Хмельницький національний університет
Факультет інформаційних технологій
Кафедра автоматизації, комп'ютерно-інтегрованих технологій та робототехніки

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Інфокомунікаційна система контролю та доступу
Назва теми

КвРТР.2019010.01.09

Галузь знань 17 «Електроніка та телекомунікації»
Шифр, назва

Спеціальність 172 «Телекомунікації та радіотехніка»
Шифр, назва

Освітня програма «Телекомунікації та інформаційно-комунікаційні технології»
Назва

Виконав:

студент IV курсу, група ТР1-19-1 _____ Максим ЛУГОВИЙ
Підпис Ім'я, ПРІЗВИЩЕ

Керівник _____ Андрій СЕЛЬСЬКИЙ
Підпис, дата Ім'я, ПРІЗВИЩЕ

Нормоконтролер _____ Людмила КОРЕЦЬКА
Підпис, дата Ім'я, ПРІЗВИЩЕ

До захисту допускаю:
зав. кафедри автоматизації,
комп'ютерно-інтегрованих
технологій та
робототехніки _____ Валерій МАРТИНЮК
Підпис, дата Ім'я, ПРІЗВИЩЕ

« 14 » червня 2023 р.

Хмельницький 2023

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет *інформаційних технологій*
Кафедра *кафедри автоматизації, комп'ютерно-інтегрованих технологій та робототехніки*
Освітній рівень *бакалавр*
Галузь знань *17 Електроніка та телекомунікації*
Спеціальність *172 Телекомунікації та радіотехніка*
Освітня програма *Телекомунікації та інформаційно-комунікаційні технології*

ЗАТВЕРДЖУЮ:
Завідувач кафедри АКІТтаР
_____Валерій МАРТИНЮК
01.02.2023р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ
Максим ЛУГОВИЙ
Прізвище, ім'я, по батькові студента

1. Тема роботи Інфокомунікаційна система контролю та доступу
2. Керівник роботи Сельський А.А., к.ф-м,н, доцент
Затверджено наказом ректора університету від 01.03.2023р. № 5
2. Строк подання студентом проекту на кафедру: 03.06.2023р.
3. Вихідні дані до проекту (роботи) Завдання на дипломне проектування
4. Зміст пояснювальної записки (перелік питань, які потрібно розробити) Вступ, Огляд методів розв'язання поставленої задачі, Розробка схемотехнічних рішень, Розробка алгоритму роботи програмного забезпечення, висновки
5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень) ___

Максим ЛУГОВИЙ
Ініціали, прізвище

Андрій СЕЛЬСЬКИЙ
Ініціали, прізвище

6. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Антиплагіат	Федула М.В., доцент кафедри АКІТтаР		
Нормоконтроль	Корецька Л.О., доцент кафедри АКІТтаР		

7. Дата видачі завдання 01.03.2023р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1 Вибір та затвердження теми кваліфікаційної роботи; розробка завдання на кваліфікаційну роботу; складання календарного графіка виконання кваліфікаційної роботи	01.03.2023	Виконано
2 Вивчення предметної області, в якій планується використання системи автоматизації; аналіз вимог до системи автоматизації	15.03.2023	Виконано
3 Проектування та розробка загальної архітектури і структури системи автоматизації, інтерфейсу користувача; вибір засобів реалізації системи автоматизації	29.03.2023	Виконано
4 Програмна реалізація та тестування системи автоматизації	12.04.2023	Виконано
5 Написання тексту пояснювальної записки та розробка графічних матеріалів	19.04.2023	Виконано
6 Остаточне коригування кваліфікаційної роботи з урахуванням зауважень керівника; оформлення кваліфікаційної роботи як документа відповідно до вимог	11.04.2023	Виконано
7 Отримання супровідних документів (відгуку керівника, рецензії, довідки про перевірку на плагіат); нормоконтроль	30.05.2023	Виконано
8 Підготовка до захисту та захист кваліфікаційної роботи	03.06.2023	Виконано

Студент _____ Максим ЛУГОВИЙ
Підпис Ініціали, прізвище

Керівник роботи _____ Андрій СЕЛЬСЬКИЙ
Підпис Ініціали, прізвище

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Інфокомунікаційна система контролю та доступу».

Автор роботи: Луговий Максим Русланович.

Керівник роботи: Сельський Андрій Анатолійович

Пояснювальна записка: 61 с., 12 рис., 3 табл., 5 дод., 45 джерел.

Графічна частина: 3 креслення.

ІНФОКОМУНІКАЦІЙНА СИСТЕМА, КОНТРОЛЬ ДОСТУПУ, МІКРОКОНТРОЛЕРНЕ КЕРУВАННЯ, БІОМЕТРИЧНІ СИСТЕМИ.

Метою роботи є розробка системи інфокомунікаційного контролю та доступу. Проведено аналіз комп'ютерних систем контролю та управління доступом. Обрано RFID метод ідентифікації користувача за його підписом. Програмну частину реалізовано з архітектурою клієнт/сервер. Розроблено базу даних та клієнт (Web-додаток) для оператора. Результатом розробки є архітектура розробленої системи, структура та схема електрична принципова пристрої контролю та управління доступом. Особливістю даної розробки є використання мікроконтролера SK-iMX53 як керуючий елемент пристрою контролю та керування доступом. Завдяки цьому пристрій володіє широкою функціональністю, а також, високим рівнем захисту даних, що передаються по мережі .

Підпис студента 

13.06.23
Дата

ЗМІСТ

ВСТУП

Впровадження заходів безпеки, запобігання витоку інформації та контроль продуктивності бізнес-персоналу є однією з найважливіших і важливих проблем для багатьох компаній сьогодні.

Традиційні методи ідентифікації особи на основі паролів або використання фізичних носіїв (наприклад, пропусків, паспортів, водійських прав) не завжди відповідають сучасним вимогам безпеки.

Проблему точної ідентифікації людей можна вирішити за допомогою систем радіочастотної ідентифікації.

Розвиток комп'ютерних технологій, поява нових матеріалів і математичних алгоритмів дозволили створити спеціалізовані ідентифікаційні пристрої – радіочастотні зчитувальні пристрої, які є основою систем ідентифікації RFID.

Ця технологія дозволяє отримувати інформацію по темі без прямого контакту. Залежно від використовуваної технології відстань, на якій можна зчитувати та записувати інформацію, може коливатися від кількох міліметрів до кількох метрів. Самі радіочастотні мітки також дуже різні - розміром з кредитну картку або дуже маленьку скляну мітку.

Радіочастотна ідентифікація має багато переваг перед іншими технологіями ідентифікації. Найбільшою перевагою радіочастотної ідентифікації є те, що відстань прийому та запису ідентифікаційної інформації може досягати десятків метрів.

У рамках зазначених завдань передбачається розробка інформаційно-комп'ютерної системи контролю та управління доступом до об'єктів охорони. Призначення цієї СКУД не настільки оригінальне в порівнянні з багатьма існуючими СКУД – не тільки забезпечити автоматичну фільтрацію відвідувачів за прапорцями – можна зайти/не можна, але й розрахувати час, який працівник проводить на своєму робочому місці. Автоматична фільтрація відвідувачів дозволяє контролювати обстановку, безпеку людей і збереження

матеріальних цінностей та інформації, а також порядок на об'єкті. Враховуйте час, проведений на робочому місці - для підвищення ефективності роботи персоналу компанії, оскільки з урахуванням цієї статистики можна ввести систему штрафів і пожертвувань. Якість виконання цього комплексу завдань залежить від типу СКУД, її можливостей і зручності використання самої системи. Комп'ютерна система повинна мати простий візуальний інтерфейс, зрозумілий будь-якому користувачеві.

1 АНАЛІЗ ІСНУЮЧИХ КОМП'ЮТЕРНИХ СИСТЕМ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ

Перш ніж розпочати аналіз існуючих комп'ютерних систем контролю та управління доступом (СКУД), необхідно дати визначення поняття СКУД. Відповідно до ДСТУ 51241-2008 “Засоби та системи контролю та управління доступом. Класифікація. Загальні вимоги. Методи випробувань”, СКУД – це сукупність засобів контролю та управління доступом, які мають технічну, інформаційну, програмну та експлуатаційну сумісність. [1-6]

Засоби управління (ЗУ) - апаратні засоби (пристрою) та програмні засоби, що забезпечують встановлення режимів доступу, прийом та обробку інформації з зчитувачів, проведення ідентифікації та аутентифікації, управління виконавчими та запобіжними пристроями, відображення та реєстрацію інформації.

Засоби контролю та управління доступом (засоби КУД) - механічні, електромеханічні пристрої та конструкції, електричні, електронні, електронні програмовані пристрої, програмні засоби, що забезпечують реалізацію контролю та управління доступом.

Пристрої, що перегороджують керовані (ППК) - у будови, що забезпечують фізичну перешкоду доступу та обладнані виконавчими пристроями для керування їх станом (турнікети, прохідні кабіни, двері та ворота, обладнані виконавчими пристроями СКУД).

Пристрій зчитуючий (ПЗ), зчитувач – це пристрій, призначений для зчитування (введення) ідентифікаційних ознак.

Пристрої виконавчі (ПВ) – це у будови або механізми, що забезпечують приведення у відкритий або закритий стан ППК (електромеханічні, електромагнітні замки, електромагнітні клямки, механізми приводу шлюзів, воріт, турнікетів та інші подібні пристрої).

Зчитувач - пристрій, призначений для зчитування (введення) ідентифікаційних ознак.

Іншим важливим поняттям СКУД є ідентифікатор користувача - унікальна характеристика суб'єкта або об'єкта доступу. Як ідентифікатори можна використовувати пам’ятні коди, біометричні чи фізичні коди. Ідентифікатор за допомогою фізичного коду – це об’єкт, в який (на) за допомогою спеціальної технології (картка, електронний ключ, брелок тощо) внесено ідентифікаційну ознаку у вигляді закодованої інформації.

1.1 Загальні принципи роботи систем контролю та керування доступом

Системи контролю доступу бувають різних модифікацій: найпростіші розраховані тільки на одні вхідні двері, а найскладніші призначені для контролю доступу на великі об'єкти (підприємства, заводи, банки). Між тим, найпростішим варіантом СКУД є звичайна рація. Незалежно від конфігурації СКУД, кожна така система складається з кількох обов'язкових вузлів, які є контролерами для управління, зчитувачами для ідентифікації та різними примусовими пристроями для обмеження доступу: турнікетами, електромагнітними замками та засувками. Електронні безконтактні картки як перепустки є найпоширенішою та зручною формою ідентифікації в системах контролю доступу.

Система контролю та управління доступом працює наступним чином: на перевантажувальному підприємстві на вході до відповідальних приміщень встановлюються пристрої контролю доступу: електромеханічні турнікети, електромеханічні або електромагнітні замки, зчитувачі безконтактних карт. Всі ці пристрої підключаються до контролера системи контролю доступу. Контролер призначений для отримання та аналізу інформації про карти контролю доступу, а також для управління різними виконавчими пристроями. Обладнання системи контролю доступу може включати два типи контролерів: контролери замків і контролери воріт, кожен з яких відповідає за контроль роботи власних вузлів. Кожному працівнику підприємства видається персональний ідентифікатор, зазвичай це безконтактна картка доступу –

пластикова картка (проксіміті-картка) з унікальним електронним кодом. Але можна використовувати магнітні картки або так звані пристрої сенсорної пам'яті. Цей ідентифікатор є і паспортом через організацію, і ключем від приміщень, які дозволено відвідувати співробітникам. Щоб пройти через ворота або зайти в відповідальне місце, працівники підприємства повинні показати картку контролю доступу картрідеру, а картрідер передасть пароль від пред'явленої картки контролеру, а контролер доступу вирішить, чи дозволити або відмовити в пропуску відповідно до інформації, що зберігається в ньому. Якщо доступ дозволений, система контролю доступу автоматично розблокує турнікет або дверний замок. Так, наприклад, контролер СКУД можна запрограмувати таким чином, щоб певні співробітники могли входити в певні кімнати лише в певні проміжки часу (наприклад, з 9 ранку до 6 вечора). До контролера СКУД можна підключити охоронну сигналізацію, включаючи датчики безпеки. Усі події, що проходять через пункти контролю, фіксуються в пам'яті системи контролю доступу та можуть бути використані для автоматичного підрахунку робочого часу, а також для отримання протоколів трудової дисципліни чи можливих офіційних розслідувань з боку бізнесу. За допомогою СКУД також можна контролювати в'їзд автотранспорту на територію суб'єкта, в такому випадку після пред'явлення ідентифікатора відкриваються двері або піднімаються шлагбауми. [7-15]

1.2 Основні можливості системи контролю та управління доступом

Нижче ми перерахуємо основні можливості, які відкриває установка СКУД на об'єктах, що охороняються:

1) Контроль і управління доступом є основними функціями системи. Як було сказано раніше, завдяки цій функції можна розділити доступ співробітників до певних кімнат і навіть заборонити доступ тим, кому він не потрібен. Крім того, можна дистанційно керувати блокуючими пристроями

(замками, турнікетами тощо). СКУД дозволяє заборонити прохід працівникам у святкові та вихідні дні, а також після робочого дня.

2) Збирати та надавати статистичні дані. СКУД збирає інформацію про людей, які проходять через певні точки контролю доступу. Для кожного працівника доступна наступна інформація: час входу та виходу, спроби проникнути в заборонені йому місця та зони, спроби проходу в невизначений час. Також є можливість відстежувати переміщення співробітників в межах зони, вказуючи, де і коли. Таким чином, усі виявлені порушення трудової дисципліни можуть бути внесені до особової справи працівника та повідомлено керівництво порушника у трудовому наказі. Крім того, за інформацією про останню точку проходу СКУД може в будь-який момент визначити місцезнаходження співробітника.

3) Співробітники можуть отримати доступ лише через персональний ідентифікатор. При проходженні з ідентифікаційною карткою вся інформація та фотографії співробітників можуть відображатися на екрані моніторингу на контрольно-пропускному пункті, а ідентифікаційні картки інших осіб не можуть використовуватися для пропуску. Крім того, на рівні правил реагування СКУД можна запобігти передачі ідентифікатора іншій особі та запобігти повторному входу на територію суб'єкта за тією ж карткою доступу.

4) Облік годин. Слідкуйте за тим, коли ви прибуваєте та коли виходите, за допомогою вбудованої системи обліку часу. Таким чином, можна визначити загальний час перебування працівника на робочому місці з урахуванням обідніх перерв. А на початку дня, наприклад о 9:30, вбудована система обліку робочого часу може створити груповий звіт про співробітників, які не пройшли через порт в'їзду. Це дозволяє вам ідентифікувати співробітників на вашому робочому місці, які запізнюються або не з'являються для виконання масових замовлень. Подібний звіт можна отримати в кінці робочого дня при виході з території підприємства або офісу.

5) Автономність роботи системи. СКУД обладнана системою безперебійного живлення, яка може працювати без перебоїв у разі

відключення електроенергії в будівлі. Крім того, завдяки функціональності контролера система контролю доступу здатна продовжувати роботу, наприклад, у разі збою комп’ютера.

6) Захист об'єктів в режимі реального часу. СКДУ може встановити певні місця як захищені та зняти з них захист. Крім того, ви можете отримувати інформацію в режимі реального часу про різні аварійні та тривожні ситуації за допомогою спеціальних сповіщень від відповідальної особи. Крім того, всі тривожні події та події реєструються в базі даних системи, що дає можливість отримати доступ до цієї інформації в майбутньому, коли це буде необхідно. Завдяки методам, доступним в СКУД, охоронець може не тільки контролювати двері та турнікети, а й за допомогою комп’ютера подавати сигналізацію зі свого робочого місця. План будівлі з картою розташування контролерів контролю доступу можна ввести в комп'ютер СКУД персоналу охорони.

7) Керування системою дистанційно через Інтернет або мобільний телефон. Якщо під час інсталяції підключити СКУД до Інтернету, адміністратори отримають можливість дистанційно керувати системою. Так само, як і можливість управління з мобільного телефону, хоча це більше підходить для систем контролю доступу GSM.

8) Інтеграція СКУД з іншими системами безпеки. Система контролю та управління доступом ідеально поєднується та інтегрується з іншими системами безпеки: системами відеоспостереження, охоронної та пожежної сигналізації. Так, наприклад, контроль доступу разом з відеоспостереженням забезпечує абсолютний контроль над приміщенням, що охороняється. У екстрених випадках така система дозволила б виявити та зупинити порушників у найкоротші терміни.

Інтегруючи СКУД і охоронну сигналізацію, можна налаштувати спільну реакцію системи на несанкціоноване проникнення в конкретне приміщення. Наприклад, ви можете ввімкнути сирени на охоронних пунктах, світлові сигнали або навіть замкнути всі двері в потрібних частинах будівлі.

Інтеграція СКУД з системою пожежної сигналізації дозволяє автоматично відмикати двері, турнікети та проходи у разі пожежі. Ці заходи значно полегшили евакуацію людей у важкі часи. [8, 16, 18]

1.3 Огляд комп'ютерних систем контролю та керування доступом

Зараз існує велика кількість систем СКУД. Аналіз існуючих комп'ютерних систем допоможе виявити їх сильні та слабкі сторони.

СКУД на основі розпізнавання геометрії рук і пальців

Ці методи ідентифікації особистості добре відомі. Розпізнавання руки існує вже 20 років. Щоб ідентифікувати особу, системі достатньо виміряти фізичні характеристики пальців або руки, такі як довжина, ширина, товщина та площа поверхні руки. Цікавою особливістю цієї методики є невеликий розмір вибірки (кілька байтів) біометричних даних, необхідних для ідентифікації. Розпізнавання руки довело свої переваги у великій кількості застосувань.

