

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра спеціалізованих комп'ютерних систем

ГЕРЛЯХ Степан Романович

**Автоматизована система контролю доступу на територію
промислового об'єкту / Automated access control system for
an industrial facility**

спеціальність: 151 – Автоматизація та комп'ютерно-інтегровані
технології
освітньо-професійна програма – Автоматизація та комп'ютерно-
інтегровані технології

Кваліфікаційна робота

Виконала студентка групи АКІТ - 41
С.Р. Герлях

Науковий керівник
к.е.н., доцент А.М.Шевчук

Кваліфікаційну роботу допущено
до захисту:

«_____» _____ 2025 р.

Завідувач кафедри

_____ А.І.Сегін

ТЕРНОПІЛЬ – 2025

Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра спеціалізованих комп'ютерних систем
Освітній ступінь "бакалавр"

Спеціальність: 151 - Автоматизація та комп'ютерно-інтегровані технології
Освітньо-професійна програма – Автоматизація та комп'ютерно-інтегровані технології

ЗАТВЕРДЖУЮ

Завідувач кафедри СКС

А.І.Сегін

“___” _____ 20__ р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
ГЕРЛЯХ Степан Романович

(прізвище, ім'я по-батькові)

1. Тема кваліфікаційної роботи: Автоматизована система контролю доступу на територію промислового об'єкту / Automated access control system for an industrial facility.

керівник роботи

к.е.н., доцент А.М. Шевчук

затверджені наказом по університету від «28» листопада 2024 р. № 938

2. Строк подання студентом закінченої кваліфікаційної роботи: 15.05.2025р.

3. Вихідні дані до кваліфікаційної роботи:

1. Сучасні системи контролю та управління доступом.

2. Будова та функції систем контролю доступу.

3. Принцип роботи та керування систем контролю доступу.

4. Засоби автоматизації процесу контролю доступу.

4. Основні питання, які потрібно розробити:

1. Аналіз функцій та принципу побудови систем контролю і управління доступом.

2. Проектування автоматизованої системи контролю доступу на територію промислового об'єкта.

3. Реалізація системи автоматичного керування доступом на територію промислового об'єкта.

5. Перелік графічного матеріалу у роботі:

1. Архітектура АСКД.

2. Структурна схема АСКД.

3. Схема алгоритму ідентифікації та управління доступом.

4. Схема електрична принципова прототипу АСКД.

6. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Шевчук А.М.		
2	Шевчук А.М.		
3	Шевчук А.М.		

7. Дата видачі завдання 01 грудня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назви етапів випускної кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз функцій та принципу побудови систем контролю і управління доступом	12.2024р. – 01.2025р.	
2	Проектування автоматизованої системи контролю доступу на територію промислового об’єкта	02.2025р. – 03.2025р.	
3	Реалізація системи автоматичного керування доступом на територію промислового об’єкта	04.2025р. – 05.2025р.	

Студент

_____ Герлях С.Р.
(підпис)

Керівник роботи

_____ к.е.н., доцент Шевчук А.М.
(підпис)

АНОТАЦІЯ

Герлях С.Р. Автоматизована система контролю доступу на територію промислового об'єкту. – Рукопис.

Дослідження на здобуття освітнього ступеня «бакалавр» за спеціальністю 151 «Автоматизація та комп'ютерно-інтегровані технології», освітньо-професійна (наукова) програма. – Західноукраїнський національний університет, Тернопіль, 2025.

У роботі проаналізовано функціональні можливості та принципи побудови систем контролю доступу. Досліджено їх архітектуру та принципи керування. Розроблено автоматизовану систему контролю доступу, що підтримує інтеграцію з інформаційно-безпековими системами, незалежне управління доступом для пішоходів і транспорту, фіксацію подій, а також високу надійність і енергоефективність. Розроблено алгоритм роботи, що забезпечує ідентифікацію користувачів, реагування на аварійні ситуації та ведення журналу подій.

ANNOTATION

Herliakh, S.R. Automated access control system for an industrial facility. - Manuscript.

Doctoral studies for the education level «Bachelor'» with the title 151 Automation and Computer-Integrated Technologies. – West Ukrainian National University, Ternopil, 2025.

The work an analysis of the functional capabilities and design principles of access control systems. The architecture and control principles of such systems are examined. An automated access control system has been developed that supports integration with information and security systems, independent access management for pedestrians and vehicles, event logging, as well as high reliability and energy efficiency. An operational algorithm has been developed to ensure user identification, emergency response, and event log maintenance.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ.....	5
ВСТУП	6
1. АНАЛІЗ ФУНКЦІЙ ТА ПРИНЦИПУ ПОБУДОВИ СИСТЕМ КОНТРОЛЮ І УПРАВЛІННЯ ДОСТУПОМ.....	8
1.1 Призначення та функціональні можливості систем	8
1.2 Класифікація систем контролю доступу.....	10
1.3 Будова та основні елементи системи.....	15
1.4 Вимоги до розробки системи для промислового об'єкта.....	19
2. ПРОЕКТУВАННЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ НА ТЕРИТОРІЮ ПРОМИСЛОВОГО ОБ'ЄКТА.....	22
2.1 Дослідження архітектури системи контролю доступу.....	22
2.2 Розробка структури проектованої системи.....	28
2.3 Обґрунтування вибору технічних засобів для реалізації системи.....	30
3. РЕАЛІЗАЦІЯ СИСТЕМИ АВТОМАТИЧНОГО КЕРУВАННЯ ДОСТУПОМ НА ТЕРИТОРІЮ ПРОМИСЛОВОГО ОБ'ЄКТА.....	37
3.1 Розробка алгоритму роботи системи.....	37
3.2 Моделювання проектованої системи.....	41
3.3 Реалізація проектованої системи.....	43
ВИСНОВКИ.....	48
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	50
ДОДАТОК А Схема електрична принципова прототипу АСКД.....	53
ДОДАТОК Б Програмний код для моделювання роботи прототипу АСКД	54

					ДП.АКІТ.10660533.00.00.000ПЗ							
Змн.	Арк.	№ докум.	Підпис	Дата	Автоматизована система контролю доступу на територію промислового об'єкту / Automated access control system for an industrial facility			Літ.	Арк.	Акрушіє		
Розроб.		Герлях С.Р.									4	52
Перевір.		Шевчук А.М.						ЗУНУ.ФКІТ.АКІТ-41				
Консульт.		Шевчук А.М.										
Н. Контр.		Заставний О.М.										
Затверд.		Сегін А.І.										

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АРМ - автоматизоване робоче місце;

АСКД - автоматизована система контролю доступу;

БД - бази даних;

ВМ - виконавчий механізм;

ДБЖ - джерело безперебійного живлення;

КП - контрольний пункт;

ПЗ - програмний засіб;

СКУД - система контролю та управління доступом;

ТЗ - транспортний засіб.

					ДП.АКІТ.10660533.00.00.000ПЗ	Арк.
Зм.	Арк.	№ докум.	Підп.	Дата		5

ВСТУП

Актуальність теми. Промислові об'єкти, як правило, характеризуються великим масштабом, розгалуженою територією, складною інфраструктурою та багаторівневою організацією виробничих процесів. Це обумовлює специфічні вимоги до систем їх безпеки та необхідність обмеження доступу до окремих функціональних зон через високу вартість обладнання, потенційні ризики проникнення сторонніх осіб, викрадення матеріальних ресурсів (обладнання, продукції, сировини) чи витоку конфіденційної інформації, а також загрози порушення безперервності виробничого процесу. У таких умовах традиційні механічні або автономні засоби захисту не є достатньо ефективними, тому потребують модернізації та автоматизації.

Одним із важливіших напрямів забезпечення технічної безпеки є розробка та впровадження автоматизованих систем контролю доступу (АСКД). Такі системи володіють високим рівнем надійності, масштабованості та можливістю дистанційного керування. Вони дозволяють забезпечити ідентифікацію персоналу та транспорту, контроль їх переміщень, ведення журналу подій та реакцію на нештатні ситуації, а також здатні автономно приймати рішення, інтегруватися з іншими підсистемами безпеки та гнучко адаптуватися до змін умов експлуатації.

Актуальність обраної теми дослідження зумовлена потребою у створенні недорогих, ефективних і гнучких рішень, здатних забезпечити високий рівень безпеки та надійності функціонування системи в умовах промислового середовища. Впровадження сучасних засобів автоматизації, зокрема мікроконтролерів, сенсорної техніки, а також можливості моделювання систем у віртуальному середовищі до їх фактичної реалізації дають можливість створювати системи, що легко масштабуються та адаптуються до специфіки вимог конкретного об'єкта. Поєднання апаратних засобів з програмною логікою забезпечують основу для побудови інтелектуальних систем контролю та управління доступом (СКУД), які відповідають вимогам автоматизації та комп'ютерно-інтегрованих технологій.

Мета кваліфікаційної роботи є розробка АСКД, що відповідає вимогам

					ДП.АКІТ.10660533.00.00.000ПЗ	Арк.
Зм.	Арк.	№ докум.	Підп.	Дата		6

сучасних промислових об'єктів.

Поставлена мета обумовлює необхідність вирішення ряду завдань:

- проаналізувати функціональні можливості та типи систем контролю і управління доступом;
- дослідити архітектурні підходи до побудови СКУД;
- розробити структуру проектованої автоматизованої системи;
- обґрунтувати вибір технічних засобів для реалізації проектованої АСКД;
- реалізувати прототип автоматизованої системи контролю доступу.

Предметом дослідження є система контролю доступом до об'єктів промислової інфраструктури.

Об'єктом дослідження технічні засоби та алгоритми функціонування автоматизованих СКУД.

Методи дослідження - аналіз і синтез, математичне моделювання, методи системного аналізу та оптимізації, експериментальні дослідження.

Практичне значення одержаних результатів полягає у розробці АСКД, що дозволє централізовано контролювати та архівувати події, здійснювати моніторинг у реальному часі. Результати дослідження можуть бути використані під час проектування та впровадження аналогічних систем на підприємствах із розгалуженою інфраструктурою, де необхідне поєднання високої надійності, низької вартості впровадження та можливості масштабування.

Публікації.

1. Герлях Степан, Працінь Володимир, Давлетова Аліна Автоматизована система моніторингу та обмеження доступу до контрольованого об'єкту / Збірник матеріалів всеукраїнської науково-практичної конференції «Автоматизація та комп'ютерно-інтегровані технології» (АКІТ - 2025), Тернопіль, 2025.- с.31-34.

					ДП.АКІТ.10660533.00.00.000ПЗ	Арк.
						7
Зм.	Арк.	№ докум.	Підп.	Дата		

1. АНАЛІЗ ФУНКЦІЙ ТА ПРИНЦИПУ ПОБУДОВИ СИСТЕМ КОНТРОЛЮ І УПРАВЛІННЯ ДОСТУПОМ

1.1 Призначення та функціональні можливості систем

Сучасні вимоги до безпеки промислових об'єктів зумовлюють необхідність впровадження автоматизованих рішень для ідентифікації осіб та регулювання доступу. Одним із найефективніших засобів у цьому напрямі є система контролю та управління доступом (СКУД), яка дозволяє автоматизувати процеси пропуску, реєстрації, обмеження та моніторингу доступу персоналу, транспорту та відвідувачів.

СКУД (рисунок 1.1) це сукупність технічних і програмних засобів (ПЗ), призначених для організації та регулювання доступу осіб і транспорту до певних об'єктів або зон. Система дає змогу здійснювати ідентифікацію користувачів, регулювати їх доступ до певних приміщень чи зон, вести журнал подій та поєднуватися з іншими системами безпеки [1-3].

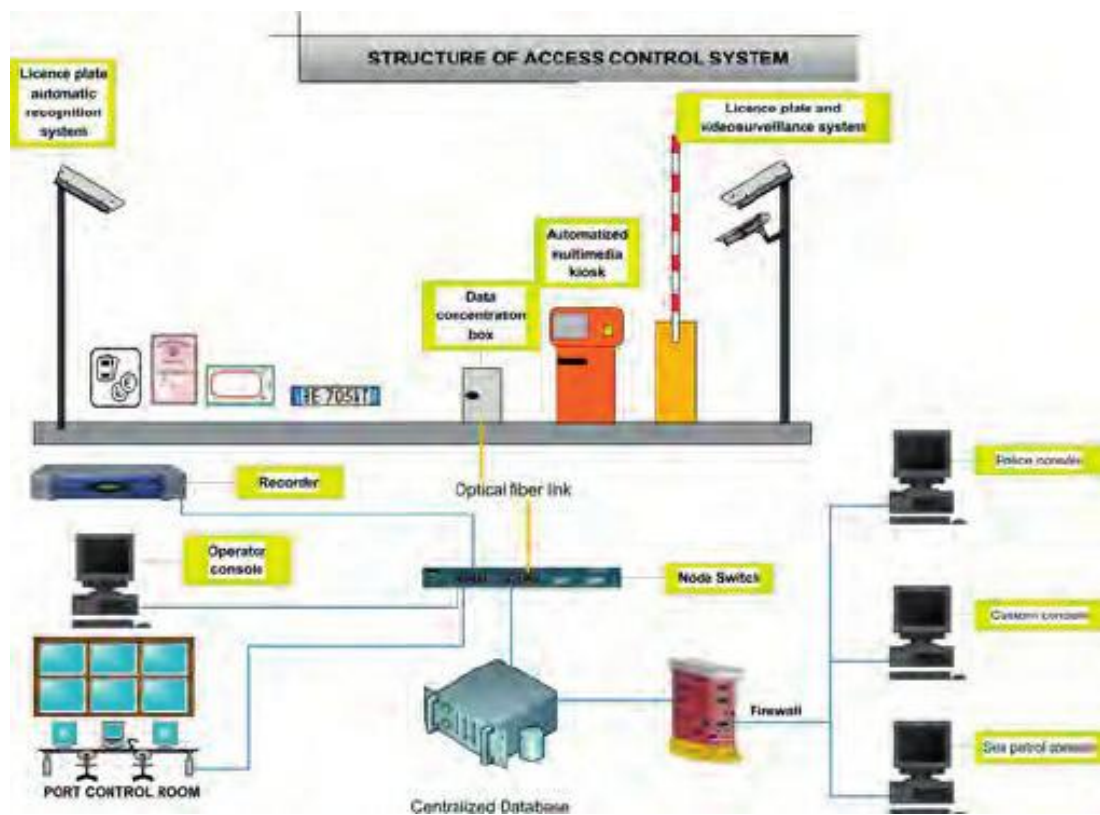


Рисунок 1.1 – Загальна будова СКУД

					ДП.АКТ.10660533.00.00.000ПЗ	Арк.
Зм.	Арк.	№ докум.	Підп.	Дата		8

Основне призначення СКУД полягає у забезпеченні автоматизованого регулювання доступу до певних зон або територій, а також у фіксації всіх подій, пов'язаних із переміщенням осіб чи транспортних засобів (ТЗ) [3, 4]. Така система дозволяє запобігати проникненню сторонніх осіб, контролювати наявність персоналу, вести облік робочого часу, а також реалізовувати політику обмеження доступу відповідно до рівня повноважень кожного користувача.

