Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра обчислювальної техніки

БАКАЛАВРСЬКА ДИПЛОМНА РОБОТА

на тему:

Автоматизована система управління пропускною охоронною системою

ПОЯСНЮВАЛЬНА ЗАПИСКА

08-23.БДР.038.00.000 ПЗ

Виконав студент 2 курсу, групи 1КІ-20мс
спеціальності 123 - Комп'ютерна інженерія
Твердохліб Н.М.

Керівник роботи к.т.н., доц. каф. ОТ
Богомолов С.В.
"16" 06 2022 р.

Рецензент к.т.н., доц. каф. МБІС
Шиян А.А.
"17" 06 2022 р.

Допущено до захисту
д.т.н., проф. Азаров О.Д.
"20" 06 2022 р.

ВНТУ 2022

ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра обчислювальної техніки
Освітній рівень - магістр
Спеціальність - 123 Комп'ютерна інженерія

ЗАТВЕРДЖУЮ

Завідувач кафедри обчислювальної техніки

О.Д. Азаров

"08" 02 2022 р.

З А В Д А Н Н Я

НА БАКАЛАВРСЬКУ ДИПЛОМНУ РОБОТУ

студенту **Твердохлібу Назару Миколайовичу**

1 Тема проекту «Автоматизована система управління пропускною охоронною системою», керівник проекту Богомолов Сергій Віталійович, к.т.н., доцент, затверджені наказом вищого навчального закладу від 24.03.2022 року №66

2 Строк подання студентом проекту 14.06.2022.

3 Вихідні дані до проекту: опис систем управління пропускними охоронними системами, технічний опис Arduino Mega та електронних компонентів, опис середовища Arduino IDE.

4 Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити): вступ, огляд і аналіз систем управління пропускними охоронними системами, особливості проектування систем управління пропускними охоронними системами, огляд аналогів, формування вимог до системи, проектування мікропроцесорної системи управління пропускною охоронною системою, розробка схеми системи, мікропроцесорна платформа Arduino Mega, програмування мікропроцесорної системи, висновки, перелік джерел посилання, додатки.

5 Графічний матеріал (з точним зазначенням обов'язкових креслень)-схема електрична принципова.

6 Консультанти розділів роботи представлено в таблиці 1

Таблиця 1 — Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1- 3	Богомолов С.В., к.т.н., доцент кафедри ОТ		

7 Дата видачі завдання 10.02.2022.

8 Календарний план виконання МКР приведений в таблиці 2.

Таблиця 2 — Календарний план

з/п	Назва етапів виконання бакалаврського проекту	Строк виконання етапів роботи	Примітка
1	Постановка задач проекту	14.02.22	вик.
2	Огляд і аналіз	15.02-28.02.22	вик
3	Огляд і аналіз автоматизованих систем управління пропускною охоронною системою	01.03-14.03.22	вик
4	Проектування апаратної частини	15.03-28.03.22	вик
5	Проектування програмної частини	29.03-11.04.22	вик
6	Оформлення пояснювальної записки та ілюстративного матеріалу	12.04-25.04.22	вик
7	Аналіз виконання проекту. Висновки. Додатки	26.04-09.05.22	вик
8	Перевірка якості виконання бакалаврського проекту та усунення недоліків	17.05.22	вик

Студент _____ Твердохліб Н.М.

Керівник роботи _____ Богомолов С.В.

АНОТАЦІЯ

Дипломний проект стосується теми контролю та управління доступом до захищених об’єктів.

Пояснювальна записка складається з 69 сторінок, 24 рисунки, 8 таблиць, перелік посилань містить 9 джерел.

Система створена за допомогою комплектуючих Arduino.

Розроблена система допоможе автоматизувати обробку біометричних даних співробітників та ведення обліку робочого часу, обробку і передачу отриманої інформації у базу даних, що їй відповідає. Таке рішення спростить роботу та управління керівників установ і користувачів та співробітників організацій.

Ключові слова: охоронна система, мікроконтролер, сканер, мітка, зчитувач, 1С.

ABSTRACT

The diploma project deals with the topic of control and management of access to protected objects.

The explanatory note consists of 69 pages, 24 figures, 8 tables, a list of references to revenge 9 sources.

The system is created using Arduino components.

The developed system will help to automate the processing of biometric data of employees and the accounting of working time, processing and transmission of information to the database that corresponds to it. This solution will simplify the work and management of heads of institutions and users and employees of organizations.

Keywords: security system, microcontroller, scanner, label, reader, 1C.

ЗМІСТ

ВСТУП..... 8

1 ОГЛЯД І АНАЛІЗ АВТОМАТИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ ПРОПУСКНОЮ ОХОРОННОЮ СИСТЕМОЮ 11

1.1 Автоматизовані системи пропуску……....11

1.2 Концепція побудови……12

1.3 Огляд аналогів……..13

1.3.1 Пропускна охоронна система компанії BOLID 13

1.3.2 Пропускна охоронна система компанії PERCo..... 15

1.4 Вимоги до створюваної системи……18

2 ПРОЕКТУВАННЯ АПАРАТНОЇ ЧАСТИНИ ПРОПУСКНОЇ ОХОРОННОЇ СИСТЕМИ 20

2.1 Розробка структурної схеми системи……20

2.2 Визначення моделей компонентів системи……...21

2.2.1 RFID-зчитувач та RFID-мітка..... 22

2.2.2 Сканер відбитків пальців FPM10A..... 28

2.2.3 Мікроконтролер Atmega2560 30

2.3 Функціональна схема системи……....34

2.4 Розробка електричної принципової схеми……34

3 ПРОЕКТУВАННЯ ПРОГРАМНОЇ ЧАСТИНИ ПРОПУСКНОЇ ОХОРОННОЇ СИСТЕМИ 36

3.1 Розробка основного алгоритму роботи……..36

3.2 Розробка алгоритму ідентифікації карти і управління……37

3.3 Розробка алгоритму управління пропускним пристроєм по кнопці…..39

3.4 Вибір засобів для програмування мікроконтролера…….40

3.5 Вибір засобів для програмування сервера…….45

ВИСНОВКИ 50

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ 52

ДОДАТОК А Технічне завдання 53

ДОДАТОК Б Код програми для мікроконтролера 56

ДОДАТОК В Протокол перевірки кваліфікаційної роботи на наявність текстових запозичень 69

ВСТУП

Пропускні охоронні системи — ефективний метод захисту від проходу сторонніх осіб на територію установ, а також ефективний засіб для поділ працівників відповідно наданому рівню доступу. У більшості випадків пропускні охоронні системи являють собою одние із елементів комплексної системи безпеки, поряд із системою відеоспостереження і сигналізацією.

Подібні охоронні системи мають багато рішень — починаючи з локальних (одні двері чи шлюз) до глобальних багаторівневих систем які можуть використовуватись у приміщеннях чи пропускних пунктах з великою кількістю точок проходу.

Вибір подібних систем залежить від завдань, котрі ставляться перед виробниками.

Електронний кабінет — це охоронна система контролю доступу, що може керувати одним замком.

Електронна прохідна — це система, за допомогою якої можна створити контроль доступу на пункті пропуску на територію різних підприємств і установ. Ця система складається із турнікетів з під'єднаними до них контролерами, зчитувачами та програмного забезпечення.

Автоматизована система контролю доступу представлена у вигляді електронної, або електронно-механічна системи, призначенням якої є надання, або заборона на доступ для проходу працівників, проїзд автомобілів або переміщення вантажів через вхід і вихід пунктів пропуску чи зон до яких доступ обмежено.

Пропускні системи класифікують як:

— автономні — дані про переміщення осіб не будуть передаватися на головний пульт охорони і не будуть контролюватися оператором;

— мережеві — буде відбуватись обмін даними з відділом охорони, це надає можливісь управління замками, турнікетами, шлюзами віддалено;

— універсальні — в задежності від ситуації, мають можливість функціонувати в автономному та в мережевому режимі.

Коли трапляється збій у центральному пристрої керування, системи даного типу автоматично перемикаються на автономний режим роботи.

Перевагою використання пропускних охоронних систем зводиться до виключенні людського фактора. Це гарантує максимальну точність у розпізнаванні загрози і швидке реагування виконавчих пристроїв.

Пропускні охоронні системи складаються з комп'ютерів, за допомогою яких, відбувається процес керування під’єднаними до них контрольними панелями. У них може зберігатись інформація про режими функціонування систем, перелік працівників, котрі мають доступ на об’єкт і їх рівень доступу до стратегічних приміщень установи.

Контрольну панель може бути підключено до зчитувача, завданням якого є сканування інформації з ідентифікаторів різних видів (ключ-картки, брелока, відбитка пальця). Після сканування інформація надсилається у контрольну панель, саме вона визначає рівень доступу і чи дозволено працівнику пройти.

У теперішній час є велика кількість різноманітних зчитувачів та ідентифікаторів. Експерти радять проводити процес монтажу точок контролю доступу на прохідних, на входах до офісів, місць проїзду автомобілів.

Коректно обране обладняння гарантує максимальний рівень безпеки від несанкціонованого доступу на територію підприємств, а також може здійснювати контроль переміщення осіб. Зазвичай директори великих організацій, що мають велику кількість робітників не можуть особисто відслідковувати відвідування персоналу.

Пропускні системи можуть збергати всю необхідну інформацію на контрольній панелі, за допомогою якої можна формувати звіти про облік робочого часу працівників, а також порушень ними встановлених правил. Така система контролю дає можливість підтримувати дисципліну, тому що без великих зусиль допоможе визначати запізнення робітників.

Отже, монтаж подібних пропускних систем допоможе вирішити одразу декілька проблем:

— контроль відвідування працівників, підозріла активність осіб, перебування на об’єкті у позаробочий час;

— можливість обмежити доступ працівникам до окремих приміщень на об’єкті;

— миттєве виявлення спроби потрапити на підприємство, склад чи магазин невідомих осіб;

— мінімізація витрат на утримання спеціального охоронного персоналу, який має вести облік робочого часу;

— наявність можливості визначити осіб, які перебували на об’єкті у разі виникнення надзвичайної ситуації.

Задачі дослідження:

— проаналізувати пропускні охоронні системи та методи їхньої реалізації;

— проведення огляду та аналізу методів реалізації мікропроцесорних систем;

— спроектувати пропускну охоронну систему;

— проведення тесту пристрою.

Об’єкт дослідження — процеси, що відбуваються у автоматизованих системах управління пропускними охоронними системами.

Предмет дослідження — методи та засоби ідентифікації осіб з використанням біометричних даних та безконтактних пропускних карток і ключів.

Практичне значення одержаних результатів.

Спроектовано автоматизовану систему управління пропускною охоронною системою.

Апробація. Участь у LI науково-технічній конференції факультету інформаційних технологій та комп'ютерної інженерії 2022 з доповіддю «Автоматизована система управління пропускною охоронною системою». Тези опубліковано 30.05.22.

1 ОГЛЯД І АНАЛІЗ АВТОМАТИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ ПРОПУСКНОЮ ОХОРОННОЮ СИСТЕМОЮ

1.1 Автоматизовані системи пропуску

У теперішній час є декілька видів автоматизованих систем пропуску:

Система пропуску по відбитку пальця, основою якої є автономний біометричний зчитувач, який об'єднаний в єдину систему з електрозамком. Захист за протоколом IP65 гарантує запобігання потраплянню пилу та бруду всередину.

Така система застосовується на дверях із замками електромагнітного типу. Для виходу із приміщення використовується контактна кнопка. Для доступу до пам'яті пристрою заносяться відбитки. Для кожного співробітника можна встановити прив'язку до 10 відбитків, що дозволяє прикладати до зчитувача будь-який з пальців.

Управління та настроювання зчитувача здійснюється через спеціалізоване програмне забезпечення. Комп'ютер або ноутбук з ним підключається через мережу. Є варіант налаштування зчитувача за допомогою спеціальної майстер-картки.

У системі з використанням турнікетів, рішення про надання доступу приймає контролер, який зчитує дані з безконтактної картки. При з'єднанні системи з персональним комп'ютером, на який заздалегідь було завантажено необхідне програмне забезпечення, з'являється можливість фіксації кожного відвідувача шляхом його фотографування.

Також пристрій турнікету дозволяє впровадити журнал відвідувань, формувати звіти та організовувати рівні доступу.

Системи вимірювання температури, призначені для безконтактної ідентифікації співробітників організації та встановлення температури тіла. Вони дозволяють визначити перевищення норми температурних показників окремої людини, та записує дані у спеціальний журнал.

Така установка є сучасним високотехнологічним рішенням для швидкого вимірювання температури людей та запобігання утворенню черг на прохідній. Якщо буде виявлено відхилення в нормі термометричних показників, комплекс може реалізувати різні сценарії.

Технологія розпізнавання обличчя, процедура розпізнавання обличчя з використанням системи відеоспостереження дозволяє визначити та ідентифікувати людину без необхідності звертатися до додаткових джерел та проводити будь-які дії для визначення особи людини.

Процес проникнення через прохідну з використанням розпізнавання осіб - найпопулярніша технологія. Людина дивиться в камеру, знімає окуляри, зайві аксесуари та система його пропускає після впізнавання.

При емпіричних дослідженнях впізнавання є стовідсотковим. Тому технологія практична та корисна.

1.2 Концепція побудови

У загальному вигляді пропускна охоронна система представляється, як показано на рисунку 1.1.

Автоматизована системи пропуску містить декілька компонентів.

Зчитувач — прилад, який слугує для сканування даних з ідентифікаторів, після чого передавання цих даних в контролер.

