ЗВІТ З ПЕРЕВІРКИ НА ПЛАГІАТ

ЦЕЙ ЗВІТ ЗАСВІДЧУЄ, ЩО ПРИКРПЛЕНА РОБОТА
Баранов_Є.О._КІ_129
БУЛА ПЕРЕВІРЕНА СЕРВІСОМ ДЛЯ ЗАПОБІГАННЯ ПЛАГІАТУ MY.PLAG.COM.UA І МАЄ:

СХОЖІСТЬ

11%

РИЗИК ПЛАГІАТУ

100%

ПЕРЕФРАЗУВАННЯ

2%

НЕПРАВИЛЬНІ ЦИТУВАННЯ

0%

Назва файлу: Баранов_Є.О._КІ_129.docx
Файл перевірено: 2023-06-21
Звіт створено: 2023-06-21

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПРИВАТНЕ АКЦІОНЕРНЕ ТОВАРИСТВО «ПРИВАТНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД «ЗАПОРІЗЬКИЙ ІНСТИТУТ ЕКОНОМІКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ» (WWW.ZIEIT.EDU.UA)

Кафедра інформаційних технологій

ДО ЗАХИСТУ ДОПУЩЕНА

Зав. кафедрою _____

д.е.н., доц. Левицький С.І.

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

ПРОЕКТНА РЕАЛІЗАЦІЯ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ НА ОБ'ЄКТ

Виконав
ст. гр. КІ-129 _____ Баранов Є. О.

Керівник
професор _____ Н.Р. Полуектова

Запоріжжя

2023

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ БАКАЛАВРСЬКУ РОБОТУ

студенту гр. КІ-129, спеціальності 121 - «Комп'ютерна інженерія»

Баранову Євгену Олександровичу

1. Тема: «Проектна реалізація системи контролю доступу на об'єкт»

затверджена наказом № 02-02 від 11 січня 2023 р.

2. Термін здачі студентом закінченої роботи: 16 червня 2023 р.

3. Перелік питань, що підлягають розробці:

1. Провести огляд літератури, що присвячена тематиці досліджень.

2. (library.econom.zp.ua) Виконати аналіз існуючих систем контролю та управління доступом.

3. Дослідити стан та проблеми системи контролю доступу в навчальному закладі.

4. Описати вимоги до компонентів СКУД

5. Розробити компонентний склад СКУД та особливості взаємодії компонентів.

6. Розробити план впровадження системи та рекомендації щодо подальшої експлуатації

7. Оформити звіт за результатами роботи

К А Л Е Н Д А Р Н И Й Г Р А Ф І К
підготовки кваліфікаційної бакалаврської роботи
здобувачем освіти інституту ЗІЕІТ денної форми навчання
гр. КІ-129 Барановим Євгеном Олександровичем
2022-2023 навчальний рік

№ етапу	Зміст	Терміни виконання	Готовність по графіку %, підпис керівника	Підпис керівника про повну готовність етапу, дата
1	Збір практичного матеріалу за темою кваліфікаційної бакалаврської роботи	16.01.23-11.02.23		
2	І атестація І розділ кваліфікаційної бакалаврської роботи	27.03.23-31.03.23		
3	ІІ атестація ІІ розділ кваліфікаційної бакалаврської роботи	24.04.23-28.04.23		
4	ІІІ атестація ІІІ розділ кваліфікаційної бакалаврської роботи, висновки та рекомендації, додатки, реферат (library.econom.zp.ua)	22.05.23-26.05.23		
5	Перевірка кваліфікаційної бакалаврської роботи на оригінальність	15.05.23-12.06.23		
6	Доопрацювання кваліфікаційної бакалаврської роботи, підготовка презентації, отримання відгуку керівника і рецензії	29.05.23-12.06.23		
7	Попередній захист кваліфікаційної бакалаврської роботи	12.06.23-18.06.23		
8	Подача кваліфікаційної бакалаврської роботи на кафедру	за 3 дні до захисту		
9	Захист кваліфікаційної бакалаврської роботи (dut.edu.ua)	19.06.23-24.06.23		

Керівник _____ Н.Р. Полуектова

Здобувач освіти _____ Е.О. Баранов

РЕФЕРАТ

Кваліфікаційна бакалаврська робота містить 58 сторінок, 23 рисунки, 12 бібліографічних посилань.

Метою роботи є розробка проекту системи контролю та управління доступом в Запорізький гімназії №106.

Об’єктом дослідження є СКУД Запорізький гімназії №106.

Предметом дослідження є проект системи контролю та управління доступом на об’єкт.

В роботі описані принципи побудови сучасних СКУД-систем, состав, структура та методи взаємодії їх компонентів. В результаті розроблено проект, який дозволить вдосконалити існуючу СКУД в Запорізький гімназії №106 за рахунок використання сучасних компонентів забезпечення контролю та взаємодії з іншими системами забезпечення безпеки у навчальному закладі.

СКУД, НАВЧАЛЬНИЙ ЗАКЛАД, КОНТРОЛЛЕР, ЗЧИТУВАЧ, ПКЗ

ЗМІСТ

ВСТУП

В сучасному світі, де забезпечення безпеки та контроль доступу стають все більш важливими, розробка ефективної системи контролю доступу є актуальною задачею. Особливо в установах освіти, де безпека учнів та персоналу має велике значення. У рамках даного дипломного проекту була поставлена мета розробити проєктну документацію для системи контролю доступу в школі №106, забезпечуючи надійний та зручний механізм контролю доступу для всіх приміщень школи

Основною метою дипломного проекту є створення системи контролю доступу, яка буде забезпечувати безпеку учнів, персоналу та майна школи, контроль відвідування та забезпечення автоматичного контролю доступу до різних приміщень. Застосування передових технологій та розробка ефективного проектного рішення дозволять забезпечити високу ефективність та надійність системи контролю доступу.

Для досягнення поставленої мети, в рамках кваліфікаційної бакалаврської роботи будуть розглянуті різні аспекти проектування системи контролю доступу, включаючи вибір необхідних компонентів, план розташування, аналіз питань електропостачання та розробку рекомендацій щодо подальшої експлуатації системи. Кожен крок розробки буде ретельно аналізований та описаний, з метою забезпечення оптимального функціонування системи контролю доступу.

Очікується, що результатом даного дипломного проекту буде детально розроблене проектне рішення для системи контролю доступу в школі №106, яке може бути використане для подальшої реалізації проекту та забезпечення безпеки та контролю доступу в установі освіти.

РОЗДІЛ 1. АНАЛІЗ ІСНУЮЧИХ СИСТЕМ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ

1.1 Основні принципи роботи систем контролю та управління доступом

Системи контролю та управління (er.nau.edu.ua) доступом є важливою складовою безпеки будь-якого об'єкта, будь то приватний будинок, офісна будівля або промисловий об'єкт. Основною метою таких систем є обмеження доступу до певних приміщень, ресурсів та інформації, забезпечення безпеки працівників та запобігання несанкціонованому доступу[1].

Основні принципи роботи систем контролю та управління доступом (er.nau.edu.ua) включають[1]:

- Аутентифікація - це процес ідентифікації користувача та підтвердження його правомірності. Для цього використовуються різні методи, такі як використання карток доступу, біометричних даних, паролів тощо.
- Авторизація - це процес визначення прав користувача та надання йому доступу до певних ресурсів та приміщень відповідно до його ролі та повноважень.
- Керування правами доступу - це процес визначення рівнів доступу користувачів до різних об'єктів та ресурсів, забезпечення диференційованого доступу та виключення можливості несанкціонованого доступу.
- Моніторинг та аудит - це процес відстеження та запису дій користувачів в системі, забезпечення контролю та аудиту доступу до ресурсів та об'єктів.
- Забезпечення цілісності та конфіденційності даних - це процес захисту даних від несанкціонованого доступу та втручання, забезпечення цілісності та конффіденційності інформації, що зберігається в системі контролю та управління доступом.

Ці принципи є основою роботи будь-якої системи контролю та управління доступом. Вони забезпечують надійність та ефективність системи, зменшуючи ризики несанкціонованого доступу та забезпечуючи безпеку приміщень та ресурсів.

Крім того, в системах контролю та управління доступом можуть використовуватися додаткові принципи, які забезпечують ще більшу безпеку та ефективність роботи системи. Наприклад, можуть використовуватися такі принципи [2]:

- Централізоване керування - це принцип, за яким керування системою здійснюється з одного центрального пункту. Це забезпечує більш ефективне та надійне керування системою.
- Резервне керування - це принцип, за яким система має додаткові засоби керування у разі відмови основного центрального пункту.
- Автоматизація - це принцип, за яким процеси контролю та управління доступом здійснюються автоматично, що забезпечує більш ефективну та точну роботу системи.
- Масштабованість - це принцип, за яким система може розширюватися та адаптуватися до змін потреб користувачів.
- Відкритість - це принцип, за яким система має відкритий код та може інтегруватися з іншими системами безпеки.

Оскільки системи контролю та управління доступом є важливим елементом (sci-conf.com.ua) безпеки будь-якого об'єкта, розуміння основних принципів їх роботи є ключовим для ефективного та надійного захисту ресурсів та приміщень.

Робота СКУД відбувається так. Біля входу в контрольоване приміщення встановлюються спеціальні пристрої зчитувачі, які призначені для зчитування інформації з ідентифікатора, введення пароля чи кодового числа, введення біометричних даних людини. На рис. 1.1 представлені способи біометричної ідентифікації.

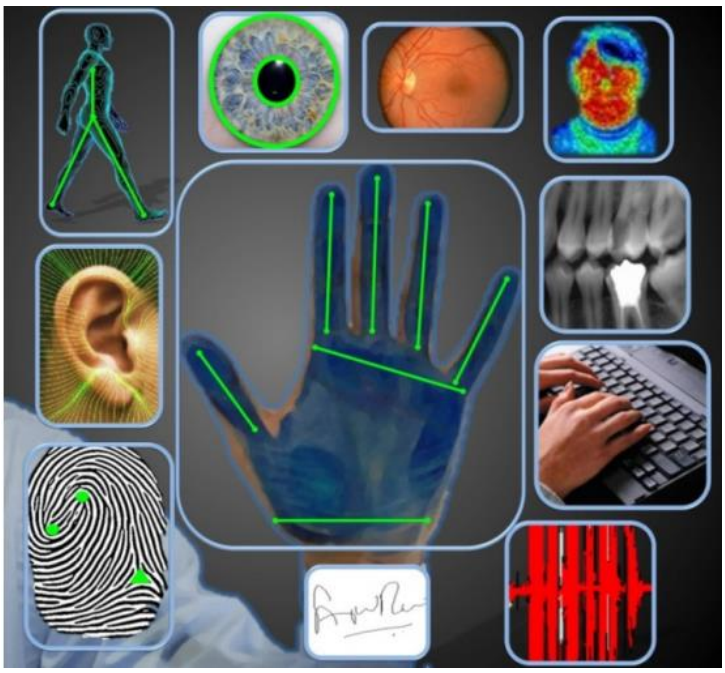

Рис. 1.1. - Способи біометричної ідентифікації

На рис. 1.2. можна бачити типи перепусток (ідентифікаторів)

а б в г

Рис. 1.2. - Типи електронних ідентифікаторів (а- картка, б – електронний браслет, в, г – брелки Touch Memory)

Далі інформація надходить на контролери доступу, які на підставі аналізу даних про власника забезпечують управління перегороджуючими та виконавчими пристроями: відкривають або блокують двері, включають сигнал тривоги, реєструють присутність людину на робочому місці і т.д. На рис. 1.3 представлена загальна логічна схема побудови системи контролю та управління доступом.

