# ВСТУП

Забезпечення безпеки, запобігання витоку інформації, і контроль ефективності роботи персоналу на підприємстві є одними з найбільш важливих і значних проблем на багатьох підприємствах, в наш час. Традиційні методи персональної ідентифікації, засновані на застосуванні паролів або матеріальних носіїв, таких як пропуск, паспорт, водійське посвідчення, не завжди відповідають сучасним вимогам безпеки. Рішенням проблеми точної ідентифікації особистості можливе застосування радіочастотних систем ідентифікації. Розвиток комп'ютерних технологій, поява нових матеріалів і математичних алгоритмів забезпечило можливість створення спеціалізованих пристроїв ідентифікації - радіочастотних зчитувачів, які і лежать в основі RFID систем ідентифікації. Дана технологія дозволяє отримувати інформацію про предмет без потреби прямого контакту. Дистанції, на яких може проходити зчитування і запис інформації можуть варіюватися від декількох міліметрів за кілька метрів, в залежності від застосовуваної технології. Самі радіочастотні мітки теж є дуже різними - розміром з кредитну карту, або зовсім крихітні імплантовані скляні мітки.

Радіочастотна ідентифікація має низку переваг у порівнянні з іншими технологіями ідентифікації. Найбільшою перевагою радіочастотної ідентифікації є, то що відстань, на яку може відбуватися отримання і запис ідентифікаційної інформації, варіюється до декількох десятків метрів.

В рамках поставленого завдання передбачається розробка інформаційно-комп'ютерної системи контролю та управління доступом до об'єктів. Призначення даної СКУД не настільки примітивно у порівнянні з багатьма існуючими - забезпечити не тільки автоматичну фільтрацію відвідувачів за ознакою - можна увійти / не можна, але і облік проведеного часу співробітником підприємства на своєму робочому місці. Автоматична фільтрація відвідувачів дозволяє контролювати ситуацію, безпеку персоналу

і збереження матеріальних цінностей та інформації, а також порядок на об'єкті. Облік проведеного часу на робочому місці - дозволити підвищити ефективність роботи персоналу підприємства, так як на основі даної статистики можна буде ввести систему штрафів і заохочень. Якість виконання цієї сукупності завдань залежить від виду СКУД, її функціональності і зручності роботи з самою системою. Дана комп'ютерна система повинна мати простий і наглядний інтерфейс, який буде зрозумілий будь-якому користувачеві.

# 1 АНАЛІЗ ІСНУЮЧИХ КОМП'ЮТЕРНИХ СИСТЕМ КОНТРОЛЮ І УПРАВЛІННЯ ДОСТУПОМ

Перш ніж почати аналіз існуючих комп'ютерних систем контролю і управління доступом (СКУД), необхідно дати визначення поняттю СКУД. Згідно ГОСТ 51241-2008 "Засоби і системи контролю і управління доступом. Класифікація. Загальні технічні вимоги. Методи випробувань ", СКУД - це сукупність засобів контролю та управління доступом, що володіють технічної, інформаційної, програмної та експлуатаційної сумісністю.

Засоби управління (ЗУ) - апаратні засоби (пристрої) і програмні засоби, що забезпечують установку режимів доступу, прийом і обробку інформації з зчитувачів, проведення ідентифікації і аутентифікації, управління виконавчими і перегороджуючими пристроями, відображення і реєстрація інформації.

Засоби контролю доступу в приміщення (кошти КУД) - механічні, електромеханічні пристрої і конструкції, електричні, електронні, електронні програмовані пристрої, програмні засоби, що забезпечують реалізацію контролю і управління доступом.

Пристрої, що перегороджують керування (ППК) - пристрої, що забезпечують фізичні перешкоди доступу і обладнані виконавчими пристроями для управління їх станом (турнікети, прохідні кабіни, двері і ворота, обладнані виконавчими пристроями СКУД).

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

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

Зчитувач - пристрій в складі ПВІО, призначене для зчитування (введення) ідентифікаційних ознак.

Ще одним важливим поняттям СКУД є ідентифікатор користувача - унікальна ознака суб'єкта або об'єкта доступу. В якості ідентифікатора може використовуватися запам'ятований код, біометричні ознаки або речовинний код. Ідентифікатор, що використовує дійсний код - предмет, в який (на який) за допомогою спеціальної технології занесена ідентифікаційна ознака у вигляді кодової інформації (карти, електронні ключі, брелки та ін. Пристрої).

## 1.1 Загальні принципи роботи систем контролю і управління доступом

Існують різні конфігурації систем контролю доступу в приміщення: найпростіші з них розраховані всього на одну вхідну дверь, а найскладніші призначені для контролю доступу на великих об'єктах - підприємствах, заводах і банках. При цьому найпростіший варіант СКУД вдає із себе звичайний домофон. Незалежно від конфігурації СКУД, кожна подібна система складається з декількох обов'язкових вузлів, це - контролери для управління, зчитувачі для ідентифікації, а також всілякі виконавчі пристрої обмеження доступу: турнікети, електромагнітні замки і защіпки. Електронні безконтактні карти в якості перепусток є найпоширенішим і зручним засобом ідентифікації в системах контролю доступу.

Працює система контролю і управління доступом в такий спосіб: на прохідній підприємства, при вході в відповідальні приміщення встановлюються засоби контролю доступу: електромеханічні турнікети, електромеханічні або електромагнітні замки, зчитувачі безконтактних карт. Всі ці пристрої підключаються до контролерів системи управління доступом. Контролери призначені для прийому і аналізу інформації про пропонованих картах доступу, а також для управління різними виконавчими пристроями. До складу обладнання системи контролю доступу можуть входити 2 типу контролерів: контролери замку і контролери турнікета, кожен з яких відповідає за контроль роботи власного вузла. Кожному співробітнику

підприємства видається персональний ідентифікатор, зазвичай цим виявляється безконтактна карта доступу - пластикова картка з унікальним електронним кодом (Proximity карта). Але можливо і застосування магнітних карт або т.зв. Touch memory пристроїв. Цей ідентифікатор одночасно є пропуском на прохідній організації і ключем від тих приміщень, куди співробітникові дозволений доступ. Для проходу через турнікет або входу в відповідальне приміщення працівники підприємства повинні піднести свою карту доступу до зчитувача, після чого зчитувач передає код пред'явленої карти в контролер, а контролер доступу приймає рішення про дозвіл або заборону проходу на підставі закладеної в нього інформації. У разі якщо доступ дозволений, система контролю доступу автоматично розблокує турнікет або замок на двері. Так, наприклад, контролер СКУД може бути запрограмований на пропуск конкретних співробітників в певні приміщення тільки в задані проміжки часу, скажімо, з 9 до 18 годин. До контролера СКУД також можна підключити охоронну сигналізацію, до складу якої входять охоронні датчики. Всі події, пов'язані з проходами через контрольні пункти фіксуються в пам'яті системи управління доступом і можуть використовуватися для автоматизованого обліку робочого часу, а також для отримання звітів по дисципліні праці або для можливих службових розслідувань на підприємстві.

## 1.2 Основні можливості системи контролю та управління доступом

За допомогою СКУД можна здійснювати контроль в'їзду автотранспорту на територію об'єкта, в цьому випадку після пред'явлення персонального ідентифікатора відбувається відкриття воріт або підйом шлагбаума.

Перерахуємо нижче основні можливості, які надає установка СКУД на об'єкті, що охороняється:

Контроль і управління доступом це основна функція системи. Як вже було відмічено раніше, за допомогою даної функції проводиться поділ прав доступу співробітників в певні приміщення, а також відмова в доступі небажаним особам. Крім того, можливе дистанційне керування блокувальними пристроями (замки, турнікети і пр.). СКУД дозволяє заборонити прохід для співробітників у святкові та вихідні дні, а також після закінчення робочого дня.

Збір і надання статистики. СКУД збирає інформацію про осіб, які пройшли через певні точки контролю доступу. По кожному співробітнику можливе отримання такої інформації: час входу та виходу, спроби доступу до заборонених для нього приміщення і зони, а також спроби проходу в недозволений час. Також можливо відстежити переміщення співробітника по території із зазначенням місця і часу. Таким чином, всі виявлені порушення трудової дисципліни можуть бути занесені до особової справи співробітника, а керівництво порушника повідомлено в робочому порядку. Крім того, виходячи з інформації, про останнє місце проходу, СКУД дозволяє визначити місцезнаходження співробітника в будь-який момент часу.

Доступ співробітника тільки за особистим ідентифікатором. При проході за допомогою ідентифікаційної карти на екрані монітора в пункті охорони може відображатися вся інформація по співробітникові і його фотографія, що виключає можливість проходу по чужому ідентифікатору. Також на рівні правил реакції СКУД можна забезпечити захист від передачі ідентифікатора іншій особі і блокувати повторний вхід на територію об'єкта з тієї ж самої карті доступу.

### 1.3 Ознайомлення з системою контролю і управління доступом

СКУД призначена для того, щоб забезпечувати санкціонований доступ в приміщення, що охороняються, контролювати його і запобігати несанкціоноване проникнення.

Основними завданнями СКУД є:

- обмеження доступу на задану територію;
- ідентифікація особи, яка має доступ на задану територію.

Додаткові завданнями СКУД:

- облік робочого часу;
- ведення бази персоналу / відвідувачі;
- інтеграція з системою безпеки.

Співробітники, які мають право проходити в об'єкт, що охороняється, можуть використовувати для цього різні ідентифікатори - клавіатури, на яких набирається код; безконтактні карти, з яких зчитується інформація про людину. Останнім часом стали частіше використовуватися біометричні ідентифікатори - райдужна оболонка, відбиток пальця, звуки голосу. Все це зчитується спеціальними пристроями і передається на контролер для ідентифікації. СКУД управляє також включенням / виключенням дверей, турнікетів, автоматичних шлагбаумів і шлюзових кабін.

### 1.3.1 Функції СКУД

СКУД забезпечує виконання таких функцій:

– ведення та підтримка баз даних користувачів і карт / ідентифікаторів;

– зберігання фотографій користувачів в базі даних;

– фіксація дати і часу проходу в базі даних;

– завдання рівнів доступу;

– автономна робота контролерів системи зі збереженням основних функцій управління при порушенні зв'язку з комп'ютером;

– реєстрація та зберігання інформації про події в незалежній пам'яті контролерів СКУД;

– збереження ідентифікаційних ознак в пам'яті системи при відмові і відключенні електроживлення;

– відкривання ППК (пристрій, прегороджуючий вхід (двері, турнікет, шлагбаум та ін.) При зчитуванні зареєстрованого в пам'яті системи ідентифікаційної ознаки;

– заборона відкривання ППК при зчитуванні незареєстрованої в пам'яті системи ідентифікаційної ознаки.

Програмне забезпечення:

– заборона відкривання ППК при зчитуванні незареєстрованої в пам'яті системи ідентифікаційної ознаки.

– Облік робочого часу.

– Контроль часу знаходження на об'єкті відвідувачів.

– Пошук співробітників на об'єкті.

– Реєстрація та протоколювання тривожних подій СКУД (відкриття дверей силою, утримання дверей відкритими, помилка рівня доступу та ін.).

- Управління роботою ППК в точках доступу по командам оператора (в тому числі блокування проходу в разі нападу).

### 1.3.2 Зміст СКУД

До складу СКУД входять наступні основні компоненти:

– ідентифікатор призначений для контролю доступу та визначення прав власника;

– турнікет;

– контролер;

– зчитувач;

– сервер СКУД;

– структурована мережа;

– робоче місце оператора;

– робоче місце адміністратора.

### 1.3.3 Структура СКУД

Склад системи контролю доступу наведено на рис. 1.1.

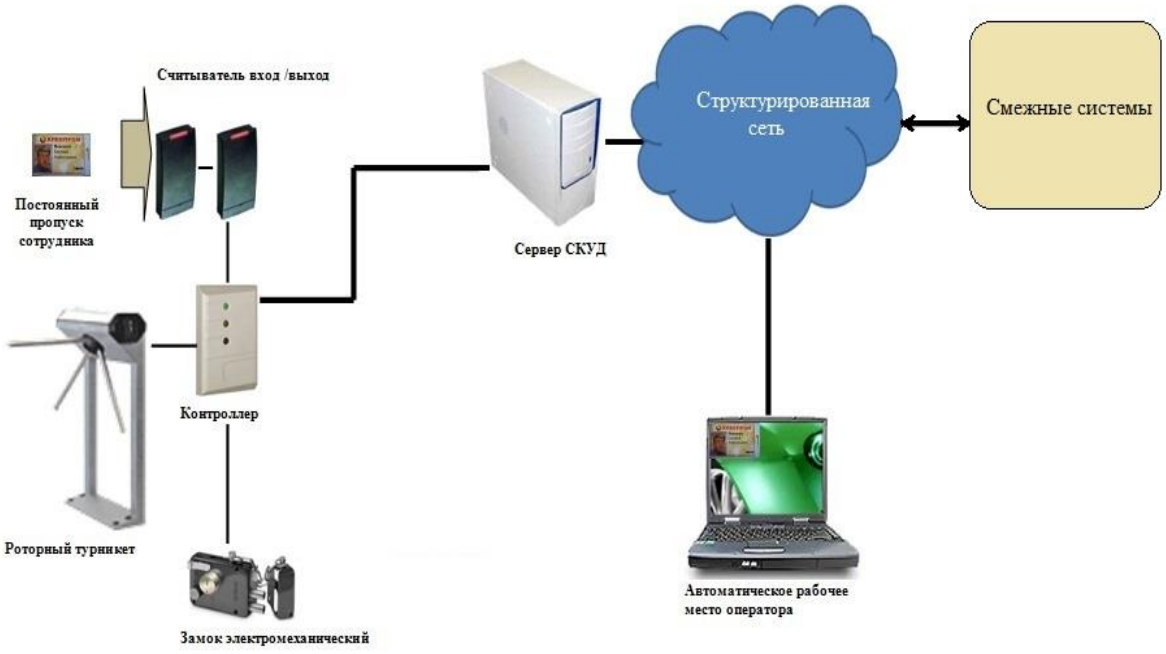



Рисунок 1.1 - Склад системи контролю доступу

## 1.4 Методи і засоби ідентифікації

### 1.4.1 Загальні відомості смарт-карт

Безконтактні пластикові картки є одним з основних елементів систем радіочастотної ідентифікації об'єктів (RFID - систем), які працюють на відстані від рідера (разом з чіпом у пластиковій картці розміщується антена, за допомогою якої проводиться прийом і випромінювання радіохвиль).