Точка проходу являє собою перешкоду, яка обладнується виконавчими пристроями та зчитувачем. Вона може контролюватися як повністю, так і частково. У одному випадку, точки проходу обладнуються двома зчитувачами, для входу та виходу. У іншому випадку зчитувач може бути встановлено тільки на вхід, у такому випадку вихід буде або вільний, або за допомогою натискання кнопки RTE.

Кнопка RTE кнопка потрібна для примусового відкриття виконавчих пристроїв, у тому випадку, коли ви знаходитесь на території підприємства, заради можливості проходу через пропускні пункти. Під час натискання цієї кнопки, спрацювання виконавчих пристроїв може бути зафіксовано у пам'яті контролера,

але встановити особу буде неможливо. Одною з причин встановлення кнопок RTE є потреба у швидкому виході з території чи будівлі.

Контролер — це основний вузол пропускних систем. Пристрій, функціями якого є обробка даних від зчитаних ідентифікаторів, приймання рішень і на основі цих дій - керування виконавчими пристроями.

Рисунок 1.1 — Концепція пропускної охоронної системи

1.3 Огляд аналогів

1.3.1 Пропускна охоронна система компанії BOLID

На сьогоднішній день однією з відомих СКУД можна назвати систему ISO «Orion», створену на базі компанії BOLID (рисунок 1.2).

Архітектура ISO «Оріон» заснована на принципі модульності. Це означає, що система складається з багатьох безпечних взаємозамінних пристроїв. Усі пристрої можуть об’єднуватись у мережу. Як транспортний рівень системи в основному використовуються інтерфейс RS-485 і мережа Ethernet.

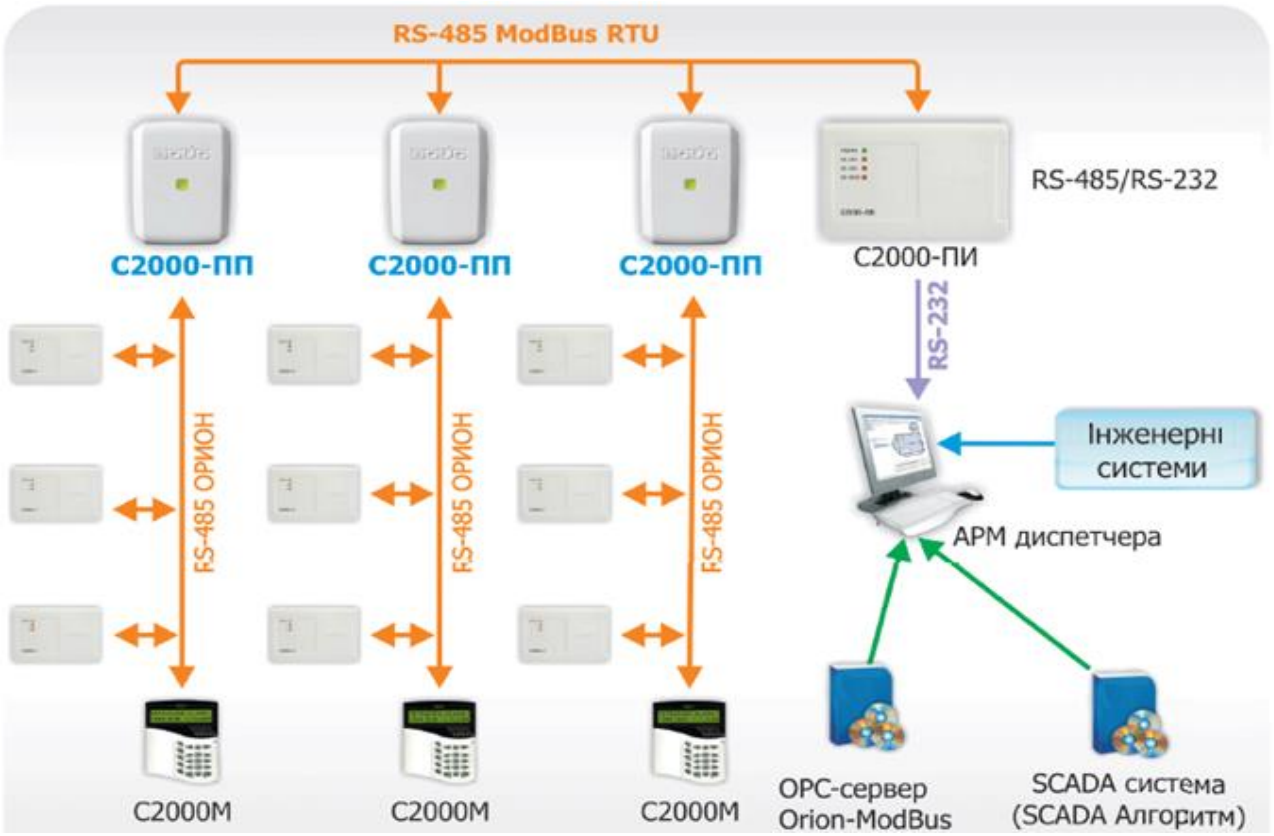

Рисунок 1.2 — Пропускна охоронна система компанії BOLID

До переваг даної системи можна віднести рішення системи завдань для різних типів приміщень, а саме:

— за результатами аналізу часу приходу та виходу працівників з підприємства запровадити контрольний облік кадрового потоку.

— покращити безпеку підприємства шляхом інтеграції СКУД та систем пожежної сигналізації. Система забезпечує вільний доступ у разі пожежі.

Ще однією вагомою перевагою системи ІСО «Оріон» є контролер доступу С2000-2, який є універсальним для будь-яких приміщень на підприємстві. Користувач вирішує, яким буде його алгоритм роботи. Кожен такий контролер здатний обслуговувати:

— двоє дверей з одним зчитувачем;

— одні двері з контролем напрямку проходу;

— турнікет;

— шлагбаум або шлюз.

Недоліками такої системи є висока вартість обладнання, особливо, якщо потрібно організувати контроль доступу для великих територій.

При інтегруванні СКУД з пожежною системою безпеки або будь-якою іншими системами, слід пам’ятати про додаткові охоронні засоби території (наприклад, відеоспостереження), щоб унеможливити несанкціонований доступ, що може спричинити збільшення витрат підприємства.

1.3.2 Пропускна охоронна система компанії PERCo

Компанія PERCo пропонує окремі невеликі системи та комплексні рішення, які здатні інтегруватися з різними системами. Виробники компанії пропонують системи з різними вимогами та ступенями безпеки.

Для прикладу візьмемо систему безпеки PERCo-S-20 «Школа». Особливістю системи є те, що у її функціонал входить можливість сповіщення батьків про час, коли дитина приходить і виходить зі школи, інформування відбувається через смс-повідомлення.

Дана система має декілька функцій:

— захист від втручання сторонніх осіб (система не допустить повторного проходу по карті, у тому випадку коли людина вже знаходиться у приміщенні).

— верифікація, дає можливість працівникам служби безпеки ідентифікувати карти доступу, порівнюючи візуально кадри, що отримуються за допомогою камер відеоспостереження, з фотографіями з бази даних.

— контроль відвідування (розклад занять заноситься в базу даних, а потім порівнюється час проходу і внесений розклад).

— інтеграція з Інтернет-ресурсом «Електронний щоденник».

Рисунок 1.3 — Пропускна охоронна система PERCo-S-20 «Школа»

Серед клієнтів компанії система контролю доступу PERCo-Web є найпопулярнішою (рисунок 1.4).

Система має такий функціонал:

— захист від несанкціонованого проникнення;

— розмежування прав доступу співробітників і відвідувачів;

— верифікація проходу співробітників і відвідувачів;

— автоматизація обліку робочого часу;

— контроль відвідування співробітників (фіксація запізнень і прогулів);

— автоматизація роботи бюро перепусток, відділу персоналу та бухгалтерії.

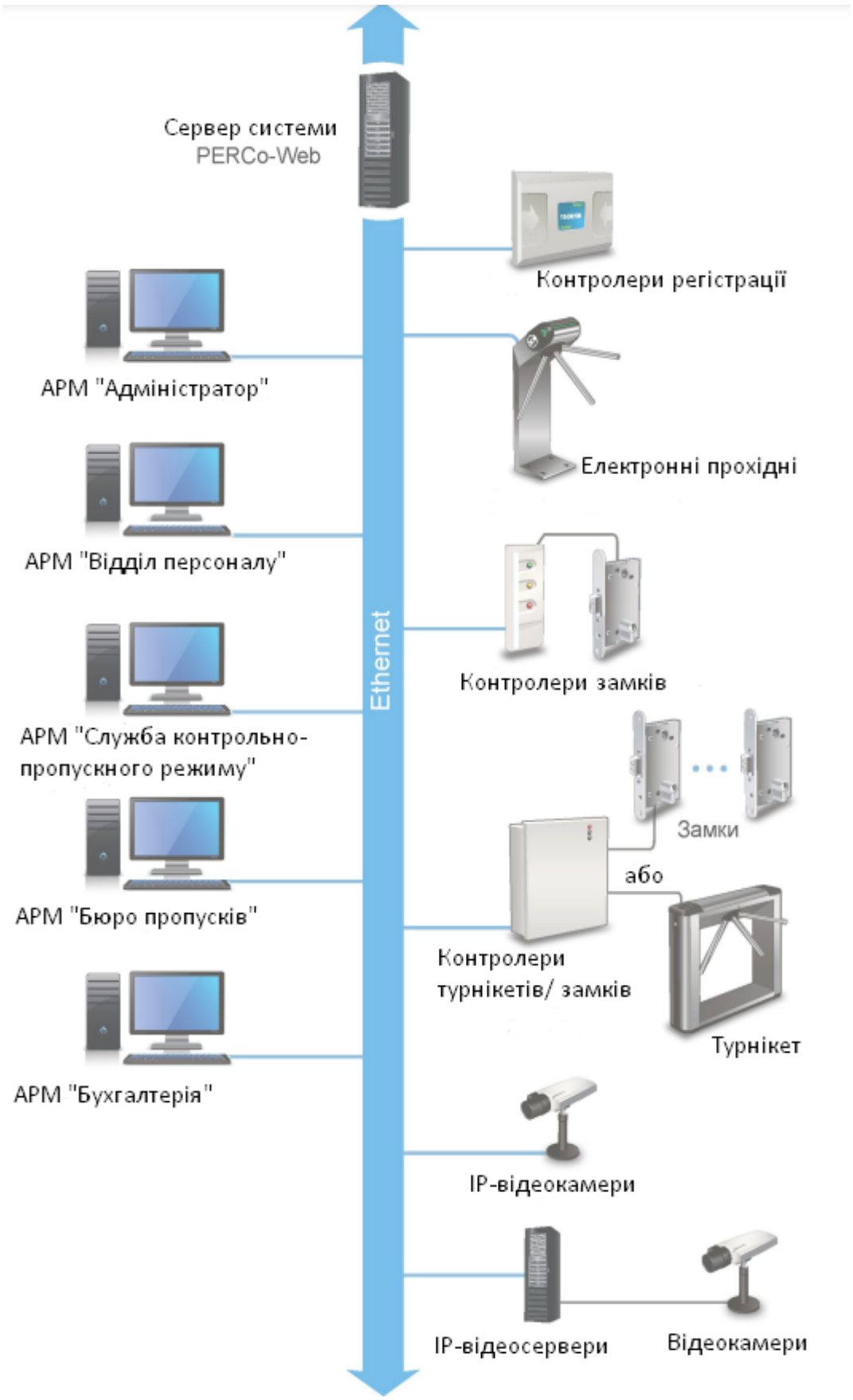

Рисунок 1.4 — пропускна охоронна система PERCo-Web

Перевагами систем компанії PERCo є:

— велика кількість завдань, які можна вирішити;

— детальна та зрозуміла інструкція по монтажі та використанню систем;

— безкоштовне програмне забезпечення;

— виробництво біометричного обладнання;

— велика кількість продукції.

Системи можна інтегрувати з іншими підсистемами компанії, що дає можливість забезпечити масштабованість.

Недоліками систем є тільки висока вартість на комплекси систем та деких видів обладнання. Ціна на базове програмне забезпечення (ПЗ) системи PERCo-SS01 «Школа» становить 356 €. Під час огляду аналогів було зроблено висновок, що ці системи мають один вагомий недолік — висока вартість.

Отже, є потреба у виборі елементів з найменшою вартістю, які необхідні для створення системи з мінімальними витратами, але які не поступалися б за функціональністю іншим існуючим системам.

1.4 Вимоги до створюваної системи

Пропускна охоронна система, що створюється, має забезпечити:

— включення та виключення живлення системи.

— внесення ID-ключів в пам'ять системи.

— збереження ID-ключів в пам'яті системи.

— подавання сигналу для відкриття виконавчих пристроїв під час зчитування ID-ключів, що збережено у пам'яті системи.

— перебуття виконавчих пристроїв у початковому режимі у тому випадку, коли відбулося зчитування незареєстрованого в системі ID-ключа.

— створення атоматичного сигналу закривання, який передається на замки, якщо не було проходу людини.

— надання різних рівнів доступу.

— фіксацію спроби несанкціонованого доступу у систему, яка зберігає дані.

– передавання інформації щодо надавання чи заборону доступу у систему, що зберігає дані.

Отже, на момент закінчення розробки приладу він повинен виконати усі зазначені вище дії.

