МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Сумський державний університет

Факультет електроніки та інформаційних технологій

Кафедра електроніки і комп'ютерної техніки

«До захисту допущено»

Завідувач кафедри ЕКТ

_____ Анатолій ОПАНАСЮК

(підпис)

____ _____ 2024 р.

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня «бакалавр»

зі спеціальності 171 «Електроніка»

освітньо-професійної програми «Електронні системи та компоненти»

на тему:

ПРИСТРІЙ УПРАВЛІННЯ КОНТРОЛЕМ ДОСТУПУ

Здобувача групи ЕС-01 Базюри Богдана Володимировича

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

_____ Богдан БАЗЮРА

(підпис)

Керівник, доцент, к.т.н. Віталій ГРИНЕНКО _____

(підпис)

Суми – 2024

Анотація

Робота містить: 48 сторінок, 21 рисунок, 2 таблиці, 15 джерел літератури.

Мета роботи полягає в розробці пристрою управління контролем доступу, який забезпечує високий рівень безпеки та ефективності.

У ході виконання роботи було проведено аналіз існуючих технологій контролю доступу, розробку алгоритму роботи, структурну, функціональну та принципову схеми пристрою та розробку програмного забезпечення.

За основу було взято мікроконтролер ATMega328P, зчитувачі RC522, символьні дисплеї LCD1602, модуль Wi-Fi ESP-01S, пасивні зумери KY-006, модуль пам’яті W25Q128JVSIG та електромагнітний замок Trinix TML-200.

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Факультет електроніки та інформаційних технологій

Кафедра електроніки і комп'ютерної техніки

Напрям підготовки 171 Електроніка

Освітня програма Електронні системи та компоненти

ЗАТВЕРДЖУЮ

Зав. кафедрою Опанасюк А. С.

"___"_____ 2024 р.

З А В Д А Н Н Я

на кваліфікаційну роботу бакалавра

Базюра Богдан Володимирович

1. Тема роботи Пристрій управління контролем доступу.

затверджена наказом по університету "13" березня 2024 р. № 0256-VI.

2. Термін здачі студентом завершеної роботи "6" червня 2024 р.

3. Вихідні дані до роботи 1. Ідентифікація користувачів за допомогою RFID технологій; 2. Двонаправлений контроль доступу через одну точку проходу; 3. Ведення журналу подій; 4. Віддалене управління пристроєм; 5. Інтеграція з іншими системами безпеки.

4. Зміст розрахунково-пояснювальної записки (перелік питань, що належить розробити) 1) Огляд літератури та постановка задачі роботи. 2) Розробка алгоритму роботи проектованого електронного пристрою. 3) Розробка структурної схеми проектованого електронного пристрою. 4) Розробка функціональної схеми проектованого електронного пристрою. 5) Розробка принципових схем блоків проектованого електронного пристрою. 6) Розробка програмного забезпечення проектованого електронного пристрою (при необхідності).

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень) 1) Схема алгоритму. 2) Схема електрична структурна. 3) Схема електрична функціональна. 4) Схема електрична принципова.

6. Дата видачі завдання "14" лютого 2024 р.

7. Керівник роботи Гриненко Віталій Вікторович

8. Завдання прийняв до виконання _____

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назва етапів дипломного проекту	Термін виконання етапів роботи	Примітки
1	Огляд літератури та постановка завдання проектування	06.05.24 – 09.05.24	
2	Розробка структурної схеми проектованого електронного пристрою	10.05.24 – 13.05.24	
3	Розробка алгоритму роботи проектованого електронного пристрою	14.05.24 – 16.05.24	
4	Розробка функціональної схеми проектованого електронного пристрою	17.05.24 – 22.05.24	
5	Розробка принципових схем блоків проектованого електронного пристрою	23.05.24 – 30.05.24	
6	Розробка програмного забезпечення проектованого електронного пристрою	31.05.24-04.06.24	
7	Оформлення пояснювальної записки	05.06.24 – 07.06.24	
8	Оформлення графічного матеріалу	08.06.24 – 09.06.24	
9	Представлення роботи керівнику і отримання відгуку	10.06.24	
10	Представлення роботи кафедрі для отримання рецензії	10.06.24	

Студент _____

Керівник роботи _____

«___» _____ 2024 р.

Зміст

Умовні позначення та скорочення

ПУКД – пристрій управління контролем доступу;

СКД – система контролю доступу;

СКУД – система контролю та управління доступом;

ОРЧ – облік робочого часу;

RFID (Radio frequency identification) – радіочастотна ідентифікація;

EEPROM (Electrically Erasable Programmable Read-Only Memory) – програмована пам'ять тільки для читання з електричним стиранням;

UID (User identifier) – ідентифікатор користувача.

Вступ.

У сучасних умовах, забезпечення безпеки приміщень стало вирішальною складовою для успішного функціонування будь-якої організації, незалежно від її розміру чи сфери діяльності. Небезпека несанкціонованого доступу, викрадення матеріальних цінностей або виток конфіденційної інформації ставить під загрозу не лише фізичну безпеку, але й стабільність та довіру до організації. У зв’язку з цим, впровадження надійних систем контролю доступу стає невід'ємною необхідністю.

Технологічний прогрес та розвиток електронних систем безпеки призвели до появи ефективних засобів захисту, які дозволяють ефективно контролювати доступ до будь-яких приміщень. Пристрої управління контролем доступу створюють надійні бар'єри, які заважають несанкціонованому проникненню в об'єкт. Вони забезпечують ефективну ідентифікацію та авторизацію користувачів, моніторять та реєструють всі події доступу, забезпечуючи тим самим високий рівень безпеки.

Ці системи демонструють свою корисність не лише для захисту від потенційних загроз, але й для підвищення ефективності управління приміщеннями. Інтеграція пристроїв управління контролем доступу з іншими системами безпеки, такими як відеоспостереження та системи сигналізації, дозволяє створити комплексну систему моніторингу та реагування на будь-які потенційні загрози. Цей підхід забезпечує не лише захист від потенційних атак, але й можливість оперативно реагувати на будь-які події та зберігати дані для подальшого аналізу, що робить його незамінним елементом сучасної безпекової інфраструктури.

Метою кваліфікаційної роботи є дослідження сучасних технологій і методів, що використовуються у пристроях управління контролем доступу для забезпечення безпеки приміщень, а також розробка прототипу такого пристрою. У роботі розглянуто весь спектр аспектів, пов'язаних з проектуванням та розробкою пристрою управління контролем доступу. Проведено аналіз існуючих наукових та технічних публікацій, проаналізовано поточний стан технологій контролю доступу, виявлено основні проблеми та визначено завдання для вирішення в рамках даної роботи. Також розроблено загальну структуру пристрою, що включає всі необхідні компоненти та їх взаємозв'язки. Розроблено детальну схему, що відображатиме функції кожного компонента та їх взаємодію, а також

детальні електронні схеми окремих модулів системи, розроблені. Крім цього, розроблено програмне забезпечення, яке забезпечить коректну роботу всіх компонентів системи, включаючи інтерфейси для користувачів та адміністраторів.

1. Огляд літератури та постановка завдання.

1.1 Огляд пристрою управління контролем доступу.

Пристрій управління контролем доступу або система контролю доступу (СКД/СКУД) – це комплекс технічних та програмних засобів безпеки, що здійснює регулювання входу, виходу та переміщень людей чи транспортних об’єктів на територіях, які знаходяться під охороною, для адміністративного моніторингу та попереджень несанкціонованого проникнення.

Завдання, що вирішує система контролю доступу:

1. Безпека об’єкта. Система контролю і управління доступом грає важливу роль в комплексній системі охорони підприємства, забезпечує збереження майна споруд і працівників.

2. Облік робочого часу персоналу. Невід'ємною рисою сучасних СКУД є можливість здійснення обліку робочого часу співробітників. Облік робочого часу (ОРЧ) – це програмно-апаратний комплекс. Програмне забезпечення дозволяє керувати відвідуваністю, виробляти онлайн-моніторинг і будувати більше 15 різних звітів про відвідуваність.

3. Скорочення витрат. Правильно спроектована та інстальована СКУД дозволяє знизити витрати на охорону. Крім цього, сучасні системи контролю доступом містять великий потенціал до скорочення постійних витрат за рахунок автоматизації процесів.

Елементи та принцип роботи системи контролю доступу:

1. Ідентифікатори. Це ключові елементи, що встановлюють право доступу особи на контрольну територію.

2. Зчитувачі. Спеціальні пристрої, що зчитують та передають інформацію з ідентифікатора на контролер.

3. Контролери. Пристрій, що на основі отриманих даних приймає рішення щодо надання чи заборони доступу.

4. Виконавчі пристрої. Фізично перешкоджають доступу до контрольованого об’єкту.

1.2 Способи ідентифікації.

1. Магнітні картки – це вид пластикових карт, обладнаних магнітною смужкою, яка містить інформацію про власника або користувача. Ці карти

широко використовуються для реалізації систем контролю доступу, а також у фінансових установах для здійснення операцій з банківськими рахунками.

Для зчитування таких карток використовуються так звані рідери. Така назва дісталася пристрою від англомовної назви зчитувачів магнітної смуги – Magnetic Stripe Reader. Зчитувачі магнітних карт умовно поділяються на:

– Ручні. В таких зчитувачах користувач самостійно переміщає магнітну смугу вздовж магнітної головки зчитувача;

– Автоматизовані. Такий пристрій виконує всі необхідні для зчитування операції самостійно.

В процесі зчитування картка стикається з пристроєм, що з часом зношує нанесену магнітну смугу і пластик. Постійне використання такої картки призводить до появи на поверхні подряпин. Тому наразі такий спосіб ідентифікації в системах контролю доступу майже не використовується.

2. Радіочастотна ідентифікація (Radio Frequency Identification, скорочено RFID) — це сучасна технологія автоматичної ідентифікації, що дозволяє автоматизувати процес збору та обробки інформації безконтактним способом.

RFID — безконтактна технологія, носієм інформації є радіохвиля. Для забезпечення роботи системи не потрібен ні контакт зі зчитувачем, ні пряма видимість зчитувача на відміну від систем з магнітних карт.

RFID–міткою називають мініатюрний запам'ятовуючий пристрій. В його основі лежить мікрочип, який зберігає інформацію, а також антена, яка відповідає за передачу та отримання даних.

Типи RFID-міток по частоті роботи:

– Низькочастотні мітки LF (Робоча частота 125 – 134 кГц, дистанція зчитування до 10 см) Невелика дальність передачі даних, схильні до ефекту колізії.

– Високочастотні HF (Робоча частота 13,56 МГц, дистанція зчитування до 5 см) Перевагою RFID мітки 13.56 МГц є незалежна пам'ять EEPROM з захищеною областю, доступною для перезапису. Це забезпечує додатковий захист даних і дозволяє використовувати мітки в складних системах аутентифікації.

– Ультра високочастотні UHF (Робоча частота 860 – 960 МГц, дистанція до 18м) Безконтактна UHF мітка відрізняється великою дальністю зчитування, високою швидкістю і підтримкою механізму антиколізії. Мітка UHF

RFID оптимально підходить для ідентифікації рухомих і стаціонарних об'єктів, може використовуватися в складних умовах експлуатації.

Ця мітка може бути активною (працювати від джерела живлення), або пасивною (живляться від отриманого антеною сигналу з зчитувача). Мітки можуть мати різні форми і розміри, вони можуть бути вбудовані в картки, брелоки, браслети, ключі або навіть безпосередньо в предмети.

Для зчитування таких міток використовують RFID зчитувачі. Зчитувач генерує магнітне поле, яке створює електричний струм у котушці індуктивності мітки, який заряджає конденсатор. Конденсатор запитує мікросхему, що передає інформацію на зчитувач. Як і мітки, зчитувачі класифікуються за частотою роботи, але на відміну від міток, зчитувачі можуть одночасно працювати в декількох частотних діапазонах, такі зчитувачі називають універсальними.

