МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
КАФЕДРА КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
_____ С.В. Казмірчук
«_____»_____2021 р.

На правах рукопису
УДК 004.056:004.738.5(079.2)

ДИПЛОМНА РОБОТА

ЗДОБУВАЧА ВИЩОЇ ОСВІТИ
ОСВІТНЬОГО СТУПЕНЯ «БАКАЛАВР»

Тема: Система контролю та управління доступом у віддаленому офісі

Виконавець: А.І. Созонова
Керівник: к.т.н., доцент М.Б. Гумен
Нормоконтролер: к.т.н., доцент М.Б. Гумен

Київ 2021

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет: Кібербезпеки, комп'ютерної та програмної інженерії

Кафедра: Комп'ютеризованих систем захисту інформації

Освітній ступінь: Бакалавр

Спеціальність: 125 «Кібербезпека»

Освітньо-професійна програма: «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ С.В. Казмірчук
«_____»_____2021 р.

ЗАВДАННЯ

на виконання дипломної роботи

здобувача вищої освіти Созонової Аліни Ігорівни

1. Тема: *Система контролю та управління доступом у віддаленому офісі* затверджена наказом ректора від «26» квітня 2021 р. № 652/ст.
2. Термін виконання: з 10.05.2021 р. по 20.06.2021 р.
3. Вихідні дані: проаналізувати існуючі системи контролю та управління доступом; на основі проведеного аналізу визначити переваги та недоліки кожної з них; розробити свою систему контролю та управління доступом у віддаленому офісі.
4. Зміст пояснювальної записки: аналіз існуючих систем контролю та управління доступом; розробка системи аналізу та оцінки ризиків для даної системи; розробка системи контролю та управління доступом у віддаленому офісі.

КАЛЕНДАРНИЙ ПЛАН

виконання дипломної роботи

№ п/п	Етапи виконання дипломної роботи	Термін виконання етапів	Примітка
1.	Уточнення постановки задачі	10.05.2021	*Виконано*
2.	Аналіз літературних джерел	11.05.2021-14.05.2021	*Виконано*
3.	Обґрунтування вибору рішення	15.05.2021 - 17.05.2021	*Виконано*
4.	Збір інформації	18.05.2021 - 22.05.2021	*Виконано*
5.	Дослідження сучасних систем контролю та управління доступом	23.05.2021-24.05.2021	*Виконано*
6.	Розробка методики та структури системи контролю та управління доступом	25.05.2021-28.05.2021	*Виконано*
7.	Дослідження апаратної та програмної складової систем	29.05.2021-02.06.2021	*Виконано*
8.	Розробка системи контролю та управління доступом у віддаленому офісі	03.06.2021	*Виконано*
9.	Перевірка на антиплагіат	04.06.2021-06.06.2021	*Виконано*
10.	Оформлення і друк пояснювальної записки	07.06.2021-08.06.2021	*Виконано*
11.	Оформлення презентації	09.06.2021	*Виконано*
12.	Отримання рецензій від рецензента	10.06.2021	*Виконано*

Здобувач вищої освіти А. Созонова

(підпис, дата)

Керівник дипломної роботи М. Гумен

(підпис, дата)

РЕФЕРАТ

Дипломна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, загальним обсягом робота складає 69 сторінок, має 17 рисунків, 12 таблиць та 2 додатки. Список використаних джерел містить 21 найменування і займає 2 сторінки.

Метою дипломної роботи є проектування системи контролю та управління доступом віддаленого офісу компанії «Plexon Inc.» в м. Київ.

У дипломній роботі розглянуто питання ризиків для систем захисту персональних даних, а також проаналізовані та запропоновані методи та основні напрями захисту.

Розроблена система може використовуватися на будь-яких об’єктах де мають місце ризики нанесення шкоди та викрадення персональних даних.

Ключові слова: персональні дані, система захисту персональних даних, інформація, шкідливе програмне забезпечення, інформаційна система.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ЗІ - захист інформації

ІС - інформаційна система

НСД - несанкціонована спроба доступу

ОС - операційна система

ПЗ - програмне забезпечення

СКД - система контролю доступу

СКУД - система контролю та управління доступом

ВСТУП

Актуальність. Перед сучасним підприємством сьогодні стоїть безліч проблем: утримання клієнтів, пошук кращих постачальників, що в кінцевому підсумку повинно вплинути на збільшення прибутку і зниження витрат.

Проте всі зусилля компанії можуть бути марними, у тому разі якщо нові технології, які використовує компанія на ринку, стануть доступні конкурентам.

Для захисту комерційної таємниці компанії від зовнішніх зазіхань застосовують безліч технологій, включаючи спеціалізоване обладнання та програмне забезпечення. Проте, за статистикою найбільше число крадіжок інформації пов'язано не з зовнішніми «ворогами», а власними співробітниками, які мають доступ або до самої інформації, або до технологій її отримання.

Рішення проблеми лежить зазвичай в розробці комплексної політики безпеки на підприємстві, яка включає як спеціалізоване програмне і апаратне забезпечення, так і організаційне, правове та інші види забезпечення.

В даний час існує багато варіантів систем захисту і контролю доступу в приміщення.

Починають отримувати поширення інтегровані системи забезпечення безпеки, які дозволяють здійснювати повний спектр електронного управління всіма процесами, що відбуваються в структурі об'єкта.

У разі організації системи контролю доступу за допомогою електронного обладнання кожному з користувачів (співробітники підприємства, охорона, гості і т.д.) видається електронний ідентифікатор: магнітна карта, яка отримала найбільше поширення в останні роки, але, на жаль, вже не дозволяє уникнути підробок і досить швидко зношуються, індуктивна карта або ключ, що мають більш високу стійкість до копіювання і значно більший термін життя або спеціальний ключ (брелок) з вбудованим мікрочіпом, термін життя яких практично дорівнює часу життя системи, а спроба злому призводить до руйнування носія інформації.

Захист будь-якого об'єкту включає кілька рубежів, число яких залежить від рівня режимності об'єкта. При цьому у всіх випадках важливим рубежем буде система управління контролю доступом (СКУД) на об'єкт. СКУД – це комплекс технічних та програмних засобів безпеки, що здійснює регулювання входу / виходу та переміщень людей чи транспортних об’єктів на територіях, які знаходяться під охороною, для адміністративного моніторингу та попереджень несанкціонованого проникнення.

Створена на основі сучасних технічних засобів СКУД дозволить вирішувати цілий ряд задач, до яких відносяться протидія розкраданню, саботажу і навмисного пошкодження матеріальних цінностей, облік робочого часу, контроль трудової дисципліни та ін.

Слід зазначити, що СКУД є одним з найбільш розвинених сегментів ринку безпеки як в Україні, так і за кордоном. В якості найбільш часто використовуваних засобів контролю і управління доступом на підприємстві перерахуємо турнікети, двері, замки, ідентифікатори різної природи та ін.

Актуальними трендами в сучасних умовах є інтеграція СКУД з іншими системами безпеки, ідентифікація по смартфону, біометрична ідентифікація [5]. В даний час пандемія COVID-19 змушує роботодавців задуматися про інтеграцію систем контролю доступу з тепловізорами, ІК-термометрами з метою автоматизації процесу виявлення осіб з підвищеною температурою. Однак такі системи мають високу собівартість і є виправданими лише на досить великих підприємствах.

Мета дипломної роботи: проєктування системи контролю та управління доступом віддаленого офісу компанії «Plexon Inc.» в м. Київ.

Об'єкт дослідження: процес контролю та управління доступом віддаленого офісу компанії.

Предмет дослідження: засоби та методи контролю та управління доступом віддаленого офісу.

Практична цінність полягає у розробці системи контролю і управління доступом, що може використовуватись як основа для віддалених офісів та

малих підприємств, та дає змогу посилити безпеку працівників і клієнтів установ, їх безперебійну роботу, попередити потенційні незаконні втручання, скоротити матеріальні збитки і мінімізувати наслідки можливої надзвичайної ситуації.

Завдання роботи:

- аналіз існуючих систем контролю і управління доступом та доцільності їх використання;
- охарактеризувати віддалений офіс компанії «Plexon Inc.» м. Київ з погляду інформаційної безпеки;
- розробити проєкт системи контролю та управління доступом віддаленого офісу компанії «Plexon Inc.» в м. Київ для підвищення ефективності забезпечення його безпеки;
- розрахувати економічні витрати на впровадження системи контролю та управління доступом віддаленого офісу компанії «Plexon Inc.» в м. Київ.

Область застосування результатів роботи поширюється на широке коло об'єктів підприємницької діяльності.

РОЗДІЛ 1. АНАЛІЗ ІСНУЮЧИХ СИСТЕМ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ

1.1 Загальні принципи роботи СКУД

Згідно ДСТУ EN 50133-2-1 система контролю і управління доступом (СКУД) – сукупність засобів контролю і управління, що володіють технічною, інформаційною, програмною та експлуатаційною сумісністю [1].

В основі роботи СКУД закладений принцип порівняння тих чи інших ідентифікаційних ознак, що належать або властивих конкретному суб'єкту (фізичній особі) або об'єкту (предмету, транспортному засобу), з інформацією, закладеної в пам'яті системи.

Поняття ідентифікатора і ідентифікації є основними поняттями для СКУД. Термін ідентифікація означає – упізнання, пошук за ознакою. Ідентифікація може проводитися за такими основними принципам:

- за кодом, що вводиться вручну за допомогою клавіатури, кодових перемикачів або інших подібних пристроїв;
- по коду, записаного на фізичному носії (ідентифікатор) в за який застосовуються різні ключі, карти, брелоки і т.д.;
- біометрична ідентифікація, заснована на визначенні індивідуальних фізичних ознак людини.

Кожен з користувачів (співробітників) отримує індивідуальний ідентифікатор. В якості такого предмета може бути використана пластикова карта, брелок, браслет або інший подібний предмет (рис. 1.1).

Ідентифікатор може бути закріплений також на певному предметі та транспортному засобі. Пароль, кодове число, а також предмет ідентифікатор відносяться класу присвоєних ідентифікаційних ознак.

При цьому ідентифікується не сама людина, а присвоєна їй ознака.

Рис. 1.1. Види ідентифікаторів: *а* – пластикова карта; *б* – браслет; *в, г* – брелоки *Touch Memory*

В якості ідентифікаційних ознак можуть використовуватися притаманні ознаки людини (біометричні дані) такі як, відбитки пальців, геометрія кисті руки, голосові характеристики і т.д.) (рис. 1.2).

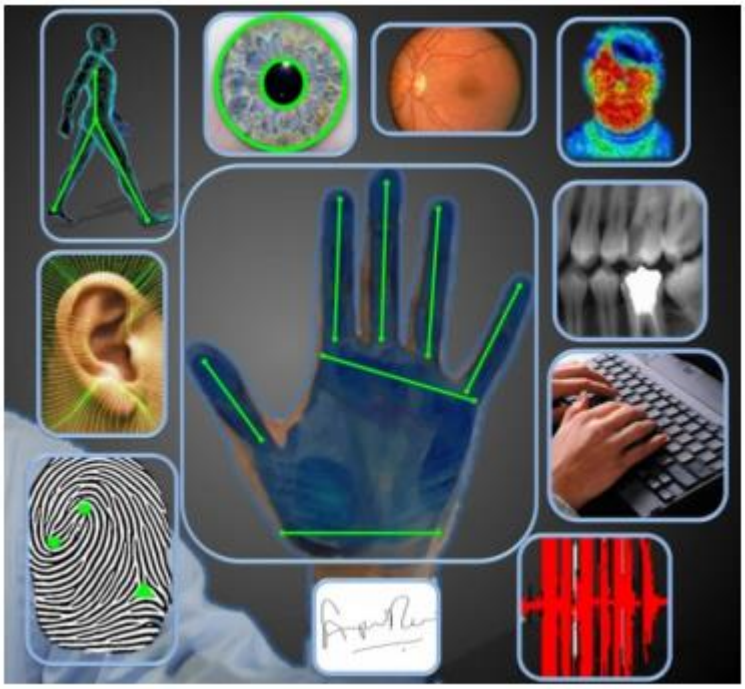


Рис. 1.2. Способи біометричної ідентифікації

Робота СКУД відбувається наступним чином. Біля входу в контрольоване приміщення встановлюються спеціальні пристрої-зчитувачі, які призначені для зчитування інформації з ідентифікатора, введення пароля або кодового числа, введення біометричних даних людини. Далі інформація надходить на контролери доступу, які на підставі аналізу даних про власника забезпечують управління перешкоджаючими і дозволяючими пристроями: відкривають або

блокують двері, включають сигнал тривоги, реєструють присутність людини на робочому місці і т.д. На рис. 1.3 представлена загальна логічна схема побудови системи контролю та управління доступом.

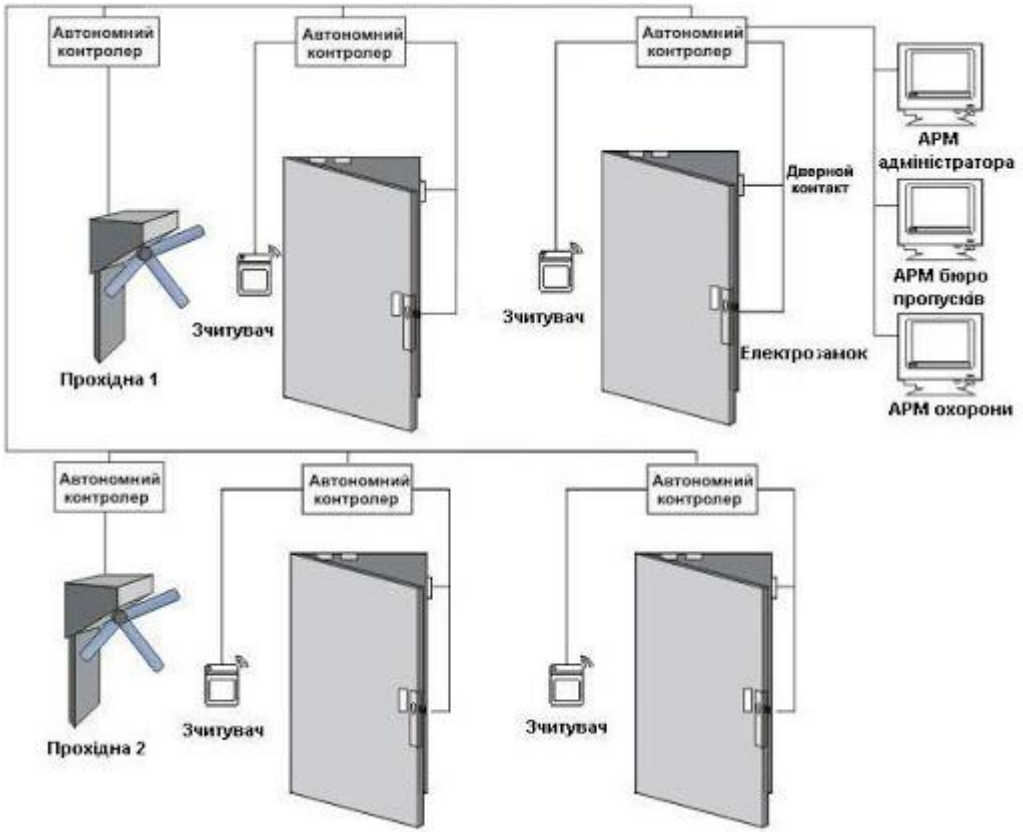


Рис. 1.3. Загальна схема роботи СКУД

Таким чином, СКУД є одним з елементів комплексних рішень для забезпечення високого рівня безпеки об'єкта. Принцип роботи СКУД дозволяє строго контролювати будь-які переміщення в зоні дії. Розберемо докладніше можливості СКУД.

