НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

До захисту допущено
Завідувач кафедри

_____ **Дмитро ЛАНДЕ**
(підпис)

«_____»_____2023 р.

Дипломна робота

на здобуття ступеня бакалавра

за освітньо-професійною програмою

«Системи технічного захисту інформації»
спеціальності 125 «Кібербезпека»

на тему: ОСОБЛИВОСТІ ЗАСТОСУВАННЯ СИСТЕМ КОНОТРОЛЮ ДОСТУПУ ДЛЯ РІЗНИХ ТИПІВ ПІДПРИЄМСТВ

Виконав (-ла): здобувач вищої освіти **IV** курсу, групи ФЕ-91
(шифр групи)

Безсонова Анастасія Олександрівна _____
(прізвище, ім'я, по батькові) (підпис)

Керівник ст. викладач каф. ІБ Василенко Олексій Дмитрович _____
(посада, науковий ступінь, вчене звання, прізвище, ім'я, по батькові) (підпис)

Рецензент к.ф.-м.н., доцент каф. ММАД Іван Миколайович Терещенко _____
(посада, науковий ступінь, вчене звання, прізвище, ім'я, по батькові) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Здобувач вищої освіти _____
(підпис)

Київ – 2023 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

Рівень вищої освіти – перший (бакалаврський)
Спеціальність – 125 «Кібербезпека»
Освітньо-професійна програма «Системи технічного захисту інформації»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Дмитро ЛАНДЕ
(підпис)
«___»_____2023 р.

ЗАВДАННЯ
на дипломну роботу здобувачу вищої освіти

Безсонова Анастасія Олександрівна
(прізвище, ім'я, по батькові)

1. Тема роботи: Особливості застосування систем контролю доступу для різних типів підприємств,
керівник роботи Василенко Олексій Дмитрович, ст. викладач каф.,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «26» травня 2023 р. № 2028-с

2. Термін подання здобувачем вищої освіти роботи «7» червня 2023 р.

3. Вихідні дані до роботи: методи ідентифікації, характеристика і вимоги до системи контролю доступу, критерії вибору її елементів.

4. Зміст роботи: Принципи роботи СКД, їх компоненти та критерії вибору. Класифікація підприємств. Оцінка СКД для різних підприємств.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо): 30 рисунків, 12 таблиць, презентація

6. Дата видачі завдання: 3 жовтня 2022 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка
1	Отримання завдання	03.10.2022	виконано
2	Огляд та опрацювання літературних джерел	04.10.2022-15.11.2022	виконано
3	Формування мети та завдання роботи	16.11.2022-30.12.2022	виконано
4	Написання першого розділу з теоретичним оглядом принципів роботи систем контролю доступу	31.12.2022-12.02.2023	виконано
5	Написання другого розділу з класифікацією підприємств	13.02.2023-10.04.2023	виконано
6	Проходження переддипломної практики	17.04.2023-21.05.2023	виконано
7	Розробка рекомендацій для підприємств щодо вибору систем контролю доступу	11.04.2023-25.05.2023	виконано
8	Написання третього розділу та висновків	26.05.2023-05.06.2023	виконано
9	Передзахист дипломної роботи	07.06.2023	виконано
10	Доопрацювання дипломної роботи	07.06.2023-18.06.2023	виконано

Здобувач вищої освіти _____ Анастасія БЕЗСОНОВА
(підпис) **(Власне ім'я, ПРІЗВИЩЕ)**

Керівник роботи _____ Олексій ВАСИЛЕНКО
(підпис) **(Власне ім'я, ПРІЗВИЩЕ)**

РЕФЕРАТ

Робота обсягом 63 сторінки, містить 30 рисунків, 12 таблиць, 28 літературних посилань.

Метою роботи є надання рекомендацій щодо вибору систем та компонентів СКД в залежності від типу підприємств.

Об’єктом дослідження є особливості застосування системи контролю доступу для різних типів підприємств.

Предметом дослідження є характеристики, можливості та прибуток різних підприємств.

Для досягнення поставленої мети було використано експертний аналіз методом попарного порівняння.

В результаті роботи надані рекомендації для чотирьох типів підприємств з урахуванням їх вимог та бюджету щодо вибору системи контролю доступу.

Ключові слова: СКД, СИСТЕМА КОНТРОЛЮ ДОСТУПУ, ПІДПРИЄМСТВО, ІДЕНТИФІКАЦІЯ, БІОМЕТРІЯ.

ABSTRACT

The work is 63 pages long, contains 30 figures, 12 tables, and 28 literary references.

The purpose of the work is to provide recommendations on the selection of ACS systems and components depending on the type of enterprises.

The object of the study is the peculiarities of the application of the access control system for various types of enterprises.

The subject of the study is the characteristics, capabilities and profits of various enterprises.

To achieve the goal, expert analysis by the method of pairwise comparison was used.

As a result of the work, recommendations were provided for four types of enterprises, taking into account their requirements and budget regarding the choice of an access control system.

Keywords: ACS, ACCESS CONTROL SYSTEM, ENTERPRISE, IDENTIFICATION, BIOMETRY.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

БД – база даних;

КПП – контрольно-пропускний пункт;

КУД – контроль управління доступом;

МЗК – мережа загального користування;

ПЗ – програмне забезпечення;

ПК – персональний комп’ютер;

СКД – система контролю доступу;

СКУД – система контролю та управління доступом;

ACS – англ. Access Control System. система контролю доступу;

PIN – англ. Personal Identification Number, персональний ідентифікаційний номер;

RFID – англ. Radio Frequency IDentification, радіочастотна ідентифікація.

ВСТУП

У сучасному світі підприємства в різних галузях все більше покладаються на системи контролю доступу (СКД), щоб захистити свої цінні активи та забезпечити конфіденційність інформації. Під цими системами зазвичай розуміють комплекс технічних та програмних засобів безпеки, призначені для обмеження, реєстрації та контролю входу-виходу об'єктів (людей, транспорту) на визначеній території через "точки проходу" [1]. Вони запобігають проникненню несанкціонованих осіб у зони обмеженого доступу або доступу до конфіденційних даних. Розуміння загальних можливостей, класифікації, методів ідентифікації та компонентів СКД є основою для розуміння специфіки їх застосування. Актуальність роботи полягає в тому, що на сьогоднішній день існує багато типів підприємств, тому вибір тої чи іншої СКД для кожного з них є досить ускладненим.

Метою роботи є надання рекомендацій щодо вибору систем та компонентів СКД в залежності від типу підприємств.

Об’єктом дослідження є особливості застосування СКД для різних типів підприємств.

Предметом дослідження є характеристики, можливості та прибуток різних підприємств.

Для того, щоб досягнути поставленої мети, необхідно було виконати наступні завдання:

- аналіз існуючих СКД;
- аналіз існуючих типів структур підприємств;
- оцінка вартості компонентів СКД;
- вибір та обґрунтування установки структур СКД для підприємств.

Для виконання цих завдань було використано методи аналітичного огляду експертного аналізу (методи попарного порівняння та зважених коефіцієнтів).

Практичне значення одержаних результатів може скеровувати фахівців у виборі та впровадженні компонентів СКД, адаптованих до потреб та фінансових можливостей різних підприємств.

На базі цієї роботи написана наступна публікація:

Безсонова А. О. Застосування систем контролю доступу для різних типів підприємств / А. О. Безсонова, О. Д. Василенко. // Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених. – 2023. – С. 117–120.

1 СИСТЕМА КОНТРОЛЮ ДОСТУПУ

Згідно ДСТУ EN50133 − 1:2006 «Системи тривожної сигналізації. Системи контролювання доступу охоронного призначення» [2], система контролю доступу (СКД) – це система, що містить усі конструктивні і організаційні засоби, а також ті, що мають відношення до апаратури, яка необхідна для контролювання та керування доступом.

У загально му випадку під СКД зазвичай розуміють комплекс технічних та програмних засобів безпеки, призначений для обмеження, реєстрації та контролю входу-виходу об'єктів (людей, транспорту) на визначеній території через "точки проходу" – такі як двері, ворота та контрольно-пропускні пункти (КПП). Крім цього, СКД також використовується для збирання різноманітної інформації про працівників, їх переміщення по території підприємства, перебування у відділах тощо [1].

СКД спрямовані на дотримання принципу найменших привілеїв, що означає надання користувачам мінімального рівня доступу, необхідного для виконання їхніх службових функцій. Контролюючи доступ до ресурсів на основі попередньо визначених правил і дозволів, організації можуть зменшити ризики та захистити цінні активи від несанкціонованого розголошення, зміни або знищення [3].

СКД можуть бути різних типів, починаючи від окремих рішень, таких як контроль доступу до однієї з дверей або турнікету, і до складних багаторівневих систем для приміщень з багатьма точками проходу.

1.1 Принципи роботи СКД

Принцип роботи СКД полягає у використанні інформації від спеціальних пристроїв-зчитувачів, які ідентифікують особу (транспорт) по ідентифікатору, паролю, набраній кодовій комбінації або біометричних даних. На основі

обробки отриманої інформація особа пропускається або ні на контрольовану територію (приклад на рис. 1.1) [4].

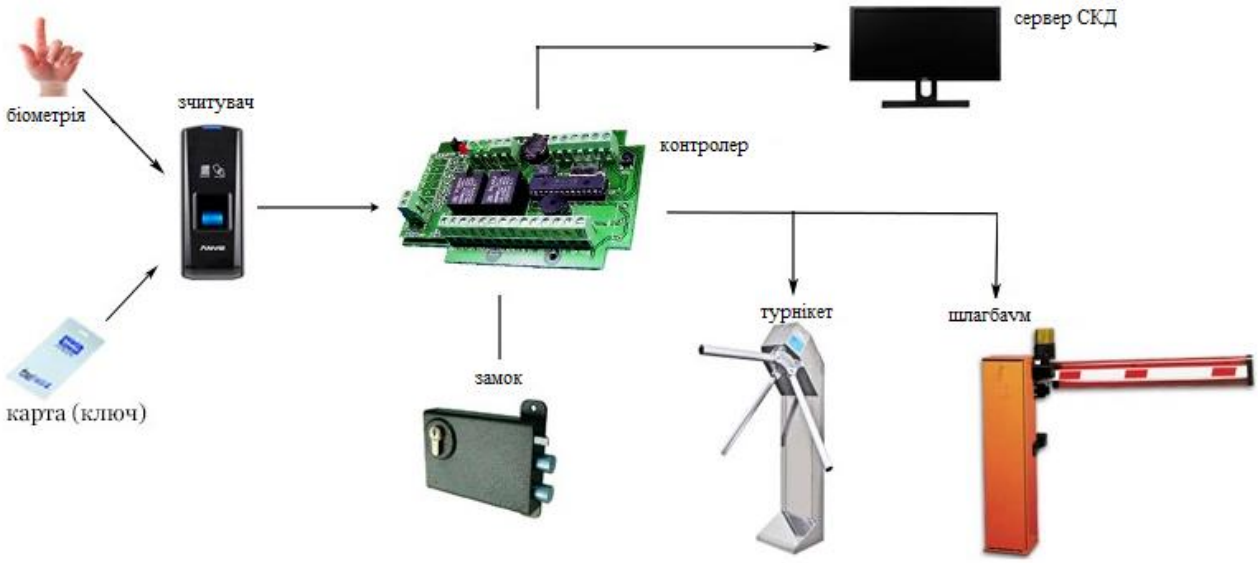

Рисунок 1.1 – Схема роботи СКД [5]

Додатковими функціями СКД є:

- облік часу входу/виходу кожної особи;
- облік транспортних засобів, які в'їжджають на територію, та їх власників;
- облік часу звертання до матеріальних цінностей ;
- облік проносу та виносу металевих виробів.

