

Центральноукраїнський національний технічний університет
Механіко-технологічний факультет
Кафедра кібербезпеки та програмного забезпечення

”Допущено до захисту”
Завідувач кафедри кібербезпеки
та програмного забезпечення
д.т.н., професор
_____ Олексій СМІРНОВ
“ ____ ” _____ 2026 р.

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА
за першим (бакалаврським) рівнем вищої освіти
на тему:

**Програмне забезпечення комп’ютеризованої системи доступу в
приміщення на основі RFID-технології**

Виконав здобувач вищої освіти
IV курсу, групи КІ-22-2
ОПП «Комп’ютерна інженерія»
спеціальності 123 «Комп’ютерна інженерія»
_____ Жиганов А.Б.
« ____ » _____ 2026 р.

Керівник проекту
кандидат технічних наук, доцент
_____ Кислун О.А.
« ____ » _____ 2026 р.

Рецензент _____

Центральноукраїнський національний технічний університет

Факультет *Механіко-технологічний*

Кафедра *Кібербезпеки та програмного забезпечення*

Рівень вищої освіти *бакалавр*

Галузь знань *12* "Інформаційні технології"

Спеціальність *123* "Комп'ютерна інженерія"

Освітньо-професійна (освітньо-наукова) програма *"Комп'ютерна інженерія"*

ЗАТВЕРДЖУЮ

Завідувач кафедри

д.т.н., проф.

Олексій СМІРНОВ

" " 2026 року

ЗАВДАННЯ НА ВИПУСКНУ КВАЛІФІКАЦІЙНУ РОБОТУ ЗА ПЕРШИМ (БАКАЛАВРСЬКИМ) РІВНЕМ ВИЩОЇ ОСВІТИ ЗДОБУВАЧА ВИЩОЇ ОСВІТИ

Жиганову Антону Борисовичу

(прізвище, ім'я, по батькові)

1. Тема роботи *Програмне забезпечення комп'ютеризованої системи доступу в приміщення на основі RFID-технології*

2. Керівник роботи *Кислун Олег Андрійович, канд. техн. наук, доцент*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом закладу вищої освіти від "27" лютого 2026 року №136-02

3. Строк подання роботи до захисту *10.06.2026 р.*

4. Мета та завдання випускної кваліфікаційної роботи. *Метою роботи є розробка програмного забезпечення системи доступу на основі RFID-технології*

5. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Призначення та область використання.

2. Перегляд аналогічних існуючих систем.

3. Опис і обґрунтування проектних рішень.

4. Етапи програмування системи.

5. Впровадження системи в промислову експлуатацію

6. Висновки.

6. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

Структурна схема системи *1 аркуш*

Функціональна схема системи керування *1 аркуш*

Діаграма взаємодії процесів *1 аркуш*

Блок-схема алгоритму роботи *1 аркуш*

Блок-схема алгоритму контролю доступу *1 аркуш*

7. Дата видачі завдання *«27» лютого 2026р.*

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти	Строк виконання етапів випускної кваліфікаційної роботи за першим (бакалаврським) рівнем вищої освіти	Примітка
1.	Аналіз існуючих систем керування	10.03.2026	
2.	Постановка задачі, оформлення ТЗ	15.03.2026	
3.	Розробка моделі компонента	20.03.2026	
4.	Розробка структур даних	25.03.2026	
5.	Розробка алгоритмів зв'язку та відображення	30.03.2026	
6.	Програмування алгоритмів	10.04.2026	
7.	Оформлення ПЗ	17.05.2026	
8.	Попередній захист роботи	23.05.2026	

Дата видачі завдання
«__»_____2026р.

Підпис керівника

(прізвище та ініціали)

Завдання прийнято до виконання
«__»_____2026р.

Підпис здобувача

(прізвище та ініціали)

АНОТАЦІЯ

Жиганов А.Б. Програмне забезпечення комп'ютеризованої системи доступу в приміщення на основі RFID-технології. 123 Комп'ютерна інженерія. Центральноукраїнський національний технічний університет. Кропивницький. 2026.

В даній кваліфікаційній бакалаврській розроблено У кваліфікаційній бакалаврській роботі розглянуто розроблення програмного забезпечення комп'ютеризованої системи доступу до приміщень на основі RFID-технології. Актуальність дослідження зумовлена необхідністю підвищення рівня безпеки, автоматизації контролю доступу та оптимізації обліку робочого часу працівників на підприємствах.

У роботі проведено аналіз сучасних підходів до організації систем ідентифікації та авторизації користувачів, зокрема з використанням RFID-технологій. Обґрунтовано вибір апаратної складової системи та розроблено її структурну організацію. Особливу увагу приділено створенню програмного забезпечення для взаємодії з RFID-зчитувачем, обробки ідентифікаційних даних і передачі їх до серверної частини.

Розроблено архітектуру програмної системи, яка забезпечує зберігання даних у базі, облік робочого часу працівників, а також формування звітної та аналітичної інформації.

Реалізовано функції авторизованого доступу, ведення журналу подій, генерації звітів і візуалізації статистичних показників, що дозволяє оцінювати ефективність використання робочого часу та рівень трудової дисципліни.

Мета роботи – розроблення апаратного та програмного забезпечення системи моніторингу параметрів мікроклімату у виробничих приміщеннях.

Ключові слова: RFID-технологія, система контролю доступу, облік робочого часу, програмне забезпечення, база даних, автоматизація, ідентифікація користувачів.

ABSTRACT

Zhyganov A.B. Software for computerized access control systems based on RFID technology. 123 Computer Engineering. Central Ukrainian National Technical University. Kropyvnytskyi. 2026.

This qualification bachelor's thesis considers the development of software for a computerized access system to premises based on RFID technology.

The relevance of the study is due to the need to increase the level of security, automate access control and optimize the accounting of employees' working hours at enterprises.

The paper analyzes modern approaches to organizing user identification and authorization systems, in particular using RFID technologies.

The choice of the hardware component of the system is justified and its structural organization is developed. Special attention is paid to the creation of software for interaction with an RFID reader, processing identification data and transmitting them to the server part.

The architecture of a software system is developed, which provides data storage in the database, accounting of employees' working hours, as well as the formation of reporting and analytical information.

The functions of authorized access, event logging, report generation and visualization of statistical indicators have been implemented, which allows assessing the efficiency of working time use and the level of labor discipline.

The purpose of the work is to develop hardware and software for a system for monitoring microclimate parameters in production premises.

Keywords: RFID technology, access control system, working time accounting, software, database, automation, user identification.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ	2
ВСТУП.....	3
1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ	3
1.1 Призначення системи.....	5
1.2 Область застосування.....	12
2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ	13
2.1 Огляд існуючих систем, технологій, архітектур та програмних рішень за профілем теми випускної кваліфікаційної роботи за першим (бакалаврським рівнем вищої освіти)	13
2.2 Обґрунтування вибору засобів для побудови системи та мови програмування.....	35
2.3 Розгорнута постановка завдання	37
3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ	38
3.1 Опис функціонування системи	38
3.2 Розробка структурної схеми.....	39
3.3 Розробка функціональної схеми	40
3.4 Розробка діаграми процесів.....	45
4 РЕАЛІЗАЦІЯ РОБОТИ. РОЗРАХУНКИ І ЕКСПЕРИМЕНТАЛЬНІ ДАНІ, ЩО ПІДТВЕРДЖУЮТЬ ВІРНІСТЬ ПРОЕКТНИХ ТА ПРОГРАМНИХ РІШЕНЬ.....	46
4.1 Розробка блок-схем та опис алгоритмів функціонування системи.....	46
4.2 Захист розробленого програмного забезпечення.....	67
5 ВПРОВАДЖЕННЯ СИСТЕМИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ	71
6 ОСНОВНІ ВИСНОВКИ.....	77
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	79

					ВКРБ-123.26.0042.00.00.ПЗ			
Вим	Арк.	№ докум.	Підп.	Дата	Програмне забезпечення комп'ютеризованої системи доступу в приміщення на основі RFID-технології	Лім.	Аркуш	Аркушів
Розроб.	Жиганов А.Б					Б	1	72
Перев.	Кислун О.А					Ков		
Н.контр.	Коваленко А.С					ЦНТУ КІ-22-2		
Затв.	Смірнов О.А.							

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

APM	—	автоматизоване робоче місце
АСУ	—	автоматизована система управління
МК	—	мікроконтролер (microcontroller)
БС	—	дистанційне управління
Arduino Uno	—	апаратно-програмна платформа на МК ATmega328
AVR	—	лінійка мікроконтролерів фірми Atmel
LCD	—	рідкокристалічний індикатор/дисплей
RAM (ОЗП)	—	перативний запам'ятовуючий пристрій
ПДУ	—	пульти дистанційного управління
ПЗ	—	програмне забезпечення
UML	—	Unified Modelling Language
RFID	—	Radio frequency identification

ВСТУП

Стрімкий розвиток інформаційних технологій проявляється в їх активному впровадженні у всі сфери бізнесу, що сприяє автоматизації бізнес-процесів у конкретних предметних областях. Такі технології забезпечують підвищення ефективності, рівня захисту та надійності, продуктивності й гнучкості використання комп'ютеризованих систем, що приносять відчутні переваги власникам бізнесу.

Важливою складовою застосування комп'ютерних систем є організація процесів авторизації та аутентифікації користувачів із визначенням їхніх прав доступу. Зокрема, системи аутентифікації широко застосовуються в автомобільній галузі під час організації запуску двигуна, де іммобілайзер перевіряє відповідність ключа та приймає рішення щодо надання доступу до запуску.

Крім того, сьогодні спостерігається широке використання технологій авторизованого доступу до під'їздів багатоквартирних будинків на основі RFID-міток, у транспортних системах та в інших сферах. Для оцінювання ефективності роботи персоналу впроваджуються програмні або програмно-апаратні засоби контролю робочого часу, що залежить від специфіки діяльності підприємства. Наприклад, контроль робочого часу з можливістю фіксації використаних працівником інструментів реалізовано у програмному забезпеченні Yawage, однак цей продукт переважно орієнтований на компанії, що займаються розробкою програмного забезпечення. У разі потреби створення системи авторизації в інших галузях виникає необхідність комплексного використання апаратних і програмних засобів.

Зазначене завдання є актуальним у сучасних умовах і передбачає розроблення програмно-апаратного комплексу, який забезпечить авторизацію працівників, наприклад, із використанням RFID-технології, а також автоматизує

					ВКРБ-123.26.0042.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		3

процес нарахування заробітної плати залежно від тривалості перебування працівника на робочому місці. Саме розробці комп'ютеризованої системи контролю доступу до приміщення на основі RFID-технології присвячено дану кваліфікаційну роботу.

Передбачається, що ключовими перевагами такої системи стануть ефективна авторизація працівників під час доступу до приміщень підприємства, облік робочого часу, формування статистичної звітності за обраний період для кожного працівника, а також підготовка узагальненого звіту щодо ефективності ведення бізнес-діяльності.

К6ПЗ_2026

					ВКРБ-123.26.0042.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		4

1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ

1.1 Призначення системи

Комп'ютеризована система контролю доступу до приміщень на основі RFID-технології призначена для підвищення ефективності діяльності підприємства, раціонального використання робочого часу та нарахування заробітної плати працівникам відповідно до зафіксованого часу роботи.

Система повинна поєднувати апаратну та програмну складові. У межах бакалаврської кваліфікаційної роботи необхідно виконати аналіз сучасних підходів і технологій організації авторизованого доступу, обрати оптимальне за технічними та економічними критеріями апаратне забезпечення, розробити програмне забезпечення для взаємодії з RFID-сканером, а також спроектувати базу даних для обліку робочого часу та зберігання інформації про працівників. Крім того, потрібно налаштувати сервер бази даних і створити зручний користувацький інтерфейс для роботи зі сканером та базою даних.

Доцільність розроблення комп'ютеризованої системи контролю й управління доступом полягає у забезпеченні авторизації працівників підприємства, формуванні статистичних показників ефективності його діяльності шляхом автоматичного створення звітів і візуалізації даних про перебування персоналу на робочому місці. Основними користувачами системи є адміністративні підрозділи підприємства, зокрема відділ кадрів, бухгалтерія та інші управлінські структури.

Основною метою розроблення комп'ютеризованої системи контролю доступу до приміщень та автоматизація процесу реєстрації авторизованого входу працівників на робоче місце та формування статистичних даних, що використовуються для аналізу ефективності функціонування підприємства.

Для досягнення поставленої мети необхідно вирішити такі завдання:

– виконати аналіз існуючих підходів до організації систем аутентифікації та

					ВКРБ-123.26.0042.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		5

сформувати вимоги до системи авторизованого доступу;

- спроектувати структуру та принципову схему апаратної частини комп'ютеризованої системи;

- обґрунтувати вибір апаратного забезпечення системи;

- розробити програмне забезпечення для зчитування та обробки даних з апаратної частини комп'ютеризованої системи;

- спроектувати архітектуру і реалізувати користувацьке програмне забезпечення комп'ютерної системи;

- забезпечити формування статистичних показників продуктивності праці;

- реалізувати можливість створення звітів різних типів і призначення на основі даних, отриманих із RFID-сканера, зокрема: співвідношення відпрацьованих і пропущених робочих днів, друк звітів щодо робочого часу, побудову діаграм і графіків порушень трудової дисципліни та нарахування штрафних санкцій.

Комп'ютеризована система контролю доступу на основі RFID-технології може застосовуватися на підприємствах і в установах державної та приватної форм власності, де, зокрема, заробітна плата нараховується за погодинною системою оплати праці.

Автоматизація процесів обліку робочого часу працівників і нарахування заробітної плати потребує використання на апаратному рівні таких компонентів:

- мікроконтролера, що забезпечує керування та координацію роботи всієї системи;

- RFID-зчитувача для ідентифікації працівників за допомогою безконтактних міток;

- RFID-міток (карток або брелоків), які використовуються працівниками для авторизації;

- модуля зв'язку (наприклад, Wi-Fi або Ethernet) для передавання даних до сервера або комп'ютера;

- пристрою індикації (LCD-дисплей, світлодіоди або звуковий

					ВКРБ-123.26.0042.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		6

сигналізатор) для відображення стану системи та результатів авторизації;

– виконавчого механізму (електромагнітного замка, сервоприводу тощо) для керування доступом до приміщення;

– джерела живлення, що забезпечує стабільну та безперебійну роботу всіх елементів системи.

На апаратному рівні система передбачає використання:

- RFID-сканера;
- середовища передавання даних;
- сервера обробки даних.

На програмному рівні комп'ютеризована система повинна містити:

- модуль обробки даних, отриманих зі сканера;
- базу даних для зберігання інформації та обліку робочого часу;
- модуль розрахунку заробітної плати.

Під час проектування складових комп'ютеризованої системи, зокрема апаратного та програмного забезпечення, необхідно виконати аналіз предметної області й розробити концептуальні схеми взаємодії компонентів, а також визначити розподіл прав доступу до даних.

Комп'ютеризована система організації доступу на основі RFID-технології має забезпечувати підвищення ефективності функціонування підприємства. На її основі реалізуються функції обліку робочого часу та нарахування заробітної плати, що сприяє зростанню продуктивності праці та покращенню контролю за роботою співробітників різних підрозділів.

Система повинна надавати можливість авторизації працівника, формувати часову мітку для збереження інформації у сховищі даних, а також оперативно й надійно реагувати на спроби несанкціонованого доступу. Загалом у проєктованій системі мають бути забезпечені:

- надійність функціонування апаратної частини;
- точність обліку робочого часу та коректність розрахунку заробітної плати;

					ВКРБ-123.26.0042.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		7

- висока продуктивність програмного забезпечення;
- можливість одночасного доступу різних користувачів до бази даних;
- розмежування прав доступу до інформації;
- ефективне використання часу та ресурсів комп'ютеризованої системи.
- забезпечення зручного та інтуїтивно зрозумілого користувацького інтерфейсу для роботи з RFID-сканером і відповідним програмно-апаратним комплексом.

До складу та функціональної структури комп'ютеризованої системи контролю доступу до приміщення на основі RFID-технології входять:

- мікроконтролер Arduino Uno Rev3;
- RFID-зчитувач SparkFun RFID Reader Breakout;
- RFID-картка (RFID/NFC Card);
- Wi-Fi модуль ESP8266;
- зумер;
- LCD-дисплей;
- сервопривід SG90;
- системне та прикладне програмне забезпечення для Arduino Uno Rev3;
- сервер баз даних;
- база даних обліку та контролю робочого часу;
- клієнтська частина, що забезпечує взаємодію користувачів із базою даних.

Загалом концептуальна модель комп'ютеризованої системи повинна відображати предметну область, зокрема бізнес-процеси авторизації працівників, формування статистичних показників та нарахування заробітної плати на основі фактичного часу перебування на робочому місці. Клієнтська частина програмного забезпечення відповідає за облік даних і забезпечення їхнього захисту.

Функціональні вимоги до комп'ютеризованої системи передбачають:

- можливість зчитування та запису інформації зі сканера;
- введення, редагування та видалення даних про працівників;

- ведення довідників норм робочого часу;
- ведення довідників для нарахування заробітної плати;
- сортування даних про робочий час за визначеними критеріями.
- забезпечення запобігання несанкціонованому (логічному) доступу та можливість формування звітів за облікованим робочим часом;
- можливість керування правами доступу до інформаційних ресурсів;
- розмежування прав доступу між користувачами;
- забезпечення часової ефективності роботи системи на рівні до 2 с;
- масштабованість програмної та апаратної складових комп'ютеризованої системи.

Обмін даними між RFID-карткою та RFID-зчитувачем здійснюється за допомогою електромагнітного поля на відстані до 10 см. RFID-зчитувач, зумер, світлодіоди та модуль ESP8266 безпосередньо підключаються до плати Arduino Uno. Мікроконтролер Arduino Uno приймає дані з унікальним ідентифікатором мітки та через модуль ESP8266 із використанням технології Wi-Fi передає їх на комп'ютер-сервер. Передавання інформації здійснюється за протоколом TCP/IP. У цілому структура та архітектурне рішення комп'ютеризованої системи відповідають моделі «клієнт-сервер».

Перспективи розвитку та модернізації системи передбачають можливість переходу на нові версії мікроконтролерів Arduino або інші платформи, а також інтеграцію додаткових засобів аутентифікації та авторизації, наприклад сканера відбитків пальців, системи розпізнавання обличчя чи введення PIN-коду. При цьому апаратна частина системи не повинна зазнавати суттєвих змін, а програмне забезпечення має залишатися гнучким і придатним до масштабування.

У разі модернізації системи шляхом підключення нових пристроїв і отримання додаткових даних система керування базами даних повинна забезпечувати архівування історичної інформації або додавання нових записів без порушення цілісності наявних даних.

Комп'ютеризована система доступу до приміщення має бути захищена на

					ВКРБ-123.26.0042.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		9

кількох рівнях: фізичному, рівні операційної системи та рівні доступу до бази даних. Фізичний рівень захисту повинен гарантувати надійний контроль доступу до апаратного забезпечення, зокрема мікроконтролера, підключених до нього компонентів, а також сервера.

На рівні операційної системи повинен бути організований доступ на основі визначених прав доступу до використання програмного забезпечення, що функціонує та керує даними при реалізації RFID-технології доступу у приміщення.

Доступ до інформації, що зберігається у базі даних, повинен бути авторизованим на рівні системи керування базами даних. Лише користувачі з наділеним правом доступу та адміністратори мають можливість вносити зміни у базу даних в межах їхньої компетенції.

