Вінницький національний технічний університет
(повне найменування вищого навчального закладу)

Факультет інформаційних технологій та комп'ютерної інженерії
(повне найменування інституту)

Кафедра обчислювальної техніки
(повна назва кафедри)

Пояснювальна записка

до магістерської кваліфікаційної роботи
магістр
(освітньо-кваліфікаційний рівень)

на тему: Система безпеки цивільних та виробничих об'єктів на базі мікропроцесорної платформи

Виконав: студент 2 курсу, групи КІ –18м
спеціальності:
123 «Комп'ютерна інженерія»
(шифр і назва напряму підготовки)

Рознюк Р.О.
(прізвище та ініціали)

Керівник: к.т.н., проф. Азарова А.О.
(прізвище та ініціали)

Рецензент: к.т.н, доц. Дудатьєв А.В.
(прізвище та ініціали)

м. Вінниця - 2020 рік

Вінницький національний технічний університет
(повне найменування вищого навчального закладу)

Факультет_Інформаційних технологій та комп'ютерної інженерії_____
Кафедра_Обчислювальної техніки_____
Освітньо-кваліфікаційний рівень_магістр_____
Спеціальність_123 «Комп'ютерні системи та мережі»_____
(шифр і назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри_____
д.т.н., професор Мартинюк Т. Б.
"____" _____20___року

З А В Д А Н Н Я

на магістерську кваліфікаційну роботу

_____Рознюку Роману Олександровичу_____
(прізвище, ім'я, по батькові)

1.Тема магістерської кваліфікаційної роботи: Система безпеки цивільних та виробничих об'єктів на базі мікропроцесорної платформи_____
керівник магістерської кваліфікаційної роботи: Азарова Анжеліка Олексіївна, к. т. н., професор кафедри ОТ._____
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від «06» березня 2020 року №76
2. Строк подання студентом роботи_____
3. Вихідні дані до роботи_технічні характеристики систем доступу, технічий опис мікроконтролерів Atmel, техінчий опис платформ Arduino, середовище розробки ПЗ Arduino IDE для мікроконтролерів Atmel.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)_ Техніко-економічне обґрунтування доцільності розробки. Огляд і аналіз існуючих ситем безпечного доступу до цивільних та виробничих об'єктів. Класифікація замків з електронною картою. Методи аутентифікації за технологія RFID. Проектування мікропроцесорної системи доступу по технології RFID. Схема підключення та вибір електронних компонентів. Розробка та відлагодження програмного забезпечення.
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
Структурно-функціональні схеми. Електрична принципова схеми. Алгоритм роботи системи.

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1-3	к. т. н., професор Азарова Анжеліка Олексіївна		
1-3	к. т. н., доцент Богомолов Сергій Віталійович		
4	к. е. н., доцент Бальзан Марина Володимирівна		

7. Дата видачі завдання_____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Пошук та огляд інформаційних джерел	11.02.2020р.	виконано
2	Огляд і аналіз методів аутентифікації	17.02.2020р.	виконано
3	Дослідження способів побудови систем безпеки	03.03.2020р.	виконано
4	Огляд основних функції та архітектури платформ	17.03.2020р.	виконано
5	Розробка електричної принципової схеми	31.03.2020р.	виконано
6	Розробка та відлагодження програмного забезпечення	14.04.2020р.	виконано
7	Економічна частина	28.04.2020р.	виконано
8	Оформлення пояснювальної записки і презентації	12.05.2020р.	виконано
9	Попередній захист	25.05.2020р.	виконано

Студент _____ Рознюк Р.О.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Азарова А.О.
(підпис) (прізвище та ініціали)

ANNOTATION

Master's thesis is devoted to the development of a security system for access control and monitoring of staff on a microprocessor platform

In the master's qualification diploma work the review and the analysis of ways of construction of microprocessor systems of control of the admission is made. The structural-functional and electrical-schematic schemes are developed, and also the choice of electronic components is carried out. The algorithm of operation and software of the device are also developed. Made a working model of the devic

АНОТАЦІЯ-

Магістерську кваліфікаційну роботу присвячено розробці системи безпеки контролю доступу та моніторингу робочого персоналу на мікропроцесорній платформі

У магістерській кваліфікаційній дипломній роботі зроблено огляд та аналіз способів побудови мікропроцесорних систем контролю допуску. Розроблено структурно-функціональну та електрично-принципову схеми, а також здійснено вибір електронних компонентів. Також розроблено алгоритм роботи та програмне забезпечення пристрою. Виготовлено діючий макет пристрою.

ЗМІСТ

ВСТУП 8
1 ТЕХНІКО-ЕКОНОМІЧНЕ ОБҐРУНТУВАННЯ ДОЦІЛЬНОСТІ РОЗРОБКИ 11
1.1 Суть технічної проблеми та існуючі способи її вирішення 11
1.2 Огляд існуючих підходів до забезпечення безпеки 13
1.2.1 Засоби і системи охоронної, тривожної та пожежної сигналізації. .. 13
1.2.2 Засоби і системи охоронного відеоспостереження 14
1.2.3 Засоби і системи контролю і управління доступом 17
1.2.4 Засоби і системи оповіщення та управління евакуацією людей 20
1.2.5 Засоби і системи охорони периметра 20
1.3 Огляд електричних пристроїв доступу 23
1.4 Потенційні ринки збуту та прогнозування попиту 25
1.5 Обґрунтування вибору системи контролю доступу 26
2 ВИБІР ПРИСТРОЇВ ДЛЯ СИСТЕМИ ІДЕНТИФІКАЦІЇ ВІДВІДУВАЧІВ ІЗ ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ RFID 33
2.1 Класифікація електричних замків 33
2.2 Огляд мікропроцесорних платформ 44
2.3 Вибір компонентів системи 53
2.4 Інтерфейси підключення пристроїв 60
2.5 Методи автентифікації за технологія RFID 65
2.6 Огляд програмного середовища Arduino IDE 70
3 ПРОЕКТУВАННЯ МІКРОПРОЦЕСОРНОЇ СИСТЕМИ БЕЗПЕЧНОГО ДОСТУПУ ДО ОБ’ЄКТІВ 74
3.1 Вибір мікропроцесорної платформи та компонентів 74
3.2 Розробка конструкції пристрою 87

3.3 Розробка алгоритму роботи.....92
3.4 Розробка та налагодження програмного забезпечення 93
3.5 Інструкція по використанню пристрою.....97
4 ЕКОНОМІЧНА ЧАСТИНА 100
4.1 Оцінювання комерційного потенціалу розробки 100
4.2 Прогнозування витрат на виконання науково-дослідної роботи та впровадження її результатів 104
4.3 Прогнозування комерційних ефектів від реалізації результатів розробки....110
4.4 Розрахунок ефективності вкладених інвестицій та періоду їх окупності 111
ВИСНОВКИ 115
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ 116
ДОДАТОК А Технічне завдання..... 118
ДОДАТОК Б Розпіновка плати Arduino UNO 121
ДОДАТОК В Блок-схема алгоритму роботи 122
ДОДАТОК Г Лістинг програмного забезпечення 123

ВСТУП

Захист будь-якого об'єкта включає кілька етапів, число яких залежить від рівня режимності об'єкта. При цьому у всіх випадках важливим етапом буде система управління контролю доступом на об'єкт

В рамках даної роботи передбачається розробити, створити та налагодити невелику діючу модель пристрою контролю доступу та моніторингу персоналу на мікропроцесорній платформі Така модель дозволить практично продемонструвати роботу електронного замка і супутніх йому елементів.

Електринний замок — спеціальний електронний пристрій, необхідне для того, щоб запобігти доступ в закрите приміщення сторонніх осіб, або обмежити вихід з приміщення. Система контролю приймає рішення про дозвіл на доступ в приміщення на основі сигналів від різних пристроїв: зчитувачів магнітних карт, штрих-кодів, датчиків контактної пам'яті, біометричних датчиків, складальної клавіатури, зчитувачів магнітних карт, дистанційного керування та інших всіляких датчиків. У більшості випадків електронний замок є частиною складної системи контролю доступу в приміщення. Як механізми, що перешкоджають доступу в приміщення, використовуються електромеханічні і електромагнітні запірні пристрої. Використання мікроконтролера дозволить спростити основні маніпуляції з системою контролю доступу і самим електронним замком.

З початком осілого життя первісного суспільства і будівництва перших будівель, у людей з'явилася, і з часом все більше загострювалася, необхідність захищати своє майно, рішенням став шматок дерева, закриває вхід в житло. Це була перша версія двері, просто відсовуються в сторону. Пізніше їх стали вішати на навіси, тим самим спростивши відкриття. З ростом поселення виник політичний устрій. Правителі вважали небезпечним своє життя і майно одноплемінникам, для захисту були створені перші замки. Це були звичайні засуви відмикає деревинкою певної форми. З розвитком суспільства розвивалися і технології, двері, ключі і замки набували все більш різні і складні форми. особливо великий скачок стався за останнє сторіччя. Зараз існує велика кількість

дверей і замків. Для відкриття сучасних замків не обов'язково потрібен ключ, точніше ключ в звичному для нас вигляді. Це може бути і числова послідовність вводиться за допомогою клавіатури, і звуку певної частоти Однак не для всіх дверей необхідний замок. Так наприклад, приміщення в якому лікар готується до операції відокремлена від операційної дверима, в будь-якому випадку подолати цю перешкоду лікаря допомагає санітар. Поставити туди автоматичні розсувні двері або залишити взагалі без перегородки не можна, щоб не допустити в операційну вірусів, які можуть викликати у хворого ускладнення. У технології «чисте приміщення» переміщення між кімнатами з різним класом чистоти супроводжується проходженням через спеціальну камеру, в якій проводиться обробка людини або техніки. Довірити обробку автоматиці можна, оскільки через збій двері може відкритися до проведення всіх ступенів обробки, тому при кожній такій камері знаходиться оператор, що стежить за процедурою очищення. Але він може не помітити того, що побачить людина знаходиться в камері, проте після очищення йому не можна взаємодіяти з чим або в камері щоб не занести в приміщення чогось зайвого.

Метою даної роботи є створення системи ідентифікації відвідувачів із використанням технології RFID, яка має можливість введення обліку та контролю відвідувачів. Актуальність даної роботи зумовлена необхідністю забезпеченням безпеки методом контролю доступом та моніторингу персоналу на робочому місці.

Об'єктом дослідження є технологія ідентифікації персоналу і заміни відкриття дверей ключами на відкриття дверей з використанням радіочастотної ідентифікації по технології RFID. Предметом дослідження є методи і засоби реалізації даної технології за допомогою контролера фірми Arduino і зчитувача карток RC522.

Мета і задачі дослідження.

Мета роботи полягає у забезпеченні опрацювання цифрової інформації мікропроцесорною системою із застосуванням сканера технології RFID.

Для досягнення поставленої мети наукового дослідження необхідно вирішити такі задачі:

— здійснити огляд і аналіз видів існуючих систем що забезпечують безпеку;

— здійснити класифікацію систем безпеки;

— дослідити способи та методи ідентифікації з використанням технології RFID;

— здійснити обґрунтування вибору ключа ідентифікації;

— здійснити вибір мікропроцесорної платформи;

— здійснити розробку алгоритму роботи, структурно-функціональної та електрично-принципової;

— здійснити розробку та відлагодження програмного забезпечення.

— Наукова новизна одержаних результатів.

У даній кваліфікаційній магістерській роботі наукова новизна полягає в методі побудови системи безпеки та моніторингу робочого персоналу.

Практичне значення одержаних результатів.

Практичне значення даної магістерської роботи полягає у розробці мікропроцесорної системи безпеки яка забезпечує контроль доступу до приміщення, ідентифікації та моніторингу робочого персоналу системи ідентифікації відвідувачів із використанням технології RFID.

1 ТЕХНІКО-ЕКОНОМІЧНЕ ОБҐРУНТУВАННЯ ДОЦІЛЬНОСТІ РОЗРОБКИ

1.1 Суть технічної проблеми та існуючі способи її вирішення

Суть магістерської кваліфікаційної роботи передбачає застосування знань та принципів побудови технічного і програмного забезпечення мікроконтролерів і мікропроцесорних систем, методологію їхнього застосування в різних пристроях обробки і передачі інформації на прикладі розробки системи забезпечення безпеки доступу до цивільних та промислових об’єктів на базі мікропроцесорної платформи.

У процесі написання магістерської кваліфікаційної роботи необхідно проаналізувати особливості архітектури мікропроцесорних платформ розробки і програмного забезпечення для їх програмування, визначити типові мікропроцесорні комплекти, розглянути технології контролю доступу та автентифікації

Для досягнення мети необхідно здійснити розробку двох основних частини пристрою: апаратної та програмної. Перша з них, в свою чергу, полягає в виборі мікропроцесорної платформи та огляді його архітектури, розробці структурної схеми та вибору електронних компонентів.

З огляду на програмну реалізацію пристрою, слід віддати належне розробці алгоритму функціонування принципової схеми та програми, що керує роботою мікропроцесора.

Пристрій необхідно виконати з урахуванням новітніх досягнень в галузях цифрової техніки, на основі сучасної елементної бази та забезпечити мінімально можливу споживану потужність, високу надійність, малі габаритні розміри та масу, високі технічні характеристики і доступну повторюваність при серійному виробництві та мінімальні економічні витрати.

В даний час електронні системи контролю доступу в приміщення набувають все більшого поширення в життя величезної кількості людей. Електронні замки використовуються там, де заборонено перебувати стороннім, наприклад, в складських приміщеннях підприємств, в підсобних приміщеннях в

магазинах і великих супермаркетах. Незважаючи на це, електронні системи контролю доступу є досить дорогим обладнання для звичайної людини. Але що якщо існують рішення, які б дозволили широкому колу населення використовувати електронні замки в різних цілях.

Системи доступу, будь то звичайний амбарний замок або складна біометрична система по визначенню користувача, завжди були актуальні у людства, так як не дозволяли стороннім особам проникати на закриту територію. Особливо система доступу актуальна в місцях з великим скупченням людей і перешкоджає випадковому проникненню, так і зловмисникові.

Головною метою роботи є розробка системи контролю доступу що обмежує вільний прохід стороннім особам на територію цивільних та промислових об’єктів.

Пристрій повинен володіти як електронним, так і механічним пристроєм доступу, інакше в разі розряду аварійного акумулятора або непередбаченого виходу з ладу електронної частини пристрою, відкрити замок буде можливо без допомоги ключа

Виходячи з вищесказаного, розробка багатофункціонального пристрою контролю доступу в приміщення на мікропроцесорній платформі є актуальним завданням.

Метою даної роботи є: виготовлення діючого макета пристрою, що забезпечує безпечний доступ до приміщення на базі мікропроцесорної платформи.

Для досягнення цієї мети поставлені і виконані наступні завдання:

— огляд існуючих рішень;

— розробка схеми пристрою;

— вибір необхідних компонентів;

— задання алгоритму роботи;

— створення програми роботи пристрою;

— виготовлення макета пристрою;

— налагодження програми і макета.

1.2. Огляд існуючих підходів до забезпечення безпеки

1.2.1 Засоби і системи охоронної, тривожної та пожежної сигналізації

Системи охоронної, тривожної та пожежної сигналізації призначені для виявлення, своєчасного інформування і припинення спроб несанкціонованого проникнення на об'єкт, що охороняється, а так само для забезпечення безпеки життя і здоров'я людей і запобігання псуванню майна та інших цінностей від пожежі, витоку газу, води та ін. При виникненні позаштатної ситуації система подає сигнал тривоги і включає виконавчі пристрої.

Системи охоронної та пожежної сигналізації отримали дуже велике поширення і застосовуються повсюдно на великих об'єктах (заводи, виробничі комплекси, склади, бізнес-центри, великі магазини), середніх (офіси, багатоквартирні будинки, кафе, ресторани, фітнес-центри, гаражі, парковки) і маленьких (приватні будинки, квартири, гаражні бокси, майстерні). Таке поширення обумовлено високою надійністю, ефективністю і економічністю систем, так як автоматика не може вступити в змову з охороною, відволіктися і не схильна до іншим людських факторів, але для певних об'єктів, особливо великих або з підвищеними вимогами до безпеки, електронні системи забезпечують підвищення ефективності служб охорони, так як автоматика не може повністю замінити людину, забезпечити швидке припинення порушень , передбачити всі позаштатні ситуації та ін.

У зв'язку з тим, що охоронна, тривожна і пожежна сигналізація дуже близькі за ідеологією побудови, то, як правило, на невеликих об'єктах їх поєднують на базі єдиного контрольного блоку.

Системи охоронної, тривожної та пожежної сигналізації включають в себе:

— засоби виявлення і ініціації тривоги;

— засоби збору і відображення інформації;

— засоби оповіщення.

У свою чергу охоронні сповіщувачі поділяються: по виду контрольованої зони на точкові, лінійні, поверхневі та об'ємні; за принципом дії на

електроконтактні, магнітоконтактні, ударноконтактні, п'єзоелектричні, оптико-електронні, ємнісні, звукові, ультразвукові, радіохвильові, комбіновані.

Пожежні діляться на сповіщувачі ручного та автоматичної дії, в тому числі теплові, димові, полум'яні .

1.2.2 Засоби і системи охоронного відеоспостереження.

Системи відеоспостереження призначені для забезпечення візуального контролю над всією територією або певними зонами об'єкта, фіксації й запису в архів пересування людей, предметів, транспорту, забезпечення належного функціонування інших систем, з метою забезпечення захисту життя і діяльності людей, збереження матеріальних, інформаційних, інших цінностей, а так само інфраструктури об'єкта.

Принципово системи відеоспостереження можна розділити: за принципом передачі відеосигналу і обробки інформації на аналогові, цифрові та гібридні. Передача сигналу в відеоспостереження заснована на принципах передачі телевізійного сигналу в телебаченні. Аналогові системи з'явилися першими і довгий час займали лідируючі позиції, так як були першими і доступнішим за вартістю, тому в даний час частка аналогових систем відеоспостереження залишається досить великий. Цифрові системи відеоспостереження відрізняються великими можливостями, кращою якістю зображення і більшу функціональність, але і більш високою вартістю, однак, завдяки технічному прогресу, зростанню попиту і високої конкуренції, обладнання подешевшало і стало активно зганяти аналогові системи. Останнім часом дуже актуальним стало виробляти свого роду апгрейд раніше створених систем, так як цифрове обладнання. Мають більші можливості, а виробляти повну заміну обладнання системи дуже дорого, з'явився попит на гібридне обладнання, таким чином утворилося новий напрямок розвитку, яке активно завойовує ринок. Однак, швидше за все буде не дуже тривалим і триватиме до остаточного зганяння

аналогових систем, якщо звичайно не винайдуть новий спосіб передачі та обробки інформації, тоді гібридні системи отримають новий виток розвитку.

За характеристиками передачі кольору системи відеоспостереження поділяються на кольорові або чорно-білі. Чорно-білі системи отримали дуже велике поширення, так як з'явилися першими і були значно дешевше кольорових. Кольорові системи застосовувалися коли кольорове зображення несло істотну додаткову інформацію. Це було характерно для великих об'єктів, на яких використовується велика кількість відеокамер і різниця у вартості була суттєвою, але останнім часом, вартість обладнання стала нижче, доступність зросла і кольорові відеокамери стали поступово зганяти чорно-білі з ринку.

Ще однією з найважливіших характеристик системи є її роздільна здатність, тобто можливість відображати найбільш дрібні деталі зображення. Звичайним дозволом вважається 380-420 телевізійних ліній для чорно-білої відеокамери і 300-350 для кольорової. Відеомонітор повинен мати більш високу роздільну здатність, щоб не погіршувати загальний дозвіл системи. Доцільно вибирати відеомонітор з дозволом 600-800 ліній.

Устаткування, що входить в систему охоронного відеоспостереження :

— телевізійні камери (відеокамери);

— монітори;

— обладнання для обробки зображень;

— пристрою запису і зберігання відеоінформації;

— джерела живлення;

— кабельні мережі передачі інформації та харчування;

— додаткове обладнання.

Устаткування охоронного відеоспостереження докорінно відрізняється від звичної побутової техніки.

Широкий вибір обладнання, в різному ціновому діапазоні, різних виробників, якості, функціоналу і характеристик, змушує задуматися при виборі не тільки простого покупця, але навіть професіоналів, а згодом перелік тільки розширюється. Чим більше вибір, тим конкретніше і точніше повинно бути

розуміння, яку систему і для чого планується створити. Тому, перш ніж приступити до вибору обладнання, необхідно чітко визначити завдання, які вона повинна вирішити.

Забезпечення безпеки об'єкта, особливо для служб безпеки і охорони, тісно пов'язане зі швидкістю реагування на виникнення позаштатної ситуації. Тільки система охоронного відеоспостереження надає можливість негайно показати відбуваються в даний момент подія, а не тільки надати інформацію про місце і характер, як охоронна, тривожна або пожежна сигналізація. Крім того, система фіксує всі факти, зберігає в архіві, обробляє і володіє іншими важливими і корисними функціями. Правильно спроектована система дозволяє в реальному масштабі часу миттєво оцінити обстановку в контрольованих зонах, скоротити час реакції на нештатну ситуацію і забезпечити прийняття найбільш доцільних заходів захисту і протидії виникли обставин.

Можна виділити кілька основних завдань, що вирішуються за допомогою систем охоронного відеоспостереження:

— загальний нагляд за обстановкою;

— виявлення чи з'явилися в поле зору відеокамер люди, тварини, автотранспорт, предмет ;

— ідентифікація та зіставлення виявлених образів;

— фіксація і відстеження траєкторій руху виявлених об'єктів і ін. функції.

Системи відеоспостереження поділяються на прості і складні з різною обробкою зображень.

Прості системи застосовуються для поточного моніторингу за обстановкою на об'єкті в режимі реального часу, вони не володіють спеціалізованими функціями і складаються з відеокамер (одна або дві) і відеомонітора, з'єднаних між собою лінією зв'язку для передачі сигналу від камери на монітор. Така система є базовою для систем відеоспостереження будь-якої складності.

Складні системи застосовуються на об'єктах з серйозними вимогами до безпеки або безпосередньо до відеоспостереження, включають в себе кілька відеокамер, підключених через комутатори, квадратори або мультиплексори на

один-два відеомонітора. В середньому для таких систем використовується до восьми відеокамер, так як більша кількість ускладнює роботу одного оператора з моніторингу ситуації в кожній зоні спостереження. Для одного оператора оптимальним навантаженням вважається спостереження за зображенням з чотирьох відеокамер.

Системи відеоконтролю дозволяють здійснювати відеомоніторинг за ситуацією на об'єкті, реєстрацію і запис відеоінформацій в архів на спеціальні пристрої, які можуть працювати в безперервному режимі або покадрового записувати з заданими інтервалами часу між кадрами, з обов'язковим записом поточного часу і дати. При відтворенні такого запису можливий багаторазовий ретроспективний контроль всієї обстановки в підконтрольних зонах, детальне вивчення тривожну ситуацію з визначенням терміну подій.

1.2.3 Засоби і системи контролю і управління доступом

Системи контролю і управління доступом це сукупність програмно-технічних засобів і організаційно-адміністративних заходів, що забезпечують організацію, обмеження, розподіл і перерозподіл прав доступу персоналу, відвідувачів, користувачів, транспорту на підконтрольну територію об'єкта, з метою забезпечення безпеки життя і діяльності людей, збереження майна, матеріальних та інформаційних цінностей, інфраструктури і цілісності об'єкта.

Останнім часом основною тенденцією розвитку системи є їх інтелектуалізація і інтеграція з іншими системами безпеки. У систему входить велика кількість підсистем, які можуть працювати повністю автономно (домофон, турнікети, шлагбауми, електронні замки, автоматичні ворота і хвіртки), А можуть взаємодіяти з усіма системами контролю доступу та іншими системами безпеки. Системи забезпечують збір, обробку і формування звітів з використанням значної кількості інформації, і передають її на головний комп'ютер (сервер), по суті, в комплексних системах безпеки, вони виконують одну з центральних функцій, завдяки інформації отриманої і переданої система

налаштовує функції і регламент роботи інших систем, наприклад відеоспостереження, охоронної та пожежної сигналізації, охорони периметра, освітлення, вентиляції, опалення зв'язку.

До складу програмно-апаратного комплексу системи входить наступне обладнання: контролер, зчитувачі, ідентифікатори, перегороджуючі пристрої, блоки живлення, програмне забезпечення

Контролер — високонадійний електронний прилад, що забезпечує акумулювання, зберігання і зіставлення інформації про конфігурацію і режимах роботи системи, перелік осіб, які мають права доступу на об'єкт і рівень їх повноважень (в тому числі біометричні дані, для відповідних систем). У простих системах, які не потребують роботи з великою кількістю інформації і різними функціями, контролер може бути вбудований в зчитувач.

Зчитувачі — електронні пристрої, що відповідають за витяг (зчитування) відповідної інформації з певного носія (пластикові карти, штрих-коди, біометричні дані-відбитки пальців, кистей, сітківка ока, риси обличчя тощо.)

Зчитувач передає отриману інформацію контролеру, який виробляє звірку з зберігаються в ньому даними і приймає рішення про дозвіл або обмеження доступу. У більш масштабних системах цю функцію можна перенаправити на ПК, тобто остаточне рішення про дозвіл або заборону проходу буде віддаватися з комп'ютера.

Ідентифікатори особистості — носії інформації про особу, повноваження і права доступу на об'єкт конкретної особи. Вид і носій ідентифікатора залежить від системи контролю доступу і параметрів зчитувача, наприклад це можуть бути ключі, брелки, магнітні карти, пропуску з штрих-кодом, а так само біометричні дані для відповідних систем.

Перегороджуючі пристрої — це пристрої, призначені для обмеження проходу або проїзду на територію об'єкта, яке звільняє прохід або проїзд тільки після підтвердження прав доступу користувача і отримання відповідного сигналу від контролера або комп'ютера. До таких пристроїв відносяться системи

домофона і відеодомофона, електронні замки, шлагбауми, автоматичні ворота, хвіртки, турнікети, шлюзові кабіни та ін.

Пристрої контролю і стану датчиків різних типів, що відповідають за моніторинг стану перегороджують пристрою і передають відповідний сигнал в разі спроби несанкціонованого проникнення (наприклад відкриття дверей).

Блоки резервного і безперебійного живлення - призначені для забезпечення роботи системи в разі непередбаченого, аварійного або планового відключення основного електроживлення.

Програмне забезпечення — необхідний елемент СКУД середнього і високого класу, в той час як прості системи можуть обходитися без нього.

Програмний продукт встановлюється на комп'ютер і містить апаратні засоби зв'язку з контролерами і забезпечує виконання найважливіших функцій з обслуговування СКУД:

— конфігурація контролерів із забезпеченням процедури занесення в них списків користувачів і їх прав проходу;

— ведення бази даних точок контролю проходу користувачів, допущених в приміщення і на територію об'єкта, аналіз їх переміщень;

— знімання інформації про події на точках контролю, її обробка, документування та архівування;

— надання оператору системи поточної інформації;

— оперативне управління системою.

Програмне забезпечення є дуже важливою частиною системи СКУД (крім маленьких і не потребують аналітики, так як наприклад навіть система з двох зчитувачів потребуватиме ПО якщо Замовник захоче вести облік робочого часу), воно забезпечує багато функцій системи, полегшує роботу з нею і дозволяє взаємодіяти з іншими системами. Саме тому зараз багато розробників ПЗ і обладнання різних напрямків систем безпеки активно співпрацюють і інтегрують свої продукти. Нажалю, поки що зберігається ситуація, що програми управління системами доступу від різних виробників орієнтовані на управління контролерів конкретних виробників. Буває, що для обладнання одного виробника кілька

розробників пишуть своє ПЗ. Однак, глобалізація проект об'єктивний, кожен виробник обладнання програмного забезпечення і устаткування зацікавлені в його просуванні на ринку, тому створюється все більше і більше інтегрованих рішень.

1.2.4 Засоби і системи оповіщення та управління евакуацією людей

Система призначена для забезпечення своєчасного оперативного оповіщення та управління рухом людей при евакуації в безпечну зону, в разі виникнення пожежі, позаштатних ситуацій та інших загрозах для безпеки, життя і здоров'я людей. Безпечною зоною вважаються приміщення (або ділянок приміщень) всередині будівель і споруд і територія безпосередньо об'єкта, прилегла територія або приміщення і територія, що знаходяться на безпечній відстані від джерела небезпеки, але не належать до об'єкта охорони.

Залежно від функціональних характеристик система оповіщення та управління евакуацією підрозділяється на п'ять типів:

При оснащенні об'єктів системами оповіщення та управління евакуації керуються індивідуальними параметрами об'єктів і чіткими нормами регламентуючих документів, які потрібно неухильно дотримуватися. Тип системи, структура, склад обладнання системи, його технічні характеристики визначаються на підставі нормативних документів і індивідуальні для кожного об'єкта, до цього питання потрібно підходити дуже серйозно, так як від правильності і ефективності роботи системи (особливо на великих об'єктах), можуть залежати життя багатьох людей.

1.2.5 Засоби і системи охорони периметра

Периметр — це зовнішня межа території об'єкта. Система охорони периметра призначена для забезпечення безпеки об'єкта, запобігання та мінімізації ризиків несанкціонованого порушення кордонів периметра людьми,

тваринами, транспортом та іншими об'єктами, а так само для своєчасного інформування користувача і систем і служб безпеки об'єкта (в тому числі позавідомча охорона, внутрішня служба охорони та тд.), про спробу проникнення на територію об'єкта і про всіх позаштатних ситуаціях і спробах порушення кордонів периметра.

Захист периметра — це один з найважливіших елементів в системі комплексної безпеки об'єкта. По суті, периметр, це перший рубіж території, що захищається і від того, на скільки добре забезпечена його охорона і захист, залежить ступінь захищеності всього об'єкта в цілому, максимальний період часу для реагування інших систем і служб безпеки (чим краще захищений периметр, тим менше ймовірність порушення кордонів об'єкта, тим більше у інших служб часу на якісну і своєчасну реакцію щодо запобігання проникнення порушника на територію об'єкта). Охорона периметра це обов'язкова складова частина систем безпеки аеропортів, об'єктів енергетичної галузі, нафтохімічної і газової сфери, військових об'єктів, об'єктів транспорту, наукових і багатьох виробничих об'єктів і ін. Охорона периметра дозволяє виявити потенційного порушника на "ранніх підступах" до об'єкта, з новітнім обладнанням можливо зафіксувати не тільки початок дії (наприклад, коли людина вже намагається пролізти через огорожу), а в момент появи наміри (наприклад, коли людина ще тільки оцінює варіанти, варто це робити чи ні, або в якому місці це краще зробити, або тільки входить в потенційно небезпечну зону), тобто заходи щодо запобігання проникнення можна приймати набагато оперативніше і навіть припиняти такі спроби заздалегідь. Розвиток систем безпеки зробило обладнання систем охорони периметра набагато дешевше, різноманітніше і доступнішим, тому ці системи стали активно впроваджуватися не тільки на великих об'єктах, а й на порівняно невеликих, наприклад для захисту приватних будинків і котеджів, хоча ще 5 років тому це було досить дороге задоволення.

