

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

Спеціальність: 123 «Комп'ютерна інженерія»

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

Група: 4КС-57

Дипломний проект

**здобувача освіти денної форми навчання
КС.57.15.000.ДП**

***НОВАКА
ЄВГЕНІЯ
ВІТАЛІЙОВИЧА***

**м. Одеса
2024 р.**

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

Спеціальність: 123 «Комп'ютерна інженерія»

Освітньо-професійна програма: «Обслуговування комп'ютерних систем та мереж»

Група: 4КС-57

ПОЯСНЮВАЛЬНА ЗАПИСКА

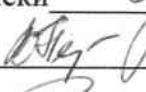
до дипломного проекту на тему:

**Розробка системи керування доступом офісу підприємства на основі
радіочастотного доступу**

Проектний матеріал складається з пояснювальної записки на 75 сторінках та
графічного (презентаційного) матеріалу на 15 аркушах (слайдах)

Дипломник  (Новак Є.В.)
Керівник  (Кільдішев В.Й.)

Консультанти:

з економічного розділу  (Іванченков В.С.)
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  (Скорнякова О.В.)

Захист «14» 06 2024 р. Протокол ЕК № 1
Оцінка ЕК 5 (відмінно) №

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 «Обслуговування комп'ютерних систем та мереж»

ЗАТВЕРДЖУЮ:

Заст. дир. з НВР Беркань І.В.

“ 15 ” 06 2024 р.

ЗАВДАННЯ

на дипломний проект

Здобувачеві освіти Новаку Євгенію Віталійовичу
(прізвище, ім'я, по батькові)

1. Тема проекту Розробка системи керування доступом офісу підприємства на основі радіочастотного доступу

затверджена наказом по коледжу від “02” 11 2023 р. № 244-Ад-ОД

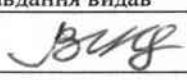
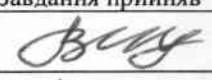
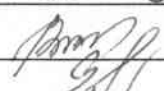
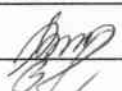
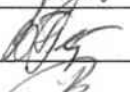
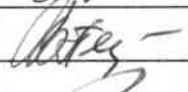
2. Термін здачі закінченого проекту 10.06.2024р

3. Вихідні дані до проекту Технологія радіочастотного розпізнавання та її використання; Різновиди зчитувачів та блокувальних елементів для системи керування доступом; Застосування мови програмування C для прошивки Arduino; Розробити пристрій для керування доступом на основі радіочастотного доступу; Реалізацію та моделювання виконувати застосовуючи мову програмування C та обчислювальну платформу Arduino

4. Зміст розрахунково-пояснювальної записки (перелік питань, які необхідно розробити)
Основні відомості про використані технології. Різновиди систем контролю і управління доступом. Вибір технологій і інструментів для реалізації СКУД. Основні відомості про платформу Arduino. Принципи роботи RFID технології. Розробка логіки та програмного коду системи. Розробка і реалізація СКУД, побудованої на Arduino. Економічні розрахунки. Заходи ТБ

5. Перелік графічного (презентаційного) матеріалу (з точним зазначенням обов'язкових креслень, кількості слайдів)
Приклади систем керування доступом; різновиди блокувальних елементів системи; різновиди плат Arduino; графічні зображення елементів системи; графік розподілу сфер використання RFID-технологій; візуальні схеми підключення системи; блок-схема системи; функціональна схема

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
Основний розділ	Кільдішев В.Й.		
Економічний розділ	Іванченков В.С.		
Розділ охорони праці	Чорновол Н.І.		
Нормоконтроль	Петрашова В.І.		
Старший консультант	Кривченко Ю.В.		

7. Дата видачі завдання _____

Керівник

Кільдішев В.Й.



(підпис)

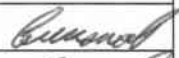
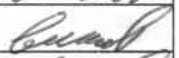
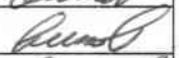
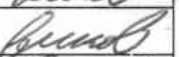
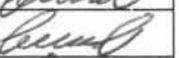
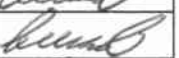
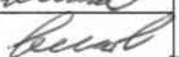
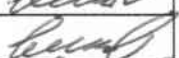
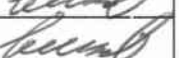
Завдання прийняв до виконання

Новак Є.В.



(підпис)

КАЛЕНДАРНИЙ ПЛАН

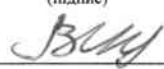
№ з/р	Назва етапів дипломного проекту	Термін виконання етапів дипломного проекту (роботи)	Відмітка про виконання
1	Вступ. Постановка мети та задач проектування	29.04.2024	
2	Вивчення технічної документації	30.04.2024	
3	Аналіз завдання роботи	01.05.2024	
4	Аналіз системи керування доступом та її види	03.05.2024	
5	Аналіз елементів системи	08.05.2024	
6	Дослідження Arduino та елементів системи	12.05.2024	
7	Вибір компонентів для розробки системи	18.05.2024	
8	Створення блок-схеми роботи системи	20.05.2024	
9	Розробка програмного забезпечення Arduino	21.05.2024	
10	Виявлення та виправлення помилок	26.05.2024	
11	Аналіз результатів, підготовка презентації	29.05.2024	
12	Економічні розрахунки та питання з охорони праці	01.06.2024	
13	Підготовка графічної частини проекту	08.06.2024	
14	Підготовка проекту до захисту та тестування	10.06.2024	

Дипломник



(підпис)

Керівник



(підпис)

[illegible]

ЗМІСТ

Вступ.....	7
1 Основний розділ	8
1.1 Аналіз завдання та системи.....	8
1.1.1 Аналіз завдання роботи.....	8
1.1.2 Аналіз та визначення системи	8
1.1.3 Типи систем керування доступом	12
1.1.4 Аналіз елементів системи доступу.....	14
1.1.5 Інтеграція СКД з іншими системами та технікою.....	20
1.2 Опис використаних пристроїв та технологій	22
1.2.1 «Мозок» системи доступу. Arduino	22
1.2.2 RFID модуль. Картка та брелок.....	27
1.2.3 Сервопривод. Блокувальник дверей	32
1.2.4 Зумер. Звуковий пристрій	33
1.2.5 Дисплей. Візуальне інформування користувача	34
1.2.6 Клавіатура.....	35
1.3 Побудова алгоритмів та схем системи.....	36
1.3.1 Моделювання системи. Побудова схем.....	36
1.3.2 Логіка програмного коду	38
1.3.3 Електрична функціональна схема	40
1.4 Розробка системи. Програмний код.....	41
1.4.1 Принципи роботи контактів плати Arduino	41
1.4.2 Написання програмного коду	42
1.4.3 Побудування макетної системи.....	46
2 Економічний розділ.....	48
2.1 Аналіз виробу	48
2.2 Розрахунки вартості та прибутку виробу	48
2.3 Прогноз обсягів продаж даного виробу.....	50
3 Розділ охорони праці та техніки безпеки.....	53
3.1 Аналіз небезпечних чинників	53
3.2 Електробезпека.....	55
3.3 Вимоги до приміщення.....	56

3.4 Пожежна безпека.....	57
Висновки	58
Перелік використаних інформаційних джерел	59
Додаток А. Програмний код мовою C++ для прошивки мікроконтролеру Arduino.....	61
Додаток Б. Слайди мультимедійної презентації.....	68

					КС 57. 15 000. 00 ДП ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		6

ВСТУП

Сучасні технології дозволяють встановлювати системи керування доступом на багато разів зручнішими та безпечнішими, ніж використовували у минулому. В сучасних системах безпеки все рідше можна побачити лише один фізичний замок з ключем. Значно зручніше піднести карточку доступу, котру можна носити в гаманці з банківськими картками, ніж носити з собою ключ та вставляти його в свердловину. Крім того, сучасні системи можуть інтегруватися з іншими технологіями, такими як відеоспостереження та системи обліку робочого часу. Це забезпечує комплексний підхід до безпеки та управління доступом на підприємстві.

Об'єкт розробки — створення системи керування доступом офісу підприємства на основі радіочастотного доступу.

Метою роботи є надання повної інформації про сучасний стан доступних рішень встановлення системи, а також представлення інформації про сучасні типи систем для вибору правильного набору елементів для системи.

Робота включає розглядання та аналіз різноманітних класифікацій елементів та різновиди самої системи. Описано принципи роботи різних елементів системи, та їх взаємодія один з одним. Зазначено всі переваги використання системи керування доступом у різних видах підприємств та додаткові функції системи, такі як облік проходжень через систему та контроль робочого часу співробітників.

В роботі має бути створено блок-схему програмної логіки та створено електронну принципіальну схему. Роз'яснено логіку функціонування коду в системі та створено програмний код прошивки мікроконтролера.

Було поставлено завдання розробити:

- алгоритм роботи системи керування доступом підприємства;
- структурну схему системи;
- функціональну схему;
- програмне забезпечення;
- макетну версію системи.

					КС 57. 15 000. 00 ДП ПЗ	Арк.
						7
Змн.	Арк.	№ докум.	Підпис	Дата		

1 ОСНОВНИЙ РОЗДІЛ

1.1 Аналіз завдання та системи

1.1.1 Аналіз завдання роботи

Завданням роботи є проектування системи керування доступом для офісу підприємства. Має бути представлено три варіанти для управління доступом до системи співробітниками.

Основою системи є допуск на основі RFID-мітки. Працівник підносить заздалегідь видану йому мітку до зчитувача, і у випадку, якщо ідентифікаційний код мітки збігається з тим, котрий було закладено у систему, доступ співробітнику буде розблоковано і двері до офісу підприємства відкрито.

Також доступ для співробітника може бути представлено за допомогою матричної клавіатури, набором цифрового паролю.

Третім варіантом є відкриття дверей за допомогою звичайної кнопки, розташованої в офісі, по той бік системи контролю. Кнопка створено для забезпечення працівникам зручного доступу до дверей для виходу з приміщення, а також швидкого доступу до системи у випадку пожежної чи іншої аварійної ситуації.

При зчитуванні коректної чи некоректної мітки, або при вводі паролю, результат зчитування та ввід паролю має бути виведено на спеціальний LCD-екран та програти звук на зумері. Приклад подібної системи серійного виробництва вказано на рис. 1.1.

1.1.2 Аналіз та визначення системи

Система керування доступом (СКД) — це група елементів, об'єднаних у одну систему, розроблених для розпізнавання (ідентифікації), ціллю якого є обмеження переміщення людей у будівлі, або до самої будівлі чи території. При розпізнаванні користувача, котрому доступ дозволено — система відкриває доступ, надсилаючи необхідний сигнал на замок/сервопривод.

					КС 57. 15 001. 00 ДП ПЗ	Арк.
						8
Змн.	Арк.	№ докум.	Підпис	Дата		

З допомогою сервоприводів, підприємства можуть контролювати переміщення та вести облік осіб у своїх приміщеннях, запобігаючи несанкціонованому доступу та забезпечуючи безпеку працівників, які знаходяться у приміщенні.



Рисунок 1.1. Серійний термінал допуску з RFID мітками

Загалом, систему можна розділити на 5 типів основних елементів:

1. Зчитувальні;
2. Ідентифікатори;
3. Мікроконтролер;
4. Виконавчий пристрій (блокувальник);
5. Допоміжні елементи.

Допоміжні елементи виконують роль інформування користувача, наприклад:

- Дисплей;
- Зуммер;
- Сирена.

Зчитувач це елемент системи, який служить «мостом» від людини до мікроконтролера. Він дозволяє отримати певні дані для ідентифікації, та передати

їх до процесора, який в свою чергу зробить аналіз цих даних, та прийме рішення, чи потрібно відкривати користувачу прохід, чи заблокувати його. Приклади зчитувачів:

- RFID-зчитувач;
- Клавіатура;
- Сканер відбитку пальців;
- Сканер сітківки ока / сканер обличчя;
- Мікрофон (сканер голосу);
- Bluetooth-технологія.

Ідентифікатор це елемент, котрий не є безпосередньою частиною системи, та служить для передачі інформації від користувача до зчитувача. Ідентифікатори можуть бути персональними, та універсальними.

Саме персональні ідентифікатори дають можливість вести адміністрування співробітників та вести облік та контроль робочого часу. Облік не можливо реалізувати використовуючи універсальні ідентифікатори, так як в такому випадку для системи всі користувачі будуть однаковими. Приклади ідентифікаторів:

1. RFID-мітка чи брелок;
2. PIN-код;
3. Палець;
4. Око / обличчя;
5. Голос;
6. Телефон.

Мікроконтролер є «мозком» системи. Він отримує дані від зчитувача. Ці дані є певним паролем, представленим у послідовності букв та цифр. Наприклад, ПІН-код це найпростіший, короткий (від 4 до 8 цифр) пароль. А ось дані від сканеру відбитка пальців мають настільки складний пароль, що модуль сканера має вбудований (окремий) процесор для обробки цього паролю. І вже після обробки, елемент передає результат на основний мікроконтролер.

					КС 57. 15 001. 00 ДП ПЗ	Арк.
						10
Змн.	Арк.	№ докум.	Підпис	Дата		

Якщо наданий пароль збігається з «білим списком» закладених у систему паролів — посилається необхідний сигнал на блокувальний елемент, та на допоміжні елементи, такі як дисплей чи зумер.

Блокувальник це елемент системи який, як правило, розташований подаль від зчитувача та мікроконтролера, та з'єднується з ними по дроту, довжина котрого може сягати декількох метрів. Він реагує на подачу сигналу від мікроконтролера, і безпосередньо рухає засув замка для відкриття та закриття фізичного доступу до приміщення.

Блокувальники можуть бути різних видів зображені на рис. 1.2, наприклад:

- Шлагбаум;
- Турнікет;
- Електронний замок;
- Автоматичні ворота.

Допоміжні елементи також є частиною СКД, але безпосередньо не впливають на обробку та роботу системи. Вони слугують інформуванням користувача та оточуючих про хід роботи системи та її результат.

- Зумер допомагає звуком сповістити користувача про обробку натискання клавіші на клавіатурі, та інтуїтивним звуком сповістити про результат вводу паролю чи обробки будь якого іншого зчитувача;

- Дисплей. На ньому можна виводити статус системи, наприклад, чи можна в даний момент починати ввід паролю чи зчитувача. Та результат виконання, паралельно з зумером. Також на дисплеї можна виводити поле з паролем, щоб користувач не помилився при його вводі;

- Сирена встановлюється не часто, її можна використовувати щоб сповістити оточуючих, якщо хтось намагається навмання підібрати пароль чи намагається використати стару мітку, це також може відлякати порушників.

Основна функція системи керування доступом — забезпечення допуску лише дозволених осіб на певну територію. Також, система може виконувати такі функції:

- Ведення електронного обліку співробітників;

					КС 57. 15 001. 00 ДП ПЗ	Арк.
						11
Змн.	Арк.	№ докум.	Підпис	Дата		

- Контролювання дисципліну працівників. Відстежувати час їх входу/виходу з приміщення;
- Забезпечення безпеки роботи співробітників.

СКД, які мають функцію обліку — підтримують дисципліну співробітників, тому що допомагає визначити та аналізувати спізнення працівників. Або навпаки, підозріле перебування на об'єкті у позаробочий час.

Згадана функція адміністрування також допомагає відстежити крадіжку (грошей чи будь чого іншого) на основі того, хто та коли був у приміщенні в той проміжок часу, коли злочин був скоєний.

1.1.3 Типи систем керування доступом

Існує два основних типи систем керування допуском — мережеві (також їх називають центральними) та автономні (локальні). Їх встановлення залежить від поставлених задач та виду підприємства.



Рисунок 1.2. Приклади різних СКД

Мережеві системи керування доступом — працюють в обміні інформацією з центральним комп'ютером. Це дозволяє дистанційно керувати та обробляти дані, які надсилає точка контролю доступу.

Використовуючи центральні точки доступу, за необхідністю можна керувати ними з будь якої точки світу, тобто вони можуть бути під'єднані до інтернету і при необхідності бути розблоковані навіть за допомогою телефону.

Мережеві системи є більш гнучкими в порівнянні з автономними, вони дозволяють створювати різні рівні допуску на різних точках. Це означає, що володіючи різними за рівнем допуску ключами, співробітники можуть мати доступ до більшої, або меншої к-сті точок в системі. Такі СКД базуються на принципі найменших привілеїв (доступів). Це означає, що співробітнику видається мінімальний рівень допуску на певні території, необхідний для виконання його сфери відповідальності.

Також, щодо обробки даних — так як всі точки під'єднані до однієї системи, власник системи може вести журнал активності точок, з вказанням конкретної персональної мітки співробітника, для доступу до розблокування точки. Це дозволяє вести облік, де і коли конкретний співробітник прийшов на роботу, які сектори відвідував, і о котрій годині він залишив робоче приміщення.

У мережевих системах є можливість автоматичного блокування та розблокування всіх (чи конкретних) точок у вихідні дні, та у позаробочій час.

Автономні системи контролю — працюють без центрального комп'ютера, і не потребують окремого налагодження, окрім додавання міток та паролів до системи. Вони починають роботу одразу після подачі необхідної напруги на блок живлення. Система такого типу складається лише з однієї точки допуску, і при додаванні другої такої, вони будуть двома непов'язаними між собою системами. Вони є більш зручнішим варіантом для будь яких підприємств, де не є необхідністю вести облік співробітників, та встановлювати велику к-сть точок контролю доступу.