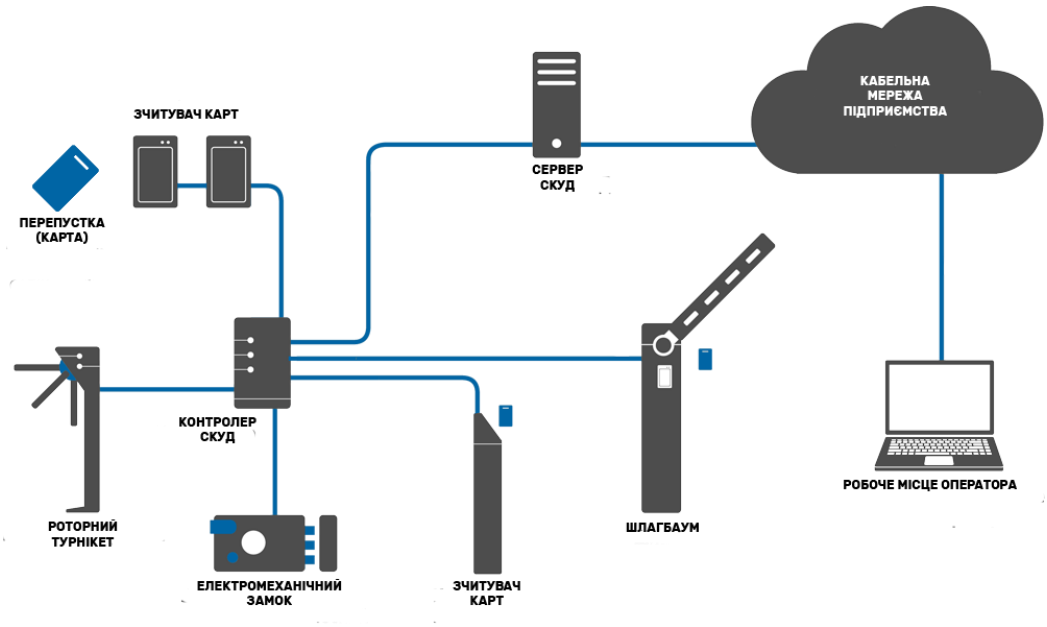

Рис. (pdfslide.tips) 1.3. - Загальна логічна схема СКУД

Для досягнення максимальної ефективності та надійності роботи систем контролю та управління доступом, (pdfslide.tips) важливо правильно вибрати та налаштувати компоненти системи. Для цього необхідно розуміти, які компоненти входять до складу системи та як вони взаємодіють між собою. Нижче (рис. 1.4) наведена загальна класифікація СКУД – систем.

Автономні СКУД повинні забезпечувати:

Видачу сигналу на відкривання постійного прохідного контролера (ППК) під час зчитування зареєстрованого в пам'яті системи ідентифікаційного пристрою. (openarchive.nure.ua) Це означає, що якщо ідентифікаційний пристрій (наприклад, картка доступу) має правильні дані та є відповідним записам у системі, то автономна СКУД видасть сигнал на відкриття ППК.

Заборону відкривання ППК під час зчитування незареєстрованого в пам'яті системи ідентифікаційного пристрою. (openarchive.nure.ua) Якщо ідентифікаційний пристрій не має відповідних записів у системі або містить неправильні дані, автономна СКУД не дозволить відкрити ППК.

Оскільки автономні СКУД працюють без постійного моніторингу та віддаленого управління, (openarchive.nure.ua) вони базуються на збереженій

внутрішній пам'яті для перевірки дозволів доступу. Це дозволяє їм працювати автономно, незалежно від зовнішніх систем або зв'язку з центральним сервером.

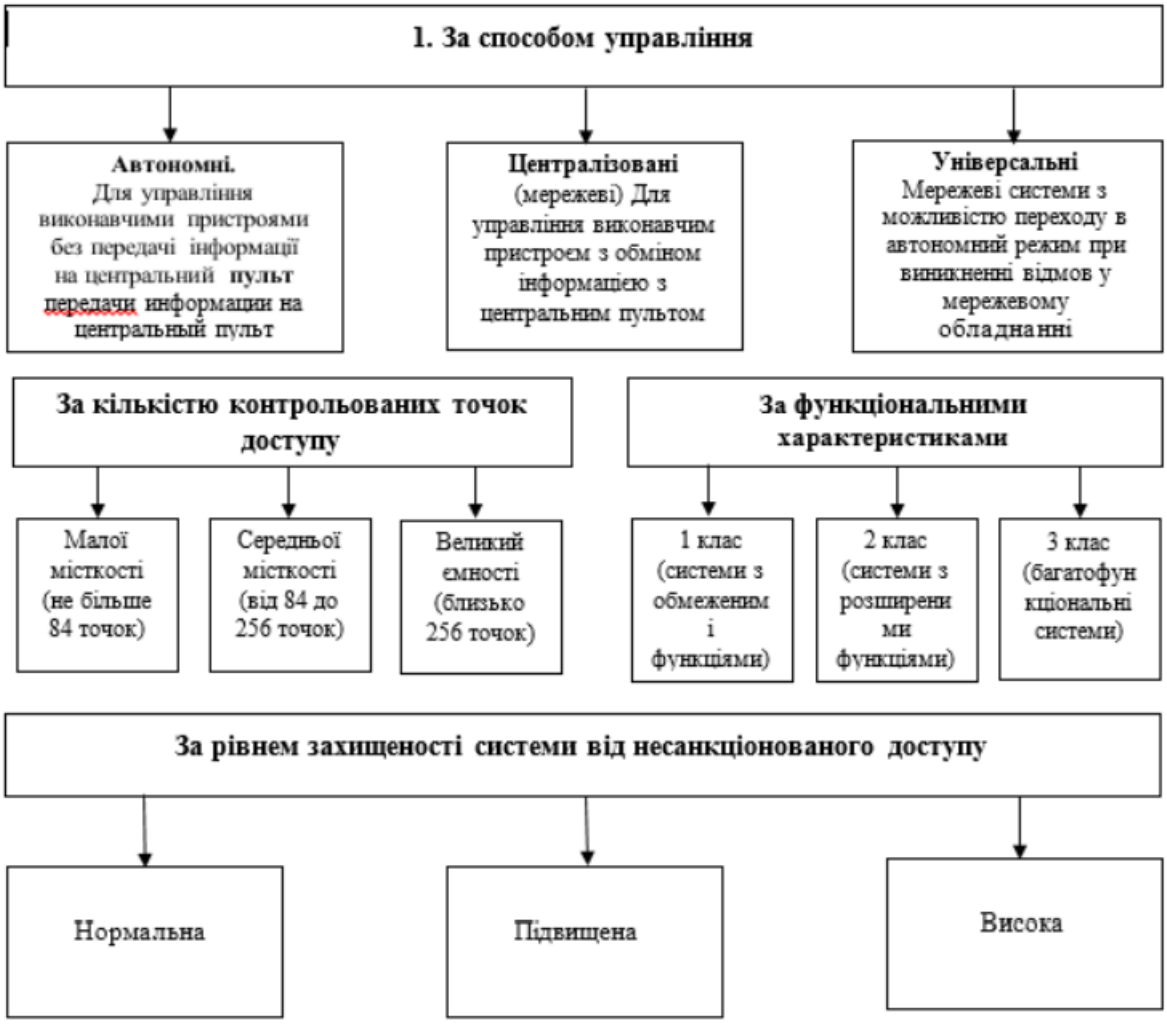

Рис 1.4. – Класифікація СКУД-систем

Централізовані системи контролю доступу (СКУД) відрізняються від автономних систем тим, що вони використовують централізовану інфраструктуру та мережу для управління та контролю доступу на об'єктах. Основні риси централізованих СКУД такі:

Централізоване управління: У централізованій СКУД існує центральний сервер або контролер, який відповідає за керування системою. Цей сервер здійснює контроль доступу, зберігає ідентифікаційні дані, приймає рішення щодо доступу та керує різними компонентами системи.

Зв'язок із зовнішніми пристроями: Централізована СКУД може мати зв'язок із різними пристроями, такими як карт-рідери, бар'єри, камери відеоспостереження тощо. Це дозволяє системі взаємодіяти з різними компонентами безпеки та забезпечувати комплексний контроль доступу.

Централізоване збереження даних: У централізованій СКУД ідентифікаційні дані, правила доступу та інша інформація зберігаються на центральному сервері або базі даних. Це дозволяє одноразово зберігати і керувати всією інформацією про доступ на об'єкті.

Масштабованість: Централізовані СКУД зазвичай є більш масштабованими, оскільки їх можна використовувати на великих об'єктах з багатьма точками доступу. Централізована архітектура дозволяє легко додавати нові пристрої та розширювати систему залежно від потреб.

Запис подій та аналітика: Централізована СКУД зазвичай забезпечує запис подій, аналітику та звіти щодо доступу на об'єкті. Це дозволяє збирати і аналізувати дані для поліпшення безпеки, контролю та виявлення відхилень.

Універсальні системи контролю доступу (СКУД) є багатофункціональними системами, які можуть задовольняти різноманітні потреби і вимоги різних об'єктів. Основні риси універсальних СКУД включають наступне:

Гнучкість та налаштовуваність: Універсальні СКУД здатні адаптуватися до різних умов та вимог об'єкта. Вони надають можливість налаштування параметрів доступу, правил та обмежень, що дозволяє враховувати унікальні особливості кожного об'єкта.

Широкий спектр ідентифікаційних технологій: Універсальні СКУД підтримують різні методи ідентифікації, такі як картки доступу, біометричні дані (відбитки пальців, розпізнавання обличчя), PIN-коди тощо. Це дає можливість використовувати різні види ідентифікації в залежності від потреб та вимог об'єкта.

Інтеграція з іншими системами безпеки: Універсальні СКУД можуть бути легко інтегровані з іншими системами безпеки, такими як системи (rt82.ru) відеоспостереження, пожежної безпеки, контролю доступу до приміщень, системи охоронної сигналізації тощо. Це дозволяє створювати комплексні системи безпеки, які працюють у взаємозв'язку.

Система звітності та аналітика: Універсальні СКУД надають можливість створювати звіти, аналізувати дані доступу та подій для контролю та аудиту. Це дозволяє виявляти відхилення, аналізувати ефективність системи та приймати відповідні заходи.

1.2 Огляд можливостей систем контролю та управління доступом (rt82.ru)

Однією з основних можливостей систем контролю та управління доступом є можливість встановлення різних рівнів доступу для користувачів, що дозволяє регулювати їх доступ до різноманітних об'єктів. Наприклад, користувачі з підвищеним рівнем доступу можуть мати доступ до більшої кількості приміщень та ресурсів, ніж користувачі з низьким рівнем доступу. Крім того, можливість налаштування різних рівнів доступу дозволяє забезпечити безпеку від зловмисників, які намагаються отримати доступ до об'єкту.

Іншою важливою можливістю систем контролю та управління доступом є централізоване керування ними. Це означає, що весь контроль за доступом до об'єкту здійснюється з одного місця. Це дозволяє забезпечити більш ефективний та надійний контроль за доступом та зменшити кількість помилок при керуванні системою.

Окрім цього, системи контролю та управління доступом можуть мати можливість інтеграції з іншими системами безпеки, наприклад системами відеоспостереження, що дозволяє забезпечити більш повну та ефективну охорону об'єкту. Також можуть бути наявні можливості резервногокерування,

що дозволяють забезпечити безперебійну роботу системи та надійність у разі виникнення непередбачуваних ситуацій.

Іншою можливістю систем контролю та управління доступом є можливість віддаленого керування. Це дозволяє адміністраторам керувати системою з віддаленого місця, що робить процес керування більш зручним та ефективним. Наприклад, адміністратор може налаштовувати рівні доступу до об'єкту зі свого комп'ютера, що знаходиться в іншому місці.

Ще однією важливою можливістю систем контролю та управління доступом є можливість автоматизації процесу керування. Наприклад, система може автоматично відкривати двері для користувачів з підвищеним рівнем доступу, що дозволяє зменшити кількість помилок та забезпечити більш ефективний процес керування.

При виборі системи контролю та управління доступом (ecofin.at.ua) слід враховувати багато факторів, таких як розмір та склад об'єкту, типи приміщень та ресурсів, рівні доступу, кількість користувачів та інші фактори. Крім того, слід враховувати можливість майбутнього розширення системи та її сумісність з іншими системами безпеки.

Більш досконалі та дорогі системи контролю та управління доступом (ecofin.at.ua) мають додаткові функціональні можливості:

- можливість отримання одноразового доступу по відбитку пальців у конкретне приміщення будівлі;

- управління (ecofin.at.ua) виконавчими пристроями в автоматичному режимі відповідно до раніше складених розкладів;

- можливість роботи з разовими або тимчасовими електронними перепустками;

- можливість спільної роботи з настільними зчитувачами для найбільш повного контролю за використанням службовцями робочого часу;

- відображення інтерактивних планів об'єкта, його поточного стану та можливістю загального керування однотипними пристроями (відкриття або блокування по тривозі) та ін.

Огляд можливостей систем контролю та управління доступом є важливим кроком у виборі правильної системи для конкретного об'єкту. Він дозволяє оцінити можливості та функціонал систем, які є на ринку і вибрати ту, яка найкраще підходить для конкретного об'єкту.

Крім можливостей систем контролю та управління доступом, слід враховувати також можливі ризики та недоліки, пов'язані з використанням таких систем. Наприклад, можливість виникнення помилок у процесі керування, можливість зламу системи з боку хакерів та інші ризики, які слід враховувати при виборі та налаштуванні системи контролю та управління доступом. (ecofin.at.ua)

Однак, щоб система контролю та управління доступом була ефективною, слід дотримуватися правильної стратегії її впровадження та експлуатації. Слід мати чіткий план впровадження та налаштування системи, визначити ролі та обов'язки персоналу, який буде працювати з системою, та забезпечити необхідне навчання користувачів. Крім того, слід регулярно проводити перевірки та аудити системи, щоб забезпечити її безперебійну роботу та вчасно виявляти та виправляти можливі проблеми.