Механічні перешкоди сповільнюють і ускладнюють проникнення на територію об'єкта, а технічні засоби дозволяють своєчасно виявити факт або намір порушення, оповістити користувачів, підняти тривогу, а так само, при

відповідних настройках, відлякати порушника (не у всіх залишиться бажання продовжувати лізти через паркан при включенні звукової сирени, спрямованих світлом прожекторів і під прицілом відеокамер).

При оснащенні периметра необхідно враховувати:

— можливість виділення смуги відчуження (забороненої зони) для розміщення технічних засобів охорони;

— особливості рельєфу місцевості та прилеглої території;

— топографію об'єкту і режим його роботи;

— види рослинності на об'єкті та на прилеглій території;

— інфраструктуру прилеглої території, наявність залізничних і автомагістралей, трубопроводів, кабельних ліній, водних шляхів та ін.

— потреби користувачів системи в комфорті;

— особливу увагу слід звернути на "зони розривів" при організації воріт, хвірток та ін.

Недбалість і неякісна інтеграція обладнання різних систем можуть знизити якість роботи системи в цілому.

Залежно від індивідуальних особливостей об'єкта лінія периметра може бути оснащена як одним, так і кількома рубежами охорони, а так само або цілком, або на окремих ділянках периметра.

Однорубежная система охорони, в свою чергу, може бути створена на базі якогось одного, найбільш підходящого для конкретних умов засоби виявлення, або складатися з комбінації сповіщувачів різного принципу дії. Наприклад нижня і середня частина сітчастої огорожі захищаються кабельноим чутливим елементів (чутливим до вібрацій і розриву з'єднання), а козирок променевим извещателем. В результаті отримуємо систему, захищену від спроби непомітного порушення цілісності огорожі і спроби перелізти зверху.

Многорубежная система охорони оснащується двома або більше рубежами, розташованими на певній відстані один від одного, поєднує в собі кілька засобів забезпечення безпеки, дає можливість визначати напрямок руху порушника і

дозволяє зберегти працездатність системи при виході з ладу одного з засобів виявлення, тому є більш надійною і функціональної.

1.3 Огляд електричних пристроїв доступу

В даний час немає дефіциту електричних пристроїв доступу, тому були обрані, для аналізу, ходові моделі зі схожими характеристиками, що і розроблювальний пристрій. Так само було враховано співвідношення ціни і якості.

На ринку популярна система контролю і управління доступом (СКУД) фірми Ашробот. У них є набори комплектів з різних функціоналів. Комплект під номером 27 підходить по функціоналу по відношенню до розробляється пристрою, відповідно аналізувати будемо його.

СКУД комплект 27 має сканер відбитків пальців для впізнання користувачів. Так само отримати доступ можливо за допомогою RFID карти і звичайного ключа. СКУД не має безперебійного джерела живлення, його потрібно докуповувати окремо. На рисунку 1.1 зображений СКУД комплект 27. У комплект входить: електромоторний виразний замок DJ05ST; біометричний зчитувач з вбудованим контролером; блок живлення.

Рисунок 1.1 — СКУД комплект 27.

Ціна комплекту 5600 гривень. Так само до комплекту можна докупити WiFi контролер і мати бездротовий доступ. Ціна контролера 1500 гривень.

Недоліком даного пристрою є розташування керуючої плати пристрою, яка знаходиться в передній панелі, що знижує захищеність. До недоліків відноситься і відсутність безперебійного живлення.

Із зарубіжних аналогів дверних замків популярна модель Aqara Smart Lock виробника Xiaomi. Пристрій виконаний в одному корпусі і харчується від чотирьох батарейок типу АА. Має сканер відбитка пальця, панель введення цифрового пароля. Так само отримати доступ можливо за допомогою RFID карти і звичайного ключа. На рисунку 1.2 зображено електронний замок Xiaomi Aqara Smart Lock. До переваг можна віднести безліч способів отримання доступу. Недоліком є живлення від батарейок. Ціна становить 7200 гривень.

Рисунок 1.2 — Електричний замок Xiaomi Aqara Smart Lock.

Якщо ж порівнювати в низькому ціновому діапазоні, то тут буде модель фірми Galo. Електронний замок від фірми Galo відкривається за допомогою RFID мітки і звичайного ключа. У деяких версіях є панель введення пароля і

дистанційний радіо пульт. Електронна частина живиться від зовнішнього джерела живлення і не має безперебійної частини. На рисунку 1.3 зображено електронний замок від фірми Galo. Перевага даного електронного замка полягає в невисокій ціні. До недоліків відноситься відсутність безперебійного джерела живлення, відсутність сканера відбитка пальця. Ціна звичайної версії становить 1700 гривень.

Рисунок 1.3 — Електричний замок від фірми Galo.

1.4 Потенційні ринки збуту та прогнозування попиту.

Обсяг продажів на світовому ринку електронних систем контролю доступу в період до 2024 року буде рости в середньому на 9,3% на рік. Такі дані отримала дослідницька компанія Research and Markets. У 2015 році він становив $ 4,7 млрд.

Головним драйвером зростання даного ринку залишається потреба в підвищенні безпеки різних об'єктів у всіх основних секторах - комерційному, промисловому, державному, приватному. Популярність контролю доступу росте на тлі повідомлень про сплески кримінальної активності, що породжують потребу в міцній фізичний захист.

Постійно з'являються нові технології, які можна застосовувати в сфері безпеки, і виробники систем контролю доступу випускають на їх основі передові

системи, адресовані різним типам кінцевих замовників. Розвиток веб-технологій сприяє впровадженню систем контролю доступу, оскільки підвищує зручність їх інсталяції і їх доступність, а також полегшує масштабованість.

У зв'язку з вищесказаним, найбільш швидкозростаючим на ринку електронних систем контролю доступу є сегмент «Контроль доступу як послуга» (Access Control as a Service - ACaaS). Ця перспективна модель відносин між замовником і професіоналами ринку за останній час набула реальних обрисів. Розвиток хмарних технологій і Інтернету речей спонукає підприємців використовувати ACaaS з метою зниження витрат на безпеку.

Серед факторів, що стримують розвиток ринку електронних систем контролю доступу, експерти виділяють брак у потенційних замовників відомостей про можливості існуючих систем і відсутність у них рішучості інвестувати в новітні досягнення IT-сфери.

Технологічні нововведення у виробництві зчитувачів і постійне розширення площ, доступ до яких необхідно обмежувати, підживлюють зростання сегмента послуг в сфері систем контролю доступу. Автори дослідження виділяють також інтенсивний розвиток інтеграції контролю доступу з іншими видами систем безпеки. Все більш значний вплив на розвиток ринку систем контролю доступу надають додатки для смартфонів.

При цьому ринок систем контролю доступу залишається сильно фрагментованим. На ньому є кілька глобальних гравців і безліч локальних виробників.

1.5 Обґрунтування вибору системи контролю доступу.

Застосуванню систем контролю і управління доступом в складі систем безпеки офісів в багатьох випадках не приділяється належної уваги. Як правило, при створенні системи безпеки обмежуються установкою системи охоронно-пожежної сигналізації для захисту майна в неробочий час. Часто це викликано браком інформації про переваги використання сучасних систем контролю і

управління доступом і додаткові можливості, які вони надають. Також поширена думка, що систем контролю і управління доступом при високій вартості і складності експлуатації не підвищує рівень безпеки об'єкта та ефективність роботи персоналу. Насправді це не зовсім вірно. Сучасні пропозиції на ринку систем контролю і управління доступом відрізняються великою різноманітністю рішень в широкому діапазоні цін і функціональних можливостей. Надійність обладнання відомих виробників дозволяє багато років експлуатувати систему без стороннього втручання. Ступінь безпеки офісу при наявності систем контролю і управління доступом підвищується, оскільки її унікальною властивістю є захист приміщень від несанкціонованого проникнення сторонніх осіб саме в робочий час, коли система охоронної сигналізації відключена. Це особливо актуально для офісів, розташованих в бізнес-центрах, орендованих приміщеннях на території підприємств і в окремих будівлях, де можливий вільний доступ відвідувачів на територію. Можливість контролю дотримання режиму роботи дозволяє підвищити трудову дисципліну співробітників і скоротити витрати. Таким чином, установка систем контролю і управління доступом є додатковим засобом підвищення безпеки та ефективності роботи. Розглянемо основні завдання, які дозволяє вирішити установка систем контролю і управління доступом, і додаткові можливості, що надаються системою.

У мінімальному варіанті системою оснащується тільки центральний вхід. Залежно від планування приміщень і місця розташування офісу це може бути вхід в будівлю, вхід на поверх бізнес-центру, вхід з коридору орендованого приміщення або вхід з клієнтської зони в службову зону офісу. З точки зору структури системи ці варіанти не мають принципових відмінностей.

При наявності запасних і службових входів або евакуаційних виходів можлива організація кількох точок доступу для проходу співробітників. Для зменшення витрат на установку системи додаткові входи можуть не оснащуватися систем контролю і управління доступом і використовуватися тільки для евакуації персоналу при виникненні нештатних ситуацій, в штатному режимі роботи вони повинні бути закриті.

Більшість систем може забезпечити два основні режими контролю доступу: односторонній, з пред'явленням ідентифікатора при вході і вільним виходом після натискання кнопки, або двосторонній, з входом і виходом по пред'явленню ідентифікатора. У першому випадку точка доступу оснащується одним зчитувачем, встановленим із зовнішнього боку, і кнопкою виходу з внутрішньої сторони дверей, у другому випадку замість кнопки виходу необхідно встановити другий зчитувач. Вибір режиму обмеження доступу залежить від пропонованих вимог. Для запобігання входу на територію сторонніх осіб досить оснастити двері одностороннім контролем доступу. Якщо планується використання точок доступу для обліку робочого часу співробітників, необхідно передбачити двосторонній контроль проходу. Двосторонній контроль також перешкоджає вільному виходу з території офісу осіб, які проникли всередину несанкціонованим способом.

Важливим моментом є вибір режиму роботи з відвідувачами. Якщо відвідувачі не є постійними клієнтами, необхідно дистанційне керування проходом. Для постійних клієнтів краще використовувати електронні ідентифікатори, оформлені у вигляді пропуску клієнта або дисконтної карти. У більшості випадків доцільніше використовувати змішаний режим роботи, що передбачає як видачу карт клієнта, так і дистанційне керування точкою доступу.

При реалізації дистанційного управління точками доступу необхідно врахувати вимоги до безпеки офісу. Якщо офіс розташовується на території, що охороняється бізнес-центру або орендованої частини будівлі, для дистанційного керування досить встановити викличний пристрій або домофон і кнопку дистанційного керування. При розміщенні офісу на охороняється території бажано встановити відео домофон або відеосистему для контролю обстановки перед входом. При наявності в офісі спеціальної клієнтської зони з вільним доступом і розміщенні основної точки доступу на вході в службову зону можна організувати прохід відвідувача в супроводі відповідального менеджера.

Наступним кроком щодо підвищення ступеня безпеки і оптимізації роботи офісу є оснащення систем контролю і управління доступом внутрішніх приміщень для розмежування доступу.

Переваги які може дати розмежування доступу. По-перше, заборонити вільний вхід сторонніх осіб і деяких співробітників в відповідальні приміщення, наприклад, бухгалтерію, переговорну або кабінет директора. Додатково для клієнтів і співробітників можна задати різні групи приміщень і інтервали часу, протягом яких дозволений доступ. По-друге, забезпечити протоколювання фактів проходу в ці приміщення з фіксацією прізвища, дати і часу проходу для аналізу нештатних ситуацій. По-третє, дозволяє організувати більш детальний облік робочого часу.

У деяких випадках обмеження доступу у внутрішні приміщення дозволяє запобігти крадіжкам майна підприємства і співробітників при короткочасній відсутності персоналу в приміщенні або знаходженні двері поза увагою, так як двері закриті для входу сторонніх осіб.

Внутрішні приміщення також можуть бути оснащені як одностороннім, так і двостороннім контролем доступу.

Облік робочого часу дозволяє спростити роботу керівників відділів і бухгалтерії по складанню табеля і нарахування заробітної плати. Додатковою перевагою запровадження електронного обліку робочого часу, як правило, стає підвищення трудової дисципліни співробітників за рахунок зменшення кількості невиробничих витрат часу, викликаних запізненнями, несанкціонованим або раннім відходом з робочого місця, так як ці факти неупереджено фіксуються в системі і не можуть бути приховані від керівництва .

У найпростішому випадку використовується одна або кілька точок доступу, через які здійснюється вхід на територію офісу. Пред'явлення карти доступу при кожному вході і виході фіксується системою обліку робочого часу для подальшого розрахунку.

У більш складних конфігураціях, коли системою оснащені внутрішні приміщення, можлива організація кількох областей контролю для різних груп

співробітників з контролем присутності персоналу безпосередньо на робочому місці.

Слід особливо підкреслити, що для роботи функції обліку робочого часу необхідно адміністративними заходами забезпечити пред'явлення ідентифікатора кожним співробітником в разі проходу через точку доступу групи з кількох людей.

Для розрахунку фактично відпрацьованого часу можуть застосовуватися різні алгоритми. Перший варіант розрахунку враховує сумарний час перебування працівника всередині галузі контролю, при цьому час перебування за її межами не враховується. Такий алгоритм застосуємо в тому випадку, якщо співробітнику не потрібно залишати офіс або робоче місце по службовій необхідності. Другий варіант розрахунку проводиться за принципом «Перший вхід - останній вихід». Тобто при розрахунку до уваги береться час перебування працівника поза області контролю протягом робочого дня. Цей механізм дозволяє вести облік в тих випадках, коли співробітник має право залишати територію або перебувати в приміщеннях офісу, які не обладнані систем контролю і управління доступом. Модуль обліку робочого часу може додатково надавати варіанти настройки обліку обідньої перерви, режимів фіксованого або гнучкого початку і закінчення робочого дня, обліку запізнень, переробок лікарняних листів, що ковзають графіків. При виборі системи необхідно звернути особливу увагу на зручність інтерфейсу і відповідність наявних функцій системи обліку встановленим вимогам.

Результати роботи системи обліку можуть надаватися у формі різних звітів, файлів даних в стандартних форматах або експортуватися безпосередньо в бухгалтерські програми, наприклад «1С». Останній варіант економить час, що витрачається бухгалтером на введення інформації, і зменшує ймовірність виникнення помилок.

Можливість надання звітів присутній у всіх систем контролю і управління доступом з функцією обліку робочого часу. Форма і деталізація звітів залежить від параметрів програмного забезпечення. Керівник відділу або бухгалтер

вибирає необхідний період часу і вид звіту, аналізує отримані дані і використовує їх для розрахунку заробітної плати.

Експорт в бухгалтерські програми або файли даних доступний не у всіх системах. Наявність цих можливостей і сумісність з використовуваним типом і версією бухгалтерського програмного забезпечення необхідно уточнювати при виборі типу систем контролю і управління доступом. Файли даних можуть бути зручні для подальшої обробки спеціалізованим програмним забезпеченням, розробленим програмістами підприємства, виробником систем контролю і управління доступом або сторонніми організаціями на підставі технічного завдання. Можливість і вартість розробки спеціалізованих модулів необхідно уточнювати при виборі системи.

Багато програмних продуктів систем контролю і управління доступом підтримують ряд додаткових функцій, призначених для підвищення безпеки об'єкта та зручності експлуатації. До них відносяться:

— відображення планів об'єкта і місць розташування обладнання, відображення стану пристроїв, автоматичне перемикання планів по тривозі;

— управління системою з комп'ютера в ручному і автоматичному режимі за тимчасовими розписами;

— робота з тимчасовими і разовими перепустками;

— підтримка роботи з настільними зчитувачами для автоматизації видачі пропусків;

— формування макета пропуску та роздруківка зображення на картах;

— фото ідентифікація користувача при пред'явленні пропуску для виявлення фактів крадіжок і підробки ідентифікаторів;

— пошук персоналу за місцем останнього пред'явлення ідентифікатора;

— підтримка додаткових робочих місць операторів системи для розподілу функцій з охорони об'єкта, адміністрування системи, управління базою даних пропусків, формуванню звітів і аналізу подій;

—гнучке налаштування повноважень операторів та адміністраторів різного рівня з управління та налаштування системи;

— інтеграція з системами телевізійного спостереження;

— інтеграція з підсистемами охоронно-пожежної сигналізації.

Значна частина цих можливостей не буде затребувана при організації систем контролю і управління доступом в невеликому офісі. Деякі з них, наприклад, відображення планів, Фото ідентифікація, робота з настільними зчитувачами, підтримка додаткових робочих місць, можуть бути присутніми в програмному забезпеченні за замовчуванням, не вимагають додаткових витрат і можуть бути використані при необхідності.

Варіанти використання системи телевізійного спостереження в офісі можуть бути найрізноманітнішими - спостереження за діями відвідувачів, автомобілями на автостоянці, входами в офіс, пошук місця знаходження співробітників в офісі, цілодобова запис відеоінформації.

Необхідність застосування інтеграції на кожному об'єкті розглядається індивідуально і залежить від багатьох факторів.

Розглянемо основні критерії вибору обладнання систем контролю і управління доступом і варіанти організації роботи з системою на етапі експлуатації.

Традиційно завдання обмеження доступу в офіс покладають на різні домофони або автономні систем контролю і управління доступом з функцією відкриття дверей електронним ключем (картою) або набором коду на клавіатурі, однак такі рішення мають ряд обмежень. По-перше, вони або не забезпечують достатній ступінь захисту від несанкціонованого проникнення, якщо для доступу використовується клавіатура, або мають складний механізм програмування і видалення ключів доступу, що вимагає значних витрат часу на зміну списку дозволених ідентифікаторів. По-друге, ці рішення не передбачають можливості протоколювання фактів проходу, обліку робочого часу і використання додаткових функцій щодо розмежування прав доступу користувачів за часом. По-третє, при організації декількох точок доступу необхідна індивідуальна настройка кожного контролера при будь-якій зміні вимог до режиму роботи, так як набір декількох автономних пристроїв, по суті, не є системою.

2 ВИБІР ПРИСТРОЇВ ДЛЯ СИСТЕМИ КОНТРОЛЮ ДОСТУПОМ ІЗ ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ RFID

2.1 Класифікація електричних замків

На сьогоднішній день існує кілька типів замків, для відкриття і закриття яких не потрібен ключ. Точніше сказати, ключ виглядає не так як ми звикли — це замки з магнітним ключем або кодові замки.

Кодовий замок - пристрій фіксації, для відкриття якого потрібно вказати кодову комбінацію, що вводиться за допомогою спеціальної клавіатури або іншими способами.

Кодові замки можна класифікувати за типом і способу управління запірним механізмом.

За типом кодові замки діляться на навісні, врізні і накладні. За способом управління замки діляться на механічні та електронні. Механічні сьогодні вважаються менш привабливими для установки, оскільки мають ряд недоліків, вони швидше виходять з ладу і зламати такі замки набагато простіше. Механічні замки підрозділяються на кнопкові, поворотні і роликові.

Основна перевага замків електронного принципу дії — це те, що їх вузол управління може розташовуватися окремо від замку. Ця особливість робить їх більш захищеними від злому.

Керується сучасний електронний замок з допомогою набору комбінацій букв і цифр на спеціальній панелі або ж за допомогою спеціального магнітного ключа. Вірний код зберігається в пам'яті електронного блоку. Замикаючий механізм такого замка повинен залишатися замкненим навіть в разі повного відключення живлення. Електричні замки схильні до злому, але зробити це може далеко не кожен, що робить цей замок більш надійним, ніж механічний.

Перевагою кодового замку є відсутність ключів (ключ від такого замку зберігається в голові господаря). Але крім переваг є і недоліки з часом кнопки кодового замка трохи западають або стираються, і побачивши цей дефект стає простіше підібрати потрібну комбінацію.

Електронний замок — електричний пристрій, призначений для обмеження доступу в приміщення або обмежити вихід. Рішення про відкриття замку приймається на основі сигналів з різних датчиків. Частиною електронної системи контролю доступу є виконавчий механізм, в якості якого використовуються електромеханічні і електромагнітні запірні пристрої.

За способом відмикання (замикання) замки діляться на:

— електромеханічний замок;

— електромагнітний замок.

За типом ключа замки підрозділяються на:

— кодовий замок;

— розумний замок;

— біометричний замок.

Магнітний замок — замикає пристрій, засноване на впливі магнітом на ригель. Пасивний електромагнітний замок працює без електричного живлення, володіє невеликою силою, застосовується для утримання дверей закритими.

Електромагнітний замок складається з корпусу з електромагнітом і у відповідь планки з металу з великою магнітною проникністю. Такі замки використовуються як виконавчі пристрої систем керування дверима. Потужність такого електромагніту повинна бути достатньою, щоб не було можливості відкрити двері силовим методом.

Переваги електромагнітного замка:

— у випадку аварійного відключення електроживлення замок відмикається, що робить можливим безперешкодне евакуацію;

— простота конструкції;

— відсутні рухомі частини.

Недоліки електромагнітного замка:

— великі габарити і маса замикаючого пристрою;

— необхідний надійне джерело живлення, без електроенергії замок відмикається.

Електронний кодовий замок, що зображено на рисунку 2.1 складається з чотирьох основних частин.

Замок з електромагнітним приводом замикаючого механізму. Якщо введений код збігається з комбінацією на носії інформації на електромагніт подається електричний імпульс відмикає або замикає засув замка.

Зовнішній пульт управління. Пристрій, що зчитує, його вид залежить від способу введення сигналу.

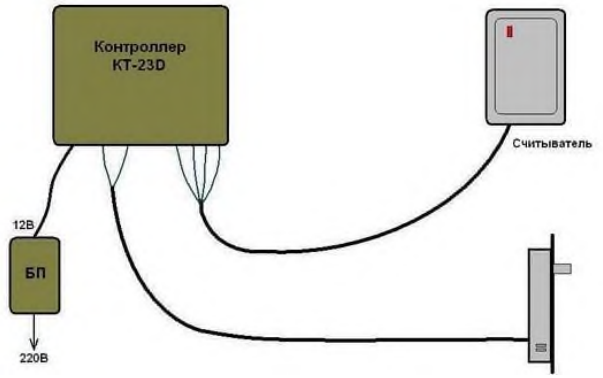

Рисунок 2.1 — Електромагнітний замок

Внутрішній блок управління. Контролер, який приймає сигнал з зчитувача і порівнює його з наявною в пам'яті комбінацією. У разі збігу подає імпульс на електромагніт замку для його відкриття.

Джерело безперебійного живлення. Наявність такого джерела обов'язково для електронних замків, оскільки при відключенні електрики замок переходить в свій нормальний стан. Ємності такого блоку досить для безперебійної роботи замка в перебігу декількох днів.

Електромеханічний замок - заснований на механічному впливі на запірний механізм. Механічний вплив здійснюється електродвигуном або соленоїдом.

Електромагнітні замки оснащені функцією контролю стану дверей.

Види замків:

— соленоїдні замки;

— замки з електроблокуванням;

— моторні замки.

В соленоїдних замках ригель приводиться в рух металевим сердечником, який втягується в соленоїд.

В замку з електроблокуванням замикання створюється за допомогою пружин. Механізм приводиться в дію соленоїдом або електродвигуном. Електромоторні замки, в конструкцію яких входить редуктор, розвивають більше зусилля, що дозволяє працювати при перекосі двері або неправильної установки замку, але працюють повільно.

Моторні замки рейкового типу працюють швидко, але з підвищеним шумом і розвивають мале зусилля (в кілька кілограмів).

Електромоторні замки мають два нормальних стану - «відкрито» і «закрито», тому не підходять для забезпечення безпеки дверей.

Електромеханічні замки підрозділяються на нормально-закриті, нормально-відкриті і моторні з двома нормальними положеннями.

Розблокування нормальнозакритих замків відбувається при подачі електричного сигналу. При відключенні харчування двері з такими замками залишаються закритими, тому їх не можна встановлювати на шляху евакуації.

При відключенні електричного живлення в нормально-відкритому механізмі відбувається блокування ригелів замка в утягненому стані. Принцип роботи електромеханічного замка Надійне замикання дверей при використанні в якості захисту електромеханічного замка забезпечується за рахунок запірного ригеля, який підключений до електроприводу. Установка даного виду замку багато в чому схожа з механічними замками. Відповідно, фіксація їх здійснюється безпосередньо на двері. До електромеханічного замку.

Принцип роботи електромеханічного замка. У той момент, коли закриваються двері, за допомогою вхідно ригеля відбувається зведення в робоче положення спеціальної пружини. В цей же час запірний ригель блокує двері за рахунок входження в відповідну планка замку. При цьому забезпечується блокування високої надійності, яка не може бути порушена навіть зломом двері методом віджимання. Розблокування дверей може бути здійснена тільки за

допомогою соленоїда: на соленоїд надходить напруга, приводячи тим самим в дію скидання фіксатора пружини, яка втягує в корпус замку запірний ригель. При закритті двері, механізм електромеханічного замка знову в автоматичному режимі здійснює її блокування.

Розумний замок, смартлок або замок неведимка — це електронний замок, що відкривається за допомогою смартфона по бездротовому мережі. В основному смартлок встановлюють на механічні замки. Для електричних і електромагнітних замків смарлок виконує роль контролера. Це дозволяє встановлювати розумні замки не тільки на вхідні двері, але і на ворота, міжкімнатні двері або шлагбаум.

Розумні замки з'явилися при популяризації смартфонів і всього за кілька років стали найпоширенішими електронними замками. механізм автентифікації Ключем для розумного замку є смартфон. Смартлок відстежує смартфони, що потрапили в його бездротову мережу, і визначає чи є у цього смартфона право на управління замком. Смартфон, який має доступ до управління замком, віддає команду «відкрити» або «закрити», яку смартлок виконує.

Спочатку віртуальний ключ знаходиться тільки у власника замку, але він може його передати іншим користувачам. Віртуальний ключ можна налаштувати за часом, зробити його тимчасовим або постійним, обмежити час дії по певних днях або годинах.

Як правило, для взаємодії зі смартфонами розумні замки використовують Bluetooth, BLE (Bluetooth Low Energy) або Wi-Fi мережі. Bluetooth і BLE мають невеликий радіус дії, але споживають небагато енергії, що дозволяє замку довгий час працювати від акумулятора. Через велику споживання електроенергії Wi-Fi модулем, інтегрувати Wi-Fi в сам замок нераціонально. Зазвичай використовується Wi-Fi-міст, підключений до мережі неподалік від замку, замок зв'язується по Bluetooth з мостом, а міст зв'язується зі смартфоном по Wi-Fi, це дозволяє управляти замком на більшій відстані.[1]

Смартлоки мають чотири основні функції:

— автоматичне відкриття при наближенні власника;

— можливість відкривати і закривати замок зі смартфона в межах Bluetooth-мережі;

— можливість видавати і відкликати віртуальні ключі для інших користувачів за допомогою смартфона;

— віддалені управління зі смартфона через Wi-Fi-мережу.

До додаткових функцій можна віднести:

— повідомлення про відкриття і закриття замку;

— зберігання даних про відкриття замку;

— повідомлення про спробу злому.

Розумний замок можна вбудувати в домашню систему автоматизації, що дозволить йому взаємодіяти з іншими інтелектуальними пристроями в будинку. Так само, є можливість через смартфона керувати розумним замком за допомогою голосу.

Процес монтажу розумного замку можна розбити на дві частини.

Установка запірного механізму. Єдина відмінність від установки звичайного замка полягає в прокладці проводів управління. Спосіб прокладки проводів залежить від типу замка - виразний або накладної. Для врізного замка дроти прокладаються всередині двері, в той час як дроти накладного знаходяться зовні і закриваються накладками. На цьому ж етапі встановлюється блок живлення, коли рівень заряду батареї замок повідомляє про це подаючи сигнал на зовнішній датчик. Так само необхідно вивести пучок проводів для підключення приймача сигналу, розташованого із зовнішнього боку дверей.

Блок управління. Монтується в безпосередній близькості від дверей. З замком з'єднується кабелем за допомогою спеціального роз'єму. До блоку управління підключається основне живлення від мережі і додаткова батарея, для роботи при припиненні подачі електроенергії.

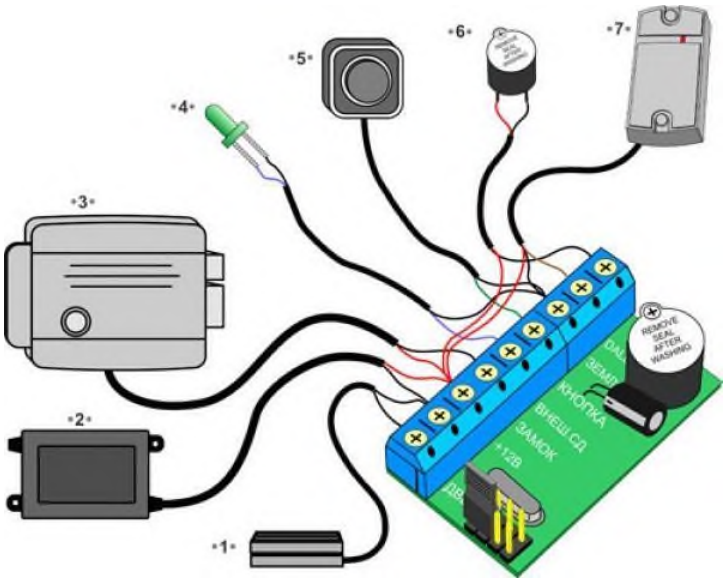

Рисунок 2.2– Підключення розумного замка

Біометричний замок — електронний замок, відкриття якого відбувається через біометричну автентифікацію (біометричні параметри людини).

Є досить багато біометричних параметрів використовуваних для автентифікації, найпоширеніші з них:

— райдужна оболонка ока;

— малюнок вен на передній частині очі;

— сітківка ока;

— відбитки пальців;

— голос.

Більшість біометричних замків працює на розпізнаванні відбитків пальців. Біометричний замок аналізує складні структури, на яких до того ж можуть бути присутніми перешкоди (наприклад дрібні подряпини на пальцях) і порівнює їх з тими, що вже внесені в базу.

У рідкісних випадках біометричний замок може не прийняти коректний ключ через перешкоди або прийняти некоректний.

Існують спеціальні параметри дають оцінку якості аналізу в біометричний замку: FRR (False Rejection Rate) показує ймовірність того, що вірний ключ не буде прийнятий як коректний і замок перед власником не відкриється.

FAR (False Acceptance Rate) показує, наскільки вели ймовірність відкриття замку при пред'явленні чужого ключа.

Імовірність помилки становить частки відсотка. Як правило FRR вище FAR, тобто біометричний замок скоріше не відкриється перед власником, ніж впустить стороннього. Це робить біометричний замок досить надійним.

Молекулярний замок - блокує система, призначена для вироблення сигналу на відкриття електронного замка. Замок реагує не на електричний сигнал від клавіатури або пристрою, що зчитує, а на датчик реагує на набір хімічних речовин. У молекулярних замках використовуються замки стенографічного типу, тобто про існування замку знає тільки людина має доступ до інформації про нього.