Читання і перезапис інформації на карті здійснюється за допомогою радіосигналу, переданого рідером і приймається індукційною котушкою карти. Основними перевагами безконтактних пластикових карт є:

– висока надійність і необмежений ресурс картки (забезпечується відсутністю необхідності механічного контакту між карткою і рідером);

– велика швидкість обміну інформацією між картою і рідером;

– можливість багаторазового використання (читання - необмежену кількість разів, перезапис - до 100 000 разів);

– висока надійність зберігання інформації (інформація на картці не піддається впливу зовнішніх полів і може зберігатися до 10 років);

– високий ступінь захисту від підробок (картку практично неможливо підробити);

– можливість багатофункціональності безконтактних пластикових карток (картки можуть нести великий обсяг перезаписуваної інформації і використовуватися одночасно для цілого ряду додатків).

Карти контролю доступу використовуються, щоб отримати фізичний доступ до будівель, кімнат, загороджений територій і т.п., а також для отримання логічного доступу до комп'ютерів або інформації, що міститься в комп'ютері.

Карти доступу в приміщення зазвичай використовують ті компанії, які хочуть обмежити доступ в приміщення, а також спостерігати за тим, хто відвідує певні приміщення. Службовцям компанії видаються смарт-карти, на яких записаний рівень доступу, визначений для кожного службовця. Картка містить фотографію, ім'я, номер власника (ID) і т.п., нанесені на поверхню карти. На картці можуть бути запрограмовані різні рівні безпеки.

### 1.4.2 Порівняльна характеристика методів ідентифікації

Технологія радіочастотної ідентифікації вже зайняла міцні позиції на ринку систем безпеки завдяки таким перевагам як пряма видимість радіочастотної мітки, висока швидкість читання міток, можливо практично одночасне читання великої кількості міток.

Виділяють такі нормативні документи і робочі частоти безконтактних карт:

– Низькочастотні proximity карти (125 кГц)

Низькочастотні RIFD-карти працюють на частоті 125 кГц. По суті, proximity карта - це дистанційний електронний пропуск з вбудованим мікрочіпом, що має унікальний ідентифікаційний код, який широко використовуються в системах контролю як фізичного, так і логічного доступу для безконтактної радіочастотної ідентифікації.

Обмін інформацією між картою і proximity зчитувачем здійснюється з відкритого протоколу.

Однак, низькочастотні RIFD-карти однаково ефективно працюють на відстані і з вуличними, і з кімнатними зчитувачами; не вимагають чіткого позиціонування об'єкта і мають низьку вартість.

– Високочастотні RFID-карти (13,56 МГц)

Високочастотні RIFD-карти - працюють на частоті 13,56 МГц. Серед виробників високочастотних карт доступу лідирують HID iCLASS SE і Seos, Mifare.

Завдяки більш широкій смузі пропускання, високочастотні RIFD-карти дозволяють забезпечити більший рівень безпеки і швидкодії. Карти доступу, що працюють на частоті 13,56 МГц, дозволяють реалізувати взаємну аутентифікацію між картою і зчитувачем, а також використовувати алгоритми шифрування даних. Порівняння цих технологій показані в табл. 1.1.

Обмін інформацією між картою і proximity зчитувачем здійснюється з відкритого протоколу, що робить проксіміті карти досить вразливими для зловмисників. Найбільш відповідною картою для СКУД є Mifare DESFire EV1.

Ключовими особливостями, через які, власне, вибір і був зупинений саме на цій карті, яка працює на частоті 13,56 MHz, тому що завдяки більш широкій смузі пропускання мають високу надійність і забезпечують швидке і надійне з'єднання, яке використовує алгоритми шифрування даних.

Таблиця 1.1 – Порівняння технологій з 125 кГц та 13,56 МГц частотами

| **Робоча частота** | 125 кГц | 13,56 МГц |
|---|---|---|
| **Наявність пам'яті** | нема | до 8 КВ |
| **Наявність криптографічного захисту** | нема | є |
| **Режим роботи** | тільки читання | читання-запис |
| **Дальність читання** | до 10 см | До 1 м |
| **Можливість програмування** | нема | є |
| **Захист від копіювання** | нема | є |
| **Типове застосування** | Найпростіші системи доступу | Складні системи доступу, системи локальної оплати |

Ще однією перевагою високочастотних RIFD-карт є наявність світового стандарту ISO14443, на відміну від низькочастотних карт доступу, що не підлягають стандартизації.

### 1.4.3 Опис зчитувача смарт-карт

Зчитувач смарт-карт (smart card reader) - це пристрій, призначений, власне, для зчитування інформації зі смарт-картки або для запису інформації на смарт-карту. Сфери застосування сучасних карт-рідерів дуже різноманітні. Зчитувачі використовують для всього спектра використання смарт-карт:

- для авторизації в операційній системі ПК;
- при організації систем контролю доступу;
- для оплати товарів і послуг;
- в програмах лояльності та ін.

Модельний ряд зчитувачів варіюється від вбудованих в клавіатуру комп'ютера до картрідерів для платіжних терміналів і вендінгових машин.

Для передачі даних і харчування може використовуватися як порт USB, так і інтерфейс PS / 2, RS-232, RS485 або безконтактний інтерфейс (GPRS, BlueTooth). Як джерело живлення смарт картрідера може використовуватися USB-шина або автономне джерело живлення. Пристрої читання смарт карт підтримують мікропроцесорні, кріптопроцесорні смарт- карти, а також всі типи карт пам'яті.

Зчитувачі карт поділяються на контактні і безконтактні. Зчитувач контактних смарт-карт - це найбільш поширений тип пристроїв для роботи зі смарт-картами. Зазвичай вони використовуються для ідентифікації та здійснення операцій, що вимагають високого рівня безпеки. Перевагою цього типу рідерів є висока швидкість передачі даних і висока ступінь захисту інформації. Обмін інформацією між картою і рідером здійснюється відповідно до міжнародних стандартів ISO 7816-1,2,3.

Зчитувач безконтактних смарт-карт обмінюється інформацією зі смарт-картою за допомогою радіосигналу. Такі пристрої (contactless card reader) призначені для читання смарт-карт на відстані за допомогою радіосигналу. Ці зчитувачі карт використовуються в системах СКУД.

На розгляд були взяті з використанням безконтактної технології зчитувачі карт, пристрої ST-PR040MF, ST-PR140MF і ST-PR140MK (рис. 1.2) з використанням для прийому коду карт технологію радіочастотної ідентифікації RFID (Radio Frequency Identification) які постійно випромінюють радіосигнал на частоті 13,56 МГц.


Рисунок 1.2 - RFID-зчитувачі карт

Коли Mifare карта потрапляє в поле дії зчитувача, в її приймальному контурі наводиться змінна напруга, достатня щоб ідентифікатор перейшов в активний режим роботи. При цьому передавач карти формує радіосигнал на тій же частоті, який модулюється унікальним кодом карти. Отриманий код RFID зчитувачі передають на контролер СКУД для звірки його з кодами в базі даних системи. При позитивній ідентифікації контролер видає санкцію на розблокування проходу для входу або виходу з приміщення, яке захищається. Технічні характеристики на RFID-зчитувачі карт Mifare приведені у табл. 1.2.

Таблиця 1.2 – Технічні характеристики на RFID-зчитувачі карт Mifare

| **Параметри** | **Значення** | | |
|---|---|---|---|
| Модель: | ST-PR040MF | ST-PR140MF | ST-PR140MK |
| Зчитувач: | Mifare, 13,56 МГц | | |
| Відстань зчитування: | 3 - 6 см | | |
| Клавіатура: | Нема | Нема | Посилка 8 біт |
| Інтерфейси: | Wiegand 34, вихід (серійний номер) | | |
| Електроживлення: | 10 - 14 В (пост. струм), не більше 40 мА | | |
| Діапазон робочих температур: | от -40 до +60 °С | | |
| Діапазон робочої вологості: | 10% - 99% | | |
| Габарити: | 134x58x26 мм | 128x82x28 мм | 128x82x28 мм |

В якості зчитувача для СКУД, найбільш підходящій був обраний зчитувач ST-PR040MF. Оскільки у нього відсутня двухфакторна ідентифікація, внаслідок чого є нижча ціна.

### 1.4.4 Загальні відомості про контролер СКУД

Контролер СКУД вважається «ядром» будь-якої системи контролю доступу. Це цифровий мікропроцесорний пристрій зазвичай діє таким чином:

– отримує інформацію зі зчитувача;

– обробляє дані, що надійшли;

– приймає рішення про допуск / заборону допуску на об'єкт;

– керує перешкоджаючими пристроями (відкриває або не відкриває двері).

Управління контролерами, так само як і обмін інформацією між усіма елементами СКУД, здійснюється за допомогою програмного забезпечення. Існує ПО для автономної роботи і для функціонування в складі комплексної системи безпеки. Крім охоронних функцій, програмне забезпечення дозволяє автоматизувати контроль трудової дисципліни, облік робочого часу, спростити роботу бюро перепусток і т.п.

За способом управління контролери СКУД діляться на три класи:

– Автономний контролер взаємодіє тільки з однією точкою доступу і розрахований на обслуговування невеликої кількості користувачів (до 500-600). Є закінченим пристроєм, незалежний від наявності центрального комп'ютера. Часто автономні контролери поєднуються зі зчитувачем, вбудовуються в електромагнітний замок.

– Мережевий контролер - працює в зв'язці з центральним комп'ютером, зі спеціальним програмним забезпеченням. В цьому випадку, рішення про допуск / заборону допуску на об'єкт приймає ПК. Такий тип контролерів застосовується для побудови масштабних систем контролю доступу з додатковими функціями, наприклад: облік робочого часу, контроль переміщення працівників по території підприємства і т.п.

– Універсальний (мережевий) контролер поєднує в собі функції двох попередніх типів. При наявності зв'язку з ПК він працює як мережевий, в разі, якщо зв'язок пропаде, діє як автономний.

На розгляд були взяті мережеві багатофункціональні контролери доступу ST-NC120 / 240/440 (рис.1.3).

Рисунок 1.3 - Контролер доступу

Технічні характеристики контролерів доступу ST-NC120 / 240/440 приведені у табл. 1.3.

Таблиця 1.3 – Технічні характеристики

| **Параметри** | **Значення** | | |
|---|---|---|---|
| Модель: | ST-NC120 | ST-NC240 | ST-NC440 |
| Кількість користувачів: | 30.000 | | |
| Рівні доступу: | 256 на пункт доступу | | |
| Двері: | 1 (вхід / вихід), 1 (вхід) | 2 (вхід / вихід), 2 (вхід) | 2 (вхід / вихід), 4 (вхід) |
| Зчитувачі СКУД: | 2 | 4 | 4 |
| Замки: | 1 | 2 | 4 |
| Датчики положення двері: | 1 | 2 | 4 |
| Інтерфейси зв'язку: | RS485, TCP/IP | | |
| Робоча температура: | від 0 до +55 ° С без конденсації | | |

Найбільш підходящим способом управління для СКУД був обраний мережевий контролер ST-NC120, тому що його функції повністю задовольняють потреби системи.

### 1.4.5 Структурована мережа

Найчастіше в локальних мережах використовуються два основні типи передачі даних між пристроями - по проводах, такі мережі називаються кабельними і використовують технологію Ethernet, також ще за допомогою радіосигналу по бездротових мережах, побудованих на базі стандарту IEEE 802.11, який більш відомий користувачам під назвою Wi -Fi.

Мережі влаштовані за принципом: пристрої (робочі станції), обладнані мережними адаптерами, з'єднуються між собою через спеціальні комутаційні пристрої, в якості яких виступає:

– Роутер - дозволяє об'єднувати декілька електронних пристроїв в єдину мережу.

– Комутатор служить для з'єднання між собою різних вузлів комп'ютерної мережі та обміну даними між ними по кабелях. В ролі цих вузлів можуть виступати як окремі пристрої, так вже і об'єднані в самостійний сегмент мережі цілі групи пристроїв.

## 1.5 Технічне завдання

**Найменування розробки**

Найменування розробки: "Система контролю і управління доступом на підприємстві"

**Призначення**

СКУД призначена для того, щоб забезпечувати санкціонований доступ в приміщення що охороняються, контролювати його і запобігати несанкціонованого проникнення.

СКУД забезпечує виконання таких функцій:

– ведення та підтримка баз даних користувачів і карт / ідентифікаторів;

– зберігання фотографій користувачів в базі даних;

– фіксація дати і часу проходу в базі даних;

– збереження ідентифікаційних ознак в пам'яті системи при відмові і відключенні електроживлення;

– відкривання ППК (двері, турнікет, шлагбаум та ін.) при зчитуванні зареєстрованої в пам'яті системи ідентифікаційної ознаки;

– заборона відкривання ППК при зчитуванні незареєстрованої в пам'яті системи ідентифікаційної ознаки.

**Вимоги до складу і параметрів технічних засобів**

До складу технічних засобів повинен входити персональний комп'ютер, що виконує роль сервера, що включає в себе:

– процесор Pentium-2.0Hz, не менше;

– оперативну пам'ять об'ємом, 1Гігабайт, не менше;

– HDD, 40 Гігабайт, не менше;

– операційну систему Windows 2000 Server або Windows 2003;

## Висновок до розділу 1

В розділі проведено аналіз існуючих комп'ютерних систем контролю і управління доступом

Визначено мету даної дипломної роботи - розробка системи контролю і управління доступом, що дозволяє запобігти несанкціонованому доступу до об'єктів підприємства, а також, що дозволяє зберегти і потім переглянути інформацію про події в системі за певний проміжок часу.

Сформовано технічне завдання на розробку. Визначені оснеовні вимоги до складу та виконуваних функцій системи.

Для досягнення поставленої мети був обраний RFID метод ідентифікації користувача. Цей метод був обраний за рахунок низьких матеріальних витрат на побудову системи, а також зіграла роль відносна звичність даного методу ідентифікації для рядового користувача.

# 2 РЕАЛІЗАЦІЯ БАЗИ ДАНИХ

## 2.1 Вибір СУБД

Вибір системи управління баз даних (СУБД) являє собою складну задачу і є одним з важливих етапів при розробці додатків баз даних. Обраний програмний продукт повинен задовольняти як поточним, так і майбутнім потребам, при цьому слід враховувати фінансові витрати на придбання необхідного обладнання, самої системи, розробку необхідного програмного забезпечення на її основі, а також навчання персоналу. Крім того, необхідно переконатися, що нова СУБД здатна принести реальні вигоди.