Зчитувачі карток бувають внутрішнього і зовнішнього виконання, тобто деякі можуть працювати в широкому діапазоні температур і перебувати під дощем на вулиці, інші зчитувачі карток можуть працювати тільки в теплому і сухому приміщенні. Так само бувають зчитувачі безконтактних карток, виконані в антивандальному металевому або навіть броньованому корпусі. Часто зчитувачі випускаються в комбінованих варіантах, наприклад, зчитувач карт доступу може бути в одному корпусі з кодовою панеллю або біометричним датчиком, який зчитує відбиток пальця.

Зчитувачі можуть працювати як самостійний пристрій, фактично будучи контролером системи контролю доступом, тобто зберігати в собі дані про паролі та мітки відвідувачів, а також можуть керувати електрозамками. Зчитувачі карт доступу можуть працювати і у складі повноцінних СКУД з центральним контролером, тоді всі функції контролю приймає центральний контролер системи керування доступом. У такому разі завдання зчитувача – отримати дані з безконтактної мітки та передати їх «нагору».

На даний момент RFID є найпопулярнішим способом ідентифікації в системах контролю доступу, через свою доступність, простоту, зручність, швидкість роботи та універсальність.

3. Біометрична ідентифікація. Біометричні системи контролю доступу використовують для ідентифікації біометричних параметрів людини, які є унікальними в кожного. Працює дана система досить просто, для того щоб потрапити в приміщення достатньо просто приставити палець до біометричного

сканера, ідентифікація триватиме всього декілька секунд, та при цьому обдурити ристрій практично нереально.

На відміну від інших способів, біометрична ідентифікація не потребує хоча й не виключає використання ключів чи карток доступу. У біометричній ідентифікації основою є використання унікальних фізичних характеристик особи, таких як відбиток пальця або розпізнавання обличчя, для підтвердження ідентичності. Це забезпечує вищий рівень безпеки та зручності для користувачів, оскільки вони можуть здійснювати доступ без необхідності носити або запам'ятовувати додаткові предмети чи паролі. Однак біометрична ідентифікація часто може доповнюватися традиційними методами доступу, забезпечуючи додаткові шари безпеки та гнучкість в управлінні доступом.

При виборі біометричної ідентифікації необхідно враховувати потребу захисту особистих даних, пов'язаних з використанням біометричних технологій. Оскільки біометричні дані є унікальними та не змінюються протягом життя, їх зберігання і обробка вимагають особливої уваги до безпеки. Це означає, що система повинна мати надійний механізм захисту від несанкціонованого доступу до біометричних даних, а також забезпечувати шифрування і захист передачі цих даних по мережі.

1.3 Типи виконавчих пристроїв.

1. Електрозамки. Електромеханічні і електромагнітні замки - це два різних типи механізмів, які використовуються для контролю доступу, але вони мають деякі відмінності у принципах роботи та застосуванні.

Основний принцип роботи електромеханічного замка полягає в тому, що він використовує механічний механізм (наприклад, замок з ключем), який керується електрично. При введенні правильного сигналу або сигналу керування, механічний механізм розблоковується, дозволяючи відкрити двері або ворота.

Ці замки можуть включати в себе різноманітні механізми блокування, такі як циліндрові замки або засувки, які управляються електрично. Вони зазвичай використовуються там, де необхідно обмежувати доступ за допомогою ключа або коду.

Електромеханічні замки надають доволі високий рівень безпеки. Проте вони можуть бути менш надійними у порівнянні з електромагнітними замками через можливість втрати ключа або злому механічних частин.

Електромагнітні замки працюють на принципі електромагнітного поля. Зазвичай електромагнітний замок складається з електромагнітної котушки і металевої пластини, розташованої на дверях або воротах. При включенні струму через котушку, створюється магнітне поле, яке притягує металеву пластину, утримуючи двері закритими.

Перевагами електромагнітних замків є їхня висока безпека. Вони мають міцне утримання завдяки якому відкрити двері без дозволу майже неможливо. Крім того, вони енергоефективні, споживаючи електроенергію лише під час розблокування або блокування. Ще однією перевагою є їх універсальність. Електромагнітні замки можуть бути встановлені на різних типах дверей, від стандартних до важких промислових дверей.

2. Турнікети - поширене обладнання систем контролю доступу, яке застосовується в інтеграції з іншими системами безпеки. Вони давно стали звичним засобом забезпечення порядку і безпеки. Економлячи нерви і кошти, вони надійно працюють на прохідних, в закритих зонах підприємств і всюди, де необхідно здійснити контроль і управління доступом. До турнікетів відноситься досить широке коло типів обладнання і їх моделей. Це і популярні трьохштангові турнікети-триподи, і роторні турнікети. так само виділяють різні турнікети типу «хвіртка».

Турнікет «трипод» є одним із типів турнікетів, що використовуються для контролю доступу. Він складається з трьох вертикальних стійок, які обмежують прохід. Кожна стійка з'єднана з центральною опорною частиною, і вони рухаються разом при проходженні.

Турнікет «трипод» зазвичай використовується для контролю доступу на об'єктах з невеликим потоком людей, таких як офісні будівлі, бізнес-центри або фітнес–центри. Цей тип турнікета відзначається своєю простотою в управлінні та економічністю. Він не вимагає складних технічних систем, але забезпечує базовий контроль доступу, що робить його популярним варіантом для об'єктів з невисоким рівнем безпеки.

Роторний турнікет – це модель турнікета, що складається з стійки, що обертається, і двох або більше стулок. Залежно від моделі стулки можуть бути виготовлені зі скла, пластику чи нержавіючих труб (у формі прапорців). Роторні турнікети можуть бути напівростовими або повноростовими.

Напівростові турнікети добре виконують функцію контролю проходу, але при належному бажанні і вправності такий турнікет можна подолати, просто його перестрибнувши.

Повноростові турнікети повністю перекривають прохід, так як їх висота (від 1.9 м і вище) дозволяє блокувати всю зону проходу. Повноростові турнікети – більш дороге, але і більш надійне рішення, яке встановлюють в місцях з підвищеними вимогами до рівня безпеки: в урядових установах, офісах банків і корпорацій, в готелях, на стадіонах і т.д.

Роторні турнікети не передбачають розблокування проходу при екстрених ситуацій, тому часто використовуються разом з хвіртками.

Турнікет–хвіртка являє собою механізм, що складається з стовпа і горизонтальної лопаті, що обмежує вхід. Лопать може бути виготовлена зі скла або металу. Завдяки особливостям конструкції цей тип турнікетів може використовуватися в обмеженому просторі, де немає місця для встановлення роторних турнікетів.

Хоча турнікет–хвіртку і можна використовувати як єдиний пристрій контролю доступу, найчастіше їх використовують в комплексі з іншими турнікетами. Через них можуть переміщувати великогабаритні вантажі, або пропускати людей з дитячими або інвалідними візками.

3. Шлагбауми - це рухомі бар'єри, які встановлюються на в'їздах або виїздах з території, щоб контролювати рух транспорту. Вони можуть керуватися вручну оператором за допомогою пульта, або керуватися автоматично завдяки контролеру. Шлагбауми можуть бути інтегровані з іншими системами, такими як системи розпізнавання номерних знаків або системи камер спостереження, для забезпечення ще більшого рівня безпеки і контролю.

Деякі з найпоширеніших місць використання:

– Промислові комплекси та фабрики. Використовуються для контролю руху вантажівок, доставок та іншого транспорту на територію підприємства.

– Аеропорти та залізничні вокзали. Використовуються для контролю доступу до пасажирських зон, автопаркінгів та інших зон обслуговування.

– Торгові центри та готелі. Використовуються для керування потоком транспорту до паркінгів для відвідувачів та гостей.

– Офісні комплекси. Встановлюються біля паркінгів офісних будівель для обмеження доступу лише для співробітників або автівок зі спеціальними пропусками.

– Житлові комплекси. Застосовуються для контролю доступу на територію або автопаркінг автомобілів мешканців та їх гостей.

1.4 Типи контролерів.

Контролер – головний елемент системи контролю доступу, він координує роботу всіх компонентів системи. Контролери бувають автономними та мережевими.

Автономний контролер. Застосовується в системах контролю доступу початкового рівня. Такий контролер передбачає обслуговування лише однієї точки доступу. Тому підходить для домашнього використання або для невеликих офісних приміщень. Має вбудовану базу даних, тобто вся отримана інформація зі зчитувачів зберігається безпосередньо на самому пристрої. Часто автономні контролери поєднують в одному корпусі декілька компонентів: сам контролер, клавіатуру для ведення пін–кодів, зчитувачі та реле.

До переваг автономних контролерів можна віднести:

– Низька ціна. Автономні контролери коштують значно дешевше на відміну від мережевих аналогів.

– Простота монтування. Встановлення та налаштування досить прості, що дозволяє швидко впровадити систему без потреби кваліфікованих фахівців.

До недоліків автономних контролерів можна віднести:

– Відсутність масштабування. Автономні контролери розраховані для роботи з однією або декількома точками пропуску, що унеможливлює їх використання для побудови великих або комплексних систем.

– Відсутність журналу активності. Автономні контролери не зберігають інформацію про авторизацію користувачів, через що неможливо реалізувати такі функції як урахування робочого часу, чи ефективність робітників.

Мережевий контролер може інтегруватися з іншими контролерами і керуючим комп'ютером, що дозволяє забезпечувати централізоване управління і контроль. Об'єднання пристроїв в одну мережу може здійснюватися за допомогою дротових (Ethernet або RS-485) чи бездротових (Bluetooth або Wi-Fi) технологій.

На відміну від автономних, мережеві контролери не обмежуються функцією дозволу чи заборони доступу. Деякі з додаткових функцій:

– Створювати звіти про наявність/відсутність працівників на робочих місцях.

– Вести облік робочого часу.

– Володіти інформацією про пересування співробітників протягом робочого дня.

– Ведення електронної бази даних працівників.

– Розмежувати доступ до різних приміщень об'єкта, що охороняється.

– Управляти охоронною сигналізацією, кнопкою виходу, камерою відеоспостереження та ін.

Перелік можливостей використання мережного контролера може бути розширений, завдяки модифікації програмного забезпечення.

1.5 Огляд готових рішень.

1. Комплект контролю доступу на базі контролера ZKTeco SA40–BE (Рисунок 1.1). Це один з найдоступніших комплектів обладнання для організації системи контролю доступу на одні двері.

Рисунок 1.1 – Комплектація автономного контролера ZKTeco SA40–BE.

Характеристики комплекту:

– Тип контролера: автономний;

– Пам’ять: 1000 користувачів;

– Використання: в приміщеннях;

– Спосіб ідентифікації: 125kHz RFID картки, Пін–код;

– Тип виконавчого пристрою: електромагнітний замок;

– Індикація: світлова;

– Живлення: імпульсній блок живлення 12В / 2А;

– Додаткове обладнання: механічна кнопка виходу, 10 безконтактних карток;

– Додаткові функції: автоматичне розблокування дверей при знеструмленні;

– Діапазон робочих температур: –10°С – +50°С.

2. Комплект контролю доступу з урахуванням робочого часу на базі мережевого контролера ZKTeco C3–100 (Рисунок 1.2). Використання мережевого контролера дозволить масштабувати та адмініструвати всю систему з одного місця з можливістю розмежування прав користувача. Такий комплект може знайти своє застосування від маленького офісу, де необхідно розуміти скільки часу співробітники проводять на робочому місці, до великих виробництв з великою кількістю користувачів, де необхідне розуміння пересування персоналу.

Рисунок 1.2 – Комплектація мережевого контролера ZKTeco C3–100.

Характеристики комплекту:

– Тип контролера: мережевий;

– Пам’ять: до 30000 користувачів, до 100000 подій;

– Використання: в приміщеннях, на вулиці;

– Спосіб ідентифікації: 125kHz/13,56MHz RFID картки;

– Тип виконавчого пристрою: електромагнітний замок;

– Індикація: світлодіодна, звукова;

– Живлення: 12В акумулятор;

– Додаткове обладнання: монтажний куток, датчик стану дверей, 10 безконтактних карток;

– Додаткові функції: автоматичне розблокування дверей при знеструмленні, урахування робочого часу, розмежування прав користувача;

– Діапазон робочих температур: 0°C – +55°C.

