

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект програмно-апаратного комплексу системи контролю і управління доступом навчальної лабораторії»

Виконав: студент 4-го курсу групи КБ-20-1
спеціальності 125 «Кібербезпека»

 Андрій ФЕРЕНЗ
Керівник: Доцент кафедри КІ та КБ, к.т.н., доцент

 Володимир КОТЕНКО

Рецензент: Старший викладач кафедри КН

 Руслан ПЕТРОСЯН

Житомир – 2024

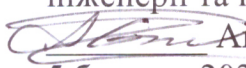
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної

інженерії та кібербезпеки

 Андрій Єфіменко

5 березня 2024 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Ференз Андрій Русланович

Тема роботи: «Проект програмно-апаратного комплексу системи контролю і управління доступом навчальної лабораторії»

затверджена Наказом університету від 5 березня 2024 р. № 98

Термін здачі студентом закінченої роботи 9 червня 2024 р.

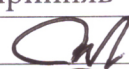
Вихідні дані роботи:

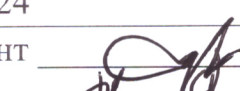
Об'єктом дослідження є системи контролю і управління доступом, їх апаратна та програмна складові. Предметом дослідження є розробка макету стенда програмно-апаратного комплексу системи контролю і управління доступом навчальної лабораторії.

Обладнання та програмне забезпечення:

1. BigBrother (v. 1.5.0.21)
2. Мережевий модуль контролю доступу iBC-01
3. Зчитувач PR-01 (B)
4. Електромагнітний замок KRF-200
5. Безперебійний блок живлення серії «ББП 20»
6. Конвертер USB - RS-485
7. Кнопка виходу накладна ART-805
8. Датчик стану дверей (геркон)

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

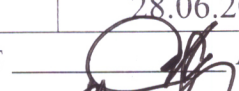
Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Котенко В.М.	05.03.2024	05.03.2024 
2	Котенко В.М.	05.03.2024	05.03.2024 
3	Котенко В.М.	05.03.2024	05.03.2024 

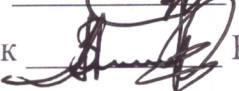
Студент  Андрій ФЕРЕНЗ

Керівник  Володимир КОТЕНКО

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	05.03.2024	Виконано
2	Розробка плану роботи	11.03.2024 - 15.03.2024	Виконано
3	Пошук інформації щодо понять СКУД та їх компонентів	18.03.2024 - 25.03.2024	Виконано
4	Аналіз технічних характеристик та можливостей пристроїв	01.04.2024 - 10.04.2024	Виконано
5	Розробка структурної схеми	12.04.2024 - 18.04.2024	Виконано
6	Розробка функціональної схеми	19.04.2024 - 25.04.2024	Виконано
7	Побудова макету стенду	29.04.2024 - 14.05.2024	Виконано
8	Встановлення та налаштування ПЗ BigBrother	16.05.2024 - 25.05.2024	Виконано
9	Проведення експериментальних досліджень для перевірки працездатності стенду	26.05.2024 - 05.06.2024	Виконано
10	Написання пояснювальної записки	06.06.2024 - 16.06.2024	
11	Отримання відгуку та рецензії	17.06.2024	Виконано
12	Підготовка презентації	18.06.2024 - 22.06.2024	Виконано
13	Захист	28.06.2024	

Студент  Андрій ФЕРЕНЗ

Керівник  Володимир КОТЕНКО

АНОТАЦІЯ

Кваліфікаційна робота містить опис проектування програмно-апаратного комплексу системи контролю і управління доступом навчальної лабораторії.

Пояснювальна записка складається з вступу, трьох розділів, висновків та списку використаної літератури. Текстова частина викладена на 80 сторінках друкованого тексту. Список використаних джерел містить 25 найменувань і займає 2 сторінки. В роботі наведено 63 рисунки та 6 таблиць. Загальний обсяг роботи 86 сторінок.

Метою кваліфікаційної роботи є розробка програмно-апаратного комплексу системи контролю і управління доступом навчальної лабораторії.

Розглянуто особливості систем контролю та управління доступом, їх компоненти та функції.

Визначені та проаналізовані технічні характеристики складових пристроїв та на їх основі побудовані структурна та функціональна електрична схеми.

На основі дослідженого матеріалу було реалізовано макет стенда системи контролю і управління доступом навчальної лабораторії. Протестовано його за допомогою створення користувача системи та експериментального відтворення інцидентів. До розробленого макета стенда було надано рекомендації по застосуванню в межах навчального закладу.

КЛЮЧОВІ СЛОВА: КОНТРОЛЬ ДОСТУПУ, МЕРЕЖЕВИЙ КОНТРОЛЕР, ЕЛЕКТРОЗАМОК, ЗЧИТУВАЧ, СТРУКТУРНА ТА ФУНКЦІОНАЛЬНА СХЕМИ.

					ККІКБ.КР.Б – 125 – 19 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Проект програмно-апаратного комплексу системи контролю і управління доступом навчаль- ної лабораторії	Літ.	Арк.	Аркушів
Розроб.		Ференз А.Р.		25.06				
Керівник		Котенко В.М.		25.06			4	86
Реценз.		Петросян Р.В.		25.06		ФІКТ, Гр. КБ-20-1		
Н. контр.		Котенко В.М.		25.06				
Затверд.		Єфіменко А.А.		26.06				

ANNOTATION

The qualification work contains a description of the design of the hardware and software complex of the educational laboratory access control and management system.

The explanatory note consists of an introduction, three chapters, conclusions and a list of references. The main text is laid out on 80 pages of printed text. The list of used sources contains 25 names and occupies 2 pages. The work contains 63 images and 6 tables. The total volume of work is 86 pages.

The purpose of the qualification work is the development of a software-hardware complex of the system of control and management of access to the educational laboratory.

Features of access control and management systems, their components and functions are considered.

The technical characteristics of the component devices were determined and analyzed, and structural and functional electrical schemes were built on their basis.

On the basis of the researched material, a mock-up of the stand of the educational laboratory access control and management system was implemented. It was tested by creating a system user and experimentally creating incidents. Recommendations for application within the educational institution were provided for the developed layout of the stand.

КЛЮЧОВІ СЛОВА: ACCESS CONTROL, NETWORK CONTROLLER, ELECTRIC LOCK, READER, STRUCTURAL AND FUNCTIONAL SCHEMES.

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		5

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1 АНАЛІЗ ФУНКЦІОНАЛЬНИХ МОЖЛИВОСТЕЙ СУЧАСНИХ СИСТЕМ КОНТРОЛЮ І УПРАВЛІННЯ ДОСТУПОМ ТА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ РОБОТИ З НИМИ	9
1.1. Актуальність теми курсової роботи	9
1.2. Поняття систем контролю і управління доступом та їх компоненти	10
1.3. Аналіз існуючих систем контролю і управління доступом.....	28
1.4. Аналіз вимог до програмно-апаратного комплексу	33
РОЗДІЛ 2 РОЗРОБКА СТРУКТУРНОЇ ТА ФУНКЦІОНАЛЬНОЇ СХЕМИ ПРОГРАМНО-АПАРATНОГО КОМПЛЕКСУ СИСТЕМИ КОНТРОЛЮ І УПРАВЛІННЯ ДОСТУПОМ НАВЧАЛЬНОЇ ЛАБОРАТОРІЇ	36
2.1 Аналіз функціональних можливостей і технічні характеристики елементів комплексу системи контролю і управління доступом	36
2.2 Аналіз функціональних можливостей програмного забезпечення для комплексу системи контролю і управління доступом	48
2.3 Розробка структурної схеми комплексу системи контролю і управління доступом	53
2.4 Аналіз функціонального призначення портів складових елементів системи та розробка структурної схеми контролю і управління доступом	55
РОЗДІЛ 3 РЕЗУЛЬТАТИ ЕКСПЕРИМЕНТАЛЬНИХ ДОСЛІДЖЕНЬ ПРОГРАМНО-АПАРATНОГО КОМПЛЕКСУ СИСТЕМИ КОНТРОЛЮ І УПРАВЛІННЯ ДОСТУПОМ	64
3.1 Опис макету стенда програмно-апаратного комплексу системи контролю і управління доступом навчальної лабораторії.....	64
3.2 Встановлення і налаштування програмного забезпечення BigBrother та проведення експериментальних досліджень по роботі з ним	70
3.3 Рекомендації по застосуванню розробленої СКУД.....	81
ВИСНОВКИ.....	83
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ	85

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

СКУД – система контролю та управління доступом

ПК – персональний комп'ютер

ПЗ – програмне забезпечення

БД – база даних

RFID – radio frequency identification (радіочастотна ідентифікація)

UPS – uninterruptable Power Supply (джерело безперебійного живлення)

ББЖ – блок безперебійного живлення

АКБ – акумуляторна кислотна батарея

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		7

ВСТУП

Актуальність теми: Сучасний світ є дуже динамічним і постійно розвивається. Це стосується не лише економічних та соціальних сфер, а й сфери безпеки. Зростаючі загрози, такі як тероризм, злочинність, техногенні катастрофи, вимагають від суспільства вжиття нових заходів для захисту життя і майна людей.

Одним із найважливіших напрямків у забезпеченні безпеки є застосування сучасних технічних засобів. Системи контролю та управління доступом є ефективними інструментами, які дозволяють своєчасно виявляти та попереджати загрози.

Метою кваліфікаційної роботи є розробка програмно-апаратного комплексу системи контролю і управління доступом навчальної лабораторії.

Визначена мета обумовлює наступні завдання:

- Аналіз систем контролю та управління доступом, їх компонентів та функцій;
- Визначення технічних характеристик складових пристроїв та побудова структурної та функціональної схем;
- Реалізація макету стенда СКУД для навчальної лабораторії.

Об'єктом дослідження є системи контролю і управління доступом, їх апаратна та програмна складові.

Предметом дослідження є розробка макету стенда програмно-апаратного комплексу системи контролю і управління доступом навчальної лабораторії.

У процесі виконання кваліфікаційної роботи було розроблено проєкт програмно-апаратного комплексу системи контролю і управління доступом навчальної лабораторії. За створеними структурною та електричною функціональною схемами було зібрано макет стенду системи.

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		8

РОЗДІЛ 1 АНАЛІЗ ФУНКЦІОНАЛЬНИХ МОЖЛИВОСТЕЙ СУЧАСНИХ СИСТЕМ КОНТРОЛЮ І УПРАВЛІННЯ ДОСТУПОМ ТА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ РОБОТИ З НИМИ

1.1. Актуальність теми курсової роботи

Розробка програмно-апаратного комплексу для системи контролю і управління доступом на прикладі системи для навчальної лабораторії відповідає актуальним викликам і вимогам сучасного сектору безпеки у багатьох сферах життя людини та освіти зокрема.

З роками кількість цінного обладнання та інформації на підприємствах та в навчальних установах тільки зростає, саме тому зростає і потреба у ефективних системах контролю доступу, що будуть запобігати крадіжкам, несанкціонованому доступу на об'єкт та псуванню майна. Значним фактором також стало забезпечення безпеки персоналу та студентів, що у навчальних закладах по всьому світу зараз є одним із пріоритетних завдань.

Автоматизовані системи контролю і управління доступом, хоча й вимагають початкових інвестицій, можуть значно знизити витрати на утримання навчальних лабораторій у довгостроковій перспективі. Вони зменшують потребу в постійному персоналі для контролю доступу, знижують ризики втрат обладнання та дозволяють ефективніше використовувати наявні ресурси. Це сприяє економії коштів та підвищенню рентабельності навчального процесу.

Що стосується специфіки впровадження СКУД у навчальних закладах, то вони можуть надавати можливість персоналізації навчального процесу, що дозволяє враховувати індивідуальні потреби та особливості кожного студента. Наприклад, система може надавати доступ до певних ресурсів або лабораторного обладнання тільки тим студентам, які вже пройшли відповідні курси або мають необхідні знання та навички. Це сприяє підвищенню якості освіти та більш ефективному використанню навчальних ресурсів.

Студентам, що вивчають дисципліни, такі як системи технічного захисту інформації стане доступна можливість працювати на реальному обладнанні та на

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		9

практиці розглядати можливості систем контролю і управління доступом. Практична робота по налаштуванню СКУД та їх компонентів, як наприклад програмування RFID-міток та Proximity карток буде корисною та цікавою для вивчення студентами, а використання програмно-апаратного комплексу для контролю доступу дозволяє студентам ознайомитися з принципами роботи автоматизованих систем, інтеграції апаратних та програмних компонентів, а також з концепціями інформаційної безпеки. Це сприяє підвищенню їхньої компетентності та готовності до професійної діяльності у майбутньому.

Побудова навчального стенду колмплексу системи управління і контролю доступу дозволить популяризувати напрямох технічного захисту інформації серед студентів та продемонструє їм специфіку роботи з обладнанням. Стенд може використовуватися під час проведення лабораторних і практичних робіт з низки дисциплін та наочно показувати учням результати їх роботи.

Варто зазначити, що велика кількість існуючих систем контролю і управління доступом, що використовуються по цей день є застарілими та вважаються негнучкими і складними в управлінні.

З огляду на ці недоліки, розробка програмно-апаратного комплексу, що буде надавати усі переваги використання систем контролю і управління доступом, а також буде автоматизувати процес контролю, буде легко налаштовуватись та розширюватись відповідно до потреб закладу і буде інтегрований з іншими пристроями за засобами системи безпеки та управління є актуальним завданням для багатьох організацій.

1.2. Поняття систем контролю і управління доступом та їх компоненти

Система контролю і управління доступом (СКУД) — це комплекс технічних засобів та програмного забезпечення, призначений для обмеження чи регулювання фізичного доступу до об'єкта чи території. Головна мета системи полягає в забезпеченні безпеки, контролі над рухом людей або транспортних засобів, а також у визначенні прав доступу для окремих користувачів чи груп користувачів.

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		10

Вони застосовуються в різних областях, включаючи бізнес-приміщення, громадські будівлі, банки, виробничі об'єкти та інші місця, де контроль доступу є ключовим елементом забезпечення безпеки і конфіденційності.

Система контролю доступу (СКУД) включає різноманітні компоненти, які спільно працюють для забезпечення ефективного контролю над фізичним доступом до об'єкта чи території. До основних компонентів СКУД належать:

1. Ідентифікатори — це унікальний код або набір даних, що дозволяє однозначно ідентифікувати кожного користувача системи. Він може використовуватися для надання або обмеження доступу до певних приміщень або ресурсів.

Кожен суб'єкт інформаційної безпеки, що повинен мати доступ до приміщень, які знаходяться під захистом та наглядом систем контролю і управління доступом, мусить мати індивідуальний ідентифікатор особистості або посади.

Для ідентифікації користувачів у системі контролю доступу використовуються наступних методи [5]:

Парольна ідентифікація - це метод контролю доступу, при якому користувач вводить унікальний код, який відомий лише йому, щоб підтвердити свою ідентичність і отримати доступ до системи чи ресурсів. Цей код може бути числовим, буквенним або комбінацією обох, і найчастіше введений разом із ім'ям користувача. Цей тип ідентифікації є доволі простим у використанні, адже як паролі часто використовуються комбінації, що легко ввести та запам'ятати, парольний захист також легко змінювати та адмініструвати. З недоліків слабкість перед атаками, особливо при використанні слабких паролів.

Біометрична ідентифікація - це метод, який використовує унікальні фізичні характеристики особи для визначення її ідентичності. До таких характеристик входять відбитки пальців, розпізнавання обличчя, розпізнавання голосу, структура розмаїття радужки, геометрія долоні та інші біологічні аспекти. Біометричні дані зазвичай вимірюються та зберігаються для подальшого порівняння при подальших спробах ідентифікації. Цей спосіб забезпечує високий рівень безпеки, адже біометричні дані унікальні для кожної особи, також на відміну від парольного варіанту, не потрібно пам'ятати пароль чи носити якийсь предмет, що можна загубити. Проте

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		11

такі системи є дуже дороговартісними, тому мають застосовуватися у місцях де такий рівень захисту є необхідним.



Рис.1.1 Різновиди біометричної ідентифікації

Апаратна ідентифікація - це метод контролю доступу, який використовує фізичні об'єкти чи пристрої для підтвердження ідентичності користувача. Це може бути виконано за допомогою електронних ключів, RFID-карт, USB-токенів, смарт-карт або інших фізичних засобів, що надають доступ. Для використання цього методу, користувач має мати фізичний об'єкт або пристрій, який може бути використаний для ідентифікації та автентифікації. Використання фізичних пристроїв чи ключів забезпечує високий рівень безпеки, не потрібно запам'ятовувати пароль, а також у разі втрати чи крадіжки апаратний ідентифікатор можна відключити від системи. З недоліків - виробництво та використання апаратних ідентифікаторів може бути дорогим.

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		12



Рис.1.2 Різновиди апаратних ідентифікаторів (RFID-мітки, Proximity-картки та Touch Memory ключі)

Найпоширенішим типом ідентифікаторів користувачів у СКУД є картки, яких є 2 типи, а саме: контактні картки, що мають металеві контакти, які зчитуються зчитувачем, коли карта вставляється в нього та безконтактні, у яких є вбудована мікросхема RFID, яка може зчитуватися зчитувачем на невеликій відстані. Безконтактні картки стають все більш популярними, оскільки їх не потрібно вставляти в зчитувач, що робить їх більш зручними у використанні.

Принцип їх роботи доволі простий:

1. Користувач пред'являє карту, що зберігає у собі унікальний ідентифікатор користувача, зчитувачу.
2. Зчитувач генерує радіочастотне поле, яке активує чіп на карті, коли вона знаходиться в його зоні дії (в середньому до декількох сантиметрів).
3. Передача даних відбувається бездротово: чіп на карті передає свій унікальний ідентифікаційний код зчитувачу.
4. Зчитувач у свою чергу передає отримані дані на контролер системи.
5. Контролер перевіряє ідентифікатор у базі даних і приймає рішення про надання або відмову у доступі.

Картки стали такими популярними через ряд переваг. Вони дуже зручні у використанні, користувачу достатньо всього лише піднести картку до зчитувача. Процес ідентифікації здійснюється швидко і точно. Ще однією перевагою є їх дешевизна та простота програмування для досвідченого адміністратора. Картки є доволі міцними та не мають рухомих частин, через що рідко ламаються, а також можуть працювати довгий час. Картки можуть бути персоналізовані з фотографією та ім'ям користувача, що робить їх більш безпечними.

2. Зчитувачі — це пристрої, що є ключовими компонентами, які використовуються для зчитування ідентифікаторів користувачів, які мають право доступу до об'єкту, та передачі цієї інформації до контролера для подальшої обробки.

Існують різноманітні моделі зчитувачів, які різняться між собою за способом ідентифікації, підтримуваними стандартами читання даних та за типом підключення:

– Зчитувачі карток – використовуються для зчитування інформації з RFID-карток, або контактних карток. У випадку безконтактних карток, зчитувачі випромінюють електромагнітне поле, здатні через катушку індуктивності заряджати конденсатор, який у свою чергу уже посиляє сигнал електронній мікросхемі, що знаходиться всередині картки. За частотою сигналу вони поділяються на 3 види:

1. Низькочастотні (LF) – працюють на частоті 125-134 кГц. Використовуються для доступу на коротких відстанях, зазвичай 2-5 см.

2. Високочастотні (HF) – працюють на частоті 13.56 МГц. Забезпечують зчитування на більших відстанях, а саме: за стандартом ISO 14443 це від 5 до 15 см, а за стандартом ISO 15693 – від 10см до 1м. При чому зі збільшенням дальності значно зменшується швидкість передачі даних (106-848 кбіт/с проти 1.6-26 кбіт/с відповідно)

3. Ультрависокочастотні (UHF) – працюють на частотах до 900 МГц. Забезпечують найбільшу зону зчитування (до 20 м), що дозволяє зручно використовувати їх з шлагбаумами для парковок і автопроездів тощо.

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		14



Рис.1.3 Безконтактний зчитувач RFID-карток

– Біометричні зчитувачі – працюють за принципом біометричної ідентифікації, до них відносяться сканери відбитків пальців, розпізнавання обличчя, райдужної оболонки ока, голосу або вен. Такі зчитувачі перетворюють отримані дані певних тілесних характеристик на цифровий код, який потім надходить до контролера або терміналу і в базу даних програмного забезпечення. Біометричні ідентифікатори зберігаються у БД як унікальний цифровий код, що запобігає можливості відновити папілярний малюнок відбитка пальця викравши його з бази. Завдяки цій технології не порушується закон про захист персональних даних. Використання таких систем має безліч переваг, наприклад, унеможливлення втрати ідентифікатора, що може призвести до того, що недопущена особа, знайшовши карту чи мітку отримає доступ до забороненої зони, або виключить можливість відмітки певного користувача без його фізичної присутності (у випадку якщо на робочому місці ведеться облік часу). Проте оскільки такі системи є дороговартісними, вони застосовуються лише у випадках коли є необхідність у збільшеному рівні безпеки та контролю.

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		15



Рис.1.4 Зчитувач відбитків пальців

– Клавіатури – пристрої, що базуються на парольній ідентифікації та є одними з найпростіших та найекономічніших рішень як для підприємств і складських приміщень так і для багатоповерхових будинків та офісів.

Окрім звичайних механічних та сенсорних клавіатур, можливі також поєднання їх з іншими зчитувачами, RFID чи біометричними, що забезпечує багатофакторну аутентифікацію.



Рис.1.5 Зчитувач відбитку пальця з клавіатурою

До переваг цих типів зчитувачів можна віднести найбільшу простоту та через це і високу надійність та довговічність. Вони легко програмуються на використання різних кодів для різних користувачів, що робить їх ідеальними для систем з багатьма користувачами. Також клавіатури зазвичай є дешевшими за інші види зчитувачів. У сенсорних клавіатурах можливе налаштування функції захисту від

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		16

підглядань шляхом випадкового порядку розташування чисел на сенсорній панелі для запобігання відстежуванню рухів пальців людини.