1.2 Види СКД

СКД бувають:

1) ручні: ідентифікація проводиться по пропуску;
2) механізовані;
3) автоматизовані:

- ідентифікація здійснюється автоматично;

- автентифікація проводиться оператором.

4) автоматичні: все здійснюється без оператора.

У СКД також включена структура управління, яка включає засоби і системи для забезпечення повної ідентифікації та автентифікації (наприклад, набір зчитувачів, контролерів та інших пристроїв). Структура управління поділяється на:

- карточки;
- зчитувачі;
- виконавчі пристрої;
- контролери.

Автономні СКД призначені для обслуговування окремого контрольно-пропускного пункту і не мають прямого зв'язку з центральним пунктом. Вони включають два типи систем:

- системи з розділеним зчитуванням та контролем;
- системи з суміщеним зчитуванням та контролем.

В автономній системі можливе використання декількох контролерів, які з'єднані в мережу. Кожен контролер може бути програмований окремо, що дозволяє налаштовувати їх роботу відповідно до конкретних вимог і потреб системи.

В централізованих СКД число контролерів залежить від ємності системи контрольно-пропускного пункту. На середній потужності ставиться додатковий персонал, який об’єднує контролери. Також можуть встановлюватися зчитувачі різної технології і різне програмне забезпечення (ПЗ).

Розподілені СКД є більш стійкими до аварійних ситуацій, оскільки всі КПП автоматично зв'язані між собою. У таких системах база даних зберігається розподілено, що забезпечує збереження інформації та доступ до неї навіть у випадку виникнення проблем на одному з пунктів.

Однією з переваг розподілених СКД є можливість зв'язку між вхідними та вихідними пристроями різних контролерів. Вхідні та вихідні пристрої різних

пунктів можуть взаємодіяти між собою, що забезпечує гнучкість та ефективність в управлінні доступом.

Крім того, ПЗ розподіленої СКД здатне забезпечувати функціональність по всій території. Система може управляти доступом та ідентифікацією на всіх пунктах контролю, забезпечуючи єдину систему управління та координацію.

1.3 Можливості СКД

Для оцінки СКД використовуються основні технічні характеристики та функціональні можливості.

Технічні характеристики СКД включають:

- рівень ідентифікації: однорівневий (заснований на одній ознаці, наприклад, зчитування коду картки) або багаторівневий (заснований на кількох ознаках, наприклад, зчитування коду картки та біометричних даних);
- кількість контрольованих місць: з малою ємністю (до 16), з середньою ємністю (від 16 до 64) або з великою ємністю (понад 64);
- пропускна здатність: визначає швидкість обробки запитів системи;
- кількість користувачів: вказує на максимальну кількість осіб, які можуть мати доступ до системи;
- умови експлуатації: враховують різні середовища, де СКД може працювати, такі як закриті опалювані приміщення, закриті неопалювані приміщення, зовнішні місця під навісом з помірно холодним кліматом, вулиці з помірно холодним кліматом або особливі умови, які включають підвищену вологість, запиленість, вібрації тощо.

Функціональні можливості СКД включають:

- можливість оперативного перепрограмування системи;
- захист від вандалізму та саботажу, включаючи схемно-технічні та програмні заходи;
- високий рівень секретності, імітостійкості та криптозахисту;

- автоматична ідентифікація за ознаками, характерними для конкретного суб'єкта доступу, наприклад, за допомогою біометрії;
- розмежування повноважень між співробітниками та відвідувачами щодо доступу до приміщень та об'єктів загалом;
- надійне механічне замикання контрольованих місць з можливістю аварійного ручного відкриття;
- автоматичний збір та аналіз даних;
- вибірковий роздрук даних, що дозволяє виводити на друкований носій потрібну інформацію [6].

1.4 Засоби для ідентифікації

Розуміння різних методів ідентифікації є важливим для розробки ефективних СКД в будь-якій організації. Засоби контролю управління доступом (КУД) класифікуються за функціональним призначенням пристроїв, функціональними характеристиками і стійкістю до несанкціонованого доступу. У табл. 1.1 і 1.2 подано класифікацію засобів КУД [7].

Таблиця 1.1 – Класифікація ідентифікаторів доступу

Вид використовуваних ідентифікаційних ознак	**Елемент, який лежить в основі принципу використання**	**Приклади ідентифікаторів**
Оптичні	Мітки, нанесені на поверхню або розташовані всередині ідентифікатора, що мають різні оптичні характеристики у відбитому або минаючому оптичному випромінюванні	Карти з штрих-кодом, топографічні мітки

Кінець таблиці 1.1

Електронні контактні	Електронний код, записаний в електронній мікросхемі ідентифікатора	Електронні ключі
Електронні радіочастотні	Радіоканал, використовуваний для передачі даних	Безконтактні карти доступу
Механічні	Елементи конструкції ідентифікаторів	Механічні ключі з перфораційними отворами

Таблиця 1.2 – Класифікація біометричної ідентифікації

Вид використовуваних ідентифікаційних ознак	**Елемент, який лежить в основі принципу використання**	**Приклади ідентифікаторів**
Акустичні	Кодований акустичний сигнал	Пристрої генерації акустичних сигналів
Біометричні	Індивідуальні фізичні ознаки людини	Відбитки пальців, геометрія долоні, малюнок сітківки ока, голос, підпис
Комбіновані	Кілька ідентифікаційних ознак	Безконтактна карта доступу і відбитки пальців

Карти з штрих-кодом (рис. 1.2) включають в себе нанесений на карту штрих-код або його варіант – баркод (Bar code). Існує складніший варіант, де штрих-код покритий матеріалом, який є прозорим лише в інфрачервоному світлі, а зчитування відбувається в інфрачервоній ділянці.

Розшифрування такого коду здійснюється у двох вимірах - по вертикалі та по горизонталі. Двовимірні коди поділяються на матричні та багаторівневі. Багаторівневі штрих-коди з'явилися в історичному аспекті раніше і включають

кілька звичайних лінійних кодів, розташованих один над одним. Матричні коди забезпечують більш щільну упаковку інформаційних елементів вздовж вертикалі.

Рисунок 1.2 – Карта з штрих-кодом [8]

Електронні ключі (рис. 1.3), зазвичай у вигляді брелоків, найчастіше використовуються в СКД, де є потреба відокремити осіб, які не мають доступу до певного об'єкта. Основним недоліком таких систем є те, що вони мають електричний контакт з мікроконтролером, тобто не мають індивідуальних зчитувачів.

Ключ Touch-memory складається з металевого корпусу і двох електрично ізольованих половин. Всередині перемикача знаходиться порожнина, що містить електронні схеми на кремнієвому кристалі. Перемикач має незалежну пам'ять і складається з сигнального контакту та контакту заземлення. Пам'ять мікросхеми ключа містить унікальний код ключа, який складається з 48-бітового ідентифікаційного номера, 8-бітового номера типу виробу та 8-бітового контрольного коду. Однак перемикачі не є безпечними, оскільки їх можна легко скопіювати.

Рисунок 1.3 – Ключ Touch-memory [9]

Безконтактні картки (рис. 1.4) є найбільш перспективним типом карток на сьогоднішній день. Працюючи дистанційно і не вимагаючи точного позиціонування, вони забезпечують стабільну роботу, простоту використання і високу пропускну здатність. Щоб зчитати інформацію з безконтактної картки, треба просто піднести її до зчитувального пристрою. При цьому слід враховувати, що такі карти призначені не для ідентифікації, а саме для надання доступу.

Зчитувач генерує електромагнітні хвилі на певній частоті, і коли картка потрапляє в зону дії зчитувача, ці хвилі через внутрішню антену подають живлення на чіп картки. Як тільки картка має достатньо енергії для роботи, вона передає ідентифікаційний номер на зчитувач за допомогою електромагнітних імпульсів певної форми та частоти. Картку можна покласти в кишеню, гаманець або піднести до зчитувача.

Рисунок 1.4 – Безконтактна картка [10]

Існують різні методи біометричної ідентифікації. Одним з них є ідентифікація за відбитками пальців (рис. 1.5), яка є найпростішою і використовує легкодоступне обладнання. Ідентифікація за відбитками пальців є надійною, унеможливлюючи несанкціонований доступ, але може давати збої в 3% випадків через пошкодження пальця або неналежне обслуговування сканера. Сканери відбитків пальців вже вбудовані в багато смартфонів, і ця технологія стає все більш дешевою і досконалою. Смартфони також мають систему розпізнавання обличчя за допомогою інфрачервоного сканера або фронтальної камери.

Інший метод – ідентифікація за долонею та формою долоні. У цьому випадку скануються не самі лінії відбитків пальців, а форма руки, наприклад, форма долоні та довжина пальців. Цей метод майже такий же надійний, але вимагає більше системного простору і коштує дорожче.

Рисунок 1.5 – Сканер відбитку пальця в смартфоні [11]

Існує два типи сканування очей, які сьогодні рідко використовуються: сканування райдужної оболонки та сітківки. Перше є простішим, але менш надійним, тоді як друге є найбільш надійним, але й більш дорогим.

Розпізнавання голосу є зручним методом, але менш надійним, оскільки голос може змінитися навіть через фізичну хворобу.

Останній метод - ідентифікація за підписом. У цьому методі людина розписується на графічному планшеті, і комп'ютер порівнює цей підпис з даними, що зберігаються в базі даних. Сам підпис можна підробити, але сучасні зчитувачі є більш надійними, оскільки враховують особливості жестів рук при підписі [6].

1.5 Компоненти СКД

СКД складається з різних компонентів, які разом забезпечують контроль доступу до ресурсів. Найбільш розповсюдженими є:

1) Турнікети на вході – це фізичні бар’єри, призначені для контролю руху осіб, які входять або виходять із зони, що охороняється. Можуть бути інтегровані з механізмами контролю доступу, такими як безконтактні або біометричні зчитувачі, для перевірки та автентифікації осіб перед дозволом на вхід.

За типом системи управління турнікети поділяють на:

– ручні;

– напівавтоматичні;

– автоматичні.

Різна організація безпеки приміщень потребує різного ступеня перекриття отвору. Відповідно до цього критерію виділяють турнікети:

– з частковим перекриттям отвору;

– з повним перекриттям отвору;

– з блокуванням відвідувача у зоні проходу.

За принципом дії механізму перегородок виділяють турнікети:

– із приводним механізмом;

– із оптичним принципом дії;

– існують також турнікети, що поєднують у собі обидва механізми.

