

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»**

*Спеціальність: 123 «Комп'ютерна інженерія»*

*Освітньо-професійна програма: «Обслуговування  
комп'ютерних систем і мереж»*

*Група: 4КС-57*

# **Дипломний проект**

**здобувача освіти денної форми навчання  
КС.57.09.000.ДП**

***КАЧАНОВСЬКОГО  
АНДРІЯ АНДРІЙОВИЧА***

**м. Одеса  
2024 р.**

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: 123 «Комп'ютерна інженерія»

Освітньо-професійна програма: «Обслуговування комп'ютерних систем і мереж»


Група: 4КС-57

**ПОЯСНЮВАЛЬНА ЗАПИСКА**

до дипломного проекту на тему:

**Системи контролю доступом підприємства на основі QR кодування**


Проектний матеріал складається з пояснювальної записки на 72 сторінках та графічного (презентаційного) матеріалу на 11 аркушах (слайдах)

Дипломник  (Качановський А.А.)

Керівник  (Кільдішев В.Й.)

**Консультанти:**

з економічного розділу  (Іванченков В.С.)

з розділу охорони праці та техніки безпеки  (Чорновол Н.І.)

з нормоконтролю  (Петрашова В.І.)

старший консультант  (Кривченко Ю.В.)

**До захисту допущений**

Голова циклової комісії  (Кривченко Ю.В.)

Завідувач відділення  (Скорнякова О.В.)

Захист «20» 06 2024 р. Протокол ЕК № 4

Оцінка ЕК 3/завдовільно/чод.

Секретар ЕК 

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**  
**ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»**

Відділення комп'ютерних систем Комісія КТ та ПІ

Спеціальність 123 «Комп'ютерна інженерія»

Освітньо-професійна програма «Обслуговування комп'ютерних систем і мереж»

ЗАТВЕРДЖУЮ:

Заст. дир. з НВР Беркань І.В.

« 15 » 01 2024 р.

**ЗАВДАННЯ**

**на дипломний проект**

Здобувачеві освіти: Качановському Андрію Андрійовичу

1. Тема проекту: Системи контролю доступом підприємства на основі QR кодування.

Затверджена наказом по коледжу від « 2 » 11 202 3 р. № 244-А2-ОД

2. Термін здачі закінченого проекту «10» червня 2024 р.







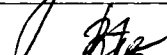



3. Вихідні дані до проекту:

1. Технологія QR кодування та застосування
2. Типи QR кодів та принципи організації контролю доступу
3. Програмне забезпечення для генерація QR коду
4. Розробити пристрій ідентифікації QR коду на основі платформи Arduino для системи контролю доступом підприємства
5. Реалізація та моделювання системи контролю доступом підприємства на основі QR кодів.



4. Зміст розрахунково-пояснювальної записки (перелік питань, які необхідно розробити): Системи QR-кодування; Організації системи контролю доступом підприємства на основі QR кодування; Генерація унікальних QR-кодів для співробітників підприємства; Платформа Arduino і аналіз її можливостей; Пристрій QR-кодування на основі платформи Arduino; Розробка і реалізація системи керування доступом; Економічні розрахунки; Заходи ТБ.

5. Перелік графічного (презентаційного) матеріалу (з точним зазначенням обов'язкових креслень, кількості слайдів): Застосування технології QR кодування; Законодавство щодо застосування QR-кодування; Порівняння характеристика технологій ідентифікації; Технічні характеристики QR-коду; Принцип роботи система контролю доступом на основі QR-кодування; Архітектура системи керування на основі QR-кодування; Оформлення бейджу працівника підприємства із згенерованим QR-кодом; Апаратна реалізація сканера QR-кодів.
















6. Консультанти по проекту, із зазначенням розділів проекту, що їх стосується



Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прий.
Основний розділ	Кільдішев В.Й.		
Економічний розділ	Іванченков В.С.		
Розділ охорони праці	Чорновол Н.І.		
Нормоконтроль	Петрашова В.І.		
Старший консультант	Кривченко Ю.В.		

7. Дата видачі завдання: «15» 01 2024 р.

Керівник Кільдішев В.Й.  (під  
Завдання прийняв до виконання Качановський В..  (під

КАЛЕНДАРНИЙ ПЛАН

№ з/р	Назва етапів дипломного проекту	Термін виконання етапів дипломного проекту (роботи)	Відмітка про виконання
1	Вступ. Постановка мети та задач проектування.	28.04.24	
2	Вивчення технічної документації.	19.05.24	
3	Огляд доцільності застосування системи контролю доступом підприємства	20.05.24	
4	Організація доступу на основі QR кодування	24.05.24	
5	Принцип організації системи контролю доступом підприємства на основі QR кодування.	25.05.24	
6	Платформа Arduino і аналіз її можливостей.	26.05.24	
7	Створення алгоритму роботи системи.	28.05.24	
8	Вибір компонентів для розробки системи.	30.05.24	
9	Розробка програмного забезпечення Arduino.	01.05.24	
10	Тестування функцій пристроїв.	02.05.24	
11	Виявлення та виправлення помилок.	03.06.24	
12	Аналіз результатів, підготовка презентації.	05.06.24	
13	Економічні розрахунки та питання з ОП.	06.06.24	
14	Підготовка графічної частини проекту.	07.06.24	
15	Підготовка проекту до захисту та тестування.	10.06.24	

Дипломник  (підпис)  
Керівник  (підпис)



# ЗМІСТ

Вступ.....	7
1 Основний розділ .....	8
1.1 Огляд доцільності застосування системи контролю доступом підприємства.....	8
1.1.1 Актуальність застосування системи контролю доступом підприємства.....	8
1.1.2 Забезпечення безпеки в системі контролю доступом підприємства .....	9
1.1.3 Управління ресурсами за допомогою системи контролю доступу.....	10
1.1.4 Збільшення продуктивності системи контролю доступу ...	12
1.2 Організація доступу на основі QR кодування.....	15
1.2.1 Розвиток системи QR-кодування.....	15
1.2.2 Принцип організації системи контролю доступом підприємства на основі QR кодування .....	16
1.2.3 Генерація унікальних QR-кодів для співробітників підприємства.....	18
1.2.4 Типи та переваги QR-кодів .....	20
1.2.5 Ідентифікаційна інформація співробітника в QR-коді.....	21
1.2.6 Генерація QR-кодів .....	22
1.2.7 Захист QR-кодів від підробки .....	23
1.2.8 Порівняння технології RFID-ідентифікації та QR кодування	24
1.2.9 Фізичні особливості генерації QR кодів.....	25
1.2.10 Методи кодування в QR-кодах.....	27
1.2.11 Переваги використання систем керування доступу на основі QR кодування.....	29
1.2.12 Сумісне використання QR кодування з іншими системами ідентифікації.....	32

1.2.13 Ризики використання QR кодів.....	35
1.3 Розробка системи контролю доступом працівників офісу на основі QR кодування.....	37
1.3.1 Алгоритм створення системи контролю доступу на основі QR кодування.....	37
1.3.2 Розробка карток працівників з QR кодами.....	38
1.3.3 Розробка пристрою QR-кодування на основі платформи Arduino.....	43
1.3.4 Розробка QR-кодів на основі он-лайн генераторів.....	48
2 Економічний розділ.....	51
2.1 Резюме.....	51
2.2 Визначення трудомісткості розробки програмного забезпечення	51
2.3 Розрахунок ціни програмного продукту.....	55
3 Розділ охорони праці та техніка безпеки.....	57
3.1 Аналіз небезпечних і шкідливих факторів, що впливають на програміста при розробці програмного комплексу.....	57
3.2 Гігієнічні вимоги до виробничого середовища.....	58
3.2.1 Вимоги до приміщення.....	58
3.2.2 Освітлення.....	58
3.2.3 Шум.....	58
3.2.4 Мікроклімат.....	59
3.2.5 Електробезпека.....	59
3.2.6 Вимоги до організації робочого місця працівника.....	60
3.3 Пожежна безпека.....	61
Висновки.....	63
Перелік використаних інформаційних джерел.....	64
Додаток А. Слайди мультимедійної презентації.....	65

## ВСТУП

Технологію доступу за QR-кодом доцільно застосовувати на тих об'єктах, де існує постійна потреба у тимчасових перепустках для відвідувачів.

Використання QR-кодів дозволить не витратити додаткові кошти на купівлю перепусток у вигляді пластикових карток, і скоротить тимчасові та людські ресурси, що витрачаються на облік, повернення та зберігання пластикових перепусток.

З урахуванням того, що QR-коди, як носії інформації, легко копіюються та розсилаються будь-яким електронним способом, тому передбачається, що вони застосовуються для одноразового доступу.

Таким чином, QR-коди, як і штрих код, – це оптимальні ідентифікатори для організації гостьового доступу. Ідентифікатори дешеві, їх можна надрукувати на картах пропуску, бейджах та квитках. Їх можна надіслати електронною поштою.

Основна перевага QR-коду - легке розпізнавання коду фотокамерою мобільного телефону, що дає можливість використання QR-коду у торгівлі, рекламі, виробництві, логістиці. Найбільшого поширення QR-коди отримали в Японії, країні де цей формат штрихового коду був розроблений. Їх можна було зустріти на великій кількості плакатів, пакувань та товарів.

Найбільше визнання QR-код отримав серед користувачів мобільного зв'язку. Для цього потрібно встановити програму розпізнавання QR-коду, за допомогою якої є можливість швидко записувати у свій телефон текстову інформацію, додавати контакти в адресну книгу, переходити по web-посиланнях.

					<b>КС 57. 09 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		7

# 1 ОСНОВНИЙ РОЗДІЛ

## 1.1 Огляд доцільності застосування системи контролю доступом підприємства

### 1.1.1 Актуальність застосування системи контролю доступом підприємства

Системи контролю доступу стали невід'ємною складовою інфраструктури більшості підприємств у сучасному світі. Актуальність цієї теми визначається кількома ключовими факторами:

1) забезпечення безпеки: системи контролю доступу дозволяють підприємствам забезпечити безпеку приміщень, обмежити доступ до конфіденційної інформації та запобігти несанкціонованому втручанню або крадіжкам;

2) управління ресурсами: використання систем контролю доступу дозволяє ефективно управляти ресурсами підприємства, зокрема контролювати робочі години працівників, відстежувати присутність та використання ресурсів;

3) збільшення продуктивності: правильно налаштовані системи контролю доступу можуть сприяти збільшенню продуктивності працівників шляхом автоматизації процесів входу та виходу, а також зменшення витрат часу на адміністративні процедури;

4) відповідність стандартам: в деяких галузях, зокрема у фінансовому секторі, медичній індустрії та інших, наявність систем контролю доступу є вимогою стандартів безпеки та конфіденційності даних;

5) технологічний прогрес: з розвитком технологій з'являються нові можливості для вдосконалення систем контролю доступу, включаючи використання біометричних ідентифікаторів, мобільних додатків та хмарних рішень.

Загалом, системи контролю доступу стають все більш важливим елементом інфраструктури будь-якого підприємства, забезпечуючи безпеку,

					<b>КС 57. 09 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		8

ефективність та відповідність стандартам. Розуміння їхньої ролі та застосування на практиці є ключовими завданнями для керівництва та управління будь-яким підприємством.

### **1.1.2 Забезпечення безпеки в системі контролю доступом підприємства**

Збільшення продуктивності є однією з ключових переваг правильно налаштованих систем контролю доступу на підприємстві. Ось як це може відбуватися:

1) автоматизація процесів входу та виходу: системи контролю доступу можуть бути налаштовані для автоматичного реєстрації входу та виходу працівників. Це дозволяє уникнути ручного введення даних і зберегти час, який раніше був би витрачений на реєстрацію працівників;

2) швидкий доступ до робочого приміщення: замість витрачання часу на очікування адміністратора або персоналу для отримання доступу до робочого приміщення, працівники можуть використовувати електронні картки, біометричні сканери або QR-коди для швидкого та зручного входу;

3) ефективне керування робочим часом: системи контролю доступу можуть допомогти відстежувати час присутності працівників на робочому місці. Це дозволяє керівництву ефективно керувати робочим графіком, уникати зайвих перерв та забезпечувати оптимальне використання робочого часу;

4) зменшення витрат часу на адміністративні процедури: замість традиційних методів реєстрації робочого часу, таких як паперові журнали або електронні таблиці, системи контролю доступу можуть автоматизувати цей процес, зменшуючи необхідність вручного введення даних та спрощуючи адміністративні процедури;

5) підвищення безпеки та конфіденційності даних: використання систем контролю доступу допомагає уникнути несанкціонованого доступу до об'єктів та інформації, що може спричинити витрату часу на відновлення даних або вирішення інцидентів безпеки.

					<b>КС 57. 09 000. 00 ДП ПЗ</b>	<i>Арк.</i>
<i>Зм.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		<b>9</b>

Загалом, правильно налаштовані системи контролю доступу можуть значно підвищити продуктивність працівників, зменшити витрати часу на адміністративні процедури та сприяти загальній ефективності підприємства.



Рисунок 1.1. Турнікет зі зчитувачем системи контролю доступом

### **1.1.3 Управління ресурсами за допомогою системи контролю доступу**

Так, управління ресурсами є однією з ключових переваг систем контролю доступу на підприємстві. Ось як це може відбуватися:

1) контроль робочих годин працівників: системи контролю доступу можуть відстежувати час входу та виходу працівників з робочого приміщення. Це дозволяє керівництву точно визначати робочий час кожного працівника і відповідно планувати графіки роботи;

2) відстеження присутності працівників: завдяки системам контролю доступу можна точно визначити, які працівники знаходяться на робочому місці у певний час. Це дозволяє керівництву вести облік присутності та вчасно реагувати на відсутність працівників без відпустки або інші невідповідності;

3) оптимізація використання ресурсів: знання того, скільки працівників присутні на робочому місці у певний час, дозволяє керівництву ефективно планувати використання ресурсів, таких як обладнання, матеріали та інші активи.

					<b>КС 57. 09 000. 00 ДП ПЗ</b>	<i>Арк.</i>
<i>Зм.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		<b>10</b>

4) контроль доступу до об'єктів та ресурсів: системи контролю доступу можуть обмежувати доступ працівників до певних об'єктів або ресурсів на підприємстві в залежності від їх ролі та повноважень. Це допомагає запобігти несанкціонованому використанню або зловживанню ресурсами;

5) аналіз ефективності використання ресурсів: системи контролю доступу можуть збирати дані про використання ресурсів та присутність працівників, що дозволяє проводити аналіз ефективності та оптимізувати використання ресурсів для досягнення більшої продуктивності та ефективності підприємства.