Автономні системи контролю використовують у підприємствах, де не має конкретної мети встановлювати велику к-сть точок та вести облік співробітників, наприклад:

- Офісні приміщення. Офіси середніх та малих розмірів оснащуються СКД у точках входу до робочого приміщення. Їх встановлення в офісах є важливим кроком для запобігання викраданню коштовностей та безпеки для

					КС 57. 15 001. 00 ДП ПЗ	Арк.
						13
Змн.	Арк.	№ докум.	Підпис	Дата		

співробітників. Загалом, такі приміщення мають одну точку для встановлення системи керування допуском, тому саме автономна є більш релевантною;

- навчальні заклади. Загалом вони мають одне-два приміщення, які потребують контролю для пересування персоналу, наприклад склад чи кабінет директора. Потік людей і потреба у кількості точок є невеликою, тому використання мережевої системи керування є невиправданим;

- супермаркети, аптеки. Мають одну точку, яка потребує встановлення системи — це склад;

- музеї;

- Гаражі.

Мережеві можуть бути такими:

- Військові об'єкти. Вони мають велику кількість приміщень, які мають бути захищеними від несанкціонованого проникнення. В армії є різні права допуску, тому саме використання мережевих СКД є більш релевантним;

- станції метро. Для забезпечення великої пропускної здатності користувачів, розташовуються великою кількістю поряд один з одним. Також, вміщують в себе велику базу карток користувачів, яка може сягати мільйони карток у великих містах. Картки користувачів мають завантажуватись через інтернет в реальному часі, тому така система придатна лише для мережевого типу;

- банки та інші фінансові структури. Потребують посиленого рівня контролю та ведення журналу, так як встановлюються у місцях, які потребують великої відповідальності;

- медичні та наукові лабораторії.

1.1.4 Аналіз елементів системи доступу

Різні елементи допуску системи мають відрізнi принципи безпеки, тому є сенс провести аналіз цих елементів. Завдяки цьому майбутній власник зможе обрати компоненти, які підходять саме для нього. Також, розуміння «дірок» безпеки системи для кінцевого користувача. Власник системи, базуючись на цих «дірках»

					КС 57. 15 001. 00 ДП ПЗ	Арк.
						14
Змн.	Арк.	№ докум.	Підпис	Дата		

зможє дати застереження до своїх співробітників як слід поводитись з елементами системи, щоб уникнути зламування системи безпеки сторонніми особами.

RFID-мітка має багато переваг, порівнюючи зі звичайним замковим ключем та самим замком. Для кінцевого користувача потребується лише піднести мітку у вигляді пластикової картки або брелка до зчитувача (на відстань від 6 см та ближче) і через одну секунду двері вже будуть відчинені. В порівнянні з замковим ключем це зручніше, та в рази пришвидшує допуск до системи. Також, при втраті замкового ключа, потрібно замінювати весь замок та всі ключі у співробітників, а при втраті RFID-мітки — лише перезаписати пароль в системі та перезаписати всі мітки робітників.

Але радіочастотна система також має «болячки» як і звичайний ключ — мітки також треба купляти, а якщо вчасно не замінити пароль в системі, то зловмисник може отримати доступ до системи.

Клавіатура не є основним засобом допуску до системи, та слугує лише резервним варіантом допуску, на випадок коли співробітник не має при собі мітку, або частотний зчитувач зламався. Перевагами над замковим ключем є те, що співробітник не має вимоги мати з собою ключ чи мітку, пароль можна запам'ятати чи записати в безпечному місці. Також при витоку паролю, його можна дуже швидко замінити без фінансових вимог.

Недоліками можна виділити те, що його ввід можуть побачити та запам'ятати сторонні люди, що є небезпечним для системи. Також, ввід паролю займає приблизно стільки ж часу, як і при використанні звичайного ключу, що в порівнянні з радіочастотним розпізнаванням є менш зручним.

Біометричні засоби, такі як сканер відбитку пальців чи обличчя є найнадійнішим засобом, який широко використовується на даний момент. Біометричні засоби мають надвелику перевагу над вищевказаними варіантами тим, що не потребують фізичного носіння мітки чи запам'ятання паролю. Їх ідентифікатори неможливо забути чи загубити. Відбиток пальця чи обличчя неможливо підробити, тому вони є одночасно найзручнішими, так і найбезпечнішими. Мінусами таких сканерів є дороговизна самого сканера, та

					КС 57. 15 001. 00 ДП ПЗ	Арк.
						15
Змн.	Арк.	№ докум.	Підпис	Дата		

потреба в потужному процесорі для обчислення даних, отриманих з нього. Загалом, біометрика зараз використовується у преміальних великих компаніях, де важлива максимальна безпека та зручність для робітників.

Кнопка, розташована в офісі слугує для виходу із приміщення співробітників, що економить бюджет та робить покидання приміщення в рази зручніше. Без кнопки, потрібно було б ставити такі ж самі елементи допуску з обох сторін дверей.

Також, кнопка слугує для зручного допуску до нього стороннього персоналу, співробітником із середини (таких як доставка, системні адміністратори, та інший сторонній персонал). Але якщо доступом заволодіє сторонній із середини, система стає беззахисною, а доступ — неконтрольованим.

Турнікет це блокувальний елемент, який, як правило встановлюється в публічних місцях. Він забезпечує найшвидший прохід, в порівнянні з аналогами, такими як електронний замок чи шлагбаум. Це можна зрозуміти, якщо уявити як абсурдно шлагбаум чи двері з електронним замком будуть виглядати в метро чи аеропорті, де потік людей великий, і ключовим параметром є час проходу людини.

На відміну від шлагбауму, при розблокуванні турнікет приводить в рух сама людина, тому швидкість проходу є вищою. А в порівнянні з дверима з електронним замком, вони не потребують «закриття» після проходу, тому при пропуску одного користувача, вони вже готові до обробки наступного. Основні види турнікетів зображені на рис. 1.3:

- турнікет-трипод;
- роторний турнікет;
- турнікет хвіртка.



Рисунок 1.3. Види турнікетів зліва направо: трипод, роторний, хвіртка

Недоліками турнікетів є їх ціна, та непристосованість триподних та роторних турнікетів до пропуску людей з великим багажем, та людей на інвалідних візках. Також, у нелюдних місцях турнікет можна перестрибнути, на відміну від дверей. Саме тому рекомендується ставити турнікети лише у публічні місця з великим потоком людей.

Двері з електромеханічним замком використовуються в системах, де вхід призначено саме для співробітників. Вони використовуються для захисту окремих приміщень. Двері надають максимальний рівень захисту серед всіх блокувальників, при чому їх встановлення є дешевшим від турнікету чи шлагбауму. Вони зазвичай встановлюються там, де вхід мають право мати лише співробітники організації. Це дозволяє контролювати, хто має доступ до приміщення, що є важливим для забезпечення безпеки. Вони забезпечують високий рівень захисту, зручність в експлуатації та можливість інтеграції з сучасними системами безпеки.

Шлагбаум — спеціалізований елемент, який використовується в місцях проїзду техніки. Шлагбаум, зображений на рис. 1.4 є найзручнішим варіантом саме для техніки, тому що через нього можна проїхати на транспорті, що не є можливим при використанні турнікету або дверей.



Рисунок 1.4. Шлагбаум в системі СКД

Не рекомендується використовувати шлагбауми для обмеження руху людей, так як вони не створюють складної перешкоди, людина може легко пройти під ними.

Автоматичні ворота — цей вид блокувальних елементів також призначений для транспорту. Вони є менш швидкими ніж шлагбаум, але водночас і більш безпечними. Види воріт зображено на рис. 1.5. Шлагбаум не претендує на захист від проходу людей, тоді як ворота повністю перекривають доступ до території, роблячи неможливим прохід до неї як транспорту, так і людей, що робить їх ідеальними для обмеження доступу до територій з проїздом транспорту.

Кожен тип блокувального елемента має свої переваги і обмеження, які важливо враховувати при виборі і встановленні в конкретному середовищі. Завдяки різноманітності доступних технологій, можна забезпечити ефективний контроль за доступом до будь-яких об'єктів і зон, враховуючи специфіку потреб кожного конкретного випадку.

					КС 57. 15 001. 00 ДП ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		18

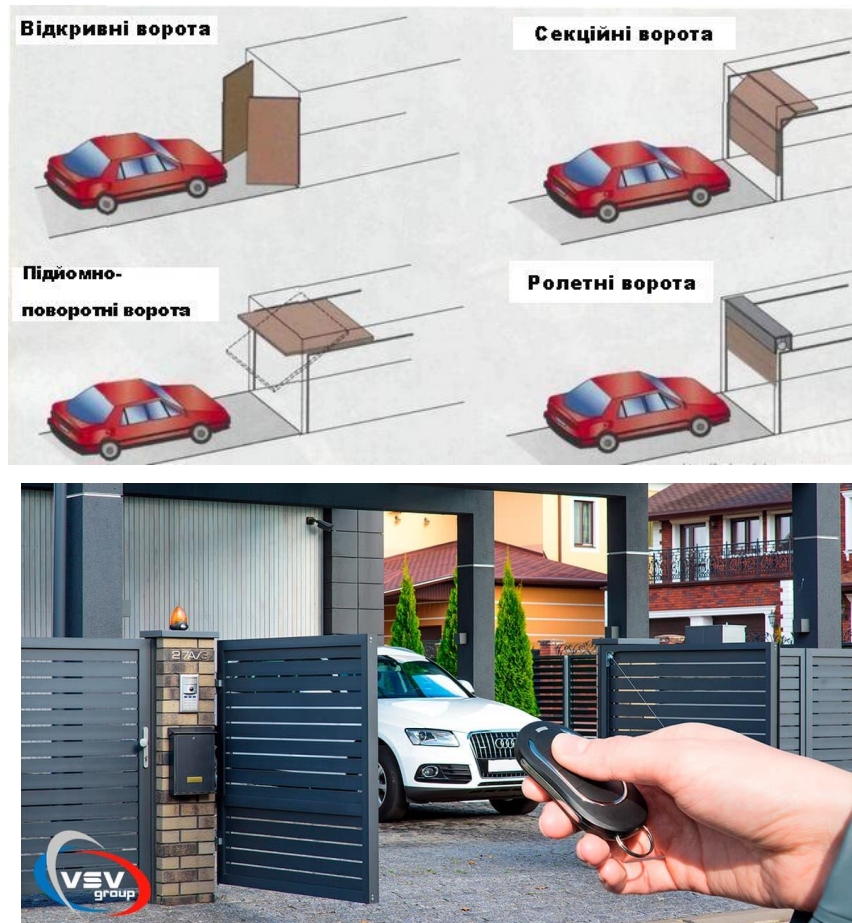


Рисунок 1.5. Види автоматичних воріт

Базуючись на вищезгаданих факторах, можна представити елементи в вигляді списку із переваг та недоліків:

Переваги використання RFID-мітки:

- швидкість зчитування (допуску);
- високий рівень безпеки ;
- зручність використання.

Недоліки використання RFID-мітки:

- фізична втрата мітки може поставити систему під загрозу;
- фінансові витрати на купівлю міток.

Переваги використання клавіатури:

- дешевизна встановлення;
- відсутня вимога фізичного носіння розпізнавального елементу.

Недоліки використання клавіатури:

					КС 57. 15 001. 00 ДП ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		19

- небезпека витоку пароллю при спостереженні сторонньою людиною;
- необхідність запам'ятання пароллю чи його запису;
- ввід великого пароллю буде затратати час.

Переваги використання біометричних засобів розпізнавання:

- максимальний рівень безпеки;
- зручність для співробітника;
- швидкість зчитування.

Недоліки використання біометричних засобів розпізнавання:

- дороговизна модулю;
- складність встановлення;
- необхідність у регулярному обслуговуванні.

Переваги встановлення кнопки всередині офісу:

- економія бюджету;
- зручний допуск « гостей » до приміщення;
- швидкість.

Недоліки встановлення кнопки всередині офісу:

- допуск до кнопки сторонніх осіб може поставити безпеку під загрозу.

1.1.5 Інтеграція СКД з іншими системами та технікою

СКД має можливість інтегрування з іншими системами та електронними приладами. Це додатково розширяє функціонал системи, який можна використовувати як додаткову перевірку для надання доступу, або для надання додаткової інформації до журналу надання доступу. Найбільш популярні системи та прилади, які можна додати до СКД:

- пожежні системи. Підключення до пожежної системи, зображеної на рис. 1.6 є важливим задля забезпечення безпеки співробітників при пожежі. Якщо пожежна система помічає спалах, вона посилає сигнал на СКД, який в свою чергу, має тримати замок відчиненим, щоб працівники мали можливість швидко та безперешкодно залишити приміщення;

					КС 57. 15 001. 00 ДП ПЗ	Арк.
						20
Змн.	Арк.	№ докум.	Підпис	Дата		

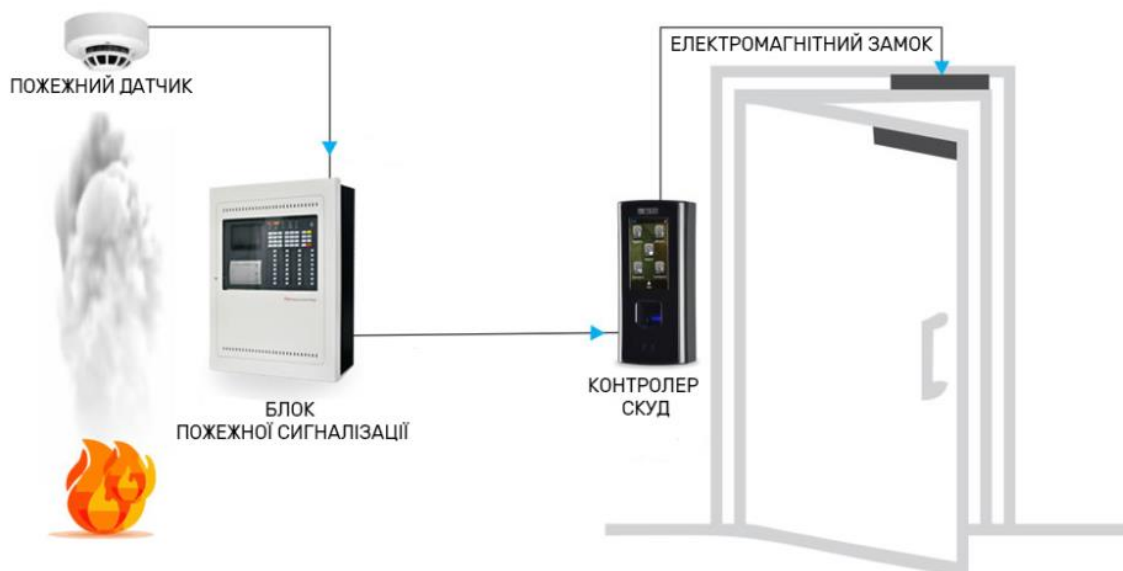


Рисунок 1.6. Пожежна система і СКД

- система відеоспостереження. Інтегрування до цієї системи надає можливість робити фотографію в момент розблокування системи, для подальшого перегляду за потреби. Також, систему можна налаштувати так, щоб фотографія робилася лише в той момент, коли доступ до системи намагаються отримати вводячи неправильний пароль, чи використовуючи неправильний RFID брелок;
- алкотестер. СКД може інтегруватися з алкотестером для перевірки людей з підвищеним рівнем алкоголю в крові. Система може просто відстежувати та робити відповідні помітки рівня алкоголю, не впливаючи на дозвіл на прохід до території. Або може бути використаною як додатковий зчитувач, і для проходу до приміщення користувач повинен мати рівень алкоголю не вище заданого рівня;
- пірометр. Пристрій який вимірює температуру тіла людини. Підключення до цього пристрою також як і в випадку з алкотестером може просто зберігати дані про температуру співробітників, а також використовуватись як додатковий параметр для входу до приміщення.

Системи контролю допуску пропонують різноманітний вибір для покупця. Саме розуміння різних елементів та видів системи дозволяє майбутньому власнику підібрати таку систему, яка задовільнить цілі та потреби його компанії. Ці потреби можуть залежати від призначення та розміру підприємства.

1.2 Опис використаних пристроїв та технологій

1.2.1 «Мозок» системи доступу. Arduino

Обчислювальною платою для створення системи керування доступом виступає один з найвідоміших та найпоширеніших виробників електронних плат під назвою «Arduino». Arduino є відносно молодою компанією, котра почала випускати плати загального користування лише 10 років тому, але завдяки простоті використання, відкритому ПЗ та невеликій ціні плат, компанія зайняла перше місце серед мікроконтролерів для створення саморобних пристроїв, так званих DIY (зроби своїми руками).

Переваги використання мікроконтролера Arduino:

- простота використання плати та її прошивка. Контакти плати мають зручні роз'єми для підключення, та мають відповідні написи поруч з контактом, завдяки чому можливість помилкового підключення зведена до мінімуму;
- вартість. Цінова доступність обумовлена великою кількістю виробників та простоті конструкції плати;
- популярність. Поширеність плати дозволяє знаходити вже вирішені проблеми, з якими може зіштовхнутись власник, або легко отримати відповідь, задавши запитання на відповідному форумі.

Недоліки плати Arduino:

- мала продуктивність. Мікроконтролер, який використовують плати Arduino мають відносно невелику продуктивність;
- обмежена пам'ять. Плати Arduino можуть зберігати до 32кб програмного коду, що може бути недостатнім при використанні великої кількості бібліотек або занадто складної логіки програмного коду.

