

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ЗАКЛАД
„ЛУГАНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА”

Навчально-науковий інститут фізики, математики та інформаційних
технологій

Кафедра інформаційних технологій та систем

Снежко Олександр Едуардович

**ПРОЄКТУВАННЯ РОЗУМНОЇ СИСТЕМИ РЕЄСТРАЦІЇ КЛІЄНТІВ
ГОТЕЛЮ**

кваліфікаційна робота

здобувача вищої освіти першого (бакалаврського) рівня

освітньої програми «Комп’ютерна інженерія»

за спеціальністю 123 Комп’ютерна інженерія

Особистий підпис _____ Олександр СНЕЖКО

Науковий керівник _____ Володимир МАТІЄВСЬКИЙ,
асистент
кафедри інформаційних технологій
та систем

Завідувач кафедри _____ Микола СЕМЕНОВ,
кандидат педагогічних наук, доцент
кафедри інформаційних технологій
та систем

Полтава – 2023

Міністерство освіти і науки України
Державний заклад „Луганський національний університет
імені Тараса Шевченка”

Факультет (інститут)	Навчально-науковий інститут фізики, математики та інформаційних технологій
	(повна назва)
Кафедра	Інформаційних технологій та систем
	(повна назва)
Освітньо-кваліфікаційний рівень	Бакалавр
	(код, назва)
Напрямок підготовки	123 Комп'ютерна інженерія
	(код, назва)

ЗАТВЕРДЖУЮ

Завідувач кафедри ІТС
М.А. Семенов

(підпис)	(ініціали, прізвище)
“ ”	2023 р.

ЗАВДАННЯ
НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ) СТУДЕНТУ

Сніжко Олександр Едуардович

(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) ПРОЄКТУВАННЯ РОЗУМНОЇ СИСТЕМИ РЕЄСТРАЦІЇ КЛІЄНТІВ ГОТЕЛЮ

Керівник кваліфікаційної роботи	Матієвський В.В. асистент кафедри ІТС
	(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджена наказом по університету ВІД

2. Строк подання студентом проекту (роботи)

3. Вихідні дані до роботи (проекту)

Специфікація системи контролю

доступу

Специфікація ARDUINO

(визначаються кількісні або (та) якісні показники, яким повинен відповідати об'єкт розробки)

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) ТЕОРЕТИЧНІ ЗАСАДИ ФУНКЦІОНУВАННЯ СИСТЕМ КОНТРОЛЮ, УПРАВЛІННЯ ДОСТУПОМ ТА РЕЄСТРАЦІЇ

МЕТОДОЛОГІЯ ТА РОЗРОБКА ТЕХНОЛОГІЇ НА ОСНОВІ ARDUINO ДЛЯ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ ТА РЕЄСТРАЦІЇ ГОТЕЛЮ

ОГЛЯД ТА ОЦІНКА ЕФЕКТИВНОСТІ РОЗРОБЛЕНОЇ СИСТЕМИ

(визначаються назви розділів або (та) перелік питань, які повинні увійти до тексту ПЗ)

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

6. Консультанти розділів проекту/роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання „_____” _____ 2023р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1.	Вибір теми роботи, вивчення наукової літератури, затвердження теми та керівника.	До 1 листопада	
2.	Аналіз літературних джерел за темою роботи. Подання структури теоретичної частини роботи та плану експериментальних досліджень.	Другий тиждень листопада (10 листопада)	
3.	Робота над теоретичною частиною. Подання теоретичної частини роботи для першого читання науковим керівником.	До 15 грудня	
4.	Усунення зауважень, урахування рекомендацій наукового керівника. Подання теоретичної частини роботи на друге читання.	До 28 січня	
5.	Проведення експериментальної роботи. Поетапний аналіз та обговорення її результатів. Перевірка стану виконання роботи.	Перший тиждень березня	
6.	Урахування рекомендацій наукового керівника, усунення недоліків, підготовка варіанта роботи до передзахисту. Розробка презентації.	До 31 березня	
7.	Попередній захист роботи на кафедрі	травень	
8.	Доопрацювання роботи з урахуванням рекомендацій після передзахисту. Подання роботи науковому керівникові та рецензентові на підготовку відгуку та рецензії	За 10 днів до державної атестації	
9.	Подання на кафедру остаточного варіанта роботи, переплетеного та підписаного автором, науковим керівником і рецензентом.	За 5 днів до державної атестації	

Студент

підпис

Олександр СНЕЖКО

(ініціали, прізвище)

Керівник проекту (роботи)

підпис

Володимир МАТІЄВСЬКИЙ

(ініціали, прізвище)

АНОТАЦІЯ

Снежко О.Е.

Тема: Проєктування розумної системи реєстрації клієнтів готелю

Спеціальність: 123 «Комп'ютерна інженерія»

Установа: ЛНУ імені Тараса Шевченка, 2023 р.

Бакалаврська робота містить: 74 с., 5 табл., 9 рис., 24 джерела, 2 додатки.

Об'єкт дослідження системи контролю доступу та реєстрації.

Предмет дослідження особливості розробки та впровадження інтелектуальної системи контролю доступу та реєстрації для готельних підприємств на основі Arduino.

Мета дослідження розробка системи, яка не тільки підвищує безпеку, але й покращує загальну ефективність процесів контролю доступу та реєстрації в готелі на основі Arduino.

Результати роботи.

Розроблено конструкцію системи RFID, яка забезпечує доступне та зручне рішення для готельних підприємств. Система компактна і проста в установці з мінімальною кількістю необхідних налаштувань. Електромагнітний замок живиться від реле, коли зчитана мітка збігається з міткою, що зберігається в мікроконтролері. Після третьої невдалої спроби спрацьовує зумер, який сповіщає про дозвіл або відмову в доступі при цьому подія реєструється. Живлення мікроконтролера і електромагнітного замка може здійснюватися від одного джерела живлення 9В, а також стабілізатора напруги і інвертуючого підсилювача.

Висновки. Запропонований гібридний дизайн системи контролю доступу та реєстрації в цій роботі поєднує в собі функції безсерверного та адаптивного до ризиків контролю доступу. На відміну від інших систем, які зосереджені на різних аспектах, таких як шифрування, нечітка логіка, мобільний доступ та інтелектуальний дизайн, проєкт зосереджений на досягненні максимальної ефективності.

Ключові слова: Інтелектуальна система контролю доступу, Ризико-адаптивний контроль доступу, Готельні підприємства, Arduino, RFID.

ABSTRACT

Sniezhko O.E.

Topic: Designing a smart hotel customer registration system

Specialty: 123 "Computer Engineering"

Institution: Luhansk Taras Shevchenko National University, 2023.

Bachelor's thesis contains: 74 p., 5 tables, tables, 9 figures, 24 sources, 2 appendices.

The object of study access control and registration systems.

Subject of research features of the development and implementation of an intelligent access control and registration system for hotel enterprises based on Arduino.

The study aims development of a system that not only increases security but also improves the overall efficiency of hotel check-in and access control processes based on Arduino.

Results. The design of the RFID system has been developed, which provides an affordable and convenient solution for hotel enterprises. The system is compact and easy to install with a minimum number of necessary settings. The electromagnetic lock is powered by a relay when the read tag matches the tag stored in the microcontroller. A buzzer is activated after the third unsuccessful attempt, which notifies access authorization or denial. The microcontroller and the electromagnetic lock can be powered from a single 9V power supply, as well as a voltage regulator and an inverting amplifier.

Conclusions. The proposed hybrid design of the access control and registration system in this work combines the functions of serverless and risk-adaptive access control. Unlike other systems that focus on various aspects such as encryption, fuzzy logic, mobile access and intelligent design, the project focuses on achieving maximum efficiency.

Keywords: Intelligent access control system, Risk-adaptive access control, Hotel enterprises, Arduino, RFID.

ИТС.4КИ.0323.01-ВП

Позначення

Найменування

**Кількість
прим/стор**

**Місцезна-
ходження /
Примітка**

Документація проекту

ITC.4KI.0323.02-T3

Проектування розумної
системи реєстрації
клієнтів готелю

1/7

Формат А4

Технічне завдання.

ITC.4KI.0323.03-ПЗ

Проектування розумної
системи реєстрації
клієнтів готелю

1/74

Формат А4

Пояснювальна записка.

ИТС.4КІ.0323.01-ВП

Змн.	Арк.	№ докум.	Підпис	Дата
------	------	----------	--------	------

Розроб.	Снежко О.Е.		
Керівник	Матієвський В.В.		
Реценз.	Козуб Ю.Г.		
Н. Контр.			
Зав. каф.	Семенов М.А..		

ВІДОМІСТЬ ПРОЕКТУ

Літ.	Арк.	Акрушів
	1	1

ЛНУ
Кафедра ІТС, Гр.4К

Літ.	Арк.	Акрушів
	1	1

ЛНУ

Кафедра ИТС, Гр.4К1

Міністерство освіти і науки України
Державний заклад «Луганський національний університет
імені Тараса Шевченка»

Факультет (інститут)	Навчально-науковий інститут фізики, математики та інформаційних технологій <small>(повна назва)</small>
Кафедра	Інформаційних технологій та систем <small>(повна назва)</small> <small>(код, назва)</small>

ТЕХНІЧНЕ ЗАВДАННЯ

на виконання програмної розробки (ПР):
**" ПРОЄКТУВАННЯ РОЗУМНОЇ СИСТЕМИ РЕЄСТРАЦІЇ КЛІЄНТІВ
ГОТЕЛЮ"**

ІТС.4КІ.0323.02-ТЗ

ПОГОДЖЕНО
Керівник кваліфікаційної роботи

_____ Матієвський В.В. _____.

“ _____ ” _____ 2022р

ВИКОНАВЕЦЬ
Студент групи 4 КІ

_____ Снєжко О.Е _____.

“ _____ ” _____ 2022р

Полтава – 2022

ЗМІСТ

ВСТУП.....	1
1. ХАРАКТЕРИСТИКИ ОБ'ЄКТА.....	1
2. ПРИЗНАЧЕННЯ ПРИСТРОЮ.....	1
3. ОСНОВНІ ВИМОГИ ДО ПРИСТРОЮ.....	2
4. ТЕХНІКО-ЕКОНОМІЧНІ ВИМОГИ ДО КІНЦЕВОГО ПРИСТРОЮ .	3
5. ВИМОГИ ДО МАТЕРІАЛІВ І КОМПЛЕКТУЮЧИХ.....	3
6. ЕТАПИ ВИКОНАННЯ ПР	3
7. ПРИЙОМ	4
8. ПОРЯДОК ВНЕСЕННЯ ЗМІН ДО ТЕХНІЧНОГО ЗАВДАННЯ, ЩО ЗАТВЕРДЖЕНО.....	5

					<i>ІТС.4КІ.0323.02-ТЗ</i>		
<i>Змн.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дат</i>	<i>ТЕХНІЧНЕ ЗАВДАННЯ</i>		
<i>Розроб.</i>		<i>Снежко О. Е.</i>					
<i>Керівник</i>		<i>Матієвський</i>					
<i>Реценз.</i>		<i>Козуб Ю.Г.</i>					
<i>Н. Контр.</i>							
<i>Зав. каф.</i>		<i>Семенов М.А..</i>			<i>ЛНУ</i> <i>Кафедра ІТС, Гр.4КІ</i>		
					<i>Літ.</i>	<i>Арк.</i>	<i>Акрушіє</i>
						2	7

ВСТУП

1.1 Найменування: Проектування розумної системи реєстрації клієнтів готелю

1.2 Шифр ПР: ІТС.4КІ.0323

1.3 Підстава для виконання ПР: Підставою для виконання даної розробки є завдання на виконання дипломного проекту, яке затверджено кафедрою інформаційних технологій та систем Луганського національного університету імені Тараса Шевченка.

1.4 Терміни розробки:

1.4.1 Початок 15 листопада 2022р.

1.4.2 Закінчення 3 червня 2023р.

1.5 Фінансується за рахунок коштів замовника. Умови фінансування - за договором № 12 / а і протоколу узгодження ціни № 12 / б.

1. ХАРАКТЕРИСТИКИ ОБ'ЄКТА

1.1 Розроблений пристрій який є елементом розумної системи контролю доступу та реєстрації готелю. До складу проекту, який створюється має входити:

1.1.1. Розроблений додаток

1.2 Концепція пристрою

2. ПРИЗНАЧЕННЯ ПРИСТРОЮ

2.1 Призначення: Розробка апаратно-програмного комплексу який виконуватиме функцію обмеження доступу та реєстрації клієнтів готелю

2.2 Основні критерії ефективності.

2.2.1 Зручний інтерфейс.

2.2.1.1 Користувач повинен мати права адміністрування системою;

2.2.1.2 Користувач повинен мати можливість дистанційного керування;

					<i>ІТС.4КІ.0323.02-ТЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		3

2.2.1.3 Користувач повинен мати можливість проводити зручний перегляд всієї інформації.

2.2.2 Пристрій повинен:

2.2.2.1 Мати інтерактивне привітальне вікно;

2.2.2.2 Відображати текстові підказки;

2.2.2.3 Посилати електричний сигнал на двері;

2.2.2.4 Обробляти можливі помилки;

3. ОСНОВНІ ВИМОГИ ДО ПРИСТРОЮ

3.1 Загальні вимоги

3.1.1 Додаток працює незалежно від операційних систем;

3.1.2 Вимоги до апаратного забезпечення:

3.1.3. Тип пристрою: Ноутбук або Комп'ютер, та плата Arduino Uno;

3.1.4 Додаток повинен мати зручний інтерфейс;

3.1.5 До складу додатку входить файл з програмною розробкою;

3.1.6 Додаток повинен проводити зручне відображення інформації.

3.2 Додаткові вимоги

3.2.1 Мова програмування C/C++.

3.2.2 Середовище розробки Arduino IDE.

3.4 Вимоги до якості і надійності

3.4.1 Пристрій повинен надійно працювати.

3.4.2 Розробник гарантує роботу пристрою без збоїв.

3.5 Вимоги до експлуатації

3.5.1 Розробник використовує власний комп'ютер, на якому додаток повинен надійно працювати.

4. ТЕХНІКО-ЕКОНОМІЧНІ ВИМОГИ ДО КІНЦЕВОГО ПРИСТРОЮ

Вартість розробки данної моделі пристрою визначається згідно з договором на розробку. Вартість розробки повинна бути конкурентноспроможною по відношенню до вже готових пристроїв.

5. ВИМОГИ ДО МАТЕРІАЛІВ І КОМПЛЕКТУЮЧИХ

5.1 В процесі розробки пристрою можливе використання програмних засобів, які безкоштовно розповсюджуються.

5.2 У процесі розробки пристрою використовується плата програмування Arduino

5.3 До комплектації пристрою входять:

5.3.1 Програмне забезпечення

5.3.2 Arduino

6. ЕТАПИ ВИКОНАННЯ ПР

Етапи виконання ПР можуть уточнювати згідно календарного плану робіт по узгодженню між замовником та виконавцем.

№	Етапи виконання роботи	Термін виконання і обсяг робіт	Звітні матеріали
1	Аналізування першого запуску та встановлення актуального забезпечення для подальшої розробки		Перша версія пристрою, яка виконує всі основні функції
2	Розробка основної моделі та програмування пристрою		Запрограмований готовий пристрій
3	Оформлення кінцевої версії розробки		Звітні матеріали згідно з пунктом 8.

7. ПРИЙОМ

7.1. Необхідні вимоги до виконання після закінчення робіт.

Оцінка результатів розробки та доцільності її продовження здійснюється замовником шляхом подання таких матеріалів:

- список файлів на носії резервної копії;
- короткий опис роботи ПР і опис всіх файлів, необхідних для роботи програми.
- перелік документів
 - Технічне завдання
 - Пояснювальна записка

7.2. Перелік облікових документів, необхідних для прийняття етапів робіт:

- короткий опис результатів етапу у вигляді анотованого звіту (для етапів 1 і 2);
- сертифікат приймання продукції.

Звітні матеріали подаються у вигляді звітів на папері по ДСТУ

7.3. Загальний перелік для отримання звітних документів, макетів та експериментальних зразків.

На приймання подаються такі документи: акт здачі-приймання продукції, акт реалізації ПРАВА.

					ІТС.4КІ.0323.02-ТЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		6

8. ПОРЯДОК ВНЕСЕННЯ ЗМІН ДО ТЕХНІЧНОГО ЗАВДАННЯ, ЩО ЗАТВЕРДЖЕНО

Дане технічне завдання може уточнюватися в процесі розробки ПР при узгодженні сторін з оформленням доповнень до ТЗ.