Конструктивно розрізняють такі види турнікетів:

– триподи (рис. 1.6);

Рисунок 1.6 – Турнікет трипод

– роторні (рис. 1.7);

Рисунок 1.7 – Турнікет роторний [12]

– speed gates (рис. 1.8);

Рисунок 1.8 – Турнікет speed gates

– хвіртки (рис. 1.9) [13].

Рисунок 1.9 – Турнікет хвіртка

2) Бар’єр для контролю в’їзду/виїзду автомобілів – бар’єр, який запобігає в'їзду несанкціонованих транспортних засобів у заборонені зони. Види шлагбаумів:

– ручні шлагбауми (рис. 1.10);

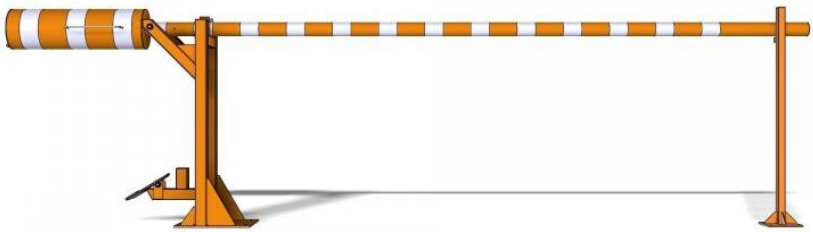

Рисунок 1.10 – Ручний шлагбаум [14]

– автоматичні шлагбауми (рис. 1.11);

Рисунок 1.11 – Автоматичний шлагбаум

– болларди (рис. 1.12);

Рисунок 1.12 – Болларди

– шипові (рис. 1.13) [15].

Рисунок 1.13 – Бар’єр з шипів

3) Електромагнітні та електромеханічні дверні замки (рис. 1.14) – використовуються для захисту окремих приміщень. Ці замки управляються електронним способом. Вони дозволяють авторизованому персоналу отримати доступ за допомогою карток доступу, біометричних зчитувачів або інших методів автентифікації.

Рисунок 1.14 – Замок електромеханічний [16]

4) Автоматичні ворота – забезпечують контрольований доступ для транспортних засобів і зазвичай використовуються на парковках або під'їздах.

– Секційні ворота (рис. 1.15). Головною особливістю цих воріт є механізм, який дозволяє стулці швидко рухатися вгору і вниз (відкриватися і закриватися). Сама стулка має кілька секцій і легко встановлюється під стелею, це полегшує монтаж;

Рисунок 1.15 – Секційні ворота

– Підйомно-поворотні (рис. 1.16). Відмінною особливістю є інтегрована структура, яка забезпечує високу теплоізоляцію. З точки зору "руху" вони схожі на секційні ворота, які рухаються вертикально вгору-вниз, тим самим "економлячи" багато місця. Суттєвим недоліком є те, що при відкритті нижня частина виступає за межі вертикальної поверхні з'їзду. Тому водіям необхідно стежити за розташуванням свого автомобіля, щоб уникнути зіткнення з такими воротами, що відчиняються/зачиняються;

Рисунок 1.16 – Підйомно-поворотні ворота [17]

– Рулонні (рис. 1.17). Особливості: при відкритті ламельна частина "ховається" всередині коробки. Перевага – гнучкість: конструкція не пошкоджується при незначному ударі об кузов автомобіля;

Рисунок 1.17 – Рулонні ворота [18]

– Відкатні консольні (рис. 1.18). Зазвичай їх встановлюють за межами захищеної території або будівлі. При відкриванні та закриванні вбудована стулка рухається паралельно паркану або стіні. Відкатні автоматичні ворота відносно недорогі, легко встановлюються і займають мало місця;

Рисунок 1.18 – Підйомно-поворотні ворота [19]

– Розпашні (рис. 1.19). Вони можуть бути встановлені майже скрізь, досить надійні та важко зламуються [20].

Рисунок 1.19 – Розпашні ворота [21]

5) Шлюзові кабіни (рис. 1.20) – це невеликі безпечні кімнати або огородження, розташовані біля входу або виходу.

Рисунок 1.20 – Шлюзова кабіна [22]

6) Контролери – це центральні процесори, які керують і координують функції системи контролю доступу. Вони отримують дані від різних зчитувачів, обробляють запити на автентифікацію та запускають такі дії, як відмикання дверей або надання доступу.

7) Безконтактні зчитувачі – використовують технологію радіочастотної ідентифікації (RFID) для автентифікації карток доступу або міток. Вони усувають потребу у фізичному контакті, дозволяючи користувачам проводити або тримати свої картки доступу або мітки біля зчитувача для швидкого та зручного доступу.

8) Біометричні зчитувачі – використовують унікальні фізіологічні чи поведінкові характеристики для автентифікації людей. Ці зчитувачі можуть включати сканери відбитків пальців, сканери долоні, сканери райдужної оболонки ока та сітківки ока, системи розпізнавання обличчя або системи розпізнавання голосу.

9) Системи відеоспостереження, та сигналізації – є ключовими компонентами комплексних СКД. Камери відеоспостереження контролюють і записують дії в приміщеннях, допомагаючи в моніторингу безпеки та розслідуванні інцидентів. Системи пожежної сигналізації забезпечують оперативне реагування у разі виникнення пожежі, а системи сигналізації сповіщають персонал служби безпеки у разі спроб несанкціонованого доступу або взлому.

Конкретні компоненти системи контролю доступу можуть відрізнятися в залежності від вимог та інфраструктури компанії.

1.6 Критерії вибору СКД

СКД не тільки надають доступ до будівель або певних частин будівель, але також можуть використовуватися для керування доступом до конфіденційної інформації та ресурсів.

Майже всі компанії можуть отримати вигоду від використання систем контролю доступу. Однак вимоги кожної окремої компанії сильно відрізняються, і контроль доступу вимагає індивідуального підходу, щоб задовольнити вимоги кожної компанії. Тож слід враховувати низку критеріїв,

щоб переконатися, що обрана система ефективно відповідає конкретним потребам організації.

По-перше необхідно забезпечення відповідних функцій. СКД повинна пропонувати відповідні функції для задоволення вимог підприємства.

Також СКД повинна обслуговуватися (перепрограмовуватися) без проблем. Це гарантує зручне виконання змін, наприклад додавання або видалення користувачів, налаштування дозволів доступу або оновлення налаштувань системи.

Важливо, щоб вибрана СКД підходила по бюджету для конкретного підприємства. Це гарантує, що підприємство може своєчасно придбати систему та мати можливість обслуговувати потенційні оновлення та поламки.

Кількість будівель підприємства, де використовуються СКД також має враховуватись. Адже від їх кількості та розташування залежить масштабованість та потужність СКД, а найголовніше – вартість.

Оцінка СКД на основі цих критеріїв вибору допоможе організаціям знайти рішення, які відповідають їхнім вимогам безпеки, операційним потребам і бюджетним міркуванням. Поглиблене дослідження, консультації з галузевими експертами та, можливо, пілотне тестування можуть додатково підтвердити ефективність та придатність обраної СКД.

Висновки до першого розділу

СКД стали невід'ємною частиною сучасного бізнесу. Компанії використовують різноманітні рішення для забезпечення гарантування безпеки своїх співробітників, активів та інформації. Вибір та встановлення правильної СКД є важливим кроком у досягненні бажаного рівня безпеки, ефективності та прибутковості і вимагає дослідження та розуміння характеристик, потреб та вимог кожної компанії.

Класифікації СКД підкреслюють різноманітність доступних рішень, включаючи автономні, мережеві та розподілені системи. Кожна класифікація пропонує унікальні переваги та міркування, засновані на розмірі, структурі та специфічних вимогах бізнесу. Крім того, методи ідентифікації ілюструють різні варіанти, доступні для перевірки та автентифікації людей, які отримують доступ до системи.

Розуміння компонентів СКД, таких як зчитувачі карток, контролери, замки та ПЗ для управління, має вирішальне значення для розробки комплексного та інтегрованого рішення. Критерії вибору визначають фактори, як масштабованість, сумісність, простота використання та вимоги до обслуговування, які бізнес повинен враховувати при виборі системи. Вони гарантують, що обрана система відповідатиме конкретним потребам і цілям компанії та забезпечить надійне й ефективне рішення.

2 КЛАСИФІКАЦІЯ ПІДПРИЄМСТВ

Відповідно до Господарського кодексу України №436-IV від 16.01.2003 [23]:

«Підприємство – самостійний суб'єкт господарювання, створений компетентним органом державної влади або органом місцевого самоврядування, або іншими суб'єктами для задоволення суспільних та особистих потреб шляхом систематичного здійснення виробничої, науково-дослідної, торговельної, іншої господарської діяльності в порядку, передбаченому цим Кодексом та іншими законами.»

Законом України від 05.10.2017 №2164-VII щодо змін до Закону України №996-XIV«Про бухгалтерський облік та фінансову звітність в Україні» [24] додано класифікацію підприємств за розміром (табл. 2.1).

Таблиця 2.1 – Класифікація підприємств за розміром

Категорія підприємства	Критерії оцінки за рік, що передує звітному		
	Балансова вартість активів, євро	Чистий дохід від реалізації продукції (товарів, робіт, послуг), євро	Середня кількість працівників, осіб
Мікропідприємства	До 350 тис.	До 700 тис.	До 10
Малі	До 4 млн	До 8 млн	До 50
Середні	До 20 млн	До 40 млн	До 250
Великі	Понад 20 млн	Понад 40 млн	Понад 250

Мікропідприємство — підприємство з вартістю активів до 350 тисяч євро та середньою кількістю працівників до 10 осіб.

Мале підприємство — підприємство, що не відповідає критеріям до мікропідприємства, з вартістю активів до 4 мільйонів євро та середньою кількістю працівників до 50 осіб.

Середнє підприємство — підприємство, що не відповідає критеріям малого підприємства та відповідає щонайменше двом критеріям:

- вартість активів — до 20 мільйонів євро;
- середня кількість працівників до 250 осіб.

Велике підприємство — підприємство, що не відповідає критеріям середнього підприємства та має середню кількість працівників більше 250 осіб та вартість активів понад 20 мільйонів євро.

Станом на 2018 рік, загальна кількість підприємств в Україні становить 355877 з розподілом на великі, середні та малі зображена на рис. 2.1 [25].

Рисунок 2.1 – Розподіл підприємств за розміром

2.1 Велике підприємство

Виробнича структура великих підприємств є ключовим фактором, що впливає на вибір елементів системи контролю доступу. Хоча на рис. 2.2 показано загальне представлення виробничої структури, важливо розуміти, що фактична структура може відрізнятися в залежності від характеру виробничого процесу.

