

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет радіоелектроніки та телекомунікації

(повне найменування інституту, назва факультету)

Кафедра захисту інформації

(повна назва кафедри)

Пояснювальна записка

до дипломного проєкту (роботи)

бакалавр

(ступінь вищої освіти)

на тему РОЗРОБКА МЕТОДИКИ ВПРОВАДЖЕННЯ СКУД В СИСТЕМУ
БЕЗПЕКИ ПІДПРИЄМСТВА
DEVELOPMENT OF THE METHODOLOGY FOR THE IMPLEMENTATION
OF THE ACS TO THE SECURITY SYSTEM OF THE ENTERPRISE

Виконав: студент 4 курсу, групи РТ-719

Спеціальності 125 Кібербезпека

(код і назва напрямку підготовки, спеціальності)

Освітня програма (спеціалізація)

Системи технічного захисту інформації,
автоматизація її обробки

ПОСТОЛЕНКО М.О.

(прізвище та ініціали)

Керівник ВОСКОБОЙНИК В.О.

(прізвище та ініціали)

Рецензент _____

(прізвище та ініціали)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет радіоелектроніки та телекомунікацій
Кафедра захисту інформації
Ступінь вищої освіти бакалавр
Спеціальність 125 Кібербезпека
(код і найменування)
Освітня програма (спеціалізація) Системи технічного захисту інформації, автоматизація її обробки
(назва освітньої програми (спеціалізації))

ЗАТВЕРДЖУЮ

Завідувач кафедри ЗІ, к.т.н, доц.
В.О. ВОСКОБОЙНИК
“ ” 2023 року

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА

ПОСТОЛЕНКА Максима Олександровича

(ПРИЗВИЩЕ, ім'я, по батькові)

1. Тема проєкту (роботи) Розробка методики впровадження СКУД в систему безпеки підприємства; Development of a methodology for introducing the access control system into the enterprise's
- керівник проєкту (роботи) к.т.н., доцент ВОСКОБОЙНИК Володимир Олександрович,
- затверджені наказом закладу вищої освіти від “ 04 ” квітня 2023 року № 94
2. Строк подання студентом проєкту (роботи) 01 червня 2023 року
3. Вихідні дані до проєкту (роботи) Розробити методику впровадження СКУД
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Теоретичні відомості про впровадження систем контролю доступу на підприємство, Нормативно-правова база, пов'язана з впровадженням систем контролю доступу, Порівняльний аналіз СКУД
5. Перелік графічного матеріалу плани об'єкту, презентація

6. Консультанти розділів проєкту (роботи)

Розділ	ПРИЗВИЩЕ, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
Розділи 1–3	ВОСКОБОЙНИК В.О., к.т.н. доцент		
Нормоконтроль	КОРОЛЬКОВ Р. Ю., к.т.н. ст.викл.		

7. Дата видачі завдання « 01 » березня 2023 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1	Постановка завдання роботи.	1 тиждень	Завдання, ТЗ
2	Опрацювання літератури та проведення емпіричного дослідження.	1 тиждень	Розділ 1
3	Аналіз предметної області.	2 тиждень	Розділ 2
4	Розробка СКУД для хлібозаводу.	3-4 тижні	Розділ 3
5	Оформлення пояснювальної записки.	6-7 тиждень	
7	Нормоконтроль та рецензування.	8 тиждень	
8	Захист дипломної роботи.	9 тиждень	

Студент(ка)

_____ Максим ПОСТОЛЕНКО
(підпис) (Ім'я ПРИЗВИЩЕ)

Керівник проєкту (роботи)

_____ Володимир ВОСКОБОЙНИК
(підпис) (Ім'я ПРИЗВИЩЕ)

РЕФЕРАТ

ПЗ: 73 с., 20 рис., 10 таб., 32 джерел.

СИСТЕМА КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ, ІДЕНТИФІКАЦІЯ, СИНХРОНІЗАЦІЯ, СТАНДАРТИ, КОНТРОЛЕРИ

Об'єкт дослідження – методи та засоби впровадження СКУД в систему безпеки підприємства - хлібозавод.

Мета роботи – аналіз сучасних методів та засобів застосування СКУД для впровадження СКУД в систему безпеки підприємства з метою забезпечення високого рівня безпеки та зменшення можливості несанкціонованого доступу.

Метод дослідження – аналіз нормативно-правових актів щодо впровадження СКУД на підприємствах, порівняння різних видів СКУД (для визначення переваг та недоліків даних видів), аналіз потреб та характеристик підприємств для впровадження системи контролю, аналіз інженерно-технічної складової впровадження СКУД, а також аналіз синхронізації між різними системами та СКУД.

У роботі розглянуті основні типи систем контролю та управління доступом (СКУД): на основі карток, біометрії, кодів доступу, мобільні системи, інтернет системи та гібридні системи. Досліджені способи ідентифікації осіб у системі контролю доступу, з'єднання між пристроями системи. Проведений аналіз переваг та недоліків використання різних типів СКУД, ринок виробників систем контролю доступу. Розглянуті можливості впровадження СКУД на підприємство та їх синхронізація.

ABSTRACT

Explanatory note to the bachelor's thesis: 73 pages, 20 figures, 10 tables, 32 sources.

ACCESS CONTROL AND MANAGEMENT SYSTEM, IDENTIFICATION, SYNCHRONIZATION, STANDARDS, CONTROLLERS

Object of research - methods and tools for implementing an Access Control System (ACS) in the security system of an enterprise - a bread factory. The aim of the work is to analyze modern methods and means of applying ACS for implementing it into the enterprise's security system in order to ensure a high level of security and to reduce the possibility of unauthorized access. Research method - analysis of regulatory acts concerning the implementation of ACS at enterprises, comparison of different types of ACS (to determine the advantages and disadvantages of these types), analysis of the needs and characteristics of enterprises for implementing the control system, analysis of the engineering and technical component of implementing the ACS, as well as the analysis of synchronization between different systems and ACS. The paper considers the main types of access control and management systems (ACS): based on cards, biometrics, access codes, mobile systems, internet systems, and hybrid systems. Ways of person identification in the access control system, connection between the system devices have been studied. The analysis of the advantages and disadvantages of using different types of ACS, the market of access control system manufacturers has been conducted. The possibilities of implementing ACS in an enterprise and their synchronization are considered.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ.....	7
ВСТУП	8
1. ЗАГАЛЬНІ ХАРАКТЕРИСТИКИ СИСТЕМ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ.....	10
1.1 Визначення та основні функції СКУД.....	10
1.2 Історія розвитку СКУД.....	13
1.3 Стандарти та технічна характеристика СКУД.....	16
1.4 Класифікація систем СКУД.....	20
1.5 Ідентифікатори СКУД.....	22
1.5.1 Оптичні ідентифікатори СКУД.....	23
1.5.2 Біометричні ідентифікатори СКУД.....	23
1.5.3 Електронні ідентифікатори СКУД.....	25
2. АНАЛІЗ СКУД ДЛЯ ПІДПРИЄМСТВ.....	27
2.1 Характеристики підприємств для запровадження СКУД.....	27
2.2 Потреби підприємств для запровадження СКУД.....	33
2.3 Аналіз ринку СКУД.....	37
2.4 Переваги та недоліки використання СКУД.....	47
3. МЕТОДИКА ВПРОВАДЖЕННЯ СКУД НА ПІДПРИЄМСТВІ.....	52
3.1 Обґрунтування вибору СКУД.....	55
3.2 Інженерно-технічна складова впровадження СКУД.....	58
3.3 Особливості програмного забезпечення СКУД.....	63
3.4 Синхронізація роботи відділів після впровадження СКУД.....	67
ВИСНОВКИ.....	70
ПЕРЕЛІК ПОСИЛАНЬ.....	71

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

СКУД – система контролю та управління доступу;

ПП – перегороджуючий пристрій;

ПЗ – програмне забезпечення;

RFID – Radio-Frequency Identification (радіочастотна ідентифікація);

IoT – Internet Of Things (інтернет речей);

TCP/IP – протоколи мережі інтернет;

HTTP – HyperText Transfer Protocol (протокол передачі гіпертексту);

HTTPS – HyperText Transfer Protocol Secure (розширений протокол передачі гіпертексту);

RS-485 – стандарт передачі даних.

ВСТУП

Питання безпеки та захисту роботи підприємств, інформаційних ресурсів, матеріальних цінностей, контроль активності працівників є актуальним для роботи різного типу підприємств. Одним з ефективних підходів до вирішення питання безпеки різних об'єктів, є використання системи контролю та управління доступом (СКУД). Встановлення системи контролю дозволяє попередити несанкціонований доступ до підприємства та приміщень в ньому, дозволяє встановлювати рівень доступу до приміщень, дозволяє контролювати переміщення співробітників та час роботи.

Загалом, за допомогою системи контролю та управління доступом досягається:

- ідентифікація осіб, які мають право доступу;
- розмежовування доступу до приміщень (за необхідності);
- керування автоматичними режимами;
- реєстрація та контроль часу перебування осіб на об'єкті;
- обробка інформації, ведення статистики та формування відповідних звітів.

Системи контролю та управління доступом включають багато технічних засобів, для ефективної роботи, а саме: контролери, пристрої ідентифікації (контактної або безконтактної), відеоспостереження та відеоаналіз, виконавчі пристрої (турнікети, шлагбауми), програмне забезпечення, мережеве обладнання. СКУД також може інтегруватися з іншими системами, наприклад система відеоспостереження, аварійна та пожежні системи. Таке інтегрування надає можливість автоматичного контролю та попередження протиправних дій та небезпечних ситуацій.

Також при встановленні СКУД важливо проаналізувати характеристики та потреби підприємства, мету та очікуваний ефект встановлення системи контролю. Це дасть змогу ефективно та якісно використовувати всі переваги СКУД.

Об'єкт дослідження – методи та засоби впровадження СКУД в систему безпеки підприємства - хлібозавод.

Предмет дослідження – ефективність методів та засобів впровадження системи контролю та управління доступу (СКУД) в систему підприємства – хлібозавод.

Метою даної роботи є детальний аналіз наявних видів системи контролю та управління доступом. Визначення характеристик та потреб підприємств для встановлення системи контролю, а також особливостей встановлення інтеграції та синхронізації СКУД з іншими системами.

Методи дослідження включають аналіз нормативно-правових актів щодо впровадження СКУД на підприємствах, порівняння різних видів СКУД (для визначення переваг та недоліків даних видів), аналіз потреб та характеристик підприємств для впровадження системи контролю, аналіз інженерно-технічної складової впровадження СКУД, а також аналіз синхронізації між різними системами та СКУД.

Актуальність дослідження: розробка методики впровадження системи контролю та управління доступу (СКУД) в систему безпеки є актуальним питанням для різних підприємств та організацій в різних сферах діяльності. За допомогою СКУД можна обмежити доступ до приміщень, конфіденційної інформації та дорогого обладнання, зменшення ризиків крадіжок та зламів, а також така система допомагає забезпечити контроль за переміщенням працівників та відвідувачів. Запровадження СКУД, також, може допомогти підприємствам виконувати вимоги законодавства, щодо безпеки праці та охорони праці, зменшити витрати на охорону підприємства. Розробка методики впровадження СКУД в систему безпеки підприємства є актуальною задачею, яка може мати позитивний вплив на функціонування підприємства та його безпеку.

1 ЗАГАЛЬНІ ХАРАКТЕРИСТИКИ СИСТЕМ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ

1.1 Визначення та основні функції СКУД

Система контролю та управління доступом (СКУД) – це комплекс технічних та програмних засобів безпеки (приклад архітектури на рисунку 1.1), який здійснює регулювання входу та виходу, переміщення людей чи транспортних засобів на територіях, які знаходяться під охороною, для моніторингу та попередження несанкціонованого доступу [1].

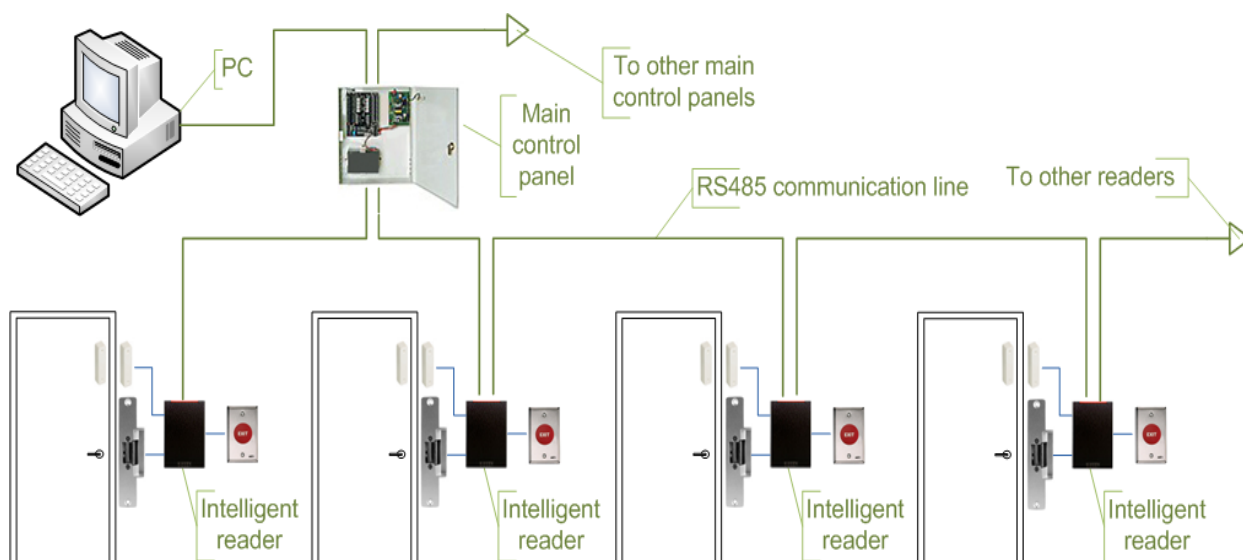


Рисунок 1.1 – Приклад системи контролю та управління доступом

Функціонал системи контролю та управління доступом контролює доступ на територію підприємства, а також дозволяє зонувати приміщення із різним типом доступу, ідентифікує користувачів (працівників), запобігає несанкціонованому доступу. Розвиток технологій дозволяє не тільки контролювати безпеку та доступ до об'єктів інфраструктури, але і до інформації підприємства.

Найважливіші елементи системи контролю та управління доступом та їхні цільові призначення висвітлено в таблиці 1.1 [2].

Таблиця 1.1 – Характеристика основних складників СКУД

Складник СКУД	Приклади пристроїв / засобів
Перегороджувальні пристрої (ПП)	Двері, турнікети, шлагбауми, електронні замки, блокпости, бар'єри, мантрапи.
Зчитувальні пристрої	Пристрої для радіочастотної та біометричної ідентифікації (зчитування відбитків пальців, сітківки ока, розпізнавання особи, ходи тощо).
Контролери	Модулі, які керують роботою СКУД, замками, пристроями загородження, аутентифікація об'єктів доступу, авторизація для доступу на об'єкт або конкретне приміщення.
Програмне забезпечення (ПЗ)	Програмні засоби для моніторингу, інтеграції з іншими системами, управління ідентифікаторами та інші.
Додаткове обладнання	Кнопки, блоки живлення тощо.