Зокрема, в освітніх закладах, де є велика кількість користувачів та різні рівні доступу до приміщень та ресурсів, система контролю та управління доступом є особливо важливою. Вона дозволяє забезпечити безпеку учнів, педагогів та інших працівників освітнього закладу та зменшити ризики несанкціонованого доступу до приміщень та ресурсів.

Основні компоненти системи контролю та управління доступом (ecofin.at.ua) в освітніх закладах можуть включати електронні замки, картки доступу, біометричні системи, системи відеоспостереження та інші компоненти. Важливо, щоб ці компоненти були інтегровані між собою та працювали як одна система.

Загалом, системи контролю та управління доступом (ecofin.at.ua) є важливими компонентами будь-якої системи безпеки, вони дозволяють забезпечити контроль за доступом до об'єкту та зменшити ризики втрати

конфіденційної інформації та несанкціонованого доступу. Важливо знати можливості та функції систем контролю та управління доступом, а також (ecofin.at.ua) дотримуватися правильної стратегії їх впровадження та експлуатації, щоб забезпечити їх ефективну та безперебійну роботу. В освітніх закладах, де система контролю та управління доступом є особливо важливою, слід враховувати специфіку роботи та потреби користувачів, а також забезпечити відповідне навчання та підтримку персоналу, який буде працювати з системою.

1.3 Основні компоненти систем контролю та управління доступом

Системи контролю та управління доступом (ecofin.at.ua) складаються з різних компонентів, які взаємодіють між собою, щоб забезпечити ефективну роботу системи.

Засоби СКУД за функціональним призначенням пристроїв поділяються на перегороджувальні керовані (ПКЗ), виконавчі, пристрої для зчитування, ідентифікатори та засоби управління у складі апаратних пристроїв та програмних засобів.

ПКЗ – пристрої, що забезпечують фізичну перешкоду доступу та обладнані виконавчими пристроями для керування їх станом (турнікети, прохідні кабіни, двері та ворота, обладнані виконавчими пристроями (dspace.wunu.edu.ua) систем контролю та керування доступом) (рис. 1.5.).

Рис. 1.5 - Приклади ПКЗ

Контролер доступу - це пристрій, (dspace.wunu.edu.ua) який встановлюється в приміщеннях або на об'єктах і контролює доступ користувачів до цих приміщень або об'єктів. Контролер доступу може бути фізичним або електронним, залежно від того, які методи ідентифікації та аутентифікації використовуються (рис. 1.6).

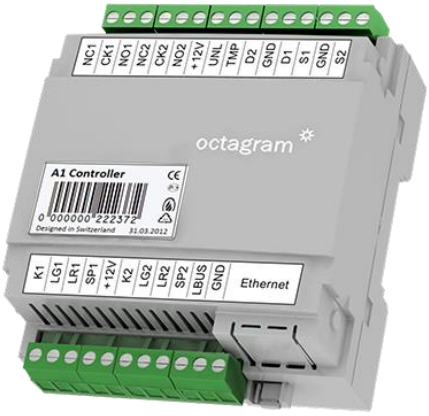

Рис. 1.6 - Приклад приладу контролера доступу
(A1TX – контролер СКУД турнікету)

- Читачі ідентифікаційних даних - це пристрої, які використовуються для зчитування ідентифікаційних даних користувачів, таких як картки доступу, брелоки або біометричні дані.

а) б)

Рис. 1.7 - Приклади приладів читачів ідентифікаційних даних
(а- карток, б-брелоків)

Найбільш поширений тип ідентифікаторів – картки. В даний час застосовуються такі типи карток:

- безконтактні радіочастотні (proximity) карти – найбільш перспективний тип картки. Безконтактні картки спрацьовують

(www.elvis.com.ua) на відстані і не вимагають чіткого позиціонування, що забезпечує їхню стійку роботу та зручність використання, високу пропускну спроможність. Зчитувач генерує електромагнітне випромінювання певної частоти та, при внесенні карти в зону дії зчитувача, це випромінювання через вбудовану в карті антену запитує чип карти. Отримавши необхідну енергію для роботи, карта пересилає на свій зчитувач ідентифікаційний номер за допомогою електромагнітного імпульсу певної форми (eprints.library.odeku.edu.ua) та частоти;

- магнітні карти – найпоширеніший варіант. Карти Віганда (Wiegand) названі на ім'я вченого, який відкрив спеціальний сплав, володіє магнітними властивостями, які важко дублювати. Усередині карти розташовані відрізки дроту (www.elvis.com.ua) із цього сплаву. Карта може бути контактної та безконтактної та зчитується шляхом піднесення чи пропускання через термінал, що називається зчитувач Wiegand. Ці карти більше довговічні, досить безпечні та забезпечують максимальний захист від підробки, але й дорожчі. (www.elvis.com.ua)

Біометричні системи є ще одним важливим компонентом систем контролю та управління доступом. Вони дозволяють ідентифікувати користувача на основі його біометричних даних, таких як відбиток пальця, голос, обличчя або радіус зап'ястя. Біометричні системи забезпечують високий рівень безпеки та точності ідентифікації користувачів.

- Програмне забезпечення, яке управляє роботою системи контролю та управління доступом. (ecofin.at.ua) Воно забезпечує автоматизацію процесу ідентифікації, аутентифікації, авторизації та аудиту користувачів.
- Сервери та бази даних - це компоненти, які використовуються для зберігання даних про користувачів, ролей та прав доступу. Вони також забезпечують роботу системи у режимі реального часу та забезпечують доступ користувачів до інформації.

Системи відеоспостереження також можуть бути використані як компонент систем контролю та управління доступом. Вони дозволяють відслідковувати рухи користувачів та контролювати доступ до об'єкту в режимі реального часу.

При виборі компонентів системи контролю та управління доступом (ecofin.at.ua) слід враховувати вимоги користувачів та особливості об'єкту. Наприклад, у великих офісах може бути необхідно використовувати системи контролю та управління доступом (ecofin.at.ua) з багатьма точками доступу, а в малих офісах може бути достатньо встановити один замок.

При встановленні системи контролю та управління доступом (ecofin.at.ua) слід також враховувати ризики та виключити можливість незаконного доступу до системи. Наприклад, замки та картки доступу повинні мати достатній рівень захисту від підробки та використання незаконними особами. Біометричні системи повинні забезпечувати високий рівень точності ідентифікації та виключати можливість підробки біометричних даних. Також важливо забезпечити захист від кібератак та використання шифрування для захисту конфіденційної інформації.

Крім того, підтримка та розвиток системи контролю та управління доступом (ecofin.at.ua) є важливим етапом у використанні такої системи. Регулярне оновлення програмного забезпечення, налагодження та технічне обслуговування компонентів системи дозволяють забезпечувати ефективну та безпечну роботу системи. Також важливо забезпечити відповідне навчання персоналу, який буде працювати з системою, щоб вони могли користуватися нею ефективно та безпечно.

Також важливо зазначити, що при встановленні системи контролю та управління доступом (ecofin.at.ua) необхідно враховувати її масштаб та потужність. Наприклад, для великих офісів з багатьма точками доступу може знадобитися система з високою потужністю, яка забезпечуватиме швидку обробку даних та ефективний контроль за доступом. У малих же офісах можна

встановити менш потужну систему, яка буде виконувати свої функції із достатньою ефективністю.

До складу компонентів системи контролю та управління доступом (ecofin.at.ua) також можуть входити програмні засоби, які дозволяють адміністраторам налаштовувати систему та керувати рівнем доступу користувачів. Наприклад, програмні засоби можуть забезпечувати можливість створення профілів користувачів, надання різних рівнів доступу, а також моніторингу подій, що відбуваються у системі.

У загальному розумінні, компоненти системи контролю та управління доступом (ecofin.at.ua) повинні бути інтегровані та взаємодіяти один з одним для забезпечення ефективної та безпечної роботи системи. Використання різноманітних компонентів дозволяє забезпечувати високий рівень контролю та зручність використання для користувачів, а також забезпечувати захист від незаконного доступу до об'єкту.

1.4 Особливості систем контролю та управління доступом в освітніх закладах

У сучасних умовах керівництво шкіл змушене постійно шукати нові та інноваційні засоби забезпечення захисту. Електронні системи керування доступом пропонують більш надійний та економний захист. Системи контролю доступу (ecofin.at.ua) можуть бути інтегровані з іншими заходами безпеки, наприклад з охоронною сигналізацією та системами відеоспостереження для досягнення максимальної продуктивності всіх технологій, що використовуються для забезпечення безпеки. У зв'язку з цим системи контролю та управління доступом (ecofin.at.ua) в освітніх закладах мають свої особливості. До них можна віднести:

- Необхідність забезпечення безпеки учнів та персоналу. В систему контролю та управління доступом повинні входити такі елементи, як

контролери доступу, читачі ідентифікаційних даних та системи відеоспостереження.

- Різні рівні доступу. Учні, викладачі та інші працівники освітніх закладів повинні мати різний рівень доступу до приміщень та інформації.
- Управління правами доступу користувачів. В систему контролю та управління доступом можуть входити такі елементи, як рольова модель, матриця прав доступу та контроль доступу на основі атрибутів, щоб забезпечити відповідність рівню доступу прав користувачів.
- Інтеграція з іншими системами безпеки. Системи контролю та управління доступом (ecofin.at.ua) в освітніх закладах можуть бути інтегровані з іншими системами безпеки, такими як системи протипожежного захисту, щоб забезпечити загальну безпеку приміщень.
- Моніторинг та аудит дій користувачів. У системі контролю та управління доступом (ecofin.at.ua) можуть бути забезпечені такі елементи, як моніторинг та аудит дій користувачів, щоб виявляти можливі порушення безпеки та усувати їх вчасно.

У таких закладах зазвичай перебуває велика кількість людей, включаючи студентів, викладачів, адміністраторів та інші категорії персоналу.

Крім того, у системах контролю та управління доступом в освітніх закладах важливо забезпечити безпеку учнів та персоналу. Наприклад, можуть бути встановлені системи аварійного виклику, які дозволяють швидко повідомляти про аварії та забезпечувати швидкий доступ до даних про студентів та персонал, які перебувають в закладі у данний час.

Також можуть бути встановлені системи відеоспостереження, які дозволяють контролювати безпеку на території закладу та реагувати на негативні ситуації. Важливо також враховувати вимоги до конфіденційності даних, які зберігаються у системі контролю та управління доступом, (ecofin.at.ua) зокрема, особистих даних студентів та персоналу.

Іншою важливою особливістю систем контролю та управління доступом в освітніх закладах є необхідність враховувати різні потреби користувачів.

Наприклад, учням можуть знадобитися інші види доступу до закладу, ніж викладачам або адміністраторам. Тому необхідно забезпечувати можливість налаштування системи контролю та управління доступом (ecofin.at.ua) відповідно до потреб користувачів.

У загальному розумінні, особливості систем контролю та управління доступом в освітніх закладах пов'язані з різноманітністю користувачів, різними рівнями доступу та потребами безпеки. Важливо забезпечити ефективну та безпечну роботу системи, враховуючи особливості кожного конкретного закладу.

Для ефективної роботи системи контролю та управління доступом (ecofin.at.ua) в освітніх закладах можуть використовуватися різні компоненти, такі як карт-рідери, біометричні сканери, датчики руху та інші. Важливо враховувати потреби користувачів та можливості бюджету закладу при виборі необхідних компонентів.

Крім того, важливо забезпечити інтеграцію системи контролю та управління доступом (ecofin.at.ua) з іншими системами, такими як система внутрішнього зв'язку, система відеоспостереження та інші. Це дозволяє забезпечити максимальну ефективність роботи системи та уникнути дублювання функціоналу.

Одним із важливих аспектів при використанні систем контролю та управління доступом в освітніх закладах є навчання користувачів. Важливо проводити навчання студентів, викладачів та іншого персоналу щодо правильного використання системи та виконання правил безпеки.

Однією з найважливіших особливостей систем контролю та управління доступом в освітніх закладах є забезпечення доступності для людей з обмеженими можливостями. Наприклад, можуть бути встановлені спеціальні пристрої для керування дверима, які дозволяють користувачам з обмеженою рухливістю вільно пересуватися по території закладу. Також можуть бути використані біометричні сканери, які дозволяють людям з вадами зору або слуху користуватися системою.

Для забезпечення безпеки важливо встановлювати систему контролю та управління доступом на всіх входах до закладу. Також можуть бути встановлені системи контролю та управління доступом (ecofin.at.ua) на окремих ділянках закладу, де зберігаються цінні речі або проводяться важливі заходи.