До недоліків можна віднести ризик крадіжки коду, що призведе до несанкціонованого доступу та забруднення чи механічні пошкодження, що призведуть до проблем зі зчитуванням натискань клавіш.

3. Контролери — це пристрої, що є основою абсолютно будь-якої системи контролю і управління доступом. Ці мікропроцесорні пристрої виконують ряд функцій, серед яких: обробляють інформацію зі зчитувачів та приймають рішення про надання або відмову в доступі, розмежовують доступ до різних зон об'єкта, шляхом управління виконавчими пристроями, також ці пристрої зберігають у собі бази даних усіх користувачів системи, а також журнали подій.

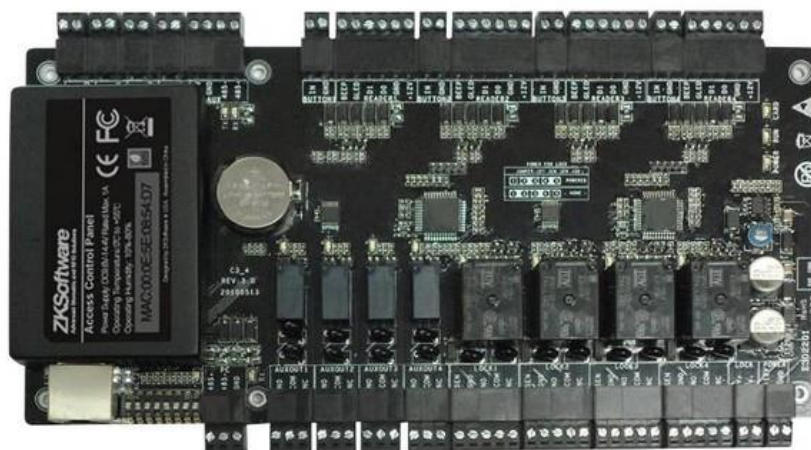


Рис.1.6 Приклад контролеру СКУД від ZKTeco

В залежності від типу контролера на нього можуть бути покладені різні завдання, через що їх функціонал може відрізнятися.

Першим типом є автономні контролери — це такі пристрої, що працюють повністю самостійно і не потребують підключення до мережі, тому його неможливо підключити до інших контролерів, так само як і до нього підключити зовнішні контролери не вийде. Через те, що такі пристрої працюють повністю автономно, за умови, що на об'єкті встановлено декілька таких контролерів, кожен з них доведеться налаштовувати окремо і вручну. Для цього потрібно буде переводити їх в режим програмування та додавати чи вилучати картки чи інші ідентифікатори.

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

Функціонал таких контролерів значно менший в порівнянні з мережевими – більшість з них не має функції керування за допомогою програмного забезпечення, яке встановлено на комп'ютері. Це призводить до того, що клієнт не може отримувати інформацію про кількість гостей, час у який вони прийшли чи вийшли та впливаючи з цього не має і можливості до проведення аналітичної роботи, до прикладу обрахунок часу, що конкретний користувач пробув на об'єкті, а також визначення часу пікових навантажень на конкретному проході.

Проте позитивних сторін автономних контролерів часто буває достатньо для більшості підприємств, щоб закрити очі на їх недоліки. Їх ціна, що значно менша ніж у мережесих контролерів, а також те, що системи з таким типом контролерів потребують мінімуму обладнання робить їх вибір недорогим і швидким рішенням для взяття під контроль точки доступу.

Вибір автономного контролера не тільки є дешевшою альтернативою, а й може бути об'єктивно кращим рішенням для низки споживачів з абсолютно різних сфер життя, адже за умови, що об'єкт має лише один-два виходи, встановлення складнішої дороговартісної системи може бути надлишковим. Ще одним значним плюсом, особливо в сучасних умовах є значно більша автономність – здатність працювати без постійного підключення до централізованої мережі робить їх надійними в умовах нестабільного інтернет-з'єднання чи взагалі при збою цієї мережі. При наявності резервних батарей спокійно функціонують при повній відсутності електропостачання.

Другим типом контролерів є мережеві – це такі контролери, що підключаються до мережі та до керуючого ПК, що дозволяє централізовано керувати системою контролю і управління доступом. В незалежності від їх кількості, легко об'єднуються у спільну мережу, зазвичай за допомогою стандартів Ethernet або RS-485.

Застосування мережесих контролерів дозволить створити СКУД будь-якого рівня складності та захищеності та підійде для будь-якого підприємства, від великих до малих, що мають потребу у збільшеному функціоналі, який надають дані пристрої.

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		18

На відміну від автономних контролерів, окрім своїх звичайних функцій, мережеві здатні збирати інформацію про користувачів, а також можуть нею оперувати, наприклад формувати звітність про присутність або відсутність працівників на їх робочих місцях, та кількість часу що вони там проводять (облік робочого часу). За допомогою мережевих контролерів можливо навіть визначати місцезнаходження співробітників у режимі реального часу, та відслідковувати їх пересування протягом робочого дня, чи певного відрізка часу.

Проте найбільшою перевагою даного виду контролерів є опція створення централізованого пункту управління доступом. Така можливість значно спрощує весь процес управління, оскільки всі налаштування, зміни прав доступу і моніторинг подій здійснюються через єдину панель керування. Адміністрування стає більш зручним, оскільки всі дані зберігаються на центральному сервері. Це дозволяє легко додавати, видаляти або змінювати права доступу користувачів, не потребуючи доступу до кожного контролера окремо.

Централізоване управління дозволяє швидше реагувати на інциденти безпеки. Адміністратори можуть миттєво блокувати доступ користувачів у разі підозрілих дій або загроз. Крім того, централізована система забезпечує кращий захист даних завдяки централізованому зберіганню і управлінню безпекою, наприклад така система надає більше можливостей для налаштування політик доступу, які включають в себе створення складних правил доступу, розкладів, обмежень за часом та датою, а також рівнів привілеїв для різних груп користувачів.

Основними плюсами для великих організацій є опція масштабування мережі. Це означає, що можна легко додавати нові точки доступу, не змінюючи існуючу інфраструктуру. Також варто відзначити, що централізована система дозволяє зберігати всі журнали подій в одному місці, що спрощує аналіз та створення звітів. Це корисно для проведення аудитів безпеки та розслідувань інцидентів. Додатково такі системи легко інтегруються з іншими, такими як системи відеоспостереження, пожежної сигналізації та системи управління будівлею (BMS).

Вирішальним фактором є й той факт, що для організацій, які потребують вищезазначеного функціоналу початкові витрати на впровадження централізованої

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

системи з мережевими контролерами можуть бути вищими, проте довгострокові експлуатаційні витрати часто знижуються за рахунок спрощеного управління, меншої кількості необхідного персоналу для адміністрування і зниження кількості помилок.

Варто відмітити і недоліки мережевих контролерів, до яких належить висока початкова вартість обладнання, програмного забезпечення та встановлення. Також для встановлення і налаштування мережі потрібно залучати кваліфікованих спеціалістів. У випадку мережевих збоїв чи втрати електроживлення система може втратити частину функціональності.

4. Виконавчі пристрої — це пристрої, мета яких забезпечення фізичної перешкоди, що обмежить доступ до контрольованого об'єкту. Вони здійснюють фізичне блокування та розблокування точок доступу (дверей, воріт, турнікетів) шляхом виконання команд контролерів, забезпечуючи реалізацію рішень про доступ.

Всі виконавчі пристрої можна розділити на дві типові групи: електрозамки та турнікети [6].

Електрозамок - це сучасний варіант замикаючого пристрою, особливістю якого є відсутність традиційної механічної серцевини як такої, або її повна або часткова (у гібридних замків) заміна на дію електромагнітної сили. Електрозамки включають різні типи пристроїв, які використовуються для блокування та розблокування дверей, воріт та інших точок доступу за допомогою електричних сигналів. Вони забезпечують безпеку та контроль доступу до приміщень і можуть мати різні механізми дії, проте для усіх них характерний один склад – це замикаюча складова (безпосередньо електронний замок) і ключі різного типу. Ключі можуть мати фізичну форму (RFID-картки, мітки, або у гібридних замках навіть звичні механічні ключі), або можуть бути замінені на дистанційне керування, включаючи можливість відкривати двері командами у телефоні чи централізованій панелі керування [8].

Основними типами є електромагнітні, електромеханічні та електроригельні замки.

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		20

Електромагнітні замки є популярним вибором у системах контролю управління доступом (СКУД) завдяки в першу чергу своїй простоті. Вони широко використовуються в різних сферах життя, не тільки на промислових об'єктах та підприємствах, а й у житлових комплексах.

Складаються вони з 2 основних частин: електромагніту, що встановлюється на дверній рамі та металевої пластини (якоря), що встановлюється на дверях. Коли електромагніт підключений до джерела живлення, він створює магнітне поле, яке притягує металеву пластину, утримуючи двері закритими. Коли живлення вимикається, магнітне поле зникає, і двері можуть бути відкриті.

Така особливість роботи магнітного замка має як переваги, так і недоліки, в залежності від ситуації. У разі відсутності електроживлення магнітний замок фактично перестає виконувати свою функцію, що є недоліком у випадках частих відключень електроенергії. Проте в умовах надзвичайних ситуацій, таких як пожежі, користувачі не залишаються замкненими всередині через раптову відсутність живлення замка. Це відбувається тому, що конструкція передбачає відкриття дверей при відсутності живлення магніту, на відміну від систем, що розраховані на відкривання за допомогою електроімпульсу. Таким чином, при відключенні живлення магніт перестає функціонувати і двері автоматично відкриваються, не залишаючи людей заблокованими у приміщенні.

Що до інших переваг замка, то це просте встановлення на поверхню дверної рами та дверей без складних монтажних робіт та забезпечення надійного утримання дверей закритими при наявності електроживлення.

Серед недоліків варто відмітити обмеження по застосуванню для місць з високими вимогами до фізичної безпеки, де потрібен механічний блокувальний механізм та посилений захист від вандалізму, а також необхідність резервного безперебійного джерела живлення (UPS) для гарантій постійної роботи в умовах вимкнення електрики.

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

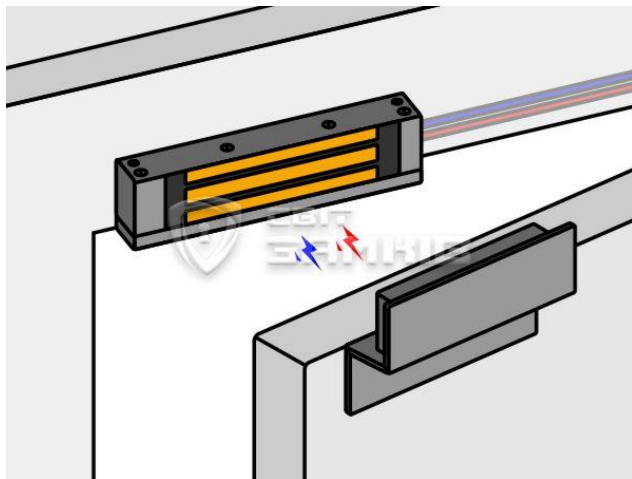


Рис.1.7 Приклад електромагнітного замка

Електромеханічні замки поєднують в собі принцип роботи механічного замка з електронним керуванням. В цілому, електрозамок майже не відрізняється від звичайного механічного. Слід зазначити, що електрозамки також можуть бути врізними або накладними, керуватися натискними або фіксованими ручками, а також відкриватися за допомогою фізичного ключа. Більшість таких пристроїв мають стандартні розміри та параметри, притаманні звичайним механічним замкам, такі як бексети, міжосьові відстані та розміри планок. Основною відмінністю є наявність додаткового способу керування.

Для функціонування електричної частини замка необхідно підключити джерело живлення, яке з іншого боку під'єднується до ідентифікатора. Такими пристроями можуть бути різноманітні компоненти системи контролю доступу, які взаємодіють з користувачем для забезпечення входу до приміщення: зчитувач магнітних карт, біометричний сенсор, кодонабірна клавіатура, брелок, кнопка або навіть дистанційне керування за допомогою смартфона. Процес відкривання або закривання замка відбувається внаслідок подачі або припинення електричного струму. За цією характеристикою електромеханічні замки поділяються на 3 типи [9]:

1. Нормально замкнені (fail-secure). Розблокування закритого замка відбувається при подачі електричного сигналу. При його відсутності – замок зачинений. Це ідеально підходить для зон із високими вимогами до безпеки, таких як серверні кімнати чи сейфи. Перевагами таких замків є їхня надійність у захисті від несанкціонованого доступу під час відключення живлення. Однак, їхній основний недолік

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

полягає у відсутності можливості екстреного виходу при виникненні аварійної ситуації, що може створювати загрозу для безпеки людей.

2. Нормально відімкнені(fail-safe). За наявності електричного сигналу замок залишається зачиненим, а при припиненні подачі – відкривається. Це забезпечує безпеку при евакуації, оскільки у випадку пожежі чи іншої надзвичайної ситуації замок автоматично відкривається, дозволяючи людям швидко залишити приміщення. Такі замки підходять для використання на аварійних виходах та інших зонах, де важливо забезпечити вільний доступ у надзвичайних ситуаціях.

3. Універсальний. Такі пристрої мають перемикач, за допомогою якого можна самостійно налаштувати потрібний режим роботи.

До електромеханічних замків можна віднести наступні типи:

Врізні замки. Аналогічно до звичайних механічних замків, електромеханічні замки можуть встановлюватися врізним методом у будь-які типи дверей, залежно від конкретної моделі. Окрім керування за допомогою електричного імпульсу, їх можна відкрити й механічно, використовуючи ключ. Блокування відбувається автоматично при простому зачиненні дверей. Розглянемо стандартний електромеханічний замок, принцип дії якого полягає в наступному: на електромагнітну котушку замка подається напруга, що приводить у дію фіксатор пружини, який втягує запірний ригель або язичок всередину корпусу замка, здійснюючи тим самим розблокування дверей. Після зачинення дверей механізм електромеханічного замка автоматично здійснює їх блокування.

Накладні замки. Метод їх монтування – накладний, з внутрішньої сторони дверей. Активуються вони зсередини зазвичай за допомогою вбудованої механічної кнопки, а ззовні за допомогою електричного імпульсу від пристрою керування або механічним ключем. Всі електромеханічні накладні замки мають всередині соленоїд, при подачі електричного струму на який, розблоковується фіксатор пружини. Вона в свою чергу втягує в корпус замка запірний ригель або язичок. Так відбувається відкривання. При зачиненні дверей механізм електромеханічного замка знову в автоматичному режимі здійснює його блокування. Деякі моделі мають можливість регулювання електромеханічного замку. Накладні електрозамки, що

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

встановлені на внутрішній стороні дверей із механічною кнопкою є оптимальним вибором для суцільних дверей. Ця кнопка може бути заблокована у натиснутому або відтиснутому стані за допомогою серцевини. Такий механізм дозволяє фіксувати замок у відчиненому положенні для вільного проходу або, навпаки, блокувати вихід зсередини.

Електрозащіпки. Їхнє встановлення передбачає заміну зворотніх планок, куди потрапляють язички звичайних механічних замків, на систему з блокуючою пелюсткою. Ця пелюстка електрозащіпки розблоковується при подачі електричного імпульсу і дозволяє відчинити двері без натиснення на ручку, достатньо просто потягнути або штовхнути їх. Тобто електрозащіпка блокує язичок замка і звільняє його при подачі сигналу, при цьому зовнішні ручки у дверей, на яких встановлений даний механізм, не повинні керувати язичком, а має бути глухими, тобто не повинні натискатись та механічно відчиняти двері. Для цієї цілі підійдуть також ручки-скоби. Встановлюються електрозащіпки здебільшого врізним методом в коробку металевих, дерев'яних та металопластикових дверей. Основним керуючим елементом є електромагнітна котушка всередині корпусу, яка блокує поворотний елемент - пелюстку. Крім того, деякі моделі електрозащіпок можуть мати додаткові функції та перемикачі, наприклад функцію механічної пам'яті (після короткочасної подачі струму защіпка залишається розблокованою до відкриття-закриття дверей, а надалі пристрій автоматично перейде в режим фіксації) та функція механічного розблокування, що реалізована за допомогою спеціального важеля на корпусі замка, який переводить защіпку в постійновідчинений режим, коли для проходу не потрібна подача напруги. Електричні защіпки, як і електромеханічні замки, можуть бути "нормально зачиненими" та "нормально відчиненими".

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

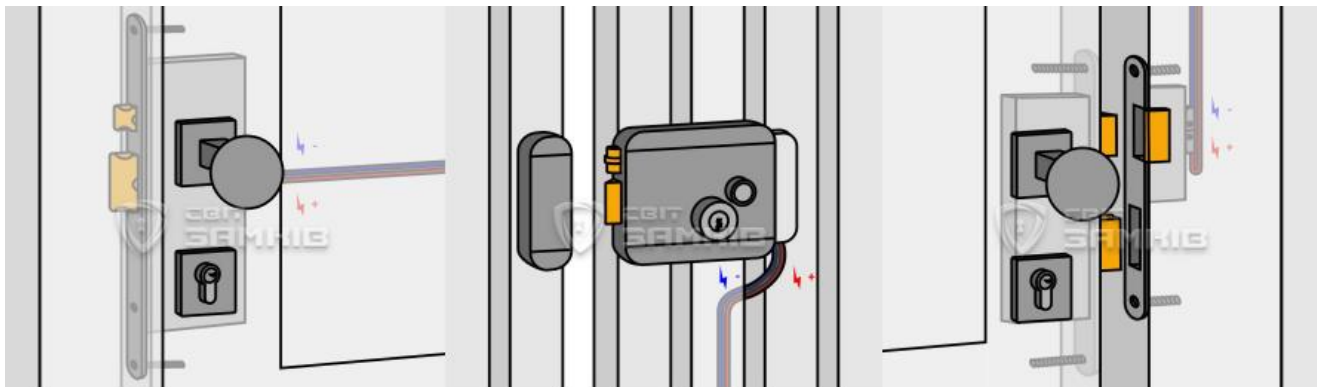


Рис.1.8 Різновиди електромеханічних замків (врізний, накладний та защіпка)

Електроригельні замки відрізняються від електромеханічних, але в обох випадках використовується схожа електромагнітна котушка. Ця котушка притягує або виштовхує ригель в залежності від типу замка. Більшість електроригельних замків «нормально відчинені», що означає, що при відсутності подачі струму вони залишаються у відкритому положенні. Щоб двері з таким замком були зачинені, потрібно постійно подавати напругу. Проте існують також “нормально зачинені” електроригельні замки. Їх можна розблокувати у разі відсутності електрики, завдяки отвору для встановлення звичайної серцевини, яка за допомогою ключа керує ригелем.

Зворотні планки електроригельних замків мають в собі звичайний магніт та вбудований геркон. Геркон - це електронний пристрій, що використовується для виявлення магнітних полів. Він складається з двох контактів, які замикаються або розмикаються в залежності від наявності магнітного поля, що знаходяться в герметичній скляній колбі. При закриванні дверей, коли замок наближується до зворотної планки, геркон реагує на магніт і висилає сигнал, що потрібно висунути ригель. Ця особливість відрізняє електроригельні замки від електромеханічних, де механічний язичок служить індикатором стану зачинених дверей і натягує пружину ригеля. В електроригельних замках цим індикатором є геркон під лицевою планкою, а природній магніт розташований під зворотною планкою.

Встановити такий тип замку можливо як і в саме полотно дверей, так і в дверну раму, що може бути корисним з огляду на спрощене протягування кабелів до нього.

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

Системи контролю доступу можуть виконувати різні функції:

Ідентифікація і аутентифікація — визначення особи або об'єкта, що намагається отримати доступ та перевірка, чи вказаний користувач має право на доступ, шляхом підтвердження ідентифікаційних даних, таких як картка, PIN-код, відбиток пальця тощо.

Розмежування доступу — визначення того, які права доступу має особа до певної зони, а також керування часом та розкладами доступу до конкретних об'єктів чи зон. Наприклад, працівник може мати право доступу до свого робочого кабінету, але не до серверної кімнати.

Фіксація часу приходу та догляду працівників — тобто, реєстрація того, коли працівники приходять на роботу та коли вони йдуть з роботи. Це може бути корисно для обліку робочого часу та контролю за відвідуваністю.

Сигналізація про несанкціонований доступ — тобто, попередження про те, що хтось намагається проникнути на об'єкт без дозволу.

Реєстрація та журналювання - фіксація всіх подій із системи, таких як входи, виходи, спроби неуспішного доступу, а також інші події, також зберігання історії подій для подальшого аналізу та вирішення спірних ситуацій.

Інтеграція з іншими системами безпеки – Синхронізація та автоматична взаємодія з системами відеоспостереження, системами пожежної та безпекової сигналізації для комплексного контролю об'єкта.

Система контролю і управління доступом (СКУД) забезпечує інтегровану роботу апаратних та програмних компонентів для ефективного контролю доступу до захищених зон. Взаємодія між компонентами починається з ідентифікації користувача, яка здійснюється за допомогою RFID-картки, брелока, біометричних даних (відбитки пальців, розпізнавання обличчя), або введенням PIN-коду на кодовій клавіатурі. Користувач підносить свій ідентифікатор до зчитувача, який зчитує унікальний код або біометричні дані та передає цю інформацію на контролер доступу.

Контролер доступу отримує зчитану інформацію та передає її на сервер авторизації через захищений канал зв'язку. Сервер авторизації звертається до бази да-

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

них, де зберігається інформація про права доступу кожного користувача. Якщо запит користувача відповідає заданим параметрам доступу (наприклад, дозволений час та зона доступу), сервер авторизації надсилає відповідний сигнал назад до контролера.