Існує багато версій цієї плати, основні з яких вказані на рис. 1.7. Вони відрізняються один від одного розміром, функціями, такими як вбудований Wi-Fi та/або Bluetooth модуль, різною кількістю портів вводу-виводу, обчислювальною потужністю процесорів та пам'яттю мікроконтролера.

					КС 57. 15 001. 00 ДП ПЗ	Арк.
						22
Змн.	Арк.	№ докум.	Підпис	Дата		

Базуючись на перевагах та недоліках, які має плата Arduino, для створення СКД було обрано саме плату цього виробника, так як вказані недоліки не є проблемою для створення та ефективної експлуатації СКД.

Для створення системи керування доступом обрано саму популярну версію — Arduino Uno. За розмірами вона стоїть по середині між найменшими моделями, такою як Arduino Nano, та великими моделями, таким як Arduino Mega.

За своїми можливостями Arduino Uno не відрізняється від Arduino Nano, але підключення елементів до Uno є в багато разів зручніше, тому ще не потребує припаювання модулів до неї, а має «гнізда» для підключення необхідних модулів.

Arduino Uno — це пристрій зображений на рис. 1.8, який дозволяє розробникам створювати і автоматизувати саморобні проекти. Плата має цифрові (14 шт) та аналогові (6 шт) виходи які можна запрограмувати за допомогою будь якого комп'ютера.

Контакти можна побачити на рис. 1.8. Він базується на 8-бітному мікроконтролері ATmega328. 8-бітні мікроконтролери є більш енергоефективними, тому не потребують активного охолодження, в порівнянні з 32 та 64 бітними процесорами які встановлюються на персональних комп'ютерах та на серверах. Також 8-бітні мікроконтролери є більш компактними та надійними.

					КС 57. 15 001. 00 ДП ПЗ	Арк.
						23
Змн.	Арк.	№ докум.	Підпис	Дата		



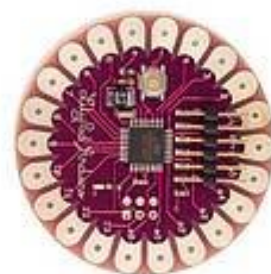
Arduino Uno



Arduino Leonardo



Arduino Mega 2560



Arduino LilyPad



Arduino Mega ADK



Arduino Fio



Arduino Ethernet



Arduino Pro



Arduino BT



Arduino Nano



Arduino Mini



Arduino Pro Mini

Рисунок 1.7. Версії плат Arduino

АТmega328 працює на частоті 16 МГц та оперує 32-ма кілобайтами flash-пам'яті, в котрих зберігається програмний код, написаний користувачем, а також 2-ма кілобайтами оперативної пам'яті, для швидкого читання тимчасових даних, таких як змінні та класи.

Електрична розмітка плати Arduino має різні контакти для під'єднання дротів до контактів, логіка яких може бути запрограмованою. Також на платі існують контакти, які слугують для керування самою платою, а також контакти зі статичними показниками напруги.

Детальніше про розмітку контактів плати Arduino:

- RX-0 та TX-1. Спеціальні порти, які працюють по UART інтерфейсу. Вони використовуються для передачі цифрової інформації між платою, та будь яким іншим пристроєм, підтримуєчим інтерфейс UART. Наприклад Bluetooth чи радіо модуль;

- цифрові порти 2, 3, 4...13. Контакти які можуть бути перепрограмованими для виконання та обробки певних задач, прописаних в коді прошивки;

- GND. З англійської «ground» — земля. Контакт для підключення до нього від'ємних контактів різних модулів;

- AREF / IOREF. З англійської AREF це скорочення «analog reference» аналогове посилення. Використовується, якщо користувач бажає змінити опорну напругу в платі (за стандартом 5 вольт). IOREF надає можливість зняти показ внутрішньої опорної напруги;

- аналогові порти A0, A1...A5. Порти, які використовуються для зчитування аналогових показників напруги. Порти працюють через аналогово-цифровий перетворювач, передаючи на мікроконтролер показ напруги у проміжку від 0 до 1023 кроків;

- Vin. Контакт, який слугує для живлення плати. Може приймати від 5 до 12 вольт;

- 5V / 3.3V. Контакти, які видають відповідну напругу. Використовуються для живлення різних елементів.

					КС 57. 15 001. 00 ДП ПЗ	Арк.
						25
Змн.	Арк.	№ докум.	Підпис	Дата		

- **RESET.** Контакт для перезавантаження плати. Після короткочасного з'єднання контакту з «землею» (GND), плата перезавантажиться та виконання коду почнеться спочатку.

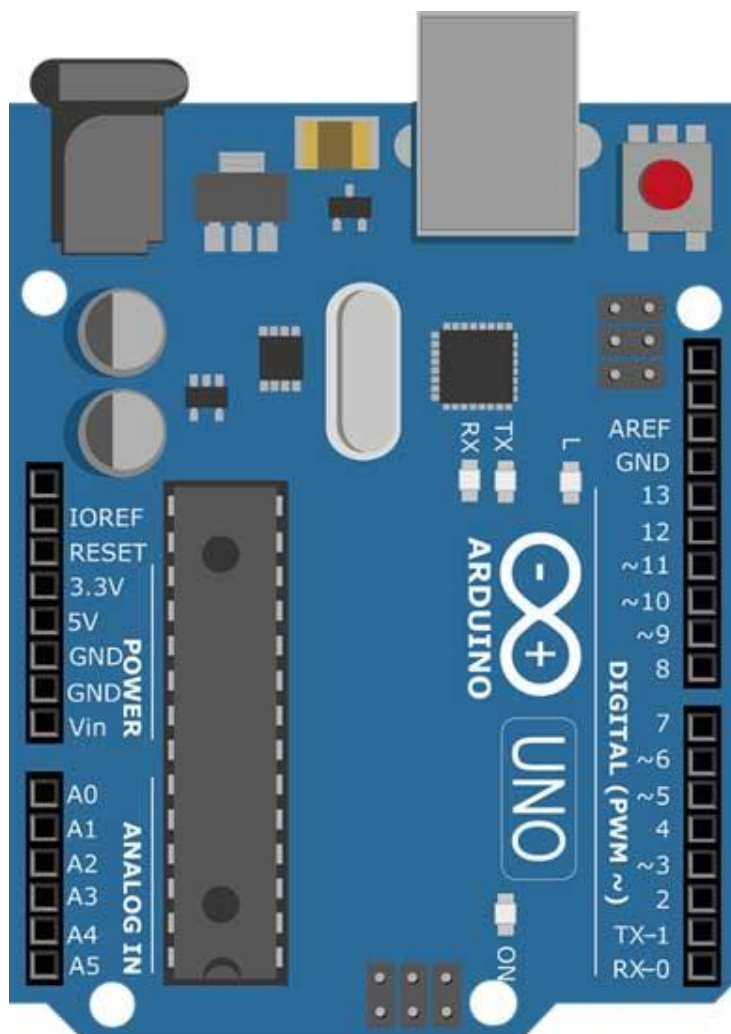


Рисунок 1.8. Візуальне зображення Arduino Uno

Arduino Uno програмується на мові програмування C++. За допомогою програми від розробника плати під назвою Arduino IDE, там вже є налагоджені функції для запуску плати і управління її контактами, середовище зображено на рис. 1.9. Вона дозволяє налагодити умови, за яких конкретний вихід плати (тобто пін), буде видавати напругу на необхідний елемент системи. Завдяки Arduino IDE можна прямо в програмі завантажити та використовувати користувацькі бібліотеки для різних модулів (по типу дисплею, rfid- приймача та інші). Це

пришвидшує написання коду, дозволяючи зосереджуватись на взаємодії модулів та логіки програми, а не створенню функцій обробки даних з модулів «з нуля».

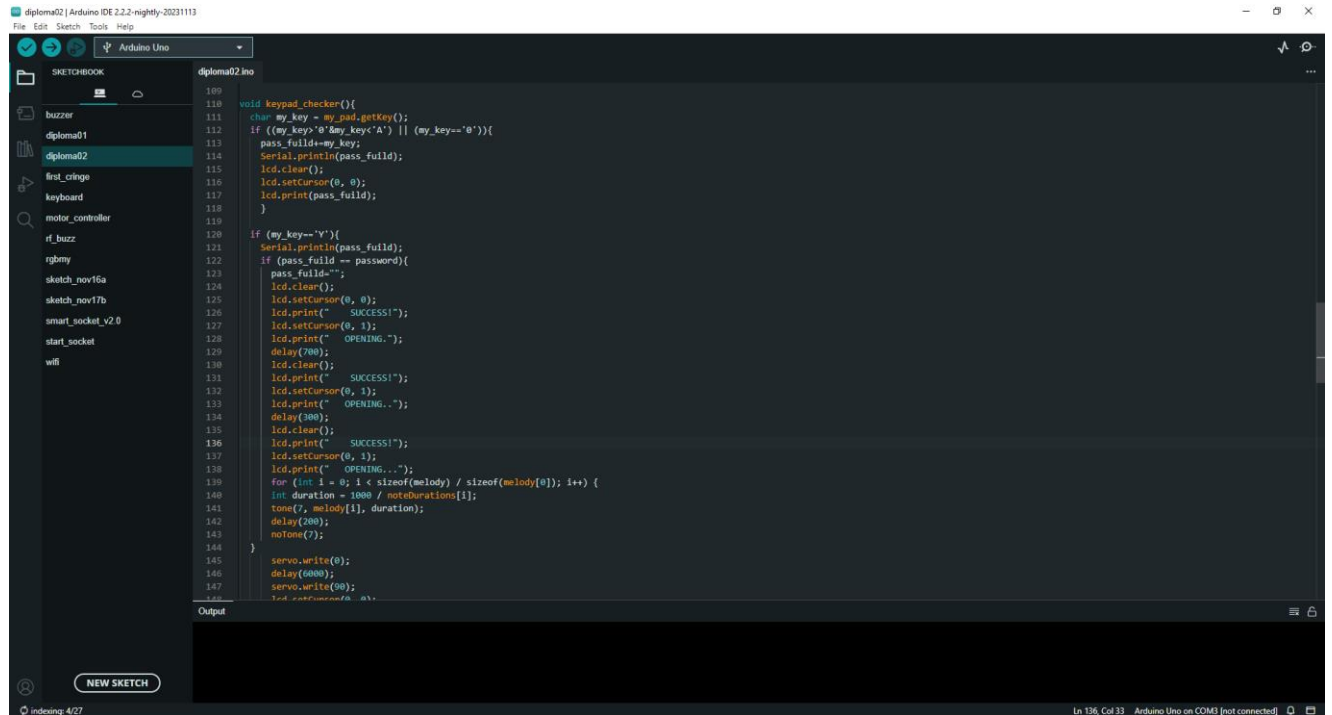


Рисунок 1.9. Зовнішній вигляд Arduino IDE

1.2.2 RFID модуль. Картка та брелок

RFID це технологія, що використовує радіочастоти для бездротового обміну даними між міткою (тобто картою чи брелком) та модулем-зчитувачем.

Існують два типи міток: активні та пасивні. На основі пасивної мітки можна описати принцип дії RFID-системи.

Принцип дії пасивної мітки наступний:

- котушка індуктивності на мітці отримує енергію від зчитувача;
- отримана енергія активує чіп, вбудований в мітку;
- активований чіп зчитує дані, зашиті в нього;
- зчитані дані чіп передає на антену;
- антена генерує радіохвилю певної частоти.

Принцип дії зчитувача наступний:

- зчитувач генерує енергію електромагнітного поля;
- зчитувач приймає радіохвилю, котру посилає мітка.

					КС 57. 15 001. 00 ДП ПЗ	Арк.
						27
Змн.	Арк.	№ докум.	Підпис	Дата		

Технологія RFID є універсальною для багатьох областей. На рис. 1.10 зображено розподіл сфер використання RFID технології. Як можна побачити, використання цієї технології у СКД займає третину ринку. Тоді як іншу третину займає транспорт.

У транспортній сфері технологію радіочастотної ідентифікації загалом використовують для:

- сигналізація авто. Брелок є активною RFID-міткою, яка посиляє сигнал на зчитувач на автівці, яка подає сигнал на відчинення дверей в авто;
- відстеження автобусів. Коли автобус проїжджає через зупинку, інформація з мітки відправляється на приймач на зупинці, і обробляється на сервері, тим самим дозволяючи відстежувати положення автобусу;
- відстеження робочого транспорту, при його в'їзді та виїзді з території підприємства;
- встановлення чіпу в автівку, для автоматичної оплати за проїзд по платній дорозі.

У сільському господарстві технологію використовують для ідентифікації та відстеження тварин за допомогою чіпів (чіпування тварин). Чіпи на тваринах дозволяють фермерам вести точний облік вакцинацій, медичних процедур, дата її народження, та будь яку іншу інформацію про дану тварину.

В логістиці RFID використовується для автоматичної інвентаризації товарів. Це зменшує час на обробку та сприяє автоматизації процесів перевозок. Автоматичне визначення товарів і вантажів стає можливим без необхідності ручного сканування або введення даних.

					КС 57. 15 001. 00 ДП ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		28

Сфери використання RFID

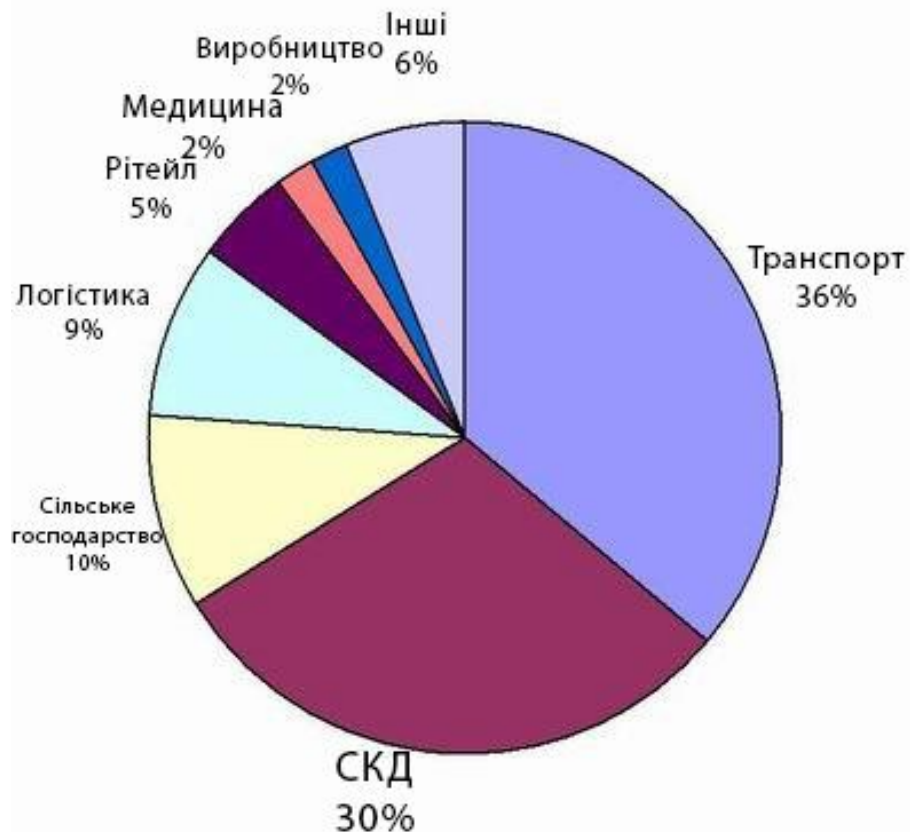


Рисунок 1.10. Розподіл сфер використання RFID технології

Пасивні мітки поділяються на 3 види за можливістю перезапису їх вмісту:

1. Read Only. Дані мітки записуються одразу на заводі, і не можуть бути перезаписані. Вони не придатні до повторного запису, і дозволяють лише зчитувати інформацію з мітки;
2. Write Once Read Many. Такі мітки мають унікальний номер, та додатковий блок з пам'яттю, який можна записати лише один раз, і в подальшому лише зчитувати записану інформацію;
3. Read and Write. Також як і попередній тип, мають унікальний номер та додатковий блок. Але, на відміну від них, додатковий блок може бути багаторазово перезаписаний.

Довжина радіохвилі, яку генерує пасивна мітка, залежить від потреби в дальності зчитування мітки. На даний момент використовуються два види:

- високочастотні мітки (HF). Це основний тип пасивних міток, який використовується на даний момент. Вони працюють на частоті 13,56 МГц. Дальність зчитування таких міток складає не більше 10 см. Вони мають великі протиколізійні властивості. Тобто якщо в радіусі його дії будуть діяти інші пристрої чи мітки, це не завадить коректної роботі мітки;

- ультрависокочастотні мітки (UHF). Є спеціалізованим типом міток, вони використовуються у випадках, де потрібно одночасно зчитати велику кількість міток, наприклад у складах при інвентаризації. Їх частота становить 860-960 МГц, що дозволяє зчитати інформацію з мітки з відстані до двох метрів.

Другий тип RFID-міток це активні мітки. Вони мають своє власне джерело живлення, завдяки чому можуть передавати інформацію на зчитувач на відстані до 100 метрів. Також в них може бути зашифровано більше інформації. Такі мітки можуть бути корисні в проектах, де є потреба у циклічній передачі/читанні даних.

Активні мітки використовуються в СКД оснований на шлагбаумі чи автоматичних воротах (наприклад для гаражу). Власник може по натиску кнопки подати сигнал на відкриття шлагбауму чи воріт гаражу.