					ІТС.4КІ.0323.02-ТЗ	Арк.
						7
Змн.	Арк.	№ докум.	Підпис	Дата		

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЗ «ЛУГАНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА»

Навчально-науковий інститут фізики, математики та
інформаційних технологій

(назва факультету, інституту)

Інформаційних технологій та систем

(назва кафедри)

Пояснювальна записка
до дипломного проекту (роботи)
БАКАЛАВРА
(освітньо-кваліфікаційний рівень)

на тему:
ПРОЄКТУВАННЯ РОЗУМНОЇ СИСТЕМИ РЕЄСТРАЦІЇ КЛІЄНТІВ
ГОТЕЛЮ

Виконав: студент 4 курсу, групи _____
напряму підготовки (спеціальності)
123 «Комп'ютерна інженерія»
(шифр і назва напряму підготовки, спеціальності)

СНЕЖКО О.Е.
(прізвище та ініціали)

Керівник: МАТІЄВСЬКИЙ В. В.
(прізвище та ініціали)

Рецензент: КОЗУБ Ю.Г.
(прізвище та ініціали)

Полтава – 2023

ЗМІСТ

ВСТУП	3
РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ФУНКЦІОНУВАННЯ СИСТЕМ КОНТРОЛЮ, УПРАВЛІННЯ ДОСТУПОМ ТА РЕЄСТРАЦІЇ.....	6
1.1. Генезис систем контролю управління доступом та реєстрації	6
1.2. Типологія та атрибути систем контролю управління доступом та реєстрації	13
1.3. Завдання, функції, цілі та вимоги до системи контролю управління доступом та реєстрацією готельного підприємства	17
Висновки до розділу 1	20
РОЗДІЛ 2. МЕТОДОЛОГІЯ ТА РОЗРОБКА ТЕХНОЛОГІЇ НА ОСНОВІ ARDUINO ДЛЯ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ ТА РЕЄСТРАЦІЇ ГОТЕЛЮ	22
2.1. Дизайн та методи розробки системи.....	22
2.2. Опис та аналіз системи.....	29
2.3. Обмеження та можливі шляхи модернізації системи	44
Висновки до розділу 2	50
РОЗДІЛ 3. ОГЛЯД ТА ОЦІНКА ЕФЕКТИВНОСТІ РОЗРОБЛЕНОЇ СИСТЕМИ	52
3.1. Методика оцінки ефективності системи.....	52
3.2. Тестування програмної частини	56
3.3. Порівняння з існуючими розумними системами контролю доступу	62
Висновки до розділу 3	65
ВИСНОВКИ	67
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	70
ДОДАТКИ	74

					ІТС.4КІ.0323.03-ПЗ		
Змн.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Снежко О.Е.					
Керівник		Матієвський В.В.					
Реценз.		Козуб Ю.Г.					
Н. Контр.							
Зав. каф.		Семенов М.А..					
					ЛІТ.		
					Арк.		
					Акрюшіє		
					1		
					ЛНУ		
					Кафедра ІТС, Гр.4КІ		

ВСТУП

Актуальність дослідження

Зі зростанням важливості безпеки в різних галузях промисловості, розробка ефективних і дієвих систем контролю доступу та реєстрації стала першочерговим завданням. У готельному бізнесі, де забезпечення безпеки та конфіденційності гостей має першорядне значення, потреба в надійному та економічно ефективному рішенні є як ніколи актуальним. Саме тому у даній роботі висвітлено особливості процесу створення системи контролю доступу та реєстрації в готелі з використанням технології Arduino.

Завдяки використанню технології Arduino, це рішення має забезпечити кастомізоване та доступне рішення, яке може бути легко впроваджене в готельному середовищі.

Мета дослідження розробка системи, яка не тільки підвищує безпеку, але й покращує загальну ефективність процесів контролю доступу та реєстрації в готелі на основі Arduino.

Визначена мета дослідження передбачає поступове виконання наступних завдань:

- висвітлити історії розвитку систем контролю управління доступом та реєстрації;
- оглянути типологію та атрибути систем контролю управління доступом та реєстрації;
- визначити основні завдання, функції, цілі та вимоги до систем доступу та реєстрації у готельному підприємстві;

					ІТС.4КІ.0723.03-ПЗ				
Змн.	Арк.	№ докум.	Підпис	Дата	ВСТУП	Лім.	Арк.	Акрушів	
Розроб.		Снежко О.Е							
Керівник		Матієвський В.В.					3	3	
Реценз.		Козуб Ю.Г.				ЛНУ Кафедра ІТС, Гр.4КІ			
Н. Контр.									
Зав. каф.		Семенов М.А..							

- обрати дизайн та методології розробки інтелектуальної системи контролю доступу та реєстрації для готельних підприємства на основі Arduino;
- навести основні обмеження та можливі шляхи модернізації розробленої системи;
- розробити методику оцінки ефективності системи у контексті готельного підприємства;
- підготувати тейст-кейси для програмної частини системи;
- провести порівняльний аналіз розробленої системи з наявними рішеннями.

Об’єкт дослідження системи контролю доступу та реєстрації.

Предмет дослідження особливості розробки та впровадження інтелектуальної системи контролю доступу та реєстрації для готельних підприємств на основі Arduino.

Практичне значення отриманих результатів

Запропоновано економічно та технологічне ефективне рішення для підвищення безпеки та ефективності систем контролю доступу та реєстрації в готелях. Завдяки використанню технології Arduino та технології RFID, запропонована система пропонує практичне і масштабоване рішення, яке може бути впроваджене майже в будь-якому готельному середовищі. Результати цього дослідження сприяють постійним зусиллям у створенні передових систем реєстрації, які відповідають зростаючим потребам готельної індустрії.

Структура і обсяг роботи

Робота складається з вступу, трьох розділів, висновків списку використаних джерел, додатків.

Обсяг роботи становить 74 сторінки, обсяг використаної літератури – 24 джерела.

					<i>ІТС.4КІ.0323.03-ПЗ</i>	Арк.
						4
Змн.	Арк.	№ докум.	Підпис	Дата		

Перший розділ містить опис та загальні теоретичні засади функціонування системи управління контролем доступом та реєстрації.

У другому розділі проводиться дослідження та розробка системи на базі Arduino.

У третьому розділі розглянуто методи оцінки та тестування розробленої системи.

Додатки містять головні елементи коду програмної частини проекту.

					<i>ІТС.4КІ.0323.03-ПЗ</i>	Арк.
						5
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ФУНКЦІОНУВАННЯ СИСТЕМ КОНТРОЛЮ, УПРАВЛІННЯ ДОСТУПОМ ТА РЕЄСТРАЦІЇ

1.1. Генезис систем контролю управління доступом та реєстрації

Системи контролю управління доступу (СКУД) слугують важливими компонентами інфраструктури безпеки, забезпечуючи санкціонований вхід і запобігаючи несанкціонованому доступу до певних зон підприємства. Генезис СКУД можна простежити у різних сферах, включаючи комерційні, урядові та інституційні установи. Саме тому цей розділ заглиблюється в історичний розвиток СКУД, розглядаючи фактори та технологічні досягнення, які сприяли еволюції цього поняття.

Основна функція перших примітивних СКУД полягала в забезпеченні базової безпеки шляхом обмеження доступу авторизованим особам за допомогою фізичних ключів [Учасники проектів Вікімедіа. (2017, January 27). Система контролю і управління доступом — Вікіпедія. Вікіпедія. https://uk.wikipedia.org/wiki/Система_контролю_і_управління_доступом]. Механічні замки використовувалися для захисту точок входу, таких як двері та ворота, а ключі були основним засобом надання доступу. Ці системи забезпечували певний рівень безпеки, але були обмеженими за своїми можливостями та вразливими місцями.

					ІТС.4КІ.0323.03-ПЗ			
Змн.	Арк.А	№ докум.№	Підпис	Дата				
Розроб.		Снежко О.Е.			РОЗДІЛ 1 ТЕОРЕТИЧНІ ЗАСАДИ ФУНКЦІОНУВАННЯ СИСТЕМ КОНТРОЛЮ, УПРАВЛІННЯ ДОСТУПОМ ТА РЕЄСТРАЦІЇ	Літ.	Арк.	Акрюшів
Керівник		Матієвський В.В.					6	16
Реценз.		Козуб Ю.Г.				ЛНУ Кафедра ІТС, Гр.4КІ		
Н. Контр.								
Зав. каф.		Семенов М.А.						

Одним з основних недоліків цих ранніх СКУД була вразливість до несанкціонованого дублювання ключів. Оскільки ключі були фізичними об'єктами, неавторизовані особи могли потенційно відтворити або підробити їх, що ставило під загрозу безпеку системи. Ця проблема становила значний виклик для ефективності контролю доступу, оскільки неавторизовані особи могли отримати доступ, використовуючи скопійовані або викрадені ключі.

Крім того, раннім версіям СКУД не вистачало комплексних можливостей моніторингу [7]. Не існувало механізму відстеження або реєстрації подій доступу, що ускладнювало встановлення того, хто входив або виходив з певної зони в той чи інший момент часу. Відсутність можливостей моніторингу не лише перешкоджала розслідуванню інцидентів безпеки, але й ускладнювала забезпечення підзвітності та дотримання політик контролю доступу.

Визнаючи обмеження цих ранніх СКУД, стала очевидною необхідність посилення заходів безпеки. Це усвідомлення призвело до розробки більш досконалих рішень, спрямованих на подолання вразливостей і недоліків механічних систем на основі замків і ключів. Подальша еволюція СКУД передбачала впровадження нових технологій і підходів для вирішення цих проблем, що в кінцевому підсумку призвело до створення сучасних систем контролю доступу.

Середина 20-го століття стала важливою віхою в еволюції систем фізичного контролю доступу (СКУД) та реєстрації подій з появою електромеханічних систем[3]. Ці системи запровадили використання компонентів з електричним живленням, таких як реле та соленоїди, для контролю доступу та ознаменували помітний перехід від суто механічних СКУД на основі замків та ключів.

					<i>ІТС.4КІ.0323.03-ПЗ</i>	Арк.
						7
Змн.	Арк.	№ докум.	Підпис	Дата		

Електромеханічні СКУД мали низку переваг над механічними аналогами. Однією з ключових переваг було посилення функцій безпеки, які вони забезпечували. Ці системи включали зчитувачі карток, клавіатури та комбінації кодів як механізми контролю доступу. Користувачі повинні були пред'явити фізичну картку або ввести код, щоб отримати доступ до захищених зон. Це створило додатковий рівень безпеки, оскільки залежність від фізичних ключів зменшилася. Зчитувачі карток і клавіатури дозволили використовувати більш складні механізми контролю доступу, такі як багатфакторна автентифікація, що ускладнило доступ стороннім особам.

Таким чином, використання компонентів з електричним живленням, таких як реле та соленоїди, дозволило створити більш складні механізми управління. Електромеханічні СКУД використовували ці компоненти для відмикання або замикання дверей і воріт у відповідь на пред'явлену картку або введений код. Ці компоненти діяли як електричні перемикачі, активуючи або деактивуючи механізм замка на основі наданих авторизованих облікових даних. Цей електричний механізм управління сприяв швидшому та надійнішому контролю доступу, зводячи до мінімуму можливість людської помилки при ручному управлінні замками [6].

Незважаючи на ці досягнення, електромеханічні СКУД все ще покладалися на фізичні ключі або картки, що обмежувало їх масштабованість і гнучкість. Кожній авторизованій особі потрібен був унікальний фізичний ключ або картка, що створювало проблеми в управлінні та розподілі цих облікових даних у великомасштабних системах. Крім того, у разі втрати або крадіжки ключа чи картки, їх потрібно було фізично замінити, що призводило до додаткових витрат і логістичних зусиль. Залежність від фізичних облікових даних також ускладнювала надання тимчасового доступу особам, які не мали фізичного ключа або картки, наприклад, відвідувачам або підрядникам.

					ІТС.4КІ.0323.03-ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		8

Крім того, централізоване управління та моніторинг електромеханічних СКУД створювали певні обмеження[21]. Оскільки ці системи працювали переважно в автономному режимі, події доступу та дані про них були важкодоступними і не зберігалися централізовано. Моніторинг у реальному часі та всебічний аудит було важко забезпечити, що ускладнювало відстеження та аналіз дій з доступу. Відсутність централізованого управління та моніторингу перешкоджала оперативному виявленню порушень безпеки та ефективному впровадженню політик контролю доступу.

Однак, інтеграція комп'ютерних технологій у системи фізичного контролю доступу (СКУД) наприкінці 20-го століття зробила революцію в цій галузі і відкрила нову еру передових можливостей контролю доступу. Комп'ютеризовані СКУД використовують цифрові технології для посилення безпеки, моніторингу та управління, пропонуючи значні переваги над попередніми електромеханічними системами.

Одним з ключових досягнень комп'ютеризованої системи контролю доступу стало впровадження безконтактної аутентифікації, смарт-карток і біометричних ідентифікаторів як засобів контролю доступу та реєстрації. Безконтактні картки, також відомі як безконтактні ключі або картки доступу, використовують технологію радіочастотної ідентифікації (RFID) для надання доступу. Ці картки за кодовані унікальними ідентифікаторами, які можуть зчитуватися зчитувачами, розташованими поблизу точок доступу. Смарт-картки, з іншого боку, мають вбудовані інтегральні схеми, які можуть зберігати та обробляти дані. Вони забезпечують більш комплексні можливості налаштування контролю доступу, такі як зберігання біометричної інформації або виконання криптографічних операцій. Біометричні ідентифікатори, такі як відбитки пальців або розпізнавання обличчя, забезпечують дуже безпечний і

надійний контроль доступу шляхом перевірки унікальних фізіологічних або поведінкових характеристик людей [5].

Комп'ютерні мережі відіграли ключову роль у забезпеченні централізованого управління та моніторингу доступу та реєстрації в режимі реального часу. Підключивши компоненти і пристрої СКУД, такі як зчитувачі карток і панелі контролю доступу, до центрального сервера або контролера, організації отримали більший контроль і нагляд за операціями контролю доступу. Централізоване управління дозволило адміністраторам легко налаштовувати та оновлювати політики контролю доступу, керувати обліковими даними користувачів та створювати вичерпні звіти. Можливості моніторингу в режимі реального часу сприяли миттєвому сповіщенню про спроби несанкціонованого доступу або порушення безпеки, що дало змогу швидко реагувати та усунути загрози.

Крім того, комп'ютеризована система управління доступом та реєстрації підвищила ефективність і масштабованість систем. Використання цифрових технологій усунуло потребу у фізичних ключах чи картках, зменшивши логістичні проблеми, пов'язані з управлінням та розповсюдженням облікових даних. Уповноваженим особам можна було надавати доступ віддалено, усуваючи необхідність фізичної присутності для видачі ключів або карток. Така масштабованість дозволила організаціям легко надавати або відкликати привілеї доступу, пристосовуючись до змін у персоналі або вимог до доступу.

Комп'ютеризована СКУД також уможливила інтеграцію з іншими системами безпеки, такими як відеоспостереження та системи виявлення вторгнень[7]. Обмінюючись даними та інтегруючи функції управління, ці системи працювали разом, підвищуючи загальну ефективність безпеки. Наприклад, більшість сучасних систем контролю доступу може активувати

					<i>ІТС.4КІ.0323.03-ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		10

запис з камер відеоспостереження при виявленні спроби несанкціонованого доступу, забезпечуючи комплексне реагування на загрозу безпеці.

За останні роки розвиток технологій систем контролю фізичного доступу (СКУД) призвів до значних змін у сфері контролю доступу. Ці досягнення відкрили нові можливості, підвищили зручність та покращили заходи безпеки. Серед ключових напрямків прогресу – бездротові протоколи зв'язку, хмарні сховища даних, інтеграція мобільних пристроїв та розвиток біометричних технологій.

Бездротові протоколи зв'язку відіграли вирішальну роль у розвитку технології СКУД. Традиційні дротові з'єднання були замінені або доповнені бездротовими протоколами, такими як Wi-Fi, Bluetooth і NFC (Near Field Communication). Бездротові компоненти СКУД, включаючи зчитувачі карток і панелі контролю доступу, тепер можуть безперешкодно обмінюватися даними, усуваючи необхідність в складних проводових установах. Таке з'єднання забезпечує більш гнучкі варіанти встановлення, знижує витрати на інфраструктуру та полегшує інтеграцію СКУД з іншими системами та пристроями.

Хмарні сховища стали ще однією революційною інновацією в технології СКУД та реєстрації. Завдяки використанню хмарних технологій, дані системи, включаючи облікові дані користувачів, журнали доступу та конфігурації системи, можна безпечно зберігати та отримувати до них доступ з віддалених місць. Такий хмарний підхід забезпечує централізоване управління і полегшує оновлення та синхронізацію в режимі реального часу між кількома пристроями та місцями розташування системи управління доступом. Адміністратори можуть віддалено керувати системами контролю доступу, надавати або відкликати привілеї доступу та аналізувати дані про доступ з будь-якого місця,

					ІТС.4КІ.0323.03-ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		11

де є підключення до Інтернету, оптимізуючи роботу та зменшуючи адміністративні накладні витрати [14].

Інтеграція мобільних пристроїв стає ще одним трендом у цьому контексті. З широким розповсюдженням смартфонів і планшетів доступ до систем СКУД та управління ними тепер можна отримати за допомогою мобільних додатків. Користувачі можуть використовувати свої мобільні пристрої як віртуальні облікові дані, замінюючи фізичні картки або ключі. Інтеграція мобільних пристроїв забезпечує більшу зручність для користувачів, оскільки їм більше не потрібно носити з собою кілька карток або ключів. Крім того, мобільні додатки можуть надавати додаткові функції безпеки, такі як двофакторна автентифікація або push-повідомлення про запити на доступ[7].

Крім того, біометрична автентифікація, така як розпізнавання відбитків пальців і обличчя, стала більш досконалою, надійною і широко застосовуваною технологією. Ці біометричні ідентифікатори забезпечують підвищений рівень безпеки завдяки перевірці унікальних фізіологічних або поведінкових характеристик людей. Біометричні системи СКУД усувають необхідність у фізичних облікових даних, зменшуючи ризик несанкціонованого доступу через загублені, вкрадені або дублікати карток чи ключів. Біометрична автентифікація також забезпечує вищий рівень точності та зменшує залежність від паролів або PIN-кодів, які можуть бути легко скомпрометовані, це також позитивно вплинуло на реєстрацію [17].

Отже, розвиток технологій СКУД здійснив революцію у сфері контролю доступу та реєстрації. Бездротові протоколи зв'язку, хмарні сховища, інтеграція мобільних пристроїв і вдосконалення біометричних технологій підвищили гнучкість, зручність і безпеку. Ці досягнення уможливили дистанційне керування, безперешкодну інтеграцію та більш надійні й точні методи ідентифікації. Оскільки технології продовжують розвиватися,

					<i>ІТС.4КІ.0323.03-ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		12

очікується подальший прогрес у сфері АСУ, що відкриває нові можливості та зміцнює загальний ландшафт безпеки.