Після успішної авторизації контролер надсилає сигнал на механізм блокування (електромеханічний замок, турнікет, ворота), який розблоковується, дозволяючи користувачу увійти до захищеної зони. Якщо права доступу не підтверджені, система відмовляє у доступі, що може супроводжуватися звуковим або світловим сигналом, інформуючи користувача про відмову.

Усі події доступу (успішні та невдалі спроби) фіксуються в журналі подій, який зберігається на сервері. Цей журнал містить інформацію про час доступу, ідентифікатор користувача, зону доступу та результат авторизації. Оператори системи можуть у реальному часі моніторити події, переглядати історію доступу та генерувати звіти для аналізу безпеки.

СКУД може бути інтегрована з іншими системами безпеки, такими як відеоспостереження (CCTV) та системи сигналізації. Наприклад, при кожному використанні системи доступу може активуватися камера відеоспостереження для запису події. У випадку тривоги або пожежі система може автоматично розблокувати всі виходи для забезпечення безпечної евакуації. Системи управління будівлею (BMS) також можуть бути інтегровані з СКУД для оптимізації використання енергоресурсів, наприклад, включення освітлення або кондиціонування повітря лише при наявності людей у приміщенні.

Таким чином, СКУД забезпечує комплексний підхід до контролю доступу, інтегруючи різні технології та системи для підвищення загального рівня безпеки та ефективного управління доступом на об'єкті.

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

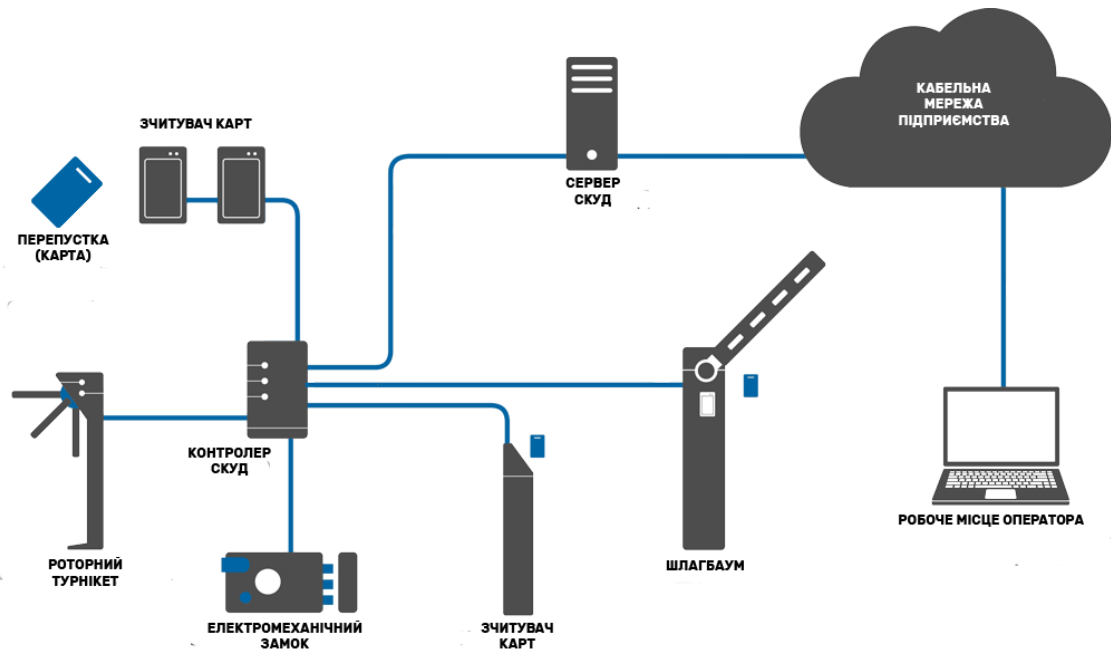


Рис.1.9 Узагальнена апаратна схема СКУД

1.3. Аналіз існуючих систем контролю і управління доступом

У сучасному світі питання безпеки стає все більш актуальним. Це стосується як житлових, так і комерційних об'єктів. Системи контролю та управління доступом (СКУД) є одним з ефективних інструментів для забезпечення безпеки.

На ринку представлено широкий спектр СКУД від різних компаній, кожна з яких пропонує свої унікальні рішення. У цьому розділі роботи буде проведено аналіз СКУД від таких відомих виробників, як HID Global, Honeywell, LenelS2, SALTO Systems та Suprema.

HID Global^[10] - це американська компанія, що спеціалізується на розробці та виробництві рішень для контролю доступу та ідентифікації, включаючи системи на основі магнітних карток, брелоків, біометрії та паролів. Її продукція використовується на різноманітних об'єктах, включаючи офісні будівлі, виробничі підприємства, державні установи, навчальні заклади та медичні заклади.

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		28



Рис.1.10 Продукція компанії HID Global

HID iCLASS SE - це бездротова система контролю доступу (СКУД), яка використовує RFID-мітки для аутентифікації користувачів. Вона є однією з найпопулярніших систем СКУД від HID Global завдяки своїй надійності, доступності та простоті використання.

Ця система дозволяє використання технології Seos, безпечні, універсальні та масштабовані смарт-картки, що використовують складні алгоритми шифрування для захисту даних користувача. Проте перевагою зчитувачів iCLASS SE є підтримка мультиформатної роботи, що дозволяє їм працювати з різними типами карток і брелоків. Оскільки картки з технологією Seos є дорожчими за звичайні проксі-міті-карти, підприємствам може бути вигідно обрати бюджетне рішення, що вдовольнить їх потреби. Також великим плюсом є можливість сумісної роботи з іншими системами контролю доступу та безпеки, що дозволяє інтегрувати її в існуючі інфраструктури. Підтримка відкритих стандартів забезпечує можливість використання різних пристроїв і програмного забезпечення.

Honeywell^[11] - це американська багатонаціональна корпорація, що займається розробкою та виробництвом широкого спектру продукції, включаючи СКУД які інтегруються з іншими системами безпеки, такими як відеоспостереження та сигналізація. Їх СКУД використовуються на об'єктах з високим рівнем безпеки, таких як банки, аеропорти та в'язниці.

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		29



Рис.1.11 Логотип компанії

Серед рішень цієї компанії варто відмітити WIN-PAK PRO Central Station - потужне програмне рішення, яке призначене для централізованого управління системами контролю доступу, відеоспостереження та сигналізації. Це рішення особливо підходить для центральних станцій моніторингу та великих підприємств, що потребують високого рівня безпеки та ефективного управління подіями.

До можливостей даного програмного продукту варто віднести можливість централізованого керування декількома системами контролю доступу, відеоспостереження та сигналізації, що забезпечує єдиний інтерфейс для моніторингу та управління безпекою у великих організаціях. Також ПЗ надає розширені можливості для створення звітів та аналізу даних про події, що дозволяє оперативно реагувати на інциденти та покращувати безпеку. Моніторинг подій забезпечується у реальному часі, що дозволяє операторам миттєво реагувати на інциденти та потенційні загрози.

LenelS2^[12] - це американська компанія, що спеціалізується на розробці та виробництві систем контролю доступу та управління доступом для складних об'єктів з великою кількістю користувачів. Їхні системи мають широкий спектр функцій, включаючи управління ролями, контроль доступу на основі часу та централізоване управління. СКУД компанії LenelS2 використовуються на таких об'єктах, як державні установи, оборонні підприємства, науково-дослідні інститути, а також на великих комерційних об'єктах.



Рис.1.12 Логотип компанії

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		30

Найвідомішим рішенням цієї компанії є OnGuard – комплексне рішення для забезпечення безпеки, яке включає в себе не тільки контроль доступу, але й інтеграцію з відеоспостереженням, сигналізацією та іншими системами безпеки. LenelS2 OnGuard можна використовувати для контролю доступу до дверей, ліфтів, воріт та інших точок доступу.

До можливостей системи можна віднести підтримку різних методів ідентифікації, моніторинг активності системи та генерування звітів про події, можливість керування за допомогою програмного забезпечення для ПК або мобільного додатка.

Завдяки відкритій архітектурі платформи OnGuard, підприємства що мають віддалені філії мають можливість здійснювати централізований контроль регіональних систем через мережі LAN/WAN.

SALTO Systems^[13] - це іспанська компанія, що спеціалізується на розробці та виробництві бездротових систем контролю доступу та управління доступом, які легко встановлюються та обслуговуються. Їх СКУД використовуються на об'єктах, де важливо зберегти естетику в дизайні інтер'єру, таких як готелі, ресторани, музеї, а також на офісних та житлових об'єктах.



Рис.1.13 Логотип компанії

Однією з найпопулярніших систем контролю управління доступом від компанії SALTO Systems є SALTO XS4. Це інноваційне рішення, яке поєднує в собі високий рівень безпеки, гнучкість і зручність використання.

SALTO XS4 використовує бездротову технологію, що забезпечує легку установку та мінімізує потребу в проводці. Це дозволяє значно знизити витрати на монтаж та обслуговування системи. Система використовує сучасні методи шифрування та захисту даних, що забезпечує високий рівень безпеки та захист від несанкціонованого доступу.

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		31

Дозволяє забезпечувати централізоване управління доступом до різних зон об'єкта через єдиний інтерфейс. Адміністратори можуть легко налаштовувати права доступу та відстежувати всі події в реальному часі.

Основними характеристиками, що вирізняють рішення цієї компанії поміж інших є зосередження не тільки на функціональній частині, а й на естетичній, а також простота встановлення. Для того щоб встановити смарт-замки, достатньо просто замінити ручку в дверях.

Suprema^[14] - це південнокорейська компанія, що спеціалізується на розробці та виробництві систем контролю доступу та управління доступом з біометричною аутентифікацією. Їх СКУД використовуються на об'єктах з високим рівнем безпеки, таких як аеропорти, банки, державні установи, а також на комерційних та житлових об'єктах.



Рис.1.14 Логотип компанії

У сфері контролю доступу компанія надає відкриту інтегровану веб-платформу безпеки – BioStar 2. Вона забезпечує комплексні функції контролю доступу та завдяки модульному, гнучкому фреймворку платформа надає персоналізовану СКУД, що залежить від масштабу системи, кількості користувачів і структури, яка використовувалася.

До функцій керування відносять керування дозволами користувачів для кожного окремого проходу, керування доступом до поверхів для ліфтів, зональне керування та моніторинг дверей зон та пристроїв у реальному часі.

Підсумовуючи огляд основних компаній, що працюють у сфері управління доступом, варто зазначити, що більшість характеристик їх рішень є спільними, а відмінності доволі незначними. При виборі варто опиратися на бюджет та архітектуру конкретного проєкту, який планується реалізовувати.

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

1.4. Аналіз вимог до програмно-апаратного комплексу

Аналіз вимог до програмно-апаратного комплексу системи контролю управління доступом (СКУД) є важливим етапом у розробці та впровадженні ефективної системи безпеки. Цей аналіз дозволяє визначити необхідні компоненти, їх взаємодію та функціональні можливості системи. Розглянемо основні вимоги до програмно-апаратного комплексу СКУД.

1. Вимоги до рівня безпеки: в першу чергу потрібно визначити який рівень безпеки повинен бути в системі, від цього напряму залежать багато факторів, як наприклад, які методи автентифікації потрібні на об'єкті (чи достатньою є проста ідентифікація за допомогою RFID-карток/міток, чи рівень безпеки вимагає біометричної ідентифікації за відбитком пальця чи розпізнаванням обличчя); чи потрібно шифрування даних у мережі та якщо потрібно, яким має бути алгоритм, що буде достатньо стійким, щоб успішно виконувати свою функцію.

2. Вимоги до функціональності: важливим аспектом вибору складових СКУД є їх функціонал, не кожна система має усі необхідні користувачу функції, або працює саме так, як потрібно. Окрім звичних функцій контролю доступу, такі системи можуть надавати безліч опцій для обліку робочого часу, управління відвідувачами, моніторингу системи та створення звітності на основі отриманих даних під час роботи). Оскільки часто системи контролю і управління доступом не виступають самостійними частинами системи захисту об'єкта, потрібно подбати про можливість інтегрування з уже встановленими чи запланованими системами відеоспостереження, охоронних сигналізацій, тощо.

3. Масштабованість: варто оцінити кількість потенціальних користувачів системи та можливий обіг, адже не кожна система може впоратися з великою кількістю інформації про її користувачів, особливо якщо потрібно до кожного з них хастосовувати особливі права, такі як доступ до конкретних зон та поверхів, у різний час та день. Також варто передбачити можливе збільшення площі мережі, що понесе за собою збільшення кількості використовуваних пристроїв. У випадку якщо система погано масштабована, додавати нові компоненти до існуючої СКУД може бути складно, або навіть неможливо. З іншого боку, якщо системі немає потреби у

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

збільшенні потужностей, то можливо зекономити чи обрати такі рішення, що зможуть дати певні переваги, які є необхідними.

4. Бюджет: один з основних критеріїв для вибору складових системи контролю і управління доступом, адже не кожна компанія, навіть при великій необхідності у керуванні правами користувачів системи, здатна виділити достатній бюджет для забезпечення всього спектру своїх потреб, тому доцільно буде визначити свої потреби за усіма вищезазначеними пунктами та обрати відповідні безпекові рішення. Більшість функціоналу, який пропнують виробники систем управління доступом є базовим для них усіх, проте варто відмітити, що якщо детально вивчити ринок та обирати складові виключно за потребами та без надлишкового функціоналу, можливо зекономити значні кошти, особливо це стосується невеликих підприємств, яким в цілому достатньо базових функцій СКУД, навіть без інтеграції її з іншими системами безпеки.

Певним вимогам повинно відповідати і програмне забезпечення для керування системами. Воно мусить бути достатнім для забезпечення функціонування усіх пристроїв системи, що було встановлено. Головними вимогами до ПЗ є відповідність зазначеним вище вимогам та здатність виконувати усі покладені на нього завдання.

Інтерфейс користувача має бути інтуїтивно зрозумілим, зручним у використанні та забезпечувати швидкий доступ до основних функцій системи. Важливо, щоб програмне забезпечення могло інтегруватися з іншими системами безпеки (відеоспостереження, сигналізація, системи управління будівлями) та інформаційними системами підприємства.

Програмне забезпечення повинно забезпечувати високий рівень безпеки, включаючи шифрування даних, захист від несанкціонованого доступу, аудит подій та управління паролями.

Важливим критерієм для ПЗ є також підтримка мобільних пристроїв та можливість повноцінно керуватися з телефону та надавати таким користувачам доступ до звітів з безпеки у режимі реального часу.

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

Для апаратної частини системи СКУД важливим є достатній для умов використання рівень відмовостійкості та надійності. Важливо щоб частина пристроїв, що мають використовуватися надворі, була захищена від вандалізму та потраплянні всередину води. Зчитувачі повинні відповідати типу використовуваних ідентифікаторів та забезпечувати швидке і точне зчитування даних.

Необхідні сервери для зберігання та обробки даних, а також мережеве обладнання для забезпечення надійного зв'язку між компонентами системи. Для забезпечення безперебійної роботи системи у випадку відключення електроенергії необхідні джерела безперебійного живлення.

Механічні або електронні замки, що керуються системою, повинні бути надійними та відповідати вимогам безпеки об'єкта. Також вони мають відповідно до цих вимог бути чи нормально замкненими чи нормально відімкненими, щоб забезпечувати вільний вихід людей під час надзвичайних ситуацій, або навпаки недопуск людей у певні небезпечні зони під час таких подій.

Висновки з першого розділу:

Досліджено актуальність теми курсової роботи та специфіку впровадження систем контролю і управління доступом до навчального процесу.

Наведено визначення систем контролю і управління доступом, сферу їх застосування та компоненти, що до неї належать. Для компонентів були визначені переваги та недоліки, різновиди реалізації та описані принципи за якими вони працюють. Визначено основні функції покладені на СКУД та наведено приклад взаємодії компонентів у такій системі та узагальнену апаратну схему.

Проведено аналіз ринку систем контролю і управління доступом, визначено основних виробників рішень для таких систем та їх головні продукти. Для цих компаній і їх розробок було визначено сильні сторони та особливості роботи.

Проведено аналіз вимог до СКУД, їх програмної та апаратної складової.

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		35

РОЗДІЛ 2 РОЗРОБКА СТРУКТУРНОЇ ТА ФУНКЦІОНАЛЬНОЇ СХЕМИ ПРОГРАМНО-АПАРАТНОГО КОМПЛЕКСУ СИСТЕМИ КОНТРОЛЮ І УПРАВЛІННЯ ДОСТУПОМ НАВЧАЛЬНОЇ ЛАБОРАТОРІЇ

2.1 Аналіз функціональних можливостей і технічні характеристики елементів комплексу системи контролю і управління доступом

На ринку вітчизняних виробників програмних та апаратних засобів для систем контролю та управління доступом провідне місце займає компанія «Сайфрекс». Вона займається розробкою рішень, виробництвом устаткування і наданням сервісів, спрямованих на організацію безпеки і підвищення ефективності бізнесу своїх клієнтів, допомагає їм вирішити питання трудової дисципліни, контролю і безпеки охоронних об'єктів, моніторингу і дистанційного забезпечення пропускового режиму [15].

Компанія володіє власною науково-технічною базою, яка використовується для проектування, розробки та модернізації обладнання для систем контролю і управління доступом (СКУД), а також спеціалізованого програмного забезпечення до них.

За роки роботи підприємство стало офіційним дилером і надійним партнером більшості провідних компаній України у сфері безпеки, таких як: «SEC», «Трініті СБ», «Каштан», «Сіріус», «Технотрейд», «Євробізнес», «Опта», «СМ-Стандарт» «Нео Лайф Систем», «Компанія Укрбезбека», «Майстер Безпеки» і багатьох інших.

При розробці комплексної схеми системи контролю та управління доступом було обрано мережевий модуль контролю доступу іВС-01 від компанії «Сайфрекс». Вибір саме цього мережевого модуля зумовлено невисокою ціною у порівнянні з аналогами та тим, що це продукт вітчизняної фірми, що зробила ім'я у галузі систем контролю і управління доступом. Він задовольняє усі потреби та вимоги, що стоять перед ним як перед контролером для навчальної лабораторії та не має надлишкового функціоналу.

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

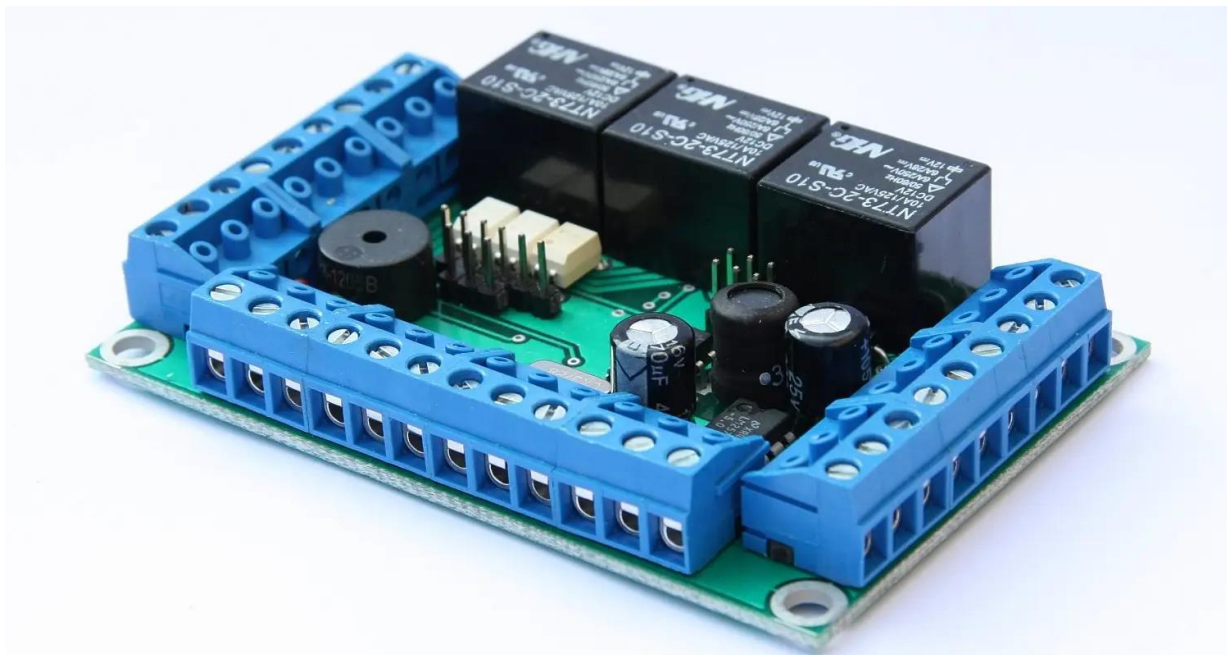


Рис.2.1 Мережевий модуль контролю доступу iBC-01

Cyphrax iBC-01 - мережевий контролер для системи контролю і управління доступом, що використовується для контролю доступу в житлових, виробничих або офісних приміщеннях. Він здатен керувати доступом в будь-які зони, оснащені електромагнітними або електромеханічними замками, проте також здатний працювати з турнікетами, шлагбаумами, боллардами і будь-якими іншими замками [17].

На основі мережевого модуля iBC-01 можна одночасно стежити за роботою двох входів. Зчитувачі до пристрою підключаються через інтерфейс 1-Wire або Wiegand. Відстань від зчитувачів до цього контролера повинна бути до 30 метрів при використанні інтерфейсу 1-Wire та до 100 метрів, якщо використовується інтерфейс Wiegand. При виборі типу інтерфейсу перевага надається 1-Wire, оскільки його єдиним недоліком є менша в порівнянні з Wiegand швидкість передачі даних. Натомість користувачі отримують низку переваг: дані та живлення, при використанні 1-Wire, передаються по одному дроту, що спрощує монтаж і зменшує кількість необхідних кабелів, цей стандарт підтримує шифрування, що підвищує рівень безпеки даних, а також дозволяє підключати до одного контролера велику кількість пристроїв, що робить його зручним для розподілених систем. Інтерфейс Wiegand рекомендується використовувати, якщо зчитувачі не підтримують 1-Wire або якщо на об'єкті уже встановлені зчитувачі, що працюють по інтерфейсу Wiegand.