Історія створення молекулярних замків Першу подібну систему в 2007 році представив професор Абрахам Шанцер разом з групою розробників з наукового інституту Вейцман (Ізраїль). Дослідники продемонстрували систему молекулярної блокування, здатної реагувати на кілька паролів. Дана розробка дозволяє молекулярним замкам і молекулярним клавіатур конкурувати з електронними замками і датчиками створюючи системи підвищеної безпеки.

В технології молекулярних замків використовуються не електричні, а хімічні та оптичні сигнали. Перевага цієї технології полягає не тільки в приховуванні пароля, секретом є сам факт наявності замка. Принцип дії замків з молекулярної клавіатурою полягає в комбінованому флуоресцентного молекулярного датчика, який реагує на різні хімічні речовини. На відміну від більшості люмінесцентних молекулярних сенсорів, які генерують оптичні сигнали, цей датчик генерує унікальні «підпису» хімічних елементів, діючи як нюхова система.

У разі електронного замка розблокування відбувається через введення правильного пароля. Розблокування біометричного замку відбувається за допомогою унікального набору біометричних характеристик людини (унікальної «підпису»). Для відкриття молекулярного замку необхідні і пароль, і оптичні відбитки, що робить такий тип замка найбільш надійним.

Для створення молекулярного замку розробники використовували цукориди (фруктоза, глюкозу, галактозу). Послідовність цих речовин - аналог електронних паролів. Молекулярні системи блокування реагують на паролі з двох, трьох або чотирьох елементів. Ці системи генерують унікальний оптичний спектр кожного набору елементів і може бути запрограмована для декількох користувачів. В цьому випадку для кожного користувача встановлюється свій флуоресцентний відбиток, який розпізнається і обробляється спеціальною програмою.

Електронні кодові замки мають одну суттєву перевагу перед механічними. Блок управління може перебувати в видаленні від основного пристрою. Його можна встановити в будь-якому місці — це основа принципу замку. Коли немає можливості бачити те, з чим доведеться мати справу, стає проблематично зламати такий пристрій. Крім того, сучасний кодовий замок — це високотехнологічний пристрій, що керується за допомогою мікропроцесора, а це мільйони різних комбінацій.

Кнопкові кодові замки з електронним управлінням. Вони набули найбільшого поширення, але в той же час це вразлива група замикаючих пристроїв. Причина, як і в разі механічних замків, та ж - стираються і западають кнопки. В основному їх встановлюють там, де не потрібно зберігати особливо цінні предмети. Їх використовують для запобігання проникнення в приміщення, наприклад в під'їзди, складські та підсобні приміщення в невеликих підприємствах або магазинах. У більшості випадків пульт управління і сам замок виготовляються одним блоком, але є моделі з роздільним оснащенням. З розвитком технологій кнопкові кодові замки отримали своє логічне продовження у вигляді замків з сенсорною панеллю. Переваги перед кнопками тут очевидні, але є серйозна проблема з тим, що на мазких сенсорних екранах при натисканні залишаються відбитки пальців, які стають помітні під певним кутом огляду. Для уникнення злому комбінації за відбитками, потрібні різні хитрощі, на які йдуть виробники замків з сенсорною панеллю. Одним із способів приховування

комбінації є введення додаткових непотрібних символів спочатку або в кінці основного коду.

Кодові замки з магнітним носієм комбінації. Це дуже надійні замки, розкрити які можна, якщо дістати сам магнітний носій. У цій ролі можуть виступати: пластикова картка, невеликий брелок, пульт дистанційного керування, що передає код приймача радіосигналом або сигналом в інфрачервоному спектрі, легко перехоплюють і декодуючи.

Комбіновані замки. Даний вид замків найбільш поширений на сьогоднішній день. Потрапити всередину приміщення можна тільки при використанні послідовно декількох різних відкривають пристроїв, наприклад, кодової комбінації і пластикової карти, що робить комбіновані замки дуже надійною системою. Їх особливістю є те, що розблокувати двері неможливість тільки за допомогою одного ключа, потрібно пройти всі послідовні дії, необхідні для відкриття, а також те, що ключі від інших виробників будуть ігноруватися при спробі їх використання.

Рисунок 2.3 — Електронний кодовий замок з сенсорною панеллю введення виробництва компанії Samsung

В мережі Інтернет також можна знайти різні схемотехнічні рішення для реалізації електронних кодових замків, наприклад, як на рисунку 2.4. Дана схема являє собою пристрій, що складається з: двох КМОП мікросхем 561ЛА7 і однієї 561ЛЕ5, транзистори VT1-VT3 - КТ361, або КТ3107, транзистор VT4 -КТ315, транзистор VT5 - КТ815. Вторинна обмотка трансформатора Т1 розрахована на 12 вольт. Трансформатор Т1 вибирається достатньої потужності, що забезпечує спрацьовування виконавчого пристрою, діоди VD3-VD7 вибираються випрямні FR107, що забезпечують достатній струм навантаження виконавчого пристрою. Діоди VD8-VD20 - малопотужні імпульсні КД521. Як акумуляторної батареї використовується малогабаритна лужна батарея, яка використовується в джерелах безперебійного живлення. Набір коду здійснюється за допомогою кнопкової панелі SA1.[2]

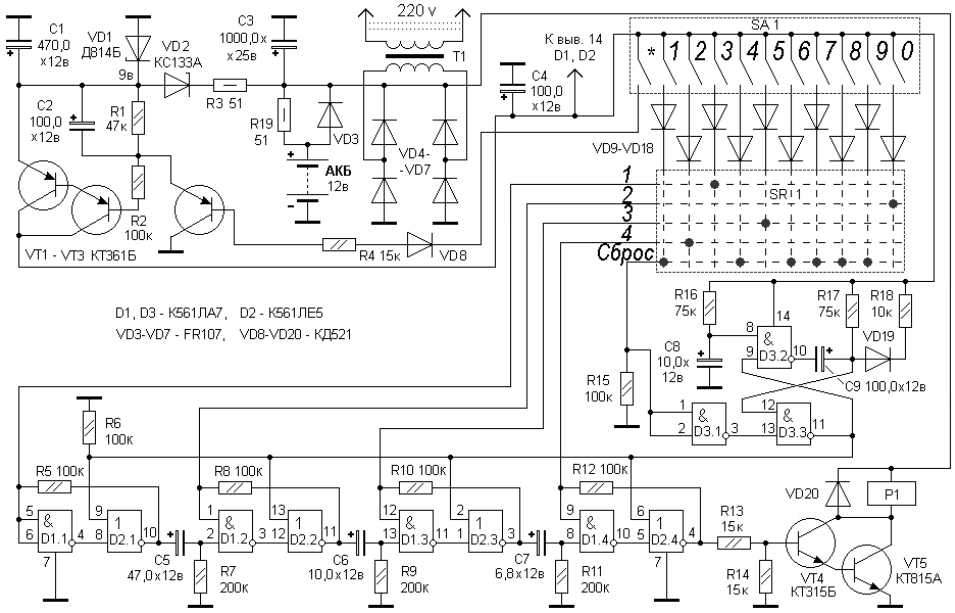

Рисунок 2.4 — Схема електрична принципова електронного кодового замка

Заявленими перевагами даної схеми в порівнянні з іншими схемо технічними рішеннями, доступними в мережі Інтернет є: висока захищеність від злому обманними кнопками, при натисканні на які замок блокується на деякий час, кнопкова панель розташовується окремо від основного пристрою, завдяки

чому злом за допомогою вимірювальної апаратури стає неможливий, живлення від акумулятора на 12 вольт, або від мережі змінного струму 220 вольт.
Незважаючи на це, представлена вище схема кодового замка має свої недоліки як електронний замок: чутливість до електромагнітних завад, важких погодних умов, вимога до безперебійної подачі живлення. Але головним фактором є те, що для створення подібних схемотехніки потрібні глибокі пізнання в схемотехніці і в мікросхемній логіці, потрібен точний підбір елементів для правильної роботи, тому через усього перерахованого вище досить важко розглядати цей тип замка в якості навчального ознайомлення. Тому в якості основи для цієї роботи був обраний електронний замок на мікропроцесорному управлінні.

Для того щоб реалізувати пристрій контролю доступу на мікропроцесорному управлінні, в якості вихідних даних були обрані способи управління за допомогою кодової комбінації, яка реалізується за допомогою кнопок, а також радіочастотна ідентифікація, що реалізується за допомогою спеціально розроблених для роботи з мікроконтролерами модулями радіочастотної ідентифікації. Розглянемо більш докладно основні принципи організації радіочастотної ідентифікації в наступному розділі.

2.2 Огляд мікропроцесорних платформ

Для забезпечення роботи системи необхідно вибрати апаратну базу для її реалізації. Для цього розглянемо основні способи і технології, їх переваги, недоліки.

Мікроконтролер — це спеціальна мікросхема, призначена для управління різними електронними пристроями. Це вже не процесор, але ще й не комп'ютер. У сучасній термінології це система на чіпі (SoC). Мікроконтролер містить один або кілька процесорних ядер, а також пам'ять і програмовані периферійні пристрої введення / виводу. Програмна пам'ять у вигляді ОЗУ, флеш-пам'яті NOR або OTP ROM також часто включається в чіп, а також невеликий обсяг оперативної пам'яті. Мікроконтролери призначені для вбудованих систем, на

відміну від мікропроцесорів, які використовуються в персональних комп'ютерах або інших додатках загального призначення, що складаються з різних дискретних чіпів. Мікроконтролери використовуються в автоматизованих пристроях, таких як автомобільні системи управління двигунами, що імплантуються медичні пристрої, пульти дистанційного керування, офісні машини, електроприлади, електроінструменти, іграшки та інші вбудовані системи. За рахунок зменшення розміру і вартості в порівнянні з конструкцією, яка використовує окремі пристрої, як мікропроцесор, пам'ять і пристрої введення, мікроконтролери дозволяють більш економно управляти ще більшою кількістю пристроїв і процесів. Таким чином, мікроконтролери забезпечують низьке енергоспоживання, достатню надійність системи, а також дуже гнучку логіку завдяки їх програмування. На рисунку 2.5 представлений один з популярних мікроконтролерів.[3]

Хоча мікроконтролери і володіють в більшості випадків низькою вартістю, але це гідність можна перекреслити складністю розробки і створення прототипу для непромислових та приватних проектів, а також відсутністю універсальності в деяких випадках.

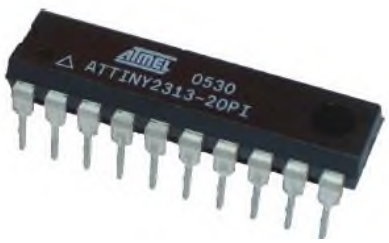

Рисунок 2.5 — Мікроконтролер ATtiny2313 американської фірми Atmel

Але поява таких рішень, як, наприклад, Arduino і одноплатні комп'ютери, вивело домашню та непромислові автоматизацію на новий рівень. Істотно знизилася вартість даних систем, без шкоди надійності. Через масове впровадження в повсякденне життя, так само знизилася і вартість датчиків (сенсорів) для них.

Arduino - це платформа з відкритим вихідним кодом, яка використовується для створення проектів електроніки. Arduino складається з фізичної програмованої монтажної плати (часто званої мікро контролером) і програмного забезпечення, або IDE (Integrated Development Environment), яка працює на вашому комп'ютері, використовується для запису і завантаження комп'ютерного коду на фізичну плату. Платформа Arduino стала досить популярною серед людей, які тільки починають працювати з електронікою, і не без підстави. На відміну від більшості попередніх програмованих друкованих плат, Arduino не потребує окремому апаратному забезпеченні для завантаження нового коду на плату - ви можете просто використовувати USB-кабель. На рисунку 2.6 представлена одна з моделей Arduino.

Рисунок 2.6 — Arduino Uno — одна з найбільш популярних плат Arduino

Крім того, в середовищі IDE Arduino використовується спрощена версія C, що спрощує навчання розробки під цю плату.

Апаратне та програмне забезпечення Arduino було розроблено для художників, дизайнерів, любителів, хакерів, новачків та всіх, хто зацікавлений в створенні інтерактивних об'єктів або середовищ. Arduino може взаємодіяти з кнопками, світлодіодами, моторами, гучномовцями, пристроями GPS, камерами, Інтернетом і навіть вашим смартфоном або телевізором. Ця гнучкість в поєднанні з тим, що програмне забезпечення Arduino безкоштовне, апаратні

плати досить дешеві, а програмне і апаратне забезпечення легко освоїти, призвело до великої кількості користувачів, які написали код і випустили інструкції для величезного розмаїття проектів на базі Arduino.[4]

Існує безліч різновидів плат Arduino, які можуть використовуватися для різних цілей. Деякі плати трохи відрізняються від наведених нижче, але більшість мають наступні компоненти (рисунок 2.7):

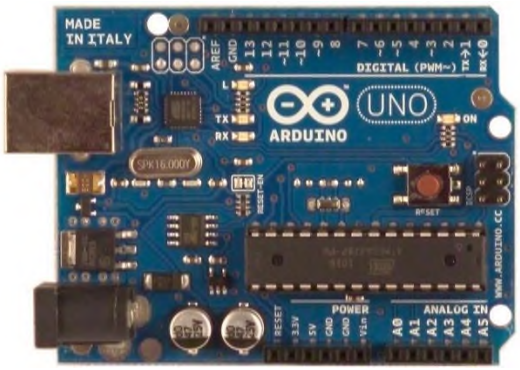

Рисунок 2.7 — Компоненти плати Arduino

За допомогою деякого простого коду Arduino може управляти і взаємодіяти з широким спектром датчиків (рисунок 2.7) - вимір яскравості світла, температури, ступеня вигину, тиску, близькості, прискорення, чадного газу, радіоактивності, вологості, атмосферного тиску.

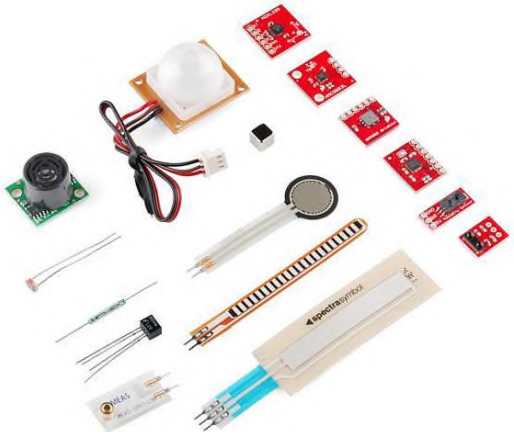

Рисунок 2.7 — Деякі датчики, які легко взаємодіють з Arduino

Плати розширення (shields). Крім того, є такі плати (рисунок 2.8), які називаються shields в основному це заздалегідь підготовлені монтажні плати, які поміщаються поверх Arduino і надають додаткові можливості управління двигунами, підключення до Інтернету, надання стільникового або іншого бездротового зв'язку, управління екраном і багато іншого.

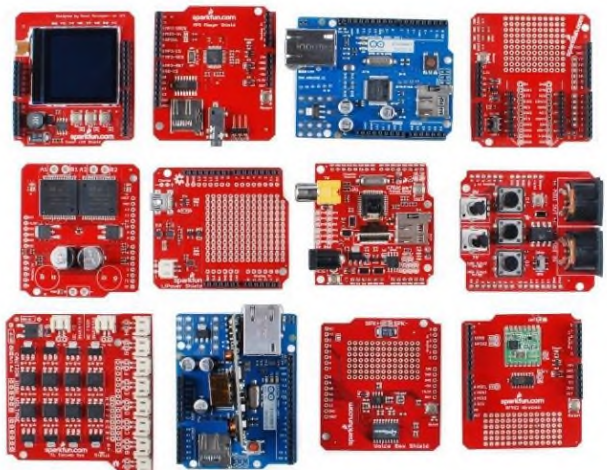

Рисунок 2.8 — Плат розширення можливостей Arduino

Таким чином, можна виділити переваги використання Arduino.

Готовність до використання: готова до використання структура робить її дуже простий у використанні. Вам не потрібно турбуватися про программаторе, настройках запобіжників, програмних засобах серійного монітора.

Приклади коду: багато стандартних бібліотек, які полегшують і прискорюють розробку. Також варто відзначити, що це є open-source продукт.

Легкі функції: в програмному забезпеченні Arduino є багато функцій, які роблять кодування настільки простим і швидким, що це неможливо при використанні простого мікроконтролера.

Велике співтовариство: є багато форумів в Інтернеті, на яких люди говорять про Arduino. Інженери, любителі і професіонали роблять свої проекти через Arduino. Ви можете легко знайти допомогу у всьому. Крім того, сам сайт Arduino пояснює всі функції Arduino.

Структура Arduino є її недоліком. Зазвичай під час створення проекту ви повинні постаратися зробити його розмір якомога меншим. Але з великими структурами Arduino ми повинні дотримуватися великих розмірів друкованих плат. Якщо ви працюєте на невеликому микроконтроллере, такому як ATmega8, ви можете легко зробити свою PCB настільки маленькою, наскільки це можливо. Найважливіший фактор, який не можна заперечувати - це вартість. Це проблема, з якою стикається кожен любитель, інженер або професіонал. Іноді для деяких рішень вигідніше організувати рішення на мікроконтролері.

Класифікація та огляд міні-комп’ютерів. Відповідно до проведених досліджень кількість міні-комп’ютерів, представлених на ринку, зростає. З'являється нові моделі різної вартості, форм-фактора, продуктивності і вартості. Міні-комп’ютерів - комп'ютер, зібраний на одній друкованій платі, на якій встановлені мікропроцесор, оперативна пам'ять, системи введення-виведення і інші модулі, необхідні для функціонування комп'ютера. Міні-комп'ютери виготовляються в якості демонстраційних систем, систем для розробників або освіти, або для використання в ролі промислових або вбудованих комп'ютерів. На відміну від традиційних персональних комп'ютерів форм-фактора «desktop», міні-комп'ютери часто не вимагають установки якихось додаткових периферійних плат. Така економія з одного боку робить все пристрій більш компактним і набагато дешевшим за рахунок використання системи на кристалі, з іншого боку, розширення можливостей зміни процесора або пам'яті є ускладненим, так як найчастіше ці компоненти напаяні на плату.

Одним з перших доступних міні-комп'ютерів став Raspberry Pi, який на даний момент є найпопулярнішим (продано понад 5 мільйонів пристроїв). Потім стали з'являється його клони і аналоги. На сьогоднішній день існує велика кількість моделей міні-комп'ютерів різного розміру, функціональності, продуктивності і вартості. Деякі з них є клонами Raspberry Pi, а деякі має зовсім інше призначення і архітектуру.

ODROID-C2 виробляється південнокорейською компанією Hardkernel. Оснащений чотирма портами USB 2.0, HDMI-мікро, USB-OTG портом, IR

приймачем, eMMC-слотом. Процесор - 64-бітний SoC Amlogic S905 (чотири ядра ARM Cortex-A53) тактова частота - 2 ГГц. ОЗУ - 2 Гб SDRAM третього покоління. Графічний прискорювач - GPU ARM Mali 450 MP3 з частотою 750 МГц. Підтримувані ОС - Ubuntu 16.04 і Android 5.1. Зовнішній вигляд представлений на рисунку 2.9.

Рисунок 2.9 – ODROID-C2

Пристрій підтримує завантаження ОС або з модуля eMMC, або з карти microSD: вибір проводиться спеціальним джампером.

Ціна від 19 $ (1 Гб ОЗУ) до 30 $ (2 Гб ОЗУ), що трохи дорожче Raspberry Pi, але при цьому пристрій надає більш високу продуктивність. Для ODROID-C2 на даний момент набагато менше ПО і готових рішень, ніж на Raspberry Pi.

BeagleBone Black комп'ютер розроблений Texas Instruments і Digi-Key. Процесор Sitara AM335X на базі двох ядер ARM Cortex-A8 з тактовою частотою 1 ГГц. Графічний процесор - SGX530. ОЗУ - 512 Мб на частоті 800 МГц. Так само на материнській платі впаяна флеш-пам'ять eMMC на 2 Гб і два порти USB 2.0. Є мікро HDMI. Пристрій працює під управлінням ОС Angström Linux, але також підтримуються Ubuntu і Android. Вартість комп'ютера - 45 $. Зовнішній вигляд представлений на рисунку 2.10.

Рисунок 2.10 — BeagleBone Black

Головною перевагою є підтримка процесором AM3359 апаратного прискорення шифрування і наявності двох PRU (Programmable Realtime Unit) модулів: грубо кажучи, це ще один процесор на загальному кристалі, куди зібраний написаний на мові Сі пакет протоколів для підлеглого пристрою.

BeagleBone Black має більш широку підтримку виробника, ніж ODROID-C2. Наявність апаратного прискорення шифрування і двох PRU дає додаткові можливості.

Недоліком комп'ютера є попередньо встановлена ОС Angström Linux, яка нестабільна і має вади вбудованого ПО. Ця проблема вирішується установкою альтернативної ОС — Ubuntu або Android.

На відміну від настільного персонального комп'ютера, одноплатні комп'ютерами часто не мають слоти розширення для периферійних функцій або пристроїв. Одноплатні комп'ютери побудовані з використанням широкого спектра мікропроцесорів. Прості конструкції, наприклад, створені комп'ютерними любителями, часто використовують статичне ОЗУ і недорогі 8- або 16-розрядні процесори.

Інші типи, такі як блейд-сервери, працюють аналогічно серверного комп'ютера тільки в більш компактному форматі. В даний час на ринку досить багато популярних моделей від різних фірм. Одні з найпопулярніших (різні моделі і варіації):

Raspberry Pi, BeagleBone, Orange Pi, Banana Pi, Asus Tinker Board. Всі вони відрізняються ціною, технічними характеристиками, дизайном і т.д.

Raspberry Pi — це крихітний комп'ютер розміром з кредитну карту, плата має процесор, ОЗУ і типові апаратні порти, які ви знайдете на більшості комп'ютерів. Головна оперативна система для Pi- Raspbian, яка заснована на Debian. Хоча основний підтримуваної операційною системою є Raspbian, ви можете встановити інші операційні системи, такі як Ubuntu mare, Ubuntu Core, OSMC, RIS OS, Windows 10 IoT і багато іншого. До теперішнього часу існують кілька версій цього комп'ютера, які відрізняються розмірами, ціною і технічними характеристиками.

Плюси Arduino:

— архітектура з низьким енергоспоживанням;

— легко почати роботу з відмінною онлайн-підтримкою, швидке, просте створення прототипів;

— просте сполучення з датчиками і збір даних;

— дешевше, ніж Raspberry Pi (для продуктів, які не мають можливості підключення до Інтернету);

— можливо відправляти дані без проводів, використовуючи Bluetooth, Rf і т.д. на сервер через комп'ютер;

— безліч GPIO з можливостями PWM і дружнім до розробників;

— можливо використовувати IDE, python, ruby, embedded C і т.д. для програмування;

— повністю відкритий вихідний код.

Мінуси Arduino:

— обмеження пам'яті (вкрай мало в порівнянні з Odroid);

— для підключення до Інтернету потрібні додаткові shields;

— менш потужний у порівнянні з Odroid;

— неможливо запустити багато важких алгоритмів, або програмувати сенсорний екран і використовуючи додаткові плати розширення.

2.3 Вибір компонентів системи

Радіочастотна ідентифікація — це технологія безконтактної ідентифікації об'єктів за допомогою радіочастотного каналу зв'язку (рисунок 2.11). Ідентифікація об'єктів проводиться за унікальним ідентифікатором, який має кожна електронна мітка. Зчитувач випромінює електромагнітні хвилі певної частоти. Мітки відправляють у відповідь інформацію ідентифікаційний номер, дані пам'яті та ін.

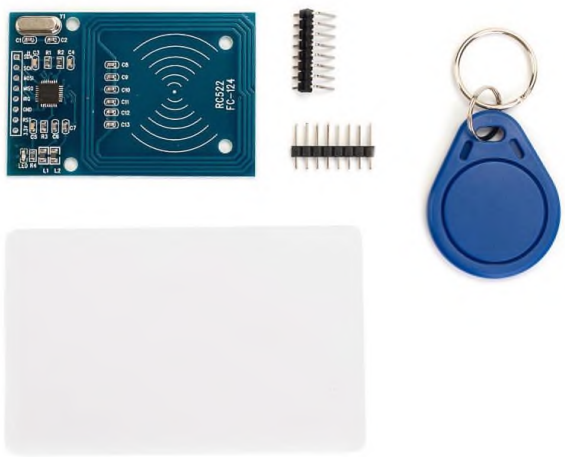

Рисунок 2.11 —. RFID модуль RC522

Переваги технології RFID:

— безконтактна;

— можливість прихованої установки міток;

— висока швидкість зчитування даних;

— можливість установки в шкідливих середовищах;

— неможливість підробки.

Існує велика різноманітність RFID міток. Мітки бувають активні і пасивні (без вбудованого джерела енергії, харчуються від струму, індукованого в антені сигналом від рідера). Мітки працюють на різній частоті: LF (125 - 134 кГц), HF (13.56 МГц), UHF (860 - 960 МГц). Прилади, які читають інформацію з міток і

записують в них дані, називаються рідерами (зчитувачами). У проектах Arduino як зчитувача дуже часто використовують модуль RFID-RC522. Модуль виконаний на мікросхемі MFRC522 фірми NXP, яка забезпечує роботу з мітками HF (на частоті 13,56 МГц). У комплекті з модулем RFID-RC522 йдуть дві мітки, одна у вигляді карти, інша у вигляді брелока.

Технічні характеристики RFID-модуля RC522

— напруга живлення: 3.3V;

— струм: 13-26mA;

— робоча частота: 13.56MHz;

— діяльність зчитування: 0 - 60 мм;

— інтерфейс: SPI;

— швидкість передачі: максимальна 10Мбіт / с;

— розмір: 40мм х 60мм;

Мікросхема MFRC522 підтримує інтерфейси SPI, UART і I2C. Вибір інтерфейсу здійснюється установкою логічних рівнів на певних виходах мікросхеми. На даному модулі який зображено на рисунку 2.12 обраний інтерфейс SPI.

Рисунок 2.12 — RFID модуль RC522

Призначення виходів інтерфейсу SPI:

— SDA - вибір веденого;

— SCK -сигнал синхронізації;

— MOSI - передача від master до slave;

— MISO - передача від slave до master;

— RST - висновок для скидання;

— IRQ - висновок переривання;

— GND - земля;

— Vcc -харчування 3.3 В.

LCD дисплей — частий гість в проектах Arduino. Але в складних схемах у нас може виникнути проблема нестачі портів Arduino через необхідність підключити екран, у якого дуже дуже багато контактів. Виходом у цій ситуації може стати I2C перехідник, який підключає практично стандартний для Arduino екран 1602 до платам Uno, Nano або Mega всього лише за допомогою 4 пінів.

Рідкокристалічний дисплей LCD 1602 який зображено на рисунку 2.13 є хорошим вибором для виведення рядків символів в різних проектах. Він коштує недорого, є різні модифікації з різними кольорами підсвічування, ви можете легко завантажити готові бібліотеки для скетчів Arduino. Але найголовнішим недоліком цього екрану є той факт, що дисплей має 16 цифрових висновків, з яких обов'язковими є мінімум 6. Тому використання цього LCD екрана без i2c додає серйозні обмеження для плат Arduino Uno або Nano. Якщо контактів не вистачає, то вам доведеться купувати плату Arduino Mega або ж заощадити контакти, в тому числі за рахунок підключення дисплея через i2c інтерфейс.[5]

Рисунок 2.13 — Рідкокристалічний дисплей LCD 1602

Технічні характеристики дисплея:

— символьний тип відображення, є можливість завантаження символів;

— світлодіодна підсвітка;

— контролер HD44780;

— напруга живлення 5В;

— формат 16х2 символів;

— діапазон робочих температур від -20С до + 70С, діапазон температур зберігання від-30С до +80 С;

— кут огляду 180 градусів.

Найшвидший і зручний спосіб використання i2c дисплея в Arduino — це покупка готового екрану з вбудованою підтримкою протоколу. Але таких екранів не дуже багато і коштують вони не дешево. А ось різноманітних стандартних екранів випущено вже величезна кількість. Тому найдоступнішим і популярним сьогодні варіантом є покупка і використання окремого I2C модуля перехідника.

З одного боку модуля виходи i2c — земля, живлення для передачі даних. З іншого боку перехідника бачимо роз'єми зовнішнього живлення. На платі є безліч ніжок, за допомогою яких модуль припаюється до стандартних виходів екрану.

У багатьох додатках потрібно введення даних з клавіатури. Це може бути реалізовано за допомогою окремих кнопок, але це не дуже зручно з точки зору використання ліній введення / виводу МК. Кращим рішенням є використання матричної клавіатури. Матрична клавіатура для Arduino використовується для завантаження даних в мікроконтролер. Вона складається з 16 кнопок, розташованих у вигляді масиву по чотири ряди і чотири стовпці.

Принцип роботи матричної клавіатури для Arduino. Чотири контакти мікроконтролера повинні бути визначені як виходи, а інші чотири pin - в якості вхідних даних. для читання стану певного ключа на стовпець подається сигнал, а потім зчитується стан рядів. Зазвичай ряди підключаються до високого потенціалу, а опитуваний стовпець сполучається з землею. Якщо при скануванні зчитується низький рівень сигналу, то це означає, що ключ у цій позиції ряд-стовпець замкнутий. Таким чином визначається, яка кнопка натиснута.

Ще один спосіб отримати дані з допомогою клавіатури 4x4 в мікроконтролер полягає в використанні готових функцій зі спеціальної бібліотеки для клавіатури. Матрична клавіатура зображена на рисунку 2.14

Рисунок 2.14 —Матрична клавіатура для Arduino

Характеристики:

— тип – модуль;

— призначення - для Arduino;

— особливості - 4 х 4, 16-клавішна клавіатура;

— додаток - DIY MCU клавіатури;

— розміри - 4.3x3.9x1.0 см;

— вага - 11г.

Модуль триколірного RGB світлодіоди може використовуватися в проектах на мікроконтролерах для світлової індикації будь-якого процесу, наприклад: подачі живлення, аварії, замикання реле, передача даних, прийом даних і т.п.

Для використання модуля триколірного RGB світлодіоди потрібно підключити до нього харчування і керуючий сигнал від контролера або іншого керуючого мікропроцесорного пристрою.

Вбудований в модуль світлодіод може світитися синім, зеленим, червоним кольорами, також кольору світіння можна включати попарно або все одночасно. Модуль може управлятися від контролера або іншого керуючого мікропроцесорного пристрою. Модуль має загальний контакт негативної полярності. За допомогою керуючого сигналу позитивної полярності значенням +3,3 - +5 В відбувається управління квітами світіння.

Модуль триколірного RGB світлодіоди має один 4-х контактний роз'єм для підключення живлення і керуючого сигналу зображено на рисунку 2.5:

— контакт, позначений «-», загальний контакт;

— контакт, позначений B (Blue), використовується для включення синього кольору світіння;

— контакт, позначений G (Green), використовується для включення зеленого кольору світіння;

— контакт, позначений R (Red), використовується для включення червоного кольору світіння.

Живлення модуля здійснюється або від керуючого пристрою, або від зовнішніх джерел живлення (блоків живлення, батарей). Напруга живлення модуля 3,3 - 5 В постійного струму.