Крім забезпечення фізичної безпеки, СКУД сприяє оптимізації внутрішніх процесів підприємства [3-5]. Наприклад, шляхом реєстрації часу входу і виходу працівників система дозволяє ефективно управляти обліком робочого часу. Інтеграція СКУД з іншими інженерними мережами, такими як системи опалення, вентиляції, охоронної сигналізації або пожежної безпеки, відкриває додаткові можливості для автоматизації і енергозбереження. У разі відсутності персоналу в певній зоні система може автоматично вимикати освітлення або кондиціонування, що знижує загальні витрати на утримання об'єкта.

Функціональні можливості СКУД включають:

- надання доступу відповідно до розкладу або прав користувача;
- запис усіх подій у журналі для подальшого аналізу;
- створення звітів про присутність співробітників;
- автоматичне блокування при підозрілих діях;
- можливість евакуаційного розблокування;
- підключення до зовнішніх систем через API або інтерфейсні протоколи.

Найбільш поширеним є застосування таких систем на промислових підприємствах, об'єктах критичної інфраструктури, державних установах, у навчальних закладах, бізнес-центрах, а також на автостоянках, складах і в житлових комплексах.

СКУД є багатофункціональним інструментом, що поєднує функції безпеки, контролю, обліку та автоматизації, підвищуючи загальний рівень організованості й ефективності функціонування сучасних об'єктів.

					ДП.АКІТ.10660533.00.00.000ПЗ	Арк.
Зм.	Арк.	№ докум.	Підп.	Дата		9

1.2 Класифікація систем контролю доступу

Класифікація СКУД (рисунок 1.2) може здійснюватися за різними критеріями залежно від призначення, масштабності, принципу дії, типу носія доступу та рівня захисту [5-8]. За масштабністю можна виділити:

- індивідуальні (локальні) , що використовуються в межах однієї точки доступу, наприклад, для сейфу, одного входу до офісу тощо;
- групові - охоплюють кілька точок доступу в межах одного об'єкта, офісної будівлі, заводу та ін.;
- корпоративні - передбачають наявність багатьох об'єктів і забезпечують централізоване управління, наприклад, мережа підприємств;
- глобальні - підключаються до інших інформаційних та безпекових систем, наприклад відеомоніторингу, ERP, SCADA тощо.



Рисунок 1.2 - Класифікація СКУД

За способом ідентифікації користувача виділяють:

- системи, засновані на знанні певної інформації користувачем - використовують PIN-коди, паролі. Вони можуть бути менш безпечними через ризик розголошення коду або пароля, їх перевага полягає в простоті та низькій вартості реалізації;
- контактні - доступ відбувається за допомогою фізичних пристроїв. Це

					ДП.АКТ.10660533.00.00.000ПЗ	Арк.
Зм.	Арк.	№ докум.	Підп.	Дата		10

найбільш традиційний і поширений тип, який включає магнітні карти, proximity-карти та смарт-карти з мікрочипом, які можуть зберігати додаткову інформацію про користувача та його права доступу;

- безконтактні (RFID) - використовують карти, що працюють на основі RFID-технології, наприклад стандарти HID, EM-Marine, NFC. Карти, що працюють на основі технології RFID дозволяють здійснювати ідентифікацію без необхідності фізичного контакту між карткою та зчитувальним пристроєм. Це забезпечує швидкість та зручність доступу, що особливо важливо в місцях з великим потоком людей, таких як офісні будівлі та промислові підприємства. Такі системи набули поширення завдяки їх надійності.

- біометричні використовують унікальні фізіологічні характеристики людини для ідентифікації, такі як відбиток пальця, сітківки ока, розпізнавання обличчя або голосу;

- мобільні - включають використання мобільних пристроїв, таких як смартфони та планшети, для ідентифікації користувача через додатки або мобільні ключі, що використовують технології Bluetooth, NFC (ближнього поля) або QR-коди. Ці системи зручні, оскільки дозволяють користувачам не носити фізичні ідентифікатори.

- комбіновані системи передбачають поєднання кількох методів, наприклад, карта та PIN-код. Для підвищення рівня безпеки деякі СКУД вимагають двофакторної аутентифікації, наприклад, поєднання біометричного сканування та PIN-коду або магнітної карти та пароля. Це забезпечує додатковий рівень захисту, запобігаючи несанкціонованому доступу навіть у разі компрометації одного з ідентифікаторів.

СКУД поділяються на автоматизовані та автономні типи залежно від способу керування. За типом контролера виділяють:

- автономні - контролер керує доступом без зв'язку з ПК;
- мережеві - підключаються до ПК або сервера, дозволяють вести журнал подій;
- інтелектуальні - мають можливість обробки логіки доступу взаємодії з іншими системами (моніторингу, сигналізації тощо).

					ДП.АКТ.10660533.00.00.000ПЗ	Арк.
Зм.	Арк.	№ докум.	Підп.	Дата		11

Автономні системи підходять для здійснення контролю за доступом на невеликих об'єктах, таких як офіси або маленькі магазини, оскільки призначені для керування однією точкою доступу. На відміну від них, автоматизовані СКУД здатні забезпечити контроль доступу будь-якої складності, включаючи розгалужені мережі з десятками або сотнями контролерів. У таких системах кожен контролер пов'язаний з центральною базою даних (БД), що забезпечує обмін інформацією в режимі реального часу.

У межах СКУД ключову роль відіграє мережевий контролер. Його завданням є забезпечення взаємодії всіх компонентів системи з головним керівним комп'ютером або сервером. До таких компонентів належать зчитувачі, сенсори на дверях та інше обладнання. Цей елемент є основою для створення інтегрованої мережі, яка забезпечує єдине керування, моніторинг та аналіз інформації щодо авторизації доступу. Завдяки швидкому обміну даними, мережевий контролер дозволяє оперативно реагувати на будь-які зміни у системі доступу, адаптувати правила, оновлювати БД згідно з поточними вимогами.

Підтримка як дротових (Ethernet), так і бездротових технологій (Wi-Fi) передачі даних робить його універсальним і гнучким рішенням для масштабованих СКУД.

Автономний контролер функціонує самостійно, без постійного з'єднання з головним сервером або комп'ютером. Він підходить для контролю в невеликих приміщеннях, де достатньо обмеженої кількості точок доступу й не потрібне об'єднання в більш широку систему безпеки. Такі пристрої можуть зберігати інформацію про політику доступу, облікові записи користувачів і журнал подій, що дозволяє керувати доступом безпосередньо на місці.

Комбіновані СКУД поєднують функціональні можливості автономних і мережевих контролерів. Це дозволяє створити гнучку та масштабовану систему, здатну адаптуватися до різних умов експлуатації та вимог безпеки. У таких системах можуть використовуватись автономні контролери для окремих точок, які за потреби з'єднуються в централізовану мережу, що забезпечує координацію роботи всієї системи.

Бездротові СКУД надають змогу керувати доступом без прокладання

					ДП.АКІТ.10660533.00.00.000ПЗ	Арк.
Зм.	Арк.	№ докум.	Підп.	Дата		12

дротових комунікацій. Використовують різні бездротові технології, такі як Wi-Fi, Bluetooth, RFID, інші способи передачі даних між контролерами доступу, зчитувачами та центральною системою управління. Завдяки гнучкості та простоті інсталяції, бездротові СКУД підходять для об'єктів, де обмежено можливості монтажу кабелів, або коли необхідне швидке, малозатратне встановлення.

За функціональними можливостями можна виділити наступні СКУД:

- інформаційні, що ведуть облік входів/виходів, журнал подій;
- керуючі - дозволяють або забороняють доступ;
- системи з контролем проходу не дозволяють повторний вхід без попереднього виходу;
- інтегровані системи безпеки - працюють разом з відеоспостереженням, охоронною і пожежною сигналізацією.

За способом відкриття точки доступу можна виділити системи, що обладнані:

- турнікетами - для проходу людей;
- автоматичними шлагбаумами чи воротами для ТЗ;
- електромагнітними / електромеханічними замками дверей чи воріт;
- з безперешкодним проходом, в яких відбувається сканування на відстані, наприклад, UHF-мітки на автомобілях.

Класифікація СКУД за класами безпеки базується на рівні забезпечення безпеки, складності архітектури, ступеню захисту, можливістю взаємодії з іншими підсистемами безпеки та масштабованістю.

Системи базового (першого) класу призначені для забезпечення мінімального рівня безпеки. Вони зазвичай використовують прості методи контролювання доступу, наприклад, магнітні або безконтактні картки без додаткових засобів автентифікації. Такі СКУД підходять для приватних помешкань, невеликих офісів чи малих підприємств, де не ставляться жорсткі вимоги до захисту.

До категорії середнього (другого) класу відносять системи з розширеною функціональністю. Вони можуть поєднуватися з відеоспостереженням, охоронною сигналізацією та іншими технічними засобами охорони. Ідентифікація

					ДП.АКТ.10660533.00.00.000ПЗ	Арк.
Зм.	Арк.	№ докум.	Підп.	Дата		13

користувачів ускладнюється за рахунок використання смарт-карт, біометричних даних. Такі системи застосовуються в бізнес-центрах, освітніх закладах та на промислових підприємствах середнього рівня критичності.

СКУД високого класу (клас 3) призначені для об'єктів з підвищеними вимогами до безпеки - банків, військових частин, об'єктів критичної інфраструктури. Системи використовують багаторівневу ідентифікацію та автентифікацію, включаючи багатофакторну перевірку, шифрування каналів зв'язку та високий рівень взаємодії з іншими захисними системами. Контроль здійснюється за допомогою комбінації декількох ідентифікаційних параметрів, що ускладнює несанкціонований доступ.

Спеціалізований клас (клас 4) охоплює СКУД, розроблені для унікальних і високоспецифічних завдань, зокрема там, де вимагається найвищий рівень захисту як фізичної безпеки, так і інформації. Вони можуть включати новітні технології розпізнавання по ході, голосу, тощо. Такі системи застосовуються в наукових лабораторіях, спецслужбах або на стратегічно важливих об'єктах.

Класифікація СКУД може базуватися на різних критеріях, можливостях що забезпечує система чи сферах застосування, враховувати мету та завдання використання системи. Поділ СКУД за функціональними можливостями дозволяє розрізняти системи за їхнім основним призначенням, зокрема це контроль доступу на територію, управління потоком працівників, ведення обліку часу, контроль доступу в житлових будинках чи автоматизація проїзду ТЗ.

В залежності від застосування можна виділити СКУД промислових об'єктів, що забезпечують контроль доступу до території підприємства тчи його; офісних приміщень чи освітніх закладів - для контролю працівників, учнів, відвідувачів; житлових комплексів - доступ мешканців, гостей, сервісу; паркінгів - контроль в'їзду/виїзду ТЗ, тощо.

Кожен тип СКУД має свої вимоги до архітектури, типу ідентифікації, обладнання та рівня взаємодії з іншими підсистемами безпеки. Тому їх класифікація дозволяє правильно обрати СКУД відповідно до рівня ризику та характеру об'єкта, що охороняється.

					ДП.АКІТ.10660533.00.00.000ПЗ	Арк.
Зм.	Арк.	№ докум.	Підп.	Дата		14

1.3 Будова та основні елементи системи

Сучасні СКУД, зазвичай, складаються з наступних основних елементів (рисунок 1.3) [1-3, 9]:

- контролери доступу - логічні пристрої, які приймають рішення про надання або заборону доступу на основі отриманих даних від зчитувачів. Вони можуть бути автономними або інтегрованими в мережу для централізованого управління;
- зчитувачі - пристрої, які здійснюють зчитування даних з ідентифікаторів для ідентифікації користувача . Вони можуть підтримувати різні методи аутентифікації;
- ідентифікатори - носії, які використовуються для ідентифікації користувача, наприклад магнітні чи пластикові карти, RFID, біометричні дані, , мобільні додатки тощо;
- виконавчі механізми (ВМ) - забезпечують фізичне блокування чи розблокування доступу, наприклад електронні замки, ригелі, запори, турнікети, шлагбауми;
- ПЗ - інтерфейс для адміністрування та керування системою, налаштування прав доступу, моніторинг та аналітика. Вони дозволяють оновлювати БД та управляти записами інцидентів безпеки, а також синхронізувати роботу системи з іншими елементами безпеки, зокрема, системи охоронної сигналізації, моніторинговими системами тощо;
- джерела безперебійного живлення (ДБЖ) - забезпечують безперервність роботи системи під час аварійного відключення електроенергії;
- мережева інфраструктура - для підключення всіх компонентів системи до локальної або хмарної БД, поєднання з іншими системами. Може включати як проводові, так і бездротові технології (Wi-Fi, Ethernet, Bluetooth, 4G/5G тощо).
- додаткові елементи, інтерактивні пристрої та системи моніторингу. Зокрема клавіатури для введення паролів використовуються для додаткової аутентифікації, наприклад, для введення PIN-кодів або паролів. Можуть бути поєднані з іншими методами ідентифікації. Екрани та монітори відображають

					ДП.АКТ.10660533.00.00.000ПЗ	Арк.
Зм.	Арк.	№ докум.	Підп.	Дата		15

статус доступу, дозволяють користувачам вводити дані, а також можуть відображати інтерфейси для адміністратора системи.