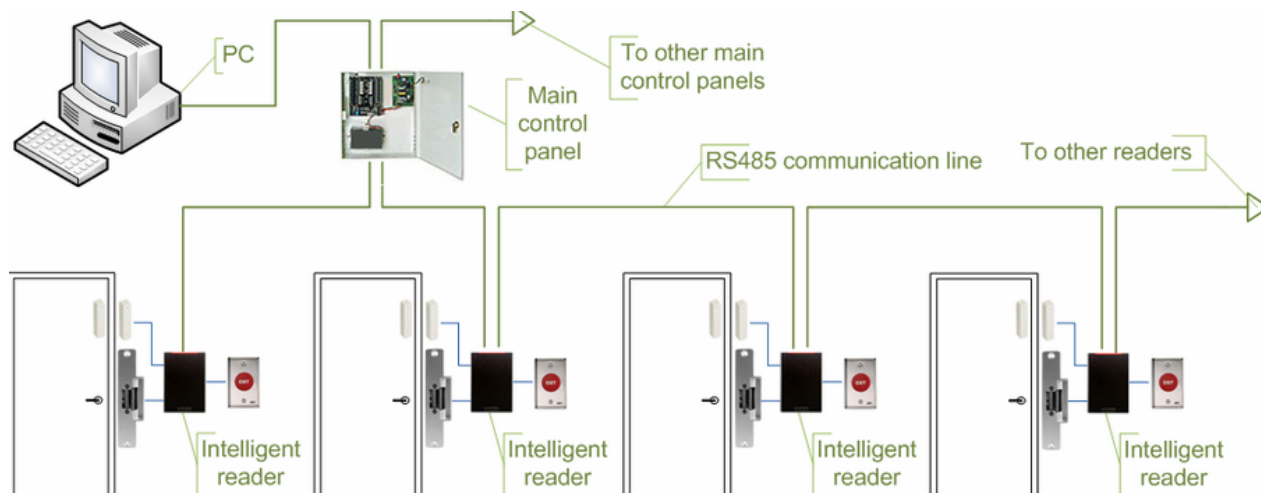


Рисунок 1.2. Система контролю доступу приміщень офісу за допомогою інтелектуальних пристроїв зчитування

Отже, використання систем контролю доступу дозволяє підприємствам ефективно управляти ресурсами, контролювати робочі години працівників, відстежувати присутність та оптимізувати використання ресурсів для досягнення більшої продуктивності та ефективності бізнесу.



Рисунок 1.3. Безконтактна картка-пропуск

### 1.1.4 Збільшення продуктивності системи контролю доступу

Правильно налаштовані системи контролю доступу можуть суттєво сприяти збільшенню продуктивності працівників. Ось детальніше, як це може статися:

1) автоматизація процесів входу та виходу: системи контролю доступу можуть бути налаштовані для автоматичного реєстрування входу та виходу працівників. Замість того, щоб працівники тратили час на оформлення паперових журналів або ручне звільнення, вони можуть використовувати картки доступу, біометричні сканери або інші електронні методи, що забезпечують швидкий та ефективний вхід та вихід;

2) зменшення витрат часу на адміністративні процедури: системи контролю доступу можуть автоматизувати адміністративні процедури, пов'язані з управлінням доступом працівників. Наприклад, вони можуть автоматично генерувати звіти про час роботи, відпустки та відсутність, що дозволяє уникнути ручного ведення цих документів та зменшити кількість помилок;

3) покращена точність та надійність: використання електронних систем контролю доступу забезпечує більш високу точність та надійність у порівнянні з традиційними методами, що може допомогти уникнути помилок та затримок, пов'язаних з людським фактором;

4) ефективне управління робочим часом: системи контролю доступу дозволяють точно відстежувати час, проведений працівниками на робочому місці, і вести облік їхньої присутності. Це дозволяє керівництву ефективно планувати робочий графік, уникати зайвих перерв та забезпечувати оптимальне використання часу.

Отже, правильно налаштовані системи контролю доступу допомагають збільшити продуктивність працівників шляхом автоматизації процесів входу та виходу, а також зменшення витрат часу на адміністративні процедури, що в кінцевому підсумку призводить до підвищення ефективності роботи підприємства.

					<b>КС 57. 09 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		12

Відповідність стандартам безпеки та конфіденційності даних є критично важливою для багатьох галузей, зокрема фінансового сектору, медичної індустрії та інших сфер, де обробка конфіденційної інформації є нормою.

Ось як системи контролю доступу сприяють відповідності стандартам:

1) захист від несанкціонованого доступу: системи контролю доступу допомагають обмежити доступ до чутливої інформації лише авторизованим користувачам. Це дозволяє підприємствам дотримуватися вимог щодо захисту даних та уникнути несанкціонованого доступу;

2) аудит доступу: багато систем контролю доступу забезпечують можливість ведення журналу доступу, який включає інформацію про всі спроби доступу до системи, включаючи дату, час і результати спроб. Це дозволяє підприємствам відстежувати та аналізувати доступ до чутливої інформації та відповідати вимогам стандартів безпеки;

3) біометрична ідентифікація: деякі системи контролю доступу використовують біометричні дані, такі як відбитки пальців або розпізнавання обличчя, для ідентифікації користувачів. Це забезпечує більш високий рівень безпеки, оскільки біометричні дані важко підробити чи підмінити;

4) шифрування даних: багато систем контролю доступу забезпечують можливість шифрування чутливої інформації, що передається через систему. Це забезпечує додатковий рівень захисту та допомагає підприємствам відповідати вимогам стандартів щодо захисту даних.

Отже, системи контролю доступу допомагають підприємствам відповідати вимогам стандартів безпеки та конфіденційності даних, забезпечуючи захист від несанкціонованого доступу, аудит доступу, використання біометричних даних та шифрування інформації.

Технологічний прогрес відкриває нові можливості для вдосконалення систем контролю доступу. Ось деякі з них:

1) біометричні ідентифікатори: використання біометричних даних, таких як відбитки пальців, розпізнавання обличчя, структура судин руки тощо,

					<b>КС 57. 09 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		13

дозволяє більш надійно ідентифікувати користувачів. Це забезпечує високий рівень безпеки, оскільки біометричні дані важко підробити;

2) мобільні додатки: розвиток мобільних технологій дозволяє використовувати смартфони та інші мобільні пристрої як засоби ідентифікації та автентифікації. За допомогою спеціальних додатків працівники можуть отримувати доступ до приміщень або ресурсів підприємства без необхідності використання фізичних ключів або карток доступу;

3) хмарні рішення: використання хмарних технологій дозволяє зберігати та обробляти дані систем контролю доступу в онлайн-режимі. Це забезпечує більшу гнучкість та доступність, оскільки дані можуть бути доступні з будь-якого місця та пристрою з Інтернет-підключенням;

4) інтеграція з іншими системами: сучасні системи контролю доступу можуть бути легко інтегровані з іншими інформаційними системами підприємства, такими як системи управління персоналом, системи відеоспостереження, системи безпеки тощо. Це дозволяє створювати комплексні та повністю автоматизовані рішення для забезпечення безпеки та контролю доступу;

5) аналітика та штучний інтелект: використання аналітики даних та штучного інтелекту дозволяє системам контролю доступу прогнозувати та виявляти аномальні події, виявляти несправності та оптимізувати роботу системи. Це дозволяє підприємствам реагувати на потенційні загрози швидко та ефективно.

Отже, розвиток технологій відкриває широкі можливості для вдосконалення систем контролю доступу, забезпечуючи більшу безпеку, гнучкість та ефективність для підприємств.

					<b>КС 57. 09 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		14

## 1.2 Організація доступу на основі QR-кодування

### 1.2.1 Розвиток системи QR-кодування

QR-коди (Quick Response Codes) були розроблені японською компанією Denso Wave у 1994 році. Основною метою їх створення було швидке читання символів та зберігання більшої кількості інформації, ніж традиційні штрих-коди.

Ось основні етапи розвитку QR-кодів:

1) створення: QR-коди були винайдені і розроблені компанією Denso Wave у 1994 році як відповідь на потребу швидкого і ефективного сканування інформації. Перша версія QR-коду була представлена в японському автомобільному промисловому секторі для відстеження запчастин та автомобільних компонентів;

2) стандартизація: у 1999 році QR-код був стандартизований як ISO/IEC 18004:2000, що дозволило йому стати загальноприйнятим у багатьох галузях та країнах;

3) популяризація: з часом QR-коди стали широко використовуватися в різних сферах, таких як маркетинг, реклама, логістика, туризм, електронна комерція та інші. Вони стали особливо популярними у Японії та Азії, а потім поширилися по всьому світу;

4) використання в мобільних технологіях: з появою смартфонів і програм для сканування QR-кодів, використання QR-кодів значно зросло. Багато смартфонів мають вбудовані камери та програмне забезпечення, що дозволяє легко сканувати QR-коди;

5) розвиток функціональності: поступово QR-коди стали більш функціональними, дозволяючи включати в них різноманітні дані, такі як URL-адреси, контактні дані, географічні координати, події календаря, Wi-Fi мережі тощо;

6) інтеграція з різними сферами діяльності: QR-коди стали необхідною частиною багатьох сучасних бізнес-процесів. Вони використовуються для

					<b>КС 57. 09 000. 00 ДП ПЗ</b>	<i>Арк.</i>
<i>Зм.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		<b>15</b>

маркетингу, реклами, лояльності клієнтів, логістики, контролю доступу, електронних платежів та інших цілей.

Загалом, QR-коди пройшли довгий шлях від свого винайдення до широкого використання в різних сферах діяльності та стали невід'ємною частиною сучасного цифрового світу.

## **1.2.2 Принцип організації системи контролю доступом підприємства на основі QR кодування**

Системи контролю доступу на основі QR-кодів можуть бути дуже ефективними для підприємств, які хочуть забезпечити безпеку своїх приміщень і контролювати доступ до різних зон. Ось деякі ключові елементи та переваги таких систем:

1) генерація QR-кодів: кожен співробітник може мати свій унікальний QR-код, який може бути згенерований спеціальним програмним забезпеченням або системою контролю доступу. Цей код може містити інформацію про рівень доступу співробітника, час його дії, ідентифікаційні дані тощо;

2) сканування QR-кодів: для входу в певну зону співробітник просто сканує свій QR-код за допомогою мобільного пристрою або спеціального QR-сканера, встановленого на вході. Це може бути швидкою та зручною процедурою;

3) цифровий контроль доступу: QR-коди можуть бути пов'язані з базою даних, яка визначає права доступу співробітників. Це дозволяє забезпечити диференційований доступ до різних зон приміщення залежно від потреб бізнесу.

4) зручність управління: адміністратори можуть легко керувати доступом, активуючи або деактивуючи QR-коди, оновлюючи права доступу та відстежуючи активність користувачів через спеціальне програмне забезпечення;

5) збереження даних із контролем доступу: системи на основі QR-кодів можуть зберігати дані про те, хто, коли і де входив або виходив. Це може бути корисно для ведення журналів доступу та аналізу активності;

					<b>КС 57. 09 000. 00 ДП ПЗ</b>	<i>Арк.</i>
<i>Зм.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		<b>16</b>

б) низька вартість впровадження: у порівнянні з деякими іншими системами контролю доступу, розробка та впровадження системи на основі QR-кодів може бути більш доступною з фінансової точки зору.

Звісно, існують і обмеження таких систем, такі як можливість підробки QR-кодів та залежність від наявності мобільних пристроїв для сканування кодів. Але в цілому, системи контролю доступу на основі QR-кодів можуть бути ефективним рішенням для багатьох підприємств.

На рис 1.4 надана основні складові системи контролю доступу на основі QR-кодів.

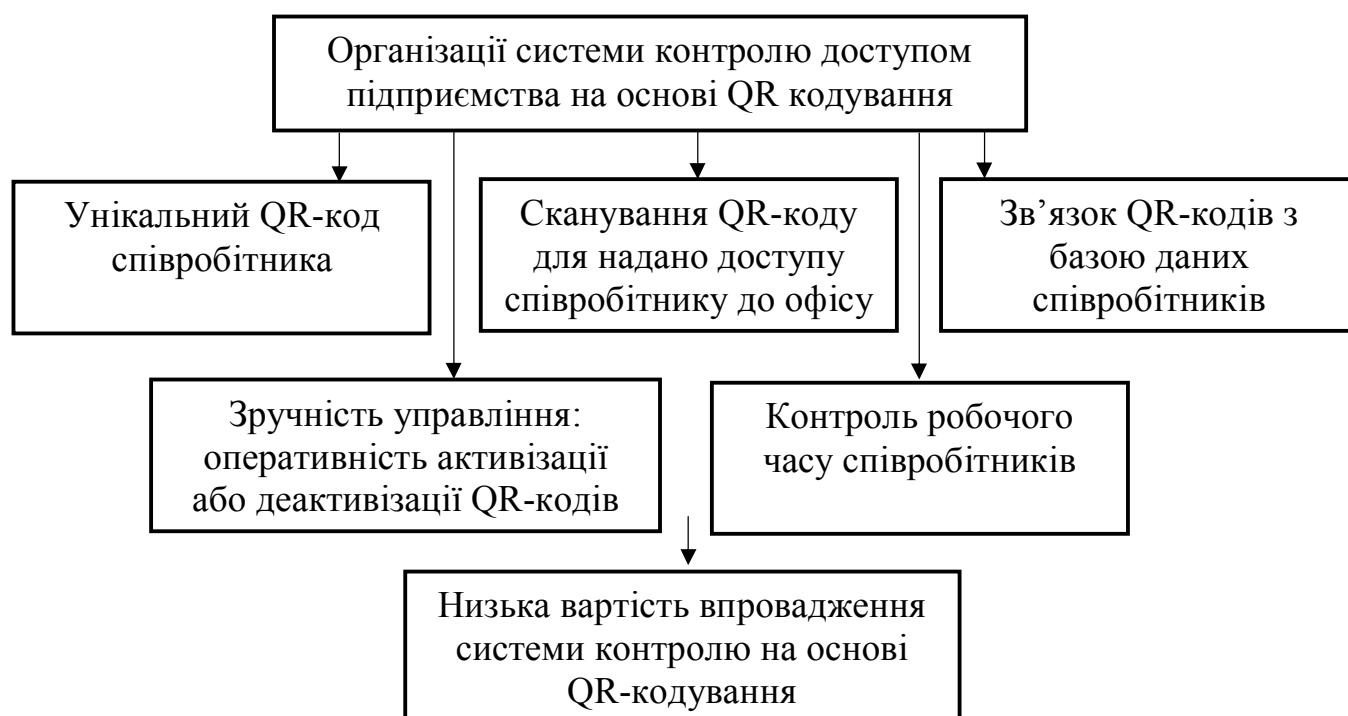


Рисунок 1.4. Основні складові системи контролю доступу на основі QR-кодів



Рисунок 1.5. Приклади нанесення QR-коду на етикетках товару

### 1.2.3 Генерація унікальних QR-кодів для співробітників підприємства

Генерація унікальних QR-кодів для кожного співробітника є ключовим етапом у створенні системи контролю доступу на основі QR-кодів. Ось деякі аспекти цього процесу:

1) унікальність кодів: кожен співробітник повинен мати свій власний унікальний QR-код, який може ідентифікувати його в системі. Це може бути забезпечено шляхом використання унікальних ідентифікаторів, таких як номери працівників або персональні дані;

2) інформація в коді: крім основної ідентифікаційної інформації, яка вказує на особу, QR-код може містити інші дані, такі як рівень доступу співробітника, час його дії (наприклад, часові обмеження доступу), дозволені зони доступу, інформація про відділ або посаду тощо;

3) генерація кодів: QR-коди можуть бути згенеровані за допомогою спеціального програмного забезпечення або систем контролю доступу. Це може включати в себе автоматичну генерацію на основі даних з бази даних або ручне створення кодів для кожного працівника;

4) захист від підробки: для забезпечення безпеки системи важливо захистити QR-коди від підробки. Це може бути досягнуто шляхом використання

криптографічних методів, захисту доступу до системи генерації кодів, а також заходів безпеки на рівні пристроїв, які сканують коди.

Загальна мета полягає в тому, щоб кожен QR-код був унікальним для кожного співробітника і містив достатню інформацію для ідентифікації та контролю доступу до приміщень або зон підприємства.