У висновку, пасивні RFID-мітки є дешевими у виготовленні та обслуговуванні, вони використовуються майже в усіх системах керування допуску. Активні ж в свою чергу лише в тих, де доступ потрібно надати з великої відстані та лише в той момент, коли власник натисне на кнопку.

Для забезпечення безконтактного доступу до системи допуску, у роботі використовується модуль RFID RC522, зображений на рис. 1.11. Ця модель працює при напрузі 3.3V та на частоті 13.56MHz. Використовує пасивну мітку.

					КС 57. 15 001. 00 ДП ПЗ	Арк.
						30
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 1.11. Приймач RFID RC522 та картка з брелоком

Даний модуль дозволяє зчитати мітку на відстані до 6 см, чого повністю вистачає для швидкого та комфортного застосування на зчитувачі.

Модуль має наступні контакти для під'єднання до плати:

- SDA. Контакт для комунікації модуля з платою. Він забезпечує двоспрямовану передачу системних даних модуля і плати;
- SCK. Синхронізує передачу даних між платою та модулем. Керує часовими інтервалами;
- MOSI. Головна лінія передачі даних з RFID модуля до плати. Саме через неї передаються покази зчитаних міток;
- MISO. Лінія прийому даних (інструкцій), які відправляє керуюча плата;
- RST. При під'єднанні контакту до «землі», перезавантажує модуль;
- GND. Контакт для «землі»;
- 3.3V. Контакт для підключення живлення RFID модуля.

1.2.3 Сервопривод. Блокувальник дверей

Сервопривод це пристрій який використовується для виконання механічного повороту валу на заданий кут, за допомогою електромотору та імпульсу від контролера (в даному випадку Arduino) виконує механічний поворот.

Принцип дії сервопривода наступна:

1. на вхід сервопривода подається певний ШІМ сигнал, який вказує на бажаний кут повороту валу;
2. внутрішній комп'ютер сервопривода порівнює значення котре надійшло через вхід (тобто необхідний кут повороту), зі значенням в якому привід перебуває на даний момент;
3. після перевірки привід починає рух в необхідному напрямку до того моменту, коли значення на приводі врівноважиться зі значенням на потенціометрі;
4. після врівноваження, рух зупиниться до моменту надходження наступного значення.

Для розробки системи контролю доступу використовується сервопривод Tower Pro 9g SG90, зображений на рис. 1.12. Даний сервопривод має обертаючий момент 1,4 кг/см та здійснює оберт на 180° за 0,36 секунд.

Модуль має 3 контакти для під'єднання до плати Arduino:

- 5V. Живлення сервоприводу від 5 вольт;
- GND. Контакт для підключення землі;
- SIGNAL. Логічний контакт, який передає інструкцію у вигляді ШІМ сигналу від керуючої плати до модуля.

					КС 57. 15 001. 00 ДП ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		32



Рисунок 1.12. Сервопривод Tower Pro 9g SG90

1.2.4 Зумер. Звуковий пристрій

Зумер (або buzzer) це електронний звуковипромінюючий пристрій. Існує два типи зумерів: пасивний та активний. В дипломному проектуванні використовується пасивний, тому буде розглядатись лише він.

Дія пасивного зумера, який зображено на рис. 1.13, заснована на п'єзоелектричному ефекті. Коли на керамічний кристал подається змінний струм, він починає коливатися. Чим вище частота струму, тим швидше рухається кристал. Коливання кристалу заставляють мембрану коливатися, і саме ця мембрана і створює звукові хвилі, котрі чує людина.

Зумери використовують в кнопкових телефонах, у будильниках, в системах сигналізації. А також в будь яких системах, де потрібно сповістити людину звуком чи мелодією.



Рисунок 1.13. Пасивний зумер

					КС 57. 15 001. 00 ДП ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		33

1.2.5 Дисплей. Візуальне інформування користувача

LCD дисплей, або ще відомий як рідкокристалічний дисплей це різновид дисплеїв котрі можуть візуально відображати інформацію.

Принцип його роботи базується в трьох пластах:

1. пластина котра випромінює світло;
2. поляризатор;
3. рідкі кристали, підключені до електрода;
4. поляризатор під кутом 90° відносно першого поляризатора;
5. зовнішнє (захисне/кольорове) скло.

По-перше, потрібно дати живлення до світловипромінюючої пластини. По-друге, видати необхідну напругу до електрода, котрий з'єднаний до скляної капсули с рідкими кристалами. Коли живлення на електроди відсутнє, світло не проходить через два перпендикулярні шари поляризаторів, і екран вважається пустим. При початку живлення електродів, кристали починають викривляти світло, аж до 90° відносно другого поляризатора при зазначеній виробником напрузі (в середньому від 2 до 4 вольт). Один заживлений електрод викривляє світло для одного «пікселя» на екрані. В цьому і базується весь принцип роботи LCD дисплеїв.

Далі діло за правильним підключенням цих електронів для коректного виводу пікселів, щоб із пікселів збудувати символи, а із символів — слова.

В частині LSD дисплеїв комп'ютер, котрий відповідає за правильне підключення кристалів вже є вбудованим в мікросхему, що набагато полегшує роботу з дисплеями, особливо для початківців. Дисплей, використаний у проектуванні має назву LCD 1602A та має вбудований контролер HD44780, зображений на рис. 1.14.

Саме наявність вбудованого контролера дозволяє підключити дисплей до керуючої плати, використовуючи лише 4 контакти:

- VIN. Живлення модулю дисплея від 5 вольт;
- GND. Контакт для підключення землі;

					КС 57. 15 001. 00 ДП ПЗ	Арк.
						34
Змн.	Арк.	№ докум.	Підпис	Дата		

- SDA. Лінія передачі для відправки та прийому даних між модулем дисплею та керуючою платою;
- SCL. Лінія для задавання тактового сигналу, для забезпечення роботи лінії SDA. Він визначає моменти часу, коли пристрою можна записувати дані на плату, або їх зчитувати.



Рисунок 1.14. Дисплей LCD 1602A з вбудованим контролером

1.2.6 Клавiатура

Клавiатура (в даному випадку матрична клавiатура) це набір елементарних пристроїв — кнопок, з'єднаних між собою матричним способом.

При натисканні кожної кнопки, вона замикає контакти між відповідним стовпцем та рядком. Клавiатура циклічно посилає електричний імпульс (опитує) всі контакти по черзі, і в тих контактах, де супротив впав, це означає що контакт було з'єднано с землею, тобто кнопка була нажата. І так, знаючи зажатий рядок і стовпець, можна вичислити координати зажатої кнопки.

Матричні клавiатури широко використовуються у багатьох електронних пристроях завдяки їх простоті та надійності. Вони забезпечують зручність у користуванні та високу швидкість реакції на натискання. Схема проводки матричної клавiатури зображено на рис. 1.15.

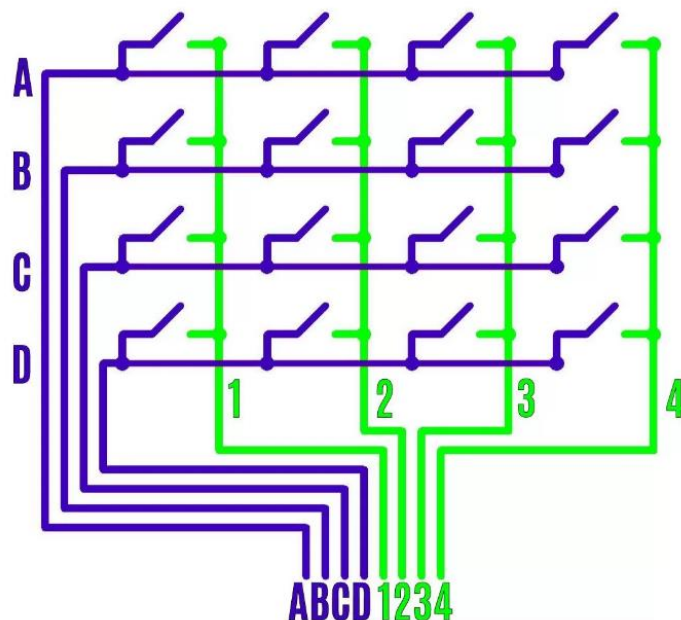


Рисунок 1.15. Спрощена схема матричної клавіатури

1.3 Побудова алгоритмів та схем системи

1.3.1 Моделювання системи. Побудова схем.

Побудування системи починається з тестового «стенду», який складається із всіх елементів керування. Тестове підключення відбувається через макетну плату, так званий «брідборд».

У збірці присутні елементи-зчитувачі:

- RFID-зчитувач;
- клавіатура;
- кнопка.

Блокувальним елементом виступає сервопривод. З додаткових елементів у системи присутні: дисплей та зумер. Всі елементи підключені до мікроконтролеру Arduino. Збірка через макетну плату зображена на рис. 1.16.

Така методика підключення дозволяє легко тестувати та швидко модифікувати систему перед її остаточним впровадженням. Після підключення на макетній платі, можна переходити до створення програмної логіки системи та написання програмного коду в програмі Arduino IDE.

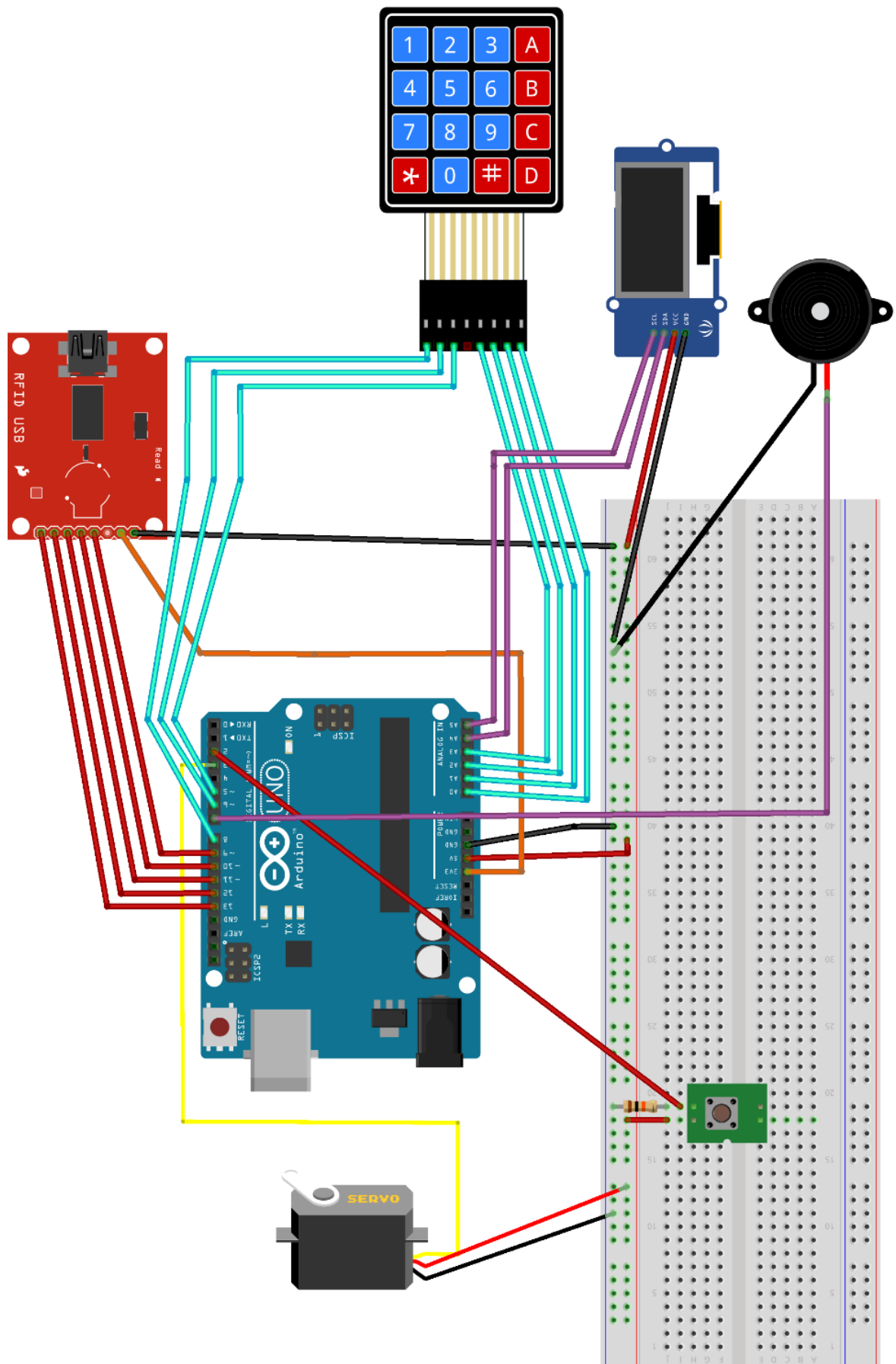


Рисунок 1.16. Візуальна схема підключення елементів системи через макетну плату

На макетній схемі підключення маємо наступні під'єднання елементів системи до плати Arduino:

- RFID-зчитувач під'єднано до живлення 3.3 V та GND. Контакти передачі даних підключені до D9, D10, D11, D12, D13;
- матрична клавіатура під'єднується до цифрових портів Arduino D5, D6, D8, A0. Та до аналогових портів, які налаштовані працювати в цифровому режимі A1, A2, A3;
- LCD-дисплей під'єднано до живлення 5V, GND. Та до портів A4, A5;
- зумер під'єднано до порту D7 та GND;
- сервопривод також під'єднується до 5V. Та до керуючого порту D3;
- кнопку під'єднано до живлення 5 вольт та до порту D2, який «прослуховує» натиск на кнопку. Також додано підтягуючий резистор.

1.3.2 Логіка програмного коду

При запуску системи, 3 паралельних (незалежних один від одного) процеси починають працювати в зацикленому режимі. Кожен паралельний процес відповідає за свій, окремий елемент доступу (зчитувач).

Перший процес найпростіший — відповідає за кнопку. Він відстежує натиск на неї, і коли вона була натиснута — Arduino посилає сигнал на до сервоприводу, тим самим відкриваючи доступ.

Другий процес відповідає за RFID-зчитувач. А саме чи піднесена мітка, та якщо вона піднесена: перевіряє чи збігається ідентифікатор закладений в мітці з таким у «білому списку» ідентифікаторів в системі. Якщо паролі збігаються — відкриває доступ.

Третій процес відповідає за клавіатуру. Він циклічно відстежує яка саме кнопка натиснута. Якщо натиснуто кнопку enter — то перевіряє, чи збігається введений пароль з паролем в системі. Якщо збігається — відкриває доступ.

Вищевказані умови можна відобразити у вигляді блок-схеми, де результатом є приведення сервоприводу до руху. Вказана на рис. 1.17 блок-схема позначає логіку елементів допуску та сервопривода.