Майже все про людину можна прочитати по її руці. Однак у біометрії для цілей ідентифікації (або автентифікації) лише проста геометрія руки — розмір і форма — і деякі інформативні орієнтири на тильній стороні руки (зображення складок між кістками пальців, модель).

У біометрії існує два основних підходи до визначення геометрії руки:

1) Перший існує вже понад 25 років - від народження біометричних систем контролю доступу до місць, які повністю базуються на геометричних особливостях руки. Такі системи економічні з точки зору компактності зображення. У найпростішому варіанті зберігається лише інформація про довжину та ширину пальця, що вимагає лише 9 байт. Звичайно, для системи, яка враховує лише довжину та ширину пальця, легко зробити картонний манекен примітивної руки. Ще більш складною є система вимірювання контурів кисті, включаючи об'єм кисті, нерівності пальців, долоні, розміщення шкірних складок у складках.

На рисунку 1.1 зображено контрольні (ознакові) точки контуру руки та 17 початкових геометричних ознак руки, позначені в даному випадку прямими відрізками, що не містяться в контурі руки. Як бачимо, вихідною біометрією руки є ширина долоні, радіус вписаного кола долоні, довжина пальців (визначається як відстань від обраної верхньої контрольної точки до середини долоні). і лінія, що з'єднує нижні контрольні точки), ширина пальців і висота кисті в трьох точках, представлених лініями a, b і c. [17-19]

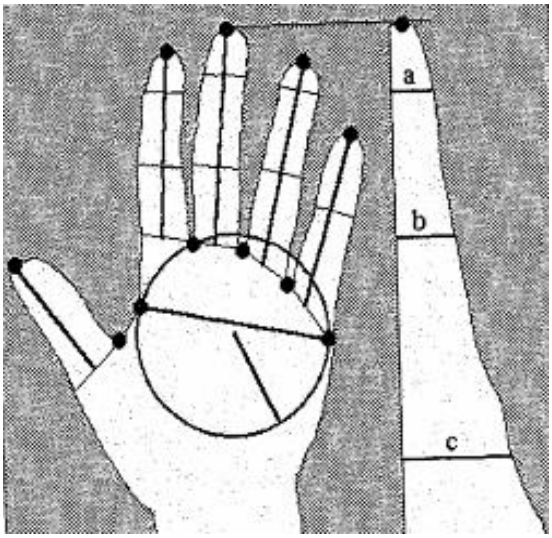


Рисунок 1.1 – Контрольні (характеристичні) точки силуету руки

2) Другий (більш сучасний) заснований на суміші геометричних і образних ознак. До останніх відносять зображення складок між фалангами пальців, малюнок (розташування) кровоносних судин під шкірою. Чотири ознаки беруться з руки, три з яких є скалярними і пов'язані з розміром пальців.

Перші три характеристики: ширина вказівного пальця 1, висота вказівного пальця 2, довжина середнього пальця 3, оцінені, як показано на рисунку 1.2. У цьому випадку риса 4 – це зображення шкірної складки в складці між середньою та нижньою фалангами вказівного пальця. Вся інформація про роздачу в системному класі може бути записана не більше ніж у 9 байтах.

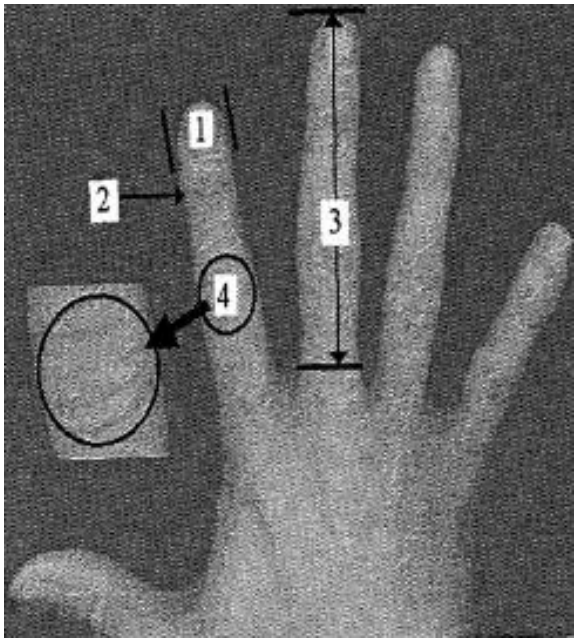


Рисунок 1.2 – Геометричні та образові характеристики силуету руки

Наприклад, розглянемо зчитувач HandKey. Сучасні біометричні системи від компанії Recognition Systems призначені для ідентифікації осіб, які потрапляють на територію охоронюваних об'єктів. На відміну від традиційних систем контролю доступу, які використовують різні електронні картки, в біометричній системі за технологією HandKey ідентифікатором є рука співробітника. Біометричні пристрої HandKey ідентифікують людей за розміром і формою руки, забезпечуючи високий рівень безпеки завдяки унікальній структурі кожної людської руки.

Метод розпізнавання HandKey 3D полягає в порівнянні контуру руки людини з попередньо отриманим шаблоном за розміром долоні, довжиною, шириною і товщиною пальців і багатьма іншими параметрами. Початковий запис шаблону геометрії руки був досягнутий шляхом тричі сканування руки співробітника та усереднення отриманої інформації.

Щоб біометрична система зчитувала дані, людині необхідно покласти долоню на панель пристрою, а спеціальні фіксуючі штифти допомагають регулювати її положення. Вбудовані світлодіоди на панелі зчитувача вказують правильне положення долоні, що полегшує взаємодію людини з комп'ютером.

Процедура перевірки рук виконується за допомогою інфрачервоного підсвічування та реєстрації даних зі спеціальної ПЗС-камери. Також пристрій отримує інформацію про товщину і розмір руки завдяки бічним дзеркалам, які потрапляють в поле зору телекамери. Відскановані зображення біологічних індикаторів за допомогою спеціальних алгоритмів перетворюються в цифрову інформацію (розмір шаблону 9 байт), а потім дані порівнюються з шаблоном, що зберігається в пам'яті. На підставі збігу отриманої інформації з шаблоном біометрична система приймає відповідне рішення.

Система HandKey виконує процес ідентифікації особи у два взаємопов’язані етапи: унікальний ідентифікаційний код із 1-10 цифр і пряме сканування руки на панелі зчитувача. У порівнянні з традиційними системами контролю доступу, які використовують різні зчитувачі електронних карт, біометричним системам потрібно лише запам’ятати код. Другий етап ідентифікації полягає у скануванні руки користувача та повному виключенні несанкціонованого доступу до охоронюваного приміщення за чужою або викраденою карткою доступу.

При цьому біометрична система контролю доступу (створена на базі біометричного зчитувача HandKey II) пропонує можливість підключення зчитувача контролю доступу, що дозволяє використовувати безконтактні картки, карти виходу та інші електронні картки без введення унікального Ідентифікатор. Клавіатура читача. Часто зчитувачі контролю доступу підключаються до біометричних зчитувачів, щоб оптимізувати час ідентифікації - великий трафік і немає необхідності витрачати час на набір ідентифікаційних номерів перед процедурами перевірки рук.

Двохетапна процедура ідентифікації користувача, яка, з одного боку, значно підвищує рівень безпеки, а з іншого – дозволяє практично миттєво верифікуватися з бази даних. Тобто людина вводить свій особистий код на системній клавіатурі (або, як альтернатива, використовує картку доступу), перш ніж аутентифікуватися формою руки, заздалегідь «повідомляючи» біометричному зчитувача, який шаблон для порівняння даних. Таким чином,

перевірка за формою руки займає не більше 1 секунди, а загальний час розпізнавання в системі з урахуванням використання кодових груп або електронних карт становить 1-5 секунд.

Переваги методів розпізнавання на основі геометрії руки та пальця:

– «ключ» завжди біля користувача;

– немає вимог до чистоти, вологості і температури;

Недоліки цього методу:

– великогабаритне обладнання (за деякими винятками);

– Виготовлення муляжів для пристроїв першого типу менш складне (з використанням тільки геометричних елементів).

СКУД на основі RFID-карти

Основним елементом пристрою безконтактної ідентифікації є спеціально організована пам'ять, що складається з електронного пристрою, виконаного у вигляді пластикової ідентифікаційної картки або іншої конструкції. Збільшення обсягу пам'яті на мітці, поділ цієї пам'яті на окремі сектори перетворює її на багатофункціональну (інформаційну) картку (ІК).

Функція ID-картки дає можливість створити єдиний багатофункціональний електронний документ для кожного об’єкта. Залежно від характеру об'єкта можна виділити два основних типи інформаційних карток:

– інфографіка нерухомості (тварини, машини тощо);

– особиста інформаційна картка, зазвичай виготовляється у вигляді стандартної пластикової картки.

Сучасний електронний рівень дозволяє створити багатофункціональний документ, який буде супроводжувати всі процеси життєдіяльності людини та дозволяє автоматизувати всі операції з його ведення.

У випадку безконтактної RFID зчитування інформації з ідентифікатора, розміщеного на об’єкті, відбувається без фізичного, електричного чи оптичного контакту. Відстань між ідентифікатором і зчитувальним пристроєм не перевищує вказану відстань (зазвичай кілька сантиметрів, десятків

сантиметрів або метрів), і між ними можуть бути будь-які неметалеві перешкоди, такі як стіна, ящик, конвеєрна стрічка, а стіни кімнати. [20-26]

Для впровадження безконтактної RFID потрібні три компоненти:

– відповідач (відповідач-ідентифікатор), розміщений на об'єкті, що ідентифікується;

– зчитувач інформації з ідентифікатора (за наявності також записує інформацію з транспондера);

– одержувачем інформації є додаток, комп'ютерна система обробки даних або оператор.

Зазвичай зчитувач складається з радіочастотного модуля (передавача і приймача), блоку управління з мікропроцесором і пам'яттю, елемента зв'язку з транспондером. Крім того, багато зчитувачів оснащені додатковими інтерфейсами (RS 232, RS 485), щоб мати можливість передавати отримані дані в іншу систему (ПК, система обробки даних).

Транспондер фактично є носієм даних системи RFID, зазвичай включає приймач для передавальної схеми, антену та блок пам'яті для зберігання інформації. Приймач, передавальна схема і пам'ять конструктивно виконані у вигляді окремих інтегральних схем. Іноді до складу RFID-мітки входить автономне джерело живлення. Коли транспондер, який зазвичай не має власного джерела напруги, не знаходиться в зоні опитування зчитувача, він повністю пасивний. Він активується лише тоді, коли транспондер знаходиться в зоні опитування зчитувача. Енергія, необхідна для активації транспондера, подається на транспондер безконтактно через блок зв'язку разом з імпульсами синхронізації та даними.

Процес радіочастотної ідентифікації здійснюється наступним чином:

– передавач зчитувача безперервно (або в заданий час) передає через антену пакети радіосигналу прийнятої системою частоти;

– транспондер, розташований у радіусі дії зчитувача, приймає цей радіосигнал через свою антену та використовує його енергію для живлення (це пасивний характер ідентифікатора – йому не потрібне джерело живлення).

Транспондер зчитує код зі свого пристрою (пам'яті) і імітує йому відповідний радіосигнал;

– зчитувач отримує відповідний сигнал, витягує код, що міститься в ньому, виконує (якщо передбачено) операції криптографічного захисту та процедури запобігання конфліктам (працюючи послідовно з декількома ідентифікаторами одночасно в діапазоні зчитувача) і передає інформацію за призначенням: додаток, дані система обробки або оператор.

Частота електромагнітного випромінювання та зворотного сигналу, що передається транспондером, суттєво впливають на робочі характеристики системи RFID, особливо на значення діапазону інформації, яка зчитується з радіочастотної мітки.

Робоча частота системи RFID визначає діапазон її застосування. Низькочастотні системи RFID прийнятні для малих відстаней між об’єктом і зчитувальним пристроєм. Типова відстань зчитування становить 0,5 метра, а відстань зчитування мікроміток зазвичай менша - близько 0,1 метра. Низька частота використовується більшістю систем контролю доступу, систем управління складами та виробництвом.

Системи RFID з проміжними значеннями робочої частоти використовуються там, де необхідно передати великі обсяги даних, наприклад, в системах контролю доступу, в смарт-картах.

Високочастотні системи RFID використовуються там, де потрібні великі відстані та висока швидкість зчитування, наприклад, під час керування залізничними транспортними засобами, контейнерами, автомобілями та системами збору відходів. Великий радіус дії дозволяє безпечно встановити зчитувач у недоступному для людей місці.

За допомогою систем RFID успішно вирішується багато складних організаційних і технічних завдань. [26]

Однак RFID також має недоліки:

– дані мають бути захищені, щоб теги не були перезаписані випадково (авторизованими зчитувачами) або навмисно (зчитувачами, якими користуються шахраї);

– час, потрібний для належної передачі всіх бітів даних до зчитувача з тегом із великим об’ємом пам’яті, може бути у багато разів довшим, ніж просто унікальний ідентифікатор.

В даний час дві найвідоміші у світі технології, які використовуються як ідентифікатори людського ока, є найнадійнішими.

Перший заснований на розпізнаванні образів райдужної оболонки ока. Другий метод використовує сканування очного дна – сітківки ока – на основі унікального кутового розподілу кровоносних судин у кожної людини.

При ідентифікації райдужних оболонок для встановлення індивідуальних ознак використовуються індивідуальні відмінності складних узорів райдужних оболонок людини. Розпізнавання райдужної оболонки ока є найточнішим із усіх систем біометричного розпізнавання. Рівень помилкової ідентифікації настільки низький, що ймовірність помилкової ідентифікації однієї людини за іншу майже дорівнює нулю. Райдужна оболонка та сітківка показані на рисунку 1.3.

Розглянемо, як ідентифікується райдужка. Першим кроком, звичайно, є отримання досліджуваних зображень. Це робиться за допомогою різних камер. Крім того, варто зазначити, що більшість сучасних систем надають не одне зображення, а кілька зображень для ідентифікації. Другий етап - підбір зображень райдужки. Сьогодні розроблено багато методів для точного отримання меж райдужної оболонки за описаними характеристиками.

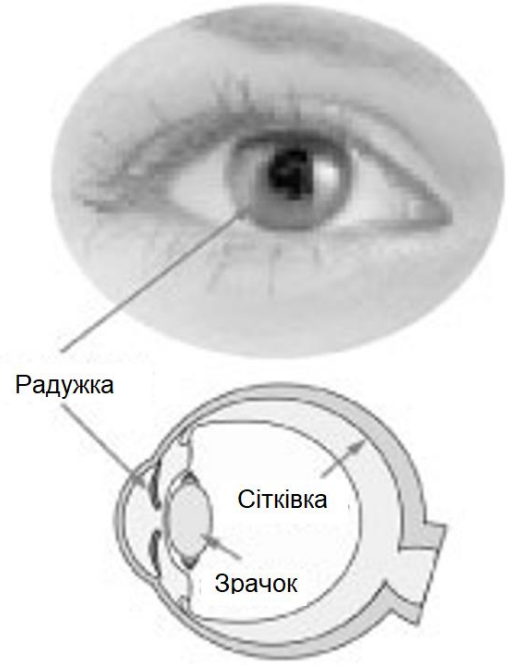


Рисунок 1.3 – Райдужка та сітківка ока

Наступним етапом розпізнавання є зміна розміру зображення райдужної оболонки до еталонного розміру. Наступним кроком є перетворення отриманого зображення райдужної оболонки ока в полярні координати. П’ятий крок у процесі ідентифікації особистості – вибір елементів райдужної оболонки ока, які можна використовувати для біометричної ідентифікації. Це найважчий етап. Нарешті, завершальним етапом ідентифікації людини за райдужною оболонкою ока є порівняння отриманих параметрів із зразками. І ця операція має одну відмінність від багатьох інших подібних завдань.

Судинна мережа сітківки кожної людини також унікальна. Він не обумовлений генетично, тому він відрізняється навіть у близнюків. При цьому він стабільний протягом усього життя людини, що робить його надзвичайно зручним ідентифікатором. У терміналі спеціальні камери з електромеханічними датчиками використовуються для ідентифікації сітківки, фіксуючи її відбивні та поглинальні властивості на відстані. Потужність світловипромінювача невелика, що виключає будь-який негативний вплив на людину і не викликає дискомфорту. Перед розпізнаванням клієнт вводить свій

PIN-код і дивиться в спеціальний окуляр. Імовірність помилки типу 2 (відмовостійкість) становить FAR = 1 на мільйон (у всіх випадках).

З точки зору зручності самого процесу, технологія розпізнавання райдужної оболонки ока має суттєву перевагу перед сітківкою, оскільки не потрібно дивитися в окуляр на відстань 3 см, достатньо підійти близько. Приблизно 25 см від зчитувача.

Слід зазначити деякі психологічні моменти - в цілому люди спокійно ставляться до процедури сканування сітківки ока, хоча з медичної точки зору вона нешкідлива. [27-36]

1.4 Порівняльна характеристика методів ідентифікації

Технологія RFID вже зайняла місце на ринку систем безпеки завдяки своїм перевагам. Потрібна пряма видимість радіочастотних тегів із високою швидкістю зчитування тегів, фактично велика кількість тегів може читатися одночасно.

