Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Система контролю доступу із захистом від витоку інформації на основі Bluetooth-технології
Назва теми

КРКБ 190108.19.01.09 ПЗ
Шифр

Галузь знань *12 «Інформаційні технології»*
Шифр, назва

Спеціальність *125 «Кібербезпека»*
Шифр, назва

Освітня програма *«Кібербезпека»*
Шифр, назва

Виконав студент 4 курсу, група КБ-19-1 — Підпис — Медвецький С.О. (Ініціали, прізвище)

Керівник — Підпис, дата — Чешун В.М. (Ініціали, прізвище)

Нормоконтролер — 07.06.23 — Підпис, дата — Мостовий С.В. (Ініціали, прізвище)

До захисту допускаю:
Зав. кафедри кібербезпеки — Підпис, дата — Кльоц Ю.П. (Ініціали, прізвище)

7 06 2023 р.

Хмельницький, 2023

Формат	Зона	Позиц	Позначення	Найменування	Кільк. листів	Примітка
A4		1	КРКБ 190108.19.01.09 ПЗ	Система контролю	69	
				доступу від витоку		
				інформації на основі		
				Bluetooth-технології		
				Пояснювальна записка		
A2		2	КРКБ 190108.19.01.09 Е8	Система контролю	1	
				доступу від витоку		
				інформації на основі		
				Bluetooth-технології		
				Загальна схема СКУД		
A2		3	КРКБ 190108.19.01.09 Е8	Система контролю	1	
				доступу від витоку		
				інформації на основі		
				Bluetooth-технології		
				Схема розміщення		
				відеоспостереження		
A2		4	КРКБ 190108.19.01.09 Е8	Система контролю	1	
				доступу від витоку		
				інформації на основі		
				Bluetooth-технології		
				Схема розміщення		
				обладнання СКУД		

КРКБ 190108.19.01.09 ВП

Зм.	Арк.	№ Докум.	Підп.	Дата
Розробив		Медвецький С.О.		6.06
Перев.		Чешун В.М.		6.06
Н. контр.		Мостовий С.В.		07.06.23
Затв.		Кльоц Ю.П.		7.06.23

Система контролю доступу із захистом від витоку інформації на основі Bluetooth-технології
Відомість проєкту

Літера	Аркуш	Аркушів
п	1	1

ХНУ, КБ-19-1

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Освітній рівень Бакалавр

Галузь знань 12 Інформаційні технології

Спеціальність 125 Кібербезпека

Освітня програма Освітньо-професійна програма підготовки бакалаврів

ЗАТВЕРДЖУЮ

Зав. кафедри Ю.П. Кльоц

"1" 03 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Медвецький Сергій Олегович

Прізвище, ім'я, по батькові студента

1. Тема роботи Система контролю доступу із захистом від витоку інформації на основі Bluetooth-технології

Керівник роботи Чешун В.М.

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджено наказом ректора університету від 01 березня 2023 р. №5 додаток №11

2. Строк подання студентом роботи на кафедру 20.05.2023р.

3. Вихідні дані до проекту (роботи) Створити систему для запобігання витоку інформації на основі Bluetooth-технології. Визначити об'єкт захисту та дослідити його роботу. Вибрати систему для розробки та обладнання. Аналізувати потреби та вимоги. Дослідити інформацію та її види. Визначити рівні та зони доступу у офісі відповідно до потреб безпеки. Встановити обладнання доступу на основі Bluetooth-технології. Впровадити систему контролю доступу в офісі з відповідним навчанням персоналу. Провести розрахунок ефективності роботи системи.

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити) Вступ. Аналіз безпеки систем контролю доступу. Проєктування системи контролю доступу на основі Bluetooth-технології. Політика безпеки користування системою та економічне обгрунтування. Висновки.