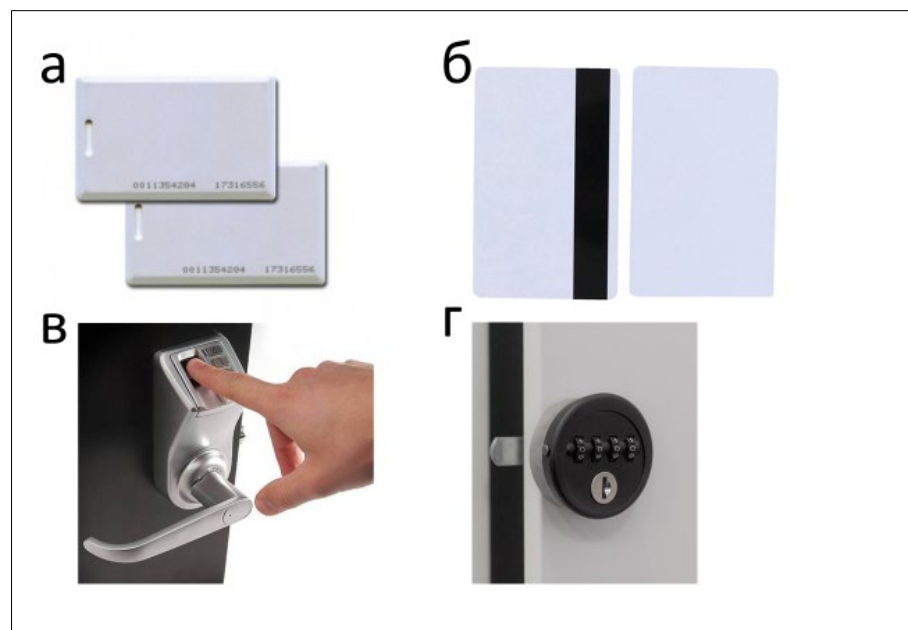
Усі системи контролю та управління доступом (СКУД) мають базові функції, які включені в систему за замовчуванням [3]:

- ведення та підтримка бази даних працівників (користувачів) та ідентифікаторів;
- фіксація дати та часу проходження користувача в базі даних;
- задання різних рівнів доступу до об'єкта, до приміщень;
- автономна робота системи, але збереження функцій управління при порушенні зв'язку із головним комп'ютером;
- реєстрація та зберігання інформації про події в енергонезалежній пам'яті контролерів;
- збереження ідентифікаційних ознак в системі при відключенні електроживлення або при відмові;

- відкриття ПП при зчитуванні зареєстрованої ідентифікаційної ознаки у пам'яті системи;
- заборона відкриття ПП при зчитуванні незареєстрованої ідентифікаційної ознаки у пам'яті системи.

За необхідності функції можна розширювати, налаштовувати відповідно до особливостей об'єкта, де буде встановлено СКУД. Система контролю та управління доступом після встановлення працює за алгоритмічним принципом.

1. Встановлення системи на об'єкті (підприємство, офіс тощо).
2. Отримання кожним співробітником унікального ідентифікатора (картка безконтактна або магнітна, біометричні дані, код) (рисунки 1.2).
3. Встановлення прав доступу в різні зони об'єкта.
4. Встановлення на входи, які потребують контролю, зчитувачів-ідентифікаторів, електромагнітних замків, контролерів.
5. Передача інформації контролеру після піднесення ідентифікатора.
6. Визначення контролером права доступу ідентифікатора.
7. Відкриття приміщення за наявності права доступу.



а – картка безконтактна; б – картка магнітна, в – біометричні дані, г – код

Рисунок 1.2 – Приклади ідентифікаторів

1.2 Історія розвитку СКУД

Розвиток системи контролю та управління доступом прямо залежить від розвитку технологій. З кожним роком виявляються нові загрози, нові методи обходу системи безпеки. Відповідно до цього СКУД постійно оновлюється, додаються нові функції, удосконалюються наявні, розробляються нові алгоритми ідентифікації.

Системи контролю доступу є важливою частиною системи безпеки об'єктів критичної інфраструктури, офісах, банках та громадських місць. Інтеграція з іншими системами (наприклад, протипожежна система, відеоспостереження, система розумного будинку) дає більш широкий спектр використання, а також забезпечує кращий контроль та безпеку об'єкта. Історію розвитку СКУД висвітлено в таблиці 1.2.

Таблиця 1.2 – Технічні характеристики СКУД в різні періоди

Період	Явище	Загальна характеристика
1960-ті роки	Поява перших систем контролю та управління доступом	Це були електронні системи контролю доступу, які використовували картки або ключі з магнітною смугою або перфоровані карти з нанесеним кодом, для доступу до об'єкта. Карту вставляли в спеціальний пристрій і система зчитування, перевіряла код та відкривала або блокувала двері. Попри те, що дана система була краще від традиційних механічних замків, вона була проста та не дуже надійна. Карти могли втратити або передати іншій особі, окрім того, система була дорогою, також вимагала спеціальних знань для встановлення та експлуатації.

Продовження таблиці 1.2

Період	Явище	Загальна характеристика
1970-ті–1980-ті роки	Вихід на ринок безконтактних карт та біометричних систем контролю доступу.	Безконтактні карти стали простішими у використанні, ніж карти з магнітною смугою, та стали популярними. Біометричні системи доступу використовували відбитки пальців, розпізнавання обличчя, сканування райдужки та сітківки ока, голосу. Дана система була більш безпечна в порівнянні із картками, проте на момент створення була дорогою та мала досить високий рівень відмов [4, 5].
1990-ті роки	Поява мережевих систем контролю доступу	Таким чином системи контролю та управління доступом стали більш досконалими. Оскільки системи були підключені до мережі, це полегшило доступ до віддалених об'єктів, а також надало можливість віддалено керувати доступом до різних об'єктів.
2000-ті роки	Розробка технології «Смарткарта» (рисунок 1.3)	Смарткарта – це пластикова карта, що містить інтегральну схему, яка має певний рівень програмованості та пам'ять. На смарткарту можна зберігати більше інформації про її власника, що робить їх безпечнішими, ніж карти з магнітною смугою.
2010-ті роки	Розробка хмарних систем контролю доступу	Використання даних систем полегшило віддалене управління доступом, стали більш гнучкі, а також їх можна інтегрувати з іншими системами безпеки.

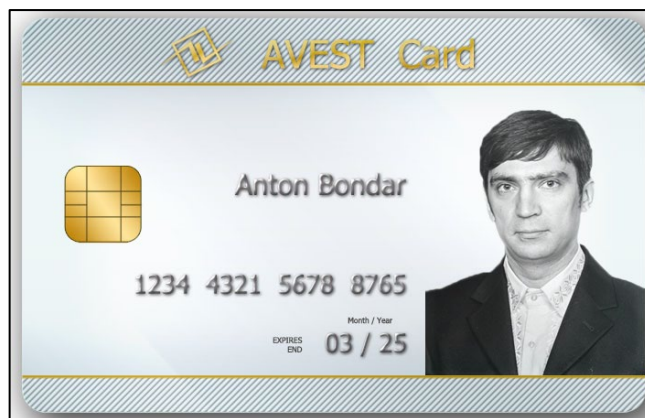


Рисунок 1.3 – Приклад смарткарти

На момент проведення теоретичної розвідки сучасні СКУД мають такі характеристики, що підвищують їхню ефективність:

- використовують комбінації карткової та біометричної автентифікації;
- часто базуються на хмарних технологіях, де контроль може відбуватися віддалено (рисунок 1.4), тим самим роблячи дані системи гнучкими та масштабованими;
- інтеграція з іншими системами безпеки дозволяє ефективніше запобігати несанкціонованим проникненням, швидше реагувати на загрози;
- розвиток технологій дозволяє керувати системою контролю та управління доступом віддалено за допомогою телефону, ноутбука та інших пристроїв [6–14].

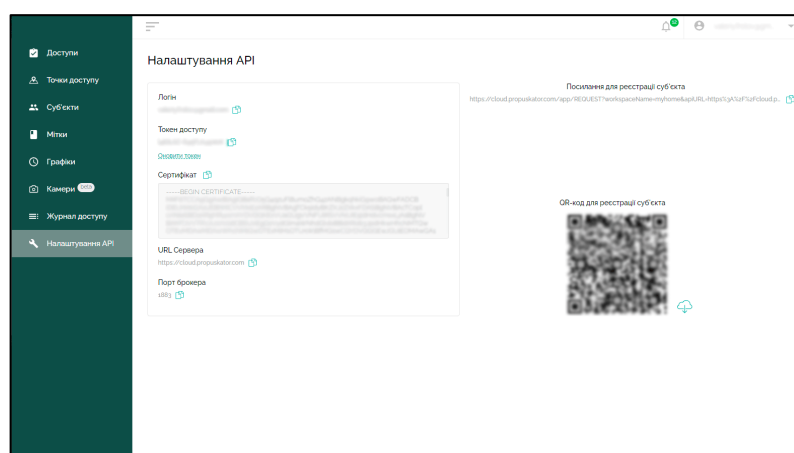


Рисунок 1.4 – Приклад хмарного сервісу для менеджменту СКУД

1.3 Стандарти та технічна характеристика СКУД

Встановлення системи контролю та управління доступом на об'єктах є однією зі складових елементів безпеки. Для забезпечення надійної та якісної роботи системи в Україні були розроблені стандарти та нормативні акти, які регулюють встановлення та експлуатацію СКУД. Окрім безпеки об'єктів дані стандарти забезпечують збереження та захист персональних даних (див. Таблицю 1.3).

Таблиця 1.3 – Положення нормативно-правової бази стосовно СКУД

Назва нормативно-правового акту	Змістове наповнення
Національний стандарт України «Системи контролю доступу. Вимоги до проектування, монтажу, експлуатації» (ДСТУ EN 50133-1:2017).	Містить вимоги до проектування, монтажу та експлуатації систем контролю та управління доступом. Визначає методи встановлення СКУД та вимоги до складових системи (системи ідентифікації, контролери, електронні замки та інші) [15].
Національний стандарт України «Системи безпеки. Вимоги до використання та експлуатації систем контролю доступу» (ДСТУ 4783:2007).	Містить вимоги експлуатації системи контролю та управління доступом з точки зору безпеки. Надає рекомендації щодо забезпечення безпеки та захисту персональних даних, які містяться та обробляються системою [16].
Наказ МВС України від 21.06.2013 р. №488 «Методичні рекомендації щодо застосування СКУД в охоронній діяльності».	Містять поради щодо застосування СКУД в охоронній діяльності, вибір компонентів системи, проектування та монтаж, безпека та захист персональних даних [17].
Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».	Регулює відносини у сфері захисту інформації в електронних, інформаційних, комунікаційних та інформаційно комунікаційних системах [18].
«Державні будівельні норми України»	Норми, що стосуються проектування, встановлення та експлуатації системи безпеки в будівлях [19].

Дані стандарти є одними з основних, їхнє виконання обов’язкове під час встановленні СКУД на різних об’єктах інфраструктури. Таким чином забезпечується безпека та конфіденційність даних працівників та відвідувачів. Недотримання даних стандартів та норм може призвести до накладання штрафів та юридичних наслідків.

СКУД, що відповідають зазначеним стандартам, можуть відрізнятися за технічними параметрами, що впливає на ефективність функціонування системи та відповідно вибір СКУД для використання на підприємствах, в офісах та інших об’єктах. Основні технічні характеристики СКУД охоплюють такі положення [2, 6].

Таблиця 1.4 – Основні технічні характеристики СКУД

Технічна характеристика СКУД	Опис параметра
Швидкість реакції	Час, який потрібен системі для обробки запиту на доступ. Швидкість реакції залежить від обладнання, яке використовується, зазвичай від 0.1 до 1 секунди, швидка реакція дозволяє уникнути затримок у проходженні персоналу та збільшує продуктивність системи.
Точність ідентифікації	Наскільки точно система може ідентифікувати користувача. Залежить від технології, яка використовується на об’єкті. Наприклад система, яка використовує картки доступу менш ефективні та точна, ніж система яка використовує біометричні дані (сканування відбитків, розпізнавання обличчя та інші).
Масштабованість	Можливість розширення системи (збільшення кількості приміщень та користувачів). Пристосування системи до змін потреб організації, збільшення кількості пристроїв ідентифікації, зменшення часу для установки та налаштування системи, без втрати продуктивності

Продовження таблиці 1.4

Технічна характеристика СКУД	Опис параметра
Підтримка протоколів	Підтримка стандартних протоколів зв'язку (TCP/IP, RS-485 та інші) з іншими системами безпеки (відеоспостереження, пожежна безпека та інші). Така інтеграція систем дозволяє забезпечити більш ефективний моніторинг та управління безпекою на об'єкті.
Віддалений доступ	Доступ до системи з будь-якого місця в будь-який час. Такий доступ може здійснюватися через інтернет або мережу. Це досить зручно, якщо об'єкт має декілька приміщень розташованих у різних місцях.
Резервне копіювання	Дозволяє зберігати копії даних системи контролю та управління доступом, що дає можливість відновити дані у випадку втрати основних даних. Таким чином зберігається безпека та доступність даних.
Надійність та безпечність	Стійкість до збоїв та висока доступність забезпечує надійність системи. Також система має містити резервування та відновлення даних для забезпечення неперервної роботи системи.
Ступінь доступу	Однією із важливих характеристик СКУД є ступінь доступу – недостатній (1-ий клас), середній (2-ий клас), високий (3-ий клас), дуже високий (4-ий клас) [3]. Опис даних класів подано нижче.

СКУД 1-го класу – працюють в автономному режимі, малофункціональні системи з малою місткістю. Системи даного ступеню доступу забезпечують:

- допуск до зони, яка під охороною осіб, які мають відповідний ідентифікатор;
- вбудована індикація режимів роботи;
- управління (ручне або автоматичне), відкриттям/закриттям пристроїв загородження (двері, ворота, шлагбаум та інші).

Системи даного типу застосовують для забезпечення контрольованого доступу працівників та відвідувачів, при цьому не акцентується увага на часі

доступу і виходу з приміщення, реєстрації проходів, передавання даних на центральний комп'ютер. Використовується, щоб обмежити доступ сторонніх осіб на об'єкт.

СКУД 2-го класу – працюють у мережевому або автономному режимі, однорівневі та багаторівневі системи малої та середньої місткості.

Системи даного ступеню доступу забезпечують:

- обмеження доступу в зону, що охороняється, групи осіб або конкретної особи за часовими інтервалами відповідно до наявного ідентифікатора;
- автоматична реєстрація подій у буфері пам'яті;
- передача тривожних сповіщень на зовнішні сповіщувачі або пост охорони та автоматичне відкриття/закриття пристроїв загородження.

Системи даного типу застосовують як доповнення до системи охорони, на об'єкті, де потрібний контроль та облік присутності працівників у приміщеннях.

СКУД 3-го класу – працюють у мережевому режимі, однорівневі та багаторівневі системи середньої місткості.

Системи даного ступеню доступу забезпечують:

- функції СКУД 2-го класу;
- контроль переміщення працівників по підприємству;
- введення обліку та баз даних по працівниках, безперервний автоматичний контроль справності системи;
- інтеграція із системами та засобами пожежної сигналізації та системою відеоконтролю на релейному рівні.

Системи даного типу застосовуються на об'єктах де потрібний облік та контроль переміщення працівників по об'єкту, для спільної роботи із пожежною системою, системою охорони та відеоконтролю.

СКУД 4-го класу – працюють у мережевому режимі, багаторівневі та великої місткості.

Системи даного ступеню доступу забезпечують:

- функції СКУД 3-го класу;
- пожежну безпеку, охорону, системи відеоконтролю та інші системи безпеки на управління доступом на програмному рівні;
- автоматичне керування пристроями загородження у разі виникнення надзвичайних ситуацій.