В залежності від статусу працівника рівень доступу буде відріснятись. Директор та адміністратор на підприємстві можуть отримати найвищий рівень доступу, що передбачає безперешкодний прохід у будь-яке приміщення, а також, отримати доступ до системи зберігаючої дані. Співробітники можуть бути розділені, в залежності від рівня наданих прав: з високим і низьким рівнем доступу. Співробітники, які мають низький рівень доступу можуть скористатися ним на контрольно-пропускному пункті на територію установи. Співробітники, які мають високий рівень доступу, крім привілеїв про які було сказано раніше, також можуть отримати доступ до приміщень з обмеженим доступом, але не зможуть отримати доступ до системи зберігаючої дані.

2 ПРОЕКТУВАННЯ АПАРАТНОЇ ЧАСТИНИ ПРОПУСКНОЇ ОХОРОННОЇ СИСТЕМИ

2.1 Розробка структурної схеми системи

Для покращення розуміння влаштування системи було розроблено структурну схему пристрою (рисунку 2.1).

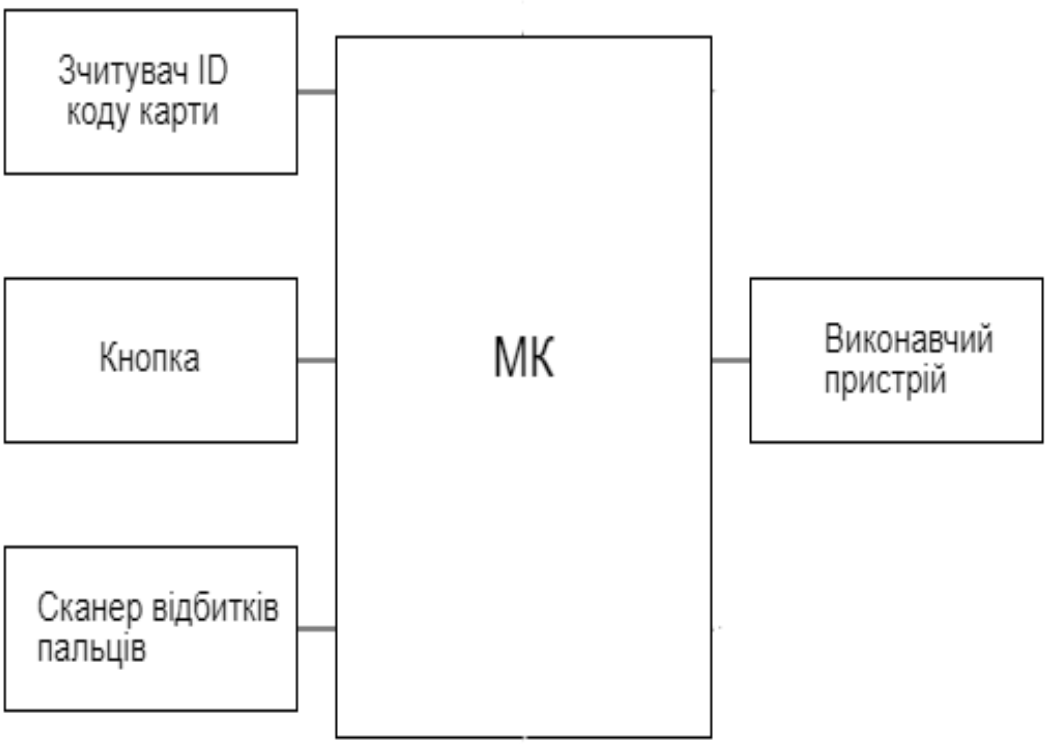

Рисунок 2.1 — Структурна схеми системи

Схема має такі системні блоки:

— контролю і управління;

— введення;

— виконавчих пристроїв.

Блок контролю і управління являє собою «центр» всієї системи, що реалізований на МК. З пристроїв введення МК приймає зі зчитувача дані. Далі МК на основі отриманої інформації приймає рішення і надсилає відповідний сигнал до блоку виконавчих пристроїв.

Якщо у базі даних є необхідна інформація, то МК надішле сигнал до блоку виконавчих пристроїв.

Якщо у базі даних немає потрібної інформації, то виконавчі пристрої залишаються в початковому стані.

Кнопка являє собою пропускний пристрій, якщо є потреба вийти з приміщення, вона може встановлюватись всередині біля дверей. Коли на МК приходить сигнал з кнопки, то МК буде вважати це позитивною відповіддю, що було описано вище.

2.2 Визначення моделей компонентів системи

За результатами досліджень існуючих пропускних охоронних систем, відповідно вимогам та структурній схемі, підібрано усі необхідні компоненти для системи що проектується.

Найважливіший і базовий елемент — це МК. Система побудована на мікроконтролері AVR Atmega2560.

На роль зчитувальних пристроїв обрано:

— RFID-зчитувач RC522;

— сканер відбитку пальця FPM10A.

Виконавчими пристроями можуть слугувати: електромагнітні замки, електромагнітні засувки, шлюзи, шлагбауми, турнікети, механізми приводу воріт в залежності від розташування системи. Для прикладу обрано турнікет, який встановлено з метою контролю доступу на підприємство.

2.2.1 RFID-зчитувач та RFID-мітка

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

RFID — безконтактна технологія, носієм інформації є радіохвиля. Для забезпечення роботи системи не потрібно ні контакту зі зчитувачем, ні прямої видимості зчитувача на відміну від систем з використанням штрих-кодування, магнітних та smart карт. Надійна робота гарантована при роботі в агресивних середовищах та несприятливих кліматичних умовах. У даному приладі використовується портальний RFID-зчитувач, призначенням якого є реєстрація RFID-міток в контрольованих проходах.

RFID-RC522 — це модуль із SPI-інтерфейсом для роботи з RFID-мітками (рисунок 2.2). Зчитувач підтримує інтерфейси SPI, UART і I2C, за допомогою яких можне відбуватись обмін даними з іншими пристроями. Зчитувач базується на мікросхемі MFRC522. Технічні характеристики вказані у таблиці 2.1.

Рисунок 2.2 — RFID-RC522

Під час обміну даними, за допомогою протоколу Mifare 1K, відбувається радіоідентіфікація RFID. Mifare — бренд, що поєднує в собі кілька видів чіпів пластикових карт, мікросхем запису та зчитування для стаціонарних пристроїв та різноманітних продуктів на їх основі. У пристроях цього бренду використовується стандарт ISO 14443 Type A.

Зчитувач RFID RC522 спрацьовує при піднесенні RFID-мітки. Зчитування відбувається за допомогою рамкових антен, які знаходяться у мітці та модулі. Джерелом енергії для мітки виступає сигнал модуля. Він може обробляти інформацію одночасно від декількох міток.

Таблиця 2.1— Технічні характеристики RFID-RC522

Технічні характеристики	Значення
Напруга живлення	3.3V
Споживаний струм	Від 13 mA до 26mA
Робоча частота	13.56 МГц
Дальність зчитування	Від 0 мм до 60 мм
Інтерфейс	SPI
Максимальна швидкість передачі	10Мбіт/с;
Розмір	40мм х 60мм
Робоча температура	Від мінус 20 до 80 С °.
Температура зберігання	Від мінус 40 до 85 С °.

Мітка RFID (рисунок 2.3) — це пристрій, здатний зберігати дані і передавати їх безконтактним способом за допомогою радіохвиль.

RFID-мітки можуть бути класифіковані кількома способами.

В основі першог оспособу лежить у визначенні наявного вбудованого джерела живлення:

— пасивні;

— активні.

Рисунок 2.3 — RFID-мітки в корпусі

Пасивні мітки даного виду не мають вбудованого джерела живлення, тому для свого живлення і передавання інформації мітка може використати енергію яку випромінює зчитувач. Конструкція пасивної мітки дуже проста і не має компонентів, що рухаються. В результаті така мітка може довго працювати, та зазвичай може витримати жорсткі умови навколишнього середовища. Наприклад, деякі пасивні мітки можуть чинити опір таким корозійним хімічним речовинам, як кислоти, і нагріванню понад 200°C.

Під час сканування мітки ініціатором зв’язку є зчитувач, а потім обмін здійснює мітка. Для відправки даних міткам такого типу обов’язково потрібен зчитувач.

Зазвичай, через простоту у виконанні, пасивні мітки мають менші розміри у порівнянні з активними чи напівактивну мітками. Оптимальною відстанню для зчитування інформації з подібої мітки є від 2,5 см і до 9 м.

Безконтактна смарт-карта є особливим типом пасивної RFID-мітки і використовується сьогодні в різних областях (наприклад, як жетони-посвідчення в

системах безпеки). Дані, що зберігаються на такій карті, зчитуються в безпосередній близькості від зчитувача. Для зчитування не потрібно щоб карта була у фізичному контакті з пристроєм читання.

Основними компонентами пасивної мітки є:

— мікрочіп;

— антена.

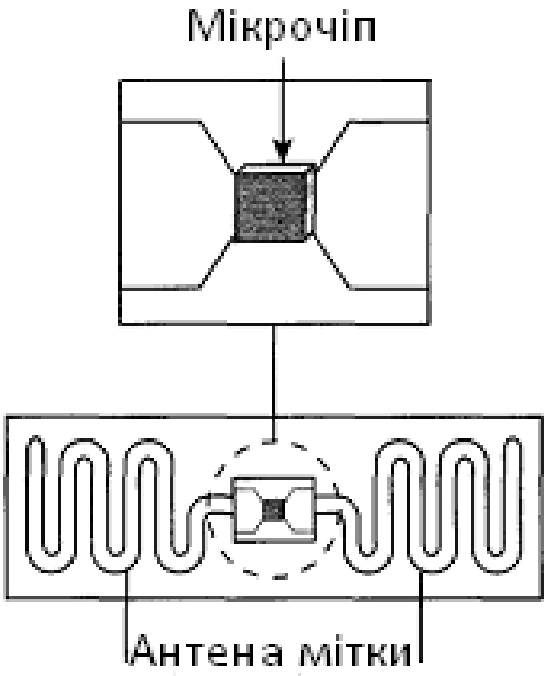

Рисунок 2.4 — Компоненти пасивної мітки

Випрямляч може перетворити напругу живлення змінного струму, яув одержується від сигналу антени зчитувального пристрою, у напругу живлення постійного струму. Також даний прилад подає живлення іншим компонентам мікрочіпа.

Виділювач — пристрій, що може уловлювати тактову частоту із сигналу який відправляє зчитуючий пристрій.

Модулятор — пристрій, що слугує для модулювання сигналу, який відправляє зчитувальний прилад. До модульованого сигналу додається відповідь мітки, після цього сигнал знову передається до зчитувального пристрою.

Логічна схема відповідає за реалізацію протоколу інформаційного обміну. Для зберігання даних використається пам'ять мікрочіпа. Зазвичай пам'ять розбита на сегменти (складається з кількох блоків чи полів).

Адресаність означає здатність звернутися (тобто прочитати або записати інформацію) до окремих ділянок пам'яті мікрочіпа. Блок пам'яті може містити дані різних типів, наприклад порцію ідентифікаційних даних зазначеного об'єкта, розряди контрольної суми (наприклад, циклічний надлишковий код — CRC) для перевірки точності даних, що передаються і тощо.

Останні технічні досягнення дозволяють зробити мікрочіпи розміром із піщинку. Але фізично розміри мітки визначаються не величиною мікрочіпа, а розташуванням та розміром її антени.

Антена встановлюється на мікрочіп та слугує для отримання, потрібної для функціонування, енергії, отримання сигналу від зчитувального приладу та обміну даними.

Можливі незліченні конструкції антен, особливо для УВЧ-діапазону, та їх проектування є так само мистецтвом, як і наукою. Довжина антени прямо пропорційна робочій довжині хвилі мітки.

Дипольна антена складається з прямолінійного відрізка провідника (наприклад, міді) з розривом посередині. Загальна довжина дипольної антени, що оптимально передає енергію сигналу, одержуваного з антени зчитувача, дорівнює половині довжини хвилі використовуваної частоти.

Подвійна дипольна антена складається з двох диполів та значно зменшує чутливість мітки до орієнтації. Внаслідок цього зчитувач може читати таку мітку під різними кутами.

У активні RFID-мітки вбудовуються елементи живлення (наприклад хімічна батарея, але можливі й інші джерела, такі як сонячна батарея) та інша електроніка.

Для передачі даних не потрібно випромінюваної зчитувачем енергії. Вбудована електроніка може містити мікропроцесори, датчики та порти введення-виводу, які отримують живлення від внутрішнього джерела. Тому, наприклад, такі компоненти можуть вимірювати температуру навколишнього середовища та

виробляти інформацію про середню температуру, та виробляти інформацію для визначення інших параметрів — скажімо, терміну придатності товару, на якому вони знаходяться. Потім мітка може передавати цю інформацію зчитувачу (разом зі своїм унікальним ідентифікатором).

Під час обміну даними ініціатором зв'язку завжди буде мітка. Оскільки для обміну даними наявність зчитувального пристрою не потрібна, активні мітки можуть передавати дані навіть без зчитувача. Цей тип активної також відомий як передавач.

Інший тип активних міток забезпечує перехід в режим сну з низьким енергоспоживанням, якщо немає запиту від зчитувача. Мітка може вийти з цього режиму отримавши спеціальну команду від зчитувача. Така функція дозволяє заощаджувати заряд акумулятора, тому мітки такого типу служать довше, ніж мітки-передавачі.

У тому випадку, коли мітка веде передачу лише за запитом, рівень радіоперешкод у навколишньому середовищі буде нижчим. Даний тип мітки називається передавач/приймач.

Відстань, з якої можна зчитати дані з мітки може жосягати приблизно 30 м і більше тільки у разі використання активного передавача.