Ще однією важливою особливістю систем контролю та управління доступом в освітніх закладах є можливість контролювати доступ до різних зон або приміщень закладу. Наприклад, викладачі можуть мати доступ до своїх аудиторій, а студенти – до своїх класів. Така система дозволяє забезпечити максимальну безпеку та ефективність роботи закладу.

У підсумку, системи контролю та управління доступом (ecofin.at.ua) є важливим інструментом для забезпечення безпеки та ефективної роботи освітніх закладів. Важливо враховувати особливості кожного конкретного закладу при виборі та встановленні системи контролю та управління доступом. (ecofin.at.ua) Також необхідно забезпечувати навчання користувачів щодо правильного використання системи та виконання правил безпеки.

1.5 Висновки за розділом

У розділі 1 було розглянуто основні принципи роботи систем управління доступом, їх можливості та компоненти. Було також розглянуто особливості систем контролю та управління доступом в освітніх закладах.

Загальна мета систем контролю та управління доступом полягає в забезпеченні безпеки та захисту від несанкціонованого доступу (ecofin.at.ua) до різних об'єктів та ресурсів. Для цього в системі повинні бути використані надійні компоненти, які забезпечують ефективну роботу системи.

РОЗДІЛ 2: ЗАГАЛЬНА ХАРАКТЕРИСТИКА ОБ'ЄКТА ДОСЛІДЖЕННЯ ТА ОБГРУНТУВАННЯ ВИБОРУ ПРОЕКТНОГО РІШЕННЯ

2.1 Характеристика системи управління доступом до освітнього закладу на прикладі школи " Запорізька гімназія № 106"

В даному розділі буде проведено характеристику системи управління доступом до освітнього закладу на прикладі школи " Запорізька гімназія № 106".

Рис. 2.1. Будівля школи «" Запорізька гімназія № 106»

План першого поверху об’єкта представлений на рис. 2.2.

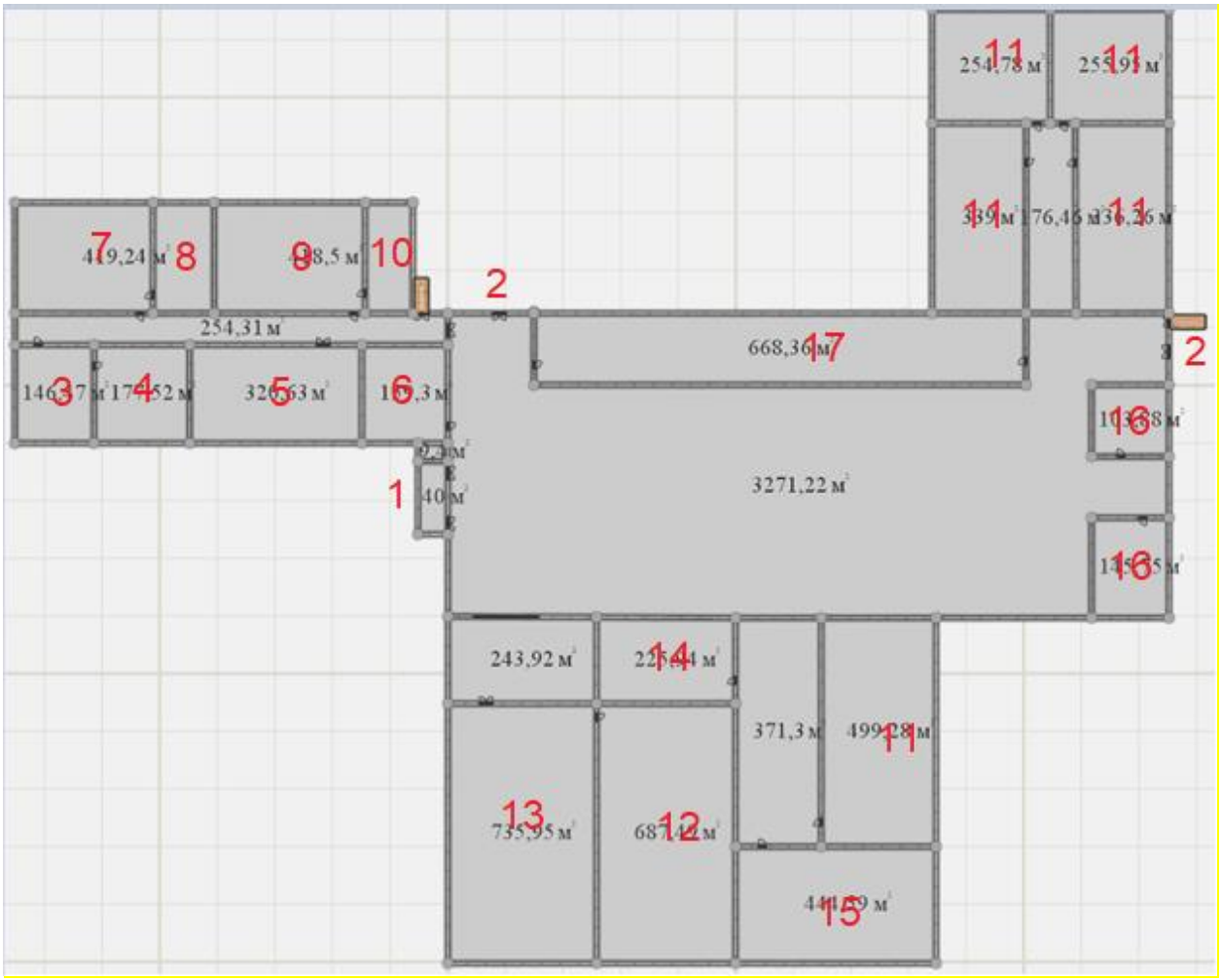

Рис. 2.2. План першого поверху будівлі школи

1. Головний вхід/вихід
2. Запасні виходи
3. Медпункт
4. Приміщення з ліками
5. Спальня
6. Вчительська
7. Кабінет хімії
8. Лабораторія хімії
9. Кабінет біології
10. Лабораторія біології
11. Клас
12. Кухня
13. Їдальня

14. Серверна
15. Майстерня
16. Гардероб
17. Комора

Система управління доступом до школи " Запорізька гімназія № 106" має на меті забезпечити безпеку та контроль над входом і виходом учнів, вчителів, персоналу школи та відвідувачів. Вона повинна складатися з наступних компонентів:

Електронні ключові картки: Кожному учаснику освітнього процесу, включаючи учнів, вчителів та персонал, видається електронна ключова картка. Ця картка містить інформацію про особу, яка має до неї доступ, і використовується для отримання доступу до школи.

Електронні замки: На всіх дверях школи повинні бути встановлені електронні замки, які можуть бути відкриті за допомогою електронних ключових карток. Це дозволяє контролювати доступ до різних приміщень школи, таких як класні кімнати, бібліотека, спортивний зал і т.д.

Контроль доступу: Система має відстежувати час і дату входу та виходу кожного учасника, реєструвати цю інформацію і зберігати в централізованій базі даних. Це дозволяє адміністрації школи вести точний облік присутності учнів і персоналу, а також контролювати безпеку шкільного простору.

Моніторинг системи: Система управління доступом у школі також має включати моніторингову систему, яка дозволяє адміністрації школи в реальному часі спостерігати за проходженням учасників через контрольні точки.

2.2 Вибір та обгрунтування проектного рішення для управління доступом у школі “Запорізька гімназія №106”

2.2.1 Загальні засади вибору СКУД

Мета передпроектного обстеження полягає у визначенні комплексу заходів та розроблення технічних пропозицій з урахуванням сформованих типових рішень. За результатами обстеження (virtuapc.ru) складається технічне завдання обладнання об'єкта СКУД. У технічному завданні вказується призначення СКУД, технічне обґрунтування та опис системи, розміщення складових частин системи, умови експлуатації коштів ККД. Прописуються основні технічні характеристики СКУД.

Для надійної роботи СКУД на об'єкті необхідно враховувати вплив електромагнітних перешкод, перепади напруги живлення, заземлення складових частин системи та т.п. У приміщенні школи шкідливий вплив навколишнього середовища слід враховувати для засобів КУД вхідних дверей.

Особливих умов (запиленість, підвищена вологість, негативна температура, агресивне середовище тощо) на об'єкті немає.

Вибір варіанта СКУД нерозривно пов'язаний із вимогами забезпечення безпеки конкретного об'єкта Закордонний та вітчизняний досвід створення інтегрованих систем безпеки показує [4], що найбільше раціональним є реалізація їхнього «інтелектуального ядра» на базі апаратно-програмних засобів СКУД. Такий підхід, зокрема, дозволяє заощадити на апаратурі СКУД та засобах охоронної сигналізації (наприклад, одні і ті ж дверні датчики положення можуть застосовуватись і в апаратурі контролю доступу, а також в охоронній сигналізації).

Вітчизняні розробки СКУД кращі, навіть якщо мають найгірші параметри щодо зарубіжних аналогів. Це пояснюється неможливістю проаналізувати математичне та програмне забезпечення імпортних СКУД. В

умовах, коли СКУД визначає рівень безпеки об'єкта, «ціна» кожної відмови і навіть простого збою в роботі апаратури надто велика.

СКУД можуть бути автономними та мережевими. Вибір варіанта залежить від цілі монтажу та типу об'єкта. Якщо потрібно лише контролювати вхід на територію, що охороняється, а аналітична інформація не має значення, вибирають автономну.

2.2.2 Порівняльний аналіз СКУД різних виробників

Для обгрунтування вибору СКУД для школи «Гармонія плюс» були проаналізовані продукти та послуги чотирьох українських компаній.

Аналіз ринка показав, що в Україні не існує підприємств, які надають спеціалізовані послуги встановленні та налаштування СКУД-систем тільки для навчальних закладів. Більшість компаній займаються продажом обладнання та за замовленням реалізують комплексні проекти з встановлення та підтримки СКУД. Серед таких систем можна виділити наступні.

1. Ohrana.ua.

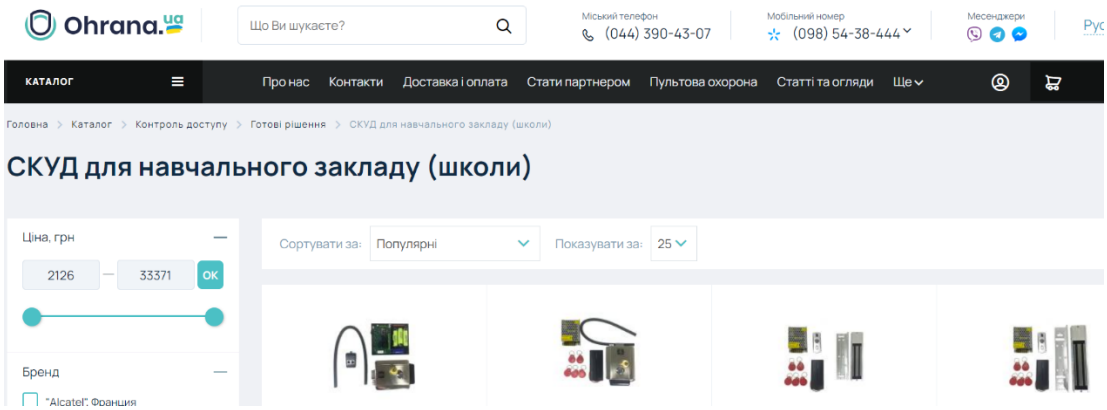

Рис. 2.2 Сайт компанії Ohrana.ua.

Компанія надає наступні послуги: підбір обладнання під запит клієнта; проектування об'єктів будь-якої складності, у тому числі систем пожежної безпеки (згідно з нормами чинного законодавства); монтаж обладнання у Києві та Запоріжжі.

2. Компанія ОТТ+

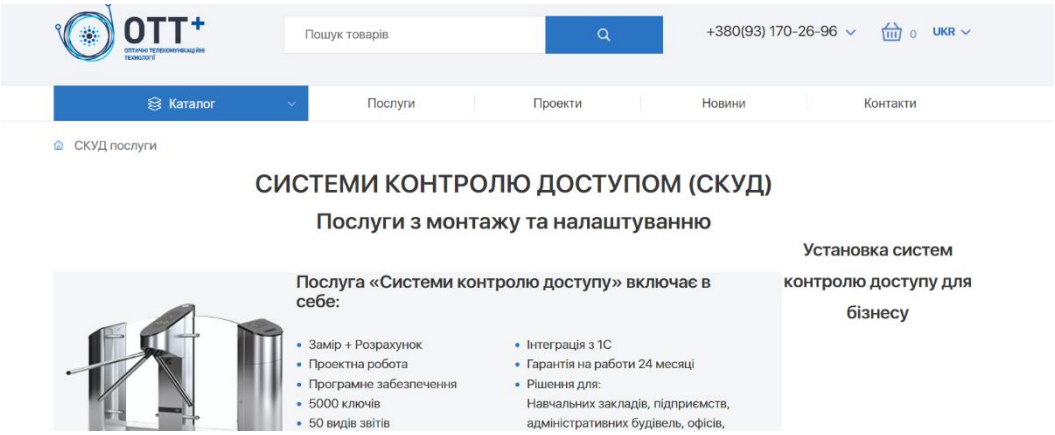

Рис. 2.3 Сайт компанії «OT TECHNOLOGIES»

Це одна з найбільших компаній, що спеціалізується на постачанні та виробництві широкого спектру телекомунікаційного обладнання (оптичний кабель, муфти, телекомунікаційні шафи, стійки, панелі, бокси, патчкорди і багато ін.). Фірма виробляє власне обладнання, а також реалізує мережеве обладнання та деяке обладнання для систем контролю доступу підприємства «Одесакабель». Як видно з малюнку, фірма виконує замовлення з монтажу та налаштування СКУД в тому числі для навчальних закладів.