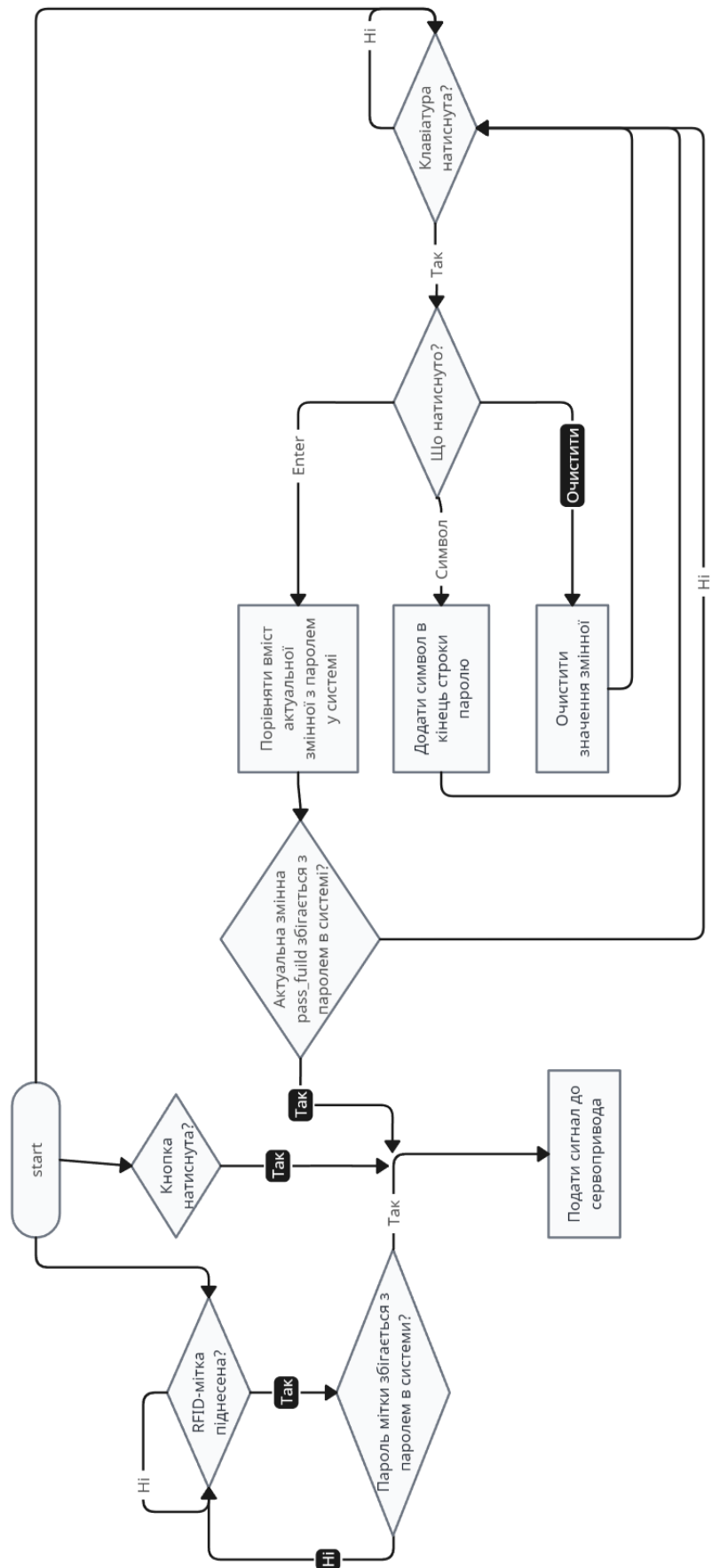
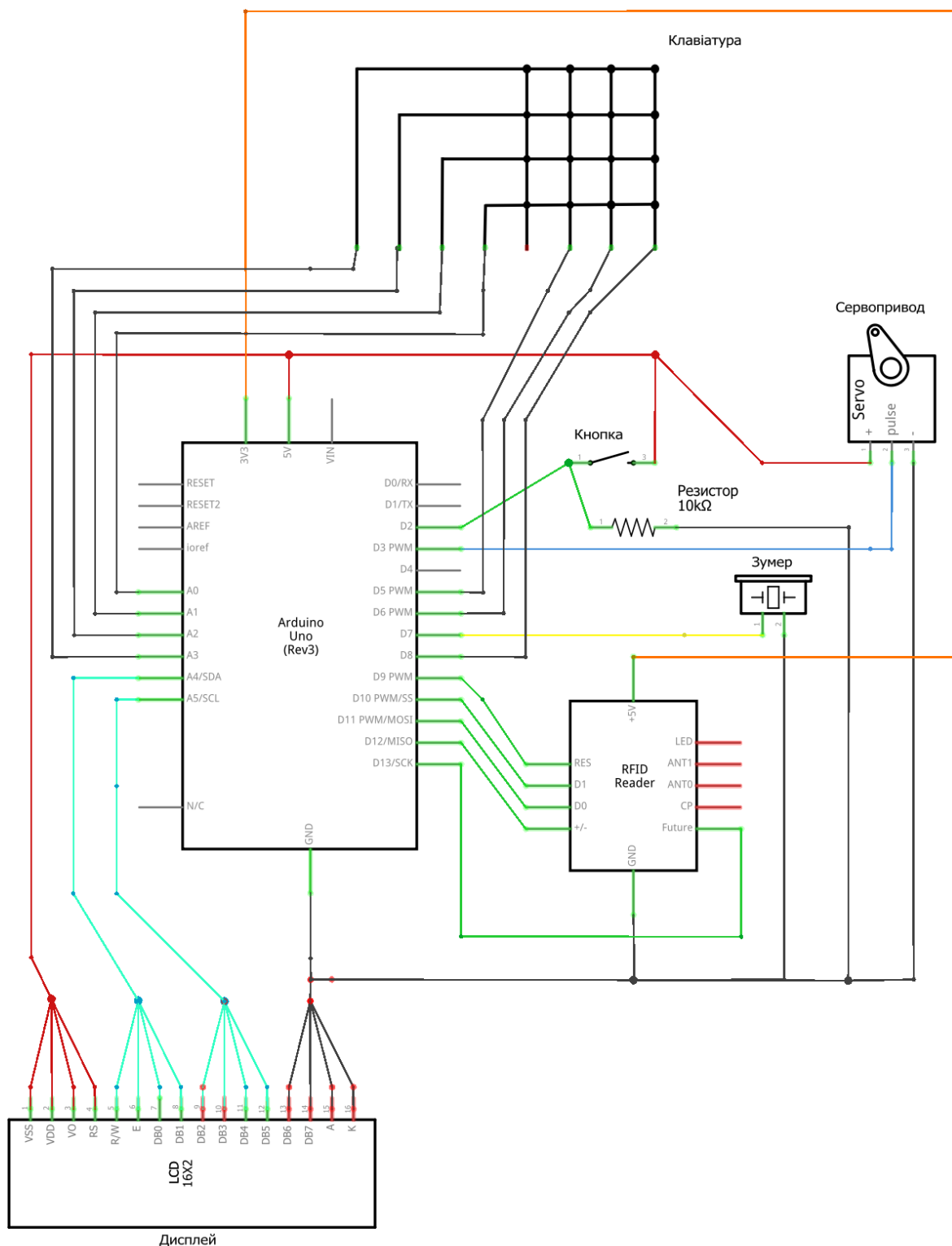


Рисунок 1.17. Блок-схема зчитувачів системи

1.3.3 Електрична функціональна схема

Функціональна схема системи, з вказанням всіх використаних елементів зображена на рис. 1.18.



fritzing

Рисунок 1.18. Функціональна схема СКД

					КС 57. 15 001. 00 ДП ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		40

1.4 Розробка системи. Програмний код

1.4.1 Принципи роботи контактів плати Arduino

Маючи логіку програми, наступним кроком є написання коду. Як було зазначено раніше, мікроконтролер Arduino працює на мові програмування C, з використанням додаткових функцій. Ці функції існують для спрощеного керування контактами (пінами) плати. Для розуміння роботи цих функцій, необхідно ознайомитись з типами портів. Їх існує два види: цифрові та аналогові.

Цифрові порти на платі Arduino Uno (загалом плата має 13 цифрових портів) можуть зчитувати напругу у двох станах: 1 (HIGH, напруга на контакті є) та 0 (LOW, напруги на контакті не має). Тоді як аналогові можуть зчитувати напругу з точністю 0.005 вольт (5 мілівольт), розбиваючи напругу від 0 до 5 вольт на 1024 пункти. Окрім зчитування, цифрові та аналогові контакти також можуть видавати напругу, але тільки у двох станах: 1 (контакт видає 5 вольт) та 0 (LOW, контакт не видає напругу).

Для більш точного виводу напруги, на платі Arduino є порти з широтно-імпульсною модуляцією (ШІМ). Вона дозволяє імітувати аналоговий сигнал, використовується у випадках, коли не можливе використання аналогових сигналів, як у випадку з Arduino. Принцип дії ШІМ полягає в короткочасному поданні та зупинці електричного сигналу з великою частотою (490Гц у випадку Arduino). На платі порти, які підтримують ШІМ розташовуються серед цифрових портів, але мають знак «~» (тільда) поруч з номером контакту.

Розуміючи принципи роботи контактів Arduino, можна виділити основні функції для їх роботи:

- pinMode(пін, режим). Функція яка використовується для задання режиму роботи цифрового контакту, де «пін» це номер контакту, а «режим» це один з двох варіантів роботи цього контакту: «input» - режим читання сигналу, або «output» - режим виводу сигналу;

					КС 57. 15 001. 00 ДП ПЗ	Арк.
						41
Змн.	Арк.	№ докум.	Підпис	Дата		

- `digitalRead(пін)`. Якщо функція `pinMode` лише задає режим роботи для контакту, то функція `digitalRead` в момент виклику зчитує напругу на контакті, і повертає «1» чи «0», в залежності від стану напруги в той момент;
- `digitalWrite(пін, значення)`. Функція використовується щоб задати електричний сигнал на контакт. Якщо «значення» є «1» або «HIGH», то контакт починає видавати напругу 5 вольт. Якщо «0» або «LOW», контакт починає працювати в режимі «землі»;
- `analogRead(пін)`. Функція схожа з `digitalRead`, але створена для роботи з аналоговими портами. Вона може повертати значення напруги від 0 до 1023, які відповідають значенням напруги від 0 до 5 вольт;
- `analogWrite(пін, значення)`. Аналог функції `digitalWrite`, але лише для цифрових портів, які мають ШІМ. Можуть імітувати вихід аналогового сигналу від 0 до 5 вольт. Аргумент «значення» може бути від 0 до 255, що розбивають 5 вольт на 256 кроків.

Код, записаний на плату Arduino також має свої особливості виконання, в порівнянні зі звичайним запуском коду на C. Код програми який має бути виконано, має бути вписаний у дві базові функції:

- функція `setup`. Весь код який було записано в функцію з цією назвою буде виконано одноразово при запуску плати. Загалом, сюди вписуються правила роботи портів, у якому вони будуть працювати, та початкові налаштування інших параметрів;
- функція `loop`. В даній функції, як правило, вписується весь код який має бути виконано на платі. Код, який вписано під функцію `loop` буде безкінечно виконуватись до тих пір, поки є живлення на плату.

1.4.2 Написання програмного коду

Початком коду є імпортування необхідних бібліотеки для керування елементами системи:

- `#include <MFRC522.h>` — бібліотека для керування RFID модулем;
- `#include <Servo.h>` — бібліотека для керування сервоприводом;

					КС 57. 15 001. 00 ДП ПЗ	Арк.
						42
Змн.	Арк.	№ докум.	Підпис	Дата		

- `#include <TaskScheduler.h>` — бібліотека для створення паралельних процесів
- `#include <Keypad.h>` — бібліотека для керування клавіатурою;
- `#include <LiquidCrystal_I2C.h>` — бібліотека для керування дисплеєм.

Позначення, на які порти Arduino підключенні різні елементи системи.

- `const int SERVO_PIN = 3;` — створення сталої з портом на який підключено сервопривод;
- `const int BUTTON_PIN = 2;` — створення сталої з портом на який підключено кнопку;
- `const int BUZZER_PIN = 7;` — створення сталої з портом на який підключено зумер.

Створення початкових налаштувань для RFID-зчитувача, зумера та LCD-дисплею.

`Servo servo;`

`String uid = " ";`

`MFRC522 mfrc522(SS_PIN, RST_PIN);`

`const int button = 2;`

`int servo_location_changer = 0;`

`LiquidCrystal_I2C lcd(0x27, 16, 2);`

Задавання змінних з початковими значеннями станів для кнопки

`boolean lastButtonState = LOW;`

`boolean currentButton = LOW;`

`int lastDebounceTime = 0;`

Внесення значення паролю в змінну «password», який має бути введеним через клавіатуру.

`const int password = "1234";`

`String pass_fuild = "";`

`int = "D33847A6";`

Створення масиву для матриці налаштування клавіатури

`Keypad my_pad = Keypad(makeKeymap(keypadd), row_pins, col_pins, ROWS, COLS);`

					КС 57. 15 001. 00 ДП ПЗ	Арк.
						43
Змн.	Арк.	№ докум.	Підпис	Дата		

Створення функції для циклічного відстеження статусу RFID-зчитувача

```
void RFID_checker(){
for (byte i = 0; i < mfrc522.uid.size; i++) {
```

Після зчитування мітки, записати значення ідентифікатора у змінну uidValue.

```
if(uidValue==card_id){
```

Перевірка, якщо код піднесеної мітки співпадає з закладеним у систему — відкрити сервопривод та програти мелодію:

```
else{
```

У випадку, якщо код мітки не співпадає з закладеним у систему — додати програвання звук «невдачі» та не посилати сигнал на сервопривод.

Створення функції для циклічного відстеження натиску на клавіатуру

```
void keypad_checker(){
char my_key = my_pad.getKey();
if ((my_key>'0'&my_key<'A') || (my_key=='0')){
```

Якщо натиснуто цифру, то додати її в значення змінної «password»

```
if (my_key=='Y'){
```

Якщо натиснуто клавішу «Ввід», перевірити, чи набраний пароль збігається зі змінною «password»

```
if (pass_fuild == password){
```

Якщо так, програти звук «успіху», відкрити сервопривод та відобразити результат на дисплеї

```
else{
```

Якщо пароль не збігається, програти звук «невдачі», відобразити результат на дисплеї та очистити значення змінної «password».

Після створення обох функцій, ініціалізувати їх паралельну циклічну роботу.

Створення умови, при якій виконується функція «button_pressed», якщо кнопку було натиснуто.

```
Task RFIDTask(200, TASK_FOREVER, &RFID_checker);
Task keypadTask(100, TASK_FOREVER, &keypad_checker);
```

Створення функції відстеження натиску на кнопку.

					КС 57. 15 001. 00 ДП ПЗ	Арк.
						44
Змн.	Арк.	№ докум.	Підпис	Дата		

Якщо кнопку було натиснуто, викликається дана функція:

```
void button_pressed(){  
if ((millis() - lastDebounceTime) > 2000) {  
if(servo_location_changer==0){
```

Якщо сервопривод знаходиться у закритому положенні — відкрити його. Якщо навпаки — то закрити. Також програти звук на зумері.

```
lastDebounceTime = millis();}}
```

Точка початку виконання коду. Функція «setup()»

```
void setup() {
```

Вивід на екран дисплею початковий текст з проханням прикласти мітку або ввести пароль.

```
lcd.begin();  
lcd.print("Tap your RFID or");  
lcd.print("enter the pass");
```

Ініціалізування очікування мітки на RFID зчитувачі

```
mfr522.PCD_Init();  
mfr522.PCD_DumpVersionToSerial();
```

Прив'язання сервоприводу до третього порту та задати початкове положення.

```
servo.attach(3);  
servo.write(90);
```

Прив'язання двох функцій до паралельних процесів

```
runner.init();  
runner.addTask(RFIDTask);  
runner.addTask(keypadTask);
```

Початок вічного циклу виконання трьох паралельних функцій

```
void loop() {  
runner.execute();}
```

					КС 57. 15 001. 00 ДП ПЗ	Арк.
						45
Змн.	Арк.	№ докум.	Підпис	Дата		

1.4.3 Побудування макетної системи

Завантаживши код на плату Arduino, елементи готові до їх встановлення на точку у приміщенні, яка стане системою керування допуском. В процесі роботи було створено макетну систему для пошуку можливих помилок в коді та інших недоліків у роботі системи. Макетна система зображена на рис. 1.19.

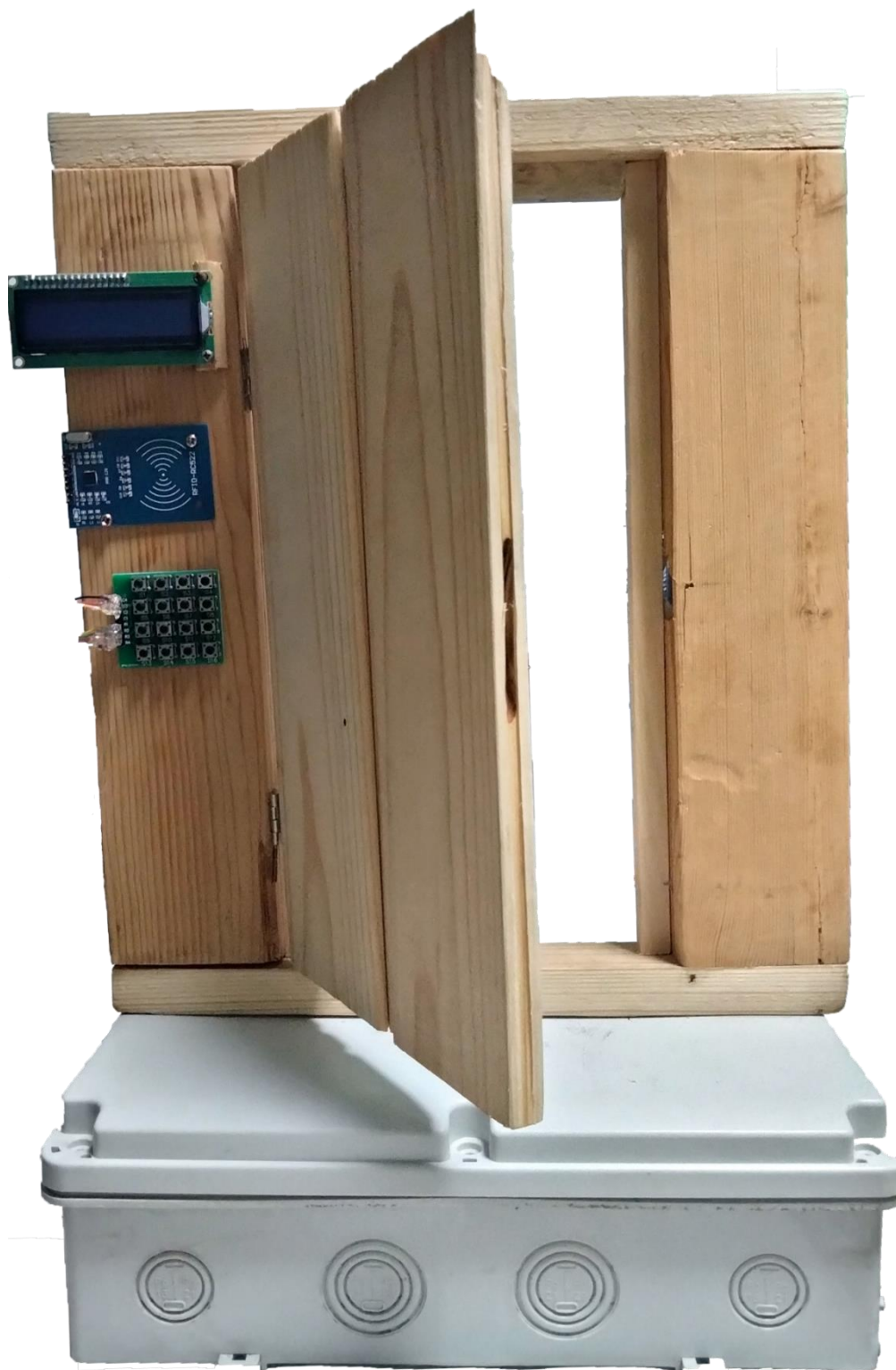


Рисунок 1.19. Макет системи керування доступом

					КС 57. 15 001. 00 ДП ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		46

Після завершення тестування та виправлення помилок в програмному коді та помилкових під'єднань елементів до портів Arduino, система готова до відтворення в стаціонарній точці на повномірній двері. Макетний пристрій, розроблений для тестування системи керування доступом, відіграє важливу роль у процесі виявлення та усунення недоліків до остаточного створення пристрою — системи керування доступом.