1.2. Типологія та атрибути систем контролю управління доступом та реєстрації

Системи контролю фізичного доступу (СКД) відіграють вирішальну роль у захисті фізичних просторів та активів, регулюючи та контролюючи доступ до них. Цей розділ має на меті надати огляд типології та атрибутів СКУД. Типологія охоплює різні категорії, засновані на механізмах, технологіях і функціональних можливостях, що застосовуються в системах контролю доступу. Крім того, атрибути СКУД охоплюють ключові характеристики та особливості, які сприяють їхній ефективності та надійності. Розуміння типології та атрибутів СКУД є важливим для проектування, впровадження та оцінки систем контролю доступу в різних середовищах.

Як вже було зазначено раніше, **Типологія СКУД** охоплює різні категорії, які класифікують системи контролю доступу на основі їхніх механізмів, технологій та функціональних можливостей. Для опису типології СКУД зазвичай використовують наступні категорії (таблиця 1.1).

Таблиця 1.1

Типологія систем контролю фізичного доступу

Категорії типології	Опис
Механічні системи контролю доступу	Покладається на традиційні механізми контролю доступу за допомогою замків і ключів. Забезпечує базову безпеку, але не має розширених функцій моніторингу.

Електро механічні системи контролю доступу	Використовує компоненти з електричним живленням (наприклад, зчитувачі карток, клавіатури) для контролю доступу. Забезпечує підвищену безпеку та операційну ефективність.
Комп'ютеризовані системи контролю доступу	Використовує цифрові технології та комп'ютерні мережі для розширених можливостей контролю доступу. Підтримує централізоване управління та моніторинг у режимі реального часу.
Бездротові системи контролю доступу	Використовує бездротові протоколи зв'язку (наприклад, Wi-Fi, Bluetooth) для безперебійного підключення та гнучких можливостей встановлення. Забезпечує можливості масштабування та інтеграції.

Джерело: складено автором за [7; 17].

1. **Механічні СКУД** покладаються на традиційні механізми замків і ключів для контролю доступу. Ці системи використовують фізичні ключі, замки та циліндри для обмеження доступу і вимагають ручного керування для надання або заборони доступу. Хоча механічні СКУД забезпечують базовий рівень безпеки, їм бракує розширених функцій, таких як моніторинг та аудит.

2. **Електро механічні СКУД** включають компоненти з електричним живленням, такі як реле та електромагніти, для контролю доступу. Ці системи зазвичай використовують зчитувачі карток, клавіатури або комбінації кодів для автентифікації користувачів. Електро механічні СКУД пропонують підвищену безпеку та операційну ефективність порівняно з механічними системами.

3. **Комп'ютеризовані СКУД** використовують цифрові технології та комп'ютерні мережі для розширення можливостей систем контролю доступу. Ці системи використовують безконтактні картки, смарт-картки або

біометричні ідентифікатори для автентифікації. Централізоване управління, моніторинг у реальному часі та інтеграція з іншими системами безпеки є ключовими особливостями комп'ютеризованої СКУД.

4. **Бездротові СКУД** використовують протоколи бездротового зв'язку, такі як Wi-Fi, Bluetooth або NFC, щоб забезпечити безперебійне підключення та зв'язок між компонентами СКУД. Ці системи пропонують гнучкі можливості встановлення, масштабування та інтеграції.

Атрибути систем контролю фізичного доступу

Атрибути СКУД охоплюють ключові характеристики та особливості, які сприяють їхній ефективності та надійності. Наступні атрибути є вирішальними факторами при оцінці систем контролю доступу (таблиця 1.2).

Таблиця 1.2

Атрибути систем контролю фізичного доступу

Атрибут	Опис
Безпека	Забезпечує доступ до зон з обмеженим доступом лише авторизованим особам. Включає методи автентифікації, шифрування та механізми захисту від несанкціонованого доступу.
Масштабованість і гнучкість	Здатність пристосовуватися до змін в потребах організації, таких як плинність кадрів і розширення об'єктів. Також відноситься до адаптивності до різних середовищ і політик контролю доступу.
Юзабіліті та користувацький досвід	Зручний інтерфейс та інтуїтивно зрозумілі механізми взаємодії. Враховує простоту використання, ефективність процесів автентифікації та зрозумілість зворотного зв'язку системи.

Інтеграція та інтероперабельність	Можливість інтеграції з іншими системами безпеки (наприклад, відеоспостереження, виявлення вторгнень) та безперешкодна функціональна сумісність для покращення загального управління та аналізу безпеки.
Моніторинг та аудит	Моніторинг подій доступу в реальному часі та комплексний аудит для відстеження та розслідування порушень безпеки. Підтримує комплаєнс, виявлення інцидентів та аналіз після інцидентів.

Джерело: складено автором за [1].

1. **Безпека** – це фундаментальний атрибут СКД, який гарантує, що тільки авторизовані особи можуть отримати доступ до зон з обмеженим доступом. Надійність заходів безпеки, таких як методи автентифікації, шифрування та механізми захисту від несанкціонованого доступу, визначає здатність системи запобігати несанкціонованому доступу та зменшувати ризики безпеки.

2. **Масштабованість та гнучкість:** система управління доступом повинна бути спроектована таким чином, щоб пристосовуватися до змін в потребах організації, таких як плинність кадрів, розширення об'єкту або зміна вимог до контролю доступу. Масштабованість означає здатність системи обробляти зростаючу кількість користувачів, точок доступу та даних, тоді як гнучкість стосується адаптивності системи до різних середовищ та політик контролю доступу.

3. **Юзабіліті та користувацький досвід:** СКУД має забезпечувати зручний інтерфейс та інтуїтивно зрозумілі механізми взаємодії для користувачів. Простота використання, ефективність процесів автентифікації та

чіткість зворотного зв'язку системи суттєво впливають на досвід користувачів та загальне сприйняття системи.

4. Інтеграція та інтероперабельність: система повинна мати можливість інтегруватися з іншими системами безпеки, такими як відеоспостереження, виявлення вторгнень або системами управління ідентифікацією. Безперешкодна інтероперабельність підвищує загальний рівень безпеки та дозволяє здійснювати комплексне управління та аналіз подій і даних про безпеку.

5. Моніторинг та аудит: СКУД також повинна забезпечувати моніторинг у режимі реального часу та комплексний аудит для відстеження подій доступу, виявлення порушень безпеки та підтримки судових розслідувань. Моніторинг та можливість аудиту мають вирішальне значення для забезпечення дотримання політик контролю доступу, виявлення інцидентів безпеки та полегшення аналізу після інцидентів, при цьому важливу роль грає реєстрація подій.

Таким чином, розуміння типології та атрибутів систем фізичного контролю доступу має важливе значення для розробки, впровадження та оцінки рішень контролю доступу в різних середовищах. Враховуючи цю типологію та атрибути, організації можуть приймати обґрунтовані рішення при виборі та впровадженні систем контролю доступу для задоволення своїх специфічних вимог до безпеки.

1.3. Завдання, функції, цілі та вимоги до системи контролю управління доступом та реєстрацією готельного підприємства

					ІТС.4КІ.0323.03-ПЗ	Арк.
						17
Змн.	Арк.	№ докум.	Підпис	Дата		

У цьому розділі розглядаються завдання, функції, цілі та вимоги до системи контролю доступу та реєстрації в контексті готельного підприємства. Оскільки готелі є динамічним середовищем з різноманітними потребами в контролі доступу, впровадження ефективної СКУД має вирішальне значення для забезпечення безпеки, зручності та операційної ефективності закладу. У цьому дослідженні розглядаються конкретні завдання, які виконує СКУД, її основні функції, основні цілі, яких вона має досягти, а також ключові вимоги, яким вона повинна відповідати, щоб задовольнити унікальні вимоги до контролю доступу на готельному підприємстві.

Системи контролю доступу є основою інфраструктури безпеки готельних підприємств. Ці системи контролюють і регулюють доступ до різних зон на території готелю, захищаючи гостей, персонал і цінні активи.

Завдання системи контролю доступу та реєстрації

СКУД на готельному підприємстві виконує кілька важливих завдань для підтримки ефективного контролю доступу. До таких завдань відносяться:

1. Автентифікація: перевірка особи осіб, які бажають отримати доступ до зон з обмеженим доступом, таких як гостьові кімнати, зони для працівників або секретні операційні зони. Це завдання гарантує, що доступ буде надано лише уповноваженим особам.

2. Авторизація: визначення привілеїв доступу осіб на основі їхньої ролі, рівня допуску або конкретних дозволів. Передбачає надання відповідних прав доступу різним категоріям користувачів.

3. Моніторинг: відстеження та реєстрація подій доступу, включаючи успішні входи, спроби порушень та підозрілі дії. Моніторинг допомагає підтримувати обізнаність про ситуацію та виявляти інциденти безпеки.

4. Управління тривогами та оповіщеннями: швидке та ефективне реагування на тривоги, сповіщення про вторгнення або збої в роботі системи.

					<i>ІТС.4КІ.0323.03-ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		18

Це завдання дозволяє вчасно втрутитися та вжити відповідних заходів у критичних ситуаціях [4].

Функції системи контролю доступу та реєстрації

Також СКУД на готельному підприємстві виконує кілька життєво важливих функцій для забезпечення комплексного контролю доступу. До таких функцій відносяться:

1. Управління фізичним доступом: регулювання доступу до різних зон у готелі, зокрема до номерів, загальних приміщень, приміщень, призначених лише для персоналу, та приміщень з обмеженим доступом. Ця функція охоплює надання або заборону доступу, контроль доступу за часом та управління відвідувачами.

2. Інтеграція з готельними системами: інтеграція СКУД з іншими системами готелю, такими як системи управління нерухомістю (PMS), відеоспостереження, сигналізація та системи автоматизації будівлі. Така інтеграція забезпечує скоординоване реагування на загрози безпеці, обмін даними та підвищення операційної ефективності.

3. Аудит і звітність: створення детальних звітів і аудиторських слідів про дії доступу, включаючи спроби доступу, успішні входи, відмову в доступі та системні події. Ці звіти підтримують дотримання нормативних вимог, розслідування інцидентів та оцінку ефективності.

4. Управління користувачами: адміністрування облікових записів користувачів, облікових даних та привілеїв доступу в рамках СКУД. Ця функція включає реєстрацію користувачів, видачу облікових даних, анулювання та ведення баз даних контролю доступу та реєстрації.

Цілі системи контролю доступу та реєстрації

Основними цілями СКУД на готельному підприємстві є:

					ІТС.4КІ.0323.03-ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		19

1. Забезпечення безпеки: захист гостей, персоналу, активів та чутливих зон від несанкціонованого доступу, крадіжок та порушень безпеки.

2. Покращення досвіду гостей: забезпечення зручного і безперешкодного доступу до номерів, зручностей і послуг, зберігаючи при цьому належний рівень безпеки та конфіденційності.

3. Підвищення операційної ефективності: спрощення процесів контролю доступу, зменшення адміністративних витрат і забезпечення ефективного моніторингу та управління подіями доступу та реєстрації.

Вимоги до системи контролю доступу та реєстрації

Щоб ефективно задовольнити потреби готельного підприємства в контролі доступу, СКУД повинна відповідати певним вимогам, в тому числі:

1. Масштабованість: пристосування до динамічної природи готельного середовища шляхом легкого масштабування системи для підтримки мінливих вимог до доступу та пристосування до майбутнього зростання.

3. Можливості інтеграції: безперешкодна інтеграція з іншими системами готелю, такими як системами відеоспостереження та сигналізації, для забезпечення комплексного управління безпекою та обміну інформацією.

3. Забезпечення інтуїтивно зрозумілого та зручного інтерфейсу для адміністраторів, персоналу та гостей, щоб полегшити безперебійну роботу та сприйняття системи.

4. Комплаєнс (система відгуків) і конфіденційність даних: забезпечення дотримання відповідних галузевих норм і стандартів конфіденційності даних для захисту особистої інформації та дотримання правових і етичних зобов'язань.

Висновки до розділу 1

1. Генезис СКУД та реєстрації можна простежити від простих механічних замків до складних комп'ютеризованих систем з розширеними

					ІТС.4КІ.0323.03-ПЗ	Арк.
						20
Змн.	Арк.	№ докум.	Підпис	Дата		

функціями безпеки. Еволюція СКУД була зумовлена потребою в підвищенні безпеки, зручності та масштабованості. Завдяки інтеграції комп'ютерних технологій, бездротового зв'язку та біометричної автентифікації, СКУД стали незамінним компонентом сучасних систем безпеки. Однак постійні виклики та поява нових технологій створюють можливості для подальшого розвитку та інтеграції, гарантуючи, що СКУД залишатиметься на передовій рішень у сфері контролю доступу та реєстрації.

2. Розуміння типології та атрибутів систем фізичного контролю доступу має важливе значення для розробки, впровадження та оцінки рішень контролю доступу в різних середовищах. Типологія охоплює категорії, засновані на механізмах, технологіях і функціональних можливостях, що застосовуються в СКУД, починаючи від традиційних механічних систем і закінчуючи сучасними комп'ютеризованими та бездротовими системами. Атрибути АСУ охоплюють такі ключові характеристики, як безпека, масштабованість, зручність використання, інтеграція та моніторинг. Враховуючи цю типологію та атрибути, організації можуть приймати обґрунтовані рішення при виборі та впровадженні систем контролю доступу для задоволення своїх специфічних вимог до безпеки.

3. На готельному підприємстві ефективна система контролю доступу та реєстрації відіграє життєво важливу роль у забезпеченні безпеки, зручності та операційної ефективності закладу. Розуміючи завдання, функції, цілі та вимоги, характерні для СКУД в готельному контексті, зацікавлені сторони можуть розробляти, впроваджувати та оцінювати рішення для контролю доступу, які задовольняють унікальні потреби готельного підприємства в контролі доступу.

РОЗДІЛ 2. МЕТОДОЛОГІЯ ТА РОЗРОБКА ТЕХНОЛОГІЇ НА ОСНОВІ ARDUINO ДЛЯ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ ТА РЕЄСТРАЦІЇ ГОТЕЛЮ

2.1. Дизайн та методи розробки системи

У цьому розділі описано методологію та процес розробки технології на основі Arduino для системи контролю фізичного доступу в готелі. Обговорюється дизайн і методи, використані при розробці цієї системи, надається уявлення про загальний підхід, апаратні та програмні компоненти, а також процедури тестування. Використовуючи технологію Arduino, це дослідження має на меті створити економічно ефективне та економічно вигідне рішення для підвищення безпеки та ефективності системи контролю доступу в готелі.

Підхід до розробки технології АСУ на базі Arduino включав наступні етапи:

					ІТС.4КІ.0323.03-ПЗ				
Змн.	Арк.	№ докум.	Підпис	Дата					
Розроб.		Снежко О.Е.			РОЗДІЛ 2 МЕТОДОЛОГІЯ ТА РОЗРОБКА ТЕХНОЛОГІЇ НА ОСНОВІ ARDUINO ДЛЯ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ ТА РЕЄСТРАЦІЇ ГОТЕЛЮ		Лім.	Арк.	Акрушіє
Керівник		Матієвський В.В.						22	28
Реценз.		Козуб Ю.Г.					ЛНУ Кафедра ІТС, Гр.4КІ		
Н. Контр.									
Зав. каф.		Семенов М.А.							

1. Аналіз вимог – критично важливий етап у розробці системи контролю фізичного доступу готелю. Він передбачає проведення ретельного аналізу потреб у контролі доступу та вимог, характерних для середовища готелю. Цей процес включає визначення ключових зацікавлених сторін, розуміння політики контролю доступу та визначення бажаних функціональних можливостей системи. Нижче наведено детальне пояснення кожного аспекту процесу аналізу вимог:

1.1. Визначення ключових зацікавлених сторін є важливим компонентом процесу аналізу вимог. В нашому випадку зацікавлені сторони – це керівництво готелю, персонал служби безпеки, співробітники і навіть регулюючі органи. Кожна група зацікавлених сторін має унікальні погляди та вимоги щодо контролю доступу. Взаємодіючи з цими зацікавленими сторонами, можна виявити певні проблеми системи, очікування та конкретні потреби в контролі доступу. Ця інформація має вирішальне значення для розробки системи, яка відповідає загальним цілям і завданням готелю.

1.2. Розуміння існуючих політик контролю доступу в готелі має важливе значення для розробки ефективної системи управління доступом. Політика контролю доступу окреслює правила та норми, що регулюють доступ до різних зон у приміщенні готелю. Це можуть бути номери, загальні приміщення, адміністративні офіси, комори та зони з обмеженим доступом. Ретельно вивчивши та зрозумівши ці політики, можна налаштувати систему контролю доступу так, щоб вона відповідала конкретним вимогам до контролю доступу, продиктованим політикою готелю. Це може включати такі функції, як обмеження доступу за часом, ієрархічні рівні доступу, протоколи управління відвідувачами та процедури екстреного доступу.

1.3. Методи автентифікації, а саме визначення бажаних методів автентифікації для надання доступу авторизованим особам. Це можуть бути

RFID-картки, коди ключів, біометричні ідентифікатори (наприклад, відбитки пальців або розпізнавання обличчя) або комбінація декількох методів.

1.4. Привілеї та ієрархія доступу: встановлення ієрархії привілеїв доступу для різних осіб у готелі. Сюди входить визначення ролей та дозволів працівників, гостей та інших зацікавлених сторін. Наприклад, гість може мати доступ до закріпленого за ним номера, тоді як менеджер може мати доступ до додаткових приміщень, наприклад, бек-офісу.

