) виконує	*Зчитування натискань клавіш, формування введеного пароля, перевірку правильності введення, управління сервоприводом і зумером та виведення інформації на дисплей*
Режим зміни пароля	*Аактивація по натисканню спеціальної клавіші (наприклад, A), перевірка старого пароля, прийом нового пароля та його підтвердження. запис нового пароля у змінну EEPROM (або оперативну пам'ять, залежно від реалізації)*
Затримка delay(500)	*checkPassword() — перевіряє правильність введеного пароля. unlockDoor() — активує сервомотор і відкриває доступ. lockDoor() — повертає сервопривід у вихідне положення. beepSuccess(), beepError() — подають звукові сигнали.*

Структура програми

Тестування працездатності пристрою керування доступом



Введення вірного пароля за замовчуванням 1234



Режим зміни пароля – натиснута спеціальна клавіша A

Висновки

У ході виконання дипломної роботи було спроєктовано, розроблено та протестовано пристрій контролю доступу на базі апаратної платформи Arduino Uno

У результаті виконання роботи було отримано:

1) Проведено аналіз сучасних систем контролю доступу, зокрема рішень на основі мікроконтролерів;

2) Обґрунтовано вибір платформи Arduino завдяки її відкритості, підтримці великої кількості периферії та простоті програмування;

3) Визначено технічні вимоги до пристрою та обрано відповідні компоненти: клавіатура 4×4, LCD-дисплей 16×2 з інтерфейсом I2C, сервомотор SG90, п'єзоелектричний зумер;

4) Розроблено електричну схему пристрою, програмне забезпечення з можливістю перевірки пароля та його зміни користувачем;

5) Проведено моделювання та тестування системи в середовищі Wokwi, яке підтвердило правильність логіки та працездатність усіх компонентів;

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

РЕЦЕНЗІЯ

на дипломний проект здобувача (здобувачки) освіти

відділення комп'ютерних систем

Коротняна Артема Андрійовича

(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 пристрою контролю доступу на територію на базі платформи Arduino*

Обсяг розрахунково-пояснювальної записки *70* сторінок

Обсяг графічної (презентаційної) частини *14* 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 пристрою контролю доступу на територію на базі 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 (аналізу предметної області, складання ТЗ, проектування рішення, реалізації та тестування), економічного розділу, розділу охорони праці та додатків. Перелічені розділи поетапно охоплюють розробку, виконані докладно та обґрунтовано. Розділ охорони праці містить загальну інформацію, аналіз небезпечних факторів та вимоги до пожежної безпеки. Економічний розділ проекту містить розрахунок вартості виконання науково-дослідної роботи.

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

Графічна частина складається з 14 слайдів мультимедійної презентації, виконаної у програмному продукті MS PowerPoint, які містять ілюстративні схеми, скріншоти роботи програмного застосунку, передбачені технічним завданням. Пояснювальна записка виконана акуратно та у відповідності до норм. Якість виконання графічної частини проекту та пояснювальної записки добра, розробку виконано у повному обсязі.

г) перелік позитивних якостей дипломного проекту *Проведено реалізацію рішення в рамках екосистеми Arduino в аспекті контролю доступу на територію. Послідовно та системно проведено реалізацію за всіма етапами життєвого циклу розробки.*

д) основні недоліки дипломного проекту *Варто було використовувати різні ідентифікатори для керування системою. Простий 4-значний PIN-код без механізму блокування після багатьох помилок. Пароль зберігається в оперативній пам'яті — втрачається після перезавантаження. Не застосовано шифрування чи хешування PIN, відсутня багатофакторна автентифікація.*

Оцінка розрахункової частини *Добре*

Оцінка графічної частини *Добре*

Загальна оцінка *Добре*

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

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

Підпис:

«23» 06 2025 р.

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

ВІДГУК

керівника на дипломний проект здобувача (здобувачки) освіти

відділення комп'ютерних систем

Коротняну Артему Андрійовичу

(прізвище, ім`я та по батькові)

Спеціальність: *123 "Комп'ютерна інженерія"*

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

Тема дипломного проекту: *Розробка пристрою контролю доступу на територію на базі 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 __ сторінки. У пояснювальній записці розглянуто напрям розробки пристрою контролю доступу на територію на базі універсальної платформи Arduino, як програмно-апаратної платформи. Графічна частина складається з слайдів мультимедійної презентації, які також містять креслення, передбачені технічним завданням. Якість виконання пояснювальної записки та графічної частини добра, розробку виконано в повному обсязі.*

б) самостійність роботи над проектом: *Протягом всього строку дипломного проектування та переддипломної практики здобувач освіти Коротнян А.А. 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 Коротнян А.А. 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 Коротнян А.А. приймав рішення щодо вибору обладнання, аналізував вимоги на етапах проектування, розробляв проектні рішення, обґрунтовував вибір платформи розробки, мови програмування та алгоритмів реалізації розробленого проекту.