3. Octagram – компанія, яка реалізує обладнання, та проєкти на базі обладнання швейцарскої компанії Octagram AG в Україні.

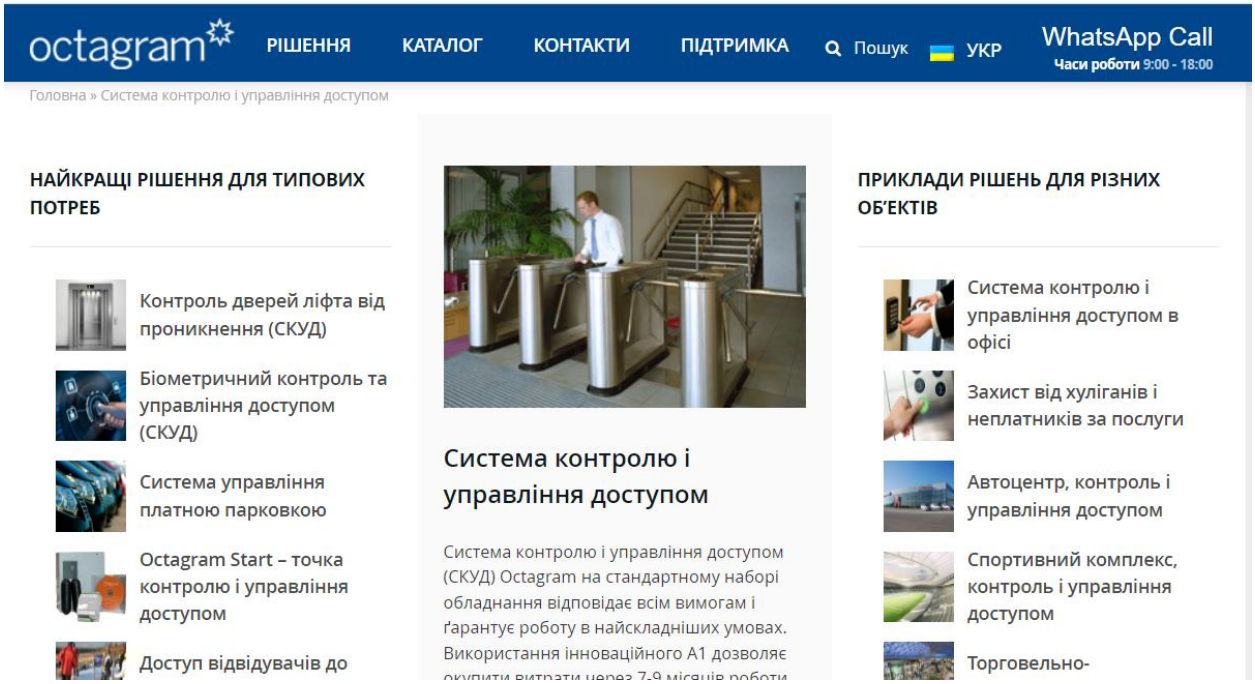

Рис. 2.4 Сайт компанії Octagram

4. Брама. Інженерні системи

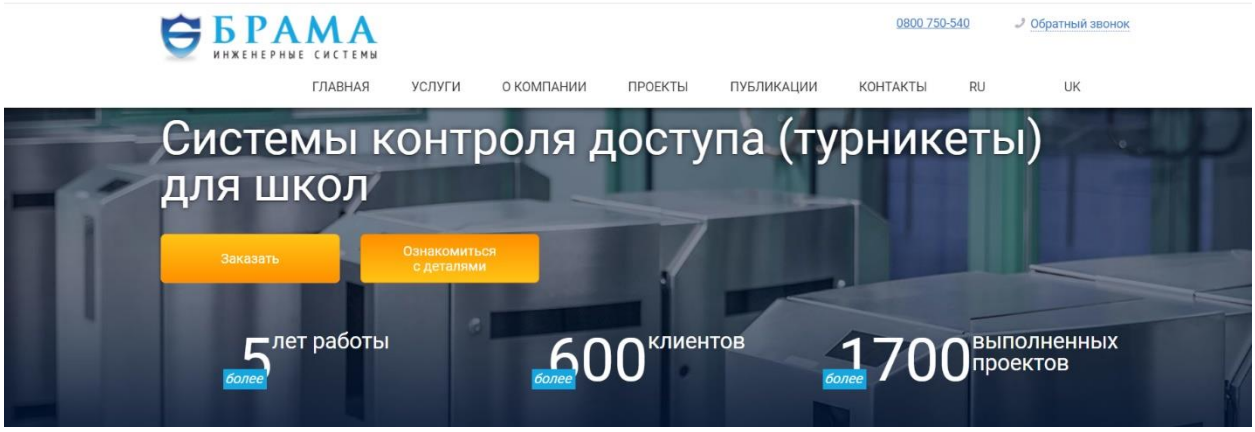

Рис. 2.5. Сайт компанії Брама

Проект «Безпечна школа», який пропонує ця компанія, це комплексне рішення, яке дозволяє контролювати відвідуваність занять та оперативно відслідковувати успішність у навчанні дітей.

Для забезпечення працездатності системи безпеки встановлюються сучасні системи контролю та керування доступом, яка доповнюється системою відеоспостереження. Пропускний режим у школі дає можливість

контролювати час входу та виходу учнів та персоналу та водночас запобігає доступу на територію навчального закладу сторонніх.

Батьки отримують доступ до таких компонентів системи, як «електронний щоденник» учня, а також «електронний журнал» класу – з будь-якого пристрою (смартфона, планшета, лептопа), підключеного до Інтернету.

Турнікет для школи, який необхідно придбати для будь-якої пропускної системи, забезпечує персоналізований доступ по ідентифікатору – пластиковій карті («шкільна карта» у вигляді стандартного учнівського квитка). Після застосування ідентифікатора до зчитувального пристрою система звіряє інформацію з базою даної і відкриває (блокує) доступ для відвідування школи з одночасним занесенням часу проходження турнікету. Після закінчення занять турнікети у школі забезпечують збирання інформації про час виходу учнів чи викладачів із закладу.

СКУД для школи від цієї компанії можуть бути доповнені сучасними системами відеоспостереження, що підвищують рівень безпеки учнів та дозволяють контролювати всю територію навчального закладу. Відеоспостереження – це програмно-апаратний комплекс, що складається з камер, відеореєстраторів для обробки та запису сигналу, кабельних трас, джерел безперебійного живлення, місць зберігання даних.

Так, можуть використовуватися як дротові, так і бездротові відеокамери (IP-відеоспостереження) або їх комбінації (гібридне відеоспостереження). Вся інформація записується та зберігається на серверах певний час, відкриваючи доступ до будь-якої камери школи. Така автоматизація шкіл дозволяє забезпечити найвищий безпековий рівень, який дозволяє і батькам, і вчителям контролювати відвідуваність і вести моніторинг успішності учнів (на допомогу прийде «електронний щоденник школяра»).

РОЗДІЛ 3 РОЗБУДОВА ПРОЕКТА СКУД ДЛЯ ШКОЛЫ ЗЗБНВК №106

3.1 Технічне завдання на проектування СКУД

3.1.1 Загальне уявлення про технічне завдання

Технічне завдання на проектування системи керування і управління доступом (СКУД) для школи 106 включає розробку теоретичного плану та інструкції з впровадження СКУД у майбутньому. Вибір саме цієї школи для проекту обумовлений досвідом знайомства з нею та відсутністю функціонуючої СКУД на даний момент. Головна мета цього проекту - забезпечити безпеку, контроль та ефективне управління доступом до приміщень школи.

Основні виклики, які передували розробці СКУД для школи 106, включають контроль відвідування школи учнями, забезпечення безпеки учнів та персоналу, контроль доступу до приміщень, а також автоматичне відкриття дверей у разі пожежі або інших надзвичайних ситуацій. Ці проблеми спонукали до впровадження СКУД, оскільки ця система забезпечує автоматизований контроль та управління доступом до приміщень, що дозволяє ефективно реагувати на потенційні небезпеки та забезпечити безпеку у школі.

Технічне завдання передбачає використання різних функцій та компонентів СКУД для забезпечення потрібного функціоналу. До основних функцій, що планується реалізувати, входять:

1. Контроль доступу: СКУД буде забезпечувати можливість використання різних видів пропусків, що дозволить ідентифікувати учнів, персонал та вчителів, а також контролювати їх доступ до конкретних приміщень школи.

2. Запис даних: Система буде здатна зберігати дані про входи та виходи учнів, персоналу та вчителів. Ця інформація може бути збережена на

хмарному сховищі або локальному сервері для забезпечення зручного доступу та архівування даних.

3. Відеоспостереження: У складі СКУД може бути включена система відеоспостереження, що дозволить відстежувати події, відбуваються в різних зонах школи. Це сприятиме забезпеченню додаткової безпеки та контролю внутрішньошкільної діяльності.

4. Система пожежогасіння: У проекті СКУД може бути передбачена інтеграція з системою пожежогасіння. У разі виникнення пожежі система СКУД автоматично відкриє всі двері, що дозволить учням, персоналу та вчителям швидко та безпечно покинути будівлю.

5. Мобільний додаток та веб-сайт: Планується створення мобільного додатку або веб-сайту, які забезпечать батькам можливість контролювати відвідування своїх дітей у школі. Вони матимуть змогу отримувати онлайн-звіти про входи та виходи своєї дитини, а також переглядати важливі дані у режимі реального часу.

Цей проект СКУД для школи 106 спроектовано з урахуванням потреб у контролі доступу та забезпеченні безпеки школярів. Технічне завдання надає теоретичний план та інструкцію для майбутнього впровадження СКУД у школі, включаючи вибір компонентів та функціоналу.

3.1.2 Опис вимог до компонентів СКУД

При проектуванні системи керування і управління доступом (СКУД) для школи 106, були встановлені конкретні вимоги до компонентів, які забезпечать ефективне функціонування системи. Основні вимоги включають:

1. Читачі пропусків: Необхідно обрати високоякісні читачі пропусків, які забезпечать надійне і швидке зчитування інформації з пропусків учнів, вчителів та персоналу. Ці читачі повинні бути сумісні з обраною системою і забезпечувати точність та швидкість ідентифікації.

2. Контролери доступу: Необхідно встановити контролери доступу, які будуть керувати процесом відкриття та закриття дверей у школі. Ці контролери повинні бути надійними, мають багатофункціональний інтерфейс та підтримувати різні види авторизації доступу.
3. Електромагнітні замки: Для забезпечення безпеки учнів та персоналу, потрібно встановити електромагнітні замки на дверях. Ці замки мають бути потужними, надійними та відповідати всім необхідним стандартам безпеки.
4. Система відеоспостереження: Для забезпечення додаткової безпеки в школі, рекомендується встановити систему відеоспостереження. Ця система повинна мати високоякісні камери з можливістю запису та зберігання відео, а також можливість дистанційного перегляду зображень.
5. Система звукового сигналізування: Для швидкого та ефективного інформування учнів та персоналу про надзвичайні ситуації, необхідно встановити систему звукового сигналізування. Ця система повинна бути достатньо потужною та має вмонтовану функцію автоматичного відкриття дверей у разі пожежі або інших надзвичайних ситуацій.
6. Система керування та моніторингу: Для ефективного управління та моніторингу СКУД, необхідно використовувати програмне забезпечення, яке дозволить адміністраторам контролювати доступ до приміщень, переглядати журнали доступу та отримувати повідомлення про надзвичайні події.

Вибір відповідних компонентів для СКУД базувався на врахуванні потреб школи 106 у контролі відвідуваємості, безпеці учнів та персоналу, контролі доступу та швидкому реагуванні на надзвичайні ситуації. Вищезазначені компоненти були обрані з метою забезпечити надійність, ефективність та зручність використання системи СКУД у школі 106.

