Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

на тему:

Метод контролю доступу на основі RFID-технологій для забезпечення інформаційної безпеки приватного підприємства

Галузь знань 12 - Інформаційні технології

Спеціальність 125 – Кібербезпека

КРМКБ.220186.22.01.13 ПЗ

Виконав: студент 2 курсу, група КБм-22-1 _____ Колісник В.В.
Підпис

Керівник доц., к.т.н, доцент кафедри Кб _____ Тітова В.Ю.
Підпис

Нормоконтролер ст. викладач кафедри Кб _____ Мостовий С.В.
Підпис

До захисту допускаю:

Зав. кафедри кібербезпеки, к.т.н., доц. _____ Кльоц Ю.П.
Підпис

11 12 2023 р.

Хмельницький, 2023

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Освітній рівень Магістр

Галузь знань 12 Інформаційних технологій

Спеціальність 125 Кібербезпека

Освітня програма Кібербезпека

ЗАТВЕРДЖУЮ

Зав. кафедри Ю.П. Кльоц

"30" 08 2023 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

Колісніку Вадиму Валерійовичу

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Метод контролю доступу на основі RFID-технологій для забезпечення інформаційної безпеки приватного підприємства

Керівник роботи Тітова Віра Юріївна

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

кандидат технічних наук, доцент

Затверджена наказом № 30 ректора університету, додаток №25 від 15.08.2023

2. Строк подання студентом проєкту (роботи) на кафедру 15.11.2023

3. Вихідні дані до проекту (роботи) Розробка раціонального методу контролю доступу на основі RFID-технологій для забезпечення інформаційної безпеки приватного підприємства.

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити) Вступ. Огляд систем та методів безконтактної ідентифікації. Метод безконтактної ідентифікації в контексті забезпечення інформаційної безпеки приватного підприємства. Реалізація методу безконтактної ідентифікації на основі RFID-технологій для забезпечення інформаційної безпеки приватного підприємства. Оцінка ефективності функціонування розробленої системи безконтактної інтеграції на основі RFID-технологій для забезпечення інформаційної безпеки приватного підприємства. Висновок.

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

6. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали і посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Мостовий С.В. Старший викладач кафедри кібербезпеки		

7. Дата видачі завдання «01» вересня 2023р.

КАЛЕНДАРНИЙ ПЛАН

з/п	Назва етапів (розділів) кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Вибір напряму дослідження і узгодження тематики КРМ з керівником	01.06.2023	
2	Ознайомлення з предметною областю; формулювання мети і завдань дослідження; визначення об'єкта, предмета і методів дослідження	04.09.2023	
3	Робота над розділом 1 – аналіз відомих систем та методів безконтактної ідентифікації	18.09.2023	
4	Робота над розділом 2 – метод безконтактної ідентифікації в контексті забезпечення інформаційної безпеки приватного підприємства	02.10.2023	
5	Робота над розділом 3 – реалізація методу безконтактної ідентифікації на основі RFID-технологій	16.10.2023	
6	Робота над розділом 4 – оцінка ефективності функціонування розробленої системи	06.11.2023	
7	Робота над науковою публікацією	10.11.2023	
8	Узгодження отриманих результатів, оформлення пояснювальної записки згідно вимог	15.11.2023	
9	Попередній захист роботи	17.11.2023	
10	Захист роботи на засіданні ЕК	12.12.2023	

Студент _____ В.В. Колісник
Підпис Ініціали, прізвище

Керівник проекту (роботи) _____ В. Ю. Тітова
Підпис Ініціали, прізвище

АНОТАЦІЯ

Тема кваліфікаційної роботи: Метод контролю доступу на основі RFID-технологій для забезпечення інформаційної безпеки приватного підприємства.

Автор роботи: Колісник Вадим Валерійович

Керівник роботи: к.т.н., доц. Тітова Віра Юріївна

Загальний обсяг роботи: 106 сторінок, 50 рисунків, 8 таблиць, 3 додатки, 123 посилання.

Ключові слова: RFID, СКУД, контроль доступу, інформаційна безпека, Arduino, RFID-RC522.

Мета дослідження – розробка раціональної системи контролю доступу на основі технологій RFID для забезпечення інформаційної безпеки приватного підприємства.

Дана кваліфікаційна робота присвячена розробці системи контролю доступу для складського комплексу приватного підприємства на базі технології RFID з розробкою RFID-зчитувача, спроєктованого на основі мікроконтролера Arduino Nano та RFID-модуля – RFID-RC522.

11. 12. 2023

ANNOTATION

The topic of the qualification work: An access control method based on RFID technologies to ensure information security of a private enterprise.

Author of the work: Kolisnyk Vadym Valeriiovych

Mentor: Ph.D., Assoc. Titova Vira Yuriyivna

Total volume of work: 106 pages, 50 figures, 8 tables, 3 appendixes, 123 references.

Keywords: RFID, ACS, access control, information security, Arduino, RFID-RC522.

The purpose of the study is to develop a rational access control system based on RFID technologies to ensure the information security of a private enterprise.

This qualification work is devoted to the development of an access control system for a warehouse complex of a private enterprise based on RFID technology with the development of an RFID reader designed on the basis of an Arduino Nano microcontroller and RFID module – RFID-RC522.

11. 12. 2023

ЗМІСТ

ВСТУП

Напрямок дослідження, що реалізується в рамках поточної кваліфікаційної роботи: метод контролю доступу на основі RFID-технологій для забезпечення інформаційної безпеки приватного підприємства.

Актуальність дослідження. Дослідження методу контролю доступу на основі технологій RFID (Radio-Frequency Identification) для забезпечення інформаційної безпеки приватних підприємств в наш час є особливо актуальним і важливим [1]. Ця актуальність обумовлена кількома ключовими факторами.

По-перше, цифрова трансформація підприємств відбувається на швидкому та непередбачуваному темпі, що призводить до накопичення великих обсягів конфіденційної та критичної інформації. Ця інформація є цінним активом, і, отже, залежить від інформаційної безпеки. З усією цією ціннісною інформацією пов'язані загрози безпеці, включаючи хакерські атаки, витоки даних і кібершпигунство [2, 3].

По-друге, вимоги до захисту особистих даних та конфіденційної інформації, які накладаються регуляторними органами, стали надзвичайно суворими. GDPR в Європі і подібні законодавчі акти в інших регіонах вимагають від підприємств дотримуватися строгих стандартів захисту даних та реагувати на порушення з високою відповідальністю [4, 5].

По-третє, еволюція загроз безпеці включає в себе постійне вдосконалення технік атак і підходів, включаючи нові види соціального інженірінгу та адаптацію до захисних заходів. Відповідно, системи безпеки повинні надавати відповідь на ці зміни [6, 7].

По-четверте, внутрішні загрози від працівників підприємства можуть бути не менш небезпечними, ніж зовнішні атаки. Тому контроль доступу до різних ресурсів та приміщень підприємства стає критичним елементом для запобігання інсайдерським загрозам [8, 9].

Отже, дослідження та впровадження методу контролю доступу на основі RFID-технологій стає важливою стратегією для забезпечення інформаційної безпеки приватних підприємств у сучасному інформаційному середовищі. Така система дозволить підприємствам підвищити рівень захисту конфіденційної інформації, відповідати регуляторним вимогам і зменшити зовнішні та внутрішні загрози.

Мета дослідження – розробка раціонального методу контролю доступу на основі RFID-технологій для забезпечення інформаційної безпеки приватного підприємства.

Завдання дослідження:

– огляд систем та методів безконтактної ідентифікації: види систем безконтактної ідентифікації; огляд обладнання безконтактної ідентифікації; стандарти та нормативні вимоги до функціонування систем безконтактної ідентифікації;

– метод безконтактної ідентифікації в контексті забезпечення інформаційної безпеки приватного підприємства: загальна концепція системи інформаційної безпеки приватного підприємства; роль безконтактної ідентифікації в забезпеченні інформаційної безпеки приватного підприємства; огляд типових рішень з улаштування безконтактної ідентифікації для забезпечення інформаційної безпеки приватних підприємств;

– реалізація методу безконтактної ідентифікації на основі RFID-технологій для забезпечення інформаційної безпеки приватного підприємства: проєктна реалізація методу у вигляді системи RFID-ідентифікації; апаратна реалізація методу у вигляді системи RFID-ідентифікації; програмна реалізація методу у вигляді системи RFID-ідентифікації;

– оцінка ефективності функціонування розробленої системи безконтактної інтеграції на основі RFID-технологій для забезпечення інформаційної безпеки приватного підприємства: налаштування розробленої системи RFID-ідентифікації; оцінка ефективності функціонування розробленої

системи RFID-ідентифікації; оцінка ефективності функціонування розробленої системи RFID-ідентифікації з урахуванням інтеграції в загальну систему безпеки приватного підприємства.

Предмет дослідження – метод безконтактної ідентифікації та контролю доступу на базі технології RFID.

Об'єкт дослідження – забезпечення контролю доступу та інформаційної безпеки приватного підприємства.

Методи дослідження. Для дослідження методу контролю доступу на основі технологій RFID для забезпечення інформаційної безпеки приватного підприємства використовуються наступні методи:

1. Аналіз інформаційних джерел: Проводиться огляд наукових публікацій, статей, та робіт, що стосуються систем контролю доступу та технологій RFID. Цей аналіз допомагає отримати загальний огляд видів систем та обладнання RFID, а також нормативних вимог і стандартів до їх функціонування.

2. Аналіз обладнання: Проводиться докладний аналіз доступного обладнання для систем контролю доступу на основі RFID, включаючи зчитувачі, мітки та інші компоненти. Цей аналіз визначає можливості використання конкретних технологій у дослідженні.

3. Аналіз стандартів і нормативних вимог: Проводиться детальний аналіз стандартів і вимог, які стосуються систем контролю доступу на основі RFID. Це допомагає встановити вимоги до безпеки та функціонування таких систем.

4. Аналіз концепції інформаційної безпеки: Проводиться аналіз загальної концепції інформаційної безпеки приватного підприємства, включаючи методи захисту даних і виявлення загроз.

5. Оцінка ролі методу контролю доступу на основі RFID: Визначається, як системи контролю доступу на основі RFID можуть сприяти забезпеченню інформаційної безпеки підприємства, зокрема, обмеження фізичного доступу до ресурсів і приміщень.

6. Розробка системи RFID-ідентифікації: Проводиться проєктна, апаратна та програмна реалізація методу у вигляді системи контролю доступу на основі RFID.

7. Аналіз ефективності системи: Проводяться експерименти, тести та аналіз даних для оцінки ефективності функціонування системи RFID-ідентифікації, з урахуванням параметрів безпеки, продуктивності та ресурсів.

8. Оцінка інтеграції: Якщо систему контролю доступу на основі RFID необхідно інтегрувати в загальну систему безпеки підприємства, проводиться оцінка ефективності такої інтеграції та її впливу на інформаційну безпеку.

Застосування цих методів дослідження дозволить провести науково обґрунтоване дослідження методу контролю доступу на основі RFID-технологій для забезпечення інформаційної безпеки приватного підприємства.

Наукова новизна дослідження полягає в доповненні та розширенні наявних знань у галузі систем контролю доступу та їхнього застосування для забезпечення інформаційної безпеки приватних підприємств за допомогою RFID-технологій. Пропонується комплексний підхід до використання технологій RFID для підвищення інформаційної безпеки підприємств. Це включає в себе фізичний контроль доступу, автентифікацію працівників та моніторинг руху в приміщеннях. Дослідження включає розробку повноцінної інтегрованої системи контролю доступу на основі RFID-технологій, що враховує специфічні потреби та вимоги приватних підприємств. Дослідження розглядає питання інтеграції методу контролю доступу на основі RFID в загальну систему безпеки підприємства, що є актуальним аспектом у сучасному бізнес-середовищі. Загальна наукова новизна полягає в тому, що дослідження розширює розуміння можливостей та переваг використання RFID-технологій для підвищення інформаційної безпеки приватних підприємств та пропонує комплексні рішення для цього питання.

Практична цінність отриманих результатів є багатоаспектною для приватних підприємств та організацій, які прагнуть забезпечити високий рівень інформаційної безпеки та контролю доступу до своїх ресурсів і приміщень. Розроблені рішення системи контролю доступу на основі RFID-технологій

дозволяють підприємствам ефективно обмежувати фізичний доступ до приміщень та об'єктів, зменшуючи ризик незаконного вторгнення та крадіжок. Використання RFID для ідентифікації працівників та гостей дозволяє контролювати доступ до конфіденційної інформації та зменшує можливість витоку цінних даних. Системи контролю доступу на основі RFID можуть спростити процес управління доступом, автоматизувати облік присутності працівників і гостей, а також надавати звіти та журнали для моніторингу. Розроблені рішення дозволяють підприємствам відповідати вимогам і стандартам щодо захисту даних і фізичної безпеки, включаючи вимоги GDPR і інших регуляторних органів. Системи контролю доступу на основі RFID допомагають запобігати інсайдерським загрозам, таким як незаконний доступ працівників до обмежених ресурсів або критичних даних. Розроблені рішення можуть бути інтегровані в загальну систему безпеки підприємства, що покращує координацію та ефективність заходів безпеки. Зменшення часу, витраченого на фізичний доступ і ідентифікацію, сприяє підвищенню продуктивності працівників. Завдяки автоматизації та оптимізації процесів контролю доступу, підприємства можуть зменшити витрати на фізичну безпеку та адміністративні витрати. Отже, отримані результати дослідження сприяють підвищенню рівня безпеки та ефективності функціонування приватних підприємств, а також допомагають відповідати сучасним вимогам і стандартам у сфері інформаційної безпеки.

До переліку публікацій за темою кваліфікаційної роботи відноситься стаття подана у журнал Вісник ХНУ. Стаття за темою кваліфікаційної роботи наведена у Додатку А.

1 ОГЛЯД СИСТЕМ ТА МЕТОДІВ БЕЗКОНТАКТНОЇ ІДЕНТИФІКАЦІЇ

1.1 Види систем безконтактної ідентифікації

Системи безконтактної ідентифікації базуються на різних технологіях і принципах, які дозволяють ідентифікувати об'єкти або осіб без прямого фізичного контакту [10 – 12]. Основні види систем безконтактної ідентифікації включають наступні технології.

RFID використовує радіочастотні сигнали для безконтактного зчитування інформації з RFID-міток або карток. Зчитувач генерує радіосигнал, який живить мітку. Мітка передає відповідь, містять ідентифікатор або дані, на зчитувач. Використовується для ідентифікації та відстеження товарів, контролю доступу до приміщень, автоматизації логістики, ведення інвентарю та багатьох інших застосувань [13, 14].

NFC (Near Field Communication) – це технологія обміну даними на найближчих відстанях (до 10 см) між двома пристроями з підтримкою NFC. Вона використовує радіохвильовий зв'язок для передачі даних. NFC використовується для безконтактної оплати (Google Pay, Apple Pay), керування електронними квитками (проїздні, квитки на заходи), обміну контактами та інших даними між смартфонами [15, 16].

Bluetooth – це бездротова технологія зв'язку, яка дозволяє під'єднувати різні пристрої для обміну даними, включаючи ідентифікацію. Протокол Bluetooth забезпечує зв'язок на короткій відстані. Використовується для бездротових навушників, клавіатур, мишок, підключення до аудіосистем в автомобілях, інтернет-розповсюджувачів та інших пристроїв [17, 18].

Біометрична ідентифікація використовує біометричні характеристики, такі як відбитки пальців, розпізнавання обличчя, голосу, структура сітківки або вен на долонях для ідентифікації осіб. Використовується для розблокування смартфонів,

входу в об'єкти з обмеженим доступом, біометричного паспорту та інших застосувань, де потрібна надійна ідентифікація особи [19, 20].

QR-код – це двомірний штрих-код, який містить інформацію. Зчитувачі QR-кодів можуть розпізнавати ці коди і отримувати інформацію з них. Використовується для сканування кодів на продуктах для отримання додаткової інформації, рекламних кампаній, логістики та інших цілей [21, 22].

Інфрачервоний зв'язок (IR) використовує інфрачервоні промені для передачі даних між пристроями на короткі відстані. Застосовується у пульті дистанційного керування, обміну даними між смартфонами та ноутбуками на найближчих відстанях [23, 24].

Кожна з цих технологій має свої особливості та застосування, і вони широко використовуються у сучасному світі для різних цілей, від ідентифікації та відстеження до спілкування та навігації.

В контексті використання у системах контролю доступу різні технології безконтактної ідентифікації (RFID, NFC, Bluetooth, біометрична ідентифікація, QR-код та IR) мають свої переваги та недоліки, які варто враховувати при виборі технології для конкретного проекту (табл. 1).

Таблиця 1 – Переваги та недоліки технологій безконтактної ідентифікації при використанні у системах контролю доступу [25 – 29]

Технологія безконтактної ідентифікації, що може бути використана для побудови системи контролю доступу	Переваги застосування	Недоліки застосування
1	2	3
RFID	Висока швидкість ідентифікації. Можливість працювати на великій відстані від зчитувача.	Вища вартість обладнання порівняно з іншими технологіями.

Продовження таблиці 1

1	2	3
	Можливість ідентифікації без прямого видимого контакту.	Можливість клонування міток, якщо не застосовується відповідний захист. Можливість перешкод для роботи в електромагнітному середовищі.
NFC	Висока безпека завдяки короткому діапазону дії. Зручність використання в сучасних смартфонах. Підтримка безконтактної оплати та інших застосувань.	Дуже коротка відстань взаємодії (до 10 см). Вразливість до перешкод та перешкод у стандартному використанні.
Bluetooth	Зручність використання в багатьох сучасних пристроях. Можливість підключення багатьох пристроїв одночасно. Висока швидкість передачі даних.	Вищий рівень енергоспоживання порівняно з іншими технологіями. Можливість атак на безпеку вразливих версій Bluetooth. Потреба в паруванні та ініціалізації.
Біометрична ідентифікація	Висока надійність та стійкість до злому при належній реалізації. Унікальність біометричних даних особи. Висока безпека.	Висока вартість обладнання для збору біометричних даних. Можливість відмови через погану якість зчитування біометричних даних (наприклад, відбитків пальців). Потреба у збереженні та захисті біометричних даних.
QR-код	Простота генерації та сканування кодів. Низька вартість реалізації.	Низька надійність, легко може бути підроблений. Обмеженість обсягу інформації в коді. Залежність від доступу до камери пристрою для сканування.

Кінець таблиці 1

1	2	3
IR	Низька вартість обладнання. Низький рівень енергоспоживання.	Дуже коротка відстань взаємодії та потреба в прямому «видимому» контакті. Вразливість до перешкод і обмежень в орієнтації.

Вибір технології для системи контролю доступу повинен базуватися на конкретних вимогах до безпеки, функціональності, бюджеті та інших чинниках. Важливо зважати на переваги та недоліки кожної технології, а також належним чином налаштовувати та захищати систему, щоб забезпечити необхідний рівень безпеки та зручності використання.

З метою обґрунтування вибору технології безконтактної ідентифікації для проєктування системи контролю доступу та забезпечення інформаційної безпеки приватного підприємства виконаємо ранжування визначених технологічних рішень за специфічними критеріями (табл. 2).

Таблиця 2 – Ранжування технології безконтактної ідентифікації для проєктування системи контролю доступу та забезпечення інформаційної безпеки приватного підприємства (за результатами експертної оцінки [30 – 34])

Критерії	RFID	NFC	Bluetooth	Біометрична ідентифікація	QR-код	IR
1	2	3	4	5	6	7
Надійність	9	8	6	8	3	4
Стійкість до злому або підробки	9	7	5	10	3	4
Доступність швидкого розгортання	7	7	8	3	9	9
Економічна обґрунтованість застосування	6	6	7	2	9	8

Кінець таблиці 2

1	2	3	4	5	6	7
Доступність використання	7	8	8	6	9	7
Ранжування	7,6	7,2	6,8	5,8	6,6	6,4

Оцінки надаються в балах від 1 до 10, де 1 – низька оцінка, а 10 – висока оцінка.

За результатами експертної оцінки за профільними критеріями для використання у системах контролю доступу та забезпечення інформаційної безпеки приватного підприємства (табл. 2), можна зробити наступні висновки:

– біометрична ідентифікація має найвищий рейтинг надійності та стійкості до злому, що робить її однією з найбільш перспективних технологій для систем контролю доступу та інформаційної безпеки. RFID також має високі показники.

– Bluetooth та QR-коди відзначаються високою доступністю для швидкого розгортання. Однак QR-коди мають перевагу з економічної точки зору. Наприклад, вони можуть бути дешевшими у використанні порівняно з біометричною ідентифікацією.

– NFC та Bluetooth мають високий рейтинг доступності використання, особливо в сучасних смартфонах. Біометрична ідентифікація також є доступною для користувачів.

Загалом, за результатами ранжування, RFID має найвищий бал загальної ефективності серед розглянутих технологій, але слід враховувати, що це залежить від конкретних вимог та обставин проекту. NFC та Bluetooth також демонструють досить високий рівень ефективності. QR-коди та IR мають менший загальний рейтинг.

Отже, вибір технології безконтактної ідентифікації для системи контролю доступу повинен базуватися на конкретних потребах та вимогах вашого проекту. Біометрична ідентифікація може бути найкращим вибором для високого рівня безпеки, але вона може бути витратною. NFC та Bluetooth можуть бути зручними

та ефективними для багатьох застосувань, а QR-коди можуть бути бюджетним варіантом для менших підприємств.

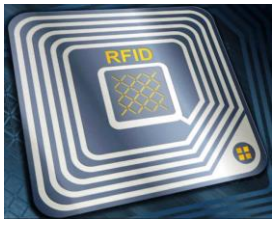
Таким чином, технологія RFID є найбільш доцільними вибором для формування системи контролю доступу та забезпечення інформаційної безпеки приватного підприємства (табл. 2). RFID отримав високу оцінку за надійність та стійкість до злому. Ця технологія відома своєю здатністю працювати навіть в найвимогливіших умовах, що робить її надзвичайно надійною для систем контролю доступу. Хоча розгортання інфраструктури RFID може бути середньою за складністю, воно все ж відзначається доступністю для швидкого розгортання в порівнянні з більш складними технологіями. Використання RFID в системах контролю доступу зазвичай є досить простим і зручним для користувачів. Проходження через точку доступу вимагає простого прокладання картки або мітки перед зчитувачем.

Загалом, за результатами ранжування (табл. 2), технологія RFID отримала найвищу експертну оцінку. Зважаючи на ці фактори, можна зробити висновок, що RFID є оптимальним вибором для формування системи контролю доступу та забезпечення інформаційної безпеки приватного підприємства.

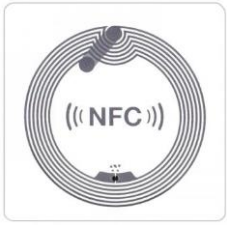
1.2 Огляд обладнання безконтактної ідентифікації

Обладнання для систем безконтактної ідентифікації включає в себе різні компоненти та пристрої, які використовуються для зчитування, розпізнавання та обробки ідентифікаційних даних (табл. 3).

Таблиця 3 – Кластеризація обладнання для технологій безконтактної ідентифікації в структурі систем контролю доступу [35– 39]

Тип обладнання	Технологія використання	Короткий опис	Загальний вигляд
1	2	3	4
Зчитувачі	RFID-зчитувачі	Це пристрої, які взаємодіють з RFID-мітками або картками та читають інформацію з них. Зазвичай це можуть бути стаціонарні чи портативні зчитувачі.	
	NFC-зчитувачі	Це пристрої, що призначені для зчитування NFC-тегів або смартфонів з підтримкою NFC. Використовуються в основному для короткодіючих дистанційних операцій.	
	Bluetooth-зчитувачі	Це пристрої, що використовуються для зчитування інформації з Bluetooth-пристроїв, таких як смартфони чи інші мобільні пристрої, які використовуються для ідентифікації.	
Мітки, теги або картки	RFID-мітки	Електронні пристрої маленького розміру, які містять інформацію і можуть бути закріплені на об'єктах або розташовані в картках.	

Продовження таблиці 3

1	2	3	4
	NFC-теги	Схожі на RFID-мітки, але здатні взаємодіяти з NFC-зчитувачами в короткодіючому діапазоні.	
	Смарт-картки	Картки, які містять чип або інші електронні компоненти для зберігання інформації та забезпечення безпеки ідентифікації.	
Біометричні пристрої	Сканер відбитків пальців	Сенсори для сканування відбитків пальців, які дозволяють ідентифікувати особу за унікальними біометричними даними.	
	Сканер обличь	Камери та програмне забезпечення для розпізнавання повністю обличчя або його елементів	
Камери відеоспостереження	Камери	Використовуються для відстеження та запису подій, пов'язаних з контролем доступу.	

Кінець таблиці 3

1	2	3	4
Контролери та центральні системи	Елементи керування	Системи керування та контролю, які обробляють інформацію з зчитувачів та виконують рішення щодо доступу.	
Інтерфейси та програмне забезпечення		Програми для налаштування, моніторингу та адміністрування системи контролю доступу.	
Інші елементи безпеки		Включають в себе елементи, такі як бар'єри, дверні замки, сигналізацію, які можуть бути активовані або деактивовані згідно з інформацією, отриманою від системи ідентифікації.	

Оскільки за результатами експертної оцінки встановлено, що для розгортання системи контролю доступу та забезпечення інформаційної безпеки приватного підприємства доцільно застосовувати технологію RFID, то детальніше зупинимось на типових схемах улаштування таких систем безпеки.

Зокрема наведемо принципову схему для розгортання системи контролю доступу RFID для керування вхідними дверима (рис.1).

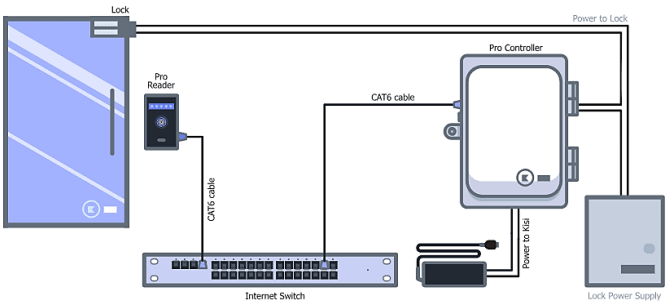


Рисунок 1 – Принципова схема системи контролю доступу RFID для керування вхідними дверима [40]

Масштабування принципової схеми до потреб підприємства потребує розгортання серверного обладнання (рис.2).

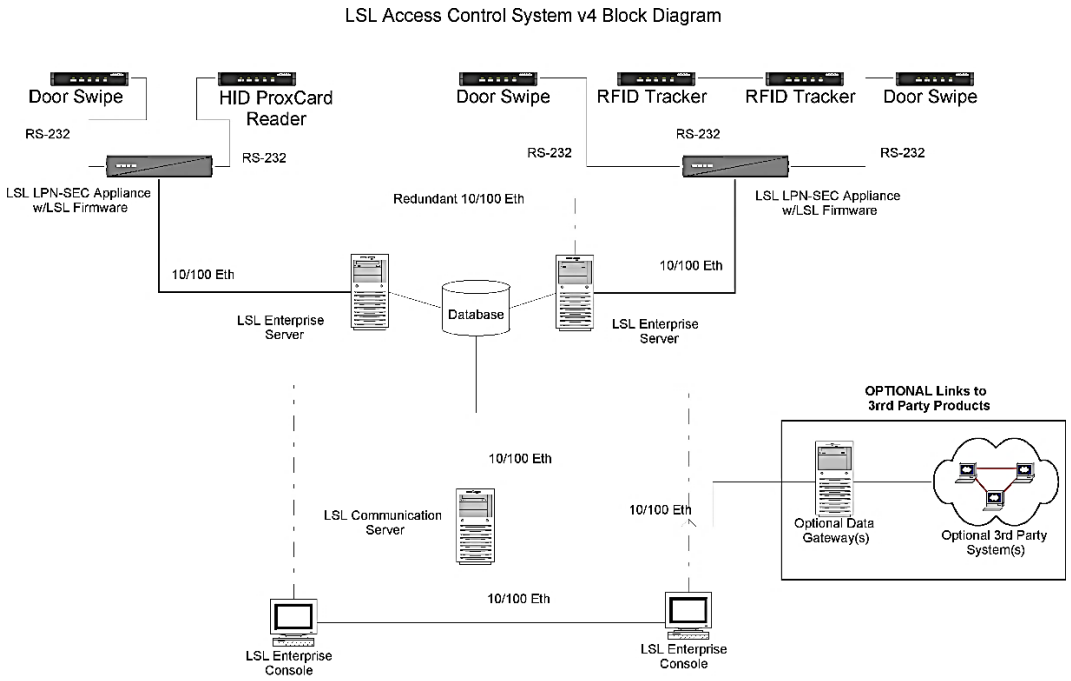


Рисунок 2 – Принципова схема розгортання системи контролю доступу RFID в масштабі підприємства [41]

LSL ACS v4 (рис.2) складається з п’яти ключових компонентів, трьох програмних компонентів LSL, одного апаратного пристрою LSL, а також сервера бази даних [41]:

– LSL LPN-SEC – апаратний пристрій, який взаємодіє з фізичними зчитувачами, спілкується безпосередньо з LES через резервний, зашифрований захищений канал AES;

– LSL Enterprise Server (LES) – основний резервний сервер, який взаємодіє з усіма компонентами, інтерфейсами до бази даних і координує всю обробку;

– LSL Communication Server (LCS) – основний сервер, який взаємодіє з компонентами графічного інтерфейсу, інтерфейсами до бази даних, інтерфейсами

до продуктів сторонніх розробників і обробляє стислі потоки даних від LSL LPN-SEC;

– LSL Enterprise Console (LEC) – графічний інтерфейс користувача для конфігурації, моніторингу та керування корпоративною системою контролю доступу та відстеження активів.

Ця система дозволяє відстежувати, перевіряти, контролювати та негайно анулювати цифрові ключі-картки в реальному часі. Кожна RFID-мітка, карта доступу або доступ до ProxCard перевіряється на базову базу даних безпеки. Якщо власнику картки дозволено доступ до зони, електромагніт дверей спрацьовує та відкривається. Для успішного входу робиться запис у журналі. Якщо доступ заборонений, двері не відчиняються, і створюється журнал безпеки [41].

Узагальнююча принципова схему елементів системи контролю доступу RFID, що може бути використана в масштабах підприємства містить графічний опис механізму функціонування проєктної системи безпеки та дозволяє сформувати висновки щодо формування архітектури досліджуваних кіберфізичних систем (рис. 3).

Рисунок 3 – Принципова схема елементів системи контролю доступу RFID для промислового використання [42]

Таким чином, для розгортання системи контролю доступу на базі технології RFID, необхідно обладнання, яке включає в себе наступні компоненти:

- RFID-зчитувачі (RFID Readers): стаціонарні RFID-зчитувачі: Ці зчитувачі монтуються на вхідних дверях або брамах і використовуються для автоматичного зчитування RFID-міток або карток при вході або виході з приміщення; Портативні RFID-зчитувачі: Ці пристрої переносяться операторами безпеки та використовуються для зчитування міток у віддалених або обмежених областях.
- RFID-мітки (RFID Tags або Cards): RFID-картки: Це пластикові картки, які містять RFID-чіп або антенну для зчитування; RFID-мітки: Маленькі мітки, які можуть бути прикріплені до об'єктів або вбудовані в етикетки, одяг чи інші предмети;
- RFID-контролери: контролери обробляють інформацію, отриману від зчитувачів, і приймають рішення щодо доступу. Вони можуть бути вбудованими в зчитувачі або окремими пристроями;
- Система керування: ПЗ для налаштування та адміністрування системи контролю доступу на основі RFID. Вона дозволяє додавати, видаляти та налаштовувати правила доступу, а також вести журнал подій.
- Дверні замки та бар'єри: зазвичай це фізичні пристрої, які керують фізичним доступом до приміщень або областей. Вони можуть бути активовані або деактивовані контролером на основі RFID.
- живлення та мережеве обладнання: забезпечення живлення для зчитувачів та контролерів, а також мережевого з'єднання для обміну даними та керування системою.
- засоби ідентифікації користувачів: RFID-картки або мітки, які видаватимуться користувачам системи для ідентифікації.
- відеоспостереження (опційно): камери та системи відеоспостереження можуть бути інтегровані з системою контролю доступу для додаткового моніторингу та безпеки.
- бази даних та сервери (опційно): для зберігання та обробки інформації про ідентифікацію користувачів.
- безпека та захист: заходи безпеки, такі як шифрування даних і захист від несанкціонованого доступу, повинні бути враховані при проектуванні системи.

Це загальний перелік компонентів, необхідних для системи контролю доступу на базі RFID. Конкретні компоненти та їх кількість будуть залежати від проєктних рішень.

1.3 Стандарти та нормативні вимоги до функціонування систем безконтактної ідентифікації

Функціонування систем безконтактної ідентифікації, включаючи системи на базі технології RFID, регулюється різними стандартами і нормативами з метою забезпечення безпеки, сумісності та правильності роботи. Ось деякі з ключових стандартів та нормативних вимог, які відповідають за цей аспект:

1. ISO 14443 [43] та ISO 15693 [44]: Ці стандарти визначають протоколи зчитування і запису для багатьох типів RFID-міток. Вони регулюють частоту, робочий діапазон, формати даних та методи шифрування для забезпечення сумісності і безпеки.
2. ISO 18000 [45]: Цей стандарт визначає загальні вимоги до RFID-систем, включаючи характеристики міток, зчитувачів та протоколи комунікації. Він сприяє розробці сумісних та стандартизованих рішень.
3. ISO 7816 [46]: Цей стандарт визначає фізичні та електричні характеристики смарт-карток, а також протоколи комунікації. Він є ключовим для безпеки смарт-карток, що використовуються в системах ідентифікації.
4. NIST SP 800-116 [47]: Даний документ визначає рекомендації щодо застосування RFID в урядових системах та публічних інфраструктурах. Він включає в себе вимоги до захисту даних та приватності.
5. EPCglobal (Electronic Product Code Global) [48]: Ця організація визначає стандарти для застосування RFID в логістиці та постачанні ланцюжка. Їх стандарти включають EPC Gen2 для UHF RFID.
6. GDPR (General Data Protection Regulation) [49]: Це європейське регулювання забезпечує захист особистих даних громадян, включаючи дані, які можуть бути зібрані та оброблені системами ідентифікації.

7. FIPS 201 [50]: Федеральний стандарт США визначає вимоги до ідентифікаційних карток та токенів, які використовуються для фізичного та логічного доступу до федеральних інформаційних систем.

Ці стандарти та нормативи мають на меті забезпечити високий рівень безпеки, прозорості та сумісності в системах безконтактної ідентифікації, а також захист особистих даних користувачів. При розгортанні системи контролю доступу на базі технології RFID важливо дотримуватися цих стандартів і вимог, щоб забезпечити надійну та безпечну роботу системи.

На території України також діють ряд нормативних регламентів, що регулюють положення використання систем безконтактної ідентифікації, зокрема RFID:

1. ДСТУ EN 16656:2020 [51] є стандартом інформаційних технологій, який стосується радіочастотної ідентифікації (RFID) для керування предметами. Цей стандарт визначає та регулює основні принципи та вимоги щодо використання технології RFID для ідентифікації та взаємодії з предметами. Стандарт містить важливі вимоги щодо використання емблем RFID (Radio Frequency Identification), включаючи вимоги до протоколів комунікації, форматів даних, безпеки та приватності. Він є ідентичним (IDT) стандарту EN 16656:2014 та має модифікації відповідно до ISO/IEC 29160:2012. Цей стандарт допомагає стандартизувати та забезпечувати сумісність в галузі використання RFID для керування предметами, що дозволяє ефективніше впроваджувати та використовувати цю технологію в різних галузях, включаючи логістику, служби безпеки та багато інших сфер діяльності.

2. ДСТУ ISO/IEC 14443-1:2008 [52] – це стандарт, який стосується ідентифікаційних карток з інтегрованими безконтактними мікросхемами, відомих як картки близької взаємодії. Ця частина стандарту фокусується на фізичних характеристиках цих карток. Стандарт визначає фізичні параметри та характеристики карток близької взаємодії, такі як розмір, форма, матеріали, взаємодія з читаючим обладнанням та електричні характеристики. Він встановлює основні стандартизовані вимоги до цих карток з метою забезпечення їхньої

сумісності та правильності роботи. Цей стандарт є важливим для виробників і користувачів ідентифікаційних карток з інтегрованими мікросхемами, оскільки він сприяє створенню стандартів та виробництву карток, які можуть взаємодіяти зі сумісними читаючими пристроями. Це дозволяє карткам близької взаємодії бути більш універсальними та використовуватися в різних сферах, включаючи системи безконтактної ідентифікації та безпеки.

3. ДСТУ ISO/IEC 15693-1:2008 [53] – це стандарт, який стосується ідентифікаційних карток на інтегрованих безконтактних мікросхемах з розширеним радіусом дії. Ця частина стандарту обговорює фізичні характеристики таких карток. Стандарт визначає параметри та характеристики цих безконтактних карток, зокрема їхні розміри, форму, електричні характеристики та інші фізичні аспекти. Він має на меті стандартизувати ці характеристики для забезпечення сумісності та правильності роботи карток із сумісними читаючими пристроями. Цей стандарт є важливим для виробників та користувачів безконтактних ідентифікаційних карток з розширеним радіусом дії, оскільки він допомагає створювати картки, які можуть ефективно працювати на великих відстанях від читаючого обладнання. Це робить їх більш універсальними та використовуваними в різних додатках, таких як контроль доступу, логістика та інші сфери діяльності.

4. ДСТУ ISO/IEC 7816-1:2008 [54] – це стандарт, який стосується ідентифікаційних карток на інтегрованих мікросхемах з контактами. Ця частина стандарту обговорює фізичні характеристики таких карток. Стандарт визначає фізичні параметри і характеристики цих ідентифікаційних карток, включаючи їхні розміри, форму, матеріали та електричні характеристики. Він має на меті стандартизувати ці характеристики для забезпечення сумісності та правильності роботи карток із контактами і сумісними читаючими пристроями. Цей стандарт є важливим для виробників та користувачів ідентифікаційних карток з контактами, таких як смарт-картки. Він допомагає створювати картки, які можуть ефективно взаємодіяти з іншим обладнанням і забезпечувати безпеку та надійність ідентифікації. Цей стандарт також має попередню версію від 1998 року (ISO/IEC 7816-1:1998), і ДСТУ ISO/IEC 7816-1:2008 є ідентичним їй (IDT).