З переліку вимог до СУБД можна виділити кілька груп критеріїв:

- моделювання даних;
- продуктивність;
- контроль роботи системи;
- надійність;
- особливості розробки додатків;
- особливості архітектури і функціональні можливості;
- вимоги до робочого середовища.

У табл. 2.1 наведені основні переваги і недоліки трьох найбільш популярних СУБД - PostgreSQL, MySQL і MS Access. Кожна база даних має свої особливості і відмінності. Оскільки для розроблюваної системи необхідно швидке сховище для простих запитів з мінімальною налаштуванням, то в якості СУБД для зберігання даних буде використовуватися СУБД MS Access. Основними критеріями, що висуваються до інформаційної БД є:

- зручний користувальницький інтерфейс, який дозволяє мати доступ до будь-якої інформації, а також оперативно змінювати інформацію в БД;
- простота і зручність в створенні бази даних і подальшій роботі з нею;

– зручне відображення результатів пошуку потрібної інформації;

Таблиця 2.1 - Переваги та недоліки різних СУБД

| СУБД | MySQL | PostgreSQL | MS Access |
|---|---|---|---|
| **Переваги** | -швидкодія; - безпека і надійність; - отсутств. високих вимог до апаратних ресурсів; - переносимість. | - підтримка БД практично необмеженого розміру; - потужні і надійні механізми транзакцій і реплікації; - успадкування; - легка розширюваність. | -повністю сумісний з операційною системою Windows,; - дуже простий графічний інтерфейс, який дозволяє не тільки створювати власну базу даних, але і розробляти програми, використовуючи вбудовані засоби. |
| **Недоліки** | - відсутність транзакцій і тригерів; - відсутні збережені процедури і вкладені запити; - немає підтримки інструкції UNION; - відсутність каскадного оновлення даних. | - відносна складність інсталяції; - невірна робота оточення PostgreSQL; - відсутність повної підтримки мов програмування VB і C #; - відсутність Intellisense при програмується. | - питаннях підтримки цілісності даних відповідає тільки моделям БД невеликої та середньої складності; - У ранніх версіях (до Access 2003) відсутні такі кошти як тригери і процедури. |

Перш ніж почати створювати будь-яку базу даних, треба чітко визначити наступне:

– як БД буде використовуватися;

– призначення бази даних;

– які відомості в цій базі даних будуть зберігатися, тобто треба виявити мета створення бази даних.

У БД що розробляється в цій роботі будуть міститися наступні відомості:

– про групу (назва);

– про користувачів (П.І.Б., адреса, телефон, фото, паспортні дані, дата народження);

– про перехід (час проведений, перехід з, перехід в, індикатор вдалого переходу, час входу, час виходу з приміщення).

Оскільки створюється реляційна БД, то виділення об'єктів предметної області - це один з важливих етапів проектування БД. Процес виділення інформаційних об'єктів предметної області може здійснюватися двома підходами: аналітичним і інтуїтивним.

Аналітичний підхід - спочатку визначаються основні завдання, для вирішення яких будується база, виявляються сукупність даних і різних відомостей про об'єкти і процеси, що характеризують дану область, перелік документів, що містять ці дані. Основним джерелом даних є довідкові, планові і оперативно - облікові документи, і, визначивши склад і структуру інформаційного об'єкта, створюємо зв'язку між ними.

Інтуїтивний підхід - відразу встановлюються типові об'єкти предметної області та їх взаємозв'язку.

Найбільш раціонально - це поєднання обох підходів, тому що на початковому етапі, як правило, немає повних відомостей про всі завдання.

Далі виконується інформаційний аналіз, який включає в себе:

– структурування інформації предметної області, тобто її уявлення окремими структурними одиницями - реквізитами і їх розміщення в джерелах - документах (структурні одиниці інформації - реквізити);

– формалізація і моделювання даних, для їх організації та обробки.

Проектування БД починається зі збору інформації про всі об'єкти предметної області. Відомо, що об'єкт має безліч реалізацій - примірників об'єкта. Кожен екземпляр об'єкта повинен однозначно визначатися серед усієї множини екземплярів, тобто ідентифікуватися значенням унікального (первинного) ключа інформаційного об'єкта. Знаємо, що унікальність ключа означає, що будь-яке значення ключа не може повторитися в будь-якому

іншому екземплярі об'єкта. Знаємо, що кожному об'єкту в моделі даних предметної області треба привласнити унікальне ім'я.

При побудові моделі даних в канонічному вигляді сукупність реквізитів об'єктів повинна відповідати вимогам нормалізації.

Реквізити кожного об'єкта канонічної моделі повинні відповідати вимогам, відповідним третій нормальній формі реляційної моделі даних:

– об'єкт повинен містити унікальний ідентифікатор - ключ;

– між описовими реквізитами не повинно бути функціональних залежностей;

– всі реквізити, що входять в складовою ключ, повинні бути взаємонезалежні;

– кожен описовий реквізит повинен залежати від ключа не транзитивній, тобто повинен бути незалежним через інший проміжний реквізит.

Виконання вимог нормалізації забезпечує побудова реляційної БД без дублювання даних і можливість підтримки цілісності при внесенні змін.

## 2.2 Розробка класів-сутностей

Аналізуючи мету створення БД системи контролю та управління доступом, є можливість відразу виділити об'єкт «system user», який матиме такі характеристики, наведені в таблиці 2.2. Ця сутність зберігає інформацію про співробітників, кому дозволений доступ до СКУД.

Таблиця 2.2 - Опис таблиці «system user»

| Назва колонки | Тип даних | Обмеження | Опис |
|---|---|---|---|
| userType | Текстовий | not null | |
| login | Текстовий | not null | Первинний ключ, логін оператора |
| PasswordHashe | Поле MEMO | not null | Пароль хешування |
| PasswordSalt | Поле MEMO | not null | Рядок даних, яки передається хеш-функції разом з паролем |

Дані цього об'єкта відповідають вимогам нормалізації:

– має унікальний ідентифікатор - ключ;

– між описовими реквізитами немає функціональної залежності;

– кожен описовий реквізит функціонально залежить від ключа.

Тобто в отриманих об'єктах все описові реквізити логічно пов'язані.

Також, в проектовану БД необхідно ввести ще шість об'єктів: «Dismissed staff», «event log», «staff», «schedule», «user types», «Тип мітки» описані в таблицях 2.3-2.8.

«Dismissed staff» Дана сутність зберігає персональні дані кожного колишнього працівника компанії, такі як П.І.Б., дата народження або посаду.

Ця сутність необхідна, так як, перш ніж пустити співробітника в приміщення, необхідно знати, чи має він на це право. Характеристики цієї сутності неведені у таблиці 2.3.

Таблиця 2.3 - Опис таблиці «Dismissed staff»

| Назва колонки | Тип даних | Обмеження | Опис |
|---|---|---|---|
| Номер паспорта | Числовий | not null | Первинний ключ, унікальний ідентифікатор рівня доступу. |
| Фамилия | Текстовий | not null | Прізвище співробітника |
| Имя | Текстовий | not null | Ім'я співробітника |
| Отчество | Текстовий | not null | По батькові |
| Дата увольнения | Дата/Час | not null | Дата звільнення співробітника |

«event log» - дана сутність зберігає дані входу / виходу кожного працівника компанії. Характеристики цієї сутності неведені у таблиці 2.4.

Таблиця 2.4 - Опис таблиці «event log»

| Назва колонки | Тип даних | Обмеження | Опис |
|---|---|---|---|
| Uid | Текстовий | not null | Ідентифікатор співробітника |
| EnterTime | Дата/час | not null | Первинний ключ, час входу |
| ExitTime | Дата/час | not null | Час виходу |

«schedule» - дана сутність зберігає робочий графік співробітника.

Характеристики цієї сутності неведені у таблиці 2.5.

Таблиця 2.5 - Опис таблиці «schedule»

| Назва колонки | Тип даних | Обмеження | Опис |
|---|---|---|---|
| Графік | Текстовий | not null | Первинний ключ, графік робочого часу |
| Начало інтервалу | Дата/час | not null | Начало робочого графіку співробітника |
| Кінець інтервалу | Дата/час | not null | Кінець робочого графіку співробітника |

«staff» - Сутність буде створено для обмеження дозволу доступу тому чи іншому співробітнику. Характеристики цієї сутності неведені у табл. 2.6.

Таблиця 2.6 - Опис таблиці «staff»

| Назва колонки | Тип даних | Обмеження | Опис |
|---|---|---|---|
| Співробітник | Текстовий | not null | Повне ім’я співробітника |
| Посада | Текстовий | not null | Посада співробітника |
| UID | Текстовий | not null | Ідентифікатор співробітника |
| Фото | Поле MEMO | not null | Фотографія співробітника |
| Табельний номер | Лічильник | not null | Первинний ключ, номер співробітника |
| Номер паспорту | Числовий | not null | Унікальний ідентифікатор рівня доступу. |
| Дата найму | Дата/час | not null | Дата найму співробітника |
| Графік | Текстовий | not null | Графік робочого часу |
| Заблокований | Логічний | not null | Блокування співробітника |
| Підрозділ | Текстовий | not null | Підрозділ співробітника |
| Тип UID | Текстовий | not null | Термін дії пропуску |

«user types» - сутність зберігає інформацію про тип співробітників. Характеристики цієї сутності неведені у таблиці 2.7.

Таблиця 2.7 - Опис таблиці «user types»

| Назва колонки | Тип даних | Обмеження | Опис |
|---|---|---|---|
| userType | Текстовий | not null | Первинний ключ, тип співробітників |

«Тип мітки» - сутність вказує на те, скільки днів допуску надається співробітнику. Характеристики цієї сутності неведені у таблиці 2.8.

Таблиця 2.8 - Опис таблиці «Тип мітки»

| Назва колонки | Тип даних | Обмеження | Опис |
|---|---|---|---|
| Код | Лічильник | not null | Первинний ключ |
| Тип метки | Текстовий | not null | скільки часу допуску надається співробітнику |
| Термін дії (доба) | Числовий | not null | Термін дії |
| | | | |

Таблиця 2.9 - Зв'язки об'єктів предметної області

| Головний об'єкт | Підлеглий об'єкт | Тип зв'язку | Ключ зв'язку |
|---|---|---|---|
| Staff | EventLog | M:M | UID |
| Staff | UIDList | 1:M | UID |
| Тип мети | Staff | 1:M | Тип метки |
| Schedule | Staff | 1:M | График |
| SystemUser | UserTypes | M:1 | userType |
| UIDList | Тип метки | 1:M | Код |

Загальна схема бази даних приведена на рисунку 2.1.

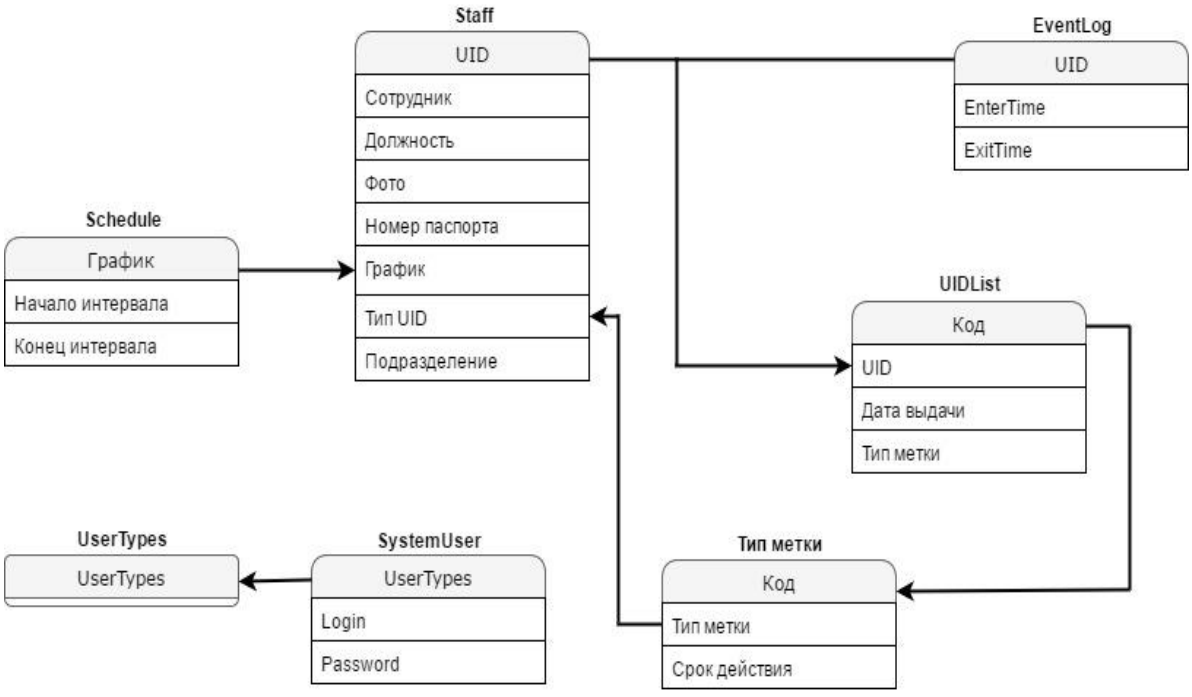



Рисунок 2.1 - Загальна схема бази даних

## 2.1 Розробка архітектури СКУД

Перш ніж приступити до розробки СКУД потрібно ознайомитися з класифікацією архітектур даних систем і прийняти вірне рішення щодо вибору архітектури, грунтуючись на вимогах до системи.

### 2.1.1 Типи архітектури СКУД

За типом архітектури СКУД класифікуються наступним чином:

- автономні;
- мережеві.

Автономні СКУД (рис. 2.2) припускають установку на об'єкті одного або безлічі незалежних контролерів, кожен з яких забезпечує функції контролю і управління доступом в певному локальному місці. У таких СКУД немає центрального контролера - сервер системи. При цьому настройку кожного контролера потрібно робити окремо. У зв'язку з тим, що контролери зазвичай встановлюються в важкодоступних місцях і, беручи до уваги можливу кількість дверей і співробітників на підприємстві, стає ясно, що такий підхід застосовується лише для невеликих об'єктів.