3. Комплект турнікету ZKTeco TS1011 Pro (Рисунок 1.3). Він дозволяє ефективно керувати проходами і забезпечують високий рівень безпеки та контролю в будь–якому типі організації чи установи, від офісних будівель до промислових об'єктів та об'єктів громадського призначення.

Рисунок 1.3 – Комплектація турнікету ZKTeco TS1011 Pro.

Характеристики комплекту:

– Тип контролера: мережевий;

– Пам’ять: до 30000 користувачів, до 100000 подій;

– Використання: в приміщеннях;

– Спосіб ідентифікації: 125kHz/13,56MHz RFID картки;

– Тип виконавчого пристрою: турнікет;

– Індикація: світлодіодні піктограми;

– Живлення: AC110В/220В;

– Додаткове обладнання: пульт керування турнікетом;

– Додаткові функції: функція антипаніка, функція заборони повторного проходу, можливість інтеграції в систему відеоспостереження, охоронно–пожежної сигналізації та ін.

– Діапазон робочих температур: 0°C – +50°C.

1.6 Постановка задачі.

Метою дипломного проекту є розробка пристрою управління контролем доступу. Пристрій повинен гарантувати безпеку та зручність в управлінні доступом до об'єкту. Для цього пристрій має підтримувати ряд ключових функцій:

– Ідентифікація користувачів. Для гарантування безпеки пристрій повинен мати можливість ідентифікації користувача перед наданням доступу.

– Керування доступом. Пристрій повинен мати можливість надавати або обмежувати доступ до об'єкту на основі результатів ідентифікації.

– Двонаправлений контроль доступу на одні двері. Пристрій повинен забезпечувати контроль доступу як на вхід, так і на вихід через одну точку проходу. Це дозволить точно фіксувати всі переміщення через контрольовану зону та підвищить рівень безпеки.

– Ведення журналу подій. Для забезпечення контролю та аналізу активності користувачів, пристрій повинен вести журнал всіх подій, включаючи інформацію про час та ідентифікацію особи.

– Управління системою. Пристрій повинен надавати можливість адміністратору системи керувати та налаштовувати параметри роботи, такі як додавання та видалення користувачів, налаштування прав доступу тощо.

– Інтеграція з іншими системами безпеки. Для забезпечення комплексного контролю до об'єкту, пристрій повинен мати можливість взаємодії з іншими системами безпеки, такими як системи відеоспостереження, системи пожежної безпеки тощо.

Реалізація цих функцій дозволить створити високоефективний пристрій управління контролем доступу, що відповідає сучасним вимогам безпеки та зручності у використанні.

2. Розробка алгоритму роботи та структурної схеми.

2.1 Розробка алгоритму роботи.

Ключовим етапом у розробці будь-якого пристрою є чітке розуміння принципів його роботи. Це особливо важливо у випадку пристрою управління контролем доступу, де безпека та ефективність відіграють ключову роль.

Необхідно розробити алгоритм, який забезпечить безпеку об'єкту та контроль доступу до нього. Цей алгоритм повинен включати в себе механізми ідентифікації користувачів, а також перевірки їхньої автентичності (Рисунок 2.1).

Крім забезпечення безпеки, алгоритм також повинен бути ефективним з точки зору швидкості та надійності роботи. Він має бути оптимізованим для роботи в різних умовах і середовищах, забезпечуючи максимальну продуктивність та стабільність системи.

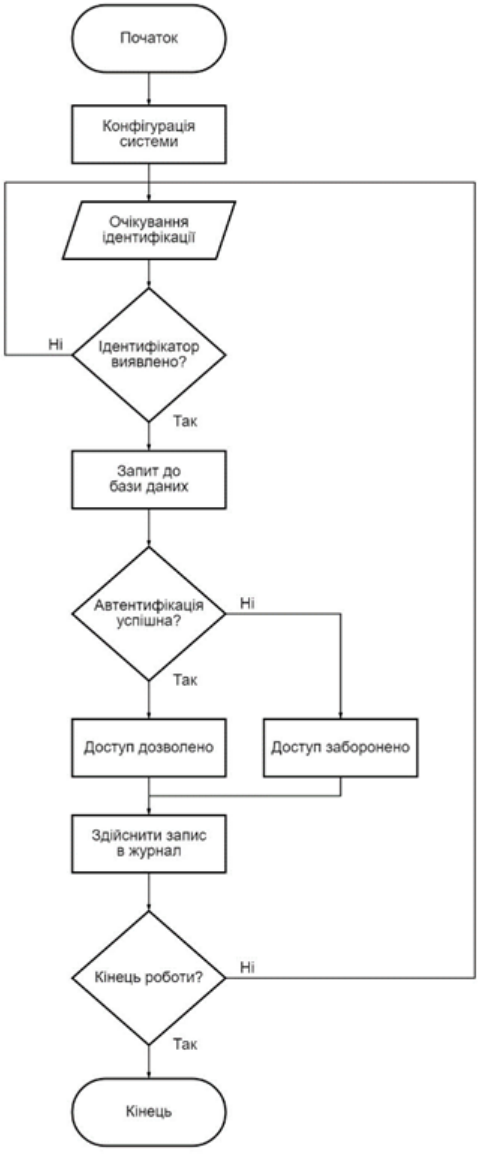

Рисунок 2.1 – Блок–схема алгоритму роботи пристрою.

Розглянемо детальніше кожен крок цього алгоритму та його значення у процесі забезпечення безпеки та контролю доступу до об’єкту:

1. Конфігурація системи: На цьому етапі відбувається налаштування всієї системи. Це може включати в себе підключення до бази даних, синхронізацію між мережевою та автономною базою даних, налаштування параметрів безпеки та інші необхідні дії.
2. Очікування ідентифікації: На цьому етапі пристрій очікує коли в радіус дії зчитувача потрапить ідентифікатор користувача.
3. Виявлення ідентифікатора: Якщо пристрою вдається виявити ідентифікатор, він переходить до автентифікації, якщо ні, пристрій чекає наступної спроби ідентифікації.
4. Автентифікація: Система порівнює виявлений ідентифікатор користувача з ідентифікаторами, що зберігаються в базі даних. Якщо виявлений ідентифікатор дійсний, пристрій надає доступ, в зворотному випадку – ні.
5. Запис: Після кожної спроби ідентифікації пристрій реєструє результат, записуючи у журнал інформацію про успішну або невдалу спробу автентифікації. Це може включати час спроби, ідентифікатор користувача, статус автентифікації та інші деталі.
6. Після завершення процесу ідентифікації система готова до нової спроби ідентифікації.

2.2 Розробка структурної схеми.

Розробка структурної схеми є таким ж важливим етапом, як і розробка алгоритму. Схема є основою для подальшого проектування та реалізації пристрою, який буде забезпечувати контроль та моніторинг доступу до об'єкту. Чітке визначення структури дозволяє зрозуміти взаємозв'язки між різними компонентами пристрою, а також визначити оптимальний спосіб їх взаємодії для досягнення поставлених цілей безпеки та ефективності.

Опис блоків структурної схеми (Рисунок 2.2) пристрою управління контролем доступу:

1. Блок зчитувачів. У пристрої використовуються два зчитувачі. Вони відповідають за отримання ідентифікаційних даних від користувачів при вході та виході.

2. Блок мікроконтролера. Це ключовий блок, що відповідає за координацію роботи всіх елементів структурної схеми. Він обробляє та передає на Wi–Fi модуль ідентифікаційні дані, які надходять від зчитувачів. На основі результатів автентифікації приймає рішення про те, чи дозволити доступ користувачеві.

3. Wi–Fi модуль. Цей блок забезпечує підключення пристрою до бази даних, розташованої на комп'ютері.

4. Блок контролю доступу. Цей блок відповідає за надання або заборону доступу користувачеві в залежності від прийнятого контролером рішення.

5. Блок дисплеїв: У пристрої використовуються два дисплеї для індикації на вході та виході. На них можуть відображатися інструкції для користувачів, статус автентифікації, повідомлення про помилки, а також інші необхідні повідомлення.

6. Блок сигналізації. В пристрої використовуються два пасивні зумери для звукової індикації на вході та виході.

7. Пам'ять. В пристрої використовується модуль флешпам'яті для збереження ідентифікаторів та журналу в автономному режимі роботи.

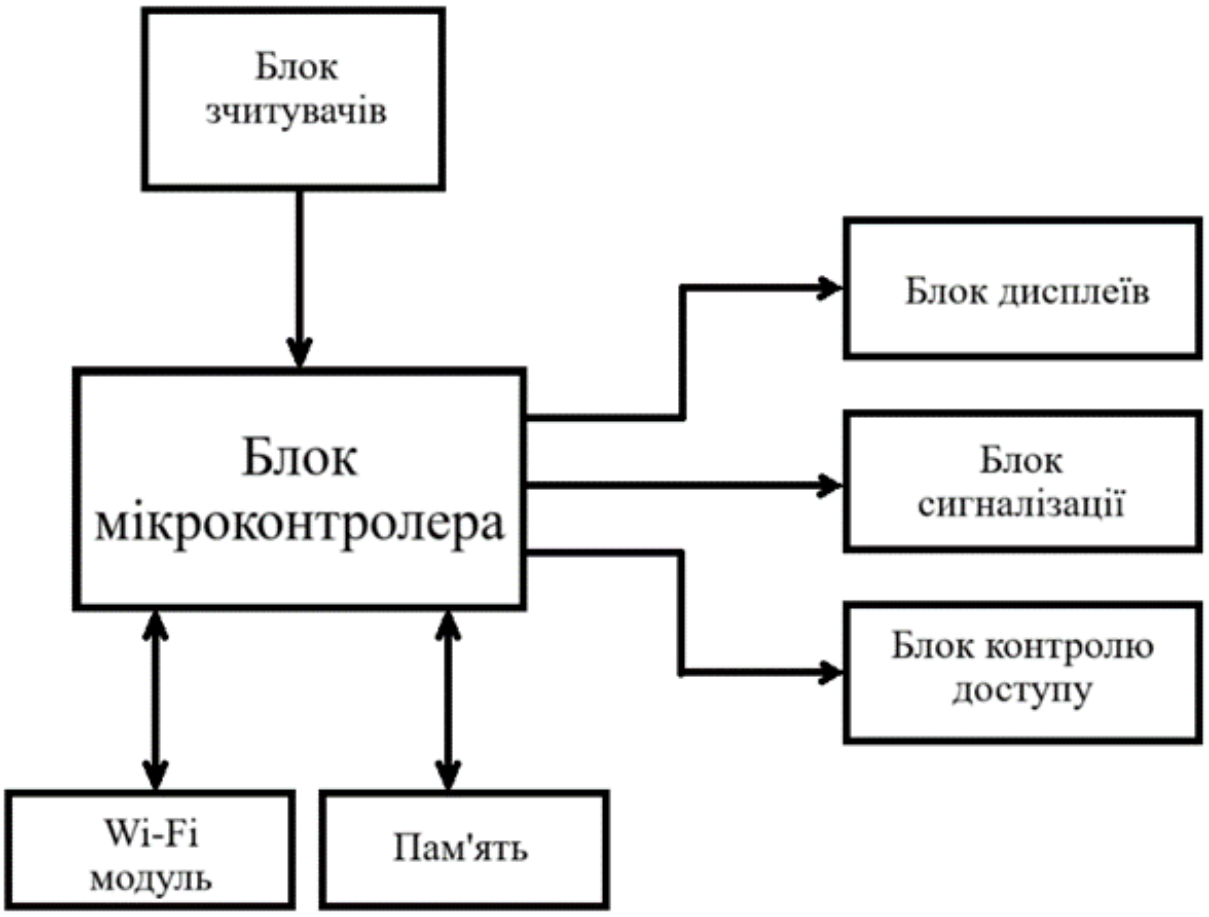

Рисунок 2.2 – Структурна схема пристрою.