Рисунок 1.6. Застосування спеціального принтеру для друк етикеток товару з QR-кодами

На рис. 1.7 наведено приклад застосування QR-коду в рекламі.

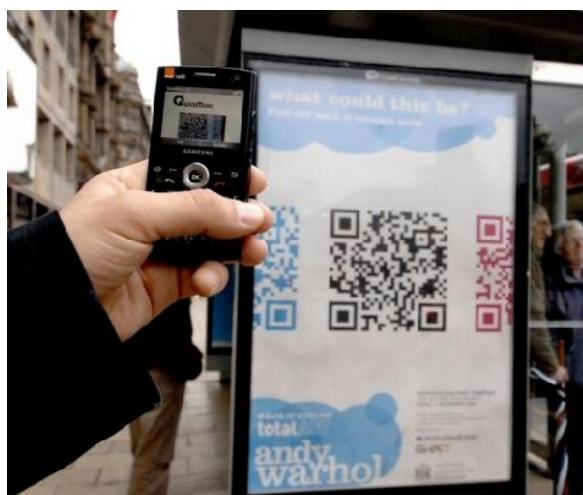


Рисунок 1.7. Приклад реалізації реклами та акції за допомогою QR-коду

					КС 57. 09 000. 00 ДП ПЗ	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		19



Рисунок 1.8. Застосування QR-коду для ідентифікації білету на проїзд

## 1.2.4 Типи та переваги QR-кодів

Сканування QR-кодів для входу в певну зону може бути швидкою та зручною процедурою як для співробітників, так і для адміністраторів. Ось деякі важливі аспекти цього процесу:

- 1) мобільність: використання мобільних пристроїв для сканування QR-кодів дозволяє співробітникам легко мати доступ до свого коду без необхідності носити додаткові картки або пристрої;
- 2) швидкість: процес сканування QR-кодів зазвичай дуже швидкий, що зменшує час, необхідний для входу в зону або приміщення. Це особливо важливо у випадках, коли потрібно обробляти багато людей;
- 3) зручність: співробітники можуть сканувати QR-коди з будь-якого кутка зони чи приміщення, що робить цей процес зручним і простим;
- 4) легкість використання: багато сучасних мобільних пристроїв вже мають вбудовані функції сканування QR-кодів, що робить цей процес ще простішим і доступним для більшості співробітників;
- 5) автоматизація: інтеграція сканерів QR-кодів з інформаційними системами підприємства дозволяє автоматизувати процеси реєстрації входу та виходу співробітників, що полегшує адміністрування та забезпечує точність даних.

					<b>КС 57. 09 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		20

Загалом, сканування QR-кодів для контролю доступу може бути ефективним та зручним рішенням для багатьох підприємств, які шукають спосіб підвищити безпеку та ефективність управління доступом.

QR-коди можуть мати різні типи, в залежності від їхньої структури та призначення. Ось деякі типи QR-кодів, які часто використовуються:

1) URL-коди: ці QR-коди містять URL-адресу, яка може бути відсканована мобільним пристроєм і відкрита веб-сторінка або додаток;

2) текстові коди: QR-коди можуть містити текстову інформацію, таку як повідомлення, контактні дані, прості тексти або будь-який інший текстовий контент;

3) контактні карти: ці QR-коди містять інформацію про контактну особу, включаючи ім'я, номер телефону, адресу електронної пошти тощо;

4) географічні місця: QR-коди можуть містити координати географічного місця, які можуть бути використані для відображення місця на мапі;

5) Wi-Fi мережі: QR-коди можуть містити дані для автоматичного підключення до Wi-Fi мережі, включаючи ім'я мережі та пароль;

6) події календаря: ці QR-коди містять дані про подію календаря, такі як дату, час і опис події, які можуть бути імпортовані в календарний додаток;

7) шифровані дані: QR-коди можуть містити зашифровані дані, які можуть бути розкодовані лише з використанням певного ключа або пароля;

8) оплата: деякі QR-коди призначені для проведення платежів, дозволяючи сканувати їх для здійснення транзакцій.

Ці типи QR-кодів покривають різноманітність сценаріїв використання від реклами та маркетингу до обміну даними та забезпечення безпеки.

### **1.2.5 Ідентифікаційна інформація співробітника в QR-коді**

Дані можуть бути включені в QR-код для ідентифікації співробітника або доступу до приміщень. Нижче подано деякі можливі варіанти:

1) основна ідентифікаційна інформація: ім'я, прізвище, фотографія, ідентифікатор співробітника або номер картки;

					<b>КС 57. 09 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		21

2) рівень доступу співробітника: це може бути роль або рівень привілеїв співробітника в системі безпеки, наприклад, "звичайний користувач", "адміністратор" тощо;

3) часові обмеження доступу: це визначає, коли співробітник може мати доступ до певних зон або будівель. Це може бути час вхідного та вихідного пункту або період дії карти доступу;

4) дозволені зони доступу: це визначає, до яких конкретних зон або приміщень співробітник має доступ. Наприклад, "зона А", "корпус 1", "офіс 302" тощо;

5) інформація про відділ або посаду: це може включати відділ або підрозділ, до якого належить співробітник, або його посаду в організації.

Враховуючи ці аспекти, QR-код може містити широкий спектр інформації, пов'язаної з ідентифікацією співробітника та його доступом до приміщень.



Рисунок 1.9. QR-коди містять URL-адресу для оплати товару

## 1.2.6 Генерація QR-кодів

QR-коди можуть бути згенеровані різними способами з використанням різних програмних засобів або систем контролю доступу (рис. 2.7). Ось кілька можливих способів генерації QR-кодів:

1) програмне забезпечення для генерації QR-кодів: існують спеціальні програми та онлайн-сервіси, які дозволяють генерувати QR-коди на основі введених даних. Це можуть бути загальнопризначені програми або спеціальні інструменти для створення QR-кодів для конкретних цілей;

					<b>КС 57. 09 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		22

2) системи контролю доступу: деякі системи контролю доступу, які використовуються в офісах або інших установах, можуть мати вбудовані функції для генерації QR-кодів. Ці системи можуть автоматично генерувати QR-коди на основі даних з бази даних про співробітників або з іншого джерела інформації;

3) бази даних: для автоматичної генерації QR-кодів можна використовувати дані з бази даних про співробітників. Система може автоматично генерувати QR-код для кожного співробітника на основі його основних ідентифікаційних даних та інших відомостей;

4) ручне створення: у випадках, коли автоматична генерація не є можливою або необхідною, QR-коди можуть бути створені вручну для кожного працівника. Це може вимагати використання спеціального програмного забезпечення або інструментів для створення QR-кодів.

### **1.2.7 Захист QR-кодів від підробки**

Захист від підробки QR-кодів дійсно є важливою аспектом забезпечення безпеки системи. Нижче наведено деякі заходи, які можна вжити для цього:

1) використання криптографічних методів: QR-коди можуть бути захищені за допомогою криптографічних методів, таких як цифровий підпис або шифрування. Це дозволить перевіряти автентичність та цілісність QR-коду під час сканування;

2) захист доступу до системи генерації кодів: система, що генерує QR-коди, повинна мати високий рівень безпеки. Це може включати аутентифікацію та авторизацію користувачів, контроль доступу до функцій генерації кодів та аудит використання системи;

3) заходи безпеки на рівні пристроїв, які сканують коди: користувачам слід надавати інструкції щодо безпечного сканування QR-кодів. Також можуть бути встановлені заходи безпеки на пристроях, які здійснюють сканування, наприклад, застосунки антивірусного захисту або програми, що перевіряють інтегритет QR-кодів перед їх використанням;

4) використання одноразових кодів або обмеження терміну дії: QR-коди можуть мати обмежений термін дії або бути одноразовими, що знижує ризик підробки. Після першого сканування код може бути недійсним або перевірений на іншій основі;

5) фізичний захист: коди можуть бути фізично захищені, наприклад, шляхом застосування спеціальних етикеток або покриття, що унеможлиблює їхнє модифікування без пошкодження.

Ці заходи можуть бути використані окремо або у поєднанні, щоб забезпечити високий рівень захисту від підробки QR-кодів.

## **1.2.8 Порівняння технології RFID-ідентифікації та QR кодування**

RFID (Radio Frequency Identification) та QR (Quick Response) кодування - це дві різні технології, які використовуються для ідентифікації та зберігання інформації. Ось деякі порівняльні аспекти обох технологій:

1) тип інформації:

- RFID: зберігає інформацію на мікрочіпах, які вбудовані в RFID-теги або мітки. Ця інформація може бути унікальним ідентифікатором або невеликим обсягом даних;

- QR код: зберігає дані у вигляді двовимірного штрих-коду, який може містити більше інформації, включаючи текст, веб-посилання, контактну інформацію тощо;

2) зчитування:

- RFID: зчитується за допомогою радіочастотного сигналу, який передається через антенну;

- QR код: сканується за допомогою камери мобільного пристрою або спеціального сканера;

3) дальність зчитування:

- RFID: може бути зчитаний на відстані без контакту або неприродною перешкодою, зазвичай декілька метрів;

					<b>КС 57. 09 000. 00 ДП ПЗ</b>	<i>Арк.</i>
<i>Зм.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		<b>24</b>

- QR код: потрібно знаходитися в межах прямого огляду та відстані, яка залежить від розміру коду;

4) витривалість та зносостійкість:

- RFID: теги можуть бути вбудовані в предмети та мати високу витривалість, оскільки вони не потребують прямого контакту для зчитування;

- QR код: потребує надійного видимого коду, що може зазнати пошкоджень або втратити зчитування при зносі;

5) вартість та масштабованість:

- RFID: зазвичай дорожчий на виробництві, особливо для вбудованих пристроїв, але може бути ефективним у великих масштабах застосування;

- QR код: виготовлення QR кодів дуже дешево, але для великих масштабів їх складно керувати;

б) застосування:

- RFID: використовується у сферах, де потрібно відстежувати та ідентифікувати предмети, як от у супермаркетах (для інвентаризації), в логістиці (для відстеження вантажів), у безпеці (для контролю доступу) і т.д;

- QR код: використовується в рекламі, маркетингу, зв'язку з споживачами, а також для швидкого доступу до веб-сайтів, відстеження даних та інших бізнес-процесів.

Обидва ці методи мають свої переваги та недоліки, і вибір між ними залежить від конкретних потреб і вимог вашого застосування.

### 1.2.9 Фізичні особливості генерації QR кодів

QR-коди (Quick Response коди) - це двовимірні штрихкоди, які можуть зберігати значно більше інформації, ніж звичайні лінійні штрихкоди. Генерація QR-кодів базується на декількох фізичних особливостях:

1) Структура QR-коду: QR-коди складаються з чорних і білих квадратів, які розміщені на квадратній сітці. Основні елементи QR-коду включають:

- форматні інформаційні блоки\*\*: вказують на використані коригувальні коди та маску;

					<b>КС 57. 09 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		25

- блоки вирівнювання: використовуються для корекції спотворень;  
- зондувальні візерунки: розташовані в трьох кутах і служать для визначення орієнтації коду;

- синхронізаційні лінії: допомагають виявляти окремі модулі в QR-коді;  
- поле тихої зони: порожнє поле навколо QR-коду для забезпечення коректного зчитування;

2) Модулі: QR-коди складаються з модулів, які представляють бінарні дані. Кожен модуль може бути білим або чорним, що відповідає бітам 0 або 1;

3) Алгоритми кодування: QR-коди можуть кодувати дані різними способами:

- Numeric Mode: для числових даних (0-9);  
- Alphanumeric Mode: для буквено-цифрових даних (0-9, A-Z, пробіл, і деякі спеціальні символи);

- Byte Mode: для байтових даних;  
- Kanji Mode: для кодування японських символів;

4) Рівні корекції помилок: QR-коди підтримують чотири рівні корекції помилок (L, M, Q, H), які використовують код Ріда-Соломона для виправлення помилок, викликаних пошкодженням або спотворенням коду:

- L (Low): до 7% помилок можуть бути виправлені;  
- M (Medium): до 15% помилок;  
- Q (Quartile): до 25% помилок;  
- H (High): до 30% помилок;

5) Генерація QR-кодів: процес генерації QR-коду включає наступні кроки:

- кодування даних: введені дані кодуються відповідно до обраного режиму;  
- розміщення даних: кодування даних розміщуються в модульній сітці відповідно до алгоритмів;

- додавання коригувальних кодів: додаються коди корекції помилок відповідно до обраного рівня<sup>4</sup>

- маскування: для зменшення можливих проблем зі зчитуванням, модулі QR-коду маскуються різними візерунками, і обирається найкращий з них;

					<b>КС 57. 09 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		26

- фінальна структура: створюється остаточний QR-код з усіма елементами;

6) Фізичне представлення: QR-коди можуть бути роздруковані на папері, наклеєні на різні поверхні, або показані на екранах електронних пристроїв. Важливо забезпечити контрастність між білими і чорними модулями, а також дотримуватися мінімальних розмірів для коректного зчитування;

7) Сканування QR-коду: для зчитування QR-кодів використовуються спеціальні сканери або камери смартфонів. Алгоритми обробки зображень визначають позиції основних елементів QR-коду, аналізують структуру модулів і декодують інформацію.

Завдяки цим фізичним особливостям QR-коди є надійним, зручним і універсальним способом зберігання та передачі інформації.

В табл. 2.1 надано рівні корекції помилок в QR-коді.

Таблиця 2.1. Рівні корекції помилок в QR-коді

Версія коду	Кількість модулів	Рівень корекції помилок	Цифри	Цифри та літери	Двійкові дані	Kanji
M1	11	-	5	-	-	-
M2	13	L (7 %)	10	6	-	-
		M (15 %)	8	5	-	-
M3		L (7 %)	23	14	9	6
		M (15 %)	18	11	7	4
M4	15	L (7 %)	35	21	15	9
		M (15 %)	30	18	13	8
		Q (25 %)	21	13	9	5

### 1.2.10 Методи кодування в QR-кодах

Інформацію в QR-код можна закодувати кількома методами, вибір яких залежить від символів, що використовуються. Якщо використовуються лише цифри від 0 до 9, застосовується цифрове кодування. Якщо крім цифр необхідно закодувати літери латинського алфавіту, пробіл та символи \$%\*+-./:;, використовується алфавітно-цифрове кодування. Також існує кодування кандзі

для шифрування китайських та японських ієрогліфів і побайтове кодування. Перед кожним способом кодування створюється порожня бітова послідовність, яка потім заповнюється.

Цифрове кодування вимагає 10 біт на 3 символи. Вся послідовність символів розбивається на групи по 3 цифри. Потім кожна група (тризначне число) перетворюється на 10-бітне двійкове число і додається до бітової послідовності. Якщо загальна кількість символів не кратна 3 і в кінці залишається 2 символи, отримане двозначне число кодується 7 бітами, а якщо 1 символ - 4 бітами.

Наприклад, є рядок "12345678", який треба закодувати. Послідовність розбивається на числа: 123, 456 і 78, потім кожне число перетворюється на двійковий вигляд: 0001111011, 0111001000, 1001110 і об'єднується в один бітовий потік: 000111101101110010001001110.

Алфавітно-цифрове кодування на відміну від цифрового кодування, для кодування двох символів потрібно 11 біт інформації. Послідовність символів розбивається на групи по 2 символи. Кожен символ у групі кодується відповідно до таблиці «Значення символів у алфавітно-цифровому кодуванні». Значення першого символу множиться на 45, після чого до цього результату додається значення другого символу. Отримане число перетворюється на 11-бітне двійкове число і додається до послідовності біт. Якщо в останній групі залишається один символ, його значення кодується 6-бітним числом.