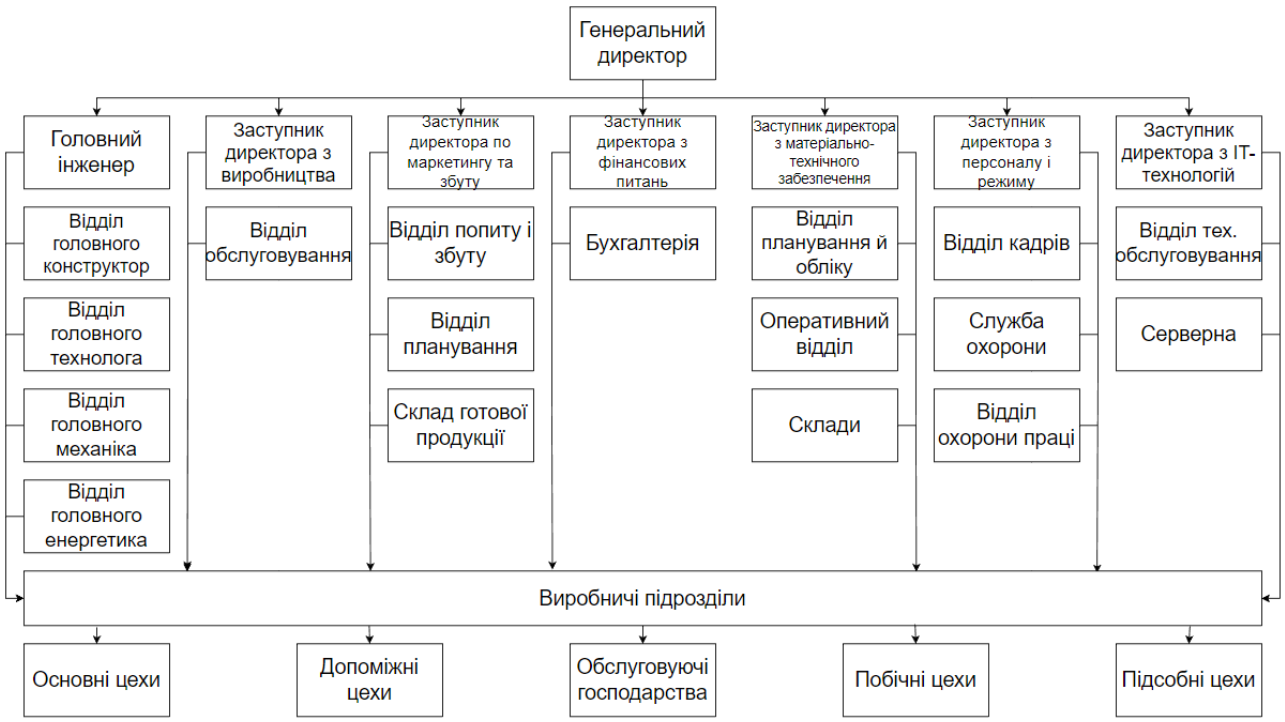

Рисунок 2.2 – Структура великого підприємства [26]

Важливою одиницею виробничої структури компанії є цех, який займається виробництвом конкретних компонентів або продуктів.

Цех - це місце, де відбувається основна виробнича діяльність, і вимагає суворих заходів контролю доступу для захисту критично важливих виробничих процесів, обладнання та інтелектуальної власності.

Компанії, що мають філії та дочірні підприємства, часто стикаються з необхідністю збирати, зберігати та архівувати персональні дані. Як наслідок, для захисту конфіденційності, цілісності та доступності даних необхідно створити спеціалізовані сховища. Такі місця зберігання забезпечують контрольоване середовище для захисту персональних даних від несанкціонованого доступу та порушень. Крім того, географічно розподілені компанії повинні використовувати розподілені бази даних (БД) для управління персональними даними, а сервери БД часто розташовані в різних приміщеннях або навіть будівлях.

Децентралізовані інформаційні системи захисту персональних даних зазвичай мають ієрархічну структуру. Ця ієрархічна модель дозволяє ефективно

управляти та контролювати права доступу на різних рівнях підприємства. Права доступу та дозволи організовані в ієрархічному порядку, забезпечуючи різні рівні прав доступу відповідно до ролей та обов'язків користувачів. Такий ієрархічний підхід полегшує тонкий контроль над конфіденційними даними і знижує ризик несанкціонованого доступу та витоку даних.

Великі підприємства мають різні характеристики з точки зору їхньої фізичної інфраструктури. Великі підприємства можна розділити на різні типи залежно від розміру та складності їхньої діяльності. По-перше, є окремі підприємства, які працюють в одній будівлі, де всі операції централізовані. Такі компанії зазвичай мають централізовану СКД, що охоплює всю будівлю. По-друге, існують складні підприємства з декількома будівлями на одній території. СКД для таких складних підприємств повинні забезпечувати безперебійну інтеграцію та координацію між кількома об'єктами, а також дозволяти безпечне пересування в межах комплексу, зберігаючи при цьому загальний високий рівень безпеки. Існують також мережеві підприємства з декількома будівлями в різних місцях. СКД на мережевих підприємствах вимагають надійного зв'язку та вдосконалених інструментів управління для створення єдиної системи безпеки в усіх будівлях.

2.2 Середнє підприємство

Середні підприємства можна умовно поділити на два типи: окремі підприємства та мережеві підприємства. Окремі підприємства працюють в одній будівлі, а їхня діяльність централізована. У такій структурі вся діяльність підприємства знаходиться в єдиному фізичному просторі, що певною мірою спрощує вимоги до контролю доступу. Однак, навіть в межах однієї будівлі, середні підприємства можуть мати окремі відділи або підрозділи (рис. 2.3).

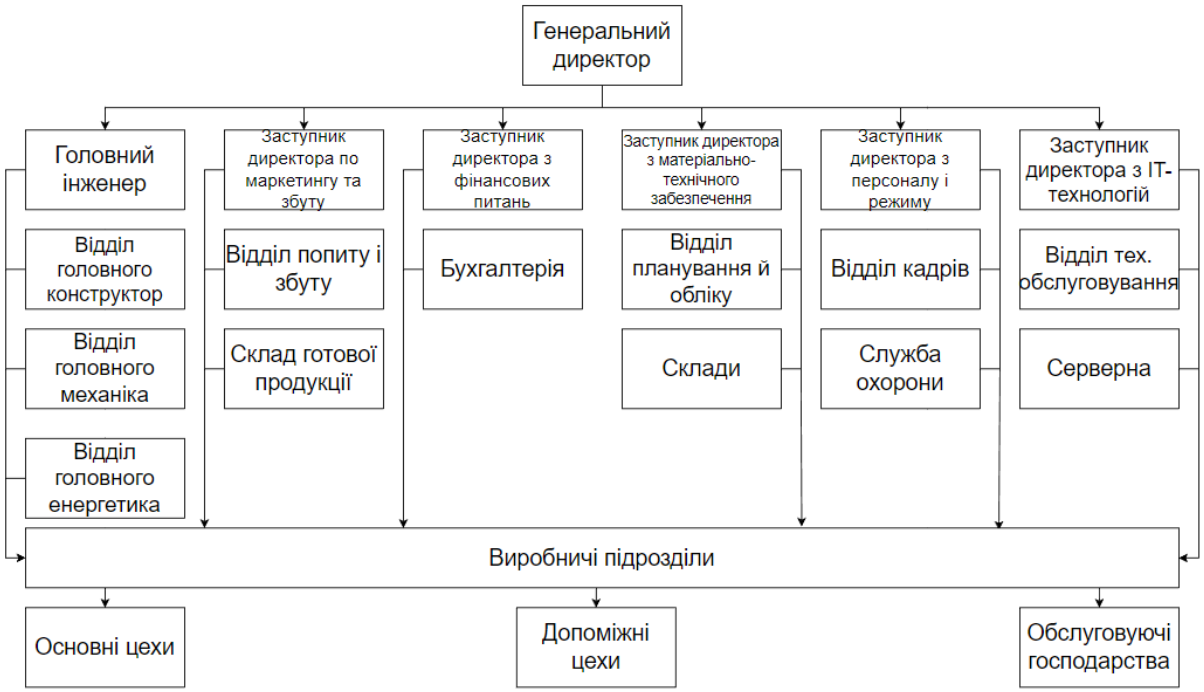

Рисунок 2.3 – Структура середнього підприємства

Мережеві компанії розподілені по декількох будівлях у різних географічних точках. Така розпорошеність створює проблеми для безпеки даних і цілісності контролю доступу. У таких випадках середньому бізнесу необхідно використовувати розподілені інформаційні системи для захисту персональних даних.

Для ефективного захисту даних мережеві середні підприємства мають централізовану інфраструктуру, яка включає в себе виділені серверні кімнати для зберігання та обробки даних. Така серверна кімната слугує центром управління даними компанії і містить необхідне обладнання, пристрої зберігання даних та мережеве обладнання.

На додаток до заходів фізичної безпеки, середній бізнес також повинен враховувати мережеву безпеку при виборі елементів свого дата-центру. Надійні брандмауери, системи виявлення вторгнень і протоколи шифрування є важливими компонентами інтегрованої системи безпеки.

2.3 Мале підприємство

Малі підприємства (рис. 2.4) зазвичай працюють в обмеженому просторі, що складається з однієї або кількох кімнат, які не є територіально розподіленими. На відміну від великого бізнесу, малі підприємства зазвичай не мають спеціальних цехів для спеціалізованої виробничої діяльності. Замість цього вони зосереджуються на наданні конкретних послуг або управлінні простими операціями в обмеженому фізичному середовищі.

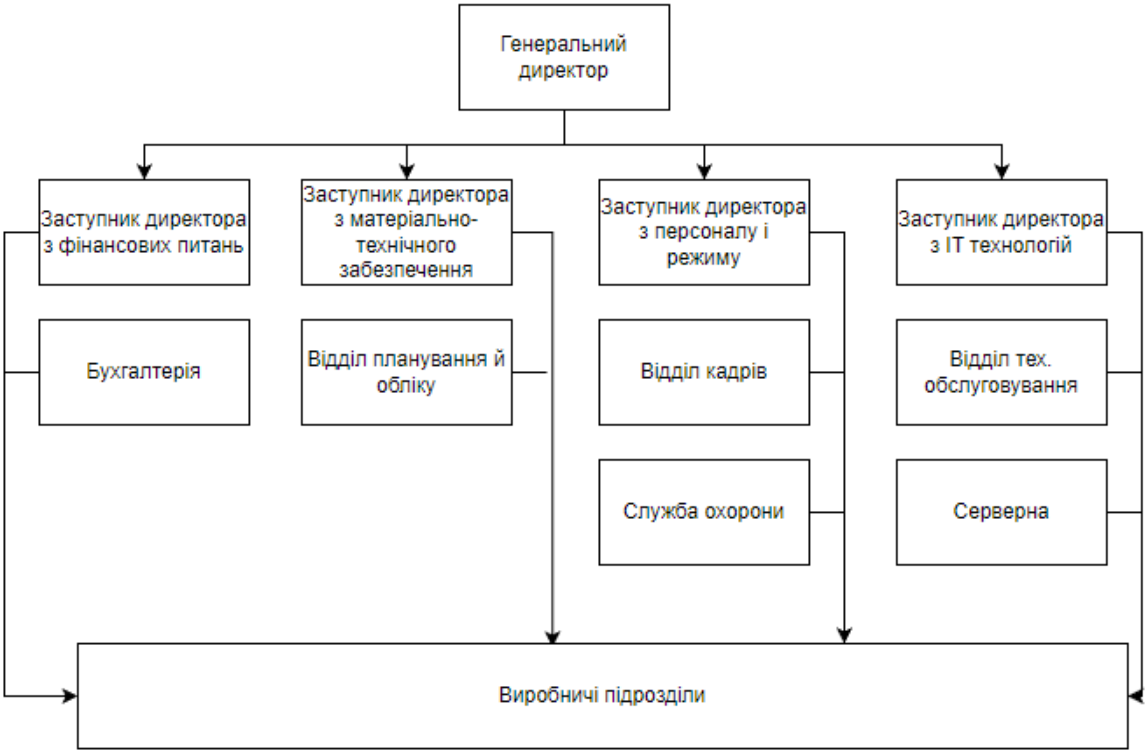

Рисунок 2.4 – Структура малого підприємства

Управління даними в малих підприємствах може відрізнятися від управління даними у великих організаціях. Наприклад, дані про співробітників зазвичай зберігаються у двох копіях, щоб забезпечити резервування і зменшити ризик втрати даних: одна копія зазвичай зберігається на папері, в окремій папці та надійно зберігається в сейфі. Це забезпечує фізичну резервну копію, до якої можна легко отримати доступ у разі потреби; друга копія існує в електронному