Функціональні вимоги та задачі, які повинна реалізовувати комп'ютеризована система організації доступу у приміщення на основі RFID-технології полягають в наступному:

- можливість зчитування унікального ідентифікатора RFID-картки;
- формування зворотного зв'язку при успішній чи невдалій аутентифікації працівника;
- передача даних від мікроконтролера до сервера, на якому розгорнуто базу даних;
- забезпечення зв'язку клієнтської частини з базою даних;
- надання точних та адекватних результатів на запит користувачів;
- забезпечення часової ефективності роботи системи;
- забезпечення контролю над доступом до інформації про перебування працівників на робочому місці;
- забезпечення зручності використання програмного продукту;
- формування статистики відвідуваності та можливості фільтрування даних;
- візуалізація графіків перебування працівників на робочому місці;

					ВКРБ-123.26.0042.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		10

- можливість розгортання та створення резервних копій бази даних.

Вимоги до апаратного забезпечення метеостанції на базі Raspberry Pi 3 передбачають використання таких компонентів:

- мікроконтролера Arduino Uno Rev3;
- RFID-зчитувача SparkFun RFID Reader Breakout;
- RFID-картки типу RFID/NFC Card.

До апаратної частини системи також входять:

- Wi-Fi модуль ESP8266;
- зумер;
- LCD-дисплей;
- сервопривід SG90.

Вимоги до клієнтських робочих станцій:

- процесор із тактовою частотою понад 1,8 ГГц та кількістю логічних ядер більше 2;
- оперативна пам'ять не менше 4 ГБ;
- обсяг жорсткого диска не менше 240 ГБ.

Вимоги до сервера:

- процесор із тактовою частотою 2,2 ГГц або потужніший, кількість логічних ядер - понад 8;
- оперативна пам'ять від 16 ГБ;
- дисковий простір не менше 1 ТБ.

Програмне забезпечення клієнтських робочих станцій:

- операційна система Windows 10, платформа .NET Framework та інше необхідне прикладне програмне забезпечення.

Програмне забезпечення сервера: - операційна система Windows Server 2012 та система керування базами даних MS SQL Server 201.

Аналіз структури та особливостей проектування комп'ютеризованих систем на основі RFID-технологій

Радіочастотна ідентифікація (RFID) - це технологія автоматизованої

					ВКРБ-123.26.0042.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		11

ідентифікації (аутентифікації), що використовує спеціальні мітки для передавання даних у відповідь на запити RFID-зчитувача. Порівняно з ідентифікацією на основі штрих-кодів, RFID-мітки забезпечують наявність унікального ідентифікатора (ключа), що сприяє підвищенню рівня конфіденційності користувачів [1].

У базовій реалізації RFID-мітка відповідає на запит зчитувача, передаючи свій фіксований унікальний серійний ідентифікатор. Такий незмінний ключ дає змогу відстежувати мітки та їхніх носіїв, інколи навіть без їхнього відома чи згоди. Окрім унікального серійного ідентифікатора, окремі RFID-мітки можуть зберігати додаткову інформацію про об'єкти, з якими вони пов'язані та до яких вони прикріплені. Отже, власник таких міток потенційно може піддаватися ризику відстеження. Значні зусилля були спрямовані на розв'язання проблем конфіденційності користувачів і промислового шпигунства під час застосування RFID-технології. Проте більшість запропонованих методів передбачають виконання складних або частих криптографічних операцій безпосередньо на RFID-мітках, що суперечить концепції їхньої низької вартості (приблизно 0,05–0,10 дол. США). Зазвичай недорога мітка здатна зберігати лише кілька сотень біт інформації та має логічні ресурси на рівні 5–10 тис. регістрів, з яких лише частина може використовуватися для забезпечення безпеки. Необхідність пошуку компромісу між рівнем криптографічного захисту та низькою вартістю стала однією з ключових проблем у розробленні RFID-міток і стримувала повноцінну заміну технології штрих-кодів.

Для вирішення цієї проблеми було запропоновано нову концепцію RFID-технології. Окрім фіксованого унікального серійного ключа, мітки містять лише замасковані ідентифікатори, що дає змогу запобігти несанкціонованому перехопленню сигналу та відстеженню. Дані про замасковані ідентифікатори зберігаються в базі даних, яка забезпечує інформаційну безпеку, цілісність і надійність системи.

У пасивній RFID-системі зв'язок між зчитувачем і міткою повністю контролюється зчитувачем, тобто мітка не передає дані самостійно, а лише у

					ВКРБ-123.26.0042.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		12

відповідь на запит. Передавання сигналу від зчитувача до мітки називається прямим каналом, тоді як передавання від мітки до зчитувача - зворотним каналом.

Приклад побудови типової комп'ютерної системи з використанням RFID-технології наведено на рисунку 1.1. Коли мітка потрапляє в зону дії RFID-зчитувача, відбувається приймання даних і їх подальше передавання на сервер. Сервер містить спеціалізоване програмне забезпечення для обробки та зберігання отриманої інформації.



Рисунок 1.1 – Принцип організації та структура системи на основі RFID-технології

Безперервна радіочастотна хвиля передається від зчитувача до мітки через прямий канал зв'язку. Передавання даних від сканера до приймача здійснюється у вигляді коротких часових інтервалів, що формуються в амплітудно-модульованій хвилі з використанням кодування Pulse Interval Encoding (PIE). На рисунку 1.2 наведено приклад кодування PIE у протоколі Gen2, де тривалість логічного «0» дорівнює T_0 , а тривалість логічної «1» становить від $1,5T_0$ до $2T_0$, при цьому ширина імпульсу (PW) змінюється в межах від $0,265T_0$ до $0,525T_0$. Значення T_0 лежить у діапазоні від 6,25 мкс до 25 мкс. Таким чином, швидкість передавання

даних у прямому каналі становить від 26,7 Кбіт/с до 128 Кбіт/с.

На рисунку 1.3 показано приклад передавання сигналу з амплітудною маніпуляцією (ASK) із застосуванням імпульсно-інтервального кодування.

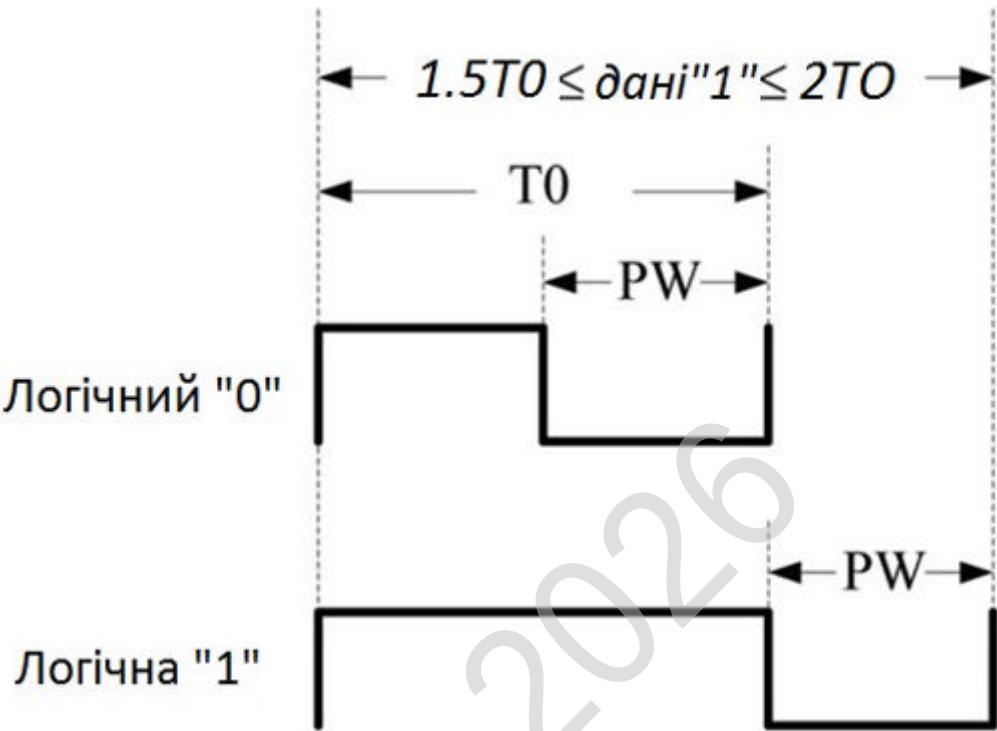


Рисунок 1.2 – Протокол Gen2 кодування PIR

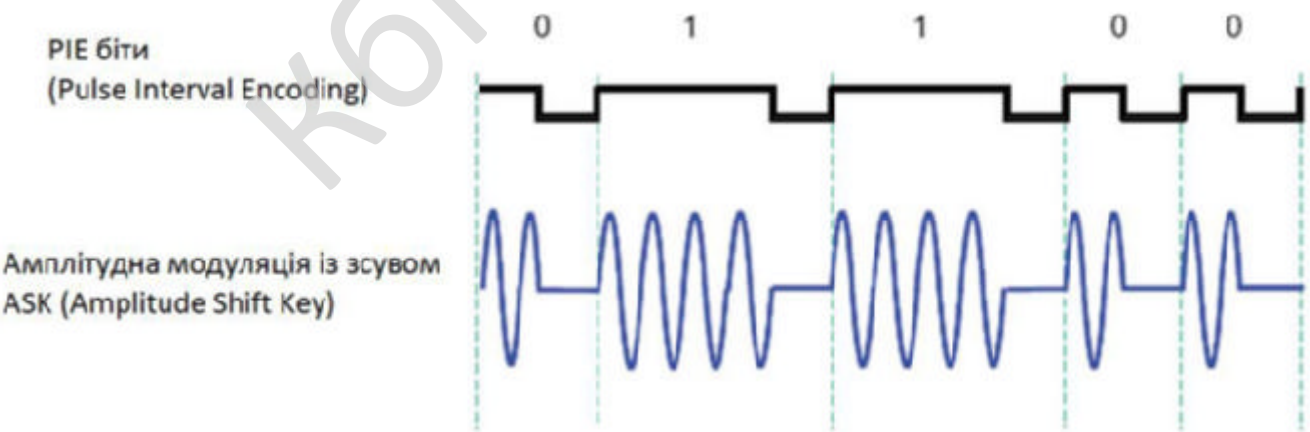


Рисунок 1.3 – Організація прямої передачі даних з використанням амплітудної модуляції із зсувом та PIR кодуванням

1.2 Область застосування

В даній випускні кваліфікаційній бакалаврській роботі буде розроблятися програмне забезпечення системи організації доступу в приміщення на основі RFID-технології.

Застосування RFID-технології продемонструвало високу ефективність у системах автоматизованого контролю переміщення об'єктів, обліку товарно-матеріальних цінностей, а також під час авторизації користувачів для доступу до приміщень з обмеженим доступом. Ця технологія відзначається високою надійністю та стабільною продуктивністю навіть в умовах агресивного навколишнього середовища.

У виробничих і технологічних процесах RFID-мітки дають змогу здійснювати моніторинг об'єктів, підвищувати стабільність та об'єктивність розв'язання логістичних завдань, а також контролювати транспортування продукції.

Технологія радіочастотної ідентифікації широко застосовується в бібліотеках, де вона автоматизує пошук книг, значно спрощує облік та інвентаризацію, прискорює обслуговування читачів і зменшує ризик крадіжок. У сфері торгівлі RFID ефективно використовується для ідентифікації товарів та запобігання їх несанкціонованому винесенню.

Залежно від способу живлення RFID-мітки поділяють на два основні класи: пасивні та активні. Пасивні мітки не мають власного джерела живлення і зазвичай містять лише унікальний ідентифікатор. Принцип їх роботи полягає в тому, що зчитувач генерує сигнал, який через антену передається мітці, після чого мітка відбиває його назад, модулюючи відбитий сигнал.

Пасивні високочастотні мітки зазвичай працюють на відстані від 1 см до 2 м. Використання вищих частот, зокрема в діапазонах 860–960 МГц і 2,4–2,5 ГГц, дозволяє збільшити дальність взаємодії приблизно до 1–10 м.

Активні RFID-мітки, на відміну від пасивних, мають власне автономне

					ВКРБ-123.26.0042.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		15

джерело живлення і не залежать від енергії зчитувача. Їх перевагою є можливість роботи на значно більшій відстані - до 300 м. Крім того, такі мітки можуть містити додаткові сенсори, наприклад для метеоспостереження (вимірювання температури, вологості тощо).

Суттєвими перевагами активних RFID-міток порівняно з пасивними є підвищена надійність і точність роботи, а також можливість застосування в складних умовах, зокрема за низьких температур, у середовищах із металевими конструкціями, у морських портах та інших промислових об'єктах.

До недоліків активних RFID-міток належать їх відносно висока вартість, а також необхідність періодичної заміни елементів живлення.

Окрім цього, існують гібридні RFID-мітки, що поєднують властивості пасивних і активних та оснащені власним джерелом живлення. Особливістю таких міток є те, що дальність їх спрацювання визначається переважно чутливістю RFID-зчитувача.

Під час реалізації RFID-міток можуть застосовуватися різні типи пам'яті:

- **мітки тільки для читання (Read Only)** - передбачають одноразовий запис інформації на етапі виробництва, що забезпечує високий рівень захисту та точність ідентифікації;

- **мітки одноразового запису і багаторазового читання (Write Once Read Many)** - містять унікальний ідентифікатор і модуль для одноразового запису з можливістю подальшого багаторазового зчитування;

- **мітки багаторазового запису і читання (Read and Write)** - мають унікальний ідентифікатор і пам'ять, що дозволяє багаторазово записувати та зчитувати інформацію.

Залежно від робочої частоти RFID-мітки поділяють на такі категорії [1]:

- **низькочастотні** - працюють у діапазоні 125–134 кГц, відповідають другій частині стандарту ISO/IEC 18000, характеризуються низькою вартістю та найчастіше використовуються, зокрема, для ідентифікації домашніх тварин;

					ВКРБ-123.26.0042.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		16

– **високочастотні** - широко застосовуються у платіжних системах, логістичних процесах, системах ідентифікації та авторизації користувачів, є відносно недорогими, відповідають третій частині стандарту ISO/IEC 18000 і не потребують додаткових екологічних чи ліцензійних сертифікатів.

– **ультрависокочастотні** – мітки, що працюють у діапазоні частот від 860 МГц до 960 МГц, відповідають стандарту ISO/IEC 18000-63, характеризуються механізмами запобігання колізіям та здатністю функціонувати на значних відстанях;

– **радіочастотні ультрависокочастотного спектру** мітки ближнього поля характеризуються здатністю ефективно працювати у магнітному полі антени сканера за агресивних умов навколишнього середовища (висока вологість, низька температура, водне середовище чи металоконструкції).

Залежно від умов і способів застосування RFID-мітки класифікують за призначенням таким чином:

- мітки, призначені для використання на металевих конструкціях;
- мітки, застосування яких не пов'язане з металевими об'єктами;
- універсальні мітки, придатні для роботи в різних умовах.

Узагальнену характеристику та класифікацію RFID-міток наведено на рисунку 1.4.

					ВКРБ-123.26.0042.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		17

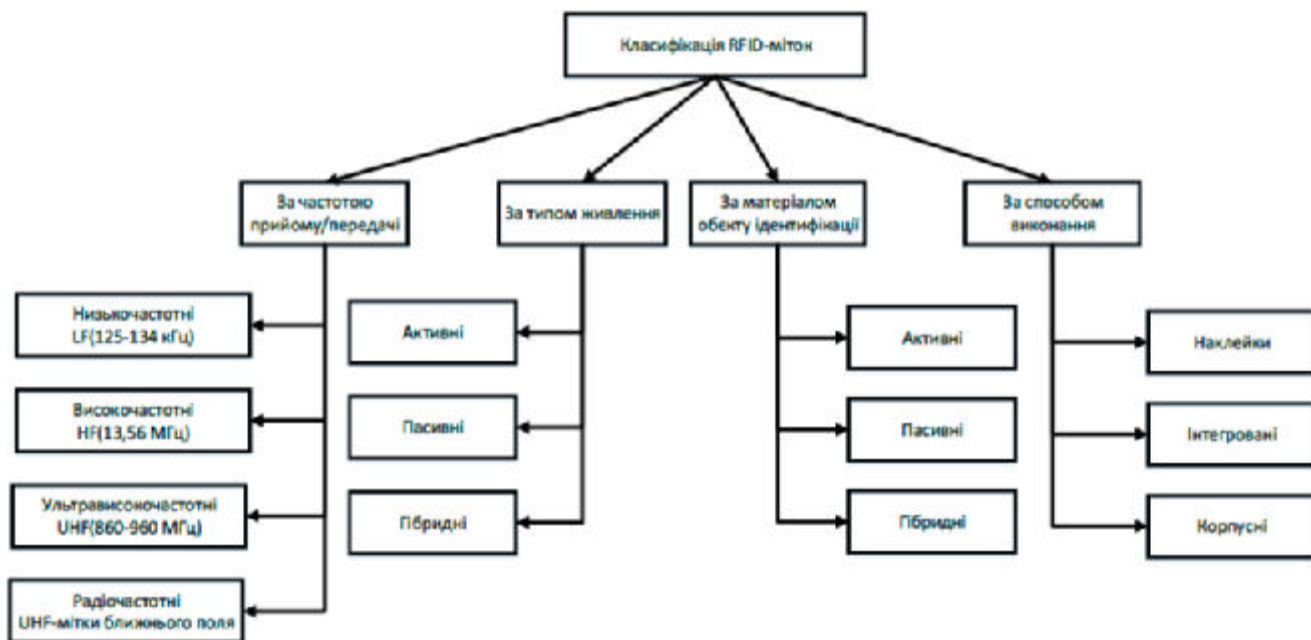


Рисунок 1.4 – Класифікація RFID-міток

Отже, на основі проведеного аналізу особливостей RFID-технології та класифікації RFID-міток можна зробити висновок, що під час проєктування комп'ютеризованої системи доступу до приміщення доцільно використовувати пасивні ультрависокочастотні RFID-мітки універсального призначення.

2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ

2.1 Огляд існуючих систем, технологій, архітектур та програмних рішень за профілем теми випускної кваліфікаційної роботи за першим (бакалаврським рівнем вищої освіти)

Проектування архітектури комп'ютеризованої системи доступу у приміщення

Проектування комп'ютеризованої системи доступу до приміщення на основі RFID-технології передбачає врахування функціональних вимог, визначених у технічному завданні (додаток А).

До основних апаратних компонентів системи належать:

- RFID-зчитувач (сканер) - пристрій, призначений для отримання даних із RFID-міток або карток;
- RFID-мітка (картка) - носій інформації, що містить унікальний ідентифікатор працівника;
- Wi-Fi маршрутизатор - використовується для передавання даних від зчитувача до сервера баз даних;
- сервер баз даних - призначений для зберігання та обробки інформації про авторизацію працівників.

Під час проектування архітектури системи необхідно також визначити групи користувачів, які матимуть доступ до комп'ютеризованої системи з метою її адміністрування та експлуатації. Відповідно до технічного завдання такими групами є:

- адміністратор системи - відповідає за налаштування параметрів доступу до RFID-зчитувача, Wi-Fi маршрутизатора та сервера баз даних;
- працівники бухгалтерії - мають визначені права доступу до бази даних для отримання інформації, необхідної для нарахування заробітної плати на основі

					ВКРБ-123.26.0042.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		19

автоматично зафіксованого робочого часу кожного працівника;

- працівники відділу кадрів - мають доступ до зовнішньої схеми бази даних для контролю дисципліни перебування працівників на робочому місці;
- керівник підприємства - має доступ до інформації, що зберігається на сервері бази даних, для аналізу діяльності підприємства.
- Архітектуру комп'ютеризованої системи контролю доступу до приміщення на основі RFID-технології наведено на рисунку 2.1.