Як і СКУД 3-го класу, використовується на об'єктах де потрібний облік та контроль переміщення працівників по об'єкту, співпраця із системами відеоконтролю, пожежною системою та охоронною системою.

В залежності від потреб та особливостей підприємств набір функцій доступу може розширюватися, поєднуватися кілька класів СКУД.

1.4 Класифікація систем СКУД

Системи контролю та управління доступом можна поділити на дві категорії: централізовані (мережеві) та автономні [3, 20].

Централізовані або мережеві системи охоплюють системи, що мають можливість контролювати присутність та пересування працівників на робочих місцях, обмежувати доступ до об'єктів за часом, розподіляти зони доступу (кабінети, поверхи, корпуси), одночасне керування значним числом пунктів пропуску, оперативно вносити зміни та додавати нові функції. Для таких типів систем розробляється програмне забезпечення для створення інформації про кожного працівника: фотокартка, особисті дані та інша інформація, яка буде необхідна для підприємства.

Передбачає управління великою кількістю точок доступу та з'єднує всі контролери з керуючим комп'ютером.

Централізовані системи встановлюють на великих промислових або офісних об'єктах з великою кількістю робітників та відвідувачів.

Автономні системи самостійно керують роботою периферійних елементів та контролюють точки доступу. До автономних СКУД належать

системи, які розташовані в одному приміщенні. Основна функція – обмеження доступу до об'єктів, що контролюються. Даний тип систем застосовується у банківській сфері, для обмеження доступу до банкоматів, встановлення спеціальних пристроїв для зчитування реквізитів з банківської карти (скімер). До таких СКУД інтегрують системи антискрімінгу, що дозволяє запобігти несанкціонованим діям злоумисників.

Автономні системи використовують в адміністративних, освітніх та суспільних закладах, приватних будинках, банківська сфера.

Також системи контролю можна класифікувати за низкою критеріїв [3]:

За технічними характеристиками та функціональними можливостями:

- кількість контрольованих місць;
- пропускна здатність;
- кількість користувачів;
- рівень ідентифікації;
- умови експлуатації.

За рівнем ідентифікації доступу:

- однорівневі – ідентифікація здійснюється за однією ознакою (введення коду користувача);
- багаторівневі – ідентифікація здійснюється за декількома ознаками (зчитування коду з карти та біометричних даних).

За умовами експлуатації:

- закриті приміщення;
- закриті неопалювальні приміщення;
- на вулиці під навісом, помірно-холодний клімат;
- на вулиці, помірно-холодний клімат;
- особливі умови (вібрації, запиленість, вологість та інші).

За кількістю контрольованих точок:

- мала місткість (до 16 місць);
- середня місткість (від 16 до 64 місць);

- велика місткість (понад 64 місць).

За основними функціональними можливостями:

- можливість оперативного перепрограмування;
- технічний та програмний захист від вандалізму та саботажу;
- високий рівень секретності;
- автоматична ідентифікація;
- розмежування доступу співробітників та відвідувачів у приміщення або на об'єкт в цілому;
- механічне замикання приміщень, з можливістю аварійного відкриття вручну;
- автоматичний збір та аналіз даних;
- видрук даних.

1.5 Ідентифікатори СКУД

Ідентифікатор – пристрій, який встановлює право доступу особи на об'єкт. Таким чином, дозволяє системі розпізнати особу. Найчастіше використовують безконтактні або контактні картки, електронні брелоки, спеціальний код для входу в зону, що охороняється, біометричні дані. Кожен ідентифікатор, що використовується, характеризується, унікальним двійковим кодом. У СКУД кожному коду ставиться у відповідність інформація про власника (особу) ідентифікатора та інформація про права доступу даної особи, до різних зон на об'єкті.

Ідентифікатори класифікуються за функціональними характеристиками, функціональним призначенням пристроїв та стійкістю до несанкціонованого доступу. Основними видами ідентифікаційних ознак є такі варіації: оптичні, електронні, біометричні, комбіновані та механічні ідентифікаційні ознаки.

1.5.1 Оптичні ідентифікатори СКУД

В основі оптичних ідентифікаторів СКУД використовують мітки, які розташовані всередині ідентифікатора або нанесені на поверхню ідентифікатора. Прикладом таких оптичних ідентифікаторів можуть бути топографічні мітки, картки зі штрих-кодом, QR-коди (рисунок 1.5) та інші [21].



а – картки зі штрих-кодом; б – QR-коди

Рисунок 1.5 – Оптичні ідентифікатори

Перевагами використання оптичних ідентифікаторів є швидка ідентифікація, легка заміна карток, невисока вартість встановлення системи.

Недоліками таких ідентифікаторів є те, що деякі із типів ідентифікаторів можуть втратити свою якість, зноситися і тим самим погіршується ідентифікація.

1.5.2 Біометричні ідентифікатори СКУД

Біометричні ідентифікатори використовують індивідуальні фізичні ознаки людини. До таких ідентифікаторів відносять: відбитки пальців,

сканування сітківки ока, ідентифікація за голосом, ходом, геометрією особи та рук (рисунок 1.6) [22].

Найбільш популярним серед біометричних ідентифікаторів СКУД є розпізнавання відбитків пальців – дактилоскопія. Алгоритм використовує характерні точки на відбитках пальців: «арочні» та спіральні лінії, папілярний візерунок. Перевагами даного методу ідентифікації є досить проста процедура сканування, низька вартість пристроїв сканування, висока ймовірність ідентифікації. Але є і недоліки такого методу, візерунок відбитка пальця дуже легко пошкодити, сканери можуть не реагувати на суху шкіру або людей похилого віку. Є ймовірність підробки відбитка, оскільки даний метод ідентифікації є досить поширеним.



Рисунок 1.6 – Технології біометричної ідентифікації

Сканування райдужної оболонки ока менш популярний метод ідентифікації СКУД через вищу ціну. Даний алгоритм більш надійний, райдужна оболонка ока захищена від пошкоджень, більша кількість методів, що захищають від підробки.

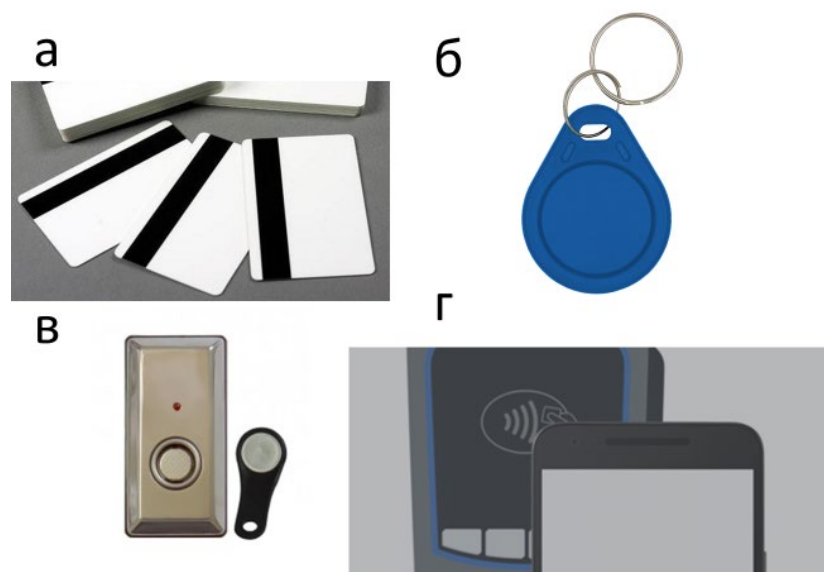
Часто використовують розпізнавання обличчя в якості біометричного ідентифікатора. Принцип роботи такого біометричного ідентифікатора полягає у тому, що система аналізує зображення обличчя з камери для встановлення таких особливостей, як форма, розмір очей, носа, рота та їх положення. Ідентифікатор такого типу використовує багато різних алгоритмів, наприклад нейронні мережі.

Переваги таких систем: швидкість, відсутність фізичного контакту з пристроєм.

Серед недоліків можна виділити, такі як помилкова ідентифікація, зниження точності при зміні умов освітлення або зміні зовнішнього вигляду людини.

1.5.3 Електронні ідентифікатори СКУД

Електронні ідентифікатори СКУД можна розділити на контактні та радіочастотні. Електронні контактні ідентифікатори – електронний код, записаний в електронній мікросхемі ідентифікатора. Наприклад: електронні ключі (рисунок 1.7).



а – магнітні картки; б – RFID-мітка, в – тач-меморі, г – NFC-токен

Рисунок 1.7 – Електронні ідентифікатори

Використовують для об'єктів, де не потрібний високий клас захищеності. Дана система не надійна, оскільки такий ключ легко скопіювати. Електронні радіочастотні ідентифікатори – радіоканали, які використовують для передачі даних. Наприклад: безконтактні карти доступу.

Радіочастотна ідентифікація (RFID) – метод автоматичної ідентифікації об'єктів, де за допомогою радіосигналів записуються або зчитуються дані, які зберігаються у RFID-мітках. Така система складається із RFID-мітки та зчитувача [23].

RFID-мітка – пристрій, який зберігає та передає інформацію за допомогою радіохвиль. Класифікація RFID-міток та систем радіочастотних ідентифікаторів відбувається за різними критеріями (рисунок 1.8):

- за діапазоном частот (низькочастотні, високочастотні, ультрависокочастотні);
- за типом джерела живлення (пасивні, напівпасивні, активні);
- за типом пам'яті (тільки на зчитування – Read Only, одноразовий запис та багаторазове зчитування – WORM, багаторазовий запис та зчитування – R/W);
- за виконанням.

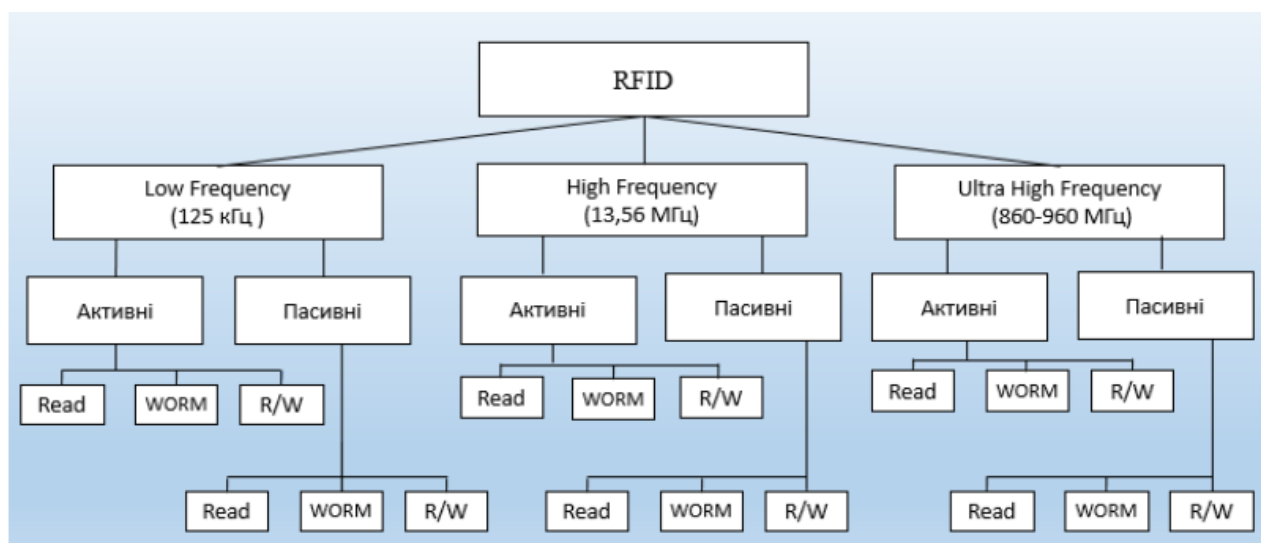


Рисунок 1.8 – Класифікація системи радіочастотної ідентифікації

2 АНАЛІЗ СКУД ДЛЯ ПІДПРИЄМСТВ

Запровадження системи контролю та управління доступом на підприємстві є досить важливим кроком, оскільки забезпечує безпеку та ефективність. Підприємства з різних сфер діяльності можуть мати різні потреби та характеристики до встановлення СКУД. Проте, незважаючи на індивідуальність роботи підприємства існують загальні характеристики та потреби, які є важливими для всіх підприємств.

2.1 Характеристики підприємств для запровадження СКУД

Характеристика підприємств відображає його основні риси та параметри, такі як сфера діяльності, кількість співробітників, розмір та інші.

Розглянемо більш детально характеристики підприємств, які необхідно враховувати при запровадженні системи контролю та управління доступом. Особливу увагу слід звернути на характеристики. (рисунок 2.1)

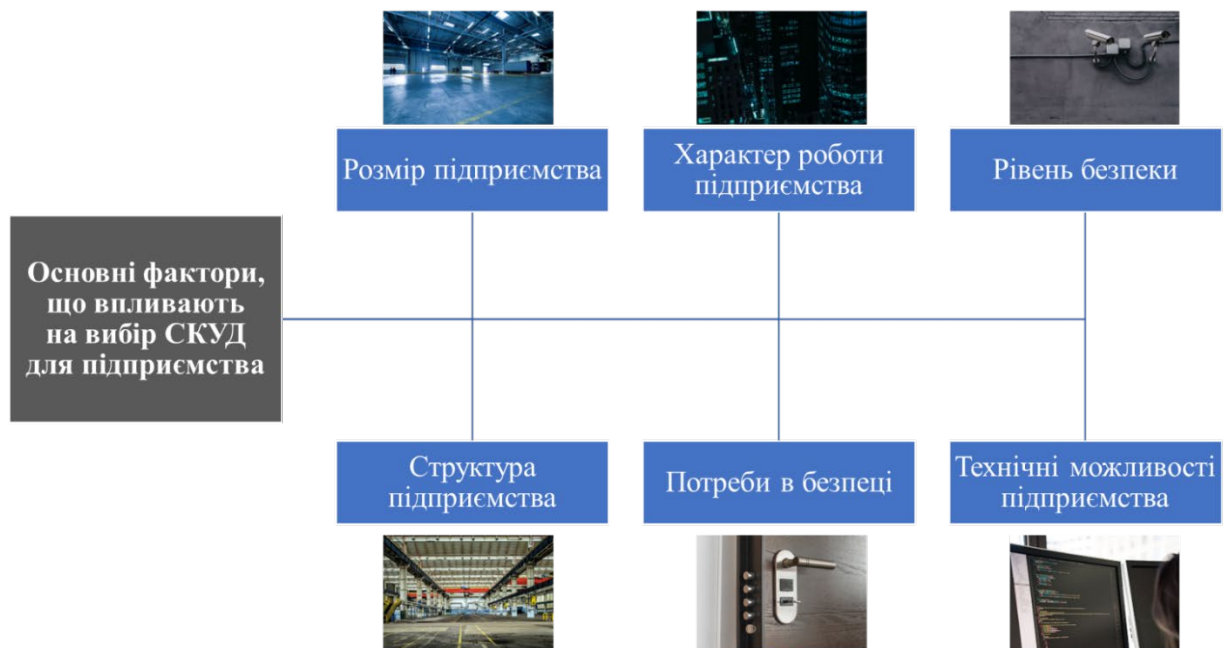


Рисунок 2.1 – Фактори, що впливають на запровадження СКУД

1. Розмір підприємства

Розмір підприємства визначається наступними ознаками: обсяг виробництва, кількість працівників, кількість відділень підприємства. Чим більша організація, тим складніше контролювати переміщення та доступ працівників та відвідувачів до різних приміщень. Для малих підприємств в більшості випадків достатньо встановити систему контролю доступу до приміщень. В той час для великих підприємств потрібна складніша система з використанням карток доступу та електронних замків. Таким чином СКУД надзвичайно важлива для забезпечення безпеки та ефективності контролю доступу.