5. ДСТУ ISO/IEC 10536-1:2008 [55] – це стандарт, який стосується ідентифікаційних карток на інтегрованих безконтактних мікросхемах, відомих як картки тісної взаємодії. Ця частина стандарту визначає фізичні характеристики таких карток. Стандарт встановлює параметри і характеристики цих безконтактних карток, такі як їх розміри, форма, матеріали та електричні характеристики. Він спрямований на стандартизацію цих фізичних аспектів для забезпечення сумісності та правильності роботи карток із сумісними читаючими пристроями. Цей стандарт є важливим для виробників та користувачів ідентифікаційних карток тісної взаємодії, оскільки він допомагає забезпечувати стандартизований фізичний дизайн цих карток. Це робить їх більш універсальними та забезпечує їхню взаємодію з різними пристроями та системами, включаючи системи контролю доступу та інші сфери застосування.

Наведені стандарти мають також інші частини, що регламентують аспекти використання елементів систем безконтактної ідентифікації, що використовуються для розгортання безпекових систем контролю доступу.

Варто відзначити, що українські нормативи є достатньо гармонізованими з аналогічними регламентами провідних держав світу.

Стандарти та нормативні вимоги до функціонування систем безконтактної ідентифікації є важливими елементами для забезпечення безпеки, сумісності та ефективності таких систем. Основні висновки з цього контексту включають таке:

1. Стандарти і нормативні вимоги сприяють створенню єдиної та універсальної системи безконтактної ідентифікації, яка може працювати з різним обладнанням та програмним забезпеченням.

2. Вимоги щодо безпеки та приватності допомагають захищати дані користувачів і запобігають несанкціонованому доступу до системи. Заходи безпеки допомагають уникати потенційних загроз інформаційній безпеці.

3. Стандарти допомагають забезпечити ефективність та надійність функціонування систем безконтактної ідентифікації. Це важливо для швидкої та точної ідентифікації об'єктів або осіб.

4. Стандарти дозволяють системам безконтактної ідентифікації бути сумісними з різними галузями, такими як логістика, безпека, медицина та багато інших. Це робить їх більш універсальними та застосовними.

5. Стандарти створюють рівні умови для виробників та користувачів, дозволяючи їм працювати з однаковим обладнанням і забезпечуючи стабільність і надійність систем.

Таким чином, стандарти та нормативні вимоги є фундаментальними елементами для розробки, розгортання та ефективного функціонування систем безконтактної ідентифікації. Вони допомагають забезпечити безпеку, сумісність і надійність цих систем у різних галузях та застосуваннях.

2 МЕТОД БЕЗКОНТАКТНОЇ ІДЕНТИФІКАЦІЇ В КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИВАТНОГО ПІДПРИЄМСТВА

2.1 Загальна концепція системи інформаційної безпеки приватного підприємства

Загальна концепція системи інформаційної безпеки (ІБ) приватного підприємства полягає в створенні та впровадженні комплексу заходів, які забезпечують захист інформації підприємства від ризиків та загроз, які можуть виникнути ззовні або всередині організації. Основна мета системи ІБ полягає в забезпеченні конфіденційності, цілісності та доступності інформації, а також у зменшенні можливих фінансових, правових та репутаційних ризиків для підприємства. Ця концепція передбачає захист інформації від несанкціонованого доступу, руйнування, втрати або розголошення, а також забезпечення можливості її використання в потрібний момент [56, 57].

ІБ приватного підприємства є складною системою, що має кілька ключових складових (рис. 4)

Виконаємо опис складових концепції ІБ приватного підприємства (рис. 4).

Моніторинг репутаційного статусу, у контексті системи інформаційної безпеки (ІБ) приватного підприємства, є невід'ємною складовою для забезпечення безпеки та захисту ділової репутації організації в цифровому віконці. Цей елемент системи ІБ виконує ключову роль у виявленні, відстеженні та відповіді на потенційні загрози та ризики, які можуть вплинути на репутацію підприємства, що напряму впливає на економічну успішність, сталий розвиток та розширення клієнтської бази [58].

Рисунок 4 – Загальна концепція ІБ приватного підприємства

Моніторинг репутаційного статусу включає в себе наступні аспекти [59, 60]:

1. Систематичний збір інформації з різних джерел, таких як соціальні медіа, новини, відгуки клієнтів, форуми тощо. Зібрана інформація аналізується для виявлення будь-яких вказівок або сигналів, що можуть вказувати на потенційну загрозу репутації.

2. Спостереження за реакцією громадськості на дії та події, пов'язані з підприємством. Це включає в себе аналіз відгуків, коментарів та відгуків у соціальних медіа та інших відкритих джерелах.

3. Виявлення можливих загроз для репутації підприємства, таких як негативні новини, атаки з боку конкурентів або витоки конфіденційної інформації.

4. Розробка планів дій і стратегій відповіді на інциденти, що можуть вплинути на репутацію. Це включає в себе створення комунікаційних стратегій та публічних заяв для зменшення негативного впливу інциденту.

5. Прийняття заходів для збереження та відновлення репутації, якщо вона була піддана негативному впливу. Це може включати в себе публічні виправлення помилок, активну комунікацію зі стейкхолдерами та інші заходи.

Моніторинг репутаційного статусу є важливим для бізнесу, оскільки погіршення репутації може призвести до втрати клієнтів, партнерів, інвесторів та негативно вплинути на фінансовий стан підприємства. Цей елемент системи ІБ допомагає підприємству оперативно реагувати на загрози та ефективно захищати свою репутацію в динамічному інформаційному середовищі [61].

Кібербезпека, і як елемент системи ІБ приватного підприємства, є комплексом спеціальних заходів та стратегій, спрямованих на захист цифрових активів, інформаційних ресурсів та інфраструктури від кіберзагроз та кібератак. Кібербезпека має на меті забезпечити конфіденційність, цілісність та доступність цифрової інформації, а також захистити цифрові системи від незаконного доступу, руйнування або крадіжки [62].

Основні аспекти кібербезпеки включають наступні елементи [63, 64]:

1. Визначення осіб чи систем, які мають доступ до цифрових ресурсів. Це включає в себе використання паролів, біометричних методів, карток доступу тощо.

2. Виявлення та блокування вірусів, троянців, шпигунського ПЗ та інших шкідливих програм, які можуть завдати шкоди системі.

3. Захист мережевої інфраструктури від несанкціонованого доступу, зломів та атак.

4. Шифрування конфіденційної інформації, забезпечення резервного копіювання даних та захист від витоків інформації.

5. Системи моніторингу та аналізу подій для виявлення аномалій та потенційних кіберзагроз.

6. Розробка планів дій та стратегій для відповіді на кіберінциденти та відновлення роботи систем після атак.

7. Навчання персоналу впізнавати та запобігати соціальним атакам та маніпуляціям.

8. Заходи для запобігання та виявлення загроз зсередини організації, таких як витоки даних або зловживання привілеями.

Кібербезпека важлива для підприємств у зв'язку зі зростанням кількості та складності кіберзагроз у сучасному цифровому світі. Забезпечення ефективної кібербезпеки є критично важливим завданням для збереження довіри стейкхолдерів та успішного функціонування підприємства в цифровому середовищі [65].

Економічна безпека, у рамках системи ІБ приватного підприємства, представляє собою важливий аспект, спрямований на захист фінансових ресурсів, активів та економічної стійкості організації в умовах цифрового середовища. Економічна безпека має на меті запобігти фінансовим втратам, зберегти фінансову стабільність та забезпечити ефективне господарювання підприємства [66].

Основні аспекти економічної безпеки включають наступні елементи [67, 68]:

1. Захист конфіденційних фінансових даних від несанкціонованого доступу та витоків, що можуть призвести до фінансових втрат.

2. Заходи для виявлення та запобігання фінансовим атакам, таким як крадіжка грошей, фінансовий обман або маніпуляції з фінансовими операціями.

3. Заходи для забезпечення доступності фінансових активів та можливості їх використання в умовах надзвичайних обставин або кіберінцидентів.

4. Моніторинг фінансових операцій та виявлення аномалій, що можуть свідчити про фінансовий обман або шахрайство.

5. Впровадження систем фінансового аудиту та внутрішнього контролю для виявлення та запобігання фінансовим невідповідностям та шахрайству.

6. Виявлення та запобігання діям внутрішніх загроз, таких як зловживання привілеями, фінансові махінації або корупція.

7. Розробка планів дій для відповіді на фінансові кризи та втрати, а також відновлення фінансової стійкості підприємства.

Економічна безпека є критично важливою для довгострокового успіху та виживання приватного підприємства. Вона допомагає забезпечити фінансову стійкість, довіру стейкхолдерів та зберегти репутацію організації, що є важливими елементами ділового успіху в сучасному світі [69].

Контроль зовнішнього доступу є одним із найважливих елементів системи ІБ приватного підприємства і спрямований на забезпечення безпеки об'єктів, приміщень та фізичної інфраструктури організації. Цей аспект ІБ включає в себе ряд заходів і технологій для захисту від несанкціонованого доступу фізичних осіб до критичних об'єктів та ресурсів [70].

Основні аспекти контролю фізичного зовнішнього доступу включають такі елементи [71, 72]:

1. Визначення і підтвердження ідентичності осіб, які намагаються отримати фізичний доступ до приміщень чи об'єктів. Це може включати в себе використання ID-карток, біометричних методів, пін-кодів тощо.

2. Надання особам певних прав доступу до конкретних об'єктів. Наприклад, обмеження доступу до облікових записів, ресурсів чи зон на підприємстві.

3. Встановлення бар'єрів, таких як двері з електронними замками, обладнання контрольованими точками доступу та системами відеоспостереження.

4. Ведення журналів та моніторинг подій щодо фізичного доступу для виявлення аномалій, спроб несанкціонованого доступу чи інцидентів.

5. Заходи для запобігання крадіжці або втраті фізичних засобів, таких як комп'ютери, сервери, інша техніка і обладнання.

6. Використання сучасних технологій для автоматизації процесів фізичного контролю доступу та їх інтеграція з загальною системою безпеки.

7. Розробка планів дій для реагування на кризові ситуації, такі як пожежі, надзвичайні події або інші загрози фізичній безпеці.

8. Проведення навчання та надання рекомендацій персоналу з питань фізичної безпеки та правил поведінки.

Контроль фізичного зовнішнього доступу є важливим елементом для запобігання несанкціонованого доступу до важливих об'єктів та ресурсів підприємства. Він допомагає захистити активи та забезпечити безпеку приміщень та об'єктів, що є критичними для нормального функціонування організації [73].

Внутрішній безпековий моніторинг є одним з головних елементів системи ІБ приватного підприємства і спрямований на забезпечення безпеки внутрішніх приміщень, об'єктів та ресурсів організації. Цей елемент системи ІБ включає в себе різні технології та системи, такі як системи відеоспостереження, системи контролю доступу, системи виявлення злому та інші автоматизовані засоби безпеки [74].

Важливі аспекти внутрішнього безпекового моніторингу включають [75, 76]:

1. Встановлення камер в приміщеннях та на території підприємства для стеження за діяльністю та забезпечення безпеки. Системи відеоспостереження дозволяють реагувати на незвичайні або підозрілі події, виявляти несанкціонований доступ та фіксувати інциденти.

2. Застосування систем, які регулюють доступ співробітників та відвідувачів до об'єктів та приміщень підприємства. Це може включати в себе використання магнітних карток, біометричних систем, кодових замків тощо.

3. Встановлення датчиків та систем виявлення, які сповіщають про спроби незаконного вторгнення, вибухів або інших аварійних ситуацій.

4. Системи, які слідкують за параметрами навколишнього середовища, такі як дим, вогонь, гази, температура, вологість та інші, і виявляють потенційні загрози для безпеки.

5. Засоби для запису аудіо- та відеоматеріалів, що можуть бути використані як докази або засоби ідентифікації осіб у разі інциденту.

6. Автоматизовані системи аналізу та реакції на події, які дозволяють оперативно реагувати на виявлені загрози або незвичайні ситуації.

Внутрішній безпековий моніторинг спрямований на попередження і виявлення потенційних загроз для безпеки підприємства, а також на забезпечення швидкого реагування в разі виникнення інцидентів. Цей елемент системи ІБ

допомагає підприємствам захищати свої активи, дотримуватися стандартів безпеки та забезпечувати стабільність бізнес-процесів [77].

Контроль внутрішнього доступу є значущою складовою системи ІБ приватного підприємства і спрямований на забезпечення захисту конфіденційної інформації та ресурсів від несанкціонованого доступу зсередини організації. Цей елемент ІБ передбачає диференціацію доступу працівникам на основі рівня їх акредитації та вживання заходів для запобігання промисловому шпигунству та прихованої співпраці з третіми особами [78].

Основні аспекти контролю внутрішнього доступу включають такі елементи [79, 80]:

1. Визначення і підтвердження ідентичності користувачів та надання їм відповідних прав доступу до інформаційних ресурсів. Це включає в себе використання паролів, біометричних методів або інших методів аутентифікації.

2. Надання різних рівнів доступу різним категоріям працівників відповідно до їх ролей та обов'язків. Це допомагає обмежити доступ до конфіденційної інформації лише тим, кому він дійсно необхідний для виконання роботи.

3. Ведення журналів та моніторинг дій користувачів для виявлення незвичайних або підозрілих активностей.

4. Заходи для запобігання витоку конфіденційної інформації, включаючи контроль використання зовнішніх носіїв даних та захист від пристроїв, які можуть передавати дані незаконно.

5. Проведення навчання та надання рекомендацій персоналу з питань безпеки, виявлення загроз і знешкодження їх.

6. Розробка стратегій та політики з питань захисту конфіденційної інформації від промислового шпигунства та попередження витоку важливих даних.

7. Запобігання прихованої співпраці з третіми особами або конкурентами, що може становити загрозу для безпеки компанії.

8. Заходи для фізичного захисту об'єктів, серверних кімнат і інфраструктури.

Контроль внутрішнього доступу є важливим елементом забезпечення безпеки на рівні приватного підприємства, оскільки він спрямований на запобігання внутрішнім загрозам та забезпечення безпеки конфіденційної інформації та ресурсів. Ця стратегія ІБ допомагає попередити ідентифікацію, експлуатацію та використання внутрішніми суб'єктами можливих вразливостей та слабких місць в системі [81].

Навчання персоналу є ключовим елементом системи ІБ приватного підприємства і відіграє важливу роль у забезпеченні всіх аспектів безпеки організації. Цей процес має на меті підготовку та інструктування персоналу щодо правил, процедур і норм, які стосуються безпеки, а також надання їм необхідних знань та навичок для ефективної реакції на інциденти та загрози ІБ [82].

Основні аспекти навчання персоналу в рамках системи ІБ приватного підприємства включають такі елементи [83, 84]:

1. Персонал повинен бути свідомий про загрози та ризики, пов'язані з інформаційною безпекою, і розуміти, як їх виявляти і запобігати.

2. Персонал повинен бути навченим, як визначати та захищати себе від кіберзагроз, таких як фішинг, віруси, шкідливі програми тощо.

3. Навчання персоналу щодо правил та процедур, які регулюють безпеку організації, включаючи доступ до інформації, паролі, зберігання даних, реагування на інциденти.

4. Створення серед співробітників обізнаність про важливість безпеки та відповідальності за її збереження.

5. Навчання персоналу, як розпізнавати та відповідати на інциденти безпеки, включаючи втрату даних, виток інформації, крадіжку обладнання тощо.

6. Проведення тестувань та симуляцій інцидентів для перевірки готовності персоналу до дій в реальних умовах.

7. Інформаційна безпека постійно змінюється, тому навчання та оновлення знань повинні бути постійним процесом.

8. Залучення персоналу до активного виявлення та повідомлення можливих загроз і вразливостей в системі ІБ.

Навчання персоналу в сфері ІБ допомагає створити обізнану та відповідальну робочу силу, яка може бути першою лінією оборони проти різних загроз та інцидентів. Воно сприяє забезпеченню безпеки і захисту конфіденційної інформації та ресурсів приватного підприємства на всіх рівнях організації [85].

Аналіз ризиків є необхідним елементом системи ІБ приватного підприємства. Цей процес спрямований на ідентифікацію, оцінку, прийняття та контроль ризиків, які можуть впливати на безпеку та стабільність організації. Аналіз ризиків допомагає приватним підприємствам визначити потенційні загрози та вразливості, розробити стратегії їх управління і прийняти обґрунтовані рішення для захисту інформації та ресурсів [86].

Важливі аспекти аналізу ризиків включають [87, 88]:

1. Спроба визначити всі потенційні загрози, які можуть впливати на інформаційну безпеку підприємства. Це можуть бути технічні загрози (віруси, хакерські атаки), організаційні ризики (недостатня політика безпеки, недостатнє навчання персоналу) і природні ризики (пожежі, природні катастрофи).

2. Аналіз і оцінка потенційного впливу ризиків на організацію. Це включає в себе визначення ймовірності виникнення ризику та впливу цього ризику на бізнес-процеси та активи підприємства.

3. Визначення та вибір стратегій управління ризиками. Це може включати в себе ухвалення заходів для зменшення ризику, перенесення ризику на страхову компанію або прийняття ризику на свій рахунок.

4. Розробка та впровадження політик, процедур та технічних засобів для захисту від ідентифікованих ризиків. Це може включати в себе застосування захисту даних, контроль доступу, резервне копіювання і багато інших заходів.

5. Спостереження за станом безпеки, виявлення незвичайних або підозрілих дій та проведення аудитів для перевірки дотримання політик і процедур безпеки.

6. У випадку зміни умов або виникнення нових ризиків, перегляд і коригування стратегій управління ризиками.

Аналіз ризиків допомагає приватним підприємствам вибрати оптимальний баланс між захистом і доступністю інформації та ресурсів. Він дозволяє підприємствам приймати обґрунтовані рішення щодо інвестицій в інформаційну безпеку та забезпечує довгострокову стійкість та стабільність бізнес-процесів організації [89].

Таким чином, система ІБ приватного підприємства є надзвичайно важливим компонентом сучасного бізнесу, оскільки вона спрямована на забезпечення конфіденційності, цілісності та доступності інформації та ресурсів організації. Враховуючи різноманітні загрози та виклики, з якими стикаються приватні підприємства в сучасному цифровому середовищі, система ІБ має включати в себе широкий спектр аспектів та інструментів для забезпечення комплексного захисту.

Перш за все, загальна концепція системи ІБ приватного підприємства передбачає розуміння та ідентифікацію загроз, важливих активів і слабких місць організації. Для цього використовуються різні методи, включаючи аналіз ризиків, інвентаризацію активів та аудит безпеки.

Основними аспектами системи ІБ приватного підприємства є заходи та політики, спрямовані на захист комп'ютерних систем та даних від кіберзагроз, включаючи хакерські атаки, віруси та інші кіберзлочини; застосування систем контролю доступу, включаючи фізичний та логічний доступ до ресурсів, а також управління правами співробітників; проведення навчальних заходів та тренінгів для персоналу щодо правил та процедур інформаційної безпеки; системи відеоспостереження, системи аналізу подій та інші інструменти для виявлення та аналізу можливих загроз; заходи для захисту приміщень та об'єктів від фізичних загроз, таких як вторгнення або крадіжки; заходи, спрямовані на захист фінансових ресурсів і майна підприємства; моніторинг та управління репутаційним статусом підприємства для запобігання негативним впливам на бренд та репутацію.

Ці аспекти взаємопов'язані і вимагають системного підходу до планування та впровадження системи ІБ. Правильно розроблена та інтегрована система ІБ допомагає підприємству попереджати інциденти, зменшувати ризики та забезпечувати стабільність бізнес-процесів. Важливо також пам'ятати, що система

ІБ має бути постійно оновлюваною та адаптованою до нових загроз та технологій, щоб забезпечити ефективний захист впродовж часу.

У ході аналізу системи ІБ приватного підприємства, було виявлено, що одним із ключових аспектів є забезпечення контролю доступу до об'єктів та ресурсів організації. У цьому контексті системи безконтактної ідентифікації на базі технології RFID (Radio-Frequency Identification) представляють собою потенційно ефективний інструмент для забезпечення ІБ.

RFID-технологія дозволяє ідентифікувати об'єкти та особи без контакту, що робить її відмінною альтернативою традиційним системам контролю доступу. Вона може бути використана для контролю доступу до приміщень, моніторингу руху об'єктів, відстеження активів та багатьох інших застосувань, які сприяють забезпеченню ІБ.

Враховуючи наукову новизну та практичну цінність результатів дослідження систем безконтактної ідентифікації на основі RFID, можна визначити, що вони мають потенціал стати важливим інструментом для підвищення рівня ІБ приватного підприємства.

Отже, фокус дослідження спрямований на вивчення, розробку та впровадження систем контролю доступу на базі технології RFID з метою забезпечення інформаційної безпеки приватного підприємства. Дослідження передбачає аналіз різних аспектів використання цієї технології, оцінку її надійності та стійкості до злому, а також врахування економічних аспектів розгортання.

2.2 Роль безконтактної ідентифікації в забезпеченні інформаційної безпеки приватного підприємства

Безконтактна ідентифікація у вигляді системи (на базі методу у вигляді технології RFID) в контексті забезпечення інформаційної безпеки (ІБ) приватного підприємства є комплексом технологічних рішень і апаратних засобів, спрямованих на ідентифікацію та автентифікацію фізичних осіб, об'єктів або ресурсів без необхідності фізичного контакту. Головною метою такої системи є

забезпечення контролю доступу, моніторингу та захисту об'єктів, інформації та активів приватного підприємства від несанкціонованого доступу, крадіжок, а також забезпечення загальної інформаційної безпеки організації [90].

Метод безконтактної ідентифікації базується на використанні RFID-міток (мікрочіпів), які вбудовуються у картки, браслети, етикетки або інші носії, а також RFID-зчитувачів, які зчитують інформацію з цих міток. При взаємодії зчитувача та мітки, система відповідає на запити, ідентифікувати об'єкти чи осіб, та приймати рішення щодо надання чи обмеження доступу на основі передбачених правил і політик безпеки [91].

Основні функції системи безконтактної ідентифікації в контексті ІБ приватного підприємства включають [92, 93]:

1. Система контролю доступу RFID визначає, хто має доступ до певних об'єктів чи приміщень на підприємстві, і надає чи обмежує цей доступ відповідно до правил і політик безпеки.

2. RFID допомагає відстежувати переміщення об'єктів, товарів або інвентарю, а також моніторити рух співробітників на території підприємства.

3. Система контролю доступу RFID забезпечує захист цінних об'єктів, інформації та ресурсів від крадіжок, несанкціонованого доступу та втрат.

4. Впровадження RFID дозволяє підприємству оптимізувати процеси контролю доступу, інвентаризації та моніторингу, знижуючи адміністративні витрати та ризик людських помилок.

Усі ці функції спільно спрямовані на підвищення рівня інформаційної безпеки приватного підприємства, забезпечуючи контроль і захист важливих ресурсів та активів організації.

RFID-система контролю доступу у складі системи ІБ ПП виконує функції з диференціювання рівнів доступу до певних об’єктів ПП (рис. 5), що характеризується системою блокування регульованих бар’єрів (дверей, турнікетів, воріт та ін.) (рис. 6) та інтегрується в загальну систему контролю та управління доступом (СКУД) ПП (рис. 7) [94, 95].

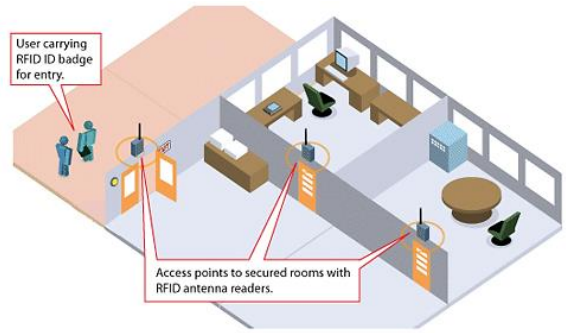


Рисунок 5 – Візуалізація функції RFID-системи контролю доступу диференціювання рівня доступу до об’єктів ПП

Рисунок 6 – Візуалізація базової функції RFID-системи контролю доступу з блокування/деблокування бар’єрів доступу

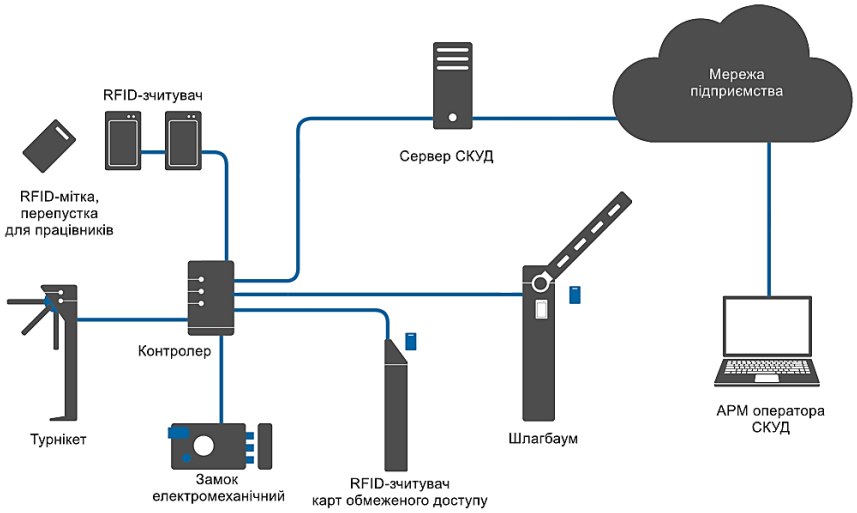


Рисунок 7 – Узагальнена концепція СКУД ПП, до якої інтегрована RFID-система контролю доступу

Наведені рішення RFID-системи контролю доступу, що виконують безпосереднє автоматизоване керування регульованих бар’єрів у складі СКУД ПП, забезпечують ІБ, виконуючи відповідні функції, як офісних (рис. 8), так і для виробничих (рис. 9) відділів ПП [96, 97].

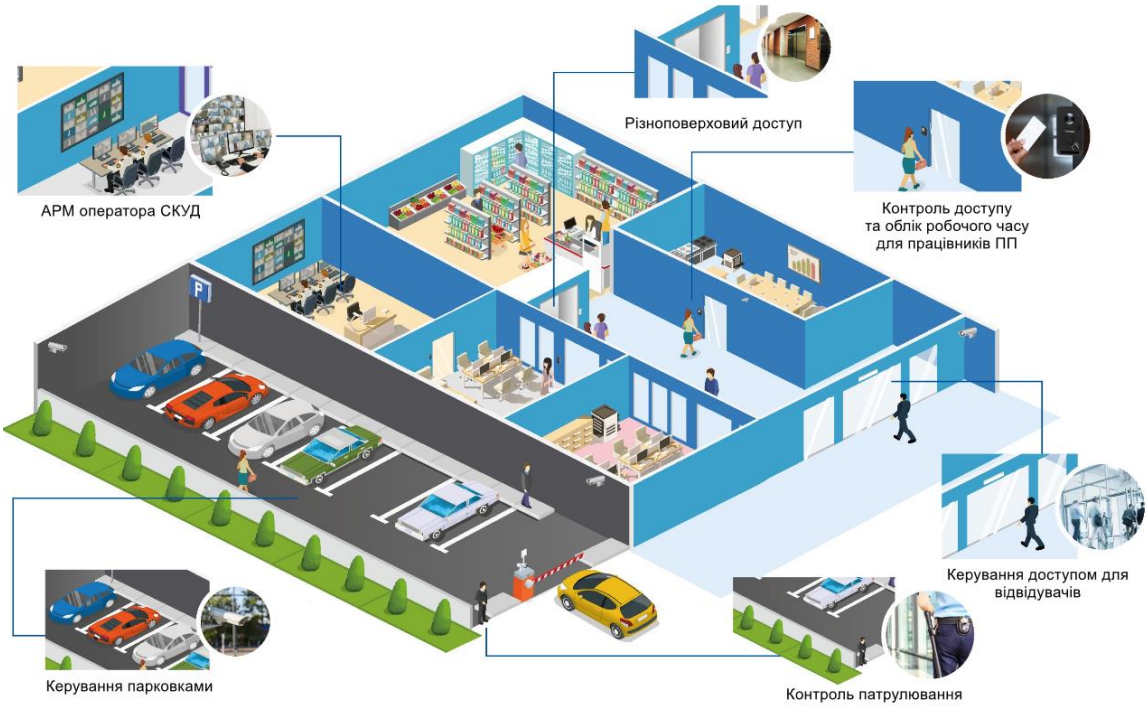


Рисунок 8 – Візуалізація функціонування СКУД з RFID для офісних відділів ПП

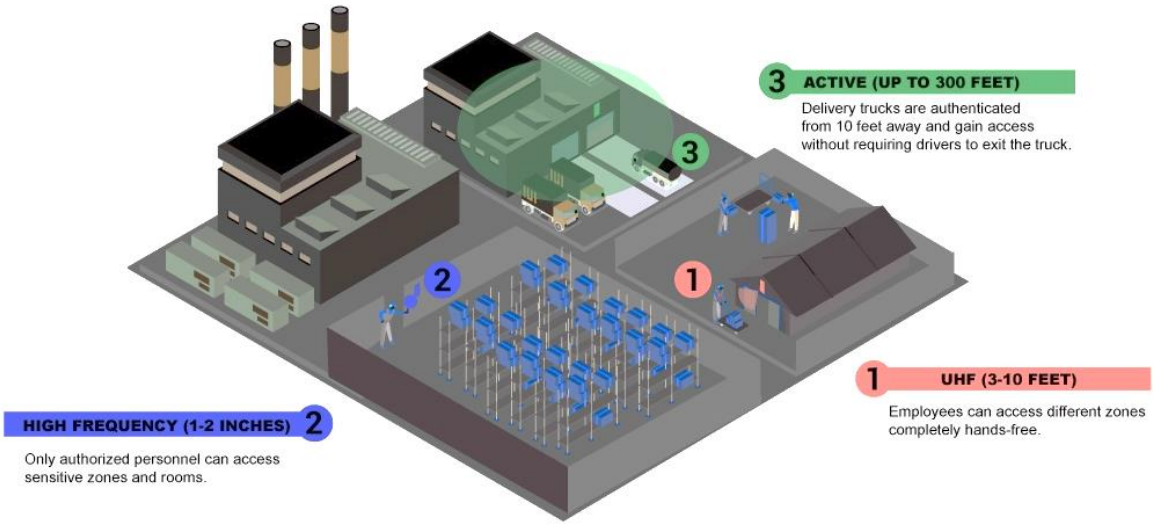


Рисунок 9 – Візуалізація функціонування СКУД з RFID для виробничих відділів ПП

Таким чином СКУД на базі технології RFID в складі ПП представляє собою інтегровану систему, спроектовану для контролю, моніторингу та обмеження фізичного доступу співробітників та відвідувачів на територію підприємства з метою забезпечення інформаційної безпеки та фізичної безпеки об'єктів підприємства. Ця система складається з ряду ключових компонентів [98, 99]:

1. RFID-мітки – бездротові електронні пристрої містять інформацію, яка ідентифікує конкретну особу або об'єкт. Кожен співробітник або відвідувач, якому надано доступ до підприємства, має особисту RFID-мітку, яка містить унікальний ідентифікатор.

2. RFID-зчитувачі – пристрої встановлюються на всіх точках входу та виходу на території підприємства. Вони зчитують інформацію з RFID-міток, які носять співробітники або відвідувачі, і передають цю інформацію до системи обробки даних.

3. Система обробки даних – централізована система включає в себе базу даних, програмне забезпечення управління та моніторингу. Вона здійснює ідентифікацію осіб, аутентифікацію та прийняття рішень щодо надання або обмеження доступу на основі інформації з RFID-міток та встановлених правил безпеки.

4. Контрольні точки доступу – точки розташовані на всіх важливих входах та об'єктах підприємства. Вони взаємодіють з RFID-зчитувачами та перевіряють доступ осіб на підприємство.

5. Програмне забезпечення управління і моніторингу – система адміністрування ПП, яка використовує спеціальне програмне забезпечення для налаштування правил доступу, моніторингу подій і аналізу даних.

6. Журнал і аналіз даних – система, що фіксує всі події, пов'язані з контролем доступу, і зберігає їх у вигляді журналів. Ці дані використовуються для аналізу активності, аудиту та виявлення потенційних загроз безпеці.

Завдяки інтеграції цих компонентів, система контролю доступу на базі технології RFID допомагає приватному підприємству забезпечити інформаційну

безпеку, ефективно контролювати доступ до ресурсів та об'єктів, а також веде детальний облік подій для подальшого аналізу та виявлення можливих ризиків.

За результатами аналізу вищенаведених матеріалів констатуємо, що RFID-системи доступу відіграють надзвичайно важливу роль в забезпеченні ІБ ПП. Аналізуючи їхню роль, можна зробити наступні висновки:

1. RFID-системи дозволяють ефективно контролювати та моніторити фізичний доступ співробітників та відвідувачів на територію підприємства. Це важливо для забезпечення безпеки об'єктів та ресурсів.

2. RFID-технологія дозволяє точно ідентифікувати осіб за допомогою унікальних RFID-міток або карток. Це робить процес контролю доступу надійним та точним.

3. Система запису та аналізу подій дозволяє вести детальний облік всіх дій, пов'язаних з контролем доступу. Це важливо для виявлення аномальної активності та реагування на можливі загрози.

4. Збір та аналіз даних з RFID-системи дозволяє виявити можливі ризики безпеки, включаючи спроби несанкціонованого доступу чи невідому активність на території ПП.

5. RFID-системи можуть бути інтегровані з іншими системами безпеки, такими як системи відеоспостереження, системи моніторингу відомостей і системи контролю доступу до мережі. Це підвищує загальний рівень безпеки на ПП.

6. Контроль доступу за допомогою RFID-систем допомагає зменшити ризик втрати конфіденційної інформації та ресурсів, таким чином сприяючи інформаційній безпеці.

7. RFID-системи дозволяють співробітникам та відвідувачам швидко та зручно пройти процедуру контролю доступу, що сприяє підвищенню продуктивності та зручності роботи.

8. Використання RFID-систем дозволяє автоматизувати багато процесів, пов'язаних з контролем доступу, включаючи відкриття дверей, реєстрацію прибуття та виходу, а також внутрішню систему обліку.

9. RFID-системи дозволяють налаштовувати рівні доступу для різних груп співробітників та відвідувачів, що забезпечує диференціацію доступу та підвищує безпеку.

10. Збір та аналіз даних з RFID-системи дозволяє оптимізувати використання ресурсів, наприклад, простору офісу, робочого часу та інших ресурсів.

Таким чином встановлено, що RFID-системи доступу є невід'ємною складовою інфраструктури інформаційної безпеки приватного підприємства. Вони забезпечують високий рівень контролю, зручність та продуктивність роботи, моніторингу та безпеки фізичного доступу, можливість аналізу та виявлення потенційних загроз, що є критичним для збереження конфіденційності та цілісності даних, а також захисту від можливих загроз.

Враховуючи всі ці переваги, є ґрунтовним висновок про те, що RFID-системи доступу є важливим і необхідним компонентом системи інформаційної безпеки приватного підприємства.

2.3 Огляд типових рішень з улаштування безконтактної ідентифікації для забезпечення інформаційної безпеки приватних підприємств

Безконтактні ідентифікації RFID, у вигляді системи, відіграють важливу роль у забезпеченні інформаційної безпеки ПП. RFID є складовою системи контролю доступу СКУД для ПП. Система контролю доступу на основі RFID використовує радіочастотну ідентифікацію для ідентифікації осіб або об'єктів і керування їх доступом до певних зон або приміщень на території підприємства. Існують різні типові рішення та підходи до улаштування таких систем, які враховують потреби та специфіку конкретного ПП [100]. Розглянемо типову схему улаштування СКУД з RFID, функціональні елементи якої облаштовуються на прохідній ПП (рис. 10).

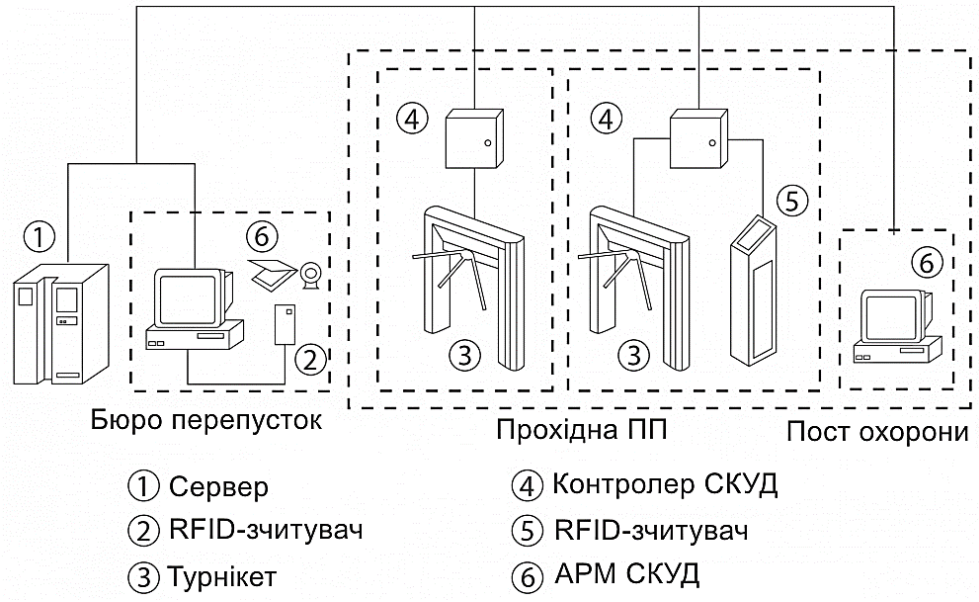


Рисунок 10 – Типове рішення з улаштуванням RFID-СКУД ПП

RFID-зчитувачі розміщені біля турнікетів і взаємодіють з RFID-мітками або картками, які користувачі пред'являють при вході або виході. Ці мітки містять індивідуальний ідентифікатор, який визначає працівника. Турнікети діють як фізичні бар'єри, контролюючи доступ і відкриваючись лише при правильному використанні дійсної RFID-мітки або картки.

Бюро перепусток відповідає за видання RFID-міток або карток співробітникам та відвідувачам. Тут також може проводитися реєстрація і відслідковування входів та виходів користувачів [101].