Рисунок 2.15 — RGB світлодіод

Характеристики:

— модель: KY-016;

— тип світлодіода: RGB;

— діаметр світлодіода: 5 мм;

— керуючий сигнал: позитивної полярності значенням +3,3 - +5 В;

— кольору світіння: синій, зелений, червоний, попарно, все одночасно;

— напруга живлення: 3,3 - 5 В;

— розміри: 20 х 15 х 15 мм;

— вага: 1 м

Одноканальний модуль реле JQC-3FF-S-Z (рисунок 2.6). Даний модуль призначений для управління потужним струмом, як постійним, так і змінним. Крім самого реле, модуль містить ще й оптоелектронну розв'язку з транзистором, які захищають висновки Ардуіно від стрибків напруги на котушці. Реле спрацьовує при подачі на вхід низького рівня сигналу

Рисунок 2.16 — Одноканальний модуль реле JQC-3FF-S-Z

Опис виходів модуля:

— VCC - підключається до 5V для живлення модуля (+);

— GND - підключається до «землі» (-);

— IN - підключається, наприклад, до плати Arduino або микроконтроллеру для управління замикання і розмикання виходів реле;

— COM - для підключення контакту керованої ланцюга;

— NO - нормально розімкнутий вихід (Normally Open), замкнеться з виходом COM при подачі високого рівня на вхід IN;

— NC - нормально замкнутий вихід (Normally Closed), розімкнеться з виходом COM при подачі високого рівня на вхід IN.

2.4 Інтерфейси підключення пристроїв

Arduino Uno підтримує такі інтерфейси як SPI, UART, I2C.

SPI (Serial Peripheral Interface) — послідовний синхронний стандарт передачі даних в режимі повного дуплексу, призначений для забезпечення простого і недорогого високошвидкісного сполучення мікроконтроллерів і периферії. SPI також іноді називають чьотирьох інтерфомсом. На відміну від стандартного послідовного порту, SPI є синхронним інтерфейсом, в якому будь-яка передача синхронізована із загальним тактовим сигналом, що генерується

провідним пристроєм (процесором). Приймаючав (ведена) периферія синхронізує отримання бітової послідовності з тактовим сигналом. До одного послідовного периферійного інтерфейсу ведучого пристрою-мікросхеми може приєднуватися кілька мікросхем .

Даний інтерфейс є одним з популярних внутріплатних послідовних синхронних інтерфейсів. Розроблений фірмою Motorola. Використовується для простої і високошвидкісної передачі даних між пристроями. SPI інтерфейс відноситься до часто-використовуваних інтерфейсів для створення зв'язку між мікросхемами. Також, SPI іноді називають чотирьох інтерфейсним, оскільки в ньому використовується чотири лінії: MOSI, MISO, SCK, SS. Лінія MOSI: вихідна лінія даних провідного інтерфейсу і вхідні лінія даних веденого інтерфейсу. Лінія призначена для передачі даних від провідного пристрою до веденого. Лінія MISO: вхідні лінія даних провідного інтерфейсу і вихідна лінія даних веденого інтерфейсу. Лінія призначена для передачі даних від відомого пристрою до ведучого. Дані передаються байтами починаючи зі старшого біта. Лінія SS: лінія вибору відомого пристрою, з яким ведучий пристрій має намір працювати. Лінія SCK: вихідна лінія тактових імпульсів ведучого вузла і вхідні лінія тактових імпульсів веденого вузла. Лінія SCK використовується для синхронізації передачі даних між ведучим і веденим інтерфейсами по лініях MOSI і MISO. Алгоритм дії заснований на принципі «Ведучий-підлеглий». Провідним найчастіше є мікроконтролер, або мікропроцесор.

Підлеглими є мікросхеми, годинник реального часу, аналого-цифрові перетворювачі, цифро-аналогові перетворювачі, різне цифрове обладнання. Головною частиною інтерфейсу SPI є зсувний регістр, сигнали синхронізації і введення / виводу бітового потоку якого і утворюють інтерфейсні сигнали. Тому, SPI протокол скоріше є протоколом обміну даними між двома зсувними регістрами, кожен з яких одночасно виконує функцію приймача і передавача, а не протоколом передачі даних. Основною умовою передачі даних по лінії SPI є генерація сигналу синхронізації шини. Цей сигнал має право генерувати тільки

ведучий шини і від цього сигналу повністю залежить робота підлеглого шини. Підключення SPI інтерфейсу зображено на рисунку 2.17.[6]

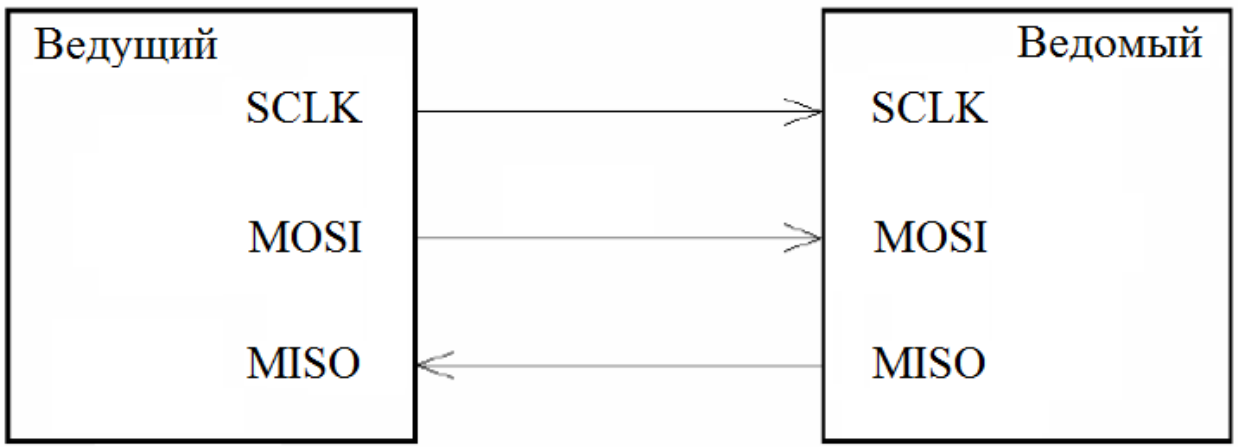

Рисунок 2.17 – Схема підключення SPI інтерфейсу

При трьохпровідному підключенні «Ведучий» визначено заздалегідь. Принцип дії: Ведучий шини передає дані по лінії MOSI синхронно зі згенерованих їм же сигналом SCLK, а підлеглий захоплює передані біти даних за певними напрямами прийнятого сигналу синхронізації. Одночасно з цим підлеглий відправляє свою посилку даних.

Переваги SPI інтерфейсу:

— простота протоколу передачі;

— висока надійність;

— висока швидкодія;

— невелика кількість проводів щодо паралельних інтерфейсів.

Недоліки SPI інтерфейсу:

— кількість проводів щодо розглянутих вище інтерфейсів більше;

— не підтверджує прийому даних з боку відомого пристрою;

— дальність передачі щодо UART набагато нижче.

Спираючись на практичний досвід роботи з SPI інтерфейсом можна уникнути деяких недоліків даного типу зв'язку, що покращує його

характеристики на тлі інших інтерфейсів. Розглянуті вище внутріплатні інтерфейси мають як свої переваги, так і недоліки. Провівши даний аналіз можна зробити висновок, що SPI інтерфейс є більш перспективним інтерфейсом, тому об'єкт дослідження випускної кваліфікаційної роботи буде розроблений з SPI інтерфейсом.

UART (Universal Asynchronous Receiver-Transmitter) — універсальний асинхронний приймач - вузол обчислювальних пристроїв, призначений для організації зв'язку з іншими цифровими пристроями. Передає дані в послідовний вид так, щоб було можливо передати їх по одній фізичній цифровий лінії іншому аналогічному влаштуванню. Метод перетворення добре стандартизований і широко застосовується в комп'ютерній техніці (особливо у вбудованих пристроях і системах) .

UART являє собою сукупність обчислювальних пристроїв, призначених для зв'язку з іншими цифровими пристроями. Асинхронна передача використовується в системах, де обмін даними відбувається час від часу, і не потрібна висока швидкість передачі даних.

Принцип роботи:

За структурою інтерфейс являє собою звичайний асинхронний послідовний протокол, тобто сторона, яка передає по черзі видає в лінію 0 і 1, а приймаюча відстежує їх і заносить в пам'ять. Синхронізація йде по часу. Приймач і передавач заздалегідь встановлюють частоту, при якій буде відбуватися обмін даними.

Підключення UART здійснюється за трьома лініями: RXD — прийом, TXD — передача і GND — загальна лінія «земля». При асинхронної передачі кожен символ передається окремою посилкою. Стартові біти попереджають про початок передачі. Потім передається символ. Для визначення достовірності передачі використовується біт парності (біт парності дорівнює 1, якщо кількість одиниць непарній, і дорівнює 0 в іншому випадку). Останній біт сигналізує про початок передачі. Підключення UART наведено на рисунку 2.18 .

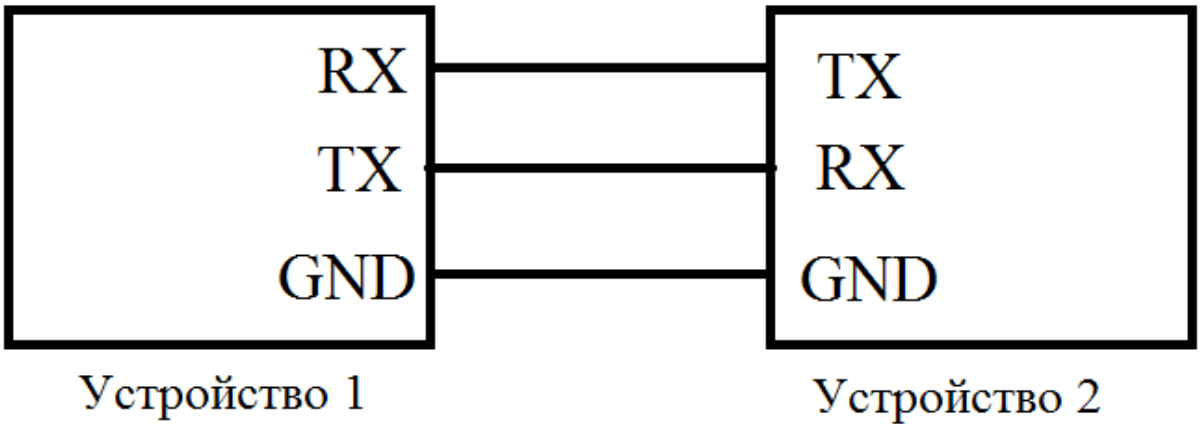

Рисунок 2.18 – Схема підключення UART

При обміні даними по каналах зв'язку використовуються три методи передачі даних:

— односпрямована: TV, радіо;

— напівдуплексна передача: по черзі прийом і передача даних;

— двонаправлена: одночасний прийом і передача кожної станції.

Переваги UART:

- відпрацьована і проста система;
- низька вартість інтерфейсного обладнання

Недоліки UART:

— одна третина пропускної здатності йде на передачу службових бітів;

— швидкість передачі даних щодо синхронної нижче;

— відсутність достовірності показань при численній помилку з використанням біта парності.

Інтерфейс I2C використовує для передачі даних двонаправлених лінії зв'язку (рисунок 2.19).

Даний інтерфейс собою послідовну шину даних для зв'язку інтегральних схем, що використовує дві двонаправлені лінії зв'язку (Serial Data і Serial Clock). Застосовують для зв'язку периферійних низькошвидкісних компонентів з

материнською платою, а також вбудованими системами і мобільними телефонами.[7]

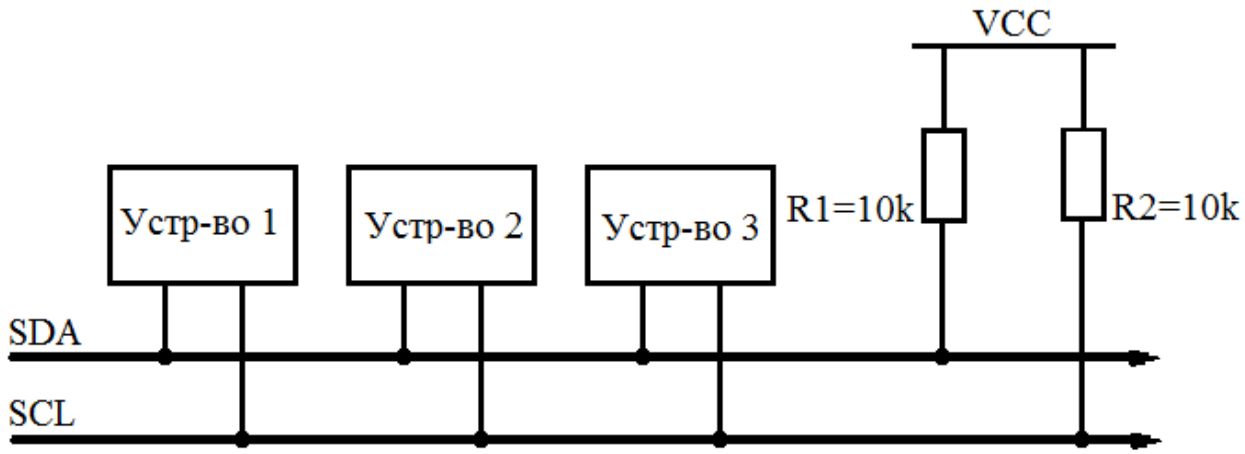

Рисунок 2.19 — Інтерфейс I2C

Переваги I2C:

— при підключенні більше двох мікросхем, кількість проводів не змінюється;

— можливе підключення декількох провідних мікросхем;

— I2C протокол є стандартизованим, тому є захист від проблем несумісності обладнання.

Недоліки I2C:

— ємність лінії становить 400 пФ;

— виникає важкість визначення несправності, якщо одне з підключених пристроїв помилково встановлює на шині стан низького рівня.

2.5 Методи автентифікації за технологія RFID

RFID — радіочастотна ідентифікація є фундаментальною і недорогою технологією, що здійснює бездротову передачу даних. Раніше ця технологія не так часто використовувалася в індустрії в зв'язку з відсутністю стандартизації у

виробничих компаніях. RFID є технологія є ефективнішою і надійнішою, в порівнянні з іншими. З RFID технологією бездротова автоматична ідентифікація приймає дуже специфічний вид: об'єкт, місце розташування, або індивід маркуються унікальним ідентифікаційний кодом, що містяться в RFID - мітки, яка якимось чином прикріплена або втиснула до об'єкта. Радіочастотна ідентифікація є не окремий продукт, а повноцінну систему. Типова RFID - система включає в себе три базові елементи: RFID мітку (транспондер), зчитувач (трансивер, запитувач) і серверну програму (базу даних), яка запитує підтримку комп'ютерної мережі. Програмне забезпечення використовується для управління, контролю, оперування, обробки, ведення обліку різних користувачів. Цифрова система блокування дверей здійснюється і управляється за допомогою RFID зчитувача, який проводить перевірку і автентифікацію користувача і автоматично відкриває двері. Він також зберігає дані про реєстрацію користувача. Дуже важливо провести автентифікацію користувача до відкриття приміщення, що охороняється і радіочастотна ідентифікація дозволяє зробити це. Система дозволяє користувачеві реєструватися в швидких, безпечних зручних умовах. Система блокування дверей відкриває їх тільки тоді, коли користувач помістить свою мітку на зчитувач, а дані про користувача зрівняються з тими, що зберігаються в базі даних. Радіо частотна ідентифікація контролює відкриття і закриття дверей. Залежно від джерела електричної енергії, мітки RFID класифікуються як активні або пасивні. Активні мітки використовують батарею для живлення і передачі інформації мітки за запитом зчитувач. Однак ці теги дуже дороги і рідко використовуються. З іншого боку, пасивні мітки отримують енергію від зчитувача для харчування їх схеми. Ці мітки дуже рентабельні і, отже, більшість додатків використовують їх. Головними перевагами пасивної технології є низька вартість і невеликі габарити. Пасивна мітка RFID передає інформацію зчитувача, коли вона потрапляє в електромагнітне поле, що генерується зчитувачем. Явище засноване на законі електромагнітної індукції Фарадея. Струм, що протікає через котушку зчитувача, створює магнітне поле, яке з'єднується з котушкою транспондера, тим самим

створюючи струм в котушці транспондера. Потім котушка транспондера змінює цей струм, змінюючи навантаження на свою антену. Ця зміна фактично є модульованим сигналом, який приймається котушкою зчитувача за допомогою взаємної індукції між котушками. Котушка зчитувача декодує цей сигнал і передає його на комп'ютер для подальшої обробки. Додаткове підключення антени дозволяє зменшити розміри пристрою.[8]

Існує кілька типів класифікації міток. Широко відома і поширена розділяє мітки на чіпові на рисуноку 2.20 і бесчіпові, зображені на рисунку 2.21

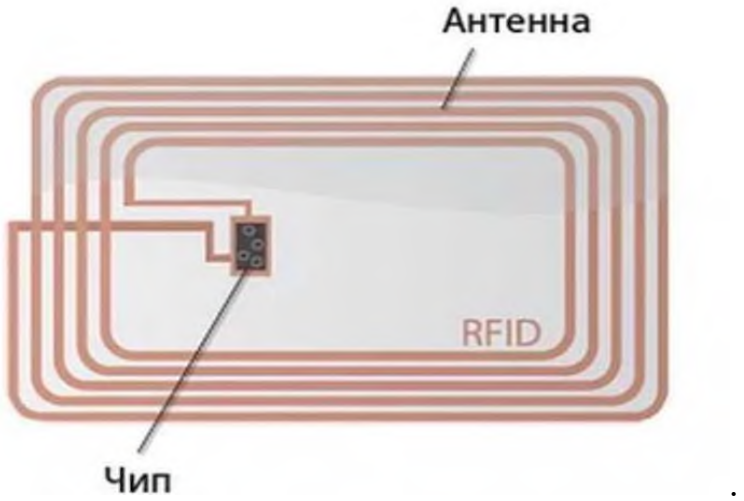

Рисунок 2.20—Чіпова RFID мітка

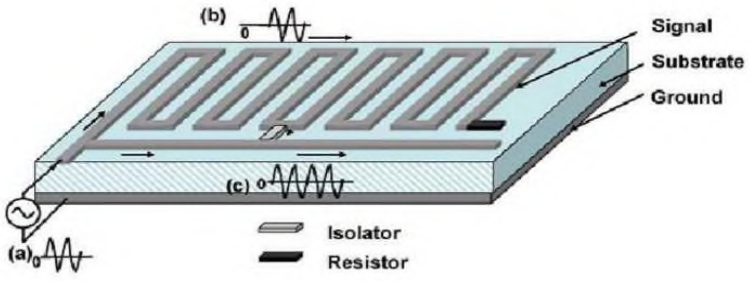

Рисунок 2.21 — Безчіпова RFID мітка

Чіпові мітки містять інтегральну мікросхему — чіп, а в безчіпових він відсутні. Друга класифікація розділяє типи міток на пасивні, напівактивні і активні. До складу пасивних міток не входить вбудований джерело живлення і

активний передавач; напівактивні мітки містять елемент живлення, але не мають активного передавача; активні мітки містять обидва елементи. У ще одній класифікації мітки підрозділяються на тільки зчитуються (read only) і зчитуються запису (read / write). Тільки зчитувальні мітки отримують свій ідентифікаційний код на виробництві. Пам'ять даного типу міток або тільки читається або одноразово програмована і багаторазово читається , тобто в ході роботи з пам'яттю, ідентифікаційний код даного типу міток можна перезаписати один раз. Мітки можуть багаторазово перепрограмувати в процесі експлуатації, і на них можна записати додаткову інформацію, а не тільки серійний номер або код.

За робочою частотою мітки діляться на мітки низькочастотного діапазону LF (125-134 кГц), високочастотного діапазону HF (13,56 МГц), і надвисокочастотного діапазону UHF (860-960 МГц).

Технологія RFID — це технологія безконтактного обміну даними, заснована на використанні радіочастотного електромагнітного випромінювання. RFID застосовується для автоматичної ідентифікації та обліку об'єктів. Типова RFID-система складається з 3-х базових компонентів: RFID-міток, RFID-зчитувачів і програмного забезпечення .Існують різні типи зчитувачів, в даній системі використовується портальний RFID-зчитувач, який призначений для регістрові RFID-міток контрольованих проходах. RFID RC522 зчитувач для безконтактної комунікації. Зчитувач підтримує інтерфейси SPI, UART і I2C через які відбувається обмін даними з іншими приладами . На платі модуля на висновках мікросхеми обраний інтерфейс SPI. Основа модуля - мікросхемаMFRC522. Радіоідентіфікація RFID відбувається при обміні даними по протоколу Mifare 1K. Mifare — торгова марка, яка об'єднує кілька типів мікросхем пластикових карт, мікросхеми зчитування і запису стаціонарних приладів і різні продукти на їх основі. Пристрої цієї марки відповідає стандарту ISO 14443 Type A. Зчитувач RFID RC522 спрацьовує при піднесенні мітки. Обмін даними відбувається через рамкові антени, що знаходяться в картці і в модулі. Сигнал модуля служить джерелом енергії для мітки. Він може обробляти інформацію одночасно від декількох міток.

Для розуміння роботи RFID системи, на рисунку 2.22 показаний принцип роботи системи.

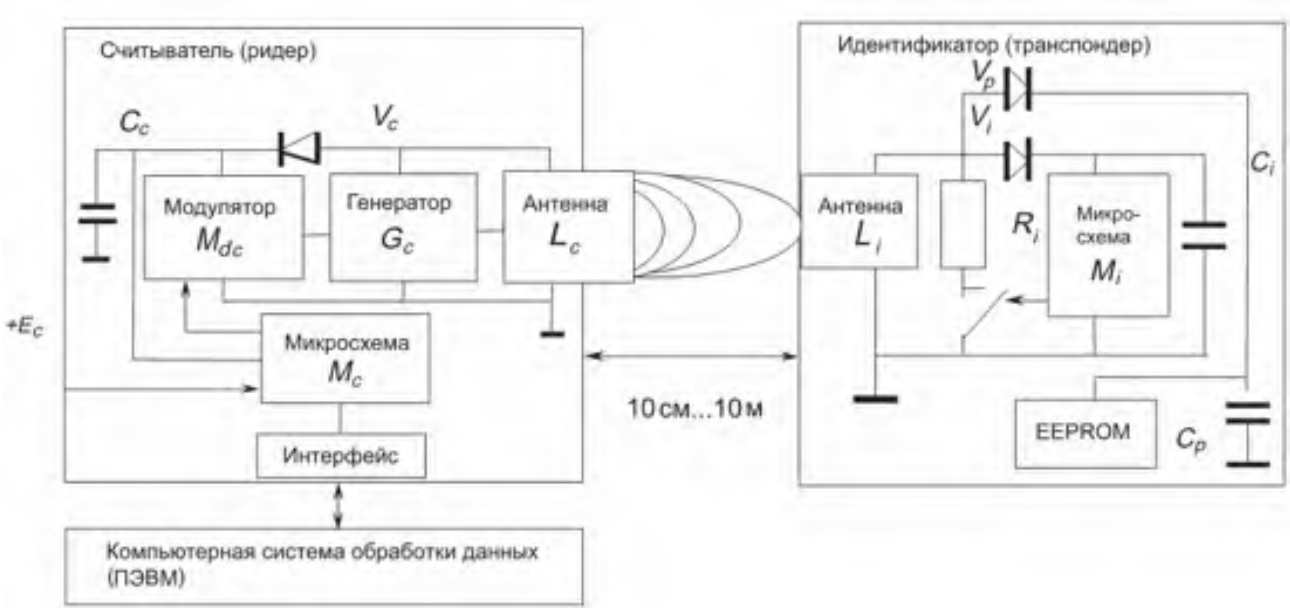

Рисунок 2.22 — Принцип роботи RFID системи

Як показано на схемі, RFID система має три основних компоненти: зчитувати, ідентифікатор і комп'ютер. RFID зчитувач має приймально-передавальний пристрій і антену, які посилають сигнал до тегу і приймають у відповідь. Основні компоненти RFID мітки: чіп і антена. Чіп має пам'ять і зберігає дані про ідентифікаційний номер або ін. Радіосигнал легко проходить через неметалеві матеріали, тому немає ніякої необхідності в контакті мітки зі зчитувачем. Дана RFID мітка є пасивною, тобто не має своїх джерел живлення, так як отримує енергію з сигналу зчитувача.[9]

Переваги RFID технології:

— не потрібен контакт або пряма видимість;

— мітки читаються швидко і точно;

— може використовуватися навіть в агресивних середовищах, а RFID мітки можуть читатися через бруд, фарбу, пар, воду, пластмасу, деревину;

— пасивні мітки мають фактично необмежений термін експлуатації;

— мітки несуть велику кількість інформації і можуть бути інтелектуальні;

— мітки практично неможливо підробити;

— мітки можуть бути не тільки для читання, а й для запису інформації.

У роботі будуть використані RFID технології, які, в результаті проведеного порівняльного аналізу показали, що краще підходять для розроблюваної інформаційної системи.

2.6 Огляд програмного середовища Arduino IDE

Середовище розробки Arduino складається з вбудованого текстового редактора програмного коду, області повідомлень, вікна виведення тексту (консолі), панелі інструментів з кнопками часто використовуваних команд і декількох меню. Для завантаження програм і зв'язку середовище розробки підключається до апаратної частини Arduino. Зовнішній вигляд середовища розробки Arduino наведено на рисунку 2.23.

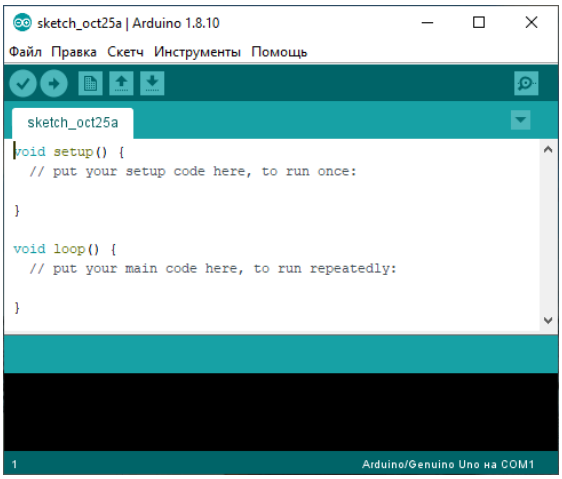

Рисунок 2.23 – Середовище розробки Arduino

Для платформи Arduino створене спеціальне середовище розробки з відкритим вихідним кодом для написання скетчів — Arduino IDE. Це середовище дає змогу писати код та завантажувати його на плату. Arduino IDE працює на всіх

відомих операційних системах: Windows, Mac OS X, Linux. Само середовище створене на мові програмування Java на основі Processing.[10]

До складу середовища розробки Arduino входить вбудований текстовий редактор програмного коду, області повідомлень, вікна виведення тексту (консолі), панелі інструментів з кнопками часто використовуваних команд і декількох меню. Середовище розробки підключається до апаратної частини Arduino для завантаження програм і створення зв'язку.

Скетч — програма, яка написана у середовищі Arduino. Він створюється у текстовому редакторі, який має різні інструменти: вирізати/ вставити, пошук/ заміна тексту. Коли проект зберігається або експортується в області повідомлень пишуться пояснення або помилки, що виникли при компіляції. Вікно де виводиться текст (консоль), у ньому відображаються повідомлення Arduino, у яких відображені повні звіти про помилки також може бути й інша інформація. Кнопки, що розміщені на панелі інструментів дають змогу перевірити та записати програму, створювати, відкривати та зберігати написані скетчі, а також відкрити моніторинг послідовної шини :

— «Verify» - Перевірка програмного коду на помилки, компіляція;

— «Load» - Перевірка програмного коду на помилки, компіляція та завантаження коду на платформу;

— «New» - Створення нового скетчу;

— «Open» - Відкриття меню доступу до всіх скетчів у блокноті;

— «Save» - Збереження скетчу.

Інші команди розподілені у меню: File, Edit, Sketch, Tools, Help. Режим доступності меню залежить від роботи, що виконується у даний момент. Copy for Discourse для копіювання у буфер обміну код скетчу для розміщення з виділенням синтаксису. Copy as HTML для копіювання коду секту у буфер обміну у вигляді HTML коду, щоб розміщувати його на веб-сторінках. Verify для виявлення помилок у скетчі. Import Library для додавання бібліотеки у скетч, зо використовується за допомогою виставлення директиви #include в код скетчу.

Show Sketch Folder для відкриття папки у якій міститься файл скетчу, на робочому столі. Add File для додавання файлу до скетчу. Новий файл буде розміщений в новій вкладці у вікні скетчу. Також його можна видалити, використовуючи меню вкладок. Auto Format для форматування коду. Board вибір використовуваної платформи. Serial Port для вибору послідовних реальних та віртуальних пристроїв на комп'ютері. Оновлення списка відбувається автоматично кожного разу при зверненні до меню Tools. Burn Bootloader для запису завантажувача (Bootloader) в мікроконтролер на платформі Arduino. Не є обов’язковою функцією, але може знадобитися, якщо використовується новий ATmega (без завантажувача). Перед записом необхідно перевірити чи правильно вибрана платформа з меню. Якщо використовується AVR ISP, то необхідно вибрати порт, що відповідає программатору з меню Serial Port.

У середовищі Arduino присутній принцип блокнота, як місце для зберігання програм (скетчів) за замовчуванням. Скетчі у блокноті можна відкрити через меню File> Sketchbook або натискаючи на кнопку Open на панелі інструментів. Для блокнота автоматично створюється директорія при першому запуску програми. Розташування блокнота можна змінити за допомогою діалогового вікна Preferences .

Закладки, Файли та Компіляція. За допомогою закладки, файла та компіляції можна одночасно працювати з декількома файлами скетів, оскільки кожен з них відкривається в окремій вкладці. Файли коду можуть бути декількох видів: стандартними Arduino (без розширення), файлами C (розширення * .c), файлами C ++ (* .cpp) або головними файлами (.h).

Для того, щоб завантажити скетч, необхідно задати параметри в меню Tools > Board і Tools > Serial Port. В ОС Mac послідовний порт має позначення dev / tty.usbserial-1B1 (для плати USB) або /dev/tty.USA19QW1b1P1.1 (для плати послідовної шини, яка підключається через адаптер Keyspan USB-to-Serial). В ОС Windows порти мають назви: COM1 або COM2 (для плати послідовної шини) або COM4, COM5, COM7 і вище (для плати USB). Виявлення порту USB

відбувається в полі послідовною шиною USB диспетчера пристроїв Windows. В ОС Linux порти можуть називатися, як / dev / ttyUSB0, / dev / ttyUSB1.

