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

До захисту допускається
Завідувач кафедри
_____Скарга-Бандурова І.С.
«____»_____ 2019 р.

ДИПЛОМНИЙ ПРОЕКТ (РОБОТА) БАКАЛАВРА

ПОЯСНЮВАЛЬНА ЗАПИСКА

НА ТЕМУ:

Система контролю доступу та обліку роботи співробітників підприємства

Освітньо-кваліфікаційний рівень "бакалавр"
Напрям 6.050101 – "Комп'ютерні науки"

Керівник проекту:	_____ (підпис)	доц. Сафонова С.О. (ініціали, прізвище)
Консультант з охорони праці:	_____ (підпис)	ст.викл. Критська Я.О. (ініціали, прізвище)
Здобувач вищої освіти:	_____ (підпис)	Андрейків В.О. (ініціали, прізвище)
Група:		КН-15бд

Сєвєродонецьк 2019

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВОЛОДИМИРА ДАЛЯ

Факультет Інформаційних технологій та електроніки
Кафедра Комп'ютерних наук та інженерії
Освітньо-кваліфікаційний рівень бакалавр
Напрям підготовки 6.050101 Комп'ютерні науки
(шифр і назва)
Спеціальність 122 "Комп'ютерні науки"
(шифр і назва)

ЗАТВЕРДЖУЮ:

Завідувач кафедри _____
_____ І.С. Скарга-Бандурова
«_____» _____2019 р.

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ) БАКАЛАВРА

Андрейківу Вадиму Олександровичу
(прізвище, ім'я, по батькові)

1. Тема роботи Система контролю доступу та обліку роботи співробітників підприємства

керівник проекту (роботи) Сафонова С.О., доц.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від " 13 " 05 2019 р. №
2. Термін подання студентом роботи
3. Вихідні дані до роботи матеріали переддипломної практики

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Аналіз предметної області і постановка задачі. Розробка системи контролю доступу та обліку роботи співробітників підприємства. Опис використаних програмних та технічних засобів. Результати застосування розробленої програмної системи. Охорона праці та безпека в надзвичайних ситуаціях.

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

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	ст.викл. кафедри КНІ Критська Я.О.		

7. Дата видачі завдання _____

Керівник _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Отримання завдання до роботи	14.05.19-18.05.19	
2	Аналіз завдання, огляд літератури	19.05.19-22.05.19	
3	Аналіз технічних засобів	23.05.19-26.05.19	
4	Розробка алгоритму	27.05.19-02.06.19	
5	Програмна реалізація	03.06.19-06.06.19	
6	Оформлення пояснювальної записки	07.06.19-09.06.19	
7	Підготовка презентації та доповіді	10.06.19-13.06.19	

Здобувач вищої освіти _____ Андрейків В.О.
(підпис) (прізвище та ініціали)

Керівник _____ Сафонова С.О.
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Пояснювальна записка до дипломного проекту (роботи) бакалавра: 93 с., 25 рис., 7 табл., 21 бібліографічних джерел посилань, 3 додатки.

Об'єкт розробки: процеси контролю доступу та обліку робочого часу для працівників підприємства.

Мета роботи: розробка програмного забезпечення для автоматизованого комплексу з метою забезпечення контрольованого доступу на територію підприємства і обліку робочого часу співробітників.

В проекті виконано:

1. Огляд особливостей систем контролю та управління доступом, сформульована постановка задачі.
2. Проектування та розробку бази даних.
3. Вибір засобів розробки програмного забезпечення.
4. Проектування та розробку програмної системи.
5. Тестування роботи системи.
6. Здійснений аналіз потенційних небезпечних і шкідливих виробничих чинників проектованого об'єкта, що впливають на персонал.

Отримано наступні результати: спроектована і реалізована система контролю доступу та обліку робочого часу для працівників підприємства.

Практичне значення, галузь застосування роботи: програмне забезпечення використовується для побудови мережі автоматизованих прохідних систем підприємства.

Ключові слова: АВТОМАТИЗОВАНА ПРОХІДНА, ТУРНІКЕТ, БЕЗКОНТАКТНІ КАРТКИ, COM-ПОРТ, DELPHI, BDE, SQL.

Умови одержання дипломного проекту: СНУ ім. В. Даля, пр. Центральний 59-А, м. Сєвєродонецьк, 93400.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

СТЗ – система технічного зору

ІП – інваріантна пряма

СКУД – системою контролю та управління доступом

ОС - операційна система;

БД - база даних;

СУБД - система управління базами даних;

API - Application Program Interface;

VCL - Visual Component Library;

DLL (Dynamic Link Library) - динамічна бібліотека;

OLE (Object Linking and Embedding) - технологія зв'язування та впровадження об'єктів;

BLOB (Binary Large OBjects) - об'єкти великих двійкових обсягів;

COM-порт - послідовний порт;

PIN-код - унікальний код;

Proximity-карта - безконтактна картка, що містить PIN-код;

UNC-ім'я - унікальне мережеве ім'я;

КПП - контрольно-пропускний пункт (автоматизована прохідна).

ВСТУП

Скільки років існує людське суспільство, яке визнало принцип приватної власності, стільки років існують і засоби захисту від посягань на цю власність. Люди завжди закривали свою хатину, замок, квартиру, офіс. Навряд чи і через пару сотень років потреба в цьому пропаде. Системи для замикання того, що людям дорого, удосконалюються разом з технічним прогресом, і в століття електроніки найсучасніші запори, звичайно ж, не можуть обійтися без мікроконтролерів і комп'ютерів.

Зайвих грошей ніколи не буває, і якщо хтось вирішив їх витратити на безпеку офісу або будинку, то варто це робити зі знанням справи, щоб не переплачувати за можливості, які ніколи не будуть використовуватися. Крім того, не треба забувати, що при побудові такого роду систем неповинно залишатися «тонких» місць, і всі компоненти системи повинні бути збалансовані.

Людина також є головною ланкою будь-якого виробничого та інтелектуального процесу сучасного суспільства. Однак якщо велику кількість індивідуумів об'єднати, наприклад, для організації промислового виробництва середніх розмірів, то практично завжди виникають складнощі з управління сформованим трудовим колективом, які негативно впливають на виробничий процес. Причина, по якій виникають складнощі полягає в тому, що людина - це жива істота, яка не тільки здійснює трудову діяльність; людина хоче жити і повина підтримувати життєдіяльність свого організму. Ясно, що люди хворіють, спізнюються на роботу, прогулюють і т.д. Ситуація ускладнюється тим, що ніхто з прогульників не хоче, щоб його зловили, і використовує всі свої інтелектуальні можливості для приховування фактів порушення трудової дисципліни.

У всі часи людської історії для організації виробничого процесу використовувалися додаткові людські ресурси, і тільки останнім часом з'явилися електронні системи, що дозволяють автоматизувати організацію процесу. Організація процесу роботи та її обліку за допомогою електронних систем дозволяє відмовитися від додаткових витрат на утримання людей, які здійснюють контроль, і підвищити рентабельність і ефективність виробництва. Як системи, що здійснюють пропускний режим, а так само керують людськими ресурсами підприємств, сьогодні використовуються системи контролю доступу.

На жаль, комерційні організації, а тим більше самі виробники систем контролю і управління доступом не пропонують жодних статистичних даних про проникненнях сторонніх на об'єкти і викликаних цим втратами. Це лише говорить про те, що ці втрати є, і, причому, досить істотні. У зв'язку з цим, перед керівниками великих і не дуже організацій стоять перш за все дві основні проблеми:

– контроль фізичного доступу в приміщення організації (з різним рівнем доступу самих працівників в різні приміщення);

– контроль за наявністю і знаходженням персоналу в межах офісу компанії (особливо актуально якщо офіс розташовується на кількох поверхах або в кількох будівлях).

Метою даної дипломної роботи є розробка доступної, недорогої і ефективної системи контролю та управління доступом, яка здатна відповідати сучасним вимогам безпеки. Цільовим колом споживачів вибрано фірми, які орендують офісні приміщення в популярних останнім часом бізнес-центрах. У останніх, як правило, вже є централізована охорона на прохідних, що забезпечує роботу СКУД. Зазвичай там застосовуються найбільш поширені системи і засоби захисту і управління доступом, такі як: proximity / smart-карти або магнітні ключі з турнікетами, домофони, спільно з системами відеоспостереження, і т.д. Це означає, що у кожного працівника вже є свій ідентифікатор (карта, ключ ...), що дає можливість проходу на

територію офісу. Але якщо є необхідність найбільш чіткої організації робочого процесу, наприклад, мати доступ до інформації про місцезнаходження кожного співробітника, і його переміщення, виникають незручності. Можна, звичайно, встановлювати контролери на кожних дверях, але це робить пересування по офісу досить складним, не кожній фірмі це підійде. Тому є сенс спростити, а ще краще - автоматизувати цю систему.

Зараз практично у кожного є мобільний телефон з технологією Bluetooth. Ця технологія найбільш підходить для реалізації такої СКУД через свою доступність та низьку енергоємність. Ідентифікатором в даному випадку є програма (клієнт), яка зашита в телефон за допомогою цієї ж технології, інфрачервоного порту або data-кабелю. Зчитувач - комп'ютер, так само з програмою (сервер) з модулем Bluetooth.

В якості мови програмування обраний Java так само через свою простоту, і можливості перенесення програми на різні платформи (з персонального комп'ютера на телефон в даному випадку) без зміни програмного коду.

1 СИСТЕМИ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ

Системою контролю та управління доступом називається сукупність програмно-технічних засобів і організаційно-методичних заходів, за допомогою яких вирішується завдання контролю і управління відвідуванням окремих приміщень, а також оперативний контроль переміщення персоналу і часу його перебування на території об'єкта. Дійсно, СКУД це не тільки апаратура і програмне забезпечення, це продумана система управління рухом персоналу.

1.1 Компоненти СКУД

У будь-який СКУД є якийсь ідентифікатор (ключ), який служить для визначення прав людини власника. Це може бути «далласовская таблетка», яка широко використовувана в під'їзних домофонах, безконтактна (proximity) картка або брелок, карта з магнітною смугою (зараз практично не використовується) (рис.1.1).

Рисунок 1.1 - Види ідентифікаторів

Крім того, в якості ідентифікатора може використовуватися код, що набирається на клавіатурі, а також ряд біометричних ознак людини - відбиток пальця, малюнок сітківки або райдужної оболонки ока. Карту або брелок можна передати, їх можуть вкрасти або скопіювати. Код можна підглянути або просто зказати комусь. Біометричні ознаки передати або вкрасти неможливо, хоча деякі з них все ж підробляються без великих зусиль. Тип використовуваного ідентифікатора багато в чому визначає захищеність системи від зловмисників. Наприклад, будь-який радіоаматор по описам, що приводяться в Інтернеті, може легко зробити імітатор «далласовской таблетки», а код, що зберігається в ній, завжди відштампований на зворотному боці. Безконтактні картки або брелоки, стандартно використовуються в системах доступу, підробляються трохи складніше, але також не захищені від цього. Сьогодні є картки з високим рівнем захищеності (використовуються потужні схеми криптографування, де ключі для шифрування може призначати сам користувач), але в стандартних СКУД ці рішення, як не дивно, поки практично не застосовуються. Біометричні ознаки підробити найскладніше (серед них відбитки пальців найбільш легко відтворювані). Взагалі, там, де потрібен високий рівень захищеності від злому, як правило, використовують одночасно кілька ідентифікаторів - наприклад, картку і код, відбиток пальця і карту або код.

При втраті механічного ключа рекомендується змінити замок або, як мінімум, личину. У разі електронних ідентифікаторів загублений «ключ» просто треба викреслити зі списку дозволених, що набагато простіше і дешевше.

При виборі типу ідентифікатора необхідно враховувати:

– В системі може бути єдина точка проходу (наприклад, турнікет на вході в будівлю), а користувачів може бути кілька сотень. У цьому випадку ціна ідентифікатора, помножена на кількість, може перевищити вартість всього обладнання. А якщо врахувати, що їх втрачають і ломають, то це заплановані витрати і на майбутнє.

– Бажано, щоб вибрані ідентифікатори були широко доступні на ринку (тобто, щоб вони вироблялися не єдиною в світі компанією, а мали б аналоги). Це запорука того, що і через кілька років буде можливість докуповувати потрібну кількість ключів.

Ідентифікатором користувача називається деякий пристрій або ознака, за якою визначається користувач. При ідентифікації відбувається перевірка наявності користувача (або його ідентифікатора) в списку зареєстрованих. При аутентифікації перевіряється приналежність висунутого ідентифікатора конкретного користувача. Доступ до захищеного об'єкта повинен здійснюватися виключно після достовірної аутентифікації, яку можна зробити тільки на основі унікальних ознак, притаманних конкретному користувачеві. У всіх інших випадках може бути проведена тільки ідентифікація, що не виключає несанкціонований доступ. Якщо ідентифікатор переданий або відомий іншому користувачеві, то він отримує доступ до захищеного об'єкта. У разі біометричних СКУД, ідентифікація і аутентифікація відбувається одночасно,

Кожен ідентифікатор характеризуються певним унікальним двійковим кодом. В системі кожному коду ставиться у відповідність інформація про права і привілеї власника ідентифікатора. Зараз застосовуються такі типи карт:

– Безконтактні радіочастотні (PROXIMITY) карти - найбільш перспективний в даний момент тип карт. Безконтактні картки спрацьовують на відстані і не вимагають чіткого позиціонування, що забезпечує їх стійку роботу і зручність використання, високу пропускну здатність. Зчитувач генерує електромагнітне випромінювання частотою 125 кГц і, при внесенні карти в зону дії зчитувача, це випромінювання через вбудовану в карті антену живить чіп карти. Отримавши необхідну енергію для роботи, карта пересилає на зчитувач свій ідентифікаційний номер на частоті, 62,5 кГц.

– Магнітні картки - найбільш широко поширений варіант. Існують карти з низько коерцитивною і високо коерцитивною магнітною смугою і з записом на різні доріжки.

– Карти Віганд - названі по імені вченого, який відкрив магнітний сплав, у якого прямокутної петлею гістерезиса. Усередині карти розташовані відрізки дроту з цього сплаву, які, при переміщенні повз них голівки, що зчитує, дозволяють зчитувати інформацію. Ці карти довговічніші, ніж магнітні, але і більш дорогі. Один з недоліків - те, що код в карту занесений при виготовленні раз і назавжди.

– Штрих-кодові карти - на карту наноситься штриховий код. Існує більш складний варіант - штрих-код закривається матеріалом, прозорим тільки в інфрачервоному світлі, зчитування відбувається в ІЧ-області.

– Ключ-брелок "Touch memory" - металева таблетка, усередині якої розташований чіп ПЗУ. При торканні таблетки зчитувача з пам'яті таблетки в контролер пересилається унікальний код ідентифікатора.

Одна і та ж картка може відкривати як одні двері, так і служити «ключем» для кількох дверей. Для тимчасових співробітників і відвідувачів оформляються тимчасові або разові «перепустки» - картки з обмеженим терміном дії.

Зчитувачі - пристрої, призначені для зчитування інформації з ідентифікатора і передачі цієї інформації в контролер СКУД (рис. 1.2). Залежно від принципів роботи ідентифікатора змінюється і технологія зчитування коду. Для «далласовські таблетки» це два електричних контакти, виконаних у вигляді лузи, для proximity карти це вже досить складний електронний пристрій, а для зчитування, наприклад, малюнка райдужної оболонки ока до складу зчитувача входить мініатюрна телевізійна камера.

Рисунок 1.2 - Зчитувачі

Зчитувач, за визначенням, має бути доступний зовні приміщення, прохід в яке необхідно отримати. Звідси і комплекс вимог. Якщо зчитувач встановлюється на вулиці (в'їзні ворота, вхідні двері будівлі), то, як мінімум, він повинен витримувати суворі кліматичні навантаження - жару і холод, сніг і дощ. А якщо прилегла територія не перебуває під наглядом, то ще буде потрібно і додаткова міцність для стійкості проти механічних пошкоджень.

Найбільш вандалостійкими можуть бути зроблені зчитувачі безконтактних карт. Якщо суцільний корпус з нержавіючої сталі здається недостатньо захищеним, можливо замурувати зчитувач в бетонну стіну або помістити за шаром міцного пластику товщиною в пару сантиметрів - при такому способі установки пошкодити зчитувач без спеціального інструменту вже неможливо. А самому зчитувачу такий захист нічим не заважає.

Біометричні зчитувачі на сьогоднішній день все ще дуже коштовні, тому їх застосування повинно бути обгрунтовано реальною необхідністю. Крім того, їм властиві ще деякі недоліки:

– Порівняно великий час ідентифікації - від десятих часток до одиниць секунд. Для великого потоку людей на заводській прохідній це може виявитися неприйнятним.

– Всі вони не розраховані на вуличне застосування.

– Зчитувачі відбитків пальців викликають у людей певний дискомфорт, хоча, по правді сказати, жоден із сучасних дактилоскопічних

зчитувачів не зберігає самі відбитки пальців, а тільки якусь їх математичну модель, за якою відбиток не відновлюється.

– Достовірність розпізнавання людини за біометричними ознаками ще жоден рік буде відрізнятися від одиниці, також може створити певні незручності.

Контролери (серце СКУД) - пристрої, призначені для обробки інформації від зчитувачів ідентифікаторів, ухвалення рішення і управління виконавчими пристроями (рис. 1.3). За способом управління контролери СКУД діляться на три класи: автономні, централізовані (мережеві) і комбіновані. Це основна частина системи. Саме контролер приймає рішення, пропустити чи ні людину в дані двері. Контролер зберігає у своїй пам'яті коди ідентифікаторів зі списком прав кожного з них. Коли ви пред'являєте ідентифікатор, код з нього порівнюється з тим, що зберігається в пам'яті, на підставі чого приймається рішення про те, відкрити двері або ворота або не відкривати.

Рисунок 1.3 - Контролер

Оскільки контролер виконує такі важливі функції, його треба розміщувати в захищеному місці, як правило, усередині приміщення, вхід в яке він охороняє. Інакше не потрібні ніякі ідентифікатори - зловмисник знайде дроти від електрозамку і відкриє його, незважаючи ні на які «розумові здібності» контролера.