3.1.3 Алгоритми роботи СКУД в окремих приміщеннях

При проектуванні СКУД для школи 106, необхідно розробити алгоритми роботи СКУД в різних приміщеннях з урахуванням особливостей доступу та безпеки. Основні алгоритми роботи СКУД будуть визначені наступним чином:

Для того, щоб це забезпечити потрібно ставити електронні замки та зчитувачі на всі двері!

1. Головний вхід та адміністративні приміщення:
    - Учні не мають доступу до адміністративних приміщень.
    - Вчителя мають доступ до адміністративних приміщень та інших необхідних приміщень, крім технічних приміщень та лабораторій, які не пов'язані з їх предметом викладання.
    - Персонал (повара, адміністратор, охорона) мають повний доступ до всіх необхідних приміщень.
2. Учбові аудиторії:
    - Учні та учителя мають доступ до своїх учбових аудиторій у встановлені години навчання.
    - Учні не мають доступу до інших учбових аудиторій, крім тих, де вони зареєстровані на урок.
    - Учителя мають доступ до всіх учбових аудиторій.
3. Технічні приміщення та склади:
    - Учні не мають доступу до технічних приміщень та складів.
    - Учителя мають обмежений доступ до технічних приміщень та складів, які пов'язані з їх предметом викладання.
    - Персонал (повара, адміністратор, охорона) мають повний доступ до технічних приміщень та складів.
4. Лабораторії:

- Учні мають доступ до лабораторій тільки в час проведення практичних занять.
- Учителя мають повний доступ до лабораторій, пов'язаних з їх предметом викладання.

5. Автоматичне відкриття дверей:
    - Для забезпечення безпеки і ефективності, встановлено систему автоматичного відкриття дверей у разі пожежі або інших надзвичайних ситуацій. Це забезпечує швидкий доступ до виходів та сприяє евакуації.

Алгоритми роботи СКУД в окремих приміщеннях враховують вимоги безпеки, забезпечують належний контроль доступу та відповідають потребам школи 106. Вони дозволяють забезпечити безпеку учнів, персоналу та майна школи, зменшити можливі ризики і забезпечити ефективне функціонування системи керування і управління доступом.

3.1.4 Робота СКУД при зміні умов функціонування

Під час розробки СКУД для школи 106 було враховано, що умови функціонування можуть змінюватися залежно від різних факторів, таких як графік роботи, перерви, святкові дні, вихідні та інші подібні ситуації. При цьому, головною метою розробки було забезпечення надійності, безпеки та ефективності роботи СКУД в будь-яких змінених умовах.

Основні аспекти, що враховані в СКУД школи 106 для роботи в змінених умовах, включають:

1. Зміна режиму доступу: СКУД дозволяє автоматично переключати режими доступу в залежності від графіка роботи школи. Наприклад, під час урочних та позаурочних годин, можуть бути застосовані різні обмеження доступу для учнів та персоналу. Це дозволяє забезпечити більш гнучкий та ефективний контроль доступу відповідно до розкладу занять.

2. Автоматичний перехід в аварійний режим: СКУД має вбудовані функціональності, які реагують на надзвичайні ситуації. Наприклад, у разі активації пожежної сигналізації чи натискання аварійних кнопок, система відразу вживає необхідних заходів, таких як відкриття дверей для евакуації або активація внутрішніх процедур безпеки. Це забезпечує швидку реакцію на надзвичайні ситуації та максимальну безпеку учнів та персоналу школи.
3. Управління та зміна умов роботи: СКУД дозволяє зручне дистанційне управління та налаштування системи. Це включає можливість зміни графіка роботи, перерв, святкових днів та вихідних в системі. Адміністратори СКУД мають повний доступ до налаштувань і можуть вносити зміни у часові параметри та режими доступу відповідно до потреб школи.
4. Автоматична діагностика та резервне живлення: СКУД має вбудовану систему автоматичної діагностики, яка контролює стан обладнання та виявляє можливі несправності. У разі виявлення проблем, система надсилає повідомлення адміністраторам для вжиття відповідних заходів. Крім того, СКУД може мати механізми резервного живлення, які забезпечують неперервну роботу системи навіть у випадку відключення основного джерела живлення.

Застосування цих функцій у СКУД школи 106 дозволяє забезпечити безпеку, надійність та гнучкість роботи системи навіть при зміні умов функціонування. Це дає можливість школі ефективно управляти доступом, регулювати графік роботи та реагувати на надзвичайні ситуації для забезпечення максимального комфорту та безпеки всіх користувачів.

3.1.5 Інтеграція додаткових функцій та систем

Під час розробки СКУД для школи 106, було виявлено потребу в інтеграції додаткових функцій та систем, які допомагають розширити

можливості та покращити функціональність СКУД. Інтеграція цих додаткових компонентів сприяє поліпшенню ефективності, безпеці та зручності використання системи контролю доступу.

Основні аспекти, які були враховані під час інтеграції додаткових функцій та систем, включають:

1. Система відеонагляду: Для забезпечення додаткового рівня безпеки та контролю, була виконана інтеграція системи відеонагляду. Це дозволяє в реальному часі відстежувати події, які відбуваються в шкільних приміщеннях, а також зберігати відеозаписи для подальшого аналізу. Адміністраторам надано можливість моніторингу подій та здійснення необхідних заходів у разі виявлення порушень.
2. Система керування режимами роботи: Інтеграція системи керування режимами роботи дозволяє змінювати графіки роботи, перерви, регулювати доступ у різних періодах, включати аварійний режим та регулювати час роботи СКУД. Це надає гнучкість та можливість адаптувати систему до змін у розкладі та потребах школи.
3. Інтеграція з системами екстреного реагування: Важливим аспектом інтеграції є забезпечення сповіщень та активування системи в разі надзвичайних ситуацій. СКУД пов'язана з системою пожежної сигналізації, що дозволяє автоматично активувати тривогу та інформувати відповідних осіб про виникнення пожежі. Також були встановлені аварійні кнопки, які надають можливість швидко сповістити служби безпеки у разі необхідності. Дистанційне управління системою дозволяє адміністраторам здійснювати контроль та вживати необхідні заходи навіть з віддаленої локації.

Інтеграція цих додаткових функцій та систем у СКУД школи 106 робить її більш функціональною та надійною. Вона забезпечує розширені можливості контролю, безпеки та управління, дозволяючи школі ефективно вирішувати завдання, пов'язані з контролем доступу та безпекою приміщень.

3.1.6 Управління та моніторинг системи

Управління та моніторинг системи контролю доступу (СКУД) для школи 106 є одними з ключових аспектів, необхідних для ефективної роботи і забезпечення безпеки приміщень. Цей підраздел присвячений детальному опису методів та інструментів управління системою СКУД, а також моніторингу її функціонування з метою забезпечення безперебійної та надійної роботи системи контролю доступу.

1. Управління доступом: Система СКУД школи 106 повинна мати інструменти для налаштування та керування доступом до приміщень. Адміністратори системи можуть змінювати права доступу для кожного користувача відповідно до їх ролі та обов'язків. Це включає обмеження доступу учнів до технічних приміщень, складів і лабораторій поза часом уроків. Учителі мають доступ до всіх приміщень, крім тих, що не відповідають їхній предметній області. Наприклад, вчитель фізичного виховання не має доступу до лабораторії, але має доступ до складу спортивного інвентарю. Крім того, персонал школи, залежно від їх класифікації та обов'язків, має відповідний доступ до відповідних приміщень.
2. Моніторинг роботи системи: Система СКУД школи 106 забезпечує постійний моніторинг роботи системи контролю доступу. Це включає відображення інформації про всі входи та виходи з приміщень, активність користувачів, а також події, що відбуваються в системі. Адміністратори можуть в режимі реального часу відстежувати ці дані та реагувати на будь-які надзвичайні ситуації, які виникають в школі. Моніторинг також включає відображення статистики по використанню системи, що дозволяє адміністрації школи аналізувати та планувати роботу системи ефективніше.
3. Сповіщення та управління подіями: Система СКУД школи 106 обладнана спеціальними функціями для сповіщення про надзвичайні

ситуації та управління подіями. Вона може отримувати сигнали від систем пожежної сигналізації, активувати аварійні кнопки та забезпечувати дистанційне управління системою. Це дозволяє швидко реагувати на потенційні небезпеки та негайно приймати необхідні заходи для забезпечення безпеки учнів, персоналу та майна школи.

4. Діагностика та резервне забезпечення: Система СКУД школи 106 має включа в себе автоматичну діагностику, яка дозволяє виявляти можливі несправності або проблеми з роботою системи. Це сприяє попередженню виникнення неполадок та дозволяє швидко вжити заходів для їх вирішення. Крім того, система має механізми резервного живлення, що забезпечують безперебійну роботу в разі відключення основного джерела енергії. Це забезпечує надійність та стабільність роботи СКУД навіть при виникненні електричних перебоїв або аварійних ситуацій.

3.1.7 Інтеграція з іншими системами

Під час проектування СКУД для школи 106 важливо врахувати можливість інтеграції з іншими системами, які вже використовуються в шкільній інфраструктурі. Інтеграція дозволяє створити єдину систему управління, оптимізувати процеси та забезпечити взаємодію різних систем всередині школи. У даному підрозділі ми розглянемо кілька аспектів інтеграції, які мають бути враховані під час проектування СКУД для школи 106.

1. Інтеграція з системою обліку та адміністративним ПЗ: СКУД школи 106 була спроектована з можливістю інтеграції з системою обліку школи та адміністративним програмним забезпеченням. Це дозволяє автоматизувати процеси обліку та адміністрування, такі як облік відвідування учнів, формування звітів про доступ та інші адміністративні завдання. Інтеграція даних між СКУД та

адміністративним ПЗ забезпечує єдине сховище інформації та зручний доступ до неї.

2. Інтеграція з системою відеоспостереження: Для забезпечення додаткового рівня безпеки та контролю всередині школи, СКУД школи 106 інтегрується з системою відеоспостереження. Це дозволяє в режимі реального часу спостерігати за подіями та своєчасно реагувати на виникаючі ситуації. У разі потреби система відеоспостереження може бути використана для аналізу інцидентів та надання доказів.
3. Інтеграція з системою пожежної безпеки: Для забезпечення безпеки учнів, персоналу та майна, СКУД школи 106 взаємодіє з системою пожежної безпеки. Вона сповіщає про активацію пожежного сповіщувача, активує аварійні кнопки та надає можливість дистанційного управління системою. Інтеграція СКУД з системою пожежної безпеки дозволяє оперативно реагувати на надзвичайні ситуації та забезпечує безпеку всередині школи.
4. Інтеграція з системою управління ресурсами: Для ефективного використання ресурсів та забезпечення комфорту внутрішнього середовища, СКУД школи 106 інтегрується з системою управління освітленням та кліматичними пристроями. Це дозволяє автоматично регулювати освітлення та температуру в приміщеннях в залежності від активності та присутності людей. Інтеграція з системою управління ресурсами сприяє енергоефективності та створенню комфортних умов для всіх учасників навчального процесу.

Отже, СКУД школи 106 має забезпечувати інтеграцію з різними системами, що дозволяє створити єдину систему управління та забезпечити безпеку, ефективність та комфорт всередині шкільного середовища.

3.2. Опис проектного рішення

Стандартний набір компонентів для системи контролю управління доступом в школі може включати наступні елементи:

Електронні замки: Електронні замки забезпечують контроль доступу до різних зон шкільного приміщення. Вони можуть бути встановлені на дверях класних кімнат, адміністративних приміщень, бібліотеки, спортивного комплексу тощо. Електронні замки дозволяють управляти доступом за допомогою карток, брелоків або пін-кодів.

Картки або брелоки доступу: Картки або брелоки є основними засобами ідентифікації користувачів. Кожен учень, вчитель або персонал школи може мати особисту картку або брелок, які вони використовують для доступу до певних зон школи.

Контролер доступу: Контролер доступу це пристрій, який керує роботою електронних замків. Він зчитує дані з карток або брелоків і приймає рішення про надання або відмову у доступі до певної зони. Контролер доступу також може зберігати інформацію про присутність учнів і персоналу школи.

Система моніторингу: Для забезпечення безпеки важливо мати систему моніторингу, яка складається з відеокамер та системи запису. Відеокамери встановлюються в ключових місцях шкільного приміщення, таких як входи, коридори, складські приміщення тощо, і дозволяють відслідковувати події в режимі реального часу або записувати їх для майбутнього аналізу.

Центральна система управління: Центральна система управління є мозком всієї системи контролю доступу. Вона дозволяє адміністраторам школи керувати доступ

3.2.2 Компонентний склад СКУД

Рішення СКУД забезпечує:

- санкціонований доступ учнів, вчителів, адміністративного та допоміжного персоналу у зони та виділені приміщення;

- видачу сигналу тривоги на АРМ чергового оператора чи пульт управління у разі несанкціонованого доступу (відкриття дверей) до зон доступу та виділені приміщення;

- комп'ютерний облік входу та виходу учнів та співробітників з веденням протоколу в комп'ютері та виведення протоколу на принтер;

- можливість тимчасового блокування турнікету.