Макет повністю відображає функціональність майбутньої стаціонарної системи керування доступом.

Розробка макетного пристрою дозволила виявити декілька важливих аспектів для покращення кінцевої версії. Наприклад вдалося оптимізувати роботу дисплея та швидкість зчитування RFID-мітки для більш чіткого та швидкого інформування користувача та надання доступу.

Результати створення макетної системи підтвердили ефективність та надійність запропонованого рішення. Після проведених тестів та вдосконалень макет готовий до впровадження у реальних умовах. Встановлення такої системи керування доступом на підприємстві забезпечить високий рівень безпеки, контроль доступу до приміщень та облік робочого часу співробітників.

Створення макетної версії системи дозволило не лише перевірити працездатність усіх компонентів і програмного забезпечення, але й забезпечити впевненість у надійності кінцевого продукту. Було протестовано довготривалу роботу системи з відстеженням нагріву елементів. Визначено швидкість зчитування RFID-мітки (0.4 секунди) та відкриття блокувальника (0.2 секунди).

Макетний пристрій є яскравим прикладом того, як можна успішно використовувати сучасні технології для створення ефективних рішень у галузі безпеки.

					КС 57. 15 001. 00 ДП ПЗ	Арк.
						47
Змн.	Арк.	№ докум.	Підпис	Дата		

2 ЕКОНОМІЧНИЙ РОЗДІЛ

2.1 Аналіз виробу

Темою даного проекту є розробка системи керування доступом офісу підприємства на основі радіочастотного доступу. Дана робота містить різновиди елементів, які можуть бути використані в СКД, а також види систем та їх аналіз для різних ситуацій. В даному розділі було зазначено вартість використаних елементів та визначається вартісна оцінка розробленого пристрою. Спочатку визначається калькуляція розробленого виробу укрупненим методом через вартість покупних комплектуючих елементів і виробів, для визначення якої складаємо перерахування елементів і виробів на основі відомості специфікацій (принципової схеми) по формі, приведеної в табл. 2.1.

2.2 Розрахунки вартості та прибутку виробу

Таблиця 2.2.1. Розрахунок відомості покупних комплектуючих елементів

Найменування, тип, модель	Од.вим	Норма витрат на виріб	Ціна , грн.	Вартість комплектуючих
Мікроконтролер Arduino Uno	шт.	1	165	165
LCD-дисплей	шт.	1	92	92
Матрична клавіатура	шт.	1	41	41
Зумер	шт.	1	5.50	5.50
RFID зчитувач	шт.	1	75	75
RFID брелок	шт.	5	8	40
Кнопка	шт.	1	4	4
Сервопривід	шт.	1	50	50
Дроти	шт.	12	1.50	18
Загальна вартість покупних комплектуючих елементів				490.50
Транспортні витрати (10%)				50
Всього (В_{пк})				540.50

Калькуляцію планової собівартості розробленого виробу розраховуємо з використанням методу питомих ваг і структури собівартості аналогічної продукції.

					КС 57. 15 002. 00 ДП ПЗ	Арк.
						48
Змн.	Арк.	№ докум.	Підпис	Дата		

Тому що, проєктований виріб відноситься до радіоелектронної апаратури, то:

Питома вага матеріалу $\rightarrow \alpha_m = 20\%$;

Питома вага покупних виробів $\rightarrow \alpha_{пк} = 62\%$

Питома вага основної заробітної плати $\rightarrow \alpha_{озп} = 18\%$

Таблиця 2.2.2. Калькуляція планової собівартості

Найменування статті витрат	Значення статті, грн.	Розрахунок
1. Сировина і матеріал	174.35	$Вм = \alpha_m * B_{пк} / \alpha_{пк}$ $Вм = 0.20 \times 871.77 = 174.35$
2. Комплектуючі вироби і покупні напівфабрикати	540.50	$Впк = 540.50$
3. Основна заробітна плата	156.92	$Воз = \alpha_{озп} * B_{пк} / \alpha_{пк}$ $Воз = 0.18 \times 871.77 = 156.92$
4. Додаткова заробітна плата	62.77	$Вдз = 0,4 * Воз$ $Вдз = 0,4 * 156.92 = 62.77$
5. Відрахування до єдиного соцфонду	48.29	$Вес = (Воз + Вдз) * 0.22$ $Вес = (156.92 + 62.77) \times 0.22 = 48.29$
6. Загально-виробничі витрати	188.24	$Взаг.вир = (1,2 \dots 1,5) * Воз$ $Взаг.вир = 1.2 \cdot 156.87 = 188.24$
7. Виробнича собівартість	1171.01	$Свир = Вм + Впк + Воз + Вдз + Вес + Взаг.вир$ $Свир = 174.35 + 540.50 + 156.87 + 62.75 + 48.30 + 188.24 = 1171.01$
8. Адміністративні витрати	47.06	$Ва = Воз * 0,3$ $Ва = 156.87 \cdot 0.3 = 47.06$
9. Витрати на збут	23.42	$Взб = Свир * 0,02$ $Взб = 1171.01 \cdot 0.02 = 23.42$
10. Інші операційні витрати	11.71	$Воп = Свир * 0,01$ $Воп = 1171.01 \cdot 0.01 = 11.71$
Повна собівартість	1253.20	$Спов. = Свир + Ва + Взб + Воп$ $Спов = 1171.01 + 47.06 + 23.42 + 11.71 = 1253.20$

Розмір планового прибутку, що включається в ціну, визначаємо по формулі:

$$П = (Спов * p) / 100\% \quad (2.1)$$

$$П = (1253.20 * 20\%) / 100\% = 250.64$$

					КС 57. 15 002. 00 ДП ПЗ	Арк.
						49
Змн.	Арк.	№ докум.	Підпис	Дата		

де: ρ -планова рентабельність продукції (10%...30%)

Оптову ціну виробу визначаємо по формулі:

$$Ц_o = C_{\text{пов}} + П \quad (2.2)$$

Ціну реалізації виробу встановлюємо з урахуванням ПДВ:

$$Ц_p = Ц_o + П_z \quad (2.3)$$

де $П_z$ - податкове зобов'язання з ПДВ:

$$П_z = Ц_o * 0,2. \quad (2.4)$$

$$\text{Звідси: } Ц_o = 1253.20 + 250.64 = 1503.84$$

$$П_z = 1503.84 * 0.2 = 300.77$$

$$Ц_p = 1503.84 + 300.77 = 1804.61$$

2.3 Прогноз обсягів продаж даного виробу

Отримана в таблиці 2.2 повна собівартість являє собою витрати виготовлення (Спк) одиниці виробу для даного року виробництва. Запропонуємо прогноз обсягів продажів даного виробу на другій стадії життєвого циклу виробу «Виробництво» з розподілом по роках (прогноз продажів передбачаємо на 4 роки). Характерні зони промислового випуску виробу представлені на рис. 2.2.1.

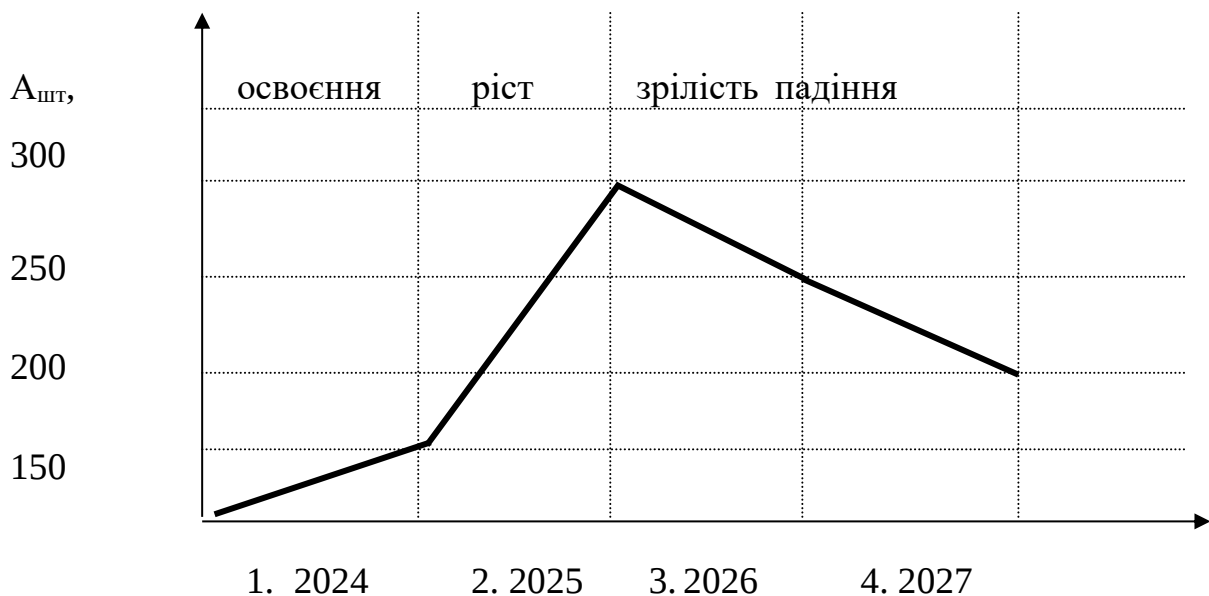


Рисунок 2.2.1. Зони промислового випуску виробу

В 2024 році обсяг продажів передбачається в розмірі 150 шт. під замовлення.

В наступному році прогнозується збільшення обсягу продажів, тому витрати виробництва визначаємо по формулі:

$$C_{\text{пов } i+1} = C_{\text{пов } i} \left(\frac{A_i}{A_{i-1}} \right)^{0.23}, \quad (2.5)$$

Де: A_i – обсяг продажів (виробництва) у 1 рік розрахункового періоду, шт;
 A_{i+1} – обсяг продажів (I+1)-ом року, шт.; 0,23 – показник ступеня, що характеризує вплив росту обсягів виробництва на собівартість продукції.

Звідси випливає, що

$$C_{\text{пов } 2025} = 1253.20 (150/300)^{0.23} = 1068,52$$

При відсутності росту обсягів виробництва, тобто якщо обсяг продажів або не змінюється або зменшується в наступному році, витрати виробництва приймаються на рівні попереднього року.

$$C_{\text{пов } 2026} = C_{\text{пов } 2027} = C_{\text{пов } 2028} = 1068,52$$

Плановий прибуток, що включається в оптову ціну підприємства, для наступного року при збільшенні обсягу продажів, визначаємо по формулі:

$$П_{i+1} = C_{ni+1} * \frac{\rho}{100} \quad (2.6)$$

Звідси:

$$П_{2025, 2026, 2027} = 1068,52 * (20\%/100) = 213,70$$

Оптову ціну підприємства в наступні роки розрахункового періоду визначаємо по формулі:

$$Ц_{O_{i+1}} = C_{n_{i+1}} + П_{i+1} \quad (2.7)$$

$$\text{Звідси: } Ц_{2025, 2026, 2027} = 1068,52 + 213,70 = 1282,22$$

Податкове зобов'язання визначається по формулі:

$$Пз_{i+1} = Ц_{O_{i+1}} * 0.2 \quad (2.8)$$

$$\text{Звідси: } Пз_{2025, 2026, 2027} = 1282,22 * 0.2 = 256,44$$

Ціну реалізації одиниці продукції в наступні роки визначаємо по формулі:

$$Ц_{P_{i+1}} = Ц_{O_{i+1}} + Пз_{i+1} \quad (2.9)$$

					КС 57. 15 002. 00 ДП ПЗ	Арк.
						51
Змн.	Арк.	№ докум.	Підпис	Дата		

$$\text{Звідси: } C_{p2025,2026,2027} = 1282,22 + 256,44 = 1538,66$$

Вартісну оцінку результатів за розрахунковий період (P_T) визначаємо по формулі:

$$P_T = \sum_{i=t_p}^{t_k} A_i * C_{p_i} * \alpha_i \quad (2.10)$$

де t_p, t_k – відповідно розрахунковий і кінцевий рік розрахункового періоду;

C_{p_i} – ціна реалізації в i -тім році, грн.; A_i – обсяг продажів у i -тім році, грн.; α_i – коефіцієнт, що включає фактор часу, тобто коефіцієнт приведення різночасних витрат і результатів до розрахункового року.

Коефіцієнт α_i визначаємо по формулі:

$$\alpha_i = |1 + E_H|^{t_p - t_i} \quad (2.11)$$

де E_H – норматив ефективності капітальних вкладень, $E_H = 0,1$;

t_p – розрахунковий рік розрахункового періоду; t_i – i -й рік розрахункового періоду, витрати і результати якого приводяться до розрахункового року.

Вартісну оцінку за розрахунковий період визначаємо по формі, приведеної в таблиці 2.3

$$B_{\text{оц}2024} = 1804.61 * 150 = 270691.5$$

$$B_{\text{оц}2025, 2026, 2027} = 1538,66 * 300 = 461598$$

Таблиця 2.2.3. Розрахунок вартісної оцінки результатів.

Найменування показника	Позначення	Розрахунок виробничого періоду				всього
		1-й	2-й	3-й	4-й	
Обсяг продажів, шт	A_i	150	300	250	200	900
Ціна реалізації, грн.	C_{p_i}	1804.61	1538,66	1538,66	1538,66	-
Вартісна оцінка результатів, грн.	$A_i * C_{p_i}$	270691.5	461598	461598	461598	1655485.5
Коефіцієнт, що враховує фактор часу	α_i	0,98	0,86	0,75	0,69	-
Вартісна оцінка результатів з урахуванням фактора часу, грн.	$A_i * C_{p_i} * \alpha_i$	265277.67	396974.28	346198.5	318502.62	1326953.07

Виробництво дає змогу одержати дохід за 4 роки 1 326 000 грн.

					КС 57. 15 002. 00 ДП ПЗ	Арк.
						52
Змн.	Арк.	№ докум.	Підпис	Дата		

3 РОЗДІЛ ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ

3.1 Аналіз небезпечних чинників

Електричні прилади мають підвищений рівень небезпеки для працівників при експлуатації. Для забезпечення коректного та безпечного використання системи керування допуском, користувач має бути проінструктованим щодо застережень та правил використання системи. Необережна взаємодія з електричним може призвести до термічного та електричного ураження тіла робітника, які можуть викликати різного виду травми. Завданням розділу з охорони праці є зведення до мінімуму ймовірності ураження робітника, та забезпечення його максимальної продуктивності праці. Перед початком експлуатації, кожен робітник має пройти інструктаж щодо правил використання системи.

Основним користувачем системи контролю допуску є співробітники, які взаємодіють з різними елементами системи. В системі створено три точки, через які користувач (співробітник) має взаємодіяти: RFID-сканер, клавіатура, кнопка.

При використанні електричного приладу співробітником, він може зіткнутися з певними ризиками при експлуатації системи. Нижче приведено список чинників які можуть загрожувати здоров'ю та продуктивності працівника: електричне ураження, термічне ураження, інфекційне зараження, електростатичне поле. Найнебезпечнішим фактором використання системи є електрична напруга, від якої даний прилад працює. Електричний удар може статися у разі пошкодження ізоляції проводів або при несанкціонованому доступі до внутрішніх компонентів системи. Для запобігання цьому, всі проводи повинні бути надійно ізольовані та захищені, а доступ до електричних компонентів обмежений лише кваліфікованим персоналом.

Слідством роботи будь якого електричного прибору є нагрів різної температури. При неправильному під'єднанні елементів або їх несправності, може статися перегрів обладнання. Перегрів елементу (або декількох елементів), може призвести до розплавлення чи деформації електронних компонентів, обмотки дротів, пластикових корпусів та інших частин системи. В залежності від елементу

					КС 57. 15 003. 00 ДП ПЗ	Арк.
						53
Змн.	Арк.	№ докум.	Підпис	Дата		

це може призвести до різних наслідків. З основних це створення перегрітим елементом короткого замикання, що в свою чергу може призвести до спалаху, а як результат — пожежі у приміщення.

Щоб уникнути цього, необхідно забезпечити достатній рівень циркуляції повітря у системі. Навіть при повністю справній системі, має місце нагрів елементів, і саме циркуляція повітря відіграє критичну роль у забезпеченні відведення тепла від пристроїв чи обладнання. Продуктивна циркуляція повітря допомагає підтримувати оптимальні температурні режими в пристроях. Також, регулярний технічний огляд та обслуговування системи допоможе завчасно виявити та замінити елементи, які вийшли з ладу та мають надмірну ступінь нагріву. Інфекційна складова також має своє місце. Система має матричну клавіатуру та кнопку, з якими співробітники будуть взаємодіяти. Такі, особливо шкідливі елементи потребують додаткової уваги, а саме регулярної профілактичної дезінфекції

Вплив зовнішніх факторів на роботу системи можуть впливати на систему керування допуском. Серед основних факторів слід виділити:

- температурні умови. Висока температура приміщення може впливати на електронні компоненти системи, викликаючи їх нестабільну роботу або пошкодження;
- вологість. Висока вологість може призводити до корозії самих елементів, контактних доріжок та інших електричних з'єднань. Волога сприяє окисленню контактів, а при її конденсації — до коротких замикань. Для запобігання вказаних ризиків, у приміщенні слід використовувати системи контролю вологості для підтримання оптимальної вологості;
- пил та бруд. Накопичення пилу та бруду на компонентах системи може призвести до зниження ефективності охолодження циркуляцією повітря, і як наслідок — призвести до перегріву елемента. Регулярне очищення зовнішніх елементів, та обслуговування внутрішніх допоможе зберегти елементи від перегріву від пилу.