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

В межах однієї системи рекомендується використання підключення зчитувачів по однаковому інтерфейсу. По-перше, однаковий інтерфейс гарантує сумісність всіх компонентів системи. Це зменшує ризик виникнення конфліктів між різними типами зчитувачів та контролерів. Стандартний інтерфейс є гарантією того, що всі зчитувачі коректно взаємодіють з центральним контролером, передаючи дані у зрозумілому для нього форматі. По-друге, використання однакового інтерфейсу значно спрощує обслуговування та адміністрування системи. Технічному персоналу легше налаштовувати та діагностувати систему, коли всі компоненти працюють за єдиним стандартом.

Вхід і вихід в приміщення здійснюються по ключам, або Proximity, або Touch Memory. Кожен ключ, крім управління замками, може мати безліч різних додаткових опцій: блокування/розблокування контролера, управління виходом другої двері. Однією з особливих функцій даного мережевого контролера є antipassback (заборона подвійного проходу), що є важливим елементом в системах контролю доступу, який підвищує їхню безпеку та забезпечує точність відстеження переміщень осіб. Ця функція запобігає повторному використанню однієї і тієї ж картки доступу для входу або виходу без проміжного виходу або входу відповідно. Якщо картка була використана для входу в зону контролю, вона не може бути використана для повторного входу, доки не буде зареєстрований вихід, і навпаки. Є можливість підключити кнопку для віддаленого керування або аварійного розблокування дверей.

Пристрій здатен записати на свою внутрішню пам'ять та обробити до 2000 користувачьких ключів та до 7000 подій (входів/виходів) користувачів. При наявності зв'язку з комп'ютером (сервером) відбувається синхронізація журналу подій з базою даних програмного забезпечення.

До додаткових функцій контролера можна віднести облік робочого часу, групове управління правами користувачів, підтримка можливості додавати фотокартки до користувацької інформації, моніторинг подій в реальному часі та формування звітів щодо подій та робочого часу користувачів.

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

Технічні характеристики іВС-01

№	Параметр	Значення
Електричні		
1	Напруга живлення	10-15 В
2	Номінальний споживаний струм (при напрузі живлення 12 В): 1. усе реле вимкнено 2. усе реле ввімкнено	- 25 мА ~ 125 мА
3	Піковий струм (при напрузі живлення 12 В), не більше	200 мА
4	Максимальний струм реле, що комутується	10 А
5	Максимальна напруга реле, що комутується	24 В
Функціональні		
6	Інтерфейс мережі	RS-485
7	Кількість подій, що запам'ятовуються, при автономній роботі	7000
8	Кількість користувацьких ключів	2000
9	Кількість зчитувачів, що підключаються	2
10	Підтримуваний тип (інтерфейс) зчитувачів	1-wire (Touch Memory)
11	Кількість релейних виходів	3
12	Кількість опторозв'язаних входів	2
13	Максимальна відстань до зчитувача	40 м
Експлуатаційні		
14	Габаритні розміри (ширина x висота x товщина)	60×90×20 мм
15	Настановний розмір	52.5×82.5 мм
16	Робочий діапазон температур	0°C - 60°C

При виборі зчитувача було обрано пристрій, що має повну сумісність із мережним контролером - PR – 01, який представлено на рисунку 2.2.

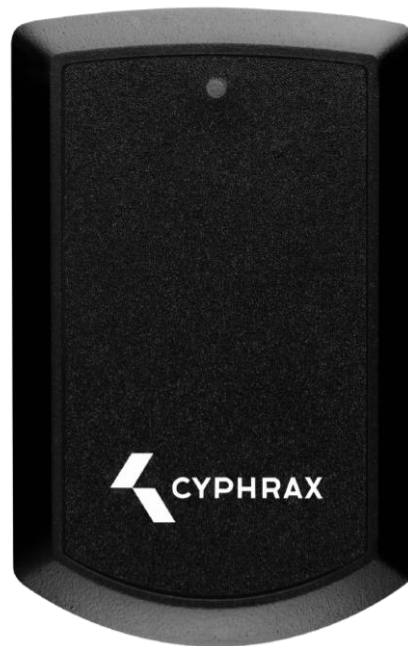


Рис.2.2 Зчитувач PR-01

Зчитувач PR-01 – пристрій, який використовується в сучасних системах контролю та управління доступом та у системах, що проводять облік часу. Принцип роботи ґрунтується на зчитуванні ідентифікаційного коду користувача, що міститься на Proximity картках і Proximity брелоках стандарту EM-Marine. Зчитувач підтримує інтерфейси Weigand 26 bit і 1-Wire. Головною особливістю, що виникає через базування на використанні цих інтерфейсів, є можливість застосування пристрою в будь-яких системах та суміщення з нити контролерами, які підтримують iButton та працюють на ключах Dallas Semiconductor DS1990 (Touch Memory) [18].

Зчитувач PR-01 може використовуватися як усередині, так і зовні приміщень. Виконано в чорному і білому кольорі, а корпус оснащено триколірним світлодіодним індикатором.

Застосовуючи додаткові програми, зчитувач PR-01 можна використовувати в режимі емуляції для введення номера брелка або картки з клавіатури. Завдяки такій особливості пристрій можна використовувати в інших програмах.

До функціональних можливостей даного пристрою можна віднести наступні його особливості:

- візуальна триколірна ідентифікація;
- звуковий сигнал зчитування карти;

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

- накладний монтаж;
- роз'ємне підключення зчитувача;
- зовнішнє управління індикацією;
- інтерфейси підключення Wiegand-26, 1-Wire (Touch Memory).

Таблиця 2.2

Технічні характеристики зчитувача PR-01

№	Параметр	Значення
1	Напруга живлення	9-12 В
2	Споживаний струм	40 мА
3	Відстань зчитування	не менше 5 см
4	Частота	125 кГц
5	Протокол	ЕМ-Marine
6	Установчий розмір	50 мм
7	Габаритні розміри	70×95×20 мм

Серед різних видів замків було обрано електромагнітний замок від компанії Trinix^[16] – KRF-200. Складається він з корпусу, який виготовлений з металевого сплаву, з магнітом та відповідної планки з металу, що має високу магнітну проникність. Замок призначений для утримання дверей у зачиненому положенні під час подавання на нього постійної напруги [19].



Рис.2.3 Електромагнітний замок KRF-200

Технічні характеристики електромагнітного замку KRF-200

№	Параметр	Значення
1	Напруга живлення	12 В
2	Споживаний струм	430 мА
3	Сила утримання	до 200 кг
4	Монтаж	Накладний
5	Встановлення	Внутрішнє
6	Габаритні розміри	170×45×22 мм
7	Вага	680 г

Здійснювати встановлення замка слід з обережністю, адже пошкодження поверхонь електромагніту або відповідної планки, що притягуються одна до одної, може призвести до зменшення сили утримання.

Тіло замка має бути жорстко закріплене на відповідній планці, що монтується на дверному полотні з використанням кріплення, що йде в комплекті. Це кріплення забезпечує можливість обертання відносно центральної точки кріплення для компенсування перекосів під час встановлення або деформації полотна. Не слід занадто жорстко закріплювати відповідну планку з метою збереження еластичності гумової шайби, щоб забезпечити можливість планки автоматично підлаштовувати своє положення відносно тіла замка для більш щільного зчеплення.

Система контролю і управління доступом потребує блоків безперебійного живлення для забезпечення стабільної та надійної роботи в умовах можливих перебоїв електропостачання. Оскільки СКУД є критично важливою для безпеки підприємств, установ та інших об'єктів, де вони впроваджені, збої у її функціонуванні можуть призвести до серйозних наслідків, таких як несанкціонований доступ до приміщень або порушення режиму безпеки.

ББЖ забезпечує безперервне живлення компонентів СКУД, таких як зчитувачі карток, електронні замки та центральний контролер, під час відсутності основного електропостачання, що дозволяє системі продовжувати функціонувати належним чином. Крім того, стабільне живлення допомагає уникнути втрати даних і налаштувань системи, що могло б ускладнити або навіть зробити неможливим її подальшу роботу після відновлення електропостачання.

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

Для нашої системи було обрано рішення від торгової марки «Ніктон-С» - імпульсний безперебійний блок живлення серії «ББП 20». Він розроблений для забезпечення живлення постійним струмом пристроїв, що повинні продовжувати працювати при відключенні мережі (наприклад: охоронні системи, домофони, системи зв'язку і т.д.) [21].

Блок випускається в трьох конструктивних варіантах: як закінчений пристрій в металевому боксі з місцем під АКБ, у вигляді налаштованої плати з виведеними джгутами для комутації та індикації та у вигляді налаштованої плати зі штирями для монтажу в «материнську» плату.

Випускається ББЖ у 2 конструктивних варіантах в електричних модифікаціях на 12 та 24 В.

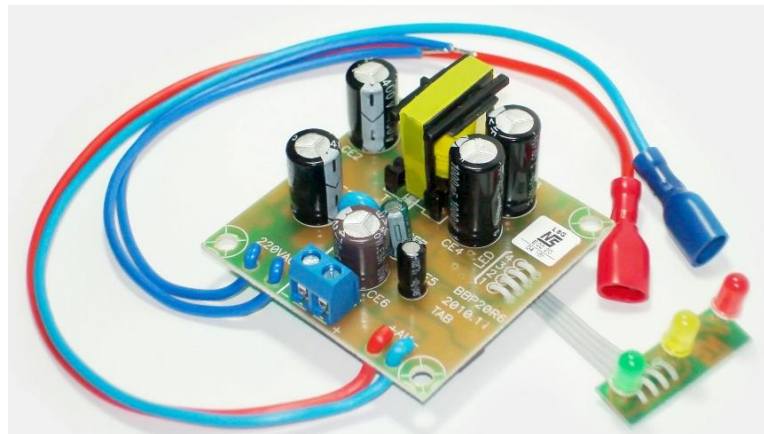


Рис.2.4 Безперебійний блок живлення серії «ББП 20» у вигляді налаштованої плати з виведеними джгутами



Рис.2.5 Безперебійний блок живлення серії «ББП 20» як закінчений пристрій в металевому боксі

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

До функціональних можливостей даного пристрою відносяться:

- захист від перегріву;
- захист від короткого замикання при навантаженні;
- захист від протилежної полярності АКБ (запобіжник багаторазовий 2А);
- автоматичний зарядний пристрій з режимом стабілізації по струму;
- захист АКБ від глибокого розряду (при роботі блока від АКБ);
- «холодний» старт від АКБ при відсутності мережі;
- світлодіодна індикація режимів роботи (зелений - робота блока від мережі, жовтий - наявність вихідної напруги, червоний - заряд акумулятора при наявності мережі).

Таблиця 2.4

Технічні характеристики імпульсного безперебійного блока живлення серії «ББП 20» (для модифікації 12 В)

№	Параметр	Значення
1	Вхідна напруга	~155...~245 (короткочасно ~300 В)
2	Вихідна напруга	13.2 В
3	Загальна нестабільність	5%
4	Вихідний струм номінальний	1.0 А
5	Вихідний струм максимальний	1.4 А
6	Струм заряду АК	0.30 – 0.40 А
7	Напруга заряду АК	13.5 – 13.8 В
8	Напруга відсічки АК	10.5 - 11.0 В
9	Температурний діапазон	0°C - 45°C
10	Режим роботи	довгостроковий
11	Габаритні розміри	а) 200×168×75 мм б) 55×55×35 мм в) 55×65×35 мм

До безперебійного блоку живлення підключена акумуляторна кислотна батарея Mustang Energy, що призначена для використання в системах резервного та автономного електропостачання. До рекомендованих сфер використання цих акумуляторів відносяться наступні: джерела безперебійного живлення, системи пожеж-

ної та охоронної сигналізації, системи аварійного та автономного освітлення, автономні системи електропостачання на базі сонячних панелей і вітрогенераторів та системи живлення обладнання для телекомунікацій і зв'язку.



Рис.2.6 Акумуляторна кислотна батарея Mustang Energy

Акумулятор виготовлений за технологією SLA. При цій технології електролітом є знерухомлена сірчана кислота, а сепаратором - скловолокно. Щільне заповнення запобігає обсіпанням свинцю з пластин, а отже і їх короткому замиканню, що збільшує термін служби акумулятора. Акумуляторна батарея є герметичною і не потребує обслуговування (не потребує доливу електроліту впродовж всього терміну служби). Такі акумулятори можуть працювати при температурах нижче нуля, але для тривалого терміну експлуатації їх слід розміщувати у непроникному для морозу приміщенні.

Акумулятори цього типу призначені для роботи в буферному режимі, але якщо з якихось причин стався глибокий розряд акумулятора, необхідно якнайшвидше зарядити його до повної ємності (або мінімум до половини), оскільки тривале перебування в розрядженому стані призводить до сульфатації пластин і виходу акумулятора з ладу. Корпус акумулятора виготовлений з міцного негорючого пластику, що забезпечує додатковий рівень безпеки при експлуатації в умовах підвище-

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		45

ного ризику виникнення пожежі. Це робить їх особливо корисними для встановлення в місцях із підвищеними вимогами до пожежної безпеки, таких як серверні кімнати, центри обробки даних тощо.

Таблиця 2.5

Технічні характеристики акумуляторної кислотної батареї Mustang Energy

№	Параметр	Значення
1	Тип акумулятора	не обслуговуваний, герметичний
2	Вихідна напруга	12 В
3	Номінальна ємність	7 А * г
4	Максимальний струм заряду	не більше 2.1 А
5	Маса	1.95 кг
6	Температурний діапазон	0°C - 45°C
7	Режим роботи (рекомендований)	буферний
8	Габаритні розміри	151×95×66 мм

Для інтеграції пристроїв з інтерфейсом RS-485 у комп'ютерні системи через USB-порт використовується спеціальний перетворювач. Його підімкнено до мережевого модуля контролю доступу іВС-01, що дозволяє по USB-порту приєднати цей модуль до ПК з подальшим підключенням програмного забезпечення для керування системою.



Рис.2.7 Конвертер USB - RS-485

Для відкриття замкнених дверей з внутрішньої сторони, встановлена накладна кнопка виходу ART-805 від компанії «TRINIX». Вона має Н/Р (нормально розімкнений) тип контакту та призначена для внутрішнього встановлення в місцях із високою інтенсивністю використання, адже виконана у дюралюмінієвому корпусі, що є більш зносостійким, у порівнянні з пластиковим, який може не впоратися з частим використанням [22].



Рис.2.8 Кнопка виходу накладна ART-805

Для забезпечення моніторингу стану дверей, на них було встановлено накладний геркон, що діятиме як сенсор та буде визначати чи двері відчинені чи зачинені, і передаватиме цю інформацію до центральної системи контролю. Це потрібно для контролю за залишенням дверей незачиненими, запобігаючи несанкціонованому доступу та підвищуючи загальну ефективність системи безпеки.

Було обрано дротовий варіант пристрою через його меншу ціну на незалежність від заряду батарейки. Дротові геркони отримують живлення по шині управління.

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		47



Рис.2.9 Геркон

2.2 Аналіз функціональних можливостей програмного забезпечення для комплексу системи контролю і управління доступом

Big Brother – це комплексна система контролю доступу та обліку робочого часу, що розроблена компанією «Сайфрекс», призначена для забезпечення безпеки, контролю та ефективного використання ресурсів у підприємствах та організаціях. Ця система надає можливість контролювати доступ до приміщень, визначати робочий час співробітників, а також вести детальний облік робочого часу. Крім того, що такі системи надають компаніям можливість покращення власної безпеки та інформативності, вони також дозволяють ставити управління персоналом на більш високий рівень, підвищують дисципліну та продуктивність праці [23].

Система Big Brother має спеціальне програмне забезпечення, яке дозволяє адміністраторам керувати системою, налаштовувати права доступу та групові політики.

Одними з основних завдань програми є облік робочого часу персоналу: можливість легко відстежувати відвідуваність, запізнення і ранні відходи. Даний софт дозволяє вести візуальну ідентифікацію та облік відвідувачів, моніторити і аналізувати переміщення користувачів по об'єкту з метою отримання статистики і побудови звітів.

У сфері обліку робочого часу до особливостей програми, що можуть бути корисними при роботі з одним зчитувачем, можна відзначити:

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

- у випадку якщо користувачі забувають про відмітку на робочому місці, програма може автоматично проставляти відсутню реєстрацію за робочим розкладом або за часом дня;
- можливість переглянути усі випадки, коли користувач не відмітився при приході або виході;
- можливість відмічати першу подію пов'язану з користувачем як прихід на роботу;
- облік нічної роботи;
- розрахунок обідніх перерв.

Система Big Brother має спеціальне програмне забезпечення, яке дозволяє адміністраторам керувати системою, налаштовувати права доступу, переглядати історію входів та виходів, а також генерувати звіти.

Система контролю доступу й обліку робочого часу Big Brother побудована по архітектурі "клієнт-сервер". Приклад цієї архітектури зображено на рисунку 2.10.

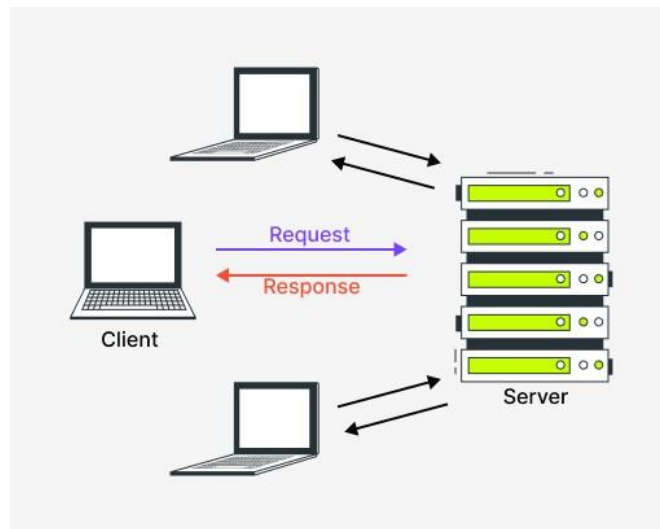


Рис.2.10 Схематичне зображення клієнт-серверної архітектури

У СКД Big Brother серверна частина називається "Сервер пристроїв" її завдання - збір даних із пристроїв і їх збереження в єдину базу даних. Сервер пристроїв встановлюється на комп'ютер до якого підключено встаткування (контролери ібс-01), як правило, на цьому ж комп'ютері розташована база даних, у якій перебувають налаштування й журнали подій системи.

Клієнтська частина СКД Big Brother називається "Робоче місце користувача". Клієнтська частина може розташовуватися на будь-якому комп'ютері локальної мережі, у тому числі й на сервері. За допомогою клієнтської частини здійснюється керування користувачами, устаткуванням, побудова звітів та ін. Кожний клієнтський додаток може бути настроєне на розв'язок певного кола завдань, наприклад, бюро пропусків - виконує керування користувачами (видача пропусків, призначення робочого розкладу та ін.), відділ кадрів - виконує завдання обліку робочого часу, прохідна - спостереження за переміщенням користувачів і т.д.

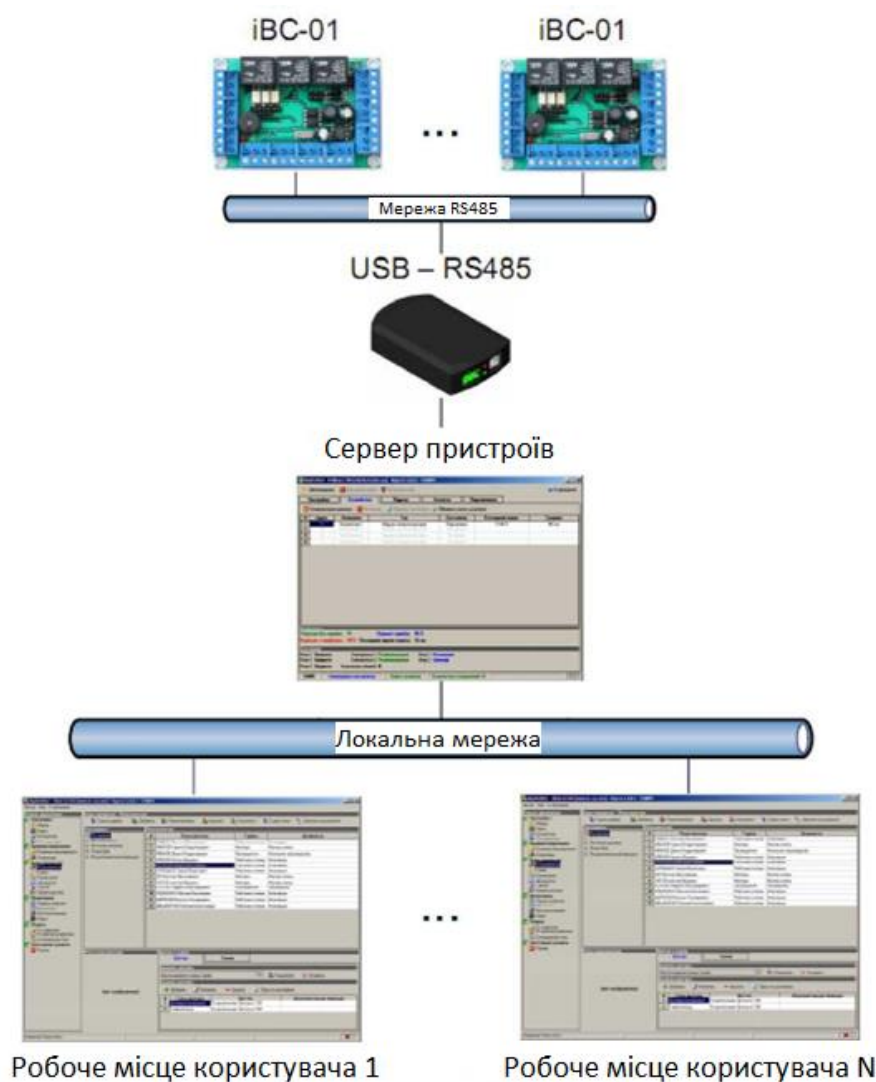


Рис.2.11 Структурна схема, що пояснює принцип побудови СКД Big Brother

СКД Big Brother складається із двох модулів "Сервер пристроїв" і "Робоче місце користувача" (див. розділ Структура, СКД_ Big Brother). Тому можливі наступні варіанти установки програмного забезпечення на ПК:

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		50

Клієнт + Сервер

Даний варіант установки використовують у тих випадках, коли сервер пристроїв і робоче місце користувача - це один комп'ютер. Цей варіант установки також рекомендується використовувати у випадку якщо сервер пристроїв це звичайний робочий комп'ютер.