Отже, пристрій працює наступним чином: блок мікроконтролера отримує ідентифікатор користувача від одного з зчитувачів та передає його через послідовний інтерфейс на Wi–Fi модуль для подальшої передачі. Wi–Fi модуль передає ідентифікатор на комп’ютер з спеціальним застосунком, де він порівнюються з інформацією в базі даних. Застосунок виконує процес автентифікації, порівнюючи ідентифікатор з інформацією в базі даних. Після аналізу застосунок надсилає відповідь, яка містить результат автентифікації, на Wi–Fi модуль. Wi–Fi модуль передає отриману відповідь назад на мікроконтролерний блок, який на основі отриманої відповіді приймає рішення про дозвіл або заборону доступу користувачу, за допомогою замка.

3. Розробка функціональної схеми.

Центральним елементом схеми (Рисунок 3.1) є мікроконтролер, який координує роботу всіх інших компонентів. Він відіграє ключову роль у забезпеченні злагодженої взаємодії між різними частинами системи, що дозволяє їй функціонувати ефективно та надійно. Мікроконтролер отримує дані зі зчитувачів, взаємодіє з модулем Wi-Fi та флешпам’яттю, виводить інформацію на дисплеї, активує зумери та керує електромагнітним замком. Для комунікації він використовує різні інтерфейси: SPI, I2C та UART, що дозволяє забезпечити гнучкість і масштабованість системи.

За допомогою SPI до мікроконтролера під’єднані два зчитувачі RFID та модуль пам’яті. Інтерфейс SPI дозволяє здійснювати швидкий обмін даними між мікроконтролером і підключеними пристроями. Вони використовують спільні виводи MISO, MOSI та SCK, але кожен з них має окремий вивід для сигналу початку/завершення сеансу зв'язку SS, SS2, SS3. Це дозволяє мікроконтролеру вибирати, з яким пристроєм взаємодіяти в конкретний момент часу. Зчитувачі сканують ідентифікаційні дані з RFID-міток, що дозволяє системі розпізнавати користувачів або об’єкти. Модуль пам’яті, використовується для збереження та зчитування даних, необхідних для роботи системи в автономному режимі. Це забезпечує збереження важливої інформації навіть у випадку відсутності живлення або збою в системі.

LCD-дисплеї відіграють важливу роль у взаємодії з користувачем, відображаючи інформацію про стан системи або інші повідомлення. Вони підключаються паралельно через I2C інтерфейс, використовуючи виводи SDA та SCL. Інтерфейс I2C дозволяє підключати до мікроконтролера кілька пристроїв (за умови, що вони мають різні адреси) з використанням лише двох виводів, що значно спрощує схему і зменшує кількість необхідних з'єднань.

Wi-Fi модуль забезпечує бездротовий зв'язок, дозволяючи системі обмінюватися даними з зовнішніми серверами або іншими пристроями. Він підключений через UART інтерфейс, використовуючи виводи RXD для прийому та TXD для передачі даних. Це дозволяє системі передавати дані на віддалений сервер для моніторингу або отримувати команди для керування.

Зумери, що генерують звукові сигнали, використовуються для забезпечення звукової індикації подій або стану системи. Вони керуються окремими виводами

мікроконтролера: PD5 та PD6. Це дозволяє системі генерувати звукові сигнали у випадку успішного зчитування RFID-мітки, помилки або інших подій.

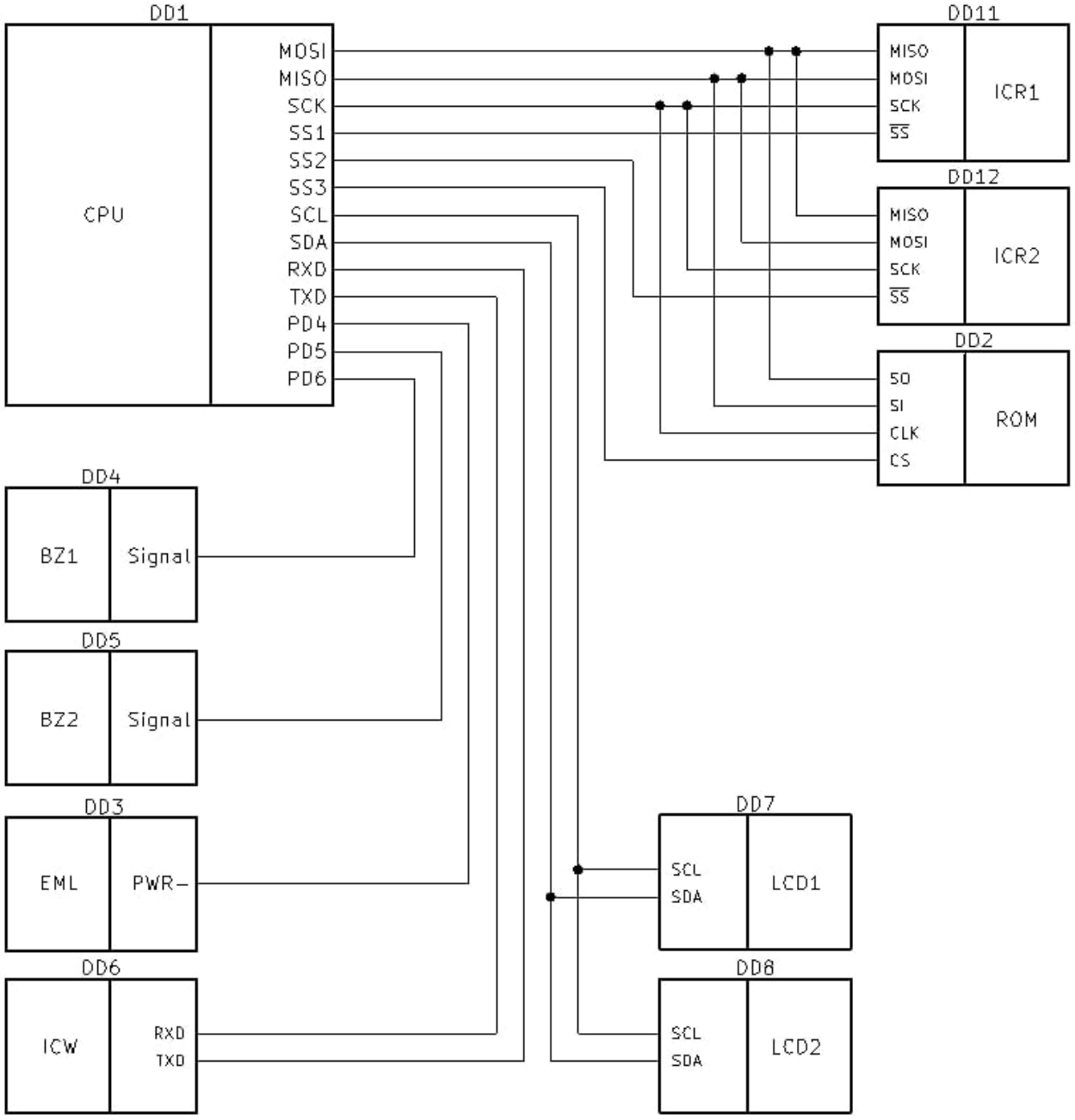

Рисунок 3.1 – Функціональна схема пристрою.

Електромагнітний замок керується сигналом PD4 від мікроконтролера. Це дозволяє системі відкривати або закривати замок у відповідь на певні події, наприклад, успішну ідентифікацію користувача.

Таким чином, мікроконтролер координує всі операції в системі, забезпечуючи злагоджену роботу всіх компонентів

4. Розробка принципової схеми.

4.1 Блок мікроконтролера.

Мікроконтролер є ключовим блоком, що відповідає за координацію роботи всіх елементів схеми. Він обробляє ідентифікаційні дані, які надходять від зчитувачів, за допомогою Wi-Fi модулю передає їх на комп'ютер, де вони порівнюються з інформацією, збереженою в базі даних та на основі відповіді керує електромагнітним замком. Також він керує аудіовізуальною індикацією, виводячи повідомлення на символьні дисплеї та активуючи зумери при різних подіях та сценаріях.

Для реалізації цього пристрою, мікроконтролер повинен відповідати таким вимогам:

- Помірна ціна;
- Достатня швидкодія;
- Наявність SPI, I2C, UART інтерфейсів;
- Достатня кількість GPIO;
- Широка підтримка в середовищі розробки.

Беручи до уваги перелічені вимоги, ATmega328P є підходящим вибором для виконання ролі мікроконтролера в нашому пристрої, оскільки він забезпечує необхідну кількість інтерфейсів і GPIO та достатню швидкодію для виконання поставлених задач. ATMega328P керуватиме всіма елементами пристрою управління контролем доступу, забезпечуючи надійну і ефективну роботу системи. Його гнучкість і надійність роблять його відмінним вибором для реалізації даного пристрою.

До переваг мікроконтролера ATmega328P можна віднести: 32кбайт флеш-пам'яті, що дозволяє зберігати достатньо великий обсяг коду, 23 порти введення/виведення для підключення різноманітних периферійних пристроїв, 2кбайт ОЗП для обробки даних під час виконання програм, 1кбайт EEPROM для зберігання налаштувань і даних, що потребують збереження після вимкнення живлення, а також висока енергоефективність, що забезпечує тривалий час роботи від акумулятора. Додатково, мікроконтролер має розвинену екосистему бібліотек, що полегшує розробку і налагодження пристрою.

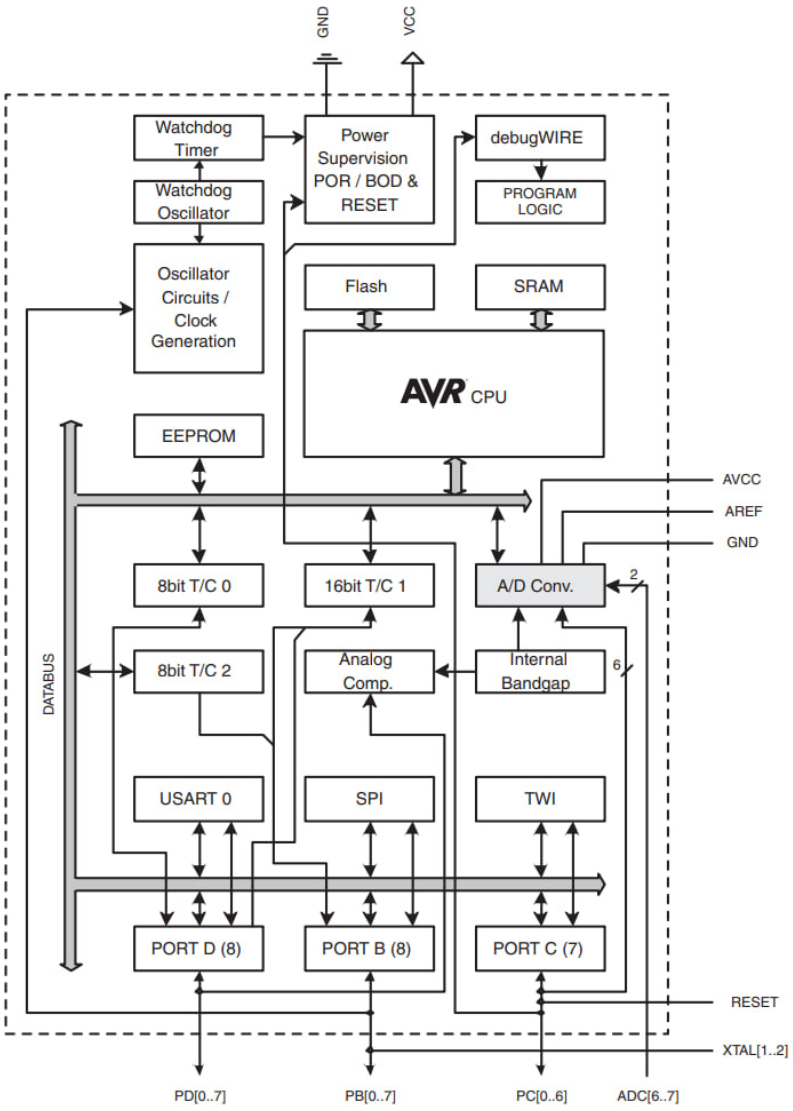

Рисунок 4.1 – Структурна схема ATMega328P.