Розглянемо характеристики кожної системи: стійкість до підробок, стійкість до навколишнього середовища, простота використання, вартість, швидкість, довгострокова стабільність (табл. 1.2). Давайте введемо шкалу від 1 до 10 у кожному стовпчику. Чим ближче оцінка до 10, тим краща система в цьому.

Таблиця 1.1 - Оцінка систем ідентифікації

	Стійк. до підробки	Стійк. до навколишнього середовища	Стоїмо.	Швидкість.	Стабільність визна. в часі
Конфіг. долоні	5	6	3	6	5
Райдужна оболонка/сітківка	7/5	9/10	1/5	7/3	6 / 6
Rfid - карта	5	8	1 0	10	8

Відповідно до вимог опису технічного завдання в якості ідентифікації інформаційно-комп'ютерних систем управління найбільш прийнятною є радіочастотна карткова ідентифікація. Власне, ключовими характеристиками, які зупиняються внаслідок вибору цього методу ідентифікації, є:

1) Вартість такої системи відносно невисока

2) Другий фактор – не потрібно щоразу передавати ID-картку картрідеру, достатньо підійти до картрідера на відстані 1-2 метри, і картрідер зчитає картку.

1.5 Висновки до першого розділу

В розділі проаналізовано методи побудови систем контролю управління доступом. Розглянуті системи що базуються на аналізі руки людини, сітківки ока. Показано переваги та недоліки таких систем.

Встановлено, що найбільш ефективним і надійним методом є використання RFID міток. Така система найбільш ефективна і надійна.

2 РОЗРОБКА ІНФОРМАЦІЙНО-КОМП'ЮТЕРНОЇ СИСТЕМИ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ

Системи контролю та управління доступом призначені для захисту об'єктів, що охороняються, від несанкціонованого доступу.

СКУД може бути як набором автономних елементів, призначених для вирішення простих завдань безпеки, так і складною системою, що відповідає певним вимогам.

У процесі проектування СКУД необхідно:

– визначити тип розв’язуваної задачі;

– обрати склад елементів системи для вирішення поставленої задачі найбільш ефективним способом;

– підібрати спеціальне програмне забезпечення для розрахунку робочого часу та централізовано керувати системою за допомогою АРМ;

– визначити місце установки обладнання згідно характеристик об'єкта та умов технічного завдання;

– для підвищення ефективності СКУД її можна комбінувати з системами відеоспостереження, а також охоронно-пожежною сигналізацією.

2.1 Розробка архітектури СКУД

Перед початком розробки системи СКУД необхідно ознайомитися з архітектурною класифікацією таких систем і прийняти правильне рішення щодо вибору архітектури, виходячи з вимог системи.

Автономна система управління (рисунок 2.1) передбачає установку одного або кількох незалежних контролерів на об’єкті, причому кожен контролер виконує функції контролю та управління доступом у певній локалізованій зоні. Така СКУД не має центрального контролера - сервера системи. У цій конфігурації кожен контролер має бути налаштований окремо. Враховуючи, що контролери часто встановлюють у важкодоступних місцях

(наприклад, за підвісними стелями), а також враховуючи ймовірну кількість дверей і співробітників на підприємстві, зрозуміло, що такий підхід підходить лише для невеликих приміщень.

Рисунок 2.1 - Структура автономної СКУД

На відміну від автономної, мережева СКУД (рис. 2.2) містить центральний контролер — сервер системи, до якого підключені всі локальні контролери. Тому для побудови мережевої СКУД необхідно прокласти кабельні лінії для забезпечення інформаційного зв'язку між контролерами. Однак при спілкуванні за допомогою контролера мережевого інтерфейсу Ethernet для цих цілей можна використовувати наявну на об’єкті комп’ютерну мережу.

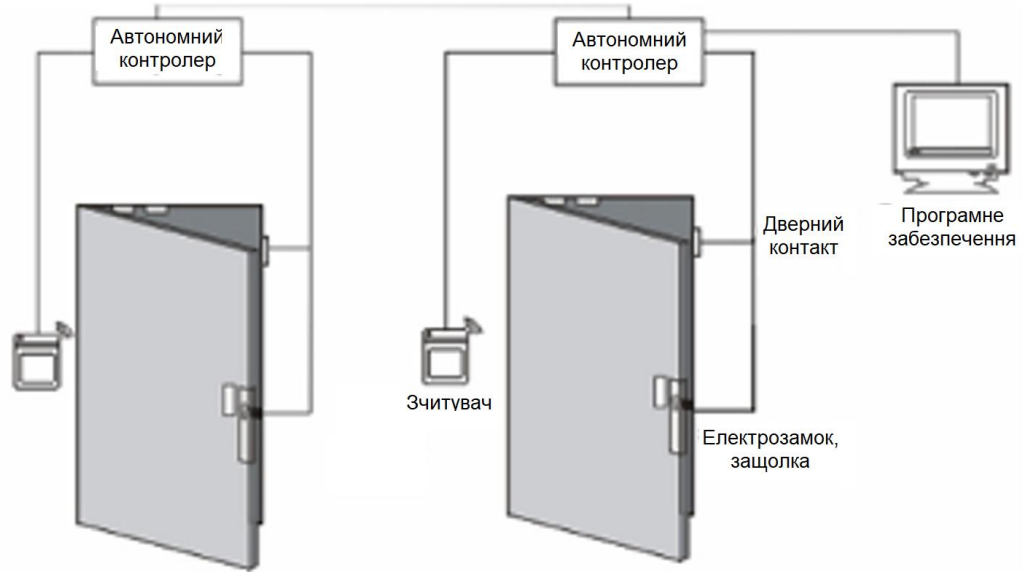


Рисунок 2.2 - Структура мережевий СКУД

Оскільки система, що розробляється, повинна контролювати максимум 100 комірок відповідно до вимог, описаних у технічному завданні, рекомендується застосовувати мережеву архітектуру, побудовану СКУД.

Архітектура комп'ютерної системи, що контролює та управляє доступом до об'єктів, що охороняються.

Розробка архітектури є невід'ємною частиною етапу розробки системи. Розроблена система обслуговує велику кількість користувачів, оскільки згідно з технічним завданням максимальна кількість користувачів СКУД, що розробляється, 100 осіб, а кількість ППК – 20, то СКУД, що розробляється, є середньою, тобто. десятки точок доступу та десятки до сотень користувачів (підприємства, готелі тощо).

Усі дані для СКУД, що розробляється (всі дані, які проходять через базу даних – час, дата, ім'я користувача та місцезнаходження) повинні зберігатися в одному місці, в одній базі даних. Підсумовуючи, можна зробити невтішний висновок, що найбільш підходящою архітектурою для розробки систем буде архітектура клієнт-сервер (рис. 2.3).

Рисунок 2.3 - Архітектура клієнт-сервер

Клієнт-серверна архітектура – це архітектура розподіленої обчислювальної системи, в якій програми поділяються на клієнтські процеси та серверні процеси.

Серцем системи, побудованої на архітектурі клієнт-сервер, є сервер бази даних, програма, яка виконує набір дій з керування даними — виконання запитів, зберігання та резервне копіювання даних, відстеження цілісності посилань, перевірка прав і привілеїв користувачів тощо. на., звичайний персональний комп'ютер можна використовувати як робоче місце, не відмовляючись від звичайного робочого середовища.

На основі аналізу існуючих рішень розроблено власну архітектуру комп’ютеризованої системи контролю та управління доступом, яка складається з двох частин програмної та апаратної підсистем.

З вимог, описаних у технічному завданні, в якості ідентифікатора було вирішено використовувати RFID-ідентифікацію, оскільки вартість побудови системи на основі цього методу значно нижча, ніж при використанні будь-якого іншого методу ідентифікації. Крім того, ідентифікація RFID відносно знайома людям. [37-40]

Загальну архітектуру інформаційно-комп’ютерної системи контролю та управління доступом до об’єктів охорони наведено на рисунку 2.4.

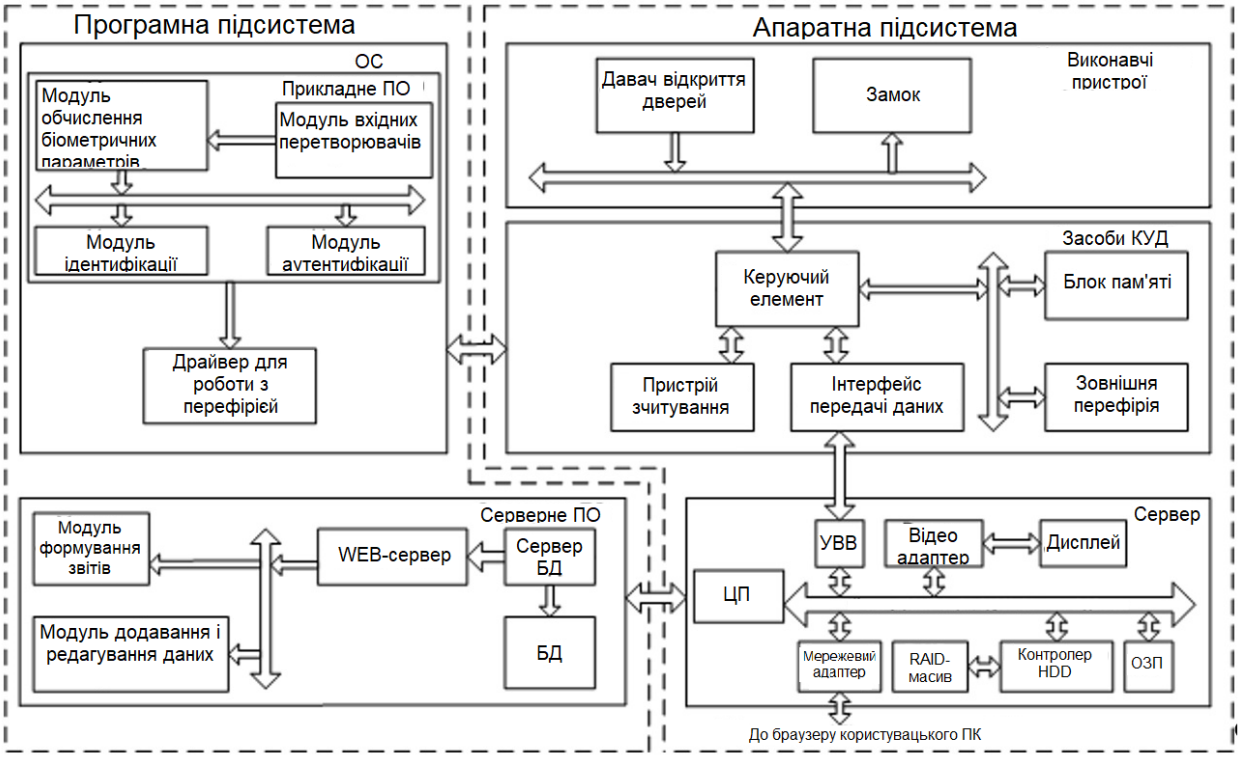


Рисунок 2.4 — Архітектура комп'ютерної системи контролю та управління доступом до об'єктів, що охороняються

Програмна підсистема складається з серверної частини, яка безпосередньо відповідає за контроль і управління доступом, і операційної системи Linux.

Серверна частина складається з веб-сервера та сервера бази даних.

Частина, яка відповідає за контроль і управління доступом, представлена як «товстий» клієнт. «Жирні» клієнти здійснюють ідентифікацію та аутентифікацію користувачів.

Апаратна підсистема складається з серверного обладнання, засобів контролю та управління доступом, виконавчого обладнання.

Серверна частина програмної підсистеми працює на серверному обладнанні.

Компонентами СКУД є: пристрій зчитування (для зчитування ідентифікаторів RFID), блоки пам'яті та периферійні пристрої (для ядра системи пам'яті). Для прийому та обробки інформації необхідний елемент

управління. Для надсилання/отримання даних із сервера потрібен інтерфейс передачі даних, у нашому випадку передбачається Ethernet.

Як виконавчі пристрої, в системі, що розробляється, передбачається використовувати замки і датчики відкриття дверей.

2.1 Виділення основних елементів СКУД

Апаратна підсистема СКУД включає:

– ПЗ (використовується для зчитування ідентифікатора та передачі відповідної інформації контролеру);

– контролер (обробляє інформацію, отриману від зчитувачів, приймає рішення про надання або заборону доступу, передає інформацію на сервери системи);

– сервер (збирає всю інформацію, що проходить через ВПС – час, дату, ПІБ користувача та посаду);

– комп’ютер з програмним забезпеченням (для забезпечення моніторингу, централізованого управління системою, реєстрації подій, звітності);

– охоронне обладнання (в нашому випадку - замки, що забезпечують блокування дверей і проходів);

– блок живлення (живлення пристроїв системи від мережі та автономного живлення);

– інше обладнання (кнопка виходу забезпечує розблокування виконавчого обладнання при виході з контрольованої зони; доводчик забезпечує зачинення дверей).

Оскільки веб-сервер буде розташований на сервері на додаток до сервера бази даних, необхідно враховувати, що для його ефективного функціонування машина повинна мати значну кількість системних ресурсів. Тобто сервер, на якому працює система, повинен мати потужну апаратну

платформу. Ця вимога стосується, зокрема, обсягу оперативної пам'яті та частоти процесора.

Дані будуть зберігатися в базі даних. Через значні наслідки втрати цих даних сервер повинен мати апаратну резервну копію бази даних у формі копії бази даних.

Елемент керування

Апаратне керування повинно забезпечувати отримання інформації від зчитувача, обробку та формування керуючих сигналів на пристрої виконання.

Як керуючий елемент в системі, що розробляється, слід використовувати мікроконтролер.

Мікроконтролер повинен забезпечувати:

– обмін інформацією по лініях зв'язку між диспетчером і засобами централізованого управління;

– зберігати дані в системній пам'яті на випадок відключення лінії зв'язку, відключення живлення та перемикання на резервне живлення в режимі централізованого керування;

– лінії зв'язку між контролером керування та пристроєм централізованого керування.

Протокол обміну інформацією повинен забезпечувати необхідний імунітет, швидкість обміну інформацією та (за необхідності) стійкість до підробки (властивість, яка характеризує стійкість до атак з боку порушників, метою яких є нав’язування неправдивої інформації, заміна переданих повідомлень або збереження даних про зміни). захист інформації (для розширених і високостабільних систем).

Мікроконтролер повинен мати входи для підключення кнопки запиту на вихід, контакту відкритого корпусу, контакту розділення стінки. Мікроконтролер СКУД також може мати вхід для підключення шлейфу охоронної сигналізації.

Мікроконтролер повинен мати вихід для підключення до схеми керування виконавчого пристрою, вихід керування для світлової індикації

стану доступу в кожному напрямку, вихід керування для світлової та звукової індикації стану тривоги.

На основі розробленої системи дані радіочастотного зчитувача інформації будуть передаватися на сервер через Ethernet, необхідний захист переданих даних, а також вирішення проблем, які можуть виникнути при проходженні інформаційних пакетів через різні шлюзи та маршрутизатори, розділяє підмережі. Вирішенням вищезазначених проблем є організація VPN-з'єднання (Virtual Private Network) за протоколом SSL (Secure Sockets Layer) між контролером мережі та сервером системи. VPN у поєднанні з SSL наразі вважається найбезпечнішим методом передачі даних в Інтернеті.

Звичайно, для цього необхідна реалізація VPN в програмному забезпеченні контролера, для чого більш вигідним виглядає варіант з вбудованою ОС.

Щоб використовувати ОС, вам знадобиться мікроконтролер, оперативна пам'ять і статична пам'ять — достатньо для роботи ОС. Але не варто також забувати, що інструментарій QT необхідний для створення автономної підсистеми СКУД там, де підходи централізованого управління не працюють. Подібним чином QT також має створити демон-процес для опитування порту, щоб забезпечити зв'язок між зчитувачем і сервером системи.

Враховуючи перераховані вище особливості, спробуємо підібрати оптимальну операційну систему та пристрій. Для підтримки QT нам потрібна операційна система Linux з версією ядра не нижче 2.6.32. або Windows Embedded Compact 7.

Запустіть Linux із ядром версії 2.6.32 або новішої. Windows Embedded Compact 7 вимагає 512 МБ оперативної пам'яті та 256 МБ місця на жорсткому диску.

Для ефективного запуску графіки Windows Embedded Compact 7 вам потрібні: Процесор із частотою 1 ГГц.

Виходячи з вищесказаного, основними вимогами до мікроконтролера будуть:

– частота щонайменше 1ГГц;

– можливість підключення оперативної пам'яті об'ємом <512Мб;

– підтримка завантаження операційної системи із Flash пам'яті;

– NAND-flash пам'яті та CompactFlash;

– пристрій зчитування.

Зчитувальний пристрій повинен забезпечувати:

– зчитування ідентифікаційної ознаки;

– перетворення введеної інформації на електричний сигнал;

– передачу інформації на контролер СКУД.

Зчитувальні пристрої повинні бути захищені від маніпуляцій шляхом класифікації та вибору ідентифікаційних ознак. Блок керування не повинен спричиняти розмикання UPU у разі поломки або від’єднання, розриву чи короткого замикання. [40-46]

Оскільки RFID-карта обрана як ідентифікатор у EMS, що розробляється, зчитувальним пристроєм має бути RFID-сканер.

Основні вимоги до читача:

– передача даних через USB, RS-232;

– діапазон частот 13,56 МГц.

Аналіз і вибір технології читання

Одним з основних елементів системи контролю та управління доступом до об'єкта охорони є пристрій зчитування. Виберіть RFID Reader як систему.