1.2 Огляд можливостей СКУД

В процесі своєї роботи СКУД повинна виконувати наступні функції:

- санкціонування – процедура присвоєння кожному користувачеві персонального ідентифікатора, коду, реєстрацію його в системі (або реєстрацію його біометричних ознак);
- завдання для користувача тимчасових інтервалів і рівня доступу (в які приміщення, коли і хто має право заходити);

• ідентифікація – процедура впізнання користувача за пред'явленим ідентифікатором або біометричного ознакою;

• авторизація – перевірка повноважень, яка полягає в перевірці відповідності часу та рівня доступу встановленим в процесі санкціонування;

• аутентифікація – встановлення автентичності користувача за ознаками ідентифікації;

• дозвіл доступу або відмову в доступі – виконується на підставі результатів аналізу попередніх процедур;

• реєстрація – протоколювання всіх дій в системі;

• реагування – реакція системи на несанкціоновані дії (подача попереджувальних і тривожних сигналів, відмова в доступі і т.д.).

Процедура санкціонування проводиться оператором або адміністратором системи, всі інші процедури можуть здійснюватися через систему автоматично. Очевидно, що процедура аутентифікації може бути виконана повноцінно тільки за допомогою біометричних систем [7].

Отже, системи контролю і виконання доступом не тільки запобігають проникненню будь-яких небажаних людей на територію, що охороняється, а й забезпечують цілісність і захист матеріальних цінностей, важливої інформації, гарантують безпеку для персоналу та відвідувачів. Відзначимо важливість для виявлення порушень трудової дисципліни таких функцій, як відстеження переміщення всіх співробітників в офісі, облік і фіксація відпрацьованого співробітниками часу (дані про прогули, хто запізнився, що пішли з роботи завчасно і т.п.).

Основними найбільш затребуваними на практиці функціями СКУД є [8]:

• розмежування доступу до закритих внутрішніх приміщень;

• облік робочого часу і контроль своєчасного приходу персоналу на роботу в інтеграції з платформами бухгалтерського обліку («1С: Бухгалтерія», «Парус», БЕСТ-3 і ін.).

Більш досконалі і дорогі системи контролю та управління доступом мають додаткові функціональні можливості [9]:

• можливість отримання одноразової доступу по відбитку пальців в конкретне приміщення будівлі;

• управління виконавчими пристроями в автоматичному режимі відповідно до раніше складеними розкладами;

• можливість роботи з разовими або тимчасовими електронними перепустками;

• можливість спільної роботи з настільними зчитувачами для більш повного контролю використання службовцями робочого часу;

• відображення інтерактивних планів об'єкта, його поточного стану і можливістю спільного управління однотипними пристроями (відкриття або блокування по тривозі) і ін.

Представлена на рис. 1.4 схема СКУД PERCo-S-20 [10] є багатофункціональною.

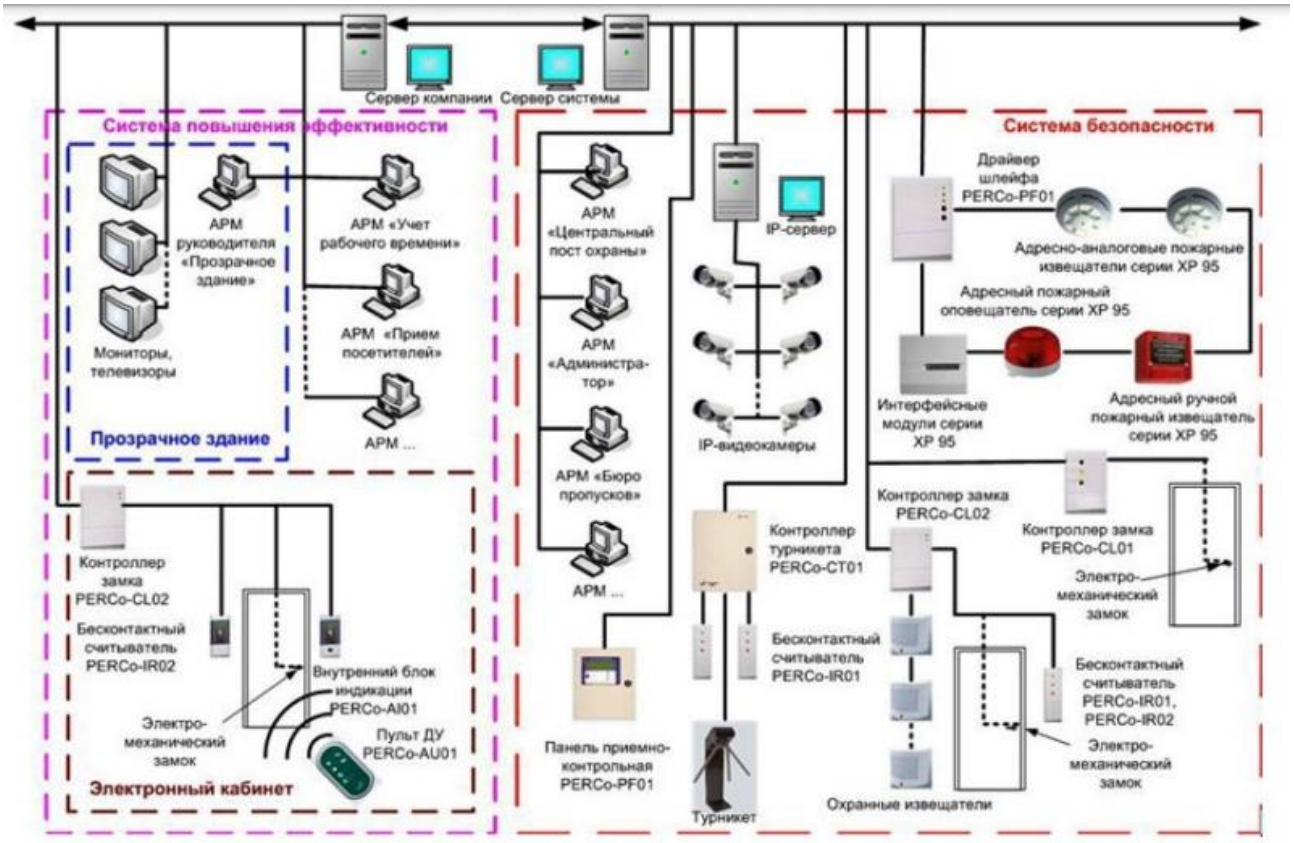


Рис. 1.4. Схема СКУД PERCo-S-20

У мережі СКУД зв'язок здійснюється по інтерфейсу Ethernet. В якості ідентифікаторів використовуються безконтактні (Proximity) карти і брелоки. Як

виконавчі пристрої в СКУД PERCo-S-20 можуть використовуватися турнікети, хвіртки, електромагнітні та електромеханічні замки. Наявність в контролерах доступу вбудованої підтримки шлейфів охоронної сигналізації дозволяє контролювати весь обсяг приміщення.

Як видно на рис. 1.4, система забезпечення безпеки інтегрована з системою підвищення ефективності трудової діяльності.

На даний момент існує величезна кількість різних типів систем контролю і управління доступом, які відрізняються ступенями надійності, складністю налаштування і обслуговування, вартістю, але, як правило, виконують такі основні функції: виявлення, упізнання, управління, контроль, які представлені у вигляді схеми на рис. 1.5.

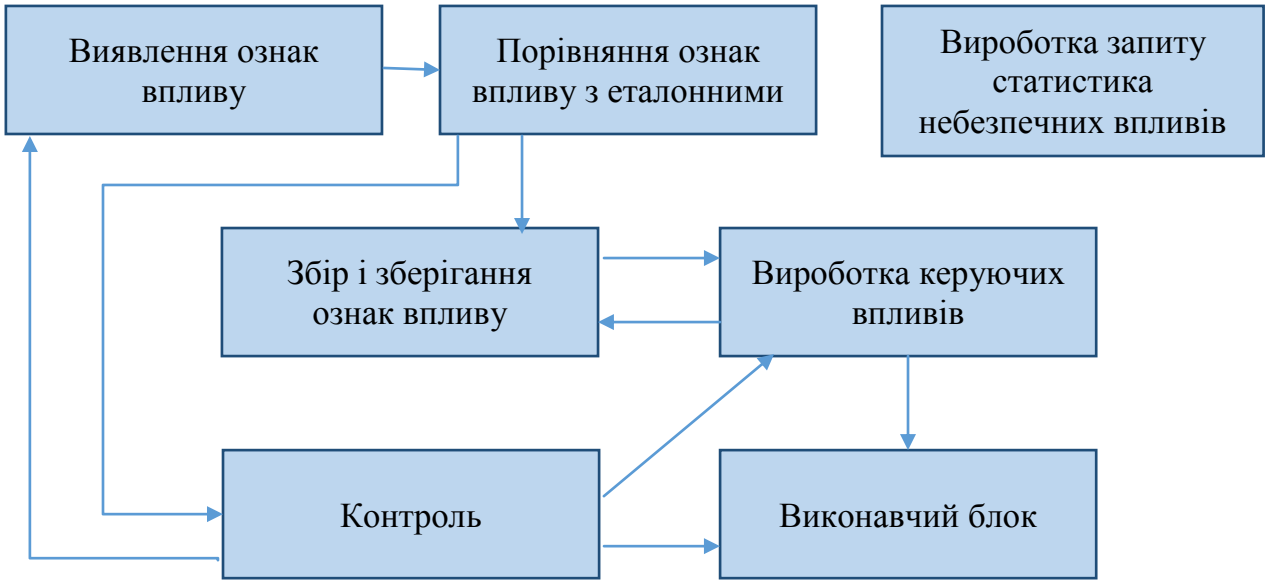


Рис. 1.5. Функціональна схема системи контролю та управління доступом

Архітектура СКУД, що представляє собою гнучку, модульну систему, дозволяє вибрати з наявних на ринку саме той комплект обладнання, який буде оптимально відповідати потребам підприємства і може бути згодом модернізований. У світлі цього розглянемо компонентний склад систем контролю і управління доступом.

1.3 Основні компоненти СКУД

Основними компонентами систем контролю і управління доступом є засоби контролю і управління доступом – механічні, електромеханічні, електричні, електронні пристрої, конструкції і програмні засоби, що забезпечують реалізацію контролю і управління доступом (рис. 1.6) [1].

Засоби контролю і управління доступом класифікуються за функціональним призначенням пристроїв; функціональних характеристик; стійкості до несанкціонованого доступу (НСД).

Рис. 1.6. Засоби контролю та управління доступом

Засоби КУД за функціональним призначенням пристроїв поділяються на забороняючі керовані (УПУ), виконавчі, зчитувальні пристрої, ідентифікатори і засоби управління в складі апаратних пристроїв і програмних засобів.

УПУ – пристрої, що забезпечують фізичне перешкода доступу і обладнані виконавчими пристроями для управління їх станом (турнікети, прохідні кабіни, двері і ворота, обладнані виконавчими пристроями систем контролю і управління доступом) (рис. 1.7).

До складу СКУД можуть входити додаткові кошти, призначені для забезпечення роботи СКУД (блоки безперебійного живлення; датчики стану УПУ; дверні доводчики; світлові і звукові сповіщувачі; кнопки ручного управління УПУ; пристрої перетворення інтерфейсів мереж зв'язку; апаратура передачі даних по різних каналах зв'язку і ін .).

Компонентами СКУД є також апаратно-програмні засоби – засоби обчислювальної техніки (СВТ) загального призначення (комп'ютерне обладнання, обладнання для комп'ютерних мереж, загальне програмне забезпечення).

Рис. 1.7. Виконавчі пристрої систем контролю і управління доступом

За функціональними характеристиками УПУ класифікуються по виду перекриття отвору проходу:

- з частковим перекриттям (турнікети, шлагбауми);
- з повним перекриттям (повнозростові турнікети, спеціаліні ворота);
- із суцільним перекриттям отвору (суцільні двері, ворота);
- з блокуванням об'єкта в отворі (шлюзи, кабіни прохідні).

Виконавчі пристрої класифікуються за способом замикання на електромеханічні та електромагнітні замки; електромагнітні засувки; механізми приводу дверей, воріт.

Пристрої введення ідентифікаційних ознак (УВІП) – електронні пристрої, призначені для введення і зчитування кодової інформації з ідентифікаторів. До складу УВІП входять зчитувачі і ідентифікатори.

Зчитувач – пристрій в складі УВІП, призначене для зчитування ідентифікаційних ознак та передачі цієї інформації в контролер системи контролю доступу в приміщення (рис. 1.8).