Після того, як був вибраний порт і платформа вибору порту потрібно натиснути кнопку завантаження на панелі інструментів або вибрати пункт меню File> Upload to I / O Board. Платформи Arduino сучасних випусків автоматично перезавантажуються перед завантаженням. На платформах випусків минулих років, потрібно кожного разу натискати кнопку перезавантаження. Більшість плат оснащені світлодіодами RX і TX , які будуть світиться під час роботи. Після завантаження буде виведено повідомлення про закінчення завантаження або про наявність помилки. Для того, щоб завантажити скетч необхідно використовувати завантажувач Arduino, це невелика програма, що завантажується в мікроконтролер на платі. З її допомогою можна завантажувати код без застосування додаткових пристроїв. Завантажувач працює при перезавантаженні платформи та при завантаженні будь-якого скетчу на мікроконтролер. При робота завантажувача миготить світлодіод.

Моніторинг послідовної шини відображає дані, що надсилаються на платформу Arduino (плата USB або плата послідовної шини). Для того, щоб відправити дані, спочатку необхідно написати текст і натиснути кнопку Send або Enter. Після цього обрати швидкість передачі даних, яка відповідає значенню Serial.begin в скетчі. На ОС Mac або Linux платформа Arduino перезавантаження відбудеться при підключенні моніторингу послідовної шини.[11]

3 ПРОЕКТУВАННЯ МІКРОПРОЦЕСОРНОЇ СИСТЕМИ БЕЗПЕЧНОГО ДОСТУПУ ДО ОБ’ЄКТІВ

3.1 Вибір мікропроцесорної платформи та компонентів

На сьогоднішній день існує величезна кількість різних вільно програмованих пристроїв. Їх використовують в різних сферах і завданнях, починаючи від іграшок і закінчуючи медичною технікою. І з кожним днем виникають все нові і нові галузі. Але для простого обивателя італійці розробили готові набори з електронного блоку і програмного забезпечення. Це плати Arduino і їх аналоги

Arduino Uno - це пристрій на основі мікроконтролера ATmega328. У його склад входить все необхідне для зручної роботи з мікро контролером: 14 цифрових входів / виходів (з них 6 можуть використовуватися в якості ШІМ-виходів), 6 аналогових входів, кварцовий резонатор на 16 МГц, роз'єм USB, роз'єм живлення, роз'єм для внутрисхемного програмування (ICSP) і кнопка скидання. Для початку роботи з устройством досить просто подати живлення від AC / DC-адаптера або батарейки, або підключити його до комп'ютера за допомогою USB-кабелю.

Arduino - це проста у використанні відкрита електронна платформа, що включає програмне забезпечення і призначена для швидкого створення інтерактивних електронних пристроїв. Вона була створена групою ентузіастів, які позиціонували свою розробку як платформу для швидкої реалізації невеликих проектів. Arduino будується на базі мікроконтролерів Atmel і використовується для отримання сигналів від аналогових і цифрових датчиків, управління різними виконавчими пристроями і обміну інформацією з комп'ютером за допомогою різних інтерфейсів. Сенсори і датчики підключаються до плати Arduino функціонують для збору і передачі даних.

При отриманні даних про зовнішнє середовище, пристрій обробляє отриманий сигнал і відправляє дані в центральне сховище даних або сервер де ці дані аналізуються і зберігаються для подальшого дослідження. Вимірювальних

приладів на сьогоднішній день багато: сенсори, прості датчики температури, прилади обліку споживання і т.д, вони володіють чотирма основними можливостями: зондування, обробка даних, передача даних і, в деяких випадках, активування, тобто управління іншими пристроями, такими як електродвигуни, інші датчики, системи сигналізації і т.д., такі перетворювачі можуть виявляти енергію різних фізичних, хімічних та інших явищ і перетворювати її в сигнал, електричний імпульс і т.д.

Сенсорні технології застосовувалися і застосовуються в багатьох областях, таких як національна безпека, наземний моніторинг як поверхні землі, так і води, збір інформації з метою захисту, моніторинг навколишнього середовища, аналіз і прогнозування погоди і клімату, спостереження і моніторинг зони конфлікту, моніторинг сейсмічного прискорення , навантаження, температури, швидкості вітру і GPS-даних.

Arduino дає можливість досягти високого рівня автономності, набагато спрощує процес роботи з мікроконтролерами і має ряд переваг перед іншими пристроям.

Arduino широко поширена торгова марка апаратно-програмних засобів для побудови простих систем автоматики і робототехніки, орієнтована на непрофесійних користувачів. У даній роботі використовується модель контролера Arduino UNO R3, виконана на базі мікроконтролера ATmega328.

Вибір конкретної моделі контролера виконаний на підставі аналізу вирішуваних завдань, доступності, вартості, простоти освоєння і інших критеріїв, за якими Arduino UNO значно перевершує інші варіанти. Програмна частина Arduino UNO складається з безкоштовної програмної оболонки для написання програм, їх компіляції та програмування апаратури.

Апаратна частина являє собою набір змонтованих друкованих плат, що продаються як офіційним виробником, так і сторонніми виробниками. Повністю відкрита архітектура системи дозволяє вільно копіювати або доповнювати лінійку продукції Arduino. На рисунку 3.1 представлено зовнішній вигляд Arduino Uno.

.

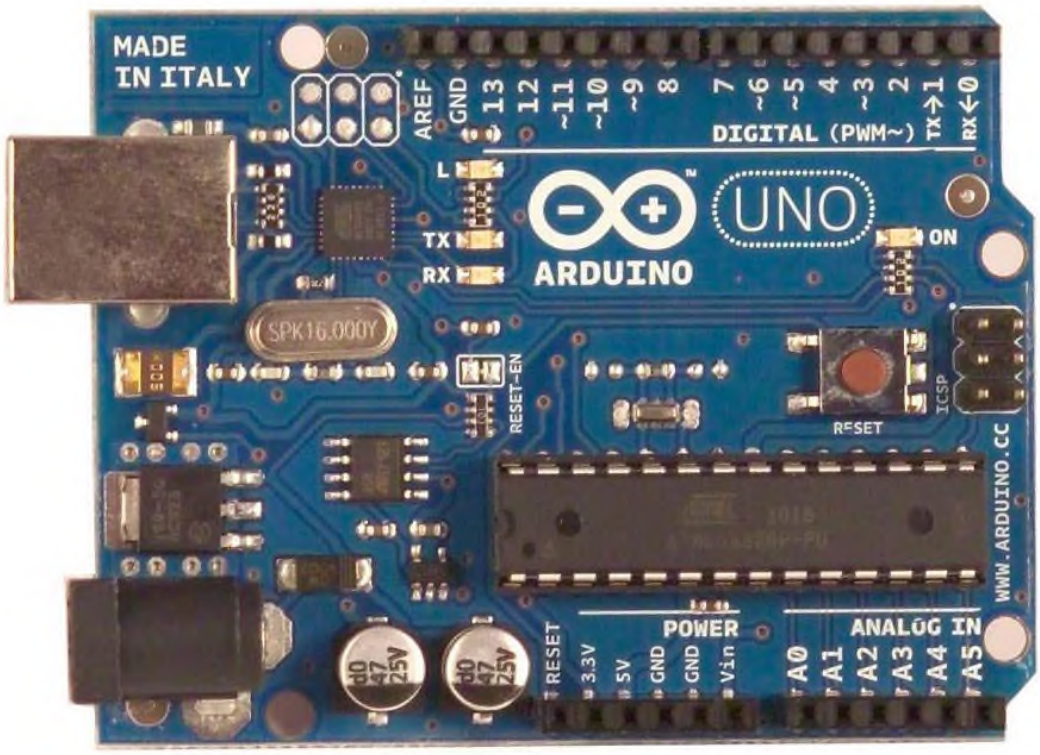

Рисунок 3.1.— Зовнішній вигляд контроллера Arduino Uno

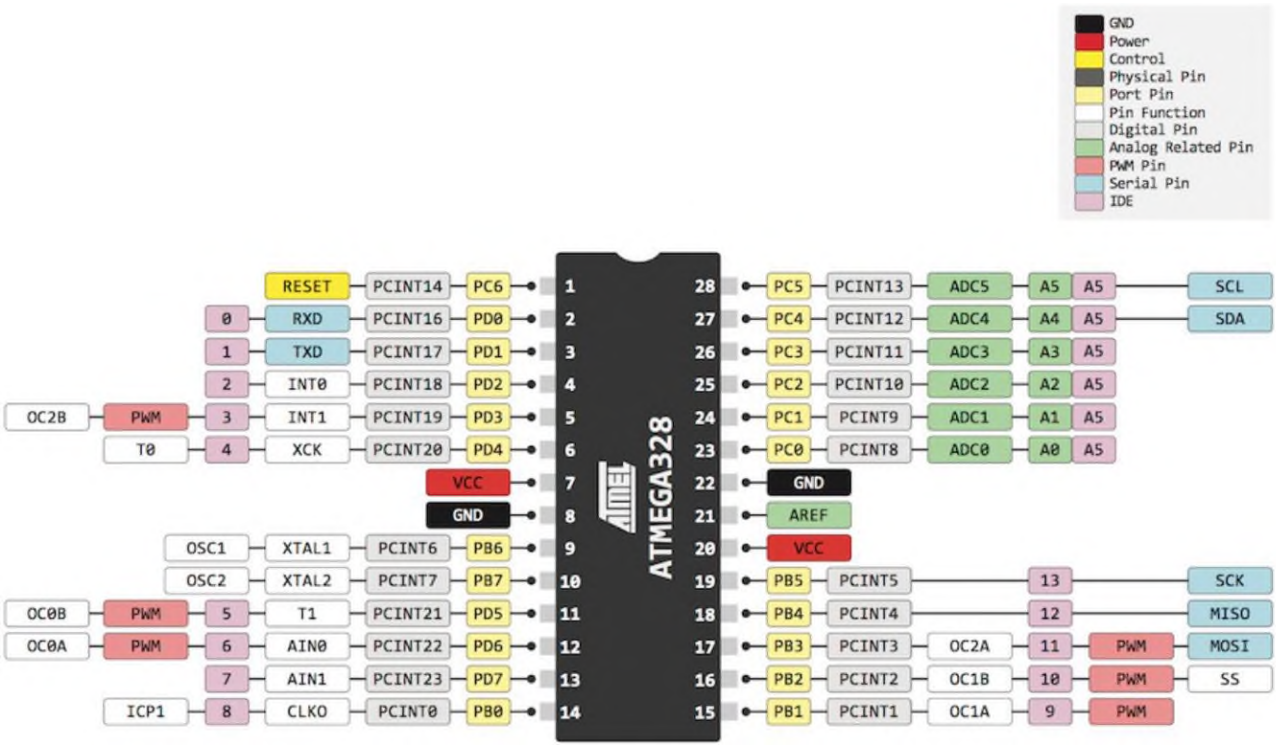

Рисунок 3.2— Контролера ATmega328p

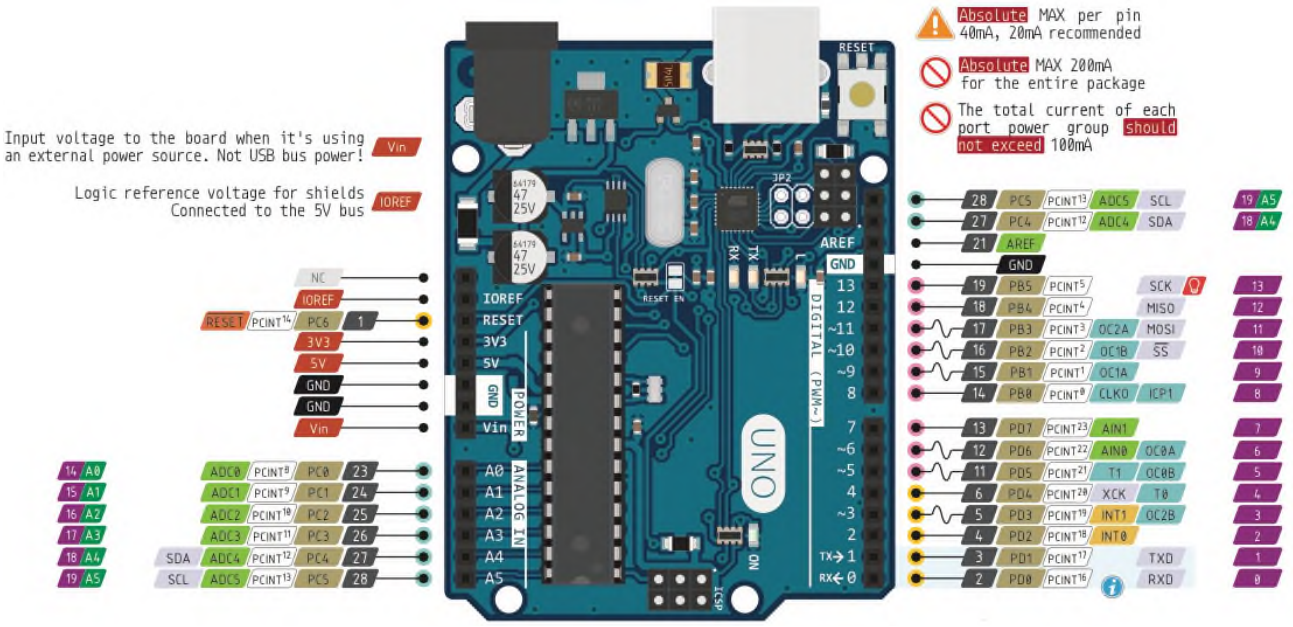

Рисунок 3.3 — Призначення виходів Arduino Uno

Arduino Uno R3 - це пристрій на основі мікроконтролера ATmega328. У його склад входить: 14 цифрових входів / виходів під номерами 0-13 (з них 6 можуть використовуватися в якості ШІМ-виходів, на платі позначені зі знаком "~"), 6 аналогових входів A0-A5, кварцовий резонатор на 16 МГц, роз'єм USB, роз'єм живлення, роз'єм для внутрисхемного програмування (ICSP) і кнопка скидання. Для початку роботи потрібно подати живлення від AC / DC-адаптера або батарейки, або через USB-кабель від персонального комп'ютера. Порт AREF задає опорну напругу аналогових входів. Порт IOREF дозволяє платам розширення підлаштовуватися під робочу напругу Arduino. Він необхідний для сумісності плат розширення як з 5 вольт (В) Arduino на базі мікроконтролерів AVR, так і з 3.3В платами Arduino Due. Основні характеристики Arduino Uno R3 представлені нижче. Робоча напруга живлення 5В, рекомендований напруга живлення від 7 до 12В, максимальне напруження харчування в діапазоні 6-20В. 14 цифрових входу / виходу, 6 аналогових входів, максимальний струм одного виведення дорівнює 40 мА, максимальний струм виводу 3.3V дорівнює 50 мА. У мікроконтролера присутній Flash-пам'ять на 32 кілобайт (КБ) (ATmega328), яка використовується при створенні програм, з яких 0.5 КБ використовуються

загрузчиком, а також електрично стирається незалежна жорсткий диск EEPROM на 1 КБ. Тактова частота кварцового резонатора 16 МГц.[12]

Характеристики Arduino UNO:

— мікроконтролер ATmega328;

— робоча напруга 5В;

— вхідна напруга (рекомендована) 7-12 В;

— вхідна напруга (граничне) 6-20 В;

— цифрові Входи / Виходи 14 (6 з яких можуть використовуватися як виходи ШІМ);

— аналогові входи 6;

— постійний струм через вхід / вихід 40 мА;

— постійний струм для виведення 3.3 В 50 мА;

— флеш пам `ять 32 Кб (ATmega328) з яких 0.5 КБ використовуються для завантажувача;

— ОЗУ 2 Кб (ATmega328);

— EEPROM 1 Кб (ATmega328);

— тактова частота 16 МГц .

Для реалізації радіочастотної ідентифікації був обраний RFID модуль RC522. Його характеристики представлені нижче. Напруга живлення 3,3 В, споживаний струм не більше 30 мА, робоча смуга частот 13,55-13,57 МГц, зчитується на відстані 0-25 мм, фізичний розмір зчитувача 40 х 60 мм, робоча температура від 20 до 80С °.Супроводжувані карти: класи S50, S70, Ultralight, Pro, DESFire; типи Mifare S50, Mifare S70, Mifare UltraLight, Mifare Pro, Mifare DESfire. Швидкість передачі інформації 106, 212, 424, 848 кбіт / с. Шифрування Security Features Mifare classic (термін Mifare може тільки компанія NXP Semiconductors, а також компанії, що мають ліцензію від NXP на виробництво чіпів). Мітки MiFare Classic працюють на високочастотних радіохвилях, зокрема на частоті 13,56 МГц. Це та ж частота, на якій працюють пристрої з підтримкою Near Field Communication (NFC). У RFID мітках відсутня мікропроцесор і захищений елемент, здатний до аутентифікації. RFID мітки MiFare були введені

NXP Semiconductors в 1995 році, і з тих пір було продано більше мільярда міток у всьому світі. Діючи в якості систем контролю доступу та електронних гаманців, мітки привернули увагу дослідницьких груп, які провели численні дослідження, що стосуються безпеки, які пропонують мітки. MiFare Classic реалізують власний криптографічний алгоритм під назвою CRYPTO-1. Це потоковий шифр з 48-бітовим ключем, який використовується для забезпечення конфіденційності даних і взаємної автентифікації між міткою і зчитувачем.

Зовнішня схема пристрою для зчитування RFID міток представлена на рисунку 3.4.

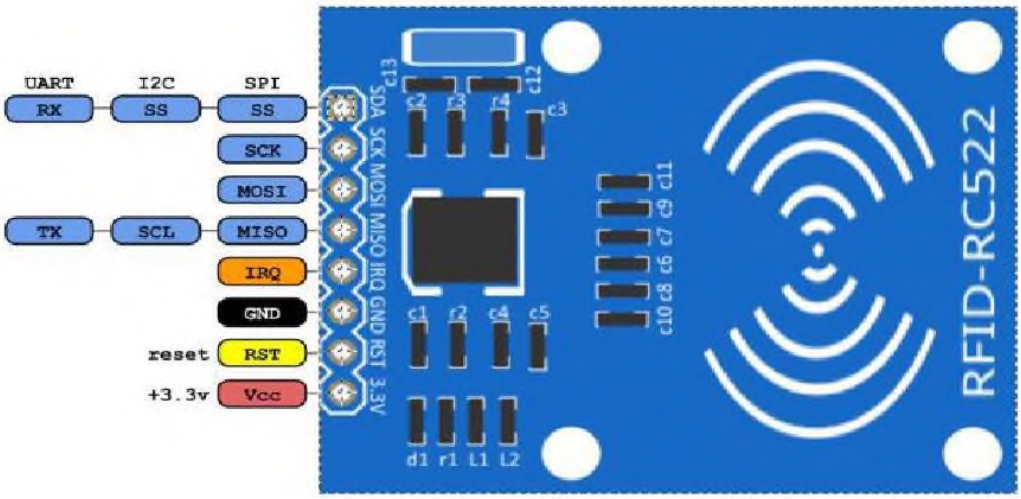

Рисунок 3.4 —Зчитувач RC522

Контакти і сигнали RFID RC522:

— VCC — Живлення 3.3V;

— RST — Reset. Лінія збросу, вхід;

— GND — Ground. Земля;

— MISO — Master Input Slave Output — дані від відомого ведучого, вихід;

— MOSI — Master Output Slave Input — вхід SPI;

— SCK — Serial Clock — тактовий сигнал, вхід SPI;

— SDA — Slave Select — вхід SPI;

— IRQ — лінія прерываний, вихід.

Зчитувач підтримує інтерфейси SPI, UART і I2C через які відбувається обмін даними з іншими приладами. На платі модуля RFID RC522 установкою логічних рівнів на спеціальних висновках мікросхеми обраний інтерфейс SPI. З одним Arduino можуть працювати кілька приладів, підключених до шини SPI.

Підключення модуля RC533 до Arduino Uno проводиться відповідно таблиці 3.1. Для нормальної роботи представленого вище модуля вихід IRQ не вдалося підключитися до Arduino.

Таблиця 3.1 - Підключення RC522 до Arduino Uno

MFRC522	Arduino Uno
RST	9
SDA	10
MOSI	11
MISO	12
SCK	13
3.3V	3.3V
GND	GND

У комплекті з даним модулем входить біла пластикова карта Mifare Classic 1K або мітка у вигляді брелка, зображена на рисунку 3.5.

Рисунок 3.5 — RFID мітка Mifare 1K

Всередині неї знаходяться антена і мікросхема Mifare S50, що містить пам'ять і родючості. Розмір пам'яті 1 кілобайт, тип EEPROM. Вона розділена на 16 секторів, що складаються з 4 розділів. У кожному розділі три інформаційних частини і одна для ключів. Усередині однієї частини є 16 байт пам'яті. Термін зберігання даних 10 років, кількість циклів перезапису 100000.

Унікальність картки Mifare забезпечується привласненням виробником номера, використовуваного в якості ідентифікаційного коду. Для захисту даних в мікросхемі карти використано апаратне шифрування. Під час роботи дані з картки надходять на зчитувач тільки після взаємної ідентифікації коду, записаного в сектор пам'яті картки і зберігається в зчитувачі.

Для роботи в середовищі розробки Arduino можна скористатися різними сторонніми бібліотеками, розробленими для того, щоб істотно спростити роботу зі зчитувачем RC522. Для запису і читання з карти необхідно знати її унікальний номер, необхідний для роботи системи радіочастотної ідентифікації. Для цього потрібно завантажити програму зі списку прикладів бібліотеки RFID під назвою «CardInfo», підключити RC522 до Arduino, і запустити програму в середовищі розробки Arduino IDE. При знаходженні робочої мітки в зоні дії RFID зчитувача на моніторі порту з'явиться інформація про карту, представлена на рисунку 3.6.

```
Card found
Cardnumber:
Dec: 60, 121, 172, 213, 60
Hex: 3C, 79, AC, D5, 3C
```

Рисунок 3.6 — Ідентифікація номеру RFID міток

Програма виводить ряд чисел: 60, 121, 172, 213, 60. Необхідно записати їх в зворотному порядку. Перше число виключається (контрольна сума), яке спочатку було останнім, а що залишилися числа переводяться в шістнадцятковий код. Потім вони записуються в тому ж порядку, але без пробілів. Отримане велике число необхідно перевести в десятковий код, внаслідок чого вийде

ідентифікаційний номер карти. З його допомогою вже можна проводити різні маніпуляції і складати різні програми, наприклад системи контролю доступу в приміщення.

Для того, щоб вводити кодову комбінацію, можна скористатися спеціально сконструйованої для роботи з мікроконтролерами матричної клавіатурою, що складається з 16 кнопок внутрішня схема якої зображена на рисунку 3.7.

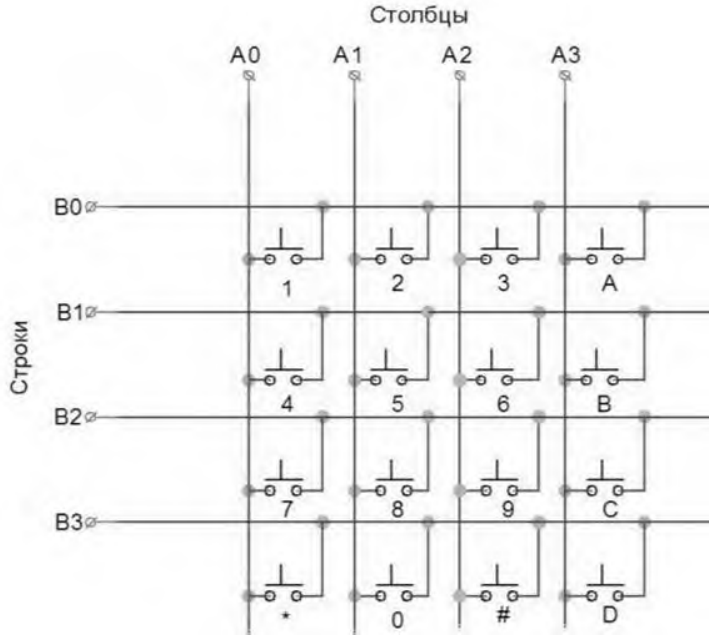

Рисунок 3.7 — Схема матричної клавіатури 4x4

Матричні клавіатури для мікроконтролерів досить різноманітні в своєму побудові. Крім 16-кнопкових клавіатур існують рішення з 12 або з 4 кнопками, з мембранної підкладкою або з простими кнопками. Для вирішення поставлених завдань, скористаємося типовим рішенням у вигляді матричної клавіатури з 16 кнопок.

Для того щоб підключити матричну клавіатуру до Arduino, від плати виведено 8 контактів, які підключаються через сполучні дроти до цифрових входів мікроконтролера.

У пристрої багатьох електронних замків може бути присутнім елемент, який відтворює звук. Для цих цілей підійде п'єзокерамічних випромінювач звуку,

який може відтворити звук на основі п'єзоелектричного ефекту. Пьезодінамік, складається з металевої пластини, з нанесеною на ній п'єзоелектричної кераміки, що має струмопровідні напилення. Пластина і напилення є контактами полярність яких - плюс і мінус. Якщо до контактів прикласти напругу, під дією зворотного п'єзоелектричного ефекту випромінювач почне відтворювати звук, а якщо механічно впливати на п'єзоелемент, то на його контактах з'явиться напруга. Щоб підключити пьезодінамік до мікроконтролеру, контакт, позначений знаком «+» підключається до будь-якого цифрового входу, а мінусовій контакт до виходу GND.

Зручним способом відображення різної інформації, необхідної під час роботи пристрою контролю доступу, є рідкокристалічний дисплей. Виберемо найпростіший в управлінні символьний дисплей LCD1602 на основі контролера HD44870, зображений на рисунку 3.8. На цьому малюнку також зображена плата послідовного 12C-інтерфейсу на основі мікросхеми PCF8574AT, за допомогою якої можна підключати дисплей до мікроконтролеру через 4 дроти. Підключення відбувається дуже просто: SDA і SCL входи підключаються до входів SDA і SCL мікроконтролера, VCC і GND відповідно до +5 В і GND мікроконтролера.

Рисунок 3.8—Дисплей LCD 1602 і плата підключенння 12C-інтерфейса

Для наочності використовуємо модуль RGB-світлодіоди KY-016, представлений на рисунку 3.9. У цьому модулі висновки, що відповідають за передачу кольору, вже підключені через резистори номіналом 220 Ом, тому немає необхідності в окремих резисторах, щоб захистити світлодіод від виходу з ладу. Висновки R, G, B з'єднуються з цифровими входами мікроконтролера, а висновок "-" до входу GND.

Рисунок 3.9 — RGB-світлодіод KY-016

Для комутації різних приладів використовується спеціальний одно канальний модуль реле для мікроконтролерів, зображений на малюнку 2.10, а принципова схема пристрою на рисунок 3.10.

Рисунок 3.10 – Схематичне зображення реле (вид зверху)

До складу реле входять: резистори номіналом 1 кОм (R1, R2), що підтягує резистор R3 на 10 кому, p-n-p транзисторуТ1), зворотний діод (У1) 2) і, реле (К1). VD1 (червоний світлодіод) - індикація подачі живлення на модуль, загоряння VD3 (зелений світлодіод) свідчить про замиканні реле. Контакти реле показані на рисунку 3.11.

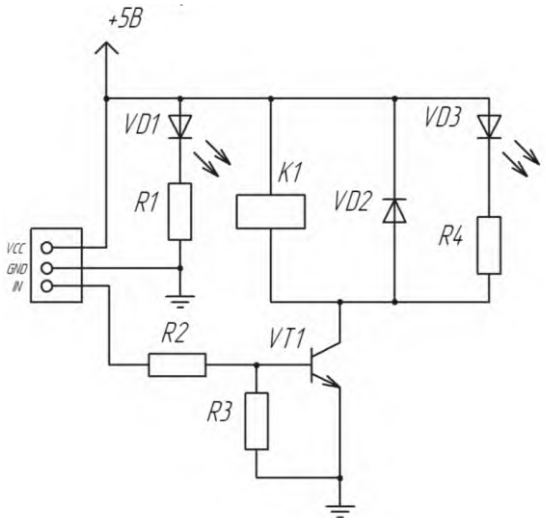

Рисунок 3.11 – Принципова схема модуля реле

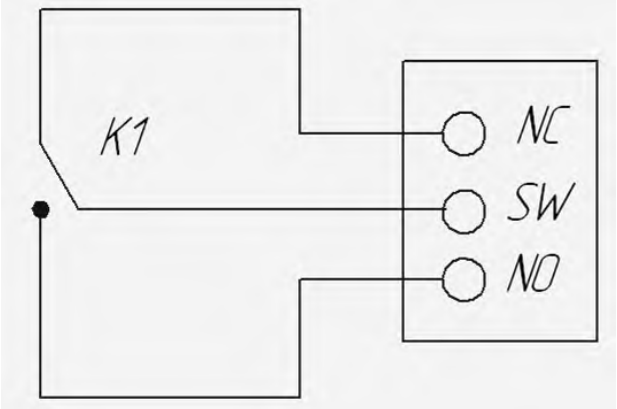

Рисунок 3.12 — Контакти одноканального реле

При включенні висновки знаходяться в високоомному стані, транзистор не відкритий. Так як транзистор p-n-p типу, то для його відкриття потрібно подати на базу мінус. Для цього потрібно використовувати функцію digitalWrite (pin,

LOW). Реле спрацьовує, коли транзистор відкритий і через керуючу ланцюг тече струм. Для відключення реле слід закрити транзистор, подавши на базу плюс за допомогою функції digitalWrite (pin, HIGH). Контакти реле NC - нормально замкнутий, SW - контакт перемикання, NO - нормально розімкнутий.

На відміну від всіх попередніх плат Ардуіно, Uno в якості перетворювача інтерфейсів USB-UART використовує мікроконтролер ATmega16U2 (ATmega8U2 до версії R2) замість мікросхеми FTDI.

Для підключення різних модулів до мікроконтролеру Arduino існує спеціальну макетну плату, на якій зручно розташовувати різні елементи схеми, а також з'єднувати їх проводами між собою і мікро контролером. В кінцевому підсумку, вийшла схема, представлена на рисунок 3.14. Всі елементи з'єднані з мікро контролером згідно принциповими схемами, які були розроблені в спеціалізованих програмах моделювання Autodesk Circuits і Fritzing.