					КС 57. 15 003. 00 ДП ПЗ	Арк.
						54
Змн.	Арк.	№ докум.	Підпис	Дата		

Електростатичне поле, яке генерується LCD-дисплеєм має значний біофізичний вплив на людину, найпримітнішим є вплив на нервові клітини. Воно може змінювати електричний потенціал нервових клітин, що впливає на передачу нервових імпульсів. Це може призводити до нервового перенапруження, головного болю, дратівливості та порушень сну. З часом такі зміни можуть викликати більш серйозні неврологічні проблеми. Електростатичне поле може спричиняти накопичення пилу на поверхні шкіри людини, що може призводити до подразнень, алергічних реакцій та запалень. Тривалий контакт з пилом може викликати дерматит та інші шкірні захворювання. Також, при вдихуванні повітря, цей пил потрапляє в організм і може викликати легеневі захворювання та алергічні реакції.

Основою системи є допуск на основі RFID технології. Вона використовує радіохвилі на частоті 13,56 МГц для обміну інформацією між зчитувачем та міткою, яку підносить співробітник. Радіохвилі на частоті від 1 МГц при проникненні через шкіряну поверхню людини викликають нагрів клітин, як зовнішніх, так і внутрішніх. Конкретний вплив радіохвиль на організм людини не є остаточно дослідженим, але деякі з досліджень припускають їх залежність з когнітивними та поведінковими функціями. В деяких дослідженнях помічалось порушення уваги та пам'яті, з'являлась тривожність та порушення сну. Хоча використаний у системі генератор радіохвиль є низькоінтенсивним, його впливом не можна нехтувати. При його використанні співробітникам слід триматись подалі від зчитувача при його використанні, тобто підносити мітку до зчитувача на відстані витягнутої руки, а також при зчитуванні мітки, одразу прибрати її від зчитувача задля запобігання надмірної генерації радіохвиль міткою.

3.2 Електробезпека

Забезпечення електробезпеки обслуговуючого персоналу. При обслуговуванні системи необхідно дотримуватися заходів, що мінімізують ризики ураження електричним струмом та інших наслідків. Перед початком роботи з системою кожен працівник має пройти інструктаж з електробезпеки. При проведенні обслуговування системи необхідно використовувати спеціальні засоби захисту, такі як діелектричні рукавиці, взуття та інші засоби, що захищають від

					КС 57. 15 003. 00 ДП ПЗ	Арк.
						55
Змн.	Арк.	№ докум.	Підпис	Дата		

можливого ураження електричним струмом. Регулярно проводити перевірку ізоляції проводів та компонентів системи на предмет пошкоджень. Всі виявлені дефекти мають бути усунені. Забезпечити надійне заземлення всіх металевих частин системи, що може запобігти утворенню потенціалу ураження у разі замикання.

Електробезпека. Перед встановленням системи, її дроти та інші елементи мають бути ізольованими від оточення. Мікроконтролер інші елементи, з якими користувач має взаємодіяти мають знаходитись у закритому вентильованому контейнері, а дроти які ведуть до органів керування та інформування — ізольованими.

3.3 Вимоги до приміщення

Приміщення, в якому має бути встановлено систему, має задовольняти ряду вимог, задля забезпечення безпеки та комфорту співробітників. Система встановлюється безпосередньо на двері, які ведуть у дане приміщення. Виходячи з аналізу чинників, вказаних у попередньому підрозділі, можна скласти перелік вимог для приміщення:

- розміри приміщення. Незважаючи на невеликі розміри системи, її органи керування мають бути встановлені у комфортному місці для їх використання. Елементи, які не потребують взаємодії з користувачем мають бути встановлені у місці, яке не буде заважати переміщенню та використанню системи користувачами;

- мікроклімат. Як було зазначено, вимогами до мікроклімату є вентиляція повітря, задля запобігання підвищеної вологості повітря, і як наслідок — конденсації вологи, та для регуляції температури навколо системи та працівників. Також, вентиляція (провітрювання) приміщення знизить наслідки електростатичного поля, які може створювати система;

- освітлення. Вимоги до освітлення полягають у безпечному використанні органів керування системою. Користувач має чітко бачити кнопки та інші елементи системи, для правильної та безпечної взаємодії з ними. Тривала робота з недостатнім освітленням може призвести до порушення якості зору.

					КС 57. 15 003. 00 ДП ПЗ	Арк.
						56
Змн.	Арк.	№ докум.	Підпис	Дата		

3.4 Пожежна безпека

Система управління доступом включає електронні компоненти, які можуть спричиняти загоряння у разі несправності або неправильного монтажу. У конструкції системи мають використовуватися матеріали, що не підтримують горіння та не виділяють токсичних речовин при нагріванні. Власник системи має встановити у приміщенні, де знаходиться система — вогнегасники, а саме розмістити їх у доступних місцях поблизу системи. Персонал повинен бути навчений користуванню вогнегасниками. Необхідно періодично проводити технічне обслуговування системи, що включає перевірку стану всіх компонентів на предмет перегріву та інших несправностей, що можуть спричинити пожежу. Важливим компонентом є встановлення в приміщенні системи автоматичного пожежогасіння та пожежної сигналізації, які дозволять швидко реагувати на виникнення пожежі та попередити співробітників.

При виникненні пожежі, система може створити небезпечну ситуацію для людей, які знаходяться у приміщенні. Суть системи — регулювати прохід людей до приміщення. Але при виникненні пожежі, вона не має створювати перешкоду для покидання приміщення. Для цього у системі передбачено кнопку, яка розташовується по той бік двері, вхід до якого і контролює система. Система не повинна розташовуватись регулюючою стороною до приміщення, яке веде до аварійного виходу з будинку. Так як система має підвищений рівень пожежної безпеки, поруч з встановленою системою, власник системи повинен встановити вогнегасник та проінструктувати персонал в його використанні. За необхідністю, власник системи може встановити у приміщенні додаткові елементи безпеки, такі як система автоматичного пожежогасіння, димові детектори, аварійне освітлення. Також, у приміщеннях мають бути установлені знаки з позначенням запасного виходу з будівлі. Такі знаки позначаються зеленим кольором з білими надписами «ВИХІД» або «Запасний ВИХІД» чи зображенням стрілки яка веде до запасного виходу.

					КС 57. 15 003. 00 ДП ПЗ	Арк.
						57
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

У роботі було розглянуто та проаналізовано різноманітні різновиди системи керування доступом. Сьогодні системи керування доступом використовується майже в кожному підприємстві. Вони є розповсюдженим і невід’ємним елементом його безпеки.

У роботі було проведено ознайомлення з поняттям системи, вказані його класифікації та розібрані компоненти, з якого він складається. Описано принципи роботи елементів, які можуть бути встановлено в систему. Зазначено переваги використання системи керування доступом у різних підприємствах та додаткові функції системи.

В ході роботи були створено блок-схему програмної логіки та створено функціональну схему. Розглянуто логіку функціонування коду в системі та створено програмний код прошивки мікроконтролера. Надано повну актуальну інформацію про стан доступних рішень встановлення системи. Написано код для прошивки мікроконтролеру Arduino мовою програмування C++.

Було виконані завдання з розробки алгоритму роботи системи керування доступом підприємства, та створенню структурної та функціональної схеми пристрою.

Результатом роботи стало конструювання макетної версії системи на основі RFID-технології, яка допоможе надійно контролювати пропуск людей до приміщення офісу.

Таким чином, виконана робота дозволила створити ефективне рішення для керування доступом на підприємстві, яке може бути адаптоване до різних умов і вимог. Система є надійним інструментом для забезпечення безпеки та організації контрольованого доступу до об’єктів. Дана робота демонструє можливості сучасних технологій у сфері безпеки та їхнє значення для захисту підприємств.

Виконана робота є важливим етапом на шляху до впровадження сучасних технологій у сфері безпеки та управління доступом на підприємствах.

					КС 57. 15 000. 00 ДП ПЗ	Арк.
						58
Змн.	Арк.	№ докум.	Підпис	Дата		

ПЕЛЕРІК ВИКОРИСТАНИХ ІНФОРМАЦІЙНИХ ДЖЕРЕЛ

- 1) Головін Ю. О. Основи радіозв'язку : підручник. Київ : КПІ ім. Ігоря Сікорського, Політехніка, 2021. 234 с.
- 2) Довгий С. О., Воробієнко П. П., Гуляєв К. Д. Сучасні телекомунікації : Мережі, технології, безпека, економіка, регулювання. С.О. Київ : Азимут-Україна, 2013. 608 с
- 3) Benantar, Messaoud. Access control systems. Security, identity management and trust models. Access Control Systems: Security, Identity Management and Trust Models, 2006
- 4) RC522 RFID Module. URL: <https://components101.com/wireless/rc522-rfid-module>
- 5) RC522 RFID Module: Pin Configuration, Arduino Wiring, Datasheet. URL: <https://www.easybom.com/blog/a/rc522-rfid-module-arduino-module-pin-configurations-tutorial>
- 6) RC522 RFID Module with Arduino. URL: <https://lastminuteengineers.com/how-rfid-works-rc522-arduino-tutorial/>
- 7) Arduino Analog Input Pins. URL: <https://docs.arduino.cc/learn/microcontrollers/analog-input/>
- 8) Мікроконтролер Arduino. URL: <https://bitkit.com.ua/shho-take-arduino>
- 9) Arduino Uno. URL: https://uk.wikipedia.org/wiki/Arduino_Uno
- 10) Системи контролю доступу: різновиди та поради щодо вибору. URL: <https://insider-media.net/life/systemy-kontroliu-dostupu-riznovydy-ta-porady-shchodo-vyboru>
- 11) Інтеграція з системами СКУД. URL: <https://ussi.com.ua/products/integracijni-mozhливosti>
- 12) How to Add a Simple Circuit to Your Arduino. URL: <https://www.digikey.com/en/maker/tutorials/2018/how-to-add-a-simple-circuit-to-your-arduino>
- 13) СИСТЕМА КОНТРОЛЮ ДОСТУПУ. URL: <https://www.arsenal-st.com.ua/skud/>

					КС 57. 15 000. 00 ДП ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		59

- 14) SG90 9 g Micro Servo. URL:
<https://www.friendlywire.com/projects/ne555-servo-safe/SG90-datasheet.pdf>
- 15) Servo Motor SG-90. URL: <https://components101.com/motors/servo-motor-basics-pinout-datasheet>
- 16) How LCDs Work. URL: <https://electronics.howstuffworks.com/lcd.htm>
- 17) Understanding LCD: How Do LCD Screens Work?. URL:
<https://riverdi.com/blog/understanding-lcd-how-do-lcd-screens-work>
- 18) How a Key Matrix Work. URL:
https://pcbheaven.com/wikipages/How_Key_Matrices_Works/

					КС 57. 15 000. 00 ДП ПЗ	Арк.
						60
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТОК А. Програмний код мовою C++ для прошивки мікроконтролеру Arduino

```
#include <MFRC522.h>
#include <Servo.h>
#include <TaskScheduler.h>
#include <Key.h>
#include <Keypad.h>
#include <Wire.h>
#include <LiquidCrystal_I2C.h>
#define RST_PIN      9
#define SS_PIN       10
Servo servo;
String uid = " ";
MFRC522 mfrc522(SS_PIN, RST_PIN);
const int button = 2;
int servo_location_changer = 0;
bool isTurning = false;
#define NOTE_E7 2637
#define NOTE_G7 3136
#define NOTE_A7 3520
#define NOTE_B7 3951
#define NOTE_C8 4186
#define NOTE_REST 0
int melody[] = {NOTE_E7, NOTE_G7, NOTE_A7, NOTE_B7,
NOTE_C8, NOTE_REST};
int noteDurations[] = {5000, 5000, 5000, 500, 5000, 10000};
boolean lastButtonState = LOW;
boolean currentButton = LOW;
```

```

int lastDebounceTime = 0;
LiquidCrystal_I2C lcd(0x27, 16, 2);
const int password = "1234";
String pass_fuild = "";
const byte ROWS = 4;
const byte COLS = 3;
char keypadd[ROWS][COLS]= {
    {'1','2','3'}, {'4','5','6'}, {'7','8','9'}, {'Y','0','N'}};
byte row_pins[ROWS]= {A3,A2,A1,A0};
byte col_pins[COLS]= {5,6,8};
Keypad my_pad = Keypad(makeKeymap(keypadd), row_pins,
col_pins, ROWS, COLS);
void RFID_checker(){
    if (!mfrc522.PICC_IsNewCardPresent())
        return;
    if (!mfrc522.PICC_ReadCardSerial())
        return;
    String uidValue = "";
    for (byte i = 0; i < mfrc522.uid.size; i++) {
        char hex[3];
        sprintf(hex, "%02X", mfrc522.uid.uidByte[i]);
        uidValue += hex;
    }
    if(uidValue=="D33847A6"){
        lcd.setCursor(0, 0);
        lcd.clear();
        lcd.print("Correct label!");
        lcd.setCursor(0, 1);
        lcd.print("Opening...");
        for (int i = 0; i < sizeof(melody) / sizeof(melody[0]); i++) {

```

```
        int duration = 1000 / noteDurations[i];
        tone(7, melody[i], duration);
        delay(200);
        noTone(7);
    }

    servo.write(0);
    delay(6000);
    servo.write(90);
    lcd.setCursor(0, 0);
    lcd.clear();
    lcd.print("Tap your label");
    lcd.setCursor(0, 1);
    lcd.print("or enter a pass");
}

else{
    lcd.setCursor(0, 0);
    lcd.clear();
    lcd.print("Wrong RFID label");
    lcd.setCursor(0, 1);
    lcd.print("Write to manager");
    tone(7, 100);
    delay(300);
    noTone(7);
    delay(1700);
    lcd.setCursor(0, 0);
    lcd.clear();
    lcd.print("Tap your label");
    lcd.setCursor(0, 1);
    lcd.print("or enter a pass");
}
```

```

}
void keypad_checker(){
    char my_key = my_pad.getKey();
    if ((my_key>'0'&my_key<'A') || (my_key=='0')){
        pass_fuild+=my_key;
        Serial.println(pass_fuild);
        lcd.clear();
        lcd.setCursor(0, 0);
        lcd.print(pass_fuild);
    }
    if (my_key=='Y'){
        Serial.println(pass_fuild);
        if (pass_fuild == password){
            pass_fuild="";
            lcd.clear();
            lcd.setCursor(0, 0);
            lcd.print("  SUCCESS!");
            lcd.setCursor(0, 1);
            lcd.print("  OPENING.");
            delay(700);
            lcd.clear();
            lcd.print("  SUCCESS!");
            lcd.setCursor(0, 1);
            lcd.print("  OPENING..");
            delay(300);
            lcd.clear();
            lcd.print("  SUCCESS!");
            lcd.setCursor(0, 1);
            lcd.print("  OPENING...");
            for (int i = 0; i < sizeof(melody) / sizeof(melody[0]); i++) {

```

```
    int duration = 1000 / noteDurations[i];
    tone(7, melody[i], duration);
    delay(200);
    noTone(7);
}

servo.write(0);
delay(6000);
servo.write(90);
lcd.setCursor(0, 0);
lcd.clear();
lcd.print("Tap your RFID or");
lcd.setCursor(0, 1);
lcd.print("enter the pass");
}

else{
    pass_fuild="";
    lcd.clear();
    lcd.setCursor(0, 0);
    lcd.print("WRONG!");
    lcd.setCursor(0, 1);
    lcd.print("Try again");
    tone(7, 100);
    delay(300);
    noTone(7);
    delay(1700);
    lcd.setCursor(0, 0);
    lcd.clear();
    lcd.print("Tap your label");
    lcd.setCursor(0, 1);
    lcd.print("or enter a pass");
```

```

    }
    }
    if (my_key=='N'){
        pass_fuild="";
        lcd.clear();
        lcd.setCursor(0, 0);
        lcd.print("Cleared!");
        lcd.setCursor(0, 1);
        lcd.print("Enter your pass");
    }
}

Scheduler runner;
Task RFIDTask(200, TASK_FOREVER, &RFID_checker);
Task keypadTask(100, TASK_FOREVER, &keypad_checker);
void setup() {
    Serial.begin(9600);
    while (!Serial);
    SPI.begin();
    mfrc522.PCD_Init();
    mfrc522.PCD_DumpVersionToSerial();
    Serial.println("Please, place RFID-label over the reader");
    pinMode(7, OUTPUT);
    servo.attach(3);
    servo.write(90);
    pinMode(button, INPUT_PULLUP);
    attachInterrupt(0, button_pressed, FALLING);
    lcd.begin();
    lcd.backlight();
    lcd.print("Tap your label");
    lcd.setCursor(0, 1);

```

```
lcd.print("or enter a pass");
runner.init();
runner.addTask(RFIDTask);
runner.addTask(keypadTask);
RFIDTask.enable();
keypadTask.enable();
}
void button_pressed(){
  if ((millis() - lastDebounceTime) > 2000) {
    isTurning = true;
    servo.write(0);
    lastDebounceTime = millis();
  }
}
void loop() {
  if (isTurning && millis() - lastDebounceTime < 6000) {
    for (int i = 0; i < sizeof(melody) / sizeof(melody[0]); i++) {
      int duration = 1000 / noteDurations[i];
      tone(7, melody[i], duration);
      delay(200);
      noTone(7);
    }
  }
}
```

ДОДАТОК Б. Слайди мультимедійної презентації

Створення системи керування доступом офісу підприємства на основі радіочастотного доступу

Виконав Новак Євгеній



Проектування системи керування доступом

Варіанти управління системою

1



RFID-зчитувач

Доступ на основі
радіочастотного
розпізнавання

2



Клавіатура

Введення пін-коду

3



Кнопка

Кнопка розташована по ту сторону
системи для зручного виходу з
приміщення

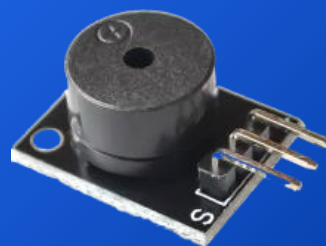
3

Інформування користувача

LCD-дисплей



Зумер



4



Що таке СКД? З чого вона складається?