Рис. 1.8. Зчитувач ST-11

Ідентифікатор користувача – унікальний ознака суб'єкта або об'єкта доступу. В якості ідентифікаторів використовуються магнітні картки, безконтактні proximity-карти, брелоки, різні радіобрелки, а також різні фізичні ознаки конкретної людини, як наприклад зображення райдужної оболонки ока, відбиток пальця або відбиток долоні. В даний час застосовуються такі типи карт: – безконтактні радіочастотні (proximity) карти – найбільш перспективний 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 певної частоти і, привнесення 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 за допомогою електромагнітного імпульсу певної форми і частоти; – магнітні картки – найбільш широко поширений варіант. Карти Віганд (Wiegand) названий так на честь вченого, який відкрив спеціальний сплав, що володіє магнітними властивостями, які важко дублювати. Усередині карти розташовані відрізки дроту з цього сплаву. Карта може бути контактною та безконтактною і зчитується шляхом піднесення або пропускання через термінал, званий зчитувач Wiegand. Ці карти довговічніші, досить безпечні і забезпечують максимальний захист від підробки, а й дорожчі. Один з недоліків – те, що код в карту занесений при виготовленні раз і назавжди; – штрих-кодові карти – на карту наноситься штриховий код; – ключ-брелок – металева таблетка, усередині якої розташований чіп постійного

пам'яті. При торканні таблеткою зчитувача з пам'яті таблетки в контролер пересилається унікальний код ідентифікатора.

Ідентифікатори і зчитувачі класифікуються за такими ознаками:

- за видом використовуваних ідентифікаційних ознак (ідентифікатори та зчитувачі);
- за способом зчитування ідентифікаційних ознак (зчитувачі).

По виду використовуваних ідентифікаційних ознак ідентифікатори і зчитувачі можуть бути:

- механічні – ідентифікаційні ознаки являють собою елементи конструкції ідентифікаторів (перфорацію, елементи механічних ключів і т.д.);
- магнітні – ідентифікаційні ознаки являють собою намагнічені ділянки поверхні або магнітні елементи ідентифікатора (картки з магнітною смугою, карти Виганда і т.д.);
- оптичні – ідентифікаційні ознаки являють собою нанесені на ідентифікатор мітки, які мають різні оптичні характеристики (карти зі штрих-кодом, голографічні мітки і т.д.);
- електронні контактні – ідентифікаційні ознаки являють собою електронний код, записаний в електронній мікросхемі ідентифікатора (дистанційні карти, електронні ключі і т.д.);
- електронні радіочастотні – електронні ідентифікатори, зчитування коду з яких відбувається шляхом передачі даних по радіоканалу;
- акустичні – ідентифікаційні ознаки являють собою кодований акустичний сигнал;
- біометричні (тільки для зчитувачів) – ідентифікаційні ознаки являють собою індивідуальні фізичні ознаки людини (відбитки пальців, геометрія долоні, малюнок сітківки ока, голос, динаміка підпису і т.д.);
- комбіновані – для ідентифікації використовуються одночасно кілька ідентифікаційних ознак.

За способом зчитування ідентифікаційних ознак зчитувачі можуть бути з ручним введенням, контактні, безконтактні, комбіновані.

Засоби управління – пристрої та програмні засоби, що встановлюють режим доступу та забезпечують прийом і обробку інформації з пристроїв ідентифікації, управління пристроями, що, відображення і реєстрацію інформації.

Класифікація засобів управління СКУД включає в себе: апаратні засоби (пристрої) – контролери доступу (прилади приймально-контрольні доступу); програмні засоби – програмне забезпечення СКУД.

Всі пристрої в системі спілкуються між собою за певними правилами, які називаються протоколами. Існують стандартні протоколи, і це дозволяє використовувати в одній системі обладнання різних виробників. Програмне забезпечення здійснює настройку і управління обладнанням, моніторинг його параметрів, систематизацію та архівування всієї інформації системи.

Контролери – основа апаратної частини системи, до них підключається необхідне додаткове обладнання: зчитувачі, інтерфейсні модулі, замки, геркони (дверні контакти), кнопки виходу, охоронні датчики та інше периферійне устаткування. За способом управління контролери системи контролю та управління доступом діляться на три класи: – мережеві контролери мають на увазі можливість роботи контролерів в мережі під управлінням комп'ютера (рис. 1.9)

Рис. 1.9. Мережеві контролери

Автономні контролери – пристрої, призначені для обслуговування, як правило, однієї точки проходу (рис. 1.10).

Рис. 1.10. Автономний контролер СКУД Z-5R 5000

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; – комбіновані контролери об'єднують функції мережевих і автономних контролерів (рис. 1.11). При наявності зв'язку з керуючим комп'ютером контролери працюють як мережний пристрій, при відсутності зв'язку – як автономні.

Рис. 1.11. Комбіновані контролери

Прочитавши інформацію з карти (або іншого пристрою ідентифікації), контролер звіряє її зі своєю базою даних і приймає рішення: давати чи не давати команду на виконавчий пристрій – замки, турнікети, шлагбауми, хвіртки.

На рис. 1.12 показана схема пристрою системи контролю та управління доступом. Системи КУД класифікують за способом управління, кількості

контрольованих точок доступу, функціональних характеристик, рівнем захищеності системи від несанкціонованого доступу до інформації. За кількістю контрольованих точок доступу системи КУД бувають:

- малої місткості (до 64 точок);
- середньої місткості (від 64 до 256 точок);
- великої місткості (понад 256 точок).

Рис. 1.12. Схема пристрою системи контролю та управління доступом

За способом управління системи КУД можуть бути:

- автономні – для управління одним або декількома УПУ, без передачі інформації на центральний пристрій управління і без контролю з боку оператора;
- мережеві – для управління УПУ з обміном інформацією з центральним пультом і контролем і управлінням системою з боку центрального пристрою управління;
- 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 функціональними характеристиками системи КУД можуть бути трьох класів: з обмеженими і розширеними функціями, а також багатофункціональні.

Класифікація засобів КУД по стійкості до несанкціонованого доступу (НСД) визначається стійкістю до руйнівних і неразрушающим впливів за трьома рівнями стійкості: нормальної; підвищеної; високою.

УПУ класифікують по стійкості до руйнівним діям: злому, пулестійкості (тільки для УПУ із суцільним перекриттям отвору), стійкості до вибуху.

Нормальна стійкість УПУ забезпечується механічною міцністю конструкції. Для УПУ підвищеної та високої стійкості із суцільним перекриттям отвору (суцільні двері, ворота) і з блокуванням об'єкта в отворі (шлюзи, кабіни прохідні) встановлюється класифікація по стійкості до злому, вибуху і пулестійкості.

Пристрої виконавчі (замки, засувки) класифікують за стійкістю до руйнівним діям в залежності від конструкції. За стійкістю до неразрушающим впливів кошти КУД в залежності від їх функціонального призначення класифікують за стійкістю до розтину, маніпулювання, спостереження для зчитувачів введення запам'ятовується коду (клавіатури, кодові перемикачі і т.п.), копіювання (для ідентифікаторів), захисту засобів обчислювальної техніки (СВТ) коштів управління СКУД від несанкціонованого доступу до інформації. Ознайомлення з компонентним складом СКУД дозволяє перейти до їх розгляду досвіду їх проєктування.

1.4 Огляд програмної складової роботи СКУД

Для коректної роботи системи контролю та управління доступом до віддаленого офісу необхідно правильно організувати архітектуру клієнт-сервер.

Клієнт-серверна архітектура набула своєї популярності завдяки динамічному розвитку мережі Інтернет та зосередження значної частини інформації в базах даних на серверах.

Клієнт-серверну архітектуру можна означити, як концепцію інформаційної мережі в якій основна частина її ресурсів зосереджена в

серверах, обслуговуючих своїх клієнтів. Така архітектура визначає такі типи компонентів:

- набір серверів, які надають інформацію або інші послуги програмам, які звертаються до них;
- набір клієнтів, які використовують сервіси, що надаються серверами;
- мережа, яка забезпечує взаємодію між клієнтами та серверами.

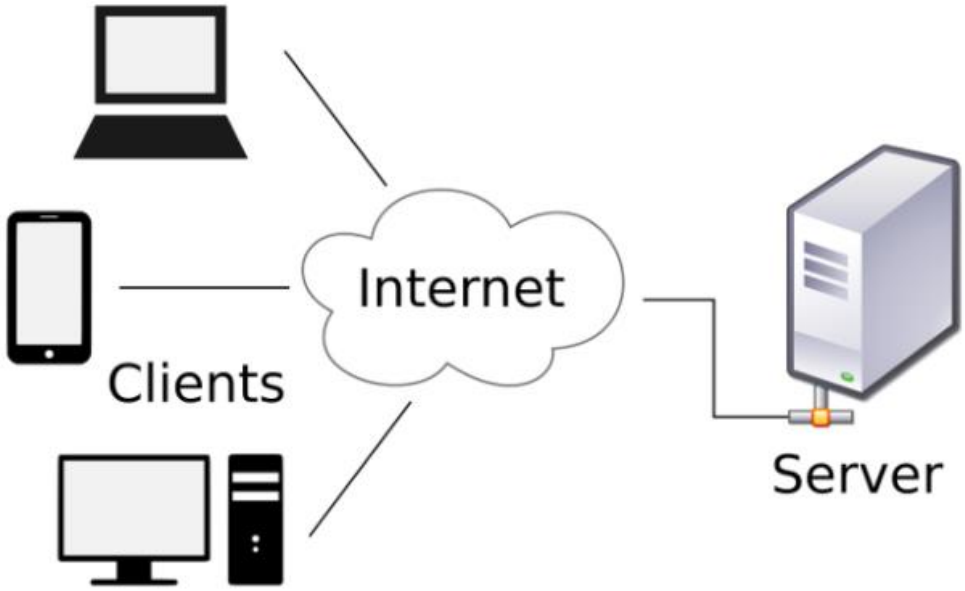


Рис. 1.13. Схема клієнт-серверної архітектури

Правила взаємодії між клієнтом і сервером називаються протоколом обміну (протоколом взаємодії)

Модель взаємодії клієнт-сервер визначається насамперед розподілом відповідальності між клієнтом і сервером. Логічно виділити три рівні операцій:

- рівень представлення даних, який, по суті, є інтерфейсом користувача і відповідає за представлення даних користувачеві та введення команд управління від нього;
- рівень програми, який реалізує основну логіку програми і на якому здійснюється необхідна обробка інформації;
- рівень управління даними, який забезпечує зберігання та доступ до даних.

Дворівнева архітектура клієнт-сервер передбачає взаємодію двох програмних модулів – клієнта та сервера. Залежно від того, як вищезазначені функції розподілені між ними, є:

- модель тонкого клієнта, в якій вся логіка управління програмами та даними зосереджена на сервері. Клієнтська програма забезпечує лише функції рівня презентації;
- товста клієнтська модель, в якій сервер керує лише даними, а обробка інформації та користувальницький інтерфейс зосереджені на клієнтській стороні. Товстих клієнтів також часто називають пристроями з обмеженою потужністю: КПК, мобільні телефони тощо.

Трирівнева архітектура клієнт-сервер, яка почала розвиватися в середині 1990-х, передбачає відокремлення рівня додатків від управління даними. Виділяється окремий програмний рівень, який фокусується на логіці програми програми. Програми середнього рівня можуть працювати на спеціальних серверах додатків, але такі програми можуть працювати і на звичайному веб-сервері. Нарешті, даними керує сервер даних.

Дворівнева архітектура простіша, оскільки всі запити обслуговуються одним сервером, але через це вона менш надійна і ставить більш високі вимоги до продуктивності сервера.

Трирівнева архітектура є більш складною, але через те, що функції розподілені між серверами другого та третього рівня, ця архітектура демонструє:

- високий ступінь гнучкості та масштабованості.
- високий рівень безпеки (оскільки захист може бути визначений для кожної послуги або рівня).
- висока продуктивність (оскільки завдання розподіляються між серверами).

Прикладом взаємодії клієнт-сервер є служба WWW. Існує величезна кількість веб-серверів, на яких розміщується та чи інша інформація. У найпростішому випадку ця інформація являє собою набір веб-сторінок, які

можна зберігати на сервері як файли, позначені мовою розмітки HTML. Але ситуація, як правило, складніша; значна частина веб-ресурсів на сучасному етапі є динамічними, тобто вони не існують у заздалегідь підготовленому вигляді, а створюються безпосередньо в процесі обробки запиту від користувача.

Основна ідея архітектури клієнт-сервер полягає в розділенні мережевого додатка на кілька компонентів, кожен з яких реалізує певний набір послуг. Компоненти такої програми можуть працювати на різних комп'ютерах, виконуючи серверні та / або клієнтські функції. Це підвищує надійність, безпеку та продуктивність мережевих додатків та мережі в цілому.

Ролі сервера

Роль – це функція сервера (наприклад, пошти, контролера домену тощо). Один сервер може грати одну або кілька ролей одночасно.

Залежно від ролі наданої послуги, існують такі сервери:

Веб-сервер

Сервер, який отримує запити HTTP від клієнтів, як правило, веб-браузерів, дає їм відповіді HTTP, як правило, разом із HTML-сторінкою, зображенням, файлом, медіа-потоком або іншими даними. Веб-сервер є основою Всесвітньої павутини.

Веб-сервер – це і програмне забезпечення, яке діє як веб-сервер, і комп'ютер, на якому працює програмне забезпечення.

Клієнти отримують доступ до веб-сервера за URL-адресою веб-сторінки або іншого потрібного їм ресурсу.

Сервер додатків

Сервер, який запускає деякі програми. Цей термін також відноситься до програмного забезпечення, яке встановлено на такому сервері та забезпечує виконання прикладного програмного забезпечення.

Сервери баз даних

Сервери баз даних використовуються для обробки запитів користувачів у SQL. Таким чином, СУБД знаходиться на сервері, до якого підключені клієнтські програми.

Файловий сервер

Сервер, який зберігає інформацію у вигляді файлів та надає користувачам доступ до неї. Як правило, файловий сервер забезпечує певний рівень захисту від несанкціонованого доступу.

Сервер друку

Сервери друку використовуються для забезпечення та контролю доступу до принтерів. Роль сервера друку дозволяє вам керувати принтерами через веб-браузер, друкувати через URL-адресу принтера за допомогою IPP та підключати принтери за допомогою Point і Print.

Поштовий сервер

Дозволяє вам підтримувати основні поштові скриньки ваших користувачів і дозволяє отримувати та надсилати пошту з сервера. Вхідну пошту можна зберігати на сервері, а потім отримувати від користувача через POP3. На роль

1.5 Огляд існуючих СКУД та доцільність придбання

Різноманіття наявних на ринку виробників СКУД обумовлено спробою задовольнити безліч потреб замовників. У кожного виробника свій напрямок діяльності по функціоналу обладнання та програмного забезпечення. Хтось пропонує великі, складні системи, що підтримують інтеграцію з пожежними системами, системами відеоспостереження, і т.д., а хтось має спрямованість на невеликі будівлі і приміщення з невеликим числом співробітників.