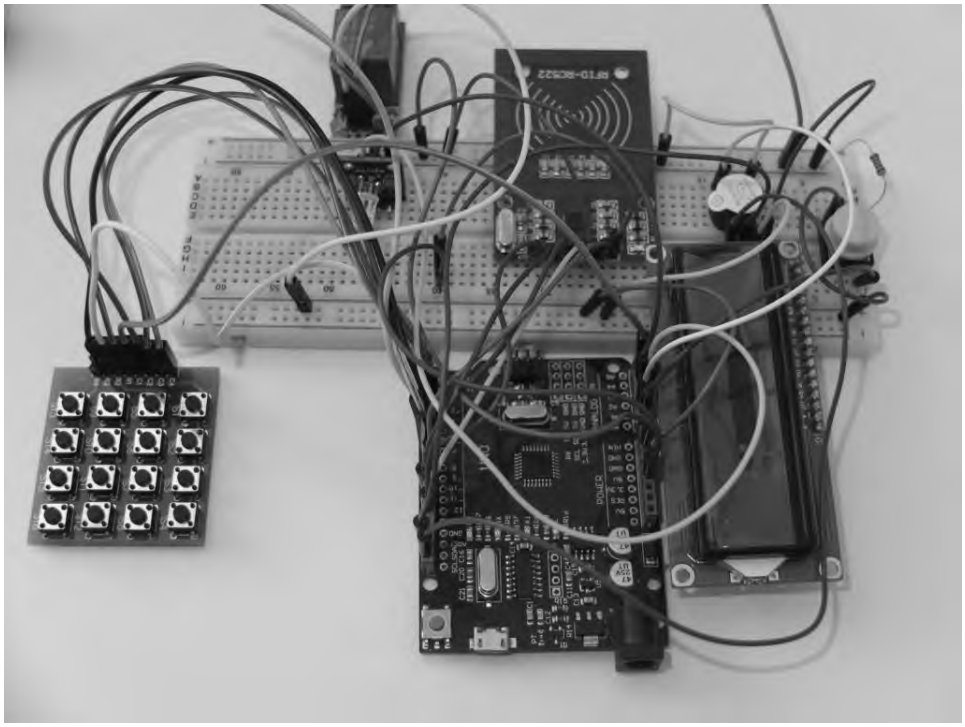

Рисунок 3.14 – Моделювання пристрою

Розглянемо підключення RFID-зчитувача RC522, представленим на рисунку 3.15, і світлодіода, представленого на рисунку 3.3.

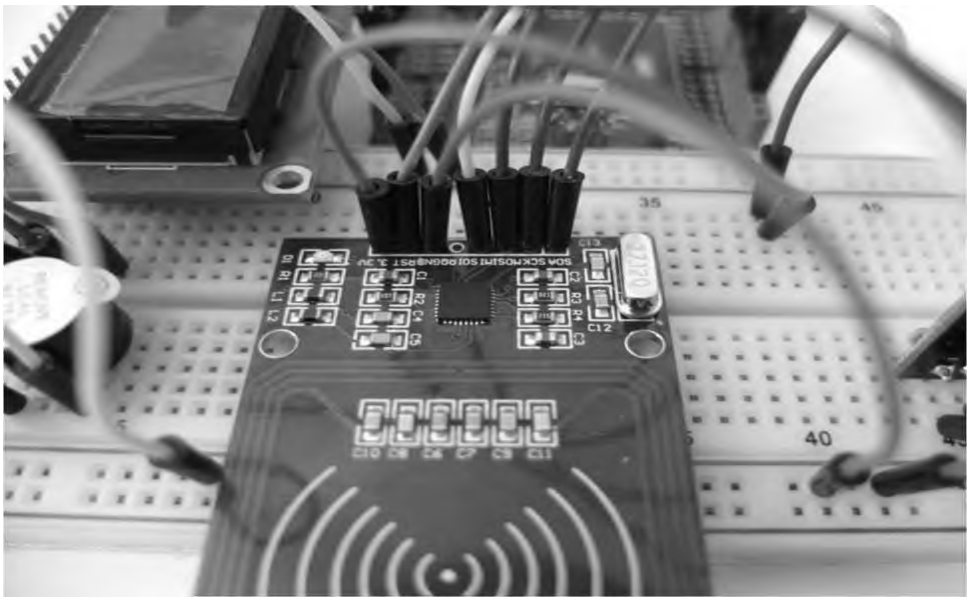

Рисунок 3.15 — Зєднання RC522 з Arduino

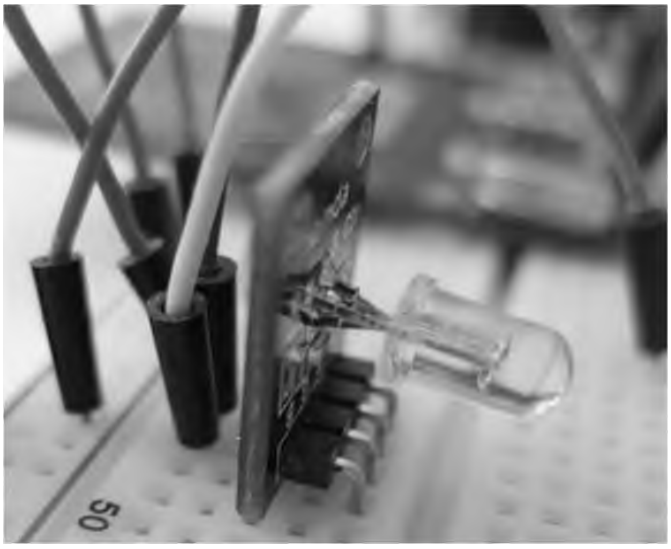

Рисунок 3.16 — Зєднання RGB-світлодіода з Arduino

3.2 Розробка конструкції пристрою

Для подання конструкції пристрою контролю доступу скористаємося дуже зручною програмою для візуалізації всіх етапів роботи з Arduino. За допомогою програми Autodesk Circuits з електронного ресурсу circuits.io, поширюваної на безкоштовній основі і не вимагає установки на персональний комп'ютер, можна

моделювати різні рішення, які будуть показані в зручній для користувача формі макета або схеми підключення.[14]

Промоделюємо модулі за допомогою Autodesk Circuits, використовувані спільно з мікро контролером Arduino, і виведемо їх схеми підключення до Arduino Uno R3, показані на малюнках 3.17 — 3.20**.**

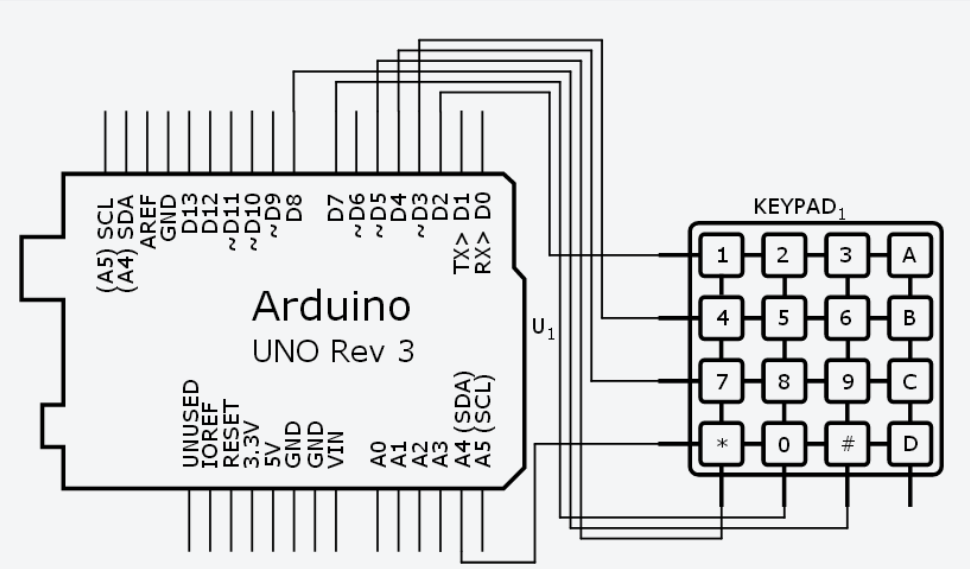

Рисунок 3.17 – Схема підключення матричної клавіатури

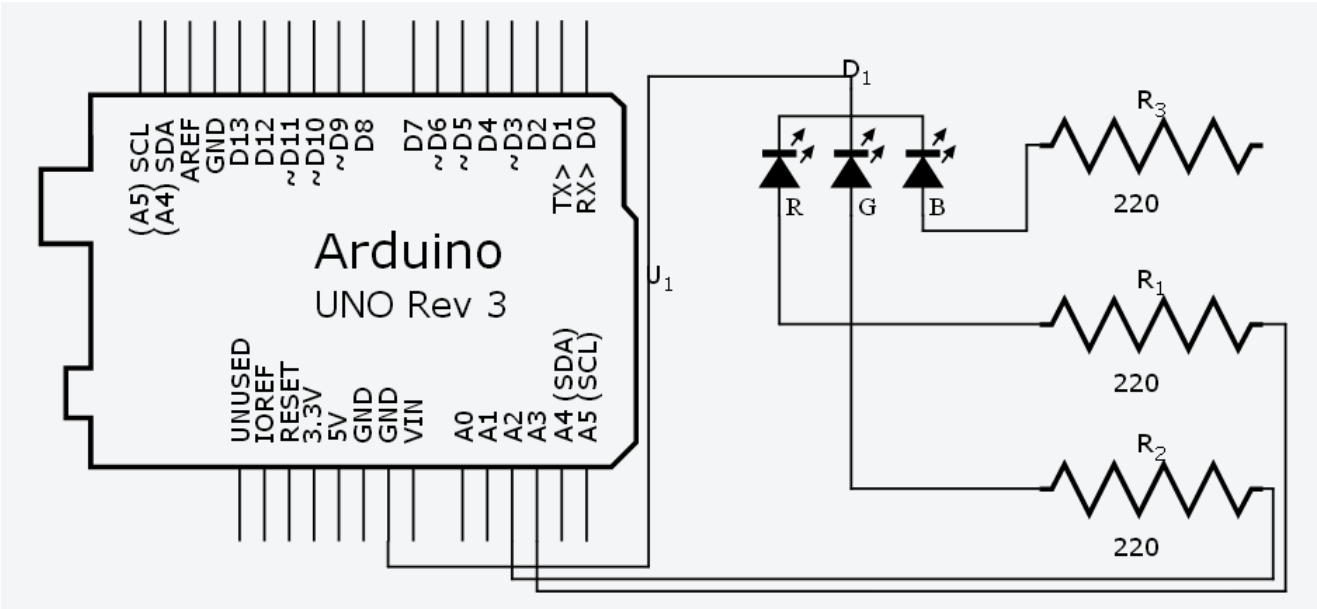

Рисунок 3.18 – Схема підключення RGB- світлодіода

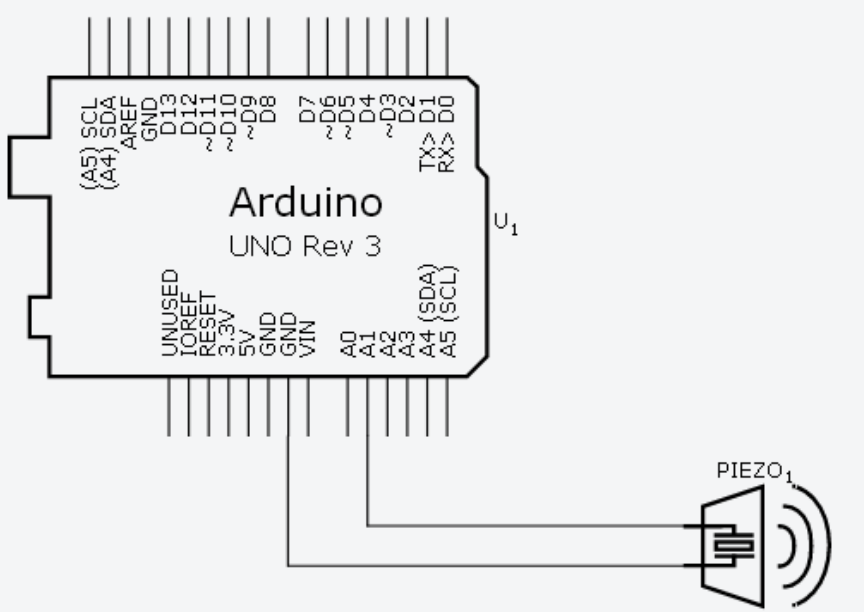

Рисунок 3.19 — Схема підключення пьєзодинаміка

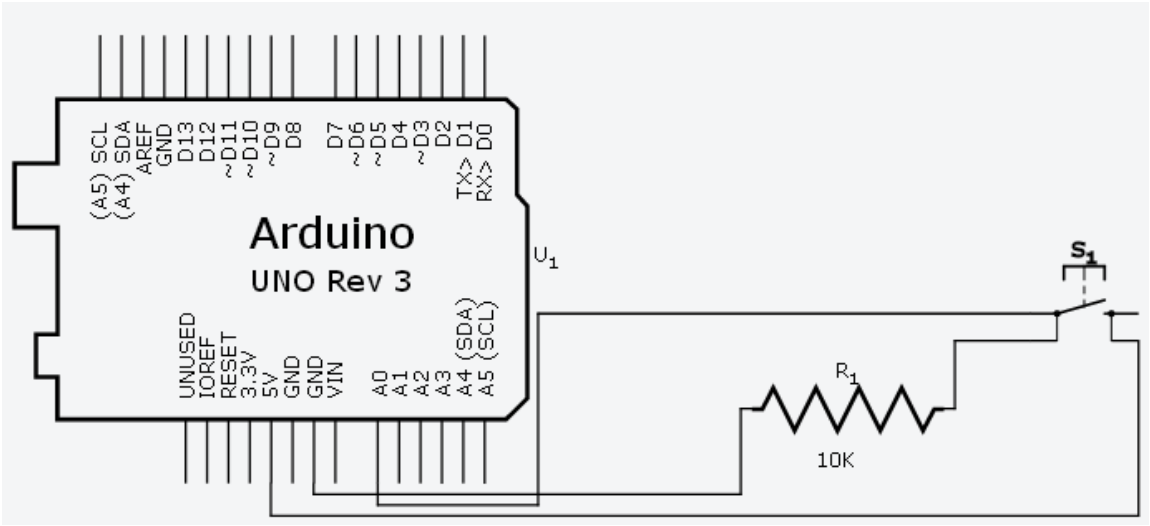

Рисунок 3.20 — Схема підключення кнопки збросу EEPROM

Незважаючи на всі переваги представленої вище програми, у неї є істотний недолік - сильно обмежена кількість елементів, з якими можна працювати. Тому подальше моделювання системи проводилося в програмному середовищі розробки Fritzing, спеціально розробленої для моделювання схем Arduino. Схеми підключень, створені в програмному середовищі Fritzing, зображені на малюнках 3.21 - 3.23.

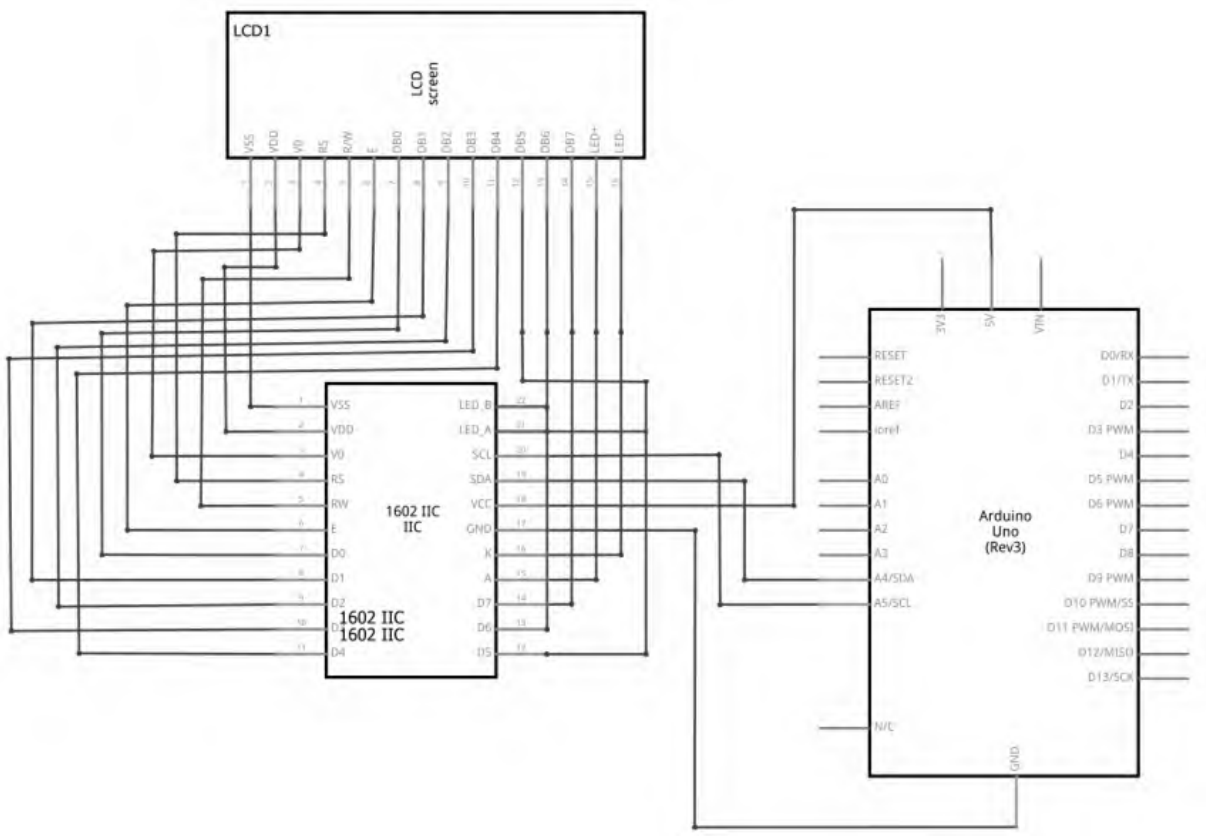

Рисунок 3.21 — Схема підключення дисплею LCD 1602 за допомогою інтерфейсу I2C

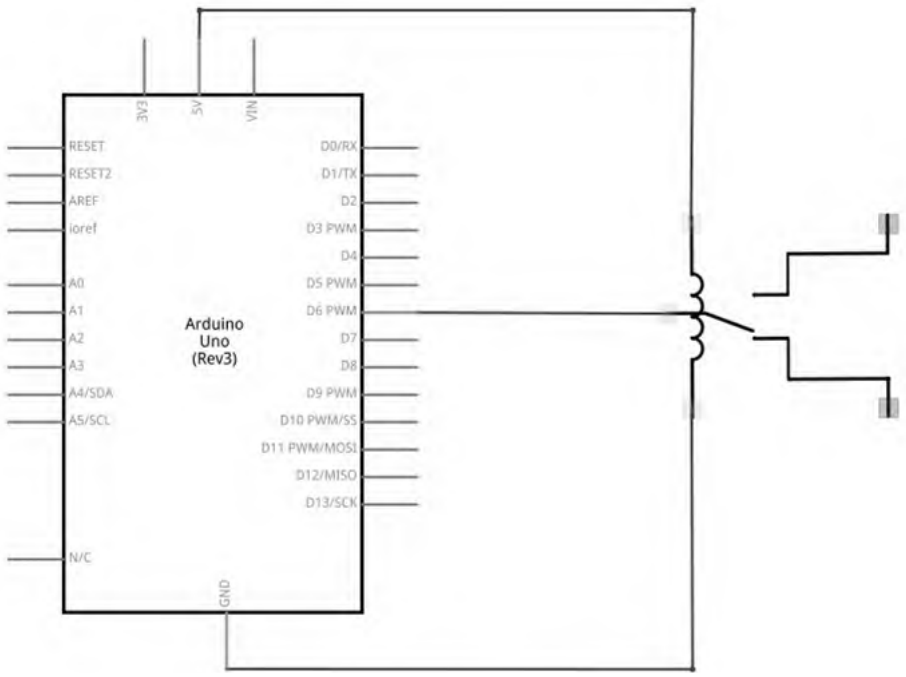

Рисунок 3.22 — Схема підключення одноканального реле

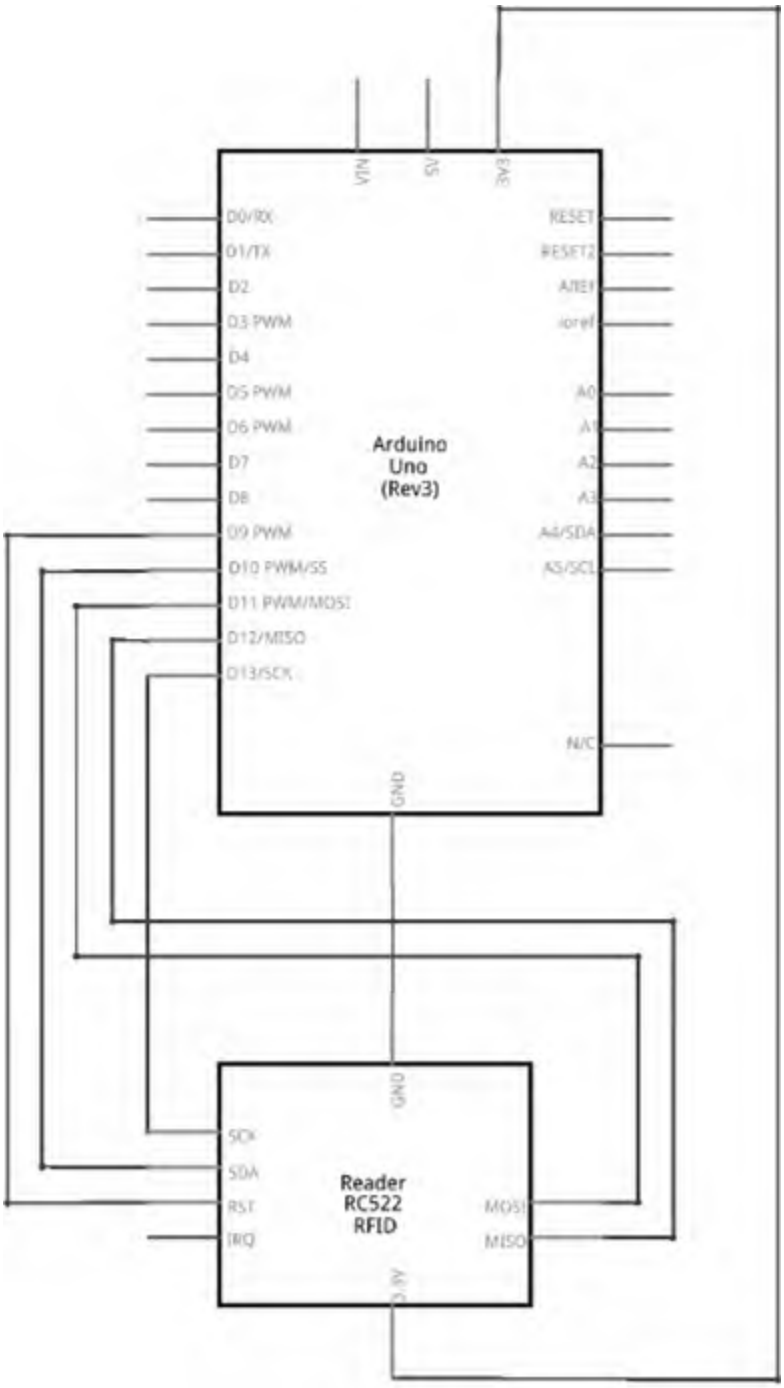

Рисунок 3.23 — Схема підключення RFID зчитувача RC522

Схема підключення всіх необхідних компонентів для пристрою контролю доступу до мікроконтролеру зображено на рисунку 3.24.

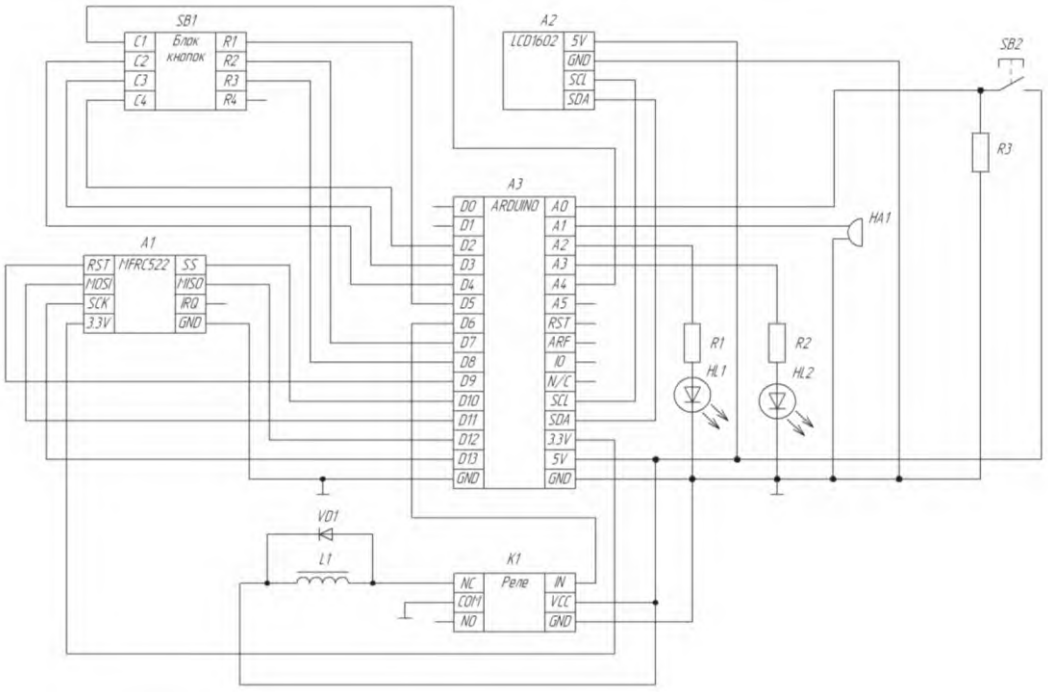

Рисунок 3.24 — Схема підключення всіх компонентів

3.3 Розробка алгоритму роботи

Робота будь-якої системи в своїй основі вимагає опису алгоритму її роботи. Алгоритм — послідовність, система, набір систематизованих правил виконання обчислювального процесу, що обов'язково приводить до розв'язання певного класу задач після скінченного числа операцій. При написанні комп'ютерних програм алгоритм описує логічну послідовність операцій. Для візуального зображення алгоритмів часто використовують блок-схеми.

Кожен алгоритм є списком добре визначених інструкцій для розв'язання задачі. Починаючи з початкового стану, інструкції алгоритму описують процес обчислення, які відбуваються через послідовність станів, які, зрештою, завершуються кінцевим станом. Перехід з одного стану до наступного не обов'язково детермінований — деякі алгоритми містять елементи випадковості. Кожен алгоритм передбачає існування початкових (вхідних) даних та в результаті роботи призводить до отримання певного результату. Робота кожного алгоритму відбувається шляхом виконання послідовності деяких елементарних

дій. Ці дії називають кроками, а процес їхнього виконання називають алгоритмічним процесом.

Необхідною умовою, яка задовольняє алгоритм, є детермінованість, або визначеність. Це означає, що виконання команд алгоритму відбувається у єдиний спосіб та призводить до однакового результату для однакових вхідних даних
Для того щоб почати розробляти програму необхідно спочатку задатися базовим алгоритмом роботи пристрою, необхідним для розуміння процесів виконання різних ситуацій (рисунок 2.19). Базовий алгоритм роботи пристрою контролю доступу представлено в додатку В.

Для написання програми скористаємося спеціально розробленим середовищем розробки Arduino IDE, яка поширюється у вільному доступі в мережі Інтернет і яку можна знайти на офіційному сайті розробника www.arduino.cc. У підсумку, після тривалого процесу розробки шляхом проб і помилок була складена програма, за допомогою якої можна реалізувати основний функціонал роботи електронного замку на основі Arduino Uno R3. Для правильної роботи програми необхідно заздалегідь встановити кілька сторонніх бібліотек або через програму «Arduino» - «Скетч» - «Підключити бібліотеку» - «Керувати бібліотеками» - «Пошук», або через ресурси мережі Інтернет, встановивши її по шляху «Arduino» - « скетч »-« Підключити бібліотеку »-« Додати .ZIP бібліотеку ». Необхідні сторонні бібліотеки для роботи з програмою: «Keypad», «Password», «MFRC522», «LCD_1602_RUS», «Bounce2». Лістинг програма, що реалізує потенціал пристрою контролю доступу в приміщення наведена в додатку Г.

3.4 Розробка та налагодження програмного забезпечення

Arduino використовує власну середу розробки Arduino IDE, що складається з вбудованого текстового редактора програмного коду, області повідомлень, вікна виведення тексту (консолі), панелі інструментів і декількох меню . Для завантаження програм і зв'язку середовище розробки підключається до апаратної

частини Arduino за допомогою інтерфейсу USB. Мовою програмування вибрана мова, заснований на C / C ++, як єдиний можливий варіант для обраної середовища програмування. Для написання програми для МК обрана Arduino IDE версії 1.8.12. на момент розробки дана версія є новітньою і стабільної

В ході практичної роботи і створення моделі електронного пристрою контролю доступу, виникли деякі проблеми, а також нові ідеї щодо модернізації програмної частини. Зокрема, була проведена заміна робочої бібліотеки RFID з Rfid.h на MFRC522, у якій функціонал перевершував попередню бібліотеку. Потім була додана окрема функція squeaker (), за допомогою якої було простіше і зручніше налаштовувати пьезодінамік. На платі мікроконтролера Arduino UNO R3 присутні два додаткових входу SDA і SCL, що дозволяють працювати по протоколу I2C з різними пристроями, в нашому випадку, з дисплеєм LCD1602. Зміни відбулися і з інформацією, яка виводилася на дисплей. Спочатку все символи, що виводяться під час роботи пристрою, були записані латинськими літерами. Вирішити це питання допомогла стороння бібліотека LCD_1602_RUS.h, що дозволяє використовувати кирилицю. В кінцевому підсумку, найголовнішим рішенням було додавання програмної роботи з незалежною перезаписуючою пам'яттю EEPROM мікроконтролера, внаслідок чого ідентифікаційні номери RFID-міток, а потім і кодова комбінація, що вводиться за допомогою матричної клавіатури. Вони стали записуватися в цю незалежну пам'ять і при роботі програми виводитися в послідовний порт персонального комп'ютера, а не здаватися в самій програмі, як було раніше. Разом з EEPROM була додана спеціальна кнопка скидання пам'яті мікроконтролера, яка заміняла б всі дані в EEPROM на нульові значення, крім значень, використовуваних в паролі.

Тепер слід перевірити основні етапи роботи пристрою контролю доступу. На рисунку 3.25 показана інформація, яка виводиться в послідовний порт комп'ютера. Інформацію з послідовного порту можна відобразити на екрані монітора, зайшовши в середу розробки Arduino IDE, в рядку «Інструменти» - «Порт» вказати номер COM порту, до якого підключений мікроконтролер, а

потім в рядку «Інструменти» - «Монітор порту», що дозволить вивести інформацію на екран монітора.

```
Start

KEYS COUNT: 1
------------------------------
KEY: 0 | 60 121 172 213
------------------------------

PASSWORD: 1204
------------------------------
```

Рисунок 3.25 — Інформація, яка вказує кількість доступних системі ключів, їх ідентифікаційний номер, а також пароль

При запуску програми з чистою EEPROM пам'яттю, або ж коли вона була очищена за допомогою спеціальної кнопки скидання, на екрані відобразиться інформація, представлена на рисунку 3.26. В цьому випадку контакти реле будуть замкнуті, таким чином моделюючи відкритий стан, програма запросить прикласти RFID-ключ до зчитувача, який згодом і стане майстер-ключем.

```
Memory cleaning is completed


Start

The master key is not in memory. The first presentation to the key will be the master!
```

Рисунок 3.26 — Інформація, яка вказує, що в пам'яті відсутні RFID-мітки.