До складу СКУД входять:

- станційне обладнання, до складу якого входять сервер (er.nau.edu.ua) FRAY S3-FSSDK4-H та АРМ співробітника охорони на базі комп'ютера «Оріон ПРО», реалізовані на базі персональних комп'ютерів, об'єднані в локальну мережу;

- лінійне обладнання, що включає контролери СКУД NDC F18IP. Контролери з'єднані між собою двопровідною лінією зв'язку з інтерфейсом Wiegand за схемою загальної шини. Як середовище (er.nau.edu.ua) для передачі даних інтерфейсу Wiegand використовуються мідні кручені пари. Ці групи контролерів підключені до сервера, з якого здійснюється керування та програмування кожного контролера; (er.nau.edu.ua)

- абонентські пристрої:

електромеханічний турнікет Класик-Елегант-СМ, електромагнітні замки SEVEN ML-7726, зчитувачі карт доступу U-Prox mini, кнопки «ВИХІД» та кнопки розблокування замків (турнікета) у разі виникнення надзвичайної ситуації. У Додатку А показано загальну схему приміщення. Точка контролю доступу функціонально складається з контролера доступу, виконавчого механізму (турнікет, двері), зчитувачів, магнітоконтактних сповіщувачів. До складу ТКД входить джерело резервованого живлення для підтримки

працездатності пристроїв при тимчасовому пропаданні напруги мережі живлення.

Прохід через точки з контролем доступу здійснюється при піднесенні картки до зчитувача. У разі успішної ідентифікації картки доступу системою виконавчий пристрій розблоковується, дозволяючи (er.nau.edu.ua) одноразовий прохід. Кожній карті в базі даних СКУД надаються певні права доступу та відомості: список дозволених точок входу; розклад дозволеного проходу; дані по учня або співробітника (П.І.Б., посада та тощо); фотографія учня або співробітника; табельний номер; Додаткові параметри (за потреби).

Кожна точка проходу контрольована системою може бути відкрита для проходу різними способами:

- автоматичний (за пред'явленням безконтактної картки зчитувачу)

- пряма команда з АРМ у разі потреби вільного доступу або доступу за разовими перепустками;

- централізоване відключення замикаючих пристроїв на всіх точках проходу, що застосовується в екстрених ситуаціях, пов'язаних із природними катаклізмами, пожежею тощо.

- ручне керування з кнопок розблокування.

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

Управління системою та моніторинг за її роботою здійснюється з сервера та з АРМ оператора. Сервер є високопродуктивним комп'ютером. Контролери доступу підключаються до сервера за допомогою перетворювача інтерфейсів USB/wiegand. Сервер працює під (er.nau.edu.ua) керуванням операційної системи Windows 10 та програмного комплексу Оріон ПРО.

Автоматизоване робоче місце є персональним комп'ютером, який працює під керуванням операційної системи Windows 10 та програмного модуля для робочих місць. З АРМ здійснюється контроль, управління та

налаштування обладнання. Сервер та АРМ об'єднуються в локальну мережу за допомогою мережного комутатора.

Двостороннім доступом обладнуються приміщення та кабінету директора. У цьому випадку зчитувачі встановлюються з обох сторін двері. З внутрішнього боку додатково встановлюється кнопка пожежної розблокування. При виникненні екстреної ситуації двері може бути розблоковано зсередини кнопкою розблокування. При цьому подія «Ручне розблокування дверей» фіксується у протоколі подій системи.

У холі розташований турнікет для учнів та співробітників. Проектним рішенням передбачається встановлення одного турнікету для безперешкодного та своєчасного проходу. Висновок зроблений на основі даних спостережень за кількістю учнів. Спостереження проводилися протягом 6 робочих днів протягом дня. Пропускна спроможність турнікету 15 чол./хв.

Розміщення обладнання СКУД за точками доступу представлено у табл. 3.1.

Таблиця 3.1

Розміщення обладнання СКУД

Точка доступу	Розташування	Обладнання
ТД1	Вхід до будівлі	Турнікет
ТД2	Лабораторії	Магнітний замок, зчитувач карток
ТД3	Вчительська	Магнітний замок, зчитувач карток
ТД4	Серверна	Магнітний замок, зчитувач карток
ТД5	Приміщення з ліками	Магнітний замок, зчитувач карток
ТД6	Кухня	Магнітний замок, зчитувач карток
ТД7	Майстерня	Магнітний замок, зчитувач карток
ТД8	Комора	Магнітний замок, зчитувач карток
ТД9	Аварійні виходи	Магнітний замок, зчитувач карток

.

Таким чином, проектне рішення забезпечує всі дев’ять точок доступу засобами ККД.

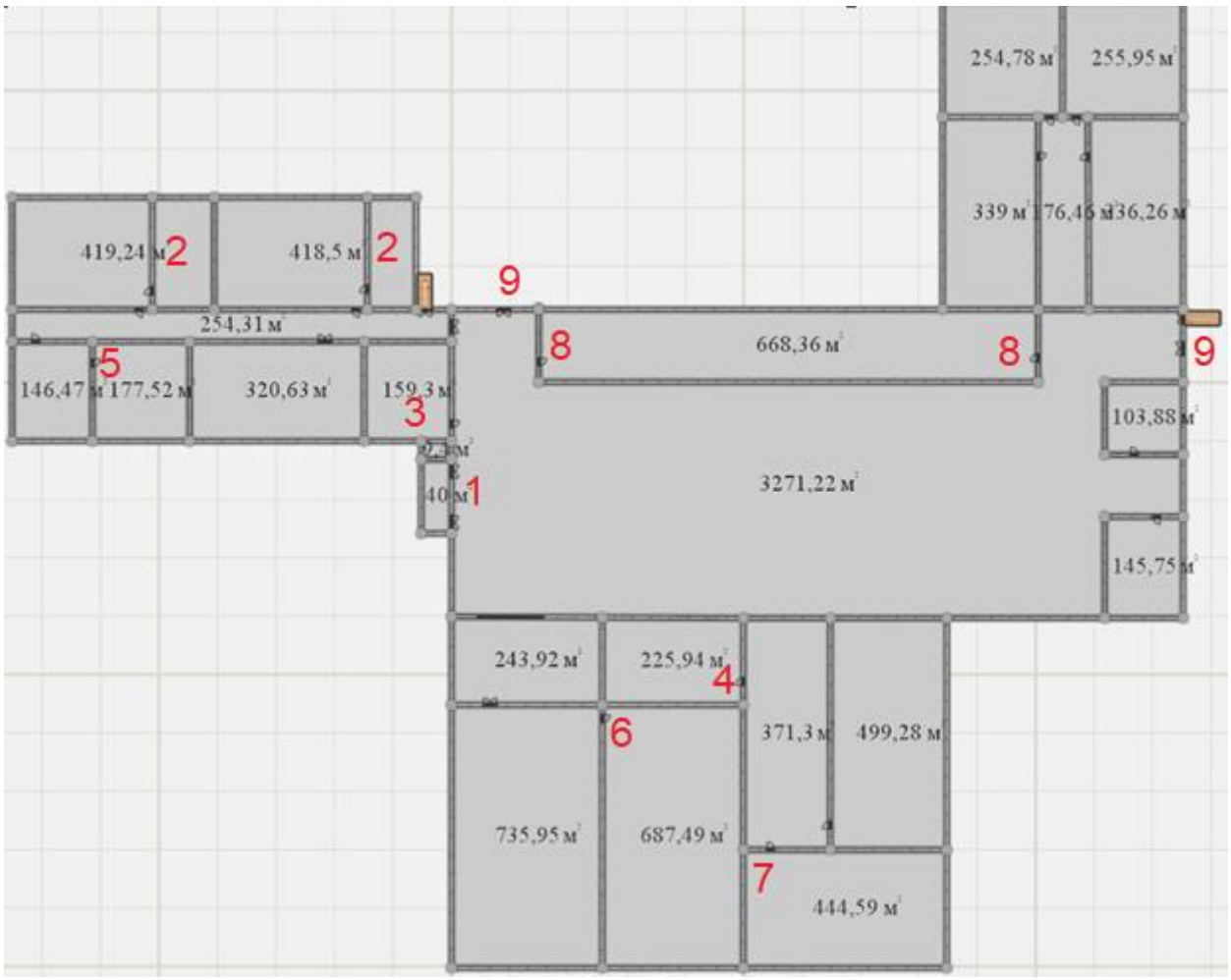

Рис. 3.1 Розташування точок доступу

3.2.3 Електропостачання СКУД

У процесі проектування СКУД було приділено особливу увагу питанню електропостачання системи з метою забезпечення надійності та безперебійної роботи. Всі необхідні компоненти та заходи були вжиті, щоб забезпечити стабільну та безпечну електроподачу. Нижче наведено детальний опис електропостачання СКУД:

Основне джерело живлення: Для постачання електричної енергії СКУД використовується стабільна та надійна електромережа школи. Це основне джерело живлення забезпечує постійний електричний струм необхідної напруги та частоти для безперебійної роботи системи.

Стабілізатори напруги: Для забезпечення стабільної роботи всіх компонентів СКУД, встановлені стабілізатори напруги, які регулюють коливання напруги та компенсують можливі зміни у електричній мережі. Це допомагає підтримувати сталу та оптимальну напругу на всій системі.

Захист від перенапруг: Для захисту СКУД від перенапруг та небезпечних електричних сплесків, були встановлені спеціальні пристрої захисту. Вони реагують на зростання напруги та автоматично відключають живлення системи, щоб уникнути можливих пошкоджень та збоїв.

Резервне живлення: З метою забезпечення неперебійної роботи СКУД у випадку відключення основного джерела живлення, встановлено резервне живлення. Це може бути безперебійне живлення (UPS) або дизель-генератор, які автоматично активуються у разі відключення основного джерела, забезпечуючи постійне живлення системи протягом визначеного періоду часу.

Заземлення: В рамках забезпечення безпечної роботи електрообладнання та захисту від електричних розрядів, було проведено належне заземлення. Це створює стійкий електричний контур і допомагає уникнути електростатичного розряду, перенапруги та пошкодження обладнання.

Всі вищезазначені компоненти електропостачання були ретельно підібрані, встановлені та протестовані згідно з вимогами проекту СКУД. Це забезпечує надійну та безперебійну роботу системи контролю доступу, сприяє безпеці та зручності для учнів, вчителів та персоналу школи.

3.2.4 Вимоги до монтажу обладнання та прокладання кабельних трас

Контролери СКУД встановлюють у безпосередній близькості від точок проходу в недоступному для сторонніх осіб місці. (er.nau.edu.ua) Кріплення здійснюють саморізами та пластиковими дюбелями. Пульт керування турнікетом встановлюють на стіл робочого місця поста охорони. Турнікет встановлюють згідно з інструкцією з експлуатації на бетонну поверхню. Дроти

до турнікетів підводять у гофрованих трубах під поверхнею підлоги (er.nau.edu.ua) в штробах згідно з інструкцією з експлуатації. Зчитувач встановлюють на привід турнікета відповідно до технічними умовами.

Зчитувачі, що контролюють прохід через двері, встановлюють на рівні 1,2 м від рівня підлоги, згідно зі схемами встановлення обладнання дверей та інструкції з експлуатації. Електромагнітні замки, доводчики встановлюють згідно з інструкцією з експлуатації та кресленнями виробника. Лінії зв'язку виконують виконують кабелем КПВ-ВП 4х2х0,52 у разі внутрішнього прокладання і кабелем КПВЭ-ВП 4*2*0,54 у разі вуличного прокладання. Лінії зв'язку лінійного обладнання встановлюють проводами відповідно до схем підключення контролерів. Підведення мережевого живлення до автоматів живлення СКУД здійснюють відповідно до ПУЕ, забезпечуючи необхідне заземлення або занулення живильної мережі. Електроживлення підводять до апаратури кабелями ПВС 3×1 відповідно до технічних описів пристроїв. З'єднання вузлів системи виконують відповідно до схем підключення та технічної документації виробників.

3.2.5 Технічні характеристики основних вузлів

Система побудована на базі мережевого контролера доступу NDC F18IP, до якого підключаються зчитувачі і виконавчий пристрій – турнікет.

NDC F18IP (U-Prox IP400) обробляє інформацію, що надходить зі зчитувачів, і за допомогою чотирьох реле здійснює комутацію (відчинення/зачинення) турнікета. Контролер може працювати як автономно, так і в складі мережі. Для об'єднання в мережу СКУД служить інтерфейс Ethernet.

В якості замикаючого механізму використовується турнікет. Вхід і вихід з приміщення через турнікет завдяки наявності двох зчитувачів забезпечується за безконтактними картками стандарту EM-Marine. Керувати турнікетом також можна за допомогою пульта.