При такому розмаїтті виробників і значній кількості характеристик обладнання покупцеві досить складно вибрати продукт, який йому підходить. Тому доводиться або звертатися до консультантів, або вибирати те, що більш сподобалося зовні.

У більшості випадків замовник може ознайомиться з основними можливостями систем використовую інформацію представлену на офіційних сайтах виробників. Не останню допомогу при виборі і огляді конкретної системи надають спеціалізовані видання.

Проведемо огляд та порівняльна характеристика представлених на ринку СКУД. На основі бізнес-кейсу, наближеного до реальної ситуації, проаналізовано основні технічні та програмні можливості більшості продуктів.

Розглянемо характеристики найбільш потужних, з точки зору можливостей розширення і інтеграції в автоматизовані системи підприємства, СКУД представлених на ринку.

OnGuard: інтегрована система безпеки компанії Lenel для висотних будівель і організацій з територіально розподіленими офісами [11]. Відмітна особливість системи OnGuard компанії Lenel Systems International – це комплексне рішення по забезпеченню безпеки офісних будівель компаній з чисельністю від 100 до 100 000 чоловік, коли робота різних компонентів системи здійснюється з єдиною базою данних, з єдиними вихідними програмними кодами і використовується єдиний графічний інтерфейс для всіх додатків. При цьому інтегрована система безпеки Lenel легко масштабується: всі складові частини платформи OnGuard можуть працювати в умовах як невеликих, так і дуже великих підприємств, а купивши спочатку один модуль для системи контролю доступу (СКД), споживач завжди може доповнити його системою відеоспостереження, охоронної, пожежною сигналізацією та ін. охоронними системами. Крім того, платформа OnGuard має відкриту архітектуру, тому для підприємств, що мають віддалені філії, можливий централізований контроль регіональних систем через LAN / WAN.

Система централізованого контролю доступу WIN-PAK PRO Central Station від компанії honeywell пропонує економічне і легко кероване рішення для комерційних підприємств і можливість отримання регулярного доходу для компаній-установників систем безпеки [11]. Основні переваги:

- реалізація хмарної моделі надання додатки для системи контролю та

управління доступом;

- зниження вартості системи, збільшення кількості клієнтів;
- зниження витрат на установку, навчання персоналу і обслуговування системи;
- представлення додаткових послуг, що продовжують співпрацю підрядника з замовниками;
- користувачі можуть управляти своїми системами через вебінтерфейс.

ІСО «Оріон» компанії Болід – це не тільки СКД [7]. Система являє собою найбільш універсальний апаратно-програмний комплекс серед представлених на ринку. Комплекс дозволяє в рамках єдиного інформаційного простору будувати взаємодіючі системи охоронної та пожежної сигналізації, пожежної автоматики, СКД, відеоспостереження та диспетчеризації. В основі архітектури ІСО «Оріон» покладається модульний принцип. Система складається з безлічі розподілених по захищається взаємозамінних приладів, які, в залежності від проведених на етапі налагодження налаштувань, вирішують одну або кілька із зазначених вище завдань. В якості транспортного рівня єдиного інформаційного простору системи в основному використовуються RS-485 інтерфейс і мережі Ethernet. Крім того, існують рішення по організації бездротових ліній зв'язку.

Впровадження СКД на базі ІСО «Оріон» дозволить вирішити три основні завдання:

1. Організація контролю переміщення персоналу.
2. Організація охорони підприємства.
3. Організація обліку.

Проаналізуємо основні технічні параметри, переставлені в таблиці 1.1.

Таблиця 1.1

Порівняльна характеристика технічних характеристик СКУД

Параметр	OnGuard	WIN-PAK PRO Central Station	ІСО «Оріон»
Макс. кількість індентифікаторів для точки проходу	12 500	65 500	8 192
Макс. Кількість контролерів в мережі	Не обмежено	1 000	32 385
Макс. Кількість користувачів в системі	Не обмежено	Не обмежено	64 897
Зональний antipassback	Наявно	Наявно	Наявно
Інтерфейс підключення контролерів	Ethernet, RS-485	Ethernet, RS-485	Ethernet, RS-485
Максимальна довжина магістралі до контролера	1 219 м	1 219 м	1 200 м
Наявність часових зон	Наявно	Наявно	Наявно

Незважаючи на незначні відмінності розглядаються СКУД схожі. Слід зазначити, що більшість виробників СКУД не пропонує типових рішень. Архітектура конкретного проєкту ґрунтується на потребах замовника. У більшості випадків на ринку пропонується обладнання, що дозволяє конструювати системи під будь-які потреби.

1.6 Особливості СКУД у віддаленому офісі

Особливістю будь-якої віддаленої роботи є захист інформації.

Документи не повинні зберігатися на локальних пристроях співробітників. Малі об’єми файлів можна зберігати на Google Docs / Office 365. Це використовується для того, щоб при зідзвоні з головним офісом була можливість відкрити і працювати з документами одночасно. Це одна з основних і дуже зручних особливостей при віддаленій роботі.

Інформацію, яку співробітник пересилає на хмарне сховище, можуть перехопити, а приватну розмову по скайпу можуть просто підслухати в

коворкінг. Втрата або розголошення інформації може нести величезні ризики для компанії.

Установка багаторівневої аутентифікації, паролів, файерволов стає першочерговою необхідністю при роботі з конфіденційними даними.

Однак захист інформації не обмежується виключно технічними засобами. Не менш важливим є наявність чітких правил захисту інформації в компанії, а також регулярне проведення різних тренінгів і воркшопів, в ході яких роз'яснюються правила зберігання важливої інформації, використання особистої пошти, Фейсбуку або скайпу для робочих цілей, використання електронних пристроїв для особистих цілей і багато іншого.

Висновки до розділу 1

Розглянувши функціональні можливості СКУД, вимоги до них, оцінивши методи ідентифікації можна зробити висновок, що СКУД це система, основне завдання якої управління доступом на задану територію, що включає можливості розмежування прав доступу, що дозволяє проводити ідентифікацію користувача і включає додаткові аналітичні функції. Сукупність різних методів ідентифікації дозволяє організувати максимальний рівень захисту об'єкта від несанкціонованого доступу.

У даному розділі було розглянуто загальні принципи роботи СКУД і проаналізовано їх основні можливості. Наведено головні компоненти систем контролю і управління доступом, виявлена затребуваність СКУД на об'єктах малих підприємств. Аналіз та порівняння можливостей існуючих СКУД підтвердив необхідність створення власної СКУД, адаптованої під даний тип підприємсв. Огляд особливостей систем контролю і управління доступом у віддалених офісах виявив необхідність установки СКУД у віддалених офісах малих підприємств. Отже, необхідно спроєктувати систему контролю і управління доступом відповідно до всіх нормативних документів, що регламентують безпеку підприємства.

Вивчивши актуальні тенденції в області СКУД як в Україні, так і за кордоном, вважаємо за необхідне використовувати в проєкті обладнання, пристрої та матеріали, що відповідають сучасним вимогам, в т.ч. таким аспектам, як ефективність, оптимальна вартість, ремонтопридатність і можливості модернізації.

РОЗДІЛ 2. ЗАГАЛЬНА ХАРАКТЕРИСТИКА ОБ'ЄКТУ ДОСЛІДЖЕННЯ

2.1 Характеристика «Plexon Inc.»

Віддалений офіс «Plexon Inc.» є єдиним віддаленим офісом підприємства. Головний офіс знаходиться у штаті Нью Джерсі, США.

Основна діяльність підприємства:

- Використання способу *Dropsipping* для продажу товарів на інтернет-сервісі *Amazon*.
- Розробка програмного забезпечення.
- Підтримка власної бази даних товарів постачальників;
- Опрацювання скарг та відгуків покупців.

Віддалений офіс розташований за адресою:, Україна, місто Київ, вулиця Маршала Малиновського, будинок 4, 04212 (рис. 2.1).

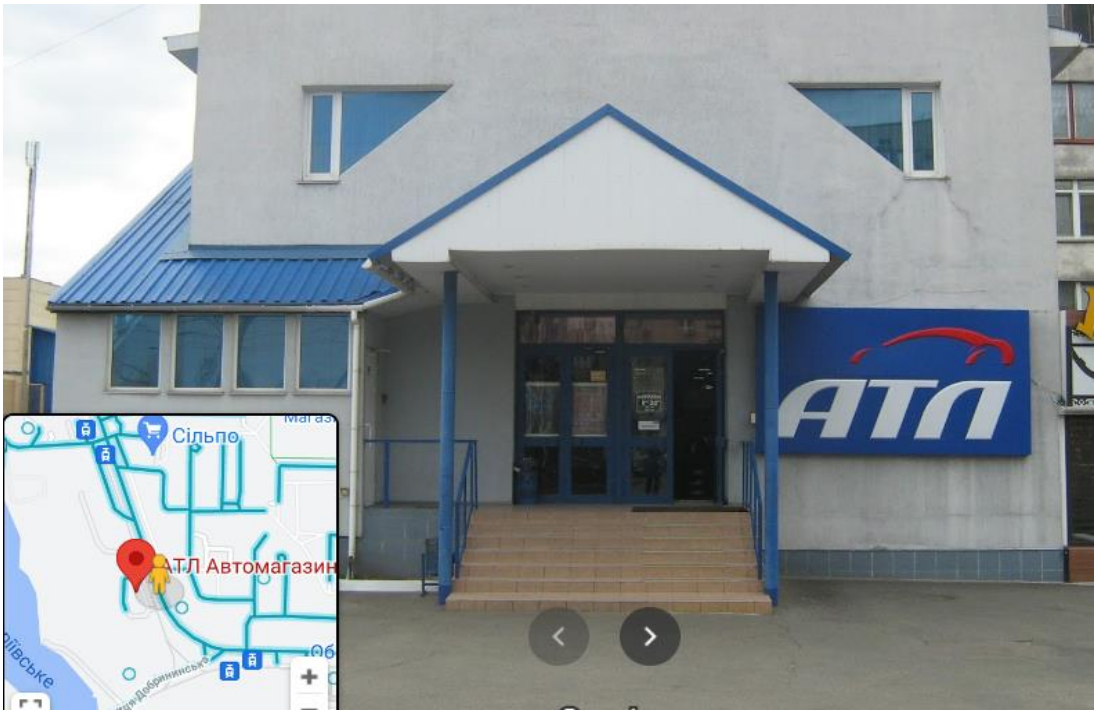


Рис. 2.1. Загальний вигляд приміщення офісу

Віддалений офіс підприємства «Plexon Inc.» розміщено на другому поверсі окремо розташованої двоповерхової будівлі. Територія знаходиться під

постійною охороною. Вхід у офіс є окремим з вулиці. На вході ззовні та по всій внутрішній площі приміщення розміщено 8 камер спостереження. Загальна площа території офісу складає 380 м^2.

Загальна кількість працівників, включаючи допоміжний персонал, становить 19 осіб. Віддалений офіс підприємства «Plexon Inc.» в м. Київ включає в себе наступні основні приміщення: вестибюль, кабінет директора, кабінет менеджера з розробки програмного забезпечення, кабінет розробки програмного забезпечення, кабінет бухгалтера, кабінет менеджерів з продажу, кабінет підтримки клієнтів, кімната відпочинку, кухня та два санвузли.

Офіс є закритого типу, відвідуваність становить близько 1 людини на 1-2 тижня. Віддалений офіс підприємства «Plexon Inc.» в м. Київ не відноситься до об'єктів з масовим перебуванням людей. На об'єкті є в наявності план евакуації людей у разі пожежі із позначеними місцями зберігання первинних засобів пожежогасіння.

Фізична охорона здійснюється співробітниками охоронної служби «Guard_Kiev» цілодобово. Пост охорони розташований на першому поверсі і є загальним для всієї території будівлі. Фізична охорона призначена для забезпечення безпеки клієнтів і персоналу, дотримання громадського порядку, збереження майна, фінансів і цінностей магазину АЛТ, розташованого на першому поверсі та віддаленого офісу підприємства «Plexon Inc.», розташованого на другому поверсі.

Приміщення офісу має об'ємно-планувальне рішення і конструктивне виконання шляхів евакуації, які забезпечують безпечну евакуацію людей при пожежі. Є один евакуаційний вихід, що веде з приміщень назовні. Евакуаційні шляхи і проходи утримуються в належному стані. Напруга електромереж 380/220 В, їх експлуатація, а також контроль за технічним станом здійснюється відповідно до вимог нормативних документів по електроенергетиці спеціалізованою організацією, що має на даний вид діяльності відповідну ліцензію.

2.2 Аналіз існуючої СКУД у віддаленому офісі «Plexon Inc.»

Для забезпечення безпеки функціонування досліджуваного об'єкта використовуються, крім фізичної охорони, системи контролю і управління доступом, охоронного відеоспостереження, охоронної сигналізації, пожежної сигналізації.

Вхід і вихід працівників відбувається через основний вихід, обладнаний охоронною сигналізацією. У встановлений час перед початком робочого дня співробітник охорони в присутності керівника (заступника керівника) здійснює зняття приміщення з охоронної сигналізації, відкриваючи його. Факт розкриття фіксується в журналі за двома підписами. Далі співробітник охорони контролює проходження працівників на робочі місця, залишаючись на місці протягом доби. Автоматична ідентифікація особистості працівників не проводиться, записи в системі обліку робочого часу не здійснюються. Якщо протягом робочого дня співробітнику необхідно неодноразово входити і виходити, то важко оцінити час перебування його офісі.

Отже, очевидна необхідність оптимізації системи контролю та управління доступом для підвищення контролю пропускного та внутрішнього режиму. При оснащенні офісу системою відеоспостереження застосовувався принцип тотального контролю всієї території. У систему охоронного відеоспостереження у офіс входять:

- вісім IP-камер (вісім внутрішніх «Logitech Alert 700n Indoor Security Camera);
- джерело безперебійного живлення Back-UPS BK650EI (650 ВА) (виробник – «APC by Schneider Electric», США);
- комутатор TL-SG105E (виробник компанія «TP-LINK», Китай);
- сервер з програмним забезпеченням, де записується і архівується інформація з камер відеоспостереження.

Несанкціоноване проникнення на об'єкт система охоронної сигналізації детектує за допомогою магніто-контактних сповіщувачів в кількості 4 шт. Для блокування дверних прорізів на відкривання або зміщення використовуються

точкові магнітоконтактні охоронні сповіщувачі ІВ 102-14, виробник ТОВ НВКФ «Комплектстройсервіс» (рис. 2.2).