Контролер для своєї роботи вимагає електроживлення, тому дуже важливо, щоб він міг працювати навіть в разі аварії електромережі (а таку аварію може організувати і зловмисник). Професійні контролери, як правило, мають власний акумулятор, який підтримує працездатність контролера від декількох годин до декількох діб. Якщо застосовується зовсім простий автономний контролер без власного блоку живлення, то краще не живити його від звичайного адаптера для електронних іграшок, що включається в розетку, - є сенс придбати джерело безперебійного живлення, який спеціально для цього призначений.

Якщо завдання СКУД полягає в обмеженні проходів через звичайні двері, то запірним пристроєм буде електрично керований замок (рис.1.4).

Рисунок 1.4 - Електронний замок

Замки недорогі, легко встановлюються майже на всі двері, а оскільки зазвичай ставляться в одвірку, то не вимагають гнучкого підведення живлення до самих дверей. За захищеності від злому це найгірший з варіантів, тому рекомендується використовувати там, де ймовірність злому з боку зловмисника мінімальна - зазвичай це двері всередині офісу. На ніч обладнані двері зазвичай замикають механічним ключем.

Слід зазначити, що електрозамки, як і інші типи замків, бувають відкриваються напругою (тобто двері відкриються при подачі напруги живлення на замок) і закриваються напругою. Останні відкриваються, як

тільки з них знімається напруга живлення. За вимогами пожежного нагляду, всі двері, які використовуються для виходу в разі пожежі, повинні бути обладнані запірними пристроями, які замикаються напругою.

Електромагнітні замки також не є ідеальним варіантом запірного пристрою, але теж порівняно недорогі і в деяких випадках дуже зручні в установці. По можливості монтувати їх краще з внутрішньої сторони дверей. Майже всі вони відносяться до групи замків, які замикаються напругою, тобто придатні для установки на шляхах евакуації при пожежі.

Електромеханічні замки бувають самих різних типів. Як правило, можна вибрати досить стійкий до злому замок (міцний механічно, з потужним ригелем). Недоліки - це трохи більше висока ціна (без урахування простих і не дуже надійних накладних замків виробництва Південно-Східної Азії), а також необхідність гнучкого підведення на самі двері. Більшість з таких замків мають механічний перевзвод, тобто, якщо на замок подали імпульс, що відкриває, навіть невеликої тривалості, двері будуть у відкритому стані до тих пір, поки її не відкриють і знову не закриють.

Турнікети - пристрої для розмежування проходу, використовують тільки на підприємствах (рис. 1.5). Турнікети бувають двох основних типів: поясні та повнозростові. Різниця зрозуміла з назви. Турнікет при правильному налаштуванні всієї системи дозволяє дійсно пропустити по одній карті тільки одну людину. За рахунок цього, а також за рахунок високої пропускної здатності (на прохід потрібно мінімум часу) вони незамінні на вході в велике підприємство, де, до того ж, використовується система обліку робочого часу.

Повноростовий турнікет набагато дорожче поясного, але його не можна перестрибнути, що і визначає область застосування. В даний час на ринку є не тільки імпортні, а й вітчизняні турнікети, що витримують серйозні навантаження по «трафіку» протягом тривалого часу. Оскільки пристрій цей дуже не дешевий, варто придивитися до турнікетів українського виробництва.

Рисунок 1.5 - Турнікети

Найчастіше використовуються на в'їздах на підприємство і на автомобільних парковках. Основна вимога - стійкість до наших кліматичних умов і можливість управління від контролера СКУД.

До систем доступу можуть пропонувати багато різних «наворотів», корисність яких іноді викликає сумнів. Наприклад, якщо пропонують для серйозної СКУД підприємства купити GSM модуль, який пошле SMS за допомогою одного з запрограмованих телефонних номерів, то подумайте, перш ніж погодитися. Такі СКУД зазвичай обслуговуються цілодобовою охороною, і GSM модем не підвищить надійність охорони. У той же час для заміського будинку така недешева річ може виявитися досить корисною. Чи не здається правильним для мережевої СКУД можливість управління нею через Інтернет. Це модно, але, як зламують через «всесвітню павутину» звичайні комп'ютери, так само розкриють і систему безпеки.

Фотоідентифікація (Photo ID) - можливість виведення на екран монітора комп'ютера фотографії власника ідентифікатора (з бази даних). Фотоідентифікація застосовується на прохідних, як додатковий захід захисту від несанкціонованого проходу. При цьому рішення про прохід може прийматися як автоматично, так і з підтвердженням від контролера на прохідній.

1.2 Системи доступу

Автономні системи дешевше, простіше в експлуатації (часто встановлення та налаштування такої системи доступне навіть не дуже підготовленій людині), а по ефективності іноді нітрохи й не гірше. Автономні системи відрізняються від мережевих тим, що вони не вміють створювати звіти щодо подій, передавати інформацію про події на інший поверх і управлятися дистанційно.

При цьому автономні системи не вимагають прокладки сотень метрів кабелю, пристроїв сполучення з комп'ютером, так і самого комп'ютера теж. Це все пряма економія грошей, сил і часу при установці системи.

А по стійкості до злому «автономніков» нітрохи не поступаються мережевим системам, оскільки елементи, які за це відповідають - ідентифікатори, зчитувачі, запірні пристрої - в обох випадках можуть використовуватися одні й ті ж. Звичайно ж є деякі винятки. При виборі автономної системи з високими вимогами по стійкості до злому слід звернути увагу на наступні речі:

– Зчитувач повинен бути відділений від контролера, щоб зовні ланцюга, за якими можливо відкривання замка, були недоступні.

– Контролер повинен мати резервне джерело живлення на випадок тимчасового зникнення мережі або умисного її відключення.

– Зчитувач переважно використовувати в вандалозахисному виконанні.

– Надійність замикання пристрою.

Деякі автономні системи мають функції копіювання бази даних ключів. Це може виявитися корисним, якщо є кілька дверей, в які ходять одні й ті ж люди при чисельності, близькій до сотні або більше. Також при великій кількості користувачів рекомендується використання контролера, що має розвинену індикацію (наприклад, рідкокристалічний дисплей), оскільки

управління таким пристроєм набагато наочніше і зручніше. Різниця в ціні в порівнянні з контролером, які мають тільки світлодіодну і/або звукову індикацію, з лишком окупиться в процесі експлуатації.

Повністю закінчений пристрій, призначений для обслуговування, як правило, однієї точки проходу. Зустрічаються найрізноманітніші варіації: контролери, суміщені зі зчитувачем, контролери, вбудовані в електромагнітний замок і так далі. Автономні контролери розраховані на застосування найрізноманітніших типів зчитувачів. Як правило, автономні контролери розраховані на обслуговування невеликої кількості користувачів, зазвичай до п'ятисот.

У мережній системі всі контролери з'єднані один з одним через комп'ютер, що дає безліч переваг для великих систем, але зовсім не потрібно для «домашньої» СКУД. Питома вартість однієї точки проходу в мережевій системі завжди вище. Крім того, для керування такою системою вже потрібен хоча б один кваліфікований фахівець. Але, незважаючи на ці мінуси, мережеві системи незамінні для великих об'єктів (офіси, виробничі підприємства), оскільки управлятися навіть з десятком дверей, на яких встановлені автономні системи, стає головним болем. Незамінні мережеві системи і в наступних випадках:

– Якщо потрібен контроль за подіями, які відбувалися в минулому, або оперативний додатковий контроль в реальному часі. Наприклад, в мережевій системі службовець на прохідній може на екрані монітора бачити фотографію людини, яка пред'явила тільки що свій ідентифікатор, що підстраховує від передачі карток іншим людям.

– Якщо потрібно організувати облік робочого часу і контроль трудової дисципліни. У тому чи іншому вигляді така функція входить в програмне забезпечення практично всіх сучасних мережевих СКУД. Але модуль обліку робочого часу імпортної системи може не підійти українській компанії, оскільки не розрахований на наш менталітет і прийняті на більшості об'єктів правила.

– Якщо потрібно забезпечити тісну взаємодію з іншими підсистемами безпеки (охоронної сигналізації, телеспостереження).

У мережній системі з одного місця можна не тільки контролювати події на всій території, що захищається, а й централізовано керувати правами користувачів, швидко заносячи або видаляючи ідентифікатори. Всі мережеві системи мають можливість організувати кілька робочих місць, розділивши функції управління між різними людьми і службами.

При виборі великої системи важливі її топологія, тобто принципи об'єднання в мережу контролерів і комп'ютерів, максимальні параметри (кількість підтримуваних точок проходу), можливість організації декількох робочих місць. Природно, все кількісні характеристики треба розглядати через призму потенційного зростання на кілька років вперед, оскільки, виклавши кілька десятків тисяч доларів за систему сьогодні, не хотілося б встати в глухий кут через пару років при підключенні ще одних дверей до мережевої СКУД. Також слід звернути увагу на те, яка СУБД використовується в даній СКУД. Якщо система маленька (кілька дверей, один комп'ютер, пара сотень користувачів), то так званої «плоскої» СУБД і їм подібної вистачить цілком. Такі СУБД невибагливі до ресурсів комп'ютера і прості в експлуатації. Для системи з декількох сотень точок проходу з персоналом в пару десятків тисяч чоловік слід вибирати архітектуру «клієнт-сервер». СУБД цього типу витримують набагато більші кількісні навантаження, але натомість вимагають більш потужних комп'ютерів і добре підготовлених фахівців для супроводу системи.

Дуже важлива для мережевої системи технічна підтримка, оскільки проблеми можуть виникнути навіть у самій надійній системі, а від терміну вирішення проблем залежить коли успіх бізнесу, а коли і життя людей. Тому, вибираючи систему, необхідно визначити, скільки фахівців у вашому місті, області, в країні зможуть прийти на допомогу в скрутну хвилину.

Не дуже вдалий термін, що позначає можливість роботи контролерів в мережі під управлінням комп'ютера. У цьому випадку функції ухвалення

рішення лягають на персональний комп'ютер з встановленим спеціалізованим програмним забезпеченням. Мережеві контролери застосовуються для створення СКУД будь-якого ступеня складності. При цьому адміністрація отримує величезну кількість додаткових можливостей. Крім просто дозволу або заборони проходу маєте, як правило, такі можливості:

– отримання звіту про наявність чи відсутність співробітників на роботі;

– можливість практично миттєво дізнатися, де саме знаходиться співробітник;

– ведення автоматичного табеля обліку робочого часу;

– отримання звіту про те, хто і куди ходив практично за будь-який період часу;

– можливість сформувати часовий графік проходу співробітників, тобто хто, куди і в який час може ходити;

– можливість ведення бази даних співробітників (електронної картотеки), в яку заноситься вся необхідна інформація про співробітників, включаючи їх фотографії;

– можливість розширення функціональності СКУД.

Заборона подвійного проходу - це заборона на пропуск через одну і ту ж точку проходу користувача, що не вийшов з приміщення. Природно, ця можливість існує тільки для повністю контрольованої точки проходу, так як зрозуміти, що людина увійшла, але не вийшла, можна тільки на проході, обладнаному двома зчитувачами на вхід і на вихід. Заборона подвійного проходу введена для того, щоб утруднити передачу ідентифікатора іншій особі.

Підтримка такого режиму проходів, при якому людина, що пройшла в приміщення, обладнане повністю контрольованою точкою проходу, не може пройти ні в яке інше приміщення, попередньо не вийшовши з контрольованого.

Точка проходу наділена особливими функціями. Людина, що не пройшла через точку проходу, позначену як прохідна, не зможе потрапити ні в одне приміщення об'єкта. Як правило, саме за часом проходу через прохідну підраховується робочий час.

Деяка перешкода (бар'єр), обладнана зчитувачем і виконавчим пристроєм. Точка проходу може бути повністю контрольованою і контрольованою на вхід. У першому випадку, прохід оснащується двома зчитувачами - на вхід і на вихід. У другому випадку - тільки зчитувачем на вхід, вихід здійснюється вільно або по кнопці RTE.

1.3 Принцип функціонування системи контролю та управління доступом

Кожен співробітник, клієнт, відвідувач фірми одержує ідентифікатор (електронний ключ) - пластикову картку або брелок з індивідуальним кодом. «Електронні ключі» видаються в результаті реєстрації перерахованих осіб за допомогою засобів системи. Паспортні дані, фото (відеозображення) і інші відомості про власника «електронного ключа» заносяться в персональну «електронну картку». Персональна «електронна картка» власника і код його «електронного ключа» зв'язуються один з одним і заносяться в спеціально організовані комп'ютерні бази даних.

Біля входу в будівлю або в приміщення, що підлягає контролю, встановлюються зчитувачі, що зчитують з карток їх код та інформацію про права доступу власника карти і передають цю інформацію в контролер системи.

У системі кожному коду поставлена у відповідність інформація про права власника картки. На основі зіставлення цієї інформації та ситуації, при якій була пред'явлена картка, система приймає рішення: контролер відкриває

або блокує двері (замки, турнікети), переводить приміщення в режим охорони, включає сигнал тривоги і т.д.

Всі факти пред'явлення карток і пов'язані з ними дії (проходи, тривоги і т.д.) фіксуються в контролері і зберігаються в комп'ютері. Інформація про події, які викликані пред'явленням карток, може бути використана в подальшому для отримання звітів по обліку робочого часу, порушень трудової дисципліни та ін. На підприємствах можна виділити чотири характерні точки контролю доступу: прохідні, офісні приміщення, приміщення особливої важливості, і в'їзди/виїзди автотранспорту. Залежно від того, яке завдання стоїть, можно вибрати відповідну систему контролю і управління доступом.

Невелика СКУД дозволить запобігти доступ небажаних осіб, а співробітникам точно вказати ті приміщення, в які вони мають право доступу.

Складніша система дозволить крім обмеження доступу призначити кожному співробітнику індивідуальний часовий графік роботи, зберегти і потім переглянути інформацію про події за день. Системи можуть працювати в автономному режимі і під управлінням комп'ютера.

Комплексні СКУД дозволяють вирішити питання безпеки і дисципліни, автоматизувати кадровий та бухгалтерський облік, створити автоматизоване робоче місце охоронця.

1.4 Класифікація систем контролю і керування доступом

За ГОСТ Р 51241-98:

– Доступ - переміщення людей, транспорту та інших об'єктів в (з) приміщення, будівлі, зони і території.

– Контроль і управління доступом (КУД) - комплекс заходів, спрямованих на обмеження і санкціонування доступу людей, транспорту та інших об'єктів в (з) приміщення, будівлі, зони і території;

– Засоби контролю доступу в приміщення - механічні, електромеханічні, електричні, електронні пристрої, конструкції і програмні засоби, що забезпечують реалізацію контролю і управління доступом;

– Система контролю і управління доступом - сукупність засобів контролю і управління, що володіють технічною, інформаційною, програмною та експлуатаційною сумісністю.

Системи КУД в залежності від розмірів і призначення класифікуються:

За способом управління системи КУД можуть бути:

– автономні - без передачі інформації на центральний пульт і без контролю з боку оператора;

– централізовані (мережеві) - з обміном інформацією з центральним пультом і контролем і управлінням системою з боку оператора;

– універсальні - включають функції як автономних, так і мережевих систем, що працюють в мережевому режимі під управлінням центрального пристрою управління і перехідні в автономний режим при виникненні відмов у мережевому обладнанні, в центральному пристрої або обриві зв'язку.

За кількістю контрольованих точок доступу системи КУД можуть бути:

– малої місткості (менше 16 точок);

– середньої місткості (не менше 16 і не більше 64 точок);

– великої місткості (64 точки і більше).

За функціональними характеристиками системи КУД можуть бути трьох класів:

– системи з обмеженими функціями;

– системи з розширеними функціями;

– багатофункціональні системи.

В системи будь-якого класу можуть бути введені спеціальні функції, які визначаються додатковими вимогами замовника.

По виду об'єктів контролю системи КУД можуть бути:

– для контролю доступу фізичних об'єктів;
– для контролю доступу до інформації.

Засоби КУД класифікують по стійкості до несанкціонованого доступу, яка визначається стійкістю до руйнівних і не руйнуючих впливів за трьома рівнями стійкості:

– нормальною;
– підвищеною;
– високою.

ППК (пристрої, що перегороджують, керовані) і ПВІП (пристрої введення ідентифікаційних ознак) класифікують за стійкістю до руйнівних дій. Стійкість ППК встановлюють по:

– стійкості до злому;
– кулестійкості;
– стійкості до вибуху.

Стійкість ПВІП встановлюють по стійкості зчитувача до злому. Для ППК підвищеної та високої стійкості встановлюють додатково 5 класів за показниками стійкості (1-й клас - нижчий):

За стійкістю до не руйнуючих впливів засоби і системи КУД в залежності від їх функціонального призначення класифікують за такими показниками:

– стійкості до розтину - для ППК і виконавчих пристроїв (замків і запірних механізмів);

– стійкості до маніпулювання;

– стійкості до спостереження - для ПВІП з кодом, що запам'ятовується (клавіатури, кодові перемикачі і т.п.);

– стійкості до копіювання (для ідентифікаторів);

– стійкості захисту засобів обчислювальної техніки від несанкціонованого доступу до інформації.

Основні компоненти мережевої багатофункціональної системи контролю доступом відображені на рисунку 1.6.