Активна мітка у своєму складі має такі компоненти:

— мікрочіп, його розміри та функціональні можливості зазвичай перевищують подібні параметри мікрочіпів пасивних міток;

— антени, вона може мати вигляд радіочастотного модуля, який може передавати сигнали мітки і приймати відповідь сигнали пристрою читання;

— внутрішнє джерело живлення;

— внутрішня електроніка.

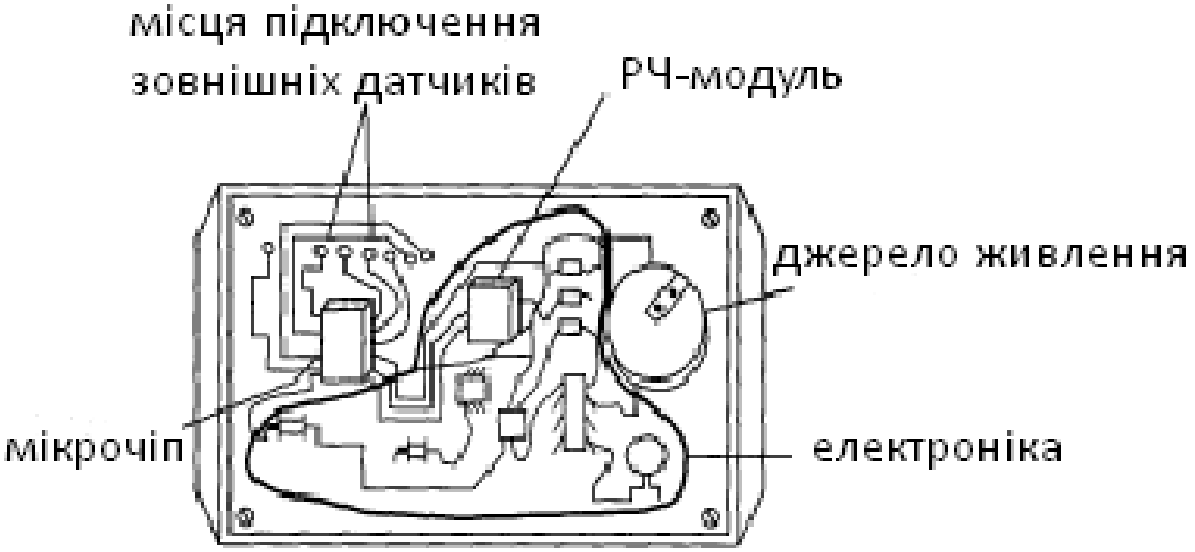

Рисунок 2.5 - Активна мітка

2.2.2 Сканер відбитків пальців FPM10A

Ідентифікація за відбитками пальців (дактилоскопія) — найпоширеніша сьогодні технологія, застосовувана в біометричних системах контролю доступу. В основі технології — унікальність малюнка папілярних візерунків на пальцях людей.

Відбиток, отриманий за допомогою сканера, перетворюється на цифровий код, який і зберігається в базі даних, а потім порівнюється з раніше введеними та перетвореними «кодами відбитків пальців».

Переваги біометричного контролю доступу за відбитками пальців:

— легкість у використанні;

— зручність та надійність;

— висока достовірність та низька вартість пристроїв, що сканують зображення відбитка пальця.

Серед недоліків:

— порушення папілярного візерунка дрібними подряпинами, порізами, хімічними реактивами;

— неможливість зчитування відбитка деякими сканерами при надмірно сухій шкірі.

Методи аутентифікації за відбитками пальців мають декілька тенологій.

Технологія Match-on-Host є галузевим стандартом. Система складається з датчика відбитків пальців, що зчитує біометричні дані із відправкою на центральний зовнішній процесор. Вся обробка і пошук відбитків, що збігаються, здійснюється на зовнішньому сервері.

Технологія Match-in-Sensor має архітектуру, замкнуту на самому чіпі (system-on-a-chip або SoC). Зчитування папілярного візерунку і обробка відбитку пальця здійснюється у IC-датчику. Така архітектура є безпечнішою, тому що шаблони відвідування шифруються та підписуються за допомогою датчика, а усі дані зберігаються у пам'яті.

Рисунок 2.6 — Сканер відбитків пальців FPM10A

У таблиці 2.2 вказано технічні характеристики сканеру відбитків пальців.

Таблиця 2.2 — Технічні характеристики FPM10A

Технічні характеристики	Значення
Струм	120 мА (140 мА макс.)
Час обробки зображення відбитка	< 1.0 секунд
Сенсор	оптичний
Розмір сенсора	14 мм x 18 мм
Розмір сигнатури	256 байт
Розмір шаблону	512 байт
Ємність	300 осередків
Рівні безпеки	1-5
Інтерфейс	UART TTL
Швидкість передачі	9600, 19200, 28800, 38400, 57600
Робоча температура	Від мінус 20 °C до 50 °C
Допустимий рівень вологості	Від 40 % до 85 % RH
Габаритні розміримм	45 мм x 26 мм x 19 мм
Вага	15 грам

2.2.3 Мікроконтролер Atmega2560

Важливий компонент плати Arduino Mega є мікроконтролер. Він представлений RISC процесором, розробленим AVR і функціонуючим на частоті 16МГц, яка є максимальною з усієї лінійки продуктів ATMel.

На кристалі його чіпа розташовані всі пристрої, що відносяться до загального поняття комп'ютерної системи: оперативна та перепрограмована постійна, а також flash пам'ять, інтерфейсні мости, помножувач. У даній платі Arduino використовується Atmega2560 (рисунок 2.7).

У даній системі мікроконтролер Atmega2560 вбудований в апаратну платформу Arduino Mega.

Рисунок 2.7 — Мікроконтролер Atmega2560

У даній системі мікроконтролер Atmega2560, технічні характеристики якого вказані у таблицях 2.3 — 2.5, вбудований в апаратну платформу Arduino Mega.

Таблиця 2.3 — Технічні характеристики пам’яті

Пам’ять	Значення
EEPROM (ППЗП)	4 Kb
SRAM (ОЗП)	8 Kb
FLASH ROM	256 Kb
Циклів перезапису EEPROM	100 000
Циклів перезапису FLASH ROM	10 000
Кількість режимів очікування процесора	6

Таблиця 2.4 — Технічні характеристики таймерів

Таймери	Значення
8bit	2
16bit	4
RTC\Real Time Clock (реального часу)	1
PWM (ШІМ-перетворювачі 8bit, вихід)	4

Таблиця 2.5 — Технічні характеристики портів

Порти	Значеня
Порти введення-виведення (загальна кількість)	86
Аналогові, по 10bit (вхід)	16
Послідовні USART	4
Послідовний SPI, працюючий (master/slave)	1
Послідовний, побайтний	1
Цифроі входи\виходи	54
Частота процесора AVR	16Мгц

Даний мікроконтролер є найголовнішою складовою платформи Arduino Mega (рисунок 2.8). Створювати різні проекти можна за допомогою ПЗ Arduino IDE, ця платформа дозволяє програмувати мікроконтролер Atmega2560. Технічні характеристики плати вказані у таблиці 2.6.

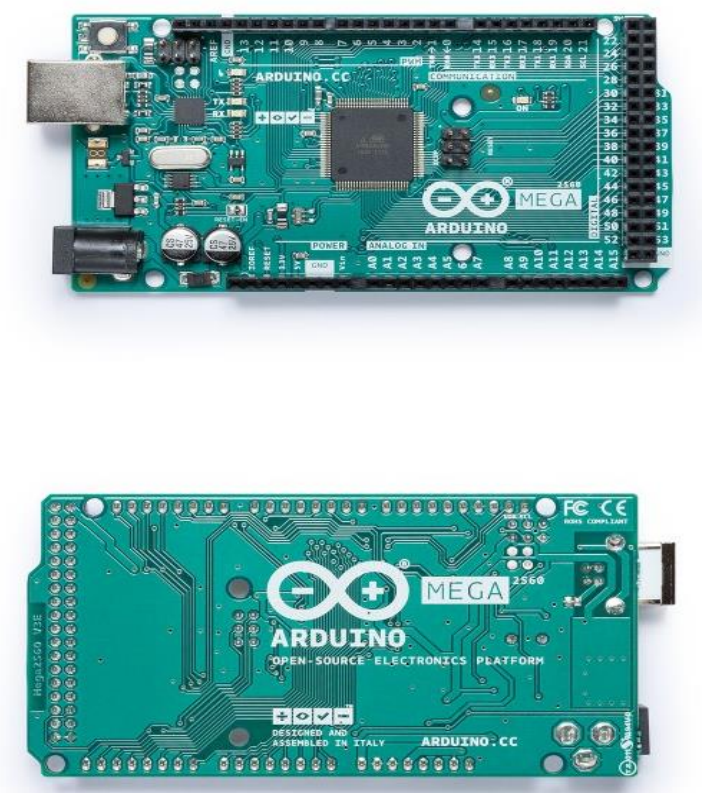

Рисунок 2.8 - Arduino Mega

Таблиця 2.6 — Технічні характеристики Arduino Mega

Технічні характеристики	Значення
Мікроконтролер	AVR Atmega2560.
Робоча напруга	5 В.
Гранична вхідна напруга	Від 7 В до 12 В.
Цифрові входи / виходи	54.
Аналогові входи	16.
Постійний струм через вхід / вихід	40 мА.
Тактова частота	16 МГц.
Розміри	101.52 мм х 53.3 мм.

Платформа має порт miniUSB, через який відбувається програмування скомпільованої програми.

Плата містить кілька пристроїв через які здійснюється зв'язок з комп'ютером, пристроями Arduino або мікроконтролерами.

Arduino Mega може отримувати енергію як через підключення по USB, так і від зовнішнього джерела живлення.

Зовнішнє джерело електроенергії (не USB) може живити плату через перетворювач AC/DC, який являє собою блок живлення, або ж звичайним акумулятором. Перетворювач напруги підключається за допомогою роз'єму 2.1 мм із полюсом на центральному контакті. Провідник від джерела живлення підключається до виводів Gnd і Vin роз'єму (POWER).

Arduino Mega може функціонувати при показниках живлення від 6 до 20 В. При напрузі живлення нижче 6 В, платформа може працювати нестабільно.

Якщо використовувати напругу вище ніж 12 В, регулятор напруги може перегрітися та пошкодити плату. Рекомендований діапазон напруги живлення від 7 до 12 В.

2.3 Функціональна схема системи

Відповідно визначеним моделям компонентів і спроектованої структурної схеми у підрозділах 2.1 та 2.2, було розроблено функціональну схему пристрою (рисунок 2.13).

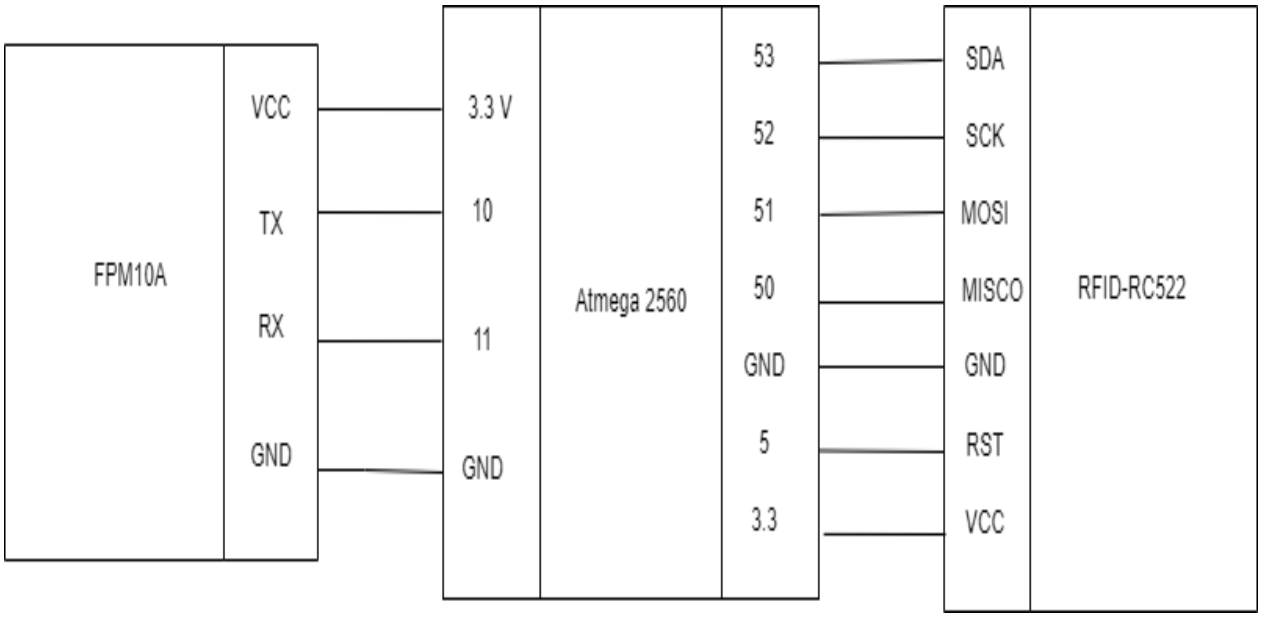

Рисунок 2.9 - Функціональна схема системи

2.4 Розробка електричної принципової схеми

Мікроконтролер Atmega2560 є «центром» проектованої системи. До портів МК будуть підключатись резистори і такі периферійні пристрої:

— зчитувач RFID-міток RC522;

— сканер відбитків пальців FPM10A (таблиця 2.8).