Рисунок 2.2 - Структура автономної СКУД

На відміну від автономних, мережеві СКУД (рис. 2.3) містять у своїй структурі центральний контролер - сервер системи, з яким пов'язані вже всі локальні контролери. Таким чином, для побудови мережевий СКУД потрібна прокладка кабельних трас, що забезпечують зв'язок контролерів. Але при використанні для зв'язку контролерів мережевого інтерфейсу Ethernet є можливість задіяти для цих завдань існуючу на об'єкті комп'ютерну мережу.

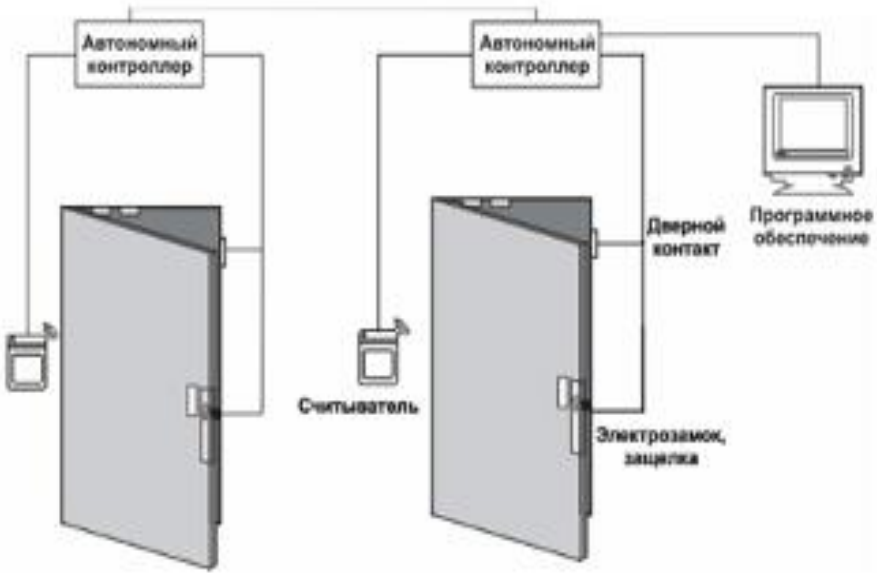



Рисунок 2.3 - Структура мережевої СКУД

Переваги мережевих СКУД:

можливість швидко реагувати і управляти всією системою: дистанційно розблокувати вибрані турнікети або двері, редагувати повноваження доступу співробітників і т.д.;

– можливість централізованого огляду всіх подій;

– можливість застосовувати систему обліку робочого часу;

– можливість захисту від недобросовісних співробітників, які намагаються пройти удвох по одному пропуску.

Доцільно застосувати мережеву архітектуру побудови СКУД. Так як, в ній більше можливостей.

Архітектура комп'ютерної системи контролю та управління доступом до об'єктів

Всі дані які розробляються СКУД (дані про всі проходах через УПУ - час, дата, П.І.Б. та посада користувача) повинні зберігатися в одному місці, тобто в одній базі даних. З вищесказаного можна зробити висновок, що найбільш відповідною архітектурою для розроблюваної системи буде архітектура клієнт-сервер (рис. 2.4).


Рисунок 2.4 - Архітектура клієнт-сервер

Архітектура клієнт-сервер - це архітектура розподіленої обчислювальної системи, в якій додаток ділиться на клієнтський і серверний процеси.

Ядром системи, побудованої на основі архітектури клієнт-сервер, є сервер баз даних, що представляє собою додаток, що здійснює комплекс дій по управлінню даними - виконання запитів, зберігання і резервне копіювання даних, відстеження посилальної цілісності, перевірку прав і привілеїв користувачів і т.д. При цьому в якості робочого місця може бути використаний звичайний персональний комп'ютер, що дозволяє не відмовлятися від звичної робочої середовища.

На основі аналізу існуючих рішень, була розроблена власна архітектура комп'ютерної системи контролю та управління доступом (СКУД), яка складається з двох частин - програмної і апаратної підсистем.

В якості ідентифікатора, вирішено було використовувати RFID ідентифікацію, тому що витрати на побудову системи на основі такого

методу істотно нижче ніж при використанні будь-якого іншого методу ідентифікації. Також, RFID ідентифікація є відносно звичної для людини.

Загальна архітектура інформаційно-комп'ютерної системи контролю та управління доступом до об'єктів представлена на рис. 2.5.

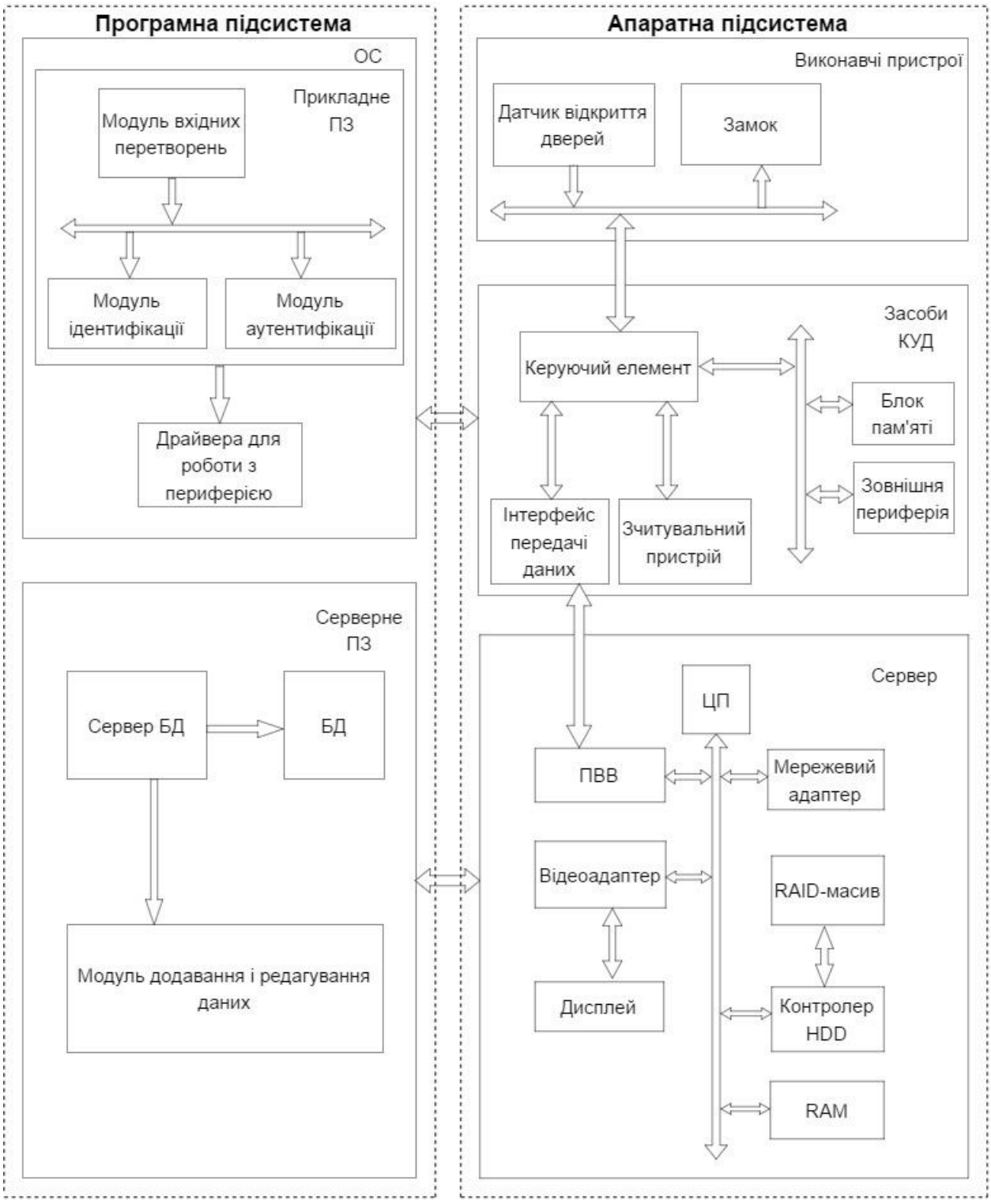



Рисунок 2.5 - Архітектура комп'ютерної системи контролю та управління доступом до об'єктів

## Висновок до розділу 2

На основі аналізу існуючих рішень, була розроблена власна архітектура комп'ютерної системи контролю та управління доступом (СКУД), яка складається з програмної системи.

Програмна система складається з серверної частини, яка відповідає безпосередньо за контроль і управління доступом і ОС Windows.

Серверна частина складається з сервера бази даних. Що відповідає за контроль і управління доступом. Клієнт виконує ідентифікацію та аутентифікацію користувачів.

Серверна частина програмної системи складається з комп’ютера на якому находиться база даних.

# 3 РОЗРОБКА ПРОГРАМНОЇ ПІДСИСТЕМИ

## 3.1 Варіанти використання системи

Відповідно до технічного завдання, програмна система повинна забезпечити функціонування згідно з діаграмами варіантів використання системи контролю та управління доступом до об'єктів, розробку структури бази даних, розробку інтерфейсу.

Загальна діаграма класів інформаційно-комп'ютерної системи контролю та управління доступом представлена на рисунку 3.1.

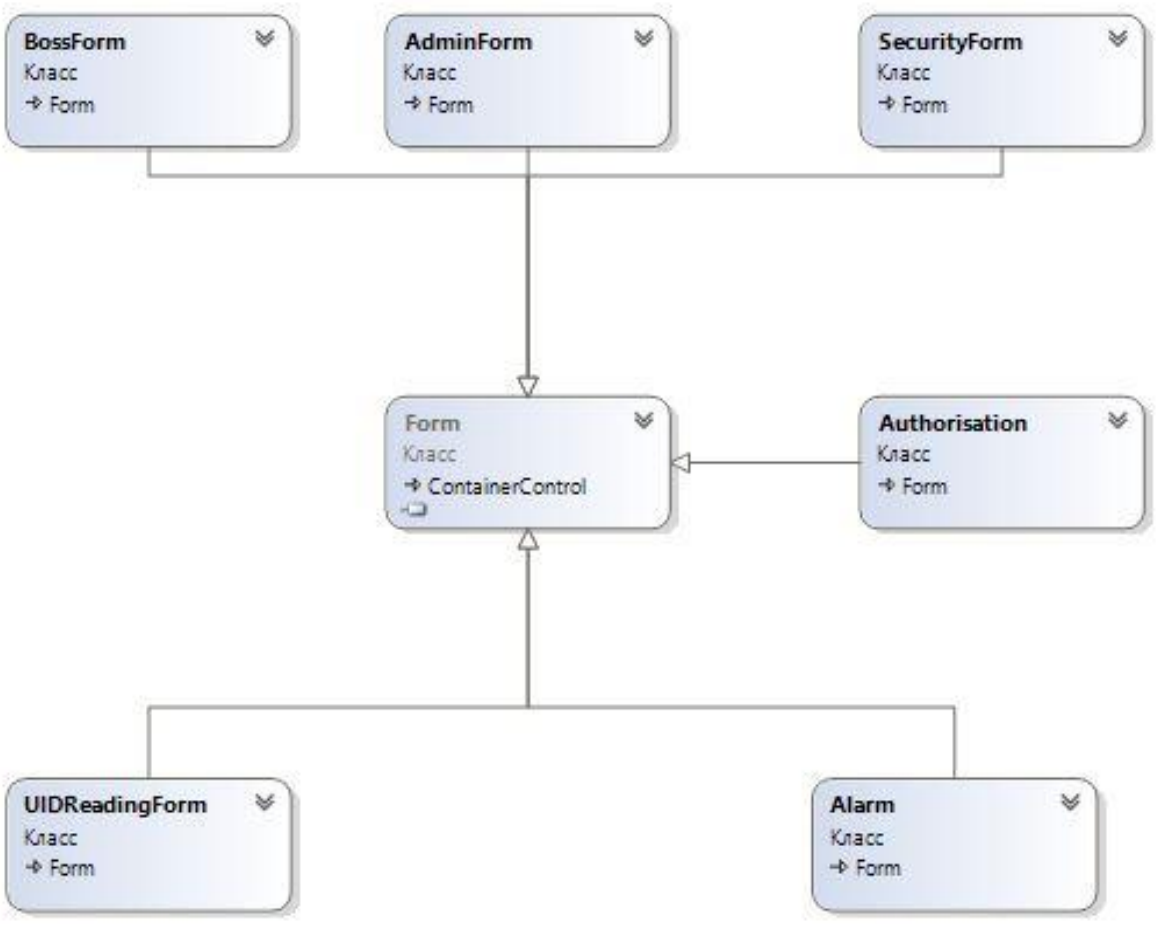



Рисунок 3.1 – Загальна діаграма класів

Діаграми варіантів використання системи контролю та управління доступом до об'єктів

Система контролю і управління доступом призначена для автоматичного управління входом / виходом людей в будівлі і приміщення.

З даною системою можуть працювати оператор і користувачі. Для кожного з них надаються свої права в системі.

Користувачеві (співробітнику підприємства) доступні дві дії (рис. 3.2) - ідентифікація (процес пізнання суб'єкта за ідентифікаційним ознакою) і аутентифікація (процес пізнання суб'єкта шляхом порівняння введених ідентифікаційних даних).

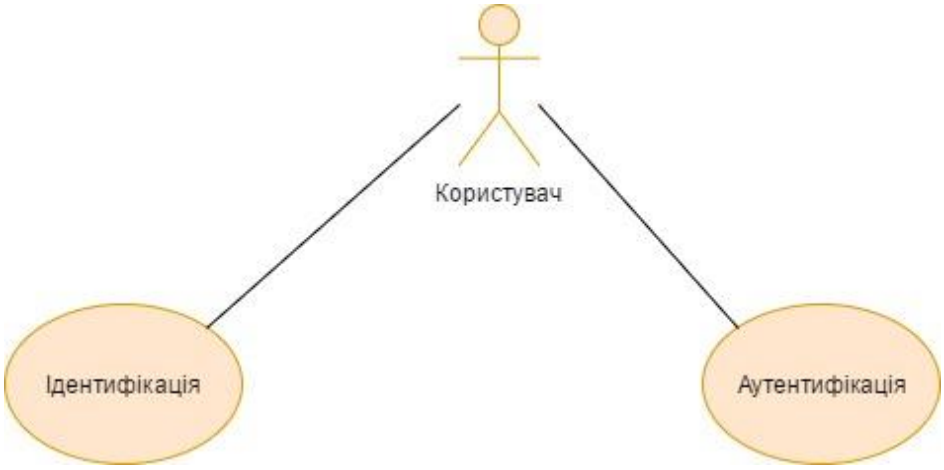



Рисунок 3.2 - Діаграма варіантів використання системи для користувача

Всі користувачі, які володіють правом доступу до охоронюваного об'єкту, попередньо повинні пройти ідентифікацію, повинен бути створений ID-номер який ідентифікує користувача. Потім, коли користувач хоче отримати доступ до об'єкту, що охороняється, він проходить аутентифікацію, тобто підносить пристрій, що зберігає ID-номер до зчитувального пристрою. Якщо id номера на сервері збігає і на пристрої збігаються, то користувач отримує доступ до об'єкту (на сервер відправляється повідомлення про санкціонованому доступі), в іншому випадку - в доступі буде відмовлено, і на сервер буде відправлено повідомлення про несанкціоновану спробі отримання доступу до об'єкта.