Зчитувачі можуть мати різну конструкцію - від простих портативних сканерів до фіксованих тунельних пристроїв, які сканують інформацію, коли вона надходить у сканер. Зчитувач активує мітку, після чого інформація, що зберігається на мітці, передається на зчитувальний пристрій.

Антена випромінює електромагнітні хвилі, які активують мітку RFID і дозволяють записувати та зчитувати дані з цієї мітки. Антена - це канал між міткою і приймачем, який контролює весь процес прийому і передачі даних. Антени відрізняються за розміром і формою. Їх можна вбудовувати спеціальними сканерами, а також ворота, турнікети, дверні прорізи тощо.

Отримуйте інформацію від об'єктів або людей, які проходять у радіусі дії антени. Конструктивно антена і приймач з дешифратором можуть розташовуватися в одному корпусі. Сигнали з антен демодулюються, декодуються і передаються через стандартні комп'ютерні інтерфейси для подальшої обробки.

Класифікація типів частот RFID виглядає так:

- низькі частоти (НЧ);
- високі частоти (ВЧ);
- ультрависокі частоти (УВЧ);
- мікрохвильові частоти.

У наступних розділах буде розглянуто всі типи частот.

Контролер - це пристрій, який перетворює вихідний сигнал (аналоговий або цифровий) у форму, придатну для подальшої обробки.

Інтерфейс являє собою вузол контролера, що складається з роз'ємів, з'єднувальних кабелів і драйверів (наприклад, конвертер між сигналами TTL і RS-232). Він призначений для передачі інформації від контролера до основного керуючого вузла системи, наприклад, до комп'ютера. Здебільшого сканери оснащені RS-232, RS-485, а останнім часом і USB.

RFID-мітка — це пристрій, який зберігає дані та безконтактно передає їх на сканер за допомогою радіохвиль.

Мітки RFID можна класифікувати двома різними способами. Список нижче показує перший спосіб класифікації тегів на основі того, чи мають вони вбудовану потужність і/або здатність підтримувати спеціалізовані завдання: пасивні, активні.

Пасивні мітки

Цей тип RFID-тегів не містить вбудованого джерела живлення (наприклад, батареї), натомість сканер використовує енергію від зчитувача для живлення та передачі даних. Пасивні теги прості за конструкцією і не містять рухомих частин. Тому така етикетка має тривалий термін служби і в цілому дуже добре витримує суворі умови навколишнього середовища. Наприклад,

деякі пасивні мітки стійкі до агресивних хімічних речовин, таких як кислоти, і високих температур понад 200°C. Коли обмін інформацією відбувається в напрямку від тега до зчитувача, зчитувач спочатку ініціює зв'язок, а потім обмін здійснюється тегом. Для передачі таких тегів наявність зчитувача обов'язкова.

Пасивні теги зазвичай менші за активні або напівактивні. Значення відстані зчитування в ньому можуть варіюватися - від менше 2,5 см до приблизно 9 м.

Пасивні теги також зазвичай коштують дешевше, ніж активні або напівактивні теги.

Безконтактні смарт-карти — це особливий тип пасивних RFID-міток, які сьогодні використовуються в різних сферах (наприклад, як ідентифікаційні маркери в системах безпеки). Дані, що зберігаються на цій картці, зчитуються біля зчитувача. Для зчитування картці не потрібен фізичний контакт із зчитувальним пристроєм.

Пасивні теги складаються з таких основних компонентів: мікрочіп, антена.

На рисунку 2.5 показані компоненти пасивної мітки

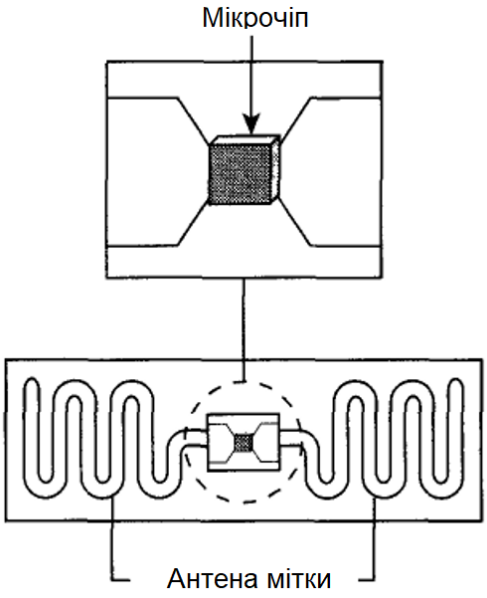


Рисунок 2.5 – Компоненти пасивної мітки

На рисунку 2.6 показано компоненти мікрочіпа. Якщо пам'ять сегментована (тобто складається з кількох блоків або полів). Адресність означає здатність адресувати (тобто читати чи записувати інформацію) до різних областей пам’яті мікрочіпа. Блок пам’яті може містити різні типи даних, наприклад ідентифікаційні дані, які визначають частину об’єкта, біти контрольної суми (наприклад, циклічний надлишковий код – CRC) для перевірки точності даних, що передаються, тощо. Останні технологічні досягнення дозволили створювати мікрочіпи розміром з піщинку. Але фізичний розмір мітки визначається не розміром мікрочіпа, а розташуванням і розміром його антени.

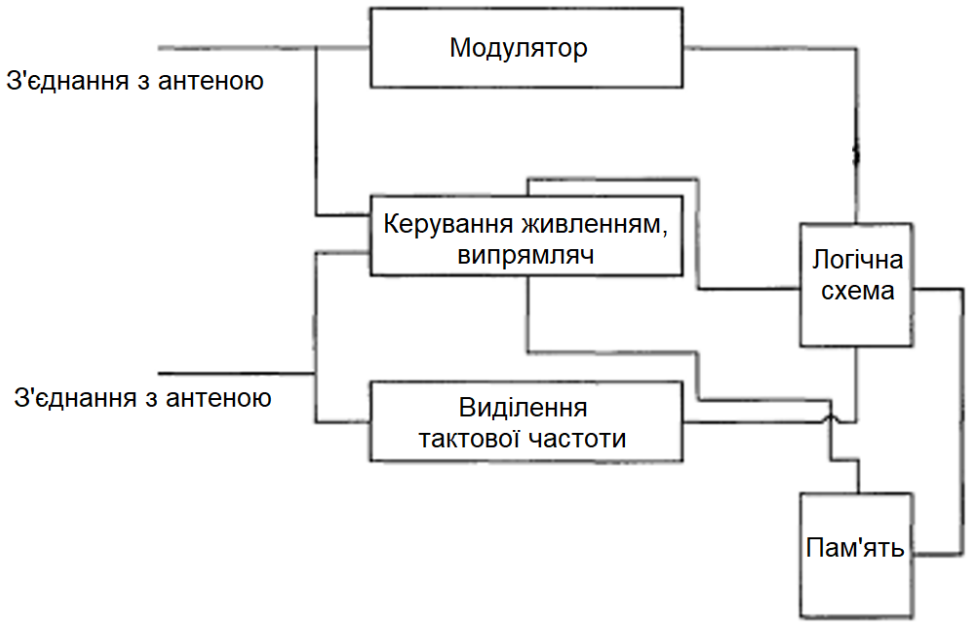


Рисунок 2.6 – Основні компоненти мікрочіпа

Антена мітки використовується для отримання енергії, яка живить мітку, сигнал зчитувача, а також для отримання та передачі даних між міткою та зчитувальним пристроєм. Ця антена фізично підключена до мікрочіпа. Можлива незліченна кількість конструкцій антен, особливо для діапазону UHF, і їх конструювання є і мистецтвом, і наукою. Довжина антени прямо пропорційна робочій довжині хвилі мітки. Дипольна антена складається з прямого відрізка провідника, наприклад мідного, із зазором посередині.

Загальна довжина дипольної антени, яка оптимально передає енергію сигналу, отриманого від антени зчитувача, дорівнює половині довжини хвилі використовуваної частоти. Подвійна дипольна антена складається з двох диполів, що значно знижує чутливість мітки до орієнтації. У результаті читачі можуть читати такі теги з різних кутів. Кільцевий диполь складається з двох або більше прямих провідників, з'єднаних паралельно, причому кожен провідник має половину довжини хвилі (використовуваної частоти). Якщо він складається з двох провідників, ви отримаєте 2-провідний контурний диполь, 3-провідний контурний диполь складається з трьох паралельно з'єднаних провідників.

Активні мітки

Активні RFID-мітки мають внутрішнє джерело живлення (наприклад, хімічну батарею; але можливі й інші джерела живлення, наприклад сонячні елементи) та електроніку для виконання спеціальних завдань. Активні теги використовують власне внутрішнє джерело живлення для передачі даних тегів на зчитувач. Передача даних не потребує енергії від зчитувача. Вбудована електроніка може містити мікропроцесори, датчики та порти введення/виведення, які отримують живлення від внутрішнього джерела живлення. Так, наприклад, такі компоненти можуть вимірювати температуру навколишнього середовища та генерувати інформацію про середню температуру, а також інформацію, яка використовується для визначення інших параметрів – наприклад, терміну придатності продуктів, до складу яких вони входять. Потім тег може передавати цю інформацію (разом зі своїм унікальним ідентифікатором) зчитувача. Активний тег можна розглядати як комп'ютер із бездротовим з'єднанням, який має додаткові властивості (наприклад, характеристики датчика або набору датчиків).

Вкладка активності складається з таких компонентів:

– мікрочіп. Розмір і можливості мікропроцесорів зазвичай перевищують аналогічні параметри мікрочіпів з пасивними мітками;

– антена. Він може мати форму радіочастотного модуля, який передає сигнал мітки і приймає відповідний сигнал від пристрою зчитування;

– внутрішній блок живлення;

– внутрішня електроніка.

На рисунку 2.7 показано приклад активної вкладки.

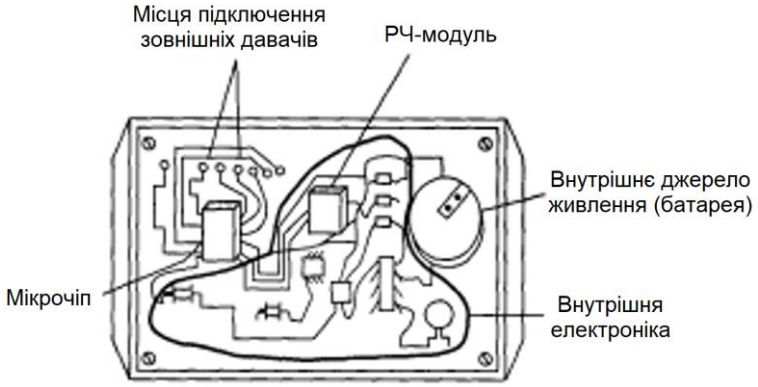


Рисунок 2.7 – Приклад активної мітки

Теги класифікуються за підтримкою можливостей перезапису даних:

– тільки для читання (Тільки для читання - RO);

– з записом раз і читанням багато (написати один раз прочитати багато - WORM);

– з багаторазовим перезаписом (читання-запис - RW);

– табличка типу SAW;

– як активні, так і пасивні теги доступні в типах RO, WORM і RW;

– мітка типу RO;

– тег RO можна запрограмувати (тобто записати) лише один раз протягом його життя.

Дані постійно вводяться в тег у заводських умовах лише на етапі його виготовлення. Для цього окремі плавкі вставки пропалюються через мікрочіп етикетки за допомогою тонкого лазерного променя. Після цього дані не можуть бути перезаписані протягом життя тегу.

Цей тип мітки також відомий як тег із заводським програмуванням. Виробник етикетки вносить дані в етикетку, а користувач етикетки взагалі не може на це вплинути.

Мітка R W Тип

Теги типу RW можна перепрограмувати (перезаписувати) багато разів. Зазвичай це число коливається від 10 000 до 100 000 разів, а то й більше! Ця можливість перезапису пропонує величезну перевагу, оскільки дані можуть бути перезаписані зчитувачем або тегом (у разі активного тегу).

Теги типу RW зазвичай містять запам'ятовуючі пристрої типу флеш або EEPROM.

Теги RW також відомі як робочі програмовані теги або теги, що перепрограмуються.

Для тегів можна вирішити завдання - гарантувати безпеку зберігання інформації.

Цей вид етикетки має хорошу економічну ефективність і прийнятну безпеку даних, і є найпоширенішим типом етикетки.

Табличка типу SAW

Мітка типу SAW, принцип дії – поверхнева акустична хвиля (surface acoustic wave – SAW).

Мітки типу SAW принципово відрізняються від міток на основі мікрочіпа. Теги SAW вже почали з’являтися на ринку і можуть широко використовуватися в майбутньому. В даний час пристрої SAW широко використовуються в мобільних телефонах, кольорових телевізорах та інших галузях.

Теги типу SAW використовують малопотужні радіохвилі в діапазоні частот 2,45 ГГц.

На відміну від мікрочіп-міток, SAW-мітки не потребують джерела постійного струму для живлення під час передачі даних.

Мітки SAW складаються з дипольної антени, з’єднаної з міжштирьовим перетворювачем (IDT) на п’єзоелектричній підкладці з ніобату літію або

танталату літію. Індивідуальні електроди розташовані в точно розрахованих місцях на підкладці, діють як відбивачі та виготовляються з алюмінію або використовуються на підкладці. Після отримання радіочастотного сигналу від зчитувача SAW антена випромінює електричний імпульс IDT. Цей імпульс генерує поверхневі хвилі, також відомі як хвилі Релея, які проходять крізь підкладку зазвичай зі швидкістю 3000–4000 м/с. Деякі з цих хвиль відбиваються назад до IDT відбивачем, а решта поглинаються підкладкою. Відбиті хвилі утворюють унікальну структуру, яка визначається положенням рефлектора і представляє задану позначку. Ці хвилі перетворюються назад на радіосигнали IDT і передаються назад на зчитувач RFID через антену мітки. Потім зчитувач декодує отриманий сигнал і витягує дані тегу.

Теги SAW мають такі переваги:

Енергоспоживання дуже низьке, оскільки для живлення не потрібне джерело постійного струму.

За допомогою нього ви можете позначати рентгеноконтрастні та радіопоглинаючі матеріали, такі як метал і вода, окремо з хорошими результатами.

Відстань зчитування більша порівняно з мітками з мікрочіпами, що працюють у тому ж діапазоні частот (тобто 2,45 ГГц).

На відміну від міток для мікрочіпів, для яких потрібен довший сигнал від зчитувача до мітки, можна використовувати коротші сплески радіосигналу.

Висока точність читання.

Проста конструкція та велика міцність.

Немає необхідності використовувати протокол запобігання зіткненням.

Протоколи запобігання зіткненням потрібно впроваджувати лише на рівні зчитувача, на відміну від міток мікрочіпів, які потребують таких протоколів як на рівні зчитувача, так і на рівні міток (це зменшує вартість міток SAW).

Зчитувачі SAW менш чутливі до перешкод від інших зчитувачів SAW.

Теги SAW, ймовірно, будуть єдиним варіантом у деяких ситуаціях маркування та можуть стати більш поширеними в майбутньому.

Вибір технології передачі даних

Технологія передачі визначає потенційну відстань між контролером і комп'ютером і навіть складність і вартість встановлення мережевого СКУД. Необхідно зосередитися насамперед на методах стандартизації. На даний момент існує кілька можливих варіантів, а саме:

Розглянемо мережу протоколу RS-232;

Мережа на основі технології Ethernet;

Мережа на основі технології USB.

Інтерфейс RS-232 є інтерфейсом передачі між двома пристроями на відстані до 20 м, а інформація передається по дроту, рівень сигналу якого відрізняється від стандартного 5 В, що забезпечує більшу перешкодозахисну здатність. Асинхронна передача даних здійснюється із заданою швидкістю при синхронізації з рівнем стартового імпульсного сигналу.

Інтерфейс RS-232-C призначений для простого застосування, яке чітко визначається його назвою «інтерфейс між кінцевим обладнанням і комунікаційним обладнанням з послідовним обміном двійковим кодом». Кожне слово в назві є важливим, воно визначає інтерфейс між терміналом (DTE) і модемом (DCE) для передачі послідовних даних.

Сигнали слабшають і спотворюються після проходження через кабель. Загасання збільшується з довжиною кабелю. Цей ефект пов'язаний з ємністю кабелю. За стандартом максимальна навантажувальна здатність становить 2500 пФ. Типова робоча ємність кабелю становить 130 пФ, тому максимальна довжина кабелю обмежена приблизно 17 м.

Мережева СКУД на основі технології Ethernet дозволяє організувати значну кількість точок доступу, кількість яких обмежена лише можливостями програмного забезпечення. Така мережева СКУД може бути як локальною, так і розподіленою, і може взаємодіяти зі своїми компонентами через Інтернет.

2.2 Розробка програмної підсистеми

Програмна підсистема повинна забезпечувати роботу за картою варіантів використання систем контролю та управління доступом до об’єктів, що охороняються, розробку структур баз даних, розробку веб-інтерфейсів, розробку алгоритмів зчитування пристроїв.

Схема варіантів використання систем контролю та управління доступом до захищеного об'єкта.

Інформаційно-комп’ютерні системи контролю та управління доступом призначені для автоматичного контролю входу/виходу людей у/з будівель і місць.

Системою можуть користуватися оператори та користувачі. Кожен з них має свої права в системі.