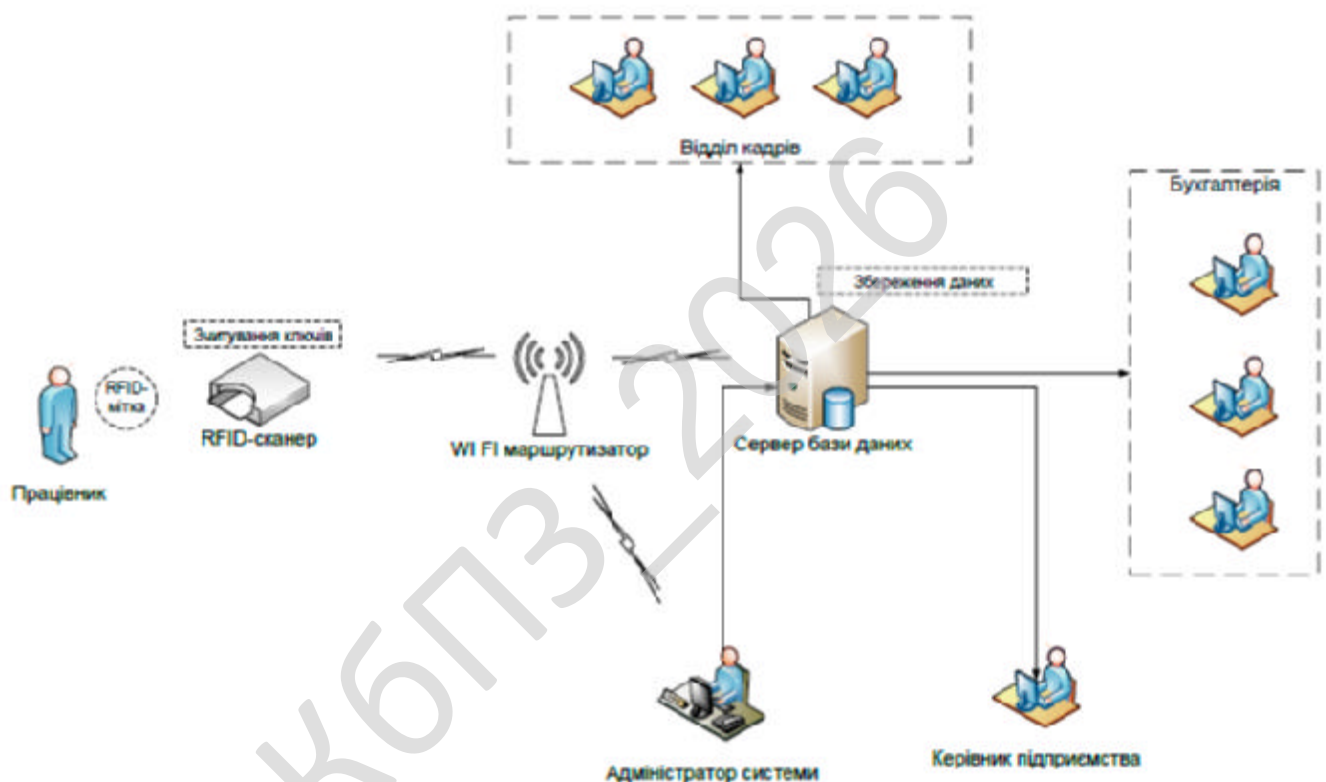


Рисунок 2.1 – Архітектура комп'ютеризованої системи доступу у приміщення на основі RFID-технології

Після розроблення архітектури системи на високому концептуальному рівні наступним етапом досягнення мети роботи є обґрунтування вибору апаратного забезпечення для авторизації працівників із використанням RFID-міток, а також розроблення системного та прикладного програмного забезпечення.

2.2 Обґрунтування вибору засобів для побудови системи та мови програмування

Обґрунтування мікроконтролера для управління процесом зчитування та передачі даних на основі RFID-технології

Для створення прототипу комп'ютеризованої системи контролю доступу до приміщення на основі RFID-технології доцільно використати плату Arduino Uno R3. З огляду на її технічні характеристики та доступну вартість, вона є оптимальним вибором для реалізації поставленого завдання. На рисунку 2.2 наведено зовнішній вигляд і розташування виводів плати Arduino Uno R3.

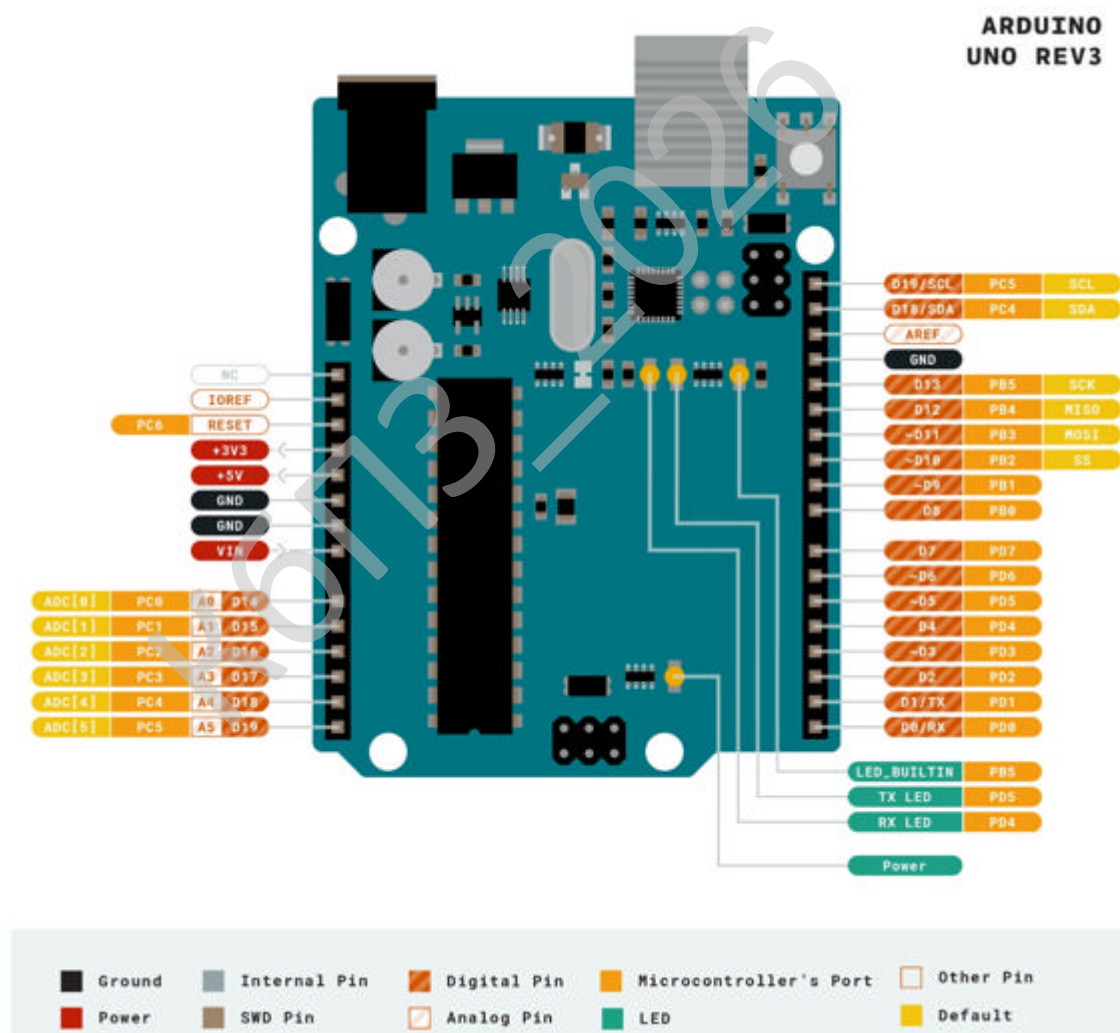


Рисунок 2.2 – Arduino UNO REV 3

До складу Arduino Uno R3 входять 6 аналогових виводів та 14 цифрових, що дозволяє підключити відповідно аналогові та цифрові пристрої. Більш детально технічні характеристики цієї плати представлено у таблиці 2.1, а компоненти плати на рисунку 2.3.

Таблиця 2.1 – Характеристики Arduino Uno R3

Характеристика	Значення
Тип мікроконтролера	ATmega328P
Операційна напруга	5В
Вхідна напруга (рекомендована)	7-12В
Вхідна напруга (крайні значення)	6-20В
Цифрові входи/виходи	14
Цифрові виходи	6
Аналогові входи	6
Живлення (струм) виводів входу/виходу 5В	20 мА
Живлення (струм) виводів входу/виходу 3,3В	50 мА
Flash пам'ять	32 КБ (ATmega328P)
SRAM	2 КБ
EEPROM	1 КБ
Частота процесора	16 МГц
Довжина	68.6 мм
Ширина	53.4 мм
Вага	25 г

Живлення подається на виводи VCC та GND мікроконтролера і не повинно перевищувати значень, визначених у технічній документації. Для мікроконтролера ATmega328P верхня межа рекомендованої напруги живлення становить 5,5 В, тоді як абсолютне максимальне значення — 6 В. Тривала експлуатація при такій напрузі може призвести до пошкодження мікроконтролера.

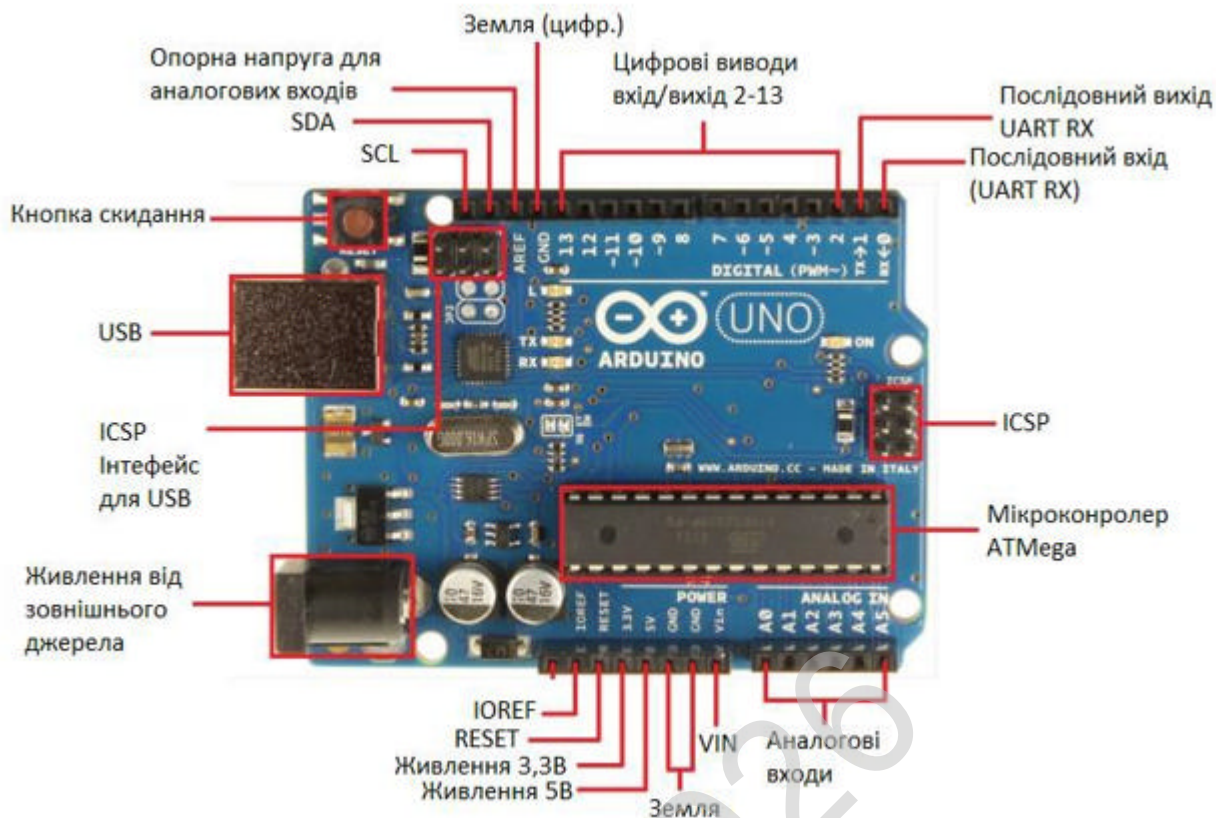


Рисунок 2.3 – Призначення компонентів опис компонентів Arduino UNO REV 3

Плата розробки Arduino Uno R3 створена на основі мікроконтролера ATmega328, розташування виводів якого наведено на рисунку 2.4.

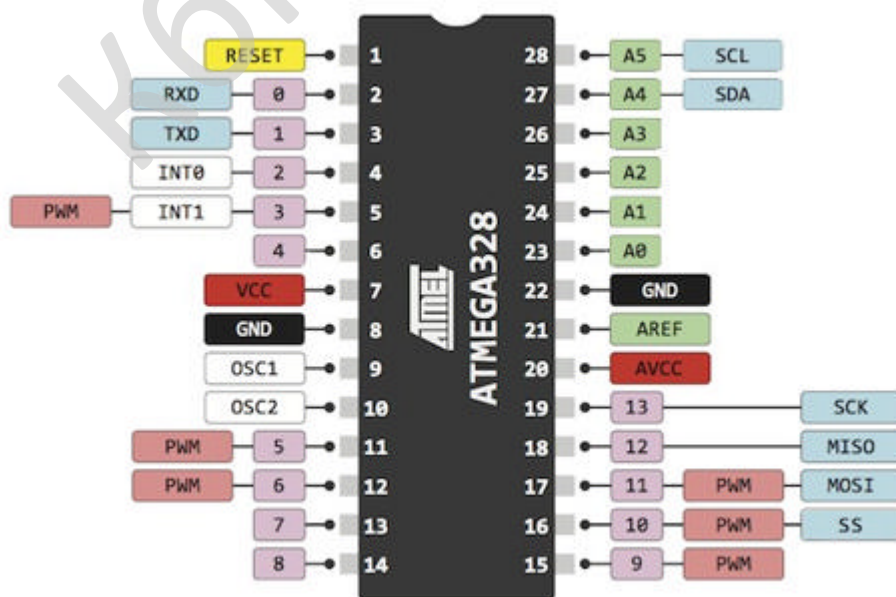


Рисунок 2.4 – Розпіновка мікроконтролера ATМega 328

Для зменшення впливу високочастотних завад у колі живлення рекомендується встановлювати керамічний конденсатор ємністю 0,1 мкФ між виводами VCC і GND. При цьому конденсатор слід розміщувати якомога ближче до контактів живлення мікроконтролера, щоб мінімізувати паразитну індуктивність і опір підвідних провідників. Мікроконтролер ATmega328P має подвійне живлення: виводи VCC і GND (контакти 7 і 8) використовуються для живлення цифрової частини, тоді як AVCC і GND (контакти 20 і 22) призначені для живлення аналого-цифрового перетворювача.

Електричну принципову схему плати Arduino Uno R3 наведено на рисунку. 2.5.

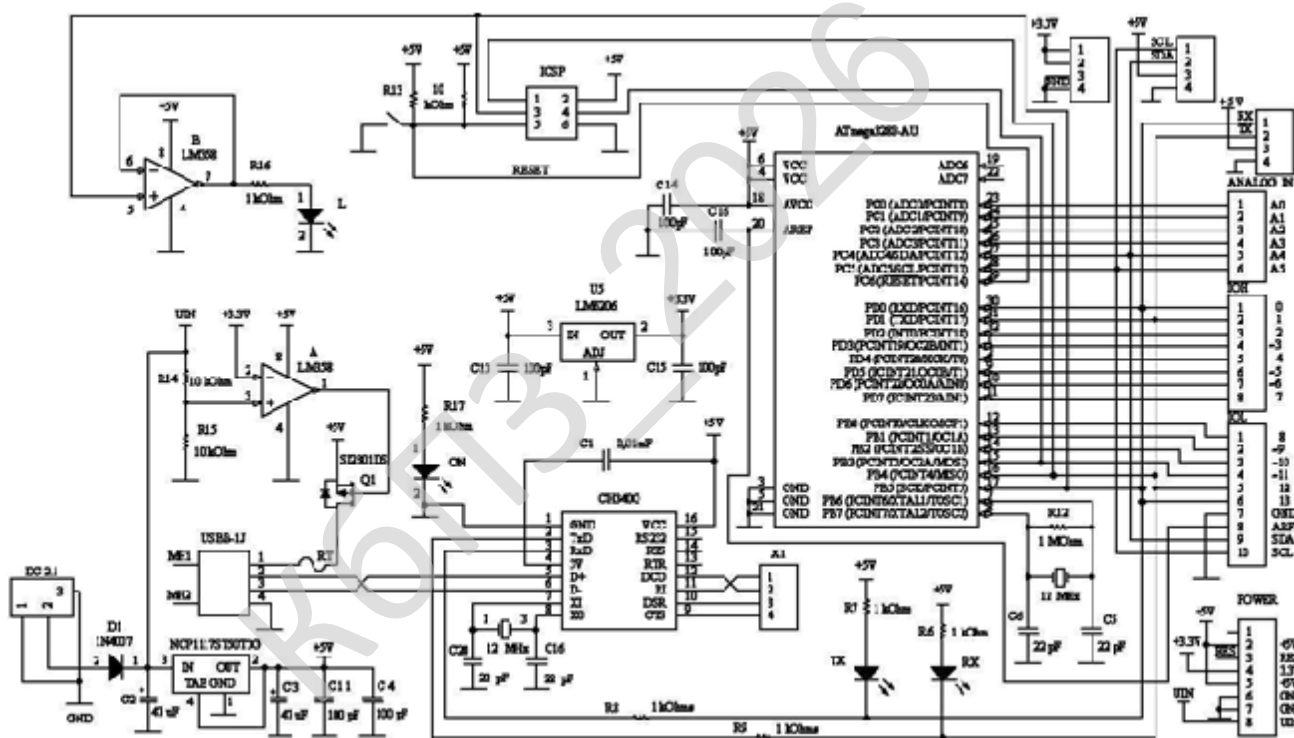


Рисунок 2.5 – Схема електрична принципова Arduino Uno R3

На підставі проведеного аналізу можна зробити висновок, що плата Arduino Uno R3 є достатньою для реалізації комп'ютеризованої системи контролю доступу до приміщення на основі RFID-технології. Вона забезпечує можливість підключення та керування пристроями зчитування радіочастотних міток, передавання даних за допомогою технології Wi-Fi, а також керування

сервоприводом, який імітує роботу дверного замка.

Крім того, до Arduino Uno R3 можна підключити LCD-дисплей і світлодіоди, що виконуватимуть функцію індикаторів готовності системи до зчитування унікального ідентифікатора RFID-мітки.

Обґрунтування вибору і технічні характеристики RFID-компонентів



Рисунок 2.6 – Типова схема організації взаємодії між RFID-сканером та RFID-міткою

Організацію сканера RFID-міток запропоновано організувати на основі SparkFun RFID Reader. Цей RFID-зчитувач виконує дві функції: передачу та прийом. До його складу входять:

- антена;
- радіочастотний модуль;
- блок управління.

На рисунку 2.7 показано зовнішній вигляд плати SparkFun RFID Reader, а на рисунку 2.8 – його структурну схему.