Сервер пристроїв

Варіант установки тільки серверної частини додатка. Може бути використаний, коли комп'ютер, до якого приєднано встаткування, - це системний блок, який установлений у безлюдному місці :) (наприклад, у серверній). Ми рекомендуємо для сервера завжди використовувати варіант установки Клієнт + Сервер, тому що це полегшує налаштування системи з одного комп'ютера.

Робоче місце користувача

Це установка мережного робочого місця, тобто установка на комп'ютер, який не є сервером пристроїв, наприклад - бухгалтерія, директор (начальство), відділ кадрів і т.д.

Для підготовки встановлення серверної частини ПО необхідно:

1. Підключити перетворювач USB-RS485 до вільного USB порту комп'ютера та установити драйвер. Драйвера перебувають на диску з ПО.
2. Визначте номер COM порту в диспетчері пристроїв (номер порту на вашому комп'ютері може відрізнятися від того що зображений на малюнку).

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		51

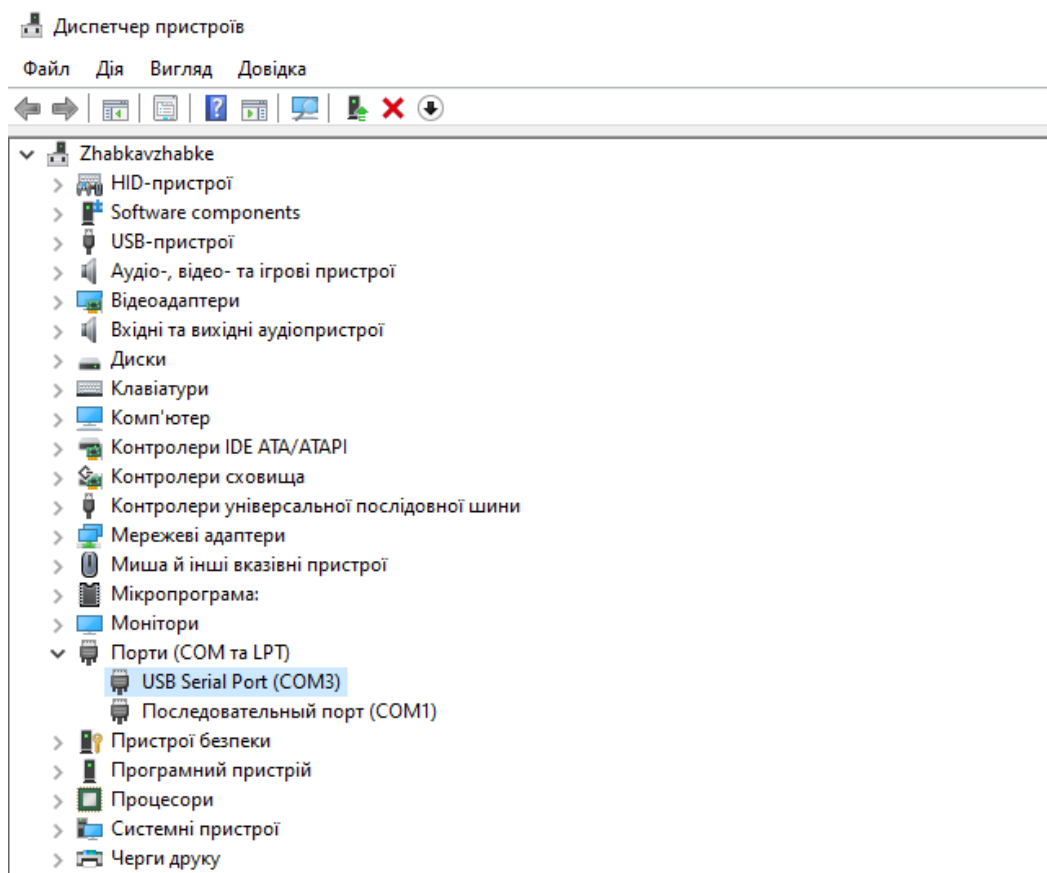


Рис.2.12 Потрібний COM порт в диспетчері пристроїв

Для підготовки встановлення серверної частини ПО потрібно переконатися, що для папки бази даних (БД) установлений загальний доступ по мережі й включені дозволи на читання й запис. Ці дії необхідно зробити на комп'ютері, на якому перебуває БД:

1. Натиснути праву кнопку миші на папці, у якій перебуває БД, і вибрати пункт меню "Загальний доступ і безпека ...".
2. Вибрати опцію "Відкрити загальний доступ до цієї папки".
3. У поле "Загальний ресурс" увести ім'я (можна залишити ім'я за замовчуванням).
4. Натиснути на кнопку "Дозволу".
5. Вибрати потрібну групу або користувача (у найпростішому випадку "Усі").
6. Установити прапорець "Повний доступ".

2.3 Розробка структурної схеми комплексу системи контролю і управління доступом

Після аналізу технічних характеристик пристроїв, описаних у першому підрозділі, а саме мережевого модуля контролю доступу iBC-01, зчитувача Proximity карток PR-01, електромагнітного замку KRF-200, безперебійного блоку живлення серії «ББП 20», кнопки виходу накладної ART-805, геркону та конвертера USB - RS-485, можна зробити висновок про наявність технічної можливості реалізувати програмно-апаратний комплекс системи контролю і управління доступом навчальної лабораторії у вигляді макету стенда, що дасть можливість перевірити його працездатність та протестувати роботоспроможність на наявний на пристроях функціонал.

Втілити задум побудови стенда можливо з наступних причин:

Мережевого модуля iBC-01 може одночасно стежити за роботою двох входів, що є цілком достатнім у рамках СКУД для навчальної лабораторії, де зазвичай не більше одного входу.

Блок живлення формує постійну вихідну напругу живлення 12 В з максимальним вихідним струмом до 1.4 А для живлення усіх пристроїв що працюватимуть у рамках однієї системи

Напруга живлення для нашого мережевого модуля контролю доступу, зчитувача Proximity карток та електромагнітного замка лежить в межах наявних у мережі 12 В.

Пікове споживання струму мережевим модулем при 12 В дорівнює 200 мА, для зчитувача Proximity карток це значення дорівнює 40 мА у той час як електромагнітний замок споживає 430 мА. В сумі ці значення становлять половину від можливих потужностей блоку живлення.

Використання конвертера допоможе під'єднати ПК по порту USB до мережевого модуля контролю доступу, що дасть змогу керувати мережею за допомогою встановленого застосунку для контролю доступу та обліку робочого часу BigBrother.

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		53

Виходячи з аналізу технічних характеристик усіх складових елементів нашої системи контролю і управління доступом навчальної лабораторії, її структурна схема буде виглядати наступним чином:

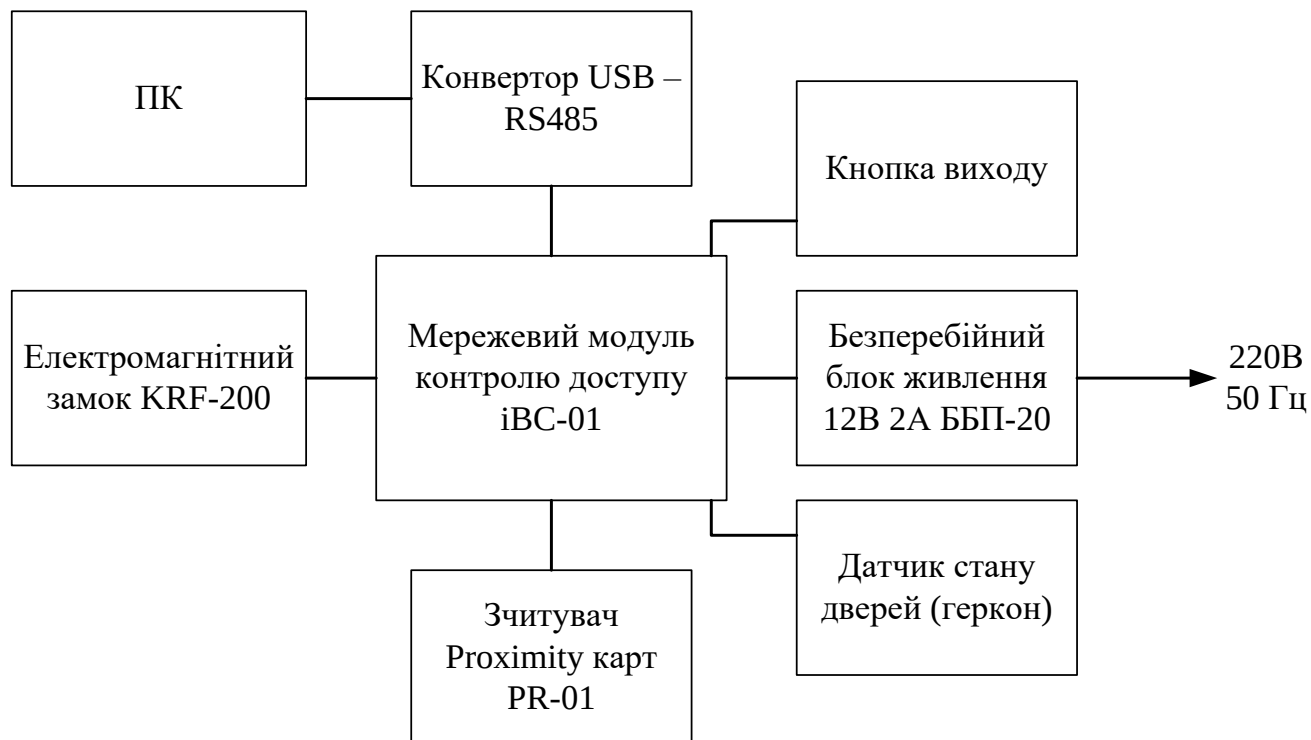


Рис.2.13 Структурна схема системи контролю і управління доступом навчальної лабораторії

Система контролю і управління доступом, зображена на нашій схемі, працює як єдина інтегрована система для забезпечення безпеки та контролю доступу в приміщення. Для розуміння роботи системи по структурній схемі потрібно описати, як відбувається взаємодія між компонентами:

ПК з програмним забезпеченням для керування (BigBrother) є центральним пунктом керування всією системою. Програмне забезпечення дозволяє адміністратору налаштовувати систему, додавати або видаляти користувачів, переглядати журнали доступу та отримувати сповіщення про усі події, що відбулися.

Конвертер USB-RS485 забезпечує зв'язок між ПК та мережевим модулем контролю доступу iBC-01 через інтерфейс RS485, що є шляхом для надійної передачі даних на великі відстані (при швидкості 10 Мбіт/с максимальна довжина лінії — 120 м, при швидкості 100 кбіт/с — 1200 м) [24].

Мережевий модуль контролю доступу iBC-01 є основним контролером системи, що обробляє сигнали від зчитувача карток PR-01, кнопки виходу, геркона та електромагнітного замку. Взаємодіє з ПК через конвертер USB-RS485 для обміну даними та отримання команд.

Зчитувач Proximity карт PR-01 встановлюється біля дверей для зчитування безконтактних карт доступу у користувачів системи. При зчитуванні картки передає дані до мережевого модуля контролю доступу iBC-01 для перевірки прав доступу.

Електромагнітний замок KRF-200 встановлюється на дверях і контролює їх блокування/розблокування. Отримує сигнали від мережевого модуля iBC-01 для відкривання дверей після успішної автентифікації картки.

Безперебійний блок живлення серії «ББП 20» забезпечує стабільне живлення усіх пристроїв системи. Підключений до 220В мережі змінного струму, забезпечує безперебійну роботу навіть у випадку відсутності основного живлення.

Кнопка виходу накладна ART-805 встановлюється з внутрішньої сторони дверей для ручного відкривання замка. При натисканні кнопки подає сигнал до мережевого модуля iBC-01 для тимчасового розблокування замка KRF-200.

Геркон (датчик стану дверей) визначає чи двері є зачиненими чи відчиненими та передає інформацію про стан дверей до мережевого модуля iBC-01, що дозволяє виявляти спроби несанкціонованого проникнення.

2.4 Аналіз функціонального призначення портів складових елементів системи та розробка структурної схеми контролю і управління доступом

Перед розробкою функціональної схеми стенда комплексу системи контролю і управління доступом навчальної лабораторії, що покаже конфігурацію мережі та її пристроїв, полегшить розуміння системи та її компонентів, а також допоможе в навчанні та дослідженнях, потрібно провести аналіз характеристик наявних на цих пристроях портів. На рисунку 2.14 зображена схема роз'ємів мережного модуля контролю доступу iBC-01.

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		55

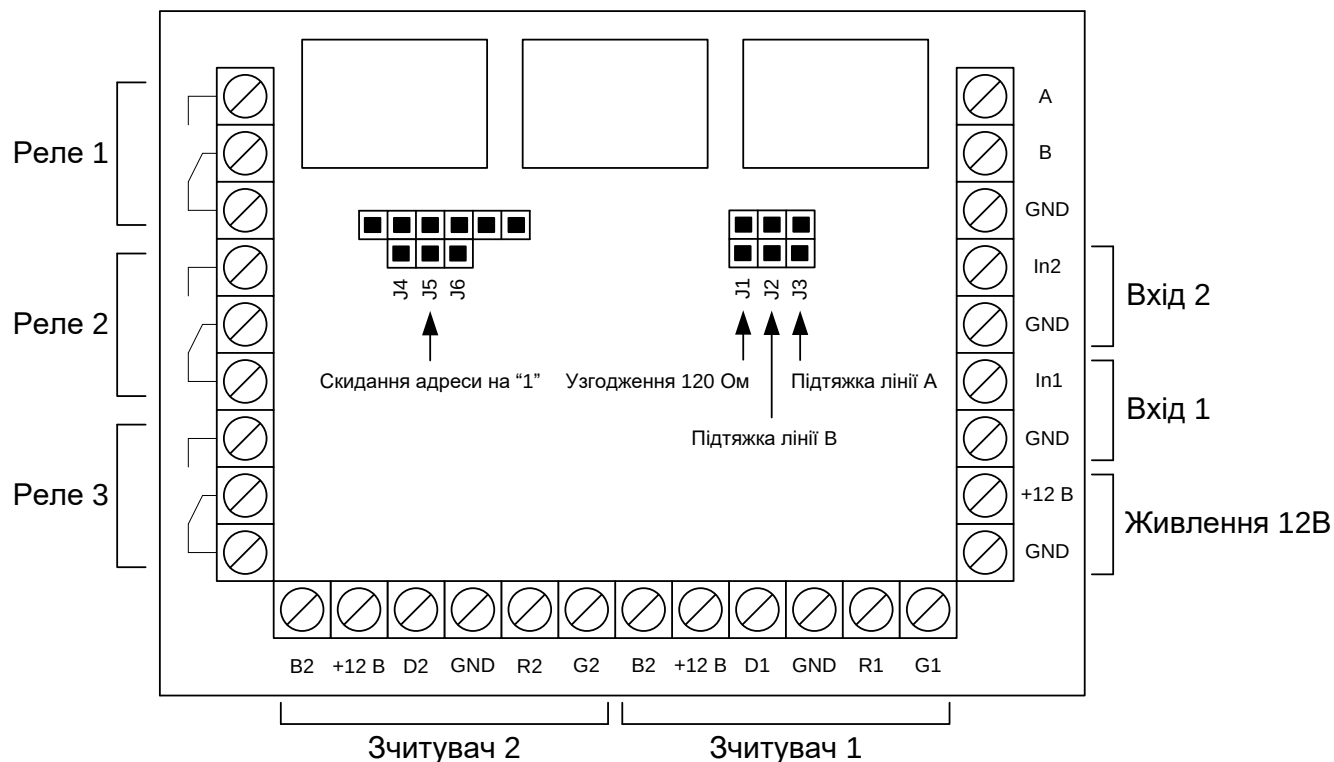


Рис.2.14 Схема роз'ємів мережного модуля контролю доступу iBC-01

На мережевому модулі наявні наступні роз'єми:

- А, В – клемні з'єднувачі для підключення по стандарту RS-485;
- GND – земля;
- In1, In2 – вхідні контакти (опис їх роботи буде проведено під час характеристики функціональної схеми системи).
- + 12 В – клемний з'єднувач для підключення живлення пристроїв;
- G1, G2 – підключення зелених світлодіодів;
- R1, R2 – підключення червоних світлодіодів;
- D1, D2 – 1-Wire (Touch Memory);
- B2 – клемне з'єднання «загальне».

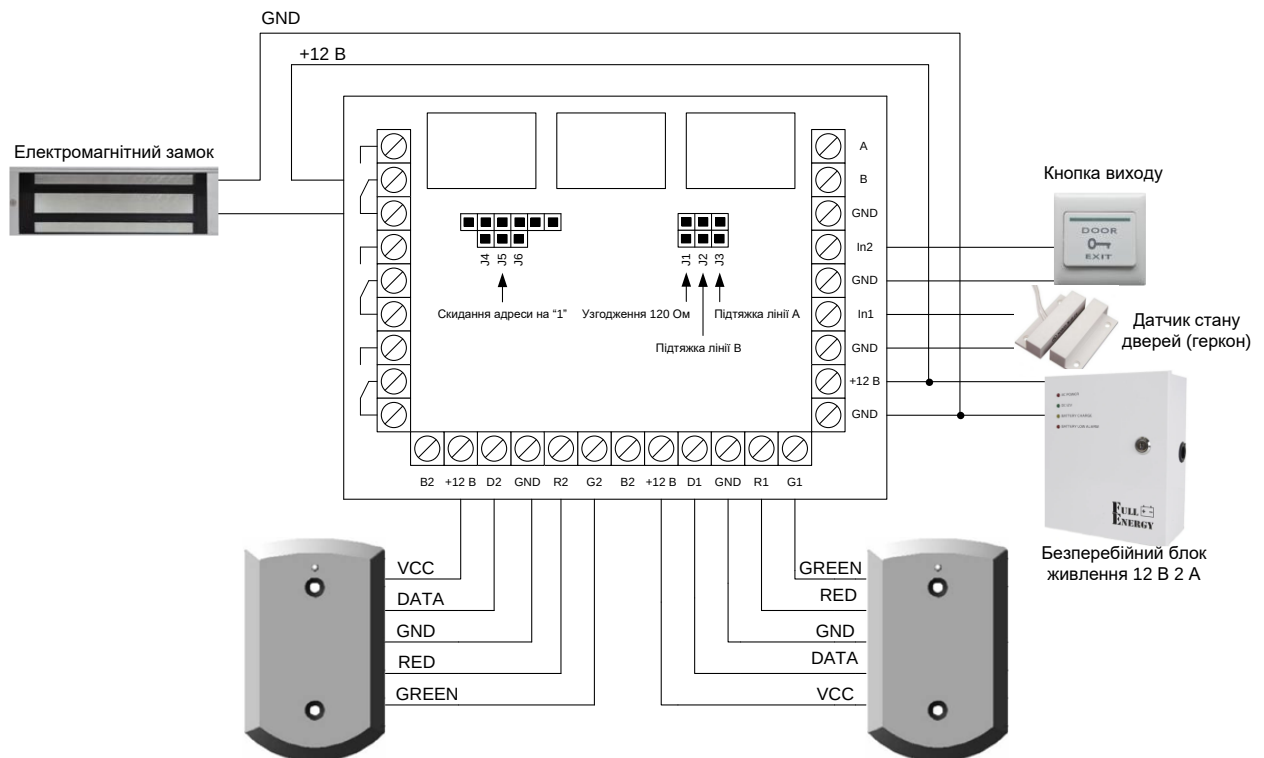


Рис.2.15 Підключення пристроїв зі зчитувачами Proximity карт для однієї дверей (зчитувач на вхід та на вихід)

При побудови стенду та реальної мережі на об'єкті слід розташовувати контролери якомога ближче до точок проходу (дверей), для того щоб мінімізувати довжину кабелів від зчитувачів до контролера, що дозволить збільшити швидкість передачі даних і відповідно час очікування, а також зменшить ризик впливу завад на сигнал.

У свою чергу довжина лінії RS-485 не критична до відстані, адже даний стандарт розроблявся для зв'язку із віддаленими об'єктами та має відмінну завадозахищеність.

Прокладати таку лінію слід на максимально можливій відстані від силових кабелів та світильників денного світла. В якості лінії зв'язку RS-485 рекомендується використовувати кабель типу "вита пара" - FTP Category 5. Екран кабелю, за можливості, слід заземлити з одного кінця.

Таким чином, за можливості, краще зробити вибір на користь довшої лінії зв'язку між контролерами, аніж між контролером та під'єднаними до нього зчитувачами.