Розглянемо приклад: «PROOF». Розбиваємо послідовність символів на групи: PR, OO, F. Знаходимо відповідні значення символів кожної групи (дивимося в таблицю): PR - (25, 27), OO - (24, 24), F - (15). Знаходимо значення кожної групи:  $25 * 45 + 27 = 1152$ ,  $24 * 45 + 24 = 1104$ ,  $15 = 15$ . Перетворюємо кожне значення у двійковий вигляд:  $1152 = 10010000000$ ,  $1104 = 10001010000$ ,  $15 = 001111$ . Об'єднуємо в одну послідовність: 1001000000010001010000001111.

Байтове кодування дозволяє закодувати будь-які символи. Вхідний потік символів кодується в будь-якому кодуванні (рекомендовано в UTF-8), після чого перетворюється на двійковий вигляд і об'єднується в один бітовий потік.

					<b>КС 57. 09 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		28

Наприклад, слово "Мир" кодується в Unicode (HEX) у UTF-8: М – D09C; и – D0B8; р – D180. Перетворюємо кожне значення в двійкову систему числення: D0 = 11010000, 9C = 10011100, D0 = 11010000, B8 = 10111000, D1 = 11010001 і 80 = 10000000. Об'єднуємо в один бітовий потік: 11010000 10011100 11010000 10111000 11010001 10000000.

Кандзі – кодування ієрогліфів (та інших символів) базується на таблиці символів або списку зображень ієрогліфів з їх кодами, відомої як "character set". Для японської мови основне значення мають дві таблиці символів: JIS 0208:1997 та JIS 0212:1990, де друга є доповненням до першої. JIS 0208:1997 поділена на 94 сторінки по 94 символи. Наприклад, сторінка 4 містить хірагану, 5 – катакану, 7 – кирилицю, сторінки 16-43 – кандзі першого рівня, а сторінки 48-83 – кандзі другого рівня. Кандзі першого рівня (JIS дайті суйдзюн кандзі) упорядковані за вонами, тоді як кандзі другого рівня (JIS дайні суйдзюн кандзі) упорядковані за ключами, а всередині ключів – за кількістю характеристик.

### **1.2.11 Переваги використання систем керування доступу на основі QR кодування**

Порівняння системи керування на основі QR-кодування з іншими системами включає оцінку різних аспектів, таких як зручність використання, обсяг збереженої інформації, швидкість зчитування, надійність, безпека та вартість реалізації (табл. 2.2). Розглянемо ці фактори детальніше, порівнюючи QR-коди з традиційними штрихкодами, RFID-мітками та NFC:

#### 1) Зручність використання:

- QR-коди: можуть бути зчитані будь-яким пристроєм з камерою та відповідним програмним забезпеченням. Вони можуть бути легко надруковані та прикріплені до різних об'єктів;

- штрихкоди: вимагають спеціальних сканерів для зчитування. Мають обмежену кількість даних, які можна закодувати;

- RFID: вимагає спеціальних RFID-сканерів. Мітки можуть бути прочитані без прямої видимості, що зручно для автоматизації процесів;

					<b>КС 57. 09 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		29

Таблиця 2.2 – Порівняння системи керування на основі QR-кодування з іншими системами

Критерій	QR-коди	Штрихкоди	RFID	NFC
Зручність використання	Легко зчитуються будь-яким пристроєм з камерою	Потрібні спеціальні сканери	Потрібні спеціальні сканери, зчитування без прямої видимості	Потрібні пристрої з підтримкою NFC, працює на близькій відстані
Обсяг збереженої інформації	До 7,089 цифр або 4,296 символів	Обмежений кількістю символів (до кількох десятків)	До кількох кілобайт, може бути перепрограмований	До 8 КБ
Швидкість зчитування	Швидке зчитування при прямій видимості	Швидке зчитування при прямій видимості	Миттєве зчитування без прямої видимості	Швидке зчитування на близькій відстані
Надійність	Вбудовані механізми корекції помилок до 30%	Менш стійкі до пошкоджень	Висока надійність, стійкість до пошкоджень	Висока надійність, вразливість до фізичних пошкоджень
Безпека	Відкриті, можуть бути зчитані будь-яким	Відкриті, легко зчитуються	Можливе шифрування та захист паролями	Підтримує шифрування та захищені транзакції
Вартість реалізації	Дешеві у виготовленні та впровадженні	Недорогі, потребують спеціального обладнання	Висока вартість міток та сканерів	Вартість варіюється, дешевше за RFID, дорожче за QR-коди та штрихкоди

Зм.	Арк.	№ докум.	Підпис	Дата

КС 57. 09 000. 00 ДП ПЗ

Арк.

30

- QR-коди: відкриті, можуть бути легко зчитані будь-ким, хто має пристрій з камерою;

- штрихкоди: також відкриті, легко зчитуються;

- RFID: може бути захищений паролями та шифруванням, що підвищує безпеку;

- NFC: необхідні пристрої з підтримкою NFC. Працює на невеликій відстані, але зручний для безконтактних платежів та ідентифікації;

#### 2) Обсяг збереженої інформації:

- QR-коди: можуть зберігати до 7,089 цифр або 4,296 символів у байтовому форматі, що значно більше, ніж традиційні штрихкоди;

- штрихкоди: зберігають обмежену кількість інформації (до кількох десятків символів);

- RFID: може зберігати великі обсяги даних (кілька кілобайт), а також дозволяє перепрограмування;

- NFC: може зберігати дані обсягом до 8 КБ, достатньо для багатьох додатків;

#### 3) Швидкість зчитування:

- QR-коди: зчитуються швидко, але для цього необхідна пряма видимість та правильне вирівнювання;

- штрихкоди: також зчитуються швидко, але вимагають прямої видимості та відповідного вирівнювання;

- RFID: мітки можуть бути зчитані миттєво, навіть без прямої видимості, що забезпечує високу швидкість обробки;

- NFC: зчитування відбувається швидко, але вимагає близького контакту між пристроями;

#### 4) Надійність:

- QR-коди: мають вбудовані механізми корекції помилок (до 30%), що дозволяє зчитувати інформацію навіть при частковому пошкодженні коду;

- штрихкоди: менш стійкі до пошкоджень. Пошкоджений штрихкод може бути неможливо прочитати;

					<b>КС 57. 09 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		31

- RFID: висока надійність, мітки стійкі до фізичних пошкоджень та забруднень;

- NFC: висока надійність при правильному використанні, хоча мітки можуть бути вразливими до фізичних пошкоджень;

5) Безпека:

- NFC: підтримує шифрування та захищені транзакції, що робить його безпечним для фінансових операцій;

6) Вартість реалізації:

- QR-коди: виготовлення та впровадження коштує дешево, потрібно лише друк кодів;

- штрихкоди: також недорогі у виготовленні, але вимагають спеціального обладнання для зчитування;

- RFID: вартість міток та сканерів вища, але забезпечують автоматизацію та ефективність;

- NFC: вартість залежить від типу міток та пристроїв, зазвичай дорожче, ніж QR-коди та штрихкоди, але дешевше за RFID.

Отже, QR-коди є зручними, універсальними та дешевими у впровадженні, що робить їх ідеальними для багатьох застосувань, де потрібно зберігати та зчитувати велику кількість інформації. Вони перевершують традиційні штрихкоди за обсягом даних та надійністю, але поступаються RFID та NFC за швидкістю зчитування та безпекою. RFID та NFC, хоча й дорожчі, забезпечують більш високий рівень автоматизації та безпеки, що робить їх більш підходящими для складних систем керування та фінансових транзакцій.

### **1.2.12 Сумісне використання QR кодування з іншими системами ідентифікації**

Сумісне використання QR-кодування з іншими системами ідентифікації може забезпечити додаткові переваги для різних сфер застосування. Давайте розглянемо можливості та переваги поєднання QR-кодів з іншими технологіями, такими як штрихкоди, RFID та NFC.

					<b>КС 57. 09 000. 00 ДП ПЗ</b>	<i>Арк.</i>
<i>Зм.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		<b>32</b>

## Приклади сумісного використання:

### 1) Роздрібна торгівля:

- штрихкоди та QR-коди: продукція може мати штрихкод для швидкого зчитування на касі, а також QR-код, який надає доступ до інформації про продукт, відгуки, рецепти або інструкції з використання;

- RFID та QR-коди: використання RFID для автоматизованого обліку товарів на складі та QR-кодів для надання покупцям доступу до детальної інформації про товар;

- NFC та QR-коди: NFC для безконтактної оплати, QR-коди для отримання електронної квитанції або додаткових бонусів та знижок;

Таблиця 2.3 – Інтеграція системи керування на основі QR-кодування з іншими системами

Технологія	Переваги	Сценарії сумісного використання
Штрихкоди	Легко впроваджуються	Використання QR-кодів та штрихкодів на одному товарі: штрихкод для простих операцій, QR-код для додаткової інформації.
	Швидке зчитування	Застосування штрихкодів для базової ідентифікації, а QR-кодів для збереження розширених даних (інструкції, URL-адреси).
RFID	Висока швидкість зчитування	Поєднання RFID для автоматичного відстеження та QR-кодів для забезпечення легкого доступу до додаткової інформації або посилань.
	Зчитування без прямої видимості	Використання RFID для інвентаризації, QR-кодів для деталізованої інформації на кожному товарі.
	Великий обсяг збережених даних	Відстеження логістичних ланцюгів: RFID для відстеження руху товарів, QR-коди для зчитування детальної інформації при перевірці.

Зм.	Арк.	№ докум.	Підпис	Дата

КС 57. 09 000. 00 ДП ПЗ

Арк.

33

NFC	Безконтактна передача даних	Застосування NFC для безконтактних платежів, а QR-кодів для отримання електронних квитанцій або інформації про транзакцію.
	Висока безпека	Використання NFC для ідентифікації користувачів або пристроїв, QR-кодів для доступу до детальної інформації або інструкцій.
	Простота інтеграції з мобільними пристроями	Застосування NFC для швидкої аутентифікації, а QR-кодів для надання додаткових даних або посилань на веб-ресурси.

## 2) Логістика та управління запасами:

- RFID та QR-коди: RFID для відстеження переміщення товарів по логістичному ланцюгу, QR-коди для зберігання детальної інформації про товар, наприклад, походження, дати виробництва та терміну придатності;

- штрихкоди та QR-коди: штрихкоди для швидкого зчитування під час приймання або відправлення товарів, QR-коди для забезпечення доступу до розширеної інформації або інструкцій;

## 3) Охорона здоров'я:

- NFC та QR-коди: NFC для швидкої ідентифікації пацієнтів або медичного обладнання, QR-коди для доступу до електронних медичних записів або інструкцій з використання медичних пристроїв;

- RFID та QR-коди: RFID для відстеження ліків та медичних інструментів, QR-коди для надання медичним працівникам доступу до важливої інформації про пацієнтів або медичні процедури.

Таким чином, сумісне використання QR-кодів з іншими системами ідентифікації може підвищити ефективність та зручність у різних сферах застосування, забезпечуючи швидкий доступ до необхідної інформації, автоматизацію процесів та підвищену безпеку. Кожна з технологій має свої

переваги, і їх поєднання дозволяє використовувати сильні сторони кожної з них для досягнення кращих результатів.

### 1.2.13 Ризики використання QR кодів

Використання QR-кодів приносить багато переваг, але також супроводжується певними ризиками, які важливо враховувати для забезпечення безпеки. Ось основні ризики, пов'язані з використанням QR-кодів, та способи їх мінімізації:

#### 1) Фішинг та соціальна інженерія:

- ризик: зловмисники можуть створювати підроблені QR-коди, які перенаправляють користувачів на шкідливі вебсайти або запитують конфіденційну інформацію;

- заходи: перевіряти джерело QR-кодів перед скануванням;

- використовувати програмне забезпечення для сканування, яке попереджає про потенційно небезпечні посилання;

- навчати користувачів безпечно використання QR-кодів та розпізнавання підозрілих кодів;

#### 2) Підробка QR-кодів:

- ризик: зловмисники можуть підробити QR-код для отримання несанкціонованого доступу до ресурсів або інформації;

- заходи: використовувати динамічні QR-коди, які змінюються після кожного використання або через певний проміжок часу;

- впроваджувати цифрові підписи або хеші для перевірки автентичності QR-кодів;

- використовувати додаткові методи аутентифікації (наприклад, двофакторну аутентифікацію);

#### 3) Шкідливий код та посилання:

- ризик: QR-коди можуть містити шкідливі посилання або код, який може призвести до завантаження шкідливих програм на пристрій користувача;

					<b>КС 57. 09 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		35

- заходи: використовувати програмне забезпечення для сканування QR-кодів, яке перевіряє безпеку посилань перед їх відкриттям;

- навчати користувачів уникати сканування QR-кодів з невідомих або ненадійних джерел;

4) Несанкціоноване відстеження та збір даних:

- ризик: QR-коди можуть бути використані для відстеження місцезнаходження або діяльності користувачів без їх відома.

- заходи: забезпечити прозорість у використанні QR-кодів та даних, що збираються за їх допомогою;

- дотримуватися політик конфіденційності та інформувати користувачів про те, як їхні дані використовуються та зберігаються;

5) Злом QR-кодів для доступу до конфіденційної інформації:

- ризик: QR-коди, що надають доступ до конфіденційних даних або систем, можуть бути використані зловмисниками для отримання несанкціонованого доступу;

- заходи: використовувати шифрування для захисту інформації, що міститься в QR-кодах;

- впроваджувати додаткові рівні безпеки, такі як паролі або PIN-коди, разом із QR-кодами;

6) Фізична безпека QR-кодів:

- ризик: QR-коди можуть бути пошкоджені або замінені зловмисниками, що може призвести до збоїв у системах або несанкціонованого доступу;

- заходи: розміщувати QR-коди в захищених або контрольованих місцях;

- регулярно перевіряти та оновлювати QR-коди для запобігання їх пошкодженню або підміні;

7) Відсутність стандартів та сумісності:

- ризик: відсутність стандартів може призвести до проблем з сумісністю між різними системами або пристроями для сканування QR-кодів;

- заходи: використовувати загальноприйняті стандарти та протоколи для генерації та зчитування QR-кодів;

					<b>КС 57. 09 000. 00 ДП ПЗ</b>	<i>Арк.</i>
<i>Зм.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		<b>36</b>

- забезпечувати сумісність програмного забезпечення для сканування з різними типами QR-кодів.

Отже, врахування цих ризиків та впровадження відповідних заходів безпеки допоможе мінімізувати потенційні загрози при використанні QR-кодів. Це забезпечить безпечне та ефективне використання цієї технології в різних сферах, таких як доступ до ресурсів, фінансові операції та маркетинг.