Ця система дозволяє підприємству ефективно контролювати фізичний доступ до об'єктів та зменшує ризик несанкціонованого вторгнення. Вона сприяє загальній безпеці приміщень і допомагає вести точний облік руху осіб на території підприємства. Крім того, система легко інтегрується з іншими системами безпеки, такими як системи відеоспостереження, що підвищує загальний рівень безпеки.

Усі дані про користувачів, ролі, правила доступу та події зберігаються в базі даних системи, що робить можливим ведення журналів доступу та аналіз подій. Така система є невід'ємною частиною інформаційної безпеки приватного підприємства та сприяє забезпеченню захисту активів, ресурсів та конфіденційності даних.

Інтеграція RFID з системою відеоспостереження дозволяє відслідковувати рух осіб та події в режимі реального часу. Камери відеоспостереження фіксують відеозаписи, які можуть бути використані для перевірки і підтвердження подій, пов'язаних зі входом і виходом осіб [102]. Це забезпечує додатковий рівень безпеки та контролю (рис. 11).

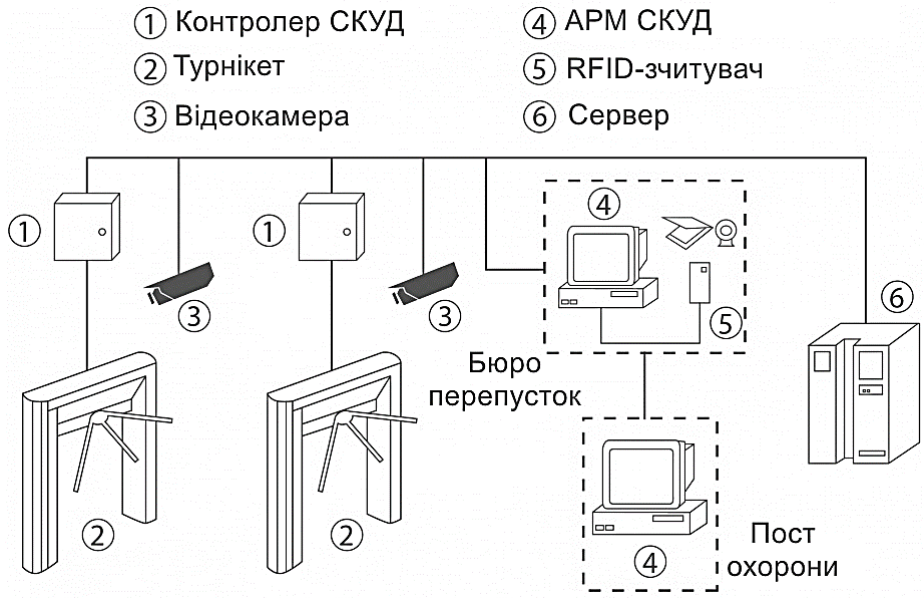


Рисунок 11 – Інтеграція RFID у СКУД з системою відеоспостереження

Крім того, аналітичні можливості інтегрованої системи дозволяють виявляти аномальні події та навіть автоматично спрацьовувати тривожні сигнали в разі несанкціонованого доступу або інших загроз. Оператори відеоспостереження можуть в реальному часі реагувати на події та при необхідності вживати заходів для забезпечення безпеки.

Усі дані про доступ та події зберігаються в базі даних, що дозволяє вести журнали доступу, створювати звіти та аналізувати події для подальшого контролю та аудиту. Ця інтегрована система забезпечує підприємство комплексним інструментом для контролю та забезпечення безпеки на своїй території, що є важливим аспектом інформаційної безпеки [103].

RFID відіграє важливу роль у автоматизації системи контролю доступу СКУД на ПП. Вона надає ефективність та зручність у процесах ідентифікації та моніторингу, що допомагає оптимізувати роботу системи СКУД та забезпечити високий рівень безпеки. Однією з ключових переваг RFID є швидкість ідентифікації. RFID-мітки або картки можуть бути швидко зчитані без контакту під час проходження через точки доступу. Це дозволяє працівникам та відвідувачам швидко та зручно входити і виходити з об'єкту, не втрачаючи часу на довгі перевірки (рис. 12).

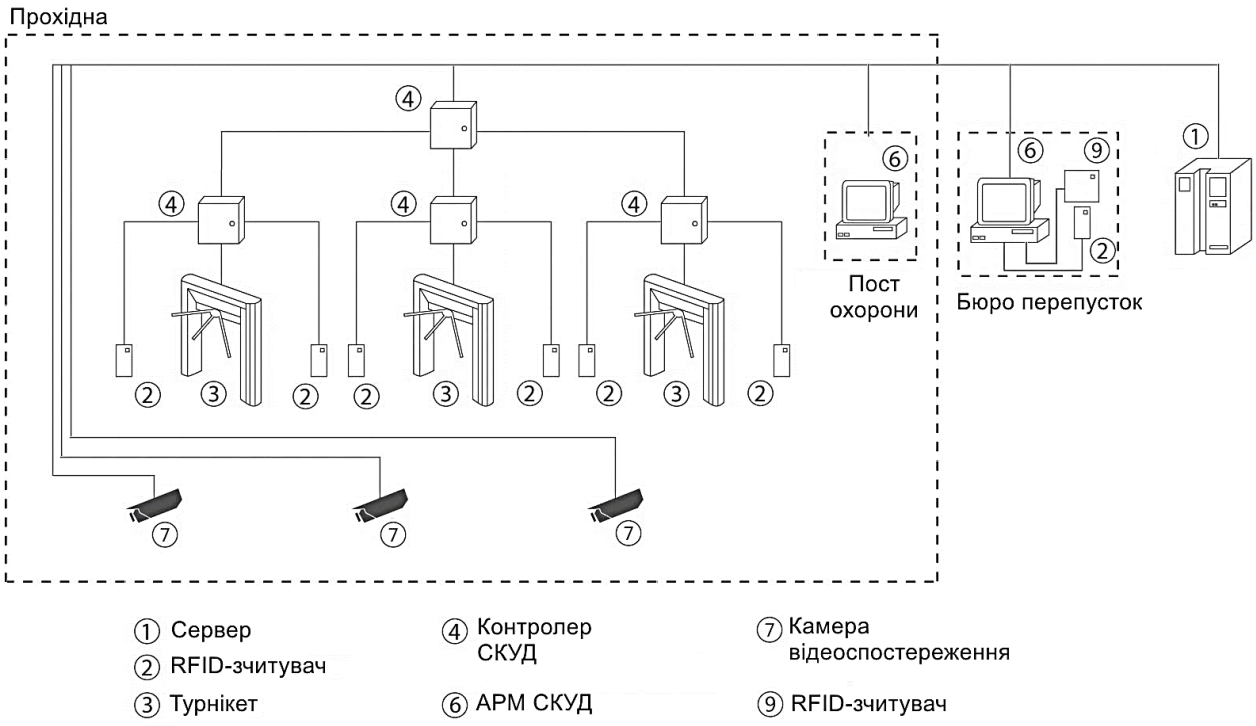


Рисунок 12 – Автоматизація СКУД ПП за допомогою RFID

RFID дозволяє легко оновлювати та керувати базою даних ідентифікаторів, що значно спрощує адміністрування системи СКУД. Інформація про працівників і відвідувачів може бути легко додана або видалена з бази даних, а також редагуватися, що робить процес управління доступом більш гнучким та швидким.

RFID може бути інтегрованим з іншими системами безпеки СКУД, такими як системи відеоспостереження та системи виявлення інцидентів. Ця інтеграція

дозволяє створити цілісну систему безпеки, яка може автоматично реагувати на події та сповіщати операторів про потенційні загрози [104].

RFID-система контролю доступу до офісних приміщень приватного підприємства (ПП) представляє собою інтегровану систему, яка базується на технології Radio-Frequency Identification для забезпечення безпеки та контролю над доступом осіб в офісні приміщення (рис. 13).

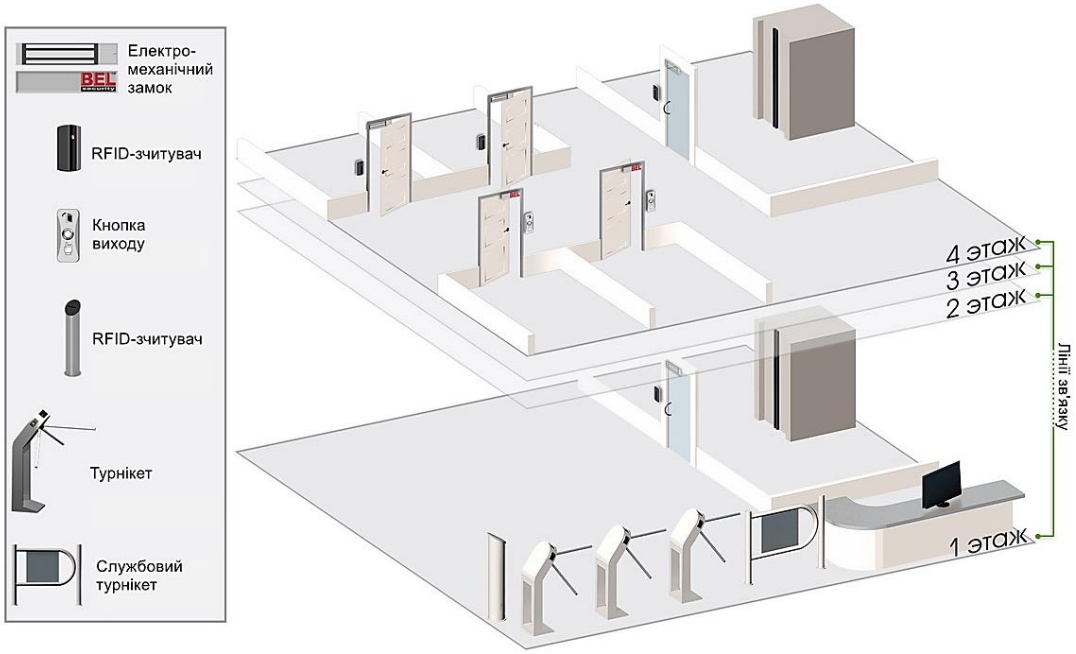


Рисунок 13 – RFID-СКУД в офісних приміщеннях ПП

RFID-система контролю доступу до офісних приміщень функціонує за наступним логічним алгоритмом:

1. При вході особа наближає свою RFID-мітку або картку до читача.
2. Читач зчитує ідентифікатор з мітки або картки.
3. Системне програмне забезпечення перевіряє ідентифікатор та порівнює його з базою даних доступу.
4. Якщо ідентифікатор відповідає дозволеним правам доступу, система дозволяє вхід у приміщення. В іншому випадку доступ блокується.
5. Усі події, такі як вхід, вихід, спроби несанкціонованого доступу та інші, фіксуються в журналах для подальшого аналізу та аудиту.

RFID-система контролю доступу дозволяє підприємствам забезпечити безпеку своїх офісних приміщень, обмежити доступ до конкретних зон та відслідковувати рух осіб у приміщенні. Вона є ефективним інструментом для забезпечення інформаційної безпеки та контролю над фізичним доступом до важливих об'єктів ПП.

Узагальнюючи розглянуті типові рішення з улаштування RFID-СКУД сформуємо унітарний підхід до проєктування досліджуваної системи контролю доступу (рис. 14).

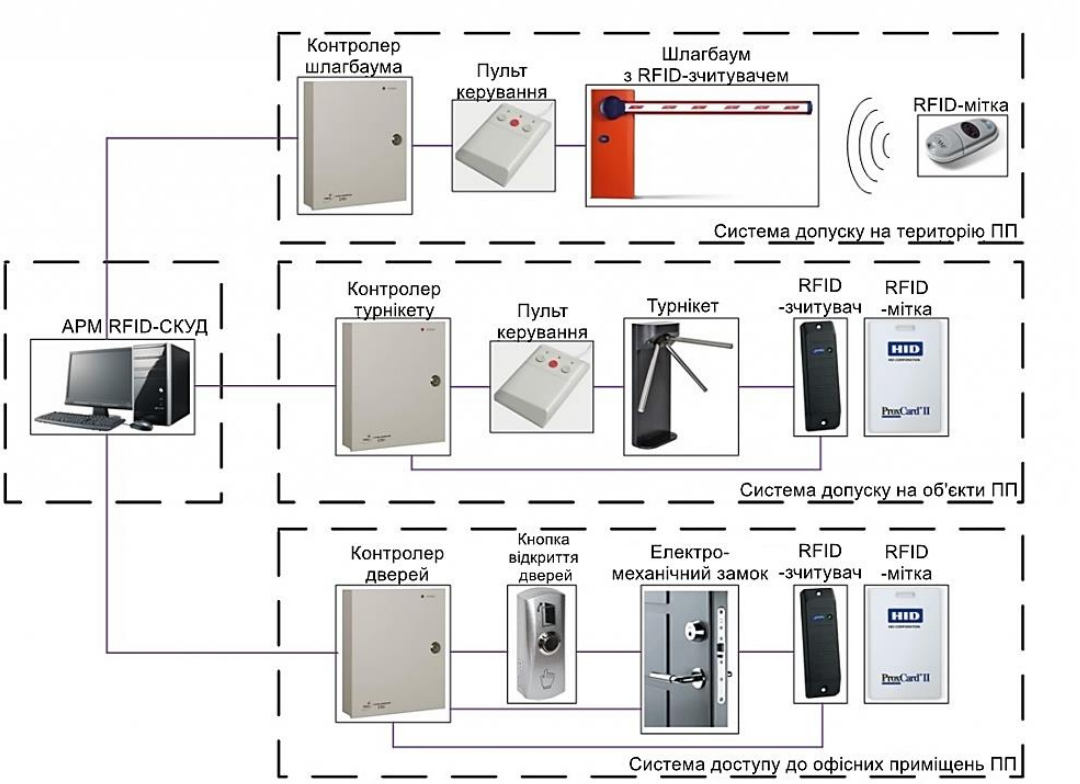


Рисунок 14 – Узагальнена принципова схема улаштування RFID-СКУД

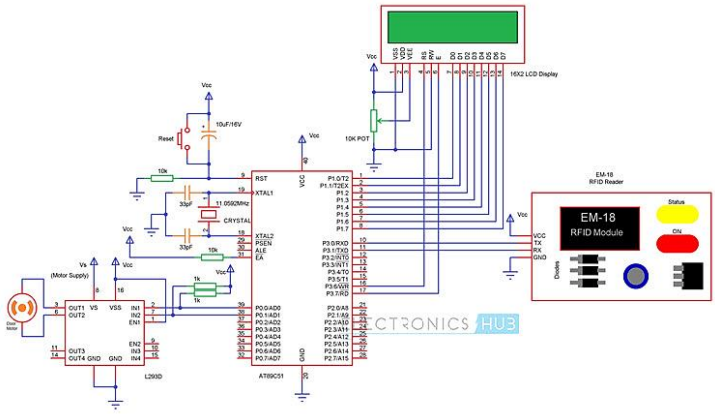
Наразі для улаштування виконавчих механізмів RFID-СКУД застосовують рішення на базі технології Arduino. Використання RFID-систем контролю доступу на базі контролерів Arduino є цікавим і доступним способом створення власної системи контролю доступу. Arduino – це платформа для розробки пристроїв, яка

включає мікроконтролери, розширювачі та програмне забезпечення для їх програмування [105].

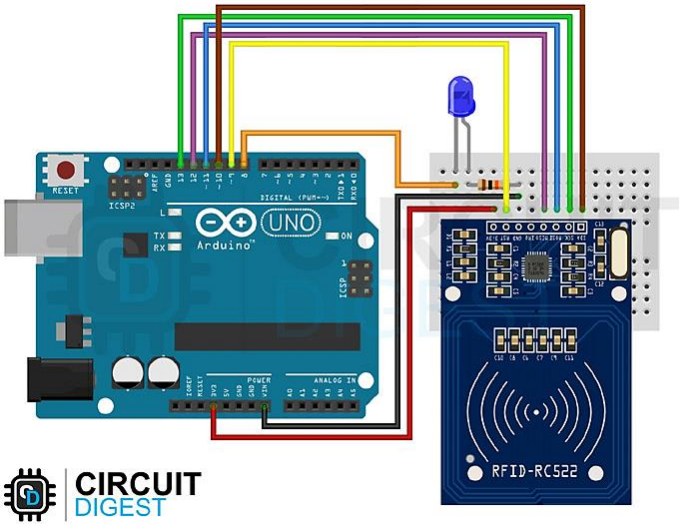
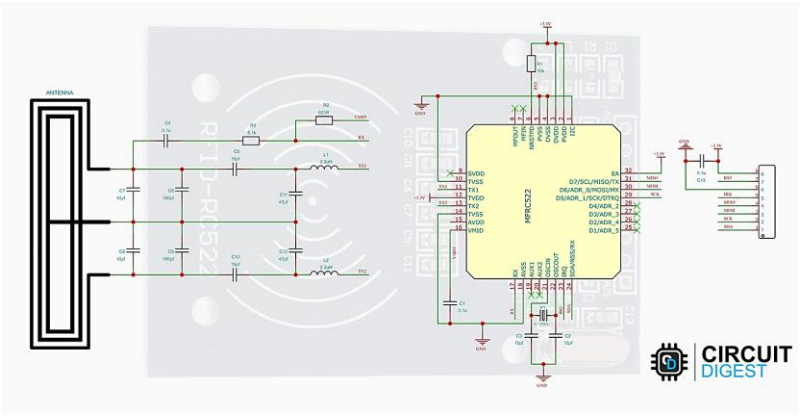
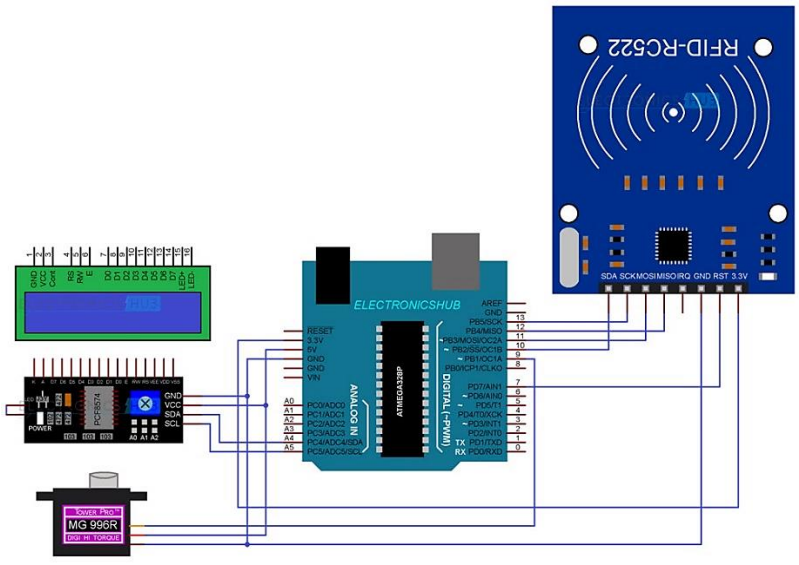
Використання Arduino для створення RFID-системи контролю доступу дозволяє реалізувати індивідуальні потреби підприємства та зменшити витрати на придбання готових систем. Однак важливо враховувати, що ця система може вимагати додаткового програмування та тестування для забезпечення надійності та безпеки [106, 107].

Розглянемо деякі типові рішення з улаштування RFID-системи контролю доступу на базі технології Arduino (табл. 4).

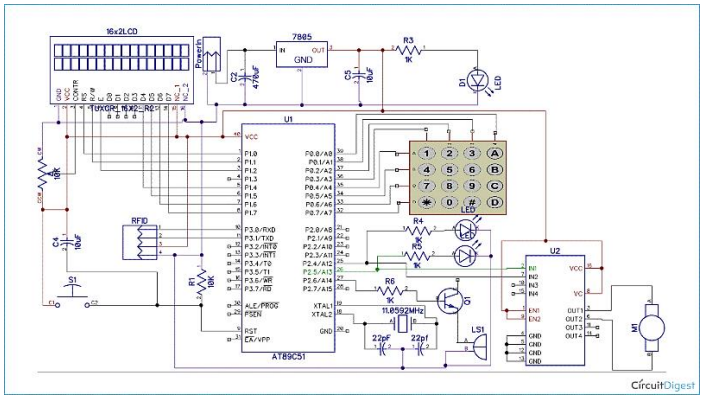
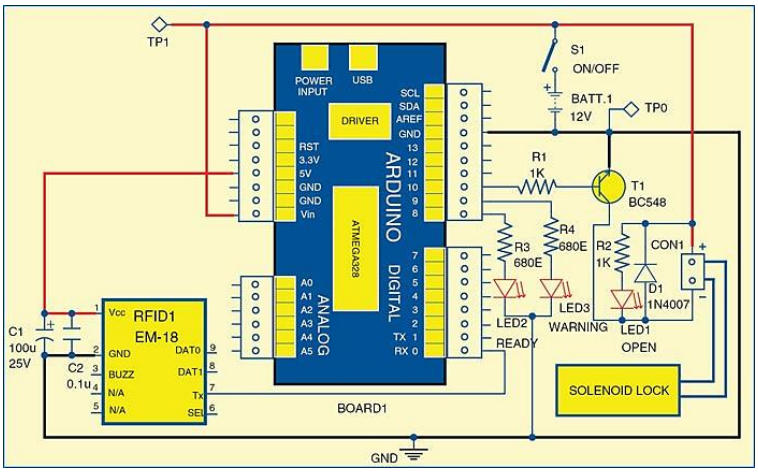
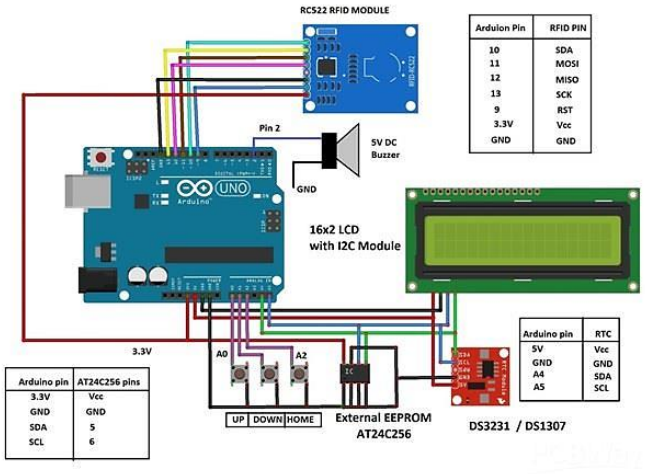
Таблиця 4 – Типові рішення з улаштування RFID-системи контролю доступу на базі технології Arduino

Схема	Тип мікроконтролеру	Посилання
1	2	3
	AT89C51	[108]

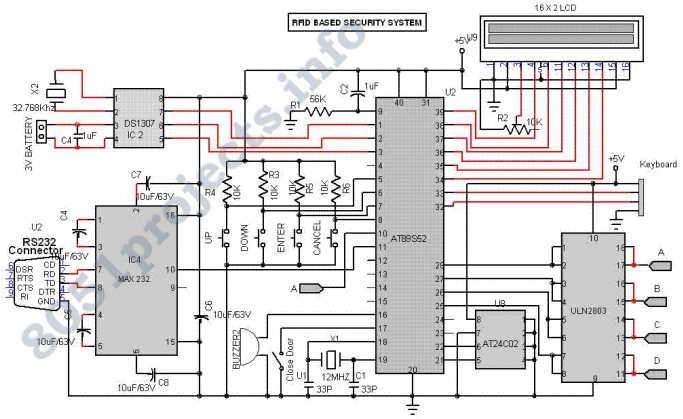
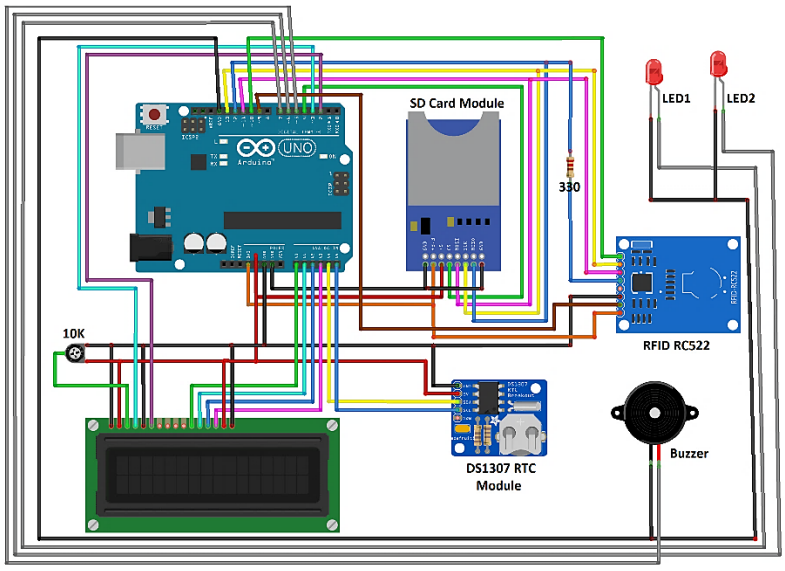
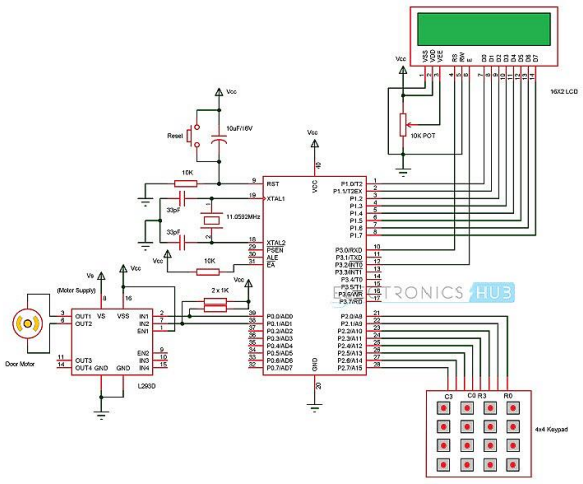
Продовження таблиці 4

1	2	3
 	RFID–RC522, Arduino UNO	[109]
	RFID–RC522, Arduino UNO	[110]

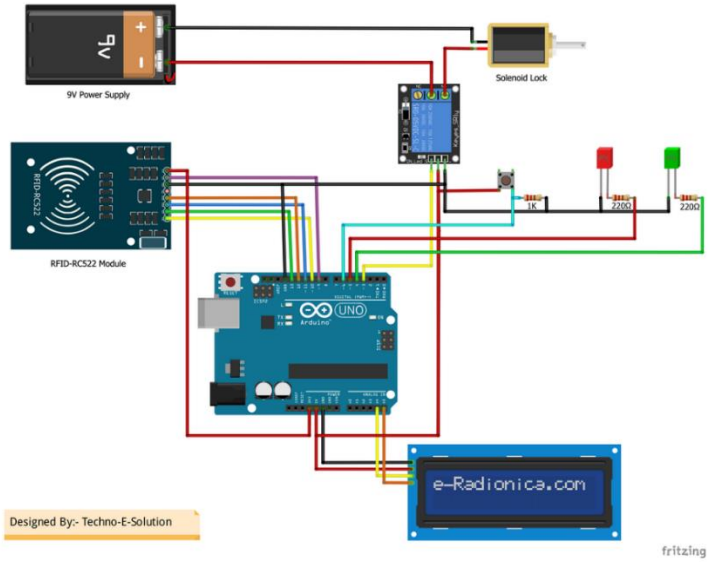
Продовження таблиці 4

1	2	3
	8051	[111]
	ATMEGA328	[112]
	RFID–RC522, Arduino UNO	[113]

Продовження таблиці 4

1	2	3
	AT89S52	[114]
	RFID–RC522, Arduino UNO	[115]
	8051	[116]

Кінець таблиці 4

1	2	3
	RFID–RC522, Arduino UNO	[117]

Відповідно до наведеного аналізу (табл. 4) більшість рішень з улаштування RFID-системи контролю доступу на базі технології Arduino базуються на використанні модулю RFID–RC522 та мікроконтролеру Arduino UNO, що відповідає результатам, наведених у релевантних наукових публікаціях [118 – 120].

Загалом, унітарна схема використання технології Arduino для RFID-системи контролю доступу формується з наступних логічних елементів [105] (рис. 15).

Використання RFID-систем контролю доступу на базі контролерів Arduino є цікавим і доступним способом створення власної системи контролю доступу. Arduino – це платформа для розробки пристроїв, яка включає мікроконтролери, розширювачі та програмне забезпечення для їх програмування. Застосування модуля RFID-RC522 з платформою Arduino в системах контролю доступу характеризується важливими перевагами. Ці переваги полягають у надійності та швидкості зчитування, сумісності зі стандартами RFID, простоті підключення та програмування, доступності за доступною ціною, компактних розмірах модуля, підтримці спільноти користувачів Arduino, а також можливості розширення функціональності. Застосування даного модуля дозволяє ефективно

впроваджувати системи контролю доступу, забезпечуючи безпеку та обмеження доступу до об'єктів інфраструктури.

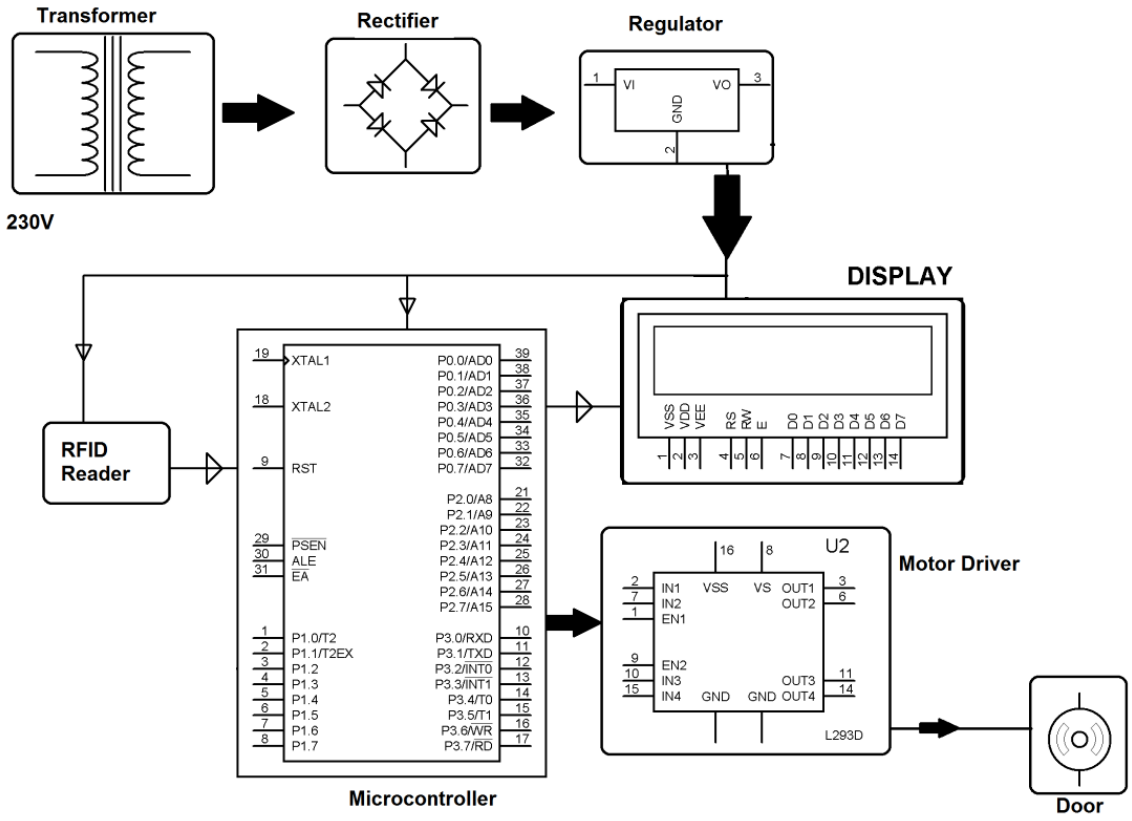


Рисунок 15 – Універсальна схема RFID-системи контролю доступу Arduino

Використання Arduino для створення RFID-системи контролю доступу дозволяє реалізувати індивідуальні потреби підприємства та зменшити витрати на придбання готових систем. Однак важливо враховувати, що ця система може вимагати додаткового програмування та тестування для забезпечення надійності та безпеки.

3 РЕАЛІЗАЦІЯ МЕТОДУ БЕЗКОНТАКТНОЇ ІДЕНТИФІКАЦІЇ НА ОСНОВІ RFID-ТЕХНОЛОГІЙ ДЛЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИВАТНОГО ПІДПРИЄМСТВА

3.1 Проєктна реалізація методу у вигляді системи RFID-ідентифікації

Проєктні рішення розробляються для приватного підприємства, що провадить свою економічну діяльність у сфері логістики. ПП представляє собою складський об’єкт з закритою територією, комбіновано облаштований на обмеженій ділянці в приміській агломерації.

Складський комплекс ПП логічно зонований та має доцільне розташування об’єктів з обмеженим доступом, для якого потрібне впровадження системи RFID-СКУД (рис. 16).

Система автоматизації складського комплексу передбачає комплекс з трьох складових, що реалізується за допомогою технології RFID: системи менеджменту складської діяльності (моніторинг та керування логістичним переміщенням товарів), системи контролю доступу (RFID-СКУД) та системи безпеки персоналу, що попереджає про небезпеку наближення транспортного засобу або складської техніки. В фокусі дослідження – система контролю доступу.

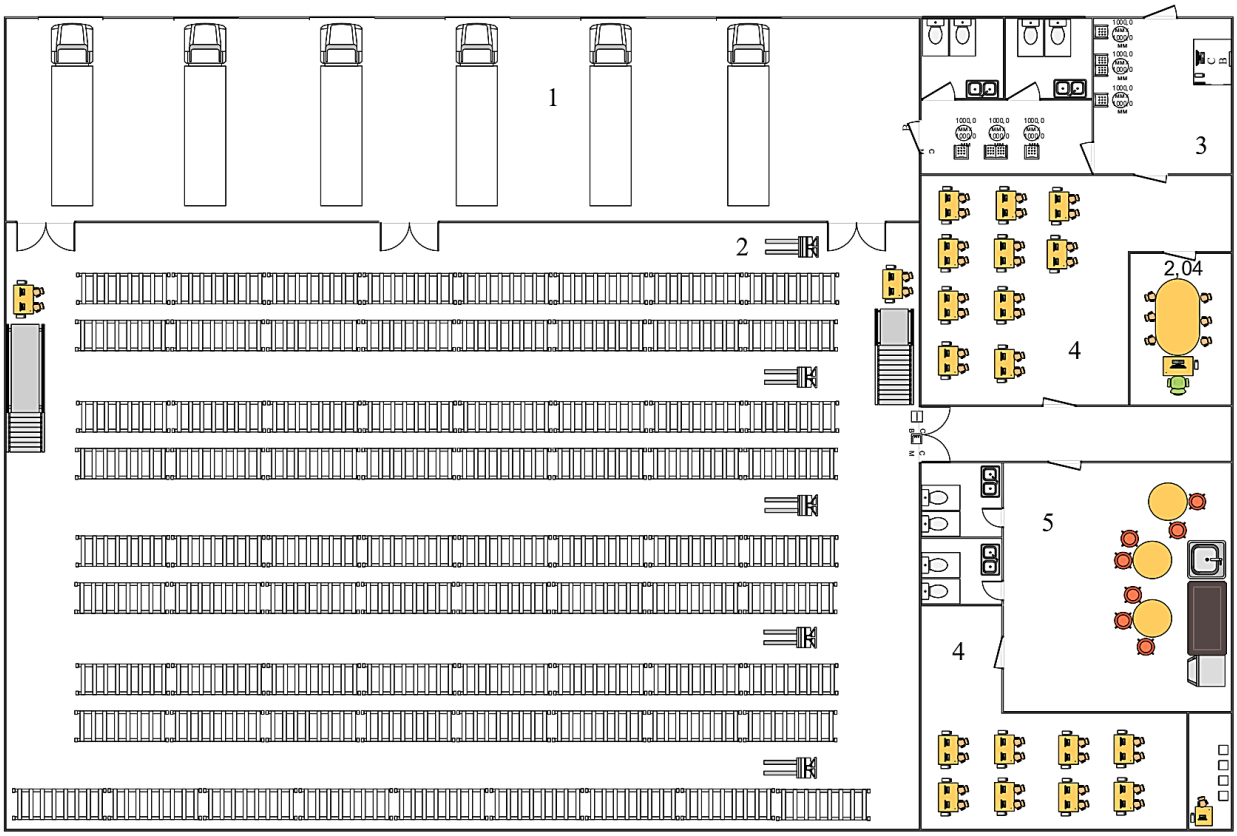
Проєктні рішення з улаштування RFID-СКУД необхідні для контролю доступу наступних об’єктів і зон складського комплексу ПП:

1. Приймально-відправне відділення: система безконтактної ідентифікації та авторизованого доступу до території складського комплексу вантажним автівкам ПП. Виконавчий механізм – портальні ворота з електромеханічним приводом.
2. Складське відділення: система безконтактної ідентифікації та авторизованого доступу складського персоналу ПП. Виконавчий механізм – турнікети.
3. Бізнес-зона та приміщення для водійського персоналу: система безконтактної ідентифікації та авторизованого доступу водійського персоналу та

ділових партнерів (за тимчасовими перепустками). Виконавчий механізм – турнікети та двері з електромеханічним замком.

4. Офіси та адміністрація: система безконтактної ідентифікації та авторизованого доступу менеджменту та керівництва ПП. Виконавчий механізм – турнікети та двері з електромеханічним замком.

5. Приміщення для складського персоналу: система безконтактної ідентифікації та авторизованого доступу складського персоналу ПП. Виконавчий механізм – турнікети.



1 – приймально-відправне відділення; 2 – складське відділення; 3 – бізнес-зона та приміщення для водійського персоналу; 4 – офіси та адміністрація; 5 – приміщення для складського персоналу

Рисунок 16 – План-схема ПП логістичного профілю діяльності

RFID-СКУД складського комплексу ПП складається з системи контролю доступу автотранспортних засобів (доступ до території та об’єктів підприємства) та системи контролю доступу до приміщень підприємства.

Для улаштування RFID-СКУД складського комплексу ПП використовується технологія пасивної надвисокочастотної (НВЧ) системи радіочастотної ідентифікації, проєктні та експлуатаційні положення якої регламентуються ISO/IEC 18000-6:2010 [121].