Потрібно врховувати, те що контакти SCK, MISO, MOSI, робота яких відбувається за допомогою протоколу SPI , будуть підключатись за допомогою роз'єму XS3. Також сюди будуть підключені контактів RFID-зчитувача (таблиця 2.7).

Таблиця 2.7 — Підключення RFID-зчитувача

Контакти сканеру RC522	Контакти плати
SDA	53
SCK	52
MISO	50
MOSI	51
RST	5
GND	GND
VCC	3,3 V

Таблиця 2.8 — Підключення сканеру відбитків пальців

Контакти сканеру FPM10A	Контакти плати
TX	10
RX	11
GND	GND
VCC	3,3 V

На виходах напруга буде становити 3,3 В, це значення напруги потрібне для нормального функціонування зчитувача RFID-міток RC522, а також для сканеру відбитків пальців FPM10A.

3 ПРОЕКТУВАННЯ ПРОГРАМНОЇ ЧАСТИНИ ПРОПУСКНОЇ ОХОРОННОЇ СИСТЕМИ

3.1 Розробка основного алгоритму роботи

Відповідно до завдання та основного набору функцій модель матиме такий алгоритм функціонування, як показано на рисунку 3.1.

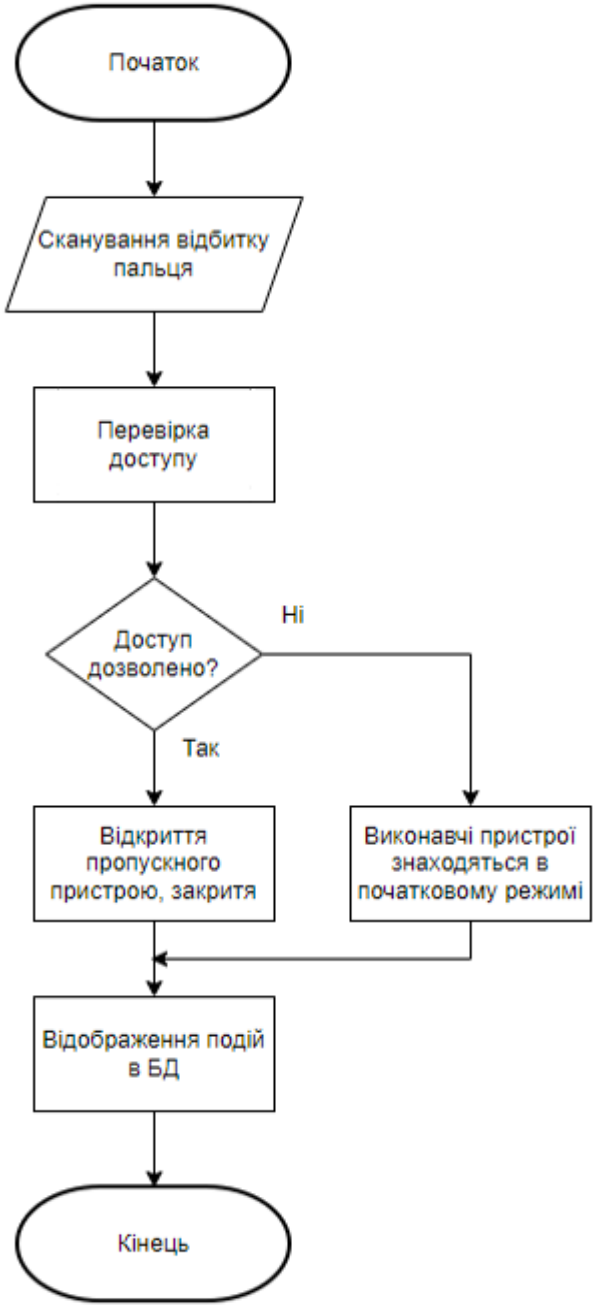

Рисунок 3.1 — Блок-схема роботи системи

Словесний алгоритм роботи системи:

— крок 1 — читання коду карти.

— крок 2 — перевірка доступу, якщо доступ дозволений, то крок 3, інакше виконавчі пристрої будуть знаходитись у початковому режимі і перейде до кроку 4.

— крок 3 — відкрвання пропускного пристрою, для того. щоб людина мала можливість пройти, і закриття.

— крок 4 — система передає дані про надання, або спробу несанкціонованого доступу, які відображаються в БД.

3.2 Розробка алгоритму ідентифікації карти і управління

Під час підключення джерела живлення, робота пропускої системи з процесу ініціалізації — запуск програми, що записана у МК.

Активний стан роботи системи передбачає моніторинг: зчитувальних компонентів та кнопки, отже відслідковує зміни стану.

Якщо піднести картку до зчитувача то система, в залежності від того, чи є код картки у базі даних чи немає, МК або подасть сигнал на виконавчі пристрої, або ж залишиться у початковому стані.

У тому випадку, коли сигнал надійде з кнопки, він буде вважатися сигналом про допуск.

Процес зчитування ID коду картки, управління пропукними пристроями, запис отриманої інформації у базу даних показано на рисунку 3.2.

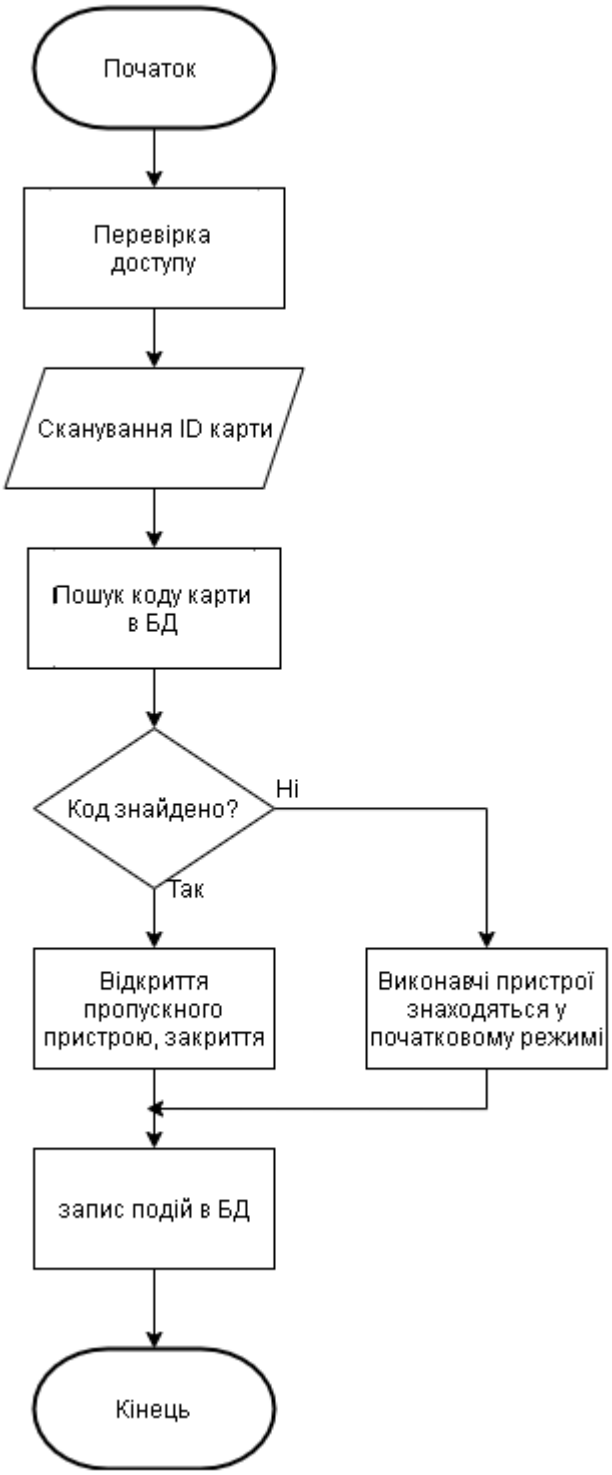

Рисунок 3.2 — Блок-схема алгоритму ідентифікації карти

Алгоритм має наступний вигляд:

— крок 1 — підключення джерела живлення, ініціалізація системи.

— крок 2 — моніторинг сигналу з пристроїв введення (зчитувачі і кнопка).

— крок 3 — перевірка наявності картки в зоні роботи зчитувального пристрою. якщо карти в зоні зчитування немає — буде виконуватись крок 2, у іншому випадку — крок 4.

— крок 4 — зчитування коду карти.

— крок 5 — перевірка відповідності кодів з бази даних з кодом картки, якщо відповідний код знайдено — крок 6, у іншому випадку виконавчі пристрої знаходяться у початковому режимі, перехід до кроку 8.

— крок 6 — надходження сигналу про отримання доступу.

— крок 7 — управління пропускнним пристроєм: відкривання і закривання пропускного пристрою.

— крок 8 — передавання даних про подіюдо бази даних, буде передаватись ID зчитаної картки та статус.

3.3 Розробка алгоритму управління пропускним пристроєм по кнопці

У пропускній системі є кнопка для виходу, вона відкриває або закриває пропускний пристрій. Сигнал з кнопки приходить на МК за допомогою зовнішнього переривання. Через це пропускна система буде мати додатковий алгоритм роботи під час надходження сигналу від кнопки:

— крок 1 — відправлення сигналу від кнопки — крок 2, у іншому випадку повторюється крок 1.

— крок 2 — сигнали про надання доступу.

— крок 3 — управління виконавчими пристроями: відкриття та закриття.

— крок 4 — передавання інформації про подію до бази даних.

Алгоритм роботи пропускної системи через сигнали від кнопки, що встановлена на вихід, на рисунку 3.3.

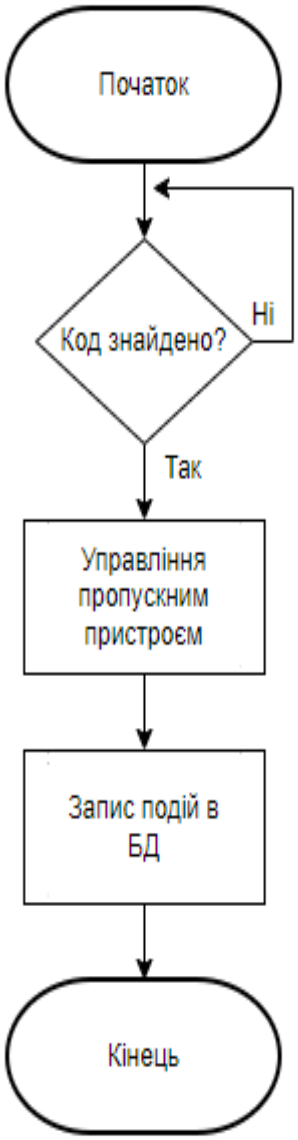

Рисунок 3.3 — Блок-схема алгоритму управління пропускним пристроєм по кнопці

3.4 Вибір засобів для програмування мікроконтролера

Arduino IDE — це інтегроване середовище розробки для Windows, MacOS та Linux, розроблене на Сі та C++, призначене для створення та завантаження програм на Arduino-сумісні плати, а також на плати інших виробників (рисунок 3.4).

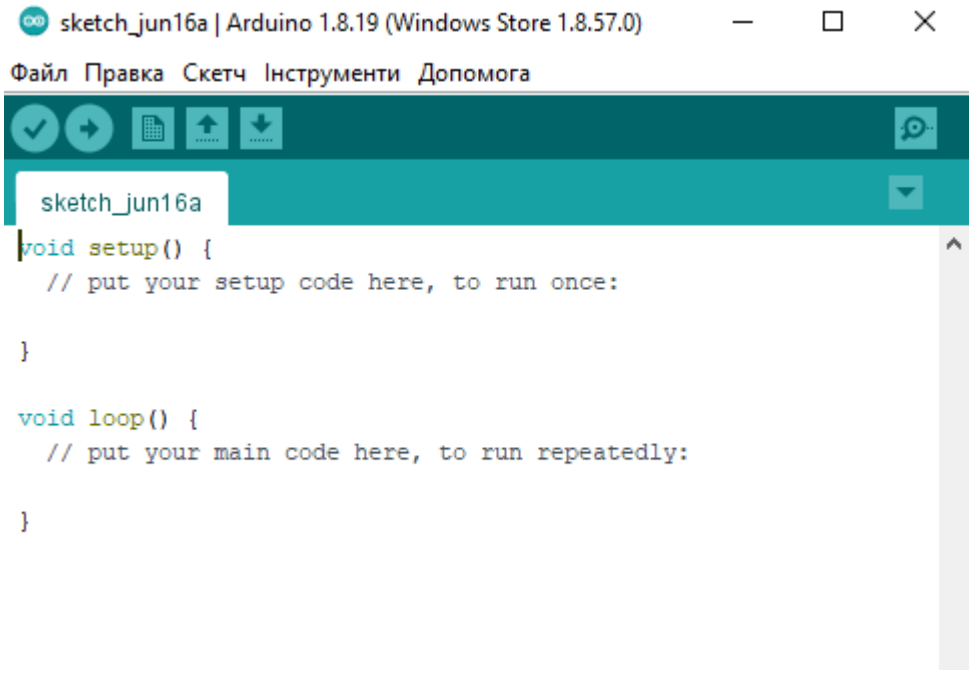

Рисунок 3.4 — Вікно програми

Програма містить такий функціонал: файл, правка, скетч, сервіс і довідка.

У пункті Файл (рисунок 3.5) можна знайти команди, що відповідають за створення нової програми, читання старої, збереження її змін, а також команди для завантаження програми на мікроконтролер.