### **1.3 Розробка системи контролю доступом працівників офісу на основі QR кодування**

#### **1.3.1 Алгоритм створення системи контролю доступу на основі QR кодування**

Створення системи контролю доступу на основі QR кодування можна реалізувати за допомогою різноманітних технологій. Ось деякі кроки та аспекти, які варто врахувати при розробці такої системи:

1) створення QR кодів:

- розробіть механізм для генерації унікальних QR кодів для кожного користувача або для кожного доступу;
- виберіть відповідний формат QR коду та рівень корекції помилок, який підходить для вашої системи;
- інтегруйте створення QR кодів у вашу систему, щоб автоматизувати цей процес;

2) мобільний додаток або веб-сайт:

- розробіть мобільний додаток або веб-сайт, який буде використовуватися для сканування QR кодів та управління доступом;
- забезпечте можливість реєстрації користувачів та призначення їм доступу за допомогою QR кодів;
- включіть функціонал для перевірки дійсності та читання QR кодів через камеру пристрою;

3) база даних користувачів та доступу:

					<b>КС 57. 09 000. 00 ДП ПЗ</b>	<i>Арк.</i>
<i>Зм.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		<b>37</b>

- створіть базу даних, в якій будуть зберігатися дані про користувачів та їх доступ;

- включіть механізми для додавання, редагування та видалення користувачів та їх прав доступу;

4) автоматизація процесу контролю доступу:

- забезпечте можливість автоматичного реєстрування та відслідковування вхідних та вихідних подій;

- інтегруйте систему з існуючими системами безпеки (наприклад, системами відеоспостереження) для підвищення ефективності контролю;

5) безпека та захист даних:

- захистить дані користувачів та інформацію про доступ від несанкціонованого доступу;

- використовуйте шифрування та автентифікацію для забезпечення безпеки даних;

6) тестування та впровадження:

- проведіть тестування системи на відповідність функціональним вимогам та на виявлення можливих проблем;

- після успішного тестування впровадіть систему в роботу;

7) підтримка та оновлення:

- забезпечте постійну підтримку системи та вчасні оновлення для забезпечення її працездатності та безпеки.

Це загальний план, і конкретні кроки можуть змінюватися в залежності від специфіки вашого проекту та ваших вимог.

### **1.3.2 Розробка карток працівників з QR кодами**

Створення системи контролю доступу за допомогою QR кодів на картках працівників може бути досить ефективним та зручним рішенням. Ось кілька кроків, які допоможуть вам реалізувати цю систему:

1) створення карток з QR кодами:

					<b>КС 57. 09 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		38

- потрібно визначте, яка інформація буде зберігатися в QR кодi на картці працівника. Це може бути, наприклад, ім'я працівника, ідентифікатор, дата створення картки тощо;

- потрібно створити QR коди з відповідною інформацією для кожного працівника;

- необхідно роздрукуйте ці QR коди на картках працівників або вбудуйте їх у спеціальні ідентифікаційні картки;

2) мобільний додаток для сканування:

- потрібно розробіть мобільний додаток для працівників, який буде використовуватися для сканування QR кодів на картках;

- необхідно включити у додаток функції, щоб він міг читати та обробляти інформацію з QR кодів;

3) реєстрація працівників та встановлення прав доступу:

- необхідно створити систему для реєстрації нових працівників у вашій системі контролю доступу;

- потрібно надати можливість призначати права доступу для кожного працівника. Це може бути, наприклад, доступ до певних зон або приміщень, графік роботи тощо;

4) контроль доступу:

- необхідно підготувати систему для сканування QR кодів на картках працівників;

- потрібно забезпечити можливість перевірки інформації з QR кодів та порівняння її з даними в базі даних;

- необхідно дозволити доступ до відповідних зон або приміщень тим працівникам, чий картки були успішно зчитані;

5) аудит та звітність:

- необхідно зберігати журнали сканування QR кодів для кожного працівника;

- потрібно забезпечити можливість створення звітів про активність працівників, включаючи вхід та вихід з робочого місця;

					<b>КС 57. 09 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		39

б) безпека та захист даних:

- потрібно захистити дані в QR кодах та базі даних від несанкціонованого доступу;

- потрібно використовуйте шифрування та автентифікацію для забезпечення безпеки даних.

Створення системи контролю доступу на основі QR кодів на картках працівників може підвищити ефективність та безпеку вашого об'єкту.

На рис. 1.10 надано алгоритм роботи системи контролю доступом на основі QR-кодування



Рисунок 1.10. Алгоритм роботи системи контролю доступом на основі QR-кодування

Застосування QR-кодів при виготовленні посвідчень і перепусток може значно полегшити і покращити процес ідентифікації та контролю доступу. Ось деякі можливі варіанти використання:

1) інформація про особу:

- QR код може містити інформацію про особу, як-от ім'я, прізвище, фотографію, дату народження, посаду та інші ідентифікаційні дані;

- ця інформація може бути корисною для швидкої ідентифікації особи та перевірки її прав доступу;

2) доступ до внутрішньої інформації:

- QR код може містити інформацію про права доступу особи. Наприклад, які зони або приміщення вона може відвідувати, або які послуги вона може отримувати;

- персонал зможе легко перевіряти цю інформацію за допомогою мобільного пристрою та спеціального додатка.

3) безпека та захист від підробки:

- QR код може містити зашифровану інформацію, що робить його важким для підробки;

- використання цифрового підпису або інших методів захисту може забезпечити автентичність та непідробність посвідчення або перепустки;

4) посилання на додаткову інформацію:

- QR код може містити посилання на додаткову інформацію, таку як правила безпеки, евакуаційні маршрути, контактні дані та інше;

- це може бути особливо корисно в екстрених ситуаціях або для швидкого отримання додаткової інформації;

5) відстеження та аудит:

- QR код може містити ідентифікатор, який дозволить відстежувати використання посвідчення або перепустки;

- це може бути корисним для аудиту доступу, виявлення незвичайних відвідувачів або для вирішення проблем безпеки;

6) мобільний доступ:

- QR код може бути сканований за допомогою мобільного телефону, що дозволяє працівникам та відвідувачам швидко та зручно отримувати доступ;

- це особливо зручно для великих компаній або подій, де необхідно швидко обробляти велику кількість людей;

7) швидке видалення доступу:

- QR код може містити дані, що дозволяють швидко відключити доступ до приміщень або послуг;

- це може бути корисно у випадку втрати або крадіжки посвідчення.

					<b>КС 57. 09 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		41

Використання QR кодів на посвідченнях і перепустках може спростити та покращити процеси ідентифікації та контролю доступу, забезпечуючи при цьому зручність, безпеку та ефективність.

Проведемо аналіз типів QR-кодів, які можна використовувати для створення посвідчень та перепусток.

QR-коди, або Quick Response codes, існують у різних варіаціях, кожна з яких призначена для вирізних цілей. Ось деякі з них:

1) QR-коди URL: цей тип містить URL-адресу веб-сторінки. При скануванні такого коду користувач переходить на відповідну сторінку;

2) QR-коди контактів: вони містять контактну інформацію, таку як ім'я, номер телефону, електронна пошта і адреса. При скануванні такого коду дані можуть бути збережені у контактах смартфона;

3) QR-коди тексту: вони містять простий текстовий рядок. При скануванні такого коду користувач отримує текстове повідомлення або додаткову інформацію;

4) QR-коди подій: використовуються для пропуску на конференцію або концерт. Містять дані про дату, час та місце події, а також інформацію про бронювання квитків;

5) QR-коди товарів: містять інформацію про продукт, виробника, інструкції з використання або посилання на веб-сторінку;

6) QR-коди Wi-Fi: містять інформацію про мережу Wi-Fi, включаючи назву мережі (SSID) і пароль. Користувач може автоматично підключитися до мережі, сканувавши такий код.

Розглянемо процес персоналізації за допомогою QR-кодів. Один із способів персоналізації продукції – це додавання QR-кодів або номерів, що дозволяє включити індивідуальну інформацію на кожен друкований виріб. Ця інформація може містити прізвища, адреси, фотографії або будь-яку іншу інформацію з бази даних або файлу.

Для виконання персоналізації потрібно підготувати та надати дані у форматі Excel, де кожне поле знаходиться в окремому стовпці і містить

					<b>КС 57. 09 000. 00 ДП ПЗ</b>	<i>Арк.</i>
<i>Зм.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		<b>42</b>

інформацію, яка має бути надрукована на виробі. Наприклад, прізвище може бути в першому стовпці, ім'я – у другому, по батькові - у третьому, а посада - у четвертому та так далі.

Після цього програмне забезпечення використовує дані з Excel-файлу для створення відповідного QR-коду.

### **1.3.3 Розробка пристрою сканування QR-коду на основі платформи Arduino**

Створення пристрою QR-кодування на базі платформи Arduino може бути використаний для різних цілей. Ось загальний опис такого пристрою та його можливостей:

1) Arduino як контролер:

- Arduino може виступати як контролер для управління процесом створення QR кодів;

- використовуючи вбудований мікроконтролер та програмування на мові Arduino, ви можете керувати генерацією QR кодів та іншими компонентами пристрою;

2) модуль зчитування QR кодів: для створення пристрою QR-кодування потрібен модуль, який може генерувати QR коди. Найпоширенішим модулем для цього є ESP32 або ESP8266, які мають можливості Wi-Fi та підтримують бібліотеки для роботи з QR кодами;

3) підключення до Інтернету: щоб отримати дані, які будуть включені до QR кодів, пристрій повинен бути підключений до Інтернету. Використовуйте модуль Wi-Fi або Ethernet для підключення до мережі;

4) бібліотеки для генерації QR кодів: існує кілька бібліотек для Arduino, які дозволяють генерувати QR коди. Одна з найпопулярніших - `QRCode.h`, яка працює з ESP32 та ESP8266 та дозволяє створювати QR коди з різними видами інформації, такої як текст, URL або контактні дані;

5) інтерфейс для взаємодії:

- створить спосіб взаємодії з пристроєм, наприклад, за допомогою LCD екрану або через веб-інтерфейс;

- використовуйте кнопки або інші елементи керування для введення даних, які будуть включені до QR кодів;

6) збереження та передача QR кодів: після створення QR коду він може бути збережений на SD картку або відправлений на сервер через Інтернет;

7) застосування: створення QR кодів для електронних візиток, підписей на електронних листах, пристроїв керування доступом або ідентифікації предметів;

8) безпека: потрібно захистити з'єднання та дані, що передаються через Інтернет, використовуючи шифрування та аутентифікацію.

Створення пристрою QR-кодування на базі Arduino вимагає знань програмування мовою Arduino та роботи з мережевими модулями, але він може бути використаний для багатьох цікавих та корисних застосувань.

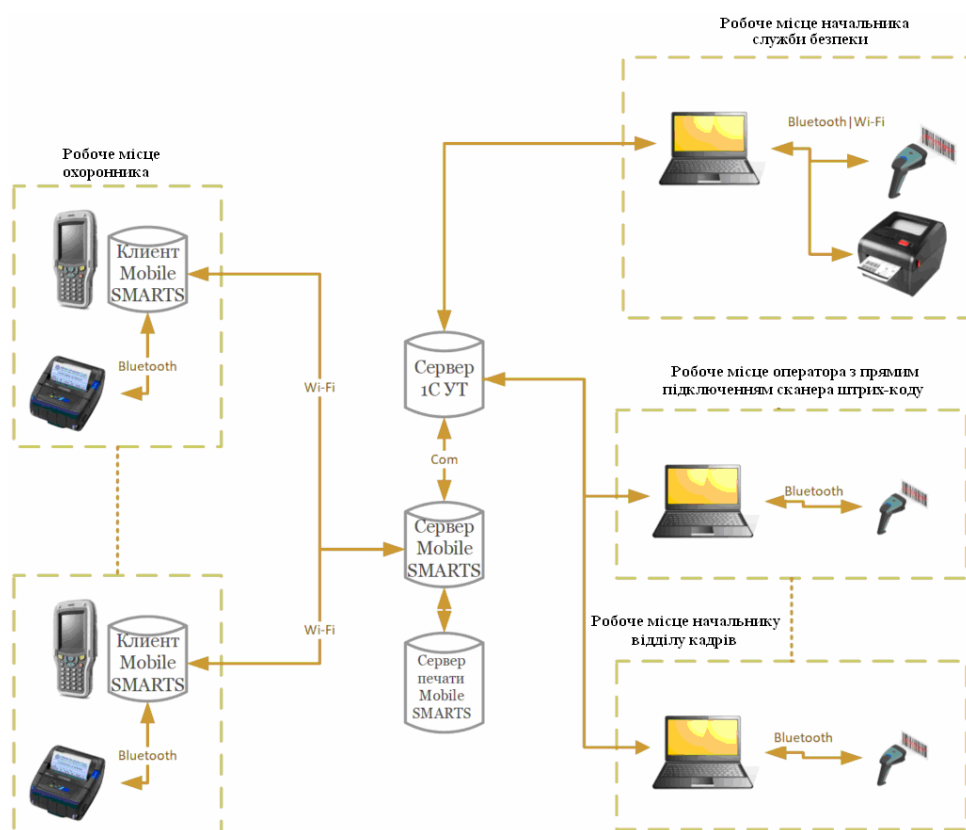


Рисунок 1.11. Система управління доступом до офісу на основі перепусток з QR-кодом

Програмне забезпечення для мікроконтролера Arduino UNO до якого підключено сканер QR кодів GM-45 виглядає наступним чином.

```
#include <SoftwareSerial.h>

// Пін для підключення сканера QR-кодів GM-45
const int qrRxPin = 2; // Пін RX (приймач) сканера
const int qrTxPin = 3; // Пін TX (відправник) сканера

SoftwareSerial qrSerial(qrRxPin, qrTxPin);

void setup() {
  Serial.begin(9600); // Ініціалізація з'єднання з комп'ютером для виводу
результатів
  qrSerial.begin(9600); // Ініціалізація з'єднання зі сканером
}

void loop() {
  // Чекаємо, поки сканер відправить QR код
  while (qrSerial.available() == 0);

  // Зчитуємо QR код зі сканера
  String qrCode = "";
  while (qrSerial.available()) {
    char c = qrSerial.read();
    qrCode += c;
    delay(10); // Затримка для накопичення більшого об'єму даних
  }

  // Виводимо зчитаний QR код на монітор
```

					<b>КС 57. 09 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		45

```
Serial.println("QR Code: " + qrCode);
```

```
// Обробка зчитаного QR коду за вашими потребами
```

```
// Очікуємо коротку паузу перед зчитуванням наступного QR коду
```

```
delay(1000);
```

```
}
```

Ця програма використовує бібліотеку SoftwareSerial, щоб забезпечити зв'язок зі сканером QR-кодів через два внутрішні піни мікроконтролера Arduino UNO (піни 2 та 3). Сканер QR кодів GM-45 підключається до цих пінів через TTL-інтерфейс.

Щоб встановити бібліотеку SoftwareSerial, виберіть пункт меню "Sketch" -> "Include Library" -> "Manage Libraries", введіть "SoftwareSerial" у поле пошуку та встановіть бібліотеку.

Програма очікуватиме на зчитування QR-кодів з сканера та виводитиме їх на моніторі серійного порту Arduino (вивід можна переглянути в Arduino IDE через "Tools" -> "Serial Monitor").

Також потрібно підключити живлення (VCC та GND) сканера QR-кодів, а також підключити його TX пін до піну RX мікроконтролера, та RX пін до піну TX мікроконтролера.