1.5. Інтеграція з існуючими системами: оцінка необхідності інтеграції з іншими існуючими системами готелю. Інтеграція дозволяє покращити координацію безпеки та обмін даними між різними системами.

1.6. Моніторинг та звітування: визначення рівня моніторингу та звітування, необхідного для діяльності з контролю доступу. Це може включати моніторинг подій доступу в реальному часі, створення аудиторських слідів та створення звітів для управлінських або регуляторних цілей.

1.7. Масштабованість і майбутнє розширення: врахування потенційного зростання і майбутніх потреб готелю. АСУ має бути масштабованою, щоб врахувати зміни в інфраструктурі готелю, такі як додаткові номери, нові зони або розширення об'єктів, та нові вимоги до реєстрації

Завдяки ретельному аналізу вимог, проектування та розробка СКУД можуть бути узгоджені з конкретними потребами та політикою контролю доступу в готелі. Це гарантує, що система буде адаптована до унікальних вимог і очікувань зацікавлених сторін, забезпечуючи при цьому безпечне та ефективне рішення для контролю доступу та реєстрації.

2. Процес вибору обладнання має вирішальне значення для створення надійної та ефективної системи контролю фізичного доступу (СКУД) для готелю. На цьому етапі обираються відповідні апаратні компоненти, які

					ІТС.4КІ.0323.03-ПЗ	Арк.
						24
Змн.	Арк.	№ докум.	Підпис	Дата		

відповідають вимогам системи СКУД. Нижче наведено детальну інформацію про процес вибору обладнання:

2.1. Мікроконтролери Arduino:

Мікроконтролери Arduino обирають за їхню доступність, універсальність і сумісність з різними датчиками та периферійними пристроями. Плати Arduino – це економічно ефективне рішення без шкоди для функціональності. Вони забезпечують зручне середовище для програмування та пропонують широкий спектр можливостей вводу та виводу, що робить їх придатними для реалізації функцій контролю доступу. Платформа Arduino також підтримує велику спільноту розробників, забезпечуючи доступність ресурсів та підтримку.

2.2. RFID-зчитувачі:

Зчитувачі RFID (радіочастотної ідентифікації) є ще одним важливим компонентом для автентифікації в СКУД. Вони зчитують інформацію, що зберігається на RFID-картках або мітках, і дозволяють доступ на основі унікальної ідентифікації картки. RFID-зчитувачі вибираються на основі їх сумісності з мікроконтролерами Arduino, а також бажаного діапазону і частоти роботи. Ці зчитувачі забезпечують швидку та безконтактну ідентифікацію, підвищуючи зручність та ефективність процесу контролю доступу.

2.3. Електронні замки:

Електронні замки замінюють традиційні механічні замки і забезпечують безпечний контроль доступу до приміщень у готелі. При виборі електронних замків вирішальним фактором є сумісність з мікроконтролерами Arduino. Замки повинні легко інтегруватися з платформою Arduino, щоб отримувати інструкції для блокування або розблокування на основі рішень про контроль доступу, прийнятих системою. Слід враховувати тип замикаючого механізму

(наприклад, електромагнітні замки або електрозамки) і сумісність з фурнітурою дверей або воріт.

2.4. Модулі вводу/виводу:

Модулі вводу та виводу розширюють можливості системи СКУД. Ці модулі взаємодіють з різними датчиками, виконавчими пристроями та периферійними пристроями. Прикладами модулів вводу є датчики руху, датчики дверей і клавіатури, а модулі виводу можуть включати світлодіодні дисплеї, сигнали тривоги або модулі зумера. Вибір модулів вводу/виводу ґрунтується на сумісності з мікроконтролерами Arduino та конкретних вимогах системи контролю доступу.

3. Етап розробки програмного забезпечення передбачає створення програмної інфраструктури, необхідної для підтримки функціональності системи. В процесі розробки програмного забезпечення розглядаються наступні аспекти:

3.1. Програмування Arduino:

Мікроконтролери Arduino програмуються за допомогою інтегрованого середовища розробки Arduino (IDE). Використовувана мова програмування – спрощена версія C/C++. Розробка програмного забезпечення передбачає написання коду для обробки різних функцій СКУД, таких як зчитування даних з RFID-зчитувачів, обробка алгоритмів автентифікації та керування електронними замками (Додаток А, Додаток Б) [9; 18; 20].

3.2. Дизайн інтерфейсу користувача:

Дизайн інтерфейсу користувача зосереджений на створенні інтуїтивно зрозумілих і зручних інтерфейсів для управління системою. Це включає розробку графічних інтерфейсів для адміністраторів для управління дозволами доступу, моніторингу подій доступу та створення звітів. Крім того, користувацькі інтерфейси призначені для автентифікації користувачів та

					ІТС.4КІ.0323.03-ПЗ	Арк.
						26
Змн.	Арк.	№ докум.	Підпис	Дата		

отримання доступу до авторизованих областей. Інтерфейси повинні бути візуально привабливими, зручними для навігації та забезпечувати безперебійну роботу користувачів.

3.3. Впровадження правил контролю доступу:

Процес розробки програмного забезпечення включає впровадження правил контролю доступу та реєстрації на основі вимог і політик готелю. Це передбачає визначення логіки надання або заборони доступу на основі результатів автентифікації, привілеїв доступу та часових обмежень. Реалізуються алгоритми для забезпечення дотримання правил контролю доступу, гарантуючи, що тільки авторизовані особи можуть отримати доступ до певних зон.

3.4. Реєстрація подій та звітність:

Розробка програмного забезпечення включає в себе реалізацію функцій реєстрації подій та звітування. Це включає в себе фіксацію та реєстрацію подій доступу, таких як успішні входи, спроби відмови у доступі та системні події. Ці журнали надають історичні дані про дії доступу, допомагаючи в розслідуванні порушень безпеки та дотриманні нормативних вимог. Крім того, можна створювати звіти, які дають уявлення про шаблони доступу, продуктивність системи та відповідність політикам контролю доступу.

Підібравши відповідні апаратні компоненти та розробивши необхідну програмну інфраструктуру, система СКУД може ефективно автентифікувати користувачів, забезпечувати дотримання правил контролю доступу, а також надавати комплексні можливості реєстрації подій та звітності. Поєднання мікроконтролерів Arduino, зчитувачів RFID, електронних замків і модулів вводу/виводу разом з програмним забезпеченням, розробленим спеціально для СКУД, забезпечує надійну та ефективну систему контролю фізичного доступу для готелю.

					<i>ITC.4KI.0323.03-ПЗ</i>	Арк.
						27
Змн.	Арк.	№ докум.	Підпис	Дата		

Таким чином, розробка СКУД на базі Arduino включала наступні ключові етапи:

1. Апаратна інтеграція: інтеграція вибраних апаратних компонентів з мікроконтролерами Arduino. Це включає підключення зчитувачів RFID, електронних замків та інших датчиків або виконавчих пристроїв відповідно до вимог контролю доступу в готелі.

2. Програмна реалізація: програмування мікроконтролерів Arduino за допомогою інтегрованого середовища розробки (IDE) Arduino для реалізації необхідних функцій. Це включало розробку модулів коду для автентифікації RFID-карт, прийняття рішень щодо контролю доступу, реєстрації подій та інтерфейсів управління системою.

3. Дизайн інтерфейсу користувача: розробка користувацьких інтерфейсів для полегшення управління та моніторингу системи. Це включало розробку графічних інтерфейсів для адміністраторів для управління дозволами доступу, моніторингу подій доступу та створення звітів.

4. Тестування та оцінка: Проведення тестування для забезпечення функціональності, надійності та безпеки розробленої системи. Це включає проведення модульного тестування окремих програмних компонентів, інтеграційне тестування апаратних і програмних модулів, а також комплексне наскрізне тестування для імітації реальних сценаріїв.

Отже, у цьому розділі було розглянуто методи проектування та розробки, використані в цій системі, що дає цінну інформацію про загальний підхід, використані апаратні та програмні компоненти, а також проведені процедури тестування. Основною метою цього дослідження є використання технології Arduino для створення економічно ефективного та гнучкого рішення, яке підвищує безпеку та ефективність системи контролю доступу в готелі.

2.2. Опис та аналіз системи

У цьому розділі представлено детальний опис та аналіз впровадження технологій на основі Arduino для розробки систем контролю доступу та реєстрації в готелях. Arduino, електронна платформа з відкритим вихідним кодом, пропонує економічно ефективне та універсальне рішення для проектування та розгортання таких систем. У дослідженні розглядаються ключові компоненти та функціональні можливості систем контролю доступу на основі Arduino, підкреслюється їх потенціал для підвищення безпеки, ефективності та зручності в готельному середовищі. Крім того, в аналізі розглядаються проблеми та обмеження, пов'язані з цією технологією, а також потенційні шляхи для майбутніх досліджень і розробок.

					ІТС.4КІ.0323.03-ПЗ	Арк.
						29
Змн.	Арк.	№ докум.	Підпис	Дата		

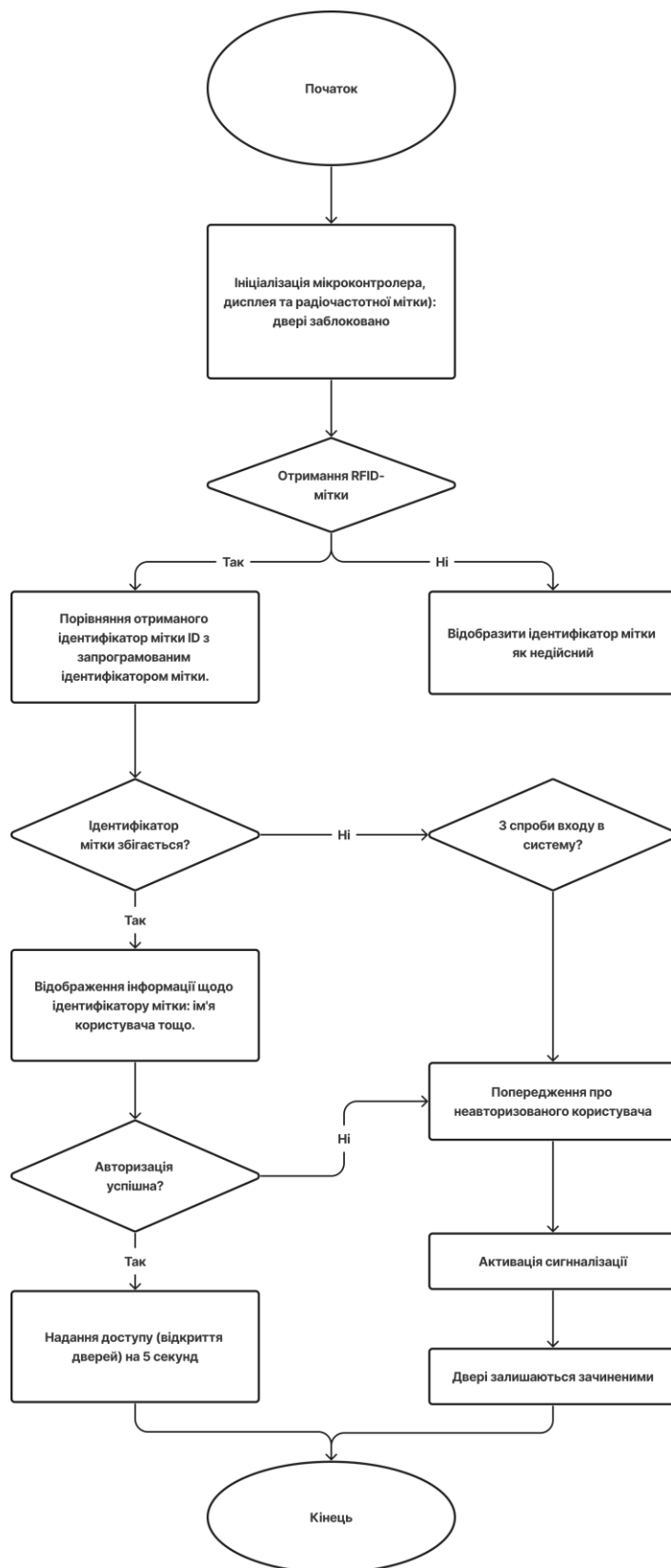


Рис. 2.1. Блок-схема проекту

ЗМН.	Арк.	№ докум.	Підпис	Дата

ІТС.4КІ.0323.03-ПЗ

Арк.

30

Джерело: складено автором за [2].

Системи RFID складаються з трьох компонентів у двох комбінаціях: трансивер (передавач/приймач) і антена, які зазвичай об'єднуються в RFID-зчитувач. Транспондер (передавач/відповідач) і антена об'єднуються для створення RFID-мітки. RFID-мітка зчитується, коли зчитувач випромінює радіосигнал, який активує транспондер, що надсилає дані назад до приймача [19].

Базова система RFID складається з трьох компонентів:

- антена або котушка
- трансивер (з декодером)
- транспондер (радіочастотна мітка), запрограмований в електронному вигляді з унікальною інформацією

На найпростішому рівні, RFID – це бездротовий зв'язок для унікальної ідентифікації об'єктів або людей. Іноді його називають спеціальним зв'язком на короткі відстані (DSRC). Системи RFID включають в себе електронні пристрої, які називаються транспондери або мітки, а також зчитувальні пристрої для зв'язку з мітками. Ці системи взаємодіють за допомогою радіосигналів, які передають дані в односпрямованому або двоспрямованому режимі. Як показано на рис. 2.2, коли транспондер потрапляє в зону зчитування, його дані зчитуються зчитувачем, а потім можуть бути передані через стандартні інтерфейси на хост-комп'ютер або запрограмований логічний контролер для зберігання або дії.

					ІТС.4КІ.0323.03-ПЗ	Арк.
						31
Змн.	Арк.	№ докум.	Підпис	Дата		

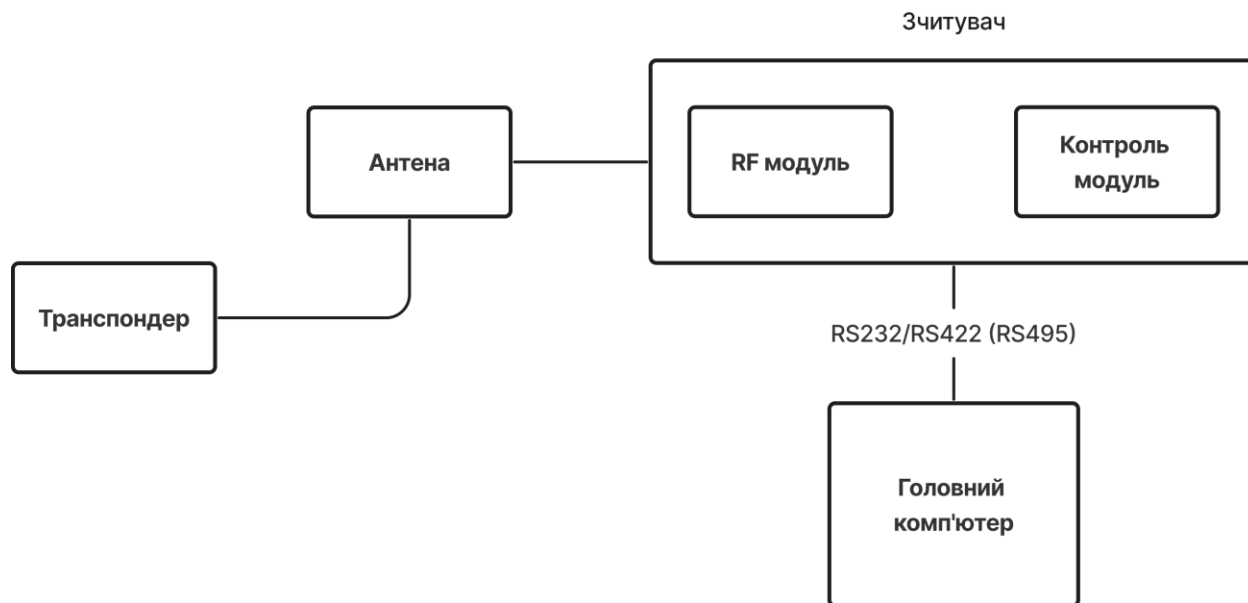


Рис. 2.2 Робота RFID

Джерело: [18; 19].

Переваги технології RFID:

Для зчитування мітка не повинна знаходитися в зоні прямої видимості приймача (на відміну від штрих-коду та його оптичного сканеру). . RFID-мітки можуть зберігати велику кількість інформації та мають можливість точно визначати місцезнаходження. Технологія є універсальною: може бути меншою за ніготь великого пальця, а може бути розміром з планшет, залежно від її використання. Однак, є певні недоліки, зокрема активна RFID може бути дорогою через батареї. Крім того, існує занепокоєння щодо конфіденційності пристроїв RFID. RFID можна легко перехопити, навіть якщо мітка зашифрована, а програмування пристроїв RFID займає багато часу.

У RFID-мітці присутні два основні компоненти:

- 1) невеликий кремнієвий чіп або інтегральна схема, яка містить унікальний ідентифікаційний номер (ID);
- 2) антена, яка може надсилати та приймати радіохвилі.

Ці два компоненти можуть бути крихітними: антена складається з плоскої металевої провідної котушки, а не виступаючої антени в стилі FM-радіостанцій, а чіп потенційно може бути менше півміліметра. Ці два компоненти зазвичай прикріплені до плоскої пластикової бирки, яку можна прикріпити до фізичного об'єкта. Ці мітки можуть бути досить маленькими, тонкими і все частіше легко вбудовуються в упаковку, пластикові картки, квитки, етикетки на одязі, палети, книги тощо.