вигляді і зберігається на персональному комп’ютері (ПК) відповідальної особи в компанії або на окремому сервері, не підключеному до мережі загального користування (МЗК). Цей метод поєднує в собі зручність і доступність цифрового зберігання з безпекою офлайн-зберігання даних.

Малі підприємства можна розділити на два типи: окремі підприємства та віртуальні підприємства. Окремі підприємства працюють в одній будівлі, використовуючи доступний простір для своєї діяльності. Віртуальні підприємства характеризуються залежністю від онлайн-платформ та цифрової інфраструктури.

2.4 Мікропідприємство

Мікропідприємства (рис. 2.5) працюють у нішевих секторах або мають обмежену сферу діяльності та невелику кількість працівників. Через свій розмір і сферу діяльності такі підприємства часто розміщуються в одній будівлі або можуть займати кілька кімнат в одному приміщенні.

Рисунок 2.5 – Структура мікропідприємства

Мікробізнес часто покладається на локальні рішення для захисту конфіденційної інформації. Це включає в себе встановлення заходів безпеки, таких як антивірусне ПЗ та брандмауери на всіх комп'ютерах і пристроях, що містять персональні дані. Впроваджуючи ці заходи на кожному пристрої

окремо, мікробізнес може знизити ризик витоку даних і несанкціонованого доступу до конфіденційної інформації. Такий підхід гарантує, що всі пристрої в організації мають необхідний захист від шкідливого ПЗ, зовнішніх загроз і потенційних вразливостей.

Використання власних систем захисту даних на мікропідприємствах має ряд переваг. Можливість безпосереднього моніторингу заходів безпеки, впроваджених організацією, забезпечує вищий рівень контролю над безпекою персональних даних. Це дозволяє швидше реагувати та пом'якшувати наслідки в разі інциденту або порушення безпеки.

Мікропідприємства також оцінюють потенційні переваги впровадження хмарних рішень або гібридних підходів, залежно від їхніх унікальних вимог. Хмарні рішення можуть забезпечити додаткову масштабованість, гнучкість і надмірність у зберіганні та захисті даних. Існують також варіанти резервного копіювання та аварійного відновлення за межами підприємства, які можуть підвищити стійкість даних у разі фізичного пошкодження або технічного збою [3].

Висновки до другого розділу

Розглянуто поділу підприємств на різні за розміром: великі, середні, малі та мікропідприємства. Розуміння характеристик і міркувань, пов'язаних з кожним розміром, дає уявлення про потреби, структуру та проблеми, з якими стикаються підприємства залежно від їхнього розміру.

Великі підприємства характеризуються масштабними операціями, великими ресурсами та складною організаційною структурою. Такі компанії часто мають багато підрозділів, філій та офісів і потребують надійних та масштабованих систем.

Середні підприємства знаходяться між великим і малим бізнесом. Зазвичай вони мають середній рівень активності та обмежену кількість співробітників.

Малі підприємства характеризуються відносно обмеженим рівнем діяльності та кількістю працівників. Зазвичай вони працюють в одному або кількох приміщеннях і можуть не мати окремого цеху. Вони можуть бути окремими або віртуальними підприємствами, що працюють переважно в онлайн-середовищі.

Мікропідприємства – це найменші підприємства, які зазвичай складаються з однієї або кількох кімнат в одній будівлі. Ці підприємства можуть мати обмежену діяльність і невелику кількість працівників.

3 ОЦІНКА СКД ДЛЯ РІЗНИХ ПІДПРИЄМСТВ

Вибір СКД дуже залежить від потреб та можливостей підприємства, яке її потребує. Обмеження доступу можна реалізувати багатьма способами, та не всі з них будуть доречними та ефективними у використанні для конкретних підприємств.

3.1 Загальна структура СКД

Для гарантування безпеки працівників, активів та інформації на підприємствах використовують найрізноманітніші варіації СКД. Вибір і впровадження правильної системи є важливим кроком для досягнення бажаного рівня безпеки, ефективності та вигідності і залежить від типу підприємства, їх фінансових можливостей та потреб.

В першому розділі були розглянуті компоненти які можна використати для створення загальної структури СКД (рис. 3.1):

- турнікети на вході;
- шлагбаум для контролю в’їзду/виїзду автомобілів;
- електромагнітні та електромеханічні замки на двері;
- автоматичні ворота;
- шлюзові кабіни;
- контролери;
- зчитувачі безконтактні;
- зчитувачі біометричні (за відбитком пальця, долоні, райдужкою та сітківкою ока, обличчям або голосом);
- системи відеоспостереження, пожежної та тривожної сигналізацій.

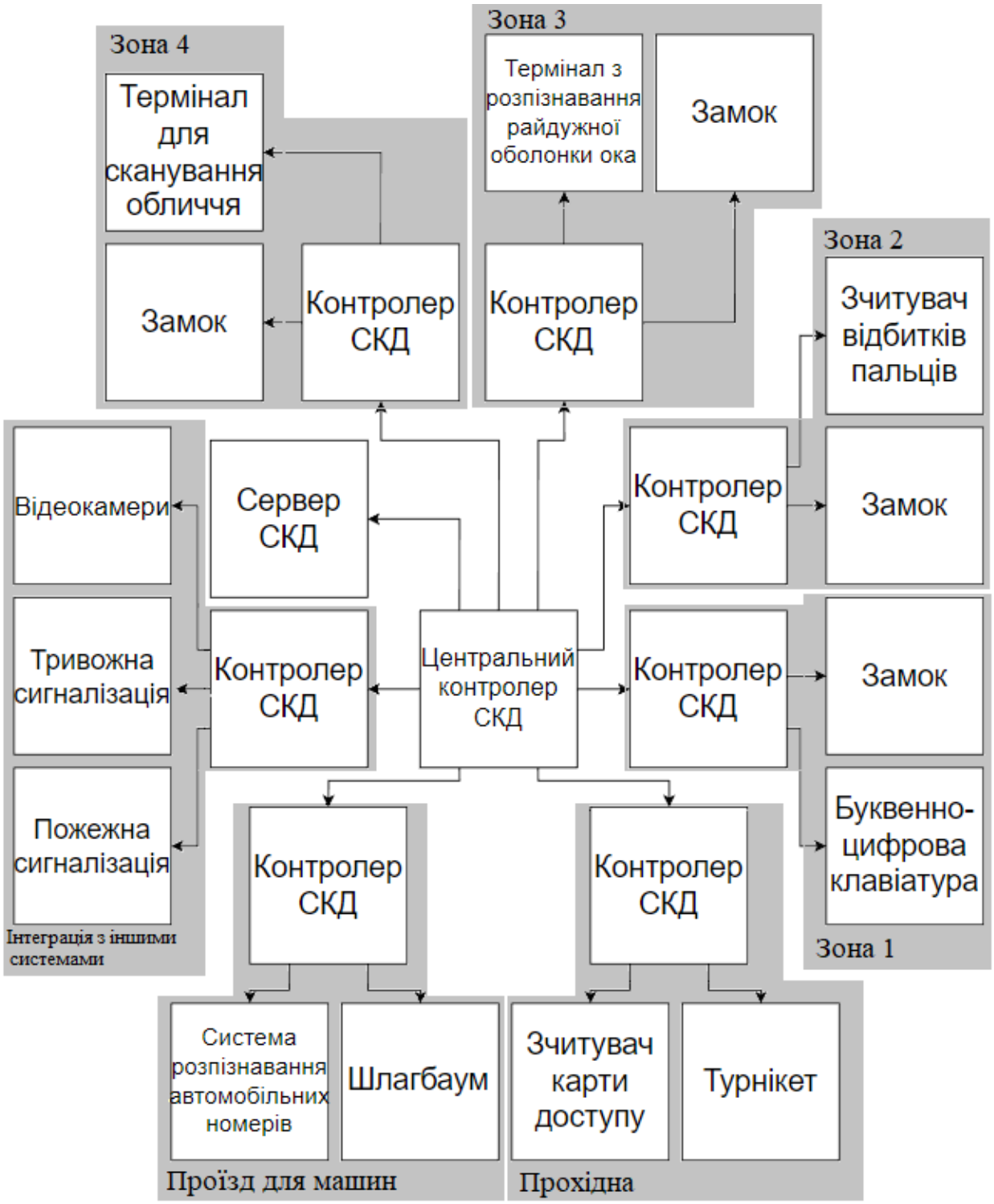

Рисунок 3.1 – Загальна структура СКД

Для того щоб спрогнозувати приблизну ціну СКД, слід вивчити ринок, на якому представлені його компоненти, та проаналізувати його вартість. Кожен з пристроїв, який використовується в системі має функціональні можливості, які задовольняють різні потреби. На їх вартість впливають якість, виробник та

наявність додаткових функцій. Не всі підприємства потребують та мають можливість придбати/утримувати СКД з повним функціоналом, тож слід підібрати оптимальний варіант під свій бюджет.

В табл. 3.1 представлені діапазони цін на компоненти СКД.