Рисунок 2.7 – Зовнішній вигляд SparkFun RFID Reader

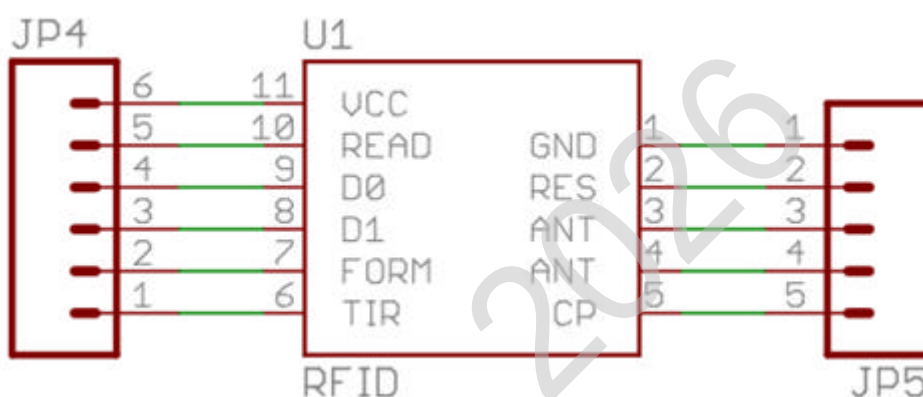


Рисунок 2.8 – Структурна схема SparkFun RFID Reader

Основні технічні характеристики модуля SparkFun RFID Reader:

- напруга живлення - 3,3 В;
- робоча частота - 13,56 МГц.

Схему можливих підключень модуля SparkFun RFID Reader (MFRC522) наведено в таблиці 2.2.

Таблиця 2.2 – Схема з'єднання MFRC522 з Arduino Uno R3

Виводи MFRC522	Виводи Arduino Uno
GND	GND
NC	NC
MISO	12/ICSP-1
MOSI	11/ICSP-4
SCK	13/ICSP-3
SDA	10

Для перевірки роботи RFID-зчитувача доцільно використати RFID-мітку у формі картки, наприклад Adafruit RFID/NFC Card, зображення якої наведено на рисунку 2.9.



Рисунок 2.9 – RFID/NFC карта

RFID/NFC-картка працює на частоті 13,56 МГц і може застосовуватися, зокрема, у системах оплати проїзду в поїздах, маршрутних автобусах, а також в інших рішеннях, де потрібен безконтактний доступ. Така мітка містить мікрочіп і антену та отримує живлення пасивно від пристрою зчитування/запису, що знаходиться на невеликій відстані. Більшість RFID/NFC-зчитувачів із частотою 13,56 МГц здатні працювати з такими картками, однак перед використанням необхідно перевірити у технічній документації зчитувача його сумісність і

підтримку стандарту ISO/IEC 14443 типу A.

Дані мікросхеми здатні записувати та зберігати до 1 КБ інформації в енергонезалежній пам'яті EEPROM, поділений на окремі блоки, а також витримують понад 100 000 циклів перезапису. Крім того, мікросхема містить постійний 4-байтовий унікальний ідентифікатор, який використовується для однозначної ідентифікації RFID-мітки.

Основні технічні характеристики RFID/NFC-мітки:

- 1 КБ (8 Кбіт) енергонезалежної пам'яті EEPROM;
- вбудований механізм шифрування з 48-бітним ключем, що включає 4 байти унікального ідентифікатора;
- робоча частота - 13,56 МГц;
- габаритні розміри - $85,5 \times 54 \times 1$ мм;
- маса - 6,3 г;
- відстань спрацювання - до 10 см від зчитувача.

LCD дисплей візуалізації стану RFID-зчитувача

Для відображення інформації про стан зчитувача та результати ідентифікації у комп'ютеризованій системі доступу на основі RFID-технології доцільно використати недорогий дворядковий LCD-дисплей на 16 символів. Плати Arduino підтримують підключення дисплеїв такого типу.

Водночас слід враховувати, що більшість платформ Arduino мають обмежену кількість ліній вводу/виводу, тому доцільно застосовувати спеціальні дисплейні модулі з інтерфейсною платою, яка забезпечує передавання даних через послідовний інтерфейс, наприклад I2C. Це дозволяє суттєво зменшити кількість задіяних контактів мікроконтролера. Для підключення дисплея з паралельним інтерфейсом можна використати перехідник I2C/TWI, з'єднавши його з одного боку з платою Arduino, а з іншого - з дисплеєм. Однією з найпоширеніших інтерфейсних плат у складі серійних LCD-модулів є LCM1602ПС, яка дає змогу використовувати лише два інформаційні канали Arduino разом із лініями живлення.

					ВКРБ-123.26.0042.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		28

На рисунку 2.10 показано схему з'єднання LCD дисплею, плати LCM1602IIC з Arduino Uno.

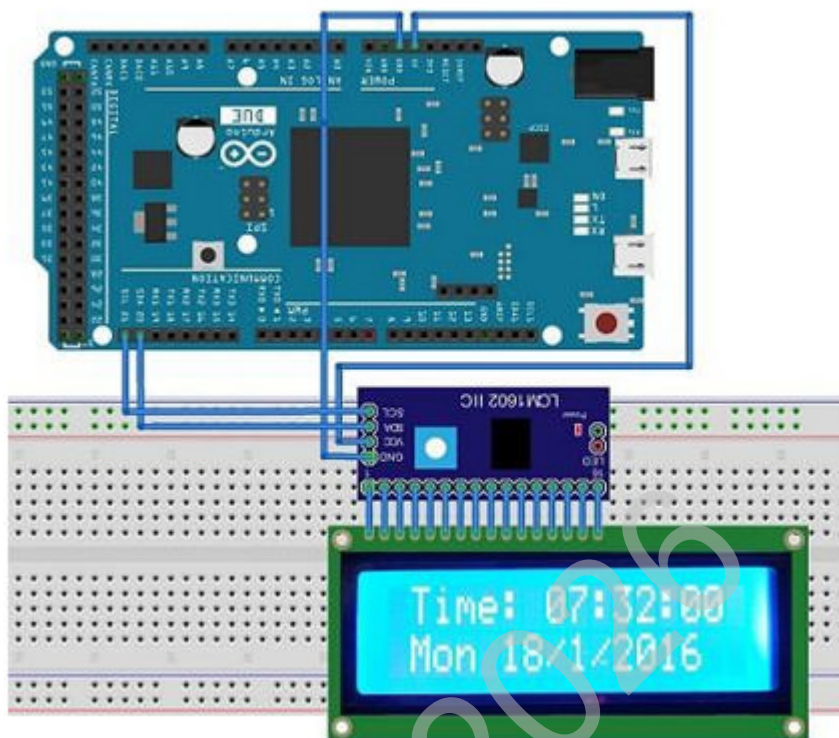


Рисунок 2.10 – Схема з'єднання LCD дисплею з Arduino Uno

LCD-дисплей у комп'ютеризованій системі контролю доступу до приміщення використовується для відображення інформації про стан зчитувача у поєднанні з трьома світлодіодами (жовтим, зеленим і червоним) та зумером. Зумер подає звуковий сигнал під час зчитування RFID-мітки. Індикація результату авторизації здійснюється таким чином:

- жовтий світлодіод і повідомлення «Очікування мітки»;
- зелений світлодіод і повідомлення «Доступ дозволено»;
- червоний світлодіод і повідомлення «Доступ заборонено».

Сервопривід

Сервопривід - це мотор-редуктор, який здатний повертати вал у задане положення та утримувати його, запобігаючи самовільному зміщенню. У даній системі сервопривід використовується для імітації роботи дверного замка.

Для моделювання роботи дверного замка доцільно використати

сервопривід SG-90, зовнішній вигляд і габаритні розміри якого наведено на рисунку 2.11.

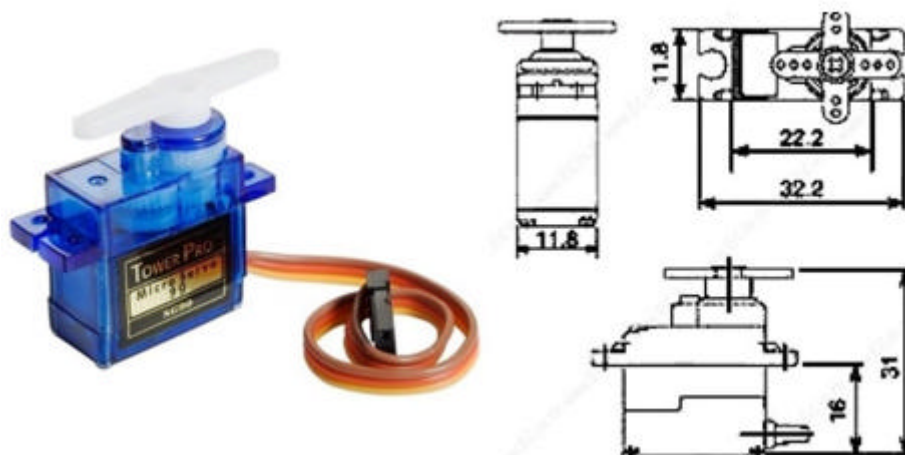


Рисунок 2.11 – Сервопривід SG-90

Під час підключення до плати Arduino та у процесі роботи сервопривід SG-90 використовує три контакти, як показано на рисунку 2.12.



Рисунок 2.12 – Виводи для з'єднання у SG-90

Робоча напруга живлення сервопривода SG-90 знаходиться в діапазоні від 4,8 В до 6 В. Час повороту на кут 60° становить приблизно 0,12 с, а крутний момент - близько 1,2 кг·см при напрузі 4,8 В.

Модуль взаємодії Arduino Uno з Wi Fi роутером

Як Wi-Fi модуль для підключення плати Arduino Uno до сервера бази даних через маршрутизатор доцільно використати модуль ESP8266, зовнішній вигляд якого наведено на рисунку 2.13.

Зазначений модуль забезпечує обмін даними між RFID-зчитувачем і маршрутизатором через технологію Wi-Fi, що дає змогу фіксувати час події та

результат авторизації RFID-мітки у базі даних, розміщених на сервері.



Рисунок 2.13 – Модуль ESP8266

Основні технічні характеристики модуля ESP8266:

- підтримка стандартів бездротового зв'язку IEEE 802.11 b/g/n/e/i;
- робочий діапазон частот - 2,4–2,5 ГГц;
- процесор - 32-розрядний Tensilica L106;
- напруга живлення - у межах 2,5–3,6 В;

Режими роботи:

- Wi-Fi станція, точка доступу та комбінований режим;
- підтримка протоколів безпеки WPA/WPA2;
- підтримка типів шифрування WEP, TKIP, AES;
- підтримка мережевих протоколів IPv4, TCP, UDP, HTTP, FTP;
- підтримка Wi-Fi Direct (P2P), включно з режимами P2P Discovery, Group Owner (GO), Group Client (GC) та керуванням енергоспоживанням P2P;
- наявність вбудованих апаратних прискорювачів: CCMP (CBC-MAC, режим лічильника), TKIP (MIC, RC4), WAPI (SMS4), WEP (RC4), CRC;
- підтримка мови програмування Lua.

Огляд існуючих СКД та їх порівняння

Окрім RFID-технологій, у сучасних системах керування доступом (СКД) широко застосовуються інші методи ідентифікації. Зокрема, значного поширення набули біометричні системи, які використовують унікальні фізіологічні характеристики людини – відбитки пальців, райдужну оболонку ока або риси обличчя – для забезпечення високого рівня автентифікації.

Також активно розвиваються мобільні СКД, що базуються на використанні смартфонів і спеціалізованих застосунків. Кодові замки з PIN-кодами залишаються економічно доступним рішенням для базового рівня безпеки. Системи на основі магнітних карток зберігають актуальність завдяки розвиненій інфраструктурі та простоті впровадження.

СКД можна класифікувати за архітектурою, способом ідентифікації, рівнем захисту та сферою застосування.

Біометричні системи

Біометричні СКД здійснюють ідентифікацію користувача на основі його унікальних фізіологічних параметрів – відбитків пальців, іридограми або геометрії обличчя. Завдяки складності підробки біометричних даних такі системи забезпечують високий рівень безпеки та застосовуються на об'єктах із підвищеними вимогами до захисту (банківські установи, державні структури тощо).

Syphrax FRD є настільним біометричним зчитувачем відбитків пальців, призначеним для організації безпечного доступу. Пристрій дозволяє реєструвати та зберігати відбитки користувачів для подальшої автентифікації, що підвищує рівень захисту порівняно з традиційними методами (паролі або фізичні ключі).

Підключення здійснюється через USB-інтерфейс, а інтеграція з операційними системами можлива, зокрема, завдяки підтримці технологій типу Windows Hello. Це забезпечує зручність використання та розширені можливості інтеграції у сучасні IT-інфраструктури (рисунок 2.14).

					ВКРБ-123.26.0042.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		32



Рисунок 2.14 – Біометричний настільний зчитувач відбитків пальців
Cyphrax FRD

Мобільні системи керування доступом

Мобільні СКД базуються на використанні персональних мобільних пристроїв, зокрема смартфонів, як засобів ідентифікації користувача. Передача даних для надання доступу здійснюється за допомогою бездротових технологій - Wi-Fi, Bluetooth або мобільних мереж - через спеціалізовані мобільні застосунки. Популярність таких систем зростає завдяки їхній зручності, оскільки вони усувають потребу у фізичних ідентифікаторах та забезпечують можливість дистанційного керування правами доступу.

Одним із відомих рішень у цій категорії є система HID Mobile Access, яка дозволяє організувати керування доступом за допомогою смартфона. Її робота ґрунтується на використанні бездротових протоколів зв'язку, зокрема Bluetooth, NFC та Wi-Fi, для автентифікації користувачів. Це забезпечує високий рівень зручності, гнучке адміністрування та можливість інтеграції з сучасними системами безпеки (рисунок 2.15).



Рисунок 2.15 - HID Mobile Access

					ВКРБ-123.26.0042.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		33

Кодові замкові системи

Кодові системи керування доступом функціонують на основі введення користувачем унікального цифрового або буквено-цифрового коду за допомогою клавіатури. Після введення правильного PIN-коду система здійснює перевірку відповідності введених даних збереженій інформації та, у разі збігу, надає доступ до приміщення чи об'єкта.

Перевагами таких систем є простота встановлення, відносно низька вартість та відсутність необхідності у фізичних носіях (картках або ключах). Вони широко застосовуються в житлових будинках, офісах, складських приміщеннях та інших об'єктах із базовими вимогами до безпеки.

Водночас кодові замки мають певні недоліки. Основним із них є ризик компрометації коду через його передачу третім особам або підбір. Крім того, часте використання може призводити до зношування клавіш, що потенційно дозволяє визначити найбільш уживані символи. Тому такі системи зазвичай рекомендуються для об'єктів із середнім або базовим рівнем захисту (рисунки 2.16).



Рисунок 2.16 – Кодовий замок Yale Assure Lock

СКД на основі магнітних карток

Системи керування доступом цього типу використовують ідентифікаційні картки з магнітною смугою, на якій зберігається закодована інформація про користувача. Зчитування даних здійснюється за допомогою спеціальних рідерів,

					ВКРБ-123.26.0042.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		34

після чого система перевіряє права доступу та приймає рішення щодо відкриття замка.

Попри те, що рівень безпеки таких систем є нижчим порівняно з RFID (через можливість копіювання магнітної смуги), вони залишаються поширеними завдяки невисокій вартості впровадження та наявності розвиненої інфраструктури, особливо в уже функціонуючих системах контролю доступу.

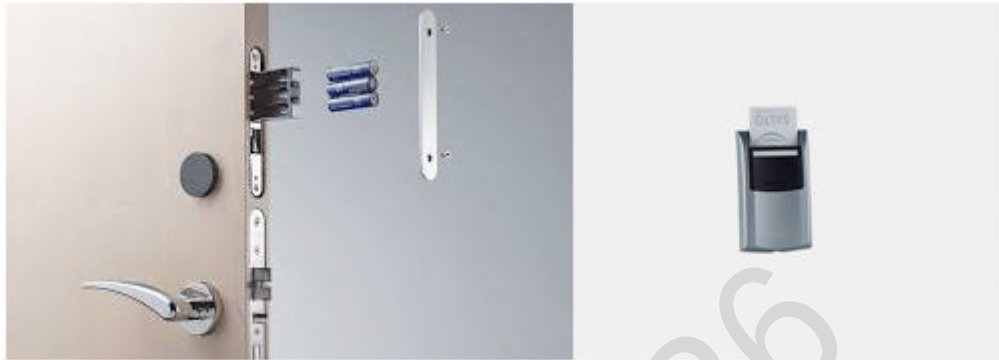


Рисунок 2.17 - Salto Systems

Salto Systems є відомим виробником електронних замків і рішень для контролю доступу, зокрема для готельного та комерційного секторів. Системи на основі магнітних карток, запропоновані компанією, відзначаються надійністю, зручністю використання та простотою адміністрування, що робить їх популярним вибором серед готелів та бізнес-центрів (рисунок 2.18).



Рисунок 2.18 – Апаратна платформа СКД XS4 SALTO [5]

Вибір конкретної системи керування доступом визначається сукупністю чинників, серед яких вирішальне значення має сфера та умови її застосування.

					ВКРБ-123.26.0042.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		35

Біометричні системи отримали широке поширення завдяки високому рівню безпеки, що забезпечується унікальністю та невідчужуваністю біометричних характеристик користувача, що робить їх доцільними для об'єктів із підвищеними вимогами до захисту.

Мобільні системи набувають популярності завдяки зручності використання та можливості оперативного керування правами доступу через програмні інтерфейси, що є особливо важливим для великих організацій із розгалуженою інфраструктурою. Кодові замкові системи відзначаються простотою експлуатації та відсутністю необхідності у фізичних носіях, що дозволяє знизити витрати на обслуговування та впровадження.

Системи на основі магнітних карток, попри певні обмеження щодо рівня безпеки, залишаються актуальними завдяки доступності, економічній доцільності та сумісності з уже існуючими системами, особливо на об'єктах зі сформованою інфраструктурою. Таким чином, вибір СКД повинен ґрунтуватися на балансі між рівнем безпеки, зручністю використання, вартістю впровадження та специфікою об'єкта.

Таблиця 2.3 – Порівняння основних СКД

№	Система	Рівень безпеки	Зручність	Вартість	Приклади використання
1	Біометричні системи	Високий	Середній	Висока	Банки, урядові установи
2	Мобільні системи	Середній-Високий	Висока	Середня	Офіси, житлові комплекси

Наведена порівняльна таблиця дозволяє наочно оцінити, чому кожен тип системи керування доступом займає власну нішу на ринку, що визначається співвідношенням рівня безпеки, зручності використання та вартості впровадження.

Технологія безконтактного ближнього радіозв'язку (Near Field

Communication, NFC), попри спорідненість із RFID, є окремим технічним рішенням. У деяких випадках NFC може розглядатися як альтернатива завдяки підвищеним можливостям захисту та підтримці сучасних протоколів безпеки. Водночас у межах даного дослідження основна увага приділяється системам керування доступом, що не використовують радіочастотний спектр, зокрема біометричним і мобільним технологіям.

Таким чином, різноманіття сучасних СКД відображає необхідність адаптивного підходу до вибору рішень. Спектр технологій варіюється від високозахищених біометричних систем до економічно доступних кодових замків. Вибір оптимальної системи залежить від конкретних умов експлуатації, зокрема рівня потенційних загроз, фінансових можливостей та наявної технічної інфраструктури. Це підкреслює багатогранність досліджуваної проблеми та визначає перспективи подальших досліджень і вдосконалення систем керування доступом.

2.3 Розгорнута постановка завдання

Згідно з технічним завданням на кваліфікаційну роботу, реалізації розробка програмного забезпечення системи організації доступу в приміщення на основі RFID-технології

В процесі розробки кваліфікаційної роботи необхідно виконати наступний обсяг проекту:

а) провести аналіз існуючих систем-аналогів для виявлення їх позитивних і негативних якостей. Результати аналізу врахувати в подальших розробках.