Рисунок 1.3 – Компоненти СКУД

У СКУД застосовуються різні ключі доступу (рисунок 1.4). Найбільш поширеними є картки, серед яких використовуються магнітні картки, оснащені магнітною смугою, на якій збережено інформацію про користувача. Щоб зчитати дані, картку потрібно провести через магнітний зчитувач. Proximity-картки є безконтактними. Вони працюють на основі RFID-технології, що дозволяє зчитувати інформацію без прямого фізичного контакту з пристроєм зчитування. Відстань зчитування зазвичай становить кілька сантиметрів.

Смарт-картки з мікрочипом мають вбудований мікропроцесор, який здатен зберігати значний обсяг інформації: дані користувача, історію доступу, криптографічні ключі тощо. Такі картки можуть бути як контактними, так і безконтактними. Деякі смарт-картки здатні зберігати біометричні дані користувача, що дозволяє реалізувати двофакторну автентифікацію для підвищення рівня безпеки.

					ДП.АКТ.10660533.00.00.000ПЗ	Арк.
Зм.	Арк.	№ докум.	Підп.	Дата		16

Гібридні картки поєднують кілька технологій, наприклад, магнітну смугу з мікрочипом або RFID-модуль із мікропроцесором. Це дозволяє використовувати одну картку в різних системах. Використовуються також картки, що мають спеціальну схему з вбудованих провідників, яка зчитується спеціалізованими пристроями. Такі ідентифікатори застосовуються в системах, де необхідна підвищена стійкість до копіювання.



Рисунок 1.4 – Види ідентифікаторів

СКУД можуть використовувати різні типи ВМ, які впливають на способи керування доступом до об'єкта або зони безпеки. На практиці використовується велике коло ВМ (рисунок 1.5). Електромеханічні замки - одні з найпопулярніших механізмів, які можуть керуватись за допомогою карт доступу, PIN-кодів, біометричних даних тощо. Такі замки забезпечують високий рівень безпеки та можуть встановлюватися на двері різного типу. Вони працюють на основі електромагнітної сили, що утримує двері зачиненими. Підходять для встановлення на скляних дверях або в тих місцях, де потрібне естетично привабливе рішення без видимих механізмів.

Турнікети, хвіртки застосовуються для обмеження доступу в громадських місцях - спортзалах, офісних центрах, транспортних вузлах. Оснащуються різними засобами ідентифікації для автоматичного керування проходом.

Шлагбауми використовуються для контролю в'їзду та виїзду з територій підприємств, паркінгів, приватних володінь. Керування шлагбаумами може здійснюватися дистанційно - за допомогою RFID-міток, розпізнавання номерних

					ДП.АКІТ.10660533.00.00.000ПЗ	Арк.
Зм.	Арк.	№ докум.	Підп.	Дата		17

знаків та інших технологій ідентифікації.

Електронні ригелі, засувки встановлюються всередині дверної конструкції та керуються різними типами ідентифікаторів. Забезпечують додатковий рівень безпеки, блокуючи або розблоковуючи механізм замикання дверей.

Доводчики з функцією контролю за доступом. Такі пристрої не лише забезпечують плавне зачинення дверей, але й можуть взаємодіяти з СКУД для автоматичного відкриття чи зачинення дверей у заданий час.



Рисунок 1.5 – Фізичні пристрої блокування доступу

ВМ є ключовим елементом будь-якої СКУД, і їх вибір залежить від конкретних умов експлуатації, вимог до безпеки та типу об'єкта.

У СКУД застосовуються різноманітні типи ідентифікації (рисунок 1.6), що дозволяє адаптувати систему під конкретні умови експлуатації та вимоги безпеки. Пристрої зчитування відіграють ключову роль у процесі ідентифікації користувача, забезпечуючи зчитування даних з різних типів ідентифікаторів. Серед них - зчитувачі безконтактних RFID-карт (HID, EM-Marine, MIFARE), зчитувачі смарт-карт із чипом, клавіатури для введення PIN-коду, а також біометричні сканери (відбитків пальців, обличчя, райдужної оболонки ока тощо). Сучасні мультимедійні зчитувачі можуть підтримувати кілька методів ідентифікації одночасно, що забезпечує гнучкість у побудові рівнів доступу та дозволяє використовувати багатфакторну аутентифікацію для підвищення загального рівня безпеки системи.



Рисунок 1.6 – Типи зчитувачів

СКУД це комплексні рішення, які дозволяють адміністраторам дистанційно регулювати допуск до приміщень або територій, застосовуючи багатофакторну аутентифікацію. До таких методів ідентифікації входять біометричні дані, електронні ключі або введення PIN-кодів, що значно підвищує рівень безпеки об'єкта.

СКУД ефективно взаємодіють з іншими системами, утворюючи комплексне рішення для повного контролю над безпекою на об'єкті. Функції журналювання та аудиту дозволяють фіксувати всі події, що відбуваються в системі, забезпечуючи можливість виявлення несанкціонованих спроб доступу та подальшої оптимізації політик безпеки.

Ще однією важливою характеристикою СКУД є масштабованість система може легко адаптуватися до потреб організації, що зростає: додавати нові точки доступу, збільшувати кількість користувачів, не порушуючи загальної структури. Гнучкість налаштувань дозволяє адміністраторам задавати індивідуальні правила доступу відповідно до специфіки бізнес-процесів чи особливих вимог установи.

1.4 Вимоги до розробки системи для промислового об'єкта

Для промислового об'єкта оптимальний варіант архітектури СКУД залежить від кількох факторів, таких як масштаб об'єкта, рівень безпеки, потреби в інтеграції з іншими системами безпеки, а також можливості майбутньої масштабованості [4, 6, 10].

Проектована АСКД має не лише забезпечувати фізичну безпеку об'єкта, але

					ДП.АКІТ.10660533.00.00.000ПЗ	Арк.
Зм.	Арк.	№ докум.	Підп.	Дата		19

й оптимізувати виробничі процеси, забезпечуючи ефективне функціонування підприємства. Система повинна забезпечити безперешкодний доступ для авторизованих осіб, зберігаючи при цьому високий рівень контролю та безпеки. Важливим аспектом є мінімізація людського втручання та автоматизація рутинних операцій, що дозволяє знижувати ймовірність помилок і збоїв, водночас підвищуючи загальний рівень безпеки. АСКД повинна мати здатність адаптуватися до змін у робочих процесах і бути досить гнучкою для управління різноманітними сценаріями доступу, враховуючи різні категорії персоналу та специфіку робочих змін. У той же час, важливо, щоб система не впливала на оперативну діяльність і дозволяла швидкий доступ до ресурсів підприємства без затримок, що може призвести до зниження продуктивності.

Основними вимогами до проекрованої АСКД є:

- надійність і безперервність роботи - система повинна функціонувати стабільно в умовах можливих електромагнітних завад, перепадів напруги, екстремальних температур та інших промислових факторів;
- масштабованість - можливість розширення системи без необхідності повної заміни технічних чи ПЗ при збільшенні кількості об'єктів контролю або користувачів;
- гнучкість у налаштуванні - забезпечення диференціації доступу за категоріями персоналу, видами робіт, зонами відповідальності тощо;
- можливість взаємодії з іншими підсистемами підприємства - взаємодія з системами відеоспостереження, сигналізації, обліку робочого часу, тощо;
- автоматизація процесів - зчитування ідентифікаторів доступу, реєстрація подій у БД, можливість віддаленого управління доступом;
- захист від несанкціонованого доступу - передбачення механізмів виявлення спроб злому, підміни або несанкціонованого доступу;
- зручність експлуатації - інтуїтивно зрозумілий інтерфейс ПЗ, зручні механізми обліку та моніторингу доступу, спрощене налаштування системи для операторів і адміністраторів.

На промислових об'єктах доцільно використовувати автоматизовану СКУД

					ДП.АКІТ.10660533.00.00.000ПЗ	Арк.
						20
Зм.	Арк.	№ докум.	Підп.	Дата		

з можливістю інтеграції різних типів зчитувачів, біометричних технологій, електромагнітних замків, турнікетів і безконтактних карт. Така система дозволяє забезпечити високий рівень безпеки, швидке реагування на зміни в доступі, а також масштабованість для розширення в майбутньому.

Для проекрованої системи АСКД на промисловому об'єкті, доцільно використовувати:

- групову або корпоративну мережеву систему;
- безконтактну ідентифікацію;
- гнучку систему проходу шлагбауми/турнікети;
- суміщення з відеоспостереженням;
- резервне живлення.

					ДП.АКІТ.10660533.00.00.000ПЗ	Арк.
Зм.	Арк.	№ докум.	Підп.	Дата		21

2. ПРОЕКТУВАННЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ НА ТЕРИТОРІЮ ПРОМИСЛОВОГО ОБ'ЄКТА

2.1 Дослідження архітектури системи контролю доступу

Дослідження архітектурних особливостей АСКД дозволяє оптимізувати їх функціональність, забезпечити безперебійний контроль доступу та поєднання з іншими інфраструктурними системами підприємства. Завдяки гнучкій архітектурі та впровадженню сучасних технологій, АСКД можуть бути адаптовані до різних масштабів об'єктів - від малих офісів до великих підприємств з багаторівневим захистом. Основною метою таких систем є забезпечення фізичної безпеки, автоматизація процесу контролю доступу, облік відвідувань і обмеження доступу для неавторизованих осіб [11-13].

На рисунку 2.1 зображено загальну архітектуру системи [11].

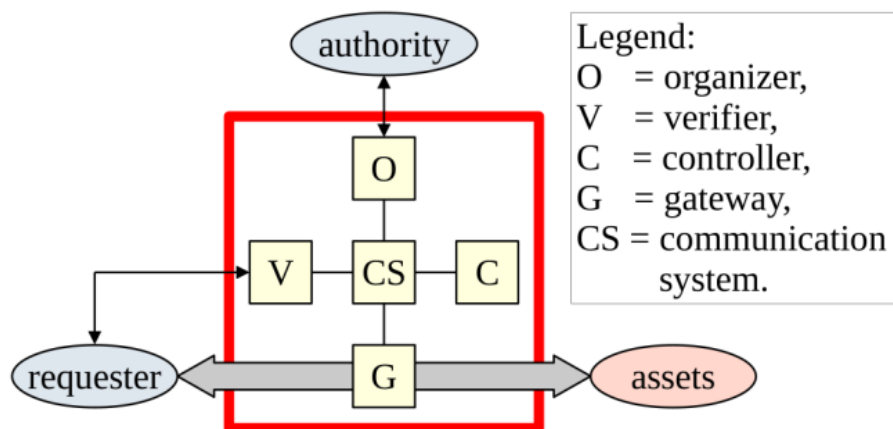


Рисунок 2.1 - Загальна архітектура СКУД

Типова архітектура системи автоматизації об'єкта, яка:

- приймає сигнали від датчиків (зчитувачів карток);
- обробляє інформацію в програмованому логічному контролері (ПЛК) або мікроконтролері;
- приймає керуючі рішення (відкрити/не відкрити шлагбаум);
- керує ВМ (електропривод шлагбаума, електронний замок тощо);
- може включати зворотний зв'язок (датчики положення шлагбаума, відеоспостереження);

					ДП.АКТ.10660533.00.00.000ПЗ	Арк.
Зм.	Арк.	№ докум.	Підп.	Дата		22

– має енергонезалежність, надійність, віддалений контроль, тобто - інтегрується у вищий рівень автоматизації.

На рисунку 2.2 [14] зображено архітектуру системи, в якій сенсори, контролери та кероване обладнання розміщені поблизу один одного, а зона відповідальності кожного контролера обмежується певною системою або підсистемою. Локальні контролери зазвичай здатні приймати сигнали від центрального контролера з метою запуску або зупинки локальних автоматизованих послідовностей, а також для налаштування контрольних параметрів, проте сам процес управління виконується саме на рівні локального контролера.

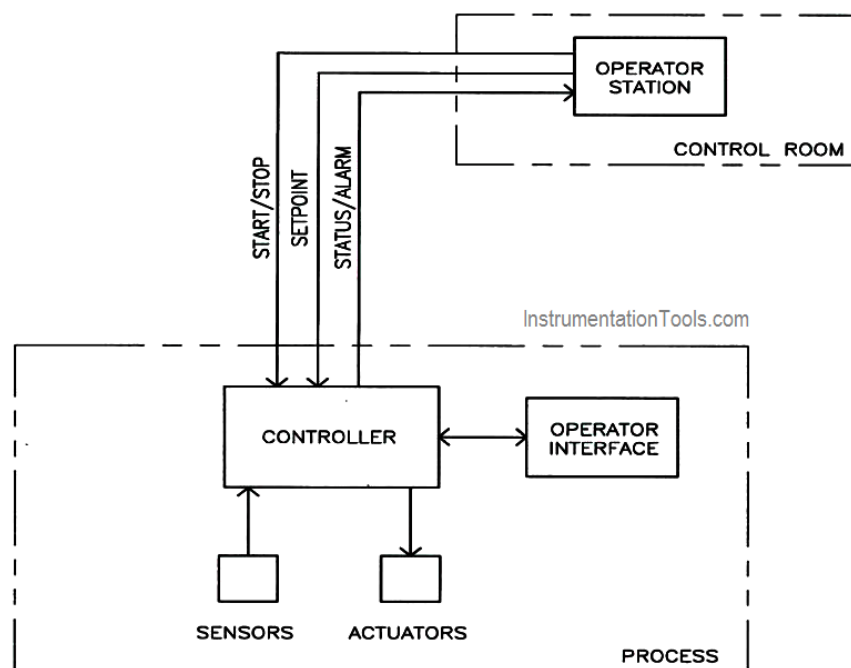


Рисунок 2.2 – СКУД з локальним керуванням

Необхідні інтерфейси оператора та екрани відображення інформації також розміщуються локально. Це створює значну перевагу для оператора під час усунення несправностей безпосередньо на місці, однак вимагає від нього фізичного переміщення територією об'єкта для спостереження за системами або реагування на непередбачувані ситуації. Така система забезпечує ефективний контроль доступу без необхідності підключення до складної мережі або серверів, що є зручним для невеликих об'єктів чи обмежених територій.