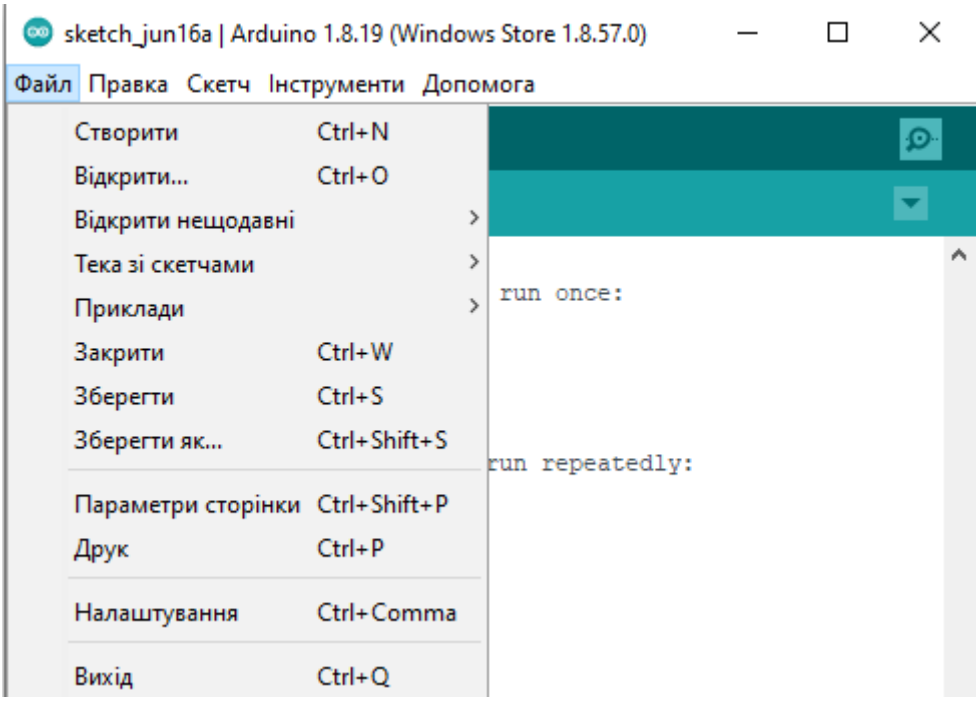

Рисунок 3.5 — Випадаюче меню пункту Файл

Правка (рисунок 3.6) включає в себе функції, які відповідають за редагуванням програмного коду, включаючи копіювання, вставку, налаштування відступів і пошук за ключовим словом.

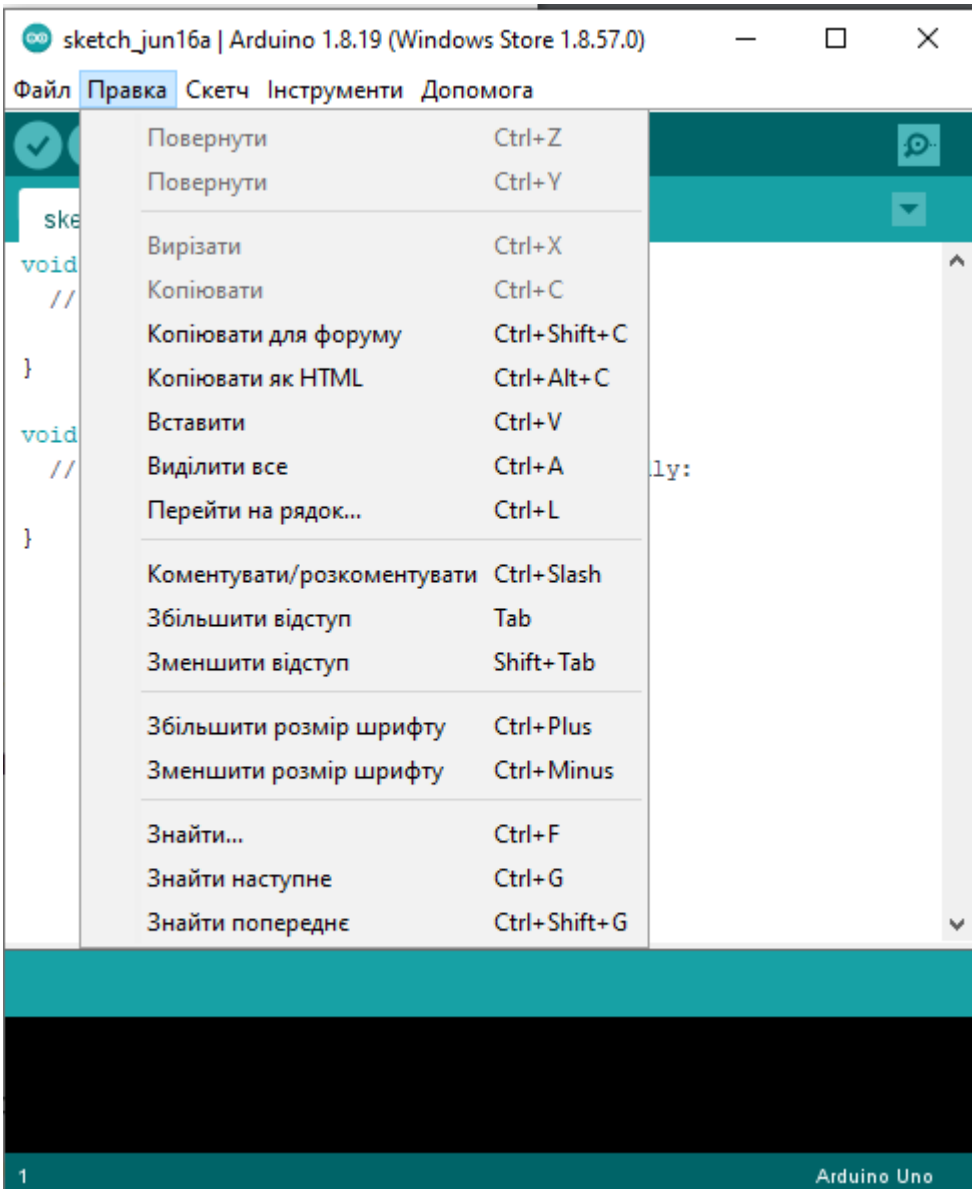

Рисунок 3.6 — Випадаюче меню пункту Правка

У розділі Скетч (рисунок 3.7) присутні засоби які дозволяють контролювати компіляцію програми.

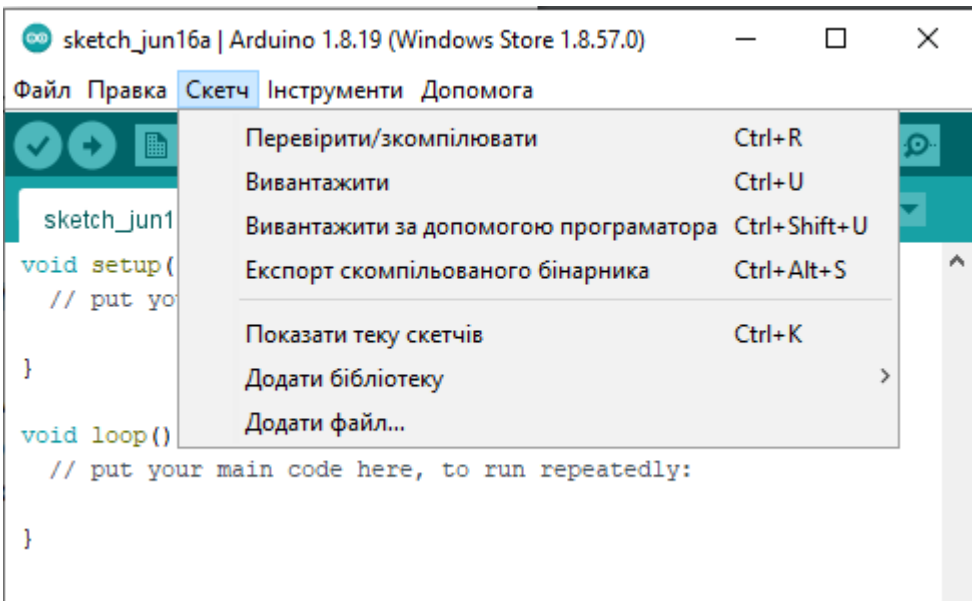

Рисунок 3.7 — Випадаюче меню пункту Скетч

Пункт меню Інструменти (рисунок 3.8) об’єднує у собі спеціальні інструменти для роботи з самим мікроконтролером.

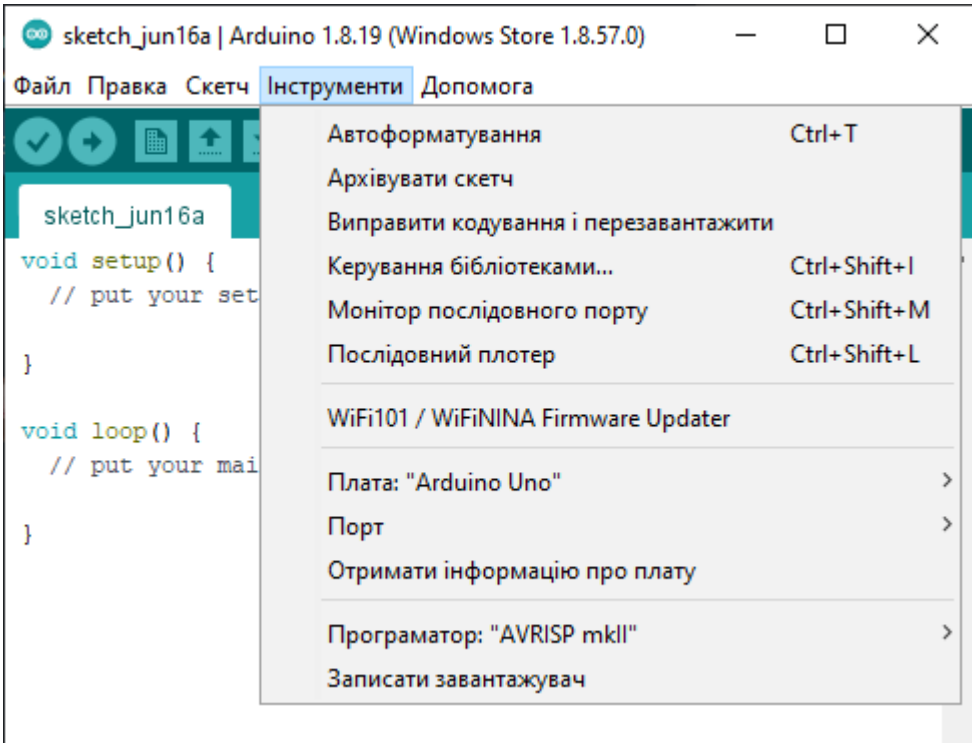

Рисунок 3.8 — Випадаюче меню пункту Інструменти

Меню Допомога (рисунок 3.9) включає у себе вичерпний опис функціоналу самого середовища Arduino IDE та повний список команд і методів роботи з платами Arduino.

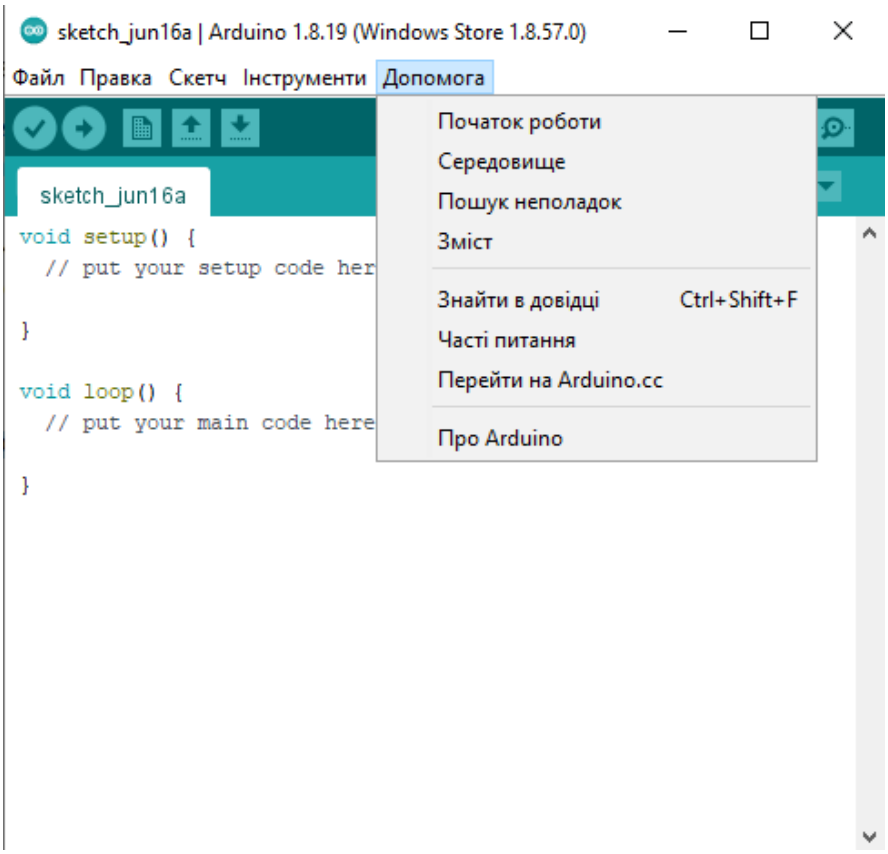

Рисунок 3.9 — Випадаюче меню пункту Допомога

Кожна програма для Arduino може складатися з декількох файлів. Для перемикання між цими файлами служить система вкладок в редакторі. Також тут є можливість, додати нову вкладку, і асоціювати з нею проект що вже збережений на персональному комп’ютері .