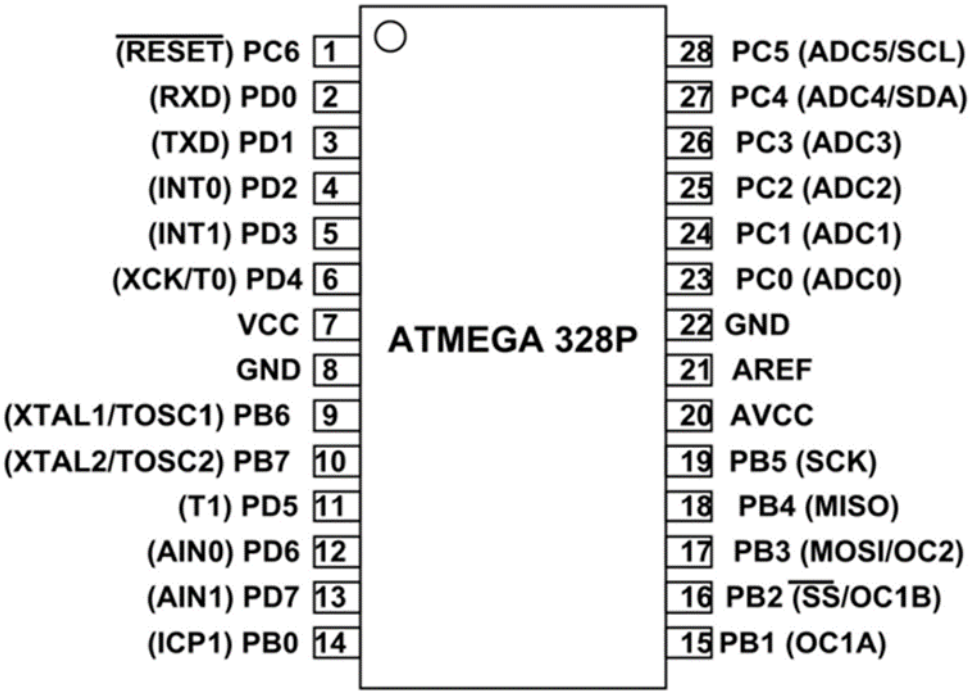

Рисунок 4.2 – Схема розташування виводів ATMega328P.

Таблиця 4.1 – Опис виходів мікроконтролера.

Позначення	Опис функцій виводу
VCC	Джерело живлення
GND	Заземлення
Port B (PB7:0)	Порт B - це 8-бітний двонаправлений порт вводу/виводу з внутрішніми підтягуючими резисторами (підбираються для кожного біта). Вихідні буфери порту B мають симетричні характеристики накопичувача з високими можливостями як стоку, так і джерела. В якості входів виводи порту B, які ззовні затягнуті на низький рівень, будуть джерелом струму, якщо активовані підтягуючі резистори. Виводи порту B переходять у трипозиційний стан, коли стає активним стан скидання, навіть якщо тактовий генератор не працює. Залежно від налаштувань запобіжника вибору тактового генератора, PB6 можна використовувати як вхід для підсилювача інвертуючого генератора і вхід для внутрішньої схеми роботи тактового генератора. Залежно від налаштувань запобіжника вибору тактового генератора, PB7 можна використовувати як вихід з підсилювача інвертуючого генератора. Якщо внутрішній калібрований RC-генератор використовується як джерело тактового сигналу мікросхеми, PB7...6 використовуються як TOSC2. 1 для асинхронного таймера/лічильника 2, якщо встановлено біт AS2 в ASSR.
Port C (PC5:0)	Порт C - це 7-розрядний двонаправлений порт вводу/виводу з внутрішніми підтягуючими резисторами (підібраними для кожного біта). Вихідні буфери PC5..0 мають симетричні характеристики накопичувача з високими можливостями як споживача, так і джерела. В якості входів, виводи порту C, які ззовні затягнуті на низький рівень, будуть джерелом струму, якщо активовані підтягуючі резистори. Виводи порту C переходять у трипозиційний стан, коли стає активним стан скидання, навіть якщо тактовий генератор не працює.

Продовження таблиці 4.1

Позначення	Опис функції виводу
PC6/RESET	Якщо запрограмовано запобіжник RSTDISBL, PC6 використовується як контакт вводу/виводу. Зверніть увагу, що електричні характеристики PC6 відрізняються від характеристик інших виводів порту C. Якщо запобіжник RSTDISBL не запрограмовано, PC6 використовується як вхід скидання. Наявність низького рівня на цьому виводі довше, ніж мінімальна тривалість імпульсу, призведе до скидання, навіть якщо тактовий генератор не працює. Мінімальна довжина імпульсу становить 2,5 мкс. Коротші імпульси не гарантують генерування скидання.
Port D (PD7:0)	Порт D - це 8-бітний двонаправлений порт вводу/виводу з внутрішніми підтягуючими резисторами (підбираються для кожного біта). Вихідні буфери порту D мають симетричні характеристики накопичувача з високою ємністю як споживача, так і джерела. В якості входів, виводи порту D, які ззовні затягнуті на низький рівень, будуть джерелом струму, якщо активовані підтягуючі резистори. Виводи порту D переходять у трипозиційний стан, коли стає активним стан скидання, навіть якщо тактовий генератор не працює.
A_{VCC}	A_{VCC} - це вивід напруги живлення для АЦП і PC3:0. Він повинен бути зовні підключений до VCC, навіть якщо АЦП не використовується. Якщо АЦП використовується, його слід підключити до VCC через низькочастотний фільтр. Зверніть увагу, що PC6...4 використовують цифрову напругу живлення, VCC.
AREF	AREF - аналоговий опорний вивід для АЦП.

Таблиця 4.2 – Функції виходів мікроконтролера.

Вивід	Позначення	Призначення
PB5	SCK	Генерує тактові імпульси для синхронізації передачі даних між мікроконтролером і RC522 №1, RC522 №2, W25Q128JVSIQ через інтерфейсі SPI.

Продовження таблиці 4.2

Вивід	Позначення	Призначення
PB4	MISO	Передає дані від RC522 №1, RC522 №2, W25Q128JVSIQ до мікроконтролера через SPI інтерфейс.
PB3	MOSI	Передає дані від мікроконтролера до RC522 №1, RC522 №2, W25Q128JVSIQ через SPI інтерфейс.
PB2	SS	Звернення до блоку зчитувача RC522 №1 при взаємодії через SPI інтерфейс.
PB1	RST	Використовується для скидання всіх підключених по SPI пристроїв до початкового стану або ініціалізації їх роботи.
PB0	ICP(SS2)	Звернення до блоку зчитувача RC522 №2 при взаємодії через SPI інтерфейс.
PC4	SDA	Двонаправлений вивід для передачі даних між мікроконтролером та дисплеями через I2C інтерфейс.
PC5	SCL	Генерує тактові імпульси для синхронізації передачі даних між мікроконтролером та дисплеями через I2C інтерфейс.
PD0	RX	Вхідний вивід, використовується для прийому мікроконтролером даних від ESP-01S по інтерфейсу UART.
PD1	TX	Вихідний вивід, використовується для передачі даних від мікроконтролера до приймача ESP-01S по інтерфейсу UART.
PD2	INT0(SS3)	Звернення до блоку пам'яті W25Q128JVSIQ при взаємодії через SPI інтерфейс.
PD4	T0	Контролює стан електромагнітного замка, дозволяючи або блокуючи доступ.
PD5	T1	Генерує зовнішній сигнал для управління зумером №1.
PD6	AIN0	Генерує зовнішній сигнал для управління зумером №2.

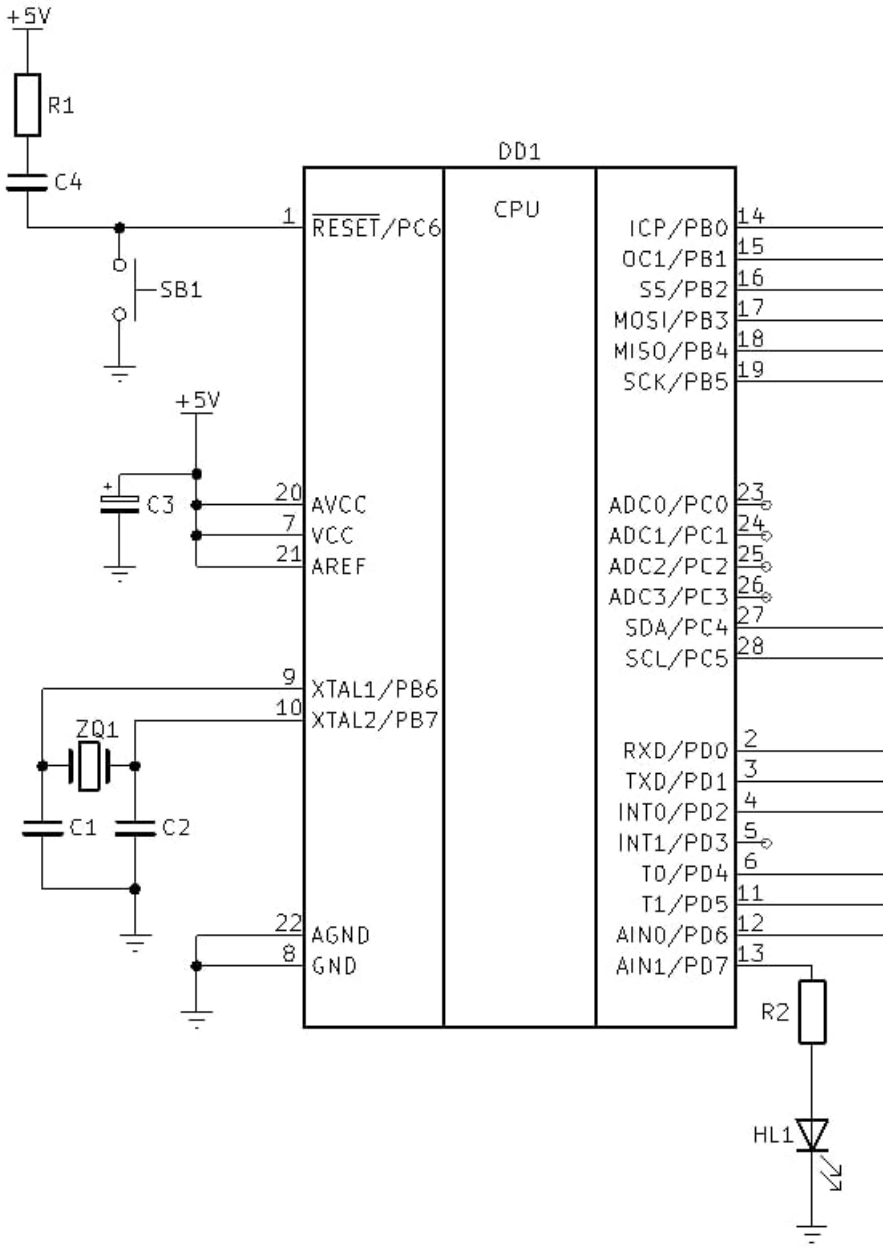

Рисунок 4.3 – Схема включення ATMega328P.

4.2 Блок зчитувачів.

В пристрої використовуються RFID зчитувачі RC522. Використання модулів RC522 дозволяє забезпечити надійну ідентифікацію користувачів за допомогою RFID технологій, що забезпечує швидке та зручне керування доступом. Незважаючи на низьку ціну, модуль поєднує у собі високу точність зчитування та простоту інтеграції, що робить його ідеальним вибором для систем контролю доступу початкового рівня.

Характеристики RFID модулю RC522:

– Напруга живлення: 2.5–3.3V;

– Споживаний струм: 13–26mA;
– У режимі очікування: 10–13mA;
– У сплячому режимі: <80μA;
– Робоча частота: 13.56MHz;
– Дальність зчитування: 0 ~ 60 мм;
– Інтерфейси: SPI, I2C, UART;
– Розмір: 40мм × 60мм.