Система контролю доступу для автотранспортного засобів обладнується 6 портальними воротами з електромеханічним приводом та RFID-зчитувачами. Портальний зчитувач складається з RFID-зчитувача та чотирьох антен, які з'єднані з зчитувачем за допомогою SMA-проводу. Для живлення RFID-зчитувачів використовуються трансформатори, що видають напругу 24 В. Сервер та комутатор живляться від мережі змінного струму (рис. 17).

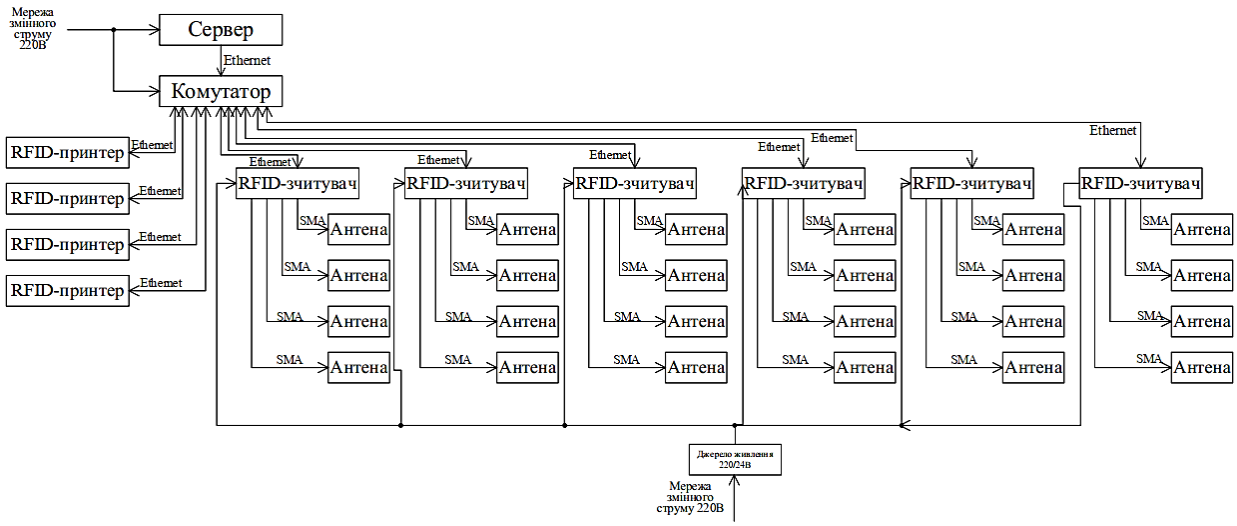


Рисунок 17 – Структурна схема RFID-системи контролю доступу автотранспортних засобів до території та об’єктів складського комплексу ПП

Система контролю та управління доступом до приміщень підприємства включає в себе сім дверей і турнікет, керовані чотирма контролерами доступу. Три з цих контролерів мають два RFID-зчитувачі та два електромагнітні замки кожен, а четвертий контролер має один RFID-зчитувач, один електромагнітний замок, турнікет та кнопку виходу. Самі контролери підключені до сервера через концентратор за допомогою двостороннього Ethernet-з’єднання. Всі контролери,

зчитувачі, замки та турнікет вимагають 12 В постійного струму, тому для організації їх використовується трансформаторний перетворювач. Сервер та комутатор живляться від мережі змінного струму (рис. 18).

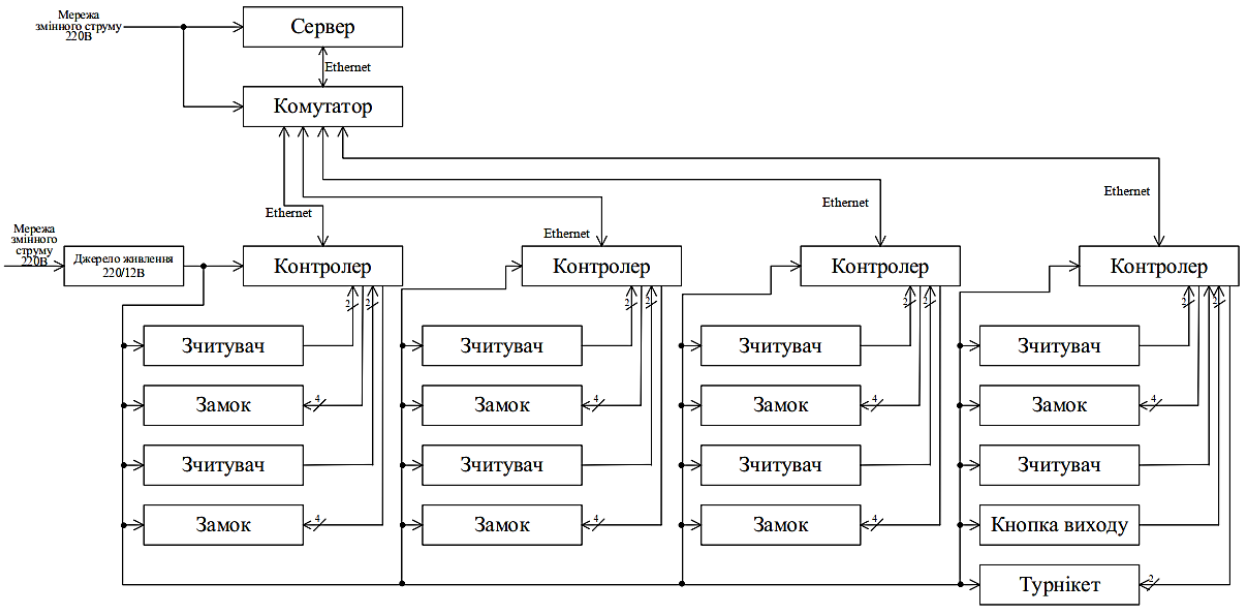
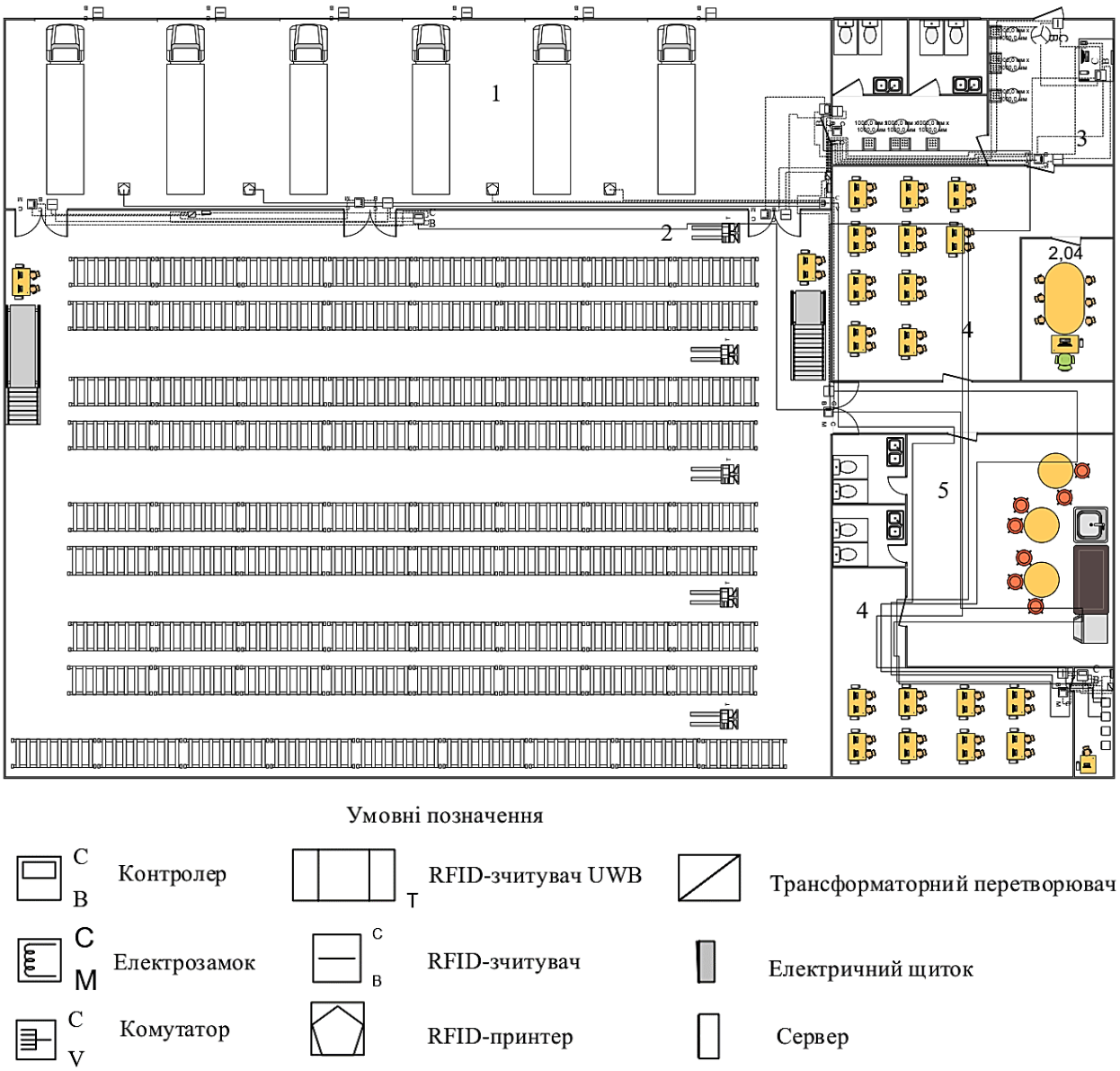


Рисунок 18 – Структурна схема RFID-системи контролю доступу до приміщень складського комплексу ПП

Отже, в рамках системи контролю доступу приватного складського комплексу використовується RFID-технологія, яка дозволяє забезпечити надійний та зручний контроль доступу для автотранспортних засобів та приміщень підприємства (рис. 19).



1 – приймально-відправне відділення; 2 – складське відділення; 3 – бізнес-зона та приміщення для водійського персоналу; 4 – офіси та адміністрація; 5 – приміщення для складського персоналу

Рисунок 19 – План-схема ПП з проєктним розміщенням структурних елементів RFID-СКУД

RFID-технологія впроваджена для забезпечення ефективного та безпечного контролю доступу на території підприємства, що є важливим елементом забезпечення інформаційної безпеки та управління доступом. Вона дозволяє забезпечити автоматизований контроль та реєстрацію руху транспортних засобів і

працівників, зменшити ризик несанкціонованого доступу та покращити загальну безпеку об'єкту.

RFID-технологія в поєднанні з іншими елементами системи контролю доступу робить складський комплекс ПП більш захищеним та дозволяє ефективно відстежувати та контролювати рух осіб і транспортних засобів на об'єкті.

3.2 Апаратна реалізація методу у вигляді системи RFID-ідентифікації

Проєктна система RFID-СКУД складського комплексу ПП будується на основі RFID-зчитувачів. Відповідно до аналізу типових рішень з улаштування системи безконтактної ідентифікації для забезпечення інформаційної безпеки приватних підприємств виконаємо розробку апаратного рішення RFID-зчитувача на базі технології Arduino та RFID-RC522.

З метою мінімізації габаритних розмірів RFID-зчитувач проєктується на базі мікроконтролеру Arduino Nano [122] (рис. 20).

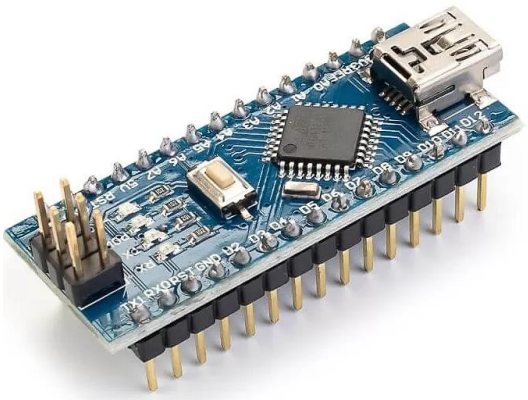


Рисунок 20 – Загальний вигляд мікроконтролеру Arduino Nano [122]

Мікроконтролер Arduino Nano - це вбудована електронна плата, яка базується на мікроконтролері ATmega328P від компанії Microchip (раніше Atmel). Він призначений для розробки пристроїв з вбудованими обчислювальними можливостями і володіє наступними технічними характеристиками [122]:

1. Мікроконтролер: Arduino Nano використовує мікроконтролер ATmega328P, який працює на тактовій частоті 16 МГц і має 32 кілобайти флеш-пам'яті для зберігання програмного коду.

2. Напруга живлення: Плата може бути живлена напругою від 7 до 12 вольт. Живлення може здійснюватися через USB-порт або за допомогою зовнішнього джерела живлення.

3. Цифрові та аналогові входи/виходи: Arduino Nano має 14 цифрових входів/виходів, включаючи 8 аналогових входів. З цих цифрових виходів 8 підтримують можливість широтно-імпульсної модуляції (PWM) для керування аналоговими пристроями (рис. 21).

4. Інтерфейси: Плата обладнана вбудованим USB-інтерфейсом для програмування і зв'язку з комп'ютером. Крім того, Arduino Nano підтримує інтерфейси UART, SPI і I2C для обміну даними з іншими пристроями.

5. Пам'ять: Під керуванням мікроконтролера є флеш-пам'ять розміром 32 кілобайти для зберігання програмного коду, 2 кілобайти оперативної пам'яті (RAM) і 1 кілобайт EEPROM для зберігання даних.

6. Розмір та формфактор: Arduino Nano має дуже компактний розмір приблизно 45 x 18 мм і має формфактор, який легко вбудовується в різні пристрої та проекти.

7. Сумісність: Він сумісний з Arduino Integrated Development Environment (IDE), що робить розробку і програмування дуже зручними для користувачів.

Arduino Nano знаходить широке застосування в розробці різноманітних електронних пристроїв, прототипуванні, робототехніці і автоматизації завдяки своїм технічним характеристикам, низькій вартості і зручності використання.

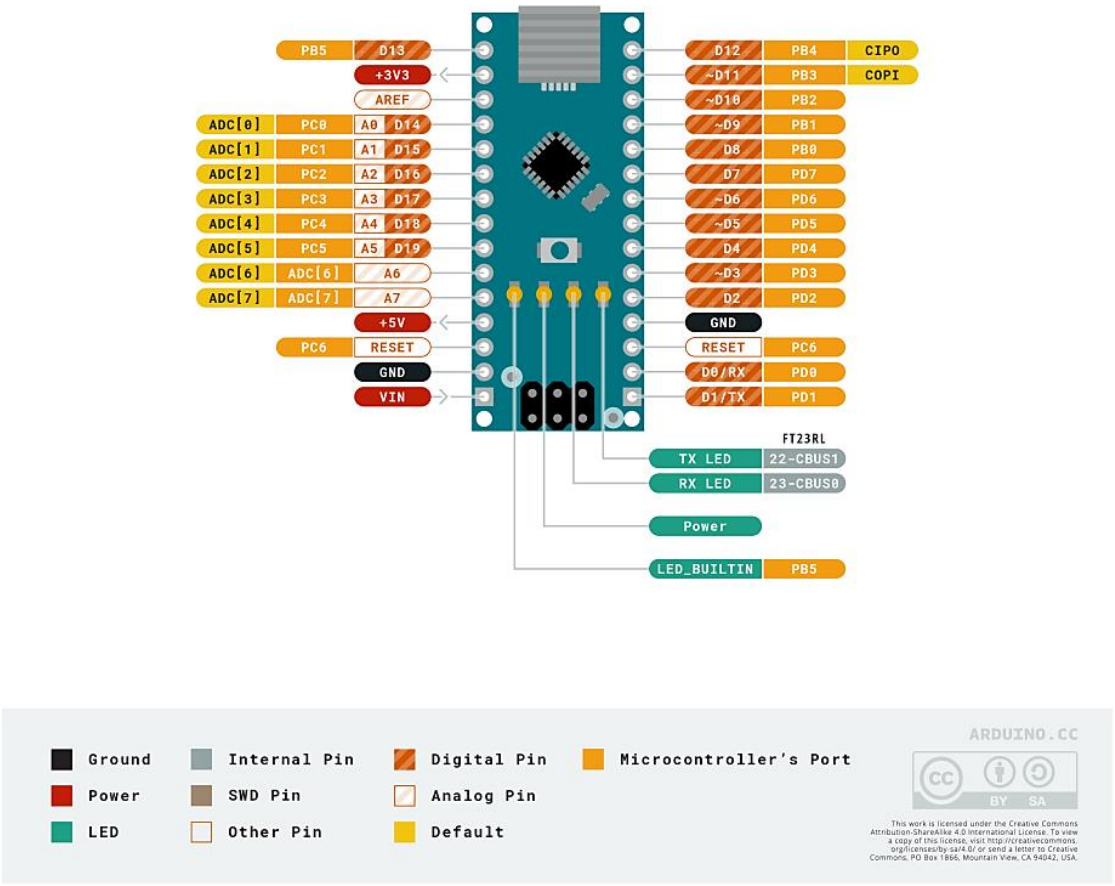


Рисунок 21 – Улаштування мікроконтролеру Arduino Nano [122]

Другим важливим елементом проєктного RFID-зчитувача є RFID-модуль RC-522 з набором безконтактних карт-ключів [123] (рис. 22).

Рисунок 22 – Загальний вигляд RFID-MFRC522 [123]

Модуль RFID-MFRC522 є інтегрованим пристроєм для безконтактного зчитування та запису інформації з RFID-міток або карток. Цей модуль базується на мікросхемі MFRC522 від NXP Semiconductors (раніше від Philips) і забезпечує зв'язок з мітками на відстані до 10 см за допомогою радіочастотної ідентифікації (RFID). Основні характеристики RFID-MFRC522 включають [123]:

1. Частота роботи: Модуль працює на стандартній частоті 13,56 МГц, яка є поширеним стандартом для систем RFID.

2. Підтримка стандартів: Він підтримує стандарти ISO/IEC 14443 A/MIFARE, що робить його сумісним з багатьма RFID-мітками та картками, що відповідають цим стандартам.

3. Інтерфейс зв'язку: Для обміну даними з мікроконтролерами та іншими пристроями модуль використовує інтерфейс SPI (Serial Peripheral Interface) (рис. 23).

4. Антена: Він має вбудовану антену, яка дозволяє зчитувати RFID-мітки на відстані до 10 см, забезпечуючи надійний зв'язок.

5. Живлення: Для живлення модуля використовується напруга від 3,3 В до 5 В, що робить його сумісним із широким спектром живлення.

6. Бібліотеки: Для полегшення програмування і взаємодії з модулем RFID-MFRC522 доступні різні програмні бібліотеки, зокрема для платформи Arduino.

7. Застосування: Модуль RFID-MFRC522 знаходить застосування в різних сферах, включаючи системи контролю доступу, системи інвентаризації та відстеження об'єктів, а також системи ідентифікації осіб.

Завдяки своїм технічним можливостям та зручному інтерфейсу, модуль RFID-MFRC522 є популярним засобом для розробки різноманітних проектів, пов'язаних з безконтактною ідентифікацією та взаємодією з RFID-мітками.

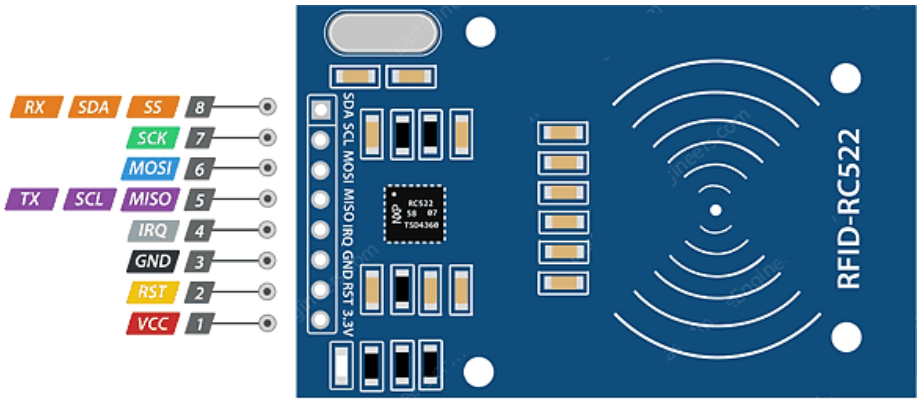


Рисунок 23 – Улаштування RFID-RC522 (MFRC522) [123]

Загальна структура проєктного RFID-зчитувача:

1. Плата Arduino Nano (рис. 20, рис. 21):

– Функціональний опис: Плата Arduino Nano є мікроконтролером, який використовується для керування та керування всією системою RFID-зчитувача. Вона відповідає за обробку інформації, передачу даних і керування різними функціями системи.

– Технічний опис: Плата має мікроконтролер ATmega328P, який працює на частоті 16 МГц. Вона оснащена вбудованим USB-інтерфейсом для програмування та живиться від джерела напруги 5 В. Ця плата має цифрові та аналогові входи/виходи, що дозволяє підключати та керувати різними датчиками та пристроями.

2. RFID-модуль RC-522 з набором безконтактних карт-ключів (рис. 22, рис. 23).

– Функціональний опис: RFID-модуль RC-522 відповідає за безконтактне зчитування інформації з RFID-міток та карт-ключів. Він визначає ідентифікаційні дані користувачів та передає їх до контролера для подальшої обробки.

– Технічний опис: Модуль включає в себе антенну систему та обчислювальний блок, який працює на частоті 13,56 МГц. Він має можливість зчитувати дані з RFID-міток на відстані до 3-5 см і підключається до Arduino Nano через SPI-інтерфейс.

3. Матрична мембранна клавіатура 4×4:

– Функціональний опис: Клавіатура використовується для введення паролів та команд в систему контролю доступу. Кожна клавіша має свій унікальний код, який передається контролеру для подальшого аналізу та обробки.

– Технічний опис: Мембранна клавіатура має 16 клавіш, організованих у формі матриці 4x4. Вона підключається до плати Arduino Nano через відповідні піни. При натисканні на клавіші створюється електричний контакт, який сприймається контролером.

4. LCD-дисплей 16x2 з I2C-інтерфейсом:

– Функціональний опис: Дисплей використовується для візуалізації інформації, такої як повідомлення, статус системи або результати ідентифікації. Він дозволяє користувачеві отримувати зворотний зв'язок в реальному часі.

– Технічний опис: LCD-дисплей має розмір 16 символів у два рядки. Він підключається до Arduino Nano за допомогою I2C-інтерфейсу, що дозволяє зменшити кількість потрібних пінів для з'єднання і спрощує використання.

5. Релейний модуль:

– Функціональний опис: Релейний модуль використовується для керування замками або іншими зовнішніми пристроями для фізичного доступу. Він дозволяє контролеру відкривати або закривати двері за командою адміністратора.

– Технічний опис: Модуль має один або декілька реле, кожне з яких може вимикати або включати електричний контур. Він підключається до Arduino Nano через цифрові виходи.

6. П'єзоелектричний випромінювач (буззер):

– Функціональний опис: П'єзоелектричний випромінювач (буззер) використовується для аудіального повідомлення користувачу про результати ідентифікації або інші події в системі.

– Технічний опис: Буззер генерує акустичні сигнали певної частоти при введенні відповідної команди з контролера. Він підключається до Arduino Nano через цифровий вихід і може бути програмований для відтворення різних звукових сигналів.

Ці елементи разом складають RFID-зчитувач, який використовується для системи контролю доступу та ідентифікації користувачів. Вони допомагають забезпечити безпеку та ефективність роботи системи контролю доступу на підприємстві.

Почнемо з розгляду модуля RFID-приймача RC-522. Цей модуль працює відповідно до SPI-протоколу і, отже, вимагає взаємодії з чітко визначеними виводами мікроконтролера Arduino Nano, на які здійснюється апаратна реалізація SPI. Згідно з документацією для плати Arduino Nano, ми маємо наступний вигляд зв'язку (рис. 24).

Необхідно врахувати, що виходи MISO, MOSI та SCK є постійними і не підлягають перепрограмуванню. В той час як виводи SS та RST можуть бути приєднані до будь-яких доступних виводів на платі Arduino Nano, і їх номери повинні бути вказані в програмному коді (скетчі).

Другий важливий аспект стосується LCD-дисплея, який використовує протокол I2C для комунікації. Для плати Arduino Nano виводи шини I2C реалізовані через виводи A4 (SDA) та A5 (SCL), як це зазначено нижче (рис. 25).

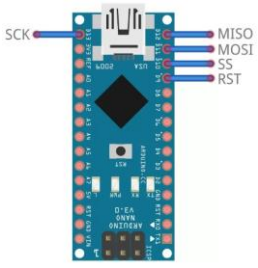


Рисунок 24 – Система комутації Arduino Nano та RC-522

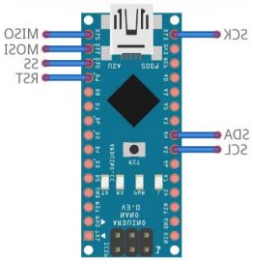


Рисунок 25 – Проєктна схема комутації Arduino Nano та RC-522

Інші компоненти схеми, такі як клавіатура, буззер і реле модуль, вимагають ще 10 виводів мікроконтролера. Згідно з представленим малюнком, вибрана плата Arduino має достатню кількість виводів для цих потреб.

Важливо відзначити, що RFID-приймач RC-522 повинен бути живлений напругою 3.3V, щоб не пошкодити його. Реле, призначене для керування електромагнітним замком, працює з логічним рівнем 5V. Також, в практиці зустрічаються реле модулі, які працюють з напругою 12V, і це також потрібно враховувати. П'єзоелектричний випромінювач звуку не включає в себе вбудований генератор звуку.

У підсумку, після врахування всіх необхідних компонентів, схема має наступний вигляд (рис. 26, рис. 27).

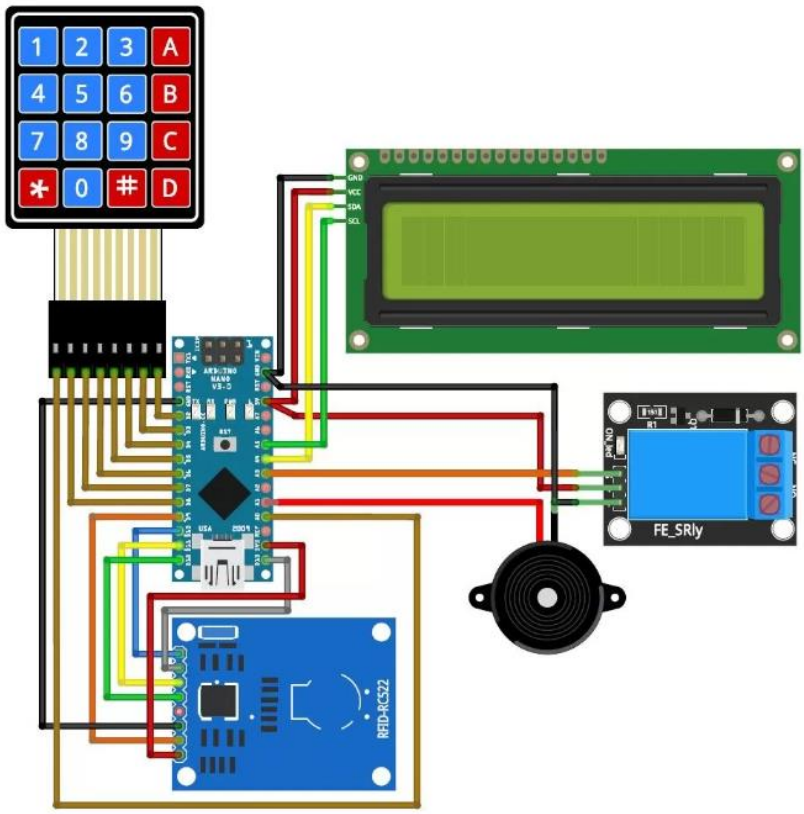


Рисунок 26 – Проєктна схема RFID-зчитувача для RFID-СКУД складського комплексу ПП

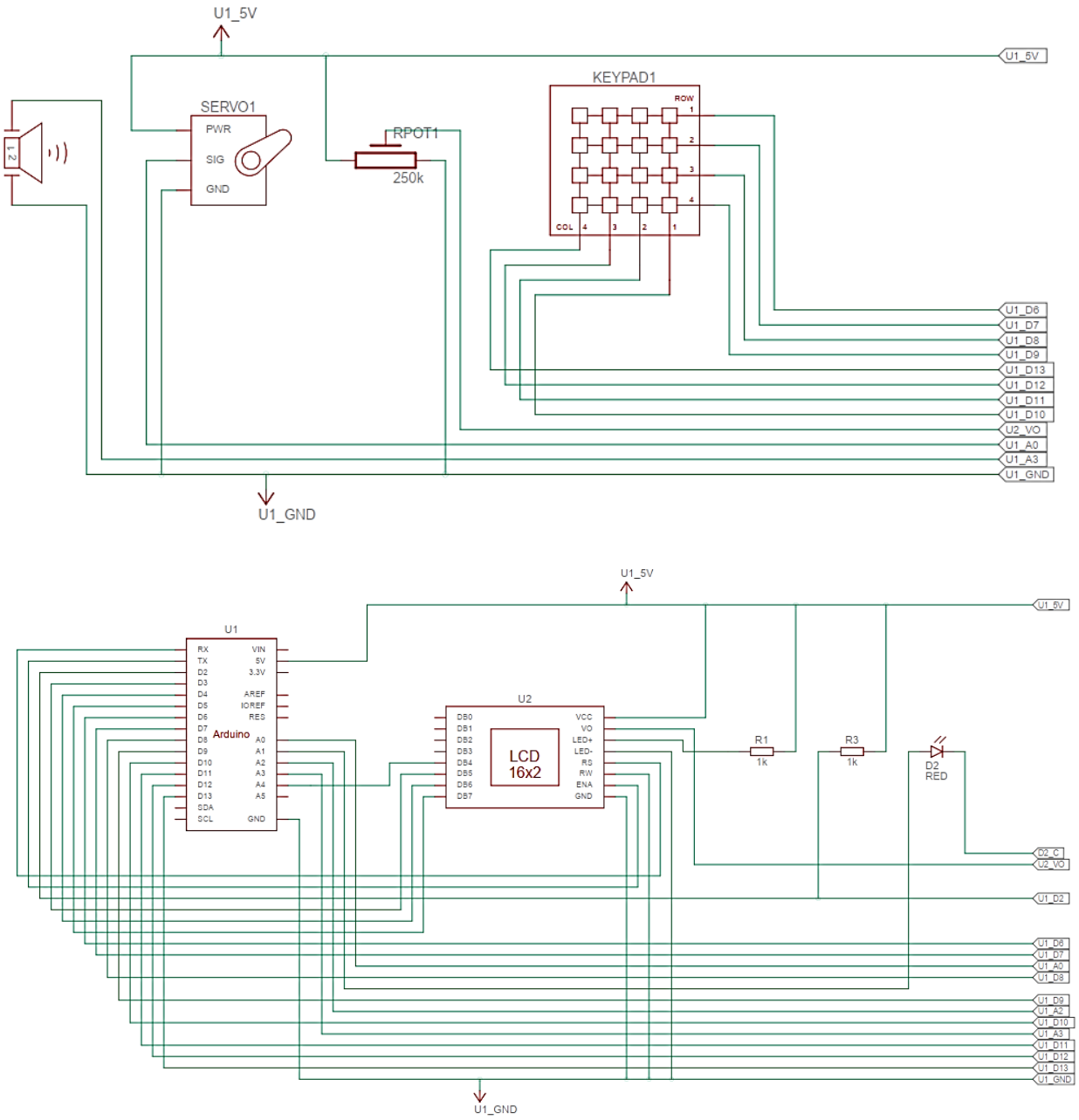


Рисунок 27 – Схема комутації проєктного RFID-зчитувача для RFID-СКУД складського комплексу ПП

Таким чином, апаратна реалізація RFID-зчитувача для системи контролю та управління доступом (СКУД) складського комплексу приватного підприємства є досить комплексною та добре обґрунтованою. Вона включає в себе ряд ключових компонентів: мікроконтролер Arduino Nano (високоефективний мікроконтролер, який відповідає за обробку даних та керування іншими компонентами системи), RFID-модуль RC-522 (цей модуль відповідає за зчитування безконтактних карт-

ключів, що використовуються для ідентифікації користувачів системи), матрична мембранна клавіатура 4×4 (використовується для введення паролів або інших команд), LCD-дисплей 16×2 з I2C-інтерфейсом (надає зручний спосіб візуалізації інформації для користувача), релейний модуль (відповідає за керування електромагнітним замком для відкриття дверей або воріт), п'єзоелектричний випромінювач (буззер) (використовується для відтворення аудіосигналів або сигналів сповіщення).

Ця апаратна реалізація дозволяє забезпечити надійний та ефективний контроль доступу до об'єктів підприємства. Вона обґрунтована з точки зору функціональності та враховує основні вимоги до системи контролю та управління доступом. Кожен компонент в цій системі відповідає за конкретну функцію і взаємодіє з іншими для забезпечення повноцінного функціонування СКУД.

3.3 Програмна реалізація методу у вигляді системи RFID-ідентифікації

Перед написання програмного коду, існує необхідність розглянути організацію даних у незалежній пам'яті мікроконтролера Arduino Nano. Згідно з технічним завданням, нам потрібно зберігати наступні типи даних у EEPROM [122]:

1. Унікальні ідентифікатори ключів доступу – 30 одиниць.
2. Пароль доступу, який дозволяє відкривати замок при його введенні.
3. Пароль адміністратора для доступу до меню налаштувань.
4. Час, протягом якого замок залишається у відкритому стані.
5. Унікальний ідентифікатор першого запуску програми.

Ця завдання вимагає обдуманої організації даних у внутрішній пам'яті мікроконтролера для ефективного доступу до них у майбутньому.

Унікальні ідентифікатори ключів доступу. Було розроблено програму для мікроконтролера Arduino Nano з використанням інтерфейсу SPI для взаємодії з RFID-модулем RC-522 та забезпечення зчитування та запису даних міток. У пам'яті EEPROM мікроконтролера зберігаються ідентифікатори (UID) RFID-міток, паролі

для доступу та інші параметри. Пам'ять EEPROM поділена на блоки, де кожен блок відповідає одному ключу доступу. Під час реєстрації міток, їх UID записується у відповідний блок пам'яті разом із відповідними налаштуваннями. Під час спроби відкрити замок за допомогою мітки, програма перевіряє UID мітки на відповідність записам у пам'яті EEPROM. У разі збігу та відповідності інших параметрів, замок відчиняється.

Кожна мітка RFID має унікальний ідентифікатор (UID) завдовжки 4 байти. Під час реєстрації кожного ключа в системі, цей ідентифікатор разом із додатковим байтом, який служить ознакою стану – порожнього або зайнятого рядка в базі даних, записується в пам'ять EEPROM. Така структура запису ключа складається з 5 байтів даних. Нижче наведена карта EEPROM, яка відображає фізичні адреси пам'яті, пов'язані з інформацією про всі RFID-ключі в системі (табл. 5).

Таблиця 5 – Структуру адресації EEPROM для RFID-ключів [122]

Номер ключа або рядку	Адреса в EEPROM					
	Ознака реєстрації ключа в базі даних (1-ключ зареєстрований; 0-комірка не зайнята)	Унікальний UID				
1	2	3	4	5	6	
Ключ №0	0000	0001	0002	0003	0004	
Ключ №1	0005	0006	0007	0008	0009	
Ключ №2	0010	0011	0012	0013	0014	
Ключ №3	0015	0016	0017	0018	0019	
Ключ №4	0020	0021	0022	0023	0024	
Ключ №5	0025	0026	0027	0028	0029	
Ключ №6	0030	0031	0032	0033	0034	
Ключ №7	0035	0036	0037	0038	0039	
Ключ №8	0040	0041	0042	0043	0044	
Ключ №9	0045	0046	0047	0048	0049	
Ключ №10	0050	0051	0052	0053	0054	
Ключ №11	0055	0056	0057	0058	0059	
Ключ №12	0060	0061	0062	0062	0064	
Ключ №13	0065	0066	0067	0068	0069	
Ключ №14	0070	0071	0072	0073	0074	
Ключ №15	0075	0076	0077	0078	0079	
Ключ №16	0080	0081	0082	0083	0084	

Кінець таблиці 5

1	2	3	4	5	6
Ключ №17	0085	0086	0087	0088	0089
Ключ №18	0090	0091	0092	0093	0094
Ключ №19	0095	0096	0097	0098	0099
Ключ №20	0100	0101	0102	0103	0104
Ключ №21	0105	0106	0107	0108	0109
Ключ №22	0110	0111	0112	0113	0114
Ключ №23	0115	0116	0117	0118	0119
Ключ №24	0120	0121	0122	0123	0124
Ключ №25	0125	0126	0127	0128	0129
Ключ №26	0130	0131	0132	0133	0134
Ключ №27	0135	0136	0137	0138	0139
Ключ №28	0140	0141	0142	0143	0144
Ключ №29	0145	0146	0147	0148	0149

З наведеної таблиці видно, що інформація про всі доступові ключі (30 штук) буде зберігатися в пам'яті EEPROM у діапазоні адрес від 0 до 149. Це не велика кількість, особливо з урахуванням того, що Arduino Nano може надати доступ до 1024 окремих комірки енергонезалежної пам'яті.

Пароль доступу та пароль адміністратора. Довжина будь-якого пароля складатиме 7 цифр, що відповідає 7 байтам даних. Оскільки паролі можуть змінюватися через меню адміністратора, їх також необхідно зберігати в пам'яті EEPROM, щоб уникнути втрати при вимкненні живлення. З використанням попереднього досвіду створення картки пам'яті для RFID-ключів, була проведена аналогічна робота для цих двох паролів (табл. 6).

Таблиця 6 – Структура адресації EEPROM для адміністрування [122]

Пароль	Адреса в EEPROM						
Доступ	0150	0151	0152	0153	0154	0155	0156
Адміністратор	0157	0158	0159	0160	0161	0162	0163

Таким чином, отримуємо, що пароль для доступу зберігатиметься в діапазоні адрес 150-156, а пароль адміністратора в діапазоні 157-163.

Час, протягом якого замок утримуватиметься у відкритому стані.

Зауважимо, що при введенні правильного пароля або піднесенні зареєстрованого ключа до терміналу має бути активоване реле, яке відповідає за відкриття електромеханічного замка. Це реле повинно бути увімкнуте протягом певного часу, щоб надати можливість відчинити двері без поспіху. Цей параметр може бути налаштований в меню адміністратора і знаходитиметься в діапазоні від 1 до 9 секунд. Отже, для збереження цього параметру потрібен ще один блок пам'яті EEPROM (табл. 7).