Рис. 2.2. Точкові магнітоконтактні охоронні сповіщувачі ІВ 102-14

Сповіщувач конструктивно складається з двох блоків: виконавчого (магнітокерованих датчика) і задає (керуючого магніту), укладених у пластмасові корпусу за формою близькою до прямокутної. З магнітокерованих датчика виведені два багатожильних дроти для підключення сповіщувача до шлейфу сигналізації, полярність підключення сповіщувачів значення не має.

Досліджуваний об'єкт оснащений системою пожежної сигналізації. З огляду на пожежне навантаження, на досліджуваному об'єкті змонтовано адресні димові оптико-електронні сповіщувачі СПД-3 (рис. 2.3) в кількості 16 шт. Виробник – ТОВ «АРТОН».

Для прийому повідомлень по адресній шині від сповіщувачів використовується адресний модуль АМ-99, який забезпечує живлення і контроль режиму роботи сповіщувача по двухпроводній адресній шині і формує сигнал для приймально-контрольного приладу «Сигнал-20П» (виробник НВП «Болід»).

Для оповіщення персоналу про пожежу у всіх приміщеннях (з постійним або тимчасовим перебуванням людей) встановлено світлозвукові оповіщувачі «Сопілка-2» (рис. 2.4). Виробник: АТ «Радій».

Рис. 2.3. Димовий оптико-електронний сповіщувач ІП 212-60А (Леонардо-О)

Рис. 2.4. Світлозвуковий оповіщувач «Сопілка-2»

Рівень сигналу на відстані 1 м від оповіщувача – 105 дБ. Оповіщувачі підключають до приймально-контрольного приладу «Сигнал-10», (виробник НВП «Болід»). Для забезпечення системою безперебійного електропостачання у офісі використовується джерело безперебійного живлення APC by Schneider Electric Back-UPS BK650EI (650 ВА) (виробник «APC by Schneider Electric», США).

Висновки до розділу 2

Офіс є закритого типу, відвідуваність становить близько 1 людини на 1-2 тижня. Віддалений офіс підприємства «Plexon Inc.» в м. Київ не відноситься до об'єктів з масовим перебуванням людей.

Таким чином, організацію системи безпеки на досліджуваному об'єкті слід визнати задовільною, однак в модернізації потребує система контролю і управління доступом, яку необхідно інтегрувати з наявними системами охоронного відеоспостереження, охоронної та пожежної сигналізації.

РОЗДІЛ 3. ПРОЄКТУВАННЯ СКУД ДЛЯ ВІДДАЛЕНОГО ОФІСУ «PLEXON INC.»

3.1 Розрахунки та аналітика

3.1.1 Технічне завдання на проєктування СКУД

Вимоги замовника становлять основу технічного завдання на створення СКУД і є документом, з якого починається робота зі створення СКУД. Крім технічних вимог, на перших етапах роботи з проєктування СКУД в якості вихідної інформації використовуються дані, отримані в процесі передпроєктного обстеження. Від грамотного підходу до технічного завдання залежать терміни проєктування і вибір необхідного обладнання для СКУД.

СКУД складається з програмної та технічної частини. Програмна частина включає в себе наступні компоненти:

- комплект серверного і призначеного для користувача програмного забезпечення;
- комплект засобів для забезпечення інтеграції системи СКУД з іншими системами безпеки офісу.

Технічна частина включає: контролери СКУД; ідентифікатори; зчитувачі та ін.

Обробка інформації відбувається на центральному сервері з встановленим серверним програмним забезпеченням. Взаємодія пристроїв СКУД здійснюється за певними каналами зв'язку: Ethernet, RS485. СКУД повинна обслуговувати такі приміщення і пристрої за типами: двері приміщень; турнікет.

Прохід через турнікет здійснюється з відеоверіфікацією, що проходить через особистий пристрій співробітника за допомогою IPкамери і контролем температури. Висновок зображення здійснюється на АРМ співробітника охорони і передається на сервер, де зберігається. При запуску системи оповіщення про пожежу турнікет автоматично відкривається. Вхідні двері,

обладнані врізним зсувними електромагнітним замком типу AL-300, в робочий час постійно відкрита.

Для службових приміщень, крім функцій контролю доступу, система повинна підтримувати виконання охоронних функцій, тобто постановку і зняття приміщення з-під охорони картою доступу. Кожне контрольоване приміщення бути обладнано світлозвуковим пристроєм, що відображає поточний стан приміщення. Світлозвуковий пристрій виконано в єдиному корпусі зі зчитувачем. На випадок нештатного блокування дверей, всередині кожного приміщення встановлюється кнопка примусового відкривання. При запуску системи оповіщення про пожежу двері всіх контрольованих приміщень, що знаходяться не під охороною, повинні перейти у відкритий стан.

Алгоритм роботи системи для вхідних дверей: в штатному режимі вхідні двері знаходиться під охороною. Вхід першого має доступ працівника в вважається зняттям приміщення з охорони. При знятті з охорони система обезструмлює виразний зсувний електромагнітний замок. В кінці робочого дня після того як виходить з приміщення останній співробітник (співробітник охорони) ставить вхідні двері на охорону. Етапи постановки приміщення під охорону повинні відображатися станом светозвукового пристрою.

Алгоритм роботи системи для службових приміщень: в черговому режимі службові приміщення стоять під охороною. На АРМ відображається планування всіх приміщень віддаленого офісу з поточним станом усіх шлейфів. У разі несанкціонованого проникнення на моніторі з'являється планування будівлі і спрацював шлейф.

Ведеться журнал обліку сработок. Відповідно до режиму роботи офісу, за 10 хв до встановленого часу відкриття, для конкретного працівника активується доступ до конкретного приміщення. При знятті з охорони приміщення шляхом ідентифікації карти доступу зчитувачем, система обезструмлює виразний зсувний електромагнітний замок. В охороняється період контролер приміщення виконує функцію реєстратора присутніх. Кожен співробітник що заходить через зчитувач реєструє свою присутність шляхом прикладання до зчитувача

персональної картки. В кінці робочого дня працівник докладає персональну картку до зчитувача-реєстратору, дверний замок переходить в закритий стан.

Етапи постановки приміщення під охорону повинні відображатися станом світлозвукового пристрою. У разі невдалої постановки на охорону, система посилає повторний запит на постановку і лише потім відправляє сигнал помилки на АРМ охорони. Алгоритм роботи системи для дверей побутової кімнати: контроль відкривання таких дверей передбачає прохід через них по реакції вхідного зчитувача на права доступу користувача.

Програмне забезпечення СКУД має забезпечувати можливість подальшого розширення системи (кількості контролерів, користувачів в системі, кількості вилучених робочих місць). Система повинна зберігати працездатність і забезпечувати відновлення своїх функцій (при перезапуску) при виникненні наступних позаштатних ситуацій:

- при збоях в роботі апаратної частини, що призводять до перезавантаження операційної системи сервера СКУД;
- при помилках в роботі програмного забезпечення СКУД; – при помилках, пов'язаних з програмним забезпеченням сторонніх виробників (наприклад, драйверів пристроїв), відновлення працездатності покладається на операційну систему сервера СКУД.

Контролери СКУД встановлюються всередині об'єкту, що охороняється (захищається) об'єкта і забезпечують цілодобовий режим роботи. За замовленням середнє напрацювання контролерів СКУД на відмову повинно становити не менше 10 000 г, середній термін служби контролерів СКУД повинен бути не менше 8 років з урахуванням проведення відновлювальних робіт. Система електроживлення контролерів СКУД забезпечує захисне відключення при перевантаженнях і коротких замиканнях в ланцюгах навантаження, а також аварійне ручне відключення і автоматичне відновлення електроживлення після усунення причини несправності. Конструкція контролерів Фактори, що шкідливі впливи на здоров'я, пов'язані з роботою контролерів СКУД не повинні перевищувати діючих норм СанПіН

2.2.2./2.4.1340-03. Конструкція контролерів СКУД повинна забезпечувати ступінь захисту оболонки IP20. Контролери повинні зберігати працездатність і виконання всіх вимог, що пред'являються при впливі зовнішніх електромагнітних завад. Контролери СКУД повинні бути універсальними і підтримувати відразу кілька типів точок доступу: двері, турнікет і ін. Контролери повинні апаратно підтримувати режим глобального AntiPassBack без участі сервера, тобто заборона подвійного проходу – запобігати прохід двох і більше відвідувачів по одному ідентифікатору, формувати точні звіти робочого часу співробітників підприємства. Контролери повинні підтримувати роботу зі зчитувачами форматів Wiegand-26 і TouchMemory. На контролері повинна бути передбачена можливість сумісності зі зчитувачами різних виробників.

Програмна частина СКУД повинна забезпечувати захист від несанкціонованого доступу. Клас захищеності інформаційної системи об'єкта захисту визначається в залежності від рівня значущості оброблюваної інформації і масштабу інформаційної системи. Віддалений офіс підприємства «Plexon Inc.» є невеликомасштабною інформаційною системою. Згідно з цим захист від несанкціонованого доступу повинна проводитися за трьома напрямками:

- ідентифікація користувача;
- перевірка повноважень користувача при роботі з системою;
- розмежування доступу користувачів.

Програмне забезпечення СКУД має відновлювати своє функціонування при коректному перезапуску апаратних засобів. Повинна бути передбачена можливість організації автоматичного і (або) ручного резервного копіювання даних системи.

Всі роботи по монтажу виконуються відповідно до чинного законодавства України з обов'язковим виконанням норм і правил охорони праці, пожежної безпеки і техніки безпеки, виробничої санітарії, з огляду на специфіку будівлі і дотриманням внутрішнього розпорядку знаходження на

території, що охороняється (дотримуватися режимних вимог і пропускний режим, встановлені на об'єкті).

При проводці кабельних ліній не пошкоджувати технічні та інженерні комунікації, запобігти доступ до них сторонніх осіб. Роботи виконувати згідно з розробленим і затвердженим

Підрядник повинен гарантувати якість виконаних робіт і використовуваних матеріалів, гарантійний термін якості виконаних робіт з моменту здачі робіт повинен становити не менше 12 місяців.

Грамотно розроблена концепція СКУД і технічне завдання дає підстави для створення проєкту СКУД – єдиного комплексу рішень, призначеного для забезпечення заданого режиму експлуатації СКУД.

Проєкт визначає оптимальну структуру СКУД і трасу прокладки кабельних проводок, розташування і склад елементів СКУД.

Проєктна документація СКУД є текстові та графічні матеріали, що визначають об'ємно-планувальні, конструктивні та технічні рішення для будівництва СКУД. Вона забезпечує детальну прив'язку компонентів СКУД до об'єкту і містить креслення, таблиці з'єднань і підключень, плани розташування обладнання і проводок і інші документи.

3.1.2 Проєкт СКУД віддаленого офісу «Plexon Inc.» в м. Київ

Рішення СКУД розроблено на основі типового проєкту, розміщеного на сайті виробника і забезпечує:

- санкціонований доступ співробітників в зони приміщення;
- видачу сигналу тривоги на АРМ чергового оператора або на пульт управління в разі несанкціонованого доступу (відкриття дверей) в зони доступу і виділені приміщення;
- комп'ютерний облік входу і виходу відвідувачів і співробітників з веденням протоколу в комп'ютері і виведення протоколу на принтер;
- контроль і реєстрацію переміщення персоналу в протоколі комп'ютера;
- можливість тимчасового блокування дверей, які не беруть участі в

забезпеченні технологічного циклу.

До складу СКУД входять:

• станційне встаткування, до складу якого входять сервер ELSYS Бастіон-2-Сервер 5000 і АРМ співробітника охорони «Бастіон-2-АРМ УРВ Про», реалізовані на базі персональних комп'ютерів, об'єднані в локальну мережу, мережевий комутатор Elsys- MB-Net;

• лінійне обладнання, що включає в себе контролери СКУД ElsysMB-SM-2A-ТП. Контролери з'єднані між собою двухпроводной лінією зв'язку з інтерфейсом RS-485 за схемою загальної шини. Як середовище передачі даних інтерфейсу RS-485 використовуються мідні кручені пари. Ці групи контролерів підключені до сервера, з якого здійснюється управління і програмування кожного контролера;

• абонентські пристрої: електромеханічний турнікет-трипод з контролем температури тіла Elsys ST-TS100, електромагнітні замки «ML200 M», зчитувачі безконтактних карт доступу Smart-wave, кнопки «ВИХІД» і кнопки розблокування замків (турнікета) в разі виникнення надзвичайної ситуації, магнітоконтактні сповіщувачі «ІВ 102-16 / 2», відеодомофон «VideoNova A40-IP-16».

У додатку А показана загальна схема приміщення.

До складу СКУД входять точки контролю доступу (ТКД) двох типів: двері одно- або двосторонні – у приміщення офісу; турнікет – вхід в будівлю. Точка контролю доступу функціонально складається з контролера доступу, виконавчого механізму (турнікет, двері), зчитувачів, магнітоконтактних сповіщувачів.

До складу ТКД входить джерело резервованого харчування для підтримки працездатності пристроїв при тимчасовому зникненні напруги мережі живлення. Прохід через точки з контролем доступу здійснюється при тому, що піднесло безконтактної карти до зчитувача. У разі успішної ідентифікації карти доступу системою виконавчий пристрій розблокується, дозволяючи одноразовий прохід. Кожній карті в базі даних СКУД

присвоюються певні права доступу і відомості: список дозволених точок входу; розклад дозволеного проходу; дані по співробітнику (П.І.Б., посада і т.д.); фотографія співробітника; табельний номер; додаткові параметри (при необхідності). Кожна точка проходу контрольована системою, може бути відкрита для проходу різними способами:

- автоматичний (по пред'явленню безконтактної карти зчитувача) – пропуск постійних співробітників, що йдуть без порушень тимчасового режиму і зони доступу;
- пряма команда з АРМ в разі необхідності вільного доступу або доступу за разовими перепустками;
- централізоване відключення замикаючих пристроїв на всіх точках проходу, що застосовується в екстрених ситуаціях, пов'язаних з природними катаклізмами, пожежею і т.п. – ручне управління з кнопок розблокування.

Будь-який з названих способів відкриття точки проходу фіксується в протоколі системи. Протокол зберігається на жорсткому диску сервера СКУД, доступ до протоколу захищений паролем.