Централізоване керування (рисунок 2.3) архітектури системи, в якій усі

сенсори, ВМ, та інше обладнання на об'єкті з'єднані з одним контролером або групою контролерів, розташованих у загальному диспетчерському центрі [14]. Така архітектура дозволяє здійснювати централізоване управління всіма процесами на території підприємства або об'єкта. Розміщення всіх засобів керування, інтерфейсів оператора та індикаторів у єдиному пункті керування підвищує обізнаність оператора про стан системи, що, у свою чергу, прискорює реагування на аварійні або нестандартні ситуації, а також дозволяє ефективно здійснювати моніторинг і управління процесами.

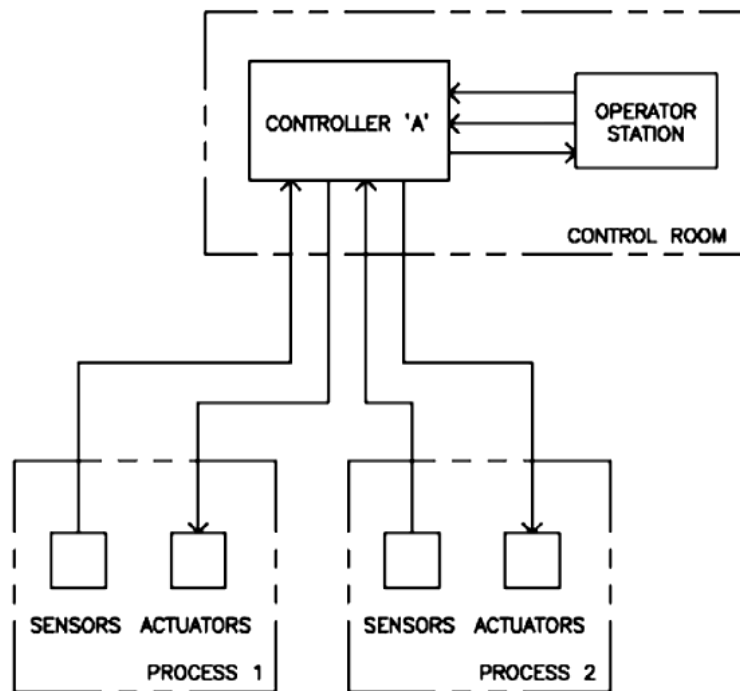


Рисунок 2.3 – СКУД з централізованим керуванням

Така архітектура набула поширення у промисловості, зокрема для електростанцій та інших об'єктів, де використовувалися одноконтурні контролери або перші цифрові системи керування. Проте сьогодні такі системи майже повністю витіснені розподіленими системами керування через високу вартість прокладання й монтажу всіх сигнальних кабелів до одного центрального місця.

Централізовані системи доцільно використовувати на невеликих промислових об'єктах. У випадку застосування такої архітектури необхідна повна резервованість процесорів. Також важливо забезпечити роздільні траси для прокладання кабелів, щоб гарантувати, що сигнали керування до обладнання або від нього, які дублюються, не будуть піддані спільним загрозам, пов'язаним з

					ДП.АКІТ.10660533.00.00.000ПЗ	Арк.
Зм.	Арк.	№ докум.	Підп.	Дата		24

електричними збоями, фізичними або навколишніми впливами.

Архітектура з централізованим керуванням забезпечує легкість у налаштуванні і контролі за параметрами всіх підсистем, що підвищує надійність і безпеку функціонування об'єкта в цілому. Проте висока вартість прокладання й обслуговування всіх сигнальних кабелів до центрального пункту управління, а також залежність від одного контролера можуть стати критичними факторами у разі відмови цього центру або пошкодження комунікаційної лінії.

Архітектура розподіленої СКУД (рисунок 2.4) поєднує характеристики локального та централізованого керування [14]. У такій системі контролери розміщуються безпосередньо біля обладнання або груп систем, за які вони відповідають, однак ці контролери об'єднані мережею з однією чи кількома операторськими станціями, що розташовані в центральному пункті. Передача даних між контролерами та операторськими станціями здійснюється через цифрові канали зв'язку.

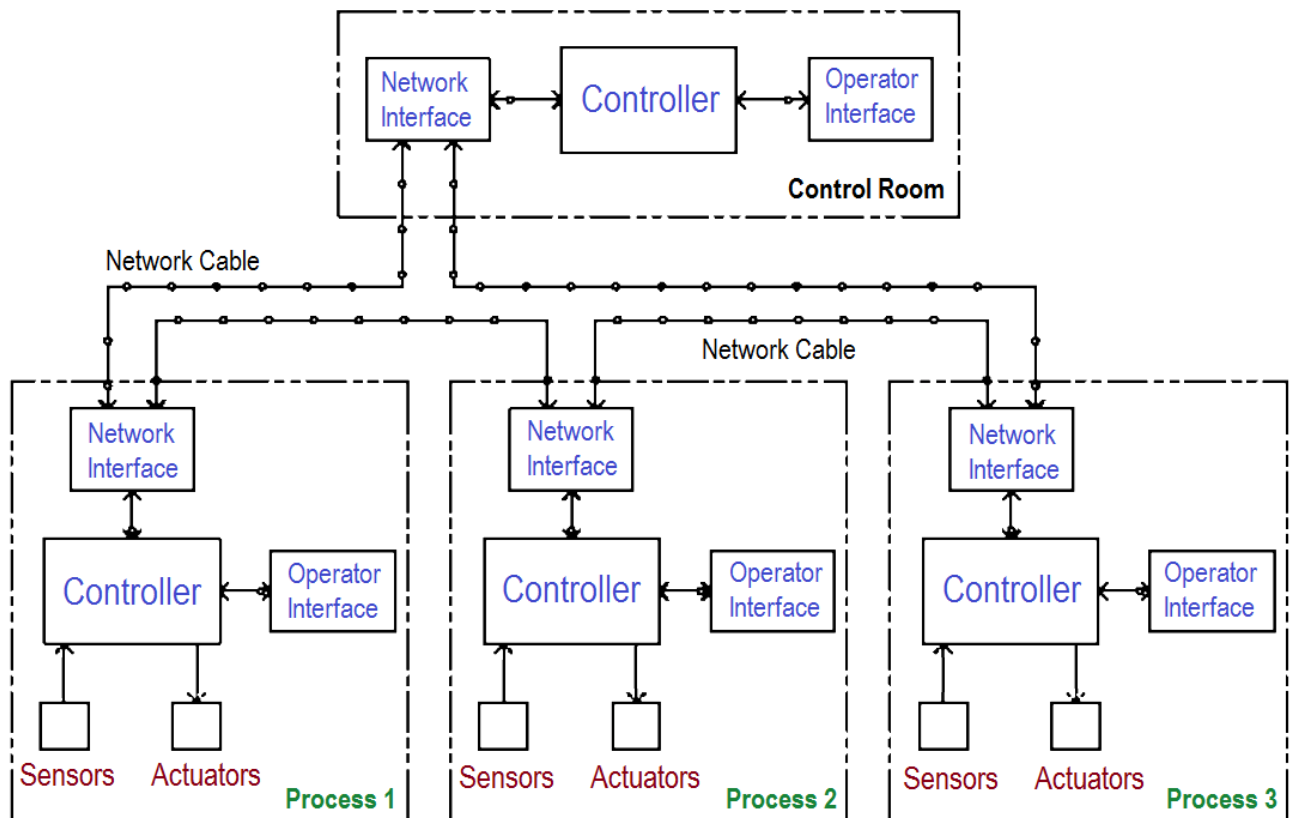


Рисунок 2.4 - Розподілена СКУД

Керуючі дії для кожної окремої системи або підсистеми реалізуються на рівні локального контролера. Водночас центральна операторська станція має

					ДП.АКІТ.10660533.00.00.000ПЗ	Арк.
Зм.	Арк.	№ докум.	Підп.	Дата		25

повну візуалізацію стану всіх систем: вона може переглядати вхідні та вихідні дані кожного контролера та, за потреби, втручатися в логіку керування локальних пристроїв.

Архітектура розподіленого керування має ряд важливих характеристик, які підвищують надійність її функціонування [10-15]:

- довжина ліній підключення вхідних та вихідних сигналів є короткою, що зменшує ймовірність їх фізичного пошкодження або впливу електромагнітних завад;
- у разі збою в одному з підрозділів об'єкта, наприклад, через пожежу чи затоплення, контролери та кабелі, розташовані в інших зонах, залишаються неушкодженими і продовжують працювати;
- кожен локальний контролер здатний автономно виконувати свої функції навіть у разі втрати зв'язку з центральною операторською станцією.

Ці переваги роблять такі архітектури придатними для використання на об'єктах зі складною структурою або підвищеними вимогами до безперервності та надійності керування.

Для об'єктів з великою кількістю точок доступу та високими вимогами до безпеки оптимальним вибором є автоматизовані СКУД з мережею контролерів. Це дозволяє централізовано управляти всіма точками доступу, забезпечувати обмін інформацією між контролерами, а також поєднувати систему з іншими елементами безпеки. Завдяки обміну даними між контролерами і центральним сервером можна без затримок реагувати на зміни в ситуації, наприклад, на інциденти безпеки або зміни в політиках доступу.

Такі системи дозволяють легко додавати нові точки доступу, розширюючи мережу в міру зростання об'єкта. Підтримка різних типів зчитувачів та ідентифікаційних технологій забезпечують гнучкість проєктованій системі. Архітектура такої системи наведена на рисунку 2.5.

Для забезпечення високої швидкості доступу, особливо на великих об'єктах, безконтактні карти можуть бути оптимальним вибором. Вони дозволяють швидко здійснювати ідентифікацію співробітників без необхідності фізичного контакту з зчитувачем. Для підвищення рівня безпеки можна використовувати біометричні

					ДП.АКІТ.10660533.00.00.000ПЗ	Арк.
Зм.	Арк.	№ докум.	Підп.	Дата		26

технології, такі як сканери відбитків пальців або розпізнавання обличчя, що допоможе уникнути шахрайства, пов'язаного з втратою або крадіжкою карт.

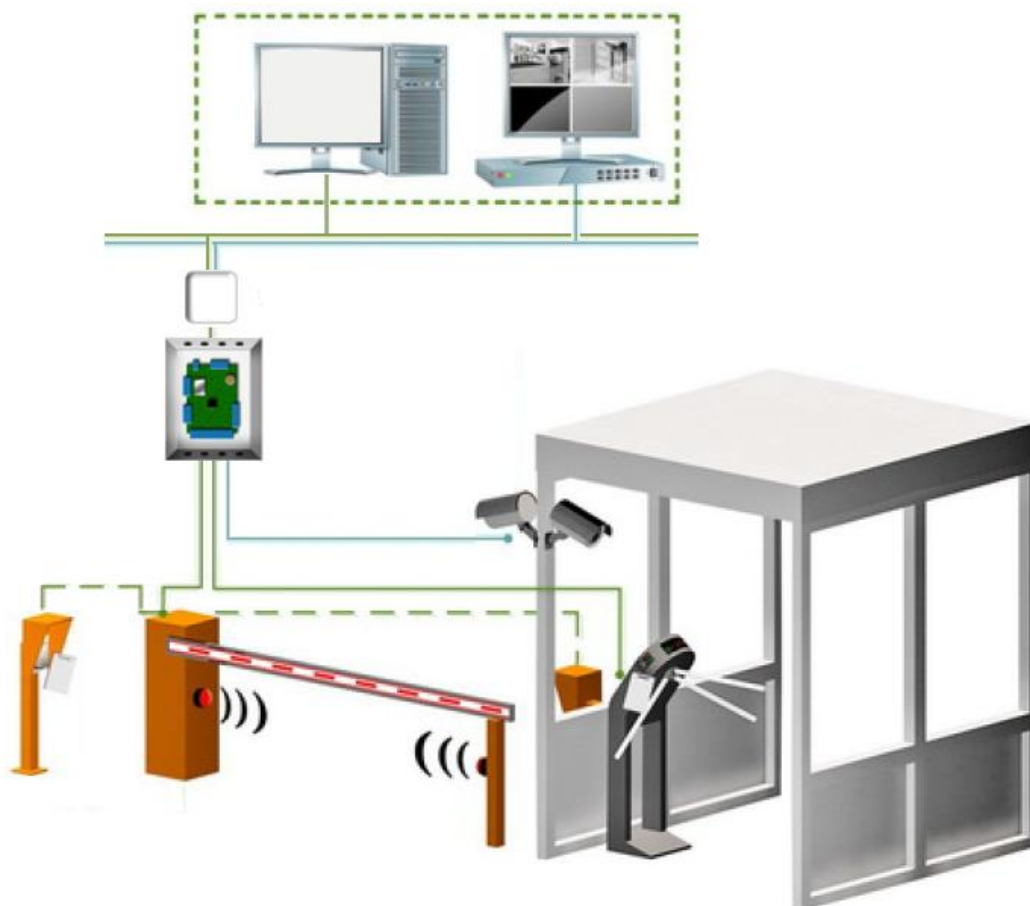


Рисунок 2.5 – Архітектура проектованої системи

Для контролю та обмеження доступу в основні зони, де потрібна підвищена безпека, можуть бути використані турнікети або електромагнітні замки. В СКУД повинна бути передбачена можливість інтеграції з відеомоніторинговими системами і аварійною сигналізацією, що дозволить забезпечувати комплексний моніторинг об'єкта.

Для централізованого управління та моніторингу в реальному часі необхідно використовувати мережеві контролери, які з'єднані з центральним сервером або БД. Це дозволяє здійснювати миттєве реагування на події та зміни. Якщо АСКД має бути розташована в певних ізольованих зонах без постійного підключення до центрального серверу, можна використовувати автономні контролери. Для деяких частин об'єкта, де прокладання кабелів є проблематичним, наприклад, на складі, в зоні обмеженого простору або на

					ДП.АКТ.10660533.00.00.000ПЗ	Арк.
Зм.	Арк.	№ докум.	Підп.	Дата		27

великих виробничих площах, можна використати бесбровові технології для зручності інсталяції та гнучкості в управлінні доступом.

2.2 Розробка структури проектованої системи

Структура проектованої АСКД (рисунок 2.6) базується на розподіленій архітектурі, що забезпечує централізоване управління з можливістю масштабування та адаптації до потреб різних точок доступу на території підприємства. На основі проведеного аналізу та дослідження архітектур, система складається з центрального пункту охорони де розміщується автоматизоване робоче місце (АРМ) та центральний контролер, який керує локальними контролерами на контрольних пунктах (КП), що безпосередньо взаємодіють із сенсорами та ВМ на об'єкті.