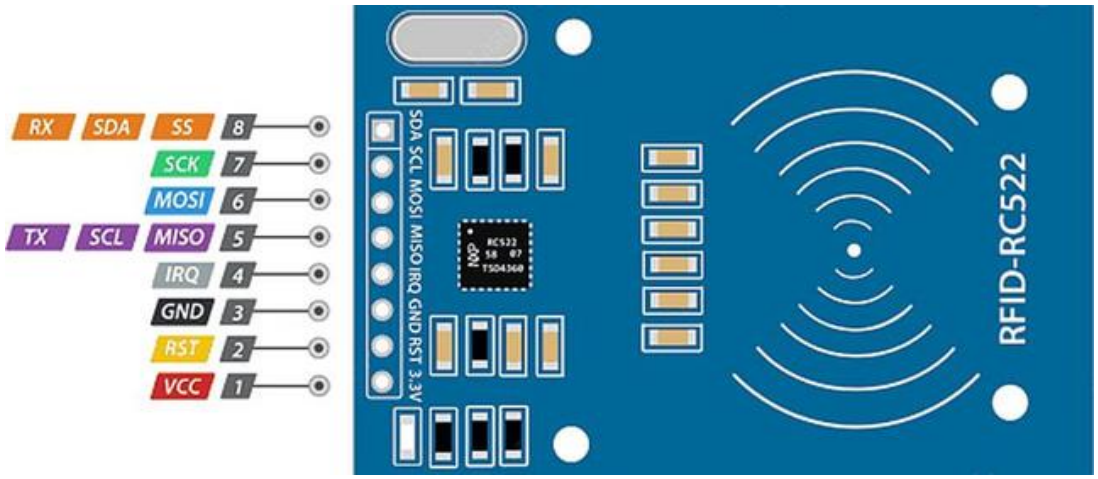

Рисунок 4.4 – Схема розташування виводів RC522.

1. VCC – джерело живлення;
2. RST – скидання;
3. GND – заземлення;
4. IRQ – переривання;
5. MISO / SCL / TX – вхід ведучого, вихід веденого для SPI, послідовна лінія тактування для I2C, послідовний вихід даних для UART;
6. MOSI – вихід ведучого, вхід веденого;
7. SCK – послідовний тактовий сигнал;
8. SS / SDA / RX – сигнал початку/завершення сеансу зв'язку для SPI, послідовна лінія даних для I2C, послідовний вхід даних для UART.

Підключення модулів буде виконуватись через інтерфейс SPI, адже він забезпечує більшу швидкість передачі даних, порівняно з іншими інтерфейсами. Ще однією перевагою SPI є можливість паралельного підключення декількох пристроїв за допомогою одного інтерфейсу (Рисунок 4.5).

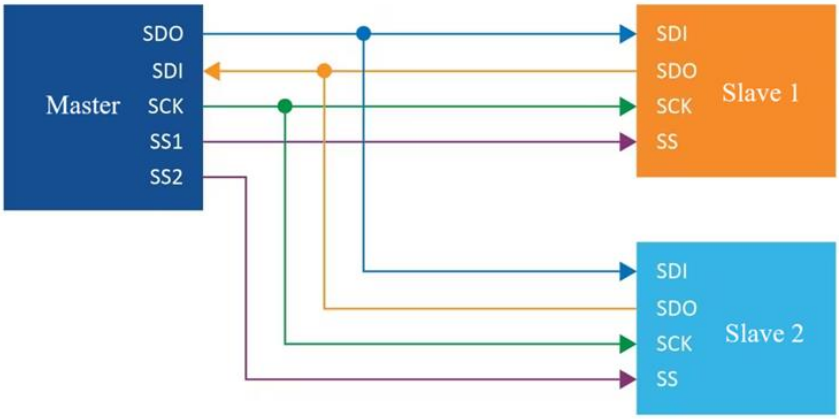

Рисунок 4.5 – Підключення декількох ведених до одного ведучого.

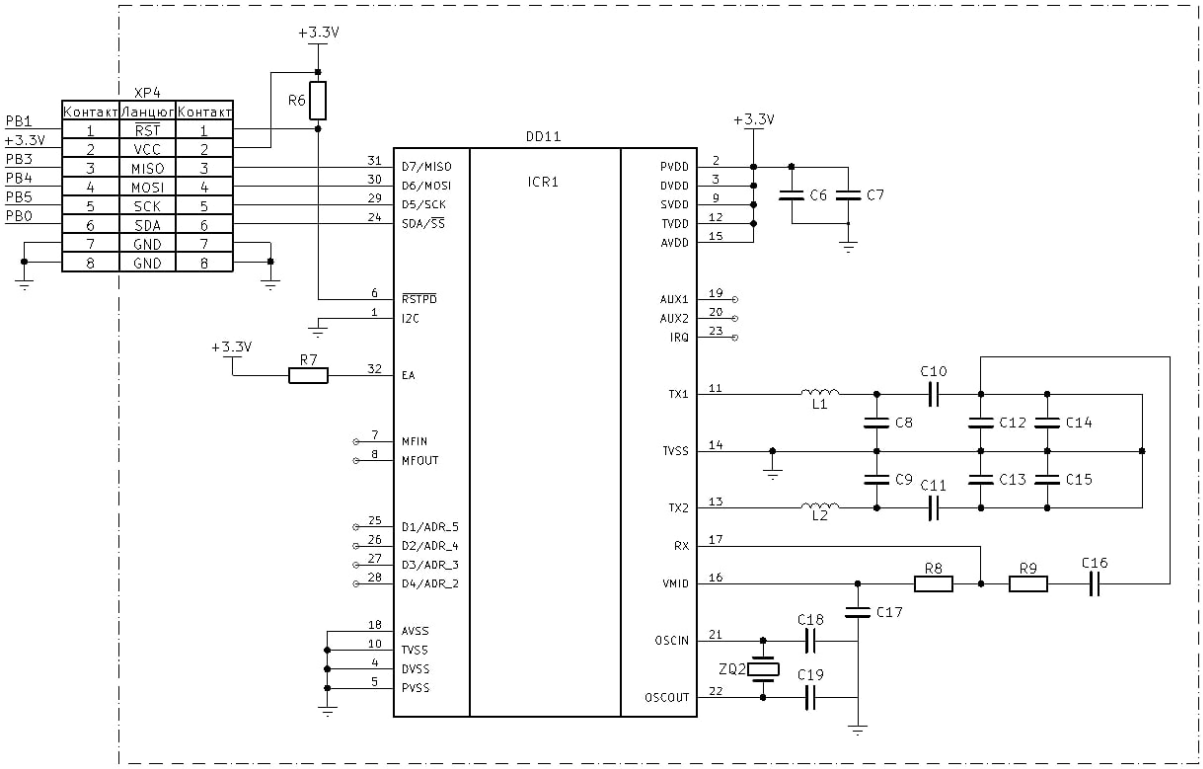

Рисунок 4.6 – Схема включення зчитувача RC522.

4.3 Блок дисплеїв.

Для індикації в пристрої будуть використовуватись дисплеї LCD1602. LCD1602 – це дисплей, який може відображати до 16 символів у двох рядках. Кожен символ складається з матриці 5x8 точок, що дозволяє відображати не тільки текст, але й прості графічні елементи.

Для зручності підключення, будемо використовувати I2C модуль. I2C модуль для LCD1602 використовує спеціалізований контролер (зазвичай PCF8574), який переводить стандартний інтерфейс дисплея (4 або 8-бітний

паралельний) в інтерфейс I2C (Рисунок 4.7). Це дозволяє значно скоротити кількість необхідних для підключення проводів з 12 до 4 (VCC, GND, SDA, SCL).

Переваги використання I2C модуля:

– Мінімізація проводів. Замість численних з'єднань паралельного інтерфейсу, використовується лише 2 лінії для даних (SDA і SCL) та 2 лінії для живлення (VCC і GND).

– Простота підключення. Легко підключається до мікроконтролера через I2C інтерфейс.

– Можливість налаштування контрасту. Більшість I2C модулів для дисплеїв 1602 мають потенціометр для налаштування контрасту екрана, що дозволяє легко налаштувати оптимальний рівень видимості символів.

– Можливість каскадування. На одну шину I2C можна підключити декілька пристроїв.

Для підключення двох дисплеїв через I2C інтерфейс, кожен з них повинен мати унікальну адресу. За замовчуванням, більшість I2C модулів для LCD1602 мають адресу 0x27, тому необхідно змінити адресу на одному з них.

Для зміни адреси на платі I2C модуля є три перемички (A0, A1, A2). Зазвичай ці перемички знаходяться в незамкнутому стані, що відповідає стандартній адресі. Змінюючи стан перемичок, можна змінити адресу модуля.

Рисунок 4.7 – Схема розташування виводів LCD1602 з I2C модулем.

1. GND – заземлення;
2. VCC – джерело живлення;
3. SDA – послідовна лінія даних;
4. SCL – послідовна лінія тактування.

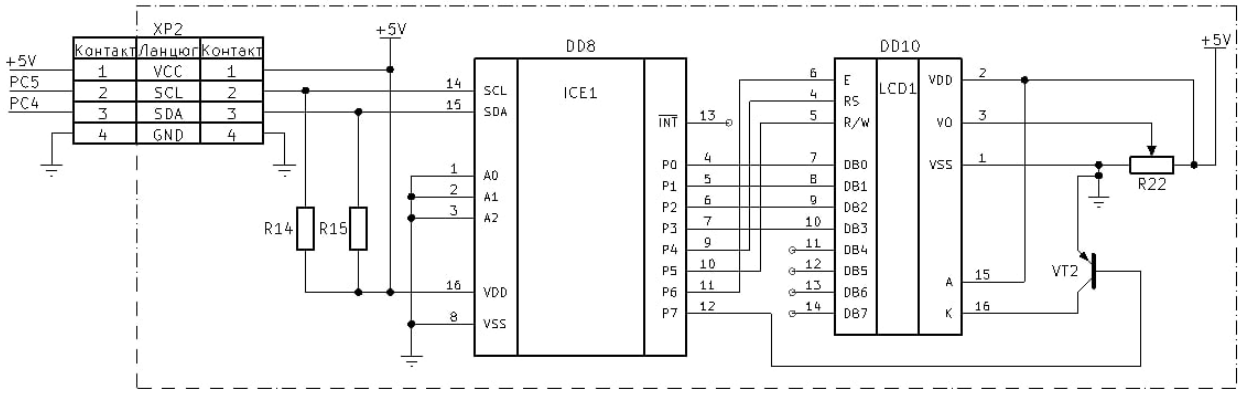

Рисунок 4.8 – Схема включення дисплею LCD1602.

4.4 Блок Wi-Fi модулю.

Для забезпечення бездротового зв’язку між пристроєм та комп’ютером було обрано ESP-01S. ESP-01S – це компактний, але потужний Wi-Fi модуль, який здобув популярність завдяки своїй доступності та простоті використання.

Модуль підтримує широкий спектр протоколів зв'язку, таких як HTTP, MQTT та WebSocket, що робить його універсальним інструментом для різних задач.

ESP-01S підтримує кілька енергозберігаючих режимів, що допускає його використання в пристроях, що живляться від акумулятора. Можна налаштувати модуль так, щоб він переходив у режим сну, коли не використовується, що дозволяє значно знизити енергоспоживання.

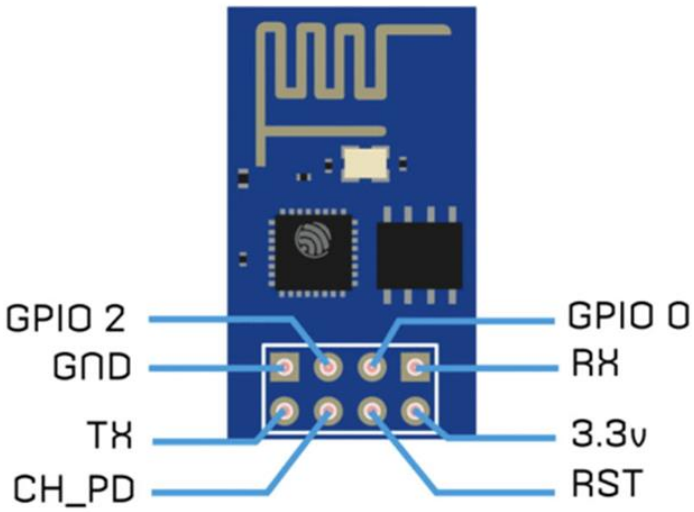

Рисунок 4.9 – Схема розташування виводів ESP-01S.