Управління системою і моніторинг за її роботою здійснюється з сервера і з АРМ оператора. Сервер являє собою високопродуктивний комп'ютер. Контролери доступу підключаються до сервера за допомогою перетворювача інтерфейсів USB / RS-485. Сервер працює під управлінням операційної системи Windows 10 і програмного комплексу «Бастіон» з драйверами устаткування «Бастіон-Elsys».

Додатково на сервер встановлюється програмний модуль «БастіонАрхів», який дозволяє здійснювати адміністрування бази даних протоколу (створювати резервні копії, проводити очищення або вивантаження даних протоколу). Автоматизоване робоче місце являє собою персональний комп'ютер, що працює під управлінням операційної системи Windows 10 і програмного модуля «Бастіон-Мережа». З АРМ здійснюється контроль, управління і налаштування обладнання.

Сервер і АРМ об'єднуються в локальну мережу за допомогою мережевого комутатора. Двостороннім доступом обладнуються приміщення бугалтерії і керівника. В цьому випадку зчитувачі встановлюються з обох боків дверей. З внутрішньої сторони додатково встановлюється кнопка пожежного розблокування. При виникненні екстреної ситуації двері можуть бути розблоковані зсередини кнопкою розблокування.

При цьому подія «Ручне розблокування дверей» фіксується в протоколі подій системи. Із зовнішнього боку дверей, обладнаного одностороннім доступом, встановлюється зчитувач безконтактних ідентифікаційних карт доступу, а з внутрішньої сторони – кнопка виходу. Блокування дверей здійснюється електромеханічним замком, встановлюються в косяк. Закривання дверей забезпечує гідравлічний доводчик. Контролер управління дверима встановлюється в безпосередній близькості від точки доступу.

Прохід через точку доступу здійснюється наступним чином: співробітник або відвідувач, надає карту доступу безконтактного зчитувача, встановленому поряд з контрольованою дверима. При успішній ідентифікації (надано доступ до такого району контролю) двері розблокуються, дозволяючи здійснити одноразовий вхід (про результат ідентифікації сигналізує сам зчитувач світлозвуковим і звуковим сповіщенням).

Для виходу з контрольованої зони співробітник або відвідувач повинні натиснути кнопку виходу, при цьому двері розблокується, дозволяючи здійснити одноразовий вихід. В холі розташований турнікет для проходу співробітників. Проєктним рішення передбачається установка одного турнікета для безперешкодного і своєчасного проходу співробітників.

Висновок зроблений на основі даних спостережень за кількістю відвідувань офісу. Спостереження проводилися протягом 5 робочих днів протягом всього дня. Дані спостережень наведені в табл. 3.1.

Таблиця 3.1

Статистика проходів через турнікет за досліджуваний період

День спостереження	Кількість проходів
День 1	36
День 2	42
День 3	38
День 4	46
День 5	54

Кількість персоналу у штаті становить 19 чол, а пропускна здатність турнікета 15 чол. / хв. В ході спостережень встановлено, що пропускна здатність одного турнікета значно перевищує кількість людей, що знаходяться в приміщенні офісу. Аналізуючи отримані результати, можна зробити висновок, що достатньо встановити один турнікет.

У додатку Б наведено структурну схему СКУД. Розміщення обладнання СКУД по точках доступу представлено в табл. 3.2.

Таблиця 3.2

Розміщення обладнання СКУД по точках доступу

Точка доступу	**Розміщення**	**Обладнання**
ТД1	Кабінет менеджера з розробки програмного забезпечення	Контролер Elsys-MB-SM-2A-ТП, зчитувач ElsysSW10-EH, магнітоконтактний сповіщувач «ІВ 102- 16/2», кнопка відкриття дверей без фіксації, замок електромагнітний «ML-200 M»
ТД2	Кабінет розробки програмного забезпечення	Зчитувач Elsys-SW10-EH, магнітоконтактний сповіщувач «ІВ 102-16 / 2», кнопка відкриття дверей без фіксації, замок електромагнітний «ML-200 M»
ТД3	Кабінет директора	Контролер ElsysMB-SM-2A-ТП, комутатор ElsysMB-Net, сервер IBM, зчитувач Elsys-SW10-EH, Магнітоконтактний сповіщувач «ІВ 102-16 / 2», кнопка відкриття дверей з фіксацією, замок електромагнітний «ML-200 M»

Продовження таблиці 3.2

ТД4	Кабінет підтримки клієнтів	Контролер Elsys-MB-SM-2A-ТП, зчитувач ElsysSW10-EH, магнітоконтактний сповіщувач «IB 102-16/2 «, кнопка відкриття дверей без фіксації, замок електромагнітний «ML-200 M»
ТД5	Кабінет менеджерів з продажу	Контролер Elsys-MB-SM-2A-ТП, зчитувач ElsysSW10-EH, Магніто-сповіщувач «IB 102-16 / 2 «, кнопка відкриття дверей з фіксацією, замок електромагнітний «ML-200 M»
ТД6	Кабінет бухгалтера	Контролер Elsys-MB-SM-2A-ТП, зчитувач ElsysSW10-EH – 2 шт., Магніто-сповіщувач «IB 102-16 / 2 «, кнопка відкриття дверей з фіксацією, замок електромагнітний «ML-200 M»
ТД7	Вестибюль	Контролер Elsys-MB-SM-2A-ТП, зчитувач ElsysSW10-EH – 2 шт., Магніто-сповіщувач «IB 102-16 / 2 «, кнопка відкриття дверей з фіксацією, замок електромагнітний «ML-200 M»
ТД8	Вхід у приміщення	Контролер Elsys-MB-SM-2A-ТП, АРМ, відеомагнітофон «VideoNova A40-IP-16», турнікет Elsys ST-TS100, замок електромеханічний

Таким чином, проєктне рішення забезпечує всі вісім точок доступу засобами КУД.

3.1.3 Програмні засоби для забезпечення роботи СКУД

Програмний модуль «Бастіон-IronLogic» призначений для конфігурації, моніторингу та управління системою контролю доступу (СКУД) «IronLogic», що працює в складі програмного комплексу «Бастіон». «Бастіон-IronLogic» містить вбудовані підсистеми роботи з пропусками (Бюро перепусток), графічних планів території, Фотоідентифікація, пошуку персоналу і облік робочого часу. Також, є програмна підтримка роботи з тимчасовими і разовими перепустками. «Бастіон-IronLogic» допускає розширення системи додатковими модулями АПК «БАСТІОН», що дозволяє будувати на його основі інтегровані решення. Кількістю підтримуваних контролерів в одній мережі 10, 20, 254 шт. в залежності від придбаного пакета ПО.

У ВО «Бастіон-IronLogic» підтримується наступне обладнання:

1 – настільний зчитувач Z-2 USB;

2 – конвертер Z-397 Guard або конвертер Z-397 Web;

3 – мережевий контролер Z-5R Net Extended;

4 – мережевий контролер Z-5R Net або Z-5R Net 8000;

5 – мережевий контролер / зчитувач Matrix-II Net;

6 – кнопка виходу;

7 – зчитувачі;

8 – турнікет або шлагбаум;

9 – замок.

3.1.4 Розрахунок надійності

Надійність – це властивість об'єкта зберігати в часі у встановлених межах значення всіх параметрів, що характеризують здатність виконувати необхідні функції в заданих режимах і умовах застосування, технічного обслуговування, ремонту, зберігання і транспортування. Згідно ДСТУ EN 50133-2-1 [1] до СКУД встановлюються наступні вимоги по надійності: средняя напрацювання на відмову повинна бути не менше 10000 г (без урахування УПУ), середній термін служби – не менше восьми років.

Будемо вважати, що СКУД працездатна, коли працездатні всі її елементи без винятку. Відмови окремих елементів виникають з причин їх природного старіння і не залежать від станів інших елементів системи. Всі структурні елементи в СКУД відновлюються. Випадкові величини часу безвідмовної роботи і часу відновлення всіх елементів СКУД розподілені за експоненціальним законом. Всі кабельні вироби вважаються абсолютно надійними. Визначимо надійність системи контролю та управління доступом, що складається з наступних компонентів (без урахування УПУ): контролер Elsys-MBSM-2A-ТП, комутатор Elsys-MB-Net (таблиця 4). До складу контролера входять наступні вузли:

- стабілізатор напруги 5 В;
- літієва батарея номінальною напругою 3 В;
- однокристальний мікроконтролер (далі – мікропроцесор);

• годинник реального часу; – незалежна пам'ять EEPROM;

• схема сполучення з лінією зв'язку RS-485;

• вхідні кола, що погоджують входи контролера з лініями мікропроцесора;

• вхідні кола, що погоджують інтерфейсні лінії зчитувачів з лініями мікропроцесора;

• вихідні ключі, що забезпечують узгодження ліній мікропроцесора з виходами базового модуля контролера;

• два реле,

• 9-елементний DIP-перемикач, який використовується для установки адреси і швидкості обміну інформацією.

Стабілізатор напруги згідно принциповій електричній схемі є складним приладом і містить елементи, представлені в табл. 3.3. У розрахунок надійності не включаємо процеси з'єднань деталей (пайки).

Таблиця 3.3

Розрахунок показників надійності стабілізатора напруги

Найменування компонента	**Кількість компонентів, N_i**	**Інтенсивність відмов,** ч$^{-1}$		**Ймовірність безвідмовної роботи, P(t)**	**Ймовірність відмов, Q(t)**
		$\lambda_i \cdot 10^6$	$N_i \cdot \lambda_i \cdot 10^6$		
Резистор	5	0,05	0,25	0,997	0,003
Операційний посилювач	1	1	1	0,99	0,01
Транзистор біполярний	1	0,3	0,3	0,997	0,003
Стабілітрон	1	0,2	0,2	0,998	0,002

За даними таблиці 3.3 і за формулою для експоненціального закону знайдемо ймовірність безвідмовної роботи стабілізатора напруги протягом t = 10000 г і середній наробіток до першої відмови:

$$P_c(10000) = e^{-\lambda_c t} = e^{-1{,}7 \cdot 10^{-6} \cdot 10000} = 0{,}98$$

$$t_{ср\cdot с} = \frac{1}{\lambda_с} = \frac{1}{1{,}7 \cdot 10^{-6}} = 585235 \text{ год} = 67 \text{ років}.$$

Розрахунок за окремими компонентами дає:

$$P_c(10000) = e^{-0{,}25\cdot 10^{-6}\cdot 10000} = 0{,}997$$
$$P_c(10000) = e^{-1\cdot 10^{-6}\cdot 10000} = 0{,}99$$
$$P_c(10000) = e^{-0{,}3\cdot 10^{-6}\cdot 10000} = 0{,}997$$
$$P_c(10000) = e^{-0{,}2\cdot 10^{-6}\cdot 10000} = 0{,}998$$

Знайдемо ймовірність безвідмовної роботи системи протягом t = 10000 год і середній наробіток до першої відмови (табл. 3.4). У розрахунку використовувалися довідкові дані про інтенсивність відмов комплектуючих компонентів [19].

Таблиця 3.4

Розрахунок показників надійності контролера

Найменування компонента	**Кількість компонентів, N_i**	**Інтенсивність відмов, ч$^{-1}$**		**Ймовірність безвідмовної роботи, P(t)**	**Ймовірність відмов, Q(t)**
		$\lambda_i \cdot 10^6$	$N_i \cdot \lambda_i \cdot 10^6$		
Стабілізатор напругою 5 В	1	1,7	1,7	0,983	0,017
Літієва батарея номінальною напругою 3 В	1	0,22	0,22	0,998	0,02
Мікропроцесор	1	0,23	0,23	0,998	0,02
Години реального часу	1	0,02	0,02	0,9998	0,0002
Енергонезалежна пам'ять EEPROM	1	0,017	0,017	0,9998	0,0002
Реле	2	0,3	0,6	0,994	0,94
DIP-перемикач	1	0,14	0,14	0,999	0,001

За даними таблиці 3.4 і за формулою для експоненціального закону знайдемо ймовірність безвідмовної роботи контролера протягом t = 10000 г і середній наробіток до першої відмови:

$$P_c(10000) = e^{-\lambda_c t} = e^{-2{,}9\cdot 10^{-6}\cdot 10000} = 0{,}97$$

$$\mathrm{t_{ср\cdot с}} = \frac{1}{\lambda_c} = \frac{1}{2{,}9\cdot 10^{-6}} = 344827 \text{ год} = 39 \text{ років}$$

Рохрахунок по окремим компонентам дає:

$$P_c(10000) = e^{-1{,}7\cdot 10^{-6}\cdot 10000} = 0{,}983$$

$$P_c(10000) = e^{-0{,}22\cdot 10^{-6}\cdot 10000} = 0{,}998$$

$$P_c(10000) = e^{-0{,}23\cdot 10^{-6}\cdot 10000} = 0{,}998$$

$$P_c(10000) = e^{-0{,}02\cdot 10^{-6}\cdot 10000} = 0{,}9998$$

$$P_c(10000) = e^{-0{,}017\cdot 10^{-6}\cdot 10000} = 0{,}9998$$

Визначимо ймовірність безвідмовної роботи СКУД в цілому без урахування УПУ протягом t = 10000 год і середній наробіток до першої відмови.

Таблиця 3.5

Розрахунок показників надійності СКУД

Найменування компонента	**Кількість компонентів, N_i**	**Інтенсивність відмов,** год$^{-1}$	
		$\lambda_i \cdot 10^6$	$N_i \cdot \lambda_i \cdot 10^6$
Комутатор	1	0,15	0,15
Контролер	7	2,9	20,3

$\sum_{i=1}^{2} N_i = 8;\ \lambda_c = \sum_{i=1}^{2} N_i \lambda_i = 3{,}05 \cdot 10^{-6}$ год $^{-1}$

За даними табл. 3.5 і за формулою для експоненціального закону знайдемо ймовірність безвідмовної роботи СКУД протягом t = 10000 г і середній наробіток до першої відмови:

$$P_c(10000) = e^{-\lambda_c t} = e^{-3{,}05 \cdot 10^{-6} \cdot 10000} = 0{,}98$$

$$t_{ср \cdot с} = \frac{1}{\lambda_с} = \frac{1}{3{,}05 \cdot 10^{-6}} = 327869 \text{ год} = 37 \text{ років}$$

Для більш повної оцінки надійності розрахуємо коефіцієнт готовності СКУД – ймовірність того, що об'єкт виявиться в працездатному стані в довільний момент часу, крім запланованих періодів, протягом яких застосування об'єкта за призначенням не передбачається, за формулою [19]:

$$К_г = \frac{Т}{Т+Т_в},$$

де Т – наробіток на відмовлення, год;

$Т_в$ – середній час відновлення, год.