Користувач (працівник підприємства) виконує дві операції (рисунок 2.8) - стандартну ідентифікацію (процес ідентифікації суб’єкта самостійно або за заданими ознаками особистості) та автентифікацію (процес ідентифікації суб’єкта шляхом порівняння введених ідентифікаційних даних з ідентифікаційними даними). [46-48]

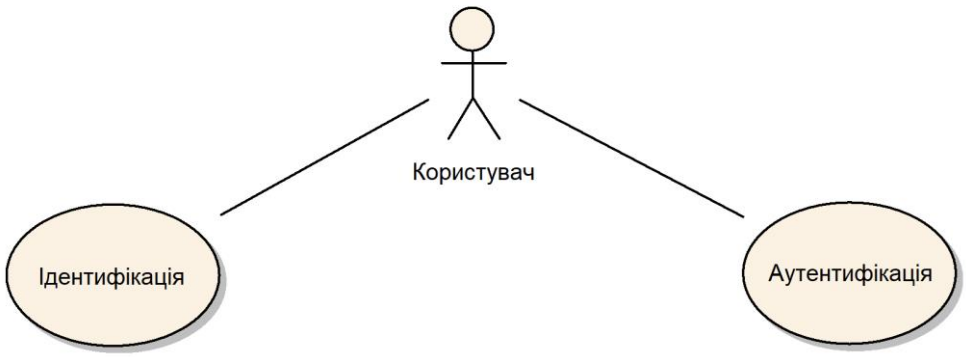


Рисунок 2.8 – Діаграма варіантів використання системи для користувача

Оператори мають права налаштовувати та керувати пристроями, переглядати поточні системні події, керувати списками об’єктів доступу, переглядати архіви та отримувати звіти.

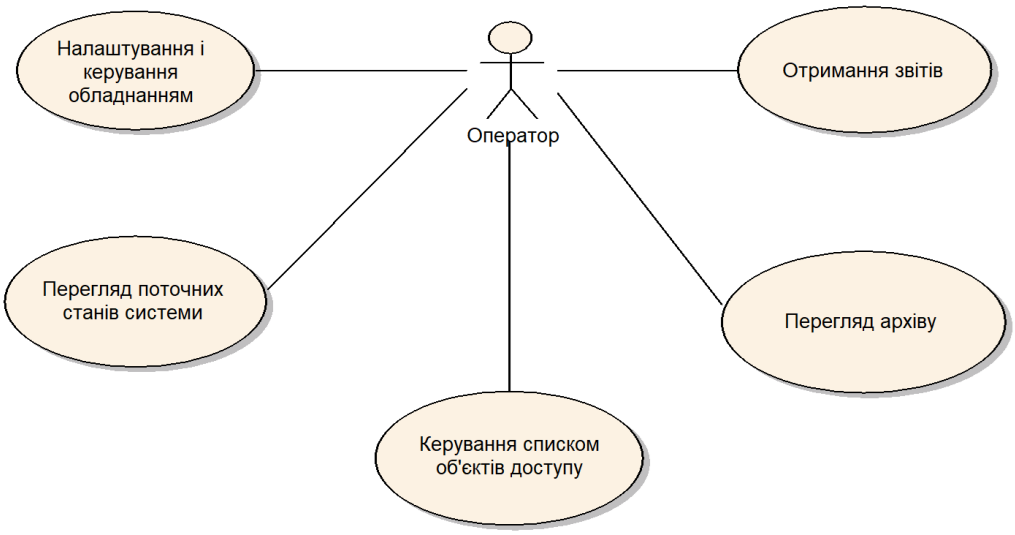


Рисунок 2.9 – Діаграма варіантів використання системи оператора

Налаштування та керування обладнанням передбачає здатність оператора:

– додати нову точку доступу (АТ); точка доступу - це місце, де здійснюється контроль доступу, в системі, що розробляється, тільки двері виступають як TD;

– видалити існуючий ТД;

– оцінити якість зв'язку з мікроконтролером.

Перегляд системних подій дозволяє оператору вибрати точки доступу, які його цікавлять (одну, кілька або всі), налаштувати фільтри системних подій (наприклад, показувати лише події зареєстрованих спроб несанкціонованого доступу) і отримати доступ до останніх подібних подій. Відбувається в цих точках доступу. Оператор також може переглядати облікову картку користувача.

У таблиці 2.1 наведено основні переваги та недоліки трьох найбільш популярних open-source СУБД – PostgreSQL, MySQL та FirebirdSQL .

Таблиця 2.1 - Переваги та недоліки різних СУБД

СУБД для зберігання даних	MySQL	PostgreSQL	FirebirdSQL
Переваги	- швидкодія; - безпека та надійність; - відсутності. високих вимог до апаратних ресурсів; - перенесення.	- підтримка БД практично необмеженого розміру; - потужні та надійні механізми транзакцій та реплікації; - успадкування; - легка розширюваність.	- багатоверсійна архітектура; - компактність (дистрибутив 5Mb); - Висока ефективний. і потужна мовна підтримка для процедур і тригерів, що зберігаються.
Недоліки	- відсутність транзакцій та тригерів; - відсутні процедури, що зберігаються, і вкладені запити; - немає підтримки інструкції UNION ; - відсутність каскадного оновлення даних.	- відносна складність інсталяції; - неправильна робота оточення PostgreSQL; - відсутність повної підтримки мов програмування VB та C#; - Відсутність Intellisense при програмірів.	- відсутність кешу результатів запитів; - відсутність повнотекстових індексів.

Кожна база даних має свої особливості та відмінності. Але оскільки система, що розробляється, повинна швидко зберігати прості запити з мінімальною конфігурацією, СУБД MySQL буде використовуватися як СУБД для зберігання даних.

2.3 Розробка класів-сутностей

При розробці системи було вирішено використовувати ORM. ORM (абревіатура від Object Relational Mapping — Object-Relational Projection) — техніка програмування, яка пов’язує бази даних із концепціями об’єктно-орієнтованих мов програмування, створюючи «віртуальну об’єктну базу даних». Суть задачі, що вирішується за допомогою рівня ORM, полягає в необхідності перетворення об'єктної структури в пам'яті додатка у форму, зручну для зберігання реляційної бази даних, і вирішення зворотного завдання - перекладу розширеної моделі реляційної бази даних в модель об’єкта, зберігаючи атрибути об’єктів і зв’язок між ними.

Розроблено ряд сутностей, які ми розглянемо нижче.

«Рівень доступу» - ця сутність буде створена для обмеження або дозволу доступу того чи іншого співробітника в різних кімнатах.

"EmployeeGroup" – ця сутність використовуватиметься для об’єднання співробітників з однаковими правами доступу, підмножини. У більшості випадків люди з одного відділу та з однієї посади мають однаковий рівень доступу, об’єднання людей з однаковим рівнем доступу створить об’єкт.

«Робоче місце» — ця сутність вказує, до яких кімнат може входити працівник і має певні права доступу. Цей суб’єкт необхідний, оскільки необхідно знати, чи має працівник таке право, перш ніж дозволити йому увійти в приміщення.

"юзер" - робітник. Ця організація зберігає особисті дані кожного співробітника компанії, такі як ПІБ, дата народження або посада.

«Відсутність за станом здоров'я» - записує кількість днів, коли працівник перебуває на лікарняному. За допомогою цієї сутності система може точно розрахувати, скільки потрібно нарахувати працівнику з урахуванням лікарняних.

«Реальна заробітна плата» - місячний заробіток, включаючи лікарняні, премії та пеню.

«Перехід» - суть контролю та зберігання всього персоналу, який переходить з одного приміщення в інше. Містить інформацію про те, коли в кімнату увійшли, про те, де відбувся перехід. Якщо співробітник зайшов в кімнату вперше за день, то в полі «звідки» буде зберігатися 0. Таким чином, можна відстежити, куди працівник їде вперше. Таким же чином сутності зберігають дані про час, проведений у тій чи іншій кімнаті.

«кімната» - зберігає номер кімнати та рівень доступу, необхідний для прямого переходу.

«Поверх» — шлях для зберігання кількості поверхів і файлу SVG (векторного малюнка), що показує план кімнат на поверсі.

«Будівля» є одним цілим, якщо офіс розташований на території більш ніж однієї будівлі. Зберігає номер будівлі, адресу, де розташована будівля, і файл SVG, що містить схематичну схему будівлі.

Алгоритм розрахунку вхідних місць

При створенні системи було реалізовано багато алгоритмів, але я не хочу їх усі деталізувати. Тому для основної мети системи, тобто алгоритму обчислення відвідувань місць, буде розглянуто кілька алгоритмів.

Спочатку розглянемо алгоритм обчислення входів місць. При введенні місця система створює об'єкт класу Transition (перехід), а в локальну змінну tempId вводить дані з карти, зчитані пристроєм зчитування, тобто ID користувача. Далі даний користувач шукається в системі за ID, і якщо користувач не знайдений, дані логічного типу "false" вводяться в поле "isAccessPermitted" класу Transition, а "nu" (No User) в поле поле "reason", після чого метод завершується і повертає false. В іншому випадку, якщо в системі є користувач з існуючим ідентифікатором, відповідні дані вводяться в поля класу «toRoom» - номер кімнати, в яку ми хочемо перейти, «timeIn» - час введення кімната. Після цього система перевіряє, чи має працівник дозвіл входити в цю кімнату, якщо працівник не має такого права, система вводить дані логічного типу «false» у поле класу «isAccessPermitted», «n a» (No Access) у поле класу «n a» (No Access). поле "reason" і завершіть метод, повернувши

false. Якщо перевірка позитивна, система вводить дані — «ок» у поля «isAccessPermitted» і «reason» логічного типу «true» (і завершує метод, повертаючи true).

Другий алгоритм, який буде наведено нижче, передбачає облік виходу з приміщень. При виході система шукає вже ідеальний вхід в потрібну співробітнику кімнату. Якщо метод пошуку повертає значення null, метод виходу закінчується, повертаючи false. В іншому випадку заповніть дані в поле об’єкта знайденої транзакції (об’єкт передається методом findTransition), тобто заповніть поле тайм-аут для часу виходу, а також заповніть provedtime venue для часу перебування в кімнаті. .

Діаграми класів

При проектуванні системи діаграми класів створюються для спрощення розуміння «логіки» системи. Розглянемо набір класів, які забезпечують обмін даними між системою і базою даних.

У верхній частині знаходиться інтерфейс IID, який розширюють усі класи сутностей. Він був створений для спрощення розуміння програмного коду. Щоб не представляти всі класи як AbstractClass<ClassName, ID>, використовуючи цей інтерфейс, ми представляємо класи як AbstractClass<ClassName>. Розглянемо кожну сутність окремо. Клас "AccessLevel" існує для зберігання рівня доступу кожної групи осіб до того чи іншого об'єкта. Клас "GroupWorker" потрібен для об'єднання людей у колекцію за різними принципами, щоб гарантувати права доступу. «Верстак» зберігає дані про те, де на підприємстві працює той чи інший співробітник. Це необхідно для того, щоб правильно обліковувати час перебування на робочому місці. Наприклад, співробітник IT-відділу має право відвідувати приміщення свого відділу, серверну, кафетерій і офіси відділу маркетингу, але в ресторані і відділі маркетингу він не може виконувати будь-яку роботу, корисну для компанії, і, відповідно, Час не зараховується як робочий час. Якщо місце відсутнє в цьому списку, відповідна група користувачів не має доступу до цього місця. У класі «RealSalary» зберігається інформація про місячну

зарплату з урахуванням лікарняних, штрафів або премій. Клас «MissByIll» використовується для відстеження лікарняних по кожному співробітнику, ця інформація необхідна для правильного розрахунку зарплати за поточний місяць.

Клас «Користувач» використовується для зберігання та перевірки особистої інформації співробітників компанії. Використовуючи ці дані, система приймає рішення дозволити доступ до місця. Якщо співробітника з таким ідентифікатором немає в базі даних, система заборонить доступ до будь-якої кімнати. Перехід потрібен для реєстрації інформації про переходи, здійснені працівниками. На основі цієї інформації будується список переміщень для певного працівника, розраховується час перебування на робочому місці та нараховується заробітна плата, і на основі цієї інформації можна дізнатися, де зараз знаходиться працівник.

Нижче наведено діаграму класів бізнес-логіки системи контролю та управління доступом. Клас Index діє як домашня сторінка системи, він створює об’єкт класу, у якому ініціалізуються всі необхідні компоненти для розміщення на домашній сторінці, а сторінка позначається. Так само клас «Індекс» відповідає за виклик усіх форм, які містять всю інформацію, необхідну для управління системою, наприклад, форма «Користувач» відображає список усіх користувачів, список можна фільтрувати за різними критеріями. У таблиці Stage показано план поверху, клацання потрібної кімнати на плані поверху кімнати відкриє список усіх працівників, які зараз перебувають у цій кімнаті. Ви також можете знайти конкретного користувача на плані кімнати, вказавши його ID або прізвище та ініціали.

Клас AbstractForm містить усі узагальнені методи всіх класів форм, такі як add, delete, replace, які надають компоненти поля користувачам для введення даних. Кожна форма забезпечує відображення даних на екрані, а також їх додавання, видалення та заміну.

На діаграмі також існує допоміжний клас. "SpringContextHelper" - цей клас забезпечує вибірку даних із сховища до контролера. Використовуйте

PagingAndSortingRepository замість класу DAO - це інтерфейс бібліотеки spring-data, яка є частиною Spring framework. Використовуючи цю бібліотеку, немає необхідності створювати абстрактні фабрики DAO і успадковувати всі загальні методи класу DAO. Але щоб коректно передавати інформацію з бази даних до контролера через репозиторій, необхідно створити SpringContextHelper. У цьому класі вам потрібно створити конструктор, у який ви передаєте змінну, яка визначає набір методів, які використовує сервлет для зв'язку зі своїм контейнером сервлету. Інакше дані не виводитимуться.

Клас Components описує розмітку, яка буде застосована до домашньої сторінки, де ініціалізуються всі компоненти інтерфейсу домашньої сторінки.

2.4 Розробка апаратної підсистеми

Пристрій КУД виконує роль апаратної підсистеми. До них відносяться: зчитувачі (RFID зчитувачі), елементи управління (контролери). Також необхідно вибрати найбільш інтерфейс передачі даних між системою і контролером. Колективна взаємодія цих апаратних засобів фактично забезпечує контроль доступу та управління.

Блок-схема для розробки блоку контролю доступу (СКУД)

Особливостями розробленого пристрою є:

– є модуль NAND FLASH, з якого буде завантажуватися операційна система;

– є модуль SD/MMC для підключення карт пам'яті;

– ДБЖ для забезпечення постійного живлення обладнання панелі керування та автоматичного живлення обладнання, підключеного до ДБЖ, від вбудованої батареї у разі збою електроживлення;

– контролери Ethernet для забезпечення зв'язку між серверами та пристроями проектування.

Основними елементами структури пристрою KUD для аутентифікації користувача є:

– зчитувач RFID ;
– мікроконтролер;
– Ethernet- контролер;
– модуль DDR3 ;
– модуль NAND FLASH;
– модуль SD/MMC.

Ethernet контролер і два блоки. Блок Ethernet MAC відповідає за прийом і формування пакетів Ethernet. Блок PHY відповідає за генерацію сигналів на проводах фізичного рівня інтерфейсу Ethernet. Блок PHY буде взаємодіяти з блоком Ethernet MAC через інтерфейс IEEE 802.3 MII (Media Independent Interface).

Основні критерії вибору мікроконтролера в порядку важливості:

– придатність до прикладної системи;
– доступність;
– підтримка розробника;
– інформаційна підтримка;
– надійність фірми виробника.

В якості елемента управління було обрано мікроконтролер сімейства Integra ARMCortex-A8-SK-iMX53, який повністю відповідає всім перерахованим критеріям.

Мікроконтролер SK-iMX53 містить процесор ARM Cortex-A8.

2.5 Висновки до другого розділу

У розділі наведено розробку інформаційно-комп'ютерної системи контролю та управління доступом. Проведена розробка архітектури СКУД. Виділено основні елементи СКУД. Виконана розробка програмної підсистеми. Також проведена розробка класів-сутностей. Зроблена розробка апаратної підсистеми.

3 РОЗРОБКА ПРОТОКОЛУ ПЕРЕДАЧІ ДАНИХ

3.1 Протоколи даних

UDP Можна використовувати наступні протоколи: UDP, TCP/IP і HTTP.

UDP є найшвидшим і найдешевшим протоколом. Дозволяє обмінюватися пакетами розміром трохи більше кадру Ethernet (приблизно 1500 байт). Але в СКУД контролер рідко обмінюється з ПК пакетами розміром більше 100 байт. Таким чином, через свою швидкість і простоту, UDP є першим кандидатом для використання в системах реального часу. Недолік UDP - відсутність гарантованої доставки повідомлення - легко подолати тим же методом, що і RS-485: підтвердження, тобто. Підтверджуйте, надсилаючи квитанцію на кожну посилку.

TCP/IP. Цей протокол забезпечує гарантовану доставку, він може «різати» з одного боку і «склеювати» великі пакети на приймальному кінці, але нам це не дуже потрібно. Однак він менш чутливий і набагато дорожчий з точки зору реалізації програмного забезпечення. Його перевага полягає в тому, що він часто використовує комутатори та маршрутизатори компанії.

HTTP є найповільнішим протоколом, він "складений" поверх TCP/IP і в основному використовується для WEB, тобто. Саме з його допомогою ми можемо отримати інформацію з Інтернету. З цього ми фактично проходимо через це в глобальному масштабі, що є певною перевагою цього. Але в системах реального часу його застосування практично неможливе через низьку швидкість.

З цього короткого огляду стає зрозуміло, що для систем реального часу, таких як системи контролю доступу, найкраще використовувати протокол UDP.

