МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Сумський державний університет
Факультет електроніки та інформаційних технологій
Кафедра електроніки, загальної та прикладної фізики

«До захисту допущено»
Завідувачка кафедри

_____ Лариса ОДНОДВОРЕЦЬ
____ _____ 2024 р.

КВАЛІФІКАЦІЙНА РОБОТА
на здобуття освітнього ступеня «бакалавр»

за спеціальністю 171 «Електроніка» освітньо-професійної програми «Електронні інформаційні системи»
на тему: «**КОНТРОЛЕРИ ДОСТУПУ В ПРИМІЩЕННЯ: КОНСТРУКЦІЯ ТА ПРИНЦИП ФУНКЦІОНУВАННЯ»**

Здобувача групи ЕП-01 Мар’єнкова Олександра Сергійовича

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

Олександр МАР’ЄНКОВ

Керівник доцент кафедри електроніки,
загальної та прикладної фізики,
канд. фіз.-мат. наук, доцент Юрій ШАБЕЛЬНИК

Суми – 2024

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ФАКУЛЬТЕТ ЕЛЕКТРОНІКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
Кафедра електроніки, загальної та прикладної фізики
Спеціальність 171 – Електроніка, освітньо-професійна програма
«Електронні інформаційні системи»

ЗАТВЕРДЖУЮ
Зав. кафедри ЕЗПФ
Лариса Однодворець
«01» травня 2024 року

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА

Мар'єнкова Олександра Сергійовича

Тема роботи: **«КОНТРОЛЕРИ ДОСТУПУ В ПРИМІЩЕННЯ: КОНСТРУКЦІЯ ТА ПРИНЦИП ФУНКЦІОНУВАННЯ»**

затверджена наказом СумДУ від «24» квітня 2024 р., № 0417-VI

2. Термін здачі здобувачем закінченої роботи 24 травня 2024 року

3. Вихідні дані до роботи (актуальність, мета):

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. СКУД є одним з найбільш розвинених сегментів ринку безпеки. В якості найбільш часто використовуваних засобів контролю і управління доступом на підприємстві є турнікети, двері, замки, ідентифікатори різної природи та ін. Зазвичай СКУД інтегрують з іншими системами безпеки, такими як ідентифікація по смартфону, біометрична ідентифікація.

Метою кваліфікаційної роботи бакалавра є вивчення конструкційних особливостей різних типів сучасних зразків контролерів для датчиків фіксації доступу в приміщення, їх параметрів, переваг та недоліків та ознайомлення з розрахунком надійності засобів для забезпечення роботи СКУД.

4. Зміст текстової частини роботи (перелік питань, які необхідно розробити):

1. Аналіз систем контролю та управління доступом (Літературний огляд)
2. Проєктування СКУД для віддаленого офісу.
3. Розрахунок надійності засобів для забезпечення роботи СКУД

4. Висновки.
5. Список використаних джерел.

4. Перелік графічного матеріалу для презентації:
Слайди № 1-2. Актуальність і мета роботи.
Слайди № 3-9. Аналіз систем контролю та управління доступом (Літературний огляд).
Слайди № 10. Проєктування СКУД для віддаленого офісу.
Слайди № 11-13. Розрахунок надійності засобів для забезпечення роботи СКУД.
Слайд №14. Висновки.
Слайд №15. Подяка.

6. Дата видачі завдання 01.05.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів виконання кваліфікаційної роботи	Термін виконання етапів роботи	Примітка про стан вик. роботи
1.	Аналіз літературних даних	до 07.05.2024 р.	*вик.*
2.	Проведення вимірювань, моделювання, розрахунків, обробка результатів	до 22.05.2023 р.	*вик.*
3.	Оформлення тексту кваліфікаційної роботи	до 26.05.2023 р.	*вик.*
4.	Попередній захист роботи	31.05.2024 р., 10-00, онлайн	*вик.*
5.	Захист кваліфікаційної роботи	06.06.2024 р., 10-00, онлайн	

Здобувач вищої освіти Олександр МАР’ЄНКОВ

Керівник Юрій ШАБЕЛЬНИК

АНОТАЦІЯ

Кваліфікаційна робота викладена на 36 сторінках, зокрема, містить 12 рисунків, 3 таблиці список використаних джерел складається з 20 найменувань.

Захист будь-якого об'єкту включає кілька етапів, число яких залежить від рівня режимності об'єкта. При цьому у всіх випадках важливим 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 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 є турнікети, двері, замки, ідентифікатори різної природи та ін.

Актуальними трендами в сучасних умовах є інтеграція СКУД з іншими системами безпеки, такими як ідентифікація по смартфону, біометрична ідентифікація.

Метою кваліфікаційної роботи бакалавра є вивчення конструкційних особливостей різних типів сучасних зразків контролерів для датчиків фіксації доступу в приміщення, їх параметрів, переваг та недоліків та ознайомлення з розрахунком надійності засобів для забезпечення роботи СКУД.

Ключові слова: БІОМЕТРІЯ, ІДЕНТИФІКАЦІЯ, СИСТЕМА КОНТРОЛЮ ДОСТУПУ, СКУД.

ЗМІСТ

РОЗДІЛ 1. АНАЛІЗ СИСТЕМ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ. (ЛІТЕРАТУРНИЙ ОГЛЯД)

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].

Робота СКУД базується на порівнянні ідентифікаційних ознак, які належать або властиві конкретній особі або об'єкту, з інформацією, що зберігається в системі.

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).

Система контролю доступу працює на осі присвоєних ідентифікаційних ознак, які можуть бути пов'язані з певним предметом чи транспортним засобом. Пароль, кодове число і предмет-ідентифікатор відносяться до цього класу ознак. Важливо зазначити, що система ідентифікує не саму людину, а присвоєну їй ознаку.