Програмний код пишеться і змінюється у головному вікні середовища. Вікно середовища розробки представляється як звичайний текстовий редактор, який може виділяти конструкції коду.

У нижній частині редактора Arduino IDE є поле, функцією якого є показ повідомлень про помилки, які ожуть виникнути в процесі компіляції програми, або під час завантаження програми в мікроконтролер.

Arduino IDE являє собою просте та функціональне середовище розробки для створення власного ПЗ, яким керуються численні пристрої, зібрані початківцями та досвідченими електронниками.

З'єднання ПК із мікроконтролером реалізовано через інтерфейс USB. Код мовою C та C++ пишеться в редакторі, в якому є підсвічування команд та спеллчекер.

Середовище розробки програмного забезпечення (IDE) для конструктів на основі плат Arduino з'явилося одночасно з апаратною частиною популярної платформи. Це логічно, адже концепція, за якої інженеру не доводиться працювати з програматором, має на увазі, що інструкції повинні бути легко прошиті в мікроконтролер.

3.5 Вибір засобів для програмування сервера

«1С: Бухгалтерія» — це лише частина комплексної системи управління підприємством 1С: Підприємство.

Після запуску програми на екрані з’явиться вікно, яке зображене на рисунку 3.10.

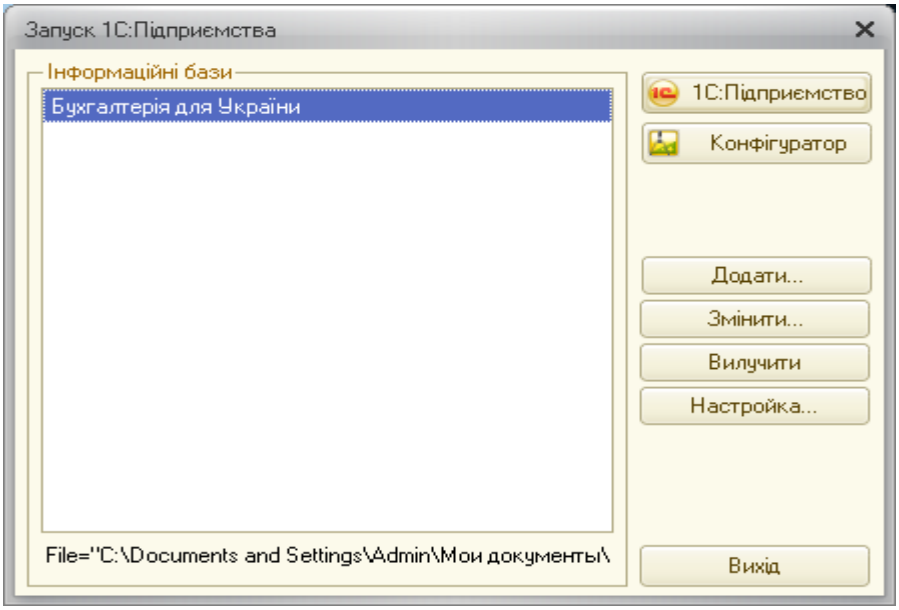

Рисунок 3.10 - Вікно запуску програми

Щоб почати працювати, потрібно у розділі Інформаційні бази обрати потрібну конфігурацію, а саме: «1С:Бухгалтерія» і натиснути кнопку ОК, або ж двічі клацнути по лівій кнопці миші на назву у списку.

Додаткові функції: Змінити, Додати і Вилучитипотрібні щоб налаштувати програму для роботи з різними інформаційними базами.

Кнопка Відміна закриває вікно, щоб припинити процес запуску 1С. Функціями кнопки Допомога є виведення випадаючого вінка підказок та необхідних інструкцій, котрі допоможуть налаштувати 1С, вона має кілька рівнів, які можна викликати з різних вікон програми, отримана інформація про роботу з програмою і з формуванням документів з точки зору бухгалтерів є дуже детальною.

Коли всі потрібні функції буде обрано, натискання на кнопку ОК призведе до заватнаження головного вікна, яке представлене на рисунку 3.11.

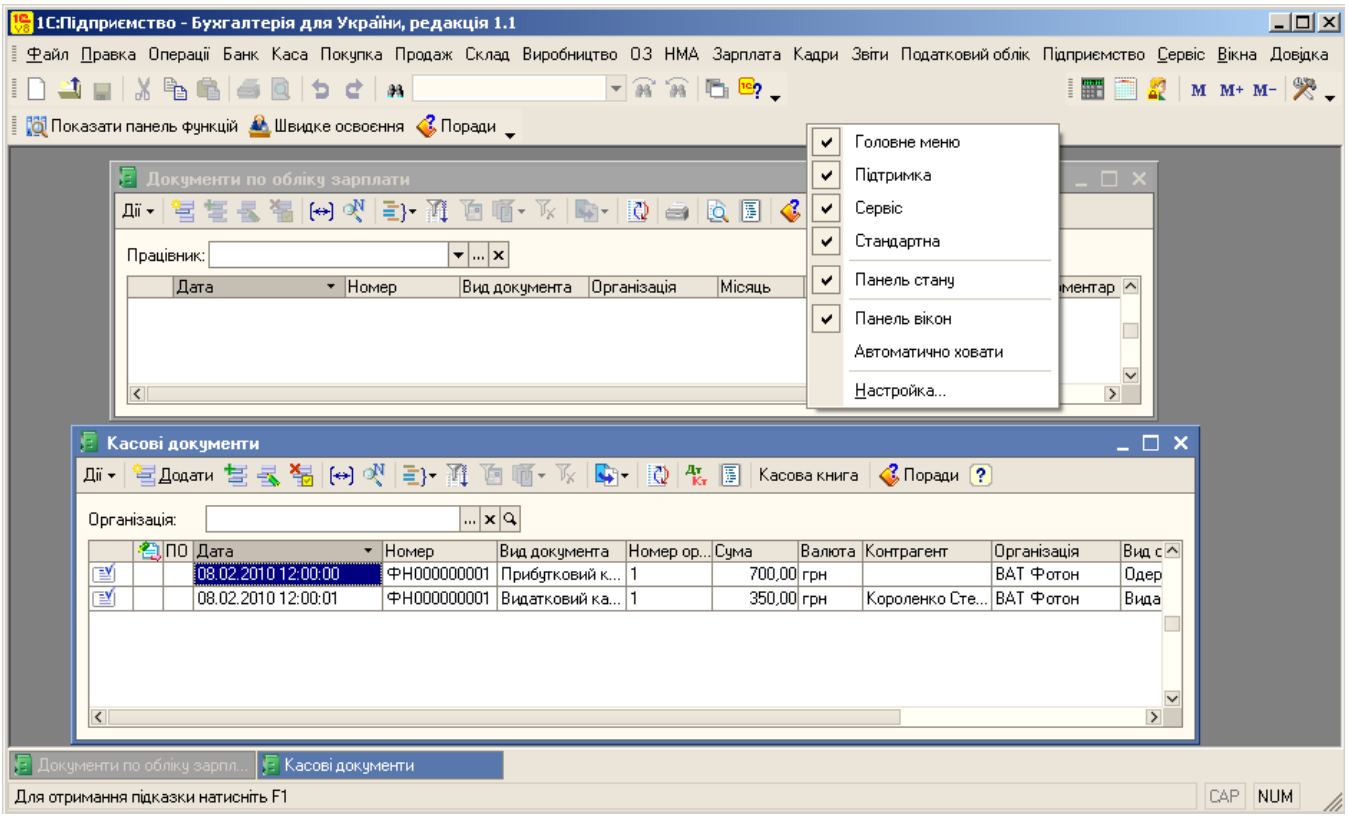

Рисунок 3.11 - Вікно програми «1С: Підприємство» (конфігурація «Бухгалтерія»)

При першому запуску програми на головному вікні можуть з’явитись з додатковою інформацією чи пропозиціями повного налаштування: «Навчання: очне навчання за програмою 1С: Бухгалтерія 8 для України», «Швидке освоєння 1С: Бухгалтерії 8», «Стартовий помічник», доступ до усіх цих функцій також можна отримати за допомогою меню Довідка.

Будь-яке налаштування 1С складається із декількох функцій.

Рядка заголовку, тут міститься назва компонента програми, а також кнопки маніпулювання вікном системи («Згорнути», «Розгорнути», «Закрити вікно»);

Головного меню, призначенням яког є виконання операцій: команди об’єднані в групи, назви груп утворюють рядок меню;

Панелей інструментів, до якого, у 1С: Бухгалтерії, входять: Стандартна, Сервіс та Підтримка, що можуть повторювати команди з меню Файл, Правка, Сервіс і Допомога.

Налаштування меню інструментів відбувається за таким же принципом, як і в будь-якій прикладній програмі операційної системи Windows (команда головного меню Сервіс>Настройка, або команда Настройка в контекстному меню Панелей інструментів):

— робочого поля, яке містить вікно з метаданими - Довідників, електронних форм Документів, Журналів, Звітів;

— панелі вікон, де розміщені назви активних вікон;

— панелі стану, яка підлаштовує поради про можливі дії під конкретну ситуацію, містить індикатори функціонування таких клавіш як: CapsLock і NumLock.

Головне меню надає можливість швидко отримати доступ до всіх головних функцій програми, яке містить наступний перелік кнопок: Файл, Правка, Операції, Банк, Каса, Покупка, Продаж, Склад, Виробництво, ОЗ, НМА, Зарплата, Кадри, Звіти, Податковий облік, Підприємство, Сервіс, Вікна, Довідка.

Таким чином, пункт меню об’єднує у собі інструменти для роботи з бухгалтерським обліком.

До складу «1С: Підприємство» входять компоненти:

— «1С: Бухгалтерія»;

— «1С: Розрахунок»;

— «1С: Оперативний облік».

Будь-яка частина «1С: Підприємства» може функціонувати окремо одна від одної, або ж об’єднуватись у велику та комплексну систему з великою кількістю функцій.

«1С: Бухгалтерія» являє собою одну з найкращих автономних систем для автоматизації бухгалтерського обліку. Універсальність цієї прикладної програми дозволяє використовувати її функціонал на найрізноманітніших підприємствах.

Також до її можливостей входить підтримувати різноманітних системи обліку і функція ведення обліку на певній кількості установ що працює лише на одній інформаційній базі.

Обширний функціонал програми, перетворює її на доволі простий і наочний засіб для ведення бухгалтерського обліку, або автоматизації ведення документів для формування звітів.

У функціонал «1С: Бухгалтерії» входить можливість ведення майже всіх видів бухгалтерського обліку:

— облік операцій з банку та каси;

— облік основних засобів та нематеріальних активів;

— облік матеріалів;

— облік взаєморозрахунків з постачальниками та покупцями;

— облік випуску продукції, розрахунків із зарплати;

— облік товарів, послуг та виробництво продукції;

— облік валютних операцій;

Введення обіку може відбуватись завдяки кільком способам:

— у режимі ручного введення операцій;

— у режимі типових операцій;

— у режимі автоматичного формування операцій із документам.

У пакет системи «1С: Бухгалтерія» включено універсальну типову конфігурацію, розроблену фірмою 1С.

Основні налаштування обліку проводяться у конфігурації системи «1С: Конфігуратор».

До них відносяться основні властивості плану рахунків, види аналітичного обліку, склад і структура довідників, документів, звітів і т.д.

ВИСНОВКИ

Результатом дипломного проекту стала реалізована система управління пропускною охоронною системою, створена за допомогою комплектуючих Arduino. Поставлені, перед виконанням роботи, завдання було виконано у повній мірі.

У першій частині дипломного проекту було проведено дослідження існуючих систем управління пропускними охоронними системами, а також визначено функції, які на даний момент реалізовані в системі.

На цій основі були визначені цілі та завдання, а також вимоги до проектування системи і було зроблено висновок, що систему необхідно розробляти з найменшими економічними витратами.

У другій частині дипломного проекту, опираючись на вимоги технічного завдання, формулюється схема структури контролера пропускної охоронної системи та схема функціональної структури системи. Також визначається склад елементів, що містяться у системі.

Моделювання схем дозволяє перевірити правильність структури систем і дає можливість розробити електричні принципові схеми схеми.

У третій частині дипломного проекту розробляється схема електричних базових елементів блоку управління системою, для реалізації розроблених функцій.

Розроблені блок-схеми, функціональні схеми та принципові схеми відкривають можливості для подальшого створення алгоритмів блоку управління системою, а також впровадження програмного забезпечення для системного контролера.

Було описано алгоритми як функціонування системи в загальному, так і окремих функцій. Розроблений алгоритм забезпечує можливість розробки програмного коду для мікроконтролерів та серверів.

Розроблена система задовільняє усі вимоги та має кілька переваг: мала собівартість, компактність і простота використання та створення в порівнянні з аналогіними системами.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. В. А. Ворона, В. А. Тихонов Системы контроля и управления доступом. Горячая Линия - Телеком - 2010. – 272 с.

2. Джереми Блум Изучаем Arduino. БХВ – Петербург – 2012.

3. А. Меньков А.В. Теоретические основы автоматизированного управления/ А.В. Меньков, В.А. Острейковский. – Учебник для вузов. – М.: Издательство Оникс, 2005. – 640 с.

4. Производитель оборудования безопасности PERCo [Электронный ресурс] - Режим доступа: https://www.perco.ru/products/sistema-kontrolya-dostupa/- Загл. с экрана. - Яз. рус.