б) вибрати та обґрунтувати методику розробки відповідної системи та програмного забезпечення. Розробити функціональну та структурну схеми системи;

в) розробити програмне забезпечення системи, що дозволить реалізувати поставлену технічним завданням задачу. Побудувати блок-схеми алгоритмів

програми та підпрограми;

г) організувати інтерфейс користувача з метою формування та виводу на екран результатів аналізу та тестування;

д) розробити рекомендації по організаційних та методичних заходах, які забезпечать впровадження системи в промислову експлуатацію та її подальшу успішну експлуатацію;

е) сформулювати висновки про виконаний обсяг робіт та одержані результати.

Висновки

У цьому розділі здійснено ґрунтовний аналіз RFID-технологій, підкресливши їхню ефективність у системах автоматизованої ідентифікації завдяки безконтактному принципу роботи, високій швидкості зчитування та можливості масштабування. Окрему увагу приділено широкому спектру застосувань RFID у логістиці, торгівлі, медицині, промисловості та системах безпеки.

Порівняння RFID із традиційними методами ідентифікації, зокрема штрих-кодуванням, дозволило виділити її ключові переваги: можливість одночасного зчитування великої кількості міток без потреби прямої видимості та високу довговічність ідентифікаторів. Разом із тим визначено певні обмеження технології, серед яких чутливість до електромагнітних перешкод, залежність дальності зчитування від типу міток та відносно вища вартість впровадження.

Також проведено порівняльний аналіз альтернативних систем керування доступом - біометричних, мобільних, кодових замків і систем на основі магнітних карток. Визначено їхні сильні сторони (наприклад, високий рівень безпеки біометричних рішень) та недоліки (висока вартість біометрії, залежність мобільних систем від наявності смартфона, обмежений рівень захисту кодових і магнітних систем), а також окреслено доцільні сфери їх застосування.

На основі проведеного аналізу сформульовано вимоги до апаратно-програмного забезпечення майбутньої системи, з урахуванням технічних

					ВКРБ-123.26.0042.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		38

характеристик, функціональних потреб, обмежень за вартістю та продуктивністю, а також вимог до захисту даних. Це створило методологічну основу для подальшого проєктування системи керування доступом.

К6ПЗ_2026

					ВКРБ-123.26.0042.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		39

3 ОПИС І ОБГРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ

3.1 Опис функціонування системи

Проектування схеми та системного програмного забезпечення комп'ютеризованої системи доступу у приміщення на основі RFID-технології

Після обґрунтування доцільності використання апаратних компонентів комп'ютеризованої системи контролю доступу до приміщення наступним етапом є розроблення схеми підключення пристроїв та створення програмного забезпечення, що забезпечує керування системою і реалізацію функцій, визначених у технічному завданні. На рисунку 3.1 наведено схему комп'ютеризованої системи доступу до приміщення на основі RFID-технології.

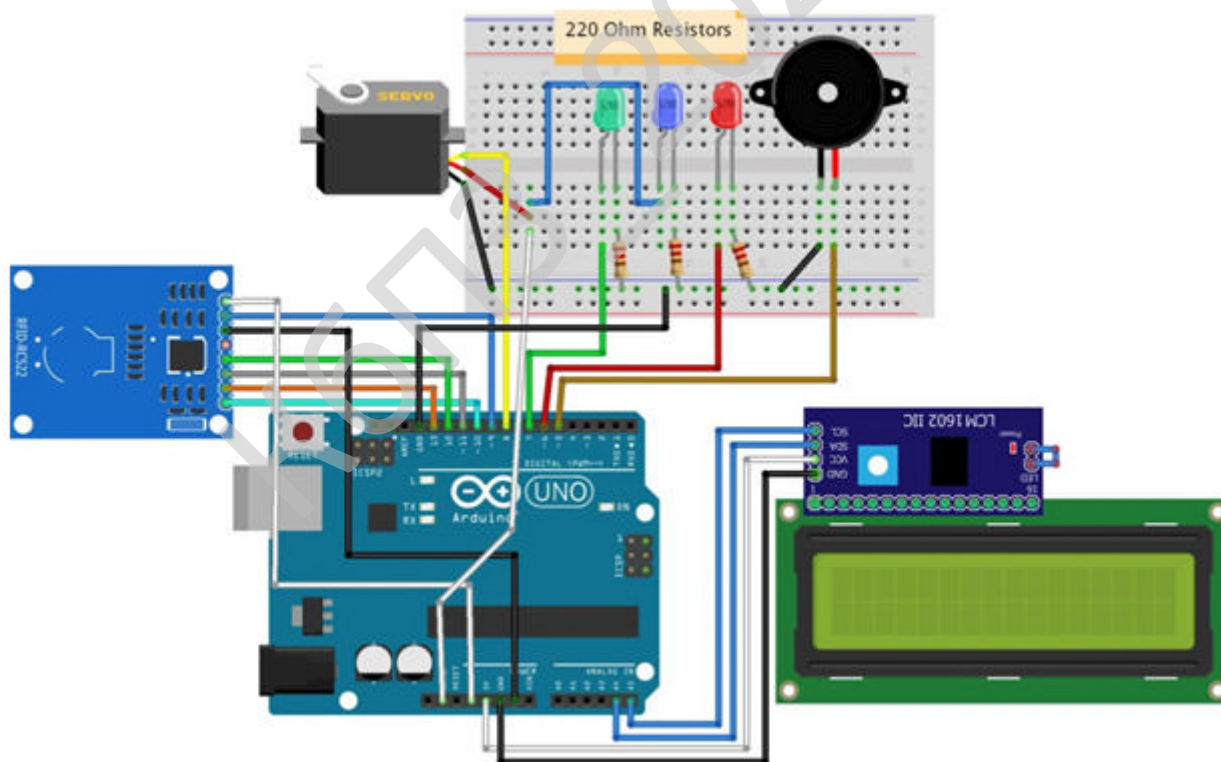


Рисунок 3.1 – Схема комп'ютеризованої системи доступу у приміщення

Раніше в табл. 2.2 було наведено, які виводи плати Arduino Uno та RFID-зчитувача задіяні фізично. Для забезпечення програмної сумісності необхідно

підключити відповідну бібліотеку та реалізувати логіку взаємодії між цими двома пристроями. У лістингу наведено приклад програмного коду підключення бібліотеки MFRC522.h.

Підключення бібліотеки MFRC522.h:

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

#define RST_PIN 9

#define SS_PIN 10

MFRC522 mfrc522(SS_PIN, RST_PIN);
void setup() { Serial.begin(9600); while (!Serial); SPI.begin();
mfrc522.PCD_Init(); delay(4);
mfrc522.PCD_DumpVersionToSerial();
Serial.println(F("Scan PICC to see UID, SAK, type, and data blocks..."));
}
void loop() {

if ( ! mfrc522.PICC_IsNewCardPresent()) { return;
}
// Select one of the cards
if ( ! mfrc522.PICC_ReadCardSerial()) { return;
}
mfrc522.PICC_DumpToSerial(&(mfrc522.uid));
}
```

Після підключення RFID-зчитувача та програмного додавання відповідної бібліотеки для роботи з ним необхідно піднести RFID-мітку до сканера для виконання її зчитування.

За умови коректного налаштування параметрів RFID-зчитувача буде отримано результат, приклад якого наведено на рисунку 3.2.

					ВКРБ-123.26.0042.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		41

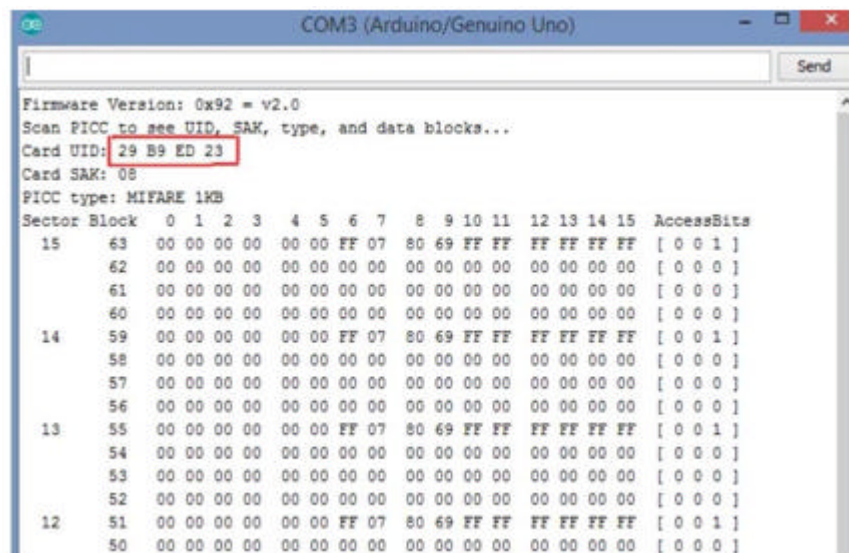


Рисунок 3.2 – Результат зчитування RFID-мітки

Вікно, наведене на рисунку 3.2, відкривається шляхом запуску монітора послідовного порту в середовищі Arduino IDE. У цьому випадку значення унікального ідентифікатора RFID-мітки має вигляд: CARD UID: 29 B9 ED 23.

Для підключення LCD-дисплея до плати Arduino Uno використано відповідні входи/виходи, схема з'єднання яких наведена в табл. 3.1.

Таблиця 3.1 – З'єднання LCD-дисплею з Arduino Uno

12C LCD	Arduino Uno
SCL	A5/SCL
SDA	A4/SDA
GND	GND
VCC	5V

Схему підключення інших додаткових пристроїв до плати Arduino Uno наведено в таблиці 3.2, зокрема:

- світлодіоди - 3 шт. (синій, червоний, зелений);
- резистори - 3 шт. номіналом по 220 Ом;
- сервопривід - 1 шт.;
- зумер - 1 шт.

Таблиця 3.2 – З'єднання додаткових пристроїв з Arduino Uno

Arduino	Діод	Сервопривід	Зумер
5V	Синій діод	Червоний провідник (+)	
Цифровий пін D8		Жовтий провідник (дані)	
Цифровий пін D7	Зелений діод		
Цифровий пін D6	Червоний діод		
Цифровий пін D5			+
GND	Підключення через резистор 220 Ом	Коричневий провідник (GND)	-

Отже, в результаті виконаного з'єднання компонентів було отримано модель комп'ютеризованої системи контролю доступу до приміщення на основі RFID-технології. Наступним етапом є розроблення програмного забезпечення, що забезпечує емуляцію процесу ідентифікації працівників.

У лістингу наведено приклад підключення та оголошення пристроїв відповідно до схеми, поданої на рисунок 3.2.

```
//Підключення бібліотек
#include <LiquidCrystal_I2C.h>
#include <SPI.h>
#include <MFRC522.h>
#include <Servo.h>

// Оголошення та ініціалізація об'єктів LiquidCrystal_I2C lcd(0x27, 16, 2);
MFRC522 mfrc522(10, 9); // MFRC522 mfrc522(SS_PIN, RST_PIN)
Servo sg90;

// Ініціалізація виводів для діодів, сервоприводу та зумера
// Синій діод під'єднаний до 5V constexpr uint8_t greenLed = 7; constexpr
uint8_t redLed = 6; constexpr uint8_t servoPin = 8; constexpr uint8_t buzzerPin =
5;

// Стрічкова змінна для зберігання UID RFID-мітки String tagUID = "29 B9 ED
23";
```

Функція ініціалізації пристроїв, підключених до Arduino Uno та самої плати наведені нижче:

```

void setup() {
    // Конфігурація виводів Arduino pinMode(buzzerPin, OUTPUT); pinMode(redLed,
OUTPUT); pinMode(greenLed, OUTPUT);
    sg90.attach(servoPin); //Оголошення 9 виводу для сервоприводу
sg90.write(0); // Положення сервоприводу на 90 градусів
    lcd.begin(); // LCD екран lcd.backlight();
    SPI.begin(); // Ініціалізація SPI шини mfrc522.PCD_Init(); // Ініціалізація
MFRC522
    lcd.clear();

```

Фрагмент програмної функції, призначеної для зчитування даних з RFID-мітки:

```

void loop() { lcd.setCursor(0, 0); lcd.print(" Двері замкнені");
lcd.setCursor(0, 1);
    lcd.print(" Покажіть вашу картку ");

    // Пошук нових міток
    if ( ! mfrc522.PICC_IsNewCardPresent()) { return;
    }
    // Вибір однієї з карток
    if ( ! mfrc522.PICC_ReadCardSerial()) { return;
    }
    //Читання RFID-мітки String tag = "";
    for (byte i = 0; i < mfrc522.uid.size; i++)
    {
        tag.concat(String(mfrc522.uid.uidByte[i] < 0x10 ? " 0" : "
"));
        tag.concat(String(mfrc522.uid.uidByte[i], HEX));
    }
    tag.toUpperCase();

```

Як видно з лістингу, робота комп'ютеризованої системи доступу до приміщення на основі RFID-технології розпочинається з ініціалізації LCD-дисплея та виведення повідомлень: у верхньому рядку - «Двері замкнені», у нижньому - «Покажіть вашу картку». Після цього система перевіряє, чи є зчитана картка новою, чи вона вже зареєстрована в системі.

Наступним етапом алгоритму є формування рядкової змінної, у яку посимвольно записується унікальний ідентифікатор RFID-мітки, після чого отриманий рядок перетворюється у верхній регістр.

Для перевірки отриманого значення ідентифікатора RFID-мітки

					ВКРБ-123.26.0042.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		44

реалізовано відповідні програмні конструкції, приклади яких наведено у лістингах:

```
if (tag.substring(1) == tagUID) lcd.clear();  
  lcd.setCursor(0, 0); lcd.print("Доступ дозволений"); lcd.setCursor(0, 1);  
  lcd.print("Двері відчинені"); sg90.write(90); digitalWrite(greenLed, HIGH);  
  delay(3000); digitalWrite(greenLed, LOW); sg90.write(0);  
  lcd.clear();  
}
```

У разі, якщо ідентифікатор RFID-мітки збігається з ключем, збереженим у пам'яті Arduino Uno, відбувається очищення екрана, після чого у верхньому рядку відображається повідомлення «Доступ дозволено», а в нижньому — «Двері відчинені». Сервопривід повертає вал на 90°, і замок дверей розблоковується. Додатковим індикатором успішної авторизації є зелений світлодіод, який світиться протягом 3 с. Після завершення цього часу світлодіод гасне, повідомлення на дисплеї повертаються до початкового стану, а сервопривід встановлюється у нульове положення.

У разі невдалої авторизації користувача (невідповідності ідентифікатора RFID-мітки) виконується програмний код, наведений у лістингу 3.6.

Алгоритм роботи системи доступу до приміщення у цьому випадку передбачає такі дії:

- очищення екрана;
- виведення повідомлення «Мітка не авторизована» у верхньому рядку дисплея.

3.2 Розробка структурної схеми

Структурна схема комп'ютеризованої системи доступу в приміщення на основі RFID-технології включає сукупність взаємопов'язаних апаратних і програмних компонентів, що забезпечують ідентифікацію користувачів та керування доступом.

Основними елементами системи є RFID-мітка, RFID-зчитувач, мікроконтролерний модуль, серверна частина (база даних) та користувацький інтерфейс (програмне забезпечення або мобільний додаток).

RFID-мітка виступає носієм унікального ідентифікаційного коду, який закріплений за конкретним користувачем. При наближенні мітки до RFID-зчитувача відбувається безконтактне зчитування даних за допомогою радіочастотного сигналу.

RFID-зчитувач приймає сигнал від мітки, декодує ідентифікаційний код та передає його до мікроконтролера. У якості мікроконтролера може використовуватися ESP32, який виконує обробку отриманих даних.

Мікроконтролерний модуль здійснює первинну обробку ідентифікатора та передає його до серверної частини системи через мережу (Wi-Fi або інший інтерфейс зв'язку). Серверна частина містить базу даних користувачів із відповідними правами доступу.

На сервері виконується перевірка отриманого ідентифікатора. У разі співпадіння з даними в базі та наявності відповідних прав доступу формується команда на відкриття доступу. У протилежному випадку доступ забороняється.

Сигнал про дозвіл або відмову повертається до мікроконтролера, який керує виконавчим пристроєм - електромагнітним замком або реле. При дозволі доступу замок розблоковується на визначений час, забезпечуючи вхід у приміщення.

Додатково система може включати інтерфейс користувача (веб-додаток або мобільний додаток), який дозволяє адміністратору додавати або видаляти користувачів, налаштовувати права доступу та переглядати журнал подій (логування входів).

Таким чином, структурна схема забезпечує повний цикл роботи системи: ідентифікацію користувача, перевірку прав доступу, керування виконавчими пристроями та ведення обліку подій.

Структура схема наведена на рисунку 3.3.

					ВКРБ-123.26.0042.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		46

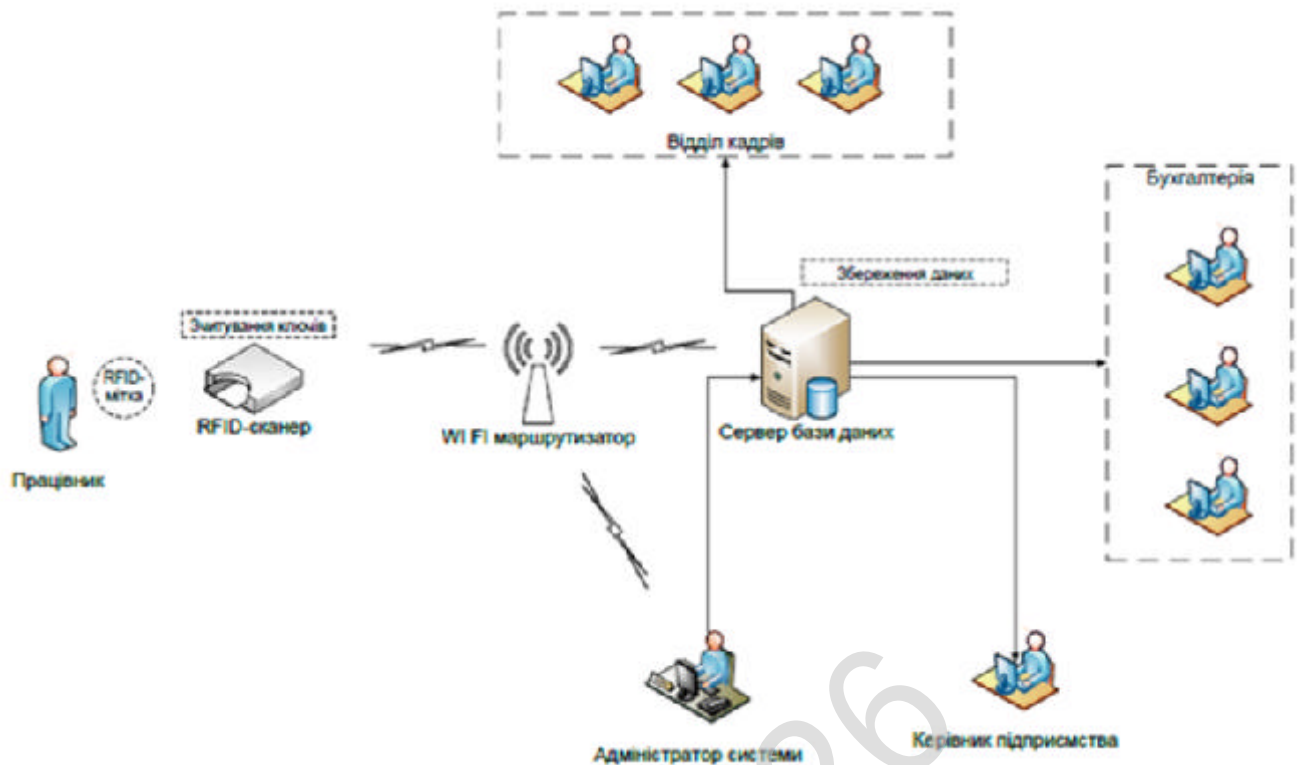


Рисунок 3.3 - Структурна схема системи

3.3 Розробка функціональної схеми

Функціональна схема (рисунок 3.3) відображає мікроконтролер ESP8266 як центральний керуючий елемент системи, який взаємодіє з основними периферійними пристроями. До нього підключено RFID-модуль для зчитування ідентифікаційних карток, LCD-дисплей для відображення службової інформації, клавіатуру для введення даних та сервопривід, що керує механізмом замка. Живлення ESP8266 здійснюється від ноутбука через USB-порт, тоді як сервопривід використовує окреме джерело живлення 5 В, 1 А. Взаємодія користувача із системою відбувається шляхом піднесення RFID-картки або введення даних за допомогою клавіатури.

Програмна складова системи включає серверний застосунок, реалізований на базі Spring Boot, який надає REST API для обробки запитів, базу даних PostgreSQL для зберігання інформації про користувачів і журнал подій доступу, а

також середовище Docker для контейнеризації та розгортання компонентів. Мікроконтролер ESP8266 здійснює обмін даними із сервером через мережу Wi-Fi, передаючи ідентифікатор RFID для перевірки та отримуючи відповідь щодо дозволу або відмови в доступі.

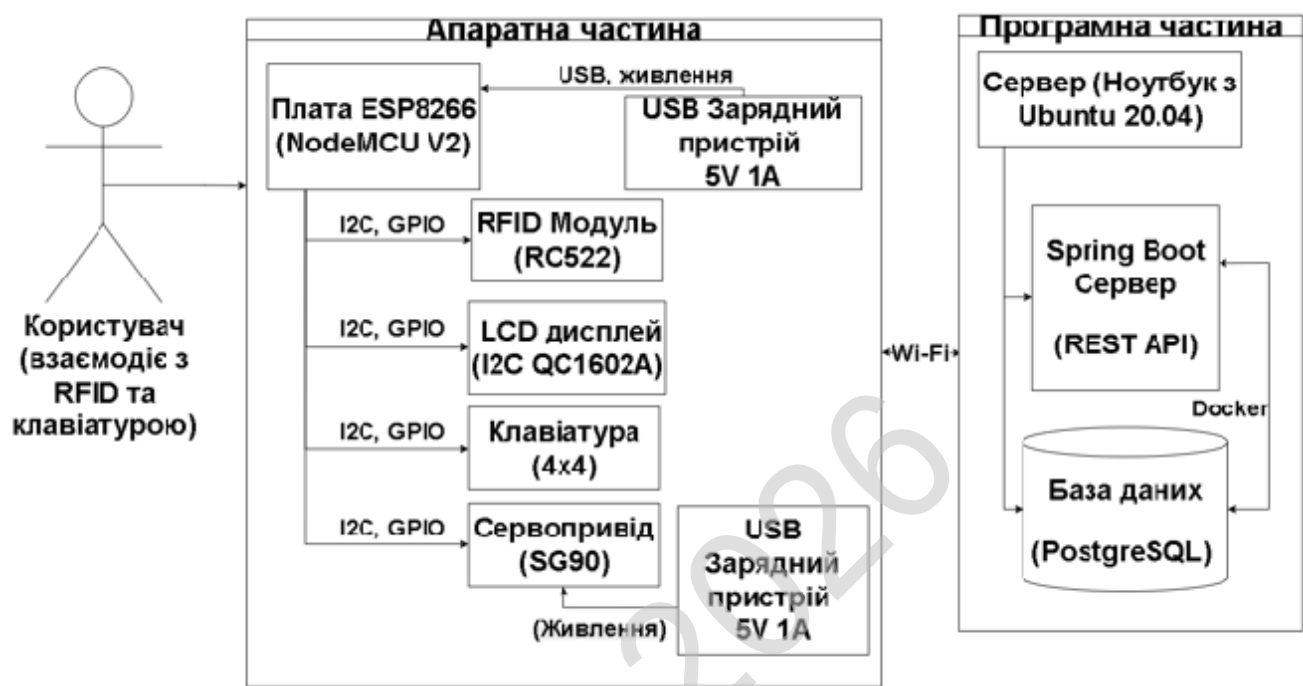


Рисунок 3.4 - Функціональна схема системи керування

3.4 Розробка діаграми процесів

Діаграма процесів відображає послідовність обробки даних у комп’ютеризованій системі доступу та взаємодію між її основними компонентами. Основною метою є ідентифікація користувача та прийняття рішення щодо надання або заборони доступу до приміщення.

Основні елементи діаграми:

- зовнішня сутність: користувач (власник RFID-мітки);
- вхідні дані: RFID-ідентифікатор;
- процеси: зчитування, обробка, перевірка, керування доступом;
- сховище даних: база даних користувачів;
- вихідні дані: сигнал доступу / відмови.

Опис процесів

1) Зчитування RFID-мітки - Користувач підносить RFID-мітку до зчитувача. Зчитувач приймає унікальний ідентифікатор та передає його до мікроконтролера.

2) Передача даних до контролера - мікроконтролер (наприклад, Arduino або ESP32) отримує ідентифікатор і виконує первинну обробку (перевірка формату, підготовка до передачі).

3) Перевірка в базі даних - ідентифікатор передається на сервер або локальну базу даних. Система перевіряє: чи існує користувач та чи має він права доступу.

4) Керування виконавчим пристроєм - мікроконтролер отримує сигнал і: відкриває замок (через реле або електромагніт) або залишає двері заблокованими.

Розроблена діаграма процесів відображає повний цикл функціонування системи доступу на основі RFID-технології: від моменту зчитування ідентифікатора до керування виконавчим пристроєм та фіксації подій. Такий підхід забезпечує надійність, контроль доступу та можливість подальшого розширення системи. Діаграма процесів наведена на рисунку 3.5.

					ВКРБ-123.26.0042.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		49

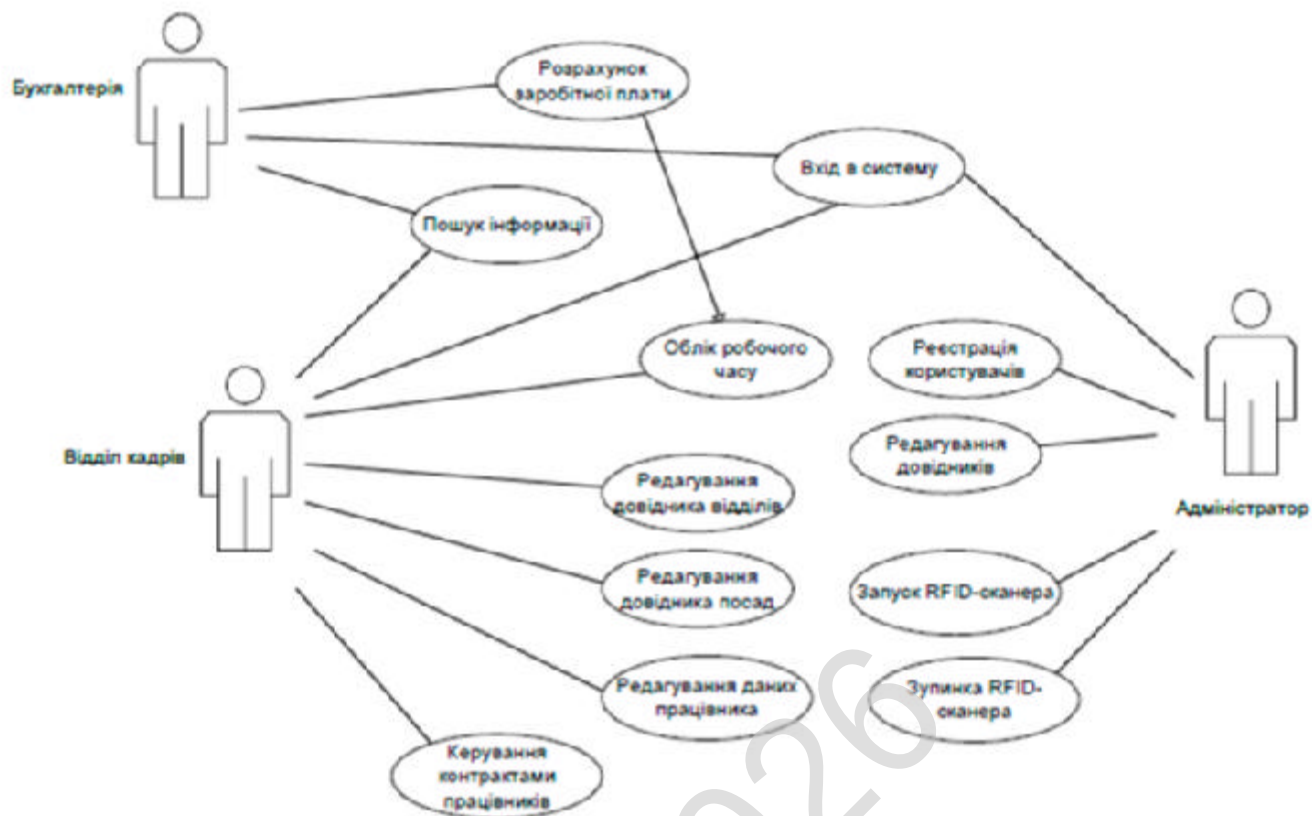


Рисунок 3.5 – Діаграма взаємодії процесів

Отже, після аналізу опису системи, структурної та функціональної схем, а також діаграми взаємодії процесів, переходимо до опису блок-схем основної програми та підпрограм, що використовуються для реалізації системи.

4 РЕАЛІЗАЦІЯ ПРОЕКТУ. РОЗРАХУНКИ І ЕКСПЕРИМЕНТАЛЬНІ ДАНІ, ЩО ПІДТВЕРДЖУЮТЬ ПРАВИЛЬНІСТЬ ПРОЕКТНИХ РІШЕНЬ

Виявлення і деталізація функціональних вимог до прикладного програмного забезпечення комп'ютеризованої системи доступу у приміщення.

Під час розроблення програмного забезпечення ключовим і базовим етапом є визначення функціональних вимог, що дає змогу чітко сформулювати уявлення про необхідні властивості та можливості системи. Сучасним інструментом моделювання різних аспектів об'єктно-орієнтованого програмного забезпечення є засоби, що підтримують мову UML. Для подання функціональних вимог у межах цієї мови використовуються діаграми варіантів використання (use-case діаграми).

З урахуванням вимог технічного завдання до комп'ютеризованої системи організації доступу до приміщення, а також визначених зацікавлених сторін - безпосередніх користувачів системи, функціональні вимоги було сформовано за ролями: адміністратор, працівники бухгалтерії та працівники відділу кадрів. Для всіх користувачів передбачено авторизований доступ до системи.

Функціональні можливості адміністратора системи:

- керування RFID-зчитувачем;
- редагування довідників бази даних;
- реєстрація користувачів.

Можливості працівників бухгалтерії:

- розрахунок заробітної плати на основі облікованого робочого часу;
- пошук необхідної інформації.
- пошук інформації про працівників;
- формування довідника структурних підрозділів підприємства;
- редагування довідників посад і персональних даних працівників;
- керування трудовими контрактами працівників.

Важливим етапом проєктування, який слугує основою для подальшої розробки, є процес відображення створеної концептуальної моделі (рисунк. 4.1) на конкретні компоненти та об'єкти прикладного програмного забезпечення. Алгоритми функціонування сучасних програмних систем зазвичай є складними й нелінійними, що вимагає від розробників та інженерів максимально ефективного формування архітектури шляхом проєктування чітко визначених статичних інтерфейсів взаємодії між її складовими.

Проектування архітектури прикладного додатку

У даній роботі для розроблення програмного забезпечення запропоновано використати варіант реалізації архітектури застосунку за моделлю «товстий клієнт». Перевагою такого підходу є зменшення навантаження на центральний сервер бази даних, а також підвищення гнучкості й автономності клієнтських прикладних програм.

Компоненти системи реалізують окремі функціональні можливості програмного продукту. Взаємодіючи через визначені інтерфейси, потоки передавання даних і спільні джерела інформації, та ґрунтуючись на єдиних принципах роботи, вони утворюють цілісну систему.

Прикладне програмне забезпечення комп'ютеризованої системи доступу до приміщення на основі RFID-технології має забезпечувати засоби обліку робочого часу та нарахування заробітної плати працівникам підприємства і включати такі функції:

- введення та збереження початкових даних (структурні підрозділи підприємства, посади, контракти, дані щодо оплати праці);
- реєстрацію робочого часу працівників;
- реєстрацію користувачів системи та визначення їх ролей;
- встановлення з'єднання з реєстратором, виконання тестування та зчитування даних;
- обчислення необхідних показників, збереження результатів і їх візуалізацію.

На основі сформованих вимог, концептуальної архітектурної моделі та

					ВКРБ-123.26.0042.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		52

відомостей про сутності предметної області було розроблено трирівневу архітектуру прикладного програмного засобу.

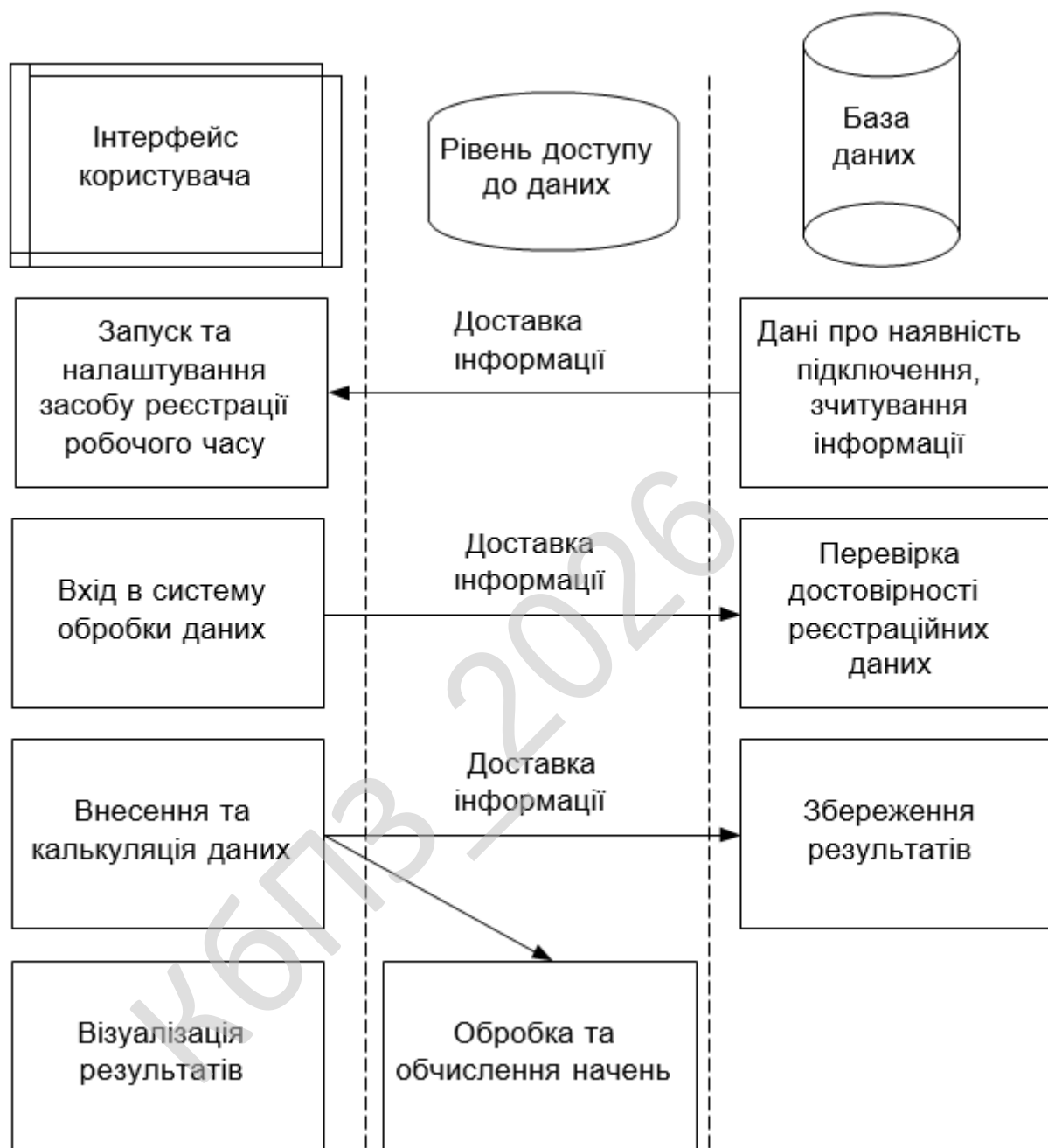


Рисунок 4.1 – Модель архітектури прикладного додатку комп'ютеризованої системи доступу

Рівень інтерфейсу користувача надаватиме графічний інтерфейс та супутній код для виконання наступних функцій:

- налаштування та запуск засобу реєстрації робочого часу – це

вибір доступних СОМ-портів, відображення інформації про наявність підключення, перевірка з'єднань із обраними серверами баз даних, візуалізація додаткової інформації, запуск зчитування даних з реєстратора.

- вхід в систему – полягає у вводі даних користувача (логіна і паролю);
- їх перевірку на сервері та визначення ролі користувача;
- внесення і обробку даних - передбачає зміну інформації про працівників, умови контрактів, відділи та посади, обчислення обраних користувачем показників і подальшу їх обробку;
- візуалізацію результатів - відображення результатів обчислень у зручному для користувача вигляді;
- рівень обробки та доступу до даних забезпечує передавання інформації між іншими рівнями архітектури, а також надає механізми запуску й виконання SQL-сценаріїв у відповідних системах керування базами даних.

Рівень бази даних відповідає за збереження початкових і обчислених даних, необхідних для функціонування системи, зокрема:

- даних про зареєстрованих користувачів;
- відомостей про посади, підрозділи та контракти;
- інформації про облікований робочий час;
- розрахованих сум заробітної плати відповідно до відпрацьованого часу.

Поділ архітектури на три рівні забезпечує прозорість їхньої взаємодії, спрощує заміну програмних компонентів і полегшує модернізацію системи відповідно до нових вимог.

Проектування та реалізація бази даних системи доступу у приміщення

Для визначення сутностей предметної області, їх атрибутів та зв'язків було проаналізовано поставлене технічне завдання, особливості функціонування комп'ютеризованої системи та специфіку предметної області. Основними сутностями при реалізації прикладного додатку комп'ютеризованої системи є:

					ВКРБ-123.26.0042.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		54

- відділ (табл. 4.1);
- працівник (табл. 4.2);
- посада (табл. 4.3);
- контракт (табл. 4.4);
- місячний графік роботи (табл. 4.5);
- тижневий графік роботи (табл. 4.6);
- облік робочого часу (табл. 4.7);
- користувач (табл. 4.8);
- роль (табл. 4.9).

Таблиця 4.1 – Сутність «Відділ» та її атрибути

Атрибут	Тип атрибута	Зв'язок
Назва підрозділу	Текст	Входить в батьківський підрозділ (факультативний, один-до-багатьох)
Батьківський підрозділ	Текст	
Керівник	Текст	

Таблиця 4.2 – Сутність «Працівник» та її атрибути

Атрибут	Тип атрибута	Зв'язок
Прізвище	Текст	Заключає контракти (обов'язковий, один-до-багатьох)
Ім'я	Текст	
По-батькові	Текст	
Дата народження	Текст	Може очолювати підрозділ (факультативний, один-до-багатьох)
Ідентифікаційний код	Текст	
Серія паспорта	Текст	
Номер паспорта	Текст	

Таблиця 4.3 – Сутність «Посада» та її атрибути

Атрибут	Тип атрибута	Зв'язок
Назва посади	Текст	
Оклад	Грошові одиниці	

Таблиця 4.4 – Сутність «Контракт» та її атрибути

Атрибут	Тип атрибута	Зв'язок
Дата початку дії	Дата	
Дата закінчення дії	Дата	
Заробітна плата	Грошові одиниці	

Таблиця 4.5 – Сутність «Місячний графік роботи» та її атрибути

Атрибут	Тип атрибута	Зв'язок
Назва місяця	Текст	
Перший робочий день	Дата	

Таблиця 4.6 – Сутність «Тижневий робочий графік» та її атрибути

Атрибут	Тип атрибута	Зв'язок
Початок тижня	Дата	Входить в робочий місяць (обов'язковий, один-до-багатьох)
Кінець тижня	Дата	
Місяць	Текст	

Таблиця 4.7 – Сутність «Облік робочого часу» та її атрибути

Атрибут	Тип атрибута	Зв'язок
Дата та час відмітки	Дата та час	Обліковується для працівника (обов'язковий, один-до-багатьох)
Працівник	Текст	

Таблиця 4.8 – Сутність «Користувач» та її атрибути

Атрибут	Тип атрибута	Зв'язок
Ім'я користувача	Текст	Входить в роль (обов'язковий, один-до-багатьох)
Пароль	Текст	
Роль	Текст	
Заблокований	Логічний тип	

Таблиця 4.9 – Сутність «Роль» та її атрибути

Атрибут	Тип атрибута	Зв'язок
Назва	Текст	

Інформаційна модель даних призначена для подання семантики предметної області в термінах формалізованих засобів опису - сутностей, їх атрибутів і взаємозв'язків. Аналіз і опис сутностей предметної області дали змогу побудувати інформаційну модель, необхідну для розроблення прикладного програмного забезпечення системи організації авторизованого доступу до приміщення.

Для систематизації знань про предметну область на основі раніше виконаного опису сутностей, їх атрибутів і зв'язків доцільно побудувати модель «сутність–зв'язок» (ER-модель). На основі ER-моделі було сформовано сценарій фізичної реалізації сховища даних у середовищі реляційної системи керування

базами даних і створено реляційну базу даних. Фізичну реалізацію ER-моделі доцільно подати у табличному вигляді із зазначенням назв таблиць і відповідних сутностей, назв та типів полів у нотації SQL, а також у графічному вигляді, як показано на рисунку 4.2.

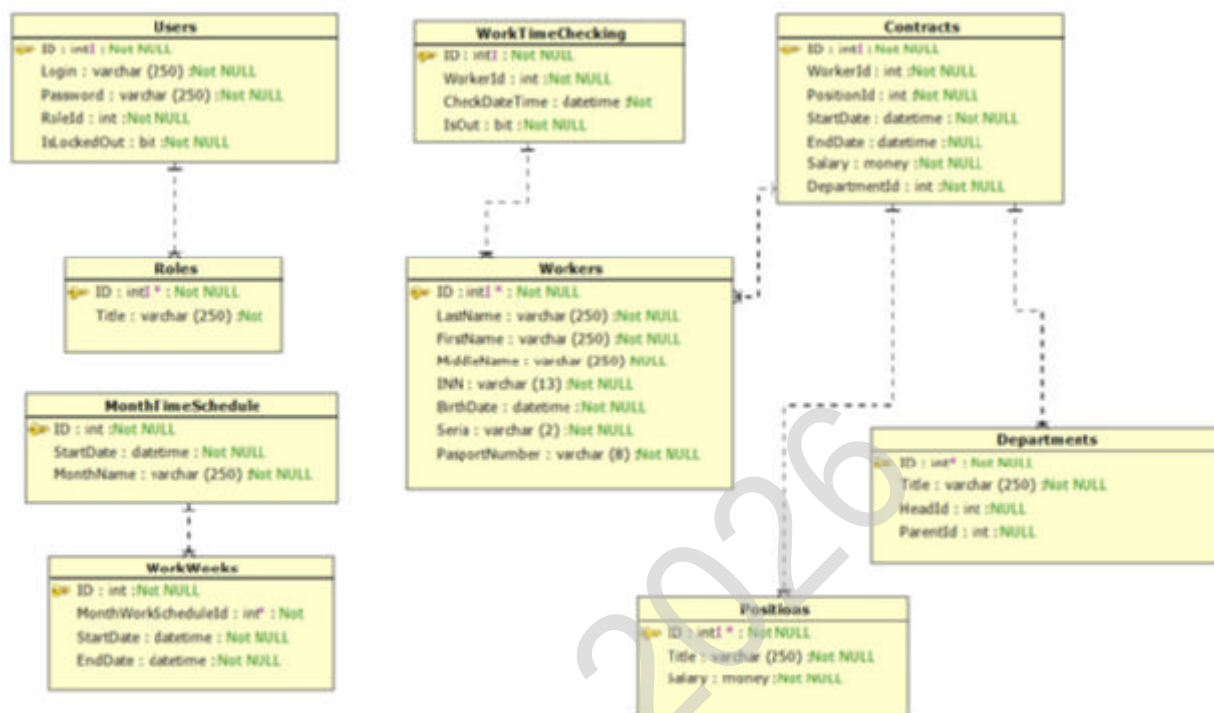


Рисунок 4.2 – ER-діаграма бази даних програмного додатку

Після проєктування архітектури прикладного програмного забезпечення та структури бази даних наступним етапом є розроблення алгоритму зчитування даних із RFID-зчитувача.

4.1 Розробка блок-схем та опис алгоритмів функціонування системи

Розробка алгоритму зчитування унікального ідентифікатора з RFID-мітки та запису в базу даних

Алгоритм взаємодії зі сканером RFID-міток розпочинається з перевірки наявності з'єднання між прикладним програмним забезпеченням і апаратною частиною зчитувача. Якщо зв'язок встановлено, виконується зчитування ідентифікатора RFID-мітки. У разі відсутності сигналу адміністратору системи

надсилається повідомлення про втрату з'єднання зі сканером.

За умови стабільного підключення до RFID-зчитувача здійснюється зчитування даних із мітки та їх порівняння із записами ідентифікаторів працівників, що зберігаються у базі даних. Якщо мітка відповідає одному із записів, зчитувачу передається команда на розблокування доступу до приміщення.

Кожен працівник перед початком роботи проходить процедуру ідентифікації. Зчитувач отримує унікальний ідентифікатор, порівнює його з наявними записами та, у разі позитивного результату, фіксує дату і час входу на робоче місце. Аналогічна процедура виконується при виході працівника з території підприємства, що дозволяє зафіксувати завершення робочого часу. Процес зчитування даних і їх запису до бази даних виконується циклічно.

Для взаємодії зі зчитувачем RFID-міток, який використовується як засіб реєстрації робочого часу працівників, розроблено прикладний додаток на основі технології Windows Forms із застосуванням компонента SerialPort. Користувацький інтерфейс забезпечує вибір COM-порту для перевірки підключення, відображення стану готовності апаратних засобів, а також запуск і зупинку процесу отримання даних від пристроїв введення.

Графічне подання алгоритму роботи з RFID-сканером наведено на рисунку 4.3.

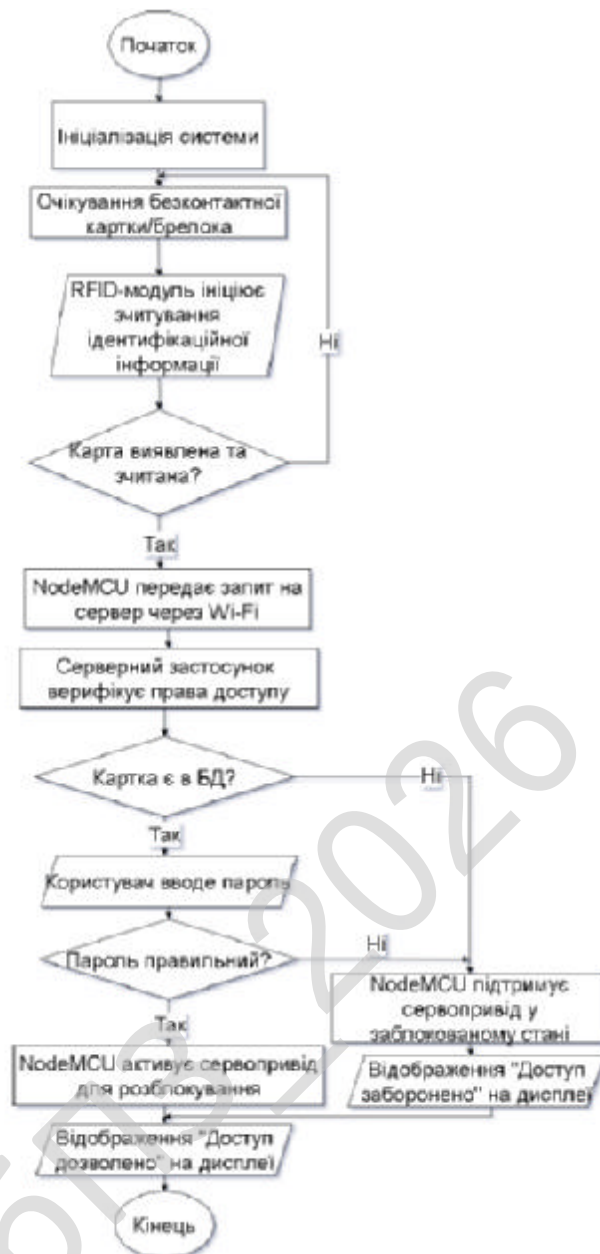


Рисунок 4.3 – Алгоритм роботи прикладного додатку з RFID-сканером

Як зазначалося раніше, прикладне програмне забезпечення системи організації доступу до приміщення на основі RFID-технології доцільно реалізувати із застосуванням технології Windows Forms, мови програмування C# та системи керування базами даних MS SQL Server.

Важливою особливістю застосунків WinForms є їх подієво-орієнтована модель роботи, що передбачає обробку різних подій. Наприклад, система може програмно реагувати на натискання кнопки на панелі навігації та виконувати відповідний код. Фрагмент, наведений у лістингу, демонструє обробку події

натискання кнопки «Зберегти» у вікні керування даними працівників.

Програмний код обробки натискання кнопки «Зберегти»:

```
private void saveToolStripButton_Click(object sender, EventArgs e)
{
    try
    {
        workersBindingSource.EndEdit();

        workersTableAdapter.Update(teacherJournalDS);
        workersDS.AcceptChanges(); MessageBox.Show("Вдало збережено",
        "Результат операції", MessageBoxButtons.OK, MessageBoxIcon.Information);
    }
    catch
    {
        MessageBox.Show("Помилка при збереженні", "Результат операції",
        MessageBoxButtons.OK, MessageBoxIcon.Error);
    }
}
```

Виконання цього фрагмента коду забезпечує збереження даних у таблиці бази даних. У разі успішного або неуспішного завершення операції користувач отримує відповідне інформаційне повідомлення. Для роботи з COM-портом використовується компонент **SerialPort**, який забезпечує доступ до ресурсів послідовного порту. Клас SerialPort надає простий і гнучкий інтерфейс взаємодії з можливостями COM-порту та дозволяє отримувати та передавати дані через послідовний порт. У лістингу нижче наведено приклад програмного коду, що демонструє запуск процесу прослуховування COM-порту.

Прослуховування COM-порту:

```
private void btStart_Click(object sender, EventArgs e)
{
    try
    {
        if (!spMain.IsOpen)
        {
            spMain.Open();
        }
        stopCurrentListener();
        ComPortListener listener = new ComPortListener(s
        pMain);
        currentListener = new Thread(listener.StartListe
        n);
        currentListener.Start(new Action<string>(WriteDa
        taToForm));
    }
    catch (Exception exc)
    {
        MessageBox.Show(exc.Message);
    }
}
```

Метод StartListen класу ComPortListener здійснює перевірку доступності COM-порту та наявності даних у буфері для зчитування. Якщо дані присутні, виконується їх зчитування з подальшим викликом методу запису інформації до бази даних.

Запис даних у базу даних із COM-порту:

```
public void StartListen(object method)
{
    var writeMethod = (method as Action<string>); if (portToListen.IsOpen)
    {
        writeMethod("Start listen..."); while (true)
        {
            if (portToListen.BytesToRead > 0)
            {
                byte[] buffer = new byte[portToListen.BytesToRead];