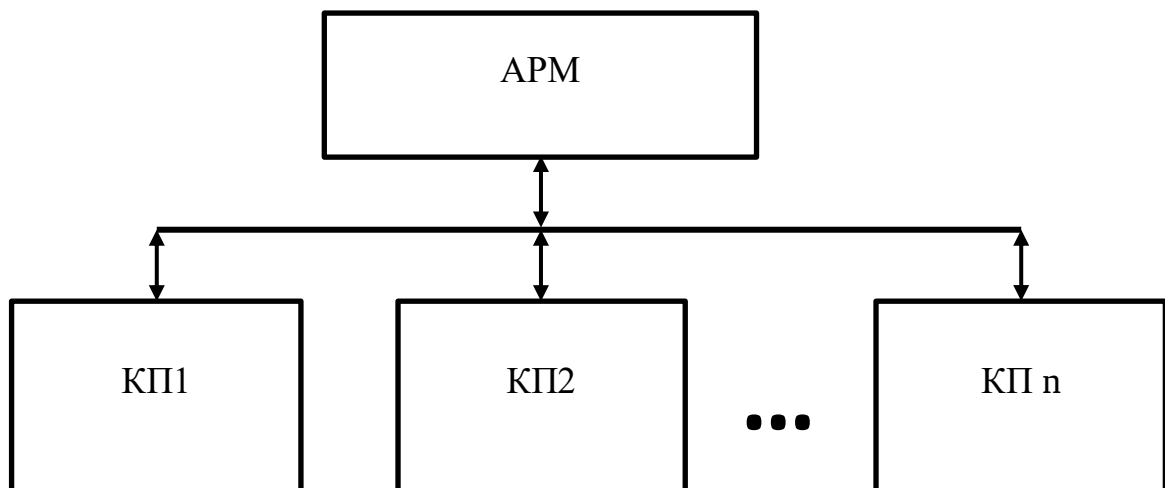


Рисунок 2.6 – Структура проектованої АСКД

АРМ це головний контрольний центр, який забезпечує моніторинг та керування всіма процесами доступу на об'єкт. Забезпечує централізоване налаштування системи, обробки даних та прийняття рішень щодо доступу. До АРМ підключені всі КП через мережу.

Кожен КП відповідає за управління конкретною точкою доступу, наприклад, вхід до воріт, шлагбауми, турнікети. Вони включають локальні контролери, що взаємодіють з сенсорами, наприклад, зчитувачами карт, та ВМ, шлагбаумами, турнікетами. Всі дані та інформація з КП передаються в АРМ для

					ДП.АКТ.10660533.00.00.000ПЗ	Арк.
Зм.	Арк.	№ докум.	Підп.	Дата		28

обробки та зберігання. Мережа зв'язку забезпечує передачу даних між АРМ та КП. Може бути реалізована за допомогою різних технологій, залежно від вимог до швидкості, надійності та масштабованості.

Запропонована структура АСКД є масштабованою, з можливістю додавання нових КП при розширенні території або зміні вимог до безпеки.

На рисунку 2.7 наведено структуру КП - автоматизованого поста, що є основною ланкою для здійснення контролю за доступом на територію об'єкта, забезпечуючи вхід як для співробітників, так і для службового чи особистого автотранспорту.

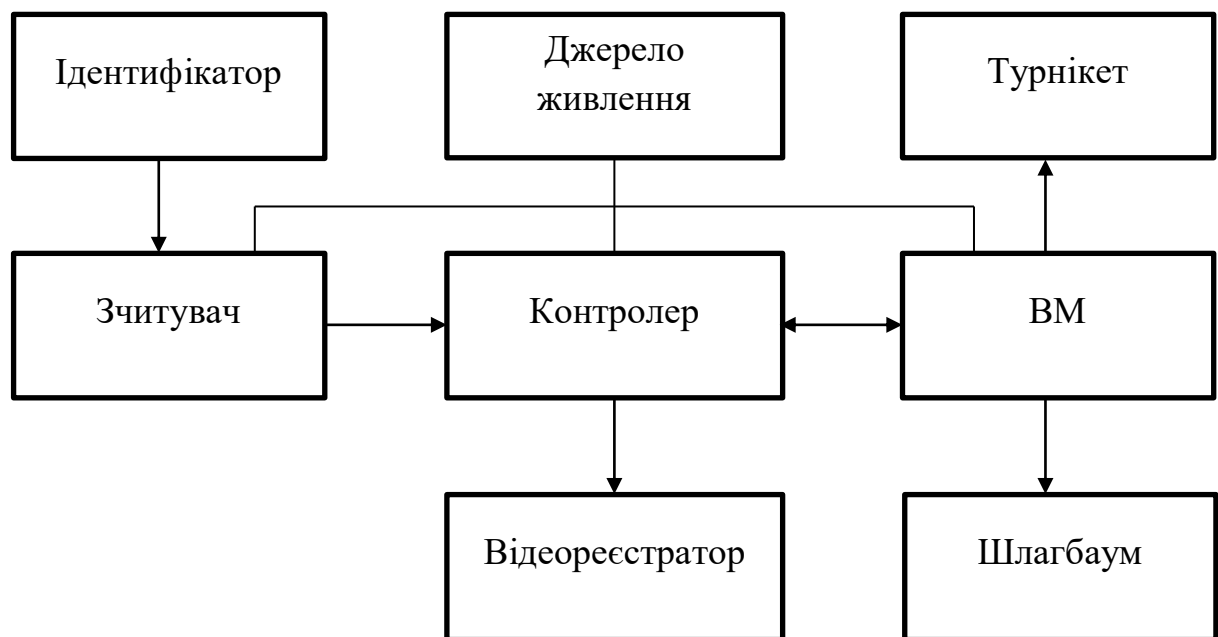


Рисунок 2.7 – Структурна схема КП

Структура КП включає в себе основні ВМ, такі як електромеханічний турнікет та автоматичний шлагбаум, які відповідають за фізичне обмеження доступу і регулювання потоку людей та ТЗ.

Після налаштування та конфігурації системи КП можуть працювати автономно, мінімізуючи необхідність втручання персоналу охорони, забезпечуючи безперервний контроль за входами та виходами. Відеокамери, розташовані в зоні проїзду автотранспорту та проходу, забезпечують цілодобове спостереження за ситуацією на КП, дозволяючи здійснювати моніторинг та архівування відеозаписів подій для подальшого аналізу або в разі необхідності.

2.3 Обґрунтування вибору технічних засобів для реалізації системи

Проектована АСКД реалізує функції для організації контролю та керування доступом: в'їзд ТЗ через автоматичний шлагбаум і проходи людей через турнікети. Система передбачає можливість ручного управління персоналом охорони для додаткового контролю або в разі необхідності втручання в процес. Це дозволяє забезпечити безпеку території, не створюючи зайвих складнощів для співробітників і відвідувачів, та забезпечує ефективний контроль доступу з мінімальними витратами часу і ресурсів. Дане рішення призначене для використання в організаціях закритого типу, таких як виробничі підприємства або склади. Зазвичай такі об'єкти мають огорожений периметр та обмежене число в'їздів.

Основними ВМ для обмеження доступу пішоходів є турнікети. Коли особа з дозволом на доступ хоче пройти, вона підносить свою персональну карту, наприклад, на основі RFID технології, до зчитувача, який знаходиться на зовнішній стороні турнікета. Якщо карта дійсна та авторизована для доступу, АСКД підтверджує право проходу і подає сигнал на турнікет для розблокування планок. Для реалізації АСКД обрано турнікет TS1000 Pro з підтримкою зчитування RFID карток, що забезпечує зручність і швидкість проходу користувачів (рисунок 2.8) [16].



Рисунок 2.8 – Турнікет

					ДП.АКІТ.10660533.00.00.000ПЗ	Арк.
Зм.	Арк.	№ докум.	Підп.	Дата		30

Пристрій працює при напрузі живлення 100-240 В з енергоспоживанням 24 Вт, що робить його енергоефективним для тривалого використання та дозволяє його використовувати в різних умовах. Час пропуску через турнікет складає 0,2 с, що забезпечує швидкий і безперешкодний прохід. Крім того, він оснащений світлодіодним індикатором, який надає візуальну інформацію про стан пристрою, наприклад, чи дозволено прохід.

Після того як людина провокує планки турнікету, вони обертаються в напрямку її руху, що дозволяє пройти у контрольовану зону. Після проходження планки знову блокуються, що забезпечує лише авторизованим особам можливість потрапити на територію об'єкта, запобігаючи несанкціонованому доступу.

Шлагбаум, що встановлюється на зоні проїзду автотранспорту, працює за аналогічним принципом: автомобіль не може заїхати на територію без авторизації. Водій ТЗ під'їжджає до шлагбаума і підносить свою персональну карту до зчитувача, розташованого на спеціальній стійці біля шлагбаума. Якщо карта водія є дійсною, то система підтверджує право на проїзд і подає сигнал для підйому шлагбаума. Водночас шлагбаум оснащений фотоелементами для запобігання несанкціонованого проїзду та забезпечення безпеки руху ТЗ.

Для реалізації проекрованої системи обрано шлагбаум ZKTeco BG1030R-LED, потужністю 120 Вт, електроживленням приводу 24В, що забезпечує високу енергоефективність та безпеку, а завдяки LED-підсвітці - покращену видимість в темний час доби (рисунк 2.9) [17].



Рисунок 2.9 - Шлагбаум ZKTeco BG1030R-LED

					ДП.АКІТ.10660533.00.00.000ПЗ	Арк.
Зм.	Арк.	№ докум.	Підп.	Дата		31

Швидкість відкриття становить 1,5 секунди, а довжина стріли до 3 м. Завдяки антикорозійному матеріалу корпусу та класу захисту IP54, пристрій забезпечує надійну роботу в умовах високої вологості та пилу, що робить його придатним для використання на паркінгах, комерційних і промислових об'єктів.

У проєктованій АСКД для ідентифікації персоналу передбачено використання RFID-карток стандартного формату для проходження через турнікет. Для ідентифікації ТЗ застосовуються UHF-мітки, які зчитуються на відстані за допомогою UHF-зчитувача. Такий розподіл дозволяє ефективно розмежувати контроль доступу людей і автотранспорту, забезпечуючи високу швидкість обслуговування та мінімізацію черг.

В таблиці 2.1 наведено порівняння даних технологій

Таблиця 2.1 - Порівняльні характеристики пристроїв для радіочастотної ідентифікації

Параметр	UHF-мітка	RFID-картка
Частотний діапазон	UHF (Ultra High Frequency) — 860–960 МГц	Зазвичай HF (High Frequency) — 13,56 МГц або LF (Low Frequency) — 125/134 кГц
Дальність зчитування	Велика (до 10–20 м і більше)	Невелика (до 10 см — для HF і LF карток)
Тип носія	Етикетка або компактна мітка, часто кріпиться на автомобілі	Картка формату пластикової банківської карти
Використання	Ідентифікація ТЗ, вантажів, у великих просторах	Контроль доступу людей, прохід через турнікети
Спосіб зчитування	Дистанційне зчитування без фізичного контакту	Ближнє зчитування або прикладання до зчитувача

Для реалізації ідентифікації та контролю для доступу ТЗ в проєктованій системі обрано безконтактний UHF зчитувач ZKTeco UHF5E Pro (рисунок 2.10). Пристрій забезпечує дальність зчитування від 2 до 8 метрів та працює в

					ДП.АКІТ.10660533.00.00.000ПЗ	Арк.
Зм.	Арк.	№ докум.	Підп.	Дата		32

частотному діапазоні 865–868 МГц. Завдяки посиленню антени 9 дБ та підтримці протоколів EPC Global UHF Class 1 Gen 2 / ISO 18000-6C, зчитувач здатен ефективно працювати в умовах зовнішньої установки [18].



Рисунок 2.10 – Зчитувач UHF-міток

Пристрій підтримує інтерфейси Wiegand, RS485 та USB для конфігурації), що забезпечує гнучкість підключення в різні СКУД. Пристрій має клас захисту IP67, що дозволяє його експлуатувати в несприятливих погодних умовах. Живлення здійснюється постійним струмом 9–15 В, а споживана потужність становить від 1,2 до 4,2 Вт. Робоча температура пристрою знаходиться в діапазоні від -20°C до +60°C [18]. Зчитувачі UHF-міток для ідентифікації ТЗ розміщуються на спеціальних стійках по обидва боки від шлагбаума для забезпечення стабільної ідентифікації незалежно від напрямку під'їзду транспорту.

Для безпечного проходу в проектованій АСКД використано індуктивний (магнітний) пристрій контролю петлі ZKTeco PSA-02 (рисунок 2.11) [19] для ідентифікації ТЗ перед шлагбаумом.



Рисунок 2.11 - Контролер індукційної (магнітної) петлі ZKTeco PSA02

Контролер працює на частоті 50-250 КГц з часом відгуку 100 мс та має вбудоване реле 250BAX/3A. Для забезпечення стабільної роботи пристрою

					ДП.АКІТ.10660533.00.00.000ПЗ	Арк.
						33
Зм.	Арк.	№ докум.	Підп.	Дата		

необхідно джерело живлення 220 В із споживаною потужністю ≤ 3 Вт. Він підтримує налаштування чутливості з трьома рівнями: низьким (L), середнім (M) та високим (H) та забезпечує надійне спрацювання релейних контактів для автоматичного управління проходом через контрольовану ділянку.

При подачі живлення на контролер автоматично виконується самодіагностика пристрою, що триває 3 секунди. Під час успішної діагностики індикатор змінює колір з миготливого на постійно горючий зелений. Коли ТЗ проїжджає через контур, активується зелений індикатор і вихідне реле, що забезпечує подальше функціонування системи.

Індукційна петля з контролером розташована на невеликій відстані від шлагбауму та призначена для виявлення автомобіля або іншого металевого ТЗ. При виявленні ТЗ вона подає сигнал на відкриття шлагбауму, забезпечуючи його автоматичне підняття при виїзді.

Для забезпечення захисту від зіткнення автомобіля зі стрілою шлагбаума, гарантуючи безпеку руху і мінімізуючи ризики пошкодження механізмів використовується ІЧ-бар'єр Lightwell (рисунок 2.12) [20].