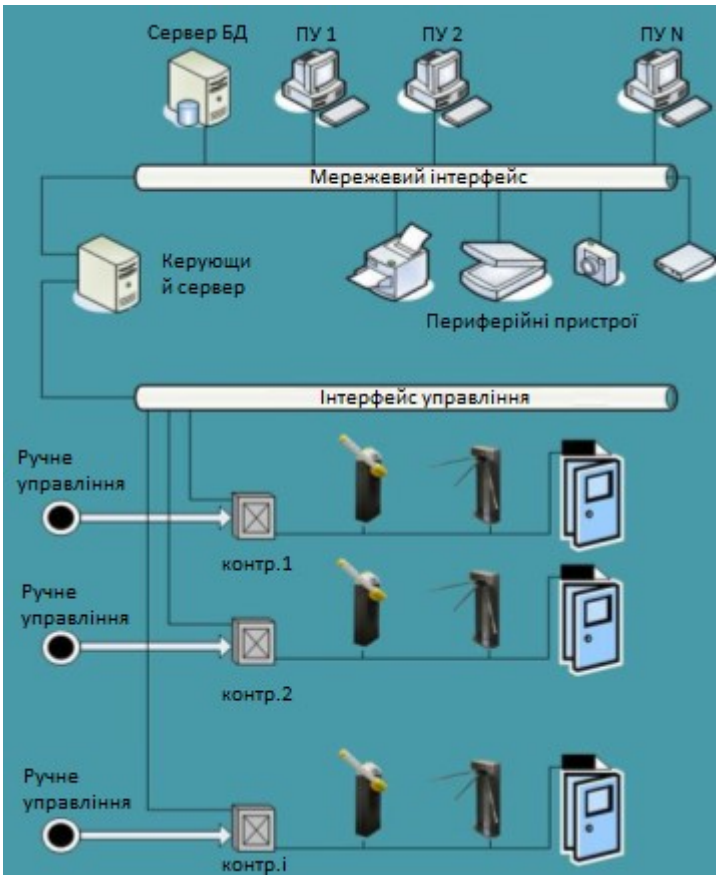


Рисунок 1.6 - Компоненти мережевої багатофункціональної системи контролю доступом

На рисунку представлений найбільш загальний варіант СКУД. За всіма процесами в системі стежить керуючий сервер. Керуючий сервер пов'язаний з мережі з сервером бази даних, пультами управління ПУ 1 - ПУ N, периферійним обладнанням, таким як принтери для друку звітів або пластикових карт, модемами, сканерами, фотоапаратами. З іншого боку керуючий сервер стежить за станом усіх контролерів, а отже і всього устаткування ідентифікації та ПВІП. Зв'язок цей здійснюється за певними протоколами, відмінними у різних виробників, і, як правило, за допомогою інтерфейсів RS-232 і RS-485. Контролери пов'язані виконавчими пристроями (шлагбаумами, турнікетами, електрозамками і т.п.) і пристроями ідентифікації (proximity зчитувачами, ключами touch memory, біометричними ідентифікаторами).

В системах ручне управління здійснюється з пультів, розташованих, як правило на точках входу на об'єкт. Дана схема може видозмінюватися в залежності від виробника обладнання.

Робота системи відбувається наступним чином. Людина підходить до ПВІП, наприклад, до турнікету і ідентифікується в системі, прикладанням proxymity карти (ключа touch memory, відбитка пальця, введенням коду) до зчитувача, розташованого як правило в безпосередній близькості від турнікета (на рисунку зчитувачі не показані). Далі, контролер мережи, отримавши інформацію від зчитувача звіряє, зіставляє унікальний номер ідентифікатора з наявною в його пам'яті базою, а так же відправляє запит на керуючий сервер, який, в свою чергу, звертається до сервера бази даних. Якщо такий ідентифікатор існує в системі, то контролер замикає реле або сухі контакти, підключені до конкретного турнікету і відкриває його, а керуючий сервер передає інформацію на ПК служби. Також, на екран ПУ, закріпленого за розглянутою точкою входу, виводиться інформація про власника ідентифікатора (посада, рівень допуску, фотографія і т.п.). Ця інформація адресована співробітникам служби охорони, які контролюють даний турнікет. Крім того, в журналі подій системи фіксується інформація

про вхід співробітника або гостя в даний час. При виході співробітника відбувається аналогічний процес, тільки з іншого боку входу.

У бюро виписки пропусків можливе отримання тимчасового дозволу на вхід на територію об'єкта. Для таких випадків, а також для випадків екстрених ситуацій, передбачений ручний режим відкриття турнікетів. Описаний алгоритм сильно спрощений, проте основні точки в ньому описані.

Для отримання принципової схеми простіших СКУД досить виключити частину обладнання з наведеної (наприклад можна залишити тільки контролер мережи, турнікет зі зчитувачем і пульт управління, така комбінація реалізує схему автономної однорівневої СКУД).

Найбільш простою системою контролю доступом є добре всім відомий домофон. У ряді випадків він інтегрується з системою відеоспостереження, в цьому випадку користувач отримує відеодомофон.

1.5 Постановка задачі

Мета роботи – розробка програмної системи "Електронна перепустка". Для досягнення мети поставлено наступні задачі:

- провести аналіз предметної області;
- визначити особливості систем контролю та управління доступом;
- обрати мову програмування;
- розробити моделі та алгоритми управління доступом для системи;
- обрати технологію та розробити програмне забезпечення;
- перевірити роботу системи з використанням тестового матеріалу;
- зробити висновки.

2 ВИБІР МОВИ ПРОГРАМУВАННЯ

Процедурні мови програмування є традиційними, вони лише зазнали змін від неструктурних до структурних мов програмування.

Об'єктно-орієнтоване програмування - порівняно новий напрям, однак воно в концептуальному плані більш привабливо, дозволяє розглядати і реалізовувати інформаційні та функціональні властивості об'єктів в нерозривному зв'язку.

2.1 Традиційні системи програмування

Традиційні системи програмування представлені засобами створення додатків на мовах третього покоління 3GL: C, Pascal, Basic та ін. Інструментальні засоби програмування можуть бути представлені набором окремих утиліт (редактор текстів, компілятор, компонувальник і відладчик) або інтегрованим середовищем програмування.

Системи програмування 3GL потрібні для організації спеціальних модулів в інформаційних програмах, для створення ефективних за швидкодією програм обробки даних. Для створення за допомогою систем програмування повноцінних інформаційних програм необхідно розширити їх за рахунок використання бібліотек діалогу і доступу до баз даних, а також макросредств вбудованої мови структурованих запитів Embeded SQL [4].

2.2 Об'єктно-орієнтовані системи програмування

Властивостями об'єктно-орієнтованих мов, що зумовлюють їх переваги, є приховування деталей реалізації об'єкта (інкапсуляція),

успадкування процедурних та інформаційних частин від об'єктів-батьків, поліморфізм як можливість налаштування на різні типи даних і ін. Прикладами об'єктно-орієнтованих систем програмування є C++ і Object Pascal.

Систему програмування Visual Basic можна використовувати для створенн простих автономних додатків і компонентів VBX і OCX, для розширення і інтеграції функціональних пакетів (Word, Excel, Access), а також як засіб програмування для розширення систем документообігу і для створення утиліт адміністрування.

Застосування Delphi можливо для створення розрахунково-аналітичних програм, для розробки DLL, для супроводу і розвитку розробок, виконаних на Turbo і Borland Pascal, а також для швидкого створення додатків. У ряді випадків вирішальним для вибору будуть помірні вимоги Delphi-додатків до системно-технічного забезпечення.

C++ застосовується для розширення системного програмного забезпечення, для розробки великих проектів, спеціальних додатків, створення бібліотек та класів для предметної області, розробки динамічних бібліотек DLL, створення програмного забезпечення для серверів додатків, використання спільно з CASE-системами, забезпечення багатоплатформності і переносимості (за стандартом ANSI).

2.3 Мова програмування Delphi

Як засоб розробки програми будемо використовувати мову Delphi, яка забезпечує програмісту розробку Windows додатків на професійному рівні. Delphi дозволяє розробнику витрачати менше часу на розробку інтерфейсу програми, а більше часу витрачати на написання коду програми.

Delphi включає в себе:

– 32-бітовий компілятор Object Pascal;

– об'єктно-орієнтований конструктор форм;

– архітектуру віртуальних даних, що дозволяє включити ваші власні засоби роботи з базами даних в VCL;

– повну підтримку Win32 API, включаючи COM, використання керуючих елементів ActiveX, багатопоточність і різні Software Development Kit (SDK) від Microsoft і сторонніх виробників;

– інструментарій для інтеграції користувальницьких звітів QuickReports;

– додатковий інструментарій для роботи з базами даних, включаючи Database Explorer, підтримку джерел даних ODBC і низькорівневий інтерфейс доступу до баз даних Borland Database Engine (BDE);

– InsiallSHIELD Express - інструментарій для поширення додатків;

– Open Tools API для розробки компонентів, інтегрованих із середовищем Delphi;

– вихідні тексти VCL і бібліотеки часу виконання (Runtime library, RTL);

– технології WebBroker, включаючи майстрів і компоненти, що полегшують розробку додатків, що використовують ISAPI, NSAPI, WinSock і CGI;

– драйвери для доступу до баз даних InterBase, Oracle, Microsoft SQL Server. Sybase, Informix і DB2;

– SQL Database Explorer, що дозволяє переглядати і редагувати специфічні метадані сервера;

– SQL Monitor, що забезпечує перегляд повідомлень обміну інформацією з сервером і полегшує налагодження та налаштування додатка;

– Data Pump Expert для швидкого підведення підсумків.

В основі Delphi лежить об'єктно-орієнтована версія мови Pascal, яка називається Object Pascal. Object Pascal містить безліч наступних доповнень і змін:

– обробка виключень (exception handling), що забезпечує відновлення після помилок під час виконання програми;

– інформація про типи часу виконання (Runtime Type Information, RTI), яка дозволяє визначати типи об'єктів під час виконання, а не на етапі компіляції програми;

– підтримка інтерфейсів, що полегшує розробку додатків з використанням COM;

– рядки необмеженої довжини, що дозволяють зосередити увагу і зусилля на написанні програми, а не на вирішенні проблем виділення пам'яті або виходу за кордон;

– тип даних Variant, що дозволяє використовувати технології типу OLE і "не типізовані" дані.

Visual Component Library (VCL) являє собою набір класів Delphi. Ця бібліотека, подібна відомим бібліотекам Object Windows Library (OWL) і Microsoft Foundation Classes (MFC), забезпечує об'єктно-орієнтоване середовище навколо найбільш часто використовуваних функцій Win32 API. Основна перевага VCL полягає в її повній інтегрованості з візуальним середовищем розробки. Кожен компонент, який перетягується з Component Palette в форму, являє собою елемент VCL.

3 РЕАЛІЗАЦІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ПРОЕКТУ

Програмне забезпечення, яке встановлюється на комп'ютер кожної з автоматизованих прохідних, назвемо програмою моніторингу "KppMonitor". Моніторинг являє собою незалежну програму. Це означає, що вона функціонує окремо від інших частин комплексу.

Програмне забезпечення, яке встановлюється на головний комп'ютер, назвемо програмою віддаленого доступу до автоматизованих прохідних "KppManager". Віддалений доступ буде можливий тільки в тому випадку, якщо комп'ютер віддаленої автоматизованої прохідної включений і функціонує.

3.1 Розробка бази даних

Загальна база даних підприємства буде розподілена по локальних базам даних автоматизованих прохідних, що є необхідним для найбільш швидкого доступу до неї. У базі даних кожної автоматизованої прохідної будуть зберігатися відомості про тих співробітників, яких вона обслуговує. Крім того, для взаємодії програмного забезпечення з локальною базою даних на комп'ютері кожної прохідної необхідно буде встановити Borland Database Engine, що входить в стандартну поставку Delphi.

Локальна база даних у вигляді окремих файлів-таблиць розташовується на жорсткому диску в одному каталозі, для простоти і зручності роботи шлях до якого буде прописаний в аліас конфігураційного файлу Borland Database Engine. Аліас - це механізм, що полегшує зв'язок взаємодії додатків з базами даних, в вміст якого крім шляху до бази даних також включається тип драйвера для роботи з БД і деяка інша системна інформація.

Логічну схему локальної бази даних, розробленої для зберігання інформації про структуру підприємства, співробітників і їхні права доступу, а також для зберігання подій, що відбуваються на автоматизованій прохідний, представлено на рисунку 3.1

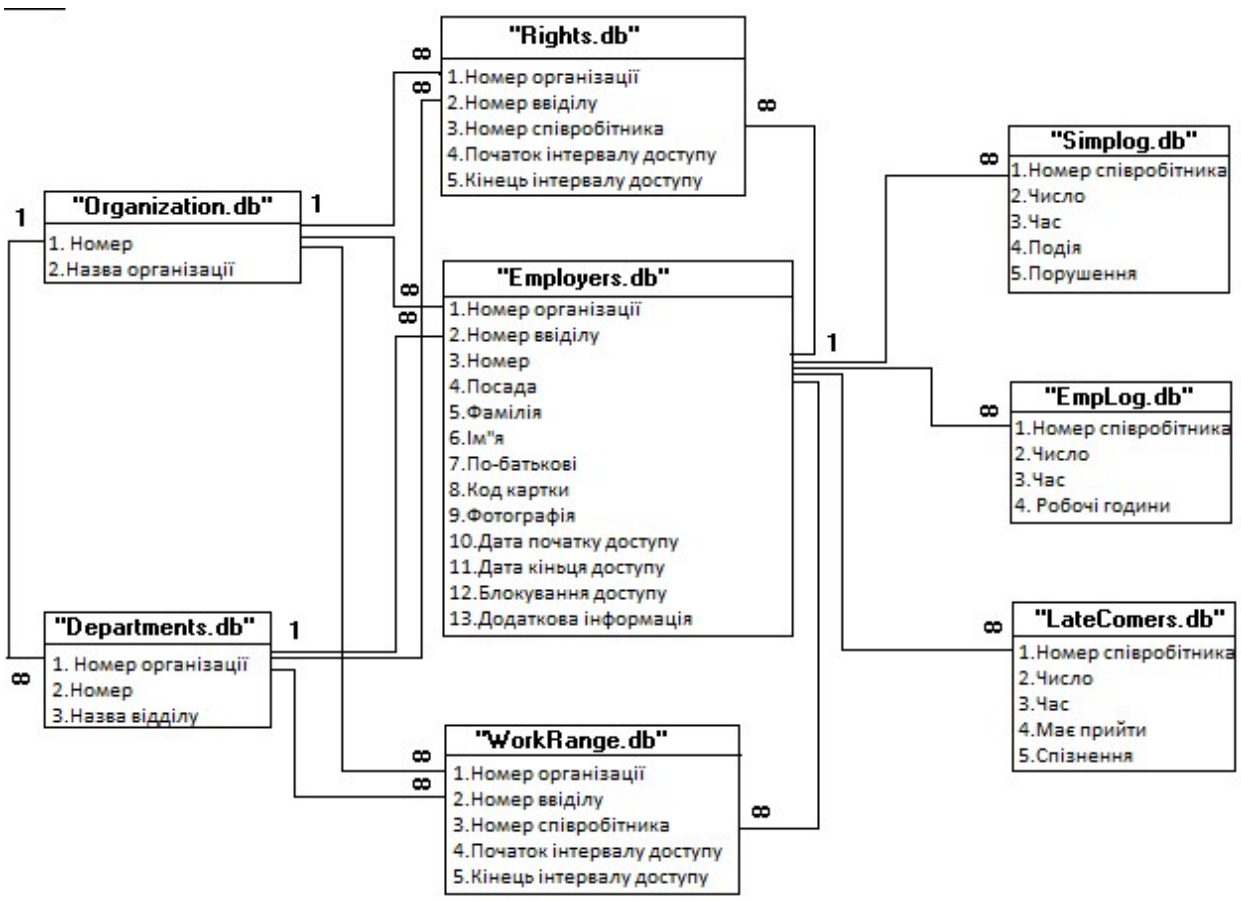


Рисунок 3.1 - Логічна схема бази даних

Зв'язки між таблицями встановлені таким способом, щоб завжди по номеру потрібного нам співробітника можна було отримати повну інформацію, що стосується його.

Перерахуємо назви всіх таблиць бази даних і опишемо для чого кожна з них призначена:

- "Organization.db" - зберігає список організацій підприємства. Містить поля: org - номер (індекс) організації, org_desc - назва організації.

- "Departments.db" - зберігає список відділів організацій підприємства, для чого має зв'язок з таблицею "Organization.db". Містить поля: org - номер організації в таблиці "Departments.db", dep - номер (індекс) відділу, dep_desc - назва відділу.

- "Employers.db" - таблиця співробітників підприємства, для кожного з яких визначено відділ і організація яким він належить. Поля таблиці: org, dep - номер організації, відділу для співробітника, empkey - номер співробітника в таблиці, tabnum - займана посада, Fname, Lname, Mname - прізвище, ім'я, по батькові, keycode - код картки, photo - фотографія, startacces, endaccess - дати початку і кінця доступу по картці, blocking - блокування доступу, addinfo - додаткова текстова інформація.

- "Rights.db" і "WorkRange.db" - необхідні відповідно для зберігання прав доступу співробітників на територію підприємства і інтервалів робочого часу, в перебігу яких співробітники зобов'язані перебувати на робочому місці. Поля: org, dep, empkey - номера організації, відділу, співробітника для яких встановлюється часовий інтервал: t_from, t_to.

- "Simplog.db" - журнал для фіксування подій (входи/виходи) і їх можливих порушень. Поля: empkey - номер співробітника в таблиці "Employers.db", today, time - дата і час, event - подія, alert - порушення.

- "EmpLog.db" - журнал для запису проведених інтервалів робочого часу. Поля: empkey - номер співробітника в таблиці.

- "Employers.db", today, time - дата і час, accesstime - інтервал проведеного робочого часу.

- "LateComers.db" - журнал для фіксування запізнень співробітників відповідно. Поля: empkey - номер співробітника в таблиці "Employers.db", today, time - дата і час, mustcome - час необхідного приходу співробітника, lating - запізнення.

- "Systemt.db" - зберігає закодовані паролі для входу в систему. Поля: loginname - ім'я користувача, password - пароль.

3.2 Створення локальної бази даних

Створити описану базу даних можна за допомогою утиліти DataBase DeskTop (DBD), що входить в стандартну поставку Delphi. Опис для роботи з утилітою можна знайти в [5].

Після створення необхідно зареєструвати аліас бази даних в файлі конфігурації Borland Database Engine "Idapi.cfg", що полегшить в подальшому розробку програми. Для цього скористаємося утилітою BDE Administrator. У розділі "Object" виберемо пункт "New", вкажемо в вікні тип драйвера "STANDART" для роботи з базою даних і в розділі визначення параметрів нового аліаса (розділ "Definition"), навпроти рядка "Path" вкажемо повний шлях до місця положення нашої бази даних на жорсткому диску. Потім назвемо створений аліас, як "KppBase".