При установці майстер-ключа, програма запише його ідентифікаційний номер і вкаже на його приналежність (рисунок 3.27).

```
UID: 60 121 172 213
master key is created
```

Рисунок 3.27 — Створення мастер-ключа

Майстер-ключ дозволяє вносити в пам'ять мікроконтролера нові ключі при його утриманні у зчитувача, а також виходити з цього режиму програмування за той же час утримання. В цей час реле замикає свої контакти, і не розмикає до тих пір, поки не відбудеться вихід з режиму програмування нових ключів (рисунок 3.28). Весь цей етап супроводжується звуковими сигналами і повідомлення на дисплеї

```
UID: 60 121 172 213
MASTER PROGRAMMING MODE ON

UID: 101 229 204 101
add key in eeprom

KEYS COUNT: 2
------------------------------
KEY: 0 | 60 121 172 213
KEY: 1 | 101 229 204 101
------------------------------

UID: 60 121 172 213
MASTER PROGRAMMING MODE OFF
```

Рисунок 3.28 - Режим програмування

Введення вірною кодової комбінації або одного із записаних в пам'яті ключів супроводжуються характерними звуковими сигналами, інформації на дисплеї (рисунок 3.29), а також замиканням контактів реле і спрацьовуванні зеленого світлодіода протягом п'яти секунд, після система приходить в початкове положення. Неправильний код або невідомий ключ змушують систему реагувати негативно: недоступні на короткий проміжок часу, відтворюється характерний звуковий сигнал, на екрані дисплея з'являється повідомлення «Доступ запрещен», після цього система повертається до вихідної позиції.

Рисунок 3.29 — Інформація на диплеї при правильному рішенні

Кодова комбінація «0000» дозволяє входити в режим зміни пароля. Після цього дається три спроби на введення попередньої комбінації, інакше виводиться повідомлення, зображене на рисунку 3.30.

```
Pass 7777
Attention!_3xWrong_Pass for change pas - cancel change pass
Access denied!
```

Рисунок 3.30 - Повідомлення на спробу введення неправильного пароля втретє

При зміні пароля також неприпустимим є комбінація «0000», а також колишній пароль. У цьому випадку на дисплеї відображається повідомлення «Старий пароль», але програма дозволяє ввести новий. Коли нова комбінація успішно введена, загоряється зелений світлодіод, потім система переходить в початковий стан.

3.5 Інструкція по використанню пристрою

Для початку роботи з пристроєм контролю доступу (електронним замком), необхідно підключити мікроконтролер Arduino UNO R3 до персонального

комп'ютера через USB-кабель для того, щоб спостерігати інформацію, що надходить від пристрою. При підключенні харчування загоряться червоні світлодіоди у реле і RGB-світлодіоди, а на екрані дисплея LCD1602 з'явиться повідомлення - «Очікування дії». Якщо EEPROM пам'ять мікроконтролера очищена і не містить ніяких даних, крім 0, пристрій попросить ввести початковий майстер-ключ, на дисплеї з'явиться повідомлення «Введіть майстер ключ», контакти реле будуть розімкнуті - загориться зелений світлодіод реле. Для установки першого майстер-ключа необхідно піднести RFID-позначку до зчитувача RC522. Після цього система видасть інформацію про ідентифікаційний номер ключа в послідовний порт комп'ютера, контакти реле замкнуться, зелений світлодіод реле згасне, кілька разів пролунає пьезодінамік, на дисплеї з'явиться повідомлення «Очікування дії» до тих пір, поки не буде здійснено будь-яку дію з боку користувача. Для введення пароля необхідно використовувати матричну клавіатуру. При натисканні на будь-яку кнопку пьезодінамік видаватиме звуковий сигнал, а на дисплеї відобразиться введене значення в вигляді «*». Якщо ввести неправильний пароль, то на екрані дисплея з'явиться повідомлення - «Неправильний пароль». Якщо ви неправильно введете пароль три рази, прозвучить характерний звуковий сигнал і на дисплеї з'явиться повідомлення «Доступ заборонений», і протягом п'яти секунд мікроконтролер не реагуватиме на будь-які дії. Якщо ввести правильну кодову комбінацію, загориться зелений світлодіод, контакти реле розімкнуться, на дисплеї з'явиться повідомлення «Доступ дозволено». Якщо ввести комбінацію «0000», стане можливим зміна пароля. Для цього необхідно за три спроби ввести колишню комбінацію, а потім новий пароль, інакше пристрій вийде з режиму зміни пароля і не буде доступно протягом п'яти секунд.

Якщо до зчитувача RC522 піднести майстер-ключ, то система спрацює аналогічно дії з вірним паролем. При утриманні майстер ключа у зчитувача протягом певного відрізка часу стане доступним режим програмування нових ключів, контакти реле будуть розімкнуті, моделюючи відкритий стан двері. У режимі програмування можна додавати нові ключі. Після цього майстер-ключ

утримується ще певний проміжок часу, за яким слід вихід пристрою з режиму програмування. На невідомі ключі система спрацьовує аналогічно введенню неправильного пароля три рази.

Для скидання всіх відомих ключів необхідно утримувати спеціальну кнопку скидання протягом п'яти секунд. Після цього пам'ять мікроконтролера буде очищена, за винятком кодової комбінації, пристрій зажадає встановити перший майстер-ключ. Скидання необхідне в тому випадку, якщо втрачено колишній майстер-ключ. Пароль і всі відомі ключі відображаються через послідовний порт підключення до комп'ютера при використанні функції «Монітор порту» в програмному середовищі Arduino IDE.

4 ЕКОНОМІЧНА ЧАСТИНА

4.1 Оцінювання комерційного потенціалу розробки.

Результатом магістерської кваліфікаційної роботи «Система безпеки цивільних та виробничих об’єктів на базі мікропроцесорної платформи» є розробка мікропроцесорного засобу, який дозволяє забезпечити контроль доступу та моніторинг персоналу в приміщенні. Метою проведення технологічного аудиту є оцінювання комерційного потенціалу розробки, створеної в результаті науково-технічної діяльності. Для проведення технологічного аудиту було залучено двох експертів. У нашому випадку такими експертами є: Азарова Анжеліка Олексіївна (к.т.н., проф. кафедри), Богомолов Сергій Віталійович (к.т.н., доц. кафедри).

Оцінювання комерційного потенціалу буде здійснене за критеріями, що наведені в таблиці 4.1.

Таблиця 4.1 - Критерії оцінювання комерційного потенціалу розробки бальна оцінка

Бали (за 5-ти бальною шкалою)					
Критерій	0	1	2	3	4
Технічна здійсненність концепції					
1	Достовірність концепції не підтверджена	Концепція підтверджена експертними висновками	Концепція підтверджена розрахунками	Концепція перевірена на практиці	Перевірено роботоздатність продукту в реальних умовах
Ринкові переваги					
2	Багато аналогів на малому ринку	Ринкові п Мало аналогів на малому ринку	Кілька аналогів на великому ринку	Один аналог на великому ринку	Продукт не має аналогів на великому ринку
3	Ціна продукту значно вища за ціни аналогів	Ціна продукту дещо вища за ціни аналогів	Ціна продукту приблизно дорівнює цінам аналогів	Ціна продукту дещо нижче за ціни аналогів	Ціна продукту значно нижче за ціни аналогів

Продовження таблиці 4.1

Бали (за 5-ти бальною шкалою)					
Критерій	0	1	2	3	4
4	Технічні та споживчі властивості продукту значно гірші, ніж в аналогів	Технічні та споживчі властивості продукту трохи гірші, ніж в аналогів	Технічні та споживчі властивості продукту на рівні аналогів	Технічні та споживчі властивості продукту трохи кращі, ніж в аналогів	Технічні та споживчі властивості продукту значно кращі, ніж в аналогів
5	Експлуатаційні витрати значно вищі, ніж в аналогів	Експлуатаційні витрати дещо вищі, ніж в аналогів	Експлуатаційні витрати на рівні експлуатаційних витрат аналогів	Експлуатаційні витрати трохи нижчі, ніж в аналогів	Експлуатаційні витрати значно нижчі, ніж в аналогів
Ринкові перспективи					
6	Ринок малий і не має позитивної динаміки	Ринок малий, але має позитивну динаміку	Середній ринок з позитивною динамікою	Великий стабільний ринок	Великий ринок з позитивною динамікою
7	Активна конкуренція	Активна конкуренція	Помірна конкуренція	Незначна конкуренція	Конкурентів немає
Практик на здійсненність					
8	Відсутні фахівці як з технічної, так і з комерційної реалізації ідеї	Необхідно наймати фахівців або витрачати значні кошти та час на навчання наявних фахівців	Необхідне незначне навчання фахівців та збільшення їх штату	Необхідне незначне навчання фахівців	Є фахівці з питань як з технічної, так і з комерційної реалізації ідеї
9	Потрібні значні фінансові ресурси, які відсутні. Джерела фінансування ідеї відсутні	Потрібні незначні фінансові ресурси. Джерела фінансування відсутні	Потрібні значні фінансові ресурси. Джерела фінансування є	Потрібні незначні фінансові ресурси. Джерела фінансування є	Не потребує додаткового фінансування
10	Необхідна розробка нових матеріалів	Потрібні матеріали, що використовуються у військово-промисловому комплексі	Потрібні дорогі матеріали	Потрібні досяжні та дешеві матеріали	Всі матеріали для реалізації ідеї відомі та давно використовуються
11	Термін реалізації ідеї більший за 10 років	Термін реалізації ідеї більший за 5 років. Термін окупності інвестицій більше 10-ти років	Термін реалізації ідеї від 3-х до 5-ти років. Термін окупності інвестицій більше 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій від 3-х до 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій менше 3-х років

Закінчення таблиці 4.1

Бали (за 5-ти бальною шкалою)					
Критерій	0	1	2	3	4
12	Необхідна розробка регламентних документів та отримання великої кількості дозвільних документів на виробництво та реалізацію продукту	Необхідно отримання великої кількості дозвільних документів на виробництво та реалізацію продукту, що вимагає значних коштів та часу	Процедура отримання дозвільних документів для виробництва та реалізації продукту вимагає незначних коштів та часу	Необхідно тільки повідомлення відповідним органам про виробництво та реалізацію продукту	Відсутні будь-які регламентні обмеження на виробництво та реалізацію продукту

Результати оцінювання комерційного потенціалу експертами розробки зведено в таблицю 4.2.

Таблиця 4.2 - Результати оцінювання комерційного потенціалу розробки

Критерії оцінювання	Експерти	
	Експерт 1	Експерт 2
	Бали	
Технічна здійсненність концепції	4	3
Наявність аналогів на ринку	3	3
Цінова політика	3	4
Технічні та споживчі властивості виробу	3	4
Експлуатаційні витрати	4	3
Ринок збуту	3	4
Конкурентоспроможність	2	3
Фахівці з технічної і комерційної реалізації	4	3
Фінансування	3	4
Матеріально-технічна база	3	3
Термін реалізації ідеї	3	3
Супровідна документація	4	4
Сума	39	41
Середньоарифметична сума балів	40	

За даними таблиці 4.2 можна зробити висновок, щодо рівня комерційного потенціалу розробки. Зважимо на результат й порівняємо його з рівнями комерційного потенціалу розробки, що представлено в таблиці 4.3.

Таблиця 4.3 – Рівні комерційного потенціалу розробки

Середньоарифметична сума балів $\overline{СБ}$, розрахована на основі висновків експертів	Рівень комерційного потенціалу розробки
0 – 10	Низький
11 – 20	Нижче середнього
21 – 30	Середній
31 – 40	Вище середнього
41 – 48	Високий

Рівень комерційного потенціалу розробки, становить 40 балів, що відповідає рівню «вище середнього».

Розробка є модифікацією існуючих пристроїв на ринку, але застосовані в ній моделі та методи є новими в даній предметній області. Відмінними рисами розробки є: простота й зручність у використанні, висока якість та розвинений функціонал. Дану розробку планується реалізовувати на вітчизняному ринку. Розробка готова і знаходиться на стадії дослідного зразка.

З метою мінімізації витрат на розподіл інноваційної методики на ринку обираємо прямий канал збуту – «виробник-споживач», що забезпечить економічну ефективність операцій продажу інноваційної розробки за рахунок уникнення залучення торговельних посередників, проміжних збутових ланок і різниця між ціною продажу розробки та її собівартістю дозволить покрити витрати на прямий збут. На початковому етапі збуту розповсюдження

пристрою можна здійснити безпосередньо завдяки розміщенню рекламних оголошень в Internet.[16]

Врахувавши цінову політику на ринку, а також конкуренцію можна зробити висновок, що постачати розробку необхідно за ціною яка буде на 20-30% нижчою ринкової.

4.2 Прогнозування витрат на виконання науково-дослідної роботи та впровадження її результатів.

Прогнозування витрат на виконання науково-дослідної роботи складається з таких етапів:

— розрахунок витрат, які безпосередньо стосуються виконавців даного розділу роботи;

— розрахунок загальних витрат на виконання даної роботи;

— прогнозування загальних витрат на виконання та впровадження результатів даної роботи.

Основна заробітна плата для розробника розраховується за формулою:

$$З_о = \frac{М}{Т_р} \cdot t, [грн], \quad (4.1)$$

де М — місячний посадовий оклад конкретного розробника, М= 9000 грн.;

$Т_р$ — кількість робочих днів у місяці, $Т_р$ = 21 день;

t — число днів роботи розробника, t = 35 дні.

$$З_о = \frac{9000,00}{21} \cdot 35 = 15000 \text{ (грн)}.$$

Результати розрахунків зведемо до таблиці 4.5.

Таблиця 4.5 – Основна заробітна плата розробників

Найменування посади	Місячний посадовий оклад, грн.	Оплата за робочий день, грн.	Число днів роботи	Витрати на заробітну плату, грн.
Розробник	9000	428,57	35	15000,00
Керівник проекту	14000	666,67	5	3333,35
Всього				18333,35

Додаткова заробітна плата розраховується як 12 % від суми основної заробітної плати за формулою:

$$З_д = 0,12 \cdot З_о \text{ [грн]}. \quad (4.2)$$

$$З_д = 0,12\ 18333,35 = 2200,00 \text{ (грн)}.$$

Нарахування (ЄСВ) на заробітну плату становлять 22%:

$$H_{зп} = (З_о + З_р) \cdot \frac{\beta}{100}, \text{ [грн]}, \quad (4.3)$$

де Зо — основна заробітна плата розробників, грн;

Зд — додаткова заробітна плата всіх розробників, грн;

β — ставка єдиного соціального внеску на загальнообов'язкове державне соціальне страхування, %.

$$Н_{зп} = (18333,35+2200,00)\ 0,22 = 4517,33 \text{ (грн)}.$$

Амортизація обладнання та приміщення, яке використовувалось для проведення розробки, розраховується за формулою:

$$A = \frac{Ц \cdot H_a}{100} \cdot \frac{T}{12} \text{ [грн]}, \quad (4.4)$$

де Ц — балансова вартість обладнання, грн.;

$Н_а$ — річна норма амортизаційних відрахувань;

Т — термін використання під час розробки, місяців.

Норма амортизації розраховується за формулою:

$$H_a = \frac{B_п - B_л}{B_п \cdot T_{кв}} \cdot 100 \text{ [грн]}, \quad (4.5)$$

де $В_п$ і $В_л$ — відповідно первісна та ліквідаційна вартість основних фондів;

$Т_{кв}$ — строк корисного використання, 5 роки.

Норма амортизаційних витрат становитиме:

$$H_a = \frac{10000 - 1000}{10000 \cdot 5} \cdot 100 = 18\%$$

Розрахуємо амортизаційні витрати на ноутбук, балансова вартість якого становить 10000 грн, а термін використання – 3 місяців:

$$A = \frac{10000 \cdot 18}{100} \cdot \frac{3}{12} = 450(\text{грн}).$$

Зроблені розрахунки наведено у таблиці 4.5.

Таблиця 4.5 Амортизаційні відрахування

Найменування	Балансова вартість, грн	Термін використання, р	Фактична трив. використання, міс.	Величина амортизаційних відрахувань, грн
Ноутбук	10000,00	5	3	450,00
Офісне приміщення	110000,00	15	3	1650,00
Всього:				2100,00

Інформацію про витрати на матеріали та комплектуючі, що використані при розробці внесено до таблиці 4.6 та 4.7.

Таблиця 4.6 Витрати на матеріали, що були використані для розробки продукту.

Найменування матеріалу	Одиниці виміру	Ціна за одиницю, грн	Витрачено, шт	Вартість витрачених матеріалів, грн
Папір	уп.	110	1	110
Ручка	шт.	20	2	40
Олівець	шт.	10	1	10
Загальна сума витрат за статтею				160

Таблиця 4.7 – Витрати на матеріали, що були використані для розробки продукту.

Найменування	Вартість, грн
Arduino UNO	145
RFID модуль RC522	50
LCD дисплей 1602	84
Матрична клавіатура	92
RGB-світлодіод KY-016	38
Одноканальне реле	24
Пєзодинамік	10
Всього, грн.	443

Розрахунок витрат на силову електроенергію ($В_е$) здійснюється за формулою:

$$В_е = В \cdot П \cdot Ф \cdot К_п, [грн], \quad (4.6)$$

де В — вартість 1 кВт-год. електроенергії, становить 1,7 грн./кВт.

П — установлена потужність комп'ютера, кВт (у нашому випадку становить 0,5 кВт);

Ф — фактична кількість годин роботи обладнання.

$К_п$ — коефіцієнт використання потужності, становить 0,3.

$$В_е = 1{,}7 \cdot 0{,}5 \cdot 528 \cdot 0{,}3 = 135 \text{ (грн)}.$$

Інші витрати $В_{ін}$ охоплюють: витрати на управління організацією, Інтернет, оплату службових відряджень, витрати на утримання, ремонт та експлуатацію основних засобів, витрати на опалення, освітлення,

водопостачання, Інтернет послуги. Інші витрати $І_в$ можна прийняти як 150% від суми основної заробітної плати розробника:

$$В_{ін} = 150\% \cdot (З_р) \text{ [грн]}. \quad (4.7)$$

$$В_{ін} = 1,5 \cdot 18333,35 = 27500,02 \text{ (грн)}.$$

Сума всіх попередніх статей витрат дає витрати на виконання даної частини (розділу, етапу) роботи – В:

В = 18333,35+2200 +4517,33 +2100+160+443+135+27500,02=55388,7 (грн).

Розраховуємо загальні витрати на виконання даної роботи $В_{заг}$ за формулою:

$$B_{заг} = \frac{B}{\alpha} \text{ [грн]}, \quad (4.8)$$

де α — частка витрат, які безпосередньо здійснює виконавець даного етапу роботи, у відносних. одиницях (α= 1.)

$$В_{заг.} = \frac{55388,7}{1} = 55388,7 \text{ (грн)}.$$

Визначаємо загальні витрати на виконання та впровадження результатів виконаної наукової роботи (ЗВ) за формулою:

$$ЗВ = \frac{B_{заг}}{\beta} \text{ [грн]}, \quad (4.9)$$

де β — коефіцієнт, який характеризує етап (стадію) виконання даної роботи – 0,5.

$$ЗВ = \frac{55388,7}{0,5} = 110777,4 \text{ (грн)}.$$

Витрати на виконання наукової роботи та впровадження її результатів становитиме 110777,4 грн.

4.3 Прогнозування комерційних ефектів від реалізації результатів розробки

У даному підрозділі кількісно спрогнозуємо, яку вигоду можна отримати у майбутньому від впровадження результатів виконаної наукової роботи. Розрахуємо збільшення чистого прибутку підприємства $\Delta П_i$, для кожного із років, протягом яких очікується отримання позитивних результатів від впровадження розробки, за формулою

$$\Delta П_i = \sum_{1}^{n} \left(\Delta Ц_o \cdot N + Ц_o \cdot \Delta N \right)_i \cdot \lambda \cdot \rho \cdot \left(1 - \frac{\upsilon}{100} \right), \tag{4.10}$$

де $\Delta Ц_0$ — покращення основного оціночного показника від впровадження результатів розробки у даному році.

N — основний кількісний показник, який визначає діяльність підприємства у даному році до впровадження результатів наукової розробки;

ΔN — покращення основного кількісного показника діяльності підприємства від впровадження результатів розробки:

$Ц_o$ — основний оціночний показник, який визначає діяльність підприємства у даному році після впровадження результатів наукової розробки;

n — кількість років, протягом яких очікується отримання позитивних результатів від впровадження розробки:

λ — коефіцієнт, який враховує сплату податку на додану вартість. Ставка податку на додану вартість дорівнює 20%, а коефіцієнт $\lambda = 0{,}8333$.

ρ — коефіцієнт, який враховує рентабельність продукту;

υ — ставка податку на прибуток. У 2020 році — 18%.

Припустимо, що при прогнозованій ціні 4900 грн. за одиницю виробу, термін збільшення прибутку складе 3 роки. Після завершення розробки і її вдосконалення, можна буде підняти його ціну на 200 грн. Кількість одиниць реалізованої продукції також збільшиться: протягом першого року — на 150 шт., протягом другого року — на 200 шт., протягом третього року на 250 шт. До моменту впровадження результатів наукової розробки реалізації продукту не було:

$\Delta П_1 = (0 \cdot 200 + (4900 + 200) \cdot 150) \cdot 0{,}8333 \cdot 0{,}25) \cdot (1 - 0{,}18) = 125562{,}495$ грн.

$\Delta П_2 = (0 \cdot 200 + (4900 + 200) \cdot (150+200) \cdot 0{,}8333 \cdot 0{,}25) \cdot (1 - 0{,}18) = 304937{,}488$ грн.

$\Delta П_3 = (0 \cdot 200 + (4900 + 200) \cdot (150+200+250) \cdot 0{,}8333 \cdot 0{,}25) \cdot (1 - 0{,}18) = 522749{,}979$ грн.

Отже, комерційний ефект від реалізації результатів розробки за три роки складе 953249,96 грн.

4.4 Розрахунок ефективності вкладених інвестицій та періоду їх окупності

Теперішня вартість інвестицій PV, що вкладається в наукову розробку можна вважати прогнозовану величину загальних витрат ЗВ на виконання та впровадження результатів МКР, розраховану раніше за формулою (4.9), тобто будемо вважати, що ЗВ = PV = 110777,4 грн.

Очікуване збільшення прибутку – додатковий прибуток ДП, що його отримає науковець-розробник від впровадження результатів наукової розробки, для кожного із років, починаючи з першого року впровадження. Таке збільшення прибутку також було розраховане нами раніше за формулою (4.9). Розрахуємо абсолютну ефективність вкладених інвестицій $Е_{абс}$ згідно наступної формули:

$$E_{abc} = (ПП - PV)\,(\text{грн.}) \qquad (4.11)$$

де ПП — приведена вартість всіх чистих прибутків, що їх отримає підприємство від реалізації результатів наукової розробки, грн;

$$ПП = \sum_{1}^{T} \frac{\Delta П_i}{(1+\tau)^t}, \quad (4.12)$$

де $\Delta П_i$ – збільшення чистого прибутку у кожному із років, протягом яких виявляються результати виконаної та впровадженої МКР, грн;

Т — період часу, протягом якою виявляються результати впровадженої МКР, роки;

τ – ставка дисконтування, за яку можна взяти щорічний прогнозований рівень інфляції в країні; для України цей показник знаходиться на рівні 0,1;

t — період часу (в роках).

Збільшення прибутку ми отримаємо починаючи з першого року:

ПП = (125562,495 / $(1+0,1)^1$) + (304937,488 / $(1+0,1)^2$) + (522749,979 / $(1+0,1)^3$) = 114147,72 + 252014,453 + 392749,796 = 758911,9719 грн.

Так як період часу розробки інноваційного продукту є відносно незначним і складає 35 днів (див. табл. 4.1), то, для спрощення розрахунків ним можна знехтувати, і тому життєвий цикл наукової розробки буде дорівнювати періоду отримання прибутків. Вісь часу, що характеризує рух платежів буде мати вигляд, представлений на рисунку 4.1.

Рисунок 4.1. Вісь часу з фіксацією платежів, що мають місце під час розробки та впровадження результатів НДДКР

$$E_{абс} = 758911,97 - 110777,4 = 648134,57 \text{ грн.}$$

Оскільки $E_{абс} > 0$ то вкладання коштів на виконання та впровадження результатів даної МКР може бути доцільним.

Розрахуємо відносну (щорічну) ефективність вкладених в наукову розробку інвестицій $E_в$. Для цього використаємо формулу:

$$E_в = \sqrt[T_ж]{1 + \frac{E_{абс}}{PV}} - 1, \qquad (4.13)$$

$T_ж$ – життєвий цикл наукової розробки, роки.

$E_в = \sqrt[3]{1 + 648134,57 / 110777,4} - 1 = 0,9$

Визначимо мінімальну ставку дисконтування, яка у загальному вигляді визначається за формулою:

$$\tau = d + f, \tag{4.14}$$

де d — середньозважена ставка за депозитними операціями в комерційних банках; в 2020 році в Україні d = (0,14…0,2);

f— показник, що характеризує ризикованість вкладень; зазвичай, величина f = (0,05...0,1).

$$\tau_{\min} = 0{,}14 + 0{,}05 = 0{,}19.$$

Так як $E_в > \tau_{min}$, то інвестор може бути зацікавлений у фінансуванні даної наукової розробки.

Розрахуємо термін окупності вкладених у реалізацію наукового проекту інвестицій за формулою:

$$T_{ок} = \frac{1}{E_в}, \tag{4.15}$$

$$T_{ок} = 1 / 0{,}9 = 1{,}11 \text{ р.}$$

Оскільки $T_{ок}$ < 3-х років, а саме термін окупності рівний 1,11 роки, то фінансування даної наукової розробки є доцільним.

ВИСНОВКИ

У магістерській кваліфікаційній роботі здійснено розробку, створення робочої програми, виготовлення, налагодження та діючого макету пристрою контролю доступу в приміщення на мікропроцесорній платформі.

Макет пристрою дозволяє змоделювати основні функції та завдання з контролю доступу в різні приміщення за допомогою введення кодової комбінації через матричну клавіатуру, або радіочастотної мітки, яку використовують як ключ-карти. Модуль реле і підключений до його контактів електромагніт симулюють відкритий чи закритий стан двері в приміщення. При втраті майстер-ключа передбачено скидання пам'яті мікроконтролера з метою вказівки нового майстер-ключа, використовуваного для введення нових карт доступу.

Вся налагоджувальна інформація буде надходити на комп'ютер тільки при підключенні до нього мікроконтролера через USB-інтерфейс. Таким чином, пристрій може працювати автономною через підключений адаптер змінного струму, але в цьому випадку стає недоступною налагоджувальна інформація.

Основною метою даної роботи було створення макета пристрою контролю доступу на мікропроцесорній платформі що забезпечує безпеку контролю доступу до приміщення.

У цієї випускної кваліфікаційної роботі була розроблена система автоматичної реєстрації робочого персоналу на основі Arduino.

Розроблена система відповідає всім висунутим вимогам, а також має ряд переваг, таких як низька вартість, в порівнянні з аналогами, компактність і простота використання

Роботу виконано відповідно до технічного завдання, а для досягнення поставленої мети виконано всі поставлені задачі.

В результаті економічного аналізу обрахунків показано, що спроектований пристрій дешевший за існуючі аналоги і є конкурентоспроможним.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Цирульник С.М. Проектування мікропроцесорних систем: навчальний посібник/ С.М. Цирульник, Г. Л. Лисенко. – Вінниця: ВНТУ, 2010.– 201 с.
2. Книга по программированию микроконтроллеров [Електронний ресурс] http://cxem.net/mc/book.php
3. Меньков А.В. Теоретические основы автоматизированного управления/ А.В. Меньков, В.А. Острейковский. – Учебник для вузов. – М.: Издательство Оникс, 2005. – 640 с.
4. Харазов В.Г. Интегрированные системы управления технологическими процессами. – СПб.: Профессия, 2009. – 592 с.
5. Береза А. М. Основи створення інформаційних систем: навч. посіб. / А. М. Береза. – 2 вид., перероб. і доп. – К.: КНЕУ, 2001. – 214 с.
6. ДСТУ 2226–93 Автоматизовані системи. Терміни та визначення. – К.: УкрНДІССІ, 1994. – 92 с.
7. Букреев И. Н. Микроэлектронные схемы цифровых устройств / И. Н. Букреев, В. И. Горячев, Б. М. Мансуров. – Москва : Техносфера, 2009. – 712 с.– ISBN 978–5–94836–197–0.
8. Проекты с использованием микроконтролеров. — СПб.: БХВ–Петербург, 2014. — 400 с.: — (Электроника)
9. Бродин В. Б. Системы на микроконтроллерах / В.Б. Бродин, А. В. Калинин – Москва : ЭКОМ, 2002. – 400 с.– ISBN 5–7163–0089–8.
10. Белов А.В. “Разработка устройств на микроконтроллерах AVR: шагаем от чайника до профи” – СПБ.: Наука и техника, 2013. – 528 с.
11. Основи інформаційних систем: Навч. посібник. – Вид. 2–ге, перероб. і доп. / В. Ф. Ситник, Т. А. Писаревська, Н. В. Єрьоміна, О. С. Краєва; За ред. В. Ф. Ситника. — К.: КНЕУ, 2001. — 420 с.
12. Форум обсуждения оборудования«Умный дом» [Електронний ресурс] http://cyber–place.ru/index.php

13. Книга по программированию микроконтроллеров AVR [Електронний ресурс] http://cxem.net/mc/book.php
14. Букреев И. Н. Микроэлектронные схем ыцифровых устройств / И. Н. Букреев, В. И. Горячев, Б. М. Мансуров. – Москва : Техносфера, 2009. – 712 с.- ISBN 978-5-94836-197-0.
15. Небава М. І. Економіка та організація виробничої діяльності підприємства. Ч.1. Економіка підприємства: Навчальний посібник / Небава М. І., Адлер О. О., Лесько О.Й. – Вінниця: ВНТУ, 2011. – 117 с.
16. Небава М. І. Економіка та організація виробничої діяльності підприємства. Ч.2. Організація виробництва: Навчальний посібник / Небава М. І., Адлер О. О., Лесько О.Й. – Вінниця: ВНТУ, 2011. – 131 с.
17. Васильков В. Г. Організація виробництва: Навч. посібник / Васильков В. Г. –К: КНЕУ, 2003. –524 с.
18. Економіка підприємства: підручник / [за ред. С. Ф. Покропивного]. –[Вид. 2-ге, перераб. та доп.] – К.: КНЕУ, 2005. – 528 с.

ДОДАТОК А

Міністерство освіти та науки України

Вінницький національний технічний університет

Інститут інформаційних технологій та комп'ютерної інженерії

ЗАТВЕРДЖУЮ

Завідувач кафедри ОТ

д.т.н., професор Мартинюк Т. Б._____

(наук. ст., вч. зв., ініц. та прізв.) (підпис)

"____" _____20__р.

ТЕХНІЧНЕ ЗАВДАННЯ

на виконання магістерської кваліфікаційної роботи

Система безпеки цивільних та виробничих об'єктів на базі мікропроцесорної платформи

08–23.МКР.007.00.000.ТЗ

Науковий керівник: к.т.н., проф. Азарова А.О.