Оператор має доступ до налаштування і управління обладнанням, перегляду поточних подій системи, управління списком об'єктів доступу, перегляду архіву, а також отримання звітів (рис. 3.3).


Рисунок 3.3 - Діаграма варіантів використання системи для оператора

Перегляд журналу подій (рис. 3.4) полягає в тому, що оператор може бачити повну інформацію про співробітників, та відслідкувати час входу та виходу співробітників у приміщення.


Рисунок 3.4 - Діаграма варіантів використання перегляду журналу подій

Для створення програмного забезпечення під мікроконтролер існують різні мови програмування, але, мабуть, найбільш придатними є асемблер і Сі, оскільки в цих мовах в найкращій мірі реалізовані всі необхідні можливості по управлінню апаратними засобами мікроконтролерів.

### 3.2 Вибір засобів програмування

Асемблер - це низькорівнева мова програмування, що використовує безпосередній набір інструкцій мікроконтролера. Створення програми на цій мові вимагає хорошого знання системи команд програмованого чіпа і достатнього часу на розробку програми. Асемблер програє *C* в швидкості і зручності розробки програм, але має помітні переваги в розмірі кінцевого виконуваного коду, а відповідно, і швидкості його виконання.

*C* дозволяє створювати програми з набагато більшим комфортом, надаючи розробнику всі переваги мови високого рівня. Компіляція вихідних текстів, написаних на *C*, здійснюється швидко і дає компактний, ефективний код.

Основні переваги С перед ассемблером:

– висока швидкість розробки програм;

– універсальність, яка не потребує досконального вивчення архітектури мікроконтролера;

– наявність бібліотек функцій;

– підтримка обчислень з плаваючою точкою.

У мові *C* гармонійно поєднуються можливості програмування низького рівня з властивостями мови високого рівня. Можливість низькорівневого програмування дозволяє легко оперувати безпосередньо апаратними засобами, а властивості мови високого рівня дозволяють створювати зрозумілий і модифікований програмний код. Крім того, практично всі компілятори *C* мають можливість використовувати асемблерні вставки для написання критичних за часом виконання і займаним ресурсів ділянок програми.

Проаналізувавши основні особливості мов програмування *C* та асемблера, вибір був зупинений на *C* .

Для розробки серверної частини було прийнято рішення використовувати мову високого рівня, а саме об'єктно-орієнтована мова

програмування. На розгляд було запропоновано мову програмування, що задовольняють умови (об'єктно-орієнтовані, з синтаксисом, успадкованим від *C*):

*C*#, Розроблено групою інженерів під керівництвом Андерса Хейлсберг в компанії Microsoft як мова розробки додатків для платформи Microsoft.NET Framework.

Для створення інтерфейсу буде використовуватися бібліотека Windows Forms - це інтерфейс програмування додатків (API), що відповідає за графічний інтерфейс користувача і є частиною Microsoft .NET Framework. Даний інтерфейс спрощує доступ до елементів інтерфейсу Microsoft Windows за рахунок створення обгортки для існуючого Win32 API в керованому коді. Причому керований код - класи, що реалізують API для Windows Forms, що не залежать від мови розробки. Тобто програміст однаково може використовувати Windows Forms як при написанні ПЗ на C #, C ++, так і на VB.Net, J # і ін.

### 3.3 Алгоритми обліку доступу до приміщень

При розробці системи було реалізовано декілька алгоритмів. В цій частині роботи будуть розглянуті кілька алгоритмів основного призначення системи, а саме алгоритми обліку доступу в приміщення.

Спочатку розглянемо алгоритм обліку входу в приміщення. При здійсненні входу в приміщення, система створює об'єкт класу «перехід» і в локальну змінну заносяться дані з картки, а саме Id користувача, які зчитуються пристроєм читання. Далі проводиться пошук даного користувача в системі по його ID, якщо користувач не знайдений, то в поля класу «перехід» заносяться дані булевого типу «false», а в поле «reason» - «nu» (No User), після чого відбувається завершення методу і повернення false. В іншому випадку, тобто у разі якщо користувач з наявними ID присутній в

системі відбувається запис в поля класу «toRoom» заносяться відповідні дані -Номер кімнати, в яку здійснюємо перехід, «timeIn»-час входження в кімнату. Після чого система перевіряє чи має право співробітник увійти в дане приміщення, якщо працівник не володіє таким правом, то система заносить в поля класу «Authorisation.Designer» дані булевого типу «false», а в поле «reason» - «na» (No Access) і завершує метод з поверненням false. У разі позитивного результату перевірки система заносить дані в поля «Authorisation.Designer» булевого типу «true», а в поле «reason» - «ok» (і завершує метод повертаючи true.

Другий алгоритм, який буде представлений нижче, забезпечує облік виходу з приміщення. При здійсненні виходу система здійснює пошук вже вчиненого входу в кімнату, необхідним співробітником. У разі повернення результату null методом пошуку, метод виходу завершується повертаючи false. В іншому випадку в поля об'єкта (об'єкт передається методом findTransition) знайденої транзакції заносяться дані, а саме в поле timeout заноситься час виходу а в поле «spendtime» вводиться число часу проведене в приміщенні.

### 3.4 Авторизація та розробка користувачів системи

Для авторизації користувачів я вибрав класичну рольову модель управління доступом, для доступу в особистий кабінет передбачається три ролі це адміністратор, охоронець і начальник, в залежності від ролі користувач отримує доступ до відповідного функціоналу особистого кабінету.

Після запуску програми користувач потрапляє в форму авторизації, в якій він вводить ім’я користувача та пароль, як показано на рисунку 3.5.


Рисунок 3.5 – Авторизація користувача

**Адміністратор.** Даний розділ доступний тільки адміністраторам, тут міститься основна інформація про систему та список співробітників (рисунок 3.6).

В функції адміністратора входять:

– Додавання співробітника;

– Редагування співробітника;

– Видалення співробітника;

– Блокування співробітника;

– Перегляд журналу пропуску;

– Редагування користувачів системи.

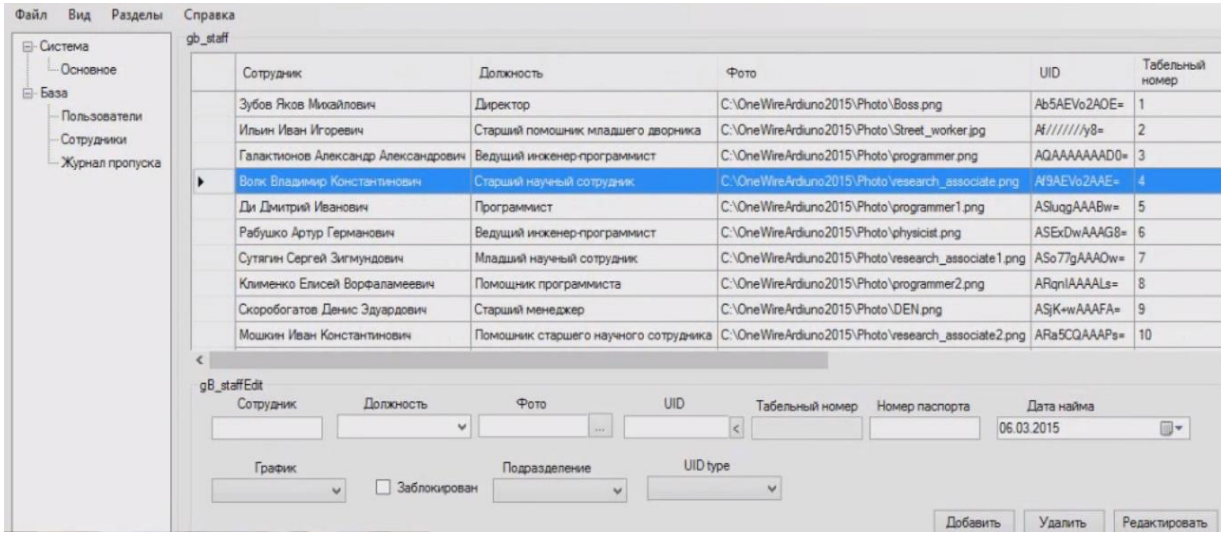



Рисунок 3.6 – Розділ адміністратора

**Охоронець.** Користувач охоронець має функцію перегляду співробітників які проходять через систему контроля. Для запобігання входу через чужу картку, охоронець звіряє власника картки з співробітником який нею користується. На рисунку 3.7 представлена форма програми роботи охоронця.


Рисунок 3.7 – Форма програми роботи охоронця

**Начальник.** В функції начальника входить перегляд журналу пропуску співробітників. Він також може обирати за який час показувати співробітників які не проходили до роботи.

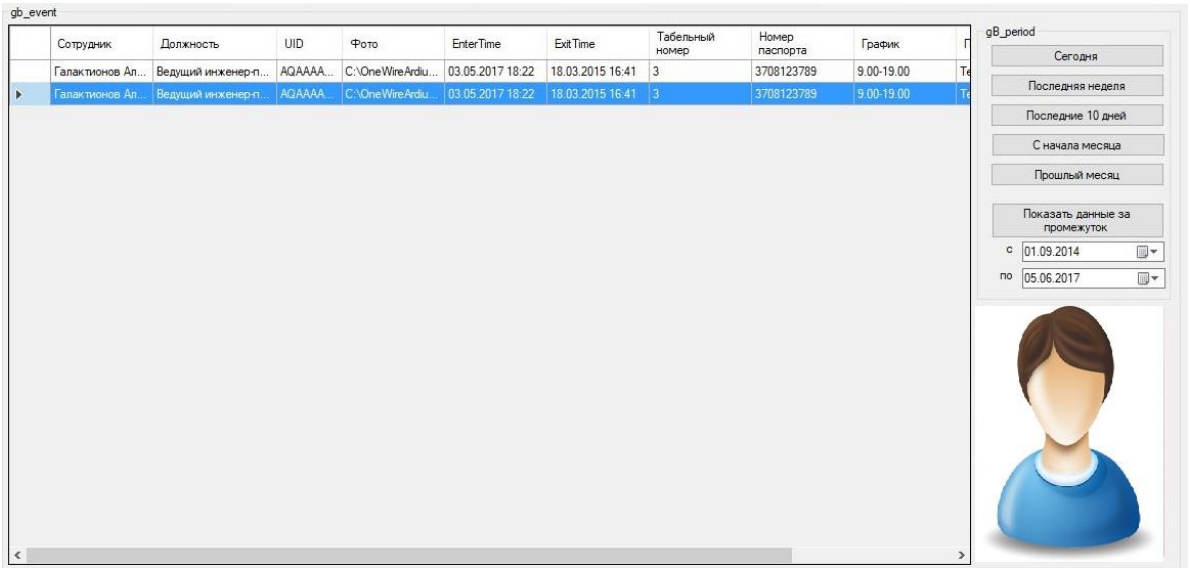



Рисунок 3.8 – Форма програми роботи начальника

Основуючись на ці рішення, були розроблені форми користувачів комп'ютерної системи контролю та управління доступом (СКУД).

## Висновок до розділу 3

Проаналізувавши засоби програмування було вирішено використовувати бібліотеку Windows.Forms.

При розробці системи були реалізовані алгоритми обліку доступу в приміщення, а також форми авторизації та користувачі системи.

# 4 ОХОРОНА ПРАЦІ

Охорона праці – це система законодавчих актів і відповідних їм технічних, гігієнічних, соціально-економічних і організаційних заходів, що забезпечують безпеку в процесі праці.

В даному розділі проведено аналіз потенційних небезпечних та шкідливих виробничих факторів, причин пожеж. Розглянуті заходи, які дозволяють забезпечити гігієну праці і виробничу санітарію. На підставі аналізу розроблені заходи з техніки безпеки та рекомендації з пожежної профілактики.

Завданням даної роботи бакалавра було доступ і облік робочого часу співробітників на підприємство, і як результат було створено СКУД. В подальшому розроблятиметься реальна система, яка значно полегшить процес

доступу та обліку робочого часу співробітників на підприємстві. Так як в процесі проектування використовувалося програмне забезпечення, то аналіз потенційно небезпечних і шкідливих виробничих чинників виконується для персонального комп'ютера на якому буде використовуватися розроблена СКУД.

## 4.1 Загальні питання з охорони праці

Умови праці на робочому місці, безпека технологічних процесів, машин, механізмів, устаткування та інших засобів виробництва, стан засобів колективного та індивідуального захисту, що використовуються працівником, а також санітарно-побутові умови повинні відповідати вимогам нормативних актів про охорону праці. В законі України «Про охорону праці» визначається, що охорона праці - це система правових, соціально-економічних, організаційно- технічних, санітарно-гігієнічних і лікувально-

профілактичних заходів та засобів, спрямованих на збереження життя, здоров'я і працездатності людини у процесі трудової діяльності. При роботі з обчислювальною технікою змінюються фізичні і хімічні фактори навколишнього середовища: виникає статична електрика, електромагнітне випромінювання, змінюється температура і вологість, рівень вміст кисню і озону в повітрі. Роботодавець повинен впроваджувати сучасні засоби техніки безпеки, які запобігають 44 виробничому травматизмові, і забезпечувати санітарно-гігієнічні умови, що запобігають виникненню професійних захворювань працівників. Він не має права вимагати від працівника виконання роботи, поєднаної з явною небезпекою для життя, а також в умовах, що не відповідають законодавству про охорону праці. Працівник має право відмовитися від дорученої роботи, якщо створилася виробнича ситуація, небезпечна для його життя чи здоров'я або людей, які його оточують, і навколишнього середовища.