Акумуляторна батарея, що входить в постачання, служить джерелом резервного живлення для контролера. (protection-key.com.ua)

Турнікет Класик-Елегант-СМ:

- Тип турнікета: напівзростовий
- Тип приводу: СМ моторизований
- Ширина перекриття проходу: 550мм
- Пропускна здатність: 20-30чел/хв
- Навантажувальна здатність: до 20000 проходів/доба
- Функції: вхід, вихід, блокування
- Функція «Антипаніка» (по команді від пульта або контролера загороджувальна штанга опускається для забезпечення аварійного виходу)
- Світлодіодна індикація
- Матеріал: нержавіюча шліфована сталь
- Робоча температура: від -10°С до + 45°С
- Розміри: 1020х420х320мм

Мережевий контролер NDC F18IP (U-Prox IP400):

- Тип контролера: мережевий
- Тип підключення: дротове
- Кількість зчитувачів, що підключаються: 2 (Wiegand)
- Кількість точок проходу: 2
- 8 входів для підключення шлейфів з контролем по струму (кінцевий резистор – 2 кОм)
- 2 реле (контакти NO/NC/COM) 5А@24В
- 2 реле (контакти NO/COM) 1А@24В
- Пам'ять: 31768 постійних ідентифікаторів + 1000 тимчасових
- Порти: USB, Ethernet 100Mbit
- Живлення: DC 12V
- Робоча температура: від 0°С до + 55°С

Зчитувач U-Prox mini:

- Тип встановлення: внутрішнє

- Тип підключення: дротове
- Підтримка стандартів карт/брелоків: EM-Marine / HID
- Робоча частота: 125кГц
- (protection-key.com.ua) Дальність зчитування: 8см
- Інтерфейси: Wiegand / Dallas Touch Memory / RS-232
- Живлення: DC 4.75-16V
- Струм споживання в режимі очікування: 30mA
- Макс. струм споживання: 50mA
- Робоча температура: від -35°C до + 60°C
- Матеріал корпусу: пластик ABS
- Розміри: (protection-key.com.ua) 80x45x12.5мм

3.3 План впровадження системи та рекомендації щодо подальшої експлуатації

Для успішного впровадження системи контролю доступу (СКУД) та забезпечення її надійної та ефективної роботи, необхідно виконати ряд кроків. Нижче наведено детальний план впровадження системи та рекомендації щодо подальшої експлуатації.

Підключення елементів системи:

- Турнікет Класик-Елегант-СМ:
    1. Підключити електричний живлення до турнікету від джерела постійного струму (наприклад, 12 В);
    2. Підключити мережевий контролер NDC F18IP до турнікету за допомогою кабелю Ethernet;
    3. Підключити зчитувач карток U-Prox mini до мережевого контролера NDC F18IP за допомогою дротів або кабелю.
- Магнітний замок SEVEN ML-7726:

1. Підключити магнітний замок до зчитувача карток у відповідному приміщенні (ТД2-ТД9);
2. Забезпечити живлення магнітного замка з відповідного джерела постійного струму (наприклад, 12 В);
3. З'єднати контакти магнітного замка з вихідними контактами зчитувача карток.

- Сервер FRAY S3-FSSDK4-H та АРМ «Оріон ПРО»:
    1. Підключити сервер до мережі за допомогою кабелю Ethernet;
    2. Встановити та налаштувати програмне забезпечення АРМ «Оріон ПРО» на сервері.

Розміщення компонентів у приміщеннях:

- ТД1: Вхід до будівлі - розмістити турнікет Класик-Елегант-СМ з мережевим контролером NDC F18IP;
- ТД2-ТД9: Відповідні приміщення - розмістити магнітний замок та зчитувач карток.

Напруга та інші параметри:

- Для живлення турнікету, магнітного замка та зчитувача карток, використовуйте джерело постійного струму з напругою, вказаною у виробничій документації кожного компонента;
- Забезпечте належний захист системи від перенапруги, перепадів напруги та інших електричних перешкод;
- Використовуйте захисні пристрої, такі як стабілізатори напруги або UPS (несперебний джерело живлення), для забезпечення надійності та стабільності електропостачання системи.

Пошагова інструкція монтажу:

1. Перевірте наявність всіх необхідних компонентів та інструментів.
2. Визначте місця розташування турнікету, магнітного замка, зчитувачів карток та сервера згідно зі специфікацією.
3. Завершіть підключення живлення до кожного компонента відповідно до вимог виробників.

4. Забезпечте заземлення всіх електричних компонентів для забезпечення електричної безпеки.
5. Підключіть мережевий контролер та зчитувач карток до турнікету за допомогою кабелю Ethernet.
6. Підключіть зчитувач карток до магнітного замка за допомогою дротів або кабелю.
7. Перевірте правильність підключення всіх компонентів та забезпечте надійну фіксацію кабелів.
8. Підключіть сервер до мережі та встановіть необхідне програмне забезпечення.
9. Перевірте налаштування системи та забезпечте коректну роботу всіх компонентів.
10. Проведіть тестування системи, включаючи перевірку доступу та реакції на зчитування карток.

Рекомендації для підтримки працездатності системи:

- Періодично перевіряйте стан живлення та стабільність напруги у системі.
- Регулярно очищуйте зчитувачі карток та перевіряйте їх на наявність пошкоджень.
- Заплануйте регулярне технічне обслуговування системи, включаючи перевірку заземлення, перевірку роботи магнітних замків та перевірку стану кабелів і з'єднань.
- Забезпечте резервне копіювання даних, що зберігаються на сервері, та регулярно оновлюйте програмне забезпечення.

Після успішного впровадження системи контролю доступу та дотримання рекомендацій щодо подальшої експлуатації, буде забезпечено безпеку та контроль доступу до відповідних приміщень, що сприятиме покращенню загальної ефективності та безпеки організації.

3.4 Система тривожної сигналізації

Система тривожної сигналізації є невід'ємною складовою частиною проектування системи контролю доступу для школи 106. Її головною метою є оперативне виявлення та повідомлення про надзвичайні ситуації або аварійні стани, що можуть виникати у шкільних приміщеннях. Це дозволяє забезпечити безпеку учнів, вчителів та персоналу школи та ефективно керувати потенційними небезпеками.

Система тривожної сигналізації включає в себе декілька складових, які інтегруються з системою контролю доступу та іншими системами безпеки школи. Основні елементи системи тривожної сигналізації включають:

Датчики тривоги, розташовані у різних зонах шкільних приміщень, які здатні виявляти різні типи небезпек, такі як пожежа, втеча газу, проникнення в неавторизовані зони тощо. Ці датчики постійно моніторять навколишнє середовище та виявляють будь-які аномалії або небезпеки.

Централізована система керування забезпечує збір, обробку та аналіз інформації з датчиків тривоги. Вона оперативно реагує на спрацювання тривожних сигналів і забезпечує передачу відповідних повідомлень операторам безпеки та відповідним службам.

Система сповіщення включає звукові сигнали, світлові сигнали, інформаційні панелі та повідомлення на мобільні пристрої, які активуються після спрацювання тривожних сигналів. Це дозволяє інформувати учнів, вчителів та персонал школи про надзвичайну ситуацію та надавати вказівки щодо поведінки.

Інтеграція з системою контролю доступу: Система тривожної сигналізації інтегрується з системою контролю доступу, щоб автоматично активувати режими безпеки в разі надзвичайних ситуацій. Наприклад, у разі пожежі або евакуації, система контролю доступу може автоматично розблокувати всі двері для швидкого виходу.

Резервне живлення: Система тривожної сигналізації також має резервне живлення, що забезпечує її безперебійну роботу навіть у разі відключення основного джерела електропостачання.

Ці складові системи тривожної сигналізації були уважно вибрані, згідно з вимогами проекту для школи 106. Вони спроектовані для забезпечення надійної та ефективної роботи системи тривожної сигналізації та максимальної безпеки всіх присутніх у шкільних приміщеннях.

3.5 Висновки за розділом

Загальною метою розділу 3 було розроблення проектного рішення для системи контролю доступу в школі №106. Цей розділ включав в себе вибір необхідних компонентів, план розташування, розгляд питань електропостачання та надання рекомендацій щодо подальшої експлуатації.

Було проведено дослідження та визначено основні виклики, які передували розробці системи контролю доступу для школи №106. Були визначені необхідні компоненти для системи контролю доступу, такі як турнікет Класик-Елегант-СМ, мережевий контролер NDC F18IP (U-Prox IP400), зчитувач U-Prox mini, замок електромагнітний SEVEN ML-7726, сервер FRAY S3-FSSDK4-H та АРМ «Оріон ПРО». Було розроблено план розташування компонентів системи в різних приміщеннях школи. Залежно від функціонального призначення кожного приміщення, були встановлені відповідні елементи контролю доступу, замки та зчитувачі карток. Для забезпечення електропостачання системи було розглянуто варіанти підключення та живлення кожного компонента. З'ясовано, що для ефективної роботи системи необхідне стабільне живлення напругою 12 В. Були надані рекомендації щодо подальшої експлуатації системи контролю доступу. Вони включали питання щодо регулярної перевірки та технічного обслуговування компонентів, збереження резервних копій даних, а також підготовку персоналу до роботи з системою.

Результатом виконання розділу 3 є детально розроблене проектне рішення для системи контролю доступу, яке може бути використане при подальшій реалізації проекту.

ВИСНОВОК

В результаті виконання кваліфікаційної бакалаврської роботи була розроблена проектна реалізація системи контролю доступу в школі №106. Цей проект має велике значення, оскільки надійна система контролю доступу є важливим аспектом забезпечення безпеки учнів, персоналу та майна школи.

У процесі виконання роботи були вивчені потреби та вимоги школи, проведений аналіз різних компонентів системи контролю доступу та їх вибір на основі критеріїв ефективності, надійності та відповідності вимогам. Було розроблено оптимальну конфігурацію системи, визначено розміщення обладнання та з'ясовано особливості підключення.

В процесі реалізації проекту було враховано електропостачання та забезпечення необхідного напруги для роботи системи. Також були вирішені питання з прокладкою кабелів, монтажем пристроїв та налаштуванням програмного забезпечення.

Отримані результати демонструють, що розроблена система контролю доступу відповідає вимогам школи та дозволяє ефективно керувати доступом до приміщень. Ця система забезпечує безпеку, упорядкування та зручність в управлінні доступом до різних зон школи.

Завдяки проведеному аналізу, проектуванню та реалізації системи контролю доступу, школа №106 отримала важливий інструмент для забезпечення безпеки та ефективної організації роботи. Дана система є потужним інструментом управління доступом, який дозволяє забезпечити високий рівень безпеки та зручності в управлінні приміщеннями школи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ГОСТ Р 51241-2008. «Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний».
2. ГОСТ Р 54831-2011 Системы контроля и управления доступом. Устройства преграждающие управляемые. Общие технические требования. Методы испытаний (ru.wikipedia.org). (ru.wikipedia.org) – М. : Стандартинформ, 2012. – 16 с
3. Царьов Р.Ю. Біометричні технології: навч. посіб. для вищих навчальних закладів / Р.Ю. Царьов, Т. М. Лемеха. – Одеса: ОНАЗ ім. (repo.knmu.edu.ua) О.С. Попова, 2016. – 140 с.: іл.
4. Бройдо В.Л. Вычислительные системы, сети и телекоммуникации/В.Л. Бройдо, Спб.: Питер, 2011. – 560 с.
5. Ворона В.А. Системы контроля и управления доступом / В. А. Ворона, В. А. Тихонов. — М.: Горячая линия–Телеком. — 2010. — Т. 272.
6. Колбин Р.В. Глобальные и локальные сети. Создание, настройка и использование (+ CD)/Р.В. Колбин, М.: Бином, 2012 – 278 с.
7. Домарев В. В. Безопасность информационных технологий. Системный подход – К.: ООО ТИД Диа Софт, 2004. – 992 с.
8. Сердюк В.А. Организация и технологии защиты информации. Обнаружение и предотвращение информационных атак в автоматизированных системах предприятий/ В.А. Сердюк, М.: Высшая Школа Экономики (Государственный Университет), (ela.kpi.ua) 2013 – 576 с.
9. Олифер, В.Г. Основы сетей передачи данных Интернет–университет информационных технологий / В. Г. Олифер, Н. А. Олифер, 2016 –960 с.
10. Не типичные функции СКУД URL: http://www.secuteck.ru/articles2/sys_ogr_dost/netipichnye-funktsii-skud/

11. Система контроля и управления доступом. Принцип действия [Электронный ресурс]. – Режим доступа: http://www.intersyst.ru/solutions/165/460/свободный.
12. Обзор возможностей СКУД [Электронный ресурс]. – Режим доступу: (ela.kpi.ua) http://www.sistema-dostupa.ru/i03.htm/вільний.