Для ідентифікації особи використовуватися її унікальні фізичні характеристики, такі як відбитки пальців, геометрія кисті руки, голосові характеристики та інші біометричні дані. Ці ознаки є притаманними конкретній особі і можуть бути використані для її ідентифікації. (рис. 1.2).

а б в г

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

Рисунок 1.2 – Способи біометричної ідентифікації. Із роботи [2]

Система контролю та управління доступом (СКУД) працює за такою схемою: біля входу в контрольоване приміщення встановлюються спеціальні пристрої-зчитувачі, які зчитують інформацію з ідентифікатора, пароля або кодового числа, або отримують біометричні дані людини. Ця інформація потім передається на контролери доступу, які аналізують дані про власника та приймають рішення щодо управління перешкоджаючими та дозволяючими пристроями. Наприклад, вони можуть відкривати або блокувати двері, активувати сигнал тривоги, реєструвати

присутність людини на робочому місці та інші дії. Загальна логічна схема побудови СКУД може бути представлена на рисунку 1.3.

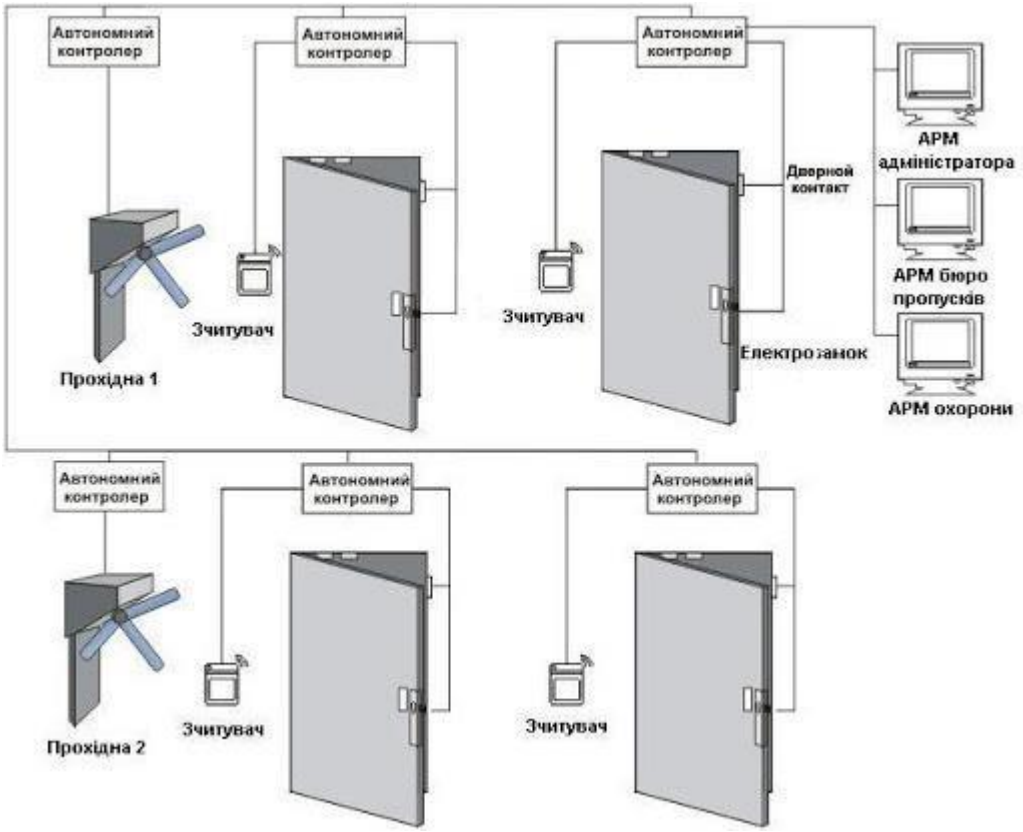

Рисунок 1.3 – Загальна схема роботи СКУД. Адаптовано із роботи [3]

СКУД є важливим компонентом комплексних рішень для забезпечення високого рівня безпеки об'єкта. Принцип роботи СКУД дозволяє точно контролювати всі переміщення в зоні його дії. Давайте розглянемо більш детально можливості, які надає 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 здійснюється оператором або адміністратором системи, в той час як інші процедури можуть автоматизуватися. Аутентифікація може бути повністю здійснена лише за допомогою біометричних систем. [7].

Отже, системи контролю та управління доступом не тільки запобігають незаконному проникненню на охоронювану територію, але й забезпечують цілісність та захист матеріальних цінностей, важливої інформації, а також гарантують безпеку для персоналу та відвідувачів. Важливими функціями СКУД є виявлення порушень трудової дисципліни, таких як відстеження переміщення співробітників в офісі, облік і фіксація робочого часу (запис про прогули, запізнення або раннє покидання роботи та інше).

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.

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.