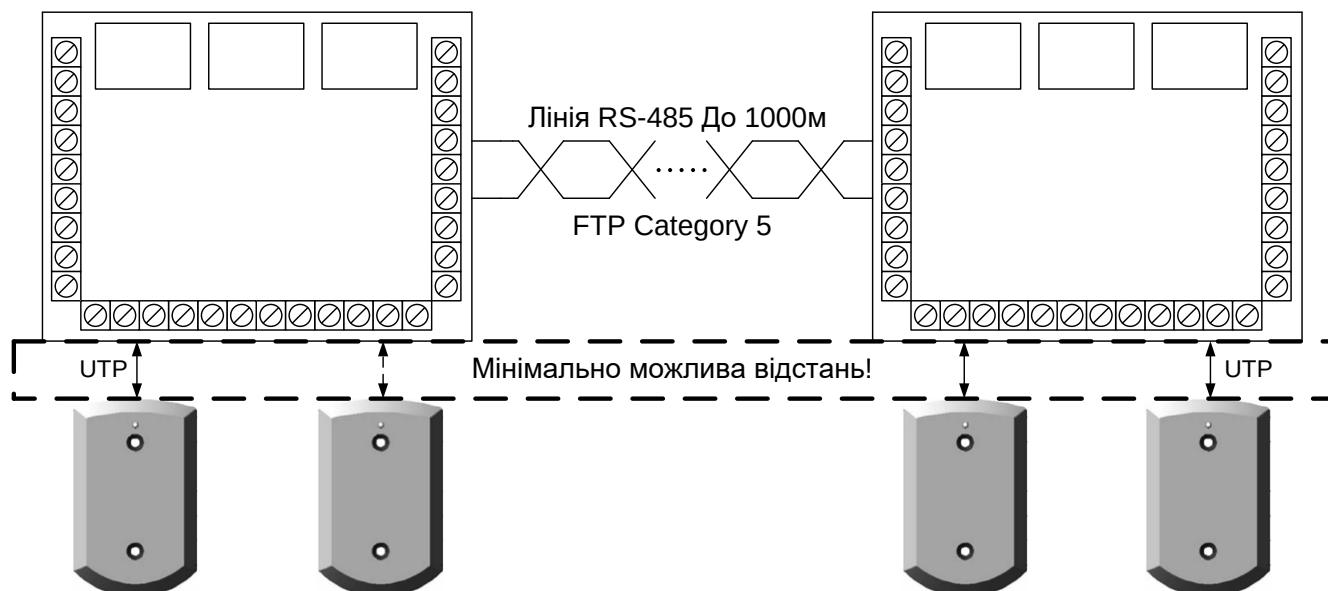


Рис.2.16 Рекомендоване розподілення довжин ліній зв'язку

Довжину проводів живлення контролера слід зробити максимально короткою, щоб уникнути значного падіння напруги на них. Після прокладки проводів слід переконатися, що напруга живлення контролера при включених замках не нижче 12 В. Якщо напруга нижче 12 В, слід збільшити переріз проводів лінії живлення або зменшити їх довжину.

У випадку використання індуктивного навантаження, наприклад електромагнітних замків, для того щоб уникнути «підгорання» і в наслідку залипання контактів реле, рекомендується використовувати варистор – напівпровідникові компоненти, резистори, що володіють здатністю стрімко знизити власний опір з 1000 МОм до 10 Ом у відповідності до прикладеного до них опору. При відчутному скачку напруги варистор переходить у відкритий стан, тобто його опір падає і з ізолюючого стану елемент переходить у електропровідний стан. Стабілізація напруги відбувається за рахунок пропускання через напівпровідник високоамперного струму. Варистори володіють багаторазовим дією, вони розподіляють енергію тепла і стрімко відновлюють власне електроопір вже при стабільній напрузі [25].



Рис.2.17 Різні види варисторів



Рис.2.18 Підключення індуктивного навантаження та використання варистора



Рис.2.19 Схема роз'ємів зчитувача PR-01

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		59

На зчитувачі Proximity карток наявні наступні роз'єми:

- VCC – клемні з'єднувачі для підключення по стандарту RS-485;
- GND – клемний з'єднувач «загальний»;
- DATA – 1-Wire (Touch Memory);
- RED – підключення червоних світлодіодів;
- GREEN – підключення зелених світлодіодів;
- DATA0, DATA1 – 2 сигнальних проводи інтерфейсу Wiegand.

У випадку якщо користувач бажає встановити зчитувач по інтерфейсу Wiegand потрібно розуміти певні його особливості. Для зв'язку між таким зчитувачем та контролером СКУД використовується трипровідна шина, яка являє собою 2 сигнальних проводи та один загальний. В якості кабелю для з'єднань використовується вита пара п'ятої категорії. Сигнали що виходять із з'єднань DATA0 та DATA1 повинні передаватися у різних парах, а другий дріт пари підключається до «загальної» клеми.

Підключення за інтерфейсом 1-Wire простіше та показане на рисунку 2.20.

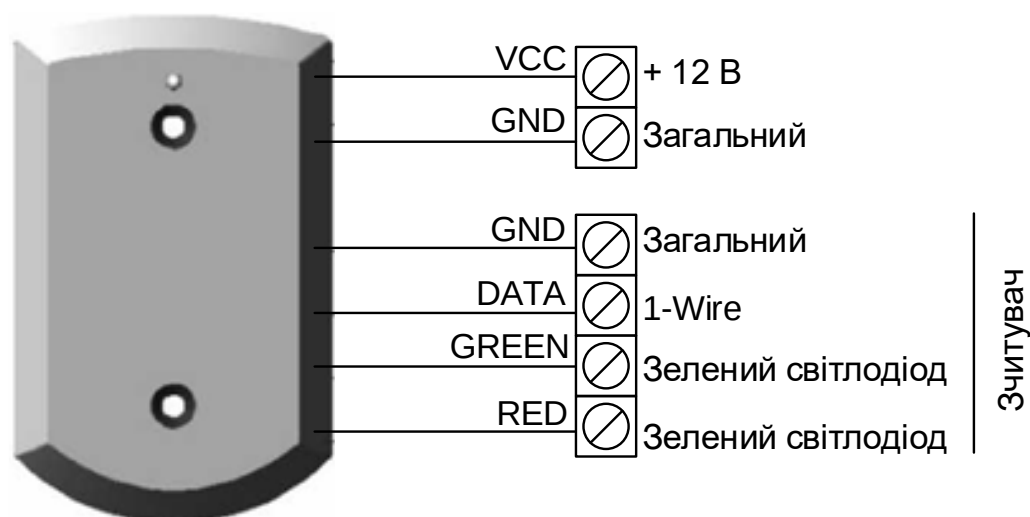


Рис.2.20 Підключення зчитувача по інтерфейсу 1-Wire

Також варто зауважити, що для стабільної роботи зчитувачів Proximity карток, при довжині дроту між контролером СКУД та зчитувачем більше 5 метрів, рекомендовано використовувати дріт типу вита пара та підключати його по схемі вказаній на рисунку 2.21.

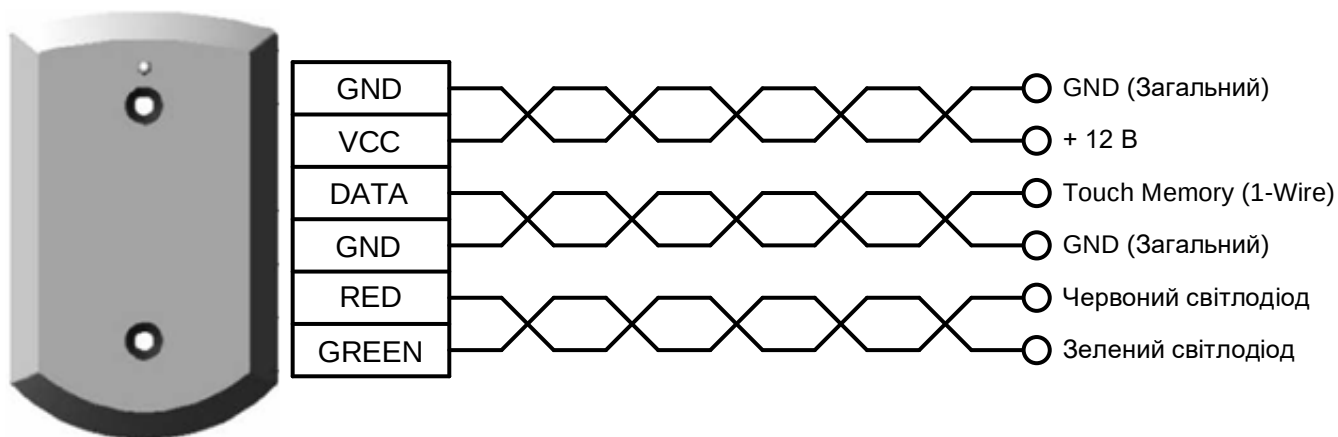


Рис.2.21 Рекомендоване підключення зчитувача Proximity карток

При встановленні більше ніж одного зчитувача мінімальна відстань між ними має бути не меншою за 20 см. Не рекомендується також встановлювати зчитувачі на металеві поверхні або поблизу масивних металевих конструкцій, оскільки це може слугувати причиною зниження відстані зчитування карт і особливо брелоків. Найчастіше саме це є причиною того, що зчитувач зчитує карти, але не брелоки, адже відстань зчитування брелоків менша.

Під час включення зчитувача пролунає відповідний сигнал. Світлова індикація визначається способом підключення зчитувача. За замовчуванням світлодіод горить помаранчевим кольором. При наявності картки в полі зчитувача, світлодіод гасне, а перехід у червоний або зелений режими світіння залежать від сигналів з контролера на виводах Green і Red та відповідають наданню та відмові у доступі.

Таблиця 2.6

Режим роботи світлодіода (+V= 3.5 – 5 В)

Стан світлодіоду	Напруга, яка подається на виводи	
	GREEN	RED
Зелений	+V або NC	GND
Червоний	GND	+V або NC
Помаранчевий	+V або NC	+V або NC

+V= 3.5 – 5 В.

NC – провід не приєднаний.

На рисунку 2.22 зображена функціональна схема системи конструйованої СКУД.

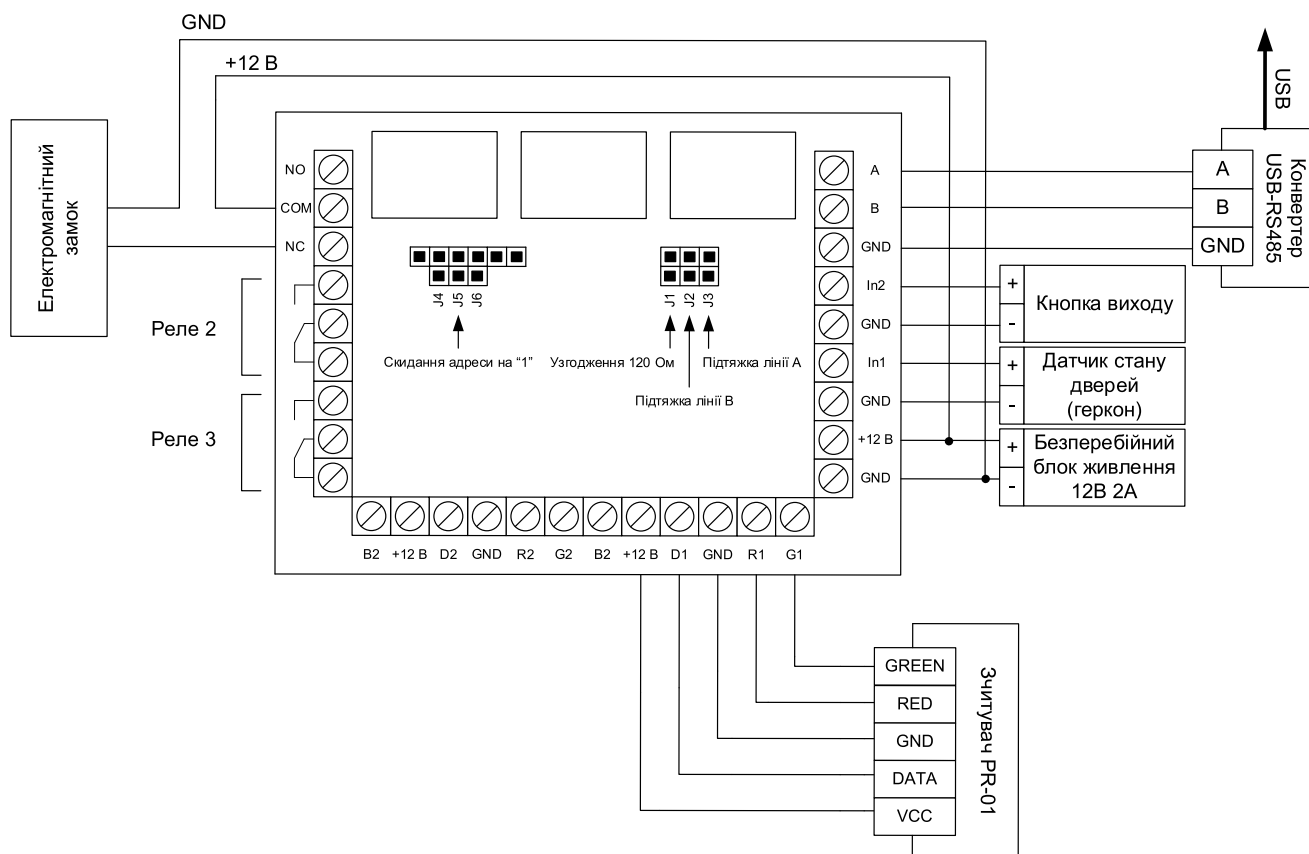


Рис.2.22 Функціональна електрична схема системи контролю і управління доступом навчальної лабораторії

Електромагнітний замок підключається до першого реле мережевого модулю керування СКУД іВС-01, до контакту що позначений як NC – normally closed. Цей контакт є нормально замкнутим в неробочому стані, тому в неробочому він забезпечує подачу електричного струму. При переведенні контакту у робочий стан, струм короткочасно переривається. Така конструкція контакту робить електрмагнітний замок працюючим увесь час, доки він під'єднаний до джерела струму. При піднесенні картки до зчитувача чи натисненні на кнопку виходу, з контролера СКУД йде сигнал до контакту, він вмикається та струм перестає іти. Це спричиняє розімкнення магніту та відкриття дверей. Одразу після відкриття струм починає іти до магніту і він знову працює, тому для того щоб двері закрилися не потрібно проводити більше ніяких дій.

Виходи In1 та In2, що розміщені на правій тороні плати модуля керування, використовуються для підключення до пристроїв, що можуть генерувати сигнали, наприклад, кнопки виходу, датчики руху, або інші подібні пристрої. Коли на ці

входи подається певний сигнал, плата може відповідно реагувати, наприклад, активувати реле або виконувати інші запрограмовані дії. У найшій системі до цих виходів підключені кнопка виходу та датчик стану дверей, або геркон.

Зчитувач підключається до мережного контролера СКУД за схемами, які були наведені вище. У нашому випадку було обрано саме підключення по інтерфейсу 1-Wire.

Висновки з другого розділу:

Проведено аналіз функціональних можливостей та технічних характеристик усіх елементів, а саме мережевого модуля контролю доступу iBC-01, зчитувача PR-01, електромагнітного замку KRF-200, безперебійного блоку живлення серії «ББП 20», акумуляторної кислотної батареї Mustang Energy, конвертеру USB - RS-485 та геркону. Розглянуто принцип роботи та завдання, які виконує програмне забезпечення для керування роботою СКУД – BigBrother. Розглянуто будову серверної та клієнтської частини додатку, а також надано певні рекомендації для його встановлення на ПК.

Розроблено структурну схему комплексу системи контролю і управління доступом у якій обраховано технічну можливість побудови стенду та зазначено функціональні обов'язки усіх складових мережі. Проведено аналіз функціонального призначення портів складових елементів системи та їх розшифрування. Наведено певні рекомендації з монтажу системи, що мають на меті роз'яснити процес побудови мережі, що буде працювати без помилок та завад.

Розроблена функціональна електрична схема готової системи контролю і управління на які було зазначено способи підключення усіх пристроїв мережі. Визначено основні аспекти роботи реле та вхідних контактів контролера, а саме першого реле, до якого підключений блок живлення та електромагнітний замок та контактів In1 та In2, до яких під'єднано кнопку виходу та датчик стану дверей.

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		63

РОЗДІЛ 3 РЕЗУЛЬТАТИ ЕКСПЕРИМЕНТАЛЬНИХ ДОСЛІДЖЕНЬ ПРОГРАМНО-АПАРАТНОГО КОМПЛЕКСУ СИСТЕМИ КОНТРОЛЮ І УПРАВЛІННЯ ДОСТУПОМ

3.1 Опис макету стенда програмно-апаратного комплексу системи контролю і управління доступом навчальної лабораторії

Беручи за основу розроблені у другому розділі структурну та функціональну електричні схеми було розроблено макет стенду програмно-апаратного комплексу системи контролю і управління доступом навчальної лабораторії. Для стенду було налаштовано сценарій по проведенню експериментальних досліджень, використовуючи ПЗ BigBrother.

Загальний вигляд розробленого макету стенду комплексу системи контролю і управління доступом представлено на рисунках 3.1 та 3.2.



Рис.3.1 - Загальний вигляд розробленого макету стенду комплексу системи контролю і управління доступом

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		64



Рис.3.2 - Загальний вигляд розробленого макету стенду комплексу системи контролю і управління доступом (з відкритими дверима)

До складу розробленого макету входять наступні пристрої (рисунок 3.1 та 3.2, зліва на право):

1. Кнопка виходу накладна ART-805.
2. Зчитувач Proximity карток PR-01.
3. Електромагнітний замок KRF-200.
4. Датчик стану дверей (геркон).
5. Мережевий модуль контролю доступу iBC-01.
6. Безперебійний блок живлення серії «ББП 20».
7. Конвертер USB - RS-485.

На рисунку 3.3 представлено дротове підключення пристроїв один до одного. Цей рисунок є фактичним представленням електронної функціональної схеми.

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		65

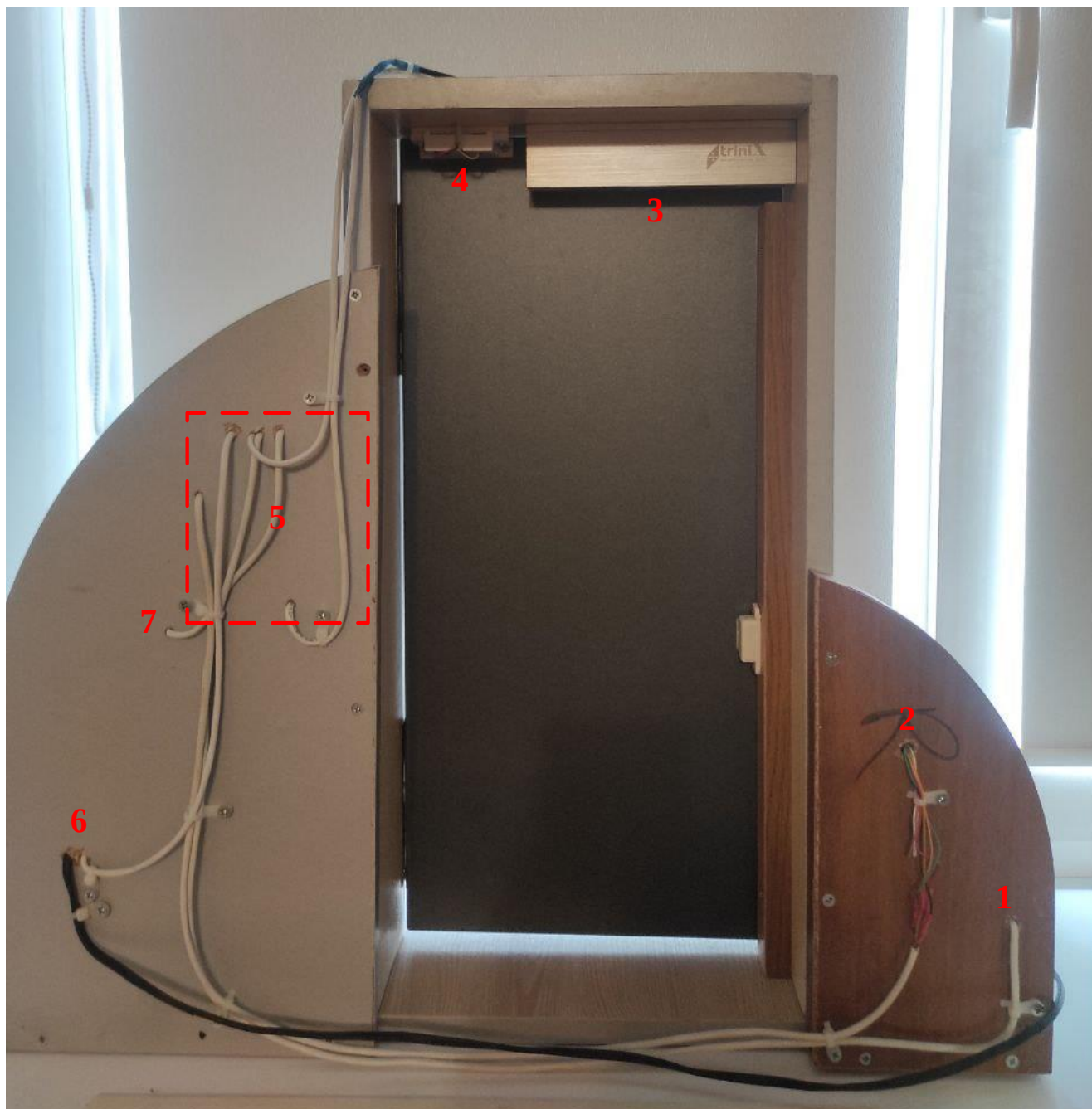


Рис.3.3 Дротове підключення пристроїв СКУД

На рисунку 3.4 представлено підключення пристроїв до мережевого модулю контролю доступу іВС-01. Червоним кольором зображено піни які були використані для підключення кожного конкретного пристрою.