2. Структура підприємства

Система контролю та управління доступом має враховувати структуру підприємства, а саме форму та розподіл функцій, повноваження між відділами та підрозділами підприємства.

Наприклад, якщо компанія розбита на декілька департаментів та відділів, важливо забезпечити доступ до окремих зон працівників, які мають відповідні повноваження. Іншими словами, потрібно забезпечити різні рівні доступу, в якому керівники мають доступ до всіх приміщень об'єкта, співробітники – до приміщень із відповідним рівнем допуску, відвідувачі – ще більш обмежений доступ.

При запровадженні СКУД потрібно враховувати структуру підприємства, оскільки вона впливає на складність системи, масштабність системи, кількість точок контролю доступу та їх розташування, налаштування прав доступу, загальний рівень безпеки.

3. Характер роботи підприємства

Характер роботи підприємств визначається режимом роботи підприємства, типом роботи, обсягом робіт та іншими.

Для підприємств з великою кількістю відвідувачів, варто забезпечити окремий доступ до приміщень та зон доступу для відвідувачів, для

забезпечення від несанкціонованого доступу, витоку інформації, порушення безпеки співробітників та підприємства.

Важливо враховувати режим роботи, оскільки підприємство може мати нічні та денні зміни, отже має бути різний рівень доступу, для робітників, що працюють в різні зміни. Також підприємство або об'єкт може працювати цілодобово, або у певний проміжок часу, тому знову ж таки потрібно контролювати доступ співробітників та відвідувачів.

Потрібно детально аналізувати характер роботи підприємства при запровадженні СКУД, для того, щоб забезпечити потрібний рівень контролю доступу та безпеки на об'єкті.

4. Потреби в безпеці

Дана характеристика визначає необхідний рівень безпеки у приміщеннях та об'єктах. В залежності від типу діяльності та ризиків, СКУД можуть встановлюватися різні заходи забезпечення безпеки.

Для промислових підприємств, де використовують небезпечні матеріали та обладнання, крім попереджувальних знаків про небезпеку (рисунок 2.2), можуть встановлювати контроль доступу до небезпечних зон, додаткові заходи безпеки для працівників.



Рисунок 2.2 – Попереджувальний знак на підприємстві з обмеженим доступом

Для фінансових установ, важливо встановлювати високий рівень захисту від крадіжок, вторгнень, зламів замків. Таким чином, СКУД може забезпечити контроль доступу до окремих зон, з використанням біометричних ідентифікаторів, високоточних пристроїв.

Також можуть бути специфічні потреби в безпеці, через високий рівень конфіденційності даних або характеру роботи. СКУД може забезпечити контроль доступу до таких об'єктів.

Потреби в безпеці мають велике значення при запровадженні СКУД і враховуються при визначенні потрібних заходів безпеки та контролю доступу до приміщень на об'єктах.

5. Рівень безпеки

Рівень безпеки підприємства – комплексний показник, який відображає ступінь захищеності об'єкта (підприємства, офісу) від можливих загроз. Такі рівні безпеки містять: кібербезпеку, пожежну та медичну безпеку, фізичну безпеку та інші. Визначається від розміру, локації та виду діяльності підприємства.

Для малих підприємств та офісів, у більшості випадків, достатньо встановлення системи контролю та надійних паролів. Для великих підприємств доцільно використовувати складні системи, які охоплюють відеоспостереження, контроль доступу до приміщень, пожежні системи. Використовувати оптичні або біометричні ідентифікатори (або їх поєднання) для контролю переміщення, входу/виходу співробітників та відвідувачів.

Загалом рівні безпеки можуть бути різними, залежать від багатьох індивідуальних факторів об'єкта. Належні заходи безпеки дозволяють забезпечити захист майна, інформації, працівників.

6. Технічні можливості підприємства

Технічні можливості підприємства – це сукупність програмного забезпечення, обладнання, інфраструктури та інших технічних засобів. Технічні можливості залежать від виду підприємства та сфери діяльності (рисунок 2.3).



Рисунок 2.3 – Технічні можливості підприємства, які впливають на функціонування СКУД

Технічні можливості мають відповідати потребам підприємства та забезпечувати потрібний рівень безпеки, а саме має бути відповідне обладнання та програмне забезпечення.

До технічних можливостей підприємства можна віднести:

- наявність системи моніторингу та запису дій працівників та відвідувачів на підприємстві;
- наявність серверного обладнання для збереження даних, керування системою контролю та управління доступом;
- технічний персонал, який буде обслуговувати та підтримувати СКУД;
- інтеграція системи контролю та управління доступом з іншими системами на об'єкті (система відеоспостереження, система сповіщення про пожежу, аварію та інші);

- наявність мережевого обладнання для забезпечення контролю доступу з різних пристроїв та з будь-якого місця;
- забезпечення резервного копіювання та відновлення даних у випадку непередбачених ситуацій;
- інформаційна система та система аналізу та моніторингу стану СКУД та виявлення потенційних загроз;
- оновлення технічної бази СКУД, щоб забезпечити безперебійну роботу та можливість додавання нових функцій.

Рівень технічних можливостей підприємства визначає ефективність та масштаби реалізації СКУД.

7. Фінансові можливості підприємства

Фінансова можливість охоплює фінансовий стан підприємства та його можливості фінансувати встановлення та обслуговування системи контролю доступу. Серед основних фінансових можливостей, які впливають на встановлення системи контролю та управління доступу, можна виділити:

- фінансові показники підприємства: прибуток, оборотні кошти, рентабельність. Представлені показники можуть вплинути на можливість виділення коштів для встановлення та обслуговування системи контролю та управління доступом;
- бюджет підприємства. Вартість СКУД може різнитися, в залежності від технічних засобів та обсягу роботи. Тому важливо точно та уважно оцінювати можливості підприємства, визначити необхідні компоненти СКУД та програмне забезпечення;
- інвестиції на капіталовкладення. Встановлення СКУД потребує значних грошових вкладень, тому можуть знадобитися капіталовкладення та інвестиції. Також вони забезпечують стабільність роботи, конкурентоспроможність, удосконалення виробництва, розвиток та розширення, впровадження нових технологій.

2.2 Потреби підприємств для запровадження СКУД.

Потреби підприємства відображають конкретні цілі та завдання, які потрібно вирішити за допомогою СКУД.

Розглянемо більш детально деякі із потреб підприємств для запровадження СКУД.

1. Забезпечення безпеки.

Основна потреба будь-якого підприємства забезпечення безпеки, саме тому впроваджують СКУД. Застосовують різні способи ідентифікації особи, наприклад: відбитки пальців, сканування обличчя, картки доступу, таким чином система допомагає зменшити зовнішні та внутрішні загрози, обмежує права доступу працівників та відвідувачів.

2. Контроль доступу.

Важливо контролювати доступ співробітників до різних приміщень об'єкта, саме тому система перевіряє права доступу, повноваження особи. Це потрібно також для того, щоб працівники які не мають спеціальних знань, не могли проникнути до технічної системи або приміщень із важливою інформацією або лабораторій (все залежить від типу об'єкта).

3. Облік робочого часу.

Одна із важливих потреб запровадження СКУД на підприємстві, оскільки можна забезпечити точний облік робочого часу співробітників. Такий облік дозволяє відстежувати запізнення або пропуск робочого часу, дозволяє точніше розраховувати заробітну плату.

4. Відстеження руху та активності співробітників та відвідувачів.

СКУД може відстежувати рух осіб, а також їх активність у приміщені. Тим самим система допомагає виявляти осіб які здійснювали нелегітимні дії, а отже відстежування порушень безпеки, крадіжки матеріальних цінностей або конфіденційної інформації. Відстежування активності, дозволяє визначити яким обладнанням користувався співробітник, через які двері проходив, що

робив. Таким чином можна виявити затримки або відхилення від звичної роботи.

5. Економія часу та грошей

Система контролю та управління доступу допомагає зменшити час необхідний для обліку робочого часу та контролю доступу. Також зменшує витрати на охорону, що зменшує похибку людському фактору при перевірці відвідувачів або співробітників. В загальному СКУД допомагає знизити витрати підприємства та покращує ефективність контролю доступу та безпеки об'єкта.

6. Покращення ефективності роботи

СКУД допомагає виявляти та усувати перешкоди для роботи співробітників та відвідувачів, а також покращувати ефективність роботи. Наприклад, сучасна система контролю доступу, пришвидшує проходження контрольних точок працівниками

7. Керування ризиками.

Встановлення системи контролю та управління доступом допомагає керувати ризиками та знижує ймовірність несанкціонованого доступу до об'єкта, приміщень або інформації. Встановлюються рівні доступу, щоб співробітники із нижчим рівнем доступу або співробітники без спеціальних знань та досвіду, не мали доступу до технічних приміщень, до конфіденційної інформації або активів.

8. Зниження витрат на охорону.

Зменшення витрат на охорону доцільне, якщо об'єкт охорони має багато працівників або приміщень, які потребують охорони. Встановлення системи контролю та управління доступом має змогу контролювати доступ до приміщень об'єкта.

9. Автоматизація процесів

Запровадження СКУД на об'єкт допомагає автоматизувати процес контролю доступу, відстежування робочого часу співробітників, а також

допомагає контролювати права доступу. Автоматизація процесів знижує кількість помилок та забезпечує точність даних.

10. Дотримання вимог законодавства

Існують закони, нормативні акти та рекомендації яких потрібно дотримуватися при встановленні системи контролю та управління доступом. Тим самим підприємство має змогу дотримуватися усіх вимог законодавства пов'язаних з охороною праці, безпекою інформації та контролем доступу до неї. СКУД може допомогти при проведенні аудитів та перевірок державних органів, оскільки всі звіти, всі дані зберігаються [15–19].

Визначивши характеристики та потреби підприємства для запровадження СКУД, варто також вказати на ресурси, які будуть потрібні для встановлення системи. А саме:

- пристрої ідентифікації користувачів (картки, ключі RFID, біометрична ідентифікація);
- спеціальне обладнання для зчитування та запису даних з RFID-пристроїв;
- програмне забезпечення, потрібне для збору, обробки та аналізу даних з системи контролю та управління доступу;
- відеоспостереження та система аналізу;
- система оповіщення (порушення режиму доступу або невідповідність доступу);
- консультація та підтримка до та після встановлення СКУД.

Запровадження системи контролю та управління доступу підвищує рівень безпеки, знижує витрати на охорону, допомагає оптимізувати виробництво і забезпечує конкурентну перевагу. Звичайно все залежить від фінансової можливості, а також технічних можливостей об'єкта. Також важливим чинником встановлення СКУД є тип підприємства або об'єкта. Для об'єкта критичної інфраструктури, обов'язково встановлювати надійну систему безпеки, щоб убезпечитися від несанкціонованого проникнення або витоку конфіденційної інформації. Маленькі компанії встановлюються СКУД, в

більшості випадків, для контролю переміщення працівників, а також контроль робочого часу.

Наведемо приклади запровадження системи контролю та управління доступом для деяких підприємств.

Бізнес-центри та офісні приміщення: встановлюють СКУД для контролю доступу до приміщень (приміщення з конфіденційною інформацією, серверні кімнати), контролю переміщення співробітників, обліку робочого часу (рисунок 2.4).



Рисунок 2.4 – Використання турікету-триподу в бізнес-центрі

Магазини та торгові центри: встановлюють СКУД для контролю доступу до зон з обмеженими правами доступу (склади, технічні приміщення та інші), забезпечує безпеку на робочому місці та знижує ризики виникнення аварій та інцидентів.

Медичні установи та лікарні: встановлюють СКУД для контролю доступу до зон з обмеженим доступом (процедурні кімнати, приміщення із

лікарськими засобами та медичним обладнанням). Також допомагає контролювати рух персоналу, забезпечує конфіденційність та безпеку пацієнтів, покращує управління процесом роботи медичного персоналу.

Школи: встановлення системи контролю та управління доступом допомагає контролювати доступ учнів та вчителів до різних зон школи (аудиторії, бібліотеки та інші), контролювати відвідуваність учнями школи, також контроль доступу батьків та інших відвідувачів, що забезпечує безпеку учнів та вчителів.

Промислові підприємства: СКУД допомагає контролювати доступ до приміщень (технічні приміщення, склади), контролює час входу та виходу працівників, відвідуваність. Загалом підвищує ефективність роботи підприємства.

Аеропорт: СКУД допомагає в контролі доступу до приміщень аеропорту (зони прильоту та відльоту, зона збереження багажу, службові та технічні приміщення), контролює час входу та виходу працівників, допомагає забезпечувати ефективну роботу персоналу, забезпечує безпеку персоналу та пасажирів.

2.3 Аналіз ринку СКУД

Ринок СКУД розвивається і стає більш конкурентним, через зріст попиту на безпеку. Безпека в свою чергу є основою для корпорацій, підприємств, офісів, приватної власності. Сьогодні можна замовити та встановити різні варіанти СКУД, окремі компоненти (контролери, пристрої ідентифікації та пропуску), програмне забезпечення, а також консультація та підтримка для потенційних покупців. Також варіація ціни, дозволяє обрати потрібну систему контролю доступу, як для великого підприємства або корпорації, так і для маленьких офісів, компаній, приватного сектора.

Розвиток технологій, а саме штучний інтелект, машинне навчання, розвитком та розширенням Інтернету речей (IoT), дозволяє більш точно та

ефективно виконувати функції СКУД. Мобільні технології дозволяють контролювати доступ до приміщень за допомогою мобільних додатків. Зростає попит на використання хмарних технологій, технологія доступу на основі біометричних даних.

Ринок СКУД наповнений різноманітними системами, простими, складними, багатофункціональними, з різним типом доступу та ідентифікації. Серед різноманітності варіантів СКУД, виділяються основні, а саме:

1. Система контролю та управління доступу на основі карток – користувачі отримують картки з чіпом або магнітною стрічкою, які при скануванні надають доступ до приміщення або об'єкта.
2. Система контролю та управління доступу на основі біометрії – система використовує біометричні дані особи: відбитки, сканування райдужки або сітківки ока, розпізнавання обличчя та інші.
3. Система контролю та управління доступу на основі кодів доступу – використання числових комбінацій для надання доступу до об'єкта та приміщень.
4. Мобільні системи контролю та управління доступу – використання мобільних пристроїв для отримання доступу до приміщення.
5. Інтернет системи контролю та управління доступу – віддалене керування доступом через мережу Інтернет.
6. Гібридні системи контролю та управління доступу представляють собою інтегроване поєднання різних варіантів систем контролю доступу (СКУД), що дозволяє отримати більш гнучкий та ефективний підхід до управління доступом у приміщеннях та об'єктах. До ключових переваг гібридних систем належать їхній високий рівень гнучкості та безпеки.

Кожен із представлених видів системи контролю та управління доступом має власні унікальні (притаманні даному видові СКУД) пристрої контролю доступу, а також спільні для всіх пристрої доступу. Більш детально опишемо пристрої доступу для різних видів СКУД та комунікацію між даними пристроями.

У таблиці 2.1 наведено пристрої контролю та управління, а також комунікація між наведеними пристроями доступу для описаних вище видів систем контролю та управління доступом.