                var value = UnicodeEncoding.Unicode.GetString(buffer); writeMethod(value);
            }
            else
            {
                writeMethod("No data"); Thread.Sleep(1000);
            }
        }
    }
    else
    {
        writeMethod("Port closed!");
    }
}
```

Використання окремих потоків виконання та динамічних делегатів дозволяє підвищити надійність і швидкодію програмної системи, а також покращити контроль процесів зчитування та збереження даних.

Розробка алгоритму доступу

Алгоритм доступу визначає послідовність дій системи при ідентифікації користувача за допомогою RFID-мітки та прийнятті рішення щодо надання або заборони доступу до приміщення.

Послідовність виконання алгоритму:

- ініціалізація системи.

Після увімкнення системи відбувається:

- запуск мікроконтролера;
- ініціалізація RFID-зчитувача;
- встановлення з'єднання з базою даних (за наявності);

- перевірка працездатності компонентів;
- Очікування RFID-мітки.

Система переходить у режим очікування та безперервно перевіряє наявність мітки в зоні дії зчитувача:

- 1) Зчитування ідентифікатора.
- 2) При виявленні RFID-мітки:
 - зчитується унікальний UID;
 - перевіряється коректність даних;
 - передача даних на обробку.
- 3) ідентифікатор передається:
 - або до локальної пам'яті мікроконтролера;
 - або на сервер (через Wi-Fi / MQTT / HTTP).

Перевірка прав доступу

Система виконує:

- пошук UID у базі даних;
- перевірку прав доступу (час, рівень доступу тощо).

Прийняття рішення

Якщо користувач знайдений і має доступ - доступ дозволено. Якщо ні - доступ заборонено. Виконання дії.

					ВКРБ-123.26.0042.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		62



Рисунок 4.4 - Блок-схема алгоритму контролю доступу

5 МЕТОДИКА ВПРОВАДЖЕННЯ СИСТЕМИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ

Користувацький інтерфейс прикладного додатку організації доступу до приміщення

Для забезпечення роботи користувачів і доступу до сховища даних було розроблено прикладний клієнтський застосунок із використанням технологій Windows Forms, Data Binding та ADO.NET Entity Framework.

Форми адміністрування підрозділів, посад і даних працівників реалізовано за принципом «загальний–детальний». Інтерфейс побудовано на основі компонентів відображення DataGridView, навігаційної панелі та полів введення інформації. Навігаційна панель забезпечує виконання операцій створення, збереження та видалення записів у базі даних, при цьому відповідні дії дублюються за допомогою кнопок керування.

Інтерфейс форми для роботи з інформацією про працівників забезпечує можливість введення, редагування та збереження персональних даних. Табличне подання дає змогу виконувати сортування записів, тоді як детальна форма призначена для перегляду окремого запису та внесення змін до нього, як показано на рисунку 5.1.

					ВКРБ-123.26.0042.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		64

Працівники

1 of 3

ID	Прізвище	Ім'я	По-батькові	Ідентифікаційний код	Дата народження	Серія	Номер паспорта
1	Петров	Іван	Семенович	1232432323412	10/21/1965	BA	232312
2	Федоренко	Федр	Петрович	2345343423412	6/14/1960	BA	222312
3	Мисайлиненко	Василь	Іванович	1231343423412	5/12/1957	BS	123423

Ім'я: Ідентифікаційний код:

Прізвище: Серія:

По-батькові: Номер паспорта:

Дата народження:

Новий запис Видалити Зберегти

Рисунок 5.1 – Вигляд інтерфейсу для роботи із довідником працівників

Форма редагування інформації про посади забезпечує можливість введення та оновлення даних щодо посад, доступних на підприємстві (рис. 5.2).

Посади

1 of 4

ID	Посада	Оплата
1	Різноробочий	10000
2	Спеціаліст	13500
3	Начальник відділу	20000
4	Генеральний ди...	45000

Посада:

Оплата:

Новий запис Видалити Зберегти

Рисунок 5.2 – Форма для роботи з даними посад підприємства

Вікно роботи з даними підрозділів забезпечує можливість формування структури та ієрархії підрозділів підприємства, а також призначення їх керівників, як показано на рисунку 5.3.

The screenshot shows a window titled "Підрозділи" (Departments). It contains a table with two columns: "Назва підрозділу" (Department Name) and "Керівник" (Manager). The table lists four departments: "Адміністрація" (Administration) managed by "Семеренко Іван Вас...", "Відділ обслуговування" (Service Department) managed by "Іванова Ганна Федо...", "Бухгалтерія" (Accounting) managed by "Терешкова Іванна П...", and "Технічний відділ" (Technical Department) managed by "Горбунков Петро Ген...". To the right of the table, there are input fields for "Назва підрозділу:" (Department Name) and "Керівник:" (Manager), both containing the same data as the first row. Below these fields are three buttons: "Новий запис" (New record), "Видалити" (Delete), and "Зберегти" (Save). A large watermark "2026" is visible across the center of the image.

	Назва підрозділу	Керівник
▶	Адміністрація	Семеренко Іван Вас...
	Відділ обслуговування	Іванова Ганна Федо...
	Бухгалтерія	Терешкова Іванна П...
	Технічний відділ	Горбунков Петро Ген...

Рисунок 5.3 – Форма для роботи з підрозділами підприємства

Клієнтський прикладний застосунок також надає інтерфейс для введення, перегляду та редагування інформації про контракти, укладені з працівниками підприємства, які працюють за погодинною формою оплати праці. Форма роботи з контрактами містить механізм фільтрації, що дозволяє знаходити контракти, актуальні у заданому часовому інтервалі. Вигляд цієї форми наведено на рисунку 5.4.

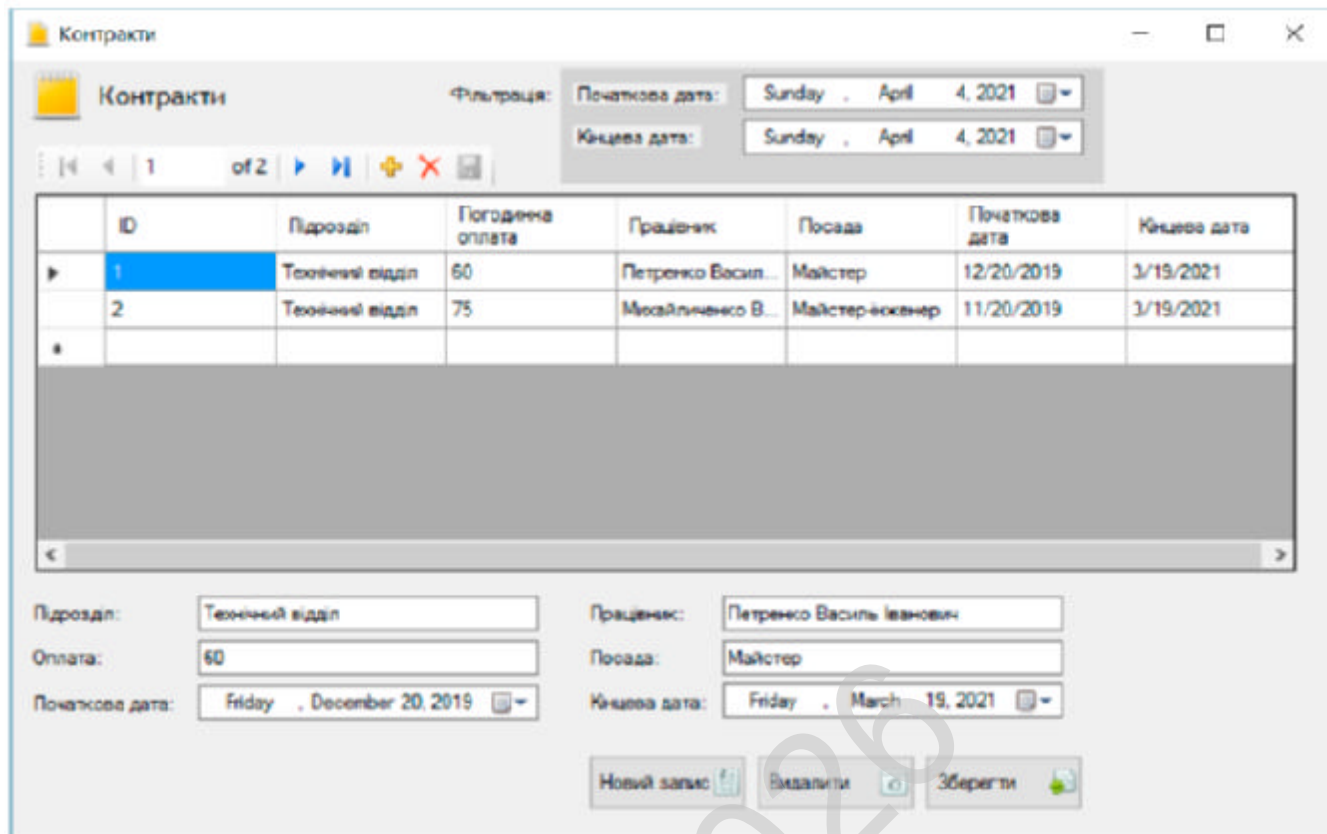


Рисунок 5.4 – Зовнішній вигляд інтерфейсу роботи із контрактами

Інтерфейс користувача для розрахунку робочого часу працівника та заробітної плати за погодинною ставкою забезпечує можливість вибору конкретного працівника і періоду, за який виконуватиметься обчислення.

Під час розрахунку відображається таблиця часових позначок працівника, отриманих за допомогою RFID-сканера. На підставі цих даних визначається загальна кількість відпрацьованих годин за вибраний період, кількість робочих днів, а також середня тривалість робочого дня. З урахуванням кількості відпрацьованих годин і погодинної ставки здійснюється обчислення заробітної плати працівника за заданий проміжок часу. Підсумкові значення відпрацьованих годин і заробітної плати наведено на рисунку 5.5.

Розрахунок зарплати

Калькуляція робочого часу

Початок періоду: Sunday, April 4, 2021

Кінець періоду: Friday, April 2, 2021

Працівник: Михайличенко

Розрахувати Генерувати звіт

Дата та час	Працівник
4/2/2021 9:10 AM	Михайличенко Васил...
4/2/2021 1:10 PM	Михайличенко Васил...
4/2/2021 2:00 PM	Михайличенко Васил...
4/2/2021 6:01 PM	Михайличенко Васил...
4/3/2021 9:05 AM	Михайличенко Васил...
4/3/2021 12:55 PM	Михайличенко Васил...
4/3/2021 2:04 PM	Михайличенко Васил...
4/3/2021 6:01 PM	Михайличенко Васил...
4/4/2021 9:07 AM	Михайличенко Васил...
4/4/2021 12:56 PM	Михайличенко Васил...
4/4/2021 2:08 PM	Михайличенко Васил...
4/4/2021 6:03 PM	Михайличенко Васил...
4/5/2021 9:03 AM	Михайличенко Васил...
4/5/2021 12:52 PM	Михайличенко Васил...
4/5/2021 2:08 PM	Михайличенко Васил...

Всього годин відпрацьовано: 160 год. 15хв

Всього днів виходу на робоче місце: 22

Робочих годин в середньому за день: 7 год. 20хв

Поточна ставка: 74 грн. 72 к.

Зарплата за період: 12000 грн.

Рисунок 5.5 – Розрахунок облікованого робочого часу та заробітної плати працівника

Форма розрахунку робочого часу та заробітної плати працівників також містить графік облікованої тривалості щоденної роботи за вибраний період. За допомогою кнопки «Згенерувати звіт» результати обчислення робочого часу та заробітної плати можуть бути передані до системи Reporting Services або експортовані в офісні програми, зокрема табличний процесор MS Excel. Приклад сформованого та візуалізованого звіту наведено на рисунок 5.6.

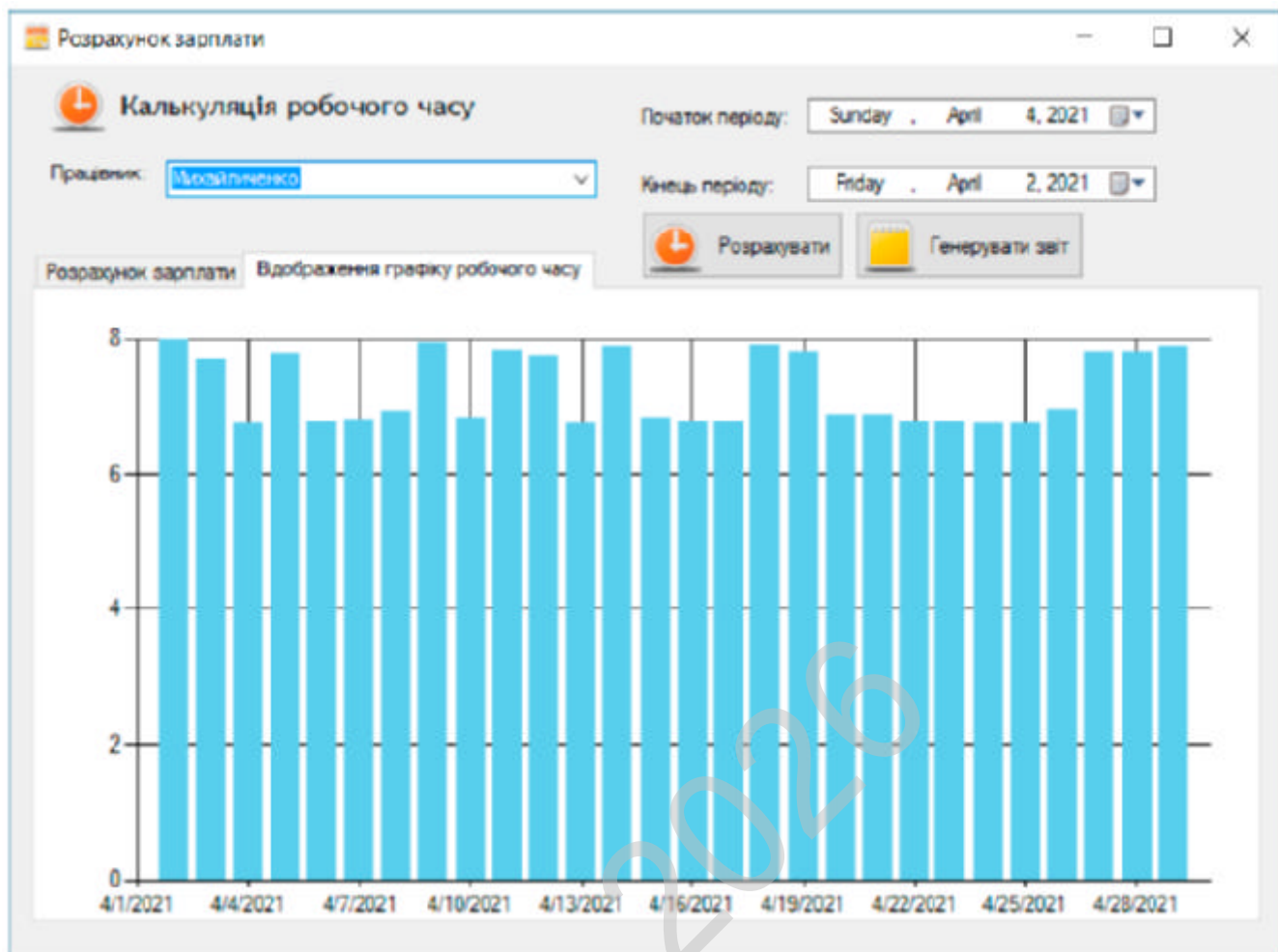


Рисунок 5.6 – Відображення графіку робочого часу працівника

Графічний інтерфейс прикладного програмного забезпечення забезпечує можливість керування системою обліку робочого часу, внесення та редагування даних у довідниках бази даних, а також виконання розрахунків відпрацьованого часу й заробітної плати працівників.

Користувачський інтерфейс є невід’ємною частиною комп’ютеризованої системи контролю доступу до приміщень, що функціонує на основі RFID-технології, та забезпечує реалізацію і підтримку прикладних завдань, які виникають у процесі виробничої діяльності.

6 ОСНОВНІ ВИСНОВКИ

У даній роботі запропоновано інженерний підхід до створення комп'ютеризованої системи контролю доступу до приміщень на основі RFID-технології. Прототип системи реалізовано на платформі Arduino Uno з використанням модуля SparkFun RFID Reader, який виконує функції зчитування RFID-міток. До складу апаратної частини також входять:

- три світлодіоди, що забезпечують візуальну індикацію готовності та поточного стану зчитувача;
- LCD-дисплей для відображення повідомлень про результат виконання операції ідентифікації;
- модуль Wi-Fi ESP8266, який забезпечує передавання даних від Arduino до сервера бази даних;
- сервопривід, що імітує роботу механізму дверного замка.

Системне програмне забезпечення для керування комп'ютеризованою системою доступу розроблено мовою C у середовищі Arduino IDE. Прикладне програмне забезпечення, призначене для підвищення ефективності використання системи шляхом реєстрації та накопичення статистики щодо часу перебування працівників на робочому місці, створено з використанням технології Windows Forms мовою C# у середовищі Visual Studio. Базу даних реалізовано мовою SQL у системі керування базами даних MS SQL Server Express 2019.

У результаті виконаної роботи створено повноцінний прототип комп'ютеризованої системи контролю доступу на основі RFID-технології, який може застосовуватися на підприємствах, де важливими є підвищення продуктивності праці та нарахування заробітної плати за погодинним принципом.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Koval V., Adamiv O., Proc. of the Third IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2005). – Sofia (Bulgaria). – 2005. – P. 120- 124.
2. Yasin, J.N., Mohamed, S.A.S., Haghbayan, MH. et al. Low-cost ultrasonic based object detection and collision avoidance method for autonomous robots. Int. j. inf. tecnol. 13, 97–107 (2021). <https://doi.org/10.1007/s41870-020-00513-w>.
3. Sabry F. Self Driving Car: Solving Full Self-driving Need Solving Real-world artificial Intelligence. One Billion Knowledgeable. 2022 . 293 p.
4. Shapiro D. G. Three Anecdotes from the DARPA Autonomous Land Vehicle Project. AI Magazine, 2008. 29(2), 40. <https://doi.org/10.1609/aimag.v29i2.2108>.
5. Young R. Critical Analysis of Prototype Autonomous Vehicle Crash Rates Six Scientific Studies from 2015-2018 SAE International. 2021. 252 p.
6. Рудик А. В. Наукові основи та принципи побудови приладової системи вимірювання прискорення мобільного робота : дис. ... д-ра техн. наук : 05.11.01– Прилади та методи вимірювання механічних величин. Київ, 2018. – 460 с.
7. Поліщук М. М., Ткач М.М. Робототехнічні системи: проектування і моделювання: навч. посіб. Київ: КПП ім. Ігоря Сікорського, 2021. 112 с.
8. Мигаль В. Д. Інтелектуальні системи в технічній експлуатації автомобілів: монографія. Х.: Майдан, 2018. 262 с.
9. Staron M. Automotive Software Architectures: An Introduction. Second Edition Springer International Publishing A&G. 2022. 274 p.
10. Vargas J. et al. An Overview of Autonomous Vehicles Sensors and Their Vulnerability to Weather Conditions. Sensors. 2021; 21(16):5397.
11. Wevolver 2020 Autonomous Vehicle Technology Report. URL:<https://www.coursehero.com/file/62601304/Wevolver2020AutonomousVehicleTechnologyReportpdf/> (accessed 2023 June 1).

					ВКРБ-123.26.0042.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		71

12. React.js [Електронний ресурс] – Режим доступу до ресурсу:
<https://uk.reactjs.org/>
13. AngularJS MVC [Електронний ресурс] – Режим доступу до ресурсу:
https://www.tutorialspoint.com/angularjs/angularjs_mvc_architecture.htm.
14. Vue.js [Електронний ресурс] – Режим доступу до ресурсу:
<https://vuejs.org/>
15. A Look Inside ADAS Modules. URL: <https://amkor.com/semiconductor-story/alook>.
16. AV and ADAS Sensors. URL [https://community.sw.siemens.com/s/article/AVand- ADAS-Sensors](https://community.sw.siemens.com/s/article/AVand-ADAS-Sensors) (accessed 2023 June 1).
17. Гуржій А. М. Основи автоматики та робототехніки: Навчальний посібник/ А.М. Гуржій, А. Т. Нельга, В. М. Співак, О. С. Ітякін:—Дніпро:«Гарант СВ», 2021.- 243с.
18. Lim, B.S. et al. Autonomous Vehicle Ultrasonic Sensor Vulnerability and Impact Assessment. In Proceedings of the IEEE World Forum on Internet of Things (WFIoT), Singapore, 5–8 February 2018; pp. 231–236.
19. Саліхов М. М. Arduino – перспективний інструмент протитопування у робототехніці // Концептуальні шляхи розвитку науки та освіти: матеріали VIII Міжнародної науково-практичної конференції м. Львів, 9-10 червня 2023 року.— Львів: Львівський науковий форум, 2023. – с. 73-79.
20. Bräunl T. Embedded Robotics: From Mobile Robots to Autonomous Vehicles with RaspberryPi and Arduino Springer Nature, 2022. 519 p.
21. Навігаційні системи [Електронний ресурс] : навч. посіб. для студ. Спеціальності 151 «Автоматизація та комп’ютерно-інтегровані технології» / С.Л. Лакоза; КПІ ім. Ігоря Сікорського, 2021. — 80 с.
22. Imad M. et al. Navigation system for autonomous vehicle: A survey. JCSTS., vol. 2, no. 2, pp. 20–35, 2020.

23. Ковалець І. В. та ін. Технологія планування траєкторій руху мобільних об'єктів з урахуванням перешкод на складній місцевості. Енергетика і автоматика. - 2017. - № 1. - С. 110-122.

24. HTML [Електронний ресурс] – Режим доступу до ресурсу: <https://developer.mozilla.org/uk/docs/Web/HTML>.

25. Aguilo I. et al. Artificial Intelligence Research and Development Hardcover by IOS Press. 2003. 500 p.

26. Гребенюк Б. А. Розробка підсистеми управління інтелектуальним роботом / Б. А. Гребенюк // «Automation and Development of Electronic Devices» ADED-2023: Collection of Students' Scientific Paper. – Kharkiv : Kind of Kharkiv National University of Radio Electronics [electronic edition], 2023. – Part 1. –336 p. P. 263-269.

27. MongoDB [Електронний ресурс] – Режим доступу до ресурсу: <https://uk.wikipedia.org/wiki/MongoDB>.

28. Becker M. et al Obstacle avoidance procedure for mobile robots. ABCM. Symposium series in Mechatronics. Vol. 2, 2006. P. 250-257.

29. CORS, XSS [Електронний ресурс] – Режим доступу до ресурсу: <https://dev.to/maleta/cors-xss-and-csrf-with-examples-in-10-minutes-35k3>.

30. AJAX [Електронний ресурс] – Режим доступу до ресурсу: <https://uk.wikipedia.org/wiki/AJAX>.

31. Fetch API [Електронний ресурс] – Режим доступу до ресурсу: https://developer.mozilla.org/ru/docs/Web/API/Fetch_API.

32. Звенігородський О.С. Інтелектуальна система планування тактики руху автономного робота в квазістаціонарному середовищі: Дис... канд. техн. наук: 05.13.23. — Д., 2002. — 127с.

33. Адамів, О.П. Моделі та інтелектуальні засоби адаптивного керування автономним мобільним роботом. Дис. канд.техн. наук. Одеса, 2007. 124 с.

34. Koval V., Adamiv O., Proc. of the Third IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2005). – Sofia (Bulgaria). – 2005. – P. 120- 124.

35. npm [Електронний ресурс] – Режим доступу до ресурсу: <https://www.npmjs.com/>

36. Install MongoDB [Електронний ресурс] – Режим доступу до ресурсу: <https://docs.mongodb.com/manual/administration/install-on-linux/>

37. Node.js [Електронний ресурс] – Режим доступу до ресурсу: <https://www.digitalocean.com/community/tutorials/node-js-ubuntu-18-04-ua>.

38. Linux [Електронний ресурс] – Режим доступу до ресурсу: <https://en.wikipedia.org/wiki/Linux>.

39. npm-audit [Електронний ресурс] – Режим доступу до ресурсу: <https://docs.npmjs.com/cli/audit>.

40. Kojima T. et al. Intelligent Technology for More Advanced Autonomous Driving. 2018. Hitachi Review Vol. 67, No. 1. p. 58–63.

41. SQL [Електронний ресурс] – Режим доступу до ресурсу: <https://uk.wikipedia.org/wiki/SQL>.

42. MongoDB Compass [Електронний ресурс] – Режим доступу до ресурсу: <https://www.mongodb.com/products/compass>.

43. Postman [Електронний ресурс] – Режим доступу до ресурсу: <https://www.postman.com/>

44. Саліхов М. М. Від автоматизованих до автономних транспортних засобів // Наукові досягнення та інновації: шлях до успіху. X Всеукраїнська мультидисциплінарна науково-практична Інтернет-конференція, 31 травня 2023, Україна, Київ : зб. матеріалів — Електрон. дан. — Київ : Яроченко Я. В., 2023. — с. 136-142.

45. SPA (Single-page application) [Електронний ресурс] – Режим доступу до ресурсу: <https://developer.mozilla.org/en-US/docs/Glossary/SPA>.

					ВКРБ-123.26.0042.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		74

46. Саліхов М.М. Самокеровані автомобілі та системи їх навігації// Практичні та теоретичні питання розвитку науки та освіти: матеріали VIII Міжнародної науково-практичної конференції: м. Львів, 19-20 червня 2023 року. – Львів: Львівський науковий форум, 2023. – С.53-59.

47. SPA (Single-page application) [Електронний ресурс] – Режим доступу до ресурсу: <https://developer.mozilla.org/en-US/docs/Glossary/SPA>.

48. Vargas J. et al. An Overview of Autonomous Vehicles Sensors and Their

49. Vulnerability to Weather Conditions. Sensors. 2021; 21(16):5397.

50. <https://www.coursehero.com/file/62601304/Wevolver2020AutonomousVehicleTechnologyReportpdf/> (accessed 2024 June 1).

К6ПЗ-2026

					ВКРБ-123.26.0042.00.00.ПЗ	Арк.
Вим.	Арк.	№ докум.	Підпис	Дата		75