Після створення, локальну базу даних необхідно оголосити доступним ресурсом в мережі Windows Network і обмежити доступ до неї. Це необхідно для того, щоб за допомогою програми віддаленого доступу мати можливість приєднуватися до неї.

Скористаємося програмою explorer.exe, в якій вкажемо шлях до створеної бази даних натиснемо правою клавішею миші на ньому, виберемо пункт "доступ". У вікні встановимо опцію "Загальний ресурс", в поле "Мережеве ім'я" призначимо ресурсу ім'я, під яким він буде видний в мережі (наприклад "KppBase"), далі визначимо тип доступу, як "повний" і в полі "пароль для повного доступу" встановимо пароль.

Тепер для мережевого при'єднання до локальної бази даних необхідно буде знати пароль, який обмежить доступ до неї.

Програма моніторингу буде включати в себе наступні модулі:

- Модуль для входу в систему.
- Модуль даних для зв'язку з базою даних.
- Модуль для реалізації зв'язку з COM-портом.
- Головний модуль, до якого будуть підключатися інші.

Головна функція роботи цього модуля полягає в тому, щоб запобігати несанкціонований доступ третіх осіб до роботи в програмі. На вході в систему буде запитуватися роль користувача в системі і пароль до неї. Визначено дві ролі: "Admin" і "Operator", вони відрізняються тим, що користувач з роллю "Admin" має право доступу і зміни програмних налаштувань, в той час, як "Operator" може лише спостерігати коректність роботи програми і вживати необхідних заходів в екстрених випадках (тобто виконує функції охоронця).

Паролі будуть у файлі-таблиці "SystemT.db" в закодованому вигляді, причому для кодування паролів використовується компонента TBlowFish. Нижче наведено фрагмент програми кодування паролів:

```
LoginName: = 'ADMIN';
BF1.Key: = 'password';
StrPCopy (Buffer, LoginName);
BF1.EncryptBlock (buffer, length (LoginName);
```

Вид вікна із запитом ролі користувача і пароля наведено в додатку А, (рис. А1).

3.3 Модуль даних

Для зв'язку програми з базою даних через Borland Database Engine в середовищі розробки додатків Delphi передбачений спеціальний модуль даних TDataModule, форму якого можна створити в меню File, пункт New DataModule.

Форма модуля даних спеціально призначена для розташування на ній компонент Delphi для роботи з базами даних [9]. Перерахуємо потрібні для програми компоненти:

– RightsQuery: TQuery - служить для генерування запитів до бази даних з метою визначення прав доступу співробітника за кодом його карти.

– AutoDelQuery: Tquery - використовується з метою автоматичного Автовидалення застарілих даних з журналів прохідний.

– StatQuery: Tquery - для занесення записів подій в журнали прохідний.

Щоб прив'язати ці компоненти конкретно до нашої створеної локальної бази даних, необхідно в їх властивостях навпроти напису "DataBaseName" написати ім'я зареєстрованого раніше аліаса "KppBase".

3.4 Модуль зв'язку з COM-портом

Для управління програмою турнікетом через контролер турнікета потрібно реалізувати зв'язок "комп'ютер-контролер" через стандартний COM-порт. Для цього можна скористатися компонентою TApdComPort [10].

Розмістимо компоненту на головній формі проекту в Delphi, компонента має перелік властивостей, які необхідно правильно налаштувати:

– ComNumber - номер COM-порту комп'ютера, до якого буде підключатися контролер.

– До порту COM1 зазвичай приєднана мишка, тому встановимо значення цієї властивості в "2"; ComSpeed - швидкість обміну по порту. Стандартна швидкістю 9600 кбіт/с.

Інші налаштування можна залишити так, як вони встановилися за замовчуванням.

У самій програмі для встановлення зв'язку комп'ютера з контролером через COM-порт створимо новий процес, описуваний класом TThread, який за допомогою компоненти TApdComPort прив'язується за вказаним номером COM-порту і посилає контролеру команди управління, одночасно читаючи відповіді, що приходять.

У таблиці 3.1 наведено список команд управління, що розуміються контролером.

Таблиця 3.1. Список команд управління контролером.

Get_st2	Команда, після якої контролер посилає у відповідь статус-байт про свій поточний стан.
Id1 (Id2)	Отримати лічений код з зчитувача N1 (або N2)
Llamp_on (Llamp_off)	Запалити (погасити) ліву стрілку на турнікеті
Rlamp_on (Rlamp_off)	Запалити (погасити) праву стрілку на турнікеті
Slamp_on (Slamp_off)	Запалити (погасити) хрестик на турнікеті
Lsol_on (Lsol_off)	Відкрити (закрити) турнікет для проходу вліво
Rsol_on (Rsol_off)	Відкрити (закрити) турнікет для проходу вправо

Для зв'язку з контролером турнікету створимо клас ComPortThread, що має своїм предком клас TThread, в який були включені наступні процедури і функції:

– constructor Create (Query: TQuery) - створення екземпляра класу, з передачею йому в якості параметра компонента TQuery, для реалізації необхідних запитів до бази даних.

– procedure Execute; override; - для запуску і синхронізації з основним потоком. 30 procedure MainCycle; - тіло нового процесу, в якому були написані вироблені їм дії.

– function GetRights (EmpKey: integer): boolean; - функція визначення прав доступу для співробітника з ключем EmpKey, що повертає в якості результату роботи "true" - якщо доступ дозволений і "false" - якщо в доступі відмовлено.

– procedure Open_tur (direction: short); - відкриття турнікета в ту чи іншу сторону, залежно від параметра "direction".

– procedure WrStat (mode: integer; emp: longint); - запис в журнал реєстрації події, що сталася.

Тоді блок-схема роботи алгоритму в модулі може бути представлена у вигляді:

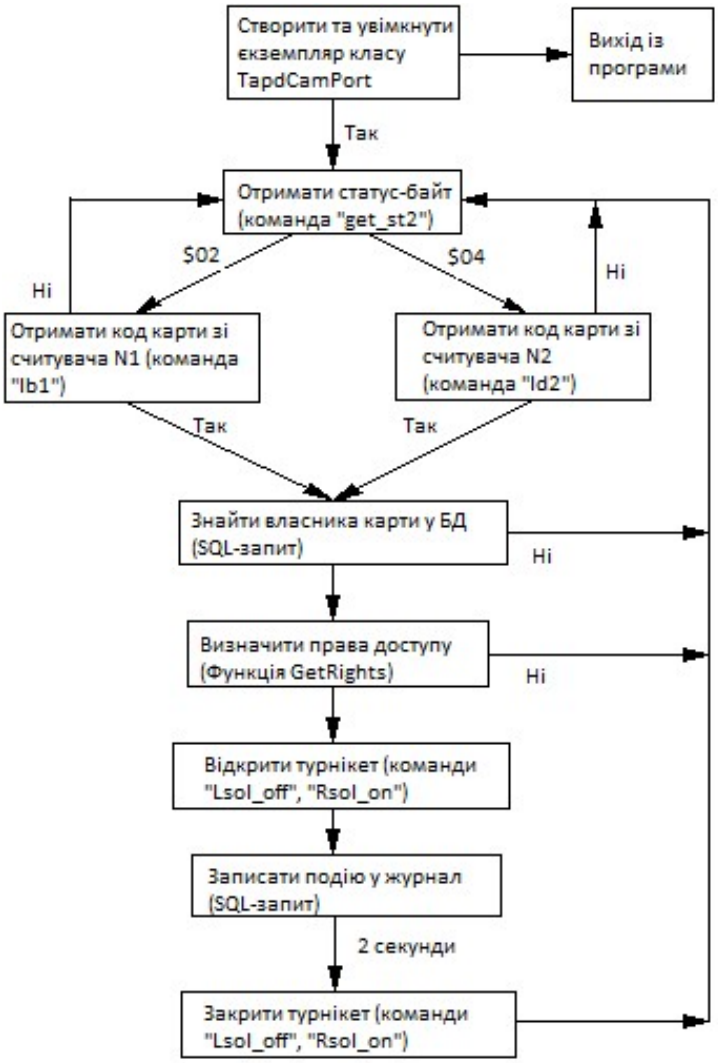


Рисунок 3.2 - Блок-схема роботи алгоритму в модулі

Детальніше зупинимося на кроці алгоритму «Запис події в журнали».

У таблицю "Simplog.db" запишеться дата, час, дані про співробітника і тип події: "увійшов" або "вийшов", щоб надалі по цій таблиці можна було отримати перший тип звіту ("Прохідна ').

У таблицю "EmpLog.db" в разі "входу" співробітника занесеться запис виду: дата, час, співробітник. У разі "виходу" спочатку знайдеться найостанніша запис "входу" для цього співробітника, потім відбудеться підрахунок різниці часу "виходу" і "входу" з урахуванням накладення маски

інтервалів робочого часу (наприклад, обідній час не береться до уваги) з таблиці "WorkRange. db ", і остаточно оновиться знайдений запис, прийнявши вигляд: дата, час, співробітник, робочий час.

У таблицю "LateComers.db" в разі "входу" співробітника спочатку визначиться, чи входив сьогодні вже? При негативній відповіді час "входу" співробітника зрівняється з часом приходу на роботу з таблиці "WorkRange.db" і при необхідності запишеться запізнення у вигляді: дата, час, співробітник, повинен прийти, запізнення.

3.5 Головний модуль

Головний модуль буде включати в себе початковий завантажувач програми, основні елементи інтерфейсу для зв'язку з користувачем і зв'язок з іншими модулями.

При запуску програми спочатку буде запускатися на виконання модуль входу в систему (в разі трьох невдалих спроб входу програма завершує свою роботу), який можна прив'язати, наприклад, на подію створення головної форми:

```
procedure TMainForm.FormCreate (Sender: TObject);
begin
if not (PasswordDialog.ShowModal = mrOK) then MainForm.Close;
```

Далі за допомогою компоненти Reg1: TLMDIniCtrl [Regestry] з системного реєстру зчитуються програмні установки:

```
// Номер COM-порту
COM_PORT: = Reg1.ReadInteger (IDS_ROOT, 'COM_PORT', 0);
// Швидкість обміну по порту
COM_SPEED: = Reg1.ReadInteger (IDS_ROOT, 'COM_SPEED1', 0);
// Автовидалення застарілих записів (вкл / викл)
AUTODEL: = Reg1.ReadInteger (IDS_ROOT, 'AUTODEL', 0);
```

// Період старіння записів в місцях

AUTODELPERIOD: = Reg1.ReadInteger (IDS_ROOT, 'AUTODELPERIOD', 0);

Потім перевіряється, чи підключений контролер до потрібного COM-порту, в разі позитивного результату створюється і запускається на виконання новий процес класу TApdComPort, що працює паралельно з основною програмою, інакше видається попередження про неможливість роботи з COM-портом.

try

if Com1 = nil then

begin

Com1: = ComPortThread.Create; // Створення екземпляра класу

Com1.Resume;

end;

except

ShowMessage ('COM-порт для турнікета зайнятий іншим пристроєм!');

end;

У разі вдалого розпізнавання введеного імені користувача і пароля з'явиться форма головного модуля, як показано в додатку А, рисунок А2.

Після появи форми робота головного модуля полягає в обробці чотирьох типів подій:

1) Вибір типу управління турнікетом: автоматичне або ручне. Подія настає при натисканні на кнопку з написом «Включити» (або «Вимкнути».) У разі активізації ручного управління, відкриття або блокування механізму турнікета здійснюється кнопками ручного пульта.

procedure TMainForm.Button1Click (Sender: TObject);

begin

if (Button1.Caption = 'Включити') then

begin

Com1.Resume; // Управління ведеться з процесу Com1

```
Button1.Caption: = 'Вимкнути';
end
else
begin
Com1.Suspend; // Управління бере на себе контролер
Button1.Caption: = 'Включити';
end;
end;
```

2) Поміняти програмні установки. За допомогою компоненти TLMDIniCtrl записуємо в реєстр нові настройки:

```
// Номер COM-порту
Reg1.WriteInteger (IDS_ROOT, 'COM_PORT', COM_PORT);
// Швидкість обміну по порту
Reg1.WriteInteger (IDS_ROOT, 'COM_SPEED1', COM_SPEED);
// Автовидалення застарілих записів (вкл / викл)
Reg1.WriteInteger (IDS_ROOT, 'AUTODEL', AUTODEL);
// Період старіння записів в місцях
Reg1.WriteInteger (IDS_ROOT, 'AUTODELPERIOD', AUTODELPERIOD);
```

3) Автовидалення застарілих записів в журналах прохідний. Подія спрацьовує кожний день у визначений час (компонента TRxClock [RXClock]) і, керуючись програмними настройками (Автовидалення) здійснює очищення журналів від старих записів за допомогою SQL-запиту за допомогою компоненти TAutoDelQuery:

```
procedure TMainForm.RxClock1Alarm (Sender: TObject);
begin
SQL.Clear;
SQL.Add ( 'delete from simplog, EmpLog, LateComers where TODAY <: TODAY');
Parambyname ( 'TODAY'). Asdatetime: = Date-AUTODELPERIOD * 30;
```

```
try
prepare;
ExecSQL;
except
MessageDlg ( 'Помилка підключення до БД!', MtError, [mbok], 0);
exit;
end;
```

Програма віддаленого доступу до локальних баз даних, розташованих на комп'ютерах автоматизованих прохідних в загальному випадку вимагає наявності наступних ресурсів комп'ютера:

- Встановлений Borland Database Engine для взаємодії з віддаленою базою даних.

- Підключення до мережі Windows Network підприємства для віддаленого доступу до даних.

- Підключений до COM-порту локальний контролер для призначення кодів карт співробітникам.

Перерахуємо також модулі, з яких буде складатися програма:

- Модуль авторизації.

- Модуль для зв'язку з базою даних.

- Модуль для підключення до мережі.

- Модуль для генерації звітів і їх експорту.

- Модуль для роботи з базою даних.

- Головний модуль, до якого будуть підключатися інші.

3.6 Модуль для зв'язку з базою даних

Модуль авторизації аналогічний модулю для входу в систему програми моніторингу та виконує таку ж функцію захисту від несанкціонованого доступу до функцій програми.

Скористаємося все тим же модулем даних TDataModule для створення зв'язку з локальними базами даних автоматизованих прохідних. Розмістимо на нього компоненти:

- DataBase1: TDatabase - для підключення бази даних;

- EmpTable: TTable - для доступу до записів в таблиці співробітників;

- ReportQuery: TQuery - для отримання зібраних статистичних даних з віддаленої бази даних;

- PasswordQuery1: TQuery - для доступу до таблиці з паролями для авторизації в програмі віддаленого доступу;

- EmpQuery: TQuery - для редагування інформації про співробітників у віддаленій базі даних;

- Query1: TQuery - для тимчасових потреб.

Для компоненти Database1 необхідно зареєструвати порожній аліас з ім'ям BossClientBase, параметри якого програмно будуть заповнюватися кожен раз інформацією про ту з баз даних, до якої програма буде виконувати підключення. Потім встановимо властивості:

AliasName = BossClientBase; // Назва порожнього аліаса

DatabaseName = ClientBase; // Назва локальної бази даних

Для всіх інших компонент необхідно встановити властивість:

DatabaseName = ClientBase, щоб вказати, що ці компоненти відносяться безпосередньо для роботи з тією базою даних, параметри якої задані в властивості компоненти DataBase1.

3.7 Модуль для підключення до мережі

Щоб приєднатися до бази даних скористаємося компонентом Database1: TDatabase, розміщеної на формі модуля даних. У цій компоненти є властивість Params, яка містить список параметрів, переданих Borland

Database Engine при встановленні зв'язку з якою-небудь базою даних. При підключенні задамо наступний параметр:

Path = \\ <IP_address> \ <Net_Resource_Name> \ <DB_Path>,

де Path - назва переданого параметра (в даному випадку параметр, що містить шлях до БД), IP_address - четирехбайтна адреса комп'ютера в мережі, Net_Resource_Name - назва доступного (Shared) мережевого ресурсу, а DB_Name - шлях до бази даних на доступному мережевому ресурсі, наприклад, "Path = \\ 198.162.10.40 \ D_DISK \ DATABASES \ DB1 \". Весь ций ланцюжок носить назву UNC – ім'я і є значенням параметра Path. Таким чином, підключення, що виконується, буде використовувати протокол TCP/IP для встановлення зв'язку і передачі даних.

У разі, якщо потрібно підключитися до локальної бази даних, параметр буде мати спрощений вигляд:

Path = <DB_Path>,

де DB_Path містить повний шлях до бази даних на локальному або підключеному мережевому диску, наприклад, "Path = C: \ DATABASES \ DB1".

Програмно всі описані дії можна реалізувати так:

DataBase1.Connected: = false; \\ Від'єднуємо БД

Database1.Params.Clear; \\ Очищаємо список параметрів

Database1.Params.Add ('PATH =' + DBName); \\ Додаємо

де DBName - рядок, що містить UNC-ім'я.

Але, треба не забувати, що для доступу до бази даних, що підключається, як до мережного ресурсу необхідно якимось чином передавати пароль при підключенні, інакше в доступі буде відмовлено (так як автоматично пароль запитуватися не буде). Для цього скористаємося засобами WinAPI [11]. Спеціально призначена функція WNetAddConnection3() дозволяє програмним шляхом встановлювати з'єднання з ресурсами мережі, передаючи в якості одного з параметрів пароль

до мережного ресурсу. Прототип функції можна дізнатися в "Win32 Programmer's reference".

Дії для під'єднання мережевого ресурсу, такі:

NR.dwType: = RESOURCETYPE_DISK; // Тип ресурсу - диск

NR.lpLocalName: = nil; // Ім'я локального диска

NR.lpRemoteName: = PChar (DBName); // UNC-ім'я

NR.lpProvider: = nil; // Провайдер за замовчуванням

WNetAddConnection3 (0, NR, Password, UserName,

CONNECT_UPDATE_PROFILE);

де NR - структура типу TNetResourceA, DBName - UNC-ім'я під'єднується ресурсу, Password - рядок з паролем, UserName - рядок з ім'ям користувача (у разі визначення доступу до ресурсів на рівні користувачів), а CONNECT_UPDATE_PROFILE - константа, оновлююча профіль поточного користувача в системі шляхом додавання UNC-ім'я в список мережних ресурсів, що підключаються.