Таблиця 2.1 – Порівняння основних типів СКУД

Вид СКУД	Пристрої	Комунікація
На основі карток доступу	- картки з чіпом або магнітним записом; - кард-рідер; - контролер	Кабель «вита пара», Bluetooth, NFC, RFID, протокол Wiegand
На основі біометрії	- біометричні сенсори (сканування відбитка, сітківки або райдужки ока, обличчя, розпізнавання голосу); - контролер.	Wi-Fi, Bluetooth, NFC
На основі кодів доступу	- клавіатура; - зчитувач кодів; - контролер.	Кабель «вита пара», Bluetooth, NFC
Мобільні системи	- мобільні додатки; - смартфони, планшети; - NFC-модулі; - Bluetooth; - QR-коди.	Wi-Fi, мобільна мережа 3G, 4G, 5G
Інтернет системи	- веб-сервер; - мережеві зчитувачі; - контролер.	зв'язок через Інтернет за допомогою протоколів TCP/IP, HTTP, HTTPS, Ethernet-кабель
Гібридні системи	- картки доступу; - кард-рідер; - біометричні сенсори; - коди доступу; - мобільні додатки; - веб-камери; - контролер.	Кабель «вита пара», Wi-Fi, Bluetooth, NFC, зв'язок через Інтернет за допомогою протоколів TCP/IP, HTTP, HTTPS

Всі системи мають свої переваги та недоліки, СКУД не є винятком. Тому важливо визначити основні переваги та недоліки різних типів СКУД, щоб ефективно впроваджувати їх на різного типу підприємства, а також щоб

визначити який з типів СКУД гарантує більш якісний захист від зовнішніх та внутрішніх загроз.

У таблиці 2.2 наведено переваги та недоліки вище описаних видів систем контролю та управління доступом (СКУД).

Таблиця 2.2 – Переваги й недоліки основних типів СКУД

Вид СКУД	Переваги	Недоліки
На основі карток доступу	- легка установка та використання; - багато пам'яті; - можливість вносити зміни прав доступу; - можливість обмеження часу доступу; - відстеження доступу працівника; - легко блокувати у разі втрати.	- легко втрачається або крадеться; - просто скопіювати або підробити; - вимагає фізичного контакту.
На основі біометрії	- висока точність ідентифікації користувача; - неможливо втратити або передати біометричні дані.	- великі витрати на установку та підтримку; - обмеження по типах біометричних даних; - біометричні дані можуть бути змінені або підроблені.
На основі кодів доступу	- порівняно дешевий варіант ідентифікації; - простий у використанні; - легко замінювати коди доступу; - можна створювати тимчасові коди доступу.	- легко зламати чи скопіювати; - потрібно запам'ятовувати коди доступу.
Мобільні системи	- зручні у використанні; - неможливість втрати або крадіжки; - можливість заблокувати користувача у разі втрати мобільного пристрою.	- потреба у сумісному мобільному пристрої; - додаткове налаштування пристрою; - втрата мобільного пристрою.
Інтернет системи	- віддалене керування доступом; - висока гнучкість в управлінні правами доступу; - можливість відстеження історії доступу.	- залежність від інтернет-з'єднання; - вразливість до кібератак.

Продовження таблиці 2.2

Вид СКУД	Переваги	Недоліки
Гібридні системи	- можливість поєднувати різні типи СКУД; - більш гнучке управління правами доступу.	- налаштування та інтеграція різних видів СКУД; - в деяких випадках, залежність від інтернет-з'єднання; - висока вартість установки та обслуговування.

В цілому, кожен вид СКУД має свої переваги та недоліки, вибір конкретного варіанту залежить від потреб та обставин конкретної ситуації. Загальна перевага всіх СКУД є можливість точного контролю до приміщення та забезпечення безпеки.

На ринку СКУД представлено багато компаній, до найбільших міжнародних виробників належать Bosch Security System Inc., Honeywell International Inc., Tyco International Ltd., Johnson Controls International plc, до українських виробників можна віднести «Захід-Комп'ютер», «Електронні технології безпеки», «Інтелтех», Ajax Systems та інші.

У таблиці 2.3 наведено порівняльну характеристику виробників систем контролю та управління доступом, а саме переваги та недоліки замовлення систем контролю у міжнародних та вітчизняних виробників.

Таблиця 2.3 – Порівняння СКУД за виробниками

Компанія виробник	Країна/рік заснування	Переваги	Недоліки
Bosch Security System	Німеччина 1886	- висока якість продукції; - технічна підтримка; - інноваційні рішення; - стабільність; - широкий асортимент продуктів та сервісів.	- високі ціни; - відсутність української локалізації на деяких продуктах.

Продовження таблиці 2.3

Компанія виробник	Країна/рік заснування	Переваги	Недоліки
Honeywell International	США 1906	- висока якість та безпека продуктів; - широкий спектр вибору продуктів та рішень; - надійність; - інтеграція з іншими системами.	- високі ціни; - відсутня пробна версія.
Tyco International	Швейцарія 1960	- широкий асортимент продуктів; - великий досвід у розробці та впровадженні; - гнучкість відносно індивідуальних потреб клієнтів.	- високі ціни; - погана технічна підтримка (часті випадки); - низький рівень безпеки продуктів.
Johnson Controls International	США 1885	- великий досвід у розробці та впровадженні систем; - висока якість продуктів; - гнучкість відносно індивідуальних потреб клієнтів; - інтеграція з іншими системами.	- високі ціни; - обмежена функціональність для великих підприємств; - обмежений асортимент продукції.
Захід-Комп'ютер	Україна 1997	- розробка власного програмного забезпечення; - розробка власного обладнання; - гнучкість; - індивідуальний підхід до потреб клієнтів; - низькі ціни та продукцію та послуги.	- обмежений асортимент продукції; - малий досвід роботи на світовому рівні; - низький рівень технічної підтримки.
Електронні технології безпеки	Україна 1994	- високі технічні характеристики продукції; - розробка власного програмного забезпечення; - розробка власного обладнання; - гнучкість до потреб клієнтів; - широкий асортимент продуктів та послуг.	- високі ціни; - обмежена функціональність для великих підприємств; - малий досвід роботи на міжнародному ринку.

Продовження таблиці 2.3

Компанія виробник	Країна/рік заснування	Переваги	Недоліки
Ajax Systems	Україна 2011	- високі технічні характеристики продуктів; - використання новітніх технологій та інновацій; - широкий асортимент продуктів та послуг; - простота та зручність.	- високі ціни; - не всі функції доступні у базовій версії; - не всі рішення підходять для великих підприємств.
Інтелтех	Україна 2000	- розробка власного програмного забезпечення; - розробка власного обладнання; - забезпечення індивідуальних потреб замовників; - широкий асортимент продуктів.	- низький рівень технічної підтримки; - обмежена функціональність для великих підприємств; - відсутність безплатної пробної версії.

Також на ринку багато середніх та маленьких підприємств, що спеціалізуються на розробці та виробництві окремих компонентів системи контролю та управління доступом. Варіативність вибору створює конкуренцію та можливість обрати оптимальний варіант для кожного клієнта. Зі збільшенням обсягів на ринку СКУД з'являються нові технології, які роблять легшою роботу з обладнанням та забезпечують більшу безпеку.

Всі компанії з виробництва та встановлення систем контролю та управління доступом, повинні відповідати певним стандартам, щоб якісно та ефективно виконувати поставлені задачі [25–27].

1. ISO 9001: міжнародний стандарт, що встановлює вимоги до системи управління якістю організації, забезпечення якості наданої продукції та послуг, а також постійне покращення системи. (Bosch Security Systems, Honeywell, Tyco, Johnson Controls (рисунок 2.5), Захід-Комп'ютер, Інтелтех).

2. ISO 14001: міжнародний стандарт, що встановлює вимоги до системи екологічного управління організації. Спрямований на зменшення

впливу виробництва на навколишнє середовище. (Bosch Security Systems, Honeywell, Tyco, Johnson Controls).

3. EN 50131: європейський стандарт, що встановлює вимоги до системи охоронної сигналізації, яка призначена для виявлення вторгнень або зломів. (Bosch Security Systems).

4. EN 50136: європейський стандарт, що встановлює вимоги до системи моніторингу безпеки для охорони майна, будівель та інших об'єктів. Стандарт включає вимоги до обладнання, програмного забезпечення та інших необхідних процедур захисту. (Bosch Security Systems – рисунок 2.6).

5. ISO 45001: міжнародний стандарт, що встановлює вимоги до системи управління охорони праці та безпеки на робочому місці. (Tyco, Johnson Controls).

6. CE: маркування, що підтверджує відповідність продукту вимогам Європейського Союзу. Встановлюється на виробках, що експортуються в ЄС, маркування забезпечує відповідність виробу основним вимогам безпеки, здоров'я та захисту навколишнього середовища. (Honeywell, Tyco, Johnson Controls, Ajax Systems, Захід-Комп'ютер, Електронні технології безпеки, Інтелтех).

7. UL: стандарт розроблений в США та прийнятий у багатьох країнах. Вимоги стандарту включають: оцінку продукту та вогнестійкість, електричну безпеку, електромагнітну сумісність, механічна стійкість та багато інших параметрів. (Honeywell, Tyco, Johnson Controls, Ajax Systems, Захід-Комп'ютер, Електронні технології безпеки, Інтелтех).



Рисунок 2.5 – Пристрій контролю доступу виробника Johnson Controls



Рисунок 2.6 – Камери відеоспостереження виробника Bosch Security Systems

Перед впровадженням СКУД на підприємство або в організацію варто дати відповідь на такі питання [28–29]:

- Яким вимогам має відповідати система?

– Де та чому потрібно встановлювати обмеження та контроль доступу? Сформулювати особливості підприємства.

– Яку роль відіграватиме СКУД на підприємстві? Просте розпізнавання користувачів чи докладний звіт із зазначенням даних особи та часових проміжків?

– Які додаткові функції можуть знадобитися?

Відповівши на дані питання, можна об'єктивно підібрати систему контролю та управління доступом для конкретного об'єкта. Також при виборі виробника СКУД, варто звернути увагу на відгуки інших користувачів, відеоогляди, консулюватися з різними виробниками та постачальниками.

Процес розробки та впровадження СКУД відбувається наступним чином:

- фахівці із встановлення збирають дані та потреби замовника;
- на об'єкті відбувається планування та підбір необхідного обладнання;
- розробляється проєкт, відповідно до зібраних даних та побажань замовника;
- можливе часткове впровадження у вигляді пілотного проєкту, для відстежування роботи системи;
- після успішного пілотного проєкту система масштабується на все підприємство.

У більшості випадків це стандартний процес розробки та впровадження СКУД. Звичайно все залежить від виробника та замовника, від типу підприємства, наповнення системи, обладнання та багато іншого. Також важливо, що компанії пропонують не тільки встановлення, але і підтримку в роботі системи та в разі виникнення неполадок – швидкий та якісний ремонт.

Звичайно існують деякі виклики, які негативно впливають на ринок СКУД. До таких викликів можна віднести: нестабільність економіки та політичної ситуації в країні, збільшення кількості кібератак та шахрайства,

висока вартість встановлення та підтримки системи, суворі правила дотримання захисту персональних даних. Також варто зауважити, що в Україні відсутні деякі законодавчі акти, які регулюють використання системи контролю та управління доступом та захист персональних даних. Що в свою чергу, може стати перешкодою для розвитку ринку СКУД в Україні.

Основні фактори, які впливають на зростання ринку СКУД в Україні:

- усвідомлення важливості безпеки та контролю робочого часу;
- висока конкуренція на ринку праці, відповідно необхідність ефективного управління персоналом;
- розвиток технологій;
- зменшення вартості обладнання.

В останні роки на ринку спостерігається зростання популярності СКУД на основі біометричних ідентифікаторів: сканування відбитків, сітківки та райдужки ока, розпізнавання обличчя. Очікується, що з розвитком технологій та потреб у безпеці, ринок СКУД продовжить зростати та стане конкурентоспроможним.

Розвиток ринку систем контролю та управління доступом пов'язаний не лише з технологічними змінами, але й змінами в законодавстві, які вимагатимуть від підприємств забезпечувати високий рівень безпеки працівників та інформації. Розвиток мережових та хмарних технологій, розширює можливості СКУД, що дозволяє забезпечувати безпеку віддалених робочих місць та віртуальних середовищ.

Зростання Використання СКУД дозволяє підвищити безпеку та контролювати робочий час співробітників, що є невід'ємною частиною успішної роботи будь-якої організації.

2.4 Переваги та недоліки використання СКУД

Система контролю та управління доступу у сучасному світі стає невід'ємною частиною забезпечення безпеки у бізнес-середовищі. СКУД

забезпечує безпеку, регулює доступ та контролює переміщення співробітників, контролює час роботи та ще багато функцій, які покращують ефективність роботи підприємства.

Звичайно кожна технологія має свої переваги та недоліки. Тому при використанні СКУД важливо враховувати всі фактори, для того, щоб обґрунтовано обрати потрібну систему, а також оптимально та ефективно використовувати всі наявні функції, зберегти час та кошти. Варто окреслити переваги використання СКУД.

1. Підвищення безпеки.

Обмеження доступу до об'єктів і зон, де це необхідно, контролю руху співробітників, попередження несанкціонованого входу до контрольованих приміщень та об'єктів, захист від крадіжок та інші порушення безпеки.

2. Ефективне керування персоналом.

Збір інформації про вхід/вихід персоналу, облік робочого часу, що в свою чергу забезпечує ефективне використання робочого часу.

3. Зниження витрат.

Зменшення витрат на охорону, заміна фізичної системи контролю доступу, покращує контроль за рухом людей та знижує витрати на охорону приміщень.

4. Простота використання.

СКУД може бути простою в управлінні та використанні, інтегрована з іншими системам управління, що дозволяє легко вести облік робочого часу, контролювати доступ до різних зон об'єкта та забезпечує безпеку.

5. Гнучкість.

СКУД можна адаптувати до потреб підприємства, а саме налаштовувати для кожного з типів підприємств, відповідно до потреб та особливостей. Також можливе розширення або зміна системи контролю, якщо потреби організації змінюються в часі. Наприклад розширення для забезпечення контролю доступу до нових зон, або відключення системи для забезпечення безперервного доступу до вже закритих зон.

6. Зручність.

Використання СКУД може зробити процес контролю доступу більш зручним для користувачів. Швидкий прохід на робоче місце, контроль часу роботи, швидка ідентифікація працівників та відвідувачів.

Переваги вказують на ефективне забезпечення безпеки за допомогою СКУД, проте як і будь-яка система, має недоліки, про які варто знати перед впровадженням СКУД на об'єкті.

1. Вартість.

Встановлення, налаштування та підтримка системи контролю може бути досить дорогим. Особливо для малих підприємств, може бути фінансово важко встановити СКУД.

2. Технічні проблеми.

Збій в системі, може спричинити значні проблеми та потенційні ризики, якщо доступ до об'єкта не буде контрольованим.

3. Конфіденційність.

Зберігання конфіденційної інформації, персональних даних про співробітників, може бути небезпечним, якщо неправильно використовувати СКУД або зловживати обов'язками.

4. Хакерські атаки.

Система контролю та управління доступом може стати метою хакерських атак, які можуть порушити безпеку, доступ до об'єкта або приміщення, витік конфіденційної інформації та персональних даних.

5. Залежність від електропостачання.

Потреба в постійному електропостачанні, оскільки при відключенні електроенергії або інших технічних неполадках система може не працювати.

6. Проблеми з інтеграцією.

Інтеграція з іншими системами контролю може бути складною та вимагати додаткових ресурсів, що може збільшити вартість та розгортання системи на об'єкті.

На сьогодні хакерські атаки стали одними із головних недоліків СКУД. Кібератака - намагання здійснити кіберзагрозу, тобто будь-які дії або події, які можуть призвести до порушення політики безпеки інформації або завдання шкоди автоматизованій системі. [30].