На законодавчому рівні визначено такі пріоритетні напрямки з безпеки праці:

– кожен працівник несе безпосередню відповідальність за порушення зазначених Законом, нормами і правилами вимог;

– напрямки реалізації конституційного права громадян на їх життя і здоров’я в процесі трудової діяльності;

– пріоритет життя і здоров’я працівників по відношенню до результатів виробничої діяльності підприємства;

– повна відповідальність роботодавця за створення належних – безпечних і здорових умов праці;

– соціальний захист працівників, повне відшкодування збитків особам, які потерпіли від нещасних випадків на виробництві та професійних захворювань;

– комплексне розв’язання завдань охорони праці;

– підвищення рівня промислової безпеки шляхом забезпечення суцільного технічного контролю за станом виробництв, технологій та

продукції, а також сприяння підприємствам у створенні безпечних та нешкідливих умов праці;

– соціальний захист працівників, повне відшкодування збитків особам, які потерпіли від нещасних випадків на виробництві та професійних захворювань;

– використання економічних методів управління охороною праці, участь держави у фінансуванні заходів щодо охорони праці;

– використання світового досвіду організації роботи щодо поліпшення умов і підвищення безпеки праці на основі міжнародної співпраці.

## 4.2 Аналіз стану умов праці

Робота над створенням СКУД проходитиме в приміщенні підприємства. Для даної роботи достатньо однієї людини, для якої надано робоче місце зі стаціонарним комп’ютером.

### 4.2.1 Вимоги до організації місця праці

При порівнянні відповідності характеристик робочого місця нормативним основні вимоги до організації робочого місця за [ДСанПіН 3.3.2.007-98 «Правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин»] (табл. 4.1) і відповідними фактичними значеннями для робочого місця, констатуємо повну відповідність.

Найбільшому ризику виникнення різноманітних порушень піддаються: органи зору, м’язово скелетна система, нервово-психічна діяльність, репродуктивна функція у жінок. Тобто наявне психофізіологічні небезпечні та шкідливі фактори: а) фізичного перевантаження: 50 - статичного; - динамічного; б) нервово-психічного перевантаження: - розумового

перенапруження; - монотонності праці; - перенапруження аналізаторів; - емоційних перевантажень. Рекомендовано застосування екранних фільтрів, локальних світлофільтрів (засобів індивідуального захисту очей) та інших засобів захисту, а також інші профілактичні заходи на ведені в [ДСанПіН 3.3.2.007-98]. Роботу за дипломним проектом визнано, таку, що займає 50% часу робочого дня та за восьмигодинної робочої зміни рекомендовано встановити додаткові регламентовані перерви: (потрібне вибрати): - для розробників програм тривалістю 15 хв через кожну годину роботи; - для операторів персональних комп'ютерів тривалістю 15 хв через дві години роботи; - для операторів комп'ютерного набору тривалістю 10 хв через кожну годину роботи.

Таблиця 4.1 - Характеристики робочого місця

| **Найменування параметра** | **Фактичне значення** | **Нормативне значення** |
|---|---|---|
| Висота робочої поверхні, мм | 750 | 680 ÷800 |
| Висота простору для ніг, мм | 730 | не менше 600 |
| Ширина простору для ніг, мм | 660 | не менше 500 |
| Глибина простору для ніг, мм | 700 | не менше 650 |
| Висота поверхні сидіння, мм | 470 | 400 ÷500 |
| Ширина сидіння, мм | 400 | не менше 400 |
| Глибина сидіння, мм | 400 | не менше 400 |
| Висота поверхні спинки, мм | 600 | не менше 300 |

Продовження таблиці 4.1

| | | |
|---|---|---|
| Ширина опорної поверхні спинки, мм | 500 | не менше 380 |
| Радіус кривини спинки в горизонтальній площині, мм | 400 | 400 |
| Відстань від очей до екрану дисплея, мм | 800 | 700 ÷800 |

### 4.3 Виробнича санітарія

На підставі аналізу небезпечних та шкідливих факторів при виробництві (експлуатації), пожежної безпеки можуть бути надалі вирішені питання необхідності забезпечення працюючих достатньою кількістю освітлення, вентиляції повітря, організації заземлення, тощо.

#### 4.3.1 Пожежна безпека

Небезпека розвитку пожежі на обчислювальному центрі обумовлюється застосуванням розгалужених систем електроживлення ЕОМ, вентиляції і кондиціювання,. Небезпека загоряння пов'язана з особливістю комп'ютерів - із значною кількістю щільно розташованих на монтажній 53 платі і блоках електронних вузлів і схем, електричних і комутаційних кабелів, резисторів, конденсаторів, напівпровідникових діодів і транзисторів. Надійна робота окремих елементів і мікросхем в цілому забезпечується тільки в певних інтервалах температури, вологості і при заданих електричних параметрах. При відхиленні реальних умов експлуатації від розрахункових можуть виникнути пожежонебезпечні ситуації.

Для гасіння пожеж в офісному приміщенні пропонується використовувати порошкові або вуглекислотні вогнегасники, так як вони є універсальними. Заземлені конструкції, що знаходяться в приміщеннях, де розміщені робочі місця (батареї опалення, водопровідні труби, кабелі із заземленим відкритим екраном), надійно захищені діелектричними щитками та/або сітками з метою недопущення потрапляння працівника під напругу. Дане приміщення оснащено системою автоматичної пожежної сигналізації, має 1 вогнегасник ВП-5 із зарядом вогнегасної речовини 8-12 кг, відповідно до вимог чинного законодавства України. Проходи до засобів пожежогасіння вільні, не захаращуються та у разі потреби забезпечувати евакуацію всіх людей, які перебувають у приміщенні через один евакуаційний вихід з дверима на шляху евакуації, що відчинятися в напрямку виходу з будівлі від робочого місця. В приміщенні наявна затверджена «План-схема евакуації з кабінету (приміщення)».

Пожежна безпека при застосуванні ЕОМ забезпечується:

1) системою запобігання пожежі;

2) системою протипожежного захисту;

3) організаційно-технічними заходами.

Запобігти утворенню горючого середовища (замінити горючі речовини і матеріали на негорючі і важкогорючі) не надається технічно можливим. Тому проектом передбачаються способи і засоби запобігання утворення (або внесення) в горюче середовище джерел запалювання, таких як:

1) застосування електроустаткування, відповідної пожежонебезпечної і вибухонебезпечної зонам відповідно до ПУЕ;

2) застосування в конструкції швидкодійних засобів захисного відключення можливих джерел запалення;

3) виключення можливості появи іскрового розряду в горючому середовищі з енергією, рівної і вище мінімальної енергії запалення.

### 4.3.2 Електробезпека

На робочому місці виконуються наступні вимоги електробезпеки: ПК, периферійні пристрої та устаткування для обслуговування, електропроводи і кабелі за виконанням та ступенем захисту відповідають класу зони за ПУЕ (правила улаштування електроустановок), мають апаратуру захисту від струму короткого замикання та інших аварійних режимів. Лінія електромережі для живлення ПК, периферійних пристроїв і устаткування для обслуговування, виконана як окрема групова три- провідна мережа, шляхом прокладання фазового, нульового робочого та нульового захисного провідників. Нульовий захисний провідник використовується для заземлення (занулення) електроприймачів. Штепсельні з'єднання та електророзетки крім контактів фазового та нульового робочого провідників мають спеціальні контакти для підключення нульового захисного провідника. Електромережа штепсельних розеток для живлення персональних ПК, укладено по підлозі поруч зі стінами відповідно до затвердженого плану розміщення обладнання та технічних характеристик обладнання. Металеві труби та гнучкі металеві рукави заземлені. Захисне заземлення включає в себе заземлюючих пристроїв і провідник, який з'єднує заземлюючий пристрій з обладнанням, яке заземлюється - заземлюючий провідник.

## 4.4 Гігієнічні вимоги до параметрів виробничого середовища

### 4.4.1 Мікроклімат

Мікроклімат робочих приміщень – це клімат внутрішнього середовища цих приміщень, що визначається діючої на організм людини з'єднанням температури, вологості, швидкості переміщення повітря. В даному приміщенні проводяться роботи, що виконуються сидячи і не потребують динамічного фізичного напруження, то для нього відповідає категорія робіт Іа. Отже оптимальні значення для температури, відносної вологості й

рухливості повітря для зазначеного робочого місця відповідають [ДСН 3.3.6.042-99 «Санітарні норми мікроклімату виробничих приміщень»] і наведені в табл. 4.2:

Таблиця А.4 – Норми мікроклімату робочої зони об’єкту

| **Період року** | **Категорія робіт** | **Температура °С** | **Відносна вологість %** | **Швидкість руху повітря, м/с** |
|---|---|---|---|---|
| Холодна | легка-1 а | 22 - 24 | 40 – 60 | 0,1 |
| Тепла | легка-1 а | 23 - 25 | 40 – 60 | 0,1 |

Дане приміщення обладнане системами опалення, кондиціонування повітря або припливно- витяжною вентиляцією. У приміщенні на робочому місці забезпечуються оптимальні значення параметрів мікроклімату: температури, відносної вологості й рухливості повітря у відповідності до [ДСН 3.3.6.042-99]. Рівні позитивних і негативних іонів у повітрі мають відповідати [ДСН 3.3.6.042-99]. Для забезпечення оптимальних параметрів мікроклімату в приміщенні проводяться перерви в роботі співробітників, з метою його провітрювання. Існують спеціальні системи кондиціонування, які забезпечують підтримання в приміщенні балансу оптимальних параметрів 57 мікроклімату. Контроль параметрів мікроклімату в холодний і теплий період року здійснюється не менше 3-х разів на зміну (на початку, середині, в кінці).

### 4.4.2 Освітлення

Світло є природною умовою існування людини. Воно впливає на стан вищих психічних функцій і фізіологічні процеси в організмі. Хороше освітлення діє тонізуюче, створює гарний настрій, покращує протікання основних процесів вищої нервової діяльності. Збільшення освітленості

сприяє поліпшенню працездатності навіть в тих випадках, коли процес праці практично не залежить від зорового сприйняття. При поганому освітленні людина швидко втомлюється, працює менш продуктивно, виникає потенційна небезпека помилкових дій і нещасних випадків.

Працюючі на ПЕОМ не повинні бачити відображення світильників на екрані. Застосовувати місцеве освітлення при роботі на ПЕОМ не рекомендується. Природне освітлення, коли робочі місця з ПЕОМ розташовуються в один ряд по довжині приміщення на відстані 0,8 - 1,0 м від стіни з віконними прорізами, і екрани знаходяться перпендикулярно цієї стіни. Основний потік природного світла при цій повинен бути зліва. Не допускається спрямування основного світлового потоку природного світла праворуч, ззаду і 58 спереду працює на ПЕОМ. Оптимальна відстань очей до екрана відео монітора повинна становити 60-70 см, допустиме не менше 50 см. Розглядати інформацію ближче 50 см не рекомендується.

*Розрахунок освітлення.*

Для виробничих та адміністративних приміщень світловий коефіцієнт приймається не менше -1/8, в побутових – 1/10:

$$S_b = \left(\frac{1}{5} \div \frac{1}{10}\right) \cdot S_n , \tag{4.1}$$

де $S_b$ – площа віконних прорізів, м2;

$S_n$ – площа підлоги, $м^2$;

$S_n = a \cdot b = 5 \cdot 5 = 25\ м^2$;

$S = 1/8 \cdot 25 = 3{,}125\ м^2$;

Приймаємо 2 вікна площею S=1,6 м 2 кожне;

Світильники загального освітлення розташовуються над робочими поверхнями в рівномірно-прямокутному порядку. Для організації освітлення в темний час доби передбачається обладнати приміщення, довжина якого складає 5 м, ширина 5 м, світильниками ЛПО2П, оснащеними лампами типа ЛБ (дві по 80 Вт) з світловим потоком 5400 лм кожна.

Розрахунок штучного освітлення виробляється по коефіцієнтах використання світлового потоку, яким визначається потік, необхідний для створення заданої освітленості при загальному рівномірному освітленні. Розрахунок кількості світильників n виробляється по формулі (А.2):

$$n = \frac{E \cdot \mathrm{S} \cdot \mathrm{Z} \cdot \mathrm{K}}{F \cdot \mathrm{U} \cdot \mathrm{M}}, \tag{4.2}$$

де Е – нормована освітленість робочої поверхні, визначається нормами – 300 лк;

S – освітлювана площа, $\mathrm{м}^2$ ; S = 25 м2;

Z – поправочний коефіцієнт світильника (Z = 1,15 для ламп розжарювання та ДРЛ; Z = 1,1 для люмінесцентних ламп) приймаємо рівним 1,1;

K – коефіцієнт запасу, що враховує зниження освітленості в процесі експлуатації – 1,5;

U – коефіцієнт використання, залежний від типу світильника, показника індексу приміщення і т.п. – 0,575;

M – число люмінесцентних ламп в світильнику – 2;

F – світловий потік лампи – 5400лм (для ЛБ-80).

Підставивши числові значення у формулу (А.2), отримуємо:

$$n = \frac{300 \cdot 25 \cdot 1{,}1 \cdot 1{,}5}{5400 \cdot 0{,}575 \cdot 2} \approx 2{,}0$$

Приймаємо освітлювальну установку, яка складається з 2-х світильників, які складаються з двох люмінесцентних ламп загальною потужністю 160 Вт, напругою – 220 В.

### 4.5 Заходи з організації виробничого середовища та попередження виникнення надзвичайних ситуацій

Відповідно до санітарно-гігієнічних нормативів та правил експлуатації обладнання наводимо приклади деяких заходів безпеки.

1) Заходи безпеки під час експлуатації персонального комп'ютера та периферійних пристроїв передбачають:

- правильне організування місця праці та дотримання оптимальних режимів праці та відпочинку під час роботи з ПК;

- експлуатацію сертифікованого обладнання;

- дотримання заходів електробезпеки;

- забезпечення оптимальних параметрів мікроклімату;

- забезпечення раціонального освітлення місця праці (освітленість робочого місця не перевищувала 2/3 нормальної освітленості приміщення);

- облаштовуючи приміщення для роботи з ПК, потрібно передбачити припливно-витяжну вентиляцію або кондиціювання повітря:

а) якщо об'єм приміщення 20 м3 , то потрібно подати не менш як 30 м3 /год повітря;

б) якщо об'єм приміщення у межах від 20 до 40 м3 , то потрібно подати не менш як 20 м3 /год повітря;

в) якщо об'єм приміщення становить понад 40 м3 , допускається природна вентиляція, у випадку, коли немає виділення шкідливих речовин.