Таблиця 7 – Структура адресації EEPROM для керування електромеханічним замком [122]

Параметр	Адреса в EEPROM
Час утримання реле електромеханічного замка	0164

Унікальний ідентифікатор первинного запуску програми. Унікальний ідентифікатор первинного запуску програми важливий для розрізнення першого запуску від всіх наступних. При першому запуску необхідно ініціалізувати значення EEPROM за замовчуванням, оскільки на той момент в ній нічого не зберігалося. Проте під час наступних запусків не повинно бути змін у енергонезалежній пам'яті, оскільки користувач може зберегти там свої дані за власним бажанням. Адреса, за якою розташовується цей ідентифікатор, буде рівною 500 (табл. 8).

Таблиця 8 – Структура адресації EEPROM для ідентифікації первинного запуску програми

Параметр	Адреса в EEPROM
Ознака первинного запуску програми	0500

Для подальшої розробки програмного коду, після складання карти енергонезалежної пам'яті, необхідно виконати додатковий крок, а саме – завантажити та встановити кілька бібліотек, які значно спростять розробку скетчу і покращать його читабельність. Ось перелік необхідних бібліотек:

1. New-LiquidCrystal-master: Ця бібліотека дозволяє працювати з LCD-дисплеєм через шину I2C.

2. Keypad-master: Бібліотека призначена для зручної роботи з матричною клавіатурою.

3. rfid-master: Ця бібліотека розроблена для взаємодії з RFID-модулем RC-522.

Встановлення цих бібліотек допоможе спростити програмування та поліпшити структуру програмного коду.

Лістинг програмного коду надається у Додатку Б.

Структура програмного коду

1. Підготовка RFID-зчитувача: оголошення пінів для підключення реле та буззера; підключення бібліотек для роботи з LCD по протоколу I2C та створення об'єкту для LCD; оголошення масивів користувацьких символів для відображення на дисплеї; підключення бібліотеки для роботи з флеш-пам'яті мікроконтролера та визначення текстових рядків меню у флеш-пам'яті; створення таблиці рядків меню; підключення бібліотеки для роботи з матричною клавіатурою та оголошення масиву-карти клавіатури; підключення бібліотек для роботи з RFID-модулем RC522 та створення екземпляра класу для модуля RC522.

2. Адаптація бібліотек. Оголошення глобальних змінних та прапорів для управління програмою, таких як: flagClearMenuScreen (прапор для очищення екрану меню), openTime (час, через який закриється замок після його відкриття), tempPassword (масив для тимчасового зберігання введеного пароля), passwordIndex (індекс цифри пароля, з якою працюється в даний момент), key (змінна для зберігання коду натиснутої кнопки), cards (масив для зберігання ідентифікаторів RFID-карт), cardsIndex (індекс для роботи з конкретною RFID-карткою, accessPassword (пароль доступу за замовчуванням), adminPassword (пароль адміністратора за замовчуванням), menuFlag (номер екрану меню), globalState (глобальний стан системи (для реалізації кінцевого автомата)), cardWeatingTime (час очікування картки для реєстрації). Підключення бібліотеки для роботи з енергонезалежною пам'яттю EEPROM.

3. Ініціалізація EEPROM.

4. Ініціалізація карти пам’яті EEPROM.

5. Ініціалізація функції читання даних про записані карти з EEPROM.

6. Ініціалізація функції сканування піднесеної до терміналу карти або ключа.

7. Ініціалізація функції виводів рядків з флеш-памяті мікроконтролера у визначені координати РКІ.

8. Ініціалізація функції подачі звукового сигналу.

9. Ініціалізації функції скидання буферного паролю.

10. Ініціалізація функції виводу короткотривалої інформації, що говорить про помилку доступу.

11. Ініціалізація функції відкриття електрозамка при правильному коді доступу.

12. Ініціалізація функції введення паролю.

13. Ініціалізація функції відображення меню.

14. Ініціалізація функції попередніх установок.

15. Виконання основного циклу програми.

Ця частина коду відповідає за основний цикл в програмі. Основні дії, які виконуються у цьому циклі:

1. Зчитується натиснута клавіша на матричній клавіатурі (якщо вона натиснута).

2. В залежності від глобального стану системи (змінна globalState), виконуються відповідні дії:

- У стані 0 відображається головний екран.
- У стані 1 обробляється введення пароля або піднесення RFID-ключа.
- У стані 2 перевіряється правильність введеного пароля.
- У стані 3 відкривається електрозамок на визначений у меню час.
- У стані 4 виводиться помилка при неправильному паролі або незареєстрованому ключу.
- У стані 100 відображається головне меню адміністратора.

– У стані 101 оброблюється клавіша, натиснута в головному меню адміністратора.

– У станах 110-115 виконується робота зі списком RFID-ключів.

– У стані 120 відображається меню зміни пароля доступу.

– У стані 121 оброблюється введення нового пароля доступу.

– У стані 130 відображається меню зміни пароля адміністратора.

– У стані 131 оброблюється введення нового пароля адміністратора.

– У стані 140 відображається меню зміни часу утримання замка у відкритому стані.

– У стані 141 оброблюється введення нового часу утримання замка у відкритому стані.

Цей основний цикл дозволяє взаємодіяти з системою, обробляти введені дані та виконувати відповідні дії в залежності від поточного стану системи. Програмна реалізація системи RFID-ідентифікації в даному коді включає в себе наступні ключові елементи та функціональність:

1. Ініціалізація: Система починає свою роботу з ініціалізації різних глобальних змінних та окремих функцій, таких як паролі доступу та адміністратора, час утримання замка у відкритому стані, інформація про RFID-карти, а також перевірка наявності даних у флеш-пам'яті мікроконтролера. Ця ініціалізація відбувається при першому запуску програми.

2. Основний цикл програми: Основний цикл постійно моніторить введені команди з матричної клавіатури і обробляє їх в залежності від поточного стану системи. Це включає в себе введення паролів, ідентифікацію RFID-ключів, управління головним меню та виконання різних дій, таких як зміна паролів, редагування списку RFID-карт, а також відкриття замка.

3. RFID-ідентифікація: Система може ідентифікувати користувачів за допомогою RFID-ключів. Вона здатна реєструвати нові ключі та перевіряти їх правильність. Всі дані RFID-ключів зберігаються у флеш-пам'яті мікроконтролера.

4. Управління паролями: Система дозволяє змінювати паролі доступу та адміністратора. Нові паролі зберігаються у флеш-пам'яті для подальшого використання.

5. Управління часом утримання замка у відкритому стані: Користувач може налаштовувати час, протягом якого замок буде відкритий після введення правильного пароля. Це дозволяє контролювати доступ до об'єкта.

6. Графічний інтерфейс та безпека: Система використовує текстовий LCD-дисплей для відображення інформації та меню. Користувач може навігувати меню за допомогою матричної клавіатури. Введені дані, такі як паролі і інформація про RFID-ключі, зберігаються у флеш-пам'яті мікроконтролера і захищені від несанкціонованого доступу.

В цілому, програмна реалізація системи RFID-ідентифікації демонструє можливість створення системи контролю доступу, яка може бути використана для забезпечення безпеки об'єктів та регулювання доступу до них за допомогою RFID-ключів та паролів.

4 ОЦІНКА ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ РОЗРОБЛЕНОЇ СИСТЕМИ БЕЗКОНТАКТНОЇ ІНТЕГРАЦІЇ НА ОСНОВІ RFID-ТЕХНОЛОГІЙ ДЛЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИВАТНОГО ПІДПРИЄМСТВА

4.1 Налаштування розробленої системи RFID-ідентифікації

Налаштування проєктного RFID-зчитувача, виконується за допомого кодування через меню доступу. Введення інформації здійснюється через матричну мембранну клавіатура 4×4, а графічне відображення процесу здійснюється за допомогою LCD-дисплея 16×2 з I2C-інтерфейсом.

Технічне завдання. Після активації живлення, пристрій ініціює сеанс роботи, відтворюючи характерний аудіо-сигнал. Модуль реле, що призначений для керування електромеханічним замком, перебуває у вимкненому стані. Протягом трьох секунд на дисплеї відображається наступний напис (рис. 28).

	A	R	D	U	I	N	O		A	C	C	E	S	S	
	C	O	N	T	R	O	L		S	Y	S	T	E	M	

Рисунок 28 – Вхід до меню доступу проєктного RFID-зчитувача

По завершенні цього інтервалу, стартовий текст зникає, і пристрій переходить у робочий режим. Система контролю доступу підтримує два основних режими: робочий та режим адміністратора. Режим адміністратора використовується для реєстрації нових карток та зміни паролів.

Робочий режим. У робочому режимі користувачу надається можливість додати до терміналу RFID-карту або ввести пароль на матричній клавіатурі. Відповідне повідомлення відображається на дисплеї (рис. 29).

A	t	t	a	c	h		R	F	I	D	-	k	e	y	
P	a	s	s	w	o	r	d	:							

Рисунок 29 – Ініціалізація процедури запису ідентифікаторів

Пароль вводиться шляхом натискання цифрових клавіш на матричній клавіатурі, з можливістю підтвердження або скасування введення за допомогою клавіші [#] для підтвердження і клавіші [*] для скасування.

У випадку, якщо до терміналу додано картку, зареєстровану в системі, або введено правильний пароль, пристрій генерує характерний звуковий сигнал і подає живлення на реле, яке керує електромеханічним замком, на протязі періоду тривалістю від 1 до 9 секунд (настроюється в меню). Дисплей відображає інформацію про успішний доступ до об'єкта та залишок часу відкритого стану замка (рис. 30).

	A	C	C	E	S	S		A	L	L	O	W	E	D	
L	o	c	k		a	f	t	e	r		0		s	e	c

Рисунок 30 – Інформація про стан доступу

У випадку неправильного введення пароля або визнання RFID-ключа, який не зареєстрований в базі даних, пристрій ініціює миготливе відображення інформації про помилку доступу, супроводжуючи це звуковим сигналом (рис. 31).

	A	C	C	E	S	S		D	E	N	I	E	D	!	
B	a	d		k	e	y	/	p	a	s	s	w	o	r	d

Рисунок 31 – Інформація про блокування доступу

Режим адміністратора. Даний режим призначений для редагування змісту енергонезалежної пам'яті Arduino, додавання або видалення нових RFID-карт, а також для зміни паролів та конфігурації робочих параметрів. Для входу в адміністраторське меню необхідно, перебуваючи в робочому режимі, ввести спеціальний пароль на матричній клавіатурі та натиснути клавішу [#]. За замовчуванням пароль складається з послідовності цифр 1234567, але його можна змінити на користувацький.

Отже, адміністраторське меню включає в себе чотири пункти, наведені нижче (рис. 32).

E	D	I	T		R	F	I	D		D	A	T	A		
A	↑		B	↓		#	–	o	k		*	–	e	s	c

A	C	C	E	S	S		P	A	S	S	W	O	R	D	
A	↑		B	↓		#	–	o	k		*	–	e	s	c

A	D	M	I	N		P	A	S	S	W	O	R	D		
A	↑		B	↓		#	–	o	k		*	–	e	s	c

S	E	T		O	P	E	N		T	I	M	E			
A	↑		B	↓		#	–	o	k		*	–	e	s	c

Рисунок 32 – Меню адміністратора

Як показано у вище наведених прикладах, навігація по пунктах меню вище та нижче виконується за допомогою клавіш [A] і [B]. Для входу в обраний підпункт меню слід натиснути клавішу [#], а для повернення на вищий рівень – клавішу [*].

Редагування RFID-карток «EDIT RFID DATA». Під час переходу до даного підменю, користувачу надається можливість додавати, замінювати або редагувати RFID-ключі в базі даних пристрою. Усього можна внести до 30 унікальних кодів

ключів у базу даних (за потреби це число можна збільшити). Для перемикання списку використовуються клавіші [A] та [B] (рис. 33).

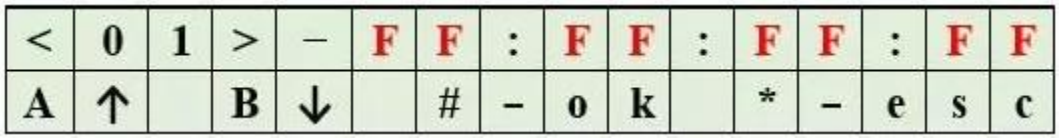


Рисунок 33 – Процедура введення ідентифікаторів

У верхньому лівому куті відображується послідовний номер комірки, який асоційований з енергонезалежною пам'яттю Arduino. Поруч з послідовним номером комірки вказаний код, прикріплений до картки (відзначений червоною маркерною смугою). Якщо комірка порожня, то замість коду відображається напис «empty», як показано нижче (рис. 34).

Рисунок 34 – Відсутність ідентифікатора

Користувач може виконати три операції з вибраною коміркою, натиснувши клавішу [#]: додати новий ключ або замінити існуючий, очистити комірку або залишити все без змін (рис. 35).

Рисунок 35 – Коригування інформації про ідентифікатора

Якщо було прийнято рішення щодо додавання або реєстрації, то після натискання клавіші [A] відтворюється звуковий сигнал, і система очікує на

піднесення карти-ключа до приймального терміналу, що відображається на дисплеї спеціальним зображенням (рис. 36).

R	E	A	D	I	N	G		C	A	R	D		U	I	D
W	e	a	t	i	n	g		f	o	r		c	a	r	d

Рисунок 36 – Процедура запису RFID-мітки

На визначення картки виділяється період тривалістю 5 секунд, після закінчення якого буде відображено повідомлення про результат реєстрації, незалежно від успішності процедури.

Процес видалення картки з комірки бази відображається швидким повідомленням «CARD DELETED». Ці дії, як описано вище для конкретного комірки <01>, аналогічні для всіх інших комірок.

Зміна пароля доступу «ACCESS PASWORD». Підменю пропонує можливість введення нового пароля для отримання доступу до об'єкта, що передбачає відкриття електромеханічного замка. Специфікація меню наведена нижче (рис. 37).

S	e	t		n	e	w		a	c	c	e	s	s		
p	a	s	s	w	o	r	d	:							

Рисунок 37 – Зміна паролю

Встановлення часу відкритого замку «SET OPEN TIME». У цьому пункті меню користувач може встановити час, протягом якого замок утримуватиметься у відкритому стані після піднесення зареєстрованої картки або введення правильного пароля. Інтерфейс виглядає наступним чином (рис. 38).

S	e	t		o	p	e	n		t	i	m	e	r	:	
>	5	s	e	c											

Рисунок 38 – Налаштування часу відкриття

Можливість встановлення часового інтервалу доступу може бути налаштована в діапазоні від 1 до 9 секунд шляхом натискання відповідної цифрової клавіші на матричній клавіатурі. Підтвердження введеного значення здійснюється клавішею [#], а скасування – клавішею [*].

Загальна схема налаштування проєктного RFID-зчитувача наводиться нижче (рис. 39).

Процедура налаштування проєктного RFID-зчитувача є ключовою складовою для забезпечення правильної роботи системи контролю доступу. Ця процедура передбачає наступні кроки:

1. Ініціалізація системи: Після подачі живлення, система ініціалізується та готова до роботи. Користувач отримує звуковий сигнал та індикацію на дисплеї, після чого система переходить у робочий режим.

2. Вибір режиму роботи: Користувач може обрати режим роботи - режим користувача або режим адміністратора. Режим адміністратора дозволяє виконувати додавання нових RFID-карт, зміну паролів та інші налаштування.

3. Введення ідентифікатора: В режимі користувача користувач має можливість ввести ідентифікатор, який може бути або RFID-картою, або паролем на матричній клавіатурі.

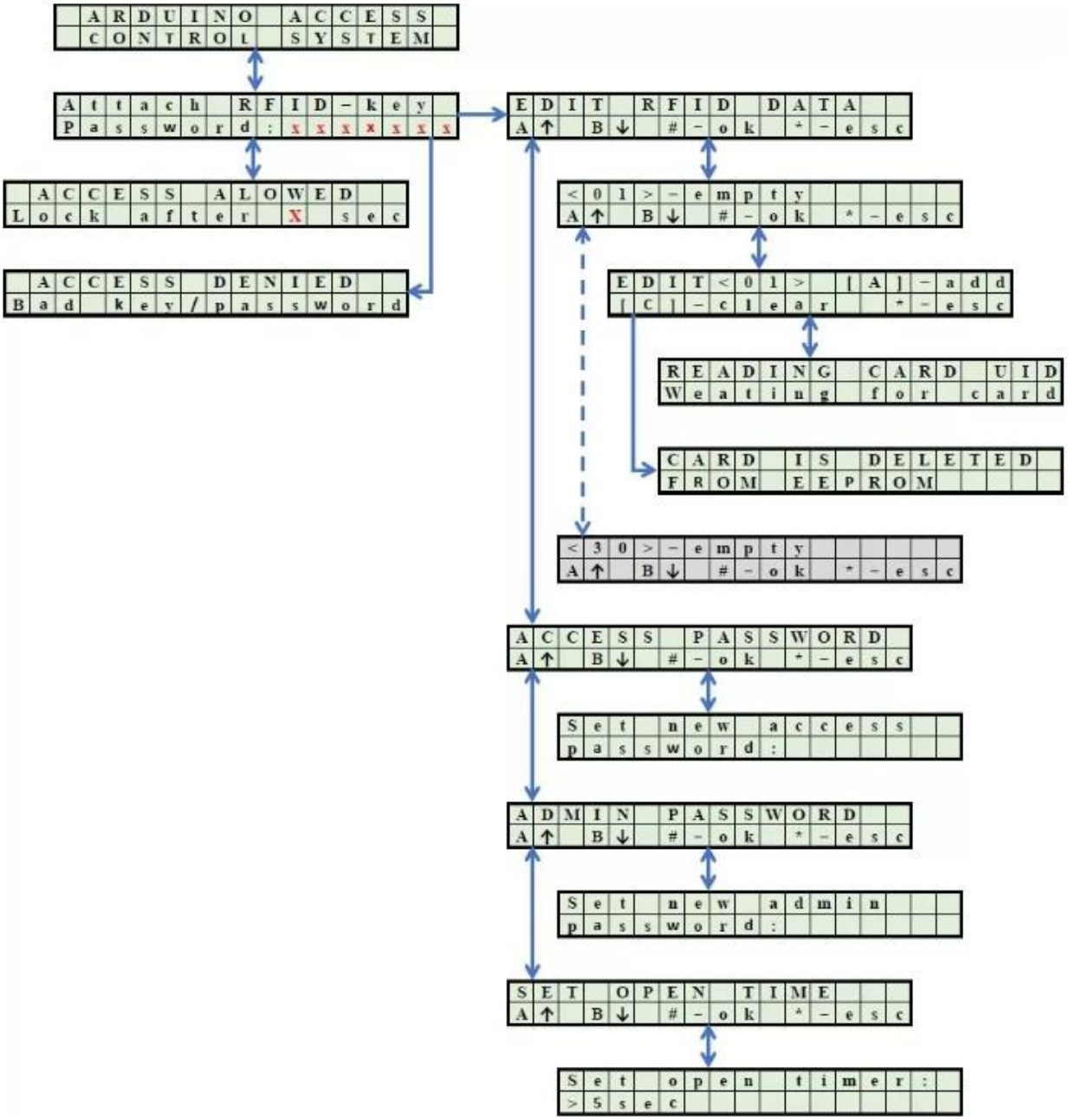


Рисунок 39 – Загальна схема налаштування проєктного RFID-зчитувача

4. Перевірка ідентифікації: Система перевіряє введений ідентифікатор на відповідність даним у базі даних. Якщо ідентифікатор вірний, система надає доступ і відповідно керує електрозамком.

5. Налаштування параметрів: У режимі адміністратора користувач може виконати налаштування системи, такі як додавання нових RFID-карт, зміну паролів або параметрів роботи замка.

6. Відображення інформації: Важливою частиною процедури є відображення інформації на дисплеї для зручності користувача. Інформація повинна бути чіткою і зрозумілою.

7. Звукові та світлові сигнали: Для інформування користувача про результати ідентифікації і стан системи використовуються звукові та світлові сигнали.

8. Управління доступом: Після ідентифікації система керує доступом до об'єкта відповідно до налаштованих параметрів.

Процедура налаштування проєктного RFID-зчитувача дозволяє забезпечити надійний та ефективний контроль доступу, забезпечуючи правильну роботу системи та зручність для користувачів.

4.2 Оцінка ефективності функціонування розробленої системи RFID-ідентифікації

Оцінка ефективності функціонування розробленої системи RFID-ідентифікації здійснюється шляхом перевірки працездатності проєктних рішень з улаштування RFID-зчитувача на дослідному стенді (рис. 40).

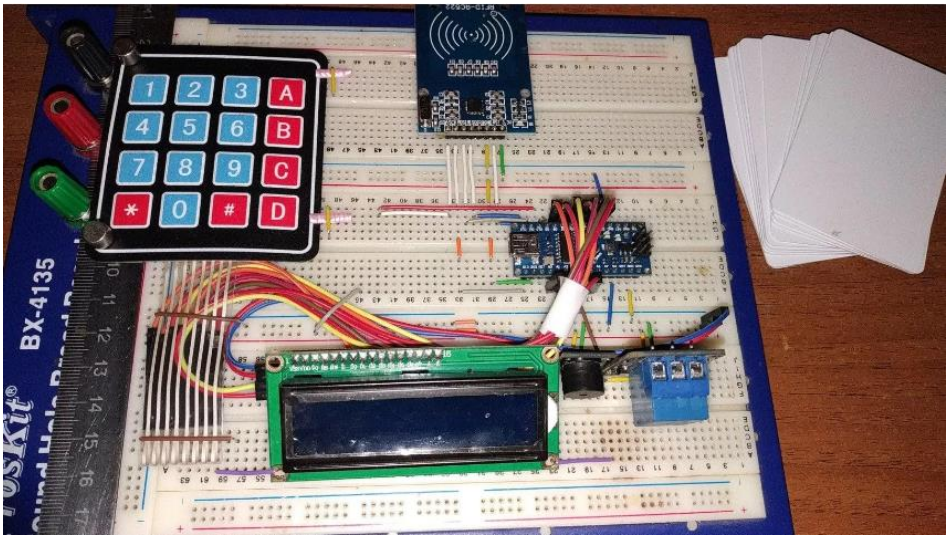


Рисунок 40 – Загальний вид дослідного стенду з проєктним RFID-зчитувачем

Далі наводимо візуалізацію функціонування проєктного RFID-зчитувача у складі дослідного стенду (рис. 41, рис. 42, рис. 43, рис. 44, рис.45, рис.46, рис.47, рис.48, рис.49, рис.50).

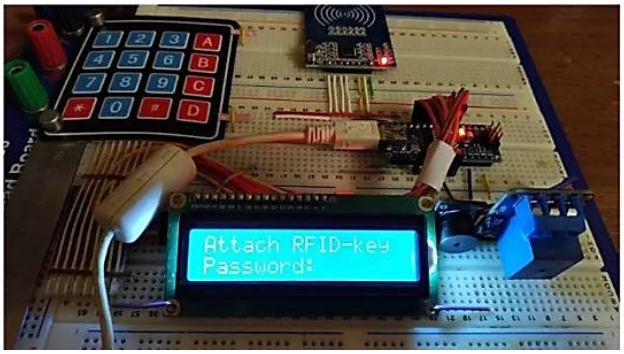


Рисунок 41 – Головний екран

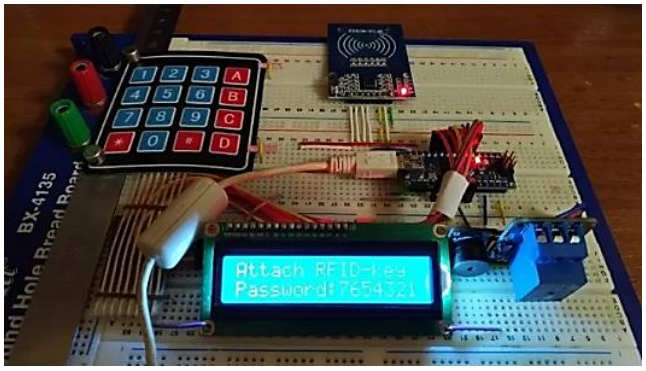


Рисунок 42 – Введення паролю доступу

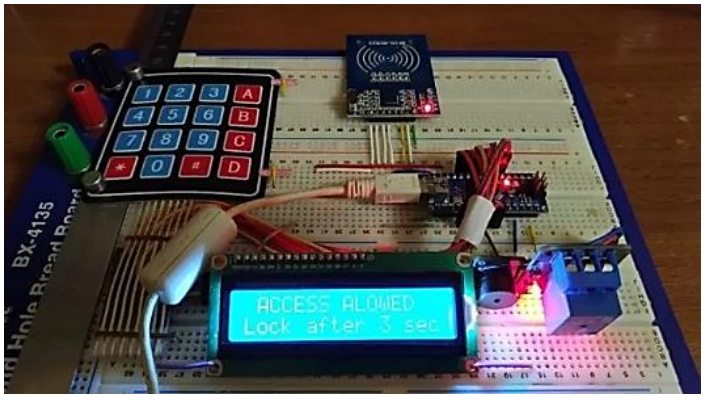


Рисунок 43 – Спрацювання реле електромеханічного замка

Рисунок 44 – У доступі відмовлено

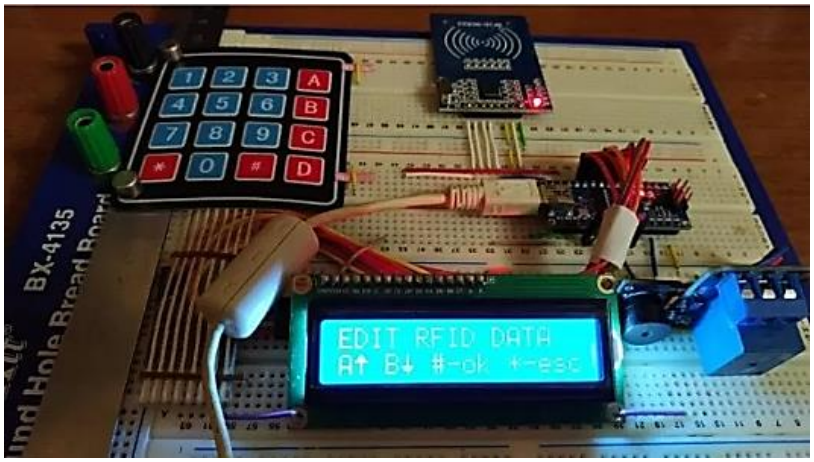


Рисунок 45 – Меню реєстрації RFID-ключа

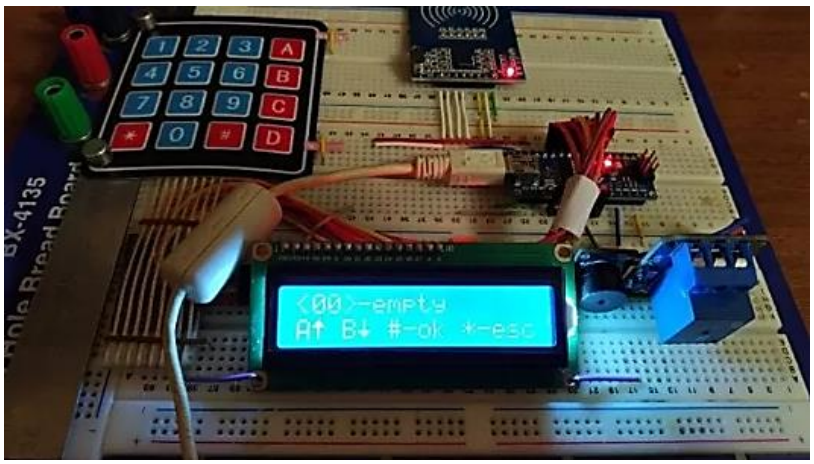


Рисунок 46 – Список RFID-ключів

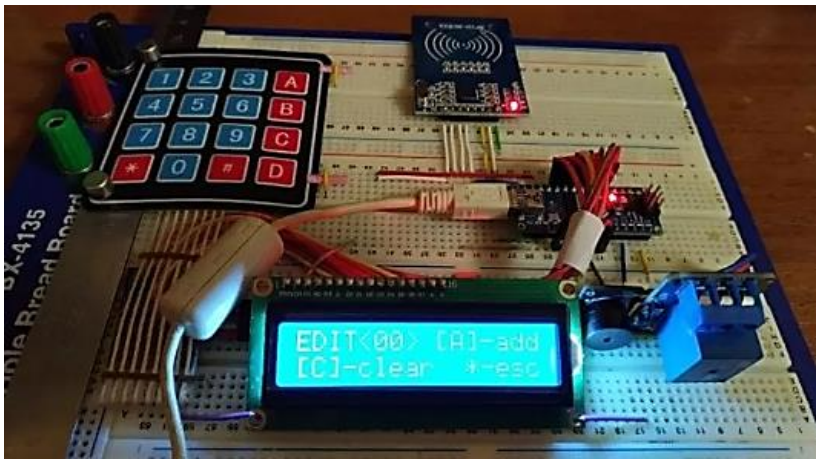


Рисунок 47 – Редагування запису про RFID-ключ

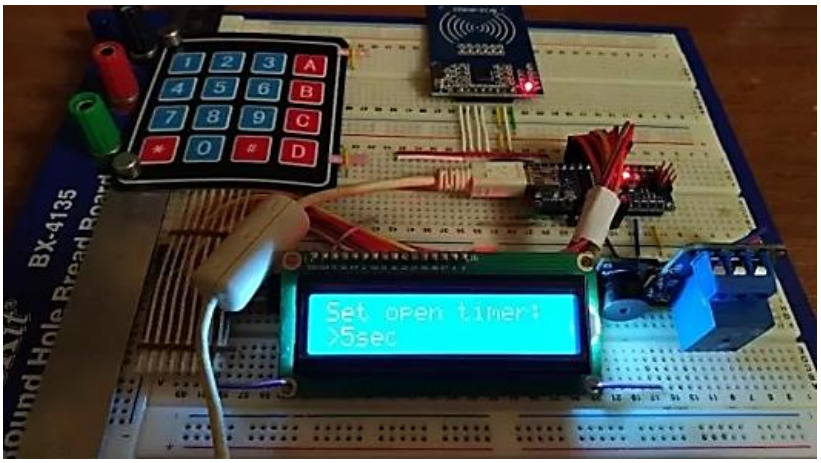


Рисунок 48 – Встановлення часу утримання електромеханічного замка

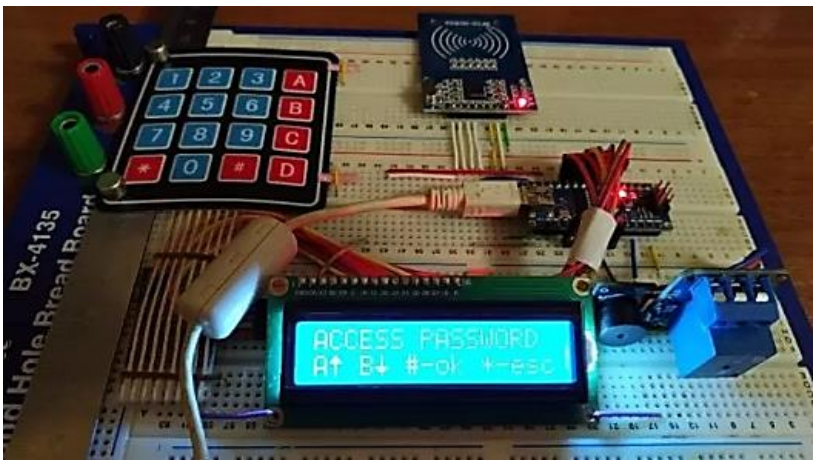


Рисунок 49 – Меню зміни паролю доступу

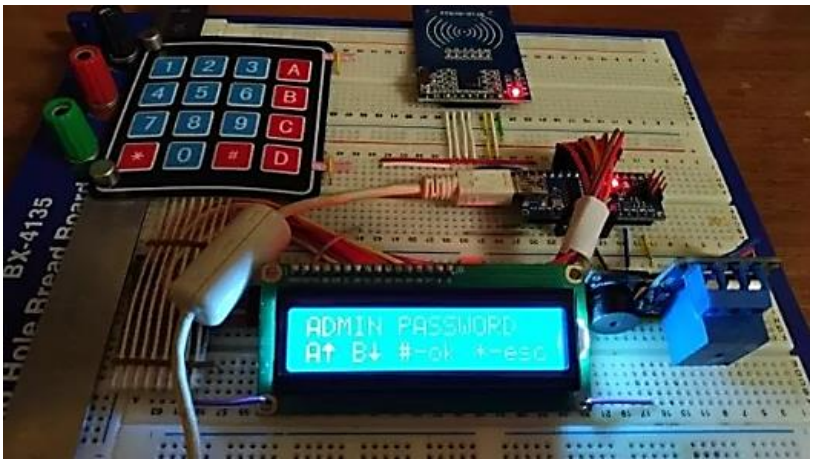


Рисунок 50 – Меню зміни паролю адміністратора

Аналізуючи функціонування розробленої системи RFID-ідентифікації на дослідному стенді, можемо зробити наступні висновки:

1. Система продемонструвала високу працездатність та надійність у виконанні основних функцій, таких як ідентифікація користувачів за допомогою RFID-карт і паролів, керування електрозамком, а також налаштування різних параметрів роботи.

2. Графічний інтерфейс системи відображається на дослідному стенді і дозволяє користувачам легко взаємодіяти з системою. Інтуїтивний інтерфейс спрощує процедуру ідентифікації та налаштування параметрів.

3. Система проявила високий рівень безпеки, оскільки надійно контролює доступ до об'єкта. Вона відмовляє у доступі, якщо ідентифікатор введено неправильно або відсутній у базі даних.

4. Система дозволяє адміністраторам легко налаштовувати параметри, такі як тривалість утримання електромеханічного замка відкритим і зміна паролів, що робить її гнучкою та адаптованою до конкретних потреб.

5. Система дозволяє реєструвати та керувати RFID-ключами в базі даних, що важливо для забезпечення контролю доступу.

6. Наявність звукових та світлових сигналів сприяє зручності користувачів і надає їм зворотний зв'язок про результати ідентифікації.

Емпіричним шляхом доведено, що розроблена система RFID-ідентифікації продемонструвала високу ефективність та функціональність під час експериментальних випробувань на дослідному стенді. Відтак, досліджувана система може бути впроваджена для реалізації систем контролю доступу в різних сферах, включаючи офіси, промислові підприємства та інші об'єкти, де забезпечення безпеки є важливим завданням.

4.3 Оцінка ефективності функціонування розробленої системи RFID-ідентифікації з урахуванням інтеграції в загальну систему безпеки приватного підприємства

Проєктна RFID-СКУД є складовою системи безпеки складського комплексу ПП. Ця система була розроблена з метою підвищення загального рівня безпеки та контролю за доступом на територію складського комплексу. Вона інтегрує сучасні технології RFID-ідентифікації, що дозволяє забезпечити надійний та ефективний контроль доступу співробітників та відвідувачів.

Однією з ключових переваг цієї системи є можливість точно ідентифікувати користувачів за допомогою RFID-карток або паролів. Це дозволяє вести облік та визначати права доступу для кожного окремого користувача. Більше того, система здатна зберігати та обробляти інформацію про зареєстрованих користувачів, що робить можливим швидке та зручне управління доступом.

Інтеграція цієї системи у загальну систему безпеки приватного підприємства сприяє підвищенню ефективності контролю та моніторингу доступу на об'єкті. Вона дозволяє враховувати специфічні потреби та вимоги ПП, забезпечуючи високий рівень захисту об'єкту від несанкціонованого доступу та недозволених дій.

Отже, розроблена система RFID-ідентифікації є важливим елементом загальної системи безпеки приватного підприємства, що сприяє підвищенню контролю, надійності та безпеки на території складського комплексу.

Оцінка ефективності функціонування розробленої системи RFID-ідентифікації в контексті її інтеграції в загальну систему безпеки приватного підприємства виявила кілька ключових аспектів.

По-перше, інтеграція цієї системи сприяє підвищенню загального рівня безпеки об'єкта. Це досягається завдяки контролю доступу до приміщень та ресурсів, що знижує ризик несанкціонованого доступу.

По-друге, система забезпечує швидку та надійну ідентифікацію співробітників та гостей за допомогою RFID-карт або паролів. Це спрощує процес ідентифікації та робить його зручним для користувачів.

По-третє, система може бути інтегрована з іншими системами безпеки, такими як відеоспостереження та контроль доступу до приміщень, що дозволяє автоматизувати та спростити процеси моніторингу та керування безпекою.

По-четверте, наявність звукових та світлових сигналів сприяє оперативному повідомленню про статус доступу та помилки, що підвищує ефективність реагування на події.

По-п'яте, система дозволяє адміністраторам керувати правами доступу, включаючи реєстрацію та видалення користувачів, зміну паролів та інші налаштування, що робить її гнучкою та пристосованою до потреб підприємства.

Усе це робить інтегровану систему RFID-ідентифікації ефективним інструментом для забезпечення безпеки на приватному підприємстві.

ВИСНОВОК

У відповідності до мети та завдання, в даній роботі отримані проєктні рішення з забезпечення інформаційної безпеки приватного підприємства шляхом інтеграції засобів безконтактної ідентифікації на базі технології RFID. Презентація роботи наведена в Додатку В.

У якості приватного підприємства прийнято зонований складський корпус, що потребує контролю доступу для автотранспортних засобів, території складського зберігання, побутових та офісних приміщень.

Використання RFID-засобів ідентифікації дозволили вирішити проблему авторизованого доступу для водійського та складського персоналу, а також представників бізнес-партнерів і адміністрації. Запропонована система контролю доступу дозволяє автоматизувати процедуру ідентифікації користувачів та скерувати відповідний сигнал на відкриття чи утримання закритим фізичного бар’єру (портальних воріт, турнікету чи дверей з електромеханічним замком).

Проєктні рішення з улаштування головного елементу RFID-СКУД, RFID-зчитувача виконані на базі технології Arduino з використанням мікропроцесору Arduino Nano та RFID-модуля RFID-RC522 (MFRC522). Ефективність проєктних рішень підтверджено на дослідному стенді.