Оцінка розрахункової частини *Добре*

Оцінка графічної частини *Відмінно*

Загальна оцінка *Добре*

Прізвище, ім'я, по батькові керівника дипломного проекту _____

Стайкуца Сергій Володимирович

Місце роботи і посада керівника дипломного проекту _____

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

Підпис 

«____»_____2025 р.

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

Ми, що нижче підписалися,

Коротнян Артем Андрійович
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 пристрою контролю доступу на територію на базі платформи Arduino» (автор роботи – Рибчинський О.О., 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 _____ / Коротнян А.А. /

Керівник _____ / Стайкуца С.В. /

«19» 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

Коротняна Артема Андрійовича

на тему *Розробка пристрою контролю доступу на територію на базі платформи Arduino*

Висновок відповідальної особи за проведення нормоконтролю:
пояснювальна записка до дипломного проєкту виконана з деякими порушеннями ДСТУ та оформлена відповідно до вимог Положення про дипломне проєктування

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

Висновок відповідальної особи за перевірку роботи на наявність академічного плагіату *згідно звіту про перевірку від 19.06.2025 р. значення коефіцієнту подібності в роботі становить 21,79%, коефіцієнт цитування – 1,63%.*

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

Попередня експертиза (малий захист) дипломного проєкту

здобувача (здобувачки) освіти *Коротяна А.А.* (П.І.Б.)

проведена « *20* » *червня* 2025 р.

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

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

StrikePlagiarism.com

Дата звіту 6/19/2025
Дата редагування 6/19/2025

Документ прийнятий

Звіт подібності

метадані

Назва організації
Odesa Technical Professional College of Odesa National University of Technology
Заголовок
Розробка пристрою контролю доступу на територію на базі платформи Arduino

Автор
Коротнян Артем Андрійович
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.

21.79% 21.79% КП 1

1.63% 1.63% КЦ

25	10269	84049
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		0
Інтервали		0
Мікропробіли		43
Білі знаки		1
Парафрази (SmartMarks)	a	90

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/server/api/core/bitstreams/44c16132-5f53-48e2-b6c0-61e9a2f0fd75/content	73 0.71 %
2	https://card-file.ontu.edu.ua/server/api/core/bitstreams/4bb7255e-46d4-4349-9726-9698476da02d/content	59 0.57 %
3	https://card-file.ontu.edu.ua/bitstreams/6cf43324-8f08-4031-ba42-f80b18efbbc8/download	54 0.53 %
4	https://forum.arduino.cc/t/how-to-convert-ascii-to-int/578348	49 0.48 %

5	https://card-file.ontu.edu.ua/server/api/core/bitstreams/fc8a1853-39fc-4671-8807-2fd27ddb0779/content	43 0.42 %
6	https://card-file.ontu.edu.ua/bitstreams/6cf43324-8f08-4031-ba42-f80b18efbbc8/download	43 0.42 %
7	https://card-file.ontu.edu.ua/bitstreams/c1f3e592-1123-419d-b14a-4c28662f0f1e/download	42 0.41 %
8	https://card-file.ontu.edu.ua/server/api/core/bitstreams/44c16132-5f53-48e2-b6c0-61e9a2f0fd75/content	41 0.40 %
9	https://card-file.ontu.edu.ua/server/api/core/bitstreams/ead3fa83-2e3d-4cd7-bfbd-1d5ed04c1ce4/content	40 0.39 %
10	https://card-file.ontu.edu.ua/bitstreams/6cf43324-8f08-4031-ba42-f80b18efbbc8/download	40 0.39 %

з домашньої бази даних (0.64 %)

ПОРЯДКОВИЙ НОМЕР	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	Розробка чат-боту з навчання принципам персональної безпеки та кібергігієни [redacted] 6/18/2025 Odesa Technical Professional College of Odesa National University of Technology (Відокремлений структурний підрозділ "Одеський технічний фаховий коледж Одеського національного технологічного університету")	56 (6) 0.55 %
2	Розробка експертної веб-системи перукарні для оптимізації роботи колористів [redacted] 6/18/2025 Odesa Technical Professional College of Odesa National University of Technology (Відокремлений структурний підрозділ "Одеський технічний фаховий коледж Одеського національного технологічного університету")	10 (1) 0.10 %

з програми обміну базами даних (0.32 %)

ПОРЯДКОВИЙ НОМЕР	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	Стасішен_Кіберфізична система моніторингу якості сну [redacted] 6/8/2025 Khmelnytskyi National University (Кафедра комп'ютерної інженерії та інформаційних систем)	21 (1) 0.20 %
2	Побутова система для контрольованого нагрівання води, як елемент Інтернету речей [redacted] 3/15/2025 National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute (National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute)	12 (1) 0.12 %

з Інтернету (20.83 %)