У контексті цього проекту ми розрізняємо 3 типи RFID-міток по відношенню до потужності або енергії:

- пасивні;
- напівпасивні;
- активні [19].



Рис. 2.3. Пасивна мітка RFID

Джерело: [19].

Пасивні мітки не мають внутрішнього джерела живлення, тому вони покладаються на енергію, індуковану зчитувачем. Це означає, що зчитувач повинен підтримувати своє поле до завершення транзакції. Через відсутність батареї ці мітки є найменшими і найдешевшими з доступних міток, але це також обмежує діапазон зчитування від 2 мм до декількох метрів. Як додаткова перевага, ці мітки також підходять для друку. Крім того, термін їх служби необмежений, оскільки вони не залежать від внутрішнього джерела живлення.

Другий тип міток – це напівпасивні мітки. Ці мітки мають внутрішнє джерело живлення, завдяки якому мікросхемі постійно перебуває під напругою, що має багато переваг. По-перше, оскільки мікросхема завжди живиться, вона може швидше реагувати на запити, збільшуючи таким чином кількість міток, які можуть бути опитані за секунду. Крім того, оскільки антена не потрібна для збору енергії, її можна оптимізувати для зворотного розсіювання і, таким чином, збільшити дальність зчитування. І останнє, але не менш важливе: оскільки мітка не використовує енергію поля, сигнал зворотного розсіювання сильніший, що ще більше збільшує дальність зчитування. Завдяки останнім двом причинам, напівактивна мітка зазвичай має більший радіус дії, ніж пасивна мітка.

Третій тип міток – активні мітки. Як і напівактивні мітки, вони містять внутрішнє джерело живлення, але використовують енергію, що подається, для живлення мікросхеми і для генерації сигналу на антені. Активні мітки, які надсилають сигнали без запиту, називаються маяками. Радіус дії активних міток може становити десятки метрів, що робить їх ідеальними для визначення місцезнаходження об'єктів або використання в якості орієнтирів. Термін служби до 5 років [19].

За частотою використання RFID-мітки поділяються на три типи:

- низька частота (НЧ, 30-500 кГц)
- висока частота (ВЧ, 10-15 МГц)
- надвисока частота (UHF, 850-950 МГц, 2,4-2,5 ГГц, 5,8 ГГц)

Rfid зчитувач

Зчитувач – це портативний або стаціонарний пристрій, який може опитувати сусідні RFID-мітки та отримувати їхні ідентифікаційні номери за допомогою радіочастотного (РЧ) зв'язку (тобто процес не потребує контакту) [8]. Коли пасивна мітка знаходиться в межах досяжності зчитувача, антена

					<i>ITC.4KI.0323.03-ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		34

мітки поглинає енергію, що випромінюється зчитувачем, спрямовує її на запуск інтегральної схеми на мітці, яка потім використовує цю енергію для передачі назад ідентифікаційного номера та будь-якої іншої пов'язаної з ним інформації.

Існує два основних класи зчитувачів RFID: зчитувачі тільки для читання, наприклад, ті, що працюють з чисто пасивними мітками EPC класу I, і зчитувачі читання-запису, які можуть записувати нову інформацію на мітку, оснащену пам'яттю для читання/запису хі. Зчитувачі стають все більш досконалими, діючи як шлюзи до мережевих комунікаційних систем модемних підприємств, підтримуючи протоколи зв'язку, такі як TCP/IP, і мережеві технології, такі як DHCP, UDP/IP і Ethernet (для бездротового відправлення даних назад на підприємство). Багато моделей зчитувачів є ручними пристроями і нагадують цінники або сканери штрих-кодів, що використовуються в супермаркетах, але зчитувачі також можуть бути закріплені на місці (наприклад, у дверних отворах або на пунктах збору плати за проїзд) і навіть приховані, наприклад, вбудовані в стелю або стіни.

Існують також зчитувачі, які можна вбудувати в кишенькові пристрої, такі як КПК і мобільні телефони, і, крім того, мітки класу 5 також відомі як зчитувачі – пристрої, які можуть зчитувати інші RFID-мітки і обмінюватися з ними даними [8].

					<i>ITC.4Kl.0323.03-ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		35



Рис. 2.4. Модулі зчитування EM-18

Джерело: [12].

RFID-зчитувач EM-18 є одним з найпоширеніших зчитувачів для зчитування міток 125KHz. Він має низьку вартість, низьке енергоспоживання, малий форм-фактор і простий у використанні. Він забезпечує вихідні формати UART та Wiegand26. Він також може безпосередньо підключатися до мікроконтролерів за допомогою UART і до ПК за допомогою конвертера RS232. Модуль випромінює 125 КГц через свої котушки, і коли пасивна RFID-мітка 125 КГц потрапляє в це поле, вона отримує енергію від цього поля. Ці пасивні RFID-мітки в основному складаються з CMOS-мікросхеми EM4102,

яка може отримувати достатньо енергії для своєї роботи від поля, що генерується зчитувачем [12].

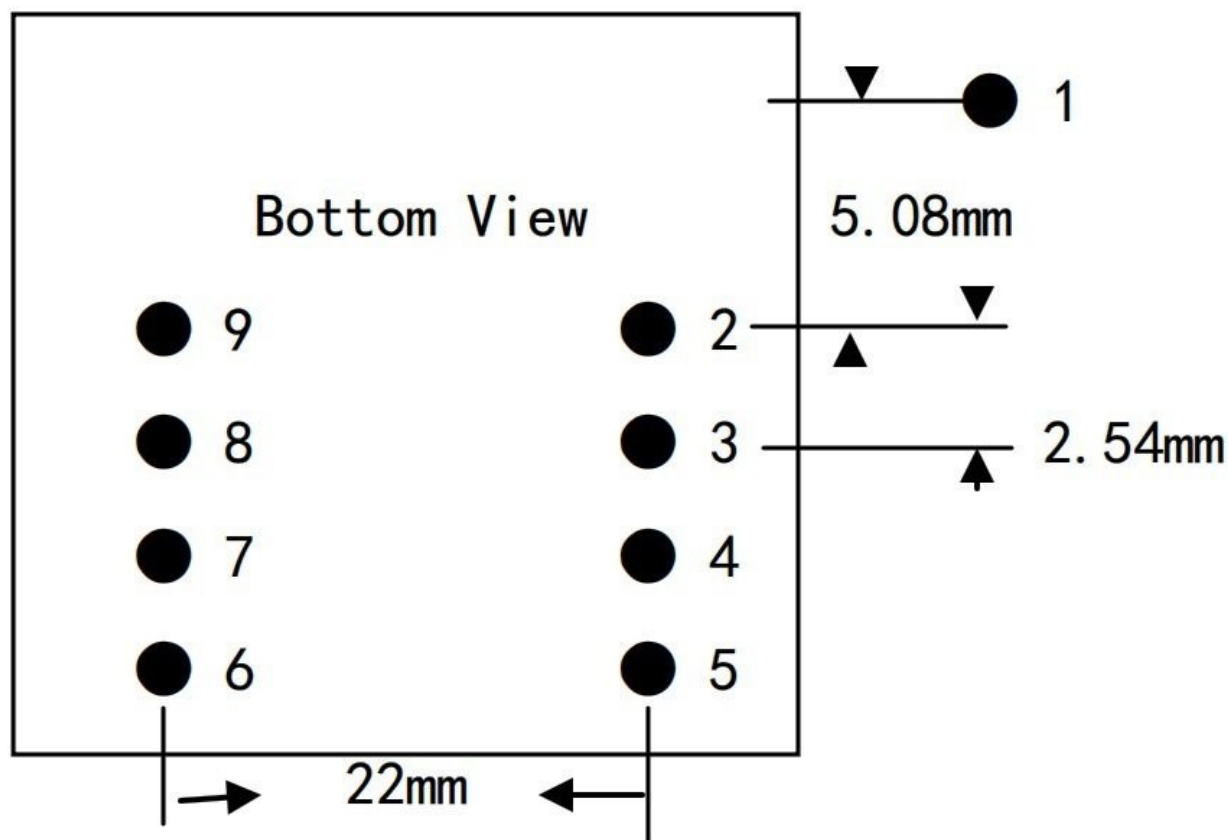


Рис. 2.5. Нижня частина модуля EM-18

Джерело: [13].

Таблиця 2.1

Функції виводів модулів EM-18

Шпилька	Ім'я	Функція
1	VCC	Електроживлення
2	GND	Земля
3	ПІСК	Звуковий сигнал і світлодіодний індикатор
4	АНТ	Не використовується
5	АНТ	Не використовується

6	SEL	Вибір RS232 (HIGH) або UART TX (LOW)
7	TX	WIEGAND Дані 1
8	DI	Дані WIEGAND 0
9	DO	Не використовується

Джерело: складено автором за [15].

Arduino UNO

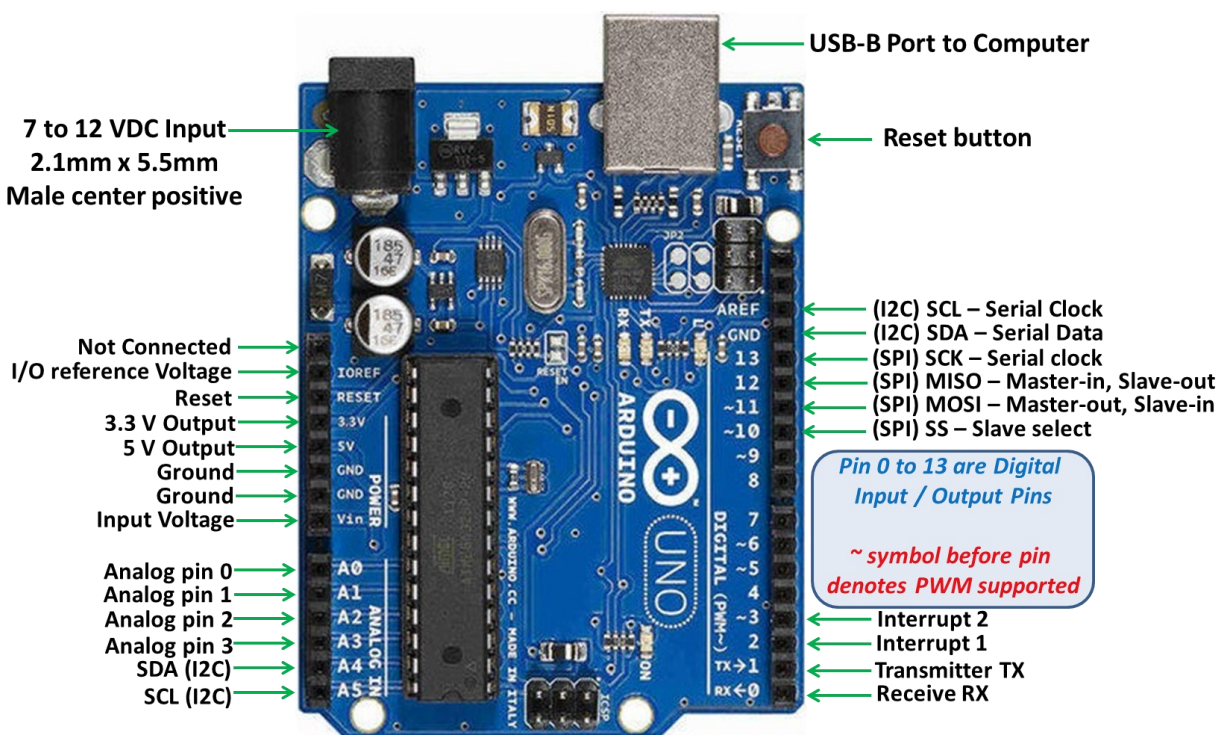


Рис. 2.6. Arduino Uno R3

Джерело: [10].

Arduino Uno – це плата мікроконтролера на базі ATmega328 (даташит). Вона має 14 цифрових входів/виходів (з яких 6 можна використовувати як ШІМ-виходи), 6 аналогових входів, керамічний резонатор 16 МГц, роз'єм JSB, гніздо порвера, заголовок ICSP і кнопку скидання.

Електромагніт

Соленоїди – це, по суті, електромагніти: вони складаються з великої котушки мідного дроту з якорем (металевою кулькою) посередині. Коли на котушку подається напруга, кулька втягується в центр котушки. Це робить електромагніт здатним тягнути з одного кінця. Цей електромагніт, зокрема, гарний і міцний, має кульку з косим зрізом і гарний монтажний кронштейн. Де-факто, це електронний замок, призначений для звичайних дверей шафи або сейфа. Зазвичай замок активний, тому ми не можемо відчинити двері, бо на заваді стоїть електромагнітна защіпка. Коли подається напруга 9-12 В постійного струму, магніт втягується і більше не стирчить, і двері можна відчинити.

Соленоїди поставляються зі скошеним магнітом, але ми можемо відкрити його за допомогою двох хрестоподібних гвинтів і повернути так, щоб він повертався на 90, 180 або 270 градусів, і щоб він відповідав дверям, з якими ми плануємо його використовувати. Для керування електромагнітом також знадобиться силовий транзистор, діод і хороше джерело живлення, оскільки для зарядки електромагніту в електромагніт буде надходити багато струму, близько 500 мА.

Привабливість однорідного поля в соленоїді полягає в тому, що, якщо соленоїд має незмірну довжину, магнітне поле буде однаковим скрізь уздовж елемента. У соленоїді це іноді призводить до того, що дуже маленькі електричні компоненти здатні виконувати величезну кількість роботи. Наприклад, потужний електромагніт може просто закрити клапан, який навіть найсильніша людина не здатна була б закрити вручну [10].

Змінюючи напрямок механічної сили, яку створює електромагніт, можна пристосувати поворотні та інші типи застосувань. Це робить їх надзвичайно гнучкими пристроями, які роблять можливими деякі з найпоширеніших

електричних компонентів і приладів. Цей дуже простий пристрій може зробити його безмежним.

Технічні деталі проекту:

- 12V DC (можна використовувати 9-12 вольт постійного струму, але нижча напруга призводить до слабшого/повільнішого оперотрона);
- Споживає 650 мА при 12V. 500 мА при 9 В при активації;
- Розраховано на час активації 1-10 секунд;
- Розміри: 23. 57 мм/0.92" і 67.47 мм/2.65"*27.59мм/1 1.08"
- Довжина дроту: 222.25 мм / 8.7 5" - Вага: 147.71g

Таким чином, прототип нашої системи матиме 3 входи і 2 виходи. Живлення є важливим входом і буде забезпечувати RFID необхідною напругою і струмом для роботи. Другий вхід – це вхід датчика RFID. Через нього інформація з RFID-мітки буде надходити в систему (табл. 2.2).

Таблиця 2.2

Особливо функціонування прототипу

Опис входу	Опис виходу
Сила	Подає напругу на дверний RFID-замок і забезпечує його живлення для всіх функцій.
Розблокувати/Заблокувати	Відчинить двері або залишить їх заблокованими залежно від RFID-мітки та налаштувань.
Вхід для датчика RFID	Сканує RFID-мітки і розблоковує або залишається заблокованим залежно від налаштувань і RFID-мітки.

Джерело: складено автором за [2].

Початкову декомпозицію першого рівня, дверний RFID-замок можна розбити на 5 основних компонентів. Вхід RFID (RFID-мітка) потрапляє в

RFID-датчик, який потім поміщається в MCU (або мікроконтролер). На основі програмування і налаштувань, встановлених користувачем, MCU надсилає інструкції магнітному реле і РК-модулю. Все, що надсилається на РК-модуль, виводиться на РК-дисплей і може сприйматися як власне РК-екран. Після того, як магнітне реле отримає сигнал, магнітне реле перемкне ланцюг на дверний замок. Потім дверний замок видасть сигнал розблокування/блокування. Дверний замок розглядається як фізичний дверний замок у дверній коробці. живлення буде подаватися на всі блоки.

Зчитувач і РК-дисплей з'єднано з Arduino Uno, як показано на рис. 2.7. Таким чином, система витягає унікальний ідентифікатор кожної RFID-мітки за допомогою коду (Додаток А). Ці UID та їх стан відповідно оновлюється та зберігається у мікроконтролері. Дверний замок буде відкриватися або знову закриватися відповідно до статусу UID.

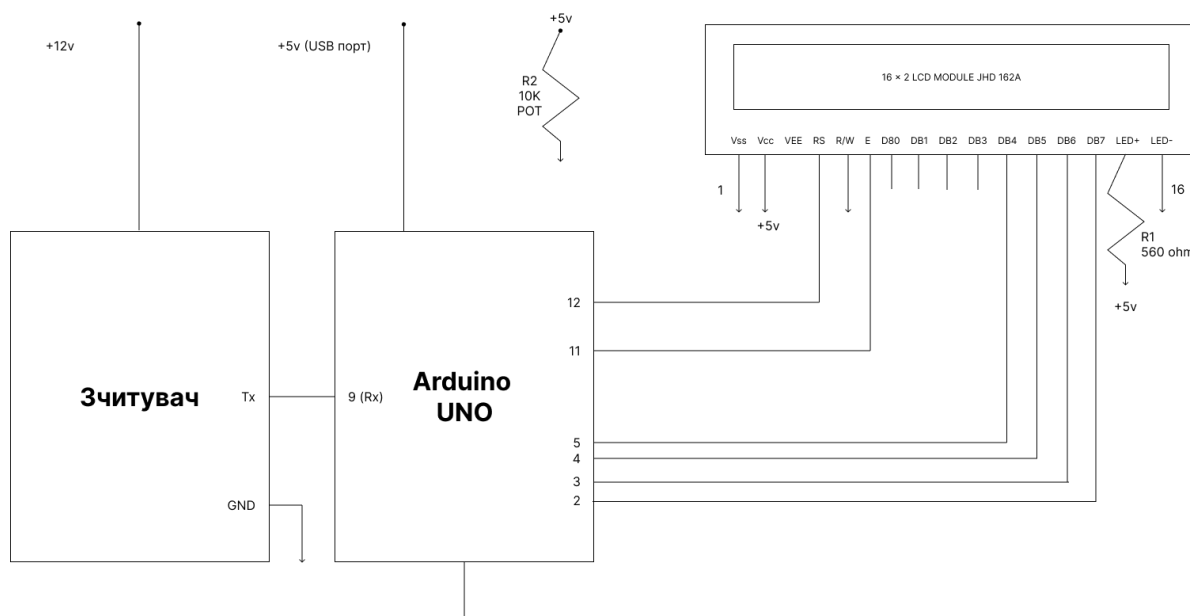


Рис. 2.7 Взаємодія РК-дисплея, Зчитувача та Arduino UNO

Джерело: складено автором за [2].