Таблиця 3.1 – Діапазон цін на компоненти СКД

Компоненти СКД	***Бюджетні, грн***	***Недорогі, грн***	***Середні, грн***	***Дорогі, грн***
Турнікет трипод	20 000	30 000	40 000	60 000
Турнікет роторний	10 000	20 000	80 000	180 000
Турнікет speed gates	42 500	113 000	245 000	400 000
Турнікет хвіртка	5 000	15 000	30 000	60 000
Шлагбаум ручний	2 500	4 200	8 500	12 000
Шлагбаум автоматичний	13 000	22 000	30 000	89 000
Болларди	950	4 600	19 000	100 000
Автоматичні ворота	5 000	12 000	33 000	50 000
Шлюзова кабіна	480 000	550 000	700 000	1 000 000
Система розпізнавання номерних знаків	15 000	35 000	60 000	197 000
Система обліку робочого часу	5 000	10 000	15 000	24 000
Камера відеонагляду	1 500	2 500	5 000	12 000
Датчик тривожної сигналізації	150	300	600	1200
Електромеханічний замок	600	1 300	1 700	2 700
Контролер	3 000	6 000	9 000	14 000
Зчитувач безконтактних карток	800	1 400	2 500	10 000
Зчитувач відбитків пальців	2 150	3 200	4 700	5 500

Кінець таблиці 3.1

Зчитувач з клавіатурою	600	1 300	2 200	3 300
Термінал розпізнавання райдужки ока	-	-	-	95 000
Термінал розпізнавання обличчя	5 000	12 000	22 000	47 000

3.2 Структура СКД для різних підприємств та їх вартість

Для початку розглянемо структуру СКД великого підприємства (рис. 3.2).

Згідно розділу 2, великі підприємства мають безліч відділів та цехів, можуть розташовуватись як в одній, так і в декількох будівлях. Їхній бюджет складає понад 20 млн, а кількість працівників перевищує 250 осіб. Завдяки цьому можна зрозуміти, що їм потрібна потужна та масштабована СКД, яка повністю покриє потреби підприємства. В бюджеті вони майже не обмежені, тож можна обирати якісні засоби СКД з широким функціоналом. Також бажано звертатись до перевірених фахівців.

Згадуючи структуру самого підприємства, можна зробити висновок, що основними приміщеннями/зонами, які потребують контролю доступу є цехи, серверна кімната, кімната служби охорони, відділ кадрів з архівом, склади, бухгалтерія, кабінет директора та безліч інших відділів. Також слід не забути про парковку та прохідну.

В структурі СКД для великого підприємства можна використати такі пристрої:

- турнікети на вході (роторні або speed gates), також бажано щоб вони були в повний зріст людини. Це дорожче за звичайні, але буде добре запобігати небажаним «гостям». Для пришвидшення пропуску людей та автоматизування

цього процесу, слід інтегрувати зчитувач карток/сканер пальців. Можна додатково обладнати системою обліку робочого часу;

- шлагбаум для контролю в'їзду/виїзду автомобілів – краще за все обрати болларди замість традиційного шлагбаума, адже вони майже «непробивні» та додати систему розпізнавання номерних знаків;
- електромагнітні та електромеханічні замки на двері;
- автоматичні ворота – їх можна використати для гаражного заїзду в складські приміщення;
- шлюзові кабіни – всі кабіни, представлені на ринку досить дорогі, проте вони значно підвищують безпеку та контроль;
- контролери – слід комбінувати використання як розділених, так і суміщених;
- зчитувачі безконтактні;
- зчитувачі біометричні (за відбитком пальця, долоні, райдужкою та сітківкою ока, обличчям або голосом) – бюджет підприємства дозволяє використовувати навіть найбільш дорогі біометричні системи ідентифікації (термінал розпізнавання райдужки ока);
- системи відеоспостереження та тривожної сигналізацій.

Рисунок 3.2 – Структура СКД для великого підприємства

Розглянемо приблизну вартість СКД для великого підприємства у табл. 3.2. Проте варто розуміти, що ціни вказані приблизні (з табл. 3.1) та без урахування кількості конкретних засобів, адже це буде залежати від кількості будівель, приміщень тощо.

Таблиця 3.2 – Приблизна вартість СКД для великого підприємства

Компонент СКД	***Кількість, шт***	***Приблизна вартість, грн***
Контролер	8	112 000
Електромеханічний замок	3	8 100
Турнікет speed gates, в повний зріст	1	400 000
Система обліку робочого часу	1	24 000
Термінал розпізнавання обличчя	1	47 000
Сканер відбитків пальців	1	5 500
Шлюзова кабіна	1	1 000 000
Термінал розпізнавання райдужки ока	1	97 000
Буквено-цифрова клавіатура	1	3 300
Зчитувач безконтактних карток	1	10 000
Відеокамера	1	12 000
Датчик тривожної сигналізації	1	1 200
Автоматичні ворота	1	50 000
	Сума	1 770 100

Розглянемо структуру СКД середнього підприємства (рис. 3.3).

Згідно розділу 2, у середніх підприємств бюджет від 4 до 20 млн гривень, а кількість працівників знаходиться в межах від 50 до 250. Тож в такому випадку треба зменшити кількість засобів СКД та обрати дешевші альтернативи. На прохідній можна використати турнікет трипод або роторний з

додаванням зчитувача відбитків пальців або безконтактних карток. Також слід додати систему обліку робочого часу. Кількість цехів і відділів тут менша, ніж у великого підприємства, тож і кількість точок доступу теж можна зменшити.

В структурі СКД для середнього підприємства можна використати такі пристрої:

- турнікети на вході;
- електромагнітні та електромеханічні замки на двері;
- контролери;
- зчитувачі безконтактні;
- шлагбаум;
- зчитувачі біометричні (за відбитком пальця/обличчя);
- системи відеоспостереження та тривожної сигналізації.

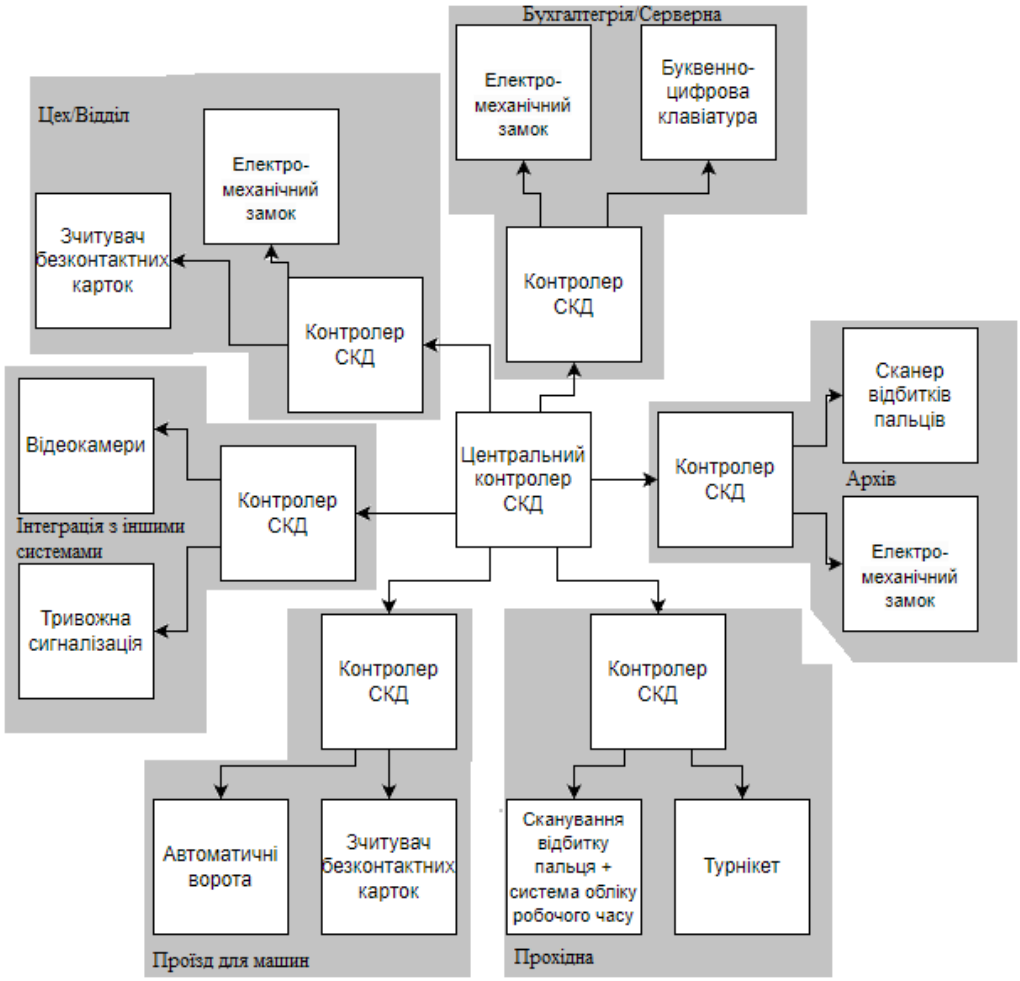

Рисунок 3.3 – Структура СКД для середнього підприємства

Розглянемо приблизну вартість СКД для середнього підприємства у табл. 3.3. Проте варто розуміти, що ціни вказані приблизні (з табл. 3.1) та без урахування кількості конкретних засобів, адже це буде залежати від кількості приміщень тощо.

Таблиця 3.3 – Приблизна вартість СКД для середнього підприємства

Компонент СКД	***Кількість, шт***	***Приблизна вартість, грн***
Контролер	7	63 000
Електромеханічний замок	3	5 100
Турнікет роторний	1	80 000
Система обліку робочого часу	1	15 000
Сканер відбитків пальців	1	4 700
Буквено-цифрова клавіатура	1	2 200
Зчитувач безконтактних карток	1	2 500
Відеокамера	1	5 000
Датчик тривожної сигналізації	1	600
Автоматичні ворота	1	33 000
	Сума	211 100

Для малих підприємств, які мають обмежені фінансові ресурси, вибір ще простішої СКД буде більш доцільним.

Оптимальний баланс між ефективністю та вартістю системи може бути досягнутий за допомогою вибору більш доступних методів ідентифікації. Наприклад, замість біометричних сканерів можна використати безконтактні картки доступу, ідентифікатори з штрих-кодом, клавіатури для введення PIN-

коду. Також можна обмежити кількість точок контролю доступу до найбільш критичних зон, таких як основний вхід, важливі кабінети або складські приміщення.

Вкладати значні кошти (більше 10% від доходу) в складні та дорогі СКД може бути нерентабельним для починаючих роботу та малих підприємств, які потребують ефективних рішень без зайвих витрат.

В структурі СКД (рис. 3.4) для малого підприємства можна використати такі пристрої:

- турнікет на вході (трипод або хвіртка);
- електромагнітні та електромеханічні замки на двері;
- контролери;
- буквено-цифрова клавіатура;
- зчитувачі безконтактні;
- системи відеоспостереження та тривожної сигналізації.