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

1. Загальна схема СКУД,
2. Схема розміщення відеоспостереження
3. Схема розміщення обладнання СКУД

6. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завданн
-			
-			

7. Дата видачі завдання 1 березня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) кваліфікаційної роботи	Термін виконання етапів проекту (роботи)	П
1	Вибір і затвердження теми кваліфікаційної роботи	Січень	
2	Пошук теоретичної інформації про системи контролю доступу	Січень	
3	Дослідження існуючих рішень	Лютий	
4	Постановка задачі	Лютий	
5	Розробка системи контролю управління доступу	Березень	
6	Політика безпеки користування системою	Квітень	
7	Розробка встановлення обладнання системи контролю доступу у офісі	Квітень\Травень	
8	Оформлення пояснювальної записки згідно вимог	Травень	
9	Оформлення графічної частини	Червень	
10	Захист КР	Червень	

Студент _____ Медвецький С.О.
Підпис Ініціали, прізвище

Керівник проекту (роботи) _____ Чешун В.М.
Підпис Ініціали, прізвище

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Система контролю доступу із захистом від витоку інформації на основі Bluetooth-технології».

Автор роботи: Медвецький Сергій Олегович.

Керівник роботи: Чешун Віктор Миколайович.

Пояснювальна записка: 69 с., 1 додаток, 20 рис., 5 табл., 40 джерел.

Графічна частина: 10 презентаційних слайдів.

Метою цієї роботи було створення системи контролю доступу із захистом від витоку інформації на основі Bluetooth-технології. Головним завданням було запобігання витоку конфіденційної інформації та забезпечення безпеки даних клієнтів.

Для досягнення цих цілей було проведено дослідження і аналіз області систем контролю доступу, існуючих методів захисту на основі Bluetooth-технології, а також теоретичної інформації про такі системи і їх моделі створення. На основі цього аналізу була розроблена і створена система, яка може виявляти витоки даних в системах контролю доступу, використовуючи Bluetooth-технології.

Також було впроваджено цю систему в юридичний офіс, забезпечивши навчання персоналу та розподіл необхідних обов'язків. Це дозволило забезпечити контроль доступу до приміщень офісу і запобігти можливим витокам конфіденційної інформації.

Дата 7.06.2023 Підпис

ANNOTATION

Course project: Access control system with protection against information leakage based on Bluetooth technology.

Author of the work: Medvetsky Serhiy Olegovych.

Supervisor: Cheshun Viktor Mykolayovych.

Amount: 69 p., 1 appendix, 20 figures, 5 tables, 40 sources.

Graphic part: 10 presentation slides.

The purpose of this work was to create an access control system with protection against information leakage based on Bluetooth technology. The main task was to prevent the leakage of confidential information and ensure the security of customer data.

To achieve these goals, research and analysis of access control systems, existing methods of protection based on Bluetooth technology, as well as theoretical information about such systems and their creation models were carried out. Based on this analysis, a system was developed and created that can detect data leaks in access control systems using Bluetooth technology.

This system was also implemented in the legal office, providing staff training and distribution of necessary responsibilities. This made it possible to control access to office premises and prevent possible leaks of confidential information.

Date 7.06.2023 Signature

ЗМІСТ

ВСТУП 3
1 АНАЛІЗ БЕЗПЕКИ СИСТЕМ КОНТРОЛЮ ДОСТУПУ 5
1.1 Компоненти системи контролю та управління доступу 5
1.2 Принцип функціонування системи контролю та управління 14
1.3 Класифікація систем контролю та управління доступом 16
1.4 Постановка задачі 20
2 ПРОЄКТУВАННЯ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ НА ОСНОВІ BLUETOOTH-ТЕХНОЛОГІЇ 21
2.1 Аналізу інформації безпеки офісу 21
2.2 Система контролю доступу 28
2.3 Захист інформації за допомогою різних пристроїв 37
2.4 Висновок 43
3 ПОЛІТИКА БЕЗПЕКИ КОРИСТУВАННЯ СИСТЕМОЮ ТА ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ 45
3.1 Інструкція з експлуатації системи 45
3.2 Економічні розрахунки 54
3.3 Політика безпеки користування системою 57
3.4 Висновок 61
ВИСНОВКИ 64
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ 66
ДОДАТОК А. Копія графічної частини 70

ВСТУП

Скільки років існує людське суспільство, яке визнало принцип приватної власності, стільки років існують і засоби захисту від посягань на цю власність. Люди завжди закривали свій будинок, замок, квартиру, офіс. Навряд чи через пару сотень років потреба в цьому зникне. Ми живемо у матеріальному світі, і нас оточують живі люди, а людям, як відомо, ніщо матеріальне не чуже. Системи для замикання того, що людям дорого, удосконалюються разом з технічним прогресом, і у вік електроніки найсучасніші запори, звичайно ж, не можуть обійтися без мікроконтролерів та комп'ютерів.