Сканер GM-45 – це компактний та потужний сканер, який призначений для швидкого та ефективного зчитування різних типів штрих-кодів, включаючи одно- та двомірні коди. Ось деякі більш детальні характеристики:

1) підтримка форматів штрих-кодів: GM-45 здатний зчитувати широкий спектр штрих-кодів, включаючи одновимірні (наприклад, EAN, UPC, Code 39) та двовимірні (наприклад, QR-коди, Data Matrix, PDF417);

2) швидкість сканування: висока швидкість сканування дозволяє швидко та ефективно зчитувати штрих-коди навіть у швидкоплинних ситуаціях;

3) підтримка QR-кодів: особливий акцент робиться на підтримці QR-кодів, що робить цей сканер ідеальним для використання в сучасних системах ідентифікації, маркетингу та служби підтримки;

4) підтримка підключення: сканер може підключатися до різних пристроїв, включаючи комп'ютери, смартфони та планшети, за допомогою різних інтерфейсів, таких як USB, Bluetooth або бездротові технології;

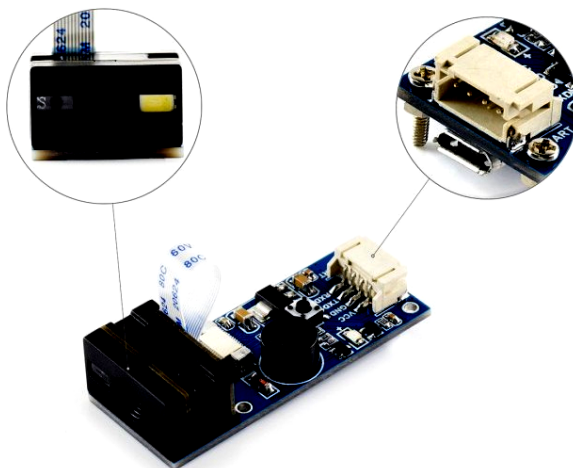
5) компактний дизайн: його компактний розмір робить його зручним для перенесення та використання в різних умовах, включаючи магазини, склади, офіси та інші місця;

6) ергономічний дизайн: зручна форма та ергономічний дизайн дозволяють користувачам комфортно використовувати сканер протягом тривалого часу без втоми;

7) надійність: GM-45 має високу надійність та стійкість до різних умов експлуатації, що робить його надійним рішенням для будь-якого бізнесу;

8) сумісність з різними операційними системами: він може працювати з різними операційними системами, такими як Windows, Android, iOS, що дозволяє його використовувати з широким спектром пристроїв.

Загалом, сканер GM-45 є потужним і універсальним інструментом для зчитування штрих-кодів у різних ситуаціях, що дозволяє ефективно використовувати його в різних галузях, від роздрібної торгівлі до складського управління та багато іншого. На рис 3.8 надано зовнішній вид сканер OR та штрих-кодів GM-45



					<b>КС 57. 09 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		47

Рисунок 1.12. Сканер OR та штрих-кодів GM-45

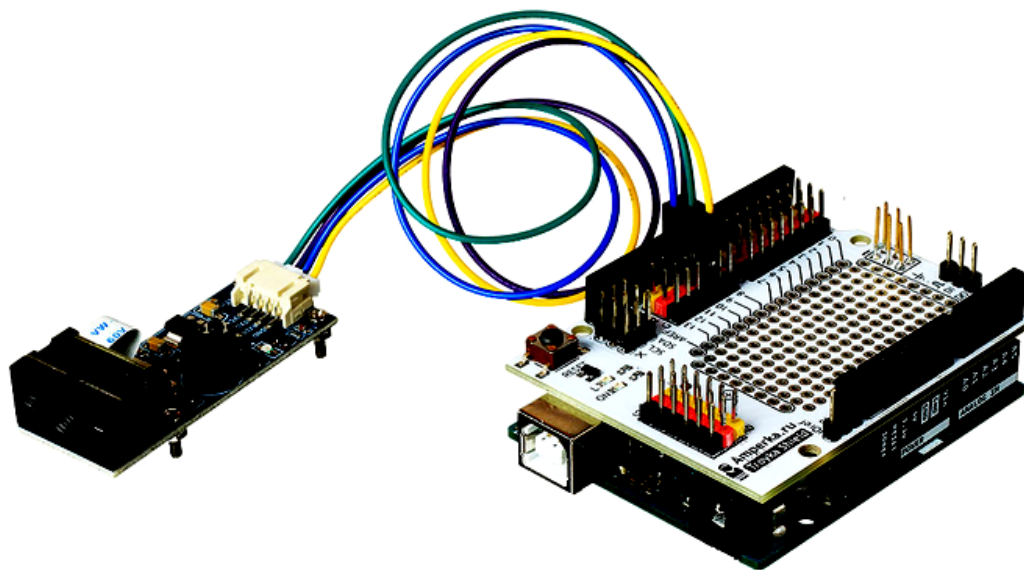


Рисунок 1.13. Підключення сканер OR GM-45 до плати Arduino-Uno

### 1.3.4 Розробка QR-кодів на основі он-лайн генераторів

Програмні генератори QR-кодів – це програми або сервіси, які дозволяють створювати QR-коди за допомогою комп'ютера, смартфона або іншого пристрою. Ось кілька популярних програмних генераторів QR-кодів:

1) QR Code Generator ([qr-code-generator.com](http://qr-code-generator.com)): це онлайн-сервіс, який дозволяє створювати QR-коди для різних цілей, таких як URL-адреси, текстові повідомлення, контактні дані, географічні координати і багато іншого. Ви можете налаштувати розмір, кольори та інші параметри QR-коду;

2) QR Code Monkey ([qr-code-monkey.com](http://qr-code-monkey.com)): ще один онлайн-генератор QR-кодів з багатьма функціями настройки. Він дозволяє створювати QR-коди для URL, тексту, електронної пошти, Wi-Fi мережі, інструкцій з оплати, зворотних дзвінків і багатьох інших;

3) QR Droid ([qr.ai](http://qr.ai)): це додаток для Android, який дозволяє створювати та сканувати QR-коди. Він має досить багато функцій, включаючи створення QR-кодів для різних типів інформації та можливість налаштування дизайну коду.

4) QR Code Studio ([apps.apple.com](http://apps.apple.com)): це додаток для iOS, який також дозволяє створювати QR-коди безпосередньо на вашому iPhone або iPad. Він має

інтуїтивний і простий інтерфейс та підтримує створення QR-кодів для URL, текстових повідомлень, контактних даних та іншого;

5) Google QR Code Generator: Google також має свій власний генератор QR-кодів. Ви можете створити QR-коди безпосередньо в результатах пошуку, використовуючи функцію "QR-код" у бічній панелі.

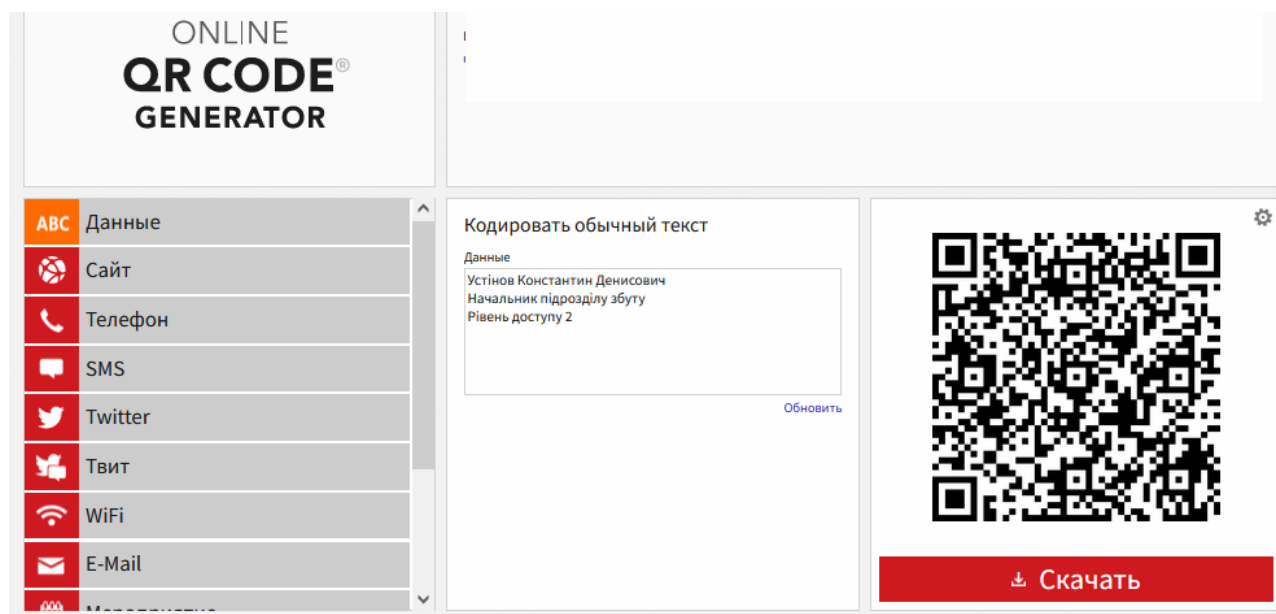


Рисунок 1.14. Створення QR-коду на основі безкоштовного он-лайн генератора

Ці програмні генератори QR-кодів різняться за можливостями та способами використання, але всі вони дозволяють створювати QR-коди для різних потреб, що варто вибрати залежно від вашого зручності та потреб.



Рисунок 1.15. Згенерований QR-код

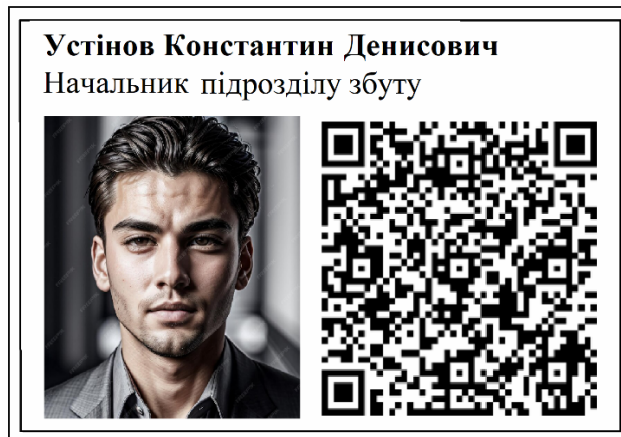


Рисунок 1.16. Бейдж співробітника підприємства з QR-кодом

На рис. 1.15 надано приклад створеного QR-коду. На рис. 1.16 показано приклад оформлення бейджу з використанням цього QR-коду.

Система керування доступом на основі QR-кодів – це система, яка використовує QR-коди для контролю та обмеження доступу до певних ресурсів або приміщень. Зазвичай така система використовується для забезпечення безпеки та контролю доступу в приміщеннях, таких як офіси, готелі, лабораторії, склади та інші обмежені зони.

Принцип роботи системи полягає в тому, що кожен користувач, який має право на доступ до певного ресурсу, отримує унікальний QR-код. Цей код може бути збережений на мобільному пристрої або надрукований на картці доступу. Код містить інформацію про користувача та його права доступу.

Для отримання доступу користувач просто сканує свій QR-код з допомогою спеціального сканера або камери смартфона. Система перевіряє інформацію, закодовану в QR-коді, з даними в своїй базі даних і приймає рішення про надання або відмову в доступі.

Однією з переваг використання системи керування доступом на основі QR-кодів є простота використання та управління. Немає потреби використовувати фізичні ключі або картки доступу, оскільки користувачі можуть мати свої QR-коди на мобільних пристроях, що робить процес більш зручним. Крім того, систему можна легко налаштувати для оновлення прав доступу або скасування QR-кодів у разі втрати або крадіжки.

## 2 ЕКОНОМІЧНИЙ РОЗДІЛ

### 2.1 Резюме

В даному дипломному проекті розроблена система керування доступом підприємства на основі перепусток з QR кодування. Для завдання досліджень було запропоновано використовувати платформу Arduino та програмні методи створення QR кодів.

Ефективність кожного програмного продукту визначається його якістю та ефективністю процесу розробки. Якість ПП визначається наступними складовими: з точки зору користувача; з позиції використання ресурсів; виконання вимог до програмного забезпечення.

Оцінка якості програмного продукту з точки зору користувача визначається необхідним на стадії функціонування розміром оперативної пам'яті ЕОТ, витратами машинного часу, пропускною спроможністю каналів передачі даних. Оцінка якості програмного продукту включає визначення трудомісткості і вартості його створення.

### 2.2 Визначення трудомісткості розробки програмного забезпечення

Тривалість розробки програмного продукту залежить від його обсягу, трудомісткості розробки, кваліфікації виконавців, а також планових термінів, визначених умовами ринку. Методом структурної аналогії по відповідних каталогах аналогів програмного забезпечення визначається обсяг програмних засобів, у тисячах умовних машинних команд програми аналога

У табл. 2.1 представлені аналоги програмного забезпечення, функції яких, у більшому або меншому ступені, виконує розроблений програмний продукт. Для нашого варіанта виділено сірим кольором.

					<b>КС 57. 09 000. 00 ДП ПЗ</b>	Арк.
						51
Зм.	Арк.	№ докум.	Підпис	Дата		

Таблиця 2.1. Каталог аналогів

Найменування ПЗ	Обсяг функції ПП = $V_0$ , ум. машинних команд
1. ПП СУБД	1300 – 8600
2. ПП введення інформації	1800 – 8800
3. ПП оптимізаційних розрахунків	13000 – 10200

Вибравши аналог ПП, що містить  $V_0$  в умовних машинних командах, трудомісткості визначати на основі табл.2.2.

Таблиця.2.2

Обсяг ПП, тис.умов.машинних команд	Норма часу, люд/год
1.00	229
2.00	244
3.00	262

На підставі отриманого значення, по довіднику, визначається укрупнена норма часу на розробку аналога програмного забезпечення (коректується поправочним коефіцієнтом враховуючої умови розробки ПП, тобто в умовах комп'ютера,  $K_k=0,7 \div 0,8$ ):  $T_{ар} = 244 \times 0,8 = 195.20$  (люд/годин).

Трудомісткість програмного продукту визначається по кожному етапу розробки окремо на підставі трудомісткості аналога з урахуванням складності розробки, ступеня новизни і ступеня використання в розробці стандартних модулів на підставі формул:

$$T_{T3} = T^a p \times L_1 \times K_H \quad (2.1)$$

$$T_{TII} = T^a p \times L_2 \times K_H \quad (2.2)$$

$$T_{PII} = T^a p \times L_3 \times K_H \times K_T \quad (2.3)$$

Для розрахунку необхідні наступні коефіцієнти:

$L_i$  – питома вага  $i$ -го етапу розробки (див. табл. 2.2.);

					<b>КС 57. 09 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		52

$K_n$  – поправочний коефіцієнт, що враховує ступінь новизни (див. табл. 2.3.);  $K_t$  – поправочний коефіцієнт, що враховує ступінь використання в розробці типових програм (див. табл. 2.4.).

Таблиця 2.2 – Значення питомих коефіцієнтів  
трудомісткості стадії в загальній трудомісткості розробки ПП

Код стадії	Ступінь новизни		
	А	Б	В
ТЗ ( $L_1$ )	0,15	0,12	0,12
ТП ( $L_2$ )	0,16	0,15	0,11
РП ( $L_3$ )	0,55	0,58	0,61

Для нашого варіанта виділено сірим кольором.

Таблиця 2.3. – Значення поправочного  
коефіцієнта, що враховує ступінь новизни

Код ступеня новизни	Ступінь новизни	Значення $K_n$
А	Принципово нові ПО	1,75 – 1,2
Б	ПО – розвиток визначеного параметричного ряду	1,0 – 0,8
В	ПО маючий аналог	0,7

Для нашого варіанта виділено сірим кольором.