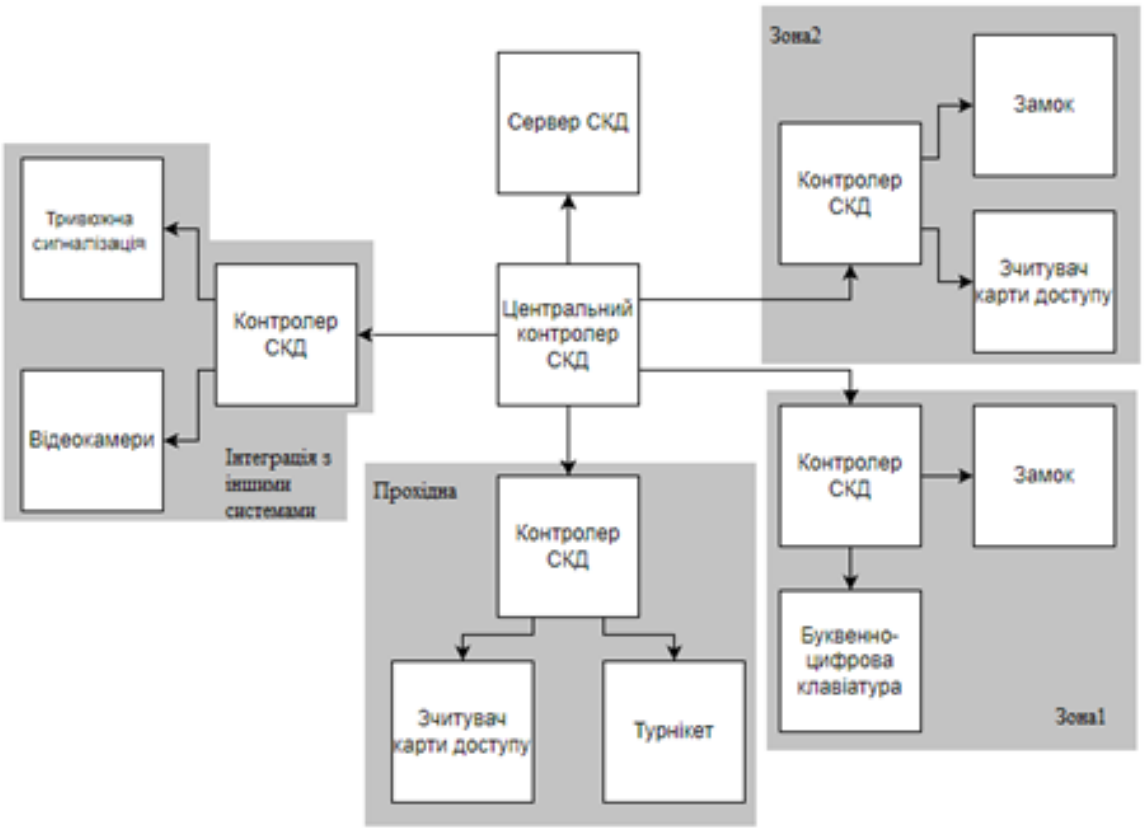

Рисунок 3.4 – Структура малого підприємства

Розглянемо приблизну вартість СКД для малого підприємства у табл. 3.4. Проте варто розуміти, що ціни вказані приблизні (з табл. 3.1) та без урахування кількості конкретних засобів, адже це буде залежати від кількості приміщень тощо.

Таблиця 3.4 – Приблизна вартість СКД для малого підприємства

Компонент СКД	***Кількість, шт***	***Приблизна вартість, грн***
Контролер	4	24 000
Електромеханічний замок	2	2 600
Турнікет трипод	1	30 000
Буквено-цифрова клавіатура	1	1 300
Зчитувач безконтактних карток	1	1 400
Відеокамера	1	2 500
Датчик тривожної сигналізації	1	300
	Сума	62 100

Так як мікропідприємства в більшості випадків використовують обмежену кількість простору (одне-два приміщень), то СКД можна значно спростити в порівнянні з малим підприємством. Сконцентрувавшись на базових компонентах СКД, слід встановити основну точку контрою та використати один з найпростіших методів ідентифікації – безконтактну карту/ключ. Також для такого спрощеного варіанту СКД буде краще використовувати локальну систему контролю і просту систему моніторингу.

В структурі СКД (рис. 3.5) для мікропідприємства можна використати такі пристрої:

- електромагнітні та електромеханічні замки на двері;

- контролер;
- зчитувачі безконтактні;
- системи відеоспостереження та пожежної сигналізації.

В такому підприємстві відеоспостереження може бути і відсутнім, особливо коли там працює до 5 осіб, а ззовні відвідування практично відсутнє. Таке можливо, коли вони самі виробляють товар і самі ж його доставляють [27].

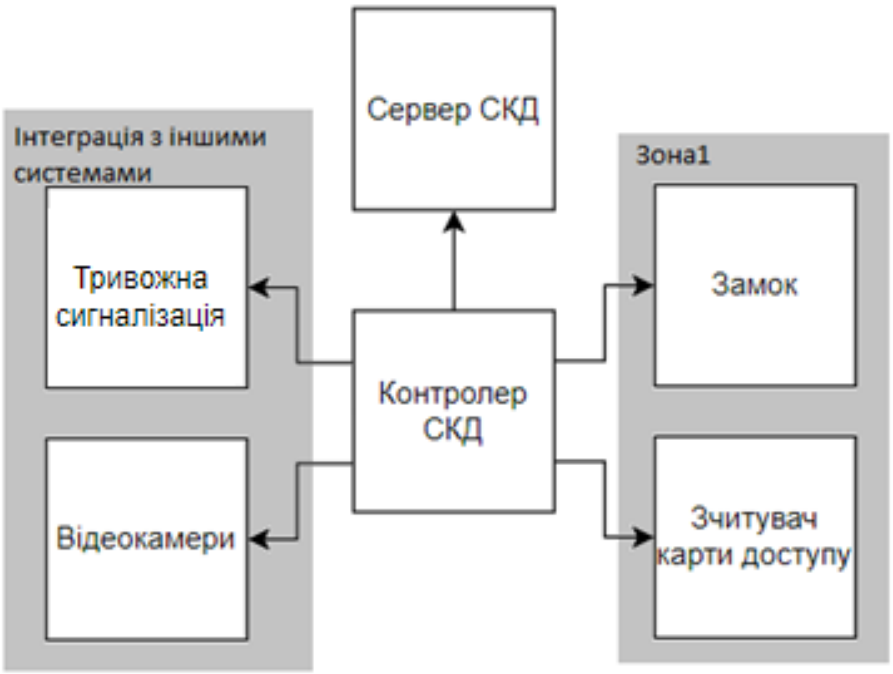

Рисунок 3.5 – Структура СКД для мікропідприємства

Розглянемо приблизну вартість СКД для мікропідприємства у табл. 3.5. Проте варто розуміти, що ціни вказані приблизні (з табл. 3.1) та без урахування кількості конкретних засобів.

Таблиця 3.5 – Приблизна вартість СКД для мікропідприємства

Компонент СКД	***Кількість, шт***	***Приблизна вартість, грн***
Контролер	1	3 000
Електромеханічний замок	1	600
Зчитувач безконтактних карток	1	800
Відеокамера	1	1 500
Датчик тривожної сигналізації	1	150
	Сума	6 050

3.3 Експертний аналіз систем біометричної автентифікації

Так як підприємства різні за розміром, та мають різну структуру і бюджет, який вони готові виділити на свої СКД, дуже важко одразу обрати підходящу систему автентифікації.

Найбільш вживаними серед підприємств є безконтактні картки через їх дешевизну та доступність. Складнощі при виборі виникають саме серед систем біометричної автентифікації. Вони варіативні, різні за рівнем безпеки, контролю та вартості. Тож потрібно проаналізувати доцільність встановлення тих чи інших систем для підприємств [28].

Оцінка систем автентифікації буде здійснюватися за допомогою експертного аналізу на основі наступних методів:

- сканування відбитків пальців;
- сканування сітківки ока;
- використання голосу.

Таблиця 3.6 – Критерії оцінки систем

№	*Критерій*	*Позначення*
1	Стійкість	x_1
2	Ймовірність пошкодження	x_2
3	Вплив зовнішніх факторів	x_3
4	Вартість системи	x_4
5	Ймовірність неправильного спрацювання	x_5
6	Вартість обслуговування	x_6
7	Простота використання	x_7
8	Доступність готових рішень	x_8

Визначення вагомості кожного параметра буде проводитись за допомогою методу попарного порівняння. Для отримання числових значень відносних коефіцієнтів вагомості a_{ij} параметри порівнюються попарно п'ятьма незалежними експертами. В цьому процесі коефіцієнти a_{ij} можуть приймати наступні значення:

- 1,5 при $x_i > x_j$;
- 1 при $x_i = x_j$;
- 0,5 при $x_i < x_j$.

Результати попарного порівняння критеріїв наведені в табл. 3.7:

Таблиця 3.7 – Порівняння критеріїв

Критерії	*1-2*	*1-3*	*1-4*	*1-5*	*1-6*	*1-7*	*1-8*	*2-3*	*2-4*	*2-5*	*2-6*	*2-7*	*2-8*
Загальна оцінка експертів	=	>	>	<	>	<	>	=	=	<	>	>	=
Коефіцієнт вагомості	1	1.5	1.5	0.5	1.5	0.5	1.5	1	1	0.5	1.5	1.5	1

Кінець таблиці 3.7

Критерії	***3-4***	***3-5***	***3-6***	***3-7***	***3-8***	***4-5***	***4-6***	***4-7***	***4-8***	***5-6***	***5-7***	***5-8***	***6-7***	***6-8***	***7-8***
Загальна оцінка експертів	>	<	>	=	=	<	=	<	=	>	>	>	=	=	=
Коефіцієнт вагомості	1.5	0.5	1.5	1	1	0.5	1	0.5	1	1.5	1.5	1.5	1	1	1

На основі наданих a_{ij} будується квадратна матриця. Розрахунок вагомості кожного критерію K_i здійснюється за наступними формулами:

$$b_i = \sum_{j=1}^{n} a_{ij};$$

$$K_i = \frac{b_i}{\sum_{j=1}^{n} b_i},$$

де b_i – вагомість і-го критерію за результатами оцінок всіх експертів (визначається як сума значень коефіцієнтів a_{ij}, визначених всіма експертами по і-тому критерію).

Відносні оцінки вагомості розраховуються кілька разів, доки наступне значення відрізняється менше ніж на 5% від попереднього значення. На другому і наступних кроках значення коефіцієнта вагомості K_i' розраховується за допомогою наступної формули:

$$K_i' = \frac{b_i'}{\sum_{j=1}^{n} b_i'},$$

де $b_i' = a_{i1}b_1 + a_{i2}b_2 + \ldots + a_{in}n$.

Мають бути дотримані дві умови:

- $\sum_{j=1}^{n} K_i = 1$;
- $\sum_{j=1}^{n} K_i' = 1$.

Розрахунок вагомості критеріїв представлений в табл. 3.8.

Таблиця 3.8 – Результати оцінок

Критерій, x_i	***Критерій,*** x_i								***Перший крок***		***Другий крок***	
x_i	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	b_i	K_i	$b¢_i$	$K¢_i$
x_1	1	1	1.5	1.5	0.5	1.5	0.5	1.5	9	0.13043	79.25	0.13219
x_2	1	1	1	1	0.5	1.5	1.5	1	8.5	0.12319	74.25	0.12385
x_3	1.5	1	1	1.5	0.5	1.5	1	1	9	0.13043	78.75	0.13136
x_4	1.5	1	1.5	1	0.5	1	0.5	1	8	0.11594	70.25	0.11718
x_5	0.5	0.5	0.5	0.5	1	1.5	1.5	1.5	7.5	0.1087	65.25	0.10884
x_6	1.5	1.5	1.5	1	1.5	1	1	1	10	0.14493	86	0.14345
x_7	0.5	1.5	1	0.5	1.5	1	1	1	8	0.11594	68.5	0.11426
x_8	1.5	1	1	1	1.5	1	1	1	9	0.13043	77.25	0.12886
Всього									69	1	599.5	1

Визначимо числове значення оцінки кожного варіанту за кожним критерієм окремо.