ПОРЯДКОВИЙ НОМЕР	ДЖЕРЕЛО URL	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	https://card-file.ontu.edu.ua/bitstreams/55e2b8f2-7d3c-4235-99fc-2be51199b96d/download	556 (60) 5.41 %
2	**https://card-file.ontu.edu.ua/server/api/core/bitstreams/44c16132-5f53-48e2-b6c0-61e9a2f0fd75/content**	**459 (27) 4.47 %**
3	**https://card-file.ontu.edu.ua/bitstreams/6cf43324-8f08-4031-ba42-f80b18efbbc8/download**	**150 (4) 1.46 %**
4	**https://card-file.ontu.edu.ua/bitstreams/62baa43e-b968-4993-bb54-8cf8761a89b2/download**	**135 (10) 1.31 %**
5	**https://card-file.ontu.edu.ua/server/api/core/bitstreams/fc8a1853-39fc-4671-8807-2fd27ddb0779/content**	**94 (4) 0.92 %**
6	**https://card-file.ontu.edu.ua/bitstreams/341a820e-d025-42f3-b7dc-27e831d6c66f/download**	**91 (4) 0.89 %**
7	**https://card-file.ontu.edu.ua/bitstreams/aed610a6-43ef-47e0-9066-e85c89456f3e/download**	**83 (5) 0.81 %**
8	**https://forum.arduino.cc/t/how-to-convert-ascii-to-int/578348**	**65 (2) 0.63 %**

9	https://card-file.ontu.edu.ua/server/api/core/bitstreams/4bb7255e-46d4-4349-9726-9698476da02d/content	64 (2) 0.62 %
10	https://card-file.ontu.edu.ua/bitstreams/53ed22ad-8700-4162-b97a-082a1ad472d6/download	57 (2) 0.56 %
11	https://card-file.ontu.edu.ua/server/api/core/bitstreams/ead3fa83-2e3d-4cd7-bfbd-1d5ed04c1ce4/content	50 (2) 0.49 %
12	https://card-file.ontu.edu.ua/server/api/core/bitstreams/8da72e29-656f-4ee4-9b22-716dedf53ff5/content	43 (2) 0.42 %
13	https://card-file.ontu.edu.ua/bitstreams/c1f3e592-1123-419d-b14a-4c28662f0f1e/download	42 (1) 0.41 %
14	https://card-file.ontu.edu.ua/server/api/core/bitstreams/76e3c1ec-4240-49ea-88c2-457a2c955630/content	37 (1) 0.36 %
15	https://card-file.ontu.edu.ua/bitstreams/1dff552d-7200-49b8-ae1d-ba76a1335685/download	36 (2) 0.35 %
16	https://card-file.ontu.edu.ua/server/api/core/bitstreams/a05c07c5-bf65-4cb0-bdfa-e28694707551/content	30 (2) 0.29 %
17	https://card-file.ontu.edu.ua/bitstreams/29489599-0581-4ce6-8890-c3b13d9f2e0e/download	26 (2) 0.25 %
18	https://mechatrofice.com/arduino/arduino-pin-number-lock-with-timeout-temporary-block	20 (3) 0.19 %
19	https://card-file.ontu.edu.ua/bitstreams/0e72a3b9-bdd7-4711-a3c6-dedc1d4287cc/download	18 (3) 0.18 %
20	https://uchni.com.ua/turizm/52396/index.html	13 (1) 0.13 %
21	https://card-file.ontu.edu.ua/bitstreams/8999d5af-6274-44f4-ae78-d23e08048d38/download	12 (1) 0.12 %
22	https://card-file.ontu.edu.ua/server/api/core/bitstreams/6eb6bf1c-5813-45e6-93c5-25539b4709d3/content	12 (2) 0.12 %
23	https://studopedia.org/11-67049.html	10 (1) 0.10 %
24	https://card-file.ontu.edu.ua/bitstreams/158e44b0-583e-4b2d-b758-6b86979e33bb/download	9 (1) 0.09 %
25	https://card-file.ontu.edu.ua/bitstreams/5240e379-7721-49f0-8ee8-27140b0b473a/download	7 (1) 0.07 %
26	https://card-file.ontu.edu.ua/bitstreams/d42aac6d-ab01-4a74-b9cb-ced2a9eff719/download	5 (1) 0.05 %
27	https://card-file.ontu.edu.ua/bitstreams/549ee9fe-7574-4ae5-b500-9fe2711f33e6/download	5 (1) 0.05 %
28	https://card-file.ontu.edu.ua/bitstreams/bbaf3f38-16a8-4070-bead-5562769b7c71/download	5 (1) 0.05 %
29	http://opkho.com.ua/oxorona-praci-pri-roboti-z-kompyuterom/	5 (1) 0.05 %

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.** 02.10.000.ДП

КОРОТНЯНА
АРТЕМА АНДРІЙОВИЧА

м. Одеса