_____

(підпис)

студент групи _КІ-18м_

_____ Рознюк Р. О.

(підпис)

Вінниця 2020р.

1. Підстава для виконання магістерської кваліфікаційної роботи (МКР)

а) актуальність досліджень;

б) наказ про затвердження теми дипломної роботи.

2. Мета і призначення МКР

а) мета – забезпечення опрацювання інформації мікропроцесорною системою із застосуванням RFID технології.

б) призначення розробки – виконання магістерської кваліфікаційної роботи, виконання організаційно – технологічних та наукових досліджень.

3. Вихідні дані для виконання МКР

- технічні характеристики RFID сканерів;
- технічні характеристики мікропроцесорних платформ Arduino;
- опис мікроконтролерів сімейства Atmel;
- середовище розробки ПЗ Arduino IDE для мікроконтролерів Atmel.

4. Вимоги до виконання МКР

- огляд і аналіз методів аутентифікації;
- класифікація методів аутентифікації;
- дослідження способи та методи аутентифікації з використанням RFID технології;
- розробка структурної та принципової схем системи;
- розробка алгоритму роботи та програмного забезпечення для мікропроцесорної системи.

5. Етапи МКР та очікувані результати

№ етапу	Назва етапу	Термін виконання		Очікувані результати
		початок	кінець	
1	Пошук та огляд інформаційних джерел	11.02.19р.	02.03.19р.	Розділ 1
2	Дослідження способів побудови систем аутентифікації	03.03.19р.	30.03.19р.	Розділ 2
3	Побудова мікропроцесорного системи управління	31.03.19р.	27.04.19р.	Розділ 3
4	Економічна частина	28.04.19р.	25.05.19р.	Розділ 4

6. Матеріали, що подаються до захисту МКР

Пояснювальна записка МКР, графічні і ілюстративні матеріали, протокол попереднього захисту МКР на кафедрі, відзив наукового керівника, відзив опонента, протоколи складання державних екзаменів, анотації до МКР українською та іноземною мовами, нормоконтроль про відповідність оформлення МКР діючим вимогам.

7. Порядок контролю виконання та захисту МКР

Виконання етапів графічної та розрахункової документації МКР контролюється науковим керівником згідно зі встановленими термінами. Захист МКР відбувається на засіданні Державної екзаменаційної комісії, затвердженою наказом ректора.

8. Вимоги до оформлення МКР

Вимоги викладені в МЕТОДИЧНИХ ВКАЗІВКАХ до дипломного проектування, ДСТУ_ 3008-95, ДСТУ 3974-2000 «Правила виконання дослідно-конструкторських робіт. Загальні положення» та діючого ГОСТ 2.114-95 ЕСКД.

9. Вимоги щодо технічного захисту інформації в МКР з обмеженим доступом

Відсутні.

ДОДАТОК Б

Розпіновка плати Arduino Uno

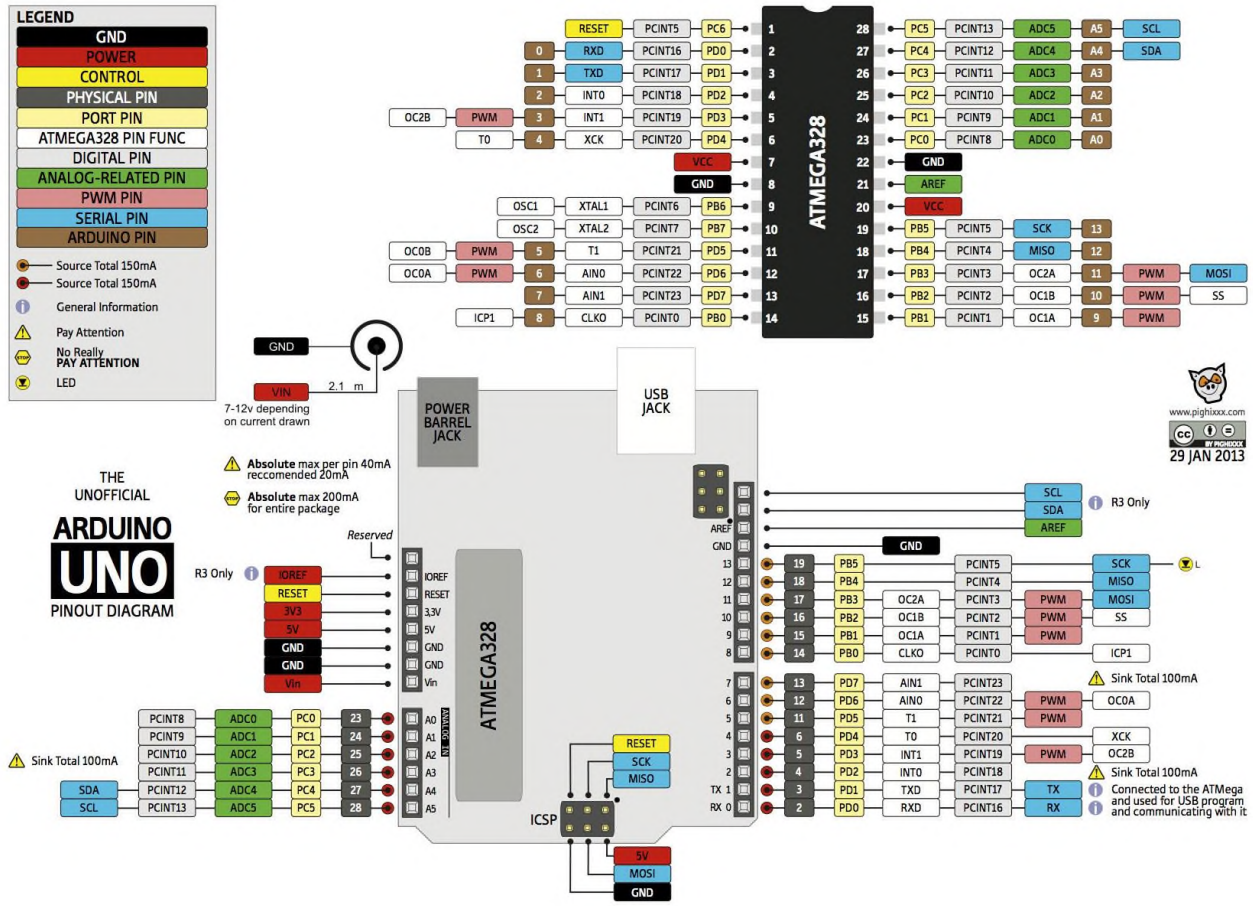

Рисунок Б.1— Розпіновка плати Arduino Uno

					08-23.МКР.007.00.000		
					СИСТЕМА БЕЗПЕКИ ЦИВІЛЬНИХ ТА ВИРОБНИЧИХ ОБ'ЄКТІВ НА БАЗІ МІКРОПРОЦЕСОРНОЇ ПЛАТФОРМИ	Літ.	Маса / Масштаб
Змн.	Арк.	№ докум.	Підпис	Дата			
Розробив		Рознюк Р.О.				Арк.	Аркушів
Керівник		Азарова А.О.					
Рецензент		Дудатьєв А.В					
					Розпіновка плати Arduino UNO	ВНТУ,гр. КІ – 18м	
Н. контроль		Швець С.І.					
Затверджую		Мартинюк Т.Б.					

ДОДАТОК В

Блок-схема алгоритму роботи

Рисунок В.1 — Блок схема алгоритму роботи

					08-23.МКР.007.00.000		
					СИСТЕМА БЕЗПЕКИ ЦИВІЛЬНИХ ТА ВИРОБНИЧИХ ОБ'ЄКТІВ НА БАЗІ МІКРОПРОЦЕСОРНОЇ ПЛАТФОРМИ	Літ.	Маса / Масштаб
Змн.	Арк.	№ докум.	Підпис	Дата			
Розробив		Рознюк Р.О.				Арк.	Аркушів
Керівник		Азарова А.О.					
Рецензент		Дудатьєв А.В			Блок схема алгоритму роботи	ВНТУ,гр. КІ – 18м	
Н. контроль		Швець С.І.					
Затверджую		Мартинюк Т.Б.					

ДОДАТОК Г

Лістинг програмного забезпечення

```
#include <avr/wdt.h>
#include <Wire.h>
#include "LCD_1602_RUS.h"
#include <SPI.h>
#include <MFRC522.h>
#include <Bounce2.h>
#include <EEPROM.h>
#include <Password.h>
#include <Keypad.h>
LCD_1602_RUS lcd(0x27, 16, 2); // инициализация дисплея, 16 столбцов, 2 строки
//Определение основных пинов, к которым подключаются различные модули:
#define PIN_RESET 14 // кнопка для сброса EEPROM
#define PIN_RELAY 6 // подключение реле
#define PIN_TONE 15 // пьезодинамик
#define PIN_RST 9 // RFID RST
#define PIN_SS 10 // RFID SS
#define RED_LED 17 // красный светодиод
#define GREEN_LED 16 //зеленый светодиод
//Инициализация RFID-считывателя:
MFRC522 mfrc522(PIN_SS, PIN_RST);
//Переменные, необходимые для работы со списком RFID-ключей:
byte **keyss;
byte keys_count = EEPROM.read(0);
//Переменные необходимые для режима программирования RFID-меток:
byte modeProgTime = 5; // Количество секунд удержания мастер ключа для входа или выхода из режима программирования
bool mode = false;
byte modeClean = 0;
unsigned long modeTimer = 0;
unsigned long resetTimer = 0;
//Управление замком:
unsigned long openTimer = 0;
//Защита кнопок от дребезга:
Bounce key_reset = Bounce();
Bounce key_open = Bounce();
//Программный reset:
void(* resetFunc) (void) = 0;
//Функция звукового оповещения. Принимает параметры: количество
//звуковых сигналов, частота в герцах, продолжительность звука, пауза в
```

```
//милисекундах (не обязательно):
void squeaker(byte count, unsigned int Hz, unsigned int duration, unsigned int sleep
= 0)
{
for(int i=0; i<count; i++) {
tone(PIN_TONE, Hz, duration);
if(sleep > 0) delay(sleep);
}
}
//Функция для считывания EEPROM и составления списка RFID-ключей.
//Первый байт в памяти содержит количество ключей. UID ключа содержит 4
//байта. Максимум можно записать 254 ключа (255-1 из-за того, что в
//EEPROM записывается кодовая комбинация из 4 символов):
void keysRead() {
//Выводим количество ключей:
Serial.print(F("KEYS COUNT: "));
Serial.println(keys_count);
int eb = 4; // Запись количества доступных ключей производится в
keyss = (byte**)malloc(sizeof(byte*)*keys_count);
// Читаем список ключей из EEPROM:
Serial.println(F("------------------------------"));
for(byte i=0; i<keys_count; i++) {
Serial.print(F("KEY: "));Serial.print(i);Serial.print(" | ");
keyss[i] = (byte*)malloc(sizeof(byte)*4);
for(byte b=0; b<4; b++) {
keyss[i][b] = EEPROM.read(++eb);
Serial.print(keyss[i][b]);
if(b < 3) Serial.print(F(" "));
}
Serial.println();
}
Serial.println(F("------------------------------"));
Serial.println();
}
//Функция вывода пароля, записанного с 1 по 5 ячейку памяти, т.к
//переменные записываются в типе char, то нужно перевести код ASCII в
//десятичный. Для цифр от 0 до 9 это можно сделать просто вычитанием из
//полученного результата числа 48:
void passRead() {
Serial.print(F("PASSWORD: "));
Serial.print(EEPROM.read(1)-48);
Serial.print(EEPROM.read(2)-48);
Serial.print(EEPROM.read(3)-48);
Serial.print(EEPROM.read(4)-48);
Serial.println();
```

```
Serial.println(F("--------------------"));
Serial.println(); }
//Функция выводит UID ключа и, при необходимости, сопроводительное
//сообщение:
void uidPrint(String text = "") {
Serial.print(F("UID: "));
for(byte i=0; i<mfrc522.uid.size; i++) {
Serial.print(mfrc522.uid.uidByte[i]);
if(i < mfrc522.uid.size - 1) Serial.print(F(" ")); }
Serial.println();
if(text.length() != 0) Serial.println(text + "\r\n");
}
int presses=0; // количество нажатий
const byte ROWS = 4; // количество строк
const byte COLS = 4; // количество столбцов
// Определение символов матричной клавиатуры:
char keys[ROWS][COLS] =
{
{'1','2','3','A'},
{'4','5','6','B'},
{'7','8','9','C'},
{'*','0','#','D'}
};
//Цифровые входы, к которым подключается матричная клавиатура:
byte rowPins[ROWS] = {2,3,4,18};
byte colPins[COLS] = {5,7,8,19};
//Инициализация матричной клавиатуры:
Keypad keypad = Keypad( makeKeymap(keys), rowPins, colPins, ROWS, COLS );
String pass; //переменная, указывающая код по умолчанию
String summ; //переменная, указывающая уже введенный код
int wrong=0; //количество ошибочных вводов кода (для блокировки)
int shetch=1; //количество набранных символов для смены пароля
int change=0; //флаг проверки кода для смены пароля
int dochange=0; //флаг производится смена пароля
//Функция, запускающаяся только в начале работы микроконтроллера или
//при аппаратном сбросе:
void setup()
{
// Настраиваем сторожевой таймер
wdt_disable();
//delay(8000);
wdt_enable(WDTO_8S);
//Запись исходного пароля в энергонезависимую память, необходимо только
//при первоначальной прошивке, чтобы задать пароль:
//EEPROM.write(1, '1');
```

```
//EEPROM.write(2, '2');
//EEPROM.write(3, '0');
//EEPROM.write(4, '4');
//Запись символов в формате char:
pass = "";
pass = pass+char(EEPROM.read(1));
pass = pass+char(EEPROM.read(2));
pass = pass+char(EEPROM.read(3));
pass = pass+char(EEPROM.read(4));
//Эти строки только для отладки, выводится в COM-порт, к которому
//подключен микроконтроллер:
Serial.println(char(EEPROM.read(1))); // первый знак пароля в
Serial.println(char(EEPROM.read(2))); // второй знак пароля
Serial.println(char(EEPROM.read(3))); // третий знак пароля
Serial.println(char(EEPROM.read(4))); // четвертый знак пароля
Serial.print("Pass "); Serial.println(pass); //весь пароль
//Инициализация используемых входов:
//Реле:
pinMode(PIN_RELAY, OUTPUT);
digitalWrite(PIN_RELAY, HIGH);
//Кнопка для сброса памяти:
pinMode(PIN_RESET,INPUT_PULLUP);
key_reset.attach(PIN_RESET);
key_reset.interval(5);
//Инициализация консоли последовательного вывода данных на экран:
Serial.begin(9600);
while (!Serial);
Serial.println(F("Start\r\n"));
//Инициализация основных модулей:
lcd.init();
lcd.backlight();
SPI.begin();
mfrc522.PCD_Init();
pinMode(RED_LED, OUTPUT);
pinMode(GREEN_LED, OUTPUT);
digitalWrite(RED_LED, HIGH);
digitalWrite(GREEN_LED, LOW);
lcd.setCursor(4,0);
lcd.print(L"ОЖИДАНИЕ");
lcd.setCursor(4,1);
lcd.print(L"ДЕЙСТВИЯ");
//Считываем количество ключей, значение должно быть =>1 т.к первый ключ
//это мастер-ключ. В случае его потери, сбросить EEPROM и создать новый
//мастер-ключ:
if(keys_count > 0 and keys_count < 255) {
```

```
keysRead();
passRead();
}
else {
keys_count = 0; //Определение нового мастер-ключа
Serial.println(F("The master key is not in memory. The first presentation to the key will be the master!\r\n"));
digitalWrite(PIN_RELAY, LOW);
lcd.clear();
lcd.setCursor(4,0);
lcd.print(L"УКАЖИТЕ");
lcd.setCursor(2,1);
lcd.print(L"МАСТЕР-КЛЮЧ");
}
}
//Функция цикла программы:
void loop()
{
// Сбрасываем сторожевой таймер микроконтроллера:
wdt_reset();
if(resetTimer > millis()+10000) resetTimer = 0;
if(openTimer > millis()+10000) openTimer = 0;
char key = keypad.getKey(); //задаем функцию для работы с кнопками клавиатуры
if (key) // если нажата кнопка клавиатуры
{
Serial.println(key);
squeaker(1, 2000, 100);
presses=presses+1; //увеличиваем на единицу счет количества символов
summ=summ+key;
Serial.print("Pass "); Serial.println(summ);
//Вывод на дисплей знаков «*» при нажатии на клавиатуру:
if(presses == 1 or shetch == 1)
{
lcd.clear();
lcd.setCursor(1,0);
lcd.print(" < PIN >");
lcd.setCursor(0,1);
lcd.print("*_");
}
if(presses == 2 or shetch == 2)
{
lcd.clear();
lcd.setCursor(1,0);
lcd.print(" < PIN >");
```

```
lcd.setCursor(0,1);
lcd.print("**_");
}
if(presses == 3 or shetch == 3)
{
lcd.clear();
lcd.setCursor(1,0);
lcd.print(" < PIN >");
lcd.setCursor(0,1);
lcd.print("***_");
}
if(presses == 4 or shetch == 4)
{
lcd.clear();
lcd.setCursor(1,0);
lcd.print(" < PIN >");
lcd.setCursor(0,1);
lcd.print("****");
}
switch (dochange) //ветвление на ввод нового пароля (case 1) и проверку (case
0)
{
case 0: //блок для обычной работы - проверка правильности ввода пароля
//В данном случае кнопки # и * приводят к сбросу количества нажатий:
if (key=='#')
{
summ="";
presses=0;
Serial.println("# for RESET");
squeaker(1, 500, 100);
};
if (key=='*')
{
summ="";
presses=0;
Serial.println("* for ENTER");
squeaker(1, 500, 100);
};
// Если правильный пароль и не было запроса на его смену:
if (summ==pass && change==0) {
Serial.println("PASS OK");
summ="";
presses=0;
wrong=0;
openTimer = millis()/1000;
```

```
squeaker(2, 3500, 200, 100);
digitalWrite(PIN_RELAY, LOW);
allow();
};
//Если нажата комбинация для смены пароля:
if (summ=="0000") {
Serial.println("Change pass go test");
summ="";
presses=0;
wrong=0;
change=1;
squeaker(3, 700, 150);
lcd.clear();
lcd.setCursor(2,0);
lcd.print(L"СМЕНА ПАРОЛЯ");
};
//Если правильный пароль и был запрос на смену кода
if (summ==pass && change==1){
Serial.println("Pass ok go change pass");
summ="";
presses=0;
wrong=0;
dochange=1;
key = keypad.getKey();
squeaker(4, 1000, 50);
lcd.clear();
lcd.setCursor(0,0);
lcd.print(L"СМЕНА РАЗРЕШЕНА");
};
//При смене пароля - если введено полное количество знаков пароля, и он
//ошибочный, формируется звуковой сигнал:
if (wrong==0 && presses==4 && change==1) {
summ="";
presses=0;
wrong=wrong+1;
Serial.println("Wrong_Pass");
squeaker(4, 500, 50);
lcd.clear();
lcd.setCursor(0,0);
lcd.print(L"НЕВЕРНЫЙ ПАРОЛЬ");
};
//При смене пароля - если два раза ошибочный код, формируем звуковые
//сигналы
if (wrong==1 && presses==4 && change==1) {
summ="";
```

```
presses=0;
wrong=wrong+1;
Serial.println("Attention!_2xWrong_Pass for change pas");
squeaker(4, 500, 50);
lcd.clear();
lcd.setCursor(0,0);
lcd.print(L"НЕВЕРНЫЙ ПАРОЛЬ");
lcd.setCursor(3,1);
lcd.print(L"ВТОРОЙ РАЗ");
};
//При смене пароля - если три раза ошибочный код, выходим из режима
//смены пароля:
if (wrong==2 && presses==4 && change==1){
summ="";
presses=0;
wrong=0;
change=0;
Serial.println("Attention!_3xWrong_Pass for change pas - cancel change pass");
squeaker(1, 500, 1000);
denied();
};
//Если введено полное количество знаков пароля, но он ошибочный:
if (presses==4 && change==0){
summ="";
presses=0;
wrong=wrong+1;
Serial.println("Wrong_Pass");
squeaker(1, 500, 300);
lcd.clear();
lcd.setCursor(0,0);
lcd.print(L"НЕВЕРНЫЙ ПАРОЛЬ");
delay(1000);
wait();
};
//Если два раза ошибочный пароль:
if (wrong==2 && presses==0 && change==0) {
Serial.println("Attention!_2xWrong_Pass");
squeaker(1, 500, 500);
lcd.clear();
lcd.setCursor(0,0);
lcd.print(L"НЕВЕРНЫЙ ПАРОЛЬ");
lcd.setCursor(3,1);
lcd.print(L"ВТОРОЙ РАЗ");
delay(1000);
wait();
```

```
};
//Если три раза ошибочный пароль:
if (wrong==3 && presses==0 && change==0) {
summ="";
presses=0;
wrong=0;
Serial.println("Attention!_3xWrong_Pass");
squeaker(1, 500, 1000);
denied();
};
break;
//Вторая часть блока для смены пароля, начало блока для смены пароля и его
//записи в энергонезависимую память:
case 1:
if (key=='#') //если введен символ # сбрасываем код
{
shetch=1;
summ="";
Serial.println("# is not an option, reset");
squeaker(1, 500, 100);
}
else if (key=='*') //если введен символ * сбрасываем код
{
shetch=1;
summ="";
Serial.println("* is not an option, reset");
squeaker(1, 500, 100);
}
else if (shetch==1 && (key)) //Меняем 1-ый символ пароля
{
Serial.print("NewPass_symbol_one "); Serial.println(key);
squeaker(1, 2000, 100);
shetch=2; //увеличиваем на единицу счет количества символов нового пароля
EEPROM.write(1, key);
Serial.println(char(EEPROM.read(1))); //проговариваем первый знак пароля в
порт
}
else if (shetch==2 && (key)) // Меняем 2-ой символ пароля
{
Serial.print("NewPass_symbol_two "); Serial.println(key);
EEPROM.write(2, key);
squeaker(1, 2000, 100);
shetch=3; //увеличиваем на единицу счет количества символов нового пароля
Serial.println(char(EEPROM.read(2))); //проговариваем второй знак пароля в
порт
```

```
}
else if (shetch==3 && (key)) // Меняем 3-ий символ пароля
{
Serial.print("NewPass_symbol_three "); Serial.println(key);
EEPROM.write(3, key);
squeaker(1, 2000, 100);
shetch=4; //увеличиваем на единицу счет количества символов нового пароля
Serial.println(char(EEPROM.read(3))); //проговариваем третий знак пароля в порт
}
else if (shetch==4 && (key)) // Меняем 4-ый символ пароля
{
Serial.print("NewPass_symbol_four "); Serial.println(key);
EEPROM.write(4, key);
squeaker(1, 2000, 100);
Serial.println(char(EEPROM.read(4))); // проговариваем четвертый знак пароля в порт
String passnew = ""; // вводим переменную, содержащую новый введенный пароль
passnew = passnew+char(EEPROM.read(1));
passnew = passnew+char(EEPROM.read(2));
passnew = passnew+char(EEPROM.read(3));
passnew = passnew+char(EEPROM.read(4));
passRead();
if (passnew==pass) // если новый пароль равен старому
{
shetch=1; // запрашиваем другой новый пароль
58
summ="";
Serial.println("NewPass equal old pass, Reset");
squeaker(5, 600, 100);
lcd.clear();
lcd.setCursor(1,0);
lcd.print(L"СТАРЫЙ ПАРОЛЬ");
}
else if (passnew=="0000") // если новый пароль равен комбинации для смены пароля
{
shetch=1; // запрашиваем другой новый пароль
summ="";
Serial.println("NewPass equal 0000, Reset");
squeaker(5, 600, 100);
lcd.clear();
lcd.setCursor(1,0);
lcd.print(L"СТАРЫЙ ПАРОЛЬ");
```

```
}
else {
//Присваиваем паролю значения из энергонезависимой памяти:
pass = "";
pass = pass+char(EEPROM.read(1));
pass = pass+char(EEPROM.read(2));
pass = pass+char(EEPROM.read(3));
pass = pass+char(EEPROM.read(4));
//Вывод в порт пароля для отладки:
Serial.println("Pass read test: ");
Serial.println(char(EEPROM.read(1))); //проговариваем первый знак пароля в порт
Serial.println(char(EEPROM.read(2))); //проговариваем второй знак пароля в порт
Serial.println(char(EEPROM.read(3))); //проговариваем третй знак пароля в порт
Serial.println(char(EEPROM.read(4))); //проговариваем четвертый знак пароля в порт
Serial.print("Pass "); Serial.println(pass); //проговариваем пароль в порт
//Выходим из цикла "case 1":
dochange=0;
change=0;
presses=0;
shetch=1;
summ="";
squeaker(5, 900, 100);
lcd.clear();
lcd.setCursor(2,0);
lcd.print(L"НОВЫЙ ПАРОЛЬ");
digitalWrite(GREEN_LED, HIGH);
digitalWrite(RED_LED, LOW);
delay(3000);
digitalWrite(GREEN_LED, LOW);
digitalWrite(RED_LED, HIGH);
wait();
break;
}
};
//конец блока для смены пароля и его записи в энергонезависимую память
}
}
//Очистка памяти:
key_reset.update();
if(key_reset.read() == HIGH) {
if(resetTimer == 0) resetTimer = millis();
```

```
else {
if((millis()-resetTimer)/1000 > 5) {
Serial.println(F("Launched memory cleaning"));
squeaker(4, 1600, 300, 200);
wdt_disable();
for(int i=5; i<=EEPROM.length(); i++) {
EEPROM.write(i, 0);
if(!(i%50)) Serial.println(F("#")); else Serial.print(F("#"));
}
Serial.println(F("\r\nMemory cleaning is completed\r\n"));
delay(1000);
resetFunc();
60
}
}
}
else if(resetTimer != 0) resetTimer = 0;
//Автоматическое закрытие двери через 5 секунд:
if(openTimer != 0) {
if(millis()/1000 - openTimer > 5) {
openTimer = 0;
digitalWrite(PIN_RELAY, HIGH);
digitalWrite(GREEN_LED, LOW);
digitalWrite(RED_LED, HIGH);
wait();
Serial.println("* closed lock\r\n");
}
}
//Если ключ отсутствует или не читается, не выполняем дальнейший код:
if(!mfrc522.PICC_IsNewCardPresent()) {
//Очистка таймера входа в режим программирования, в случае если
//считыватель свободен:
if(modeTimer != 0) {
if(++modeClean > 5) modeTimer = modeClean = 0;
}
return;
}
if(!mfrc522.PICC_ReadCardSerial()) return;
//Останавливаем режим очистки:
modeClean = 0;
//Создание мастер-ключа:
if(keys_count == 0) {
for(byte i=0; i<4; i++) EEPROM.write(i+5, mfrc522.uid.uidByte[i]);
EEPROM.write(0, keys_count = 1);
uidPrint(F("master key is created"));
```

```
digitalWrite(PIN_RELAY, HIGH);
keysRead();
squeaker(8, 1200, 100, 100);
delay(2000);
return;
}
//Проверка ключа на соответствие:
bool access = false;
bool master = false;
for(byte i=0; i<keys_count; i++) {
for(byte b=0; b<4; b++) {
if(keyss[i][b] != mfrc522.uid.uidByte[b]) break;
if(b == 3) {
access = true;
if(i == 0) master = true;
// Останавливаем проверку
i = keys_count;
}
}
}
//Контроль доступа:
if(access and !mode and !master) {
// Доступ разрешен
openTimer = millis()/1000;
digitalWrite(PIN_RELAY, LOW);
squeaker(2, 3500, 200, 200);
allow();
}
else if(!access and !mode and !master) {
// Доступ запрещен
squeaker(1, 500, 1000);
denied();
}
//Режим программирования - запись ключа:
if(access and mode and !master) {
// Попытка записи существующего ключа
uidPrint(F("error: key already exists in eeprom"));
squeaker(2, 500, 300);
lcd.clear();
lcd.setCursor(1,0);
lcd.print(L"КАРТА ИЗВЕСТНА");
delay(2000);
wait();
}
else if(!access and mode and !master) {
```

```
// Записываем новый ключ
// Максимум 255 ключей (с учетом первого байта)
if(keys_count < 255) {
for(byte i=0; i<4; i++) EEPROM.write(5 + keys_count*4 + i, mfrc522.uid.uidByte[i]);
EEPROM.write(0, ++keys_count);
uidPrint(F("add key in eeprom"));
keysRead();
lcd.clear();
lcd.setCursor(4,0);
lcd.print(L"ПРИЛОЖИТЕ");
lcd.setCursor(2,0);
lcd.print(L"НОВУЮ КАРТУ");
squeaker(2, 2200, 200, 200);
}
else // нет памяти для записи
{
uidPrint(F("error: not enough memory for recording key!"));
squeaker(2, 500, 300);
}
delay(2000);
wait();
}
//Работа с мастер-ключом:
else if(access and master) {
// Мастер ключ в обычном режиме
if(modeTimer == 0) {
modeTimer = millis()/1000;
if(!mode) {
openTimer = millis()/1000;
digitalWrite(PIN_RELAY, LOW);
// Сигнал о наличии мастер ключа в обычном режиме
uidPrint(F("MASTER KEY"));
squeaker(2, 3200, 200, 200);
allow();
}
}
else
{
if(millis()/1000 - modeTimer > modeProgTime and modeTimer != 0)
{
modeTimer = 0;
if((mode = !mode) == true)
{
//Вход в режим программирования:
```

```
digitalWrite(PIN_RELAY, LOW);
uidPrint(F("MASTER PROGRAMMING MODE ON"));
squeaker(4, 1200, 200, 200);
}
else {
// Выход из режима программирования
digitalWrite(PIN_RELAY, HIGH);
uidPrint(F("MASTER PROGRAMMING MODE OFF"));
squeaker(4, 2200, 200, 200);
}
}
delay(5000);
wait();
}
// Мастер ключ удерживается у считывателя на 5 секунд
}
}
//Функция, срабатывающая при верном пароле/ключе:
void allow()
{
Serial.println("Access accept!"); //доступ получен
digitalWrite(GREEN_LED, HIGH);
digitalWrite(RED_LED, LOW);
lcd.clear();
lcd.setCursor(0,0);
lcd.print(L"ДОСТУП РАЗРЕШЕН");
summ="";
presses = 0;
delay(5000);
digitalWrite(GREEN_LED, LOW);
digitalWrite(RED_LED, HIGH);
wait();
}
//Функция, срабатывающая при неправильном пароле/ключе:
void denied()
{
Serial.println("Access denied!"); //доступ закрыт
digitalWrite(RED_LED, HIGH);
lcd.clear();
lcd.setCursor(0,0);
lcd.print(L"ДОСТУП ЗАПРЕЩЕН");
summ="";
presses = 0;
delay(5000);
wait();
```

```
}
//Функция режима ожидания:
void wait()
{
lcd.clear();
lcd.setCursor(4,0);
lcd.print(L"ОЖИДАНИЕ");
lcd.setCursor(4,1);
lcd.print(L"ДЕЙСТВИЯ");
}
```