Дані в табл. 3.9 відображають результати експертних оцінок щодо якості системи.

Таблиця 3.9 – Оцінка якості системи

№	*Критерій, i*	*Варіант, j*	*Оцінка*			*Σ*	B_{ij}
			1	*2*	*3*		
1	Стійкість	1		0.5	1.5	2	0.33
		2	1.5		1.5	3	0.5
		3	0.5	0.5		1	0.17
2	Ймовірність пошкодження	1		0.5	0.5	1	0.17
		2	1.5		0.5	2	0.29
		3	1.5	1.5		3	0.5
3	Вплив зовнішніх факторів	1		0.5	1.5	2	0.33
		2	1.5		1.5	3	0.5
		3	0.5	0.5		1	0.17
4	Вартість системи	1		1.5	1	2.5	0.42
		2	0.5		0.5	1	0.17
		3	1	1.5		2.5	0.42
5	Ймовірність неправильного спрацювання	1		0.5	1.5	2	0.33
		2	1.5		1.5	3	0.5
		3	0.5	0.5		1	0.17
6	Вартість обслуговування	1		1.5	1.5	3	0.6
		2	0.5		0.5	1	0.2
		3	0.5	0.5		1	0.3
7	Простота використання	1		1	1	2	0.33333
		2	1		1	2	0.33333
		3	1	1		2	0.33333
8	Доступність готових рішень	1		1.5	1	2.5	0.41667
		2	0.5		1	1.5	0.25
		3	1	1		2	0.33333

Оцінка враховується за критерієм:

$$b_{ij} = \begin{cases} 0.5, \text{варіант 1 більш вигідний за варіант 2} \\ 1, \text{варіант 1 та варіант 2 однаково вигідні.} \\ 1.5, \text{варіант 2 більш вигідний за варіант 1} \end{cases}$$

Знаючи всі складові, можна розрахувати цільову функцію якості по кожному варіанту.

Цільова функція першої системи:

$$S_1 = \sum_{j=1}^{5} K_j \cdot B_{1j} = 0{,}372.$$

Цільова функція другої системи:

$$S_2 = \sum_{j=1}^{5} K_j \cdot B_{2j} = 0{,}339.$$

Цільова функція третьої системи:

$$S_3 = \sum_{j=1}^{5} K_j \cdot B_{3j} = 0{,}282.$$

На основі цих критеріїв та оцінок було вирішено, що ідентифікація за відбитками пальців є найбільш економічно вигідним варіантом для СКД на підприємствах.

Висновки до третього розділу

Аналіз СКД охоплював різні аспекти, включаючи біометричні системи автентифікації, структуру систем та їх середню вартість впровадження.

Експертний аналіз підкреслив сильні сторони та недоліки біометричних методів ідентифікації (сканування відбитків пальців, сканування сітківки ока, використання голосу.), враховуючи такі фактори, як стійкість, ймовірність пошкодження, вплив зовнішніх факторів, вартість системи, ймовірність

неправильного спрацювання, вартість обслуговування, простота використання, доступність готових рішень. Розуміючи можливості та особливості біометричних систем автентифікації, підприємства можуть приймати обґрунтовані рішення, вибираючи найбільш підходящий варіант для своїх потреб у контролі доступу.

Крім того, було розглянуто СКД на різних підприємствах. Аналіз виявив, що великі підприємства зі складними структурами та багатьма приміщеннями потребують комплексних і масштабованих СКД. Навпаки, малі та мікропідприємства можуть мати більш спрощені вимоги, часто зосереджені на локальному контролі.

Вартість впровадження СКД може змінюватися залежно від розміру підприємства, кількості контрольних точок, обраних методи автентифікації та необхідного рівня інтеграції. У той час як великі підприємства зі стабільним доходом можуть дозволити собі більш масштабні та складні системи, меншим підприємствам може знадобитися збалансувати свої бюджетні обмеження з потребами безпеки.

ВИСНОВКИ

СКД використовуються майже всюди, та попри їх розповсюдженість споживачам важко обрати для себе підходящі засоби, так як системи не є універсальними та потребують адаптації під конкретні потреби. За допомогою огляду літературних джерел було проведено ознайомленням з теоретичними даними про поняття СКД, їх можливості, класифікацію та компоненти.

Був проведений експертний аналіз за допомогою якого система сканування відбитків пальців була виявлена як найбільш підходяща система біометричної ідентифікації, яка забезпечує доступність, безпеку та економічну ефективність. Ця рекомендація була заснована на оцінці різних факторів: стійкість, ймовірність пошкодження, вплив зовнішніх факторів, вартість системи, ймовірність неправильного спрацювання, вартість обслуговування, простота використання, доступність готових рішень.

На основі вивченої інформації були запропоновані загальні структури СКД, адаптованих до різних типів підприємств. Структури враховували характеристики, вимоги та бюджетні можливості кожної з чотирьох категорій підприємств. Впроваджуючи ці загальні структури, підприємства можуть мати відправну точку для вибору відповідної СКД.

В результаті дослідження вартості засобів, використаних в рекомендованих структурах СКД, були представлені приблизні діапазони витрат для підприємств. Хоча точні ціни можуть змінюватися залежно від різних факторів, таких як розмір підприємства, кількість точок доступу та вибрані технології.

ПЕРЕЛІК ПОСИЛАНЬ

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

2. Депутати В. Р. ДСТУ EN 50133-1:2006 Системи тривожної сигналізації. Системи контролювання доступу охоронного призначення. Частина 1. Вимоги до систем. [Електронний ресурс] / В. Р. Депутати. – 2007. – Режим доступу до ресурсу: https://d naop.com/html/61076/doc-%D0%94%D0%A1%D0%A2.

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

4. Ворона В. А. Системы контроля и управления доступом. / В. А. Ворона, В. А. Тихонов. – Москва: Горячая линия - Телеком, 2010. – 272 с.

5. Що таке СКУД?. *Ohrana.ua*. [Електронний ресурс] — URL: https://ohrana.ua/uk/stati-i-obzory/chto-takoe-skud.html (дата звернення: 05.06.2023).

6. Бугаков В. П. Технические средства охраны. Системы контроля и управления доступом / В. П. Бугаков, А. В. Тельный. – Владимир: Владимирс. государственный университет, 2007. – 148 с.

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

8. Пластикові картки зі штрих-кодом та номером. [Електронний ресурс] // Друкарня «50 КОПІЙОК» – Режим доступу до ресурсу: https://www.50kopeek.kiev.ua/ua/uslugi/kartochki-numeraciya-shtrih-kodom/.

9. Ключ ТМ [Електронний ресурс] // Ohrana.ua – Режим доступу до ресурсу: https://ohrana.ua/uk/dostup/klyuch-th.html.

10. Проксіміті карта Satel KT-STD-2 [Електронний ресурс] // SMARTEL – Режим доступу до ресурсу: https://smartel.ua/ua/product/proksimiti-karta-satel-kt-std-2/.

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

12. Турнікет роторний STAR-TS [Електронний ресурс] // SmartEl – Режим доступу до ресурсу: https://smartel.ua/ua/product/turniket-rotornyy-star-ts/.

13. Види та особливості турнікетів [Електронний ресурс] // TISO – Режим доступу до ресурсу: https://ua.turniket.net/novini/262-yaki-buvayut-vidi-osoblivost-turniketi.

14. Шлагбаум механічний вертикальний МАРО ШМВ-4 [Електронний ресурс] // ROZETKA – Режим доступу до ресурсу: https://rozetka.com.ua/ua/290640173/p290640173/.

15. Шлагбауми і бар'єри HORMANN, CAME, Алютех, Faac [Електронний ресурс] // Артпрофі – Режим доступу до ресурсу: https://artprofi.com.ua/poltava-company-services-ua/barriers-and-barriers-poltava-ua.

16. Підйомно поворотні ворота [Електронний ресурс] // Алюмікс – Режим доступу до ресурсу: https://alumix.ua/ua/poleznye-materialy/podemno-povorotnye-vorota.

17. Замок електромеханічний TRL-5302BT SILVER TRINIX [Електронний ресурс] // TRINITI-SB – Режим доступу до ресурсу: https://triniti-sb.com.ua/product/zamok-trl-5302bt-silver-trinix/.

18. Рулонні ворота: чому варто встановити саме їх [Електронний ресурс] // Architecture blog – Режим доступу до ресурсу: https://remhouse.info/3901-rulonni-vorota-chomu-varto-vstanovyty-ikh.html.

19. Ворота розсувні (модульні) [Електронний ресурс] // ЗСК – Режим доступу до ресурсу: https://zsk.kiev.ua/uk/product/554-vorota2040/category_pathway-334.

20. Види автоматичних воріт та їх відмінні риси [Електронний ресурс] // Евроворота – Режим доступу до ресурсу: https://evrovorota.com/uk/vidi-avtomatichnikh-vorit-ta-їkh-vidminni-risi/.

21. Розпашні ворота ADS400 [Електронний ресурс] // Viknoplus – Режим доступу до ресурсу: https://www.viknoplus.ua/products/rozpashni-vorota-ads400/.

22. ELE 70 Light (Saima) шлюзова кабіна безпеки [Електронний ресурс] // Parkan.ua – Режим доступу до ресурсу: https://parkan.ua/p651525215-ele-light-saima.html.

23. Депутати В. Р. Господарський кодекс України [Електронний ресурс] / Р. Депутати. – 2003. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/436-15#Text.

24. Депутати В. Р. Закон України Про внесення змін до Закону України ”Про бухгалтерський облік та фінансову звітність в Україні” щодо удосконалення деяких положень [Електронний ресурс] / В. Р. Депутати. – 2017. – Режим доступу до ресурсу: https: //zakon.rada.gov.ua/laws/show/2164-19#Text.

25. Лановенко В. О. Малий бізнес в україні: стан та проблеми розвитку [Електронний ресурс] / В. О. Лановенко // Міжнародні наукові інтернет-конференції – Режим доступу до ресурсу: https://www.economy-confer.com.ua/full-article/3183/.

26. Васильков В. Г. Організація виробництва / В. Г. Васильков. – Київ: Київський національний економічний ун-т, 2003. – 522 с.

27. Безсонова А. О. Застосування систем контролю доступу для різних типів підприємств / А. О. Безсонова, О. Д. Василенко. // Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених. – 2023. – С. 117–120.

28. Дмитренко В. П. Аналіз використання різних типів систем біометричної автентифікації для різних типів підприємств / В. П. Дмитренко, О. Д. Василенко. // Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених. – 2021. – С. 136–138.