– 3.3V – живлення;
– GND – заземлення;
– TX – передача даних;

– RX – прийом даних;
– CH_PD – вимкнення модуля;
– RST – скидання модуля;
– GPIO 0 – вивід загального призначення 0;
– GPIO 2 – вивід загального призначення 2.

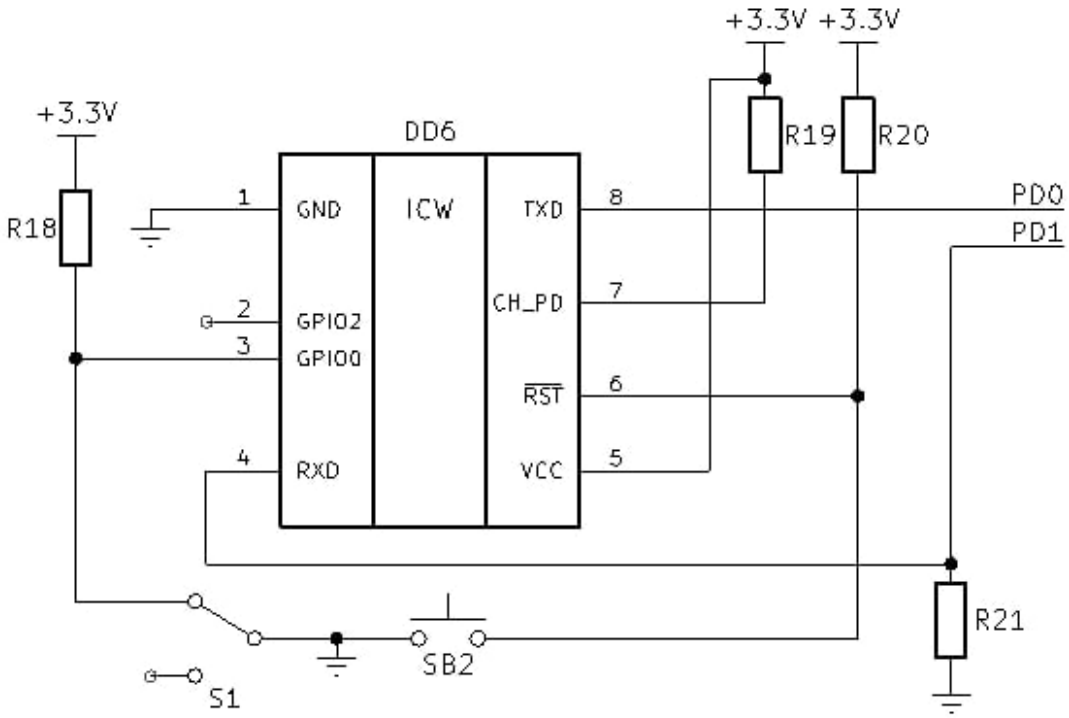

Рисунок 4.10 – Схема включення ESP-01S.

4.5 Блок пам’яті.

Для зберігання ідентифікаторів користувачів та ведення журналу подій в автономному режимі роботи, в пристрої управління контролем доступу використовується модуль пам'яті W25Q128JVSIG.

Модуль має об'єм пам'яті 128 Мбіт (16 МБ) та підтримує інтерфейс SPI, який забезпечує швидкості до 133 МГц. Напруга живлення становить 2.7В - 3.6В (типова 3.3В). Пам'ять організована у сторінки по 256 байтів кожна, сектори по 4 КБ, блоки по 32 КБ і 64 КБ.

Пам'ять енергонезалежна, що означає, що дані зберігаються без живлення з терміном зберігання до 20 років. Гарантовано не менше 100,000 циклів перезапису. Функціонал модуля включає команди для читання даних, запису, стирання сторінок, секторів, блоків і всієї пам'яті, а також підтримку команд

швидкого читання, послідовного і подвійного читання. Режим низького енергоспоживання (Deep Power-Down) дозволяє економити енергію.

Завдяки своїй високій швидкості і надійності, він забезпечує оперативний доступ до бази даних ідентифікаторів та дозволяє безперервно вести журнал подій навіть при відсутності підключення до зовнішньої бази даних.

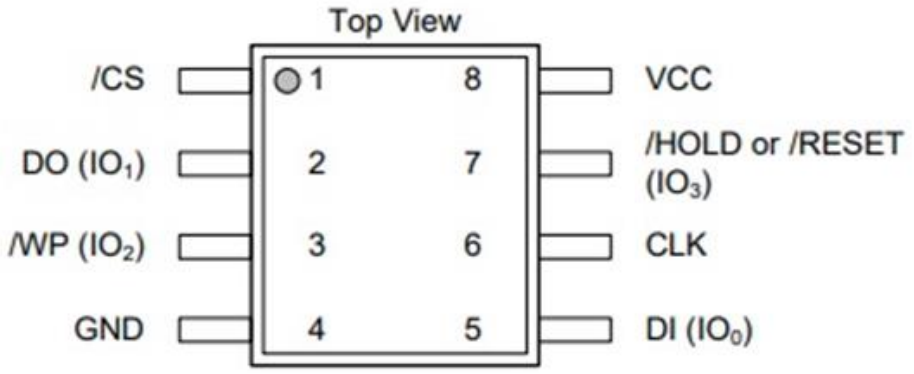

Рисунок 4.11 – Схема розташування виводів W25Q128JVSIG.

1. /CS – сигнал початку/завершення сеансу зв'язку;
2. DO – виведення даних;
3. /WP – вхід із захистом від запису;
4. GND – заземлення;
5. DI – введення даних;
6. CLK – послідовний тактовий вхід;
7. /HOLD /RESET– утримання або скидання входу;
8. VCC – джерело живлення.

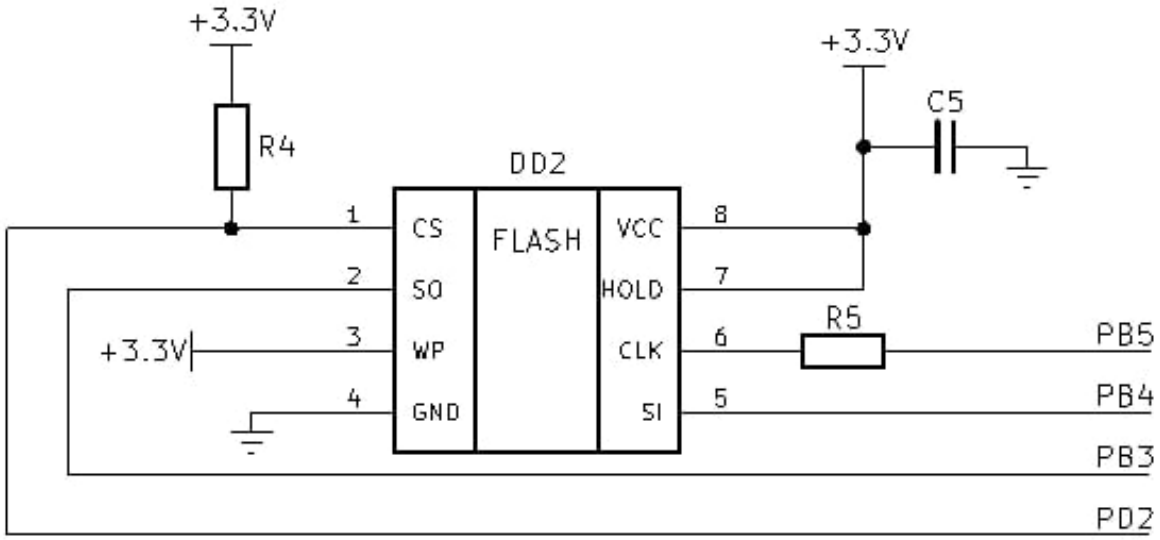

Рисунок 4.12 – Схема включення W25Q128JVSIG.

4.6 Блок сигналізації.

Для сигналізації було використано 2 пасивні зумери KY-006. На відміну від активного зумера пасивний не має вбудованого генератора частоти, тому для його роботи потрібен зовнішній сигнал (Рисунок 4.13). Звуки різної тональності генеруються залежно від зовнішнього сигналу, це дозволяє налаштувати різні звукові сигнали для різних ситуацій та сценаріїв, таких як підтвердження успішного доступу, попередження про спробу несанкціонованого доступу або сигналізацію про системні помилки. Завдяки цьому, пасивний зумер підвищує функціональність і гнучкість системи, забезпечуючи чітку і зрозумілу звукову індикацію для користувачів.

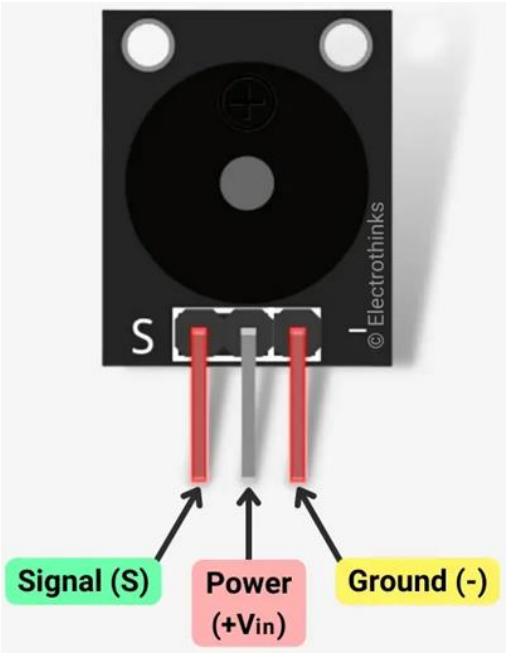

Рисунок 4.13 – Схема розташування виводів KY-006.

1. Signal – сигнальний вхід;
2. +V – джерело живлення;
3. Ground – заземлення.

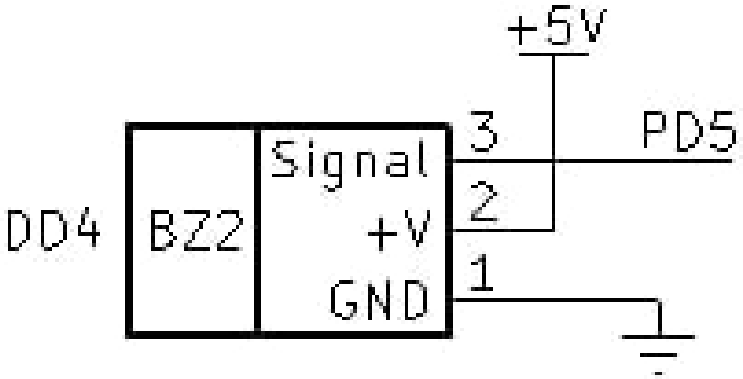

Рисунок 4.14 – Схема включення KY-006.

4.7 Блок контролю доступу.

Для контролю доступу в пристрої використовується електромагнітний замок Trinix TML-200. Він є надійним і ефективним рішенням для забезпечення безпеки в приміщенні. Цей замок забезпечує високу силу утримання до 200 кг, чого цілком достатньо для нашого проекту. Корпус замка виготовлений з високоякісного алюмінієвого сплаву, що забезпечує стійкість до корозії і тривалий термін служби. Trinix TML-200 легко монтується на різні типи дверей, включаючи дерев'яні, металеві та скляні конструкції. У разі відключення електроенергії, електромагнітний замок автоматично відкривається, забезпечуючи безпеку евакуації в екстрених ситуаціях.

Використання електромагнітного замка Trinix TML-200 гарантує високий рівень безпеки, надійність та довговічність, що є ключовими аспектами для успішного функціонування пристрою управління контролем доступу.