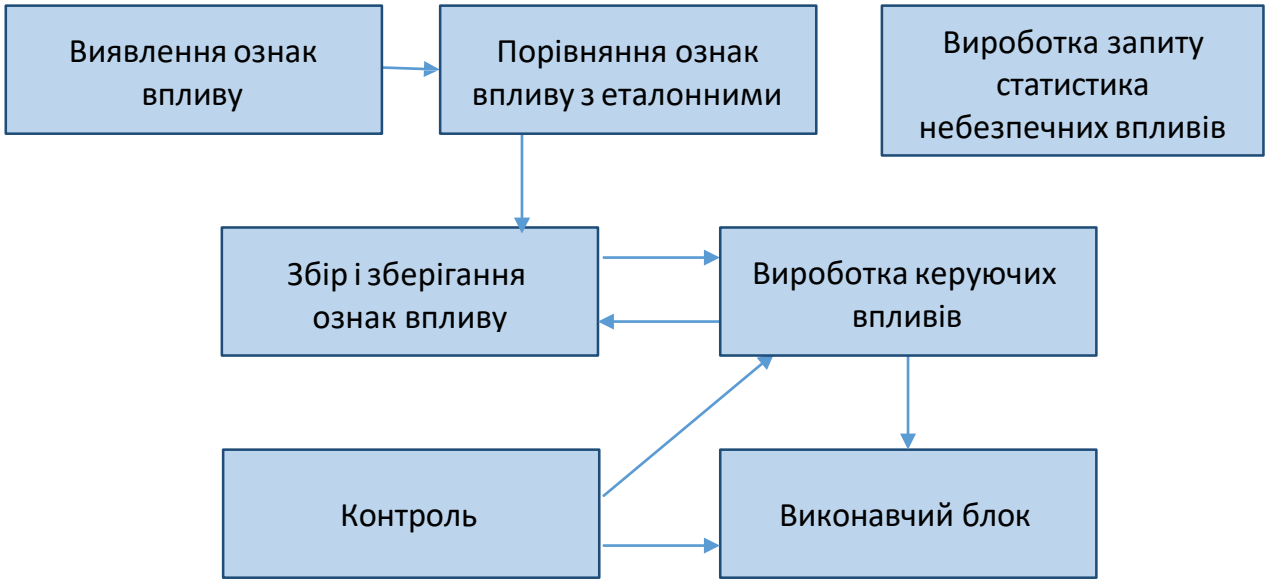

Рисунок 1.4 – Функціональна схема системи контролю та управління доступом. Адаптовано із роботи [4]

У мережі СКУД зв'язок відбувається за допомогою Ethernet-інтерфейсу.ля ідентифікації використовуються безконтактні карти і брелоки типу Proximity. В системі СКУД PERCo-S20 можуть використовуватися різні виконавчі пристрої, такі як турнікети, хвіртки, електромагнітні та електромеханічні замки. Контролери доступу також можуть мати вбудовану підтримку шлейфів охоронної сигналізації, що дозволяє контролювати всю площу приміщення.

На сьогоднішній день існує велика кількість різних типів систем контролю та управління доступом, які можуть відрізнятися за ступенем надійності, складністю налаштування та обслуговування, а також вартістю. Однак, вони зазвичай

виконують такі основні функції: виявлення, ідентифікація, управління та контроль. Ці функції можна побачити на схемі, зображеній на рисунку 1.4.

Архітектура системи контролю та управління доступом (СКУД) є гнучкою та модульною, що дозволяє вибрати оптимальний набір обладнання, який відповідає потребам підприємства, а також може бути модернізований в майбутньому.

1.3. Основні компоненти СКУД

Основними компонентами систем контролю і управління доступом є різноманітні пристрої і засоби, які забезпечують контроль і управління доступом до приміщень або об'єктів компоненти можуть бути механічними, електромеханічними, електричними або електронними пристроями, а також програмними засобами. Вони дозволяють здійснювати контроль доступу шляхом обмеження або дозволу на вхід або вихід певних осіб. (рис. 1.5) [1].

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

Рисунок 1.5 – Засоби контролю та управління доступом

Засоби контролю і улегшення доступу можна розділити на кілька категорій залежно від їх функціонального призначення. Перша категорія - це засоби

обмеженого керування, які використовуються для обмеження доступу до приміщень або об'єктів. Друга категорія - це виконавчі пристрої, які виконують команди, пов'язані з контролем доступу, такі як відкривання дверей або активація сигналізації.

Третя категорія - це пристрої для зчитування ідентифікаторів, таких як картки або браслети, які використовуються для отримання інформації про особу. Четверта категорія - це самі ідентифікатори, що використовуються для ідентифікації особи, яка намагається отримати доступ. Нарешті, п'ята категорія - це засоби управління, які можуть бути апаратними пристроями або програмними засобами, і вони використовуються для налаштування та керування системою контролю доступу.

УПУ (управління перешкодами доступу) - це пристрої, які фізично обмежують доступ і оснащені виконавчими пристроями для керування їх станом. Це можуть бути турнікети, прохідні кабіни, двері і ворота, які мають вбудовані виконавчі пристрої систем контролю і управління доступом. (рис. 1.6).

Для забезпечення ефективної роботи систем контролю і управління доступом (СКУД) можуть використовуватися додаткові пристрої і засоби. Серед них можуть бути блоки безперебійного живлення, які забезпечують неперервну роботу системи навіть при випадку відключення електроживлення. Датчики стану управління доступом використовуються для виявлення стану пристроїв і компонентів системи. Дверні доводчики автоматично закривають двері після проходження особи. Світлові і звукові сповіщувачі використовуються для інформування про стан системи та подачі сигналів. Кнопки ручного управління дозволяють операторам вручну керувати системою. Присутність пристроїв перетворення інтерфейсів мереж зв'язку дозволяє взаємодіяти з іншими системами. Апаратура передачі даних по різних каналах зв'язку забезпечує ефективний обмін інформацією. Використання цих додаткових засобів сприяє покращенню функціональності та надійності роботи СКУД.

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

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 в системі контролю і управління доступом можуть бути класифіковані залежно від способу замикання. Наприклад, електромеханічні пристрої використовуються для замикання на електромеханічні замки, або електромагнітні засувки, які активуються за допомогою електромагнітного поля. Також можуть використовуватися механізми приводу дверей або воріт, які забезпечують автоматичне відкриття або закриття. Використання цих різних типів виконавчих пристроїв дозволяє реалізувати різні методи контролю доступу та замикання об'єктів.