Законодавство України визначає: «Кібератака – це спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби та обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту» [30]. Кіберзлочинці використовують різноманітні методи зламу систем контролю та управління доступом, щоб отримати несанкціонований доступ до конфіденційної інформації або об'єктів охорони та контролю СКУД. Основними методами кібератак є перехоплення та підробка ідентифікаторів доступу, злам паролів доступу, фішингові атаки, використанні шкідливого програмного забезпечення. Загалом, під час кібератак на систему контролю та управління доступом, можуть бути зламані коди та ключі доступу, бази даних працівників та відвідувачів, клієнтів компанії або підприємства, порушені права доступу користувачів.

Декілька прикладів кібератак, які критично вплинули на роботу системи контролю та управління доступом на об'єктах критичної інфраструктури. 2015 рік – атака на українську електроенергетичну систему: група хакерів атакувала системи української електроенергетичної компанії та зупинила роботу систему контролю та управління доступом (СКУД), що призвело до

відключення електрики. Постраждали «Прикарпаттяобленерго», «Чернівціобленерго» та «Київобленерго». Атака відбулася за допомогою троянської програми «BlackEnergy». 2016 рік – атака на внутрішні мережі та урядові сайти держорганів України. Атака призвела до масштабних затримок бюджетних виплат, знищення баз даних, що мають відношення до Держказначейства та Пенсійного фонду, а також виведення з ладу комп'ютерів даних установ. Ці та ще багато прикладів (рисунок 2.7) показують, що кібератаки – серйозна загроза для СКУД та інших інтегрованих систем, які використовуються на об'єктах критичної інфраструктури. Компанії мають серйозно ставитися до подібних загроз, щоб захистити працівників, обладнання, інформацію на об'єкті.



Рисунок 2.7 – Інфографіка про найбільші кібератаки у світі від видання «Слово і діло»

Важливо ретельно оцінити всі переваги та недоліки використання системи контролю та управління доступом (СКУД) перед її впровадженням, щоб забезпечити максимальну ефективність та безпеку при використанні системи. Також важливо належно підтримувати та оновлювати систему, щоб вона була більш ефективною та менш вразливою до кібератак.

3 МЕТОДИКА ВПРОВАДЖЕННЯ СКУД НА ПІДПРИЄМСТВІ

У даному розділі детально описано процес впровадження СКУД на конкретний об'єкт (підприємство), а саме впровадження системи контролю та управління доступом на хлібозавод (рисунок 3.1).

Варто зазначити, що хлібозавод – це підприємство харчової (хлібопекарської) промисловості, яке спеціалізується на виробництві хліба та інших хлібобулочних виробів. [31].

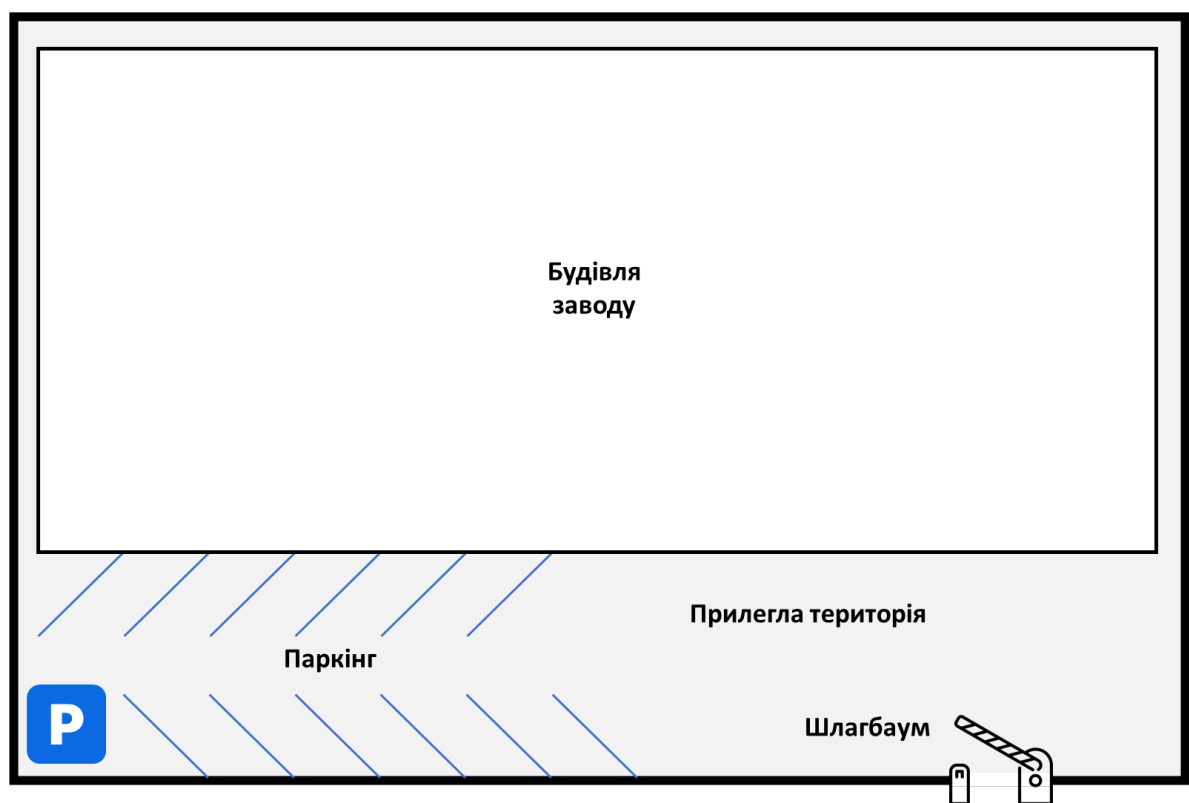


Рисунок 3.1 – Загальний план об'єкту

Територія заводу згідно із загальним планом складається з будівлі та прилеглої території, що містить паркінг для співробітників. Територія огорожена парканом (товста зовнішня лінія на плані вище).

Досліджуваний об'єкт містить низку організаційних підрозділів.

- Виробництво – головний підрозділ, виробництво хліба та інших хлібобулочних виробів.

- Логістика – підрозділ, який займається доставленням готової продукції до точок реалізації (магазини, супермаркети та інші).
 - Адміністрація – підрозділ включає керівництво хлібозаводу та інші адміністративні працівники.
 - Відділ якості – підрозділ, який займається контролем якості виробленої продукції, встановлює стандарти якості для виробничих процесів.
- Основні характеристики досліджуваного об'єкта подано в таблиці 3.1.

Таблиця 3.1 – Технічні характеристики хлібозаводу

Параметр	Значення
Розмір підприємства	1 будівля
Структура підприємства	Виробничий цех, складські приміщення, адміністративна частина (включає кабінети адміністрації, їдальню, медпункт, актову залу, санітарно-побутові приміщення). Відповідно до даної структури, потрібно забезпечити різні рівні доступу до приміщень.
Характер роботи підприємства	Хлібозавод працює безперервно. Наявні денні та нічні зміни, тож потрібно забезпечити доступ працівників у їх зміни та контролювати даний доступ.
Кількість поверхів	4
Площа	Кожен поверх – 7000 м ²
Кількість співробітників	≈400 людей

До потреб підприємства в безпеці належать:

- унеможливлення потрапляння сторонніх осіб на об'єкт;
- контроль доступу до лабораторій та виробничих цехів;

– дотримання всіх санітарних норм, оскільки даний вид підприємства виробляє продукти харчування.

1. Рівні безпеки: Для хлібозаводу важливо мати продуману пожежну та медичну безпеку, також встановити системи відеоспостереження та контролю доступу до приміщень на об'єкті, а також контроль доступу до всього об'єкту.

Особливу увагу під час встановлення системи контролю та управління доступом потрібно приділити саме доступу різних категорій працівників до приміщень хлібозаводу. Для уникнення несанкціонованого доступу, витоку інформації та порушення безпеки роботи підприємства.

Оскільки хлібозавод працює безперервно, тобто наявні денні та нічні зміни, доступ до приміщень повинен відбуватися за розкладом змін.

2. Технічні можливості: облаштоване приміщення для встановлення серверного обладнання, технічний персонал, який буде керувати та підтримувати роботу СКУД, мережеве обладнання, система відеоспостереження та система сповіщення про пожежу та інші аварійні ситуації. Також моніторинг оновлень СКУД для безперебійної роботи системи.

3. Фінансові можливості: для хлібозаводу фінансові можливості трохи обмежені, оскільки велику частину коштів витрачається на закупівлю сировини, зарплати, ремонт обладнання (за потреби). Тому обирається СКУД досить функціональна, але помірно фінансово затратна.

Доступ до приміщень хлібозаводу розділяється у спосіб, висвітлений у таблиці 3.2. Важливо зазначити, що директор хлібозаводу та керівники охорони повинні мати доступ до усіх приміщень незалежно від часу доби. Це спричинено потенціальною необхідністю відкрити певне приміщення на об'єкті з метою убезпечення співробітників заводу. Також це зумовлене необхідністю ефективного виконання обов'язків, доступу до інформації про стан робочих процесів та контролю за дотриманням правил і політик організації.

Таблиця 3.2 – Організація доступу для різних категорій співробітників

Категорія працівників	Доступ до приміщень
Працівники адміністративного управління	Всі приміщення, окрім кабінетів керівників (директора, головного інженера)
Працівники виробничого сектору	Виробничі та санітарно-побутові приміщення у часи їхніх змін
Охорона	Усі приміщення у часи їхніх змін
Керівники охорони	Усі приміщення
Директор хлібозаводу	Усі приміщення

Такий розподіл доступу, забезпечить ефективну роботу та безпеку працівників, дозволить моніторити часи роботи, унеможливить проникнення до приміщень хлібозаводу не у свою робочу зміну.

3.1 Обґрунтування вибору СКУД

Перш ніж обрати конкретний тип СКУД для встановлення на хлібозаводі, варто визначити основні характеристики та потреби запровадження системи контролю та управління доступом саме для даного типу підприємства.

Визначивши основні характеристики підприємства, потрібно, також, визначити його потреби для запровадження системи контролю та управління доступом для хлібозаводу

1. Забезпечення безпеки: ідентифікація працівників та їх робочих змін, обмеження прав доступу до технічних приміщень, до лабораторій, складів, виробничих цехів, адміністративних приміщень.

2. Контроль доступу: перевірка системою прав доступу співробітників до різних приміщень, попередження про несанкціонований доступ.

3. Облік робочого часу: важлива потреба для хлібозаводу, оскільки працівники працюють у декілька змін, тому важливо контролювати години роботи, щоб не було перевантаження. Також це дозволить контролювати запізнення або пропуск робочого часу.

4. Відстеження руху та активності співробітників: дозволяє контролювати внутрішні переміщення, відстежувати порушення безпеки та санітарних норм, затримки або відхилення від графіка роботи.

5. Економія часу та грошей: встановлення системи контролю та управління доступом на хлібозаводі дозволить працівникам швидше проходити прохідну, зменшує витрати на охорону, зменшує похибку людського фактора при перевірці співробітників та відвідувачів.

6. Покращення ефективності роботи: система контролю та управління доступу пришвидшує проходження контрольних точок (наприклад: прохідна, доступ до технічних приміщень та лабораторій), відстежування часу роботи, що в свою чергу покращує працездатність співробітників.

7. Керування ризиками: встановлення різних рівнів доступу, що перешкоджає несанкціонованому доступу до приміщень та об'єкту в цілому.

8. Зниження витрат на охорону: хлібозавод досить велике підприємство з великою кількістю приміщень, тому встановлення СКУД, а також її інтеграція з системою відеоспостереження буде більш ефективною та потребуватиме менше витрат на охорону, ніж наймати велику кількість охоронців, які муситимуть постійно роботи обхід підприємства.

9. Автоматизація процесів: автоматизація контролю доступу до приміщень та об'єкту в цілому, контроль переміщення та активності співробітників. Що в свою чергу пришвидшує та покращує роботу підприємства.

10. Дотримання вимог законодавства: вимоги та норма встановлення системи контролю та управління доступом, вимоги до встановлення систем

відеоспостереження, санітарні норми та вимоги, а також дотримання вимог пожежної та медичної безпеки.

Існує багато різноманітних систем контролю та управління доступом, проте на ринку СКУД видалено декілька основних видів: СКУД на основі доступу карток, СКУД на основі кодів доступу, СКУД на основі біометрії, мобільні та інтернет СКУД, а також гібридні СКУД (детальніше про них було описано у другому розділі). Проаналізувавши представлені типи СКУД, їх переваги та недоліки, а також пристрої та комунікацію між ними, одним із найкращих варіантів СКУД для досліджуваного хлібозаводу є гібридна система контролю та управління доступом. Гібридна система дозволяє поєднувати декілька типів СКУД, а також інтегрувати їх в інші системи. Отже, можна використовувати різні види ідентифікації працівників. Встановлення такої системи на хлібозаводі забезпечить ефективний контроль доступу працівників до різних зон підприємства.

Контроль доступу буде здійснюватися за допомогою карток доступу (рисунок 3.2).

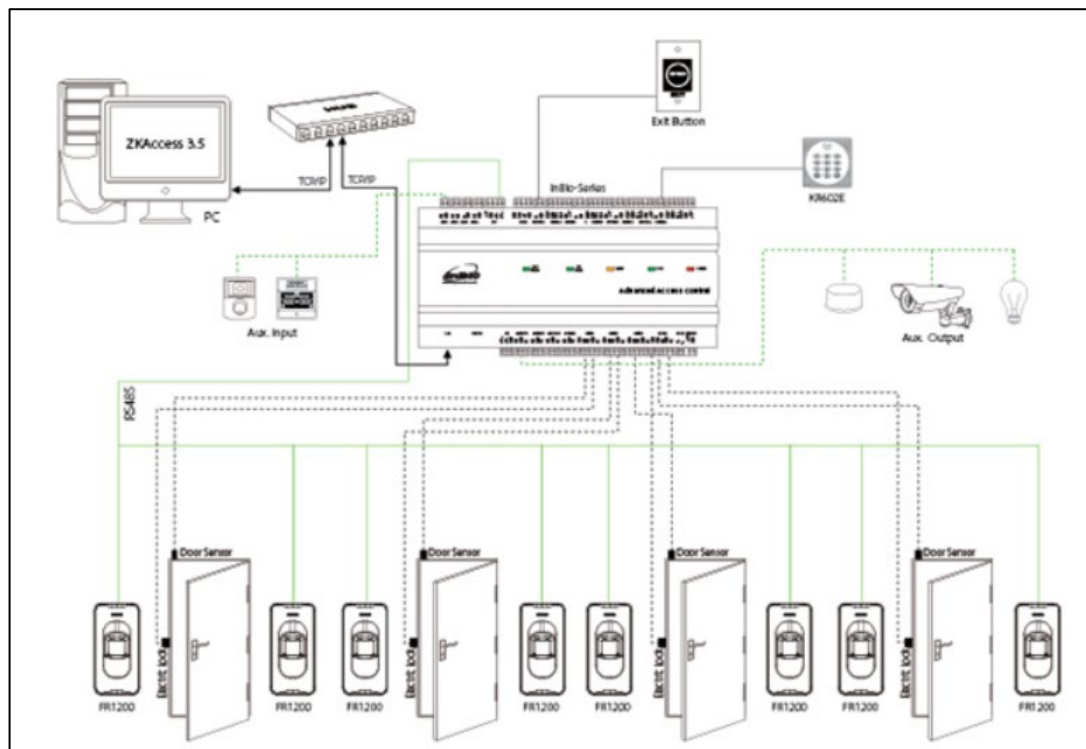


Рисунок 3.2 – Схема підключення компонентів СКУД на об'єкті

На входах до приміщень будуть встановлені карт-рідери, які дозволять працівникам здійснювати прохід лише за наявності відповідного права доступу. Також СКУД підключається до системи відеоспостереження, що дозволяє контролювати переміщення та активність працівників та реагувати на можливі порушення правил безпеки.