Ми з'єднаємо електромагнітний замок і джерело живлення 18V з мікроконтролером як показано на рис. 2.8. TIP120 – це силовий транзистор

Дарлінгтона. Його можна використовувати з Arduino для керування двигунами, вмикання світла та інших потужних гаджетів. TIP120 виступає в ролі енергетичного брокера або воротаря між сферою Arduino та сферою високої потужності, що складається з електромагнітного замка та екстремального джерела живлення.

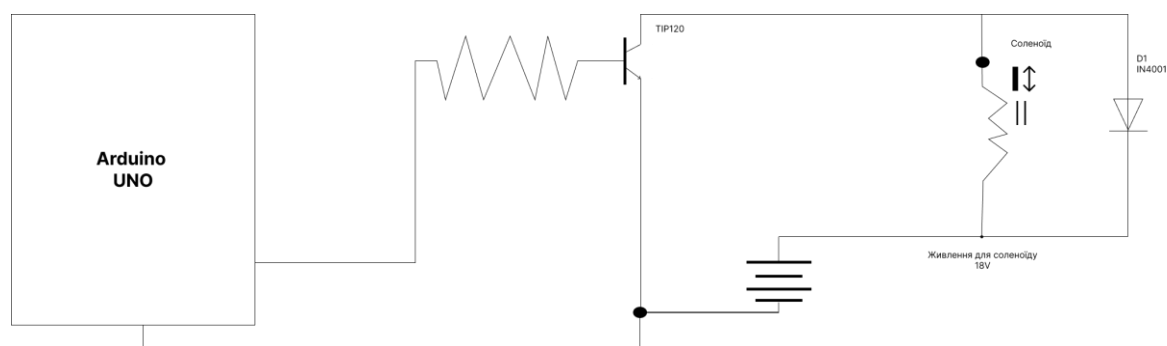


Рис. 2.8. Підключення електромагнітного замка та джерела живлення до мікроконтролер

Джерело: складено автором за [2].

Arduino може повідомити TIP120, скільки енергії потрібно передати від зовнішнього джерела живлення до електромагнітного замка, але Arduino не ділиться своєю енергією і не має спільних контактів з електромагнітним замком або його джерелом живлення. TIP120 є проміжною ланкою. Діод 1N4004 дозволяє струму проходити в одному напрямку від позитивного до негативного, але блокує будь-який блукаючий струм, який намагається пройти в протилежному напрямку, що може мати небажані наслідки для нашої схеми.

Після цього завантажуюємо в мікроконтролер наступний С-код.

```

void AccessCheck0
{
  i(entry_control:true)
  {
    i(tag_status:tue)
    t
    t
    lcd.clear$;
    delay(100);
    lcd.setCursor(0,0);
    // the tag id matches with the id saved in the microcontroller
    lcd.print("Access Granted");
    digitalWrite@delay, HIGH);
    delay(10000);
    digitalWrite(Relay, LOW);
    //door remains unlocked for 10 seconds
  )
  else
  {
    lcd.clear0;
    delay(100);
    lcd.setCursor(0,1);
    lcd.print("Access Denied");
  )
}

```

Рис. 2.9. Функція перевірки стану мітки та дверей

Джерело: складено автором за [9; 20].

Ця функція визначає, чи двері відчинені, чи зачинені. Контроль доступу та стан мітки визначаються з попередніх рядків коду. Якщо контроль доступу та стан мітки істинні, мікроконтролер надсилає сигнал на реле, а реле подає живлення на електромагнітний замок. Для зручності ми використали 5В одноканальне реле замість транзистора TIP120. Перевага використання 5В одноканального реле полягає в тому, що воно може комутувати як змінну, так і постійну напругу. Щоб відкрити електромагнітний замок зсередини приміщення, використовується перемикач, який переводить реле у високе положення, щоб користувач міг вийти з приміщення.

Таким чином, наша система пропонує дуже дешевий і доступний дизайн, який забезпечує зручність і безпеку для користувачів. Конструкція відносно

					ІТС.4КІ.0323.03-ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		43

невелика і досить проста в установці за допомогою пари гвинтів. Реле подає живлення на електромагнітний замок, якщо зчитана мітка збігається зі збереженою міткою в мікроконтролері. Якщо мітки не збігаються, сигналізація активується з третьої невдалої спроби. Таким чином користувачеві дозволяється або забороняється доступ. Для живлення мікроконтролера та електромагнітного замка можна використовувати одне джерело живлення 9В разом з стабілізатором напруги та інвертуючим підсилювачем. Для забезпечення живлення електромагнітного замка ми використали надпотужне джерело живлення 18В через обмеженість у часі.

2.3. Обмеження та можливі шляхи модернізації системи

Система, представлена в цьому звіті, є системою контролю доступу на основі RFID, яка має на меті забезпечити безпечний доступ до зон з обмеженим доступом. Однак, система має ряд обмежень.

По-перше, обмежений радіус дії RFID, який можна пояснити кількома факторами, включаючи умови навколишнього середовища, частоту системи RFID і перешкоди від інших систем та об'єктів.

Фактори навколишнього середовища, такі як вода, метал, люмінесцентне освітлення, велика техніка та конкуруючі частоти, можуть впливати на роботу систем RFID. Наприклад, вода може впливати на рівень сигналу і заважати роботі системи RFID. Металеві об'єкти також можуть заважати роботі системи RFID, оскільки метал може блокувати сигнал RFID, що призводить до зменшення дальності зчитування або зниження продуктивності.

Частота системи RFID також може впливати на дальність зчитування. Наприклад, низькочастотні (LF) RFID-зчитувачі працюють на частоті 125 КГц

					ІТС.4КІ.0323.03-ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		44

і мають меншу відстань зчитування – близько 10 сантиметрів, що означає, що мітка повинна бути дуже близько до зчитувача для ефективної комунікації [19]. На відміну від них, надвисокочастотні RFID-системи працюють на частоті близько 900 МГц і мають дальність зчитування до 100 метрів. Однак вони схильні до перешкод, які можуть зменшувати дальність зчитування і створювати потенційні ризики для безпеки.

Щоб подолати проблему обмеженого діапазону зчитування, система може використовувати більш потужний RFID-зчитувач або більш чутливу RFID-мітку. Використання більш потужного зчитувача може збільшити дальність зчитування, дозволяючи системі RFID виявляти RFID-мітки на більшій відстані. Крім того, використання більш чутливої RFID-мітки також може покращити дальність зчитування. Однак, важливо враховувати компроміс між дальністю зчитування і ризиком несанкціонованого доступу.

Таким чином, обмежений діапазон зчитування систем RFID можна вирішити, враховуючи фактори навколишнього середовища, вибираючи відповідну частоту RFID і використовуючи більш потужний RFID-зчитувач або більш чутливу RFID-мітку.

Ще одним обмеженням є використання пасивних RFID-міток, які мають обмежений термін служби через їхню залежність від енергії, що надходить від RFID-зчитувача. На відміну від активних RFID-міток, які мають вбудоване джерело живлення, пасивні мітки не мають постійного джерела живлення або акумулятора [19]. Це означає, що продуктивність і термін служби мітки залежать від матеріалів, з яких вона виготовлена, і середовища, в якому вона працює. У щадному середовищі пасивні мітки можуть працювати до 20 років. Однак відсутність вбудованого акумулятора також обмежує кількість інформації, яка може зберігатися на пасивній мітці.

Обмежений термін служби пасивних RFID-міток може призвести до збільшення витрат на обслуговування і незручностей, пов'язаних з частою заміною міток. На відміну від них, активні RFID-мітки мають довший термін служби (3-5 років), але вони дорожчі і потребують постійного джерела живлення resources.altium.com. Крім того, активні мітки більші та важчі порівняно з пасивними, що може бути недоліком у певних сферах застосування.

Щоб подолати проблему обмеженого терміну служби пасивних RFID-міток, в майбутньому система може використовувати активні RFID-мітки, які мають довший термін служби і можуть підтримувати зберігання більшої кількості інформації. Однак активні RFID-мітки дорожчі і більші за розміром, ніж пасивні [19].

Використання зчитувачів RFID в системі контролю доступу також означає, що якщо зчитувач вийде з ладу або зіткнеться з технічними проблемами, система контролю доступу не буде функціонувати належним чином. Це може призвести до втрати контролю доступу, несанкціонованого доступу або помилкових відмов. Щоб пом'якшити це обмеження, в системі може бути реалізовано резервування, наприклад, використання декількох зчитувачів RFID або резервної системи.

У щільно розгорнутій мережі RFID надлишкові зчитувачі можуть спричинити марну трату енергії і легко призвести до взаємних перешкод, оскільки радіочастоти двох або більше сусідніх зчитувачів можуть перекриватися і заважати один одному. Проблема усунення надлишкових зчитувачів є основною проблемою в системі RFID. Для вирішення цієї проблеми було розроблено покращений алгоритм на основі підрахунку (ICBA) для виявлення та усунення надлишкових зчитувачів RFID у складних мережах

RFID. ICBA базується на підрахунку кількості зчитувачів, які охоплюють кожну мітку, і кількості міток, які охоплюються зчитувачем link.springer.com.

Окрім реалізації ICBA, система контролю доступу може використовувати інші алгоритми та методи оптимізації для усунення надлишкових зчитувачів у системі RFID [19]. Наприклад, система може використовувати алгоритм усунення декількох зчитувачів для усунення надлишкових зчитувачів, забезпечуючи ефективну та результативну роботу системи контролю доступу.

Ще однією проблемою є можливість підміни в системах RFID, тобто ситуація, коли зловмисник може використовувати підроблену RFID-мітку або спеціальний емуляційний пристрій, щоб отримати несанкціонований доступ до системи. Для успішного проведення спуфінг-атаки зловмисникові необхідно заздалегідь мати знання про використовувані протоколи і секрети аутентифікації.

Атакам спуфінгу можна протидіяти, впроваджуючи додаткові заходи безпеки, такі як шифрування, автентифікація або реалізація механізму виклик-відповідь [11]. Протоколи автентифікації або друга форма автентифікації, наприклад, одноразові паролі, PIN-коди або біометричні дані, можуть допомогти запобігти підробці та імітації. Однак системи паролів без шифрування вважаються слабкими формами автентифікації, оскільки вони вразливі до підслуховування і можуть бути зламані методом проб і помилок. Тому автентифікація за допомогою пароля більше підходить для додатків, де доступ до RFID-мітки здійснюється обмежену кількість разів.

Іншим підходом до запобігання атакам підміни є псевдонімізація, коли лише авторизовані зчитувачі можуть мати доступ до оригінальної ідентичності RFID-мітки. Методи псевдонімізації, такі як хеш-блокування, рандомізоване

хеш-блокування та ланцюгові хеші, можуть бути використані для подальшого підвищення безпеки.

Атакам мережевих протоколів можна протидіяти шляхом посилення захисту всіх компонентів, які підтримують зв'язок RFID, застосування безпечних операційних систем, відключення небезпечних і невикористовуваних мережевих протоколів, а також налаштування використовуваних протоколів з найменшими можливими привілеями.

Іншою проблемою є обмежена ємність зберігання даних в RFID-мітках, таких як інформація про профіль користувача або додаткові дозволи на доступ. Як згадується в [12], RFID-транспондери пропонують більший обсяг пам'яті для зберігання даних порівняно з оптичними штрих-кодами, але обсяг пам'яті все одно обмежений.

RFID-мітки можуть зберігати невеликий обсяг даних, зазвичай до 2 кілобайт (КБ). Обсяг даних, які можуть зберігатися на RFID-мітці, залежить від виробника, застосування і типу мітки. Дані зазвичай зберігаються в пам'яті користувача на мітці, окремо від поля для унікального серійного номера, який може бути попередньо запрограмований або присвоєний користувачем.

Збільшення обсягу пам'яті RFID-міток є складним завданням через взаємозв'язок між ціною та обсягом пам'яті. Більший об'єм пам'яті безпосередньо збільшує вартість однієї мітки для готелю. Крім того, безчипова RFID-мітка створює низку технологічних проблем, включаючи збільшення ємності зберігання даних, щоб бути конкурентоспроможною з оптичними штрих-кодами або RFID-мітками на основі мікросхем.

Для подолання проблеми обмеженої ємності сховища даних система може використовувати різні методи оптимізації, такі як стиснення даних, дедуплікація даних або використання комбінації різних типів RFID-міток з різною ємністю сховища. Іншим варіантом може бути вивантаження частини

даних на зовнішні системи, такі як бази даних або хмарні сховища, які можуть забезпечити практично необмежену ємність зберігання. Однак такий підхід вимагатиме додаткової інфраструктури та механізмів синхронізації даних.

Також варто згадати про проблеми конфіденційності, які виникають у технології RFID, оскільки зчитувачі RFID потенційно можуть зчитувати інформацію з RFID-міток без відома користувача. Це може призвести до несанкціонованого доступу до конфіденційної інформації, профілювання та відстеження осіб. Щоб вирішити ці проблеми, система може впроваджувати методи підвищення конфіденційності, такі як анонімізація RFID-міток або використання шифрування для захисту збережених даних cdn.intechopen.com.

Одним з підходів до підвищення конфіденційності в системах RFID є модель підвищення конфіденційності PEM4RFID, яка пропонує механізм автентифікації ідентичності 2 + 2 (двофакторний протокол автентифікації TFAP). Модель PEM4RFID має характеристики невідстежуваності та неповторюваності інструкцій, що реалізує хороший компроміс між конфіденційністю та безпекою в RFID-системах [22].

Іншим підходом до вирішення проблем конфіденційності є анонімізація RFID-міток. Генеруючи тимчасові унікальні ідентифікатори (TUID), які не розкривають унікальний ідентифікатор оригінальної RFID-мітки, система може зменшити ризик несанкціонованого доступу та профілювання semanticscholar.org. TUID можуть генеруватися за допомогою захищеного протоколу між зчитувачем RFID і сервером, гарантуючи, що тимчасові ідентифікатори є унікальними і не пов'язані з оригінальною RFID-міткою.

Шифрування також можна використовувати для захисту даних, що зберігаються на RFID-мітках. Шифруючи дані, що зберігаються на RFID-мітках, неавторизовані зчитувачі не зможуть отримати доступ до інформації без ключа розшифрування. Цього можна досягти за допомогою різних

алгоритмів і методів шифрування, таких як симетричне або асиметричне шифрування, в залежності від конкретних вимог системи.

Таким чином, система контролю доступу RFID, представлена в роботі, має ряд обмежень, включаючи обмежений радіус дії, залежність від пасивних RFID-міток, залежність від RFID-зчитувачів, можливість підробки, обмежене зберігання даних і проблеми з конфіденційністю. Щоб покращити систему, ми могли б розглянути можливість впровадження додаткових заходів безпеки, використання активних RFID-міток, включення надмірності та вирішення проблем конфіденційності.

Висновки до розділу 2

1. У цьому розділі представлено методологію та хід розробки системи контролю фізичного доступу та реєстрації в готелі з використанням технології Arduino. Було висвітлено дизайн і методи, використані під час розробки системи з метою забезпечити всебічне розуміння загального підходу, використаних апаратних і програмних компонентів, а також реалізованих протоколів тестування. Завдяки використанню технології Arduino, це дослідження має на меті створити рішення, яке є одночасно економічно ефективним і легко налаштовується, що в кінцевому підсумку підвищує безпеку та ефективність системи контролю доступу в готелі.

2. Дверний замок RFID – це недорогий і економічно ефективний дизайн, який пропонує користувачам зручність і безпеку. Конструкція компактна і проста в установці, вимагає лише декількох гвинтів. Реле використовується для подачі живлення на електромагнітний замок, коли зчитана мітка збігається з міткою, що зберігається в мікроконтролері. Якщо мітки не збігаються, з третьої спроби спрацьовує зумер, який сповіщає про те, що користувачеві надано доступ або відмовлено в доступі. Для живлення мікроконтролера та електромагнітного замка можна використовувати одне джерело живлення 9В,

а також стабілізатор напруги та інвертуючий підсилювач. Через обмеженість у часі для електромагнітного замка було використано зовнішнє джерело живлення 18В.

3. У розділі також було висвітлено кілька розробленої системи, таких як обмежений радіус дії, залежність від пасивних RFID-міток, залежність від RFID-зчитувачів, вразливість до підробок, обмежені можливості зберігання даних і проблеми, пов'язані з конфіденційністю. Для вдосконалення системи доцільно впровадити додаткові заходи безпеки, використовувати активні RFID-мітки і вирішити проблеми конфіденційності. Відсутність автоматичної передачі даних о реєстрації користувачів.