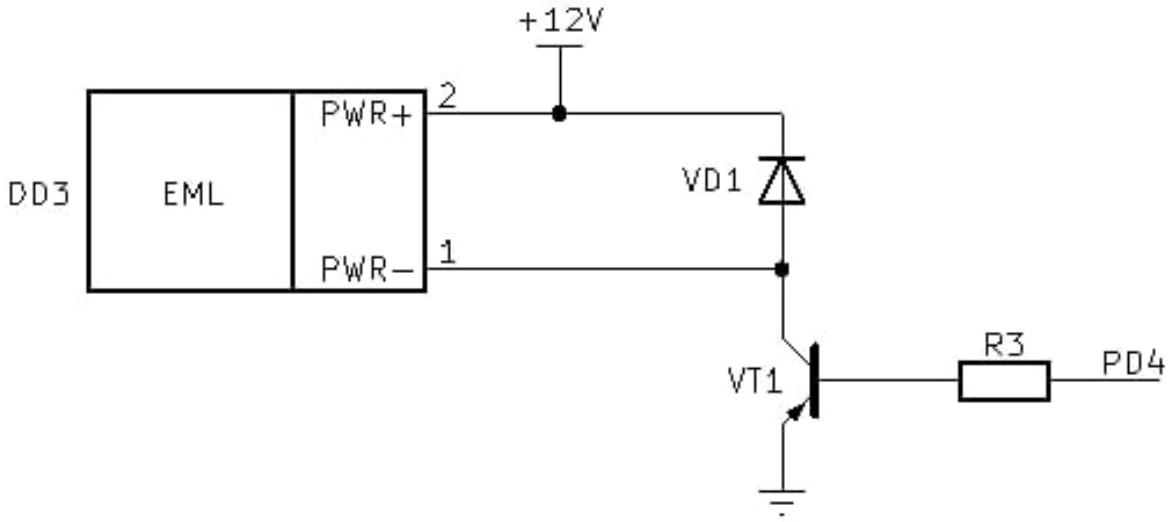

Рисунок 4.15 – Схема включення Trinix TML-200.

5. Розробка програмного забезпечення.

Розробка програмного забезпечення для пристрою управління контролем доступу є важливим етапом, що забезпечує надійність, безпеку та зручність використання системи. Наведена нижче програма, постійно перевіряє наявність нових міток в зоні дії RFID зчитувачів. Якщо нова мітка виявлена, зчитується її UID. UID карти передається на ESP-01S для перевірки у зовнішній базі даних, і програма чекає на відповідь від ESP-01S. Якщо користувач авторизований, звучить зумер, відкривається електромагнітний замок, і на дисплеї показується повідомлення "Access Granted". Якщо користувач не авторизований, звучить зумер, і на дисплеї відображається повідомлення "Access Denied". У випадку втрати зв'язку з ESP-01S, програма може використовувати дані з флеш-пам'яті для автономної роботи. Це забезпечує автоматизований контроль доступу на основі RFID технології з можливістю віддаленої перевірки користувачів через Wi-Fi модуль та локального збереження даних для автономної роботи.

```
#include <Wire.h>
#include <LiquidCrystal_I2C.h>
#include <SPI.h>
#include <MFRC522.h>
#include <SoftwareSerial.h>
#include <SdFat.h>

// Піни для зчитувачів RC522
#define SS_PIN_1 10
#define RST_PIN_1 9
#define SS_PIN_2 8
#define RST_PIN_2 7

// Піни для зумерів
#define BUZZER_PIN_1 5 // Вхід
#define BUZZER_PIN_2 6 // Вихід

// Піни для LCD
#define I2C_ADDR_1 0x27
#define I2C_ADDR_2 0x26
```

```
// Піни для ESP-01
#define ESP_RX 2
#define ESP_TX 3

// Пін для електромагнітного замка
#define LOCK_PIN 4

// Пін для флеш-пам'яті
#define FLASH_SS_PIN 10

// Ініціалізація зчитувачів RC522
MFRC522 mfrc522_1(SS_PIN_1, RST_PIN_1); // Вхід
MFRC522 mfrc522_2(SS_PIN_2, RST_PIN_2); // Вихід

// Ініціалізація дисплеїв
LiquidCrystal_I2C lcd1(I2C_ADDR_1, 16, 2); // Вхід
LiquidCrystal_I2C lcd2(I2C_ADDR_2, 16, 2); // Вихід

// Ініціалізація серійного з'єднання з ESP-01
SoftwareSerial mySerial(ESP_RX, ESP_TX); // RX, TX

// Ініціалізація об'єкта для роботи з SD карткою
SdFat SD;

// Змінні для зчитувачів RFID
bool isRead = false;
bool isNewCard = false;
String tagContent = "";
String currentUID = "";
int INTERVAL = 2000;
unsigned long previousMillis = 0;
unsigned long currentMillis = 0;
```

```
void setup() {
  Serial.begin(115200);
  mySerial.begin(4800);
  mySerial.setTimeout(5000);

  pinMode(BUZZER_PIN_1, OUTPUT);
  pinMode(BUZZER_PIN_2, OUTPUT);
  pinMode(LOCK_PIN, OUTPUT);

  SPI.begin();
  mfrc522_1.PCD_Init();
  mfrc522_2.PCD_Init();

  lcd1.init();
  lcd1.backlight();
  lcd2.init();
  lcd2.backlight();

  Serial.println("Detecting RFID Tags");

  // Ініціалізація SD бібліотеки
  if (!SD.begin(FLASH_SS_PIN, SPI_HALF_SPEED)) {
    Serial.println("Failed to initialize flash memory");
    return;
  }

  Serial.println("Flash memory initialized successfully");
}

void loop() {
  checkRFID(mfrc522_1, BUZZER_PIN_1, lcd1);
  checkRFID(mfrc522_2, BUZZER_PIN_2, lcd2);
}
```

```
void checkRFID(MFRC522 &mfrc522, int buzzerPin, LiquidCrystal_I2C &lcd) {
  if (mfrc522.PICC_IsNewCardPresent()) {
    if (mfrc522.PICC_ReadCardSerial()) {
      isRead = true;
      tagContent = "";
      byte letter;
      for (byte i = 0; i < mfrc522.uid.size; i++) {
        tagContent.concat(String(mfrc522.uid.uidByte[i] < 0x10 ? " 0" : " "));
        tagContent.concat(String(mfrc522.uid.uidByte[i], HEX));
      }
      tagContent.toUpperCase();
    }

    if (isRead) {
      currentMillis = millis();
      if (currentUID != tagContent) {
        currentUID = tagContent;
        isNewCard = true;
      } else {
        if (currentMillis - previousMillis >= INTERVAL) {
          isNewCard = true;
        } else {
          isNewCard = false;
        }
      }

      if (isNewCard) {
        previousMillis = currentMillis;
        Serial.print("Sending data to ESP-01: ");
        Serial.println(tagContent);
        mySerial.println(tagContent);
        Serial.println("Waiting for response from ESP-01...");

        int iCtr = 0;
```

```
        while (!mySerial.available()) {
          iCtr++;
          if (iCtr >= 100)
            break;
          delay(50);
        }

        if (mySerial.available()) {
          bool isAuthorized = isUserAuthorized(tagContent);
          if (!isAuthorized) {
            playNotAuthorized(buzzerPin);
            lcd.clear();
            lcd.print("Access Denied");
          } else {
            playAuthorized(buzzerPin);
            lcd.clear();
            lcd.print("Access Granted");
            digitalWrite(LOCK_PIN, HIGH);
            delay(1000);
            digitalWrite(LOCK_PIN, LOW);
          }
        }
        Serial.println("Finished processing response from ESP-01.");
      }
    } else {
      Serial.println("No card details were read!");
    }
    tagContent = "";
    isNewCard = false;
  }
}

bool isUserAuthorized(String tagContent) {
  const size_t capacity = JSON_OBJECT_SIZE(1) + 30;
```

```
  DynamicJsonDocument doc(capacity);

  DeserializationError error = deserializeJson(doc, mySerial);
  if (error) {
    Serial.println(error.c_str());
    return false;
  }

  bool is_authorized = doc["is_authorized"] == "true";
  Serial.print("is_authorized: ");
  Serial.println(is_authorized);

  return is_authorized;
}

void playNotAuthorized(int buzzerPin) {
  tone(buzzerPin, 1000, 500);
  delay(500);
  noTone(buzzerPin);
}

void playAuthorized(int buzzerPin) {
  tone(buzzerPin, 2000, 500);
  delay(500);
  noTone(buzzerPin);
}
```

Висновок.

У процесі проведеного дослідження було виявлено, що пристрої управління контролем доступу є невід'ємною складовою сучасних систем безпеки, здатною ефективно забезпечувати захист приміщень різного призначення. Вони дозволяють мінімізувати ризики несанкціонованого доступу, забезпечуючи надійну ідентифікацію та авторизацію користувачів, а також реєстрацію подій доступу та моніторинг переміщення осіб. Впровадження сучасних рішень у цій сфері дозволяє не лише забезпечити високий рівень безпеки, але й оптимізувати витрати на її забезпечення, підвищуючи оперативність реагування на потенційні загрози.

Розроблений у рамках даної роботи прототип пристрою управління контролем доступу відповідає актуальним вимогам безпеки та функціональності. Його впровадження може стати важливим кроком для підвищення рівня захищеності приміщень, забезпечення безпеки матеріальних і інформаційних ресурсів, а також персоналу організації.

Отримані результати мають практичне значення і можуть бути використані для розробки нових або вдосконалення існуючих систем управління доступом у різних сферах діяльності. Таким чином, подальші дослідження та вдосконалення пристроїв управління контролем доступу залишаються актуальними та перспективними напрямками розвитку систем безпеки, спрямованими на забезпечення надійного захисту приміщень та ресурсів.

Список використаних джерел.

1. ATMEGA328P Datasheet [Електронний ресурс] / : https://www.alldatasheet.com/datasheet-pdf/pdf/241077/atmel/atmega328p.html
2. ESP-01 Datasheet [Електронний ресурс] / : https://www.alldatasheet.com/datasheet-pdf/pdf/1179098/etc2/esp-01.html
3. Introduction to I2C communication [Електронний ресурс] / : https://www.circuitbasics.com/basics-of-the-i2c-communication-protocol/
4. Introduction to SPI Interface [Електронний ресурс] / : https://www.analog.com/en/resources/analog-dialogue/articles/introduction-to-spi-interface.html
5. Know about Access Control Systems and Their Types with Features [Електронний ресурс] / : https://www.elprocus.com/understanding-about-types-of-access-control-systems/
6. RC522 Datasheet [Електронний ресурс] / : https://html.alldatasheet.com/html-pdf/346109/nxp/rc522/4518/78/rc522.html
7. UART: A Hardware Communication Protocol [Електронний ресурс] / : https://www.analog.com/en/resources/analog-dialogue/articles/uart-a-hardware-communication-protocol.html
8. Базюра Б. В. Пристрій управління контролем доступу / Б. В. Базюра // Матеріали Міжнародної наукової конференції молодих вчених «Фізика, електроніка, електротехніка 2024» (ФЕЕ :: 2024), – Суми, 22–26 квітня 2024. – Суми «СумДУ». – 2024. – С. 57.
9. Біометричні системи контролю доступу [Електронний ресурс] / : https://klaster.ua/ua/stati-i-obzory/biometricheskie-sistemy-kontrolja-dostupa-obshchii-obzor/
10. Все про rfid-зчитувачі [Електронний ресурс] / : https://idcard.com.ua/ua/blog/vse-rfid-schityvatelyah-opisanie-raznovidnosti-harakteristiki/
11. Система контролю і управління доступом (СКУД) [Електронний ресурс] / : https://ssbb.ua/sistemy-kontrolya-dostupa/sistema-kontrolyu-dostupu/sistema-kontrolya-i-upravlinnya-dostupom/
12. Система контролю і управління доступом [Електронний ресурс] / : https://vistplus.com/it-poslugi/skud/

13. Системи контролю і управління доступом від А до Я [Електронний ресурс] / : https://deps.ua/ua/knowegable-base/reference-information/7824.html

14. Що таке система RFID [Електронний ресурс] / : https://idcard.com.ua/ua/blog/chto-takoe-sistema-rfid-v-chem-ee-osobennosti-ispolzovaniya/

15. Що таке СКУД [Електронний ресурс] / : https://idcard.com.ua/ua/blog/chto-takoe-skud-i-kak-eto-rabotaet/