Після інтеграції RFID-СКУД до загальної системи безпеки, спостереження і контроль за доступом стають більш точними і автоматизованими. Це допомагає уникнути несанкціонованого доступу, підвищує рівень безпеки об'єктів, і відповідно, зменшує ризики проникнення та порушення інформаційної безпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. Kassim S. O., Idriss A. S., Ahmed A. I. Implementation of a Sustainable Security Architecture using Radio Frequency Identification (RFID) Technology for Access Control. *arXiv preprint arXiv:2304.04628*. 2023. URL: https://doi.org/10.48550/arXiv.2304.04628 (date of access: 18.09.2023).

2. Khabarlak K. S., Koriashkina L. S. Mobile access control system based on rfid tags and facial information. *Bulletin of national technical university "khpi". series: system analysis, control and information technologies*. 2020. No. 2 (4). P. 69–74. URL: https://doi.org/10.20998/2079-0023.2020.02.12 (date of access: 18.09.2023).

3. Digital technologies' risks and opportunities: case study of an RFID system / M. Gallab et al. *Applied system innovation*. 2023. Vol. 6, no. 3. P. 54. URL: https://doi.org/10.3390/asi6030054 (date of access: 18.09.2023).

4. Vernikos, E. (2023). Investigating GDPR Compliance in European Telecommunication Industries by using ISOIEC 27001: 2013 and ISOIEC 27701: 2019 Standards. URL: https://www.diva-portal.org/smash/get/diva2:1771585/FULLTEXT02 (date of access: 18.09.2023).

5. Legal Requirements and Technical Metrics for Controlling Privacy of Employees' Location Data / U. Waldmann et al. *Mensch und Computer*. 2023. URL: https://doi.org/10.18420/muc2023-mci-ws11-364 (date of access: 18.09.2023).

6. Pal K. Security issues and solutions for resource-constrained iot applications using lightweight cryptography. *Cybersecurity issues, challenges, and solutions in the business world*. 2022. P. 138–159. URL: https://doi.org/10.4018/978-1-6684-5827-3.ch010 (date of access: 18.09.2023).

7. Tan W. C., Sidhu M. S. Review of RFID and IoT integration in supply chain management. *Operations research perspectives*. 2022. Vol. 9. P. 100229. URL: https://doi.org/10.1016/j.orp.2022.100229 (date of access: 18.09.2023).

8. Strahle M. I. *A Quantitative Survey Research Study Examining Predictors of Employees' Intentions to Accept Predictive Analytics for Insider Threat*

Monitoring (Doctoral dissertation, Capitol Technology University). 2022. URL: https://cutt.ly/8wcd9iuT (date of access: 18.09.2023).

9. A review of insider threat detection approaches with iot perspective / A. Kim et al. *IEEE access*. 2020. Vol. 8. P. 78847–78867. URL: https://doi.org/10.1109/access.2020.2990195 (date of access: 18.09.2023).

10. Design of protection of contactless identification system for ladles / D. Jančar et al. *39th meeting of departments of fluid mechanics and thermodynamics*, Horní Bečva, Czech Republic. 2023. URL: https://doi.org/10.1063/5.0128218 (date of access: 18.09.2023).

11. DIMAR: A contactless material identification algorithm for complex permittivity of dielectrics via moving RFID system / X. Liang et al. *IEEE transactions on instrumentation and measurement*. 2023. P. 1. URL: https://doi.org/10.1109/tim.2023.3309368 (date of access: 18.09.2023).

12. Zhou Z., Kumar A. Completely contactless and online finger knuckle identification for real world applications. *IEEE journal of selected topics in signal processing*. 2023. P. 1–14. URL: https://doi.org/10.1109/jstsp.2023.3254148 (date of access: 18.09.2023).

13. Use of numerical methods for the design of thermal protection of an rfid-based contactless identification system of ladles / D. Jančar et al. *Metals*. 2022. Vol. 12, no. 7. P. 1163. URL: https://doi.org/10.3390/met12071163 (date of access: 18.09.2023).

14. Contactless authentication for wearable devices using RFID / V. Bellandi et al. *2022 IEEE international conference on digital health (ICDH)*, Barcelona, Spain, 10–16 July 2022. 2022. URL: https://doi.org/10.1109/icdh55609.2022.00044 (date of access: 18.09.2023).

15. Unlocking the potential of near field communication in dentistry: identification, communication, and more / V. Narang et al. *Indian journal of dental sciences*. 2023. Vol. 15, no. 2. P. 88. URL: https://doi.org/10.4103/ijds.ijds_104_22 (date of access: 18.09.2023).

16. Dixit A., Sunori S. One Card For Every Payment And Identification Purpose Using Near-Field Communication (Nfc) Technology. *Elementary Education Online*.

2020. Vol. 20, no. 1. P. 7678–7678. URL: https://www.ilkogretim-online.org/?mno=130795 (date of access: 18.09.2023).

17. Contactless access control system based on voiceprint recognition / L. Zhang et al. *Advances in wireless communications and applications*. Singapore, 2022. P. 75–84. URL: https://doi.org/10.1007/978-981-19-3486-5_9 (date of access: 18.09.2023).

18. Smart Attendance for Faculty Monitoring System Using the Bluetooth Low Energy: Design and Implementation / S. R. Jantan et al. *Preprints* 2022, 2022110001. URL: https://doi.org/10.20944/preprints202211.0001.v1 (date of access: 18.09.2023).

19. Rajaram K., Amma N. G. B., Selvakumar S. Convolutional neural network based children recognition system using contactless fingerprints. *International journal of information technology*. 2023. URL: https://doi.org/10.1007/s41870-023-01306-7 (date of access: 18.09.2023).

20. Dong C., Kumar A. Synthesis of multi-view 3D fingerprints to advance contactless fingerprint identification. *IEEE transactions on pattern analysis and machine intelligence*. 2023. P. 1–18. URL: https://doi.org/10.1109/tpami.2023.3294357 (date of access: 18.09.2023).

21. Smart door access control system based on QR code / A. Jain et al. *International journal of informatics and communication technology (IJ-ICT)*. 2023. Vol. 12, no. 2. P. 171. URL: https://doi.org/10.11591/ijict.v12i2.pp171-179 (date of access: 18.09.2023).

22. Implantable QR code subcutaneous microchip using photoacoustic and ultrasound microscopy for secure and convenient individual identification and authentication / N. Wan et al. *Photoacoustics*. 2023. Vol. 31. P. 100504. URL: https://doi.org/10.1016/j.pacs.2023.100504 (date of access: 18.09.2023).

23. Szmolka S., Bras B., Ergincan O. Using a portable IR spectrometer for materials characterization and identification. *IOP conference series: materials science and engineering*. 2023. Vol. 1287, no. 1. P. 012034. URL: https://doi.org/10.1088/1757-899x/1287/1/012034 (date of access: 18.09.2023).

24. Implementation of artificial intelligence and non-contact infrared thermography for prediction and personalized automatic identification of different stages

of cellulite / J. Bauer et al. *EPMA journal*. 2020. URL: https://doi.org/10.1007/s13167-020-00199-x (date of access: 18.09.2023).

25. Ali M. L., Qiu M., Schmeelk S. Access control, biometrics, and the future. *IVSP 2023: 2023 5th international conference on image, video and signal processing*, Singapore Singapore. New York, NY, USA, 2023. URL: https://doi.org/10.1145/3591156.3591158 (date of access: 18.09.2023).

26. JosephNg P. S., BrandonChan P. S., Phan K. Y. Implementation of smart NFC door access system for hotel room. *Applied system innovation*. 2023. Vol. 6, no. 4. P. 67. URL: https://doi.org/10.3390/asi6040067 (date of access: 18.09.2023).

27. RiBAC: strengthening access control systems for pandemic risk reduction while preserving privacy / S. Krenn et al. *ARES 2023: the 18th international conference on availability, reliability and security*, Benevento Italy. New York, NY, USA, 2023. URL: https://doi.org/10.1145/3600160.3605039 (date of access: 18.09.2023).

28. Logeshwaran M., Sheela J. J. J. Contactless door system with temperature detection for covid-19. *2022 4th international conference on smart systems and inventive technology (ICSSIT)*, Tirunelveli, India, 20–22 January 2022. 2022. URL: https://doi.org/10.1109/icssit53264.2022.9716560 (date of access: 18.09.2023).

29. Kaur G., Singh A., Singh D. A comprehensive review on access control systems amid global pandemic. *2022 international conference on emerging trends in engineering and medical sciences (ICETEMS)*, Nagpur, India, 18–19 November 2022. 2022. URL: https://doi.org/10.1109/icetems56252.2022.10093551 (date of access: 18.09.2023).

30. Chowdhury A. M. M., Imtiaz M. H. Contactless fingerprint recognition using deep learning–a systematic review. *Journal of cybersecurity and privacy*. 2022. Vol. 2, no. 3. P. 714–730. URL: https://doi.org/10.3390/jcp2030036 (date of access: 18.09.2023).

31. Contactless palmprint recognition system: a survey / D. W. S. Alausa et al. *IEEE access*. 2022. P. 1. URL: https://doi.org/10.1109/access.2022.3193382 (date of access: 18.09.2023).

32. Dargan S., Kumar M. A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities. *Expert systems with applications*. 2020. Vol. 143. P. 113114. URL: https://doi.org/10.1016/j.eswa.2019.113114 (date of access: 18.09.2023).

33. Matsuda S., Yoshimura H. Personal identification with artificial intelligence under COVID-19 crisis: a scoping review. *Systematic reviews*. 2022. Vol. 11, no. 1. URL: https://doi.org/10.1186/s13643-021-01879-z (date of access: 18.09.2023).

34. Augmented security system for commercial buildings by manipulating object detection and admin panel / S. Brindha et al. *2022 international conference on communication, computing and internet of things (ic3iot)*, Chennai, India, 10–11 March 2022. 2022. URL: https://doi.org/10.1109/ic3iot53935.2022.9767997 (date of access: 18.09.2023).

35. Contactless and fine-grained liquid identification utilizing sub-6GHz signals / F. Shang et al. *IEEE transactions on mobile computing*. 2023. P. 1–16. URL: https://doi.org/10.1109/tmc.2023.3300356 (date of access: 18.09.2023).

36. Contactless palmprint recognition: a mini review / A. D. Wasiu et al. *Advances in intelligent applications and innovative approach*, Jaipur, India. 2023. URL: https://doi.org/10.1063/5.0149085 (date of access: 18.09.2023).

37. Face recognition system for automatic door access control / O. Ikponmwosa et al. *Engineering and technology journal*. 2023. Vol. 08, no. 02. P. 1981–1985. URL: https://doi.org/10.47191/etj/v8i2.03 (date of access: 18.09.2023).

38. IOT based contactless visitor approval and parcel sanitization system for COVID -19 / S. S. Koshe et al. *2022 international conference on connected systems & intelligence (CSI)*, Trivandrum, India, 31 August – 2 September 2022. 2022. URL: https://doi.org/10.1109/csi54720.2022.9924076 (date of access: 18.09.2023).

39. Artificial intelligence based optimal biometric security system using palm veins / K. K. Srinivas et al. *2022 international mobile and embedded technology conference (MECON)*, Noida, India, 10–11 March 2022. 2022. URL: https://doi.org/10.1109/mecon53876.2022.9752324 (date of access: 18.09.2023).

40. Access Control Cables and Wiring Diagram | Kisi. *Kisi | Cloud-Based Access Control & Security Platform*. URL: https://www.getkisi.com/guides/cables-and-wires (date of access: 18.09.2023).

41. LSL RFID Access Control System & Asset Tracking v4.1 | Linux Software Labs Inc. *Home | Linux Software Labs Inc*. URL: https://www.linux-software.com/node/49 (date of access: 18.09.2023).

42. Вебінар: «Огляд продуктів та рішень систем контролю доступу». *Компанія DEPS*. URL: https://deps.ua/ua/news/company-news/8031.html (дата звернення: 18.09.2023).

43. ISO/IEC 14443-1:2018. Cards and security devices for personal identification — Contactless proximity objects — Part 1: Physical characteristics. *ISO*. URL: https://www.iso.org/standard/73596.html (date of access: 18.09.2023).

44. ISO/IEC 15693-1:2018. Cards and security devices for personal identification — Contactless vicinity objects — Part 1: Physical characteristics. *ISO*. URL: https://www.iso.org/standard/70837.html (date of access: 18.09.2023).

45. ISO/IEC 18000-1:2008. Information technology — Radio frequency identification for item management — Part 1: Reference architecture and definition of parameters to be standardized. *ISO*. URL: https://www.iso.org/standard/46145.html (date of access: 18.09.2023).

46. ISO/IEC 7816-1:2011. Identification cards — Integrated circuit cards — Part 1: Cards with contacts — Physical characteristics. *ISO*. URL: https://www.iso.org/standard/54089.html (date of access: 18.09.2023).

47. NIST Publishes Special Publication (SP) 800-116 Revision 1, Guidelines for the Use of PIV Credentials in Facility Access. *NIST*. URL: https://www.nist.gov/news-events/news/2018/06/nist-publishes-special-publication-sp-800-116-revision-1-guidelines-use-piv (date of access: 18.09.2023).

48. EPCglobal | GS1. *GS1 | The Global Language of Business*. URL: https://www.gs1.org/epcglobal (date of access: 18.09.2023).

49. General data protection regulation (GDPR) – official legal text. *General Data Protection Regulation (GDPR)*. URL: https://gdpr-info.eu/ (date of access: 18.09.2023).

50. FIPS 201-3, Personal Identity Verification (PIV) of Federal Employees and Contractors | CSRC. *NIST Computer Security Resource Center | CSRC*. URL: https://csrc.nist.gov/pubs/fips/201-3/final (date of access: 18.09.2023).

51. ДСТУ EN 16656:2020 Інформаційні технології. Радіочастотна ідентифікація для керування предметами. Емблема RFID (EN 16656:2014, IDT; ISO/IEC 29160:2012, MOD). *БУДСТАНДАРТ Online - нормативні документи будівельної галузі України*. URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=90269 (дата звернення: 18.09.2023).

52. ДСТУ ISO/IEC 14443-1:2008 Картки ідентифікаційні. Картки на інтегрованих мікросхемах безконтактні. Картки близької взаємодії. Частина 1. Фізичні характеристики (ISO/IEC 14443-1:2000, IDT). *БУДСТАНДАРТ Online - нормативні документи будівельної галузі України*. URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=52942 (дата звернення: 18.09.2023).

53. ДСТУ ISO/IEC 15693-1:2008 Картки ідентифікаційні. Картки на інтегрованих мікросхемах безконтактні з розширеним радіусом дії. Частина 1. Фізичні характеристики (ISO/IEC 15693-1:2000, IDT). *БУДСТАНДАРТ Online - нормативні документи будівельної галузі України*. URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=96630 (дата звернення: 18.09.2023).

54. ДСТУ ISO/IEC 7816-1:2008. Картки ідентифікаційні. Картки на інтегрованих мікросхемах з контактами. Частина 1. Фізичні характеристики (ISO/IEC 7816-1:1998, IDT). *БУДСТАНДАРТ Online - нормативні документи будівельної галузі України*. URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=56483 (дата звернення: 18.09.2023).

55. ДСТУ ISO/IEC 10536-1:2008 Картки ідентифікаційні. Картки на інтегрованих мікросхемах безконтактні. Картки тісної взаємодії. Частина 1.

Фізичні характеристики (ISO/IEC 10536-1:2000, IDT). *БУДСТАНДАРТ Online - нормативні документи будівельної галузі України*. URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=96638 (дата звернення: 18.09.2023).

56. Carrapico H., Farrand B. 'Dialogue, partnership and empowerment for network and information security': the changing role of the private sector from objects of regulation to regulation shapers. *Crime, law and social change*. 2016. Vol. 67, no. 3. P. 245–263. URL: https://doi.org/10.1007/s10611-016-9652-4 (date of access: 28.09.2023).

57. Al-Harethi A. A. M., Al-Amoodi A. H. A. Organisational factors affecting information security management practices in private sector organisations. *International Journal of Psychology and Cognitive Science*. 2019. Vol. 5, no. 1, P. 9–23. https://cutt.ly/DwbgFz4g (date of access: 28.09.2023).

58. Bokhari S. A. A., Manzoor S. Impact of information security management system on firm financial performance: perspective of corporate reputation and branding. *American journal of industrial and business management*. 2022. Vol. 12, no. 05. P. 934–954. URL: https://doi.org/10.4236/ajibm.2022.125048 (date of access: 28.09.2023).

59. Shao X., Siponen M., Liu F. Shall we follow? Impact of reputation concern on information security managers' investment decisions. *Computers & security*. 2020. Vol. 97. P. 101961. URL: https://doi.org/10.1016/j.cose.2020.101961 (date of access: 28.09.2023).

60. Makridis C. A. Do data breaches damage reputation? Evidence from 45 companies between 2002 and 2018. *Journal of cybersecurity*. 2021. Vol. 7, no. 1. URL: https://doi.org/10.1093/cybsec/tyab021 (date of access: 28.09.2023).

61. Korczyński M., Noroozian A. Security Reputation Metrics. *arXiv preprint arXiv:2302.07172*. 2023. URL: https://doi.org/10.1007/978-3-642-27739-9_1625-1 (date of access: 28.09.2023).

62. Shaikh F. A., Siponen M. Information security risk assessments following cybersecurity breaches: the mediating role of top management attention to

cybersecurity. *Computers & security*. 2022. P. 102974. URL: https://doi.org/10.1016/j.cose.2022.102974 (date of access: 28.09.2023).

63. Singh N., Krishnaswamy V., Zhang J. Z. Intellectual structure of cybersecurity research in enterprise information systems. *Enterprise information systems*. 2022. P. 1–25. URL: https://doi.org/10.1080/17517575.2022.2025545 (date of access: 28.09.2023).

64. Cybersecurity enterprises policies: a comparative study / A. Mishra et al. *Sensors*. 2022. Vol. 22, no. 2. P. 538. URL: https://doi.org/10.3390/s22020538 (date of access: 28.09.2023).

65. Corallo A., Lazoi M., Lezzi M. Cybersecurity in the context of industry 4.0: a structured classification of critical assets and business impacts. *Computers in industry*. 2020. Vol. 114. P. 103165. URL: https://doi.org/10.1016/j.compind.2019.103165 (date of access: 28.09.2023).

66. Nabijonovna, B. F. Theoretical Foundations Of Private Entrepreneurship's Economic Security. *European Journal of Contemporary Business Law & Technology: Cyber Law, Blockchain, and Legal Innovations*. 2023. Vol. 1, no. 2. P. 1–4. URL: http://e-science.net/index.php/EJCBLT/article/view/85 (date of access: 28.09.2023).

67. Vivchar, O. I. Management system interpreting financial and economic security business in economic processes. *International electronic journal of mathematics education*. 2016. Vol. 11, no. 4. P. 947–959. URL: https://www.iejme.com/article/management-system-interpreting-financial-and-economic-security-business-in-economic-processes (date of access: 28.09.2023).

68. Avanesova N., Chuprin Y. Enterprise economic security: essential characteristics of the concept. *Innovative technologies and scientific solutions for industries*. 2017. No. 1 (1). P. 98–102. URL: https://doi.org/10.30837/2522-9818.2017.1.098 (date of access: 28.09.2023).

69. Ensuring economic security of enterprises taking into account the peculiarities of information security. *Philosophy, economics and law review*. 2022. Vol. 2, no. 1. URL: https://doi.org/10.31733/2786-491x-2022-1-96-107 (date of access: 28.09.2023).

70. Ju, J. Visualizing Zones: Defining the Notion of Zones in Physical Access Control for Security Management System. *DIVA*. 2023. URL: https://cutt.ly/Dwbg0UuM (date of access: 28.09.2023).

71. Parkinson S., Khan S. A survey on empirical security analysis of access-control systems: a real-world perspective. *ACM Computing Surveys*. 2022. Vol. 55, no. 6. P. 1–28. URL: https://doi.org/10.1145/3533703 (date of access: 28.09.2023).

72. Garbis J., Chapman J. W. Identity and access management. *Zero trust security*. Berkeley, CA, 2021. P. 71–91. URL: https://doi.org/10.1007/978-1-4842-6702-8_5 (date of access: 29.09.2023).

73. Integrated security management system for enterprises in industry 4.0 / S. Dotsenko et al. *Information & security: an international journal*. 2019. Vol. 43, no. 3. P. 294–304. URL: https://doi.org/10.11610/isij.4322 (date of access: 29.09.2023).

74. Jiangtao H. Discussion on the construction of substation security video surveillance system. *IOP conference series: materials science and engineering*. 2019. Vol. 563. P. 032004. URL: https://doi.org/10.1088/1757-899x/563/3/032004 (date of access: 29.09.2023).

75. Li Y. Research on Secure Interactive System of Video Surveillance Data. *2023 IEEE 12th International Conference on Communication Systems and Network Technologies (CSNT)*, Bhopal, India, 8–9 April 2023. 2023. URL: https://doi.org/10.1109/csnt57126.2023.10134670 (date of access: 29.09.2023).

76. Vahanova, I. M. Applying of measures for video surveillance on enterprises. 2018. URL: http://surl.li/lpknv (date of access: 29.09.2023).

77. Multi-Shot human re-identification for the security in video surveillance systems / B. HadjKacem et al. *2018 IEEE 27th international conference on enabling technologies: infrastructure for collaborative enterprises (WETICE)*, Paris, 27–29 June 2018. 2018. URL: https://doi.org/10.1109/wetice.2018.00046 (date of access: 29.09.2023).

78. Bandari, V. Enterprise Data Security Measures: A Comparative Review of Effectiveness and Risks Across Different Industries and Organization Types. *International Journal of Business Intelligence and Big Data Analytics*. 2022.

Vol. 6, no. 1. P. 1–11. URL: https://research.tensorgate.org/index.php/IJBIBDA/article/view/3 (date of access: 29.09.2023).

79. Chu, S. *The role of enterprise systems standardization on data breach occurrence* (Doctoral dissertation, University of British Columbia). 2023. URL: https://doi.org/10.14288/1.0430328 (date of access: 29.09.2023).

80. Enterprise data security compliance strategy: a study based on typical cases / Y. Xu et al. *SHS web of conferences*. 2023. Vol. 157. P. 03015. URL: https://doi.org/10.1051/shsconf/202315703015 (date of access: 29.09.2023).

81. Data breach management: an integrated risk model / F. Khan et al. *Information & management*. 2021. Vol. 58, no. 1. P. 103392. URL: https://doi.org/10.1016/j.im.2020.103392 (date of access: 29.09.2023).

82. Abbas J., Mahmood H. K., Hussain F. Information security management for small and medium size enterprises. *Sci. Int*, 2015. Vol. 27. P. 2393–2398. URL: https://cutt.ly/KwbhR4rC (date of access: 29.09.2023).

83. Soomro Z. A., Shah M. H., Ahmed J. Information security management needs more holistic approach: a literature review. *International journal of information management*. 2016. Vol. 36, no. 2. P. 215–225. URL: https://doi.org/10.1016/j.ijinfomgt.2015.11.009 (date of access: 29.09.2023).

84. Yildirim E. The importance of information security awareness for the success of business enterprises. *Advances in intelligent systems and computing*. Cham, 2016. P. 211–222. URL: https://doi.org/10.1007/978-3-319-41932-9_17 (date of access: 29.09.2023).

85. Cindana A., Ruldeviyani Y. Measuring information security awareness on employee using HAIS-Q: case study at XYZ firm. *2018 international conference on advanced computer science and information systems (ICACSIS)*, Yogyakarta, 27–28 October 2018. 2018. URL: https://doi.org/10.1109/icacsis.2018.8618219 (date of access: 29.09.2023).

86. Owusu Kwateng K., Amanor C., Tetteh F. K. Enterprise risk management and information technology security in the financial sector. *Information & computer*

security. 2022. URL: https://doi.org/10.1108/ics-11-2020-0185 (date of access: 29.09.2023).

87. Alshurideh M. T., Alzoubi H. M., Ghazal T. M. Risk Management Model for Telecom Enterprises Based on Variables (RM, SO, RC, SI) with Nature, Sense and Positive Psychology Hypothesis. *Journal for ReAttach Therapy and Developmental Diversities*. 2022. Vol. 5, no. 2s. P. 152–162. URL: https://www.jrtdd.com/index.php/journal/article/view/128 (date of access: 29.09.2023).

88. Preliminary risk assessment of regional industrial enterprise sites based on big data / Y. Jiang et al. *Science of the total environment*. 2022. P. 156609. URL: https://doi.org/10.1016/j.scitotenv.2022.156609 (date of access: 29.09.2023).

89. Asgary A., Ozdemir A. I., Özyürek H. Small and medium enterprises and global risks: evidence from manufacturing smes in Turkey. *International journal of disaster risk science*. 2020. Vol. 11, no. 1. P. 59–73. URL: https://doi.org/10.1007/s13753-020-00247-0 (date of access: 29.09.2023).

90. Sun H., Bai S. Enterprise information security management using internet of things combined with artificial intelligence technology. *Computational intelligence and neuroscience*. 2022. Vol. 2022. P. 1–16. URL: https://doi.org/10.1155/2022/7138515 (date of access: 08.10.2023).

91. Babii A., Samila A. Dual authentication technique for RFID access control systems with increased level of protection. *Security of infocommunication systems and internet of things*. 2023. No. 1. P. 01011. URL: https://doi.org/10.31861/sisiot2023.1.01011 (date of access: 08.10.2023).

92. Design and prototyping of a security locker system for public places using RFID technology / M. A. Sobur et al. *International journal of information technology*. 2022. Vol. 14, no. 1. P. 579–585. URL: https://doi.org/10.1007/s41870-021-00835-3 (date of access: 08.10.2023).

93. Duroc Y. From identification to sensing: RFID is one of the key technologies in the iot field. *Sensors*. 2022. Vol. 22, no. 19. P. 7523. URL: https://doi.org/10.3390/s22197523 (date of access: 08.10.2023).

94. Barriers to the implementation of radio frequency identification (RFID) for sustainable building in a developing economy / A. F. Kineber et al. *Sustainability*. 2023. Vol. 15, no. 1. P. 825. URL: https://doi.org/10.3390/su15010825 (date of access: 08.10.2023).

95. Converged security and information management system as a tool for smart city infrastructure resilience assessment / M. Hromada et al. *Smart cities*. 2023. Vol. 6, no. 5. P. 2221–2244. URL: https://doi.org/10.3390/smartcities6050102 (date of access: 08.10.2023).

96. Security framework for network-based manufacturing systems with personalized customization: an industry 4.0 approach / M. Hammad et al. *Sensors*. 2023. Vol. 23, no. 17. P. 7555. URL: https://doi.org/10.3390/s23177555 (date of access: 08.10.2023).

97. Environmental burden case study of RFID technology in logistics centre / B. Bukova et al. *Sensors*. 2023. Vol. 23, no. 3. P. 1268. URL: https://doi.org/10.3390/s23031268 (date of access: 08.10.2023).

98. Застосування систем контролю доступу та розробка макету приладу на основі RFID технології / А. Ю. Слободчук та ін. Вісник Національного технічного університету "ХПІ". Сер. : Електроенергетика та перетворювальна техніка = Bulletin of the National Technical University "KhPI". Ser. : Electricity and conversion technology : зб. наук. пр. – Харків : НТУ "ХПІ", 2019. № 1. С. 35–47. URL: https://repository.kpi.kharkov.ua/handle/KhPI-Press/49375 (дата звернення: 08.10.2023).

99. Слабінога М. О., Семків Р. Ю. Розробка апаратного та програмного забезпечення системи пропускного контролю на підприємствах. *Молодий вчений*, 2018. № 6(1). С. 19–22. URL: http://surl.li/lxvkl (дата звернення: 08.10.2023).

100. Нечипоренко О. В., Кравченко, П. В. Дослідження RFID-технологій в системах контролю доступу. *Сучасні технології в енергетиці, електромеханіці, системах управління та машинобудуванні: матеріали III Всеукраїнської науково-практичної інтернет-конференції, 29-30 листопада 2020 р.*, 120-121. URL: http://surl.li/lyfmd (дата звернення: 08.10.2023).

101. Юдін О. К., Весельська О. М. Аналіз та класифікація систем контролю та управління доступом на підприємстві. *Наукоємні технології*. 2018. № 2, С. 220–225. URL: http://surl.li/lyfmn (дата звернення: 08.10.2023).

102. Kim J., Lee D., Park N. CCTV-RFID enabled multifactor authentication model for secure differential level video access control. *Multimedia tools and applications*. 2020. Vol. 79, no. 31-32. P. 23461–23481. URL: https://doi.org/10.1007/s11042-020-09016-z (date of access: 09.10.2023).

103. Integration of RFID and image processing for surveillance abased security system / R. Pandey et al. *2023 3rd international conference on advance computing and innovative technologies in engineering (ICACITE)*, Greater Noida, India, 12–13 May 2023. 2023. URL: https://doi.org/10.1109/icacite57410.2023.10182987 (date of access: 09.10.2023).

104. Wahyudono B., Ogi D. Implementation of two factor authentication based on RFID and face recognition using LBP algorithm on access control system. *2020 international conference on ICT for smart society (ICISS)*, Bandung, Indonesia, 19–20 November 2020. 2020. URL: https://doi.org/10.1109/iciss50791.2020.9307564 (date of access: 09.10.2023).

105. Arduino - home. *Arduino - Home*. URL: https://www.arduino.cc/ (date of access: 09.10.2023).

106. IoT based RFID attendance monitoring system of students using arduino ESP8266 & adafruit.io on defined area / A. Shrivastava et al. *Cybernetics and systems*. 2023. P. 1–12. URL: https://doi.org/10.1080/01969722.2023.2166243 (date of access: 09.10.2023).

107. Rusyn V., Sambas A., Skiadas C. H. Security access using simple RFID reader and arduino UNO: a study case. *Lecture notes in networks and systems*. Cham, 2022. P. 193–202. URL: https://doi.org/10.1007/978-3-031-03877-8_17 (date of access: 09.10.2023).

108. RFID security access control system using 8051 microcontroller. *ElectronicsHub*. URL: https://www.electronicshub.org/rfid-security-access-control-system/ (date of access: 09.10.2023).

109. Interfacing RFID reader with arduino. *Circuit Digest - Electronics Engineering News, Latest Products, Articles and Projects*. URL: https://circuitdigest.com/microcontroller-projects/interfacing-rfid-reader-module-with-arduino (date of access: 09.10.2023).

110. Arduino RC522 RFID module based access control system. *ElectronicsHub*. URL: https://www.electronicshub.org/arduino-rc522-rfid-module-based-access-control-system/ (date of access: 09.10.2023).

111. RFID and keypad based security system using 8051 microcontroller. *Circuit Digest - Electronics Engineering News, Latest Products, Articles and Projects*. URL: https://circuitdigest.com/microcontroller-projects/rfid-based-security-system (date of access: 09.10.2023).

112. RFID based access control using arduino | full DIY project. *Electronics For You*. URL: https://www.electronicsforu.com/electronics-projects/rfid-based-access-control-using-arduino (date of access: 09.10.2023).

113. RFID based Attendance system using Arduino and External EEPROM - Activities - PCBway. *China PCB Prototype & Fabrication Manufacturer - PCB Prototype the Easy Way*. URL: https://www.pcbway.com/blog/Activities/RFID_based_Attendance_system_using_Arduino_and_External_EEPROM.html (date of access: 09.10.2023).

114. RFID based security system (AT89S52 + RFID). *Free Microcontroller Projects - 8051-AVR-PIC | Free Microcontroller Projects - 8051-AVR-PIC*. URL: http://www.8051projects.info/proj.php?ID=56 (date of access: 09.10.2023).

115. RFID RC522 attendance system using arduino with data logger. *How To Electronics*. URL: https://how2electronics.com/rfid-rc522-attendance-system-using-arduino/ (date of access: 09.10.2023).

116. Password based door lock system using 8051 microcontroller. *ElectronicsHub*. URL: https://www.electronicshub.org/password-based-door-lock-system-using-8051-microcontroller/ (date of access: 09.10.2023).

117. Instructables. RFID based door lock system using arduino uno. *Instructables*. URL: https://www.instructables.com/RFID-Based-Door-Lock-System-Using-Arduino-Uno/ (date of access: 09.10.2023).

118. RFID (MF-RC522) and arduino nano-based access control system / S. K. Agarwal et al. *Nanoelectronics, circuits and communication systems*. Singapore, 2020. P. 561–567. URL: https://doi.org/10.1007/978-981-15-2854-5_50 (date of access: 09.10.2023).

119. Intelligent access control system / M. Zhou et al. *2022 7th international conference on communication, image and signal processing (CCISP)*, Chengdu, China, 18–20 November 2022. 2022. URL: https://doi.org/10.1109/ccisp55629.2022.9974224 (date of access: 09.10.2023).

120. Intelligent security system in A campus building using RFID to improve security for elevator users / D. Desmira et al. *Elinvo (electronics, informatics, and vocational education)*. 2023. Vol. 8, no. 1. P. 1–7. URL: https://doi.org/10.21831/elinvo.v8i1.57848 (date of access: 09.10.2023).

121. ISO/IEC 18000-6:2010. Information technology — Radio frequency identification for item management — Part 6: Parameters for air interface communications at 860 MHz to 960 MHz. *ISO*. URL: https://www.iso.org/standard/46149.html (date of access: 09.10.2023).

122. Nano | arduino documentation. *Arduino Docs | Arduino Documentation*. URL: https://docs.arduino.cc/hardware/nano (date of access: 10.10.2023).

123. Mfrc522. *Automotive, IoT & Industrial Solutions | NXP Semiconductors*. URL: https://www.nxp.com/products/rfid-nfc/nfc-hf/nfc-readers/standard-performance-mifare-and-ntag-frontend:MFRC52202HN1 (date of access: 10.10.2023).

ДОДАТОК А

СТАТТЯ ЗА ТЕМОЮ КВАЛІФІКАЦІЙНОЇ РОБОТИ

УДК 004.056.52

DOI:

ТІТОВА ВІРА

Хмельницький національний університет

ORCID ID: 0000-0001-8668-4834

e-mail: titovav@khmnu.edu.ua

КЛЬОЦ ЮРІЙ

Хмельницький національний університет

ORCID ID: 0000-0002-3914-0989

e-mail: klots@khmnu.edu.ua

МОСТОВИЙ СЕРГІЙ

Хмельницький національний університет

ORCID ID: 0000-0002-9505-3206

e-mail: serhii.mostovyi@khmnu.edu.ua

КОЛІСНИК ВАДИМ

Хмельницький національний університет

e-mail: kolisnykvadim1712@gmail.com

СИСТЕМА КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ НА ОСНОВІ RFID-ТЕХНОЛОГІЙ

У статті розглядаються методи та особливості побудови системи контролю та управління доступом до захищених приміщень підприємства з використанням RFID-технологій. Проведено вибір компонентів контролю та управління доступом, сумісних з системами на базі мікроконтролерів Arduino. Наведено приклад практичного використання мікроконтролерів Arduino та RFID-технологій для контролю та управління доступом до захищених приміщень підприємства. Змодельовано систему контролю та управління доступом до

режимних об'єктів підприємства. Сформовано узагальнену схему управління системою та розроблено функційну схему контролю та управління доступом.

Ключові слова: система контролю та управління доступом, RFID-технології, структурна схема, функційна схема.

VIRA TITOVA, YURII KLOTS, SERHII MOSTOVYI, VADYM KOLISNYK

Khmelnitskyi National University

ACCESS CONTROL SYSTEM BASED ON RFID TECHNOLOGIES

Implementing security and preventing information leakage in an enterprise is one of the most important and significant problems in many enterprises nowadays. Traditional methods of personal identification, based on the use of passwords or physical media, such as a pass, passport, driver's license, do not always meet modern security requirements and require constant human involvement. One of the most developed and effective means of solving these problems is the use of automatic security alarm systems of various types. The automatic security alarm system is used when equipping various types of premises. At the same time, its purpose is to record any possibility of illegal entry into the protected premises or the protected territory. The basis of the security system is control sensors that transmit information to the central control point. At the same time, the security alarm can be not only autonomous, but also function in a complex with other security systems of the protected object. Automatic security alarm systems allow you to monitor the premises or territory 24 hours a day.

In this work, a system for managing access to the premises at the regime enterprise was developed, which in turn was implemented in the form of a mock-up. The authors conducted a study of the existing access control and management systems and identified the functions that are currently implemented in the ACS. Based on this, a goal was set, as well as requirements for system development were formed, and a conclusion was drawn about the need to develop a system with the lowest economic cost. A structural diagram of the ECU controller and a diagram of the functional structure of the system were

developed. The composition of the elements included in the structure of the system is also defined. Modeling was done using selected components and developed structural and functional schemes. Modeling made it possible to verify the correctness of the construction of the system structure and provided the possibility of developing an electrical schematic diagram.

Keywords: access control system, RFID technologies, structural diagram, functional diagram.

Постановка проблеми

Забезпечення безпеки та запобігання витоку інформації на об’єктах інформаційної діяльності є одним з найбільш важливих і критичних питань для багатьох організацій і підприємств на сьогоднішній день. Традиційні методи ідентифікації особистості, засновані на паролях і використанні матеріальних носіїв, таких як перепустки, паспорти і водійські права, не завжди відповідають сучасним вимогам безпеки і завжди вимагають втручання людини [1]. Одним з найбільш розвинених та ефективних засобів вирішення цих проблем є використання різних типів автоматизованих систем контролю та управління доступом (СКУД).

Автоматизовані СКУД використовуються на об'єктах різного типу. Їх призначення – виявлення можливого проникнення на об'єкт або на територію, що охороняються. Основою системи безпеки є датчик контролю, який передає інформацію на центральний пункт управління. При цьому системи безпеки бувають не тільки автономними, але й можуть працювати в комплексі з іншими системами безпеки на території, що охороняється.

Огляд існуючих рішень

У загальному вигляді СКУД можна представити як сукупність [1]: зчитувальних пристроїв, що здійснюють зчитування ідентифікаційних ознак; керованих перешкоджаючих пристроїв, що забезпечують фізичну перешкоду доступу та керуються за допомогою виконавчих пристроїв (турнікети, двері); виконавчих пристроїв, які забезпечують відкриття або закриття керованих

перешкоджаючих пристроїв (електромеханічні, електромагнітні замки, механізми приводу, турнікетів та шлагбаумів); підсистем управління (мікроконтролер), що виконують прийом та обробку інформації з пристроїв зчитування, проведення ідентифікації, надання або заборону доступу шляхом управління виконавчими пристроями, а також передачу інформації системі зберігання даних; системи зберігання даних, яка отримує від мікроконтролера дані та записує в постійний запам'ятовуючий пристрій (ПЗП), також система зберігає базу даних ідентифікаційних ознак.