					ІТС.4КІ.0323.03-ПЗ	Арк.
						51
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3. ОГЛЯД ТА ОЦІНКА ЕФЕКТИВНОСТІ РОЗРОБЛЕНОЇ СИСТЕМИ

3.1. Методика оцінки ефективності системи

У цьому розділі представлено комплексну методологію оцінки ефективності системи контролю доступу на основі RFID (радіочастотної ідентифікації) у контексті нашого дослідження. Метою дослідження є оцінка продуктивності та ефективності систем контролю доступу на основі RFID у підвищенні безпеки та ефективності в готельному середовищі. Методологія охоплює планування експериментів, збір даних і методи аналізу для вимірювання ключових показників ефективності, таких як час відгуку, точність автентифікації і загальна надійність системи. Використовуючи цю методологію, адміністратори готелів і фахівці з безпеки можуть отримати цінну інформацію про ефективність систем контролю доступу RFID і приймати обґрунтовані рішення щодо вдосконалення та оптимізації систем.

					ІТС.4КІ.0323.03-ПЗ				
Змн.	Арк.	№ докум.	Підпис	Дата					
Розроб.		Снежко О.Е..			РОЗДІЛ 3 ОГЛЯД ТА ОЦІНКА ЕФЕКТИВНОСТІ РОЗРОБЛЕНОЇ СИСТЕМИ		Лім.	Арк.	Акрушіє
Керівник		Матієвський В.В.						52	16
Реценз.		Козуб Ю.Г.					ЛНУ Кафедра ІТС, Гр.4КІ		
Н. Контр.									
Зав. каф.		Семенов М.А..							

Збір даних:

Етап збору даних є найважливішим компонентом оцінки ефективності системи контролю доступу RFID в готелях, який передбачає визначення метрик, які потрібно вимірювати. Щоб оцінити ефективність системи контролю доступу RFID в готелях, необхідно визначити конкретні показники. Ці показники повинні відповідати цілям дослідження і давати уявлення про продуктивність, точність і надійність. Зазвичай вимірювані показники включають

- 1) час відгуку: час, необхідний системі для відповіді після пред'явлення RFID-мітки для автентифікації;
- 2) точність автентифікації;
- 3) загальна надійність системи контролю доступу RFID, включаючи такі фактори, як частота помилок, час простою системи і частота відмов.

Методи відбору проб:

Для забезпечення репрезентативності та неупередженості збору даних необхідно використовувати відповідні методи вибірки. Відбір учасників, RFID-мітки та сценарії контролю доступу повинні бути ретельно продумані. Для мінімізації упереджень і отримання репрезентативної вибірки можна використовувати методи випадкової вибірки або стратифікованої вибірки.

Методи збору даних:

Методи збору даних мають бути розроблені таким чином, щоб забезпечити отримання точних і надійних даних. Можуть бути використані наступні методи:

- 1) спостереження: дослідники можуть спостерігати за взаємодією між користувачами і системою контролю доступу RFID. Це може включати в себе запис часу відгуку і будь-яких помітних проблем або помилок під час процесу автентифікації.

2) опитування та інтерв'ю: відгуки користувачів, таких як персонал готелю та гості, можна збирати за допомогою опитувань або інтерв'ю; ці якісні дані можуть дати уявлення про досвід користувачів, їхню задоволеність та пропозиції щодо покращення;

3) файли журналів і системні виходи: розроблена система контролю доступу RFID може генерувати файли журналів або вихідні дані, які фіксують системні події, такі як спроби автентифікації, надання або відмову в доступі, а також коди помилок; своєю чергою ці журнали можуть бути проаналізовані для вилучення відповідних точок даних.

Однак, для забезпечення точності та надійності даних слід застосовувати відповідні методи перевірки. Це може включати перехресну перевірку даних з різних джерел, перевірку узгодженості зібраних даних, а також очищення даних для усунення будь-яких пропусків або помилкових записів.

Під час збору даних також важливо дотримуватися етичних принципів. Дослідники повинні отримати інформовану згоду від учасників і забезпечити захист їхнього приватного життя та конфіденційності. Будь-яка зібрана особиста або конфіденційна інформація повинна бути анонімізована та надійно збережена.

Дотримуючись цих процедур збору даних, дослідники можуть збирати точні та надійні дані про такі показники, як час відгуку, точність автентифікації та надійність системи. Ці дані є основою для аналізу ефективності системи контролю доступу за допомогою радіочастотної ідентифікації в готелях і формулювання значущих висновків для вдосконалення та оптимізації системи.

Етап аналізу даних відіграє вирішальну роль в оцінці ефективності розробленої системи контролю доступу RFID в готелях. Аналіз фокусується на оцінці показників ефективності, визначених на етапі планування дослідження,

таких як час відгуку, точність автентифікації та надійність системи. Нижче наведено детальний опис процесу аналізу даних:

Перед проведенням аналізу важливо попередньо обробити зібрані дані. Це передбачає очищення даних, щоб видалити будь-які викиди, невідповідності або пропущені значення. Для забезпечення порівнянності та усунення будь-яких похибок, спричинених різними шкалами або одиницями виміру, можна також застосувати методи нормалізації або масштабування даних.

Далі, можна використовувати описову статистику, яка дає початкове розуміння даних та узагальнює їхні ключові характеристики. Такі показники, як середнє значення, медіана, стандартне відхилення та діапазон, можна обчислити для кожного показника ефективності, що дає уявлення про основні тенденції, варіабельність та розподіл даних.

Метод перевірки гіпотез дозволяє майбутнім дослідникам робити статистично значущі висновки про ефективність системи контролю доступу RFID. Цей метод охоплює формулювання нульової та альтернативних гіпотез, заснованих на цілях дослідження, і перевірку цих гіпотез за допомогою відповідних статистичних тестів. Наприклад, t-тести або ANOVA (дисперсійний аналіз) можуть бути використані для порівняння часу відгуку або точності автентифікації між різними сценаріями або конфігураціями системи.

Крім того, для оцінки можна використати регресійний аналіз, зокрема для аналізу між незалежними змінними (наприклад, конфігураціями системи або характеристиками користувачів) і залежними змінними (наприклад, часом відгуку або точністю автентифікації). Цей аналіз допомагає виявити важливі фактори, які впливають на ефективність системи, і спрогнозувати вплив потенційних змін або оптимізацій.

					ІТС.4КІ.0323.03-ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		55

Інтерпретація результатів фокусується на поясненні наслідків отриманих даних у контексті ефективності системи. Дослідники надають детальні пояснення спостережуваним закономірностям, взаємозв'язкам або тенденціям, виявленим під час аналізу даних. Інтерпретація може бути підкріплена статистичними даними, регресійним аналізом або порівняльним аналізом з попередніми дослідженнями чи галузевими показниками.

Під час обговорення можна дослідити будь-які значущі кореляції або взаємозв'язки між змінними, виявленими під час аналізу даних. Наприклад, можна вивчити зв'язок між часом відгуку і точністю автентифікації або дослідити вплив конфігурації системи на загальну надійність системи. Ці знання допомагають зрозуміти складну динаміку системи контролю доступу RFID.

Використовуючи цю комплексну методологію, адміністратори готелів і дослідники можуть ефективно оцінювати ефективність розробленої системи контролю доступу RFID в готелях, сприяючи підвищенню заходів безпеки і поліпшенню загального рівня обслуговування гостей.

3.2. Тестування програмної частини

Для написання тестів для даного модуля тегів пропонуємо створювати тестові кейси, які охоплюють різні сценарії, такі як допустимі вхідні дані, порожні вхідні дані та обробка помилок. На рис. 3.1 – 3.4 зображено приклад написання тестів за допомогою Arduino Test Library [9].

Крок перший передбачає встановлення зазначеної бібліотеки.

					ІТС.4КІ.0323.03-ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		56

```
#include <Arduino.h>
#include <Arduino_TestLib.h>
```

Рис. 3.1. Встановлення Arduino Test Library

Джерело: складено автором за [9].

Крок другий – це безпосереднє створення тестового класу для коду системи.

```
class RFIDReaderTests {
public:
    RFIDReaderTests() {}
    void setup() {
        Serial.begin(9600);
    }

    void loop() {}

    // Test cases go here
};
```

Рис. 3.2. Створення тестового класу

Джерело: складено автором за [9].

Після створення тестового класу, можна починати роботу над тестовими модулями.

					ІТС.4КІ.0323.03-ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		57

```

TEST_F(RFIDReaderTests, Read_ValidData) {
    // Test with valid input data
    int validData = 42;
    Serial.write(validData);
    Serial.print("Read data: ");
    int receivedData = Serial.parseInt();
    ASSERT_EQ(receivedData, validData);
}

TEST_F(RFIDReaderTests, Read_EmptyData) {
    // Test with empty input data
    Serial.write(0);
    Serial.print("Read data: ");
    int receivedData = Serial.parseInt();
    ASSERT_EQ(receivedData, 0);
}

TEST_F(RFIDReaderTests, Read_ErrorHandling) {
    // Test error handling with invalid input data
    Serial.write(255);
    Serial.print("Read data: ");
    int receivedData = Serial.parseInt();
    ASSERT_EQ(receivedData, -1); // -1 is returned when the input data is not a valid integer
}

```

Рис. 3.3. Тестові кейси для зчитувача

Джерело: складено автором за [9].

Наданий на рис. 3.3 фрагмент коду складається з трьох тестових кейсів для системи зчитування RFID-міток, які перевіряють поведінку системи за різних умов: дійсні вхідні дані, порожні вхідні дані та обробка помилок з недійсними вхідними даними. Для створення та виконання тестових кейсів використовується бібліотека Arduino Test Library (ATL).

Перший тест, Read_ValidData, тестує систему зчитування RFID-міток, коли вона отримує валідні вхідні дані. Тест ініціалізує ціле число validData значенням 42 і записує його в об'єкт Serial. Після запису даних тест зчитує дані з об'єкта Serial за допомогою Serial.parseInt() і перевіряє, чи дорівнюють отримані дані очікуваному значенню (42). Тест вважається успішним, якщо отримані дані дорівнюють очікуваному значенню.

					ИТС.4КІ.0721.03-ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		58

Другий тест, `Read_EmptyData`, тестує систему зчитування RFID-міток, коли вона отримує порожні вхідні дані (тобто нульове значення). Тест записує нульове значення в об'єкт `Serial`, а потім зчитує дані за допомогою `Serial.parseInt()`. Після зчитування даних тест перевіряє, чи отримані дані дорівнюють очікуваному значенню (0). Тест вважається успішним, якщо отримані дані дорівнюють очікуваному значенню.

Третій тест, `Read_ErrorHandling`, тестує обробку помилок системи RFID-зчитувача, коли вона отримує невірні вхідні дані. Тест записує неціле значення (255) в об'єкт `Serial`, а потім зчитує дані за допомогою `Serial.parseInt()`. Після зчитування даних тест перевіряє, чи отримані дані дорівнюють -1, тобто значенню, яке повертає `Serial.parseInt()`, коли вхідні дані не є дійсним цілим числом. Тест вважається успішним, якщо отримані дані дорівнюють -1.

Ці тестові кейси призначені для того, щоб переконатися, що система зчитування RFID-міток правильно поводить себе в різних умовах, дотримуючись очікуваної поведінки і забезпечуючи надійне зчитування даних. Виконуючи ці тести, ми можемо переконатися, що реалізація системи є надійною і може обробляти різні вхідні сценарії, включаючи дійсні, порожні та недійсні дані.


```

TEST_F(RFIDAccessControlTests, Access_Granted) {
    // Test with valid RFID data (assuming it matches the saved tags)
    char validRFIDData[12] = {'0', '0', '0', '0', 'A', '0', '0', '0', '0', '0', '0', '0'};
    for (int i = 0; i < 12; i++) {
        mySerial.write(validRFIDData[i]);
    }

    // Run the loop function to process the RFID data
    loop();

    // Check if the relay is set to HIGH (access granted)
    ASSERT_EQ(digitalRead(Relay), HIGH);
}

TEST_F(RFIDAccessControlTests, Access_Denied) {
    // Test with invalid RFID data (assuming it doesn't match the saved tags)
    char invalidRFIDData[12] = {'0', '0', '0', '0', 'B', '0', '0', '0', '0', '0', '0', '0'};
    for (int i = 0; i < 12; i++) {
        mySerial.write(invalidRFIDData[i]);
    }

    // Run the loop function to process the RFID data
    loop();

    // Check if the relay remains LOW (access denied)
    ASSERT_EQ(digitalRead(Relay), LOW);
}

TEST_F(RFIDAccessControlTests, ErrorHandling) {
    // Test with incomplete RFID data
    char incompleteRFIDData[6] = {'0', '0', '0', '0', 'A', '0'};
    for (int i = 0; i < 6; i++) {
        mySerial.write(incompleteRFIDData[i]);
    }

    // Run the loop function to process the RFID data
    loop();

    // Check if the relay remains LOW (access denied)
    ASSERT_EQ(digitalRead(Relay), LOW);
}

```

Рис. 3.4. Тестові кейси системи контролю доступу

Джерело: складено автором за [9].

Це три тестові кейси для системи контролю доступу RFID, які перевіряють поведінку системи за різних умов: дійсні дані RFID (доступ дозволено), недійсні дані RFID (доступ заборонено) та неповні дані RFID

					ИТС.4КІ.0323.03-ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		60

(обробка помилок). Код використовує бібліотеку тестів Arduino (ATL) для створення та виконання тестових кейсів.

Перший тест, `Access_Granted`, тестує систему контролю доступу RFID, коли вона отримує дійсні дані RFID, які відповідають збереженим міткам. Тест ініціалізує масив дійсних RFID-даних з 12 байт і записує кожен байт в об'єкт `mySerial`, імітуючи надсилання даних RFID-зчитувачем. Після обробки даних тест перевіряє, чи встановлено реле в стан HIGH, що вказує на те, що доступ надано. Тест пройдено, якщо реле зчитує як HIGH.

Другий тест, `Access_Denied`, тестує систему контролю доступу RFID, коли вона отримує невірні дані RFID, які не відповідають збереженим міткам. Подібно до попереднього тесту, тест ініціалізує масив недійсних RFID-даних з 12 байт і записує кожен байт в об'єкт `mySerial`. Після обробки даних тест перевіряє, чи встановлено реле в стан LOW, що вказує на те, що доступ заборонено. Тест пройдено, якщо реле читається як LOW.

Третій тест, `ErrorHandling`, тестує систему контролю доступу RFID, коли вона отримує неповні дані RFID, що є помилкою при передачі даних. Тест ініціалізує масив неповних RFID-даних з 6 байт і записує кожен байт в об'єкт `mySerial`. Після обробки даних тест перевіряє, чи залишається реле в стані LOW (доступ заборонено), оскільки система не повинна надавати доступ до неповних RFID-даних. Тест пройдено, якщо реле читається як LOW.

Отже, тестові кейси для системи контролю доступу RFID і системи зчитування RFID демонструють, що реалізації є надійними і можуть обробляти різні вхідні сценарії, забезпечуючи надійні і точні результати. Виконуючи ці тести, розробники можуть переконатися, що їхні реалізації функціонують так, як очікувалося, і можуть виявити потенційні проблеми, які можуть виникнути в реальних умовах застосування. Це гарантує, що системи є надійними, ефективними та зручними в обслуговуванні.

					ІТС.4КІ.0323.03-ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		61

3.3. Порівняння з існуючими розумними системами контролю доступу

Фактично наш проект пропонує гібридний дизайн ризико-адаптивної системи контролю доступу RFID, яка може бути розгорнута як онлайн на основі сервера так і офлайн без сервера.

Таблиця 3.1

Порівняння наявних систем контролю доступу

Назва системи	Опис
Удосконалена багатоклавішна гібридна система контролю доступу RFID з адаптацією до ризиків	Запропоновано вдосконалену багатоключову модель для динамічної генерації симетричного ключа шифрування на льоту.
Багаторівнева система нечіткого висновку для адаптивної до ризиків гібридної системи контролю доступу RFID	Вдосконалено попередні дослідження шляхом введення багаторівневої системи нечіткого виведення як додаткової моделі оцінки ризику, використовуючи контролер нечіткої логіки для оцінки ризику.
Мобільна система контролю доступу на основі RFID-міток та інформації про обличчя	Представляє альтернативну схему контролю доступу, яка поєднує пасивні RFID-мітки, встановлені біля турнікетів або "розумних" дверей, з авторизацією на основі смартфона та інформації про обличчя.

Розробка системи контролю доступу RFID на базі ARM	Представляє інтелектуальну систему контролю доступу RFID на базі ARM, що використовує мікросхему ARM-STM32F103VET6 в якості основного блоку управління в нижньому комп'ютері і керує інформацією про картки за допомогою бази даних MYSQL і WEB-сторінки JAVA.
--	--

Джерело: складено автором за [15; 16; 23; 24].

Для порівняння, інші існуючі системи контролю доступу, які ми знайшли, наведено у табл. 3.1.

Вдосконалена багатоключова адаптивна до ризиків гібридна система контролю доступу RFID пропонує вдосконалену багатоключову модель для динамічної генерації симетричного ключа шифрування на льоту.

Багаторівнева система нечіткого висновку для адаптивної до ризиків гібридної системи контролю доступу RFID є вдосконаленням попередньої роботи авторів, в якій вперше було запропоновано адаптивну до ризиків гібридну систему контролю доступу RFID. У цьому дослідженні багаторівнева система нечіткого виведення розроблена як додаткова модель оцінки ризику, де ризик оцінюється за допомогою контролера нечіткої логіки.

Мобільна система контролю доступу на основі RFID-міток та інформації про обличчя представляє альтернативну схему контролю доступу, яка підвищує безпеку контролю доступу при одночасному зниженні вартості. У запропонованій моделі пасивні RFID-мітки встановлюються біля турнікета або розумних дверей. Зчитування та програмування мітки здійснюється за допомогою NFC-чіпа безпосередньо на смартфоні користувача. Для підвищення безпеки, разом з авторизацією на основі смартфона, система вимагає, щоб користувач надавав свою фотографію.