- зниження рівня шуму та вібрації:

а) у джерелі виникнення, шляхом застосування раціональних конструкцій, нових матеріалів і технологічних процесів;

б) звукоізолювання устаткування за допомогою глушників, резонаторів, кожухів, захисних конструкцій, оздоблення стін, стелі, підлоги тощо;

в) використання засобів індивідуального захисту).

**Розрахунок захисного заземлення (забезпечення електробезпеки будівлі).**

Згідно з класифікацією приміщень за ступенем небезпеки ураження електричним струмом [НПАОП 40.1-1.01-97], приміщення в якому проводяться всі роботи відноситься до першого класу (без підвищеної небезпеки). Під час роботи використовуються електроустановки з напругою живлення 36 В, 220 В, та 360 В. Опір контура заземлення повинен мати не більше 4 Ом.

Послідовність розрахунку.

1) Визначається необхідний опір штучних заземлювачів $R_{\text{шт.з.}}$:

$$\mathrm{R_{шт.з.}} = \frac{\mathrm{R_д} \cdot \mathrm{R_{пр.з}}}{\mathrm{R_{пр.з}} - \mathrm{R_д}}, \tag{4.3}$$

де $R_{\text{пр.з}}$ – опір природних заземлювачів; $R_{\text{д}}$ – допустимий опір заземлення. Якщо природні заземлювачі відсутні, то $R_{\text{шт.з.}} = R_{\text{д}}$.

Підставивши числові значення у формулу (А.3), отримуємо:

$$R_{\text{шт.з.}} = \frac{4 \cdot 40}{40 - 4} \approx 4 \text{ Ом}$$

2) Опір заземлення в значній мірі залежить від питомого опору ґрунту ρ, Ом·м. Приблизне значення питомого опору глини приймаємо ρ=40 Ом•м (табличне значення).

3) Розрахунковий питомий опір ґрунту, $\rho_{розр.}$, Ом·м, визначається відповідно для вертикальних заземлювачів $\rho_{розр.в}$, і горизонтальних $\rho_{розр.г}$, Ом·м за формулою:

$$\rho_{розр.} = \psi \cdot \rho, \tag{4.4}$$

де $\psi$ – коефіцієнт сезонності для вертикальних заземлювачів I кліматичної зони з нормальною вологістю землі, приймається для вертикальних заземлювачів $\rho_{розр.в}$=1,7 і горизонтальних $\rho_{розр.г}$=5,5 Ом·м.

$$\rho_{розр.в} = 1{,}7 \cdot 40 = 68 \text{ Ом} \cdot \text{м}$$

$$\rho_{розр.г} = 5{,}5 \cdot 40 = 220 \text{ Ом} \cdot \text{м}$$

4) Розраховується опір розтікання струму вертикального заземлювача Rв, Ом, за (А.5).

$$R_в = \frac{\rho_{розр.в}}{2 \cdot \pi \cdot l_в} \cdot \left( \ln \frac{2 \cdot l_в}{d_{ст}} + \frac{1}{2} \cdot \ln \frac{4 \cdot t + l_в}{4 \cdot t - l_в} \right), \tag{4.5}$$

де $l_в$ – довжина вертикального заземлювача (для труб - 2−3 м; $l_в$=3 м);

$d_{ст}$ – діаметр стержня (для труб - 0,03−0,05 м; $d_{ст}$=0,05 м);

t – відстань від поверхні землі до середини заземлювача, яка визначається за ф. (А.6):

$$t = h_в + \frac{l_в}{2}, \tag{4.6}$$

де $h_в$– глибина закладання вертикальних заземлювачів (0,8 м); тоді

$$t = 0{,}8 + \frac{3}{2} = 2{,}3 \text{ м}$$

$$R_{в} = \frac{68}{2 \cdot \pi \cdot 3} \cdot \left( \ln \frac{2 \cdot 3}{0{,}05} + \frac{1}{2} \cdot \ln \frac{4 \cdot 2{,}3 + 3}{4 \cdot 2{,}3 - 3} \right) = 18{,}5 \text{ Ом}$$

5) Визначається теоретична кількість вертикальних заземлювачів n штук, без урахування

коефіцієнта використання $\eta_{в}$:

$$n = \frac{2 \cdot R_{в}}{R_{д}} = \frac{2 \cdot 18{,}5}{4} = 9{,}25 \tag{4.7}$$

І визначається коефіцієнт використання вертикальних електродів групового заземлювача без врахування впливу з'єднувальної стрічки $\eta_{в}$ =0,57 (табличне значення).

6) Визначається необхідна кількість вертикальних заземлювачів з урахуванням коефіцієнта

використання $n_{в}$, шт:

$$n_{в} = \frac{2 \cdot R_{в}}{R \cdot \eta_{в}} = \frac{2 \cdot 18{,}5}{4 \cdot 0{,}57} = 16{,}2 \approx 16 \tag{4.8}$$

7) Визначається довжина з'єднувальної стрічки горизонтального заземлювача $l_{с}$, м:

$$l_{с} = 1{,}05 \cdot L_{в} \cdot (n_{в} - 1), \tag{4.9}$$

де $L_в$ – відстань між вертикальними заземлювачами, (прийняти за $L_в$= 3м);

$n_в$ – необхідна кількість вертикальних заземлювачів.

$$l_с = 1{,}05 \cdot 3 \cdot (16 - 1) \approx 48 \text{ м}$$

8) Визначається опір розтіканню струму горизонтального заземлювача (з'єднувальної

стрічки) $R_г$, Ом:

$$R_г = \frac{\rho_{розр.г}}{2 \cdot \pi \cdot l_с} \cdot \ln \frac{2 \cdot l_с^2}{d_{см} \cdot h_г}, \quad (4.10)$$

де $d_{см}$ – еквівалентний діаметр смуги шириною b, $d_{см}$ =0,95b, b = 0,15 м;

$h_г$ – глибина закладання горизантальних заземлювачів (0,5 м);

$l_с$ - довжина з'єднувальної стрічки горизонтального заземлювача $l_с$, м

$$R_г = \frac{220}{2 \cdot \pi \cdot 48} \cdot \ln \frac{2 \cdot 48^2}{0{,}95 \cdot 0{,}15 \cdot 0{,}5} = 8{,}1 \text{ Ом}$$

9) Визначається коефіцієнт використання горизонтального заземлювача $\eta_{с.}$ відповідно до необхідної кількості вертикальних заземлювачів $n_{в.}$

Коефіцієнт використання з'єднувальної смуги $\eta_{с.}$=0,3 (табличне значення).

10) Розраховується результуючий опір заземлювального електроду з урахуванням з'єднувальної смуги:

$$R_{заг} = \frac{R_в \cdot R_г}{R_в \cdot \eta_{с.} + R_г \cdot n_{в.} \cdot \eta_в} \leq R_д \quad (4.11)$$

Висновок: дане захисне заземлення буде забезпечувати електробезпеку будівлі, так як виконується умова: $R_{заг}$ <4 Ом, а саме:

$$R_{заг} = \frac{18{,}5 \cdot 5 \cdot 8{,}1}{18{,}5 \cdot 0{,}3 + 8{,}1 \cdot 16 \cdot 0{,}57} = 1{,}9 \leq R_д$$

3) При виникненню пожеж при роботі на ПЕОМ від таких можливими джерел запалювання як:

– іскри і дуги коротких замикань;

– перегрів провідників, резисторів та інших радіодеталей ПЕОМ, від тривалої

перевантаження та наявність перехідного опору;

– іскри при розмиканні і розмиканні ланцюгів;

– розряди статичної електрики;

– необережному поводженню з вогнем, а також вибухи газо-повітряних і паро-повітряних сумішей.

Важливу увагу слід звернути на пожежну безпеку підприємства в цілому і окремих його приміщень. В приміщеннях не повинно накопичуватися сміття, непотрібний папір, мотлох та ін. речі, які не використовуються у виробничому процесі. Наявний вільний аварійний вихід за межі приміщення в разі пожежі, бути передбачені вогнегасники. Вони повинні бути в робочому стані і перевірятися згідно з нормами. У приміщеннях повинна бути пожежна сигналізація, вогнегасник. У разі виникнення пожежі необхідно повідомити в найближчу пожежну частину,

убезпечити інших працівників і по можливості прийняти кроки по запобіганню можливих наслідків та усуненню пожежі.

## Висновки до розділу 4

В результаті проведеної роботи було зроблено аналіз умов праці, шкідливих та небезпечних чинників, з якими стикається робітник. Було визначено параметри і певні характеристики приміщення для роботи над запропонованим проектом написаному в кваліфікаційній роботі, описано, які заходи потрібно зробити для того, щоб дане приміщення відповідало необхідним нормам і було комфортним і безпечним для робітника.

Приведені рекомендації щодо організації робочого місця, а також важливу інформацію щодо пожежної та електробезпеки. Була наведена схема, розміри приміщення та наведено значення температури, вологості й рухливості повітря, необхідна кількість і потужність ламп та інші параметри, значення яких впливає на умови праці робітника, а також – наведені інструкції з охорони праці, техніки безпеки при роботі на комп’ютері.

# ВИСНОВКИ

Проведено аналіз існуючих комп'ютерних систем контролю і управління доступом

Визначено мету даної дипломної роботи - розробка системи контролю і управління доступом, що дозволяє запобігти несанкціонованому доступу до об'єктів підприємства, а також, що дозволяє зберегти і потім переглянути інформацію про події в системі за певний проміжок часу.

Сформовано технічне завдання на розробку. Визначені оснеовні вимоги до складу та виконуваних функцій системи.

Для досягнення поставленої мети був обраний RFID метод ідентифікації користувача. Цей метод був обраний за рахунок низьких матеріальних витрат на побудову системи, а також зіграла роль відносна звичність даного методу ідентифікації для рядового користувача.

На основі аналізу існуючих рішень, була розроблена власна архітектура комп'ютерної системи контролю та управління доступом (СКУД), яка складається з програмної системи.

Програмна система складається з серверної частини, яка відповідає безпосередньо за контроль і управління доступом і ОС Windows.

Серверна частина складається з сервера бази даних. Що відповідає за контроль і управління доступом. Клієнт виконує ідентифікацію та аутентифікацію користувачів.

Серверна частина програмної системи складається з комп’ютера на якому находиться база даних.

Проаналізувавши засоби програмування було вирішено використовувати бібліотеку Windows.Forms.

При розробці системи були реалізовані алгоритми обліку доступу в приміщення, а також форми авторизації та користувачі системи.

В результаті проведеної роботи було зроблено аналіз умов праці, шкідливих та небезпечних чинників, з якими стикається робітник. Було визначено параметри і певні характеристики приміщення для роботи над запропонованим проектом написаному в кваліфікаційній роботі, описано, які заходи потрібно зробити для того, щоб дане приміщення відповідало необхідним нормам і було комфортним і безпечним для робітника.

Приведені рекомендації щодо організації робочого місця, а також важливу інформацію щодо пожежної та електробезпеки. Була наведена схема, розміри приміщення та наведено значення температури, вологості й рухливості повітря, необхідна кількість і потужність ламп та інші параметри, значення яких впливає на умови праці робітника, а також – наведені інструкції з охорони праці, техніки безпеки при роботі на комп’ютері.

# ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Ворона В. А., Тихонов В.А., Духовенскій А.С., Осадчий А.І. Системи контролю і управління доступом: Загальні питання вибору СКУД. - М .: Гаряча лінія - Телеком, 2010. - 182 с.

2. Інтегровані системи безпеки [Електронний ресурс]. - Режим доступу: http://www.aamsystems.ru/publications/?id=132. - Назва з екрану.

3. Біометричні системи контролю доступу [Електронний ресурс]. - Режим доступу: http://ien.izi.vlsu.ru/teach/books/910/theory.html#_1. - Назва з екрану.

4. Контроль доступу: пристрої контролю доступу провідних світових виробників [Електронний ресурс]. - Режим доступу: http://www.armosystems.ru/system/hid_skd.ahtm. - Назва з екрану.

5. Panasonic - Системи безпеки [Електронний ресурс]. - Режим доступу: http://security.panasonic.ru/Catalog/Receiver/WV-BM-ET200.html. - Назва з екрану.

6. Новини про мобільні пристрої і технологіях [Електронний ресурс]. - Режим доступу: URL: http://naviny.by/rubrics/computer/2005/11/13/art_12. - Назва з екрану.

7. Блог про гаджетах: новини, статті, замітки [Електронний ресурс]. - Режим доступу: URL: http://telnews.ru/Nadezhda_Balovsyak/c101972. - Назва з екрану.

8. Контролер системи контролю та управління доступом EL-C800K-V2: Інструкція по експлуатації, частина 2. Блокування повторного проходу. - 125 стор.

9. ГОСТ 51241-2008 “Средства и системы контроля и управления доступом.

10. Бєлєнков В.Д. Електронні системи ідентифікації підписів. Захист інформації. Конфидент. 1 997, №6, с. 39-42.

11. Журнал "КомпьютерПресс": (Різноманіття сенсорних дисплеїв) / С.А. Асмаков // Б.М. Молчанов - 2010. - №8. - Режим доступу до журналу: http://www.compress.ru/archive.aspx.

12. Гильманов А.А., Клименко А.Я., Странгуль О.Н., Тарасенко В.П. Карткові технології в автоматизації маркетингу. - Томськ: Видавництво НТЛ, 2000. -380 с.

13. Контроль доступу: пристрої контролю доступу провідних світових виробників [Електронний ресурс]. - Режим доступу: http://www.armosystems.ru/system/hid_skd.ahtm. - Назва з екрану.

14. Методичні вказівки до виконання і захисту дипломного проекту / Уклад.: Скарга-Бандурова І.С., Барбарук В.М., Кардашук В.С. – Сєродонецьк: СНУ ім. В. Даля, 2017. – 52 с.

15. Методичні вказівки до виконання розділу «Охорона праці та безпека в надзвичайних ситуаціях» / Уклад.: Я.О. Критська – Під ред. І.С. Скарги-Бандурової – Сєвєродонецьк: СНУ ім. В. Даля, 2017. – 67 с.