Рисунок 2.12 – ІЧ-бар'єр

Передавач і приймач інфрачервоних променів встановлюються на обох сторонах шлагбаума, створюючи невидимий інфрачервоний бар'єр. Якщо автомобіль знаходиться в межах цього бар'єра, інфрачервоні промені перекриваються, що фіксується системою. У цей момент система не дозволяє опускати стрілу шлагбаума, щоб уникнути можливого зіткнення зі стрілою під час проїзду ТЗ. Це забезпечує захист як для автомобіля, так і для механізму

					ДП.АКІТ.10660533.00.00.000ПЗ	Арк.
Зм.	Арк.	№ докум.	Підп.	Дата		34

шлагбаума. Після того, як автомобіль покидає зону дії бар'єра, стріла може бути опущена без ризику пошкодження.

Для візуального контролю та фіксації ситуації в зоні проходу і проїзду на КП в проектованій системі встановлюються відеокамери. Вони дозволяють співробітнику охорони здійснювати моніторинг в реальному часі, спостерігаючи за ситуацією в зоні пропуску. Зображення з камер виводиться на спеціальний монітор, що дає можливість швидко реагувати на будь-які нештатні ситуації та в разі необхідності вручну коригувати роботу системи. Використання відеоспостереження забезпечує додаткову безпеку, дозволяючи здійснювати архівування записів для подальшого аналізу та розслідування інцидентів.

Для АСКД обрано камери Axis M2025-LE (рисунок 2.13), оскільки її характеристики дозволяють забезпечити високоякісне відеоспостереження в умовах як денного, так і нічного часу [21].



Рисунок 2.13 - Відеокамера Axis M2025-LE

Камера має роздільну здатність 1080p, що дозволяє отримувати чітке зображення навіть при детальному огляді ТЗ або осіб, що проходять через КП. Завдяки вбудованій інфрачервоній підсвітці, камера може ефективно працювати в умовах низької освітленості, що важливо для забезпечення безпеки в нічний час.

Axis M2025-LE має високий рівень захисту від погодних умов (IP66), що робить її надійною для використання в зовнішніх умовах. Підтримка стандарту PoE дозволяє зменшити кількість необхідних кабелів, спрощуючи монтаж і знижуючи витрати на прокладку додаткових джерел живлення.

Додатковою перевагою є підтримка технології WDR (Wide Dynamic Range),

					ДП.АКІТ.10660533.00.00.000ПЗ	Арк.
Зм.	Арк.	№ докум.	Підп.	Дата		35

що дозволяє забезпечити якісне зображення навіть при контрастних умовах освітлення, таких як яскраве сонце на фоні темного об'єкта. Це важливо для забезпечення чіткої видимості об'єктів на відео, що допомагає в правильній ідентифікації ТЗ і осіб.

Контролер ZKTeco C3-400 [22] має такі характеристики, які дозволяють його ефективне використання в різних СКУД (рисунок 2.14). Він забезпечує підключення турнікета, зчитувачів RFID-карток і UHF-міток, а також управління шлагбаумом з додатковим релейним блоком для управління високою потужністю.



Рисунок 2.14 - Мережний контролер доступу ZKTeco C3-200

Пристрій підтримує підключення до 4 зчитувачів, що включає зчитувачі RFID-карток та UHF-міток, що підходить для проектованої системи. Інтерфейс Wiegand, з максимальною довжиною лінії зв'язку до 100 м, що підходить для реалізації безконтактного контролю доступу в межах території підприємства. Інтерфейси підключення через RS232/RS485 та TCP/IP забезпечують можливість побудови мережових СКД для різних підрозділів на території підприємства. Швидкість обміну даними до 34.8 Кбіт/с дозволяє здійснювати зручне та ефективне керування системою в реальному часі.

Пристрій має достатньо портів для підключення всіх необхідних пристроїв, а також підтримує мережеву взаємодію через Ethernet. Це дозволяє побудувати розподілену систему, яка легко масштабується та може контролювати всі точки доступу з одного центрального місця. Контролер дозволяє будувати масштабовані системи контролю й обмеження доступу, які можуть бути легко розширені за

					ДП.АКІТ.10660533.00.00.000ПЗ	Арк.
Зм.	Арк.	№ докум.	Підп.	Дата		36

допомогою підключення нових контролерів у локальну мережу (рисунок 2.15).

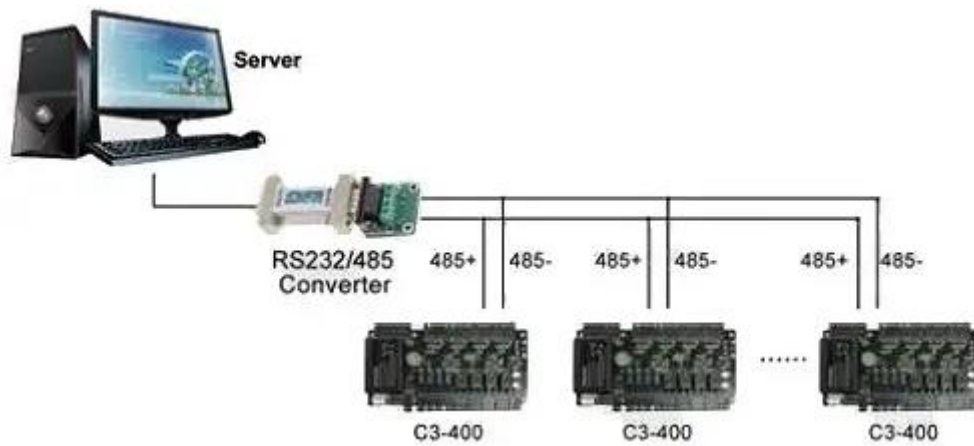


Рисунок 2.15 – Приклад побудови розподіленої АСКД

Можливість підключення додаткових датчиків та реле дає змогу підвищити ефективність роботи, розширити функції системи та реалізувати її взаємодію з іншими системами охорони й сигналізації на об'єкті (рисунок 2.16).

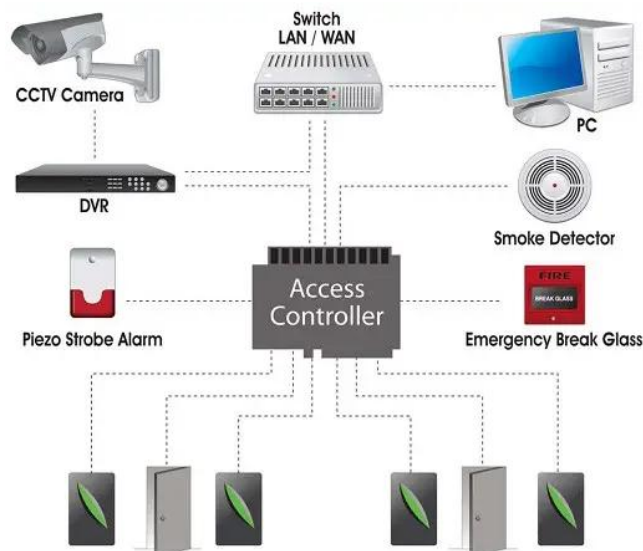


Рисунок 2.16 – Приклад інтеграції контролера з іншими системами безпеки

Це важливо для забезпечення комплексного управління доступом та моніторингу території підприємства.

3. РЕАЛІЗАЦІЯ СИСТЕМИ АВТОМАТИЧНОГО КЕРУВАННЯ ДОСТУПОМ НА ТЕРИТОРІЮ ПРОМИСЛОВОГО ОБ'ЄКТА

3.1 Розробка алгоритму роботи системи

Проектована АСКД забезпечує незалежне управління проходами для пішоходів і автотранспорту, що дозволяє ефективно контролювати доступ на територію підприємства як для співробітників, так і для ТЗ, за допомогою окремих турнікетів та шлагбаумів.

Алгоритм роботи проекрованої АСКД для персонулу через турнікет включає наступні кроки:

1. Стан в режимі очікування. У турнікета зафіксовані планки, які блокують прохід. Пристрій знаходиться в режимі очікування, чекаючи на сигнал для розблокування.

2. Процес проходу через турнікет:

- співробітник підносить свою персональну карту до зчитувача, розташованого на зовнішній стороні турнікета;
- якщо карта є дійсною, контролер доступу перевіряє рівень доступу та дозволяє здійснити прохід;
- після цього контролер посилає управляючий сигнал на турнікет, що призводить до розблокування планок;
- турнікет дозволяє здійснити прохід: користувач повертатиме планки по напрямку свого руху;
- після одиничного проходу планки автоматично блокуються для наступного користувача.

3. Повернення в режим очікування. Після проходу турнікет автоматично повертається в початковий стан.

Алгоритм роботи проекрованої системи для проїзду на територію ТЗ включає наступні кроки:

1. Процес проходу через шлагбаум:

- водій під'їжджає до шлагбаума. Індукційна петля, вмонтована в

					ДП.АКІТ.10660533.00.00.000ПЗ	Арк.
						38
Зм.	Арк.	№ докум.	Підп.	Дата		

проїжджу частину перед шлагбаумом, виявляє присутність ТЗ в зоні проїзду. Після чого, система передає сигнал контролеру доступу для ініціації перевірки картки водія;

- зчитувач, встановлений біля шлагбаума, безконтактно зчитує UHF-мітку водія на відстані, коли ТЗ перебуває в зоні дії зчитувача;
- контролер доступу перевіряє рівень доступу мітки водія;
- після успішної перевірки контролер посилає сигнал для відкриття шлагбаума;
- шлагбаум піднімається і дозволяє ТЗ проїзд.
- Після піднімання стріли шлагбаум очікує проїзду автомобіля.

Встановлений таймінг для проїзду складає час в секундах, це значення можна змінити в залежності від типу шлагбаума та потрібної швидкості доступу.

2. Процес закриття шлагбаума:

- після проїзду ТЗ шлагбаум починає автоматично закриватися;
- за допомогою ІЧ-бар'єру в зоні шлагбаума система визначається, чи є перешкода на шляху, наприклад, чи не стоїть ТЗ у зоні закриття;
- якщо датчики не фіксують перешкоди протягом заданого часу, шлагбаум закривається;
- якщо під час закриття стріли шлагбаума ІЧ-датчик виявлена перешкода, процес закриття припиняється і шлагбаум не закривається до того, як перешкода не буде усунена. Сигнал на блокування шлагбаума скидається, що запобігає його пошкодженню або псуванню автомобіля.

Алгоритм роботи системи для фіксації проходу та проїзду:

1. Виявлення активності в зоні контролю. Камери спостереження активуються автоматично, коли зчитувач виявляє присутність людини або ТЗ в зоні проходу чи проїзду. Це може бути активація через зчитування карти співробітника або сигнал від індукційної петлі, що фіксує присутність автомобіля.

2. Виведення зображення. Після активації камер, зображення з них виводиться на монітор на монітор АРМ. Це дозволяє охоронцю здійснювати візуальний контроль ситуації в реальному часі, оцінюючи безпеку і правильність виконання процесу проходу та проїзду.

					ДП.АКІТ.10660533.00.00.000ПЗ	Арк.
Зм.	Арк.	№ докум.	Підп.	Дата		39

3. Реагування на нештатні ситуації. У випадку виникнення будь-яких нештатних ситуацій (наприклад, несанкціонований доступ, затримка або перепони в процесі проходу/проїзду), охоронець має можливість вручну втрутитися в роботу системи, коригуючи її функціонування або здійснюючи відповідні дії для забезпечення безпеки.

4. Фіксація факту проходу/проїзду. Відеозапис ведеться тільки під час активності в зоні КП, тобто, коли зчитувач реєструє проходження або проїзд людини чи ТЗ. Після завершення проходу або проїзду, коли активність припиняється, запис відео автоматично вимикається для економії електроживлення та зменшення навантаження на систему зберігання даних.

На рисунку 3.1 наведена схема алгоритму роботи АСКД для ідентифікації та управління доступом на територію промислового об'єкту.

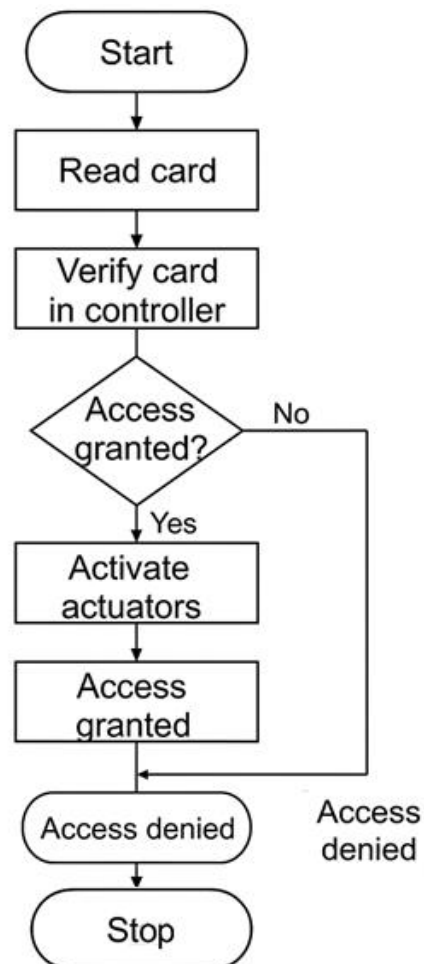


Рисунок 3.1 – Схема алгоритму ідентифікації та управління доступом

Система працює наступним чином:

1. Взаємодія ідентифікатора та зчитувача.

					ДП.АКІТ.10660533.00.00.000ПЗ	Арк.
Зм.	Арк.	№ докум.	Підп.	Дата		40

2. Код картки передається на контролер.
3. Контролер порівнює код з БД допуску.
4. Якщо код валідний – подається сигнал на відкриття ВМ - обмежувача, активується запис відео.

5. Якщо код невалідний – доступ забороняється, подія реєструється.

АСКД на території підприємства забезпечує зручний і безпечний доступ для персоналу та автотранспорту, а також має можливість ефективного моніторингу і втручання оператора в разі необхідності. Завдяки поєднанню турнікетів, шлагбаумів і фотоелементів система здатна забезпечити комплексний контроль доступу та безпеку на об'єкті.