- Зчитувач
- Ідентифікатор
- Мікроконтролер
- Блокувальник
- Допоміжні елементи (інформуючі)

5

Види систем керування доступом

Мережеві



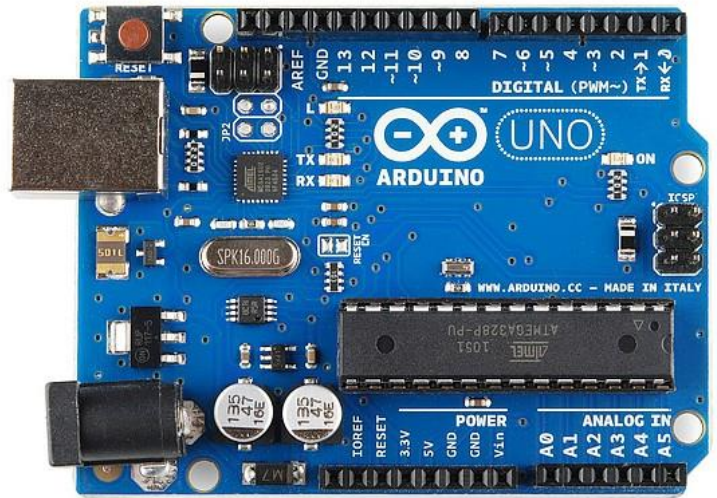
Автономні



6

Мікроконтролер Arduino UNO

- Плата для автоматизації пристроїв
- Має 13 цифрових та 6 аналогових контактів
- Частота 16 МГц, 32 кб flash-пам'яті
- Програмується на C++



7



RFID модуль RC-522

Безконтактна ідентифікація використовується у таких областях як:

- Системи керування доступом
- Сигналізація авто
- Автоматичне відстеження транспорту та товарів

Типи міток для радіо розпізнавання

- Read only
- Write Once Read Many
- Read and Write

Види за довжиною радіохвиль

- Високочастотні
- Ультрависокочастотні

8

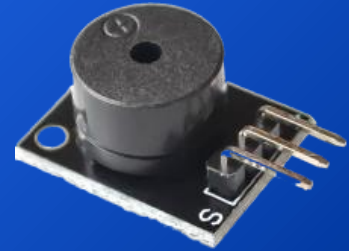
Сервопривод

- Подати ШІМ сигнал на контролер привода
- Контролер порівнює бажаний кут з реальним положенням валу
- Починається рух до врівноваження бажаного куту нахилу з реальним



Зумер

- Подати струм на керамічний кристал
- Кристал починає коливатись
- Коливання кристалу рухають мембрану, яка створює звукові хвилі



9

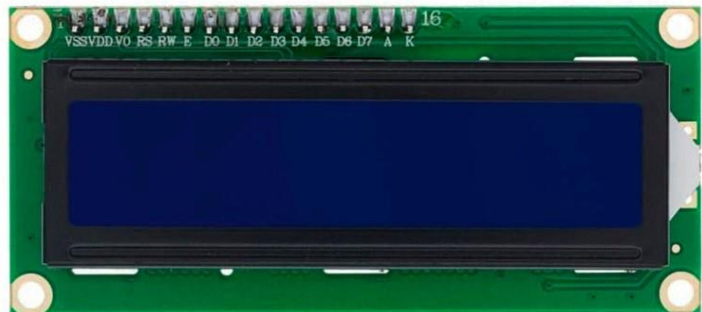
LCD-дисплей

Три групи елементів

- Світловипромінююча пластина
- Поляризатор
- Рідкі кристали

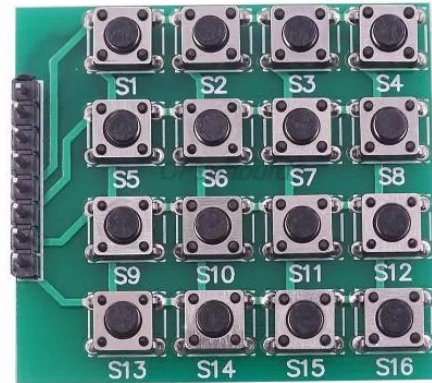
Принцип роботи дисплею

- Подати живлення до пластини та електроду
- Без живлення електроду, світло не може пройти через поляризатор
- При живленні електроду, кристали викривляють світло так, щоб воно мало можливість пройти через поляризатор

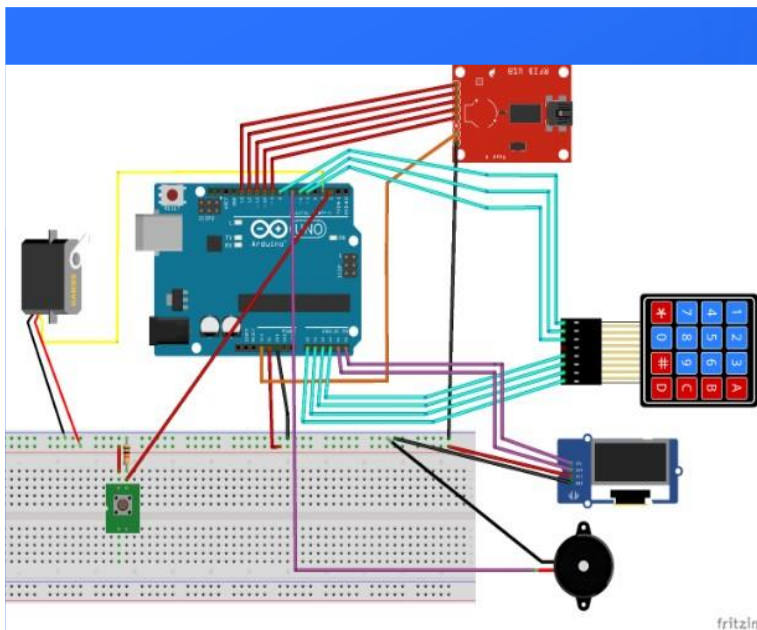


Матрична клавіатура

- Кнопки підключені матричним способом
- Мікроконтролер циклічно опитує контакти клавіатури
- При натиску кнопки, вона замикає відповідні контакти на землю



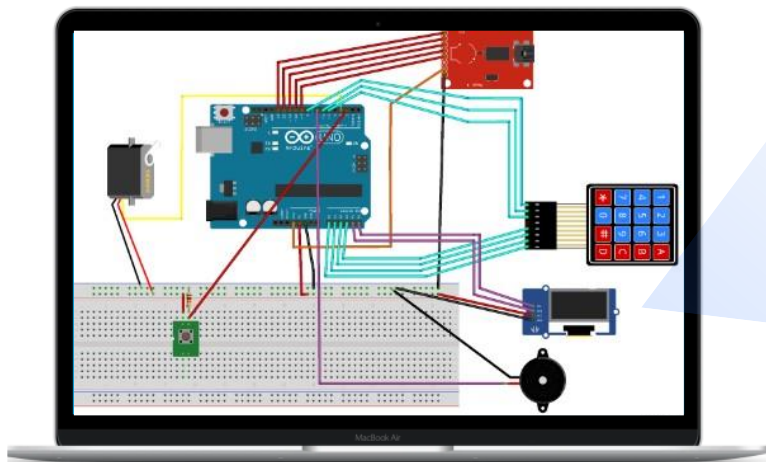
11



Побудування тестової системи

Через макетну плату

Таблиця підключень елементів до Arduino

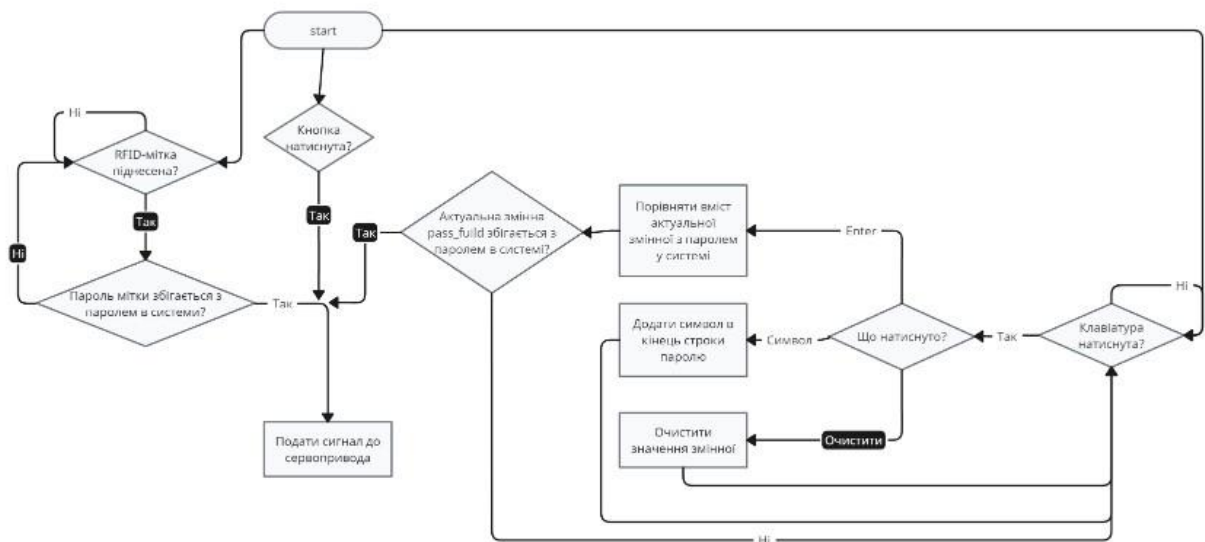


Назва елементу	Відповідний порт Arduino
RFID-зчитувач	D9, D10, D11, D12, D13, 3.3V, GND
Матрична клавіатура	D5, D6, D8, A0, A1, A2, A3
LCD-дисплей	A4, A5, 5V, GND
Зумер	D7, GND
Сервопривод	D3, 5V, GND
Кнопка	D2, 5V

Підключення всіх елементів до конкретних портів Arduino

13

Логіка програмного коду



Створення макетної системи

Виконав студент Новак
Євгеній

Дякую за увагу



ВІДГУК

керівника на дипломний проект здобувача освіти
відділення комп'ютерних систем

Новаку Євгенію Віталійовичу

(прізвище, ім'я та по батькові)

Спеціальність: 123 «Комп'ютерна інженерія»

Освітня програма: «Обслуговування комп'ютерних систем та мереж»

Тема дипломного проекту: Розробка системи керування доступом офісу підприємства на основі радіочастотного доступу.

ХАРАКТЕРИСТИКА ДИПЛОМНОГО ПРОЕКТУ

а) обсяг і якість виконання проекту (графічного матеріалу і розрахунково-пояснювальної записки) Згідно з індивідуальним завданням та темою дипломного проекту, пояснювальна записка виконана у достатньому обсязі, якісно. Відповідає розділам пояснювальної записки та відповідає етапам поставленого завдання. У достатньому обсязі виконано графічний матеріал, якісно. Графічний матеріал чітко демонструє результати роботи.

б) самостійність роботи над проектом: Студентом було самостійно обрано область та конкретну тематику дипломного проекту. Проведено детальний аналіз існуючих рішень і зроблено необхідні висновки для реалізації. Проявив навички самостійно шукати та опрацьовувати новий матеріал.

в) теоретична підготовка випускника (випускниці): Відповідає вимогам фахового молодшого бакалавру з напрямку підготовки «Обслуговування комп'ютерних систем та мереж».

г) вміння розв'язувати виробничі та конструкторські питання У дипломному
проекті було розглянуто та реалізовано актуальну тему керування
допуском персоналу на приміщення використовуючи систему контролю
допуску на основі RFID-технології. Проведено аналіз та порівняння
існуючих типів систем, та елементів, які в цих системах
використовуються.

Оцінка розрахункової частини

Відмінно

Оцінка графічної частини

Відмінно

Загальна оцінка

Відмінно

Прізвище, ім'я, по батькові керівника дипломного проекту

Б. Т. Н. Кільдішев Віталій Йосипович

Місце роботи і посада керівника дипломного проекту

Державний університет інтелектуальних технологій зв'язу,
доцент

Підпис

В.К.

«13» червня 2024 р.

РЕЦЕНЗІЯ

на дипломний проект (роботу) студента

Комп'ютерних систем

відділення

Новака Євгенія Віталійовича

(прізвище, ім'я та по батькові)

Спеціальність

123 «Комп'ютерна інженерія»

Керівник дипломного проекту (роботи)

Кільдішев Віталій Йосипович

(прізвище, ім'я та по батькові)

Тема дипломного проекту (роботи)

Розробка системи керування доступом офісу підприємства на основі
радіочастотного доступу.

Обсяг розрахунково-пояснювальної записки 75 сторінок

Обсяг графічної частини проекту 15 аркушів

ХАРАКТЕРИСТИКА ДИПЛОМНОГО ПРОЕКТУ (РОБОТИ)

а) Висновок про ступінь відповідальності виконаного дипломного проекту (роботи) завданню

Робота в повній мірі відповідає технічному завданню до дипломного проекту.
Виконана у відповідності з усіма вимогами.

б) Характеристика виконання кожного розділу проекту ступеню використання дипломником
останніх досягнень науки та техніки, передових методів на виробництві

У результаті виконання дипломного проекту студент продемонстрував уміння
шукати, оброблювати та використовувати новітні досягнення науки та техніки,
уміння працювати з літературою.

в) Оцінка якості виконання графічної частини проекту (роботи) і пояснювальної записки

Графічна частина завдання в повній мірі відповідає вимогам, виконана якісно та відображає всі основні елементи проектування системи.

г) Перелік позитивних якостей дипломного проекту (роботи)

Тема дипломного проекту дійсно є актуальною, виконана якісно, у достатньому обсязі та відповідно до поставленого завдання.

д) Основні недоліки дипломного проекту

У тексті пояснювальної записки відсутня частина посилань на використану літературу, слід було б детальніше розглянути актуальність роботи, уже існуючі на даний момент технології. Однак, дані зауваження не применшують актуальність роботи та її якість

Оцінка розрахункової частини Добре

Оцінка графічної частини Добре

Загальна оцінка Добре

Прізвище, ім'я по батькові к.т.н. Селіванова Алла Віталіївна

Місце роботи і посада рецензента Одеський національний технологічний університет, декан факультету комп'ютерної інженерії, програмування та кіберзахисту

13.06.2024 р.

Ім'я користувача:
Катерина Григоріївна Краснокутська

Дата перевірки:
08.06.2024 16:46:06 EEST

Дата звіту:
08.06.2024 17:33:05 EEST

ID перевірки:
1016335584

Тип перевірки:
Doc vs Internet + Library

ID користувача:
100011688

Назва документа: 4КС-57_Євгеній_Новак

Кількість сторінок: 55 Кількість слів: 7859 Кількість символів: 58552 Розмір файлу: 2.41 MB ID файлу: 1016136273

6.62% Схожість

Найбільша схожість: 3.65% з Інтернет-джерелом (<https://card-file.ontu.edu.ua/server/api/core/bitstreams/cd248b04-311>).

6.62% Джерела з Інтернету

296

Сторінка 57

Не знайдено джерел з Бібліотеки

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0% Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи

20

**ДОЗВІЛ
НА РОЗМІЩЕННЯ
ВИПУСКНОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ
В ЕЛЕКТРОННОМУ РЕПОЗИТАРІЇ ВСП «ОТФК ОНТУ»**

Ми, що нижче підписалися,

Новак Євгеній Віталійович,
здобувач освіти гр. 4КС-57, та

Кільдішев Віталій Йосипович,
керівник випускної кваліфікаційної роботи,

не заперечуємо щодо розміщення електронного варіанту пояснювальної записки до випускної кваліфікаційної роботи бакалавра на тему:

«Розробка системи керування доступом офісу підприємства на основі радіочастотного доступу» (автор роботи – Новак Є.В., керівник роботи – Кільдішев В.Й.)

виконаного у ВСП «Одеський технічний фаховий коледж Одеського національного технологічного університету» в 2024 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



/ Новак Є.В. /

Керівник



/ Кільдішев В.Й. /

«13» червня 2024 р.