Рисунок 1.6 – Виконавчі пристрої систем контролю і управління доступом

УВІП (пристрої введеннядентифікаційних ознак) - це електронні пристрої, які призначені для введення та зчитування кодові інформції з ідентифікаторів. УВІП складаються з двох основних компонентів - зчитувачів і ідентифікаторів. Зчитувачі

використовуються для зчитування кодової інформації з ідентифікаторів, тоді як ідентифікатори є носіями цієї інформації, які можуть бути введені в систему за допомогою зчитувачів. Ці пристрої дозволяють ефективно та швидко ідентифікувати користувачів або об'єкти, що мають відповідні ідентифікатори.

Зчитувач – пристрій в складі УВІП, призначене для зчитування ідентифікаційних ознак та передачі цієї інформації в контролер системи контролю доступу в приміщення (рис. 1.7).

Рисунок 1.7 – Зчитувач ST-11

Ідентифікатор користувача - це унікальна ознака суб'єкта або об'єкта доступу, яка використовується для ідентифікації. Для цього використовуються різні типи ідентифікаторів, такі як магнітні картки, безконтактні proximity-карти, брелоки, різні радіобрелки, а також фізичні ознаки конкретної людини, наприклад, зображення райдужної оболонки ока, відбиток пальця або долоні. Серед різних типів карт найбільш перспективним є безконтактні радіочастотні (proximity) карти. Вони працюють на відстані і не вимагають точного позиціонування, що забезпечує їх надійну роботу та зручність використання. Також цей тип карт має високу пропускну здатність. Зчитувач генерує електромагнітне випромінювання певної частоти, а коли карта потрапляє в зону дії зчитувача, це випромінювання живить чіп карти через вбудовану антену. Після отримання необхідної енергії для роботи, карта передає свій ідентифікаційний номер на зчитувач за допомогою електромагнітного імпульсу певної форми і частоти. Існують різні типи карт, такі як магнітні картки, безконтактні карти Віганд (Wiegand), штрих-кодові карти і ключ-брелоки. Магнітні картки є найбільш поширеним варіантом. Вони мають вбудовані відрізки дроту з спеціального магнітного сплаву, який є важким для

підробки. Ці карти можуть бути контактними або безконтактними, і зчитуються за допомогою зчитувача Wiegand, який піднесений або пропущений через карту. Вони мають високу довговічність, надійність та забезпечують максимальний захист від підробки, але також є дорожчими. Однак, код в них записується лише під час виготовлення і не може бути змінений. Штрих-кодові карти мають нанесений на них штриховий код, який зчитується зчитувачем. Ключ-брелок є металевою таблеткою з вбудованим чіпом постійної пам'яті. При торканні брелоком до зчитувача, унікальний код ідентифікатора передається з пам'яті брелока в контролер.

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.

У системі всі пристрої взаємодіють між собою за допомогою протоколів - правил, які визначають спосіб обміну даними. Існують стандартні протоколи, що дозволяють використовувати обладнання різних виробників в одній системі. Програмне забезпечення відповідає за налаштування та управління обладнанням, моніторинг його параметрів, організацію та архівування всієї інформації системи.
Контролери є основою апаратї частини системи контролю та управління доступом. Вони підключаються до різного додаткового обладнання, такого як зчитувачі, інтерфейсні модулі, замки, геркони (дверні контакти), кнопки виходу, охоронні датчики та інше периферійне устаткування.
Залежно від способу управління, контролери системи контролю та управління доступом поділяються на три класи. Мережеві контролери дозволяють працювати у мережі під керуванням комп'ютера. Це означає, що вони можуть комунікувати з комп'ютером через мережеве з'єднання, що дозволяє керувати ними та отримувати дані про доступ. (рис. 1.8)

Рисунок 1.8 – Мережеві контролери. Із роботи [6]

Рисунок 1.9 – Автономний контролер СКУД Z-5R 5000. Із роботи [7]

Автономні контролери – пристрої, призначені для обслуговування, як правило, однієї точки проходу (рис. 1.9).

У системах контролю і управління доступом можуть використовуватися різноманітні варіації контролерів. Наприклад, існують контролери, які поєднані зі зчитувачем, або контролери, що вбудовані в електромагнітний замок і т.д. Автономні контролери призначені для використання з різними типами зчитувачів. Зазвичай, такі контролери призначені для обслуговування невеликої кількості користувачів, зазвичай до п'ятисот. Комбіновані контролери об'єднують функції мережевих і автономних контролерів. Якщо є зв'язок з керуючим комп'ютером, контролери працюють як мережевий пристрій, а в разі відсутності зв'язку - як автономні.

Рисунок 1.10 – 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).

Рисунок 1.11 – Схема пристрою системи контролю та управління доступом. Адаптовано із роботи [5]

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 ефективної роботи системи контролю та управління доступом до віддаленого офісу необхідно належним чином організувати архітектуру клієнт-сервер. Клієнт-серверна архітектура стала популярною завдяки зростанню мережі Інтернет та зосередженню значної частини інформації в базах даних на серверах [10].

Клієнт-серверна архітектура може бути описана як концепція інформаційної мережі, в якій основна частина ресурсів зосереджена на серверах, які обслуговують 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.