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		66

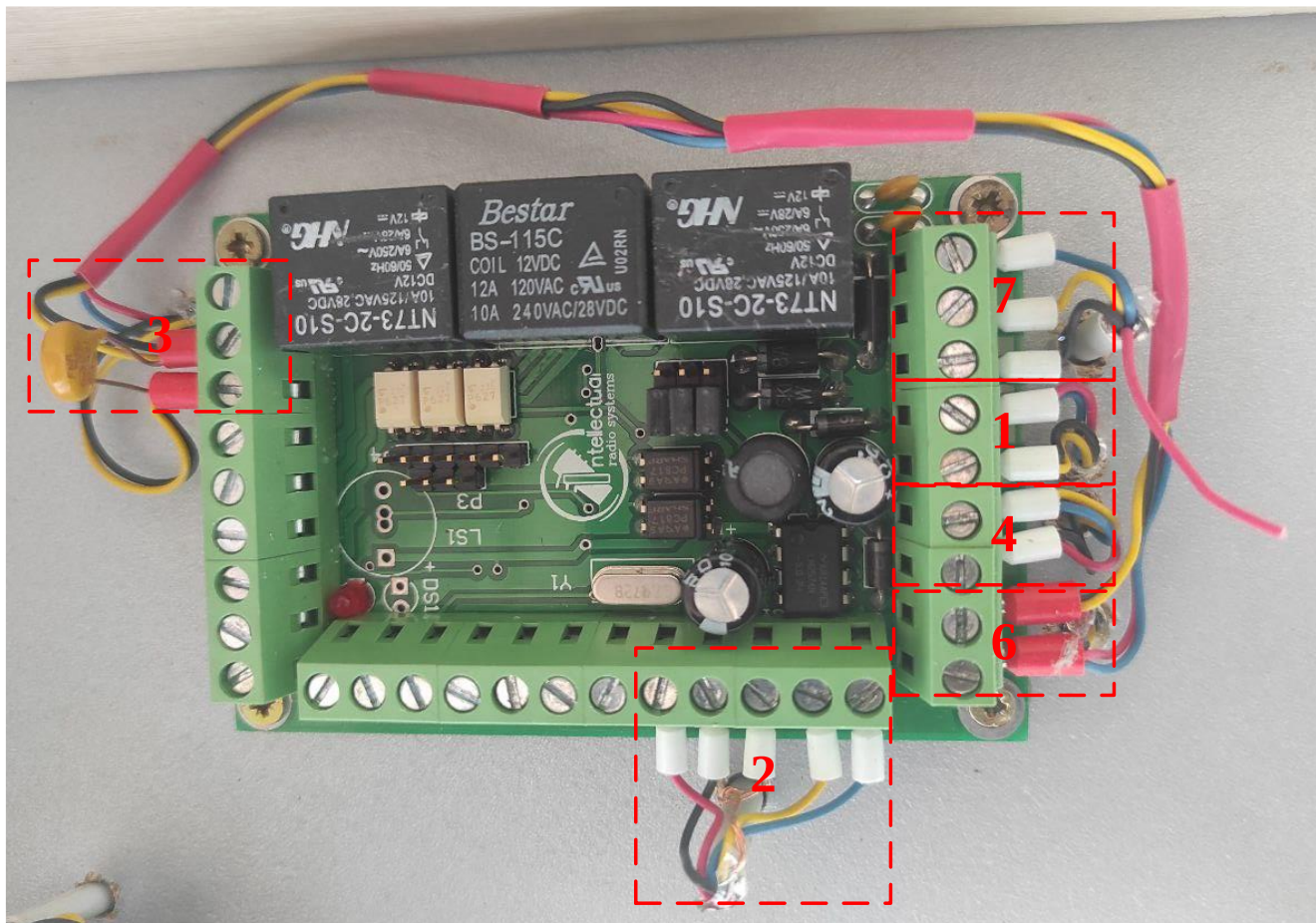


Рис.3.4 Підключення до мережевого модулю контролю доступу iBC-01

Зона 3 відповідає за підключення до мережевого модуля електромеханічного замка. Середній контакт реле, до якого здійснено підключення є загальним (COM). До нього здійснено підключення з блоку живлення, що відмічений на рисунку цифрою 6. Правий контакт реле підключений до електромагнітного замка є нормально замкнутим (NC), що дозволяє отримувати струм від джерела живлення, яке підключене до загального контакту. Такий вибір підключення зумовлений тим, що для роботи замка потрібне безперервне живлення, а нормально замкнутий контакт забезпечує його перебуваючи у неробочому стані. При появі необхідності відкрити двері мережевий модуль передасть сигнал від зчитувача карток чи кнопки виходу до цього реле. Воно у свою чергу перейде у робочий стан та тимчасово перерве електропостачання замка. У такій ситуації він перестане функціонувати та двері можна буде відкрити. Оскільки замок не залишається у неробочому стані, для повторного закриття дверей не потрібно знову натискати на кнопку чи прикладати картку до зчитувача.

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				67
Змн.	Арк.	№ докум.	Підпис	Дата		

Додатково можна побачити підключення варистора до контактів що йдуть до електромагнітного замка, який усуває негативний вплив індуктивного навантаження. Його наявність допоможе запобігти підгоранню контактів реле у випадку раптового збільшення струму.

У 2 зоні відмічено підключення до контролера зчитувача карток PR-01. Схема його підключення зображена на рисунку 2.20.

Контакти зони 1 та 4 відповідають за підключення кнопки виходу та датчику стану дверей. Підключені вони до контактів ln1 та ln2, що на мережевому контролері відповідають за підключення пристроїв, що генерують сигнали.

У зоні 6 відмічено підключення безперебійного блоку живлення до контактів призначених для підключення живлення пристроїв, а також до «землі». Сюди також підімкнений дріт заземлення електромагнітного замка.

На рисунку 3.5 видно підключення конвертора, що необхідний для налагодження зв'язку із комп'ютером на якому встановлено ПЗ для керування системою контролю і управління доступом. Зліва можна побачити підключення ліній А та В, а також заземлення, а справа USB-кабель, що проведений до ПК. Живлення конвертор отримує саме через USB.



Рис.3.5 Підключення конвертора USB - RS-485

Лінії А та В у RS-485 – це пара проводів, що використовується для передачі диференціальних сигналів. Сигнал передається як різниця напруг між цими двома

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		68

проводами. Це робить систему менш чутливою до завад, оскільки зовнішні електромагнітні перешкоди впливають на обидва дроти однаково, і різниця між ними залишається незмінною. Коли лінія А має більш високу напругу відносно лінії В, це інтерпретується як логічна одиниця (1). Коли лінія В має більш високу напругу відносно лінії А, це інтерпретується як логічний нуль (0).

Ще однією особливістю побудови макету стенду комплексу системи контролю і управління доступом є встановлення електромагнітного замка та геркону на дверну раму та рухому частину дверей. Результат встановлення наведено на рисунку 3.6.



Рис.3.6 Результат встановлення та підключення електромагнітного замка та датчику стану дверей

Електромагнітний замок встановлюється наступним чином, сам магніт кріпиться в кронштейні, який встановлюється на дверній рамі. Металева планка встановлюється на дверному полотні. Це необхідно для спрощення монтажу, адже провести комунікації до рухомої частини дверей набагато важче ніж до рами. Тим же принципом слід керуватися при встановленні датчика відкриття дверей, з єдиною відмінністю – магніт потрібно встановити на двері, а контакт, до якого буде здійснюватися підключення на дверну раму.

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		69

3.2 Встановлення і налаштування програмного забезпечення BigBrother та проведення експериментальних досліджень по роботі з ним

Для встановлення програмного забезпечення потрібно завантажити його з офіційного сайту компанії «Сайфрекс» та обрати варіант із встановленням серверної частини. Після підключення макету стенду до ПК потрібно буде обрати необхідний для підключення номер COM порту (рисунок 2.12).



Рис.3.7 Вибір порту при встановленні додатку

Після встановлення додатку для початку роботи потрібно в розділі Налаштування, обрати «Пристрої» та «Додати». Це дозволить обрати наш контролер доступу серед інших пристроїв, обрати порт та адресу підключення до нього а також обрати режим роботи (одно- чи дводверний).

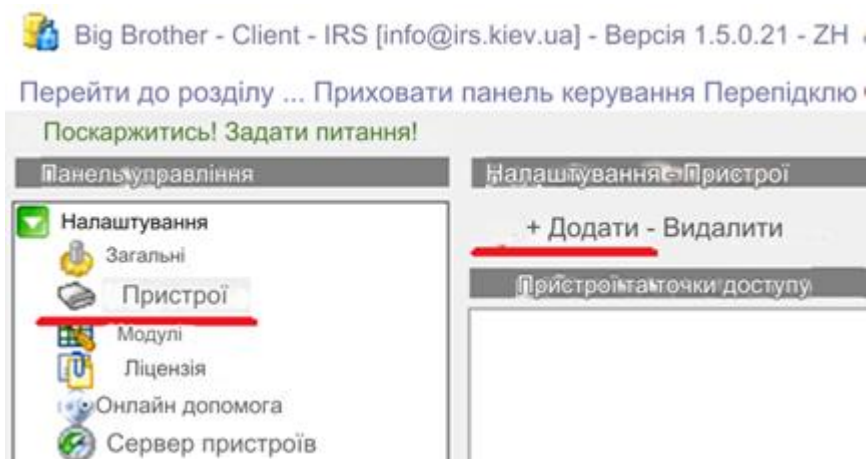


Рис.3.8 Обрання вкладки для додавання пристрою

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				70
Змн.	Арк.	№ докум.	Підпис	Дата		

Додавання нового пристрою

Загальні параметри

Адреса: 85

Назва: Контролер 1

Тип: Модуль контролю доступу IBC-01

Порт: COM3 Швидкість: 19200

Додаткові параметри

☒ Опитування з періодом, мс: 100

☐ Плавне програмування

Режим роботи: Односторонній (зчитувач на вхід та на вихід)

Контроль доступу та облік робочого часу



Максимальна кількість ключів: 100

OK Відміна

Рис.3.9 Додавання нового пристрою

Налаштування - Пристрої

+ Додати видалити Програмування Пошук зберегти зміни

Пристрої та точки доступу

Налаштування пристрою

Адреса: 85 Назва: Контролер 1

Тип: Модуль контролю доступу IBC-01

Порт: COM3 Швидкість: 19200

☒ Опитування з періодом, мс: 100

☐ Плавне програмування

Схеми та позначення роз'ємів

Загальні Зчитувачі та входи Реле Утиліти

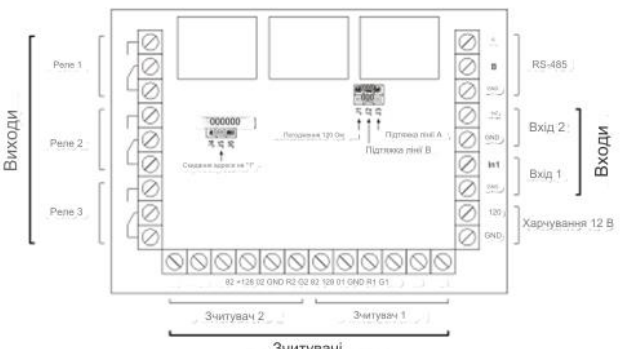


Рис.3.10 Успішне додавання нового пристрою

Рис.3.11 Інформація про зчитувачі та входи

ID	Порт	Адреса	Назва	Тип	Стан	Останнє опитування	Середнє
1	COM3	85	Контролер 1	Модуль контролю доступу IBC-01	Підключено	23:20:12	23 мс

Рис.3.12 Відображення підключеного пристрою на сервкері пристроїв

Появи мережевого контролера у цій вкладці означає появу зв'язку із ним. У випадку можливих технічних негараздів, на цій вкладці повинен бути статус пристрою.

Наступним кроком є реєстрація нового користувача. Вона відбувається у вікні «Бюро пропусків», вкладка «Користувачі». При натисканні на клавішу додати з'явиться діалогове вікно по заповненню інформації про користувача.

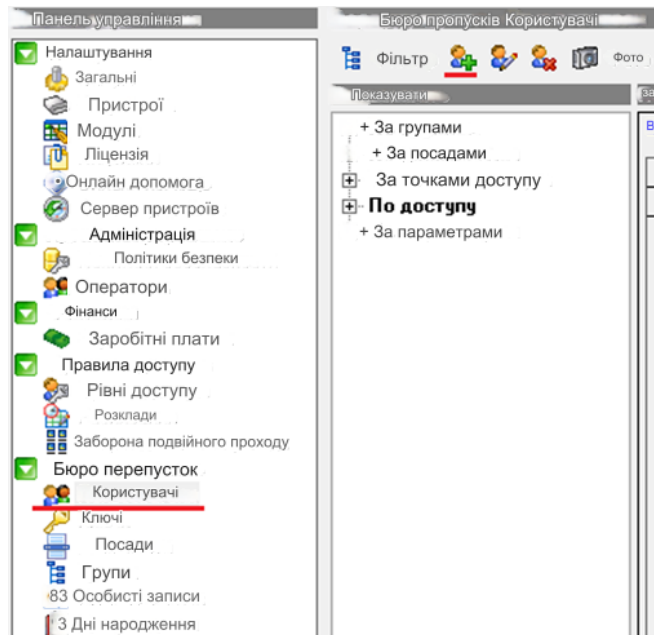


Рис.3.14 Вибір вкладки для реєстрації нового користувача у системі

У діалоговому вікні потрібно відмітити які параметри користувача буде задано. Існують можливості додати користувачу ПІБ, посаду, групу, рівень доступу, його ключ та додати фотографію. При обранні ключа для користувача є можливість обрати з декількох варіантів: вписати ключ вручну, обрати з готових ключів які містяться в БД, або зчитати ключ приклавши його з зчитувача.

Рис.3.14 Діалогове вікно створення користувача

Деякі параметри потрібно буде задавати у окремих діалогових вікнах, наприклад ім'я, фотографія та введення ключа користувача. На наступних слайдах будуть наведені ці вікна:

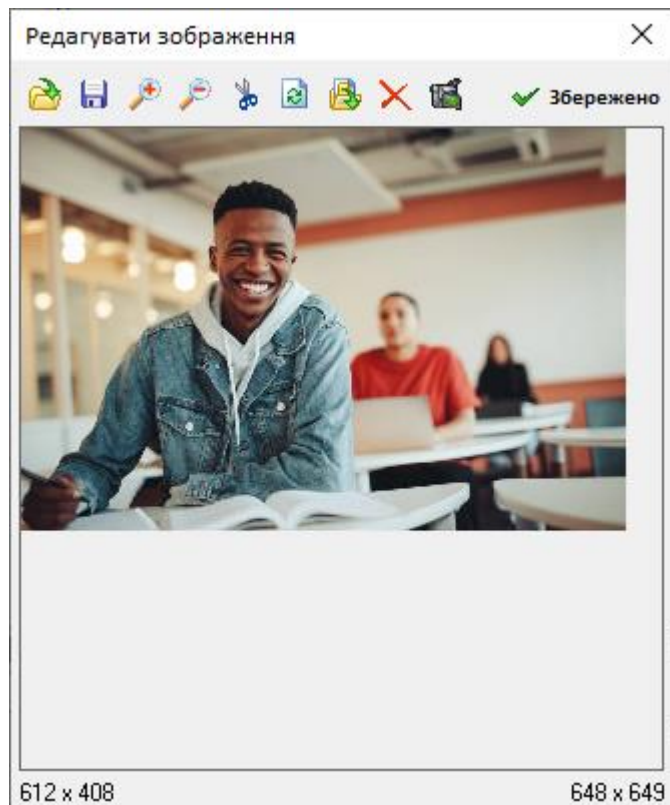


Рис.3.15 Встановлення фотографії користувача

Рис.3.16 Введення ПІБ користувача

Для того щоб зчитати ключ з пристрою необхідно у відповідному діалоговому вікні обрати бажаний пристрій та почати зчитування. У вікні з'явиться повідомлення про те, що ключ можна прикладати до зчитувача. У випадку ручного введення інформації про ключ можливо обрати формат введення серед наступних: серійний номер ключа, код ключа Touch Memory чи код ключа Wiegand (з комою). Також існує можливість додати вид ключа.

Після піднесення картки до зчитувача він відреагував звуковим сигналом, після чого поле з ключем заповнилося. Значення у ньому збігається із зазначеним на картці.

Введення ключа

Зчитати ключ з пристрою

Пристрій: [85] Контролер 1 Стоп

Додайте ключ до зчитувача

☐ Закрити вікно після зчитування ключа

Введення коду вручну

Ключ:

Формат: Серійний номер

☐ Привести до формату Weigand 26

☒ Прибрати код виробника картки

Тип ключа

Назва: Proximity карта/брелок

☐ Ввести ще один ключ ОК Відміна

Рис.3.17 Введення ключа

Введення ключа

Зчитати ключ з пристрою

Пристрій: [85] Контролер 1 Старт

Ключ успішно зчитано

☐ Закрити вікно після зчитування ключа

Введення ключа вручну

Ключ: 15170185

Формат: Серійний номер

☐ Привести до формату Weigand 26

☒ Прибрати код виробника картки

Тип ключа

Назва: Proximity карта/брелок

☐ Ввести ще один ключ ОК Відміна

Рис.3.18 Результат зчитування ключа

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				75
Змн.	Арк.	№ докум.	Підпис	Дата		



Рис.3.19 Код зображений на ключі

Наступним кроком буде встановлення правил доступу для створеного користувача. У вкладці «Доступ» потрібно буде натиснути кнопку «Додати». Після чого у діалоговому вікні потрібно буде обрати пристрій доступ до якого надається, тип доступу (цілодобовий або по розкладу), а також можливо буде обмежити час дії доступу чи кількість проходів даного користувача. Додатково можливо обрати коли користувачу зарахується прохід, який час після нього він матиме вільний доступ, а також буде відображено скільки проходів уже було зроблено.

Рис.3.20 Визначення правил доступу користувача

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		76

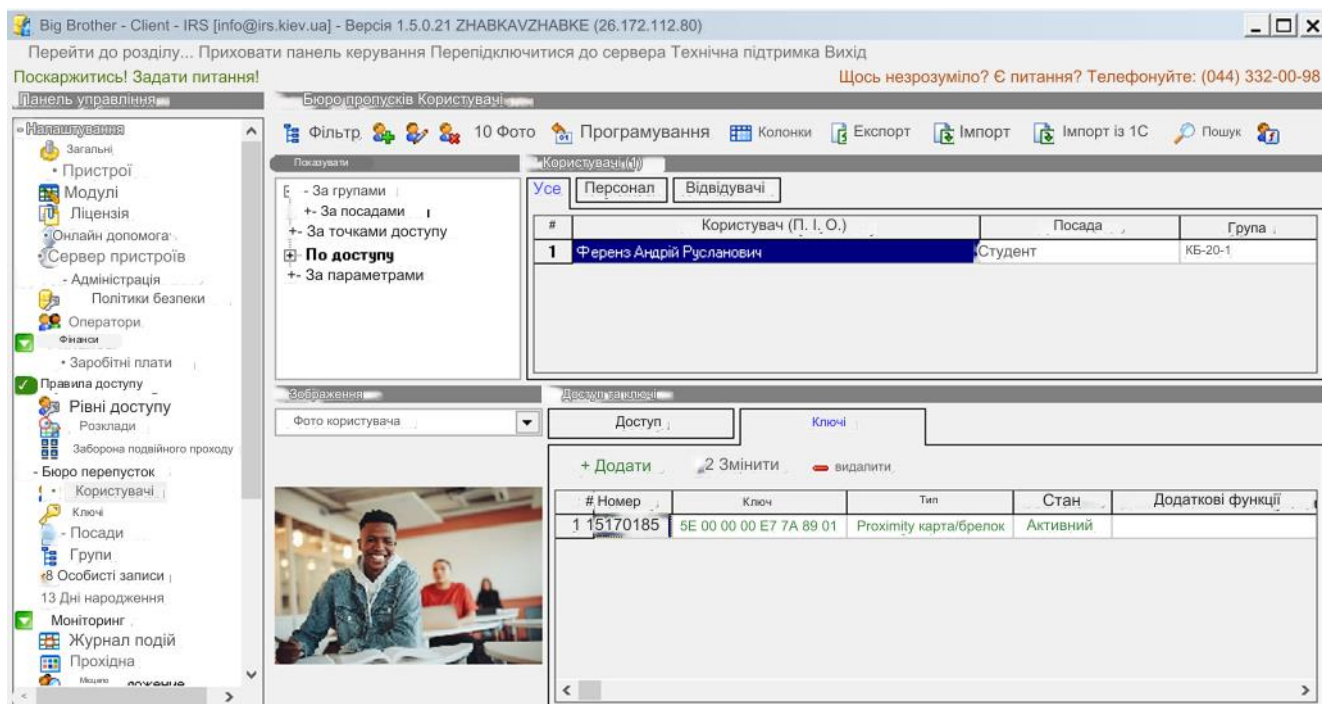


Рис.3.21 Відображення інформації про користувача

Після збереження налаштувань користувача, він з'явиться на вкладці «Користувачі», де буде видно абсолютно усю введену інформацію, та фотографію. Для внесення цієї інформації на контролер потрібно натиснути на кнопку «Програмування». Діалогове вікно сповістить про те, які дані записалися на контролер та чи збереження даних відбулося успішно.