UDP — це протокол транспортного рівня. Метою транспортного рівня є доставка даних у тому порядку, в якому вони були передані, без помилок, втрат або дублювання. При цьому не має значення, які дані передаються,

звідки, куди, тобто забезпечує сам механізм передачі. Він розбиває блоки даних на фрагменти, розмір фрагментів залежить від протоколу, короткі злиття, довгі перерви. Протоколи на цьому рівні використовуються для однорангової взаємодії. Транспортний рівень надає такі види послуг:

– встановлення транспортного сполучення;
– передача даних;
– розрив транспортного сполучення.

Функції, що виконуються транспортним рівнем:

– перетворення транспортної адреси на мережевий;
– міжкінцеве мультиплексування транспортних з'єднань у мережеві;
– встановлення та розрив транспортних з'єднань;
– міжкінцеве впорядкування блоків даних щодо окремих з'єднань;
– міжкінцеве виявлення помилок та необхідний контроль за якістю послуг;
– міжкінцеве відновлення після помилок;
– міжкінцеве сегментування, об'єднання та зчеплення;
– міжкінцеве керування потоком даних за окремими сполуками;
– передача термінових транспортних блоків даних.

Як протокол дейтаграм, протокол UDP максимально реалізує послуги, тобто гарантує доставку своїх повідомлень, тому не може компенсувати ненадійність протоколу дейтаграм IP.

Блок даних протоколу UDP називається пакетом UDP або дейтаграмою користувача. Кожна дейтаграма містить одне повідомлення користувача. Це призводить до природного обмеження: довжина дейтаграми UDP не може перевищувати довжину поля даних IP, яке, у свою чергу, обмежене розміром кадру базової технології. Таким чином, якщо UDP-буфер переповнюється, дані програми буде видалено. Заголовок UDP складається з чотирьох 2-байтових полів, які містять порт джерела, порт призначення, довжину UDP і поля контрольної суми.

Поля “Порт джерела” та порт одержувача ідентифікують передавальний та отримуючий процеси.

Поле “Довжина UDP” містить довжину пакета UDP у байтах.

Поле “Контрольна сума” містить контрольну суму UDP, що обчислюється по всьому пакету UDP з доданим псевдозаголовком.

У поле "Дані" передається наступна інформація: код співробітника, який отримав доступ до об'єкта, що охороняється, а також дата і час проходу через ППК.

Поле протоколу (8 біт) визначає протокол із заголовка IP-пакету. Для UDP це значення становить 17. Однією з областей, де UDP використовується особливо широко, є область клієнт-серверних додатків.

Недолік UDP - відсутність гарантії доставки повідомлення вирішується за допомогою квитанції, тобто підтвердження отримання кожного переданого пакета.

Щоб мати можливість організувати повторну передачу спотворених даних, відправник нумерує передані кадри даних. Для кожного кадру відправник очікує від одержувача так зване підтвердження - службове повідомлення, яке повідомляє про те, що оригінальний кадр отримано і дані в ньому виявилися правильними. Цей час очікування обмежений (під час надсилання кожного кадру відправник запускає таймер, якщо після закінчення не отримано позитивного квитанції, кадр вважається втраченим).

Існує два способи організації процесу обміну позитивними і негативними квитанціями: простої та організація «вікон».

Метод очікування вимагає, щоб джерело, що надсилає кадр, чекало підтвердження (позитивного чи негативного) від одержувача перед тим, як надсилати наступний кадр (або повторювати спотворені кадри). У цьому випадку продуктивність обміну даними істотно знижується - хоча відправник може відправити наступний кадр відразу після відправки попереднього кадру, він повинен чекати приходу прийому. Зниження продуктивності цього методу

корекції особливо помітно на низькошвидкісних каналах зв'язку, тобто в територіальних мережах.

У другому способі збільшення використання лінії джерелу дозволяється передавати певну кількість кадрів у безперервному режимі, тобто з максимально можливою швидкістю джерела, без отримання квитанцій на ці кадри у відповідь. Кількість кадрів, яку можна передати таким чином, називається розміром вікна. Як правило, кадри під час обміну циклічно нумеруються від 1 до W. Під час надсилання кадру номер 1 джерелу дозволяється передати ще W-1 кадри до отримання підтвердження для кадру 1. Якщо протягом цього часу не надійшло підтвердження отримання кадру 1, процес передачі припиняється, і після тайм-ауту кадр 1 вважається втраченим (або його прийом був втрачений) і передається знову.

Якщо потік надходжень надходить більш-менш регулярно, в межах допуску W кадрів, курс обміну досягає максимально можливого значення для даного каналу та прийнятого протоколу.

Цей алгоритм називається алгоритмом ковзного вікна, оскільки кожного разу, коли надходить квитанція, вікно переміщується (ковзає), захоплюючи нові дані, які можна передати без підтвердження.

Оскільки розроблена система є системою реального часу, то доцільніше використовувати «віконний» алгоритм збору, оскільки він може досягти максимально можливого значення швидкості обміну.

RS-232 є інтерфейсом передачі між двома пристроями на відстань до 20 м. Інформація передається по дроту, рівень сигналу якого відрізняється від стандартного 5 В, а перешкодозахисна здатність сильніша. Асинхронна передача даних здійснюється із заданою швидкістю при синхронізації з рівнем стартового імпульсного сигналу.

Широко використовуваний послідовний інтерфейс для синхронної та асинхронної передачі даних, як визначено стандартом EIA RS-232-C і рекомендацією CCITT V.24. Спочатку створіть з'єднання між комп'ютером і терміналом. В даний час використовується в різних додатках.

Інтерфейс RS-232-C з'єднує два пристрої. Лінія передачі першого пристрою з'єднується з лінією прийому другого пристрою і навпаки (повний дуплекс). Програмне забезпечення ідентифікує пристрій, який використовується для керування з'єднанням (вводить у потік даних відповідні контрольні символи). Апаратні підтвердження можуть бути організовані шляхом організації додаткових ліній RS-232 для забезпечення функцій визначення стану та контролю.

Таблиця 3.1 - Канали передачі даних RS-232

Найменування	Напрям	Опис	Контакт (25-контактний роз'єм)	Контакт (9-контактний роз'єм)
DCD	IN	Carrie Detect (Визначення несучої)	8	1
RXD	IN	Receive Data (Прийняті дані)	3	2
TXD	OUT	Transmit Data (Передаються дані)	2	3
DTR	OUT	Data Terminal Ready (Готовність терміналу)	20	4
GND	-	System Ground (Корпус системи)	7	5
DSR	IN	Data Set Ready (Готовність даних)	6	6
RTS	OUT	Request to Send (Запит на відправлення)	4	7
CTS	IN	Clear to Send (Готовність прийому)	5	8
RI	IN	Ring Indicator (Індикатор)	22	9

Структурна кабельна система (СКС) - це звичайна кабельна система для будівлі, групи будівель, призначена для використання протягом значного періоду часу без реорганізації.

Універсальність СКС передбачає використання її для різних систем:

– комп'ютерна мережа;

– телефонна мережа;

– охоронна система;

– пожежна сигналізація.

Така кабельна система не залежить від кінцевих пристроїв, що дозволяє створити гнучку корпоративну комунікаційну інфраструктуру. Структурована кабельна система – це набір пасивних комунікаційних пристроїв: кабелів (компонент, який використовується як середовище передачі даних для СКС), розеток (компонент, який використовується як точка входу в кабельну мережу будівлі), комутаторів (використовуються для управління підлогою та будівельна комутація Кабельні системи в центрах), загальні), лінії комутації (кабельні мережі для підключення оргтехніки до будівель, організація структур кабельної системи в центрах комутації).

Щоб отримати СКС, що відповідає міжнародним стандартам і може використовуватися протягом багатьох років без модернізації та заміни, в процесі проектування необхідно враховувати наступні вимоги:

Структурні кабельні системи повинні бути виготовлені відповідно до міжнародних стандартів (ISO 11801), європейських стандартів (EN 50173);

Всі комунікації на поверсі повинні бути виведені в єдиний комутаційний центр (поверховий розподільник), що прискорює обслуговування мережі і скорочує час комутації користувачів;

Конструкція СКС враховує резервування кількості користувачів і пропускної здатності, що забезпечує можливість її подальшого розширення без реорганізації;

Прокладання кабелів у коридорах слід проводити за підвісними стелями, якщо немає спеціальних кабельних каналів (коробів, лотків тощо) або в наявних прибудовах;

Якщо при побудові мережі невідома точна кількість необхідних робочих місць, СКС проектується з розрахунку одне робоче місце на 6 кв.

Кожна робоча станція повинна мати два підключених змінних роз’єми RJ45.

Обладнання контролю та управління доступом має бути встановлено на дверях, що ведуть до таких місць банку: кредитний відділ, відділ обслуговування приватних клієнтів, бухгалтерія, рецепція, кімната охорони, відділ обслуговування корпоративних клієнтів, серверна, відділ технічної підтримки, громадські. відділ зв'язків, відділ веб-дизайну та кабінет начальника відділу технічної підтримки. Крім того, на дверях загального коридору від рецепції до відділення банку планується встановити КУД для обліку робочого часу працівників банку (для цього необхідно встановити два КУД, на вході та на виході). Отже, загальна кількість встановлених приладів КУД становить 12 шт.

3.2 Опис процесу автоматизації збирання

Процес збирання виконується за допомогою Maven. Щоб проілюструвати налаштування програмного забезпечення, розгляньте вміст файлу налаштувань pom.xml, даведено у додаткуА.

3.3 Тестування програмного забезпечення

На етапі впровадження програмного забезпечення класи перевіряються, щоб переконатися, що вони працюють і функціонують належним чином. Ці класи тестуються за допомогою бібліотеки JunitTest. Програмне забезпечення досягло повністю функціонального стану під час проектування та тестування.

Як видно на скріншоті, всі тестові методи виконані успішно. Нижче наведено вміст класу "AccessLevelTets" уважніше до деяких методів тестування - Додаток Б.

3.4 Реалізація web-інтерфейсу

Інтерфейс інформаційної системи розроблений таким чином, щоб не створювати дискомфорту під час використання. Інтерфейс повинен відповідати наступним вимогам:

– має інтуїтивно зрозумілу навігацію;

- мати дійсну обрану кольорову гаму;

- надати можливість швидко та ефективно маніпулювати елементами навігації для отримання даних.

Веб-інтерфейс є важливою частиною системи, що розробляється. Через нього оператори працюватимуть із системою: переглядати звіти, що містять дані про події, системні оповіщення та дані про співробітників, переглядати журнали подій системи, додавати користувачів до списків доступу до об’єктів, що охороняються.

При вході в систему оператору відкривається форма авторизації, в якій він повинен ввести свій логін і пароль для доступу до сервера.

Якщо користувач не знає пароля або логіна оператора і намагається його знайти, після 3 невдалих спроб система видає повідомлення про блокування IP-адреси. Такий підхід необхідний для того, щоб користувачам, які не мають доступу до системи, було максимально важко вибрати пароль.

Після успішної автентифікації оператор може отримати доступ до інтерфейсу для взаємодії з системою.

Цей інтерфейс надає оператору всі засоби для керування СКУД, моніторингу його стану та отримання звітів про системні події. Натисніть на іконку у верхній частині екрана, щоб увійти у відповідний розділ, а саме: керування користувачами, статистика переходів, керування групами користувачів, перегляд плану поверху, пошук користувачів приміщень, перегляд заробітної плати за посадою в поточному місяці, перегляд список пацієнтів, розсилка інформаційних бюлетенів співробітникам, система виходу.

Натискання кнопки Групи користувачів відкриває вікно зі списком груп користувачів. Як показано на рисунку, у вікні «Працівники групи» є 3 кнопки: Додати, Змінити та Видалити. Це ж вікно можна побачити, натиснувши кнопку користувача або список пацієнтів.

Список пацієнтів – дуже важливий елемент системи, який допомагає автоматично розраховувати щомісячну суму з урахуванням лікарняних та штрафів за надмірну відсутність на робочому місці. Система сама розраховує заробітну плату до нарахування в кінці місяця та накладає штрафи на порушників відповідно до тарифів, які можна змінити, натиснувши кнопку «Налаштування». Таким чином, система не тільки корисна з точки зору безпеки, але й бере на себе частину бухгалтерської роботи.

Натискання кнопок «Видалити», «Додати» або «Змінити» відкриває вікно з відповідними полями, за допомогою яких можна виконати вибрану дію.

Інтерфейс реалізовано за допомогою jquery та ajax, що позбавляє вас від перезавантаження сторінки для кожної дії. Ця система дозволяє відкривати всі вікна управління і перемикатися між ними, як і в графічній операційній системі, без оновлення самих сторінок, що економить час і робить систему більш зручною у використанні.

СКУД дозволяє знайти потрібного співробітника і показати його місцезнаходження на території підприємства, якщо він присутній на підприємстві в даний момент. Різні списки в системі можна фільтрувати та вирівнювати за різними критеріями.

Також була розроблена інтерактивна карта, яка показує розташування співробітників на принциповій схемі офісу, плани приміщень, відображає список людей в офісі. Щоб переглянути список користувачів, просто наведіть вказівник миші на зображення кабінету та клацніть лівою кнопкою миші на об’єкті.

З метою розширення функціональних можливостей системи розроблено корпоративний «ландшафтний» модуль. Це дозволяє централізовано

контролювати та керувати доступом, якщо підприємство займає більше однієї будівлі. Для наочності модуля створено скріншоти інтерфейсу модуля.

3.5 Висновки до третього розділу

Програмна частина реалізована за архітектурою клієнт/сервер. Під час кваліфікаційної роботи фахівці розробили базу даних та товстий клієнт (веб-додаток) для оператора.

Результатом розробки є розробка архітектури системи, структури та схеми електричних принципів обладнання контролю та управління доступом.

Особливістю даної розробки є використання мікроконтролера SK-iMX53 в якості елемента керування пристроями контролю та контролю доступу. Тому пристрій має широкий набір функцій, а також високий рівень захисту даних, що передаються по мережі.

ВИСНОВКИ

Метою роботи була розробка системи контролю та управління доступом, яка дозволяє запобігати несанкціонованому доступу до об’єктів підприємства, що охороняються, а також зберігати та переглядати інформацію про події в системі за певний період часу.

Для досягнення поставленої мети було проведено аналіз аналогічних комп’ютерних систем контролю та управління доступом. Вибрано метод RFID ідентифікації користувача за його підписом. Цей метод був обраний через низькі матеріальні витрати на створення системи, а також відносну звичність цього методу ідентифікації для звичайного користувача.

Програмна частина реалізована в архітектурі клієнт/сервер. Під час цієї кваліфікаційної роботи фахівцем була розроблена база даних та жирний клієнт (веб-додаток) для оператора.

Результатом дослідження є архітектура розробленої системи, структура та схема електричного принципу роботи пристроїв контролю та контролю доступу.

Особливістю даної розробки є використання мікроконтролера SK-iMX53 як керуючого елемента пристрою контролю та контролю доступу. Завдяки цьому пристрій має широкий функціонал, а також високий рівень захисту даних, що передаються по мережі.

Використання даної системи дасть змогу якісно покращити вирішення таких важливих завдань, як охорона праці, дотримання трудової дисципліни, збереження матеріальних цінностей, комерційної таємниці.

Розробка цієї системи забезпечує наступні переваги:

– можливість контролювати робочий час співробітників;

– контроль і обмеження гостьового доступу, дозволяючи вільне пересування співробітників;

– організація бази даних кожного співробітника.

Надалі планується розширити функції цієї системи за рахунок пожежної та охоронної сигналізації, а також системи відеоспостереження.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. ДСТУ 51241-2008 “Засоби та системи контролю та управління доступом. Класифікація. Загальні вимоги. Методи випробувань”.
2. Біометрична ідентифікація та аутентифікація [Електронний ресурс]. – Режим доступу: http://www.gmmcc.com.ua?id=76.
3. Інтегровані системи безпеки [Електронний ресурс]. - Режим доступу: http://www.aamsystems.ua/publications/?id=132.
4. Біометричні системи контролю доступу [Електронний ресурс]. – Режим доступу: http://ien.izi.vlsu.ua/teach/books/910/theory.html#_1.
5. Контроль доступу: пристрої контролю доступу провідних світових виробників [Електронний ресурс]. - Режим доступу: http://www.armosystems.ua/system/hid_skd.ahtm.
6. Panasonic – Системи безпеки [Електронний ресурс]. – Режим доступу: http://security.panasonic.com/Catalog/Receiver/WV-BM – ET 200.html. – Назва з екрана.
7. Новини про мобільні пристрої та технології [Електронний ресурс]. – Режим доступу: URL: http://naviny.ua/rubrics/computer/2005/11/13/art_12.
8. Системи відеоспостереження, контролю доступу, охоронні сигналізації та домофони (відеодомофони), відеореєстратори [Електронний ресурс]. – Режим доступу: URL: http://forward.lg.ua/pages/control.html. – Назва з екрана.
9. Бєлєнков В.Д. Електронні системи ідентифікації підписів. Захист інформації. Конфідент. 2019 №6, с. 39-42.
10. Іванов А.І., Сорокін І.А. Автоматична система ідентифікації особи за динамікою підпису. // Нові промислові технології. №6, 2018, с. 56-63.
11. Державні санітарні правила та норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин. ДСанПІН 3.3.2.007-98. Головне санітарно-епідеміологічне управління України. Київ 1998. - 24 с.