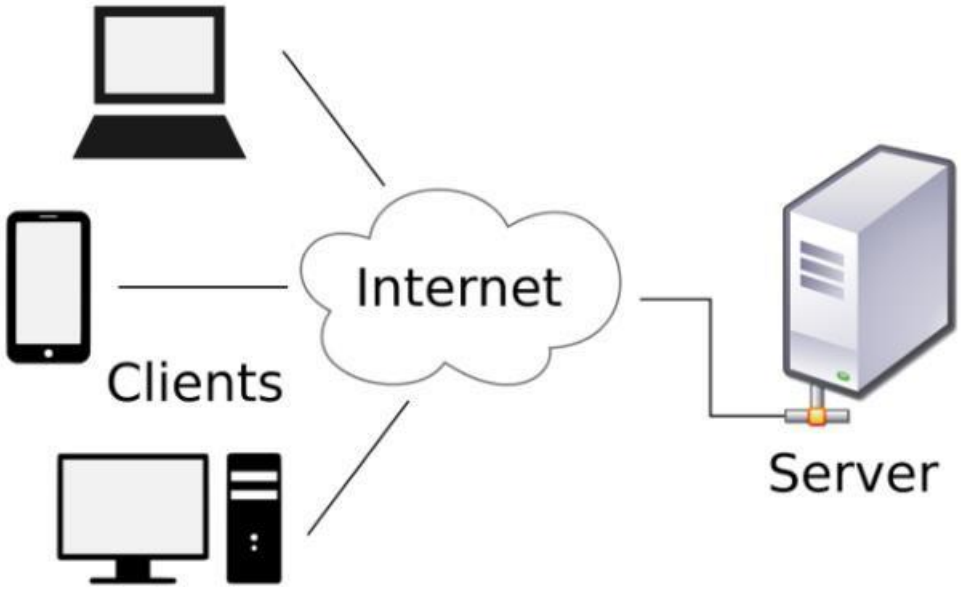

Рисунок 1.12 – Схема клієнт-серверної архітектури. Із роботи [9]

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 років, передбачає розділення рівня додатків від рівня управління даними. У цій архітектурі існує окремий програмний рівень, який зосереджений на логіці програми. Програми цього середнього рівня можуть працювати на спеціальних серверах додатків, але також можуть працювати на звичайних веб-серверах. Останнім рівнем є сервер даних, який відповідає за управління даними [11].

Дворівнева архітектура є більш простою, оскільки всі запити обслуговуються одним сервером. Однак, 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 веб-служба WWW. Існує безліч веб-серверів, на яких розміщується різна інформація У простомуипадку цянформація може бти набор веб-сторнок, зережених на сервері я файли з мовою розітки HTML Однак,асто ситуація є складнішою, оскільки значна частина веб-ресурсів є динамічними, тобто вони не існують у попередньо підготовленому вигляді, а створюються безпосередньо в процесі обробки запиту від користувача.

Основна концепція архітектри клієнт-сервер полягає в розподілі мережевого додатка на різні компоненти, які виконують певні функції. Ці компоненти можуть працювати на різних комп'ютерах, виконуючи роль сервера або клієнта. Такий підхід забезпечує більшу надійність, безпеку та ефективність мережевих додатків та мережі в цілому [12].

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 HTTP-запити від клієнтів, зазвичай веб-браузерів, надає їм відповіді HTTP, які можуть містити HTML-сторінки, зображення, файли, медіа-потоки та інші дані. Веб-сервер є основою Інтернету [13].

Веб-сервер - це програмне забезпечення, яке функціонує на комп'ютері і надає доступ клієнтам до веб-сторінок та інших ресурсів через URL-адреси. Клієнти можуть отримувати доступ до цього сервера, використовуючи веб-браузери або інші програми, що підтримують протокол HTTP.

РОЗДІЛ 2. ПРОЄКТУВАННЯ СКУД ДЛЯ ВІДДАЛЕНОГО ОФІСУ

2.1. Технічне завдання на проєктування СКУД

Технічне завдання на створення системи контролю доступу (СКУД) є основою роботи над проєктом і включає в себе вимоги замовника. Цей документ використовується як основа для проєктування СКУД, а також враховує дані, отримані під час передпроєктного обстеження. Грамотний підхід до технічного завдання дозволяє визначити терміни проєктування і вибрати необхідне обладнання для СКУД [14].

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.

Центральний сервер з встановленим серверним програмним забезпеченням відповідає за обробку інформації в системі контролю доступу (СКУД). Пристрої СКУД взаємодіють з сервером за допомогою різниханалів зв'язку, таких як Ethernet і RS485. СКУД має забезпечувати контроль доступу до різних приміщень, включаючи двері та турнікети.

Для проходу через турнікети ві контролю доступу (СКУД) використовується відеоверифікація, яка здійснюється через особистий пристрій співробітника за допомогою IP-камери та контролю температури. Зображення передається на робочу станцію (АРМ) охорони, де воно аналізується, а потім зберігається на сервері. У разі пожежі турнікет автоматично відкривається, а вхідні двері, обладнані зсувними електромагнітними замками типу AL-300, за робочий час залишаються постійно відкритими [15].

У системі контролю доступу (СКУД) дляужбових приміщень, окрім функцій контролю доступу, також передбачено можливість виконання охоронних функцій. Це означає, що за допомогою карт доступу можна поставити або зняти приміщення з-під охорони. Кожне контрольоване приміщення має бути обладнане світлозвуковим пристроєм, який відображає поточний стан приміщення. Світлозвуковий пристрій і зчитувач карт доступу розташовані в єдиному корпусі. Всередині кожного приміщення також встановлюється кнопка примусового відкривання, яка призначена для випадків невмикання дверей [16]. У разі спрацювання системи оповіщення про пожежу, двері всіх контрольованих приміщень, які не знаходяться під охороною, автоматично переходять у відкритий стан.