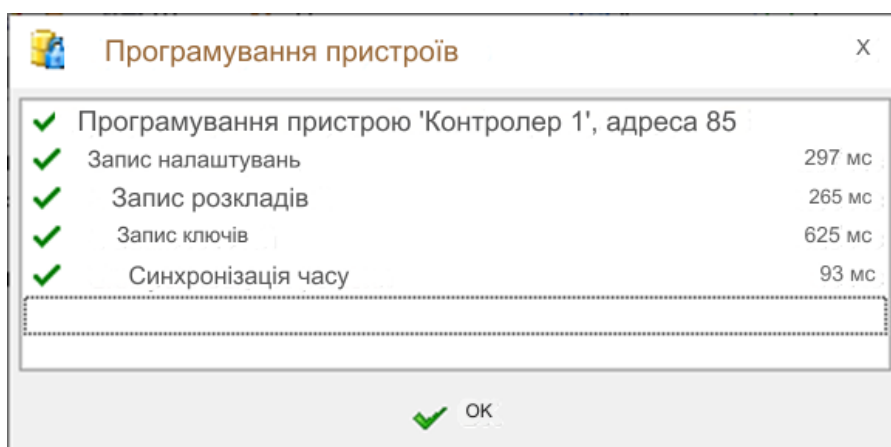


Рис.3.22 Успішне збереження налаштувань

У вкладці «Моніторинг» зберігається журнал подій, куди потрапляють записи про усі інциденти пов'язані з системою.

1	22.06.2024	00:35:14	Контролер 1	Невідомий ключ	Зчитувач 1
2	22.06.2024	00:35:12	Контролер 1	Невідомий ключ	Зчитувач 1
3	22.06.2024	00:34:10	Контролер 1	Двері зачинені	Вхід 1
4	22.06.2024	00:34:06	Контролер 1	Двері відчинені	Вхід 1
5	22.06.2024	00:34:05	Контролер 1 - Зчитувач 1	Доступ дозволено	Ференз Андрій Русланович
6	22.06.2024	00:31:05	Контролер 1	Двері зачинені	Вхід 1
7	22.06.2024	00:31:00	Контролер 1	Двері відчинені	Вхід 1
8	22.06.2024	00:30:59	Контролер 1 - Зчитувач 1	Доступ дозволено	Ференз Андрій Русланович
9	22.06.2024	00:30:27	Контролер 1	Двері зачинені	Вхід 1
10	22.06.2024	00:30:22	Контролер 1	Двері відчинені	Вхід 1
11	22.06.2024	00:30:21	Контролер 1 - Зчитувач 1	Доступ дозволено	Ференз Андрій Русланович
12	22.06.2024	00:30:10	Контролер 1	Двері зачинені	Вхід 1
13	22.06.2024	00:30:07	Контролер 1	Двері відчинені	Вхід 1
14	22.06.2024	00:30:06	Контролер 1	Нагнута кнопка	Вхід 2
15	22.06.2024	00:29:54	Контролер 1 - Зчитувач 1	Прохід не зафіксований	Ференз Андрій Русланович
16	22.06.2024	00:29:51	Контролер 1 - Зчитувач 1	Доступ дозволено	Ференз Андрій Русланович

Рис.3.23 Журнал подій

На рисунку 3.23 зображені записи із журналу подій. У них описана така інформація як: дата та час події, якого пристрою вона стосувалася (у випадку якщо у системі не один зчитувач), опис події та об'єкт якого ця подія стосувалася. До прикладу 11 запис свідчить про те, що користувач Ференз Андрій Русланович підніс картку до Зчитувача 1 о пів на першу. Оскільки цей користувач зареєстрований у системі та правила його доступу дозволяють йому пройти, система вирішила дозволити користувачу доступ та відчинила двері.

Перший та другий записи були зроблені після спроби відкрити двері незареєстрованою картою. Система позначила її як невідомий ключ та не відчинила двері.

Варто відмітити 15 запис, який свідчить про те що хоча доступ користувачу було дозволено, прохід не був зафіксований. Це сталося через те, що користувач після зчитування своєї картки не відчиняв двері впродовж певного часу, у нашому випадку цей часовий інтервал встановлено на 4 секунди (рисунк 3.11). Датчик стану дверей не подав сигналу про те, що двері було відкрито, тому система після 4-секундного очікування закрила двері та внесла запис про це до журналу подій.

У випадку оберненої ситуації, коли після проходу користувача, двері залишаються відкритими більше ніж 10 секунд, система сповіщає про це програмне забезпечення та робить відмітку у журналі подій.

1	22.06.2024	01:03:50	Контролер 1	Двері зачинені	Вхід 1
2	22.06.2024	01:02:31	Контролер 1	Двері не зачинені	Вхід 1
3	22.06.2024	01:02:22	Контролер 1	Двері відчинені	Вхід 1
4	22.06.2024	01:02:21	Контролер 1 - Зчитувач 1	Доступ дозволено	Ференз Андрій Русланович

Рис.3.24 Запис про незачинення дверей

Існує можливість змінити стан ключа будь-якого користувача у випадку якщо він його загубив та повідомив про це, або якщо цей ключ потрібно тимчасово заблокувати. Вхід по такому ключу буде заблоковано і виведено відповідне повідомлення. При повторному поверненню доступу картка одразу стає робочою знову.

Рис.3.25 Визначення ключа як втраченого

1	22.06.2024	01:47:54	Контролер 1 - Зчитувач 1	Доступ заборонено, ключ втрачено	Ференз Андрій Русланович
2	22.06.2024	01:47:38	Контролер 1	Програмування пристрою	
3	22.06.2024	01:47:37	Контролер 1	Запис налаштувань на пристрій	
4	22.06.2024	01:45:52	Контролер 1	Двері зачинені	Вхід 1
5	22.06.2024	01:45:50	Контролер 1	Двері відчинені	Вхід 1
6	22.06.2024	01:45:49	Контролер 1 - Зчитувач 1	Доступ дозволено	Ференз Андрій Русланович

Рис.3.26 Заборона доступу по загубленому ключу

В режимі прохідної, у оператора, який буде спостерігати за проходом, при відмітці користувача буде видна уся інформація про нього. В цьому режимі наведено більше інформації ніж у журналі подій. Відображається і фотографія користувача, його посада, група і тд. Видно також номер його ключа та вид доступу.

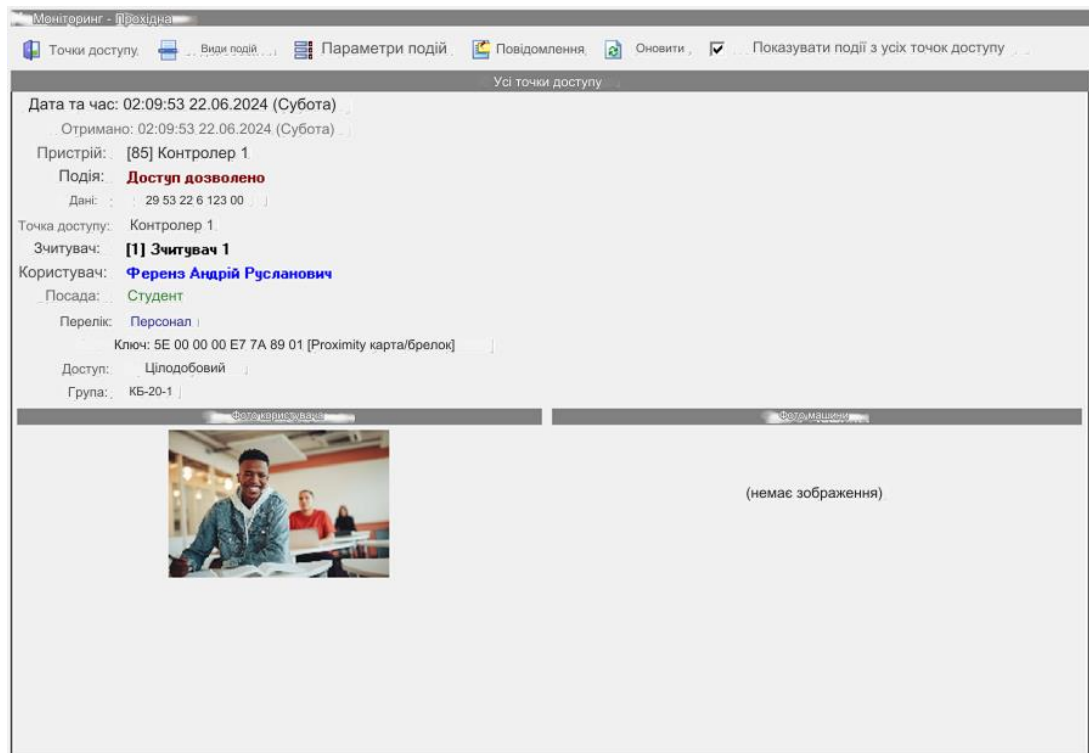


Рис.3.27 Моніторинг у режимі прохідної

Функціонал програми дозволяє вести облік подій та створювати звітність. У вкладці «Статистика проходів» розділу «Звітність» можливо побудувати графік кількості проходів та виходів кожного окремого користувача, або групи користувачів за будь-який визначений проміжок часу. Звіт по статистиці проходів створеного користувача за обраний період часу виглядатиме наступним чином:

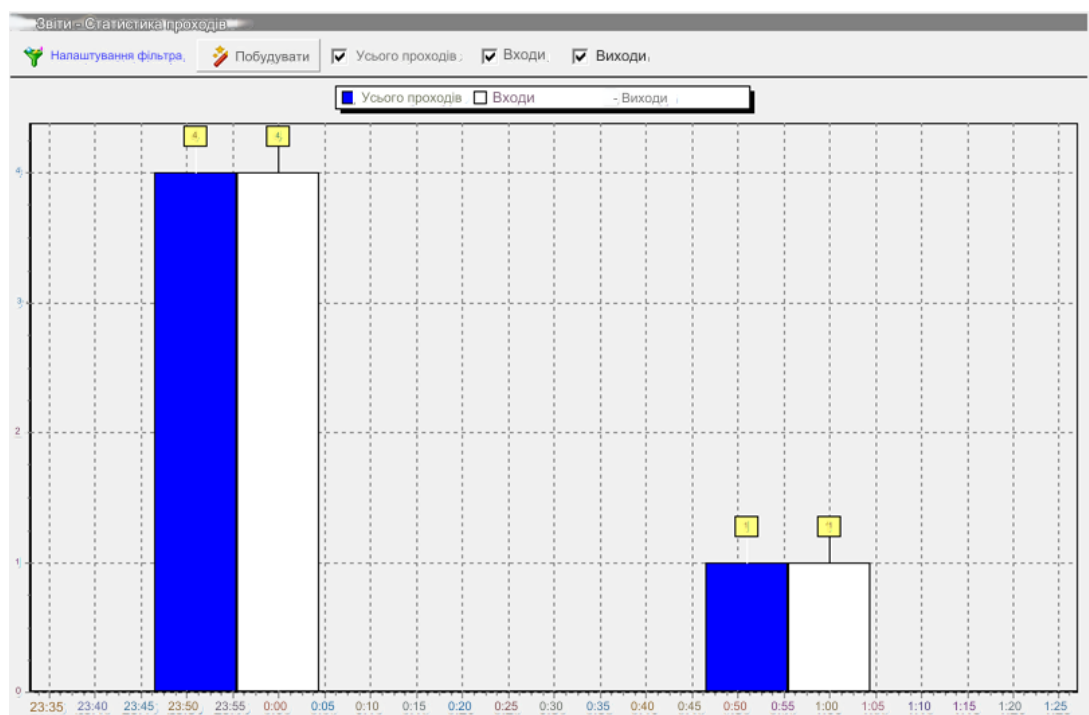


Рис.3.27 Графік проходів користувача

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				80
Змн.	Арк.	№ докум.	Підпис	Дата		

3.3 Рекомендації по застосуванню розробленої СКУД

Розроблений макет стенду програмно-апаратного комплексу системи контролю і управління доступом навчальної лабораторії є проектом, який презентує актуальну сферу сучасного сектору безпеки. Він може слугувати навчальною платформою для студентів, що вивчають такі дисципліни, як електроніка, комп'ютерна схемотехніка та системи технічного захисту інформації.

Макет стенду СКУД дозволить студентам на практиці отримати знання та вміння пов'язані із роботою, налаштуванням та підтримкою працездатності подібних систем на аналозі реальних програмно-апаратних комплексів, який складається з основних складових елементів та має повноцінний функціонал. Використання програмно-апаратного комплексу для контролю доступу дозволяє ознайомитися з принципами роботи автоматизованих систем, інтеграції апаратних та програмних компонентів, а також з концепціями інформаційної безпеки.

Навчальні заняття можна буде доповнити наступними елементами роботи зі стендом: встановлення драйверів для підключення особистих ПК студентів до існуючої мережі, додавання та налаштування пристроїв у програмному забезпеченні керування, програмування мережного контролера iBC-01. Налаштування пропусків для проходу може бути гарним елементом для практичних робіт, оскільки Proximity картки є недорогими, та ними можна забезпечити студентів на заняття, а після успішного налаштування легко скинути налаштування карток у системі, що дозволить використовувати їх багаторазово для багатьох навчальних груп.

Крім того, система може бути інтегрована з існуючими інформаційними системами навчального закладу для автоматичного ведення обліку відвідувань, що полегшить адміністративну роботу та дозволить автоматично генерувати звіти про використання лабораторії. Це забезпечить прозорість та підвищить контроль за навчальним процесом.

Також рекомендується використовувати систему для проведення наукових досліджень у галузі безпеки та інформаційних технологій. Лабораторія, оснащена такою системою, може стати базою для проведення експериментів та розробок у сфері інтернету речей (IoT), кібербезпеки та автоматизованих систем управління.

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		81

До прикладу даний стенд можливо доповнити модулем для мережної роботи та мати змогу налаштовувати та підключатися до нього з будь-якої точки по мережі інтернет.

Висновки з третього розділу:

Розроблено макет стенду програмно-апаратного комплексу системи контролю і управління доступом навчальної лабораторії, продемонстровано його загальний вигляд та підключення пристроїв. Усі пристрої було вказано та зазначено на зображеннях.

Проведено встановлення програмного забезпечення для керування СКУД BigBrother. У ньому було підключено модуль контролю доступу iBC-01, зазначено його адресу та режим роботи. Додатково було налаштовано параметри зчитувачів та входів а також перевірено підключення у сервері пристроїв.

Зареєстровано користувача, додано йому фотографію та прикріплено до його облікового запису ключ для входу, шляхом зчитування картки на зчитувачі. До створеного користувача були задіяні права доступу. Уся збережена інформація була записана на мережний контролер.

Протестовано вхід користувача з налаштованою та невідомою картками. Переглянуто журнал подій на наявність відповідних записів про спроби входу. Перевірено роботу системи у незвичайних ситуаціях, таких як невідкриття та незачинення дверей після піднесення картки та проаналізовано записи відповідних подій у журналі.

Переналаштовано ключ для зміни його статусу на загублений чи заблокований для перевірки доступу по такій картці. Наведена робота програми у режимі прохідної та під час створення звітності.

Надано рекомендації по застосуванню розробленого макета стенду СКУД у навчальному процесі та можливості використання під час роботи закладу.

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		82

ВИСНОВКИ

В результаті виконання випускної кваліфікаційної роботи було розглянуто систему контролю та управління доступом, а також розроблено схеми для побудови макету стенду СКУД для навчальної лабораторії.

На першому етапі проаналізовано актуальність теми та специфіку впровадження систем контролю і управління доступом до навчального процесу. Наведено визначення СКУД, сферу їх застосування та загальні її компоненти. Для них було визначено переваги та недоліки, різновиди реалізації та описані принципи за якими вони працюють. Визначено основні функції покладені на СКУД та наведено приклад взаємодії компонентів у такій системи та узагальнену апаратну схему.

Проведено аналіз ринку основних розробників технічних рішень для систем управління та контролю та їх головні продукти. Для цих компаній і їх розробок було визначено сильні сторони та особливості застосування.

На другому етапі було розглянуто функціональні можливості та технічні характеристики усіх елементів запропонованої СКУД. Розглянуто принцип роботи та завдання, які виконує програмне забезпечення для керування роботою СКУД – BigBrother. Розглянуто будову серверної та клієнтської частини додатку, а також надано певні рекомендації для його встановлення на ПК.

Розроблено структурну схему комплексу системи контролю і управління доступом у якій обраховано технічну можливість побудови стенду та зазначено функціональні обов'язки усіх складових мережі. Розроблена функціональна електрична схема готової системи контролю і управління на які було зазначено способи підключення усіх пристроїв мережі.

На третьому етапі було розроблено макет стенду програмно-апаратного комплексу системи контролю і управління доступом навчальної лабораторії, наведений його вигляд та дротове підключення. Вказано усі пристрої що використовуються у системі та позначено їх на рисунках.

Проведено встановлення на ПК програмного забезпечення для керування СКУД BigBrother, у якому було підключено мережевий модуль контролю доступу,

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		83

а також зазначено його адресу та режим роботи. Додатково налаштовано параметри зчитувачів та входів а також перевірено підключення у сервері пристроїв.

Для проведення перевірки працездатності розробленої системи зареєстровано користувача, додано йому фотографію та прикріплено до його облікового запису ключ для входу, шляхом зчитування картки на зчитувачі. До створеного користувача були задіяні права доступу. Уся збережена інформація була записана на мережний контролер.

Протестовано вхід користувача з налаштованою та невідомою картками. Переглянуто журнал подій на наявність відповідних записів про спроби входу. Перевірено роботу системи у незвичайних ситуаціях, таких як невідкриття та незачинення дверей після піднесення картки та проаналізовано записи відповідних подій у журналі. Для перевірки доступу по картці, яка була заблокована чи втарченна було переналаштовано ключ для зміни його статусу на відповідний. Наведена робота програми у режимі прохідної та під час створення звітності, а саме звіту по кількості проходжень певного користувача за обраний проміжок часу.

Надано рекомендації по застосуванню розробленого макета стенду СКУД у навчальному процесі та можливості використання під час роботи закладу.

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		84

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Рибальський О.В., Хахановський В.Г., Кудінов В.А. Основи інформаційної безпеки та технічного захисту інформації. – К.: Вид. Національної академії внутріш. справ, 2012. – 104 с.
2. Омельченко М. О. Характеристика та загальні вимоги до системи контролю і управління доступом. Сучасний захист інформації №4(44), 2020. DOI: 10.31673/2409-7292.2020.044650
3. Кушнір А. А., Чалий Д.С. Системи пожежної та охоронної сигналізації 2022. – с. 5–25.
4. Освітній портал [Електронний ресурс] – Режим доступу до ресурсу: <https://learn.ztu.edu.ua/course/view.php?id=1890>
5. Що таке СКУД і як це працює [Електронний ресурс] – Режим доступу до ресурсу: <https://idcard.com.ua/ua/blog/chto-takoe-skud-i-kak-eto-rabotaet/>
6. Системи контролю і управління доступом від А до Я [Електронний ресурс] – Режим доступу до ресурсу: <https://deps.ua/ua/knowegable-base/reference-information/7824.html#q3-1>
7. Контроль доступу [Електронний ресурс] – Режим доступу до ресурсу: https://expert112.com.ua/kontrol-dostupa/index_ua.html
8. Електрозамки. Особливості роботи [Електронний ресурс] – Режим доступу до ресурсу: Посилання: <https://svitzamkiv.ua/blog/elektrozamki-osoblivosti-roboti-montazhu-zastosuvannya/>
9. Fail Safe vs Fail Secure [Електронний ресурс] – Режим доступу до ресурсу: <https://www.getkisi.com/blog/fail-safe-vs-fail-secure>
10. Офіційний веб-сайт підприємства «HID Global» [Електронний ресурс] – Режим доступу до ресурсу: <https://www.hidglobal.com/solutions/access-control-systems>
11. Офіційний веб-сайт підприємства «Honeywell» [Електронний ресурс] – Режим доступу до ресурсу: <https://buildings.honeywell.com/us/en/home>
12. Офіційний веб-сайт підприємства «Lenel S2» [Електронний ресурс] – Режим доступу до ресурсу: <https://www.lenels2.com/en/>

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		85

13. Офіційний веб-сайт підприємства «SALTO» [Електронний ресурс] – Режим доступу до ресурсу: <https://saltosystems.com/en-gb/>
14. Офіційний веб-сайт підприємства «Suprema» [Електронний ресурс] – Режим доступу до ресурсу: <https://www.suprema.co.kr/en/main.asp>
15. Офіційний сайт компанії «Cyphrax» [Електронний ресурс] – Режим доступу до ресурсу: <https://cyphrax.com>
16. Офіційний сайт компанії «Trinix» [Електронний ресурс] – Режим доступу до ресурсу: <https://trinix.ua>
17. Мережевий контролер CYPHRAX iBC-01 [Електронний ресурс] – Режим доступу до ресурсу: <https://securitylab.com.ua/cyphrax-ibc-01/>
18. Зчитувач PR – 01 (B) [Електронний ресурс] – Режим доступу до ресурсу: <https://cyphrax.com/reader-pr-01-b/>
19. Замок електромагнітний накладний Trinix TML-200 [Електронний ресурс] – Режим доступу до ресурсу: <https://trinix.ua/product/zamok-magnitnyj-tml-200/>
20. Ніктон-С Блоки безперебійного живлення [Електронний ресурс] – Режим доступу до ресурсу: <http://www.nikton.com.ua/production/bbp.html#bbp20>
21. Імпульсний безперебійний блок живлення серії «ББП 20» [Електронний ресурс] – Режим доступу до ресурсу: <http://www.nikton.com.ua/doc/bbp20.pdf>
22. Кнопка виходу накладна ART-805 TRINIX [Електронний ресурс] – Режим доступу до ресурсу: <https://trinix.ua/product/knopka-vyrodu-nakladna-art-805-trinix/>
23. Облік робочого часу за 150 \$ [Електронний ресурс] – Режим доступу до ресурсу: <https://cyphrax.com/news/title-news-1/>
24. Дослідження дальності та швидкості передачі даних по скрученій парі в промислових мережах RS-485 та PROFIBUS [Електронний ресурс] – Режим доступу до ресурсу: <https://openarchive.nure.ua/handle/document/3612>
25. Що таке варистор: принцип роботи, конструкція та його застосування [Електронний ресурс] – Режим доступу до ресурсу: <https://uk.fmuser.net/content/?21147.html>

		Ференз А.Р.			ККІКБ.КР.Б – 125 – 19 – ПЗ	Арк.
		Котенко В.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		86