На сьогоднішній день одними з відомих СКУД можна назвати системи від компанії ASSA ABLOY Global Solutions [2]. В основі архітектури таких систем закладено модульний принцип. Мається на увазі, що система складається з безлічі взаємозамінних приладів, що розподіляються по об'єкту, який захищається,. Усі прилади можуть бути з'єднані у мережу. Як транспортний рівень системи в основному використовуються RS-485-інтерфейс і мережі Ethernet.

До переваг цієї системи можна віднести рішення системою завдань для різних типів приміщень, а саме: реалізація обліку контролю переміщення персоналу на основі аналізу часу приходу/уходу співробітника з підприємства; реалізація безпеки підприємства шляхом інтеграції СКУД із системою пожежної сигналізації – система надає вільний доступ у разі виникнення пожежі.

Ще однією важливою перевагою цих систем є контролер доступу, який можна адаптувати до різних об'єктів компанії. Користувач сам визначає алгоритм роботи. Кожен контролер може обслуговувати двоє дверей і один зчитувач, одні двері і контроль напрямку проходу, турнікети, шлагбауми і шлюзи.

Недоліком системи є вартість обладнання, особливо якщо потрібно організувати контроль доступу на великих територіях. Якщо СКУД інтегрована з системами пожежної безпеки або іншими системами, потрібні додаткові заходи щодо захисту території (наприклад, відеоспостереження) для запобігання несанкціонованому доступу, відповідно витрати компанії збільшуються.

Ще одною відомою на ринку СКУД є компанія ZKTeco, яка пропонує як невеликі автономні системи, так і інтегровані рішення, які можуть об'єднувати різні

системи. Виробники компанії пропонують системи з різними вимогами до безпеки [3].

Перевагами систем ZKTeco є широкий спектр вирішуваних завдань, детальні та зрозумілі інструкції з встановлення та використання систем, безкоштовне програмне забезпечення, виробництво біометричних інструментів та широкий асортимент продукції. Система інтегрована з іншими виробничими підсистемами, що забезпечує масштабованість. Недоліком системи є висока вартість комплексу та окремого обладнання.

Аналіз існуючих аналогічних систем показує, що ці системи мають спільний недолік – високу вартість апаратного та програмного забезпечення. Тому потрібно підібрати елементи, необхідні для побудови системи, яка буде найменш дорогою, але не поступатиметься за функціональністю іншим існуючим системам.

Метою роботи є: розробка мікроконтролерної системи керування доступом до приміщень на режимному підприємстві з найменшою економічною вартістю.

Виклад основного матеріалу

Система контролю та управління доступом, що розробляється, повинна забезпечувати: вмикання/вимикання живлення системи; запис ідентифікаційних ключів в пам'ять системи та їх зберігання; подачу сигналу на відкривання керованого запобіжного пристрою при зчитуванні зареєстрованого в пам'яті системи ідентифікаційного ключа; подання сигналу на заборону відкривання керованого запобіжного пристрою при зчитуванні незареєстрованого в пам'яті системи ідентифікаційного ключа; повідомлення звуковим та світловим сигналом про отримання чи заборону доступу; автоматичне формування сигналу закриття на виконавчі пристрої за відсутності факту проходу; надання різних рівнів доступу; збереження ідентифікаційних ознак у пам'яті системи при обриві зв'язку із системою зберігання даних; фіксацію спроби несанкціонованого доступу у системі зберігання даних; передачу даних про надання доступу або його заборону в систему зберігання даних (до бази даних (БД)) та їх подальше зберігання; використання інтерфейсу RJ-45 та мережі Ethernet, як транспортного рівня системи.

Рівні доступу розділені відповідно до посади працівника. Менеджери та директори компанії мають необмежений доступ до приміщень та систем зберігання даних. Працівники поділяються на дві категорії прав: з високими та низькими привілеями. Працівники з низьким рівнем привілеїв мають доступ до зон вільного доступу компанії. Працівники з високим рівнем привілеїв мають доступ до деяких зон з обмеженим доступом на додаток до вищезазначених прав, але не мають доступу до систем зберігання даних. Відповідно до поставлених завдань та вимог, була розроблена структурна схема системи, як показано на рис. 1.

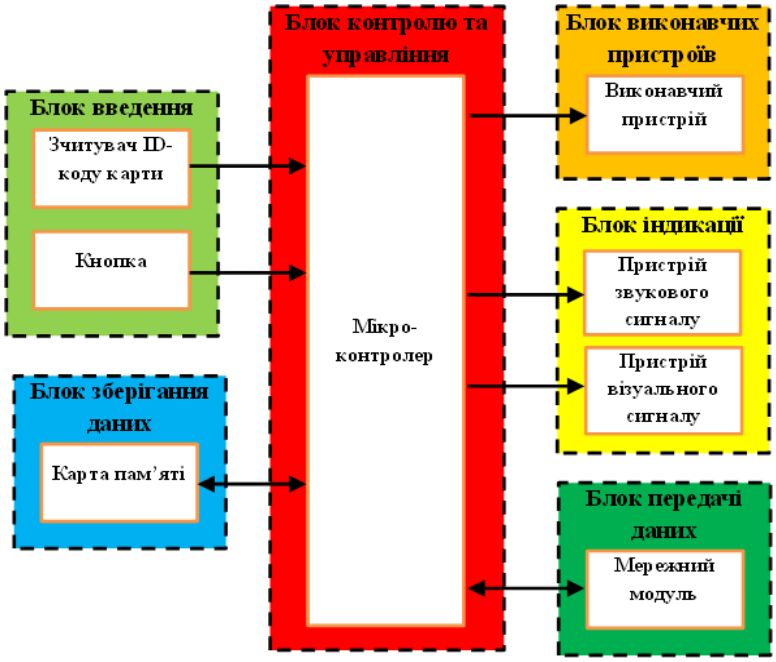


Рис. 1. Структурна схема системи контролю та управління доступом

Блок контролю та управління є "ядром" всієї системи і являє собою мікроконтролер (МК). МК отримує ідентифікаційні ключі або коди (ID-коди) від зчитувача. Потім він отримує доступ до системної карти пам'яті за умови отримання даних від зчитувача. Далі він приймає рішення на основі отриманих сигналів та даних і надсилає відповідні сигнали на виконавчий блок та блок індикації, а також надсилає необхідні дані на блок передачі даних.

Якщо МК знаходить необхідний ідентифікаційний код на карті пам'яті, тобто якщо відповідь позитивна, МК надсилає сигнал на виконавчий блок, який певним

чином активує звуковий та візуальний сигнальний пристрій у блоці індикації (лунає сигнал певного тону та тривалості, а також загоряється зелений індикатор). Потім МК надсилає ці дані до мережного модуля, звідки вони передаються в мережне середовище компанії.

Якщо МК не отримує позитивної відповіді, привід залишається в початковому стані, а блок індикації надсилає сигнал акустичному та візуальному обладнанню (лунає сигнал, що відрізняється за тональністю та тривалістю від попередньої версії, і загоряється червоний індикатор). Нарешті, МК надсилає на мережний модуль інформацію про спробу входу в зону за допомогою картки, ідентифікаційний код якої відсутній на карті пам'яті системи.

Кнопки використовуються для управління пристроями перешкод при необхідності виходу з приміщення і розміщуються біля дверей приміщення. Коли МК отримує сигнал від кнопки, МК сприймає його як вищезгадану позитивну відповідь.

Розроблена структурна схема дозволила визначити основні функційні модулі мікроконтролерної системи розроблюваної СКУД, реалізувати її функційні процеси та вибрати елементи, необхідні для складання системи.

На основі досліджень існуючих систем контролю та управління доступом [4-6], а також відповідно до вищезазначених вимог та розробленої структурної схеми визначено конфігурацію компонентів, необхідних для розроблюваної системи. Найбільш важливим та основоположним елементом є МК. В системі використовується мікроконтролер AVR Atmega328 фірми Atmel.

Як пристрій зчитування обраний RFID-зчитувач RC522 (рис. 2.а). Зі зчитувачами визначаються і мітки/ключі (магнітні карти). До виконавчих пристроїв належать електромагнітні замки, електромагнітні засувки та механізми приводу воріт або поворотної платформи, залежно від місця розташування системи на підприємстві. У даній СКУД електромагнітні замки обрані так, що система встановлюється для контролю доступу в приміщення через двері (рис 2.б.). В системі також необхідні елементи індикації для відображення статусу про надання доступу або його відмови. До таких відносяться світлодіоди та звуковипромінювачі

(зумери) (рис. 2.в). Для зберігання бази ІД-кодів використовується зовнішня пам'ять, а саме картка microSD з адаптером. Для взаємодії контролера з microSD карткою визначено модуль SD Card.

а) **б)** **в)**

Рис. 2. Складові елементи СКУД: а – зчитувач RFID-RC522, б – електромагнітний замок, в – модуль електромеханічного реле зі світлодіодами

Відповідно до розробленої структурної схеми та певного складу компонентів, розроблено функційну схему системи (рис. 3).

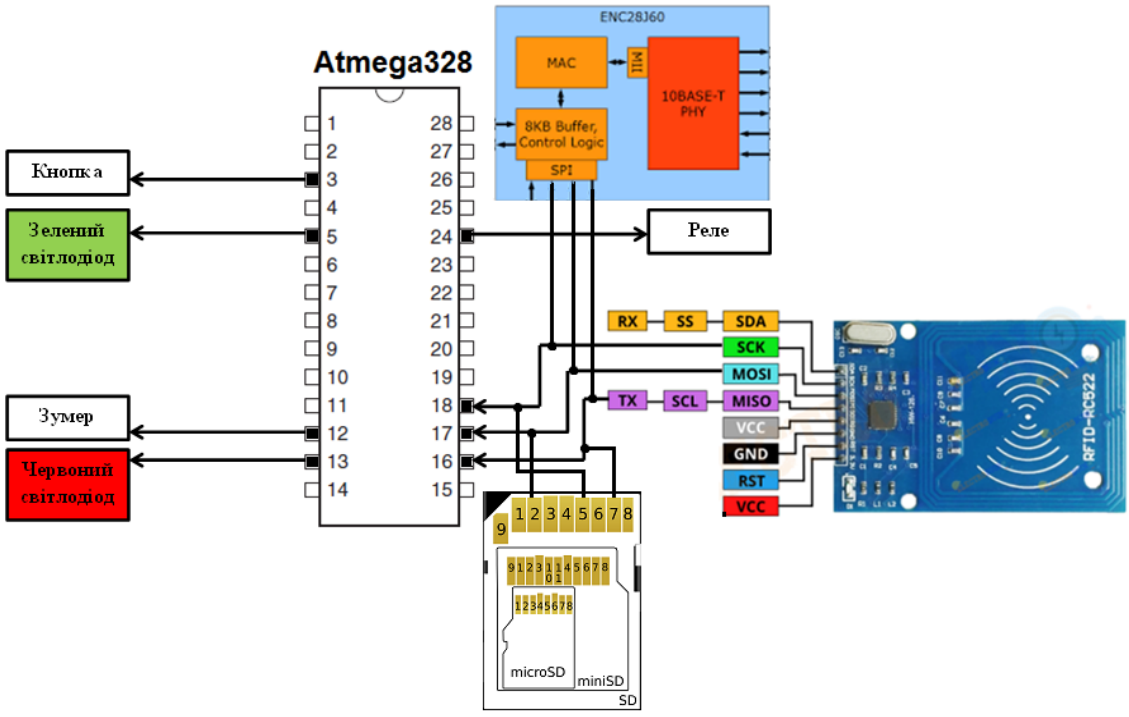


Рис. 3. Функційна схема системи контролю та управління доступом

Розроблена функційна схема дозволяє визначити алгоритми роботи системи,

створити модель працюючої системи та спроєктувати схеми блоків контролю та управління доступом.

Для моделювання системи на основі розробленої функційної схеми було створено натурну модель. На макетній платі було встановлено "ядро" системи - платформу Arduino Nano на базі AVR Atmega328 [7]. Далі за допомогою з'єднувальних проводів були підключені RFID-зчитувач, модуль SD-карти, Ethernet-модуль, світлодіоди, зумер і відповідні резистори, кнопки і сервоприводи, що використовуються в якості пристроїв безпеки. Після підключення живлення робота СКУД починається з процесу ініціалізації, під час якого активується програма, що зберігається в МК. Процес активного стану контролює стан зчитувача та кнопок. Коли картка підноситься до зчитувача, система реагує і, в залежності від того, чи є код картки в базі даних, МК вмикає відповідний світлодіод, зумер і реле (якщо доступ до картки дозволено). Сигнали світлодіода та зумера надалі називаються сигналами доступу. Коли сигнал зчитується з кнопки, сигнал також надсилається на зелений світлодіод, зумер та реле.

Алгоритм ідентифікації ID-коду картки, керування перешкоджаючим пристроєм, і відправлення даних на сервер по мережі:

Крок 1. Увімкнення живлення, запуск ініціалізації мікроконтролерної системи.

Крок 2. Очікування сигналів із блоку введення (зчитувач та кнопка).

Крок 3. Перевірка на наявність карти в області зчитувача. Якщо картка відсутня в області зчитувача, виконується крок 2. Інакше крок 4.

Крок 4. Зчитування коду картки.

Крок 5. Перевірка коду картки на відповідність до кодів у пам'яті системи. Якщо код знайдено, крок 6, інакше сигнали про заборону доступу (сигнал червоного світлодіода, звуковий сигнал) і перехід до кроку 8.

Крок 6. Сигнали про надання допуску (сигнал зеленого світлодіода та звуковий сигнал).

Крок 7. Відкриття запобіжного пристрою, затримка 5 секунд, закриття запобіжного пристрою.

Крок 8. Передача даних про подію на сервер по локальній мережі. На сервер передається ID-код прочитаної карти та статус.

Висновки

В ході дослідження було розроблено та впроваджено систему на основі RFID-технології для контролю та управління доступом до приміщення на режимному підприємстві, яка у свою чергу була реалізована у вигляді макета.

Авторами було проведено огляд існуючих систем контролю та управління доступом та визначено функції, які наразі реалізовані в СКУД. На цій основі були поставлені цілі, сформовані вимоги до розробки системи та зроблені висновки про необхідність розробки системи з найменшими економічними витратами. Створено структурну схему контролера СКУД та функційну структуру системи. Також було визначено склад елементів в структурі системи. Проведено моделювання з використанням обраних компонентів та розроблених структурної та функційної схем. Моделювання дозволило перевірити правильність обраної структури системи та є основою для подальшої розробки принципової схеми системи та її апаратної реалізації.

Розроблена система відповідає всім вимогам і має ряд переваг, серед яких низька вартість, компактність і простота використання в порівнянні з аналогічними продуктами. Система може бути використана як у загальному приватному секторі, так і в інформаційних установах з захищеними приміщеннями.

Література

1. Системи доступу: підручник/ Г. Г. Бортник, В. М. Кичак, О. В. Стальченко. Вінниця: ВНТУ, 2010. 298 с.

2. Системи контролю доступу ASSA ABLOY Global Solutions: [Електронний ресурс] – Режим доступу: https://www.assaabloyglobalsolutions.com/en/products

3. Системи контролю доступу ZKTeco: [Електронний ресурс] – Режим доступу: https://zktecoua.com/ua/solutions/skud/

4. Класифікація та аналіз загроз інформаційній безпеці в ключових системах інформаційної інфраструктури/ Ю. Васильєв// ДержНДІ Спецзв‘язку. 2015. С. 58-60.

5. Характеристика та загальні вимоги до системи контролю і управління доступом/ М.О. Омельченко// Сучасний захист інформації. 2020. №4 (44). С.46-50.

6. Аналіз та класифікація систем контролю та управління доступом на підприємстві/ О.К. Юдін, О.М. Весельська// Наукоємні технології. 2018. № 2 (38). С. 220-225.

7. Основи мікропроцесорної техніки/ В. С. Баран, Г. Г. Власюк, Ю. О. Оникієнко, О. І. Смоленська. КПІ ім. Ігоря Сікорського. Київ: КПІ ім. Ігоря Сікорського, 2019. 140 с.

References

1. Systemy dostupu: pidruchnyk/ H. H. Bortnyk, V. M. Kychak, O. V. Stalchenko. Vinnytsia: VNTU, 2010. 298 s.

2. Systemy kontroliu dostupu vid kompanii ASSA ABLOY Global Solutions: [Elektronnyi resurs] – Rezhym dostupu: https://www.assaabloyglobalsolutions.com/en/products

3. Systemy kontroliu dostupu ZKTeco: [Elektronnyi resurs] – Rezhym dostupu: https://zktecoua.com/ua/solutions/skud/

4. Klasyfikatsiia ta analiz zahroz informatsiinii bezpetsi v kliuchovykh systemakh informatsiinoi infrastruktury / Yu. Vasyliev// DerzhNDI Spetszv‘iazku. 2015. S. 58-60.

5. Kharakterystyka ta zahalni vymohy do systemy kontroliu i upravlinnia dostupom/ M.O. Omelchenko// Suchasnyi zakhyst informatsii. 2020. №4 (44). S.46-50.

6. Analiz ta klasyfikatsiia system kontroliu ta upravlinnia dostupom na pidpryiemstvi/ O.K. Yudin, O.M. Veselska// Naukoiemni tekhnolohii. 2018. № 2 (38). S. 220-225.

7. Osnovy mikroprotsesornoi tekhniky/ V. S. Baran, H. H. Vlasiuk, Yu. O. Onykiienko, O. I. Smolenska. KPI im. Ihoria Sikorskoho. Kyiv: KPI im. Ihoria Sikorskoho, 2019. 140 s.

ДОДАТОК Б

ЛІСТИНГ ПРОГРАМНОГО КОДУ

```
#define PIN_RELAY A 3 // Пін , до якого підключено реле
#define PIN_ BUZZER A 1 // Пін , до якого підключено буззер
// Підключення бібліотек для роботи з LCD за протоколом I2C
#include <Wire.h>
#include <LiquidCrystal_I2C.h>
LiquidCrystal_I2C lcd(0x27, 2, 1, 0, 4, 5, 6, 7, 3, POSITIVE);
// lcd.write ((uint8_t)0);
// Масиви користувацьких (нестандартних) символів для дисплея
uint8_t arrowUp [ 8] = {0x04, 0x0E, 0x1F, 0x04, 0x04, 0x04, 0x04, 0x00}; // Символ стрілки "вгору"
uint8_t arrowDown [ 8] = {0x04, 0x04, 0x04, 0x04, 0x1F, 0x0E, 0x04, 0x00}; // Символ стрілки "вниз"
#include < avr / pgmspace.h > // Бібліотека для зберігання рядків у флеш - пам'яті мікроконтролера
// Визначення текстових рядків меню у флеш -пам'яті мікроконтролера
const char menuStr_0[] PROGMEM = "ARDUINO ACCESS";
const char menuStr_1[] PROGMEM = "CONTROL SYSTEM";
const char menuStr_2[] PROGMEM = "Attach RFID-key";
const char menuStr_3[] PROGMEM = "Password:";
const char menuStr_4[] PROGMEM = "ACCESS ALOWED";
const char menuStr_5[] PROGMEM = "Lock after";
const char menuStr_6[] PROGMEM = "ACCESS DENIED";
const char menuStr_7[] PROGMEM = "Bad key/password";
const char menuStr_8[] PROGMEM = "EDIT RFID DATA";
const char menuStr_9[] PROGMEM = "AB #-ok *-esc";
const char menuStr_10[] PROGMEM = "EDIT< > [A]-add";
const char menuStr_11[] PROGMEM = "[C]-clear *-esc";
const char menuStr_12[] PROGMEM = "READING CARD UID";
const char menuStr_13[] PROGMEM = "Weating for card";
const char menuStr_14[] PROGMEM = "CARD IS DELETED";
const char menuStr_15[] PROGMEM = "FROM EEPROM";
const char menuStr_16[] PROGMEM = "ACCESS PASSWORD";
const char menuStr_17[] PROGMEM = "Set new access";
const char menuStr_18[] PROGMEM = "password:";
const char menuStr_19[] PROGMEM = "ADMIN PASSWORD";
const char menuStr_20[] PROGMEM = "Set new admin";
const char menuStr_21[] PROGMEM = "SET OPEN TIME";
const char menuStr_22[] PROGMEM = "Set open timer:";
// Створення таблиці рядків
```

```
const char* const menuStringTable[] PROGMEM = { menuStr_0, menuStr_1, menuStr_2, menuStr_3,
menuStr_4, menuStr_5, menuStr_6, menuStr_7,
menuStr_8, menuStr_9, menuStr_10, menuStr_11,
menuStr_12, menuStr_13, menuStr_14, menuStr_15,
menuStr_16, menuStr_17, menuStr_18, menuStr_19,
                                    menuStr_20, menuStr_21, menuStr_22};
// Масив- буффер для вилучення рядка та подальшої роботи з нею
char menuStringBuffer [ 16];
// Підключення бібліотеки для роботи з матричною клавіатурою
#include < Keypad.h >
#define ROWS 4 // Кількість рядів матричної клавіатури
#define COLS 4 // Кількість колонок матричної клавіатури
//Масив-карта матричної клавіатури
char keys [ ROWS ][ COLS ] = {
{'1','2','3','A'},
{'4','5','6','B'},
{'7','8','9','C'},
{'*','0','#','D'}
};
byte rowPins [ ROWS ] = {A0, 8, 7, 6}; // Підключення до Arduino рядів матричної клавіатури
byte colPins [ COLS ] = {5, 4, 3, 2}; // Підключення до Arduino колонок матричної клавіатури
Keypad keypad = Keypad ( makeKeymap ( keys ), rowPins , colPins , ROWS , COLS ); // Примірник класу
// Підключення бібліотек для роботи з RFID -модулем RC522
#include <SPI.h>
#include <MFRC522.h>
#define PIN_SS 10
#define PIN_RST 9
MFRC522 mfrc522( PIN_SS , PIN_RST ); // Створення екземпляра класу для модуля RC522
/* ГЛОБАЛЬНІ ЗМІННІ ТА Прапори */
bool flagClearMenuScreen = true ;
uint32_t openTime = 5; // Час, через який закриється замок його відкриття
uint8_t tempPassword [ 7] = {0, 0, 0, 0, 0, 0, 0}; // Масив для тимчасового зберігання введеного пароля
int passwordIndex = -1; // Індекс цифри пароля, з якою ми зараз працюємо
char key ; // Змінна для зберігання коду натиснутої кнопки
uint8_t cards [ 30] [5]; // Масив для зберігання ідентифікаторів RFID -карт
uint8_t cardsIndex = 0; // Індекс для роботи з конкретною RFID -карткою
uint8_t accessPassword [ 7] = {7, 6, 5, 4, 3, 2, 1}; // Пароль доступу за замовчуванням
```

```
uint8_t adminPassword [ 7] = {1, 2, 3, 4, 5, 6, 7}; // Пароль адміністратора за замовчуванням
uint8_t menuFlag = 0; // Номер екрану меню
uint8_t globalState = 0; // Глобальний стан системи (для реалізації кінцевого автомата)
uint32_t cardWeatingTime ; // Час очікування картки для реєстрації
// Бібліотека для роботи з енергонезалежною пам'яттю EEPROM
#include < EEPROM.h >
/* ФУНКЦІЯ ІНІЦІАЛІЗАЦІЇ ЕНЕРГОНЕЗАЛЕЖНОЇ ПАМ'ЯТІ */
void initEEPROM ( ) {
// Якщо ми запускаємо програму вперше (за цей контроль відповідатиме комірка №500)
  if ( EEPROM.read (500) != 84) { // Число 84, як ознака первинного запуску
// Ініціалізуємо нулями комірки, відповідальні за ознаку зберігання значень карт
    for(uint8_t i = 0; i < 30; i++) {
      EEPROM.write ((i * 5), 0);
}
// Записуємо пароль доступу та адміністратора за замовчуванням
    for(uint8_t i = 0; i < 7; i++) {
EEPROM.write(i + 150, accessPassword[i]);
EEPROM.write(i + 157, adminPassword[i]);
    }
    EEPROM.write (164, openTime ); // Запис за замовчуванням часу утримання замка у відкритому стані
    EEPROM.write (500, 84); // Запис ознаки першого запуску програми
}
  else { // Якщо програма запускається не вперше, читаємо дані з EEPROM
    for(uint8_t i = 0; i < 7; i++) {
accessPassword[i] = EEPROM.read(i + 150);
adminPassword[i] = EEPROM.read(i + 157);
}
openTime = EEPROM.read(164);
for(uint8_t i = 0; i < 30; i++) {
cards[i][0] = EEPROM.read(i * 5);
cards[i][1] = EEPROM.read(i * 5 + 1);
cards[i][2] = EEPROM.read(i * 5 + 2);
cards[i][3] = EEPROM.read(i * 5 + 3);
cards[i][4] = EEPROM.read(i * 5 + 4);
    }
}
}

/*
```

КАРТА ПАМ'ЯТІ EEPROM

[порядковий номер карти][(ідентифікатор порожнього комірки 0-порожня; 1-записана), (біт UID0), (біт UID1), (біт UID2), (біт UID3)]

Карти розміщуються за такими адресами:

Карта №01 - 0000 , 0001, 0002, 0003, 0004
Карта №02 - 0005 , 0006, 0007, 0008, 0009
Карта №03 - 0010 , 0011, 0012, 0013, 0014
Карта №04 - 0015 , 0016, 0017, 0018, 0019
Карта №05 - 0020 , 0021, 0022, 0023, 0024
Карта №06 - 0025 , 0026, 0027, 0028, 0029
Карта №07 - 0030 , 0031, 0032, 0033, 0034
Карта №08 - 0035 , 0036, 0037, 0038, 0039
Карта №09 - 0040 , 0041, 0042, 0043, 0044
Карта №10 - 0045 , 0046, 0047, 0048, 0049
Карта №11 - 0050 , 0051, 0052, 0053, 0054
Карта №12 - 0055 , 0056, 0057, 0058, 0059
Карта №13 - 0060 , 0061, 0062, 0063, 0064
Карта №14 - 0065 , 0066, 0067, 0068, 0069
Карта №15 - 0070 , 0071, 0072, 0073, 0074
Карта №16 - 0075 , 0076, 0077, 0078, 0079
Карта №17 - 0080 , 0081, 0082, 0083, 0084
Карта №18 - 0085 , 0086, 0087, 0088, 0089
Карта №19 - 0090 , 0091, 0092, 0093, 0094
Карта №20 - 0095 , 0096, 0097, 0098, 0099
Карта №21 - 0100 , 0101, 0102, 0103, 0104
Карта №22 - 0105 , 0106, 0107, 0108, 0109
Карта №23 - 0110 , 0111, 0112, 0113, 0114
Карта №24 - 0115 , 0116, 0117, 0118, 0119
Карта №25 - 0120 , 0121, 0122, 0123, 0124
Карта №26 - 0125 , 0126, 0127, 0128, 0129
Карта №27 - 0130 , 0131, 0132, 0133, 0134
Карта №28 - 0135 , 0136, 0137, 0138, 0139
Карта №29 - 0140 , 0141, 0142, 0143, 0144
Карта №30 - 0145 , 0146, 0147, 0148, 0149
Інше:

Пароль доступу: 0150, 0151, 0152, 0153, 0154, 0155, 0156

Пароль адміна: 0157 , 0158, 0159, 0160, 0161, 0162, 0163

Час утримання замку у відкритому стані: 0164

*/

```
/* ФУНКЦІЯ ЧИТАННЯ ДАНИХ ПРО ЗАПИСАНІ КАРТИ З EEPROM */
void readCardBaseFromEEPROM ( ) {
// Заповнюємо масив нульовими значеннями
  for(uint8_t i = 0; i < 30; i++) {
for(uint8_t j = 0; j < 5; j++) {
```

```
        cards [i] [j] = 0;
      }
      }
      // Читання даних з EEPROM та заповнення масиву
        for(int i = 0; i < 30; i++) {
      if(EEPROM.read((i * 5)) == 0) {
      cards[i][0] = 0;
      cards[i][1] = 0;
      cards[i][2] = 0;
      cards[i][3] = 0;
      cards[i][4] = 0;
      }
      else {
      cards[i][0] = EEPROM.read((i * 5));
      cards[i][1] = EEPROM.read((i * 5 + 1));
      cards[i][2] = EEPROM.read((i * 5 + 2));
      cards[i][3] = EEPROM.read((i * 5 + 3));
      cards[i][4] = EEPROM.read((i * 5 + 4));
         }
      }
      }
      /* ФУНКЦІЯ СКАНУВАННЯ ПІДНЕСЕННОЇ ДО ТЕРМІНАЛУ КАРТИ-АБО КЛЮЧА */
      // Повернення значень: 1-ключ підходить; 2-ключ відсутня в базі
      void compareCardWithDataBase(bool resetArray = true) {
      if(!mfrc522.PICC_IsNewCardPresent()) return 0;
      if(!mfrc522.PICC_ReadCardSerial()) return 0;
        // Скануємо піднесену карту та порівнюємо її з одою з карт, внесених до бази
        for(int i = 0; i < 30; i++) {
      if((cards[i][1] == mfrc522.uid.uidByte[0]) &&
      (cards[i][2] == mfrc522.uid.uidByte[1]) &&
      (cards[i][3] == mfrc522.uid.uidByte[2]) &&
      (cards[i][4] == mfrc522.uid.uidByte[3])) {
      globalState = 3; return 0;
      }
      else globalState = 4;
      }
      }
      /* ФУНКЦІЯ ВИВОДУ РЯДКІВ З ФЛЕШ - ПАМ'ЯТІ МІКРОКОНТРОЛЕРА У ВИЗНАЧЕНІ КООРДИНАТИ РКІ */
      void flashStringToLcd(uint8_t x, uint8_t y, uint8_t stringNumber) {
      strcpy_P(menuStringBuffer,
(char*)pgm_read_word(&(menuStringTable[stringNumber])));
      lcd.setCursor(x, y);
```

```
lcd.print(menuStringBuffer);
}
/* ФУНКЦІЯ ПОДАЧІ ЗВУКОВОГО СИГНАЛУ */
void beep(int l, uint8_t p) {
for(int i = 0; i < l; i++) {
digitalWrite(PIN_BUZZER, HIGH);
delay (p);
digitalWrite(PIN_BUZZER, LOW);
delay (p);
}
}
/* ФУНКЦІЯ СКИДАННЯ БУФФЕРНОГО ПАРОЛЮ */
void resetTempPassword() {
for(uint8_t i = 0; i < 7; i++) tempPassword[i] = 0;
  passwordIndex = -1;
}
/* ФУНКЦІЯ ВИВОДУ КОРОТКОТРИВАЛОЇ ІНФОРМАЦІЇ, ЩО ГОВОРИТЬ ПРО ПОМИЛКУ ДОСТУПУ */
void accesDenied() {
for(uint8_t i = 0; i < 3; i++) {
beep(100, 1);
flashStringToLcd(1, 0, 6); // ACCESS DENIED!
flashStringToLcd(0, 1, 7); // Bad key/password
   delay ( 500);
   lcd.clear ();
}
}
/* ФУНКЦІЯ ВІДКРИТТЯ ЕЛЕКТРОЗАМКА ПРИ ПРАВИЛЬНОМУ КОДІ ДОСТУПУ */
void accessAllowed() {
static uint8_t localState = 0;
static uint8_t counter = openTime;
if(localState == 0) {
beep(100, 1);
   digitalWrite( PIN_RELAY, HIGH); // Вимкнемо реле , відкриваємо електрозамок
flashStringToLcd(1, 0, 4); // ACCESS ALOWED
flashStringToLcd(0, 1, 5); // Lock after
localState = 1;
}
else if(localState == 1) {
lcd.setCursor(11, 1);
lcd.print(counter);
lcd.print("sec");
```

```
localState = 2;
}
else if(localState == 2) {
if(millis() % 1000 == 0) {
counter--;
if(counter == 0) localState = 3; else localState = 1;
}
}
else if(localState == 3) {
   digitalWrite( PIN_RELAY, LOW); // Закриваємо замок по закінченні часу
lcd.clear();
counter = openTime;
globalState = 0;
localState = 0;
}
}
/* ФУНКЦІЯ ВВЕДЕННЯ ПАРОЛЮ */
bool enterPassword() {
  if ( key == '*') { // Стираємо пароль
    for(uint8_t i = 0; i < 7; i++) tempPassword[i] = 0;
passwordIndex = -1;
lcd.setCursor(9, 1); lcd.print(" ");
}
else if(key == '#') {
Serial.println("ENTER");
if(passwordIndex == 6) return 1;
}
else {
lcd.setCursor(passwordIndex + 10, 1);
if(passwordIndex <= 6) {
lcd.print(key);
if(passwordIndex == 6) { lcd.setCursor(15, 1); lcd.print(key); }
if(passwordIndex < 6) passwordIndex++;
tempPassword[passwordIndex] = (key - 48); // Заносимо черговий символ в тимчасовий масив
}
}
return 0;
}
/* ФУНКЦІЯ Відображення МЕНЮ * /
void showMenu(uint8_t menuIndex) {
if(flagClearMenuScreen) { lcd.clear(); flagClearMenuScreen = false; }
switch(menuIndex) {
case 0:
```

```
flashStringToLcd(0, 0, 2); // Attach RFID-key
flashStringToLcd(0, 1, 3); // Password:
break;
case 10:
flashStringToLcd(0, 0, 8); // EDIT RFID DATA
flashStringToLcd(0, 1, 9); // AB #-ok *-esc
    lcd.setCursor (1, 1); lcd.write((uint8_t)1); // Стрілка вгору
    lcd.setCursor (4, 1); lcd.write((uint8_t)2); // Стрілка вниз
break;
case 101:
lcd.setCursor(0, 0);
lcd.print("<");
if(cardsIndex < 10) lcd.print("0");
lcd.print(cardsIndex);
lcd.print(">-");
if(cards[cardsIndex][0] == 0) lcd.print("empty");
else {
lcd.print(cards[cardsIndex][1], HEX); lcd.print(":");
lcd.print(cards[cardsIndex][2], HEX); lcd.print(":");
lcd.print(cards[cardsIndex][3], HEX); lcd.print(":");
lcd.print(cards[cardsIndex][4], HEX);
}
flashStringToLcd(0, 1, 9); // AB #-ok *-esc
      lcd.setCursor (1, 1); lcd.write((uint8_t)1); // Стрілка вгору
      lcd.setCursor (4, 1); lcd.write((uint8_t)2); // Стрілка вниз
break;
case 102:
lcd.setCursor(0, 0);
lcd.print("EDIT<");
if(cardsIndex < 10) lcd.print("0");
lcd.print(cardsIndex);
lcd.print(">[A]-add");
lcd.setCursor(0, 1);
lcd.print("[C]-clear *-esc");
break;
case 103:
lcd.setCursor(0, 0); lcd.print("READING CARD UID");
lcd.setCursor(0, 1); lcd.print("Weating for card");
break;
case 11:
flashStringToLcd(0, 0, 16); // ACCESS PASSWORD
flashStringToLcd(0, 1, 9); // AB #-ok *-esc
    lcd.setCursor (1, 1); lcd.write((uint8_t)1); // Стрілка вгору
    lcd.setCursor (4, 1); lcd.write((uint8_t)2); // Стрілка вниз
```

```
        break;
        case 111:
        flashStringToLcd(0, 0, 17); // Set new access
        flashStringToLcd(0, 1, 18); // password:
        break;
        case 12:
        flashStringToLcd(0, 0, 19); // ADMIN PASSWORD
        flashStringToLcd(0, 1, 9); // AB #-ok *-esc
            lcd.setCursor (1, 1); lcd.write((uint8_t)1); // Стрілка вгору
            lcd.setCursor (4, 1); lcd.write((uint8_t)2); // Стрілка вниз
        break;
        case 121:
        flashStringToLcd(0, 0, 20); // Set new admin
        flashStringToLcd(0, 1, 18); // password:
        break;
        case 13:
        flashStringToLcd(0, 0, 21); // SET OPEN TIME
        flashStringToLcd(0, 1, 9); // AB #-ok *-esc
            lcd.setCursor (1, 1); lcd.write((uint8_t)1); // Стрілка вгору
            lcd.setCursor (4, 1); lcd.write((uint8_t)2); // Стрілка вниз
        break;
        case 131:
        flashStringToLcd(0, 0, 22); // Set open timer:
        lcd.setCursor(0, 1); lcd.print(">"); lcd.print(openTime); lcd.print("sec");
            break ;
        }
        }
        /* ФУНКЦІЯ ПОПЕРЕДНІХ УСТАНОВОК */
        void setup ( ) {
          Serial.begin (9600);
        // Ініціалізація апаратного SPI та параметрів модуля RC522
          SPI.begin();
        mfrc522.PCD_Init();
        mfrc522.PCD_ SetAntennaGain( mfrc522.RxGain_max); // Максимальне
посилення антени модуля
          lcd.begin (16, 2); // Ініціалізація дисплея 16x2
          lcd.createChar (1, arrowUp ); // Створення символу стрілки "вгору"
          lcd.createChar (2, arrowDown ); // Створення символу стрілки "вниз"
          pinMode( PIN_RELAY, OUTPUT); digitalWrite(PIN_RELAY, LOW); //
Знеструмлюємо реле
          // Виведення привітання на дисплеї
          flashStringToLcd ( 1, 0, 0); flashStringToLcd (1, 1, 1);
        // Генерація короткого звукового сигналу
          pinMode ( PIN_BUZZER , OUTPUT );
```

```
  beep ( 500, 2);
  lcd.clear ();
  initEEPROM ( ); // Ініціалізація бази даних RFID- ключів
 }
 /* ОСНОВНИЙ ЦИКЛ ПРОГРАМИ */
 void loop ( ) {
  while ( 1) {
    key = keypad.getKey (); // Читання коду натиснутої клавіші
 // Відображаємо головний екран із запрошенням введення пароля або піднесення карти
    if ( globalState == 0) {
     showMenu ( 0);
     globalState = 1;
 }
 // Обробляємо введення пароля або піднесення RFID- ключа
    else if ( globalState == 1) {
 // Обробляємо піднесений до терміналу RFID- ключ
     compareCardWithDataBase ( );
 // Обробляємо введення пароля на матричній клавіатурі
     if(key) {
 if(enterPassword()) { lcd.clear(); globalState = 2; }
     }
 }
 // Перевірка на правильність введення пароля
    else if ( globalState == 2) {
 // Якщо введено пароль доступу до об'єкта
     if((tempPassword[0] == accessPassword[0]) && (tempPassword[1] == accessPassword[1]) &&
 (tempPassword[2] == accessPassword[2]) && (tempPassword[3] == accessPassword[3]) &&
 (tempPassword[4] == accessPassword[4]) && (tempPassword[5] == accessPassword[5]) &&
 (tempPassword[6] == accessPassword[6])) { lcd.clear(); globalState = 3; }
     // Якщо введено пароль доступу в меню адміністратора
     else if((tempPassword[0] == adminPassword[0]) && (tempPassword[1] == adminPassword[1]) &&
 (tempPassword[2] == adminPassword[2]) && (tempPassword[3] == adminPassword[3]) &&
 (tempPassword[4] == adminPassword[4]) && (tempPassword[5] == adminPassword[5]) &&
 (tempPassword[6] == adminPassword[6])) { lcd.clear(); globalState = 100; menuFlag = 10;}
     // Якщо пароль не відповідає жодному із зарезервованих у системі
     else {
```

```
        // Ідемо у стан обробки помилки
              globalState = 4;
        }
             resetTempPassword ( ); // Скидаємо буфер тимчасового пароля
        }
        // Відкриваємо елетрозамок на визначений у меню час
           else if( globalState == 3) { accessAllowed(); } // Функція відкриття замку
             // Виведення помилки при наборі неправильного пароля або незареєстрованого ключа
           else if ( globalState == 4) {
             accesDenied ( ); // Функція виведення помилки доступу
             globalState = 0; // Повернення до початкового меню робочого режиму
        }
        // Головне меню адміністратора
           else if ( globalState == 100) {
             showMenu ( menuFlag );
             globalState = 101;
        }
        // Обробка клавіатури у головному меню адміністратора
           else if(globalState == 101) {
        if(key) {
              if ( key == 'A') { // Гартуємо вгору головне меню адміністратора
                key = 'n';
        menuFlag--;
        if(menuFlag < 10) menuFlag = 13;
                globalState = 100;
        }
              else if ( key == 'B') { // Гартуємо вниз головне меню адміністратора
                key = 'n';
        menuFlag++;
        if(menuFlag > 13) menuFlag = 10;
        globalState = 100;
        }
        else if( key == '*') { // Вихід в робітник режим
        key = 'n';
                globalState = 0;
        }
              else if ( key == '#') { // Натискання ОК в одному з пунктів головного меню
                switch ( menuFlag ) { // Перевіряємо, в якому саме пункті ми натиснули ОК
                   Case 10: globalState = 110; карткиIndex = 0; break;
        Case 11: globalState = 120; break;
        Case 12: globalState = 130; break;
        Case 13: globalState = 140; break;
```