Далі необхідно встановити властивість:

Database1.Connected = true,

для виконання під'єднання до віддаленої бази даних.

3.8 Модуль для генерації звітів і їх експорту

Після того, як віддалена база даних буде успішно приєднана, можна почати роботу зі збору накопичених статистичних даних і генерації звітів по ним. Скористаємося компонентою ReportQuery: TQuery, що дозволяє за допомогою SQL-запитів одержувати записи з бази даних, що задовольняють параметрам цього запиту. Компонента ReportQuery має властивість SQL, яка в текстовому вигляді містить SQL-запит. Для генерації чотирьох типів звітів запити будуть мати вигляд:

1.Звіт по прохідний. Потрібно вибрати всіх співробітників, які відзначалися на прохідній за певний період часу:

ReportQuery.SQL.Clear; // очистимо запит

ReportQuery.SQL.Add ('select today, entertime, event, lname, org_desc, dep_desc from simplog.db, employers.db, organizations.db, departments.db

where simplog.today> =: datestart and simplog.today <=: dateend ');

ReportQuery.Open; // Зробити запит

де datestart і dateend визначають період звіту і описуються типом TdateTime.

2. Звіт про робочий час. Необхідно підрахувати сумарний робочий час для конкретного співробітника, проведений на робочому місці за певний період часу, або для всіх співробітників відділу, організації або підприємства в цілому. Одним SQL-запитом цього зробити не можна, тому звіт будемо отримувати в кілька етапів.

Спочатку отримаємо список співробітників для звіту:

ReportQuery.SQL.Clear;

case Type of

// Отримати список всіх співробітників

-1: SQL.Add ('select * from Employers.db);

// Отримати всіх співробітників обраної організації

0: SQL.Add ('select * from Employers.db and Org =' + Org_desc);

// Отримати всіх співробітників обраного відділу

1: SQL.Add ('select * from Employers.db where Dep =' + Dep_desc);

// Отримати 1 співробітника

2: SQL.Add ('select * from Employers.db where Lname =' + LName); end;

ReportQuery.open;

де змінна Type - підтип звіту, Org_desc, Dep_desc - рядки, що містять назву організації або відділу, LName - прізвище конкретного співробітника.

Далі, перебираючи отриманих співробітників, будемо підраховувати для кожного з них інтервали робочого часу з таблиці "EmpLog.db":

```
ReportQuery.First; // Встановимо покажчик на перший знайдений запис
while not ReportQuery.EOF do // перебираємо співробітників
begin
TmpQuery.SQL.Clear;
TmpQuery.SQL.Add ( 'select AccessTime from Emplog.db where Empkey =: Empkey and today> =: DateStart and today <=: Dateend and accesstime is not null');
TmpQuery.ParamByName ( 'EmpKey'). Asinteger: = ReportQuery.FieldByName ( 'EmpKey'). AsInteger;
TmpQuery.Open;
// якщо знайшли інтервали робочого часу
if TmpQuery.Recordcount> 0 then
begin
TmpQuery.First; // Беремо перший
While not TmpQuery.EOF do // Підсумовуємо з іншими
begin decodetime (fieldbyname ( 'accesstime'). asdatetime, hour, min, sec, msec);
hours: = hours + hour;
mins: = mins + min;
if mins> = 60 then
begin hours: = hours + (mins div 60); mins: = mins mod 60; end;
TmpQuery.Next; end;
end;
ReportQuery.Next; // Беремо наступного співробітника
end;
```

Таким чином можна підрахувати повний робочий час за певний період.

3.Звіт про відсутніх. По суті, цей звіт вимагає перевірки, чи був зареєстрований співробітник в журналі прохідний в певний період. SQL-запит буде таким:

```
ReportQuery.Clear;
```

ReportQuery.SQL.Add ('select org_desc, dep_desc, lname from Organization.db, Departments.db where empkey not in (select distinct empkey from Simplog.db where today> =: DateStart and today <=: Dateend)');

ReportQuery.Open; // Зробити запит

4. Звіт про тих, хто запізнився. Отримання списку співробітників, що мають запізнення за певний період. Може бути сформований таким запитом:

ReportQuery.Clear;

ReportQuery.SQL.Add ('select org_desc, dep_desc, lname, mustcome, lating from Organization.db, Departments.db, Employers.db, LateComers.db where Employers.empkey = LateComers.empkey and today> =: DateStart and today < =: Dateend ');

ReportQuery.Open; // Зробити запит

Після отримання відповідей з бази даних на запити, звіт можна переглянути на екрані, скориставшись в Delphi палітрою компонент QReport. З усієї палітри знадобляться наступні компоненти:

– QuickReport: TQuickRep - макет сторінки формату A4 для розташування на ньому елементів звіту. Володіє можливостями перегляду сторінки під різним збільшенням, записи і завантаження сторінки в формат ".QRP", а також виведення сторінки на друк;

– Band1, Band2: TQRBand - для створення "шапки" і "тіла" таблиці;

– Org, Dep, Name: TQRLabel - написи назв в "шапці" таблиці;

– SysData: TQRSysData - висновок на макет службової інформації (дата, час, номер сторінки звіту);

– Org_desc, Dep_desc, Fname: TQRDBText - для виведення списку отриманих записів з відповідних назв полів бази даних;

– Alert: TQRDBExpr - для створення тригерів на висновок записів з бази даних (умовні оператори, логічні вирази).

Як джерело даних у властивості "DataSet" всіх компонент потрібно вказувати назву компоненти "ReportQuery", яка буде містити список отриманих записів з бази даних.

Якщо потрібно експортувати отримані звітні дані для їх подальшого перерахунку, наприклад, за допомогою спеціально призначеної для цього програми Microsoft EXCEL, то найбільш простим варіантом буде перевести їх в зрозумілий EXCEL формат ".CSV".

Як можна дізнатися з [12], формат ".CSV" влаштований таким чином - це текстовий файл, в якому дані, що розміщуються за різними стовпцями таблиці EXCEL, розділяються між собою комами (Абревіатура "CSV" розшифровується, як Comma Separated Values, що в перекладі з англійської означає значення, розділені комами). А рядки таблиці EXCEL - це рядки текстового файлу.

3.9 Модуль для роботи з базою даних

Модуль для роботи з базою даних призначений для редагування і адміністрування інформації, що зберігається в ній. Наприклад, з його допомогою можна буде додавати, видаляти, редагувати інформацію про співробітників; заводити, видаляти, перейменовувати відділи та організації в структурі підприємства; призначати права доступу співробітникам і визначати рамки їх робочого часу. Крім того, експортувати дані за чотирма типами звітів в Microsoft Excel і видаляти застарілі записи з журналів прохідний.

Для наочного уявлення структури підприємства скористаємося стандартною компонентою Delphi TTreeView [13]. З її допомогою можна буде візуалізувати деревоподібну ієрархію підрозділів на головній формі програми. Дерево структури внутрішнього устрою всього підприємства можна представити трьома ярусами: організація - відділ - співробітник.

Спочатку, дані про структуру підприємства будуть читатися послідовно з трьох таблиць: "Organization.db", "Departments.db", "Employers.db" за допомогою найпростіших SQL-запитів на отримання

списку всіх наявних записів в конкретній таблиці і візуалізувати у видимій області компоненти EmpTreeView: TTreeView викликаючи методи:

EmpTreeView.Items.Add (organization); // додавання самого верхнього рівня в дереві;

EmpTreeView.Items.AddChild (Node, Name); // додавання підрівня

де organization - рядок з назвою організації, Node - структура типу TTreeNode, яка вказує рівень предка в дереві, Name - назва відділу або прізвище співробітника.

Далі, створивши компоненту EmpPopupMenu, описувану класом TPopupMenu і перерахувавши в її властивості "Items" необхідні пункти для роботи з базою даних "Додати", "Видалити", "Змінити", вкажемо її в якості меню, що з'являється, у властивості "PopupMenu" компоненти EmpTreeView, активізується при натисканні мишею на видиму область компоненти EmpTreeView. Потім додамо обробники перерахованих пунктів меню:

```
// Пункт меню "Додати"
EmpQuery.SQL.Clear; Case TreeLevel of
0: // додати нову організацію номер org, з назвою org_desc
EmpQuery.SQL.Add ( 'insert into organization values (org, org_desc)');
1: // додати новий відділ організації з номером org під номером dep
// з назвою dep_desc
EmpQuery.SQL.Add ( 'insert into departments values (org, dep, dep_desc)');
2: // додати нового співробітника у відділ номер dep організації номер
// org під номером EmpKey, з особистими даними
EmpQuery.SQL.Add ( 'insert into Employers values (org, dep, empkey, tabnum, keycode ...)');
End;
EmpQuery.Prepare; // Підготувати запит
EmpQuery.ExecSQL; // Реалізувати запит
// Пункт меню "Видалити"
EmpQuery.SQL.Clear;
```

```
Case TreeLevel of
0: // видалити організацію з назвою org_desc з усіма її відділами та
// співробітниками
EmpQuery.SQL.Add ( 'delete from organization, departments, employers where org_desc =: org_desc and organization.dep = departments.dep and organization.org = employers.org');
1: // видалити відділ з назвою dep_desc з усіма його співробітниками
EmpQuery.SQL.Add ( 'delete from departments, employers where dep_desc =: dep_desc and departments.dep = employers.dep');
2: // видалити співробітника номер під номером EmpKey
EmpQuery.SQL.Add ( 'delete from Employers where empkey =: empkey');
End;
EmpQuery.Prepare;
EmpQuery.ExecSQL; // Пункт меню "Змінити"
EmpQuery.SQL.Clear;
Case TreeLevel of
0: // перейменувати організацію з назвою org_desc в new_org_desc
EmpQuery.SQL.Add ( 'update organization set org_desc =: new_org_desc');
1: // перейменувати відділ з назвою dep_desc в new_dep_desc
EmpQuery.SQL.Add ( 'update departments set dep_desc =: new_dep_desc');
End;
EmpQuery.Prepare;
EmpQuery.ExecSQL;
```

Для того, щоб змінити особисті дані співробітника, необхідно створити і додати в проект нову форму, всередині якої буде відображатися особиста інформація про співробітника, що береться з бази даних для можливості її подальшої модифікації. На форму будуть розміщені такі компоненти:

- DBEditRole, DBEditFName, DBEditLName, DBEditMName, CodeEdit: TDBEdit - для зміни строкових полів в базі даних (посада, прізвище, ім'я, по батькові, код пропуску);

- EmpImage: TDBImage - для роботи з зображеннями формату "BMP" (фотографія);

- Blocking: TDBRadioGroup - для вибору перераховуються пунктів (пропуск: блокований / не блокувати);

- EmpMemo: TDBMemo - для відображення великих текстових полів (додаткова інформація);

- StartEdit, EndEdit: TDBDateEdit97 - для роботи з датами (період дії пропуску).

У властивості "DataSource" всіх цих компонент слід вказати джерело отримання даних з бази - компонент:

DataSource: TDataSource - зв'язок таблиці EmpTable бази даних з компонентами;

У самій таблиці EmpTable необхідно встановити властивість CashedUpdates = true,

Щоб всі зміни, вироблені за допомогою описаних компонент, накопичувалися в локальному кеші, а по завершенню редагування відсилалися в базу за допомогою методу EmpTable.Post.

Тепер зупинимося на адмініструванні бази даних і розглянемо питання про призначення прав доступу і встановлення рамок робочого часу для працівників. Таблиця "Rights.db" містить інформацію про права доступу, які можуть призначатися як безпосередньо для конкретного співробітника, так і для всього відділу співробітників або всієї організації в цілому. Для цього в полях таблиці org, dep, empkey відповідно встановлюються номера організації, відділу або співробітника, для яких діє тимчасове обмеження T_From, T_To - інтервал часу доступу на територію підприємства. Механізм успадкування прав такий, що пошук прав доступу буде здійснюватися спочатку для співробітника, потім для відділу, якому належить співробітник, і вже потім для організації, до якої входить співробітник.

Аналогічним чином влаштована таблиця "WorkRange.db", що містить інтервали робочого часу для працівників.

Скріншоти роботи програми з інформацією про КПП, підприємство, співробітника та його дії наведені у додатку А (рис. А3-А5).

3.10 Основний модуль

Основний модуль об'єднує в собі всі інші модулі і надає інтерфейс з вибору, що підключається до локальної бази даних лише у віддаленій автоматизованій прохідній.

Інтерфейс вибору, що підключається до бази даних, надає можливість вносити до списку автоматизованих прохідних нові прохідні, вказуючи в якості реєстраційних даних назву, шлях (UNC-ім'я) по якому буде здійснюватися підключення і будь-яку додаткову інформацію в якості коментаря.

Позиціонування в мережі Windows Network автоматизованої прохідної (її повне UNC-ім'я) можна реалізувати наступним чином через функції WinAPI:

```
// Функція визначення місця розташування ресурсу в мережі
function GetSelectedDir (Handle: THandle): string;
var
s: TBrowseInfoA;
IDList: PItemIDList; // Список ресурсів
function GetPathFromIDList: string;
var
Buf: array [0..MAX_PATH-1] of Char;
Res: Boolean;
begin
Result: = '';
if IDList <> nil then
begin
```

```
Res: = SHGetPathFromIDList (IDList, Buf); // вибрати шлях до БД
if Res then Result: = Buf else Exit;
end;
end;
begin
// Заповнюємо структуру TBrowseInfoA
s.hwndOwner: = Handle; // хендл вікна
s.pidlRoot: = nil;
s.pszDisplayName: = nil;
s.lpszTitle: = PChar ( 'Огляд мережевих ресурсів');
s.ulFlags: = 0; s.lpfn: = nil;
s.lParam: = 0;
s.iImage: = 0;
IDList: = SHBrowseForFolder (s); // виклик функції вибору шляху до БД
Result: = GetPathFromIDList; // Повернення результату: UNC-ім'я до БД
end;
```

Виклик функції GetSelectedDir (0) з передачею їй як параметр значення "0" - хендл поточного вікна, відобразить на екрані форму для навігації по всіх ресурсах мережі. Після вибору необхідного мережевого шляху, як результат роботи функція поверне повне UNC-ім'я для доступу до ресурсу, який можна буде додати до списку.

Алгоритм роботи наступний: зі списку зареєстрованих автоматизованих прохідних, що зберігається в локальному файлі "KppsData.ini" вибирається одна з них, до якої здійснюється підключення до мережі. Далі, користувач за допомогою модуля для отримання звітів може зібрати накопичену інформацію з журналів прохідний за певний період з можливістю її подальшого експорту в Microsoft Excel або модифікувати інформацію в базі даних співробітників підприємства за допомогою модуля для роботи з базою даних.

4 ТЕСТУВАННЯ ПРОЕКТУ

Працездатність всього комплексу перевірялася на двох комп'ютерах, на один з яких встановлювалася програма моніторингу, з підключенням всього необхідного апаратного забезпечення, що грав роль спеціалізованого комп'ютера на автоматизованій прохідній, на інший була встановлена програма віддаленого доступу.

Конфігурації комп'ютерів наведені в таблиці 4.1.

Таблиця 4.1 - Зміни комп'ютерів для тестування

Назва	Частота процесора	материнська плата	обсяг ОЗУ	Операційна система
Intel Core i3	3.2Ггц	Asus H110m	8Гб	Windows 10
Intel Core i5	3.4Ггц	Asus h310m	16Гб	Windows 7

Обидва комп'ютери були підключені до мережі Windows Network.

4.1 Тестування програми моніторингу

Тестування програми моніторингу проводилося за такими критеріями:

– Швидкість прийняття рішення програмою для блокування або пропуску співробітника по коду карти.

– Довжина кабелю між комп'ютером і контролером турнікету.

– Можливість роботи програми у фоновому режимі.

Результати тестування такі:

– Була заведена база даних на 10000 осіб, встановлена довжина кабелю 20 метрів, крім програми моніторингу на комп'ютері були запущені ще два додатки: Microsoft Word і Microsoft Excel.

– Час пошуку співробітника склав не більше 0,1 секунди (при виведенні фотографії співробітника розміром 5Kb на екран - не більше 0,5 секунди), що є достатнім для обслуговування безперервної черги людей на прохідній будь-якого підприємства. Довжина з'єднувального кабелю в цьому випадку цілком підходить для видалення комп'ютера від турнікета на потрібну відстань, а робота інших додатків показала, що комп'ютер на автоматизованій прохідній може паралельно з виконанням своєї основної функції використовуватися ще і для інших завдань, як, наприклад, набір тексту та нескладні математичні розрахунки.

4.2 Тестування програми віддаленого доступу

Основним критерієм при тестуванні програми віддаленого доступу був час отримання чотирьох типів звітів. Підключення до мережі здійснювалося з іншого сегмента мережі Windows Network, відстань між комп'ютерами була не менше 100 метрів. За допомогою програми "ping.exe" було визначено середній час отримання пакетів (по 32 байта), який склав 2 мс. База даних містила 2000 записів у всіх журналах прохідний. Всього було проведено 10 дослідів (табл.4.2).

Таблиця 4.2 - Результати часу отримання звітів

тест	звіт N1	звіт N2	звіт N3	звіт N4
час	19 сек.	18 сек.	4 сек.	20 сек.

де

"Звіт N1 "- звіт про прохідний;

"Звіт N2 "- звіт про робочий час;

"Звіт N3 "- звіт про відсутніх;

"Звіт N4 "- звіт про тих, хто запізнився.

На підставі отриманих результатів можна розрахувати приблизний час отримання звітів за місяць по накопиченим статистичним даним. Нехай на підприємстві працює 1000 Співробітників. В кожен з 22 робочих днів місяця в журнал прохідний додається в середньому по 10000 записів (дві на прихід і відхід з роботи, дві на прихід і відхід на обід і шість - на прихід і відхід по випадковим обставинам). Тоді за місяць буде накопичено 220000 записів, що в 100 разів більше, ніж було при тестуванні. Звідси випливає, що час отримання самого трудомісткого звіту за місяць склав 2000 секунд (або близько 34 хвилин). У підсумку можна сказати, що хоч результат не є хорошим з точки зору витраченого комп'ютерного часу (потрібно більше двох годин на отримання всіх звітів), але впровадження описаної технології дозволить перейти на новий виток створення високонадійних систем безпеки в тому числі і для підприємств з високим статусом секретності.