**Додаток А.**

**Презентація**

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМ. В. ДАЛЯ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЕЛЕКТРОНІКИ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

# ДИПЛОМНИЙ ПРОЕКТ БАКАЛАВРА

Тема: Система контролю та управління доступом на підприємстві

Виконав: Семиряжко О.Ю.
Керівник: Скарга- Бандурова І.С.

Сєвєродонецьк 2017

## Технічне завдання

**Найменування розробки:** "Система контролю і управління доступом на підприємстві"

**СКУД призначена** для того, щоб забезпечувати санкціонований доступ в приміщення що охороняються, контролювати його і запобігати несанкціонованого проникнення.

**СКУД забезпечує** виконання таких функцій:

- ведення та підтримка баз даних користувачів і карт / ідентифікаторів;
- зберігання фотографій користувачів в базі даних;
- фіксація дати і часу проходу в базі даних;
- збереження ідентифікаційних ознак в пам'яті системи при відмові і відключенні електроживлення;
- відкривання ППК (двері, турнікет, шлагбаум та ін.) при зчитуванні зареєстрованої в пам'яті системи ідентифікаційної ознаки;
- заборона відкривання ППК при зчитуванні незареєстрованої в пам'яті системи ідентифікаційної ознаки.

## Актуальність роботи

- Робота присвячена питанню надійності систем контролю доступу з використанням радіочастотних зчитувачів.

- Радіочастотна ідентифікація має низку переваг у порівнянні з іншими технологіями ідентифікації. Найбільшою перевагою радіочастотної ідентифікації є, то що відстань, на яку може відбуватися отримання і запис ідентифікаційної інформації, варіюється до декількох десятків метрів.

## Основні можливості, які надає установка СКУД на об'єкті, що охороняється:

- Контроль і управління

- Збір і надання статистики.

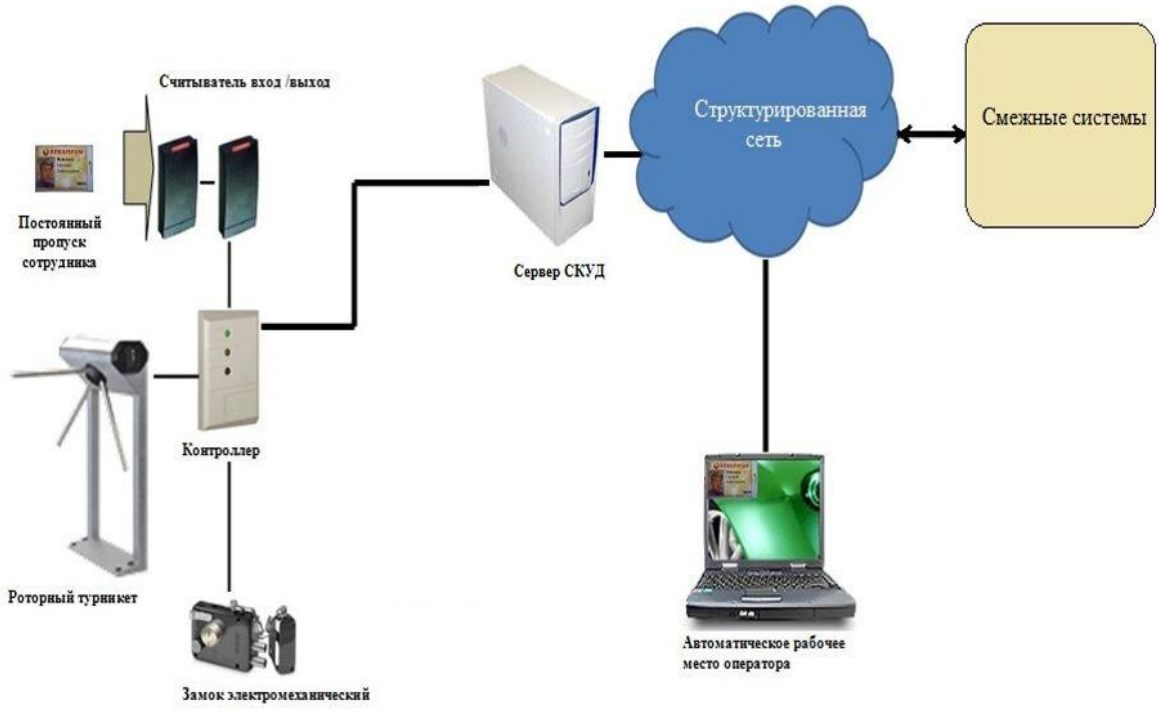
- Доступ співробітника тільки за особистим ідентифікатором.

## Функції СКУД

СКУД забезпечує виконання таких функцій:

- ведення та підтримка баз даних користувачів і карт / ідентифікаторів;
- зберігання фотографій користувачів в базі даних
- фіксація дати і часу проходу в базі даних;
- завдання рівнів доступу;
- Контроль часу знаходження на об'єкті відвідувачів.

## Склад системи контролю доступу



## Робочі частоти безконтактних карт

Виділяють такі робочі частоти безконтактних карт:

- Низькочастотні proximity карти (125 кГц)
- Високочастотні RFID-карти (13,56 МГц)

Порівняння технологій

| **Робоча частота** | 125 кГц | 13,56 МГц |
|---|---|---|
| **Наявність пам'яті** | нема | до 8 КВ |
| **Наявність криптографічного захисту** | нема | є |
| **Режим роботи** | тільки читання | читання-запис |
| **Дальність читання** | до 10 см | До 1 м |
| **Можливість програмування** | нема | є |
| **Захист від копіювання** | нема | є |
| **Типове застосування** | Найпростіші системи доступу | Складні системи доступу, системи локальної оплати |

## Опис зчитувача смарт-карт

Зчитувач смарт-карт (smart card reader) - це пристрій, призначений, власне, для зчитування інформації зі смарт-картки або для запису інформації на смарт-карту.

Зчитувачі поділяються:

- Контактні
- Безконтактні

ST-PR040MF ST-PR140MF ST-PR140MK

## Контролер

Контролер СКУД вважається «ядром» будь-якої системи контролю доступу. Це цифровий мікропроцесорний пристрій зазвичай діє таким чином:

- отримує інформацію зі зчитувача;
- обробляє дані, що надійшли;
- приймає рішення про допуск / заборону допуску на об'єкт;
- керує перешкоджаючими пристроями (відкриває або не відкриває двері).

## Структурована мережа

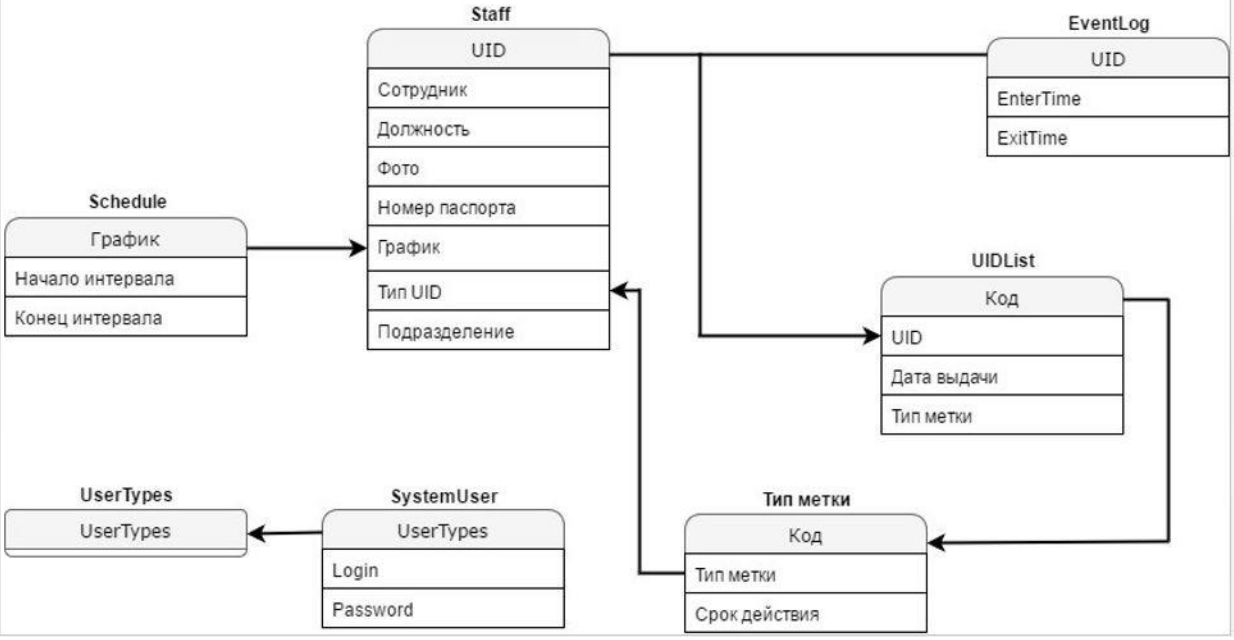
Мережі влаштовані за принципом: пристрої (робочі станції), обладнані мережними адаптерами, з'єднуються між собою через спеціальні комутаційні пристрої, в якості яких виступає:

- Роутер - дозволяє об'єднувати декілька електронних пристроїв в єдину мережу.

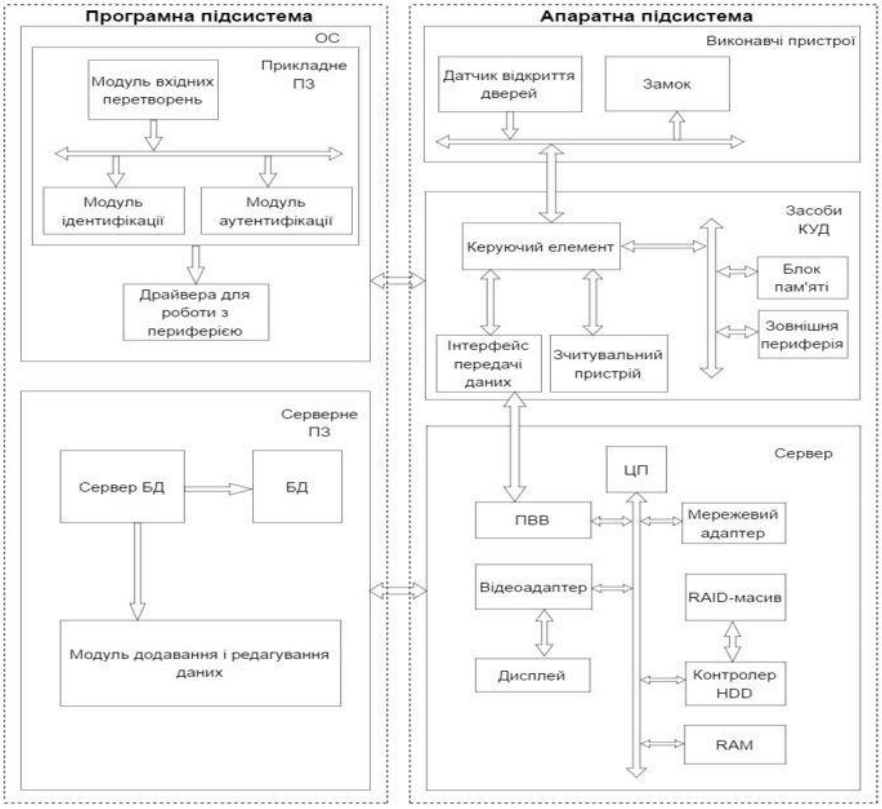
- Комутатор служить для з'єднання між собою різних вузлів комп'ютерної мережі та обміну даними між ними по кабелях. В ролі цих вузлів можуть виступати як окремі пристрої, так вже і об'єднані в самостійний сегмент мережі цілі групи пристроїв.

## Бази даних

Загальна схема бази даних




## Архітектура комп'ютерної системи контролю та управління доступом до об'єктів



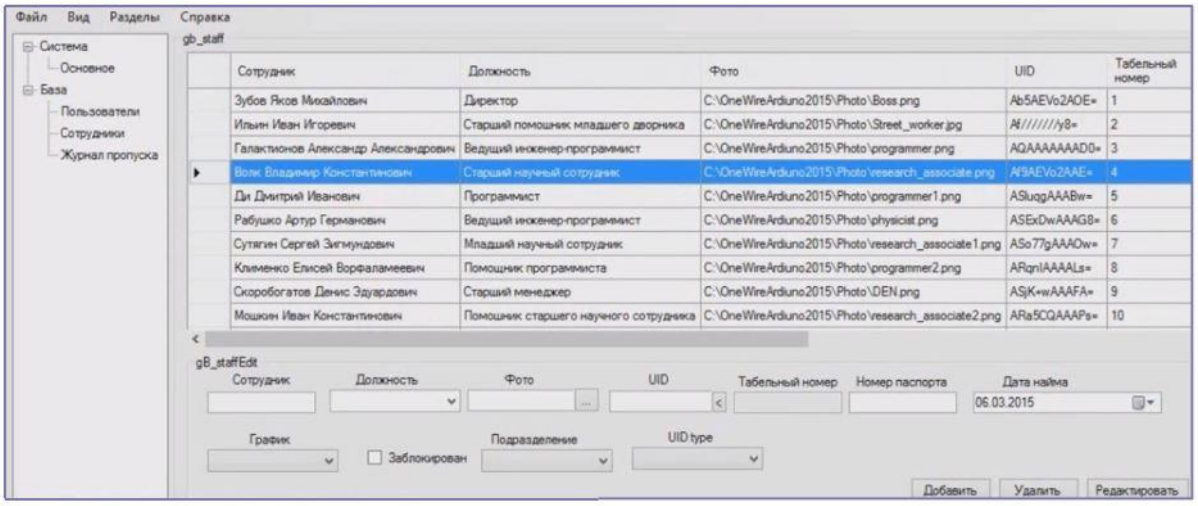
**Діаграма варіантів використання системи для адміністратора**


**Адміністратора**

В функції адміністратора входять:

- Додавання співробітника;
- Редагування співробітника;
- Видалення співробітника;
- Блокування співробітника;
- Перегляд  журналу пропуску;
- Редагування користувачів системи.

## Розділ адміністратора




## Висновки

Для досягнення поставленої мети був обраний RFID метод ідентифікації користувача. Цей метод був обраний за рахунок низьких матеріальних витрат на побудову системи, а також зіграла роль відносна звичність даного методу ідентифікації для рядового користувача.

При розробці системи були реалізовані алгоритми обліку доступу в приміщення, а також форми авторизації та користувачі системи.