Алгоритм роботи системи для вхідних дверей наступний: у штатному режимі вхідні двері знаходяться під охороною. Перший співробітник, який входить, має доступ та вважається зняттям приміщення з охорони. При знятті приміщення з охорони, система вимикає живлення виразного зсувного електромагнітного замка. В кінці робочого дня, коли останній співробітник (зазвичай співробітник охорони) виходить з приміщення, вхідні двері ставляться на охорону. Кожен етап постановки приміщення під охорону повинен відображатися станом світлозвукового пристрою.

Алгоритм роботи системи для службових приміщень наступний: у черговому режимі службові приміщення перебувають під охороною. На робочому місці оператора відображається планування всіх приміщень віддаленого офісу з актуальним станом усіх шлейфів. У разі незаконного проникнення на моніторі з'являється план будівлі, і спрацьовує відповідний шлейф.

Ведеться журнал облікуработок, в якому фіксуються всі події, пов'язані з відкриттям та закриттям приміщень. Згідно з режимом роботи офісу, за 10 хвилин до встановленого часу відкриття, конкретному працівнику надається доступ до відповідного приміщення [16]. При знятті приміщення з охорони шляхом ідентифікації карткою доступу через зчитувач, система вимикає електромагнітний замок. Протягом періоду охорони, контролер приміщення виконує функцію

реєстратора присутності. Кожен співробітник, який заходить через зчитувач, реєструє свою присутність, прикладаючи свою персональну картку до зчитувача. В кінці робочого дня працівник повторно прикладає свою картку до зчитувача-реєстратора, і дверний замок переходить в закритий стан.

Система повинна відображати етапи постановки приміщення під охорону за допомогою світлозвукового пристрою. У разі невдалої постановки на охорону, система надсилає повторний запит на постановку і тільки після цього відправляє сигнал про помилку на робоче місце оператора охорони. Алгоритм роботи системи для дверей побутової кімнати полягає в контролі відкривання цих дверей шляхом реакції вхідного зчитувача на права доступу користувача [17].

Програмне забезечення системи контролю доступу (СКУД) повинно бути гнучк і забезпечувати можливість подальшого розширення системи, включаючи кількість контролерів, користувачів та вилучених робочих місць. Система повинна зберігати свою працездатність і відновлювати свої функції після перезапуску навіть у випадку настання 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.

Контролер СКУД встановлюється всередині охоронюваного (охоронюваного) об'єкта і забезпечує цілодобову роботу. Відповідно до наказу середня напрацювання на відмову контролера СКУД повинна бути не менше 10000 g, а середній термін служби контролера СКУД з урахуванням ремонтних робіт – не менше 8 років. Система живлення контролера СКУД забезпечує захисне відключення при перевантаженні і короткому замиканні ланцюга навантаження, а також аварійне ручне відключення і автоматичне відновлення живлення після усунення причини несправності. Дизайн контролера. Шкідливий вплив на здоров'я, пов'язаний з роботою контролера СКУД, не повинен

перевищувати діючих технічних умов СанПіН 2.2.2./2.4.1340-03. Конструкція контролера СКУД повинна забезпечувати ступінь захисту корпусу IP20. Контролер повинен зберігати працездатність і відповідати всім вимогам під впливом зовнішніх електромагнітних перешкод [18]. Контролер СКУД повинен бути універсальним і підтримувати одночасно кілька типів точок доступу: двері, турнікети тощо. Контролер повинен мати апаратне забезпечення, яке підтримує глобальний режим AntiPassBack без участі сервера, який вимикає подвійне проходження, запобігаючи проходженню двох або більше відвідувачів, які використовують той самий ідентифікатор, для формування точного звіту про робочий час співробітників компанії. Контролер повинен підтримувати зчитувачі форматів Wiegand-26 і TouchMemory. Контролер повинен бути сумісний з кардрідерами різних виробників.

Програмна частина СКУД повинна бути захищена від несанкціонованого доступу. Рівень безпеки інформаційної системи, що захищається, визначається виходячи з важливості інформації, що обробляється, і масштабу інформаційної системи. Корпоративна дистанційна робота — це невелика інформаційна система. Відповідно, захист від несанкціонованого доступу повинен здійснюватися з трьох напрямків:

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

Коли апаратне забезпечення перезавантажиться належним чином, програмне забезпечення СКУД має відновити свою роботу. Повинна бути можливість організації автоматичного та/або ручного резервного копіювання системних даних.

Всі монтажні роботи проводяться відповідно до чинного законодавства України, яке зобов’язує дотримуватись норм і правил охорони праці, пожежної безпеки та техніки безпеки, промислової гігієни, враховуючи особливості будівлі та дотримуючись внутрішніх правил. правила відповідної будівлі. Знаходиться в охоронній зоні (з дотриманням нормативних вимог та встановлених на об’єкті

пропускних режимів). При прокладанні кабельних ліній не можна пошкоджувати технічні та інженерні комунікації та унеможливлювати доступ сторонніх осіб. Проводити роботу відповідно до встановлених і затверджених нормативних документів Підрядник повинен гарантувати якість виконаних робіт, а термін гарантії на якість використаних робіт повинен становити не менше 12 місяців з дати здачі робіт. Сформована концепція СКУД та технічні завдання послужили основою для створення проекту СКУД – єдиного комплексу рішень, призначеного для забезпечення заданого режиму роботи СКУД [19].

Проектом визначено оптимальну структуру та кабельну розводку СКУД, розташування та склад елементів СКУД.