12. Горошко М. П. Біометрія: Навчальний посібник. / Горошко М. П., Миклуш С.І., Хомюк П.Г. — Львів: Камула, 2004. - 236 с.

13. Radio Frequency Identification and Sensors: From RFID to Chipless RFID [Архівовано 12 листопада 2020 у Wayback Machine.], Etienne Perret, Wiley-ISTE, 2014

14. La RFID sans puce — Théorie, conception, mesures [Архівовано 21 січня 2021 у Wayback Machine.], Arnaud Vena, Etienne Perret, Smail Tedjini, ISTE, 2016

15. RCS Synthesis for Chipless RFID — Theory and Design [Архівовано 24 листопада 2020 у Wayback Machine.], Olivier Rance, Etienne Perret, Romain Siragusa, Pierre Lemaitre-Auger, ISTE-Elsevier Jul. 2017

16. Chipless RFID Reader Design for Ultra-Wideband Technology [Архівовано 25 серпня 2020 у Wayback Machine.], Marco Garbati, Etienne Perret, Romain Siragusa, ISTE-Elsevier, Fev. 2018.

17. Chipless RFID based on RF Encoding Particle — Realization, Coding and Reading System [Архівовано 8 серпня 2020 у Wayback Machine.], Arnaud Vena, Etienne Perret, Smail Tedjini, ISTE-Elsevier, Aug. 2016.

18. Chipless RFID. IDtechEx. Процитовано 16 серпня 2013.[недоступне посилання з 01.06.2019]

19. MICROWAVE READABLE DIELECTRIC BARCODE. US patent office. Процитовано 17 серпня 2013.

20. RFID Tattoos to Make a Mark on Cattle Tagging. RFID Journal. Архів оригіналу за 6 березня 2014. Процитовано 17 серпня 2013.

21. Firewall Protection for Paper Documents. RFID Journal. Архів оригіналу за 22 червня 2013. Процитовано 17 серпня 2013.

22. RFID Fibers for Secure Applications. RFID Journal. Архів оригіналу за 23 лютого 2014. Процитовано 17 серпня 2013.

23. Tag It. Архів оригіналу за 24 вересня 2015. Процитовано 16 серпня 2013.

24. Acousto-magnetic System. How Stuff Works. April 2000. Архів оригіналу за 4 серпня 2013. Процитовано 16 серпня 2013.

25. AstraZeneca case study. Sagentia. Архів оригіналу за 12 січня 2014. Процитовано 16 серпня 2013.

26. Crossfield, M. (1 січня 2001). Have null, will fly. IEE Review 47 (1): 31–34. doi:10.1049/ir:20010111.

27. The Use of Flying Null Technology in the Tracking of Labware in Laboratory Automation. JALA. Архів оригіналу за 14 червня 2015. Процитовано 17 серпня 2013.

28. Plessky, VP; Reindl, LM (March 2010). Review on SAW RFID tags.. IEEE Transactions on Ultrasonics, Ferroelectrics, and Frequency Control 57 (3): 654–68. PMID 20211785. doi:10.1109/tuffc.2010.1462.

29. Jalaly, I.; Robertson, I.D. (2005). Capacitively-tuned split microstrip resonators for RFID barcodes. Microwave Conference, 2005 European 2. с. 4 pp.– 1164. ISBN 978-2-9600551-2-2. doi:10.1109/EUMC.2005.1610138.

30. ScattererID Analysis and synthesis of wideband scattered signals from finite-size targets — aspect-independent RF analog footprint [Архівовано 10 липня 2020 у Wayback Machine.], Etienne Perret, 2018.

31. Будіщев М. С. Електротехніка, електроніка та мікропроцесорна техніка : Підручник / М. С. Будіщев. – Львів : Афіша, 2001. – 424 с.

32. Колонтаєвський Ю. П. Промислова електроніка і мікросхемотехніка / Ю. П. Колонтаєвський, А. Г. Сосков. під ред. А. Г. Соскова. – Вид. 2-ге, виправл. і доповн. – Харків : ХДАМГ, 2003. – 281 с.

33. Колонтаєвський Ю. П. Електроніка і мікросхемотехніка : підручник / Ю. П. Колонтаєвський. - Київ : Каравела, 2006. - 384 с.

34. Макаренко В. В. Цифрова та імпульсна схемотехніка. Моделювання та аналіз : навч. посіб. для студентів, які навчаються за напрямом підготовки «Акустотехніка» [Електронний ресурс] / В. В. Макаренко, В. М. Співак ; НТУУ «КПІ». -Київ : НТУУ «КПІ», 2015. - 314 с. - Режим доступу: https://ela.kpi.ua/ handle/123456789/19099.

35. Бойко В. І. Мікрокомп'ютерна техніка / В. І. Бойко, А. Т. Нельга. - 2-ге вид. - Київ : Науково-методичний центр вищої освіти, 2008. - 254 с.

36. Електроніка та мікросхемотехніка: Навчальний посібник / За ред. проф. В.Ф. Яковлєва. – К.: Аграрна освіта, 2010. – 329 с.

37. Методичні вказівки до лабораторних робіт з курсу «Мікропроцесорні пристрої» для студентів спеціальності 092206 «Електричні машини та апарати» / Уклад.: Ю. С. Грищук, Т. П. Павленко. – Харків : ХДПУ, 1999. – 32 с.

38. Мікропроцесорна техніка : підручник / Ю. І. Якименко, Т. О. Терещенко, Є. І. Сокол та ін. / за ред. Т. О. Терещенко. – Київ : Політехнік, 2003. – 440 с.

39. Алексієв О. П. Мікроконтролери для транспортних і промислових застосувань.: архітектура та програмування : навч. посіб. / О. П. Алексієв, О. Б. Богаєвський, В. П. Волков. – Харків : ХНАДУ, 2004. – 156 с.

40. Методичні вказівки до лабораторних робіт з курсу «Мікропроцесорні пристрої». – Ч. 2 : «Однокристальні мікро контролери» для студентів спеціальностей 092206 «Електричні машини та апарати» і 092205 «Електропобутова техніка» усіх форм навчання / уклад. Ю. С. Грищук. – Харків : НТУ «ХПІ», 2003. – 43 с.

41. Скорик Б.І., Астахов Д.С. Посібник до вивчення дисципліни «САПР пристроїв захисту інформації» -Д.: РРВ ДНУ ,2011.- 86 с.

42. IPC-A-600F -Acceptability of Printed Boards (Критерії приймання друкованих плат). - 1999. - 125 с.

43. IPC-D-390A Automated Design Guidelines (Посібник з автоматизованого проектування друкованих плат).

44. IPC-SM-782A Surface Mount Design and Land Patterns (Amend. 1 - 5/95) Посібник з проектування плат поверхового монтажу та контактних майданчиків. (Виправлення 1 - 5/95).

45. www.altium.com – официйний сайт Altium Designer.

Додаток А

Вміст файлу налаштувань pom.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<project>
<modelVersion>4.0.0</modelVersion>
<groupId>com.vaadin.tutorial</groupId>
<artifactId>Skudy</artifactId>
<packaging>war</packaging>
<version>1.0</version>
<name>Vaadin Web Application</name>

<properties>
<project.build.sourceEncoding>UTF-8</project.build.sourceEncoding>
<vaadin.version>7.0.0</vaadin.version>
<vaadin.plugin.version>${vaadin.version}</vaadin.plugin.version>
</properties>
<repositories>
<repository>
<id>vaadin-addons</id>
<url>http://maven.vaadin.com/vaadin-addons</url>
</repository>
<repository>
<id>vaadin-snapshots</id>
<url>http://oss.sonatype.org/content/repositories/vaadin-snapshots/</url>
<releases>
<enabled>false</enabled>
</releases>
<snapshots>
<enabled>true</enabled>
</snapshots>
```

```
</repository>
</repositories>
<pluginRepositories>
<pluginRepository>
<id>vaadin-snapshots</id>
<url>http://oss.sonatype.org/content/repositories/vaadin-snapshots/</url>
<releases>
<enabled>false</enabled>
</releases>
<snapshots>
<enabled>true</enabled>
</snapshots>
</pluginRepository>
</pluginRepositories>
<dependencies>
<dependency>
<groupId>com.vaadin</groupId>
<artifactId>vaadin-server</artifactId>
<version>${vaadin.version}</version>
</dependency>
<dependency>
<groupId>com.vaadin</groupId>
<artifactId>vaadin-client-compiled</artifactId>
<version>${vaadin.version}</version>
</dependency>
<dependency>
<groupId>com.vaadin</groupId>
<artifactId>vaadin-client</artifactId>
<version>${vaadin.version}</version>
<scope>provided</scope>
</dependency>
```

```
<dependency>
<groupId>com.vaadin</groupId>
<artifactId>vaadin-themes</artifactId>
<version>${vaadin.version}</version>
</dependency>
<dependency>
<groupId>javax.servlet</groupId>
<artifactId>servlet-api</artifactId>
<version>2.4</version>
<scope>provided</scope>
</dependency>
<dependency>
<groupId>org.eclipse.persistence</groupId>
<artifactId>javax.persistence</artifactId>
<version>2.0.4.v201112161009</version>
</dependency>
<dependency>
<groupId>org.hibernate</groupId>
<artifactId>hibernate-core</artifactId>
<version>4.1.9.Final</version>
</dependency>
<dependency>
<groupId>org.hibernate</groupId>
<artifactId>hibernate-entitymanager</artifactId>
<version>4.1.9.Final</version>
</dependency>
<dependency>
<groupId>mysql</groupId>
<artifactId>mysql-connector-java</artifactId>
<version>5.1.23</version>
</dependency>
```

```
<dependency>
<groupId>org.springframework</groupId>
<artifactId>spring-core</artifactId>
<version>3.2.1.RELEASE</version>
</dependency>
<dependency>
<groupId>org.springframework</groupId>
<artifactId>spring-context</artifactId>
<version>3.2.1.RELEASE</version>
</dependency>
<dependency>
<groupId>org.springframework</groupId>
<artifactId>spring-web</artifactId>
<version>3.2.1.RELEASE</version>
</dependency>
<dependency>
<groupId>org.springframework</groupId>
<artifactId>spring-context-support</artifactId>
<version>3.2.1.RELEASE</version>
</dependency>
<dependency>
<groupId>org.springframework</groupId>
<artifactId>spring-orm</artifactId>
<version>3.2.1.RELEASE</version>
</dependency>
<dependency>
<groupId>org.springframework</groupId>
<artifactId>spring-aop</artifactId>
<version>3.2.1.RELEASE</version>
</dependency>
<dependency>
```

<groupId>org.springframework</groupId>
<artifactId>spring-beans</artifactId>
<version>3.2.1.RELEASE</version>
</dependency>
<dependency>
<groupId>junit</groupId>
<artifactId>junit</artifactId>
<version>4.11</version>
</dependency>
<dependency>
<groupId>org.springframework</groupId>
<artifactId>spring-jdbc</artifactId>
<version>3.2.1.RELEASE</version>
</dependency>
<dependency>
<groupId>org.springframework</groupId>
<artifactId>spring-test</artifactId>
<version>3.2.1.RELEASE</version>
</dependency>
<dependency>
<groupId>org.springframework.data</groupId>
<artifactId>spring-data-jpa</artifactId>
<version>1.3.0.RELEASE</version>
</dependency>
<dependency>
<groupId>org.aspectj</groupId>
<artifactId>aspectjweaver</artifactId>
<version>1.7.1</version>
</dependency>
<dependency>
<groupId>org.springframework</groupId>

```
<artifactId>spring-aspects</artifactId>
<version>3.2.1.RELEASE</version>
</dependency>
<dependency>
<groupId>com.vaadin.addon</groupId>
<artifactId>jpacontainer</artifactId>
<version>3.0.0.beta1</version>
</dependency>
</dependencies>

<build>
<plugins>

<plugin>
<groupId>org.apache.maven.plugins</groupId>
<artifactId>maven-compiler-plugin</artifactId>
<configuration>
<source>1.6</source>
<target>1.6</target>
</configuration>
</plugin>
<!-- As we are doing "inplace" GWT compilation, ensure the widgetset -->
<!-- directory is cleaned properly -->
<plugin>
<artifactId>maven-clean-plugin</artifactId>
<version>2.4.1</version>
<configuration>
<filesets>
<fileset>
<directory>src/main/webapp/VAADIN/widgetsets</directory>
</fileset>
```

```
</filesets>
</configuration>
</plugin>
<plugin>
<groupId>com.vaadin</groupId>
<artifactId>vaadin-maven-plugin</artifactId>
<version>${vaadin.plugin.version}</version>
<configuration>
<extraJvmArgs>-Xmx512M -Xss1024k</extraJvmArgs>
<!-- <runTarget>mobilemail</runTarget> -->
<!-- We are doing "inplace" але в subdir VAADIN/widgetsets. This
way compatible with Vaadin eclipse plugin. -->
<webappDirectory>${basedir}/src/main/webapp/VAADIN/widgetsets
</webappDirectory>
<hostedWebapp>${basedir}/src/main/webapp/VAADIN/widgetsets
</hostedWebapp>
<noServer>true</noServer>
<!-- Remove draftCompile when project is ready -->
<draftCompile>false</draftCompile>
<compileReport>true</compileReport>
<style>OBF</style>
<strict>true</strict>
<runTarget>http://localhost:8080/</runTarget>
</configuration>
<executions>
<execution>
<configuration>
<!-- if you don't specify any modules, the plugin буде find them -->
<!--                                                    <modules>
<module>com.vaadin.demo.mobilemail.gwt.ColorPickerWidgetSet</module>
</modules> -->
```

```
</configuration>
<goals>
<goal>resources</goal>
<goal>update-widgetset</goal>
<goal>compile</goal>
</goals>
</execution>
</executions>
</plugin>
<plugin>
<groupId>org.mortbay.jetty</groupId>
<artifactId>jetty-maven-plugin</artifactId>
<!--<configuration>-->
<!--<jettyConfig>src/main/webapp/WEB-INF/web.xml</jettyConfig>-->
<!--</configuration>-->
</plugin>
</plugins>
</build>
</project>
```

Додаток Б

Лістинг класу "Accessleveltets":

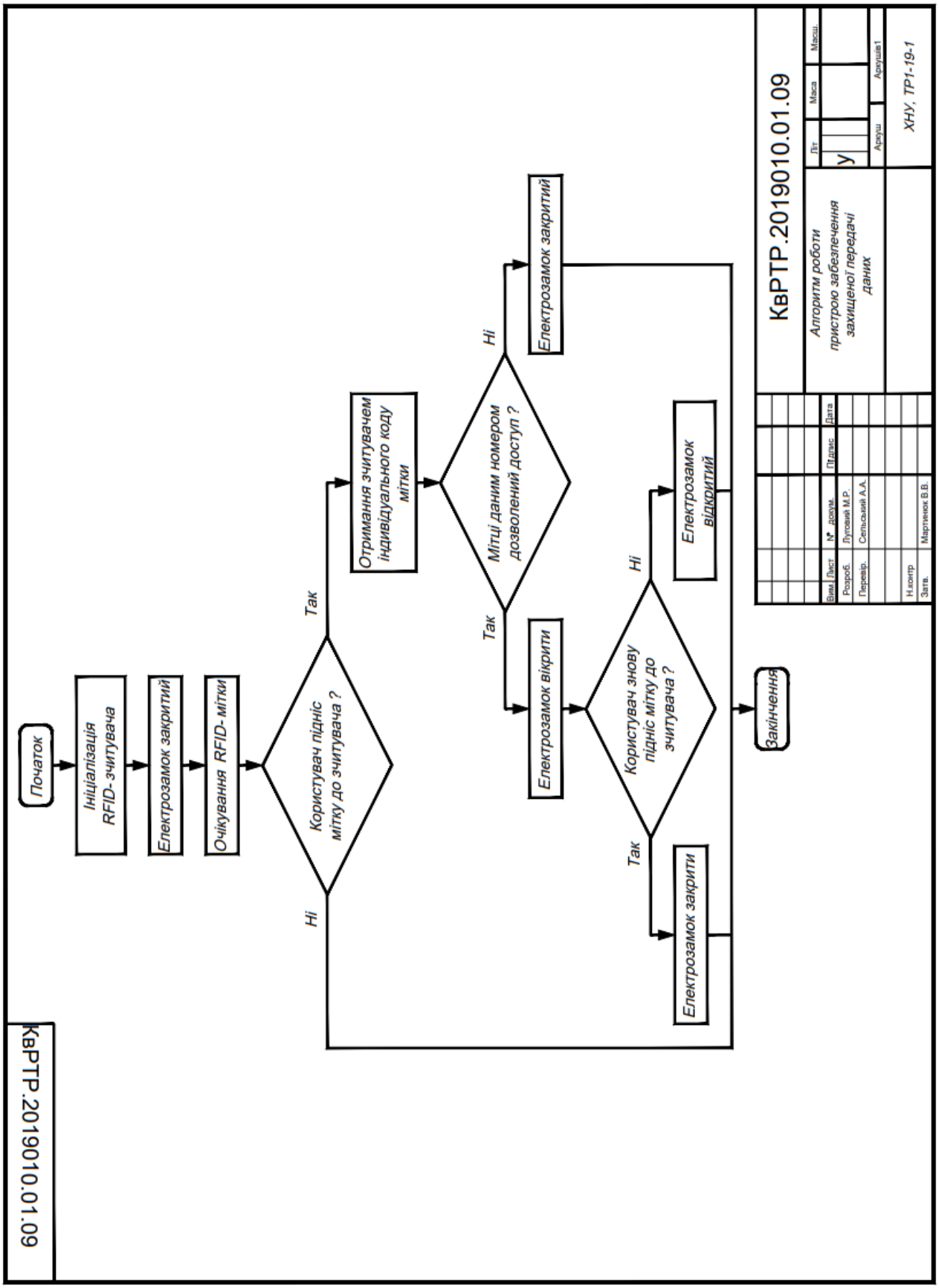
```
@ RunWith ( SpringJUnit 4 ClassRunner . class )
@ContextConfiguration(locations = { "classpath*:applicationContext.xml"})
public class AccessLevelTest {
@Autowired
private AccessRepository accessRepository;
@Autowired
private GroupRepository groupDao;
@Test
public void testCreateLevel() throws Exception {
AccessLevel accessLevel = новий AccessLevel();
accessLevel.setLevelNumber(123L);
GroupWorker groupWorker = New GroupWorker();
groupWorker.setGroupName("Banjo Men");
groupDao.save(groupWorker);
accessLevel.setGroupAccessLevel(groupWorker);
accessRepository.save(accessLevel);
Long getId = accessLevel.getId();
AccessLevel accessLevelTest = accessRepository.findOne(getId);
Long mustEquals=accessLevelTest.getLevelNumber();
Assert.assertNotNull("It was your mistake!", accessLevelTest);
Assert.assertEquals((Object) mustEquals, 123L);
accessRepository.delete(getId);
Long mD=groupWorker.getId();
groupDao.delete(mD);
AccessLevel mustNull=accessRepository.findOne(accessLevel.getId());
Assert.assertNull("It was your mistake", mustNull);
}
```