Таблиця 2.4 – Значення коефіцієнта ступеня  
використання в розробці типових програм

Ступінь охоплення реалізованих функцій розроблювального ПО типовими програмами, %	Значення $K_t$
60 і вище	0,6
40-60	0,7
20-40	0,8
До 20	0,9

Для нашого варіанта виділено сірим кольором.

Тепер розраховуємо трудомісткість по кожному етапу окремо:

Трудомісткість технічного завдання

$$T_{ТЗ} = T_a * L_1 * K_H = 195,2 * 0,12 * 0,7 = 16,40 \text{ (люд/годин)}$$

Трудомісткість розробки технічного проекту

$$T_{ТП} = T_a * L_2 * K_H = 195,2 * 0,11 * 0,7 = 15,04 \text{ (люд/годин)}$$

Трудомісткість розробки робочого проекту

$$T_{РП} = T_a * L_3 * K_H * K_T = 195,2 * 0,61 * 0,7 * 0,7 = 58,35 \text{ (люд/годин)}$$

Для подальших розрахунків визначили кількість папера, витраченого на кожен етап: технічне завдання  $N_{ТЗ}=2$  (стр), розробка ТП  $N_{ТП}=15$ (стр), розробка робочого проекту  $N_{РП}=25$  (стр), пояснювальна записка відповідно  $N_{ПЗ}=50$  (стр)  
Розрахунок зведений у табл. 2.5.

Таблиця 2.5 – Розрахунок трудомісткості ПП

Найменування етапів	Розрахунок, годин.		
	2	3	4
1.ТЗ	$T_{РТЗ}=16,40$	$T_{КК}=0,7*N_{ТЗ}=0,7*2=1,4$	$T_{НК}=0,15*N_{ТЗ}=0,15*2=0,30$
2.Розробка ТП	$T_{РТП}=15,04$	$T_{КК}=0,7*N_{ТП}=0,7*15=10,50$	$T_{НК}=0,15*N_{ТП}=0,15*15=2,25$
3.Розробка РП	$T_{РРП}=58,35$	$T_{КК}=0,7*N_{РП}=0,7*25=17,5$	$T_{НК}=0,15*N_{РП}=0,15*25=3,75$
4.Розробка ПЗ	$T_{ПЗ}=1,5**N_{ПЗ}=1,5*50=75$	$T_{КК}=0,7*N_{ПЗ}=0,7*50=35$	$T_{НК}=0,15*N_{ПЗ}=0,15*50=7,5$
Усього, в т.ч.:	230,2		
- на розробку	$\Sigma T_p=152$		
- контроль керівника		$\Sigma T_{КК}=64,4$	
- нормоконтроль			$\Sigma T_{НК}=13,8$

## 2.3 Розрахунок ціни програмного продукту

У цьому розділі для визначення ціни розраховуємо основну заробітну плату виконавців, матеріальні витрати, вартість машино – години і витрати на розробку ПЗ. Розрахунок основної заробітної плати виконавців приведений у табл. 2.7. Відповідно до статті 8 «Закону про Державний бюджет України на 2024» встановлено мінімальну заробітну плату у місячному розмірі з 1 січня 2024 року - 6500 гривень; мінімальну погодинну тарифну ставку – 39.26 грн.

Таблиця 2.6. Розрахунок основної заробітної плати виконавців

Найменування робіт	Трудомісткість робіт, години	Погодинна тарифна ставка, грн.	Розрахунок, грн.
1.Розробка ПП	152	39.26	5958,15
2.Контроль керівника	65	38,50	2502,50
3.Нормоконт-роль	14	38,50	539,00
Усього	-	-	$\Sigma Z_0 = 8999,15$

Таблиця 2.7. Розрахунок матеріальних витрат на розробку ПЗ

Найменування матеріальних витрат	Тип, модель	Кількість	Ціна одиниці, грн.	Вартість, грн.
Папір	Лист А4	60	2.60	160,0
Разом	-	-	-	$B_{Mi} = 160,0$
Транспортно– заготівельні витрати (10%)				$B_{тр\_з} = 0,1 \times B_{M1} = 0,1 \times 160,0 = 16,0$
Усього				$B_M = B_{Mi} + B_{тр\_з} = 176,0$

					<b>КС 57. 09 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		55

На підставі отриманих даних по окремих статтях витрат складена калькуляція планової собівартості в цілому ПП за формою, приведеною в табл. 2.8.

Таблиця 2.8. Розрахунок статей витрат планової собівартості

Стаття витрат	Значення , грн.	Формула розрахунку
1. Матеріали	176,0	$V_m$ (див. табл. 2.7)
2. Основна заробітна плата	8999,15	$Z_o$ (див. табл. 2.6)
3. Додаткова заробітна плата	1349,87	$Z_d = 0,15 \times Z_o = 8999,15 \times 0,15$
4. Відрахування до єдиного фонду соціального внеску	2276,78	$V_{\text{с.в.}} = 0,22 \times (Z_o + Z_d) = 0,22 \times (8999,15 + 1349,87)$
5. Накладні витрати	2699,75	$V_{\text{нак.}} = 0,3 \times Z_o = 0,3 \times 8999,15$
6. Повна собівартість	15501,55	$C_{\text{пов.}} = V_m + Z_o + Z_d + V_{\text{с.в.}} + V_{\text{нак.}} = 176,0 + 8999,15 + 1349,87 + 2276,78 + 2699,75$

Розмір прибутку, що включається в ціну, визначаємо по наступній формулі:

$$П = (C_{\text{п}} * P) / 100 = (15501,55 * 10) / 100 = 1550,15 \text{ грн} \quad (2.4)$$

Де  $p$  – плановий рівень рентабельності (10-15%).

Оптова ціна (кошторисна вартість) визначається по формулі:

$$Ц_o = C_{\text{п}} + П = 15501,55 + 1550,15 = 17051,70 \text{ грн} \quad (2.5)$$

Податок на додану вартість визначаємо по наступній формулі:

$$ПДВ = 0,2 * Ц_o = 17051,70 * 0,2 = 3410,34 \text{ грн}; \quad (2.6)$$

Виходячи з отриманих даних, ціна реалізації розробленого програмного продукту на основі наступної формули, становитиме:

$$Ц_p = Ц_o + ПДВ = 17051,70 + 3410,34 = 20462,04 \text{ грн} \quad (2.7)$$

## 3 РОЗДІЛ ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ

**Вступ.** Безпечні умови праці – не тільки запорука комфортного існування працівників у межах підприємства, а в першу чергу – їх здоров'я та працездатності, а відтак і прибутковості підприємства. Безпека праці на підприємстві може бути на належному рівні тільки тоді, коли всебічно виконуються вимоги трудового законодавства, державних стандартів України, норм і правил, розроблених для збереження здоров'я працюючих.

В розділі охорона праці дипломного проекту розглядаються питання умов праці програміста (оператора ПК), які повинні бути забезпечені на підприємстві для безпечної роботи працівника при розробки «Системи контролю доступом підприємства на основі QR кодування».

### 3.1 Аналіз небезпечних і шкідливих факторів, що впливають на програміста при розробці програмного комплексу

Небезпечним називається фактор, вплив якого на працюючу людину в певних умовах може привести до виробничої травми або іншому раптовому різкому погіршенню здоров'я. Якщо ж виробничий чинник приведе до захворювання або зниження працездатності, то його вважають шкідливим. Залежно від рівня й тривалості впливу, шкідливий чинник може стати небезпечним.

В процесі роботи на користувачів ПК можуть мати вплив наступні небезпечні та шкідливі фактори:

- ✓ Невідповідність параметрів мікроклімату нормам;
- ✓ Недостатній рівень освітленості;
- ✓ Ураження електрострумом;
- ✓ Статична електрика;
- ✓ Порушення організації робочого місця тощо.

					<b>КС 57. 09 000. 00 ДП ПЗ</b>	<i>Арк.</i>
<i>Зм.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		<b>57</b>

## **3.2 Гігієнічні вимоги до виробничого середовища**

У відповідності з Правилами охорони праці під час експлуатації ЕОМ на робочому місці користувача ПК повинні бути створенні умови для високопродуктивної праці. Розглянемо ці умови.

### **3.2.1 Вимоги до приміщення**

Для приміщень, які призначені для роботи з ВДТ, доцільно обрати орієнтацію вікон на північ або на північний схід. На вікнах повинні бути жалюзі, що регулюються, або штори, що дають можливість їх повністю закривати. Приміщення відповідно до ДБН В.2.5-28-2018 «Природне і штучне освітлення» повинні мати природне та штучне освітлення. З приміщеннях ВДТ мають бути обладнані побутові приміщення для відпочинку, психологічного розвантаження тощо.

Площа на одне робоче місце для користувачів повинна складати не менше 6 кв.м, а об'єм – не менше 20,0 куб.м. Стіни пофарбовані матовою фарбою, у відповідності з санітарними вимогами.

### **3.2.2 Освітлення**

Для освітлення приміщення, у якому працює користувач ПК, використовується змішане освітлення, тобто сполучення природного й штучного освітлення. Для загального освітлення приміщення використовуються газорозрядні лампи типу ЛД. Норма для необхідної освітленості робочого місця становить 300-500 лк.

### **3.2.3 Шум**

При розумовій праці, яка вимагає зосередженості припустимий рівень шуму становить 50дБ. Для зменшення шуму й вібрації в приміщенні устаткування, апарати й прилади встановлюють на спеціальні прокладки, що амортизують. Якщо стіни в приміщенні є джерелами шумоутворення, вони повинні бути облицьовані звуковбирним матеріалом.

					<b>КС 57. 09 000. 00 ДП ПЗ</b>	<i>Арк.</i>
<i>Зм.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		<b>58</b>

### 3.2.4 Мікроклімат

Порушення відповідності ц параметрів мікроклімату впливають на працездатність працівників, їх реакцій, збільшення кількості помилок. Тому в приміщенні повинні бути установлені оптимальні параметри мікроклімату: температура повітря 22-25 °С, вологість повітря – 40-60%, швидкість пуху повітря – 0,1-0,2 м/с. Для цього приміщення має бути оснащено системами опалення й кондиціонування, що забезпечують постійне й рівномірне нагрівання, циркуляцію й очищення повітря від пилу й шкідливих речовин.

### 3.2.5 Електробезпека

Проходячи через організм людини електричний струм робить термічну, електролітичну і біологічну дію.

Для попередження поразок електричним струмом необхідно:

- У повному обсязі виконувати правила провадження робіт і правил технічної експлуатації;
- Виключати можливість доступу працівника до частин устаткування, що працює під небезпечною напругою, неізольованим частинам, призначеним для роботи при малій напрузі й не підключеним до захисного заземлення;
- Застосовувати ізоляцію, що служить для захисту від поразки електричним струмом.

Для попередження поразок електричним струмом необхідно:

- У повному обсязі виконувати правила провадження робіт і правил технічної експлуатації;
- Виключати можливість доступу працівника до частин устаткування, що працює під небезпечною напругою, неізольованим частинам, призначеним для роботи при малій напрузі й не підключеним до захисного заземлення;
- Застосовувати ізоляцію, що служить для захисту від поразки електричним струмом.

Заземлені конструкції, що знаходяться в приміщеннях, де розміщені робочі місця операторів ( батареї опалення, водопровідні труби, кабелі із заземленим

					<b>КС 57. 09 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		59

відкритим екраном) мають бути надійно захищені діелектричними щитками або сітками з метою недопущення потрапляння працівника під напругу.

### **3.2.6 Вимоги до організації робочого місця працівника**

Робочі місця повинні бути розташовані так, щоб у поле зору працюючого не попадали поверхні, що мають властивість віддзеркалювання, вікна освітлювальні прилади. Відеотермінали повинні встановлюватися під кутом 90-100 градусів від вікон, так, щоб світло падало з боку. Робочі місця з ВДТ доцільно розміщати в глибині приміщення. Розташування відео терміналу, при якому працюючий звернений обличчям або спиною до вікон, неприпустимо при будь-якому способі реалізації загального висвітлення, як прямим, так і відбитим світлом.

Робочий стіл повинен регулюватися по висоті в границях 680-800 мм, а ширина – забезпечувати можливість виконання операцій в зоні досяжності моторного поля. Рекомендовані розміри столу: висота 725 мм, ширина 600-1400 мм, глибина 800-1000 мм. Робочий стілець повинен бути оснащений підйомно-поворотним пристроєм для регулювання висоти сидіння і спинки, а також кута її нахилу. Регулювання кожного параметра повинне вироблятися легко, бути незалежним і надійно фіксуватися.

Розташування екрана ВДТ має забезпечувати зручність зорового спостереження у вертикальній площині під кутом  $+30^{\circ}$  до нормальної лінії погляду працюючого.

Клавіатуру слід розташовувати на поверхні столу на відстані 100...300 мм від краю, звернутого до працюючого.

Організація робочого місця користувача комп'ютера повинна забезпечувати відповідність усіх елементів робочого місця та їх взаємного розташування ергономічним вимогам (рис.3.1).

					<b>КС 57. 09 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		60

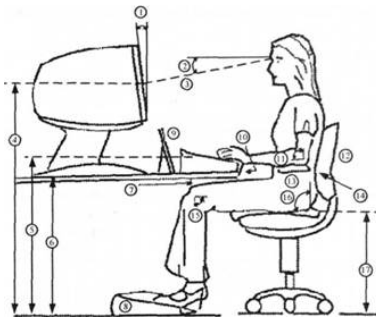


Рисунок 3.1. Робоче місце і робоча поза користувача комп'ютера:

1 — кут екрана; 2 — кут огляду (зору); 3 — відстань огляду; 4 — висота середини екрана; 5 — висота клавіатури; 6 — висота столу; 7 — відстань колін від столу; 8 — підставка для ніг; 9 — підставка для документів; 10 — положення рук; 11 — кут ліктів; 12 — спинка крісла; 13 — підлокітник; 14 — опора для попереку; 15 — кут колін; 16 — кут спинки крісла; 17 — висота сидіння

### 3.3 Пожежна безпека

Пожежна безпека приміщень, що мають електричні мережі, регламентується ГОСТ 12.1.033-81, ГОСТ 12.1.004-85. Робота оператора ЕОМ повинна вестися в приміщенні, що відповідає категорії Д пожежної безпеки (негорючі речовини й матеріали в холодному стані).

Пожежна безпека забезпечується:

- системою запобігання пожежі;
- системою протипожежного захисту;
- організаційно-технічними заходами.

Протипожежний захист приміщення забезпечується застосуванням установки автоматичної пожежної сигналізації, наявністю засобів пожежогасіння, організацією своєчасної евакуації людей.

Для ліквідації невеликих осередків пожеж, а також для гасіння пожеж у початковій стадії їх розвитку силами персоналу об'єктів, застосовуються первинні засоби пожежогасіння. Це вогнегасники (вуглекислотні та порошкові), пожежний інвентар (покривала з негорючого полотна, ящики з піском, бочки з водою), пожежний інвентар.



Рисунок 3.2. Первинні засоби пожежогасіння

					<b>КС 57. 09 000. 00 ДП ПЗ</b>	Арк.
						62
Зм.	Арк.	№ докум.	Підпис	Дата		

## ВИСНОВКИ

Результати досліджень дозволяють рекомендувати їх для оперативного створення систем керування підприємства. В роботі розроблена система керування доступом підприємства на основі перепусток з QR кодування. Для завдання досліджень було запропоновано використовувати платформу Arduino та програмні методи створення QR кодів.