Проектна документація СКУД – це текстові та графічні матеріали, що визначають об’ємно-планувальні, конструктивні та технічні рішення будівництва САУ. Він містить детальні підключення компонентів СКУД до об'єктів і містить креслення, з'єднання і таблиці з'єднань, плани розміщення обладнання та електропроводки та іншу документацію.

РОЗДІЛ 3. РОЗРАХУНОК НАДІЙНОСТІ ЗАСОБІВ ДЛЯ ЗАБЕЗПЕЧЕННЯ РОБОТИ СКУД

Здатність об’єкта підтримувати значення своїх параметрів у визначених межах з часом називається надійністю. Ця якість означає здатність об'єкта виконувати покладені на нього функції в заданих режимах і умовах використання, технічного обслуговування, ремонту, зберігання і транспортування. Відповідно до ДСТУ EN 50133-2-1 [10] критерії надійності ЕБУ включають мінімальну середню тривалість експлуатації 10 000 g (без урахування UPU) та мінімальну середню тривалість експлуатації вісім років.

Коли всі компоненти ECU працюють без збоїв, ми вважатимемо, що ECU знаходиться в робочому стані. Відмова окремого компонента відбувається внаслідок його природного старіння і не залежить від стану інших компонентів системи. Всі конструктивні елементи в ЕБУ відновлені [20]. Випадкові значення часу безвідмовної роботи та часу відновлення для всіх компонентів СКУД розподілені експоненціально. Вся кабельна продукція вважається абсолютно надійною. Визначимо надійність системи контролю та управління доступом, яка складається з наступних компонентів (крім УПУ): контролер Elsys-MBSM-2A-TP, 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.

За принциповою схемою стабілізатор напруги є складним пристроєм, що містить елементи, наведені в таблиці. 3.1 У розрахунок надійності не включаємо процес з'єднання деталей (зварювання).

Таблиця 3.1 – Розрахунок показників надійності стабілізатора напруги

Найменування компонента	Кількість компонентів, N_i	Інтенсивність відмов, год$^{-1}$		Ймовірність безвідмовної роботи, $P(t)$	Ймовірність відмов, $Q(t)$
		$\lambda_i \cdot 10^6$	$N_i \cdot \lambda_i\, 10^6$		
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

Дані таблиці 3.1 і формула експоненціального закону свідчать про те, що слід знайти ймовірність безвідмовної роботи стабілізатора напруги протягом t = 10000 g, а також середній час роботи до першої відмови:

$$Pc\,(10000) = e^{-\lambda wt} = e^{-1{,}7\cdot 10^{-6}\cdot 10000} = 0{,}98$$

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

Розрахунок за окремими компонентами дає:

$$Pc\,(10000) = e^{-0{,}25\cdot 10^{-6}\cdot 10000} = 0{,}997$$

$$Pc\,(10000) = e^{-1\cdot 10^{-6}\cdot 10000} = 0{,}99$$

$$Pc\,(10000) = e^{-0{,}3\cdot 10^{-6}\cdot 10000} = 0{,}997$$

$$Pc\,(10000) = e^{-0{,}2\cdot 10^{-6}\cdot 10000} = 0{,}998$$

Знайдемо ймовірність безаварійної роботи системи протягом t = 10000 годин, а також типовий час роботи до першої відмови (табл. 3.2). У розрахунках використовувалися довідкові дані про кількість відмов компонентів [19].

Таблиця 3.2 – Розрахунок показників надійності контролера

Найменування компонента	Кількість компонентів, N_i	Інтенсивність відмов, год$^{-1}$		Ймовірність безвідмовної роботи, $P(t)$	Ймовірність відмов, $Q(t)$
		$\lambda_i \cdot 10^6$	$N_i \cdot \lambda_i 10^6$		
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

Використовуючи дані, представлені в таблиці 3.4, і застосовуючи формулу експоненціального закону, можна визначити ймовірність безвідмовної роботи контролера протягом часу t = 10000 g, а також розрахувати середній час роботи до виникнення початкова невдача:

$$P_c(10000) = e^{-\lambda_c t} = e^{-2,9\cdot10^{-6}\cdot10000} = 0,97$$

$$t_{ср\cdot с} = \frac{1}{\lambda_с} = \frac{1}{2,9\cdot10^{-6}} = 344827 \text{ год} = 39 \text{ років}$$

Рохрахунок по окремим компонентам дає:

$$Pc\,(10000) = e^{-1,7\cdot10^{-6}\cdot10000} = 0,983$$

$$Pc\,(10000) = e^{-0,22\cdot10^{-6}\cdot10000} = 0,998$$

$$Pc\,(10000) = e^{-0,23\cdot10^{-6}\cdot10000} = 0,998$$

$$Pc\,(10000) = e^{-0,02\cdot10^{-6}\cdot10000} = 0,9998$$

$$Pc\,(10000) = e^{-0,017\cdot10^{-6}\cdot10000} = 0,9998$$

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

$$\sum_{i=1}^{2} N_i = 8;\ \lambda_c = \sum_{i=1}^{2} N_i\lambda_i = 3,05\cdot10^{-6}\ \text{год}^{-1}$$

Таблиця 3.3 – Розрахунок показників надійності СКУД

Найменування компонента	Кількість компонентів, N_i	Інтенсивність відмов, год$^{-1}$	
		$\lambda_i\cdot10^6$	$N_i\cdot\lambda_i\cdot10^6$
Комутатор	1	0,15	0,15
Контролер	7	2,9	20,3

За даними табл. 3.3 і за формулою для експоненціального закону знайдемо ймовірність безвідмовної роботи СКУД протягом t = 10000 год і середній наробіток до першої відмови:

$$P_c(10000) = e^{-\lambda_c t} = e^{-3,05\cdot10^{-6}\cdot10000} = 0,98$$

$$t_{ср\cdot с} = \frac{1}{\lambda_с} = \frac{1}{3,05\cdot10^{-6}} = 327869 \text{ год} = 37 \text{ років}$$

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.