```
@Test
public void testUpdateLevel() throws Exception {
AccessLevel accessLevel = новий AccessLevel();
accessLevel.setLevelNumber(123L);
GroupWorker groupWorker = New GroupWorker();
groupWorker.setGroupName("Banjo Men");
groupDao.save(groupWorker);
accessLevel.setGroupAccessLevel(groupWorker);
accessRepository.save(accessLevel);
AccessLevel accessLevelTest =
accessRepository.findOne(accessLevel.getId());
accessLevelTest.setLevelNumber(1234567L);
accessRepository.saveAndFlush(accessLevelTest);
Long mustEquals=accessLevelTest.getLevelNumber();
Assert.assertNotNull("It was your mistake!", accessLevelTest);
Assert.assertEquals((Object)mustEquals, 1234567L);
accessRepository.delete(accessLevel.getId());
Long mD=groupWorker.getId();
groupDao.delete(mD);
AccessLevel mustNull=accessRepository.findOne(accessLevel.getId());
Assert.assertNull("It was your mistake", mustNull);
}
@Test
public void testDeleteLevel() throws Exception {
AccessLevel accessLevel = новий AccessLevel();
accessLevel.setLevelNumber(123L);
GroupWorker groupWorker = New GroupWorker();
groupWorker.setGroupName("Banjo Men");
groupDao.save(groupWorker);
accessLevel.setGroupAccessLevel(groupWorker);
accessRepository.save(accessLevel);
```

```
        Long getId = accessRepository.findOne(accessLevel.getId()).getId();
        accessRepository.delete(getId);
        Long mD=groupWorker.getId();
        groupDao.delete(mD);
        AccessLevel groupWorkerTest=accessRepository.findOne(getId);
        Assert.assertNull("It was your mistake",groupWorkerTest);
        }
        @Test
        public void testGetGroupById() throws Exception {
        AccessLevel accessLevel = новий AccessLevel();
        accessLevel.setLevelNumber(123L);
        GroupWorker groupWorker = New GroupWorker();
        groupWorker.setGroupName("Banjo Men");
        groupDao.save(groupWorker);
        accessLevel.setGroupAccessLevel(groupWorker);
        accessRepository.save(accessLevel);
        AccessLevel accessLevelTest =
accessRepository.findOne(accessLevel.getId());
        Long mustEquals=accessLevelTest.getLevelNumber();
        Assert.assertNotNull("It was your mistake!", accessLevelTest);
        Assert.assertEquals((Object)mustEquals, 123L);
        accessRepository.delete(accessLevel.getId());
        Long mD=groupWorker.getId();
        groupDao.delete(mD);
        AccessLevel mustNull=accessRepository.findOne(accessLevel.getId());
        Assert.assertNull("It was your mistake", mustNull);
        }}
```

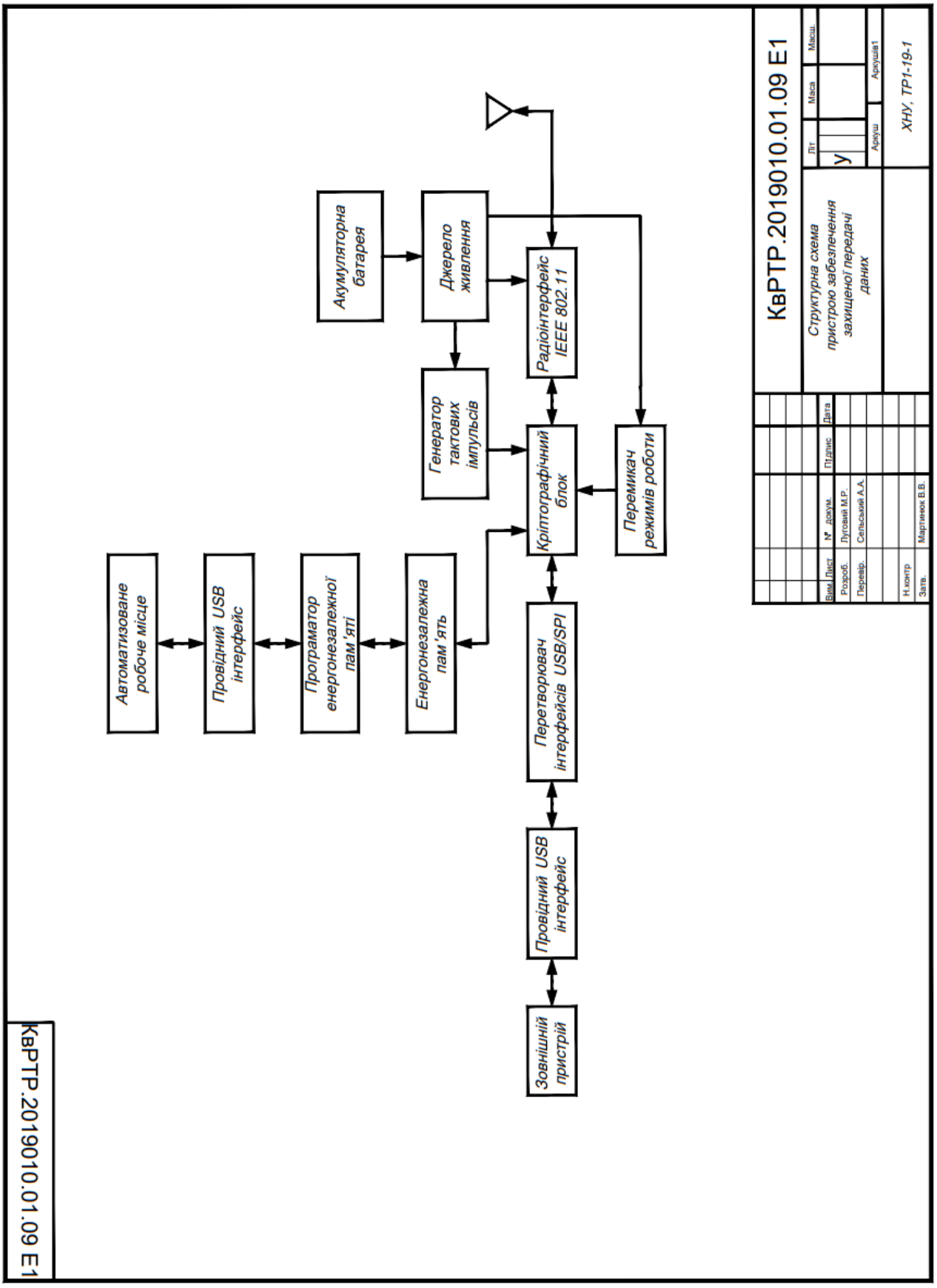
Додаток В

Алгоритм роботи пристрою забезпечення захищеної передачі даних



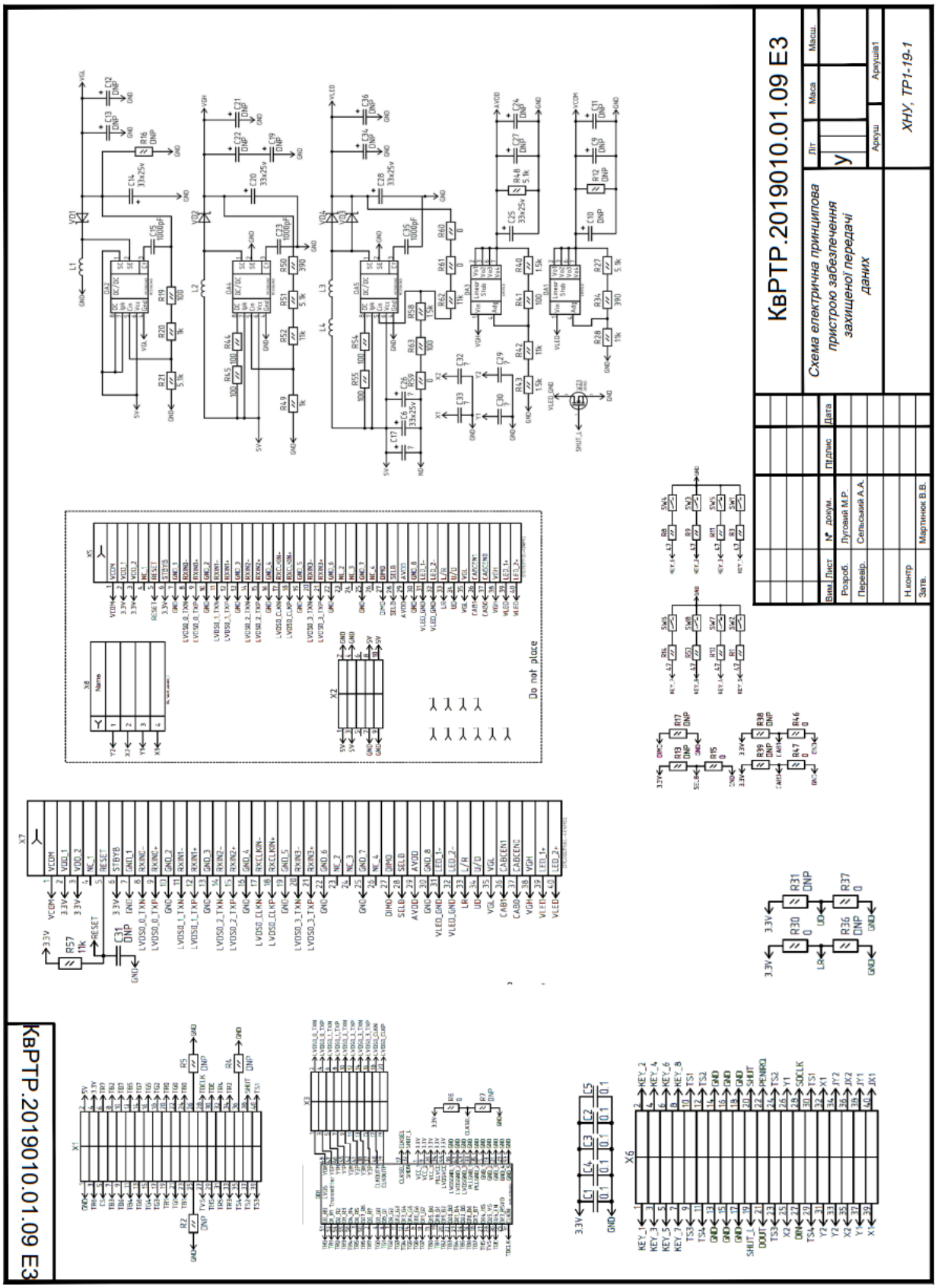
Додаток Г

Структурна схема пристрою забезпечення захищеної передачі даних



Додаток Д

Схема електрична принципова пристрою забезпечення захищеної передачі даних



UNICHECK

Ім'я користувача:
Кафедра АКІТіТК

ID перевірки:
1015575503

Дата перевірки:
13.06.2023 00:12:50 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
13.06.2023 01:16:32 EEST

ID користувача:
100005862

Назва документа: **Луговий**

Кількість сторінок: **59** Кількість слів: **12002** Кількість символів: **94846** Розмір файлу: **1.54 MB** ID файлу: **1015225937**

1107 слів позначені як "вилучені" та не враховуються у підрахунку слів

3.23%
Схожість

Найбільша схожість: **0.83%** з Інтернет-джерелом (https://pns.hneu.edu.ua/pluginfile.php/322000/mod_resource/content/.

2.85% Джерела з Інтернету	70	Сторінка 61
0.54% Джерела з Бібліотеки	7	Сторінка 61

0.07% Цитат

Цитати	3	Сторінка 62

Не знайдено жодних посилань

0.03%
Вилучень

Деякі джерела вилучено автоматично (фільтри вилучення: кількість знайдених слів є меншою за **8 слів** та **0%**)

Немає вилучених Інтернет-джерел

0.03% Вилученого тексту з Бібліотеки	6	Сторінка 62

Модифікації

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

Замінені символи	1

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 2.0%

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

	Документ		Сумарний збіг по Базі Даних	
ID: 115818 Назва: БКР Інфокомунікаційна система контролю та доступу Додано в БД: 2023-06-13 Автора: Максим ЛУГОВИЙ Керівники: Андрій СЕЛЬСЬКИЙ Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	84413	751	2043 (2%)	29 (4%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дипломник: Луговий Максим Русланович

Тема: Інфокомунікаційна система контролю та доступу

Спеціальність: 172 «Телекомунікації та радіотехніка»

Обсяг кваліфікаційної роботи:

Кількість листів креслень 3 Кількість сторінок записки 60

1. Короткий зміст роботи та прийнятих рішень: розроблено інфокомунікаційну систему контролю та доступу

2. Висновок про відповідність роботи дипломному завданню: Робота повністю відповідає поставленому завданню

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У першому розділі проаналізовано методи побудови систем контролю управління доступом. Розглянуті системи що базуються на аналізі руки людини, сітківки ока. Показано переваги та недоліки таких систем. У другому розділі наведено розробку інформаційно-комп'ютерної системи контролю та управління доступом. Проведена розробка архітектури СКУД. Виділено основні елементи СКУД. Виконана розробка програмної підсистеми. Також проведена розробка класів-сутностей. Зроблена розробка апаратної підсистеми. У третьому розділі реалізована програмна частина за архітектурою клієнт/сервер. Результатом розробки є розробка архітектури системи, структури та схеми електричних принципів обладнання контролю та управління доступом. Особливістю даної розробки є використання мікроконтролера SK-iMX53 в якості елемента керування пристроями контролю та контролю доступу. Тому пристрій має широкий набір функцій, а також високий рівень захисту даних, що передаються по мережі.

4. Позитивні сторони роботи: висока практична цінність роботи.

5. Негативні сторони роботи: у роботі наявні граматичні та стилістичні помилки

6. Оцінка графічного оформлення та пояснювальної записки роботи: Пояснювальна записка оформлена коректно, згідно діючих стандартів оформлення документації

7. Відгук про роботу в цілому: Робота виконана на належному науково-технічному рівні.

8. Інші зауваження: відсутні

9. Оцінка дипломної роботи: задовільно (3,50/D)

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) Клюх Юрій Павлович, к.т.н, доцент зав. кафедри кібербезпеки

"13" 06 2023 р. (підпис)

Завідувачу кафедри АКІТтаР
д-ру техн.наук, проф. Мартинюку В.В.

Луговий М.Р.

ПІБ здобувача вищої освіти

ФІТ, 4 курсу, групи ТР1-19-1

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 01.07.2022, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на наявність плагіату ознайомлений(а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

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

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

14.06.2023 _____

дата

_____

підпис

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ
КАФЕДРИ АВТОМАТИЗАЦІЇ, КОМП'ЮТЕРНО-ІНТЕГРОВАНИХ ТЕХНОЛОГІЙ ТА РОБОТОТЕХНІКИ
ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Інфокомунікаційна система контролю та доступу
Автор: Луговий Максим Русланович
Спеціальність: 172 Телекомунікації та радіотехніка
Освітня програма: Телекомунікації та інформаційно-комунікаційні технології
Науковий керівник: к.ф-м.н, доц. Сельський А.А.

Після аналізу звіту подібності зроблено такий висновок:

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

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) у тексті кваліфікаційної роботи системами перевірки на плагіат виявлено схожість з деякими документами в частині загальновживаних обов'язкових словосполучень у стандартних бланках (титулка, відомість документів), у структурі змісту, назвах розділів/підрозділів тощо, у назвах публікацій у переліку джерел посилання;

2) усі запозичення є фрагментарними або мають належним чином оформленні посилання;

3) виявлені модифікації тексту не впливають на відсоток схожості.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів ідентичності/ схожості, складає 3,23% і адресується до 77 джерел, що, з урахуванням наведених обґрунтувань, відповідає характеру теми і свідчить на користь кваліфікаційної роботи.

19.06.2025 р.

Завідувач кафедри _____ Валерій МАРТИНЮК

Гарант освітньої програми _____ Денис МАКАРИШКІН

Керівник кваліфікаційної роботи _____ Андрій СЕЛЬСЬКИЙ