Інтеграція гібридної системи контролю та управління доступом до пожежної та аварійної системи дозволить підвищити рівень безпеки на підприємстві та ефективніше реагувати на надзвичайні ситуації. Наприклад, у разі виявлення пожежі або аварії, автоматизована система може відключити електрику в певних зонах, щоб запобігти поширенню вогню або інших небезпек.

Гнучкість системи робить її більш пристосованою до потреб підприємства. Можна налаштовувати рівні доступу для різних зон, масштабувати, змінювати та доповнювати необхідними функціями.

В цілому, гібридна система контролю та управління доступом забезпечує ефективний контроль доступу працівників, швидку реакцію на можливі надзвичайні ситуації, інтеграцію з потрібними системами та можливість масштабування.

3.2 Інженерно-технічна складова впровадження СКУД

Гібридна система контролю та управління доступом поєднує в собі різні методи контролю. При встановленні на хлібозавод такої системи контролю доступу варто використовувати наступні пристрої (див. рисунки 3.3–3.5):

1. Контролери доступу – дані пристрої встановлюються на кожній точці контролю доступу, забезпечують збір та обробку даних про пропуски працівників. Підключення до центральної системи управління СКУД дозволяє збирати та аналізувати дані про переміщення та доступ до різних зон на заводі.

2. Зчитувачі карток доступу – встановлюються на точках контролю доступу (на дверях, на пропускній), що дозволяє ідентифікувати працівників, їх рівень доступу до приміщень, контроль руху по території.

3. Електромагнітні замки – пристрої встановлюються на двері та забезпечують їх блокування та розблокування при проходженні працівників з відповідним рівнем допуску. Електромагнітні замки є надійним та ефективним способом контролю доступу. В поєднанні із дверними доводчиками (автоматично закриває двері після проходження людини) створюють ефективну систему, що не дозволяє стороннім проникнути у приміщення.

4. Механічна кнопка виходу з приміщення – розташовується в середині приміщення, для якого встановлено контроль доступу. При натисненні на кнопку розблоковуються двері, що дає змогу вийти з приміщення.

5. Камери відеоспостереження – камери встановлюються у різних точках заводу та дозволяють контролювати рух та активність працівників на території, виявляти незвичайні або підозрілі дії. Наприклад в цеху для контролю процесу виробництва та спостереження за дотриманням правил техніки безпеки; на прохідній для додаткового контролю за входом працівників на об'єкт; на складі для контролю за умовами зберігання готової продукції та сировини, попередження крадіжок. Камери відеоспостереження допомагають вирішувати спірні ситуації та дозволяють збирати докази у разі виявлення правопорушення.

6. Контрольно-пропускні пристрої – встановлення таких пристроїв дозволяє обмежити несанкціонований доступ до об'єкта. Встановлення турнікетів на прохідній контролює доступ до приміщень всередині об'єкту. Встановлення шлагбаумів дозволяє контролювати потік машин, які в'їжджають та виїжджають з території хлібозаводу. Крім цього, на КПП передбачено присутність двох представників відділу охорони.

7. Пристрої системи аварійного сповіщення – система використовується для негайного повідомлення оператора про можливу загрозу на підприємстві.

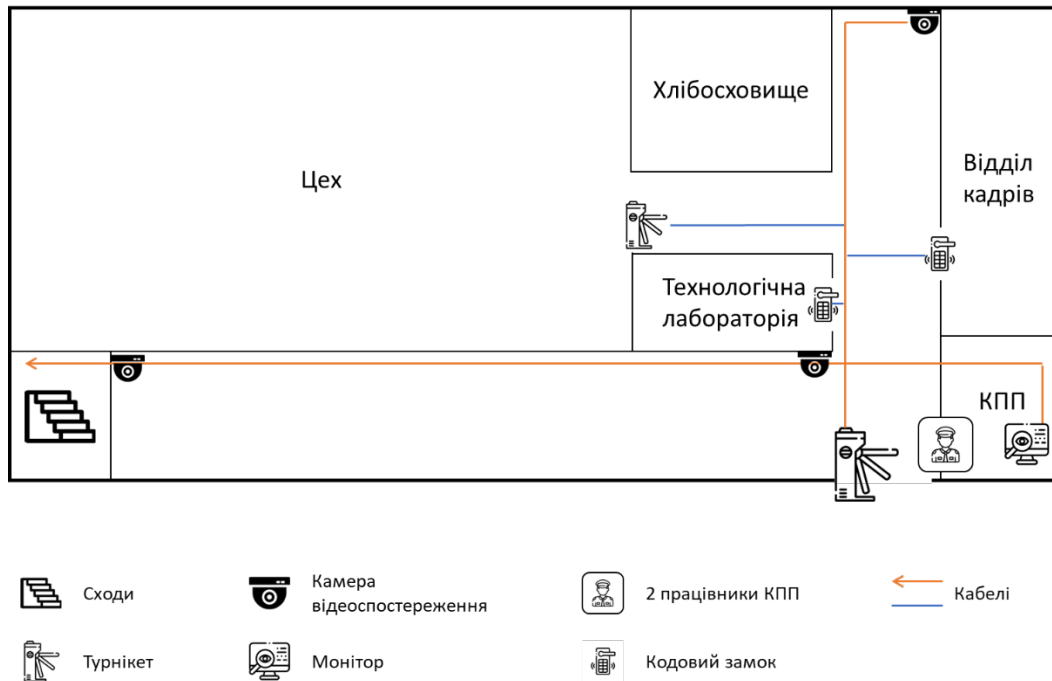


Рисунок 3.3 – План підключення компонентів СКУД (1 поверх)

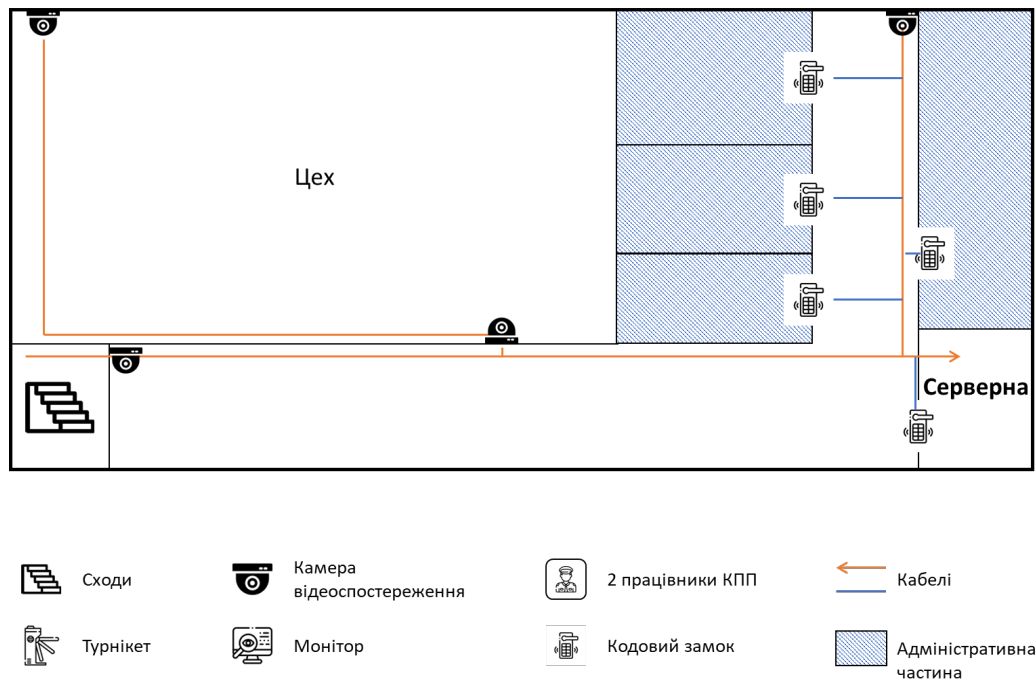


Рисунок 3.4 – План підключення компонентів СКУД (2 поверх)

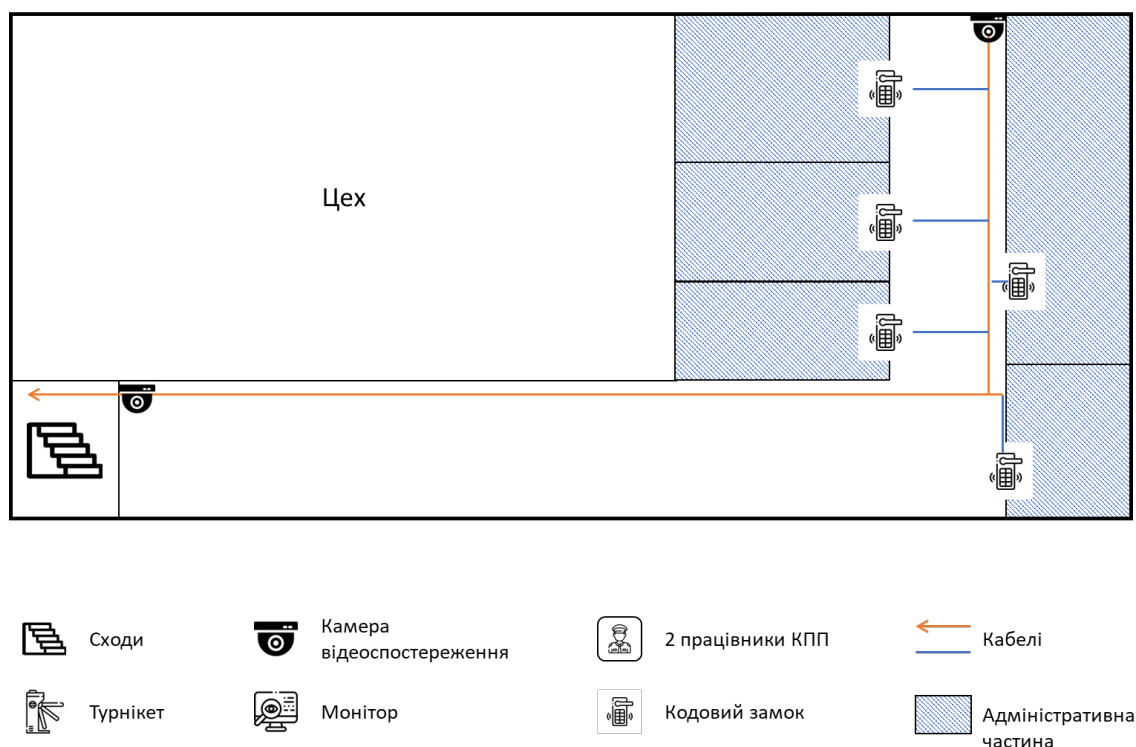


Рисунок 3.5 – План підключення компонентів СКУД (3–4 поверхи)

Потрібно встановити сирени та звукові сигналізатори для повідомлення про небезпеку або надання інструкцій персоналу на території заводу. Кнопки аварійного виклику для негайного сповіщення оператора про можливу небезпеку або аварійну ситуацію. Такі кнопки обов'язково встановлюються у виробничому цеху, оскільки там багато обладнання, яке у разі пошкодження або неправильного поводження може серйозно травмувати працівників. Також встановити інтерфейс для аварійного сповіщення для зв'язку з іншими системами та території хлібозаводу, наприклад пожежна система, система відеоспостереження, система контролю доступу. Такий зв'язок між системами дозволить швидко знаходити та усувати небезпеку, а також безперешкодно покидати потенційно небезпечне приміщення.

Також встановлюються сервери та програмне забезпечення для обробки, збору та аналізу інформації яка надходить від контролерів.

Особливу увагу потрібно приділити також комунікації між пристроями системи контролю та управління доступом.

Виробники та спеціалісти по встановленні систем контролю доступу пропонують наступну схему комунікацій між пристроями. А саме комунікація між контролерами та пунктом керування здійснюється за допомогою перемикача (Switch), зв'язок здійснюється через Інтернет за допомогою протоколів TCP/IP.

Комунікація між контролером карт-рідером, електромагнітними замками, дверними сенсорами та механічною кнопкою виходу з приміщення здійснюється за допомогою кабелю «вита пара» та протоколів зчитування Wiegand та OSDP. У випадку контролю доступу до приміщення за допомогою карток, використовується протокол Wiegand.

У разі потреби контролери можуть з'єднуватися з іншими системами на об'єкті, наприклад відеоспостереження, пожежна та аварійні системи за допомогою допоміжних входів та виходів.

Шлагбауми та турнікети також з'єднуються з контролерами через кабелі «вита пара» або протоколи TCP/IP. Контролер передає інформація про проходження карти до СКУД, якщо карта валідна і користувачеві дозволено вхід на територію, то турнікет або шлагбаум відкривається і працівник або транспортний засіб проходить на територію підприємства. У випадку, якщо карта не валідна, або інформація про користувача не відповідає дійсності, вхід блокується та подається сигнал тривоги про несанкціонований доступ.

Також при монтажу та налаштуванні системи потрібно враховувати можливість відключення світла та режими роботи підприємства.

У цьому випадку, хлібозавод працює безперервно, тобто має денні та нічні зміни. Тому потрібно налаштувати систему контролю та автоматичний перехід з денного режиму роботи на нічний, щоб уникнути несанкціонованого доступу на виробництво. Кількість працівників у денні та нічні зміни майже однакова, але для нічної зміни варто налаштувати більш обмежений режим доступу. Наприклад працівник денної зміни може мати доступ до бухгалтерії, актовій зали, менеджерів, працівник нічної зміни вже не матиме доступу до цих приміщень, оскільки співробітники цих відділів відсутні на робочих місця

вночі. Саме тому зазвичай денна змінні має більше груп доступу та меншу обмеженість по часу доступу. Для безпеки працівників нічної зміни варто встановити додаткові камери відеоспостереження, щоб забезпечити кращий огляд території та збільшити час проходження контрольних точок, щоб працівники мали додатковий час на вхід або вихід з приміщення.

Відключення світла є основною проблемою для підприємств, оскільки всі компоненти потребують живлення. У разі вимкнення світла встановлюється резервне живлення – батареї або генератори, для забезпечення роботи на певний проміжок часу. Якщо живлення не відновиться за деякий проміжок часу, система переходить в режим обмеженого доступу, який обмежить доступ до деяких приміщень або вимкне деякі пристрої контролю доступу.

Важливо встановити додаткове освітлення та резервний вихід для евакуації персоналу у разі надзвичайної ситуації. Розробити план дій для працівників, щоб не було паніки.

3.3 Особливості програмного забезпечення СКУД

Програмне забезпечення системи контролю та управління доступом складається з різних модулів, які в свою чергу відповідають за різні системи моніторингу, наприклад моніторинг камер відеоспостереження, контроль доступу з використанням засобів ідентифікації (картки, коди, біометрія), облік робочого часу працівників та багато інших. Базове програмне забезпечення СКУД може здійснювати обмін інформацією між інтегрованими системами та забезпечує загальне управління СКУД.

Відповідно до специфіки роботи, характеристики підприємства та побажань замовника систему можна доповнювати різними модулями. Наприклад, при розширенні території підприємства або перепланування, систему можна доповнювати, а також інтегрувати елементи.