5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯЇХ

В даному розділі проведено аналіз потенційних небезпечних та шкідливих 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 була розробка програмного забезпечення для автоматизованого комплексу з метою забезпечення контрольованого доступу на територію підприємства і обліку робочого часу співробітників. Так як в процесі проектування використовувалося комп’ютерне обладнання, то аналіз потенційно небезпечних і шкідливих чинників виконується для персонального комп'ютера, на якому буде виконуватися розробка.

5.1 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» [1] 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.

Основним організаційним напрямом у здійсненні управління в сфері

охорони праці є усвідомлення пріоритету безпеки праці і підвищення соціальної відповідальності держави і особистої відповідальності.

5.2 Аналіз стану умов праці

Робота над створенням сервісу для системи обліку та тарифікації наданих послуг проходитиме в приміщенні багатоквартирного будинку. Для даної роботи достатньо однієї людини, для якої надано робоче місце зі стаціонарним комп’ютером.

5.2.1 Вимоги до приміщень

Геометричні розміри приміщення зазначені в табл. 5.1.

Таблиця 5.1 – Розміри приміщення

Найменування	**Значення**
Довжина, м	5
Ширина, м	5
Висота, м	2.8
Площа, $м^2$	25
Об’єм, $м^3$	70

Згідно з [2] розмір площі для одного робочого місця оператора персонального комп’ютера має бути не менше 6 кв. м, а об’єм — не менше 20 куб. м. Отже, дане приміщення цілком відповідає зазначеним нормам.

5.2.2 Вимоги до організації місця праці

При порівнянні відповідності характеристик робочого місця нормативним основні вимоги до організації робочого місця за [3] (табл. 5.2) і відповідними фактичними значеннями для робочого місця, констатуємо повну відповідність.

Приміщення знаходиться на другому поверсі трьох поверхової будівлі і має об’єм 70 $м^3$, площу – 25 $м^2$. Обладнано одне місце праці укомплектоване ПК.

Таблиця 5.2 - Характеристики робочого місця

Найменування параметра	Фактичне значення	Нормативне значення
Висота робочої поверхні, мм	700	680 ÷800
Висота простору для ніг, мм	750	не менше 600
Ширина простору для ніг, мм	550	не менше 500
Глибина простору для ніг, мм	700	не менше 650
Висота поверхні сидіння, мм	500	400 ÷500
Ширина сидіння, мм	450	не менше 400
Глибина сидіння, мм	470	не менше 400
Висота поверхні спинки, мм	400	не менше 300
Ширина опорної поверхні спинки, мм	400	не менше 380
Радіус кривини спинки в горизонтальній площині, мм	400	400
Відстань від очей до екрану дисплея, мм	750	700 ÷800

Температура в приміщенні протягом року коливається у межах 18–24°C, відносна вологість — близько 50%. Швидкість руху повітря не перевищує 0,2 м/с. Шум знаходиться на рівні 50 дБА. Система вентилювання приміщення — природна неорганізована, а опалення — централізоване.

5.2.3 Навантаження та напруженість процесу праці

За фізичним навантаженням робота відноситься до категорії легкі роботи (Іа), її виконують сидячи з періодичним ходінням. Щодо характеру організування виконання дипломної роботи, то він підпадає під нав’язаний режим, оскільки певні розділи роботи необхідно виконати у встановлені конкретні терміни.

Рекомендовано застосування екранних фільтрів, локальних світлофільтрів (засобів індивідуального захисту очей) та інших засобів захисту.

Роботу за дипломним проектом визнано, таку, що займає 50% часу робочого дня та за восьмигодинної робочої зміни рекомендовано встановити додаткові регламентовані перерви програм тривалістю 15 хв. через кожну годину роботи.

5.3 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.

5.3.1 Аналіз небезпечних та шкідливих факторів при виробництві (експлуатації) виробу

Аналіз небезпечних та шкідливих факторів виконується у табличній формі (табл. 5.3). Роботу, пов'язану з ЕОП з ВДТ, у тому числі на тих, які мають робочі місця, обладнані ЕОМ з ВДТ і ПП, виконують із забезпеченням виконання НПАОП 0.00-7.15-18 [6] «Вимоги щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями», які встановлюють вимоги безпеки до обладнання робочих місць, до роботи із застосуванням ЕОМ з ВДТ і ПП. Основними робочими характеристиками персонального комп'ютера є:

- робоча напруга U=+220В +-5%;
- робочий струм I=2А;
- споживана потужність Р=350 Вт.

Робоче місце має відповідати вимогам Державних санітарних правил і норм роботи з візуальними дисплейними терміналами електронно-обчислювальних машин, затверджених постановою Головного державного санітарного лікаря України від 10.12.98 N 7 [3].

Таблиця 5.3 – Аналіз небезпечних і шкідливих факторів

Небезпечні і шкідливі виробничі фактори	Джерела факторів (види робіт)	Кількісна оцінка	Нормативні документи
1	2	3	4
фізичні			
- підвищений рівень напруги електричної мережі, замикання якої може відбутися через тіло людини	-//-	4	[4]

Продовження таблиці 5.3

1	2	3	4
- недостатність природного світла	порушення умов праці (вимог до приміщень)	2	[5]
- недостатнє освітлення робочої зони	порушення гігієнічних параметрів виробничого середовища	3	[5]
психофізіологічні:			
- нервово-психічна перевантаження (розумове, перенапруження аналізаторів-зорових)	- пошук інформації для постановки теми; - пошук та аналіз аналогів і літератури; - пошук наявних технологій, моделювання та аналіз алгоритмів; - виконання роботи за темою диплома, тестування; - оформлення роботи	4	[6] [3]
- фізичні (статичне – сидіння)	порушення умов праці (організації місця праці- сидіння користувача,) та організації робочого часу - безпервна робота)	2	[6] [3]

5.3.2 Пожежна безпека

Небезпека розвитку пожежі обумовлюється застосуванням розгалужених систем електроживлення ЕОМ, вентиляції і кондиціювання.

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

Згідно ДБН В.2.5-28:2018 [5] таке приміщення, площею 25 м^2, відноситься до категорії "В" (пожежонебезпечної) та для протипожежного захисту в ньому можливо встановлення автоматичної пожежної сигналізації із застосуванням датчиків-сповіщувачів РІД-1 (сповіщувач димовий ізоляційний) в кількості 1 шт., і застосуванням первинних засобів пожежогасіння.

Продуктами згорання, що виділяються на пожежі, є: окис вуглецю; сірчистий газ; окис азоту; синильна кислота; акромін; фосген; хлор і ін. При горінні пластмас, окрім звичних продуктів згорання, виділяються різні продукти термічного розкладання: хлорангідридні кислоти, формальдегіди, хлористий водень, фосген, синильна кислота, аміак, фенол, ацетон, стирол.

5.3.3 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.

5.4 Гігієнічні вимоги до параметрів виробничого середовища

5.4.1 Мікроклімат

Мікроклімат робочих приміщень – це клімат внутрішнього середовища цих приміщень, що визначається діючої на організм людини з'єднанням температури, вологості, швидкості переміщення повітря. Оптимальні значення мікроклімату для робочого місця відповідають ДСН 3.3.6.042-99 [2] (табл. 5.4):

Таблиця 5.4 – Норми мікроклімату робочої зони об’єкту

Період року	**Категорія робіт**	**Температура C^0**	**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

У приміщенні на робочому місці забезпечуються оптимальні значення параметрів мікроклімату. Дане приміщення обладнане системою опалення, кондиціонування повітря. Також має здійснюватися провітрювання приміщення, в залежності від погодних умов, тривалість повинна бути не менше 10 хв. Найкращий обмін повітря здійснюється при наскрізному провітрюванні.

Рівні позитивних і негативних іонів у повітрі мають відповідати ДСН 3.3.6.042-99 [2].

5.4.2 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.

У приміщенні, де розташовані ЕОМ передбачається природне бічне освітлення, рівень якого відповідає ДБН В.2.5-28:2018 [5]. Джерелом природного освітлення є сонячне світло. Регулярно повинен проводитися контроль освітленості, який підтверджує, що рівень освітленості задовольняє ДБН і для даного приміщення в світлий час доби достатньо природного освітлення.

Розрахунок освітлення.

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

$$S_b = \left(\frac{1}{5} \div \frac{1}{10}\right) \cdot S_n, \qquad (5.1)$$

де S_b – площа віконних прорізів, м^2;

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.

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 (5.2):

$$n = \frac{E \cdot S \cdot Z \cdot K}{F \cdot U \cdot M}, \qquad (5.2)$$

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

S – освітлювана площа, м^2; S = 25 м^2;

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.

5.4.3 Шум та вібрація, електромагнітне випромінювання

Рівень шуму, зумовлений як роботою системного блоку, клавіатури, так і друкуванням на принтері, а також зовнішніми чинниками, коливається у межах 50–65 дБА ДСН 3.3.6.042-99 [2].

Віброізоляцію можливо здійснювати за допомогою спеціальної прокладки під системний блок, яка послаблює передачу вібрацій робочого столу. Вібрація на робочому місці в приміщенні, що розглядається, відповідає нормам ДСН 3.3.6.042-99 [2].

5.5 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.

2) Заходи безпеки під час експлуатації інших електричних приладів передбачають дотримання таких правил:

- постійно стежити за справним станом електромережі, розподільних щитків, вимикачів, штепсельних розеток, лампових патронів, а також мережевих кабелів живлення, за допомогою яких електроприлади під'єднують до електромережі;
- постійно стежити за справністю ізоляції електромережі та мережевих кабелів, не допускаючи їхньої експлуатації з пошкодженою ізоляцією;

- не тягнути за мережевий кабель, щоб витягти вилку з розетки;

- не закривати меблями, різноманітним інвентарем вимикачі, штепсельні розетки;

- не підключати одночасно декілька потужних електропристроїв до однієї розетки, що може викликати надмірне нагрівання провідників, руйнування їхньої ізоляції, розплавлення і загоряння полімерних матеріалів;

- не залишати включені електроприлади без нагляду;

- не допускати потрапляння всередину електроприладів крізь вентиляційні отвори рідин або металевих предметів, а також не закривати їх та підтримувати в належній чистоті, щоб уникнути перегрівання та займання приладу;

- не ставити на електроприлади матеріали, які можуть під дією теплоти, що виділяється, загорітися (канцелярські товари, сувенірну продукцію тощо).

5.6 Розрахунок захисного заземлення (забезпечення електробезпеки будівлі)

Згідно з класифікацією приміщень за ступенем небезпеки ураження електричним струмом, приміщення в якому проводиться робота відноситься до першого класу (без підвищеної небезпеки). Коефіцієнт використання вертикальних заземлювачів $\eta_в$ в залежності від розміщення заземлювачів та їх кількості знаходиться в межах 0,4…0,99. Взаємну екрануючу дію горизонтального заземлювача (з'єднувальної смуги) враховують за допомогою коефіцієнта використання горизонтального заземлювача η_c.

Послідовність розрахунку.

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

$$R_{шт.з.} = \frac{R_д \cdot R_{пр.з.}}{R_{пр.з.} - R_д}, \quad (5.3)$$

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

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

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

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:

$$\rho_{розр..} = \psi \cdot \rho, \quad (5.4)$$

де ψ – 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.

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

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

4) Розраховується опір розтікання струму вертикального заземлювача $R_в$, Ом, за формулою (5.5).

$$R_в = \frac{\rho_{розр.в}}{2 \cdot \pi \cdot l_в} \cdot \left(\ln \frac{2 \cdot l_в}{d_{ст}} + \frac{1}{2} \cdot \ln \frac{4 \cdot t + l_в}{4 \cdot t - l_в} \right), \quad (5.5)$$

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 формулою (5.6):

$$t = h_в + \frac{l_в}{2}, \tag{5.6}$$

де $h_в$ – глибина закладання вертикальних заземлювачів (0,8 м); тоді $t = 0,8 + \frac{3}{2} = 2,3$ 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 $\eta_в$:

$$n = \frac{2 \cdot R_в}{R_д} = \frac{2 \cdot 18,5}{4} = 9,25 \tag{5.7}$$

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:

$$n_в = \frac{2 \cdot R_в}{R_д \cdot \eta_в} = \frac{2 \cdot 18,5}{4 \cdot 0,57} = 16,2 \approx 16 \tag{5.8}$$

7) Визначається довжина з'єднувальної стрічки горизонтального заземлювача $l_с$, м:

$$l_с = 1,05 \cdot L_в \cdot (n_в - 1), \tag{5.9}$$

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:

$$R_г = \frac{\rho_{розр.г}}{2 \cdot \pi \cdot l_с} \cdot \ln \frac{2 \cdot l_с^2}{d_{см} \cdot h_г}, \quad (5.10)$$

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:

$$R_{заг} = \frac{R_в \cdot R_г}{R_в \cdot \eta_с + R_г \cdot n_в \cdot \eta_в} \le R_д. \quad (5.11)$$

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

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

Висновки до розділу 5

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.

Перелік корисних посилань до розділу 5

1. Закон України «Про охорону праці». Режим доступу: https://zakon.rada.gov.ua/laws/show/2694-12 - 10.14.1992 р.

2. Державні санітарні норми. ДСН 3.3.6.042-99 «Санітарні норми мікроклімату виробничих приміщень» - Режим доступу: https://zakon.rada.gov.ua/rada/show/va042282-99 - 01.02.1999 р.

3. Державні санітарні правила і норми. ДСанПіН 3.3.2.007-98 «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» - Режим доступу: https://zakon.rada.gov.ua/rada/show/v0007282-98 - 10.12.1998 р.

4. Державний стандарт України. ДСТУ Б В.2.5-82:2016 «Електробезпека в будівлях і спорудах. Вимоги до захисних заходів від ураження електричним струмом» - Режим доступу: http://epicentre.co.ua/dstu/doc28522.html - 01.07.2016 р.

5. Державні будівельні норми. ДБН В.2.5-28:2018 «Природне і штучне освітлення» - Режим доступу: http://www.minregion.gov.ua/wp-content/uploads/2018/12/V2528-1.pdf - 03.10.2018

6. Нормативно-правовий акт з охорони праці. НПАОП 0.00-7.15-18 «Вимоги щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями» - Режим доступу: https://zakon.rada.gov.ua/laws/show/z0508-18 - 14.02.2018 р.

ВИСНОВКИ

В результаті проведеної роботи була спроектована і реалізована система контролю доступу та обліку роботи співробітників підприємства. З її допомогою можна значною мірою полегшити і оптимізувати роботу з охорони підприємства і скоротити витрати на утримання робочого персоналу. Фактично, програмно-апаратний комплекс покладає всю рутинну, канцелярську роботу на себе, виконуючи її точно і своєчасно, що дозволяє економити час.

З впровадженням комплексу, як було відмічено, набагато підвищується дисципліна робочого персоналу. Люди вже не можуть прийти на роботу пізніше або піти з неї раніше, залишаючись непоміченими. Ця обставина сприяє підвищенню продуктивності роботи підприємства, однак при особливій конфігурації системи, можна знизити такі жорсткі рамки, встановивши інший розпорядок робочого часу, наприклад ввести відпрацювання пропущених годин.

Система має подальші перспективи розвитку. У плани на майбутнє входить розробка автономних контролерів, здатних зберігати в своїй пам'яті коди карт, що володіють правом доступу в приміщення і накопичують статистику про переміщення співробітників. Вартість таких пристроїв буде в кілька разів менше, ніж вартість спеціалізованих комп'ютерів, що встановлюються на автоматизовані прохідні, а для обслуговування всієї мережі потрібно тільки один головний комп'ютер, за допомогою якого будуть виконуватися приєднання до автономних контролерів з метою їх адміністрування (додавання, видалення кодів карт) і збору накопичених статистичних даних для складання звітів. Крім того, нові пристрої будуть споживати значно менше електроенергії і мати автономні батареї, що робить їх надійніше в разі відключення електроживлення.