5. Контроль и управление доступом систем безопасности BOLID [Электронный ресурс] - https://bolid.ru/projects/iso-orion/safety-and-security/ - Загл. с экрана. - Яз. рус.

6. Биометрические системы контроля и управления доступом [Електронний ресурс]. - Режим доступу до ресурсу: http://www.capitalpost.ru/uk/biometricheskie-sistemyi-kontrolya-i-upravleniya-dostupom/ (дата звернення: 14.05.2022).

7. Волхонский В.В. Системы контроля и управления доступом. – СПб: Университет ИТМО, 2015. – 105 с. Рис. 96. Библ 6.

8. A Simple Explanation Of 'The Internet Of Things' [Електронний ресурс] – режим доступу: https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanationinternet-things-that-anyone-can-understand/?sh=5c7c02081d09

9. 1С:Бухгалтерия 8 для Украины. Первые шаги. А.М.Шаталов ред. 2

ДОДАТОК А

Міністерство освіти та науки України

Вінницький національний технічний університет

Факультет інформаційних технологій та комп'ютерної інженерії

ЗАТВЕРДЖУЮ

Завідувач кафедри ОТ ВНТУ

д.т.н., проф.

_____О. Д. Азаров

"__" _____ 2022 р.

ТЕХНІЧНЕ ЗАВДАННЯ

на виконання бакалаврського дипломного проекту

«Автоматизована система управління пропускною охоронною системою»
08-23.БДП.038.00.000 ПЗ

Науковий керівник к.т.н., доц. каф. ОТ

_____ Богомолов С.В.

Студент групи 1КІ-20мс

_____ Твердохліб Н.М.

Вінниця 2022

1 Найменування та область застосування

Автоматизована система управління пропускною охоронною системою на базі Arduino з можливістю автоматичного опрацьовування отриманих даних з ID карток та сканеру відбитків пальців.

2 Основи для розробки

Основою для розробки є дисципліни комп'ютерна логіка, комп'ютерна електроніка, комп'ютерні системи.

3 Мета та призначення розробки

Створення пропускної охоронної системи, яка допоможе автоматично опрацьовувати дані про ідентифікацію персоналу, опрацьовувати, накопичувати та передавати їх у відповідні БД.

4 Етапи БДП та очікувані результати

Робота виконується в п'ять етапів, що наведені в таблиці 4.1.

Таблиця 4.1 - Етапи виконання роботи

№ етапу	Назва етапу	Термін виконання		Очікувані результати
		початок	кінець	
1	Аналіз завдання. Вступ	14.02.22	25.02.22	Вступ
2	Огляд і аналіз систем управління пропускною охоронною системою	17.02.22	11.03.22	Розділ 1
3	Проектування апаратної частини	12.03.22	25.03.22	Розділ 2
4	Проектування програмної частини	27.03.22	09.04.22	Розділ 3
5	Оформлення ПЗ	11.04.20	28.05.20	ПЗ, презентація

5 Матеріали, що подаються до захисту бакалаврської дипломної роботи.

До захисту дипломної роботи подаються: пояснювальна записка, графічні і ілюстративні матеріали, відзив наукового керівника, рецензія опонента, анотації українською та іноземною мовами, довідка про відповідність оформлення бакалаврської дипломної роботи діючим вимогам.

6 Порядок контролю виконання та захисту БДП

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

7 Вимоги до оформлення БДП

— ДСТУ 3008 : 2015 «Звіти в сфері науки і техніки. Структура та правила оформлювання»;

— ДСТУ 8302 : 2015 «Бібліографічні посилання. Загальні положення та правила складання»;

— ГОСТ 2.104-2006 «Едина система конструкторської документації. Основні написи»;

— документами на які посилаються у вище вказаних.

Технічне завдання до виконання отримав _____ Твердохліб Н.М.

ДОДАТОК Б

Код програми для мікроконтролера

```
#include <Adafruit_Fingerprint.h>
#include <SoftwareSerial.h>
#include <SPI.h>
#include <MFRC522.h>

const int     buttonPin = 2;
int           buttonState = 0;
int           modeState = 0;
uint8_t       id;
String        frcUID = "";
int           rfidYes = 0;

SoftwareSerial  mySerial(10, 11);
Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);

MFRC522 mfrc522(53, 5);

void setup() {

  pinMode(buttonPin, INPUT);

  Serial.begin(9600);
  while (!Serial);
```

```
  delay(500);
  SPI.begin();
  mfrc522.PCD_Init();
  mfrc522.PCD_DumpVersionToSerial();

  delay(500);
  Serial.println(". . . Scan sensor . . .");
  finger.begin(57600);
  Serial.println(finger.verifyPassword());
  if (finger.verifyPassword()) {
    Serial.println(". . . Found sensor! . . .");
  }
  else {
    Serial.println(". . . Did not find sensor . . .");
    while (1);
  }
  Serial.println(". . . Please put your finger on the scanner or rfid . . .");

}

void loop() {


  buttonState = digitalRead(buttonPin);

  if (buttonState == HIGH) {
    modeState = 1;
```

```
 }

 switch (modeState) {
  case 0:

    frcUID = "";

    if (finger.getImage()        == FINGERPRINT_OK) {
     if (finger.image2Tz()        == FINGERPRINT_OK) {
      if (finger.fingerFastSearch() == FINGERPRINT_OK) {
          frcUID = ". . . Found ID=" + String(finger.fingerID) + ", confidence=" +
String(finger.confidence) + "! . . .";
        Serial.println(frcUID);
      }
     }
    }

    if (mfrc522.PICC_IsNewCardPresent()) {
     delay(100);
     if (mfrc522.PICC_ReadCardSerial()) {
      frcUID = "";
      for (byte i = 0; i < mfrc522.uid.size; i++) {
       frcUID = frcUID + (mfrc522.uid.uidByte[i]);
      }
      frcUID = ". . . Found RFID UID=" + frcUID + "@ . . .";
      Serial.println(frcUID);
     }
```

```
  }

  delay(100);
  Serial.println(". . . Please put your finger on the scanner or rfid . . .");
  break;

case 1:
  Serial.println(". . . Programming mode . . .");
  delay(400);
  Serial.println(". . . Programming mode . . .");
  delay(400);
  Serial.println(". . . Programming mode . . .");
  delay(400);
  Serial.println(". . . Programming mode . . .");

  id = readnumber();
  if (id >= 255) {
    modeState = 0;
  } else {
    if (id < 254) {
      modeState = 2;
    }
    else {
      modeState = 3;
    }
  }
  break;
```

```
case 2:
  while (!getFingerprintEnroll());
  modeState = 1;
  break;

case 3:
  rfidYes = 0;

  Serial.println(". . . Put RFID in Scanner! . . .");
  delay(400);
  Serial.println(". . . Put RFID in Scanner! . . .");
  delay(400);
  Serial.println(". . . Put RFID in Scanner! . . .");
  delay(5000);

  if (mfrc522.PICC_IsNewCardPresent()) {
    delay(100);
    if (mfrc522.PICC_ReadCardSerial()) {
      frcUID = "";
      for (byte i = 0; i < mfrc522.uid.size; i++) {
        frcUID = frcUID + (mfrc522.uid.uidByte[i]);
      }
      frcUID = ". . . New RFID UID=" + frcUID + "@ . . .";
      rfidYes = 1;
      Serial.println(frcUID);
      delay(400);
```

```
        Serial.println(frcUID);
        delay(400);
        Serial.println(frcUID);
        delay(400);
        Serial.println(frcUID);
      }
    }

    if (rfidYes == 0) {
      Serial.println(". . . RFID error! . . .");
      delay(400);
    }

    modeState = 1;
    break;
  }
}

uint8_t readnumber(void) {
  int num = -1;
  while (num < 0) {
    while (!Serial.available());
    while (Serial.available()) {
      char c = Serial.read();
      if (isdigit(c)) {
        if (num < 0) {
          num = 0;
```

```
      } else {
        num *= 10;
      }
      num += c - '0';
    } delay(5);
  }
 }
 return num;
}

uint8_t getFingerprintEnroll() {
 int p;
 p = -1;
 Serial.println(". . . Please put your new finger on the scanner . . .");

 delay(400);
 Serial.println(". . . Please put your new finger on the scanner . . .");

 delay(400);
 Serial.println(". . . Please put your new finger on the scanner . . .");

 delay(400);
 Serial.println(". . . Please put your new finger on the scanner . . .");


 while (p != FINGERPRINT_OK) {
```

```
   p = finger.getImage();
   switch (p) {
     case FINGERPRINT_OK:  Serial.println(" Ok!");
 break;
     case FINGERPRINT_NOFINGER: Serial.println(". . . Please put your new finger on the scanner . . .");
break;
            case FINGERPRINT_PACKETRECIEVEERR: Serial.println(". . . Communication error . . .");
break;
     case FINGERPRINT_IMAGEFAIL:  Serial.println(". . . Imaging error Please try again . . .");
 break;
     default:    Serial.println(". . . Unknown error Please try again . . .");
 break;
   }
  }
  p = finger.image2Tz(1);
Serial.print  (". . . Image converting . . .");
  switch (p) {
   case FINGERPRINT_OK: Serial.println("Ok!");
break;
   case FINGERPRINT_IMAGEMESS:        Serial.println(". . . Image too messy . . .");                  return p;
        case FINGERPRINT_PACKETRECIEVEERR:        Serial.println(". . . Communication error . . .");              return p;
```

```
    case FINGERPRINT_FEATUREFAIL:         Serial.println(". . . No fingerprint on
image . . .");
 return p;
    case FINGERPRINT_INVALIDIMAGE:        Serial.println(". . . No fingerprint on
image . . .");
 return p;
   default:  Serial.println(". . . Unknown error . . .");
return p;
  }
   p = 0;
  while (p != FINGERPRINT_NOFINGER) {

    Serial.println(". . . Please remove your finger from the scanner . . .");

    delay(400);

    p = finger.getImage();
  }
  Serial.println(" Ok!");

  p = -1;
  Serial.println(". . . Place same finger again . . .");

  delay(400);

  while (p != FINGERPRINT_OK) {
```

```
   p = finger.getImage();
   switch (p) {
     case FINGERPRINT_OK:              Serial.println(" Ok!");
break;
      case FINGERPRINT_NOFINGER: Serial.println(". . . Place same finger again . .
.");
break;
              case    FINGERPRINT_PACKETRECIEVEERR:    Serial.println(".    .    .
Communication error . . .");
break;
     case FINGERPRINT_IMAGEFAIL: Serial.println(". . . Imaging error . . .");

break;
default:                        Serial.println(". . . Unknown error . . .");
break;
   }
  }
  p = finger.image2Tz(2);              Serial.print  (". . . Image 2 converting . . .");

 switch (p) {
   case FINGERPRINT_OK:       Serial.println("Ok!");
 break;
 case FINGERPRINT_IMAGEMESS: Serial.println(". . . Image too messy . . .");

 return p;
   case FINGERPRINT_PACKETRECIEVEERR: Serial.println(". . . Communication
error . . .");
```

```
return p;
    case FINGERPRINT_FEATUREFAIL:        Serial.println(". . . No fingerprint on image . . .");              return p;
     case FINGERPRINT_INVALIDIMAGE: Serial.println(". . . No fingerprint on image . . .");
return p;
default: Serial.println(". . . Unknown error . . .");
return p;
  }

  p = finger.createModel();  Serial.print  (". . . Creating model . . .");
  if (p == FINGERPRINT_OK             ) {
   Serial.println(". . . Model create! Ok! . . .");
  } else
    if (p == FINGERPRINT_PACKETRECIEVEERR) {
     Serial.println(". . . Communication error . . .");
     return p;
    } else
     if (p == FINGERPRINT_ENROLLMISMATCH  ) {
       Serial.println(". . . Fingerprints did not match . . .");
       return p;
     } else
     {
       Serial.println(". . . Unknown error . . .");
       return p;
     }
```

```
p = finger.storeModel(id);

Serial.println(". . . Saving model . . .");

if (p == FINGERPRINT_OK             ) {
  frcUID = ". . . Model save in ID=" + String(id) + "! . . .";
  Serial.println(frcUID);
  delay(1500);
  Serial.println(frcUID);
  delay(400);
  Serial.println(frcUID);
  delay(400);
  Serial.println(frcUID);

} else
  if (p == FINGERPRINT_PACKETRECIEVEERR) {
    Serial.println(". . . Communication error . . .");
    return p;
  } else
    if (p == FINGERPRINT_BADLOCATION     ) {
      Serial.println(". . . Could not store in that location . . .");
      return p;
    } else
      if (p == FINGERPRINT_FLASHERR       ) {
        Serial.println(". . . Error writing to flash . . .");
        return p;
      } else
```

```
        {
          Serial.println(". . . Unknown error . . .");
          return p;
        }
}
```

ДОДАТОК В

ПРОТОКОЛ
ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ НА
НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: Автоматизована система управління пропускною охоронною системою

Тип роботи: бакалаврська дипломна робота
(БДР, МКР)

Підрозділ кафедра обчислювальної техніки
(кафедра, факультет)

Показники звіту подібності Unicheck

Оригінальність 92,9% Схожість 7,1%

Аналіз звіту подібності (відмітити потрібне):

- ✓ Запозичення, виявлення у роботі, оформлені коректно і не містять ознак плагіату.
- □ Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.
- □ Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа, відповідальна за перевірку _____ Захарченко С.М.

Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.

Автор роботи _____ Твердохліб Н.М.

Керівник роботи _____ Богомолов С.В.