Основним та найбільш потрібним завданням програмного забезпечення СКУД є можливість моніторингу робочого часу працівників. Це дає змогу контролювати робочий час, прорахувати ефективність роботи працівників, планувати робочі процеси та прогнозувати терміни виконання тих чи інших завдань. Також моніторинг робочого часу дозволяє ефективно попереджувати проблеми інформаційної безпеки.

Основні особливості програмного забезпечення СКУД [32]:

1. Автоматизоване управління доступом: програмне забезпечення СКУД дозволяє керувати доступом осіб до відповідних зон та приміщень за допомогою електронних ключів, карток або інших ідентифікаторів.
2. Можливість інтеграції з іншими системами безпеки: СКУД може бути інтегрована з іншими системами безпеки, такими як системи відеоспостереження, системи пожежної сигналізації та інші, для забезпечення вищого рівня безпеки.
3. Моніторинг і аналітика: програмне забезпечення СКУД може збирати та аналізувати дані про доступ осіб до зон та приміщень, що дозволяє керувати та оптимізувати систему контролю доступу.
4. Функції автоматичного повідомлення: СКУД може автоматично повідомляти про порушення правил доступу, наприклад, про спроби несанкціонованого доступу або про невідповідність доступу працівнику.
5. Можливість дистанційного керування: програмне забезпечення СКУД може бути кероване з віддаленого місця, що дозволяє забезпечувати контроль доступу навіть віддалено.
6. Висока захищеність: програмне забезпечення СКУД повинно бути захищене від несанкціонованого доступу, що дозволяє забезпечити безпеку об'єкта та інформації про доступ до нього.

Декілька прикладів програмного забезпечення СКУД [32]:

Honeywell Pro-Watch: це програмне забезпечення СКУД, яке забезпечує безпеку та контроль доступу для середніх та великих об'єктів. Воно підтримує різні види ідентифікації, включаючи картки, брелоки та біометричні дані.

Lenel OnGuard: це програмне забезпечення СКУД, яке може бути використане для контролю доступу до будь-якого типу об'єкта, включаючи офіси, склади та інші. Воно підтримує багато видів ідентифікації, включаючи карти, пін-коди та біометричні дані.

Software House C•CURE 9000: це програмне забезпечення СКУД, яке забезпечує безпеку та контроль доступу для середніх та великих об'єктів. Воно підтримує різні види ідентифікації, включаючи картки, біометричні дані та мобільні пристрої.

Avigilon Access Control Manager: це програмне забезпечення СКУД, яке забезпечує безпеку та контроль доступу для об'єктів будь-якого розміру. Воно підтримує різні види ідентифікації, включаючи картки, біометричні дані та QR-коди.

Raxton Net2: це програмне забезпечення СКУД, яке забезпечує безпеку та контроль доступу для малих та середніх об'єктів. Воно підтримує різні види ідентифікації, включаючи картки, брелоки та біометричні дані.

Програмне забезпечення СКУД використовується на хлібозаводі для контролю доступу до приміщень та об'єктів, зберігання даних про працівників, планування графіків роботи, контролю робочого часу, контролю якості продукції та багатьох інших завдань.

Нижче подано приклади використання програмного забезпечення та його функції для відділів на хлібозаводі (таблиця 3.3).

Таблиця 3.3 – Функції програмного забезпечення на об'єкті

Назва відділу	Функції ПЗ
Відділ кадрів	Зберігання даних про працівників, контроль доступу до робочого місця та обліку робочого часу.

Продовження таблиці 3.3

Відділ безпеки	Контроль доступу до об'єктів, збереження записів відеоспостереження та аудіозаписів, а також для контролю робочого часу охоронців.
Відділ виробництва	Контроль доступу до виробничих приміщень та обладнання, планування графіків роботи та контролю якості продукції.
Відділ логістики	Контроль доступу до складських приміщень та вантажівок, планування маршрутів транспорту та контролю руху вантажівок.
Відділ фінансів	Контроль доступу до фінансової інформації та забезпечення безпеки даних, контроль доступу до фінансових приміщень та контролю робочого часу фінансових працівників.
Відділ юридичних питань	Контроль доступу до юридичної інформації, забезпечення безпеки даних та контролю робочого часу юристів.
Відділ інформаційних технологій	Забезпечення безпеки мережі та контролю доступу до серверних приміщень, зберігання інформації про користувачів та їх права доступу до різних додатків та інформації.
Відділ маркетингу	Контроль доступу до маркетингової інформації та рекламних матеріалів.

Окрім того, програмне забезпечення СКУД інтегрується з іншими системами на хлібозаводі, такими як система відеоспостереження, система керування виробництвом, система електронного документообігу, пожежна та аварійна системи тощо. Це дозволяє забезпечити повну автоматизацію бізнес-процесів на підприємстві та збільшити ефективність роботи різних відділів, а також ефективне реагування на внутрішні та зовнішні загрози.

Крім того, СКУД використовується для підвищення рівня безпеки на хлібозаводі, забезпечення контролю доступу до об'єктів та місць зберігання продукції, запобігання крадіжок та злочинів, а також для забезпечення точного обліку робочого часу працівників та регулювання доступу до зон з обмеженим доступом.

3.4 Синхронізація роботи відділів після впровадження СКУД

Встановлення та налаштування системи контролю та управління доступом та інтеграція її з іншими системами, такими як відеоспостереження, аварійна та пожежна система це лише частина роботи. Варто також синхронізувати роботу відділів підприємства для якісної та ефективної роботи та унеможливлення помилок.

Для забезпечення синхронізації роботи відділів використовують спеціальні інтеграційні модулі, які дозволяють обмінюватися інформацією та даними між відділами. Також потрібна інтеграція з іншими системами, наприклад система керування виробництвом, система документообігу, система відеоспостереження. Така інтеграція дозволяє забезпечити обмін даними між системами та автоматизувати процеси на підприємстві.

Наприклад відділ кадрів повинен мати усю актуальну інформацію про співробітників (ім'я, прізвище, дата народження, посада), щоб встановити рівень доступу та контролювати рух по підприємству. Отже, відділ кадрів повинен тісно співпрацювати з відділом охорони, який відповідає за контрольні точки та моніторить рух працівників по хлібозаводі. Відділ

охорони має в свою чергу надати інформацію про осіб, яким заборонений доступ до об'єкта в цілому або до конкретних приміщень на хлібозаводі. Таким чином використовується інтеграційний модуль для синхронізації роботи відділів кадрів та охорони, що автоматично синхронізує дані про працівників та контрольні точки.

При зміні прав доступу для співробітників відділом кадрів, інформація автоматично синхронізується із СКУД та іншими системами, що забезпечує однаковість прав доступу для даного співробітника у різних системах хлібозаводу.

Якщо відділ виробництва вирішив змінити розклад роботи працівників, це повинно бути відображено в СКУД, щоб система могла коректно працювати. А саме повідомити відділ кадрів про зміни в графіку роботи, відділ кадрів повинен змінити графіки роботи та повідомити працівників про зміни, відділ охорони повинен забезпечити доступ працівників до приміщень, попередньо перевіривши права доступу, також відділ охорони повинен проконтролювати чи всі працівники з'явилися на робочих місцях відповідно до нового розкладу. Важливо переконатися, що новий графік роботи відповідає вимогам безпеки та всі працівники мають доступ до необхідної інформації.

Для налаштування синхронізації роботи між відділами використовують різні методи, наприклад:

1. Чітке визначення обов'язків та прав доступу: кожен відділ повинен мати відповідального за налаштування та підтримку СКУД. Також потрібно чітко визначити, які функції та дані доступні кожному відділу, щоб уникнути помилкових втручань.

2. Регулярні оновлення даних: відділи повинні регулярно оновлювати дані в СКУД, щоб уникнути недоречностей у відстеженні доступу до приміщень та контролю робочого часу працівників.

3. Ретельне тестування: перед впровадженням будь-яких змін в системі СКУД необхідно провести ретельне тестування, щоб уникнути помилок та збоїв в роботі системи.

4. Організація тренінгів: для забезпечення ефективної роботи з СКУД, необхідно організувати тренінги для працівників кожного відділу. Професійна підготовка допоможе відділам користуватися СКУД більш ефективно та уникнути помилок.

5. Система зворотного зв'язку: для того, щоб уникнути помилок та збоїв в роботі СКУД, необхідно створити систему зворотного зв'язку, яка дозволить працівникам повідомляти про будь-які проблеми з роботою системи. Це допоможе оперативно вирішувати проблеми та покращувати роботу системи.

Одним з ключових аспектів синхронізації роботи між відділами після встановлення СКУД є створення єдиного центру управління доступом. Це може забезпечити інтеграцію різних систем та платформ, що використовуються різними відділами, у єдину систему, яка може керувати доступом до приміщень, обліком робочого часу та іншими аспектами безпеки на території хлібозаводу. Усі відділи повинні працювати разом, щоб забезпечити коректну роботу СКУД, вводити актуальну інформацію в систему, вчасно вносити зміни до розкладів роботи та інші зміни, які можуть впливати на роботу системи. Таким чином, синхронізація роботи між відділами є важливим елементом у забезпеченні безпеки працівників та ефективності виробництва на хлібозаводі з використанням СКУД.

Отже, синхронізація роботи між відділами на хлібозаводі після встановлення СКУД грає важливу роль у забезпеченні безпеки працівників та ефективності виробництва. Кожен відділ повинен відповідати за свої дії та забезпечувати правильну інформацію в СКУД, щоб система могла коректно працювати та забезпечувати доступ до різних зон і приміщень в залежності від рівня доступу кожного працівника. Також це дозволяє підвищити ефективність виробництва та забезпечити безпеку працівників в умовах роботи на виробництві.

ВИСНОВКИ

У даній роботі були проаналізовані системи контролю доступу, їх основні функції, стандарти та характеристики. Також було розглянуто історія розвитку СКУД, класифікацію та ідентифікатори. Було проведено порівняльну характеристику типів СКУД, а саме: СКУД на основі карток, кодів доступу, біометрії, мобільні системи, інтернет системи та гібридні системи. В результаті порівняння визначено переваги та недоліки кожної в вищевказаних систем.

Проаналізовано ринок систем контролю та управління доступом. Створена порівняльна характеристика провідних компаній з розробки, виготовлення та встановлення систем. Було наведено переваги та недоліки кожної компанії.

В роботі детально представлено характеристики та потреби підприємств для запровадження СКУД. До основних характеристик відносяться: розмір, структура, характер роботи, потреби в безпеці, рівень безпеки, технічні та фінансові можливості. До основних потреб впровадження СКУД на підприємстві, можна віднести: забезпечення безпеки, контроль доступу, облік робочого часу, відстеження руху та активності співробітників та відвідувачів, економія часу та грошей, покращення ефективності роботи, керування ризиками, зниження витрат на охорону, автоматизація процесів, дотримання вимог законодавства.

Проаналізовано методику впровадження системи контролю та управління доступом на хлібозавод. Визначено тип СКУД, який ефективно та якісно буде здійснювати контроль на об'єкті – гібридний тип СКУД. Визначено та описано основні потреби та характеристики впровадження СКУД на хлібозаводі. Описано інженерно-технічну складову, особливості встановлення програмного забезпечення, а також синхронізацію роботи відділів після встановлення системи контролю.

ПЕРЕЛІК ПОСИЛАНЬ

1. Система контролю і управління доступом. URL: https://uk.wikipedia.org/wiki/Система_контролю_і_управління_доступом
2. Ворона, В. А. "Системы контроля и управления доступом." М. : Горячая линия-Телеком, 2010. - 272 с.
3. Юдін, О. К., Весельська О. М. "Аналіз та класифікація систем контролю та управління доступом на підприємстві." Science-based technologies 38.2 (2018): 220-225.
4. "The History of Access Control." Brivo.com, 2012. - 4 p.
5. "The First Access Control Systems." Axis Communications, 2019.-11p.
6. Hernandez Ramos, Jose Luis. "Access Control Systems: Security, Identity Management and Trust Models." Boca Raton: CRC Press, 2014. - 263 p.
7. Weissman, Michael A., та William J. Caelli. "Access Control, Security, and Trust: A Logical Approach." Morgan Kaufmann Publishers Inc., 2010. - 176 p.
8. Anderson, Ross J. "Security Engineering: A Guide to Building Dependable Distributed Systems." John Wiley & Sons Ltd, 2010. - 1080 p.
9. Zhao, Wenbing, та Ke Xu. "Access Control, Authentication, and Public Key Infrastructure." Jones and Bartlett Publishers, 2003. - 526 p.
10. Engebretson, Patrick. "The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy." Syngress, 2013. - 225 p.
11. Mackenzie, R. "Access Control and Personal Identification Systems." Elsevier Advanced Technology, 1996. - 296 p.
12. Stallings, W., та B. W. Lampson. "Access Control, Authentication, and Public Key Infrastructure." Addison-Wesley Professional, 1999. - 464 p.
13. Gibbs, Michael. "Physical Access Control Systems Handbook: Implementation and Management." Elsevier Butterworth-Heinemann, 2004. - 240 p.
14. Batchelor, Ben. "The Evolution of Access Control Technology." SecurityWorldMarket.com, 2012. - 8 p.

15. ДСТУ EN 50133-1:2017. Національний стандарт України "Системи контролю доступу. Вимоги до проєктування, монтажу та експлуатації".
16. ДСТУ 4783:2007. Національний стандарт України "Системи безпеки. Вимоги до використання та експлуатації систем контролю доступу".
17. Наказ МВС України від 21.06.2013 р. № 488 "Про затвердження Методичних рекомендацій щодо застосування систем контролю доступу в охоронній діяльності".
18. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах".
19. "Державні будівельні норми" (ДБН). URL: <http://www.dkrs.gov.ua/pro-nas/ofsjd/dbn>
20. Що таке СКУД і як організувати систему контролю доступу в офісі чи іншому об'єкті? URL: <https://bas-ip.kiev.ua/shcho-take-skud-i-yak-orhanizuvaty-systemu-kontroliu-dostupu-v-ofisi-chy-inshomu-obiecti/>
(01.04.2023)
21. Li L.H., Chen H., Guo Y.Y. Design of an Access Control System Based on Optical Identification Technology. Applied Mechanics and Materials. 2013. Vol. 370-373. P. 1408-1412.
22. Jain A.K., Ross A., Nandakumar K. Introduction to Biometrics. New York: Springer, 2016. - XIV, 518 p.
23. Радіочастотна ідентифікація (RFID). URL: https://uk.wikipedia.org/wiki/Радіочастотна_ідентифікація
24. ISO 14001:2015. Системи управління навколишнім середовищем. Вимоги з інструкціями щодо використання. Женева, Швейцарія: Міжнародна організація стандартизації.
25. EN 50131:2006. Системи охоронної сигналізації - системи протипожежної безпеки. Брюссель, Бельгія: Європейський комітет стандартизації.

26. UL 94. Стандарт безпеки займистості пластикових матеріалів для частин пристроїв і приладів. Нортбрук, Іллінойс: Underwriters Laboratories Inc.
27. ISO 45001. Системи управління охороною праці. Вимоги. Лондон, Великобританія: Британський інститут стандартів.
28. [Електронний ресурс] URL: <https://deps.ua/ua/katalog.html>
29. [Електронний ресурс] URL: <https://ohrannyesystemy.com.ua/ua/p1298347156-turniket-ts1022-pro.html>
30. Перелік кібератак. URL: https://uk.wikipedia.org/wiki/Перелік_кібератак (08.04.2023)
31. Хлібзавод. URL: <https://uk.wikipedia.org/wiki/Хлібзавод> (дата звернення: 10.04.2023)
32. [Електронний ресурс] URL: <https://smartel.ua/ua/programmnoe-obespechenie/>