У табл. 3.6 представлені розрахунки коефіцієнта готовності за компонентами СКУД.

Для розрахунку коефіцієнта готовності СКУД в цілому потрібно знати значущості показника надійності елемента для загального показника надійності СКУД, тому на даному етапі дослідження не представляється можливим розрахувати коефіцієнт готовності СКУД, який становить 0,93.

Таблиця 3.6

Розрахунок коефіцієнта готовності

Найменування обладнання	Час напрацювання на відмовлення, год	Час відновлення, год	Кофіцієнт готовності. $К_г$
Комутатор Elsys-MB-Net	20000	6	0,9997
Контролер Elsys-MB-SM-2A-ТП	20000	6	0,9997
Зчитувач Elsys-SW10-EN	60000	6	0,9999
Електромагнітний замок «ML-200M»	100000	6	0,9999
Турнікет Elsys-ST-TS100	30000	6	0,9998
Сповіщувач магнітоконтактний «IO 102-16/2»	500000	6	0,9999
Процесор АРМ	15000	6	0,9996
Монітор АРМ	50000	6	0,9999

3.2. Фінансовий менеджмент, ресурсоефективність та ресурсозатратність

3.2.1. Розрахунок вартості обладнання СКУД

Розрахунок вартості обладнання системи контролю і управління доступом проводиться на підставі цін постачальника за одиницю обладнання. Кошторис на прилади та обладнання представлена в табл. 3.7.

Таблиця 3.7

Кошторис на прилади та обладнання

Найменування	Всього, грн
Контролер Elsys-MB-SM-2A-ТП	11800,00
Зчитувач Elsys-SW10-EN	10300,00
Сповіщувач магнітоконтактний «IO 102-16/2»	224,00
Кнопка відкривання дверей без фіксації	361,00
Електромагнітний замок «ML-200M»	5864,00
Комутатор Elsys-MB-Net	9632,00
Сервер IBM	9822,00

Продовження таблиці 3.7

Відеомагнітофон «VideoNi=ova A40-IP-16»	7260,00
Турнікет Elsys-ST-TS100	7270,00
Замок електромеханічний	769,00
Монітор	3280,00
Всього:	67582,00

Наведено основні витрати на обладнання і матеріали, вартість кабельних виробів і елементів кріплення не враховувалася. Отже, загальна вартість приладів та обладнання склала 67582,00 грн.

3.2.2 Розрахунок вартості пусконалаштувальних робіт

Вартість монтажу була визначена за середніми показниками цін різних підприємств, що займаються монтажем систем контролю та управління доступом в м. Київ.

Таблиця 3.8

Кошторис на пусконалагоджувальні роботи

Вид роботи	Вартість, грн
Встановлення контролерів	2000,00
Встановлення зчитувачів	448,00
Всатановлення магнітоконтактних зчитувачів	338,88
Встановлення електромагнітних замків	630,00
Встановлення кнопок відкривання	250,00
Прокладання кабел, на 100 м	2200,00
Встановлення турнікету	300,00
Встановлення блоку безперебійного живлення	80,00
Всього:	15000,00

Підсумкова вартість пусконалагоджувальних робіт становить 15000 грн.

3.2.3 Розрахунок технічного обслуговування СКУД в період експлуатації

Системи контролю і управління доступом містять обладнання, яке потребує поточного і періодичного технічного обслуговування. Наприклад, датчики-сповіщувачі можуть ефективно працювати при дотриманні правил

експлуатації, але на них негативно впливає цілий ряд факторів – пил, водяні пари, гази і ін. Не варто виключати і потенційну можливість навмисної псування устаткування зловмисниками.

Щоб усунути негативний вплив на компоненти системи контролю та управління доступом, проводять технічне обслуговування: перевірка зовнішнього стану і функціонування компонентів, при необхідності – коригування налаштувань, перевірка працездатності.

Відповідно до рекомендацій з технічного обслуговування, розробленими виробниками систем контролю і управління доступом, щодня виконуються: – огляд цілісності технічних засобів захисту; – перевірка стану шлейфів, датчиків-сповіщувачів та іншого обладнання (відсутність пошкоджень, бруду, слідів корозії і т.п.);

- визначення працездатності компонентів системи, цілісність пломб опломбованих приладів. Щомісяця рекомендується перевіряти:
- надійність підключень до джерела живлення, працездатність резервного джерела живлення;
- тестування на працездатність компонентів системи контролю та управління доступом;
- заміна непрацездатних, зношених, дефектних компонентів. Щорічно виконується повна перевірка стану всіх компонентів системи контролю та управління доступом і перевірка заземлення системи в цілому, а також кожного компонента окремо. Один раз в три роки перевіряють ізоляцію струмоведучих елементів на цілісність. Розрахунок витрат на технічне обслуговування наводиться в табл. 3.9.

Таблиця 3.9

Розрахунок вартості обслуговування системи контролю та управління доступом

Найменування	Вартість в рік, грн
Сповіщувач магнітоконтактний «ІО 102-16/2»	5000,00
Кнопка відкривання дверей без фіксації	3500,00
Електромагнітний замок «ML-200M»	60,00
Комутатор Elsys-MB-Net	90,00
Сервер IBM	2550,00
Відеомагнітофон «VideoNi=ova A40-IP-16»	5000,00
Турнікет Elsys-ST-TS100	3800,00
Замок електромеханічний	-
Монітор	-
Контролер Elsys-MB-SM-2A-ТП	769,00
Зчитувач Elsys-SW10-EN	2000,00
Всього:	22000,00

В обов'язки виконавців, крім робіт з технічного обслуговування системи контролю та управління доступом, входить ще й ведення необхідної документації (журналів перевірок). Графік проведення технічного обслуговування обладнання СКУД на 2021 р наводиться в табл. 3.10.

Таблиця 3.10

Графік проведення технічного обслуговування на 2021 р

Найменування	Вид обслугогування	1 квартал			2 квартал			3 квартал			4 квартал		
		01	02	03	04	05	06	07	08	09	10	11	12
Сповіщувач магнітоконтактний «ІО 102-16/2»	Огляд	×	×	×	×	×	×	×	×	×	×	×	×
	Перевірка			×			×			×			×
	Профілактика							×					
Електромагнітний замок «ML-200M»	Огляд	×	×	×	×	×	×	×	×	×	×	×	×
	Перевірка			×			×			×			×
	Профілактика							×					
Комутатор Elsys-MB-Net	Огляд	×	×	×	×	×	×	×	×	×	×	×	×
	Перевірка			×			×			×			×
	Профілактика							×					
Сервер IBM	Огляд	×	×	×	×	×	×	×	×	×	×	×	×

Продовження таблиці 3.10

	Перевірка			×			×			×			×
	Профілактика							×					
Відеомагнітофон «VideoNi=ova A40-IP-16»	Огляд	×	×	×	×	×	×	×	×	×	×	×	×
	Перевірка			×			×			×			×
	Профілактика							×					
Турнікет Elsys-ST-TS100	Огляд	×	×	×	×	×	×	×	×	×	×	×	×
	Перевірка			×			×			×			×
	Профілактика							×					
Зчитувач Elsys-SW10-EN	Огляд	×	×	×	×	×	×	×	×	×	×	×	×
	Перевірка			×			×			×			×
	Профілактика							×					
Контролер Elsys-MB-SM-2A-ТП	Огляд	×	×	×	×	×	×	×	×	×	×	×	×
	Перевірка			×			×			×			×
	Профілактика							×					

У таблицю включені наступні види технічного обслуговування: зовнішній огляд устаткування, перевірка його працездатності; Профілактичні роботи. Нормативи за вартістю обслуговування в даній роботі представлені ТОВ «Феорана», основним видом діяльності якого є монтаж, технічне обслуговування і ремонт засобів забезпечення безпеки на промислових об'єктах. Розрахунок витрат за статтею «Податки, відрахування в бюджет і позабюджетні фонди» включає відрахування за встановленими законодавством нормами до пенсійного фонду, до фонду соціального захисту населення, на обов'язкове медичне страхування, на інші соціальні потреби. Витрати за цією статтею виконуються за формулою:

$$С_н = \frac{(С_{озп} + С_{дзп}) \cdot (С_{с.н.} + С_{стр})}{100}$$

де $С_{озп}$ – основна зарплата працівників офісу, грн.;

$С_{дзп}$ – додаткова зарплата працівників офісу, грн.;

$С_{с.н.}$ – ставка соціального податку (прийняти 30,2%);

$С_{стр}$. – ставка страхових внесків по іншим видам обов'язкового страхування (прийняти 0,7%);

$C_н$ = (15000 + 500) · 30,2+0,7 / 100 = 4789,5 грн.

3.3 Соціальна відповідальність

3.3.1. Опис робочого місця співробітника віддаленого офісу «Plexon Inc.» в м. Київ

Робоче місце кожного штатного співробітника розташоване в кабінеті віддаленого офісу підприємства «Plexon Inc.» в м. Київ.

Розміри найменшого кабінету: довжина 4,0 м; ширина 4,0 м; висота 2,7 м.

В кабінеті такої площі працює одна людина. Співробітником використовується обладнання автоматизованого робочого місця (комп'ютер, багатофункціональний пристрій, телефон) і матеріали (канцелярські товари), меблі (стіл та крісло комп'ютерне).

Робоче місце співробітника охорони відповідає ергономічним вимогам, наведеним в ДСТУ 2293 2014. Розпорядок робочого часу співробітника: восьмигодинний робочий день, практично 100% робочого часу співробітник знаходиться у приміщенні.

У приміщенні комбіноване освітлення – природне за рахунок віконних прорізів і штучне (люмінесцентні лампи Philips 18 Вт G13 4000 K). Опалення водяне. Вентиляція здійснюється природним шляхом через віконні отвори. У приміщенні змонтований кондиціонер Electrolux EACS-07 HFE / N3.

Факт наявності професійного ризику пошкодження здоров'я співробітників при здійсненні ними трудових функцій і наведено перелік окремих шкідливих і (або) небезпечних виробничих факторів: протиправні дії інших осіб; пожежа або вибух; фізичні і нервовопсихічні перевантаження; підвищена або знижена температура повітря робочої зони; підвищений рівень шуму та вібрації; підвищена запиленість повітря; недостатня освітленість робочої зони; підвищена або знижена вологість і підвищена рухливість повітря робочої зони; розташування робочого місця на висоті від поверхні землі (підлоги); небезпечних електричних контактів через тіло працівника.

3.3.2 Пожежна безпека

Загоряння на даному об'єкті може виникнути внаслідок порушення правил техніки безпеки, цілісності електричної проводки, поломки електроприладів. З метою зменшення ризику виникнення пожежі на об'єкті розроблений ряд заходів.

До організаційних заходів належать: проведення інструктажів, навчання пожежно-технічного мінімуму, видання наказів з питань посилення пожежної безпеки.

До експлуатаційних заходів належать правильна експлуатація електроустаткування, профілактичні ремонти, огляди і випробування обладнання і пристроїв, в тому числі систем безпеки. До технічних заходів належать: дотримання протипожежних норм і правил при влаштуванні та встановлення систем безпеки, кондиціонування, підведення електропроводки, захисного заземлення.

До режимних заходів відноситься заборона куріння в невстановлених місцях. Для зменшення ризику виникнення пожежі через порушення цілісності електропроводки в приміщеннях офісу стан електропроводки перевіряється один раз на півроку відповідно до відомчого наказу відповідно до встановленого графіка.

Електропроводка виконана кабелем з оболонкою з матеріалу, що не поширює горіння. З метою забезпечення пожежної безпеки на посту охорони є інструкція про порядок дій на випадок виникнення пожежі в денний і нічний час, телефон, електричний ліхтар, засіб індивідуального захисту органів дихання та зору людини від токсичних продуктів горіння (газодимозахисної протигаз «Шанс» з часом захисту від продуктів горіння не менше 60 хв).

У приміщенні офісу є один евакуаційний вихід. Шляхи евакуації не захаращені. Висота евакуаційного виходу становить 2,3 м; ширина 0,96 м.

Приміщення обладнане системою автоматичної пожежної сигналізації на базі приймально-контрольного приладу «Сигнал-20П» з використанням димових пожежних сповіщувачів. Для оповіщення персоналу про пожежу у

всіх приміщеннях (з постійним або тимчасовим перебуванням людей) встановлено світлозвукові оповіщувачі «Сопілка-2». Розрахунковий час прибуття підрозділу пожежної охорони при середній швидкості руху 40 км / год складає менше 5 хв, що відповідає вимогам Закону України.

Аналізований об'єкт оснащений первинними засобами пожежогасіння. З огляду на пожежне навантаження, в приміщенні можливі класи пожежі А (горіння твердих речовин, що супроводжується тлінням) і Е (горіння електрообладнання, що знаходиться під напругою).

Керуючись вимогами Правил протипожежного режиму в України, в приміщенні встановлено три порошкових вогнегасника марки ОП-3. Вогнегасники промарковані, на них заведені паспорти, заведений журнал обліку наявності, перевірки і стану первинних засобів пожежогасіння.

3.3.3 Охорона навколишнього середовища

На робочому місці кожного співробітника утворюється невелика кількість твердих побутових відходів різних видів – харчові, пластик, папір, текстиль та ін.

Відходи належать до III-IV класів небезпеки згідно з документом «Державні санітарні правила та норми. 2. Комунальна гігієна. 2.7. Грунт, очистка населених місць, побутові та промислові відходи, санітарна охорона грунту. «Гігієнічні вимоги щодо поводження з промисловими відходами та визначення їх класу небезпеки для здоров'я населення» ДСанПіН 2.2.7.029-99 від 01.07.1999. Відходи накопичуються в контейнері і вивозяться на спецмашинах для поховання на полігоні твердих побутових відходів згідно з договором. Офіс приєднаний до централізованої системи каналізації, куди зливаються утворюються рідкі побутові відходи.

3.3.4 Захист в надзвичайних ситуаціях

До потенційних надзвичайних ситуацій (НС) природного характеру, можливим в м. Київ, відносяться: землетруси, урагани, повені. МНС України в м. Київ своєчасно інформує об'єкти про НС.