На даному етапі дослідження неможливо розрахувати коефіцієнт готовності СКУД, який становить 0,93, оскільки для розрахунку коефіцієнта готовності СКУД в СКУД необхідне розуміння значущості показника надійності елемента для загального показника надійності СКУД загальний.

ВИСНОВКИ

1. Системи контролю доступу виконують ідентифікаційну аутентифікацію і авторизацію користувачів і об'єктів, оцінюючи необхідні облікові дані для входу, які можуть включати паролі, особисті ідентифікаційні номери (*PIN*-коди), біометричне сканування, токени безпеки або інші чинники аутентифікації. Багатофакторна аутентифікація, яка потребує двох або більше факторів аутентифікації, часто є важливою частиною багаторівневого захисту для захисту систем контролю доступу.

2. Програмні інструменти можуть бути локальними, в хмарі або їх гібридом. Вони можуть зосередитися в першу чергу на управлінні внутрішнім доступом компанії або можуть зосередитися зовні на управлінні доступом для клієнтів.

3. Був проведений розрахунок надійності системи СКУД. Ймовірність безвідмовної роботи сучасних СКУД становить від 0,983 до 0,9998. Середній час до першої відмови становить близько 40 років.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Юдін О. К. Аналіз та класифікація систем контролю та управління доступом на підприємстві. / О. К. Юдін, О. М. Весельська. // Наукоємні технології. – 2018. – С. 220–221.

2. Whitman M. E. Principles of information security. Cengage Learning. / M. E. Whitman. – Boston: Course Technology, 2012. – 658 p.

3. Що таке СКУД?. Ohrana.ua. [Електронний ресурс] — URL: https://ohrana.ua/uk/stati-i-obzory/chto-takoe-skud.html (Дата доступу: 25.04.2024).

4. Роговий М. Дослідження особливостей використання охоронних СКУД / М. Роговий. // Харківський національний університет радіоелектроніки. – 2019. – С. 23–40.

5. Сканер відбитків пальців: як це працює? Який краще – ємнісний, оптичний чи ультразвуковий? [Електронний ресурс] // Магазин «КТС» – Режим доступу до ресурсу: https://ktc.ua/blog/skaner_vidbitkiv_palciv_yak_ce_pracyuye_yakij_krashhe__yemnisnij_optichnij_chi_ultrazvukovij_.html. (Дата доступу: 24.04.2024 р.)

6. Турнікет роторний STAR-TS [Електронний ресурс] // SmartEl – Режим доступу: https://smartel.ua/ua/product/turniket-rotornyy-star-ts/ (Дата доступу: 22.04.2024 р.)

7. Види та особливості турнікетів [Електронний ресурс] // TISO – Режим доступу до ресурсу: https://ua.turniket.net/novini/262-yaki-buvayut-vidiosoblivost-turniketi (Дата доступу: 22.04.2024 р.)

8. Бройдо В.Л. Обчислювальні системи, мережі та телекомунікації / В.Л. Бройдо, Дніпро: 2021. – 560 с.

9. Ворона В.А. Системи контролю та управління доступом / В. А. Ворона, В. А. Тихонов. – К.: Гаряча лінія-Телеком. – 2020. – Т. 272.

10. Особливості монтажу СКУД [Електронний ресурс] – Режим доступу: https://deps.ua/ua/knowegable-base/articles/10139.html (Дата доступу: 25.04.2024 р.).

11. Система контролю та управління доступом (базова). Технічна

документація / Укл.: Ю.Р. Герасим, П.А. Пуля, Т.Б. Крет. – Львів: НУ «Львівська Політехніка», 2011. – 22 с.

12. W. Ejaz, A. Anpalagan, Internet of Things for Smart Cities: Overview and Key Challenges // Internet of Things for Smart Cities. – 2019. – P. 1-10.

13. S.G. Varghese, C.P. Kurian, V. George, A. John, V. Nayak, A. Upadhyay, Comparative study of zigBee topologies for IoT-based lighting automation // IET Wireless Sensor Systems. – 2019.

14. W. Li, T. Logenthiran, V.-T. Phan, W.L. Woo, A Novel Smart Energy Theft System (SETS) for IoT based Smart Home // IEEE Internet of Things Journal. – 2019.

15. H. Ning, F. Shi, T. Zhu, Q. Li, L. Chen A novel ontology consistent with acknowledged standards in smart homes // Computer Networks. – 2019. – V. 148. – P 101-107.

16. S. Badabaji, V.S. Nagaraju, An IoT Based Smart Home Service System // International Journal of Pure and Applied Mathematics. – 2018. – V. 119 No 16. – P. 4659-4667.

17. S.J. Ramson, D.J. Moni, Wireless sensor networks based smart bin // Computers & Electrical Engineering. – 2017. – V. 64. – P. 337-353.

18. P. Pongle, G. Chavan, A Survey: Attacks RPL and 6LowPAN in IoT // International Conference on Pervasive Computing (ICPC 2015), Pune, India, 2015, pp. 1-6.

19. J. Paek, O. Gnawali, M. Vieira, S. Hao, Embedded IoT systems: network, platform, and software // Mobile Information Systems. – 2017. – ID 5921523.

20. A. Dorri, S.S. Kanhere, R. Jurdak, P. Gauravaram, Blockchain for IoT security and privacy: The case study of a smart home // Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA, 13-17 March 2017; pp. 618-623.