					ІТС.4КІ.0323.03-ПЗ	Арк.
						63
Змн.	Арк.	№ докум.	Підпис	Дата		

Проектування системи контролю доступу RFID на базі ARM представляє інтелектуальну систему контролю доступу RFID на базі ARM. Ця система складається з верхнього комп'ютера та нижнього комп'ютера. Мікросхема ARM-STM32F103VET6 використовується як основний блок управління в нижньому комп'ютері. База даних MYSQL використовується у верхньому комп'ютері для управління інформацією на картці та відображення інформації на веб-сторінці JAVA.

Щодо нашої моделі, то вона генерує симетричний ключ шифрування динамічно для кожного користувача на вимогу, а це означає, що не існує єдиного головного ключа, який можна скомпрометувати для отримання доступу до системи. Це допомагає посилити безпеку системи, зменшуючи ризик несанкціонованого доступу через єдину точку відмови.

Традиційним системам контролю доступу бракує здатності справлятися з динамічним середовищем, де на процес прийняття рішень можуть впливати кілька факторів. Вони базуються на заздалегідь визначених і статичних політиках доступу, що робить їх нездатними динамічно адаптуватися до мінливих умов. На противагу цьому, модель контролю доступу подібна розробленій у цій роботі адаптується до ризиків, пропонує кращу альтернативу як з технічної, так і з економічної точки зору.

Моделі подібні нашій привертають все більше уваги дослідницької спільноти як альтернативний підхід до подолання обмежень традиційних моделей контролю доступу. Запропонована нами конструкція може поєднати в собі риси як безсерверної, так і ризико-адаптивної систем контролю доступу. Запропонований дизайн системи контролю доступу RFID може динамічно перемикатись між двома режимами контролю доступу, онлайн серверним та офлайн безсерверним, щоб адаптуватися до рівня ризику в залежності від вимог.

					ІТС.4КІ.0323.03-ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		64

Однак, існують деякі потенційні недоліки використання такої моделі контролю доступу. Розгортання нашої моделі онлайн потребує більш досконалих технологій та алгоритмів для розрахунку та управління факторами ризику, що може дуже вагомо збільшити вартість та складність системи і нівелювати її економічну перевагу. Крім того, наша модель може потребувати більшої обчислювальної потужності та обсягу пам'яті для обробки збільшеного обсягу даних і розрахунків в залежності від розміру підприємства. Чинний дизайн передбачає можливість збільшення, але не дуже оптимізований для цього.

Отже, розроблена система може бути складнішою в налаштуванні та обслуговуванні, ніж традиційні системи контролю доступу, що може призвести до помилок і вразливостей, якщо ними не керувати належним чином.

Висновки до розділу 3

1. У цьому розділі наведено методику оцінки ефективності системи на готельному підприємстві. Наприклад, можна дослідити зв'язок між часом відгуку і точністю автентифікації або оцінити вплив конфігурації системи на загальну надійність системи. Ці дані допомагають зрозуміти складну динаміку системи контролю доступу RFID і проливають світло на її експлуатаційні характеристики.

Використовуючи цю комплексну методологію, адміністратори готелів і дослідники можуть ефективно оцінювати ефективність систем контролю доступу RFID в готелях. Цей процес оцінки сприяє вдосконаленню заходів безпеки та покращенню загального досвіду гостей. Висновки та ідеї, отримані в результаті цього дослідження, дозволяють приймати обґрунтовані рішення щодо вдосконалення системи, а також впроваджувати заходи, які оптимізують продуктивність, надійність і зручність використання системи.

2. Тестові приклади, проведені як для системи контролю доступу RFID, так і для системи зчитування RFID, підтвердили надійність їхніх реалізацій і здатність обробляти різні вхідні сценарії, забезпечуючи таким чином надійні і точні результати. Ці тести слугують для розробників засобом перевірки правильності функціонування їхніх реалізацій і виявлення будь-яких потенційних проблем, які можуть виникнути в практичному застосуванні. Таким чином, протестовані системи демонструють свою надійність, ефективність та ремонтпридатність.

Виконуючи ці комплексні тести, розробники переконуються, що їхні реалізації дотримуються очікуваної функціональності та відповідають необхідним специфікаціям. Тестові кейси дають можливість змоделювати реальні сценарії та оцінити продуктивність системи за різних умов. Завдяки цьому процесу розробники можуть виявити та виправити будь-які недоліки, забезпечуючи безперебійну роботу системи в реальних сценаріях контролю доступу.

3. Запропонований нами гібридний дизайн усуває обмеження традиційних систем контролю доступу, динамічно генеруючи симетричні ключі шифрування для кожного користувача, усуваючи вразливість єдиного скомпрометованого головного ключа. Такий підхід посилює безпеку системи та зменшує ризик несанкціонованого доступу через єдину точку відмови.

Традиційним системам контролю доступу бракує адаптивності розробленої системи. І загалом, запропонований у цій роботі гібридний дизайн поєднує в собі економічну та технологічну ефективність, в той час як інші існуючі системи контролю доступу здебільшого зосереджені на чіткій спеціалізації і різних аспектах, таких як шифрування, нечітка логіка, мобільний доступ та інтелектуальний дизайн тощо.

					<i>ІТС.4КІ.0323.03-ПЗ</i>	Арк.
						66
Змн.	Арк.	№ докум.	Підпис	Дата		

Конструкція системи RFID забезпечує доступне та зручне рішення для готельних підприємств. Система компактна і проста в установці з мінімальною кількістю необхідних налаштувань. Електромагнітний замок живиться від реле, коли зчитана мітка збігається з міткою, що зберігається в мікроконтролері. Після третьої невдалої спроби спрацьовує зумер, який сповіщає про дозвіл або відмову в доступі та подія реєструється. Живлення мікроконтролера і електромагнітного замка може здійснюватися від одного джерела живлення 9В, а також стабілізатора напруги і інвертуючого підсилювача.

					ІТС.4КІ.0323.03-ПЗ									
Змн.	Арк.	№ докум.	Підпис	Дата										
Розроб.		Снежко О.Е.			ВИСНОВКИ					Лім.	Арк.	Акрушіє		
Керівник		Матієвський В.В.										67	3	
Реценз.		Козуб Ю.Г.								ЛНУ Кафедра ІТС, Гр.4КІ				
Н. Контр.														
Зав. каф.		Семенов М.А..												

У роботі також висвітлюються обмеження системи контролю доступу та відповідно реєстрації, зокрема обмежений радіус дії, залежність від пасивних радіочастотних міток, залежність від зчитувачів радіочастот, вразливість до підробок, обмежений обсяг пам'яті та проблеми з конфіденційністю. Для вдосконалення системи рекомендується впровадити додаткові заходи безпеки, такі як використання активних RFID-міток, запровадження резервування та вирішення питань конфіденційності.

Тести з розділу 3.2 сприяють встановленню надійності та точності систем. Піддаючи реалізації суворій оцінці, розробники можуть підтвердити, що результати є послідовними, точними і надійними. Така перевірка має важливе значення для гарантування ефективності систем у точному розпізнаванні та перевірці RFID-міток, забезпечуючи, таким чином, цілісність процесу контролю доступу.

Крім того, тестові кейси дозволяють оцінити ефективність і масштабованість системи. Аналізуючи час виконання, використання ресурсів і швидкість відгуку під час тестів, ми можемо отримати уявлення про характеристики продуктивності системи. Ця інформація допомагає оптимізувати роботу проекту, підвищити загальну ефективність і гарантувати, що система може обробляти різні робочі навантаження і масштабуватися за необхідності.

На закінчення, розроблені тестові кейси здатні перевірити і продемонструвати стійкість і надійність як системи контролю доступу RFID, так і системи зчитування RFID. Ці тести гарантують, що реалізації функціонують за призначенням, ефективно обробляють різноманітні вхідні сценарії та надають точні та надійні результати. Комплексний процес оцінки підтверджує надійність, ефективність і ремонтпридатність систем,

					<i>ITS.4KI.0323.03-ПЗ</i>	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		68

підтверджуючи їхню придатність для застосування в реальних умовах контролю доступу.

Отже, запропонований гібридний дизайн системи контролю доступу та реєстрації в цій роботі поєднує в собі функції безсерверного та адаптивного до ризиків контролю доступу. На відміну від інших систем, які зосереджені на різних аспектах, таких як шифрування, нечітка логіка, мобільний доступ та інтелектуальний дизайн, наш проект зосереджений на досягненні максимальної економічної та технологічної ефективності в будь-яких умовах.

					ІТС.4КІ.0323.03-ПЗ	Арк.
						69
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Готельні системи безпеки. *Новини туризму*. URL: <https://tourism-book.com/pbooks/book-38/ua/chapter-1903/> (дата звернення: 07.05.2023).
2. Двоканальна система дистанційного керування доступом до приміщення на базі Arduino. *Електронний репозитарій КРС ЧНУ ім. Петра Могили: Home*. URL: <https://krs.chmnu.edu.ua/jspui/handle/123456789/684> (дата звернення: 03.05.2023).
3. Захист комп'ютерних систем - Технічні засоби, захист бізнесу. *Віртуальна читальня освітніх матеріалів*. URL: <https://subject.com.ua/economic/safety/55.html> (дата звернення: 04.04.2023).
4. Системи безпеки: профілактика помилкових тривог. *Worldvision*. URL: <https://worldvision.com.ua/top-10-sposobov-predotvrashcheniya-lozhnoy-trevogi-sistemy-domashney-bezopasnosti/> (дата звернення: 01.04.2023).
5. Учасники проєктів Вікімедіа. Система контролю і управління доступом. *Вікіпедія*. URL: https://uk.wikipedia.org/wiki/Система_контролю_і_управління_доступом (дата звернення: 02.05.2023).
6. Учасники проєктів Вікімедіа. Смарт-картка. *Вікіпедія*. URL: <https://uk.wikipedia.org/wiki/Смарт-картка> (дата звернення: 03.04.2023).

					ІТС.4КІ.0323.03-ПЗ							
Змн.	Арк.	№ докум.	Підпис	Дата								
Розроб.		Снежко О.Е.			СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ			Літ.		Арк.	Акрушіє	
Керівник		Матієвські .ВВ..								70	3	
Реценз.		Козуб Ю.Г.										
Н. Контр.												
Зав. каф.		Семенов М.А..										
						ЛНУ Кафедра ІТС, Гр.4КІ						

7. Що собою являє інтегрована система управління контролем доступу?. *Worldvision*. URL: <https://worldvision.com.ua/articles/chto-soboy-predstavlyaet-integrirovannaya-sistema-upravleniya-kontrolem-dostupa> (дата звернення: 02.04.2023).
8. [PDF] enhanced multi-keyed risk adaptive hybrid RFID access control system. *Semantic Scholar | AI-Powered Research Tool*. URL: <https://www.semanticscholar.org/paper/Enhanced-Multi-keyed-Risk-Adaptive-Hybrid-RFID-AI-Zewairi-Hamdan/606a7e584826dd8ca246872d1d89dc29f779223a> (date of access: 03.05.2023).
9. A universal UHF RFID reader antenna. *IEEE Xplore*. URL: <https://ieeexplore.ieee.org/abstract/document/4806172/> (date of access: 04.04.2023).
10. Arduino UNO . board component. arduino shields. *PIJA Education*. URL: <https://pijaeducation.com/arduino/introduction-arduino-arduino-uno/> (date of access: 11.05.2023).
11. Arduino. *Home*. URL: <https://www.arduino.cc> (date of access: 07.06.2023).
12. Electronic warfare: jamming, spoofing, and ground stations. *RBC Signals*. URL: <https://rbcsignals.com/blog/electronic-warfare-jamming-spoofing-and-ground-stations/> (date of access: 02.05.2023).
13. EM18 - RFID reader module. *Components101*. URL: <https://components101.com/modules/em18-rfid-reader-module> (date of access: 07.06.2023).
14. EM-18 EM18 RFID reader module in pakistan. *Electronics Hub*. URL: <https://electronicshub.pk/product/em-18-em18-rfid-reader-module-in-pakistan/> (date of access: 07.04.2023).

					ITC.4KI.0323.03-ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		71

15. ICS NUFT. Хмарні сховища Ч1, 2023. *YouTube*.
URL: <https://www.youtube.com/watch?v=iqlBT-ARWv4> (дата звернення: 11.04.2023).
16. Mobile access control system based on RFID tags and facial information. *arXiv.org*. URL: <https://arxiv.org/abs/2103.06767> (date of access: 12.05.2023).
17. Multilevel fuzzy inference system for risk adaptive hybrid RFID access control system. *Semantic Scholar | AI-Powered Research Tool*.
URL: <https://www.semanticscholar.org/paper/Multilevel-Fuzzy-Inference-System-for-Risk-Adaptive-AI-Zewairi-Suleiman/45fc707eeea484e62ada15be04e5b8cb7f53b093> (date of access: 07.05.2023).
18. NURE TV. Методи біометричної поведінкової аутентифікації та ідентифікації користувачів, 2021. *YouTube*.
URL: <https://www.youtube.com/watch?v=p6p98wBWmHY> (дата звернення: 02.01.2023).
19. PEM4RFID: privacy enhancement model for RFID systems / G. Xu et al. *SpringerLink*. URL: https://link.springer.com/chapter/10.1007/978-3-319-27137-8_49 (date of access: 02.03.2023).
20. RFID devices for Conformance certification: Injectable transponders (Pets). *ICAR – Network. Guidelines. Certifications*. URL: <https://www.icar.org/index.php/rfid-injectable/> (date of access: 12.05.2023).
21. RFID tags & readers - UHF, passive, HF, LF & interfaces | RFID, inc. URL: <https://www.rfidinc.com> (date of access: 09.04.2023).
22. Risk adaptive hybrid RFID access control system. *Semantic Scholar | AI-Powered Research Tool*. URL: <https://www.semanticscholar.org/paper/Risk->

					ITC.4KI.0323.03-ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		72

adaptive-hybrid-RFID-access-control-system-Al-Zewairi-

Alqatawna/ed917b39bb98a5203e477090f7f2f36356d74ad0 (date of access: 17.04.2023).

23. Standard C++. URL: <https://isocpp.org> (date of access: 01.05.2023).

24. Tiatek. Системи контролю і управління доступом (СКУД). *Розрахунок і монтаж систем безпеки*. URL: <https://tiatek.com.ua/skud/systemy-kontrolyu-dostupu.htm> (дата звернення: 21.04.2023).

					ІТС.4КІ.0323.03-ПЗ	Арк.
						73
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

Додаток А. Код для міток

```

int count = 0;

void setup() {
  Serial.begin(9600);
}

void loop() {
  if (Serial.available()) {
    char input = Serial.read();
    Serial.print(input);
    count++;
    // delay(S);
  }
  Serial.println();
  Serial.print("Tag Length : ");
  Serial.print(count);
  Serial.println(" Bytes");
}

```

					ІТС.4КІ.0323.03-ПЗ				
Змн.	Арк.	№ докум.	Підпис	Дата	ДОДАТКИ		Лім.	Арк.	Акрушіє
Розроб.		Снежко О.Е.							
Керівник		Матієвський В.В.						74	10
Реценз.		Козуб Ю.Г.					ЛНУ Кафедра ІТС, Гр.4КІ		
Н. Контр.									
Зав. каф.		Семенов М.А..							

Додаток Б. Основна програмна частина

```

#define Relay 10
#define buzzer 13
#include <SoftwareSerial.h>
#include <LiquidCrystal.h>

LiquidCrystal lcd(12, 5, 4, 3, 2);
SoftwareSerial mySerial(0, 1);
int read_count = 0;
int attempt_count = 0;
boolean flag = false;
int i = 0, k = 0;
int RFID_data[12];
char Saved_Tag[3][12] = {"123", "456", "789"};

boolean tag_check, tag_status, entry_control;

void setup() {
  mySerial.begin(9600);
  Serial.begin(9600);
  pinMode(Relay, OUTPUT);
  pinMode(buzzer, OUTPUT);
  digitalWrite(Relay, LOW);
  lcd.begin(16, 2);
}

void loop() {

```

					ITC.4KI.0323.03-ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		75


```

RecieveData();
CheckData();
AccessCheck();
}

void RecieveData() {
    lcd.setCursor(0, 0);
    lcd.print("Swipe Your Card");
    if (mySerial.available() > 0) {
        char temp = mySerial.read();
        RFID_data[read_count] = temp;
        read_count++;
    }
}

```

```

void CheckData() {
    if (read_count == 12) {
        entry_control = true;
        for (k = 0; k < 3; k++) {
            for (i = 0; i < 12; i++) {
                if (Saved_Tag[k][i] != RFID_data[i]) {
                    tag_check = false;
                    break;
                }
            }
            else {
                tag_check = true;
            }
        }
    }
}

```

```

    }
    if (tag_check == true) {
        tag_status = true;
        break;
    }
}
read_count = 0;
}
}

void AccessCheck() {
    if (entry_control == true && tag_status == true) {
        lcd.clear();
        delay(100);
        lcd.setCursor(0, 0);
        lcd.print("Access Granted");
        digitalWrite(Relay, HIGH);
        delay(5000);
        digitalWrite(Relay, LOW);
        attempt_count = 0;
    }
    else {
        for (int r = 0; r < 12; r++) {
            RFID_data[r] = 0;
        }
        entry_control = false;
        tag_status = false;
    }
}

```

					ITC.4Kl.0323.03-ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		77

```

attempt_count++;
lcd.clear();
delay(100);
lcd.setCursor(0, 0);
lcd.print("Access Denied");
if (attempt_count == 3) {
    digitalWrite(buzzer, HIGH);
    delay(1000);
    digitalWrite(buzzer, LOW);
    attempt_count = 0;
}
}
}

```

					ITC.4KI.0323.03-ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		78