На уже згадуваному об'єкті розроблений план заходів щодо забезпечення безпеки співробітників в умовах НС. Крім того, на даному об'єкті можуть виникнути НС техногенного характеру (раптове обвалення будівлі, аварії на комунальних системах постачання).

Оскільки аналізований об'єкт знаходиться на другому поверсі окремо розташованої будівлі на орендованих площах, заходи щодо запобігання обвалення будівлі реалізує орендодавець: створено спеціальну комісію, яка з періодичністю раз на півроку проводить огляд будівлі та виносить приписи щодо необхідних заходів, а також стежить за їх виконанням.

3.4 Аналіз результатів роботи спроєктованої СКУД

Після встановлення спроєктованої нами системи контролю та управління доступом у віддаленому офісі підприємства «Plexon Inc.» було проведено аналіз результатів її роботи. Дані для порівняння наведено у табл. 3.11.

Таблиця 3.11

Результати встановлення спроєктованої СКУД

Показник	До	Після
Прохід на територію сторонніх осіб	1-2 люд./тиж.	0 люд./тиж.
Запізнення співробітників	10-12 р./тиждень	1 р./тиждень
Викрадення паролів до систем	1-2 р./півроку	0 р./півроку
Перехоплення даних	2 р./рік	1 р./рік

З табл. 3.11 бачимо, що після встановлення спроєктованої системи контролю та управління доступом у віддаленому офісі підприємства «Plexon.Inc.» показники рівня забезпечення безпеки інформації, майна та співробітників підприємства зросли приблизно на 50%. Отже, можна зробити висновок, що проєктування системи було вдалим і нами було досягнено мети.

Висновки до розділу 3

У розділі 3 розроблено технічне завдання на проєктування СКУД. Був проведений порівняльний аналіз пропозицій найбільш затребуваних споживачами, за критеріями вартості та функцій компонентів СКУД, а також

комплексна оцінка по клієнтоорієнтованості, на основі яких вибрано рішення обрати СКУД Elsys з ВО «Бастіон» компанії ТОВ «ЄС-проміті».

Підібрано обладнання для восьми точок доступу, а також джерела безперебійного живлення, які забезпечують нормальну роботу системи контролю та управління доступом при відключенні централізованого електропостачання. Розраховані показники надійності СКУД з висновком про достатній рівень надійності для підприємства такого формату.

Також проведено розрахунки вартості розробки системи контролю та управління доступом віддаленого офісу підприємства «Plexon Inc.». в м. Київ (104582,00 грн.).

Розрахунки вартості обладнання розробленої системи контролю та управління доступом – 67582 грн.

Розрахунок витрат на пусконалагоджувальні роботи – 15000 грн.,

Розрахунок технічного обслуговування системи контролю та управління доступом – 22000 грн.

Результати проведеного аналізу шкідливих і небезпечних виробничих факторів свідчать, що вони відповідають нормативам.

Для забезпечення безпечної життєдіяльності на об'єкті прийняті наступні заходи:

а) на об'єкті встановлена автоматична пожежна сигналізація, об'єкт забезпечений первинними засобами пожежогасіння згідно з нормами;

б) діяльність співробітників характеризується наявністю загрози життю і здоров'ю в результаті можливих протиправних дій інших осіб;

в) аналізований об'єкт не має значного шкідливого впливу на навколишнє середовище.

Після встановлення спроєктованої системи контролю та управління доступом у віддаленому офісі підприємства «Plexon.Inc.» показники рівня забезпечення безпеки інформації, майна та співробітників підприємства зросли приблизно на 50%. Отже, можна зробити висновок, що проєктування системи було вдалим і нами було досягнено мети.

ВИСНОВКИ

Дипломна робота містить в своїй основі аналіз нормативно-технічної документації, наукової літератури з проблеми дослідження. Під час виконання дипломної роботи в результаті аналізу нормативних документів, технічної та спеціальної літератури було вирішено поставлені завдання. Було розглянуто сучасні тенденції у використанні систем контролю і управління доступом до малих підприємств офісного формату.

До них відносяться:

- використання багатофункціональних СКУД (контроль доступу, облік робочого часу персоналу і ін.);
- біометрична ідентифікація;
- доступ з допомогою смартфону;
- в зв'язку з неблагополучною ситуацією з коронавірусною інфекцією інтеграція СКУД з пірометрами або тепловізорами для автоматизації процесу виявлення осіб з підвищеною температурою з подальшим недопуском їх на робоче місце і направленням на консультацію до лікаря.

Дано характеристику досліджуваного об'єкта – віддаленого офісу підприємства «Plexon Inc.». в м. Київ, розглянуто застосовувану в даний час систему забезпечення безпеки його функціонування.

Відзначено, що застосовувана в даний час система контролю і управління доступом потребує модернізації, яка була здійснена проєктним рішенням: розроблено технічне завдання, на основі якого підібрано обладнання для восьми точок доступу.

Попереднє обстеження об'єкту захисту, аналіз застосовуваної системи безпеки дозволили розробити технічне завдання на проєктування СКУД. Було проведено порівняльний аналіз пропозицій трьох українських та зарубіжних виробників, відзначених як найбільш затребуваних серед споживачів, за критеріями вартості та функцій компонентів СКУД, а також комплексна оцінка

по клієнтоорієнтованості, на основі яких було прийнято рішення обрати СКУД Elsys з ВО «Бастіон» компанії ТОВ «ЄС -проміті».

Нами було підібрано обладнання для восьми точок доступу, а також джерела безперебійного живлення, які забезпечують нормальну роботу системи контролю та управління доступом при відключенні централізованого електропостачання. Розраховано показники надійності СКУД та зроблено висновки про достатній рівень надійності.

Технічні рішення, прийняті при розробці СКУД відповідають вимогам санітарно-гігієнічних, протипожежних та інших нормативів, що діють на території України, і забезпечують безпечне для життя і здоров'я працівників об'єкта при дотриманні пропонованих заходів.

В роботі зроблено розрахунок економічних витрат на впровадження СКУД для віддаленого офісу підприємства «Plexon Inc.» в м. Київ, що включає вартість проєктування, обладнання та матеріалів, встановлення, пуско-налагоджувальних робіт. Загальні витрати склали 104582 грн. Для забезпечення надійної експлуатації СКУД розроблено графік її перевірки і технічного обслуговування на 2021 р.

У дипломній роботі проведено оцінку впливу шкідливих і небезпечних виробничих факторів на робочому місці співробітника, а також шкоди, що завдається функціонуванням віддаленого офісу підприємства «Plexon Inc.». в м.Київ навколишньому середовищу.

Після встановлення спроєктованої системи контролю та управління доступом у віддаленому офісі підприємства «Plexon.Inc.» показники рівня забезпечення безпеки інформації, майна та співробітників підприємства зросли приблизно на 50%. Отже, можна зробити висновок, що проєктування системи було вдалим і нами було досягнено мети.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ДСТУ EN 50133-2-1 Системи тривожної сигналізації. Охоронні теле(відео) системи і системи контролювання доступу 2001. – 63 с.

2. Проєктирование СКУД: эксперты советуют [Электронный ресурс] / Системы безопасности. – Режим доступа: lib.secuteck.ru/articles2/sys_ogr_dost/proektirovanie-skyd-eksperti-sovetyut.

3. Мобильная идентификация в СКУД – смартфон вместо пропуска [Электронный ресурс] / Системы контроля. Управление доступом. – Режим доступа: https://www.drdoors-msc.ru/.

4. Евдокимов Н.О. Система контроля и управления доступом по аудиоданным пользователя [Электронный ресурс] // Гаудеамус. – 2014. – №2 (24). – Режим доступа: https://cyberleninka.ru/article/n/sistema-kontrolya-iupravleniya-dostupom-po-audiodannym-polzovatelya.

5. Офіційний інтернет-сайт компанії «PERCo». – Режим доступу: https://www.perco.ru.

6. Международный форум «Технологии безопасности» [Электронный ресурс]. – Режим доступа: https://www.tbforum.ru/.

7. Обзор решений СКУД [Электронный ресурс] / СКУД: обзоры и срезы рынка безопасности. – Режим доступа: http://www.techportal.ru/review/#obzoryresheniy-skud.

8. Особенности СКУД: выбор экспертов [Электронный ресурс] / Системы безопасности. – Режим доступа: https://www.secuteck.ru/blog/tag/.

9. Бронников А.А. Сейсмическая система охраны объекта // Вестник КемГУ. Технические науки. – 2019. – №2-2. – с. 43– 56.

10. Борисов С.П. Единый специализированный объектовый протокол – повышение информативности для централизованной охраны // Алгоритм безопасности. – 2017. – № 4. – С. 23–39.

11. Байтимиров А.Д. Беспроводные технологии в промышленности [Электронный ресурс] // Вестник Казанского технологического университета. – 2014. – №14. – Режим доступа: https://cyberleninka.ru/article/n/besprovodnyetehnologii-v-promyshlennosti.

12. Терентьев А.М. Ложные срабатывания систем охраны [Электронный ресурс] // Национальные интересы: приоритеты и безопасность. – 2013. – №4. – Режим доступа: https://cyberleninka.ru/article/n/lozhnye-srabatyvaniyaantivirusnyh-sredstv .

13. ДСТУ 8773:2018 Склад та зміст розділу інженерно-технічних заходів цивільного захисту в складі проєктної документації на будівництво об`єктів. Основні положенняб 2018. – 48 с. 98

14. ДСТУ 9047:2020 Системи протипожежного захисту. Настанова з підтримання експлуатаційної придатності 2020. – 52 с.

15. Правила устройства электроустановок. – 7-е изд. – М.: Изд-во НЦ ЭНАС, 2005. – 706 с.

16. ДБН В.1.1-7:2016 Пожежна безпека об`єктів будівництва. Загальні вимоги

17. Волковицкий В.Д., Волхонский В.В. Системы контроля и управления доступом. – СПб.: Университет ИТМО, 2015. – 53 с.

18. Офіційний інтернет-сайт компанії «Hikvision». Режим доступу: https://hikvision.ru

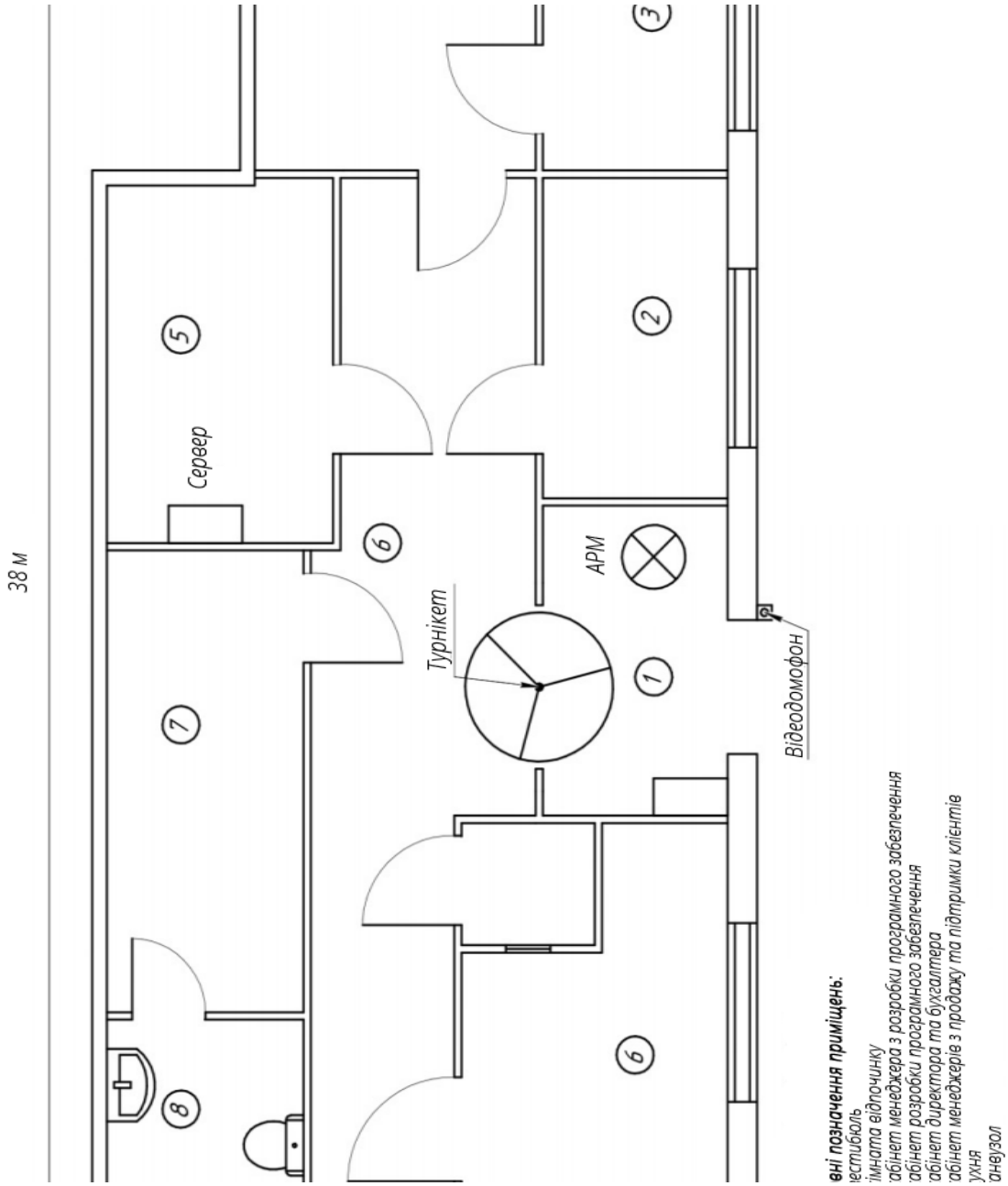
19. Луговцова Н.Ю. Расчеты надежности технических систем и техногенного риска: учебное пособие / Н.Ю. Луговцова; Юргинский технологический институт. – Томск: Изд-во Томского политехнического университета, 2019. – 342 с.

20. Малафеев С.И., Копейкин А.И. Надежность технических систем. Примеры и задачи: Учебное пособие. – СПб.: Издательство «Лань», 2012. – 320 с.

21. ДСТУ 2293:2014 Охорона праці. Терміни та визначення основних понять 2005 51 с.

Додаток А

Схема приміщення віддаленого офісу підприємства «Plexon.Inc»



Додаток Б

Структурна схема системи контролю та управління доступом