Впровадження описаної технології дозволить перейти на новий виток створення високонадійних систем безпеки в тому числі і для підприємств з високим статусом секретності.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Оліфер Н.А., Оліфер В. Г. Мережеві операційні системи. - http://www.citforum.tsu.ru/operating_systems/sos/contents.shtml
2. Мінас М. WindowsNT проти Linux. // Windows 2007 Magazine.- 2014. - N3.
3. Дантеманн Д. Програмування в середовищі Delphi - К .: НДВФ "ДиаСофт Лтд.", 2017. - 608 с.
4. Джеймс. Р. Грофф, Пол Н. Вайнберг. SQL: повне керівництво, пер з англ. Є.П. Куріна. - К .: Видавнича група BHV, 2018. - 608с.
5. Epsylon Technologies. Введення в Delphi., Урок 32. - http://www.citforum.ru/programming/32less/les32.shtml
6. Проектування, розробка і продажу систем контролю доступу. - http://www.perco.ua
7. Оліфер Н.А. Використання мережевих технологій. -http: //www.citforum.ua/operating_systems/sos/glava_4.shtml#_1_4_3.
8. Довідкова система допомоги по Windows 7.
9. Болскі М. І. Delphi: компоненти для роботи з базами даних. / Пер. з нім. Денисенко С. В. - К .: Видавнича група BHV, 2017. - 200 с.
10. Компонента TApdComPort. - http://www.turbopower.com/products/APRO
11. WinAPI help. - Win32.hlp
12. Формати файлів. - http://www.halyava.ru/document/ind_form.htm
13. Delphi Help. - Delphi.hlp
14. Компонента TLMDIniCtrl. - http://www.lmd.de/download/edownl.html
15. Компонента TRXClock. - http://rx.demo.ua/download/rxtools.html

Додаток А

Скриншоти роботи програми

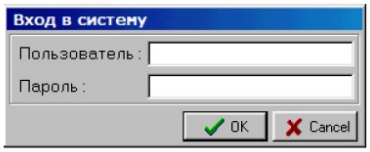


Рисунок А.1 - Вікно із запитом ролі користувача і пароля

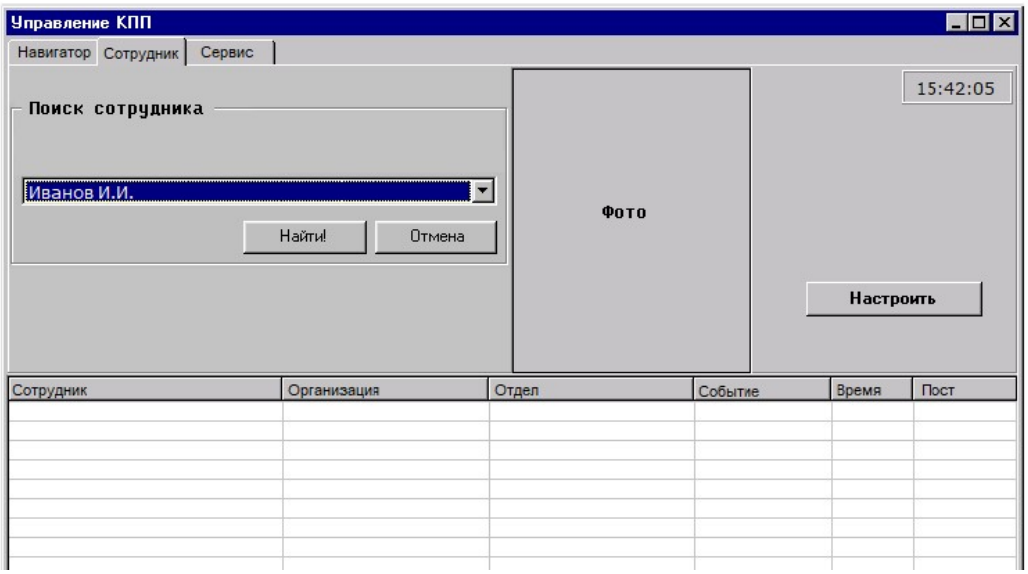


Рисунок А.2 - Форма головного модуля. Вікно пошуку співробітника по БД

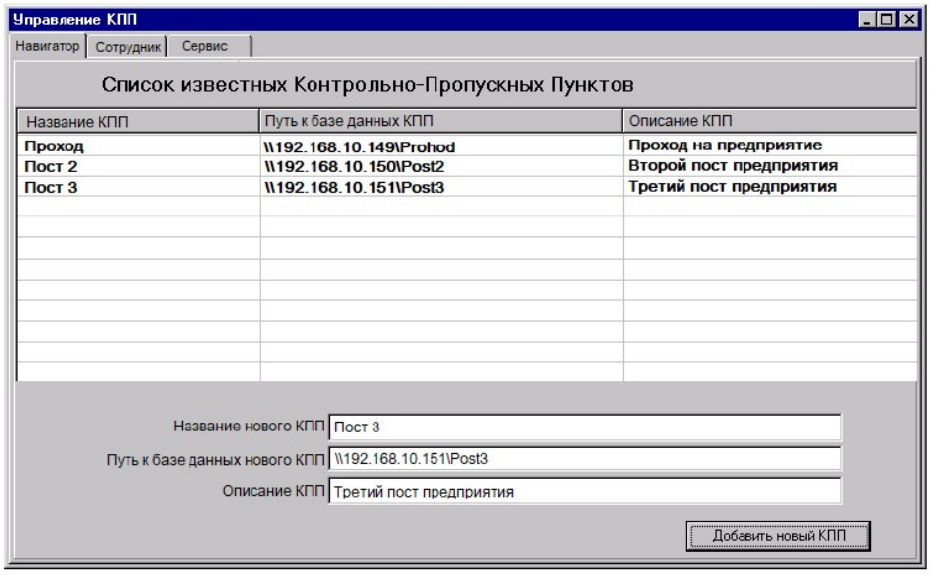


Рисунок А.3 - Вікно зі списком відомих КПП

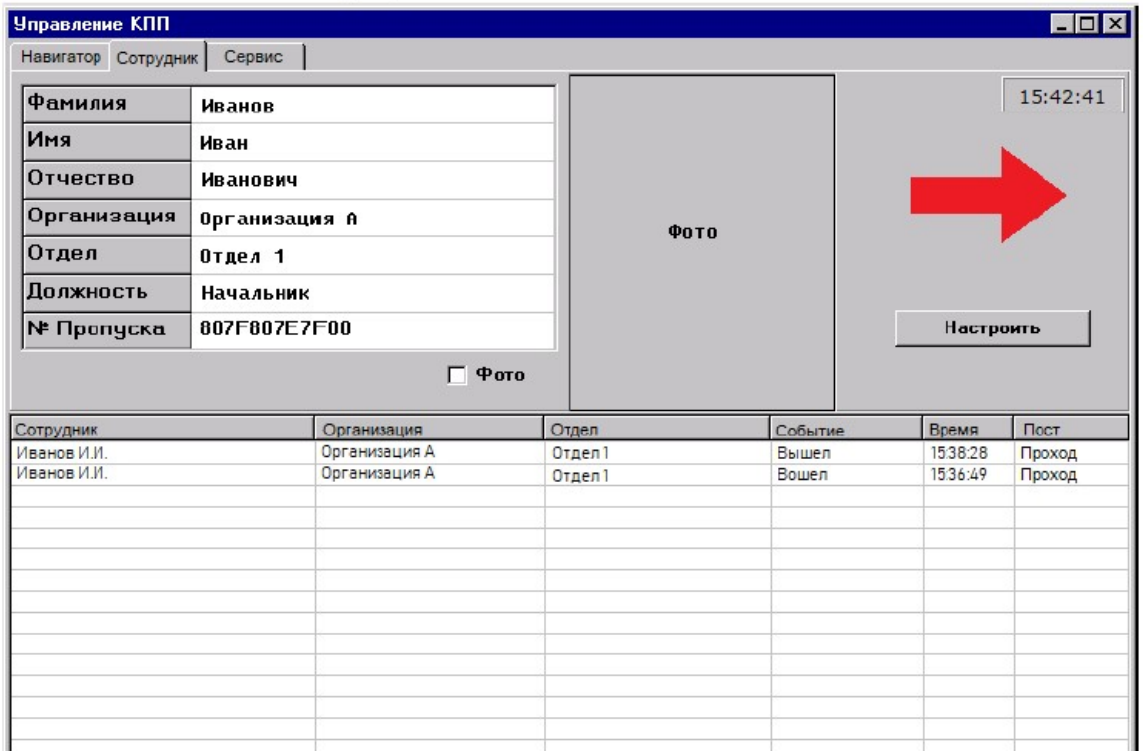


Рисунок А.4 - Вікно з інформацією про співробітника та його дії

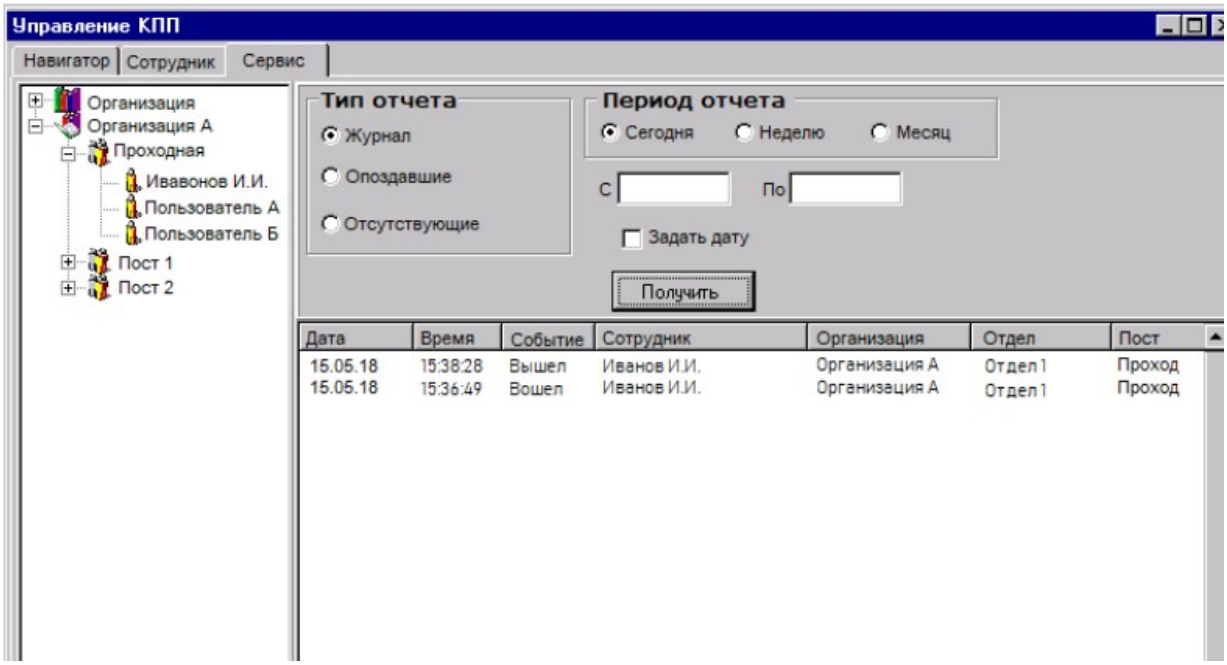


Рисунок А.5 - Вікно з інформацією про підприємство

Додаток Б

Лістинг коду програми

```
1. SystemT.db:
2. LoginName: = 'ADMIN';
3. BF1.Key: = 'password';
4. StrPCopy (Buffer, LoginName);
5. BF1.EncryptBlock (buffer, length (LoginName);
6. procedure TMainForm.FormCreate (Sender: TObject);
7. begin
8. if not (PasswordDialog.ShowModal = mrOK) then MainForm.Close;
9. Далі за допомогою компоненти Reg1: TLMDIniCtrl [Regestry] з
   системного реєстру зчитуються програмні установки:
10.// Номер COM-порту
11.COM_PORT: = Reg1.ReadInteger (IDS_ROOT, 'COM_PORT', 0);
12.// Швидкість обміну по порту
13.COM_SPEED: = Reg1.ReadInteger (IDS_ROOT, 'COM_SPEED1', 0);
14.// Автовидалення застарілих записів (вкл / викл)
15.AUTODEL: = Reg1.ReadInteger (IDS_ROOT, 'AUTODEL', 0);
16.// Період старіння записів в місцях
17.AUTODELPERIOD: = Reg1.ReadInteger (IDS_ROOT,
   'AUTODELPERIOD', 0);
18.try
19.if Com1 = nil then
20.begin
21.Com1: = ComPortThread.Create; // Створення екземпляра класу
22.Com1.Resume;
23.end;
24.except
25.ShowMessage ( 'COM-порт для турнікета зайнятий іншим пристроєм!');
26.end;
27.procedure TMainForm.Button1Click (Sender: TObject);
28.begin
29.if (Button1.Caption = 'Включити') then
30.begin
31.Com1.Resume; // Управління ведеться з процесу Com1
32.Button1.Caption: = 'Вимкнути';
33.end
34.else
35.begin
36.Com1.Suspend; // Управління бере на себе контролер
```

```
37.Button1.Caption: = 'Включити';
38.end;
39.end;
40.TAutoDelQuery:
41.// Номер COM-порту
42.Reg1.WriteInteger (IDS_ROOT, 'COM_PORT', COM_PORT);
43.// Швидкість обміну по порту
44.Reg1.WriteInteger (IDS_ROOT, 'COM_SPEED1', COM_SPEED);
45.// Автовидалення застарілих записів (вкл / викл)
46.Reg1.WriteInteger (IDS_ROOT, 'AUTODEL', AUTODEL);
47.// Період старіння записів в місцях
48.Reg1.WriteInteger (IDS_ROOT, 'AUTODELPERIOD',
   AUTODELPERIOD);
49.procedure TMainForm.RxClock1Alarm (Sender: TObject);
50.begin
51.SQL.Clear;
52.SQL.Add ( 'delete from simplog, EmpLog, LateComers where TODAY <:
   TODAY');
53.Parambyname ( 'TODAY'). Asdatetime: = Date-AUTODELPERIOD * 30;
54.try
55.prepare;
56.ExecSQL;
57.except
58.MessageDlg ( 'Помилка підключення до БД!', MtError, [mbok], 0);
59.exit;
60.end;

61.ReportQuery.SQL.Clear;
62.case Type of
63.// Отримати список всіх співробітників
64.-1: SQL.Add ( 'select * from Employers.db);
65.// Отримати всіх співробітників обраної організації
66.0: SQL.Add ( 'select * from Employers.db and Org =' + Org_desc);
67.// Отримати всіх співробітників обраного відділу
68.1: SQL.Add ( 'select * from Employers.db where Dep =' + Dep_desc);
69.// Отримати 1 співробітника
70.ReportQuery.First; // Встановимо покажчик на першу знайдену запис
71.while not ReportQuery.EOF do // перебираємо співробітників
72.begin
73.TmpQuery.SQL.Clear;
74.TmpQuery.SQL.Add ( 'select AccessTime from Emplog.db where Empkey
   =: Empkey and today> =: DateStart and today <=: Dateend and accesstime
   is not null');
```

```
75.TmpQuery.ParamByName ( 'EmpKey'). Asinteger: =
   ReportQuery.FieldByName ( 'EmpKey'). AsInteger;
76.TmpQuery.Open;
77.// якщо знайшли інтервали робочого часу
78.if TmpQuery.Recordcount> 0 then
79.begin
80.TmpQuery.First; // Беремо перший
81.While not TmpQuery.EOF do // Підсумовуємо з іншими
        i. begin decodetime (fieldbyname ( 'accesstime'). asdatetime,
           hour, min, sec, msec);
82.hours: = hours + hour;
83.mins: = mins + min;
84.if mins> = 60 then
85.begin hours: = hours + (mins div 60); mins: = mins mod 60; end;
86.TmpQuery.Next; end;
87.end;
88.ReportQuery.Next; // Беремо наступного співробітника
89.end;
90.EmpTreeView:
91.// Пункт меню "Додати"
92.EmpQuery.SQL.Clear; Case TreeLevel of
93.0: // додати нову організацію номер org, з назвою org_desc
94.EmpQuery.SQL.Add ( 'insert into organization values (org, org_desc)');
95.1: // додати новий відділ організації з номером org під номером dep
96.// з назвою dep_desc
97.EmpQuery.SQL.Add ( 'insert into departments values (org, dep, dep_desc)');
98.2: // додати нового співробітника у відділ номер dep організації номер
99.// org під номером EmpKey, з особистими даними
100.   EmpQuery.SQL.Add ( 'insert into Employers values (org, dep, empkey,
   tabnum, keycode ...)');
101.   End;
102.   EmpQuery.Prepare; // Підготувати запит
103.   EmpQuery.ExecSQL; // Реалізувати запит
104.   // Пункт меню "Видалити"
105.   EmpQuery.SQL.Clear;
106.   Case TreeLevel of
107.   0: // видалити організацію з назвою org_desc з усіма її відділами та
108.   // співробітниками
109.   EmpQuery.SQL.Add ( 'delete from organization, departments, employers
   where org_desc =: org_desc and organization.dep = departments.dep and
   organization.org = employers.org');
110.   1: // видалити відділ з назвою dep_desc з усіма його співробітниками
111.   EmpQuery.SQL.Add ( 'delete from departments, employers where
   dep_desc =: dep_desc and departments.dep = employers.dep');
```

```
2: // видалити співробітника номер під номером EmpKey
EmpQuery.SQL.Add ( 'delete from Employers where empkey =: empkey');
End;
EmpQuery.Prepare;
EmpQuery.ExecSQL; // Пункт меню "Змінити"
EmpQuery.SQL.Clear;
Case TreeLevel of
0: // перейменувати організацію з назвою org_desc в new_org_desc
EmpQuery.SQL.Add ( 'update organization set org_desc =: new_org_desc');
1: // перейменувати відділ з назвою dep_desc в new_dep_desc
EmpQuery.SQL.Add ( 'update departments set dep_desc =: new_dep_desc');
End;
EmpQuery.Prepare;
EmpQuery.ExecSQL;
UNC:
// Функція визначення місця розташування ресурсу в мережі
function GetSelectedDir (Handle: THandle): string;
var
s: TBrowseInfoA;
IDList: PItemIDList; // Список ресурсів
function GetPathFromIDList: string;
var
Buf: array [0..MAX_PATH-1] of Char;
Res: Boolean;
begin
Result: = '';
if IDList <> nil then
begin
Res: = SHGetPathFromIDList (IDList, Buf); // вибрати шлях до БД
if Res then Result: = Buf else Exit;
end;
end;
begin
// Заповнюємо структуру TBrowseInfoA
s.hwndOwner: = Handle; // хендл вікна
s.pidlRoot: = nil;
s.pszDisplayName: = nil;
s.lpszTitle: = PChar ( 'Огляд мережевих ресурсів');
s.ulFlags: = 0; s.lpfn: = nil;
s.lParam: = 0;
s.iImage: = 0;
```

```
153.    IDList: = SHBrowseForFolder (s); // виклик функції вибору шляху до
    БД
154.    Result: = GetPathFromIDList; // Повернення результату: UNC-ім'я до
    БД
155.    end;
```