3.2 Моделювання проекрованої системи

АСКД розробляється з метою забезпечення автоматичного управління та обмеження доступу до території підприємства, ідентифікації користувачів, управління ВМ та фіксації подій.

Система включає наступні основні елементи, кожен з яких виконує певну функцію:

- безконтактні персоналізовані ідентифікатори користувачів у вигляді RFID-карток або UHF-міток, які містять інформацію про користувача;
- пристрій для зчитування ідентифікаційних даних – можуть підтримувати різні стандарти зв'язку, забезпечуючи високу швидкість і точність ідентифікації;
- стійка для зчитувача – це елемент, який забезпечує зручне і надійне розміщення зчитувача;
- фізичні пристрої, які обмежують доступ до певної території, забезпечують контроль доступу та регулюють прохід;
- контролер – центральний елемент системи, який здійснює обробку даних, що надходять від зчитувачів і сенсорів, та приймає рішення щодо доступу на основі перевірки рівня доступу та інших параметрів;
- перетворювач інтерфейсу – відповідає за узгодження різних стандартів

					ДП.АКІТ.10660533.00.00.000ПЗ	Арк.
Зм.	Арк.	№ докум.	Підп.	Дата		41

зв'язку між компонентами системи та забезпечує правильну їх взаємодію, навіть якщо вони використовують різні технології передачі даних;

- ДБЖ забезпечує безперебійну роботу системи у випадку зникнення основного джерела електропостачання;
- відеокамера - для відеоспостереження та фіксації подій у зоні доступу;
- датчики присутності – сенсори, які визначають наявність ТЗ або осіб у зоні доступу забезпечуючи безпеку та коректну роботу системи.

Контур керування включає:

- сенсори (зчитувач, ІЧ-бар'єр, індуктивна петля) – формують вхідний сигнал системи;
- контролер (регулятор) – аналізує сигнал і виробляє команду керування;
- ВМ (шлагбаум, турнікет,ю відеокамера, пристрої індикації) – реалізують дію за командою;
- об'єкт керування (КП) – безпосередньо змінює стан (відкрито/закрито);
- зворотній зв'язок – інформація про фактичний стан ВМ, статус шлагбауму, відео, живлення тощо.

Модель системи у вигляді блок-схеми наведена на рисунку 3.2. Система реалізує дискретне регулювання на основі програмної логіки.

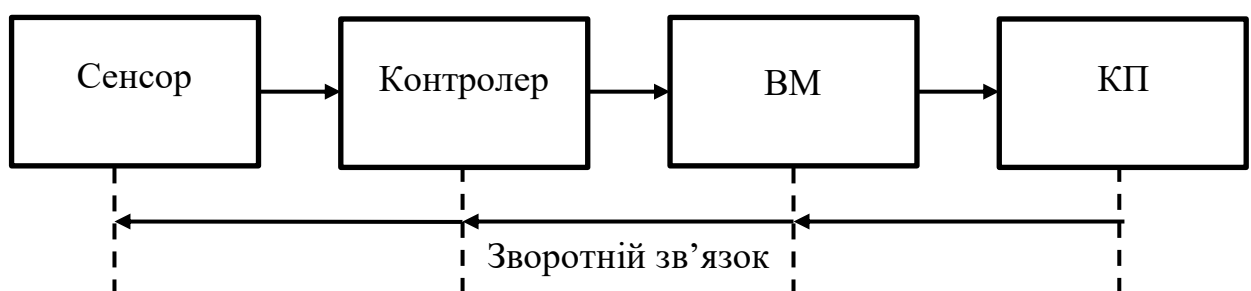


Рисунок 3.2 - Модель АСКД у вигляді блок-схеми

Кожен стан системи «доступ дозволено» / «доступ заборонено» є результатом логічної обробки вхідного сигналу. Для реалізації алгоритмів прийняття рішень може використовуватись ПЛК або вбудований мікроконтролер.

					ДП.АКІТ.10660533.00.00.000ПЗ	Арк.
Зм.	Арк.	№ докум.	Підп.	Дата		42

Переваги впровадження запропонованої АСКД включають підвищення безпеки промислового об'єкта за рахунок повної автоматизації процесу управління доступом. Можливість журналювання та аудиту доступу, що дозволяє оперативно аналізувати дії користувачів та підвищує прозорість доступу. Високу надійність системи завдяки застосуванню ДБЖ, що забезпечує стабільну роботу навіть у випадках зникнення основного електропостачання. Забезпечення зворотного зв'язку через фіксацію факту проходження або проїзду, дозволяє контролювати реальний стан системи в режимі реального часу.

3.3 Реалізація проектованої системи

Робота АСКД реалізується через логічні умови, які можуть бути записані у вигляді псевдокоду або таблиці логічних переходів. Псевдокод алгоритму роботи шлагбаума дозволяє реалізацію на рівні контролера:

Початок.

Ініціалізувати:

- зчитувач карток;
- реле управління шлагбаумом;
- інтерфейс зв'язку з БД користувачів;
- система відеофіксації.

Цикл:

1. Очікування ідентифікатора → Зчитати UID

2. Перевірити UID у БД:

- Якщо UID знайдено:
 - > Надати дозвіл.
 - > Відкрити шлагбаум (активувати реле).
 - > Вести відеозапис.
 - > Зберегти подію до журналу.
- Інакше:
 - > Відмова у доступі.
 - > Сповістити через звуковий сигнал / індикатор.

					ДП.АКІТ.10660533.00.00.000ПЗ	Арк.
Зм.	Арк.	№ докум.	Підп.	Дата		43

-> Вести відеозапис події.

3. Очікування закриття шлагбаума.

4. Повернутися до початку циклу.

Кінець.

В таблиці 3.1 наведено логічні умови роботи контролера АСКД.

Таблиця 3.1 - Логічні умови роботи контролера

№	Умова	Дія контролера
1	Картку піднесено	Зчитати UID
2	UID у БД знайдено	Активувати реле → Відкрити шлагбаум
3	UID не знайдено	Заборонити доступ, подати сигнал
4	Шлагбаум відкрито	Старт таймера / слідкування за сенсором
5	Час вичерпано / авто в'їхало	Закрити шлагбаум
6	Будь-яка подія	Внести запис у лог подій, зберегти відео

В таблиці 3.2 представлено логіку роботи контролера із забезпеченням обробки аварійних ситуацій та логування подій, що може бути адаптована для систем керування на базі ПЛК (FBD/LD) або мікроконтролерів (Arduino/ESP32).

Таблиця 3.2 - Логіка реакції системи на аварійні ситуації

№	Аварійна ситуація	Реакція системи
1	Втрата зв'язку з БД	Заборонити доступ, сигнал тривоги
2	Несправність зчитувача	Вивести повідомлення, блокувати систему
3	Неможливо закрити шлагбаум (ІЧ-сенсор активний)	Сигнал тривоги, блокувати нові запити доступу
4	Перевищено час відкриття	Автоматичне закриття, логування
5	Живлення від ДБЖ (основне живлення зникло)	Включення енергозбереження, інформування охорони

Для реалізації та моделювання роботи проекрованої АСКД на територію промислового об'єкта реалізовано прототип, що відтворює роботу двох

					ДП.АКІТ.10660533.00.00.000ПЗ	Арк.
Зм.	Арк.	№ докум.	Підп.	Дата		44

незалежних каналів доступу: для ТЗ та для пішоходів. Прототип АСКД побудовано з використанням платформи Arduino Uno та моделювального середовища Tinkercad Circuits [23], до якого підключені компоненти, що наведені в таблиці 3.3.

Таблиця 3.3 – Компоненти протопиту АСКД

Функціональна частина	Компонент моделі	Призначення
Контролер	Arduino Uno	Центральний керуючий пристрій
Зчитувач доступу (авто)	Кнопка	Імітація зчитувача для авто
Зчитувач доступу (люди)	Кнопка	Імітація зчитувача для пішохода
Засіб обмеження доступу (авто)	Серво SG90	Імітація автоматичного шлагбауму
Засіб обмеження доступу (люди)	Серво SG90	Імітація турнікета
Світлова індикація доступу	Зелений/червоний світлодіоди	Статус дозволу/заборони доступу
Камера спостереження	Білий світлодіод	Імітація активності камери
Джерело живлення	Батарея (віртуальна)	Забезпечення живлення системи

На рисунку 3.3 наведено прототип АСКД.

В додатку А схема електрична принципова змодельованої АСКД. В додатку Б програмний код Arduino для моделювання роботи прототипу АСКД.

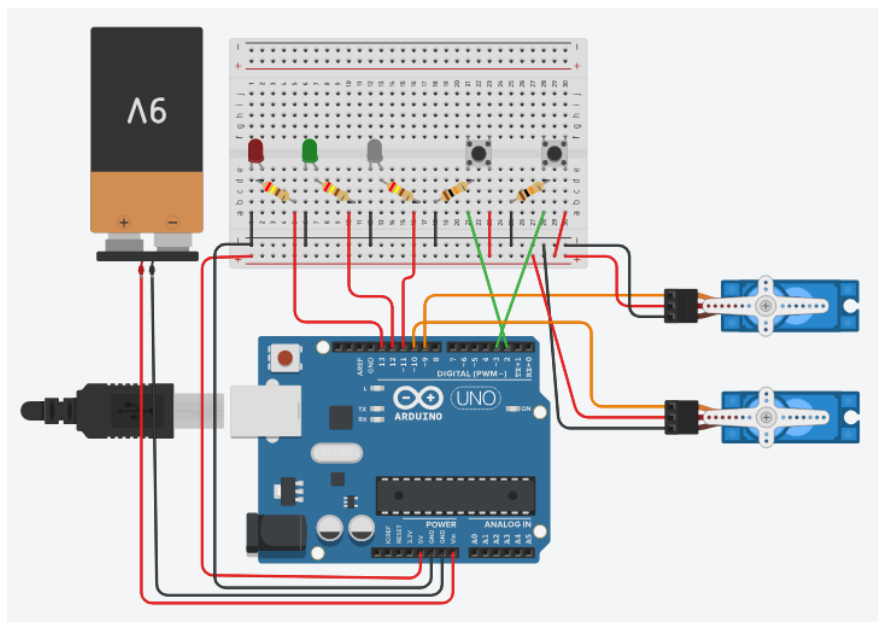


Рисунок 3.3 – Протопит АСКД

Результати моделювання АСКД показали:

- час відгуку системи: 0.5-1 секунду для зчитування UID і перевірки доступу;
- енергоефективність - система в режимі очікування споживає мінімум енергії, активуючи ВМ лише при необхідності;
- надійність - завдяки безконтактному зчитуванню та використанню ДБЖ система є стійкою до можливих збоїв.

Принцип роботи системи полягає в наступному. Система працює в режимі очікування до моменту активації одного з зчитувачів (імітація - натискання кнопки). Після зчитування умовно дозволеного доступу відбувається:

1. Для автомобіля:

- Відкриття шлагбауму (серво повертається на 90°),
- Активація камери (включення білого світлодіода),
- Засвічується зелений світлодіод,
- Після затримки шлагбаум автоматично закривається.

2. Для пішохода:

- Активація турнікета (серво повертається на 45°),
- Камера активується,
- Доступ дозволяється (зелений світлодіод),

					ДП.АКІТ.10660533.00.00.000ПЗ	Арк.
Зм.	Арк.	№ докум.	Підп.	Дата		46

- Після затримки турнікет блокується.

При несанкціонованому доступі (кнопка не натиснута) активується червоний світлодіод, і доступ блокується.

Модель передбачає паралельний підхід до контролю доступу з окремою логікою для ТЗ і пішоходів, симуляцію роботи камери відеоспостереження, світлову індикацію стану системи, імітацію живлення від резервного джерела (батарей), а також можливість розширення функціоналу шляхом підключення Ethernet/Wi-Fi модулів і LCD-дисплеїв для відображення даних.

Кожен запит до системи заноситься в журнал, який зберігається на накопичувач SD-карту, у БД або у лог-файл на сервері у вигляді наведеному в таблиці 3.4.

Таблиці 3.4 – Журнал подій АСКД

Дата/Час	UID	Подія	Статус
2025-04-23 08:42	A1B2C3D4	Спроба доступу	Дозволено
2025-04-23 08:45	11223344	Спроба доступу	Відмовлено
2025-04-23 08:47	—	Втрата живлення	Тривога

Розроблений прототип демонструє базові функціональні можливості АСКД на промисловий об'єкт, що може бути масштабована за рахунок інтеграції з реальними зчитувачами (RFID, NFC, ANPR), системами обліку персоналу БД, а також передачею даних на центральний сервер через Wi-Fi/Ethernet-модулі. Це дозволяє адаптувати модель під реальні задачі промислової безпеки та обліку й контролю доступу.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи розроблена АСКД, що забезпечує ефективне управління потоками персоналу та транспорту, інтеграцію із загальною інфраструктурою об'єкта, а також характеризується безперебійною роботою та підвищенням енергоефективності.

Проведено аналіз СКУД, зокрема загальної будови та компонентів системи та її основного призначення. Визначено, що такі системи поєднують функції безпеки, контролю, обліку та автоматизації, що дозволяє підвищити загальний рівень організованості й ефективності функціонування об'єктів. Проведений аналіз дав змогу класифікувати СКУД за різними характеристиками, такими як рівень безпеки, масштабність, тип керування, спосіб ідентифікації тощо. В результаті визначено оптимальний рівень складності та функціональності АСКД, який відповідає вимогам щодо надійності, гнучкості та адаптивності системи для промислового об'єкта.

Проведено дослідження архітектур СКУД різного рівня організації, зокрема локальних, централізованих і розподілених. Визначено переваги та недоліки кожного типу керування, що сприяло формуванню вимог до проектованої системи. Проведені дослідження дозволили врахувати особливості побудови АСКД, оцінити вимоги до комунікацій, масштабованості та взаємодії між компонентами системи. У результаті розроблено архітектуру АСКД розподіленого типу з централізованим моніторингом, де автономні контролери на кожному КП здійснюють локальне керування, а центральне АРМ забезпечує візуалізацію, логування подій та адміністрування.

Розроблено структуру проектованої системи, що забезпечує комплексне управління процесом доступу. Усі складові функціонують у єдиному середовищі, реалізуючи логіку автоматичного керування згідно з заданими алгоритмами.