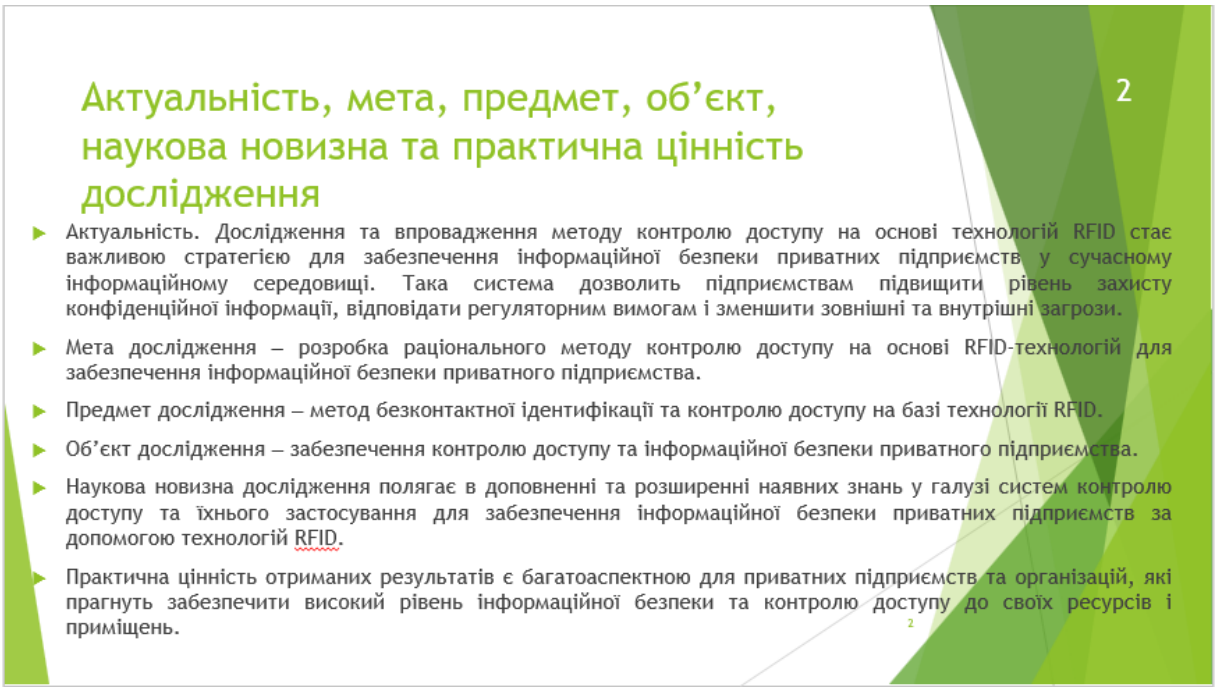
```
        }
}
      lcd.clear ();
}
}
// Переходимо в режим перегляду зареєстрованих у системі карток
   else if(globalState == 110) { showMenu(101); globalState = 111; }
   else if ( globalState == 111) {
// Обробляємо введення пароля на матричній клавіатурі
     if ( key ) {
      if ( key == 'A') { // Гартуємо вгору список RFID- ключів
        key = 'n';
карткиIndex--;
if(cardsIndex == 255) cardsIndex = 29;
globalState = 110;
}
else if( key == 'B') { // Гартуємо вниз список RFID- ключів
key = 'n';
cardsIndex++;
if(cardsIndex > 29) cardsIndex = 0;
globalState = 110;
}
else if( key == '*') { // Вихід в робітник режим
карткиIndex = 0;
globalState = 100;
}
else if(key == '#') {
        globalState = 112;
}
      lcd.clear ();
}
}
// Переходимо в підменю редагування запису про RFID -ключ
   else if(globalState == 112) { showMenu(102); globalState = 113;}
   else if ( globalState == 113) {
// Визначаємо, що робити з обраним записом
     if(key) {
if(key == '*') { globalState = 110; }
else if(key == 'C') {
cards[cardsIndex][0] = 0;
cards[cardsIndex][1] = 0;
cards[cardsIndex][2] = 0;
cards[cardsIndex][3] = 0;
cards[cardsIndex][4] = 0;
```

```
// Видаляємо карту з EEPROM
EEPROM.write(cardsIndex * 5, 0);
EEPROM.write(cardsIndex * 5 + 1, 0);
EEPROM.write(cardsIndex * 5 + 2, 0);
EEPROM.write(cardsIndex * 5 + 3, 0);
EEPROM.write(cardsIndex * 5 + 4, 0);
lcd.clear(); lcd.setCursor(0, 0); lcd.print("RFID-key cleared");
delay (2000);
globalState = 110;
}
else if(key == 'A') {
globalState = 114;
}
lcd.clear();
}
}
else if(globalState == 114) {
showMenu(103);
cardWeatingTime = millis();
globalState = 115;
}
// Чекаємо піднесення RFID- ключа до терміналу для наступною реєстрації
else if(globalState == 115) {
if((millis() - cardWeatingTime) > 10000) {
beep(100, 1);
lcd. clear();
globalState = 110;
}
if(!mfrc522.PICC_IsNewCardPresent()) return 0;
if(!mfrc522.PICC_ReadCardSerial()) return 0;
beep(100, 1);
cards[cardsIndex][0] = 1;
cards[cardsIndex][1] = mfrc522.uid.uidByte[0];
cards[cardsIndex][2] = mfrc522.uid.uidByte[1];
cards[cardsIndex][3] = mfrc522.uid.uidByte[2];
cards[cardsIndex][4] = mfrc522.uid.uidByte[3];
    // Запис ідентифікатора ключа в EEPROM
    EEPROM.write ( cardsIndex * 5, 1);
    EEPROM.write(cardsIndex * 5 + 1, cards[cardsIndex][1]);
EEPROM.write(cardsIndex * 5 + 2, cards[cardsIndex][2]);
EEPROM.write(cardsIndex * 5 + 3, cards[cardsIndex][3]);
EEPROM.write(cardsIndex * 5 + 4, cards[cardsIndex][4]);
```

```
      lcd.clear ();
      globalState = 110;
}
// Переходимо в режим зміни пароля доступу
    else if(globalState == 120) { showMenu(111); globalState = 121; }
    else if ( globalState == 121) {
// Обробляємо введення пароля на матричній клавіатурі
      if ( key ) {
        if ( enterPassword ( )) {
// Зберігаємо новий пароль в EEPROM
          for(uint8_t i = 0; i < 7; i++) {
accessPassword[i] = tempPassword[i];
EEPROM.write(i + 150, accessPassword[i]);
}
          resetTempPassword( ); // Скидаємо буфер тимчасового пароля
lcd.clear();
          menuFlag = 11; // Повертаємося до попереднього меню
          globalState = 100;
}
}
}
// Переходимо в режим зміни пароля адміністратора
    else if(globalState == 130) { showMenu(121); globalState = 131; }
    else if ( globalState == 131) {
// Обробляємо введення пароля на матричній клавіатурі
      if ( key ) {
        if ( enterPassword ( )) {
// Зберігаємо новий пароль в EEPROM
          for(uint8_t i = 0; i < 7; i++) {
adminPassword[i] = tempPassword[i];
EEPROM.write(i + 157, adminPassword[i]);
}
resetTempPassword(); // Скидаємо буфер тимчасового пароля
lcd.clear();
          menuFlag = 12; // Повертаємося до попереднього меню
          globalState = 100;
}
}
}
// Переходимо в режим зміни часу утримання замка у відкритому стані
    else if(globalState == 140) { showMenu(131); globalState = 141; }
else if(globalState == 141) {
if(key) {
if(key == '*' || key == '#' || key == 'A' || key == 'B' || key == 'C' || key == 'D') {
```

```
        key = 'n';
        lcd.clear();
        menuFlag = 13;
        globalState = 100;
        EEPROM.write(164, openTime);
        }
        else {
        openTime = (key - 48);
        lcd.setCursor(1, 1); lcd.print(key);
              }
        }
        }
        } // while ( 1)
        }
        //*****************************************************
**************************************************
```

ДОДАТОК В
ПРЕЗЕНТАЦІЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ



Види систем безконтактної ідентифікації

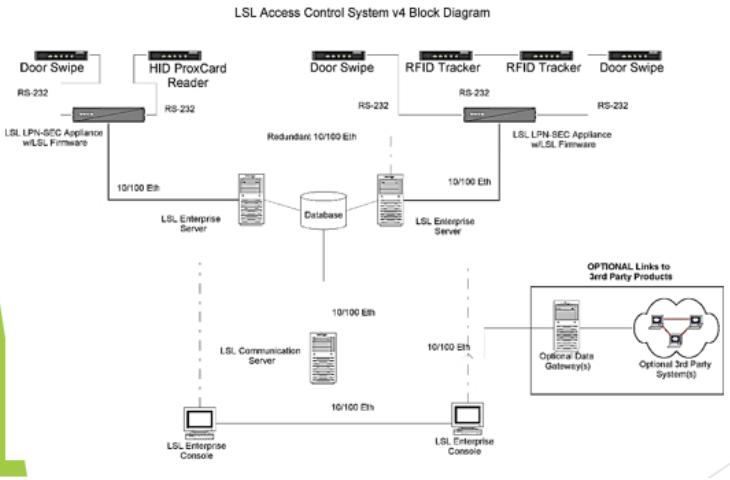
3

Технологія безконтактної ідентифікації, що може бути використана для побудови системи контролю доступу	Переваги застосування	Недоліки застосування
RFID	Висока швидкість ідентифікації. Можливість працювати на великій відстані від зчитувача. Можливість ідентифікації без прямого видимого контакту.	Вища вартість обладнання порівняно з іншими технологіями. Можливість клонування міток, якщо не застосовується відповідний захист. Можливість перешкод для роботи в електромагнітному середовищі.
NFC	Висока безпека завдяки короткому діапазону дії. Зручність використання в сучасних смартфонах. Підтримка безконтактної оплати та інших застосувань.	Дуже коротка відстань взаємодії (до 10 см). Вразливість до перешкод та перешкод у стандартному використанні.
Bluetooth	Зручність використання в багатьох сучасних пристроях. Можливість підключення багатьох пристроїв одночасно. Висока швидкість передачі даних.	Вищий рівень енергоспоживання порівняно з іншими технологіями. Можливість атак на безпеку вразливих версій Bluetooth. Потреба в парувані та ініціалізації.
Біометрична ідентифікація	Висока надійність та стійкість до злому при належній реалізації. Унікальність біометричних даних особи. Висока безпека.	Висока вартість обладнання для збору біометричних даних. Можливість відмови через погану якість зчитування біометричних даних (наприклад, відбитків пальців). Потреба у збереженні та захисті біометричних даних.
QR-код	Простота генерації та сканування кодів. Низька вартість реалізації.	Низька надійність, легко може бути підроблений. Обмеженість обсягу інформації в коді. Залежність від доступу до камери пристрою для сканування.
IR	Низька вартість обладнання. Низький рівень енергоспоживання.	Дуже коротка відстань взаємодії та потреба в прямому «видимому» контакті. Вразливість до перешкод і обмежень в орієнтації.

Критерії	RFID	NFC	Bluetooth	Біометрична ідентифікація	QR-код	IR
Надійність	9	8	6	8	3	4
Стійкість до злому або підробки	9	7	5	10	3	4
Доступність швидкого розгортання	7	7	8	3	9	9
Економічна обґрунтованість застосування	6	6	7	2	9	8
Доступність використання	7	8	8	6	9	7
Ранжування	7,6	7,2	6,8	5,8	6,6	6,4

Огляд обладнання безконтактної ідентифікації

4



LSL ACS v4 (RFID для підприємства) складається з п'яти ключових компонентів, трьох програмних компонентів LSL, одного апаратного пристрою LSL, а також сервера бази даних [41]:

- LSL LPN-SEC – апаратний пристрій, який взаємодіє з фізичними зчитувачами, спілкується безпосередньо з LES через резервний, зашифрований захищений канал AES;
- LSL Enterprise Server (LES) – основний резервний сервер, який взаємодіє з усіма компонентами, інтерфейсами до бази даних і координує всю обробку;
- LSL Communication Server (LCS) – основний сервер, який взаємодіє з компонентами графічного інтерфейсу, інтерфейсами до бази даних, інтерфейсами до продуктів сторонніх розробників і обробляє стислі потоки даних від LSL LPN-SEC;
- LSL Enterprise Console (LEC) – графічний інтерфейс користувача для конфігурації, моніторингу та керування корпоративною системою контролю доступу та відстеження активів.

Стандарти та нормативні вимоги до функціонування систем безконтактної ідентифікації

5

- Функціонування систем безконтактної ідентифікації, включаючи системи на базі технології RFID, регулюється різними стандартами і нормативами з метою забезпечення безпеки, сумісності та правильності роботи.
- Наведені стандарти мають також інші частини, що регламентують аспекти використання елементів систем безконтактної ідентифікації, що використовуються для розгортання безпекових систем контролю доступу.
- Варто відзначити, що українські нормативи є достатньо гармонізованими з аналогічними регламентами провідних держав світу.
- Стандарти та нормативні вимоги до функціонування систем безконтактної ідентифікації є важливими елементами для забезпечення безпеки, сумісності та ефективності таких систем. Основні висновки з цього контексту включають таке:
- 1. Стандарти і нормативні вимоги сприяють створенню єдиної та універсальної системи безконтактної ідентифікації, яка може працювати з різним обладнанням та програмним забезпеченням.
- 2. Вимоги щодо безпеки та приватності допомагають захищати дані користувачів і запобігають несанкціонованому доступу до системи. Заходи безпеки допомагають уникати потенційних загроз інформаційній безпеці.
- 3. Стандарти допомагають забезпечити ефективність та надійність функціонування систем безконтактної ідентифікації. Це важливо для швидкої та точної ідентифікації об'єктів або осіб.
- 4. Стандарти дозволяють системам безконтактної ідентифікації бути сумісними з різними галузями, такими як логістика, безпека, медицина та багато інших. Це робить їх більш універсальними та застосовними.
- 5. Стандарти створюють рівні умови для виробників та користувачів, дозволяючи їм працювати з однаковим обладнанням і забезпечуючи стабільність і надійність систем.
- Таким чином, стандарти та нормативні вимоги є фундаментальними елементами для розробки, розгортання та ефективного функціонування систем безконтактної ідентифікації. Вони допомагають забезпечити безпеку, сумісність і надійність цих систем у різних галузях та застосуваннях.

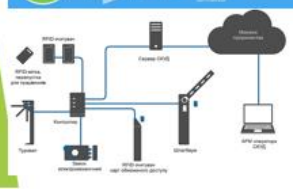
Загальна концепція системи інформаційної безпеки приватного підприємства

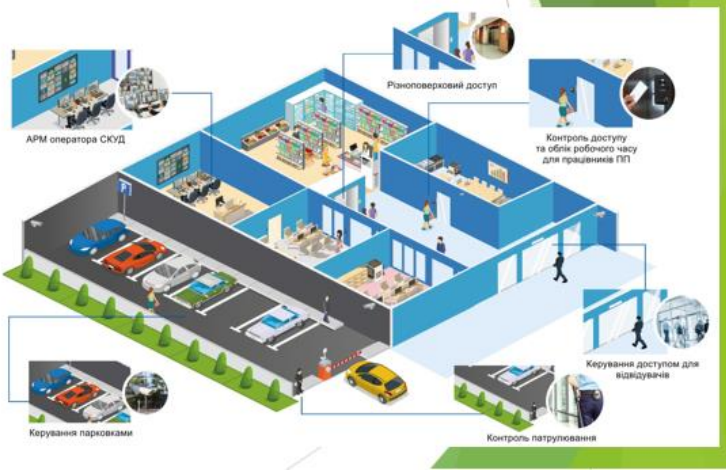
6

- Загальна концепція системи інформаційної безпеки (ІБ) приватного підприємства полягає в створенні та впровадженні комплексу заходів, які забезпечують захист інформації підприємства від ризиків та загроз, які можуть виникнути ззовні або всередині організації. Основна мета системи ІБ полягає в забезпеченні конфіденційності, цілісності та доступності інформації, а також у зменшенні можливих фінансових, правових та репутаційних ризиків для підприємства. Ця концепція передбачає захист інформації від несанкціонованого доступу, руйнування, втрати або розголошення, а також забезпечення можливості її використання в потрібний момент

Роль безконтактної ідентифікації в забезпеченні інформаційної безпеки приватного підприємства

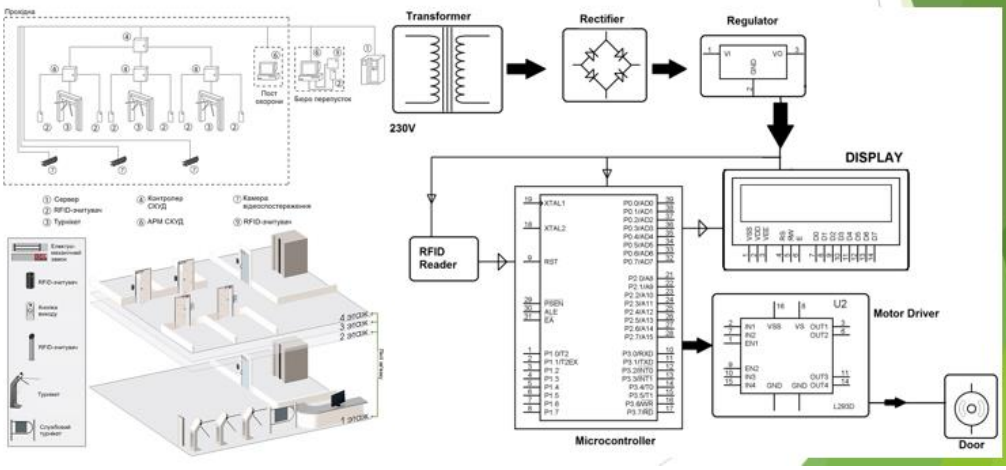
7





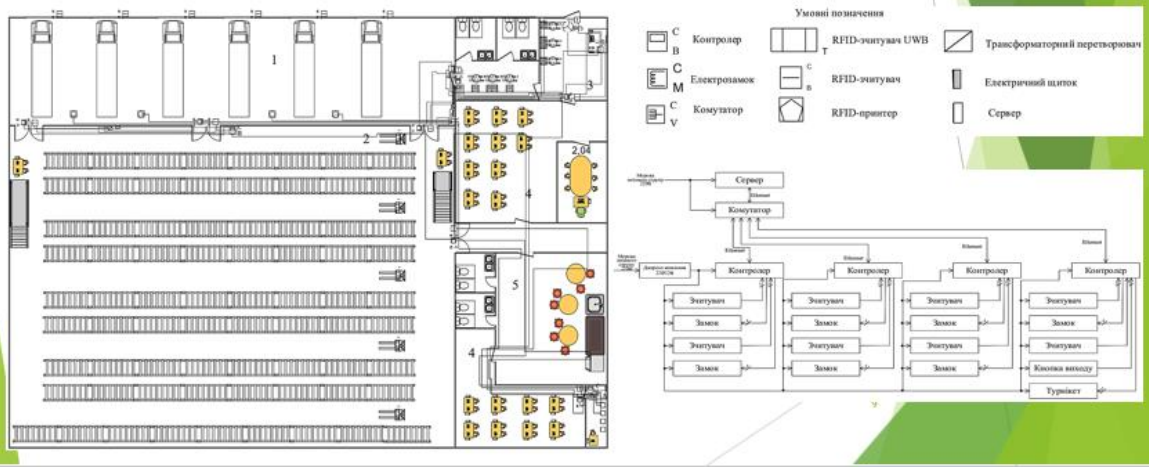
Огляд типових рішень з улаштування безконтактної ідентифікації для забезпечення інформаційної безпеки приватних підприємств

8



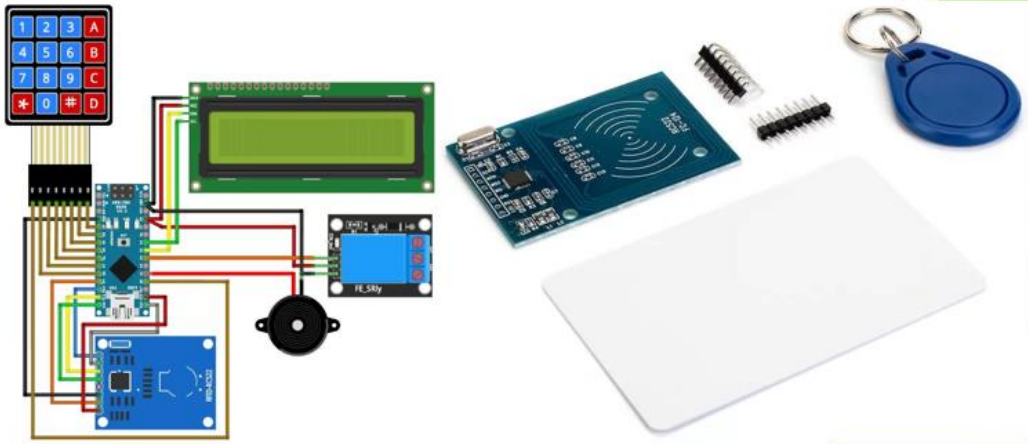
Проєктна реалізація методу у вигляді системи RFID-ідентифікації

9



Апаратна реалізація методу у вигляді системи RFID-ідентифікації

10



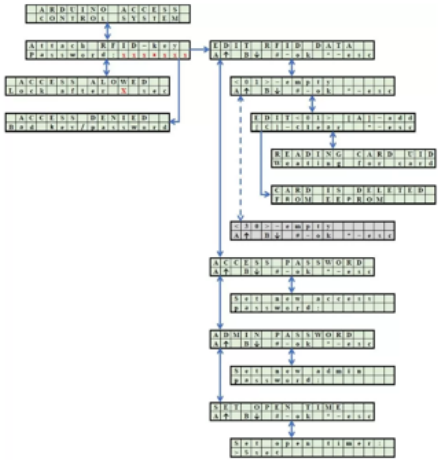
Програмна реалізація методу у вигляді системи RFID-ідентифікації

11

Номер ключа або рядку	Адреса в EEPROM				
	Ознака реєстрації ключа в базі даних (1-ключ зареєстрований; 0-комірка не зайнята)	Унікальний UID			
Ключ №0	0000	0001	0002	0003	0004
Ключ №1	0005	0006	0007	0008	0009
Ключ №2	0010	0011	0012	0013	0014
Ключ №3	0015	0016	0017	0018	0019
Ключ №4	0020	0021	0022	0023	0024
Ключ №5	0025	0026	0027	0028	0029
Ключ №6	0030	0031	0032	0033	0034
Ключ №7	0035	0036	0037	0038	0039
Ключ №8	0040	0041	0042	0043	0044
Ключ №9	0045	0046	0047	0048	0049
Ключ №10	0050	0051	0052	0053	0054
Ключ №11	0055	0056	0057	0058	0059
Ключ №12	0060	0061	0062	0062	0064
Ключ №13	0065	0066	0067	0068	0069
Ключ №14	0070	0071	0072	0073	0074
Ключ №15	0075	0076	0077	0078	0079
Ключ №16	0080	0081	0082	0083	0084
Ключ №17	0085	0086	0087	0088	0089
Ключ №18	0090	0091	0092	0093	0094
Ключ №19	0095	0096	0097	0098	0099
Ключ №20	0100	0101	0102	0103	0104
Ключ №21	0105	0106	0107	0108	0109
Ключ №22	0110	0111	0112	0113	0114
Ключ №23	0115	0116	0117	0118	0119
Ключ №24	0120	0121	0122	0123	0124
Ключ №25	0125	0126	0127	0128	0129
Ключ №26	0130	0131	0132	0133	0134
Ключ №27	0135	0136	0137	0138	0139
Ключ №28	0140	0141	0142	0143	0144
Ключ №29	0145	0146	0147	0148	0149

Налаштування розробленої системи RFID-ідентифікації

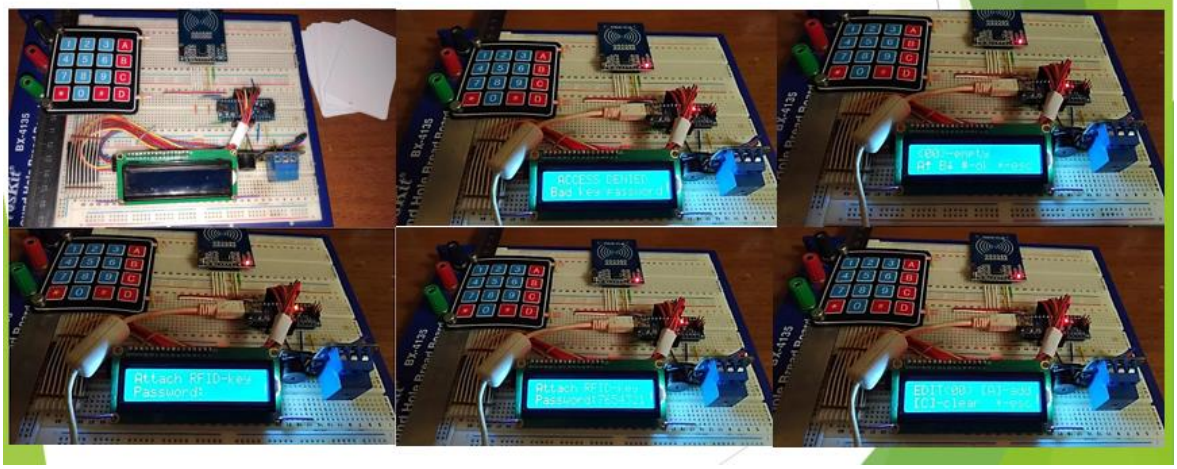
12



- Процедура налаштування передбачає наступні кроки:
- 1. Ініціалізація системи: Після подачі живлення, система ініціалізується та готова до роботи. Користувач отримує звуковий сигнал та індикацію на дисплеї, після чого система переходить у робочий режим.
- 2. Вибір режиму роботи: Користувач може обрати режим роботи - режим користувача або режим адміністратора. Режим адміністратора дозволяє виконувати додавання нових RFID-карт, зміну паролів та інші налаштування.
- 3. Введення ідентифікатора: В режимі користувача користувач має можливість ввести ідентифікатор, який може бути або RFID-картою, або паролем на матричній клавіатурі.
- 4. Перевірка ідентифікації: Система перевіряє введений ідентифікатор на відповідність даним у базі даних. Якщо ідентифікатор вірний, система надає доступ і відповідно керує електрозамком.
- 5. Налаштування параметрів: У режимі адміністратора користувач може виконати налаштування системи, такі як додавання нових RFID-карт, зміну паролів або параметрів роботи замка.
- 6. Відображення інформації: Важливою частиною процедури є відображення інформації на дисплеї для зручності користувача. Інформація повинна бути чіткою і зрозумілою.
- 7. Звукові та світлові сигнали: Для інформування користувача про результати ідентифікації і стан системи використовуються звукові та світлові сигнали.
- 8. Управління доступом: Після ідентифікації система керує доступом до об'єкта відповідно до налаштованих параметрів.

Оцінка ефективності функціонування розробленої системи RFID-ідентифікації

13



Оцінка ефективності функціонування розробленої системи RFID-ідентифікації з урахуванням інтеграції в загальну систему безпеки приватного підприємства

14

Оцінка ефективності функціонування розробленої системи RFID-ідентифікації в контексті її інтеграції в загальну систему безпеки приватного підприємства виявила кілька ключових аспектів.

- По-перше, інтеграція цієї системи сприяє підвищенню загального рівня безпеки об'єкта. Це досягається завдяки контролю доступу до приміщень та ресурсів, що знижує ризик несанкціонованого доступу.
- По-друге, система забезпечує швидку та надійну ідентифікацію співробітників та гостей за допомогою RFID-карт або паролів. Це спрощує процес ідентифікації та робить його зручним для користувачів.
- По-третє, система може бути інтегрована з іншими системами безпеки, такими як відеоспостереження та контроль доступу до приміщень, що дозволяє автоматизувати та спростити процеси моніторингу та керування безпекою.
- По-четверте, наявність звукових та світлових сигналів сприяє оперативному повідомленню про статус доступу та помилки, що підвищує ефективність реагування на події.
- По-п'яте, система дозволяє адміністраторам керувати правами доступу, включаючи реєстрацію та видалення користувачів, зміну паролів та інші налаштування, що робить її гнучкою та пристосованою до потреб підприємства.

Усе це робить інтегровану систему RFID-ідентифікації ефективним інструментом для забезпечення безпеки на приватному підприємстві.

14

Висновок

15

- У відповідності до мети та завдання в даній роботі отримані проєктні рішення з забезпечення інформаційної безпеки приватного підприємства шляхом інтеграції засобів безконтактної ідентифікації на базі технології RFID.
- У якості приватного підприємства прийнято зонований складський корпус, що потребує контролю доступу для автотранспортних засобів, території складського зберігання, побутових та офісних приміщень.
- Використання RFID-засобів ідентифікації дозволили вирішити проблему авторизованого доступу для водійського та складського персоналу, а також представників бізнес-партнерів і адміністрації. Запропонована система контролю доступу дозволяє автоматизувати процедуру ідентифікації користувачів та скерувати відповідний сигнал на відкриття чи утримання закритим фізичного бар'єру (портальних воріт, турнікету чи дверей з електромеханічним замком).
- Проєктні рішення з улаштування головного елементу RFID-СКУД, RFID-зчитувача виконані на базі технології Arduino з використанням мікропроцесору Arduino Nano та RFID-модуля RFID-RC522 (MFRC522). Ефективність проєктних рішень підтверджено на дослідному стенді.
- Після інтеграції RFID-СКУД до загальної системи безпеки, спостереження і контроль за доступом стають більш точними і автоматизованими. Це допомагає уникнути несанкціонованого доступу, підвищує рівень безпеки об'єктів, і відповідно, зменшує ризики проникнення та порушення інформаційної безпеки.

ДЯКУЮ ЗА УВАГУ!

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «магістр»

Студент Колісник Вадим Валерійович

Тема Метод контролю доступу на основі RFID-технологій для забезпечення інформаційної безпеки приватного підприємства

Галузь знань 12 «*Інформаційні технології*» Спеціальність 125 «*Кібербезпека*» Освітня програма «Кібербезпека»

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «магістр»:
кількість листів креслень - ; кількість сторінок записки 108

1. Короткий зміст роботи та прийнятих рішень У кваліфікаційній роботі запропоновано комплексний підхід до використання технологій RFID для підвищення інформаційної безпеки підприємств. Це включає в себе фізичний контроль доступу, автентифікацію працівників та моніторинг руху в приміщеннях. В рамках дослідження розроблено повноцінну інтегровану системи контролю доступу на основі RFID-технологій, що враховує специфічні потреби та вимоги приватних підприємств, розглянуто питання інтеграції методу контролю доступу на основі RFID в загальну систему безпеки підприємства, що є актуальним аспектом у сучасному бізнес-середовищі.

2. Висновок про відповідність кваліфікаційної роботи завданню Кваліфікаційна робота у повній мірі відповідає поставленому завданню як в теоретичній, так і в практичній частині роботи

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі подана загальна характеристика поставленої задачі, чітко визначено об'єкт, предмет та методи дослідження, сформульована актуальність; визначені задачі, які необхідно вирішити для досягнення поставленої мети, практична цінність отриманих результатів, їхня новизна та наведені відомості про публікації. У першому розділі було проаналізовано і досліджено системи безконтактної ідентифікації, стандарти та нормативні вимоги до їх функціонування. У другому розділі були розглянуті типові рішення з улаштування безконтактної ідентифікації для забезпечення інформаційної безпеки приватних підприємств, визначено їх переваги та недоліки. У третьому розділі реалізовано метод безконтактної ідентифікації на основі RFID-технологій для забезпечення інформаційної безпеки приватного підприємства. Четвертий розділ присвячено оцінці ефективності функціонування розробленої системи безконтактної інтеграції на основі RFID-технологій для забезпечення інформаційної безпеки приватного підприємства.

4. Позитивні сторони роботи полягають у тому, що розроблені рішення системи контролю доступу на основі RFID-технологій дозволяють підприємствам ефективно обмежувати фізичний доступ до приміщень та об'єктів, зменшуючи ризик незаконного вторгнення та крадіжок. Використання RFID для ідентифікації працівників та гостей дозволяє контролювати доступ до конфіденційної інформації та зменшує можливість витоку конфіденційних даних.

5. Негативні сторони роботи відсутні

6. Оцінка графічного оформлення та пояснювальної записки роботи Оформлення всіх матеріалів кваліфікаційної роботи є якісним, здійснене з дотриманням актуальних стандартів та інституційних положень ХНУ. Пояснювальна записка відповідає нормам щодо її оформлення як за структурою, так і за представленням і форматуванням матеріалу.

7. Відгук про роботу в цілому В загальному кваліфікаційна робота заслуговує відмінної оцінки. Весь матеріал кваліфікаційної роботи структурований, чіткий та послідовний. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики кваліфікаційної роботи. Ілюстративний матеріал дозволяє наочно побачити доцільність та ефективність рішень, які були прийняті за основу для досягнення поставленої мети.

8. Інші зауваження

9. Оцінка кваліфікаційної роботи Розглянувши позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що робота заслуговує оцінки «відмінно».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) Завідувач кафедри автоматизації, комп'ютерно-інтегрованих технологій та робототехніки, доктор технічних наук, професор Мартинюк Валерій Володимирович.

« 8 » грудня 2023 року _____ (підпис)

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Колісника Вадима Валерійовича
ПІБ здобувача вищої освіти

Студента ФІТ, 2 курсу, групи КБм-22-1

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у хмельницькому національному університеті» від 31.08.2023, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

11.12.2023
дата


підпис

UNICHECK
by Turnitin

Ім'я користувача:
Кафедра кібербезпеки

ID перевірки:
1015973393

Дата перевірки:
05.12.2023 18:30:43 EET

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
05.12.2023 18:34:38 EET

ID користувача:
100008300

Назва документа: **Записка_Колісник**

Кількість сторінок: **92** Кількість слів: **15288** Кількість символів: **119467** Розмір файлу: **4.29 MB** ID файлу: **1015652628**

Виявлено модифікації тексту (можуть впливати на відсоток схожості)

4.52%
Схожість

Найбільша схожість: **1.45%** з Інтернет-джерелом (https://3d-diy.ru/wiki/projects/sistema-besprovodnogo-dostupa-rfid)

4.23% Джерела з Інтернету	411	Сторінка 94
0.71% Джерела з Бібліотеки	54	Сторінка 95

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

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

Замінені символи	3
Підозріле форматування	14 сторінок

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 0.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 11%**

	Документ		Сумарний збіг по Базі Даних	
ID: 121811 Назва: Метод контролю доступу на основі RFID-технологій для забезпечення інформаційної безпеки приватного підприємства Додано в БД: 2023-12-05 Автора: Колісник В.В. Керівники: Тітова В.Ю. Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	99331	1486	538 (1%)	8 (1%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:
Назва: Метод контролю доступу на основі RFID-технологій для забезпечення інформаційної безпеки приватного підприємства

Автор: Колісник Вадим Валерійович
Спеціальність: 125 – Кібербезпека
Освітня програма: освітньо-професійна
Науковий керівник: Тітова Віра Юріївна, к.т.н, доцент
Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв`язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою Unichek складає 95,48%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v-15.257 складає 99,9%.

Згідно з Положенням про систему забезпечення академічної доброчесності у ХНУ (https://khmnu.edu.ua/wp-content/uploads/normatyvni-dokumenty/polozhennya/pro-systemu-zabezpechennya-akademichnoyi-dobrochesnosti.pdf) така авторська робота, обсяг оригінального тексту у відсотках до загального обсягу матеріалу в якій складає 90-100 %, визнається роботою з високою унікальністю тексту.

Виявлені в роботі модифікації є символами формул.

Керівник роботи _____ В.Ю. Тітова

Гарант ОП _____ В.Ю. Тітова

Завідувач кафедри кібербезпеки _____ Ю. П. Кльоц