Результати досліджень, виконаних в роботі дозволили встановити, що:

1) створення даної системи можливо на основі платформи ARDUINO, яка має усі необхідні пристрої: сканер QR кодів та штрих-кодів GM-45 та мікроконтролерів різних видів;

2) проведений порівняльний аналіз систем керування доступом на основі QR кодів та радіочастотного доступу RFID дало змогу виявити, що доступ на основі QR кодів простіше організувати та дешевше;

3) створення QR-коду можливо на основі безкоштовного он-лайн генератора QR-кодів;

4) застосування на бейджах фотографії співробітника з QR-кодом дозволяє не тільки візуальну ідентифікацію, але і за допомогою QR-код.

					<b>КС 57. 09 000. 00 ДП ПЗ</b>	<i>Арк.</i>
<i>Зм.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		<b>63</b>

# ПЕРЕЛІК ВИКОРИСТАНИХ ІНФОРМАЦІЙНИХ ДЖЕРЕЛ

1. Богуш В.М. Інформаційна безпека держави. Навчальний посібник / В.М. Богуш, О.К. Юдін // – К.: «МК-Прес», - 2005. – 432 с.

2. Шон Харрис CISSP Руководство для подготовки к экзамену / Шон Харрис // Пятая редакции, 2019. - 875 с.

3. Белов А.В. Управление модулем ARDUINO по Wi-Fi с мобильных устройств / А.В. Белов // Микроконтроллеры Arduino – М.: «Наука и Техника», - 2020. – 496 с.

4. [ресурс]. – Режим доступа: [http://arduino.ru/Arduino\\_environment](http://arduino.ru/Arduino_environment).

5. Getting Started with Arduino UNO. [Електроний ресурс]. – Режим доступа: <https://www.arduino.cc/en/Guide/ArduinoUno>.

6. Джеджула, В. В., and I. Ю. Єпіфанова. "Методичні підходи до побудови функцій належності нечітких математичних моделей." Modeling the development of the economic systems, 1: 42-46. (2021).

7. Beskorovainyi V., Berezovskyi H. Identification of preferences in decision support systems // Econtechmod. An International Quarterly Journal. 2017. Vol. 06, No. 4, P. 15–20.

8. Інтроепективний аналіз. Методи та засоби експертного оцінювання / В.В. Крючковський, Е.Г. Петров, Н.А. Соколова, В.Є. Ходаків. Херсон: Гринь ДС, 2018. 284 с. 27. Петров, К. Э., et al. "Компараторна ідентифікація моделі багатофакторного оцінювання альтернатив з використанням методу беггінга." Біоніка інтелекту 2.93 (2019): 21 с.

					<b>КС 57. 09 000. 00 ДП ПЗ</b>	Арк.
Зм.	Арк.	№ докум.	Підпис	Дата		64

# ДОДАТОК А. Слайди мультимедійної презентації

## *СИСТЕМИ КОНТРОЛЮ ДОСТУПОМ ПІДПРИЄМСТВА НА ОСНОВІ QR КОДУВАННЯ*

ДИПЛОМНИЙ ПРОЕКТ

Дипломник: Качановський А.А.  
Керівник: Кільдішев В.Й.

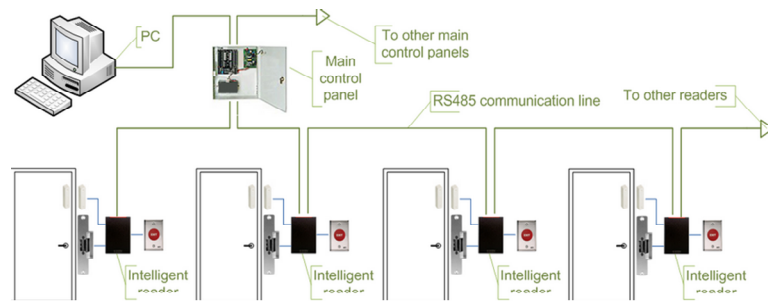
2024

---

Забезпечення безпеки в системі контролю доступом підприємства

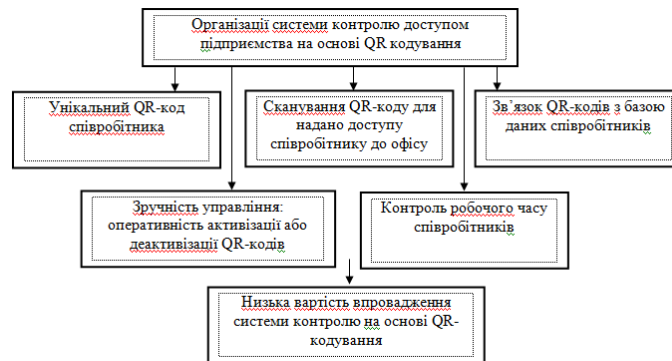


## Система контролю доступу приміщень офісу за допомогою інтелектуальних пристроїв зчитування



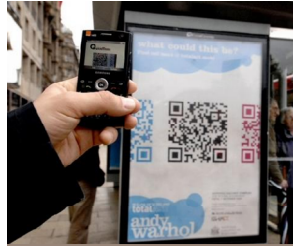
3

## Основні складові системи контролю доступу на основі QR-кодів

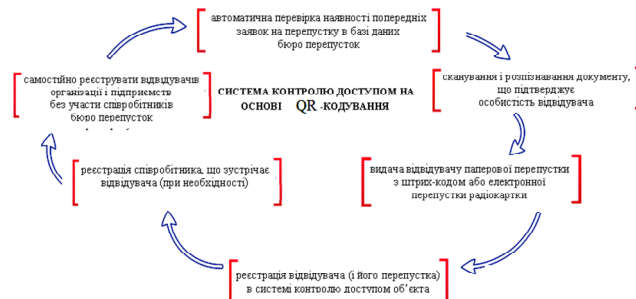


4

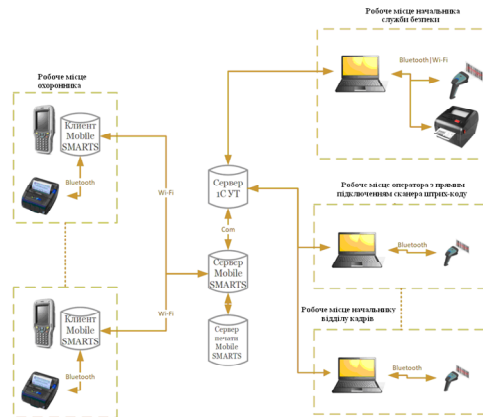
## Приклади генерація та використання унікальних QR-кодів



## Алгоритм роботи системи контролю доступом на основі QR-кодування

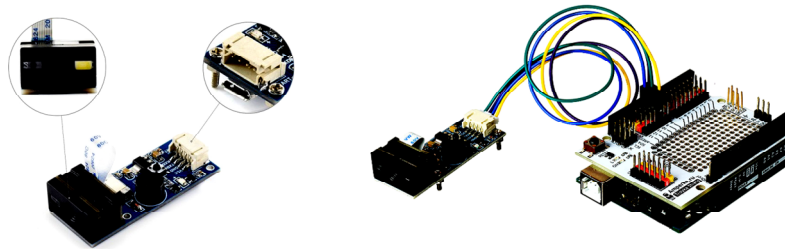


## Система управління доступом до офісу на основі перепусток з QR-кодом

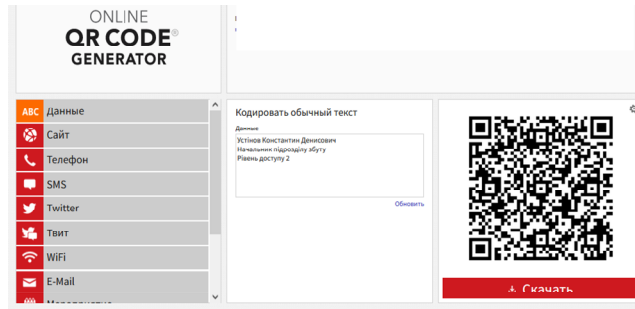


7

## Підключення сканер OR GM-45 до плати Arduino-Uno



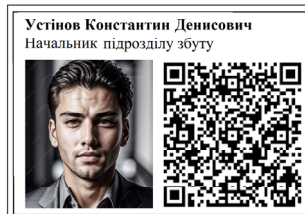
## Створення QR-коду на основі безкоштовного он-лайн генератора



9

---

## Бейдж співробітника підприємства з QR-кодом



10

---

**ДЯКУЮ ЗА УВАГУ!**



# ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

## ВІДГУК

керівника на дипломний проект здобувача освіти  
відділення комп'ютерних систем

Качановського Андрія Андрійовича  
(прізвище, ім'я та по батькові здобувача/здобувачки освіти)

Спеціальність 123 «Комп'ютерна інженерія»

Освітня програма «Обслуговування комп'ютерних систем і мереж»

Тема дипломного проекту: Системи контролю доступом підприємства на основі  
QR кодування»

### ХАРАКТЕРИСТИКА ДИПЛОМНОГО ПРОЕКТУ

а) обсяг і якість виконання проекту (графічного матеріалу і розрахунково-пояснювальної записки)

Пояснювальна записка виконана якісно, у достатньому обсязі, відповідно до індивідуального завдання та теми дипломного проекту, розділи пояснювальної записки відповідають етапам рішення завдання, поставленого у дипломному проекті

Презентація виконана якісно, у достатньому обсязі. Презентація наочно демонструє результати роботи.

б) самостійність роботи над проектом: \_\_\_\_\_

Студент самостійно обрав напрям та тематику кваліфікаційної роботи. Проведено аналіз аналіз внутрішнього і зовнішнього середовища підприємства . Представлено вимоги, обрано вибір СКД, проведені необхідні розрахунки. В рамках захисних заходів представлено організаційні заходи, план забезпечення діяльності, модель безпеки, тощо.

в) теоретична підготовка випускника \_\_\_\_\_  
відповідає вимогам, що надаються здобувачу освіти зі спеціальності  
«Комп'ютерна інженерія»

г) вміння розв'язувати виробничі та конструкторські питання \_\_\_\_\_

У дипломному проекті проведено аналіз оптимальних варіантів, а саме, проведено необхідні налаштування системи контролю доступом, досліджено ефективність функціонування усієї ланки СКД при провадженні. Для захисту інформаційного середовища застосовано QR кодування.

Оцінка розрахункової частини \_\_\_\_\_ 4 (добре)

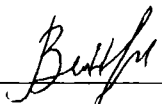
Оцінка графічної (презентаційної) частини \_\_\_\_\_ 4 (добре)

Загальна оцінка \_\_\_\_\_ 4 (добре)

Прізвище, ім'я, по батькові керівника роботи \_\_\_\_\_ Кільдішев Віталій Йосипович

Місце роботи і посада керівника роботи \_\_\_\_\_ к.т.н., доцент кафедри кібербезпеки та технічного захисту інформації ДУІТЗ

« 10 » \_\_\_\_\_ 06 2024 р.

  
(підпис)

Кільдішев В. І  
(прізвище та ініціали керівника)

# ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

## РЕЦЕНЗІЯ

на дипломний проект (роботу) студента  
відділення комп'ютерних систем

Качановського Андрія Андрійовича

(прізвище, ім'я та по батькові)

Напрямку підготовки 123 «Комп'ютерна інженерія»

Керівник кваліфікаційної роботи

Кільдішев Віталій Йосипович

(прізвище, ім'я та по батькові)

Тема кваліфікаційної роботи

«Системи контролю доступом підприємства на основі QR кодування»

Обсяг пояснювальної записки 70 сторінок

Обсяг графічної (презентаційної) частини проекту // аркушів (слайдів)

### ХАРАКТЕРИСТИКА КВАЛІФІКАЦІЙНОЇ РОБОТИ

а) заключення про ступінь відповідності виконаної роботи завданню

Робота відповідає технічному завданню до дипломного проекту. Виконана у відповідності з вимогами.

б) характеристика виконання кожного розділу роботи

При виконанні дипломного проекту студент продемонстрував уміння використовувати останні досягнення науки та техніки, уміння працювати з літературою. Так, студент грамотно дослідив та проаналізував системи контролю доступом підприємства.

в) оцінка якості виконання графічної (презентаційної) частини роботи і пояснювальної записки

Графічна частина відповідає вимогам, виконана якісно та відображає основні елементи проектування системи. Містить організація доступу на основі QR кодування. Досліджено генерацію унікальних QR-кодів для співробітників підприємства. Запропоновано системи контролю доступом працівників офісу на основі QR кодування.

г) перелік позитивних якостей роботи \_\_\_\_\_  
Тема дипломного проекту є актуальною, виконана у достатньому обсязі, якісно, відповідно до поставленого завдання.


д) основні недоліки роботи У тексті пояснювальної записки присутні помилки оформлення. Було б доцільним розглянути пристрої QR-кодування не тільки на основі платформи Arduino.

Оцінка розрахункової частини _____	Добре
Оцінка графічної (презентаційної) частини _____	Добре
Загальна оцінка _____	Добре

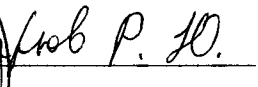
Прізвище, ім'я та по батькові рецензента \_\_\_\_\_ Царьов Роман Юрійович

Місце роботи і посада рецензента Державний університет інтелектуальних технологій і зв'язку, ст. викладач, зав. кафедри комп'ютерної інженерії та інформаційних систем

« 14 » серпня 2024 р.

  
(підпис)



  
та ініціали рецензента)

Ім'я користувача:  
Катерина Григоріївна Краснокутська

ID перевірки:  
1016324243

Дата перевірки:  
05.06.2024 16:59:54 EEST

Тип перевірки:  
Doc vs Internet + Library

Дата звіту:  
05.06.2024 17:05:38 EEST

ID користувача:  
100011688

Назва документа: 4КС-57\_Андрій\_Качановський

Кількість сторінок: 46 Кількість слів: 6845 Кількість символів: 49572 Розмір файлу: 6.26 MB ID файлу: 1016122923

## 3.62% Схожість

Найбільша схожість: 0.32% з Інтернет-джерелом (<http://dspace.onua.edu.ua/bitstream/handle/11300/6589/Negodchenk..>)

3.62% Джерела з Інтернету 258

Сторінка 48

Не знайдено джерел з Бібліотеки

## 0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

## 0% Вилучень

Немає вилучених джерел

**ДОЗВІЛ  
НА РОЗМІЩЕННЯ  
ВИПУСКНОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ  
(ДИПЛОМНОГО ПРОЕКТУ)  
В ЕЛЕКТРОННОМУ РЕПОЗИТАРІЇ ВСП «ОТФК ОНТУ»**

Ми, що нижче підписалися,

***Качановський Андрій Андрійович,***  
здобувач освіти гр. 4КС-57, та

***Кільдішев Віталій Йосипович,***  
керівник дипломного проекту,

не заперечуємо щодо розміщення електронного варіанту пояснювальної записки до дипломного проекту фахового молодшого бакалавра на тему:

***«Системи контролю доступом підприємства на основі QR кодування»  
(автор роботи – Качановський А.А., керівник роботи – Кільдішев В.Й.)***

виконаного у ВСП «Одеський технічний фаховий коледж Одеського національного технологічного університету» в 2024 році, у повному обсязі в електронному репозитарії ВСП «ОТФК ОНТУ» для вільного доступу через мережу Інтернет.

Несемо відповідальність за ідентичність електронного та друкованого варіантів випускної кваліфікаційної роботи і даємо згоду на обробку персональних даних.

Виконавець



/ Качановський А.А. /

Керівник



/ Кільдішев В.Й. /

«10» червня 2024 р.