Додаток В

Комп'ютерна презентація

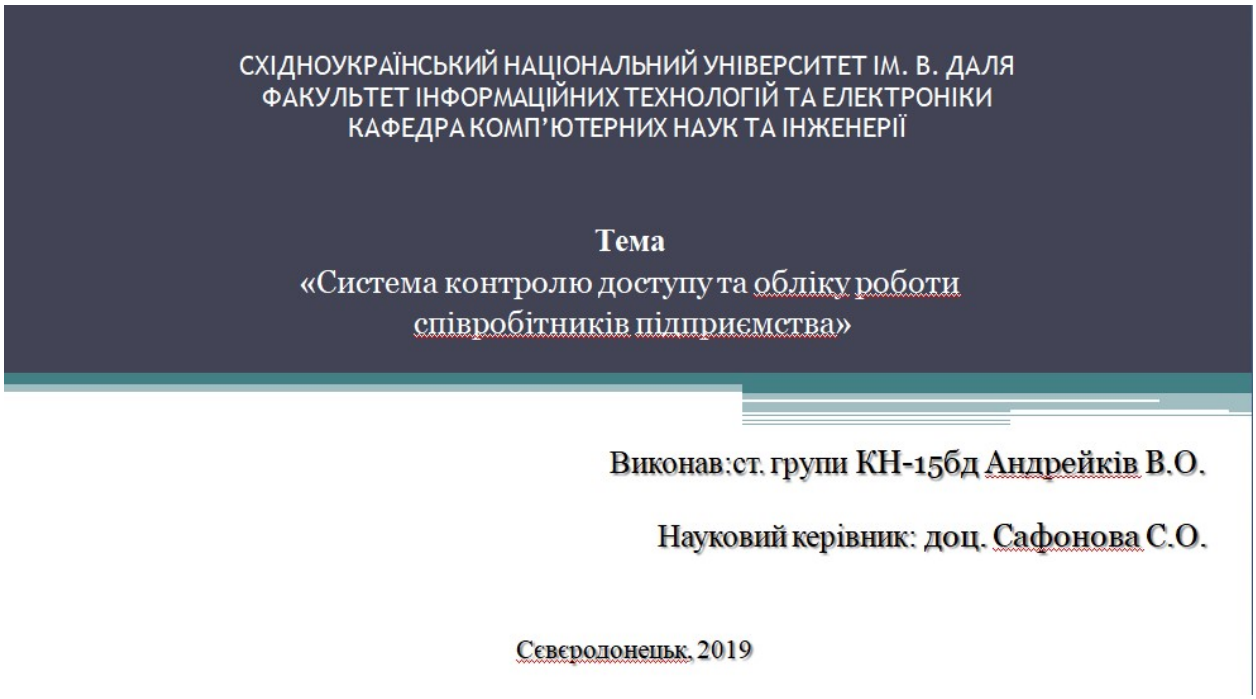


Рисунок В.1 – Слайд 1

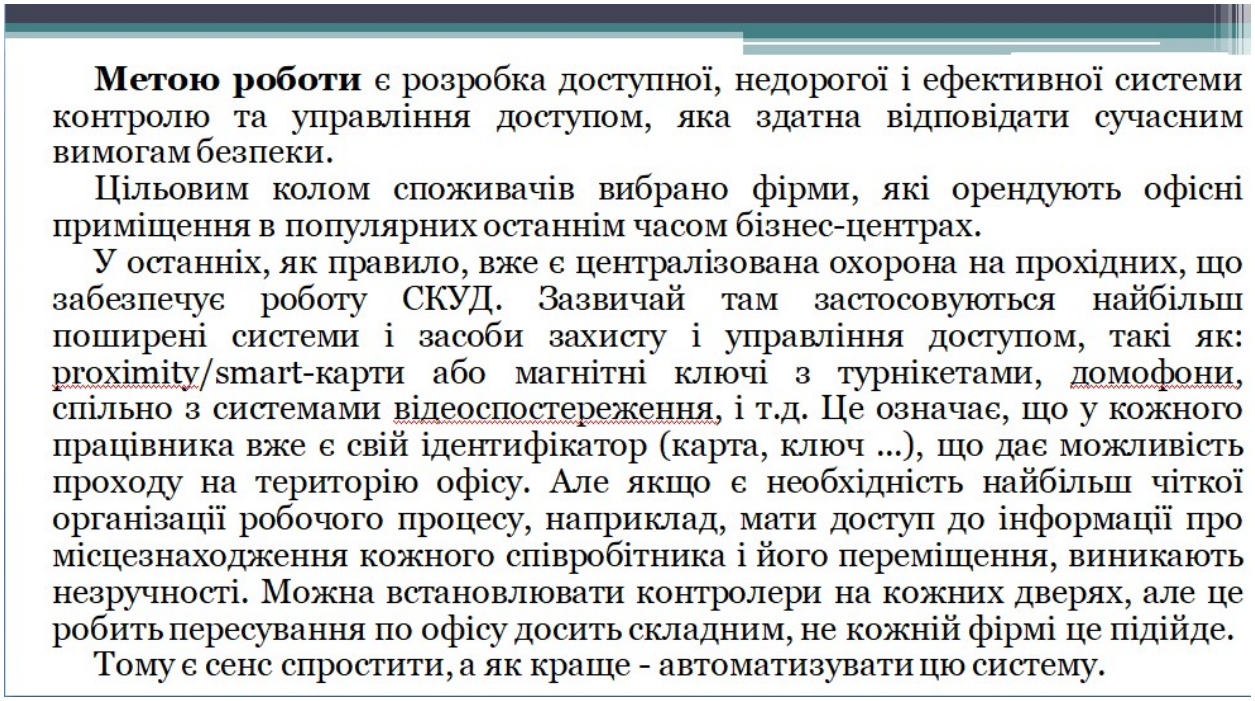


Рисунок В.2 – Слайд 2

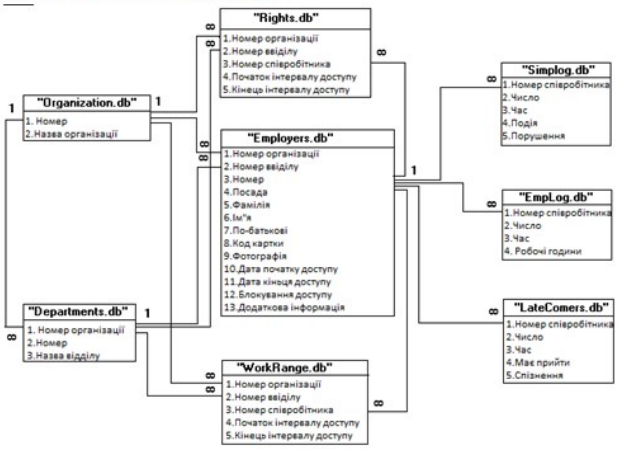
Для досягнення мети вирішено наступні задачі:

- проведено аналіз предметної області;
- визначено особливості систем контролю та управління доступом;
- обрано мову програмування;
- розроблено моделі та алгоритми управління доступом для системи;
- обрано технологію та розробити програмне забезпечення;
- перевірено роботу системи з використанням тестового матеріалу.

Рисунок В.3 – Слайд 3

Логічна схема бази даних

Логічну схему локальної бази даних, розробленої для зберігання інформації про структуру підприємства, співробітників і їхні права доступу, а також для зберігання подій, що відбуваються на автоматизованій прохідний, представлено на рисунку



Загальна база даних підприємства розподілена по локальних базам даних автоматизованих прохідних, що є необхідним для найбільш швидкого доступу до неї. У базі даних кожної автоматизованої прохідної будуть зберігатися відомості про тих співробітників, яких вона обслуговує.

Для взаємодії програмного забезпечення з локальною базою даних на комп'ютері кожної прохідної необхідно буде встановити Borland Database Engine, що входить в стандартну поставку Delphi.

Локальна база даних у вигляді окремих файлів-таблиць розташовується на жорсткому диску в одному каталозі, шлях до якого буде прописаний в аліас конфігураційного файлу Borland Database Engine

Рисунок В.4 – Слайд 4

Вибір мови програмування

Як засоб розробки програми будемо використовувати мову Delphi, яка забезпечує програмісту розробку Windows додатків на професійному рівні. Delphi включає в себе:

- 32-бітовий компілятор Object Pascal;
- об'єктно-орієнтований конструктор форм;
- архітектуру віртуальних даних, що дозволяє включити ваші власні засоби роботи з базами даних в VCL;
- повну підтримку Win32 API, включаючи COM, використання керуючих елементів ActiveX, багатопоточність і різні Software Development Kit (SDK) від Microsoft і сторонніх виробників;
- інструментарій для інтеграції користувальницьких звітів QuickReports;
- додатковий інструментарій для роботи з базами даних, включаючи Database Explorer, підтримку джерел даних ODBC і низькорівневий інтерфейс доступу до баз даних Borland Database Engine (BDE);
- InsiallSHIELD Express - інструментарій для поширення додатків;
- Open Tools API для розробки компонентів, інтегрованих із середовищем Delphi;
- вихідні тексти VCL і бібліотеки часу виконання (Runtime library, RTL);
- технології WebBroker, включаючи майстрів і компоненти, що полегшують розробку додатків, що використовують ISAPI, NSAPI, WinSock і CGI;
- драйвери для доступу до баз даних InterBase, Oracle, Microsoft SQL Server. Sybase, Informix і DB2;
- SQL Database Explorer, що дозволяє переглядати і редагувати специфічні метадані сервера;
- SQL Monitor, що забезпечує перегляд повідомлень обміну інформацією з сервером і полегшує налагодження та налаштування додатка;
- Data Pump Expert для швидкого підведення підсумків.

Рисунок В.5 – Слайд 5

Розроблений програмний продукт складається з модулів:

- Модуль даних.
- Модуль зв'язку з COM-портом.
- Головний модуль.
- Модуль для зв'язку з базою даних.
- Модуль для підключення до мережі.
- Модуль для генерації звітів і їх експорту.
- Модуль для роботи з базою даних.

Блок-схема роботи алгоритму в модулі зв'язку з COM-портом представлена на рисунку.

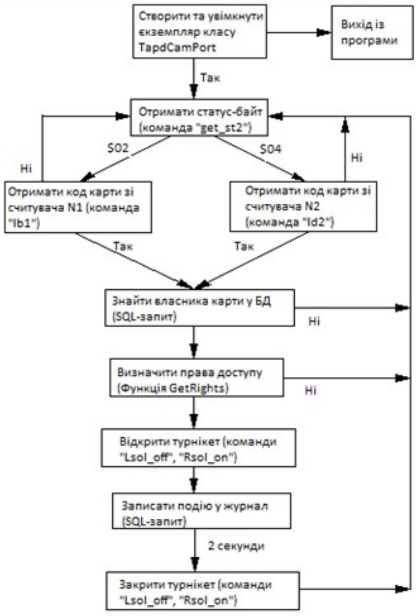


Рисунок В.6 – Слайд 6

Скриншоти роботи програми

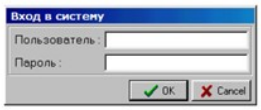


Рисунок 3 - Вікно із запитом ролі користувача і пароля

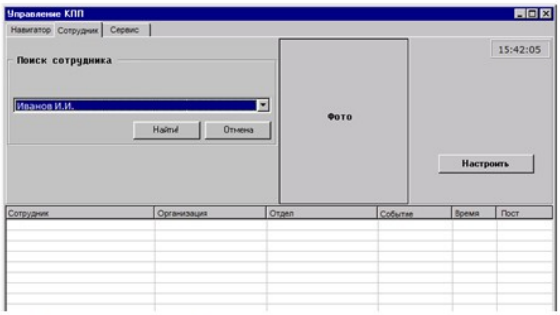


Рисунок 4 - Форма головного модуля. Вікно пошуку співробітника по БД

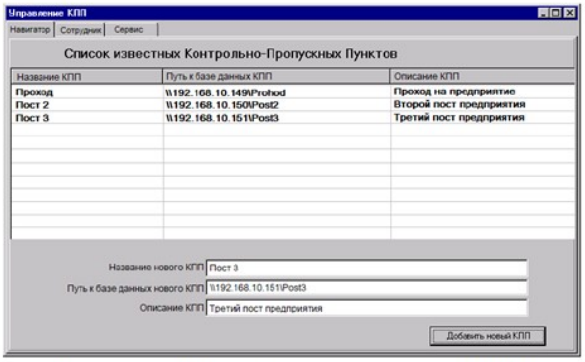


Рисунок 5 - Вікно зі списком відомих КПП

Рисунок В.7 – Слайд 7

Скриншоти роботи програми

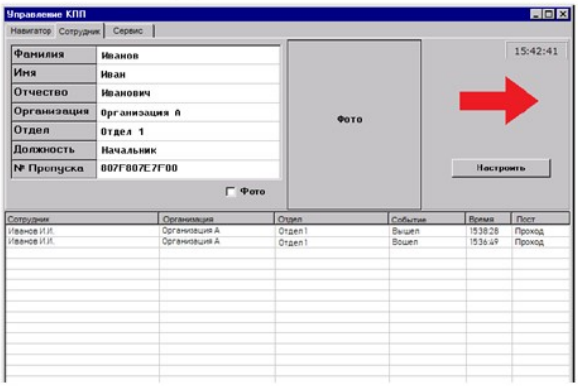


Рисунок 6 - Вікно з інформацією про співробітника та його дії

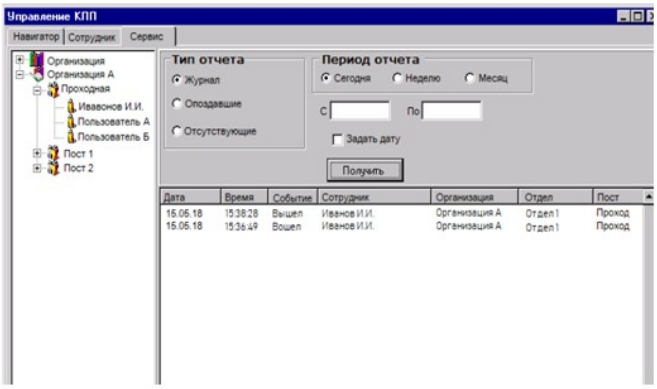


Рисунок 7 - Вікно з інформацією про підприємство

Рисунок В.8 – Слайд 8

Тестування проекту

Працездатність всього комплексу перевірялася на двох комп'ютерах, на один з яких встановлювалася програма моніторингу, з підключенням всього необхідного апаратного забезпечення, що грав роль спеціалізованого комп'ютера на автоматизованій прохідній, на інший була встановлена програма віддаленого доступу.

Конфігурації комп'ютерів наведені в таблиці 1.

Таблиця 1 - Зміни комп'ютерів для тестування

Назва	Частота процесора	материнська плата	обсяг ОЗУ	Операційна система
Intel Core i3	3.2Ггц	Asus H110m	8Гб	Windows 10
Intel Core i5	3.4Ггц	Asus h310m	16Гб	Windows 7

Обидва комп'ютери були підключені до мережі Windows Network.

Рисунок В.9 – Слайд 9

Тестування програми моніторингу

Тестування програми моніторингу проводилося за такими критеріями:

- Швидкість прийняття рішення програмою для блокування або пропуску співробітника по коду карти.
- Довжина кабелю між комп'ютером і контролером турнікету.
- Можливість роботи програми у фоновому режимі.

Результати тестування:

Була заведена база даних на 10000 осіб, встановлена довжина кабелю 20 метрів, крім програми моніторингу на комп'ютері були запущені ще два додатки: Microsoft Word і Microsoft Excel.

Час пошуку співробітника склав не більше 0,1 секунди (при виведенні фотографії співробітника розміром 5Kb на екран - не більше 0,5 секунди), що є достатнім для обслуговування безперервної черги людей на прохідній будь-якого підприємства. Довжина з'єднувального кабелю в цьому випадку цілком підходить для видалення комп'ютера від турнікета на потрібну відстань, а робота інших додатків показала, що комп'ютер на автоматизованій прохідній може паралельно з виконанням своєї основної функції використовуватися ще і для інших завдань, як, наприклад, набір тексту та нескладні математичні розрахунки.

Рисунок В.10 – Слайд 10

Тестування програми віддаленого доступу

Основним критерієм при тестуванні програми віддаленого доступу був час отримання чотирьох типів звітів. Підключення до мережі здійснювалося з іншого сегмента мережі Windows Network, відстань між комп'ютерами була не менше 100 метрів. За допомогою програми "ping.exe" було визначено середній час отримання пакетів (по 32 байта), який склав 2 мс. База даних містила 2000 записів у всіх журналах прохідний. Всього було проведено 10 дослідів (табл.2).

Таблиця 4.2 - Результати часу отримання звітів

тест	звіт N1	звіт N2	звіт N3	звіт N4
час	19 сек.	18 сек.	4 сек.	20 сек.

де
"Звіт N1 "- звіт про прохідний;
"Звіт N2 "- звіт про робочий час;
"Звіт N3 "- звіт про відсутніх;
"Звіт N4 "- звіт про тих, хто запізнився.

На підставі отриманих результатів можна розрахувати приблизний час отримання звітів за місяць по накопиченим статистичним даним. Нехай на підприємстві працює 1000 Співробітників. В кожен з 22 робочих днів місяця в журнал прохідний додається в середньому по 10000 записів (дві на прихід і відхід з роботи, дві на прихід і відхід на обід і шість - на прихід і відхід по випадковим обставинам). Тоді за місяць буде накопичено 220000 записів, що в 100 разів більше, ніж було при тестуванні. Звідси випливає, що час отримання самого трудомісткого звіту за місяць склав 2000 секунд (або близько 34 хвилин).

Рисунок В.11 – Слайд 11

ВИСНОВКИ

В результаті проведеної роботи була спроектована і реалізована система контролю доступу та обліку роботи співробітників підприємства. З її допомогою можна значною мірою полегшити і оптимізувати роботу з охорони підприємства і скоротити витрати на утримання робочого персоналу. Фактично, програмно-апаратний комплекс покладає всю рутинну, канцелярську роботу на себе, виконуючи її точно і своєчасно, що дозволяє економити час.

З впровадженням комплексу набагато підвищується дисципліна робочого персоналу. Люди вже не можуть прийти на роботу пізніше або піти з неї раніше, залишаючись непоміченими. Ця обставина сприяє підвищенню продуктивності роботи підприємства, однак при особливій конфігурації системи, можна знизити такі жорсткі рамки, встановивши інший розпорядок робочого часу, наприклад ввести відпрацювання пропущених годин.

Система має подальші перспективи розвитку. У плани на майбутнє входить розробка автономних контролерів, здатних зберігати в своїй пам'яті коди карт, що володіють правом доступу в приміщення і накопичують статистику про переміщення співробітників. Вартість таких пристроїв буде в кілька разів менше, ніж вартість спеціалізованих комп'ютерів, що встановлюються на автоматизовані прохідні, а для обслуговування всієї мережі потрібно тільки один головний комп'ютер, за допомогою якого будуть виконуватися приєднання до автономних контролерів з метою їх адміністрування (додавання, видалення кодів карт) і збору накопичених статистичних даних для складання звітів. Нові пристрої будуть споживати значно менше електроенергії і мати автономні батареї, що робить їх надійніше в разі відключення електроживлення.

Впровадження описаної технології дозволить перейти на новий виток створення високонадійних систем безпеки в тому числі і для підприємств з високим статусом секретності.

Рисунок В.12 – Слайд 12