Обґрунтовано вибір засобів автоматизації та елементів комп'ютерно-інтегрованих технологій для реалізації системи, яка забезпечує автоматичне виявлення об'єктів, прийняття рішень, керування виконавчими механізмами, а також оптимальний баланс між вартістю, функціональністю та масштабованістю.

					ДП.АКІТ.10660533.00.00.000ПЗ	Арк.
Зм.	Арк.	№ докум.	Підп.	Дата		48

Розроблено алгоритм роботи проектованої системи, який забезпечує незалежне управління проходами для пішоходів і ТЗ, автоматичну фіксацію фактів проходу, а також підтримує енергоефективний режим роботи за рахунок активації відеоспостереження лише в момент виявлення об'єкта у зоні КП з подальшим її автоматичним вимкненням через заданий інтервал часу після закриття обмежувача доступу. Робота АСКД реалізується через набір логічних умов, що визначають порядок прийняття рішень контролером на основі вхідних сигналів від сенсорів та стану об'єкта керування. Наведено логіку реакції системи на типові та аварійні ситуації, що забезпечує її адаптивність і надійність.

Проведено моделювання АСКД, у результаті якого визначено контур керування, що включає сенсори, контролер, виконавчий механізм, об'єкт керування та зворотний зв'язок. Система реалізує дискретне регулювання на основі програмної логіки з можливістю фіксації проходу або проїзду, що забезпечує зворотний зв'язок і дозволяє контролювати реальний стан системи в режимі реального часу. Передбачено можливість журналювання подій та аудиту дій користувачів, що підвищує прозорість і керованість процесів доступу.

Розроблено та реалізовано прототип АСКД, який підтверджує працездатність обраного підходу. Проведене тестування дозволило оцінити ефективність реалізованих алгоритмів та логічних умов керування, а також виявити напрями для подальшого вдосконалення системи. Розроблений прототип може бути використаний як основа для впровадження повнофункціональної системи.

					ДП.АКТ.10660533.00.00.000ПЗ	Арк.
Зм.	Арк.	№ докум.	Підп.	Дата		49

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Корчинський В., Тарасенко І., Рациборинський С., Хаджиогло А.. Автоматизовані системи керування доступом. Herald of Khmelnytskyi National University. Technical Sciences, 331(1), 2024, 291-296. <https://doi.org/10.31891/2307-5732-2024-331-44>
2. Айко О.В., Василенко О.Д., Степаненко В.М. Системи автоматизації контролю доступу на об'єкти. Теоретичні і прикладні проблеми фізики, математики та інформатики: матеріали XXII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених, Київ, 2024, С. 106-108.
3. Фещенко А.Б., Борисова Л.В., Собина В.О., Тарадуда Д.В., Демент М.О., Неклонський І.М. Автоматизовані системи управління та зв'язок: підручник. Х.: НУЦЗУ, 2021, 288 с.
4. Роговий М. Дослідження особливостей використання охоронних СКУД. Харківський національний університет радіоелектроніки, 2019, С. 23-40.
5. Юдін О. К., Весельська О. М. Аналіз та класифікація систем контролю та управління доступом на підприємстві./ Наукоємні технології, 2018, С. 220-221.
6. Писаренко Д. Г. , Нестюк Ю. Ю. , Васюра А. С.. Сучасна система контролю та управління доступом. Матеріали XLIX науково-технічної конференції підрозділів ВНТУ, Вінниця, 2020. [Електронний ресурс].- Режим доступу: <https://conferences.vntu.edu.ua/index.php/all-fksa/all-fksa-2020/paper/view/9077>.
7. Джулій В.М., Кльоц Ю.П., Муляр І.В., Чешун В.М.. Методи і алгоритми захисту інформаційних ресурсів комп'ютерних систем: навч. посіб. Хмельницький: ХНУ, 2021, 174 с.
8. Системи контролю і управління доступом від А до Я. [Електронний ресурс].- Режим доступу: <https://deps.ua/ua/knowegable-base/reference-information/7824.html>
9. Тітова В., Кльоц Ю., Мостовий С., Колісник В. Система контролю та управління доступом на основі RFID-технологій. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (4), 2023, 44–48.

					ДП.АКІТ.10660533.00.00.000ПЗ	Арк.
Зм.	Арк.	№ докум.	Підп.	Дата		50

<https://doi.org/10.31891/2219-9365-2023-76-5>

10. Омельченко М.О. Характеристика та загальні вимоги до системи контролю і управління доступом. Наук.-техн. журн Сучасний захист інформації, Київ, №4, 2020, С. 46-50.

11. Burda K. Universal description of access control systems. International Journal of Computer Science and Netvirk Security, Vol,24, No8. 2024, p. 43-53. 10.22937/IJCSNS.2024.24.8.5.

12. Architecture of Access Control & Time Attendance System Solution. [Електронний ресурс].- Режим доступу: <https://www.ravirajtech.com/architecture-of-access-control-system.html>

13. Rivals I., Personnaz L. Nonlinear Internal Model Control using Neural networks: application to Processes with Delay and Design Issues. IEEE transactions on neural networks Volume: 11, Issue: 1, 2000, p. 80-90. 10.1109/72.822512.

14. Different Types of Control Systems Architecture. [Електронний ресурс].- Режим доступу: <https://www.linkedin.com/pulse/different-types-control-systems-architecture-ahmed-yasser/>

15. Velas A., Boroš M., Kuffa R., Lenko F. Testing of Permeability of RFID Access Control System for the Needs of Security Management. Applied Sciences, 2024, 14, 4227. 10.3390/app14104227.

16. Турнікет-трипод ZKTeco TS1000. [Електронний ресурс].- Режим доступу: https://www.bezpeka-shop.com/ua/product/turniket-zkteco-ts1000-pro/?__store=ua&__from_store=ru&srsltid=AfmBOopYP5nMqZWZ4_Dc8QLGyLirMeZWKD5ae6l1L3z24nKRu20XdrXc

17. Шлагбаум ZKTeco BG1030R-LED. [Електронний ресурс].- Режим доступу: <https://www.bezpeka-shop.com/ua/product/shlagbaum-zkteco-bg1030r-led-s-pryamoj-streloy-3-m-so-svetodiodnoy-podsvetkoy-pravyu/>

18. UHF-зчитувач ZKTeco UHF10 E Pro дальньої дії. [Електронний ресурс].- Режим доступу: <https://www.bezpeka-shop.com/ua/product/uhf-schityvatel-zkteco-uhf-5e-pro/>

19. Контролер PSA02 магнітної (індукційної) петлі. [Електронний ресурс].- Режим доступу: <https://protection-key.com.ua/kontroler-indukcijnoyi-magnitnoyi->

					ДП.АКІТ.10660533.00.00.000ПЗ	Арк.
Зм.	Арк.	№ докум.	Підп.	Дата		51

petli-zkteco-psa02

20. ІЧ-бар'єри Lightwell. [Електронний ресурс].- Режим доступу:
<https://www.bezpeka-shop.com/ua/blog/obzor/ik-barery-lightwell-okhranyaemaya-territoriya-pod-kontrolem/?srsltid=AfmBOooGCgMsPXbCB8rO5MIerlYAcney6jePkGc6Go4JjrF7-rP91mMA>

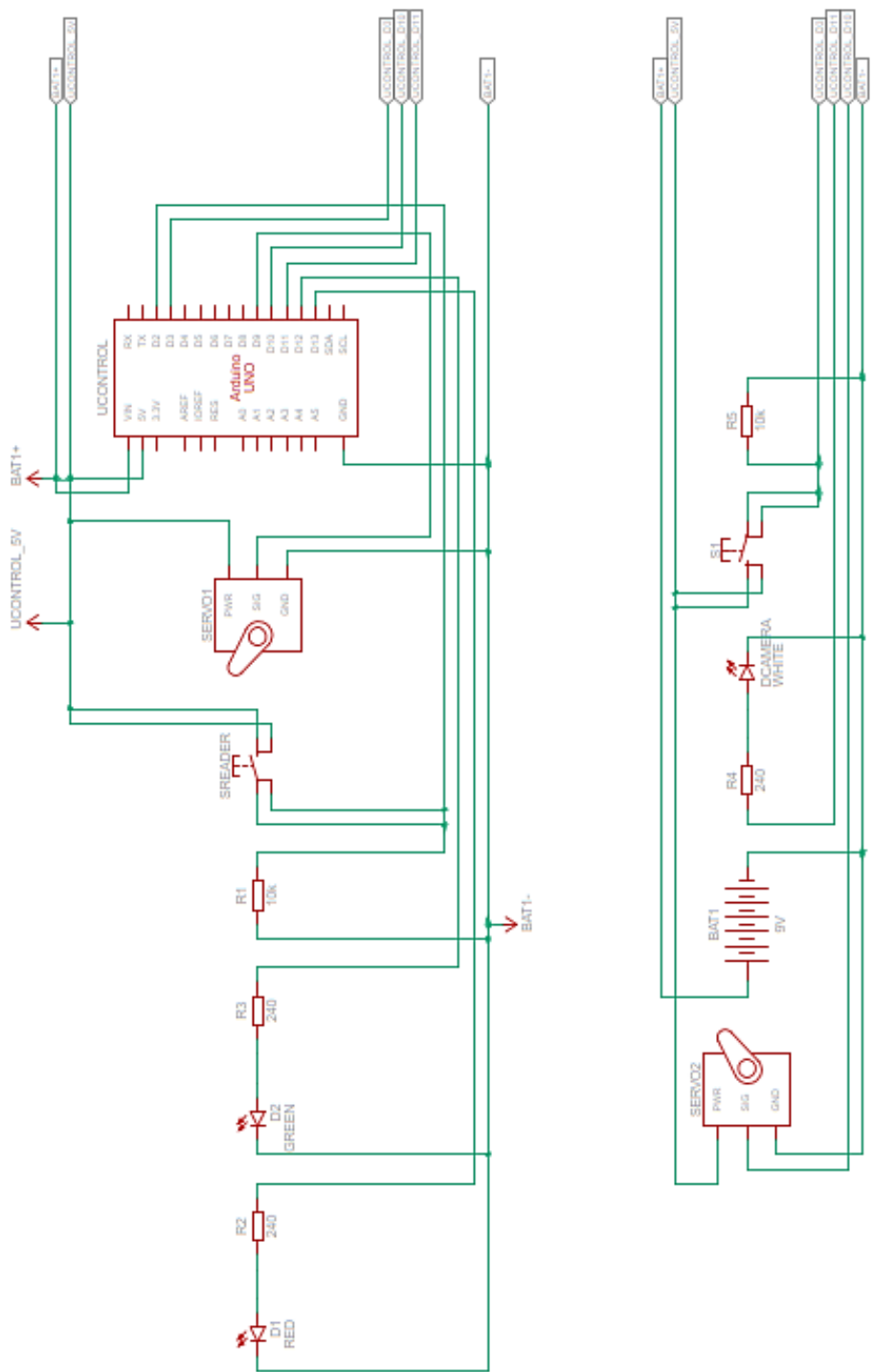
21. Axis M2025-LE. [Електронний ресурс].- Режим доступу:
<https://www.ipteam.com.ua/ip-cams/ip-cameras-axis/outdoor-axis/m2025-le.html>

22. Мережний контролер доступу ZKTeco C3-400. [Електронний ресурс].-
Режим доступу: https://zkstore.com.ua/p6135539-zkteco-400-kontroller.html?source=merchant_center&gad_source=1&gbraid=0AAAAADxvwBzm2bJkYcAd90O8mwQCPGxQ2&gclid=Cj0KCQjwzrzABhD8ARIsANlSWNP3jW4Y0FXKfEggb3dIXroJHymkIJHoXWlTVY7OZ2f_de1W1HLjYMsaAkDkEALw_wcB

23. Autodesk. (n.d.). Tinkercad. [Електронний ресурс].- Режим доступу:
<https://www.tinkercad.com/>

					ДП.АКІТ.10660533.00.00.000ПЗ	Арк.
Зм.	Арк.	№ докум.	Підп.	Дата		52

Схема електрична принципова прототипу АСКД



Програмний код для моделювання роботи прототипу АСКД

```

#include <Servo.h>

Servo barrierServo;
Servo turnstileServo;

// Ініціюємо підключення
int carButton = 2;
int personButton = 3;
int cameraLED = 11;
int greenLED = 12;
int redLED = 13;

void setup() {
  barrierServo.attach(9);
  turnstileServo.attach(10);

  // Початкове положення
  barrierServo.write(0);
  turnstileServo.write(0);

  pinMode(carButton, INPUT);
  pinMode(personButton, INPUT);
  pinMode(redLED, OUTPUT);
  pinMode(greenLED, OUTPUT);
  pinMode(cameraLED, OUTPUT);
}

void loop() {
  digitalWrite(redLED, HIGH);

  if (digitalRead(carButton) == HIGH) {

    // Імітація проїзду авто
    digitalWrite(cameraLED, HIGH);
    digitalWrite(redLED, LOW);
    digitalWrite(greenLED, HIGH);
    barrierServo.write(90); // Відкрити шлагбаум
    delay(50000); // Затримка до опускання
    barrierServo.write(0); // Закрити
    delay(1000); // Затримка до вимкнення камери
  }
}

```

					ДП.АКІТ.10660533.00.00.000ПЗ	Арк.
Зм.	Арк.	№ докум.	Підп.	Дата		54

```

digitalWrite(cameraLED, LOW);
digitalWrite(greenLED, LOW);
}

if (digitalRead(personButton) == HIGH) {

    // Імітація проходу людини
    digitalWrite(cameraLED, HIGH);
    digitalWrite(redLED, LOW);
    digitalWrite(greenLED, HIGH);
    turnstileServo.write(45); // Повернути турнікет
    delay(1000);    // Затримка до блокування
    turnstileServo.write(0); // Закрити
    delay(1000);    // Затримка до вимкнення камери
    digitalWrite(cameraLED, LOW);
    digitalWrite(greenLED, LOW);
}

// Режим очікування
digitalWrite(redLED, HIGH);
}

```

					ДП.АКІТ.10660533.00.00.000ПЗ	Арк.
Зм.	Арк.	№ докум.	Підп.	Дата		55