Зайвих грошей ніколи не буває, і якщо хтось вирішив їх витратити на безпеку офісу чи будинку, то варто це робити зі знанням справи, щоб не переплачувати за можливості, які ніколи не будуть використовуватись. Крім того, не треба забувати, що при побудові таких систем не повинно залишатися «тонких» місць, і всі компоненти системи повинні бути збалансовані.

Сьогодні застосування систем контролю доступу стало невід’ємною складовою при утворенні периметру комплексного захисту у вирішенні задач інформаційної безпеки. Один із варіантів таких систем - системи контролю доступу із застосуванням Bluetooth-технології.

Bluetooth – це міжнародний стандарт, що підтримує та застосовує величезна кількість різноманітних компаній по всьому світу [1,2].

На жаль, комерційні організації, а тим більше самі виробники систем контролю та управління доступом не надають жодних статистичних даних про проникнення сторонніх на об'єкти та спричинені ними втрати. У зв'язку з цим перед керівниками великих і малих організацій стоять дві основні проблеми:

– контроль фізичного доступу до приміщення організації (з різним рівнем доступу самих працівників у різні приміщення);

– контроль за наявністю та перебуванням персоналу в межах офісу компанії (особливо актуально якщо офіс розташовується на декількох поверхах або в декількох будинках).

Метою даної кваліфікаційної роботи є розробка доступної, недорогої та ефективної системи контролю та управління доступом (СКУД), здатної відповідати сучасним вимогам безпеки. Цільовим колом споживачів я вибрав агентство, що орендує офісне приміщення у популярному, останнім часом, бізнес-центрі. Останні, як правило, вже мають централізовану охорону на прохідних, що забезпечує роботу СКУД. Зазвичай там застосовуються найбільш поширені системи і засоби захисту та управління доступом, такі як: proximity/smart-карти або магнітні ключі з турнікетами, домофони, разом із системами відеоспостереження тощо. Це означає, що кожен працівник вже має свій ідентифікатор (карта, ключ і т.п.), що дає можливість проходу на територію офісу. Але якщо є необхідність найчіткішої організації робочого процесу, наприклад, мати доступ до інформації про місцезнаходження кожного співробітника, і його переміщеннях протягом робочого дня, виникають незручності. Можна, звичайно, встановлювати контролери на кожних дверях, але це робить пересування по офісу дуже скрутним, не кожній фірмі це підійде. Тому є сенс спростити, а ще краще – автоматизувати цю систему [3,4].

Зараз практично кожен має мобільний телефон з технологією Bluetooth. Ця технологія найбільше підходить для реалізації такої СКУД через свою доступність і низьку енергоємність. Ідентифікатором в даному випадку є програма (клієнт), зашита в телефон за допомогою цієї технології, інфрачервоного порту, або data-кабеля. Зчитувач – комп'ютер, також із програмою (сервер) з модулем Bluetooth.

1 АНАЛІЗ БЕЗПЕКИ СИСТЕМ КОНТРОЛЮ ДОСТУПУ

1.1 Компоненти системи контролю та управління доступом

Система контролю та управління доступом (СКУД) - це сукупність програмно-технічних засобів і організаційно-методичних заходів, які використовуються для забезпечення контролю та управління відвідуванням окремих приміщень, а також оперативного контролю руху персоналу та його часу перебування на території об'єкта. Справді, СКУД - це не лише обладнання та програмне забезпечення, але й ретельно продумана система управління рухом персоналу (рисунок 1.1).

Рисунок 1.1 – Компоненти СКУД

У будь-якій системі контролю та управління доступом (СКУД) існує ідентифікатор (ключ), який використовується для визначення прав власника. Це може бути "далласовська таблетка", широко використовувана у вхідних домофонах, безконтактна картка або брелок, а також код, набраний на клавіатурі, та ряд біометричних ознак людини - відбиток пальця, рисунок сітківки або райдужної оболонки ока [5,6].

Картки або брелоки можна передати, їх можуть викрасти або скопіювати. Код можна підглянути або просто повідомити комусь. Біометричні ознаки неможливо передати або викрасти, хоча деякі з них все ж можуть бути підроблені без великих зусиль.

Тип використовуваного ідентифікатора у великому відношенні визначає безпеку системи від зловмисників. Наприклад, будь-який радіолюбитель, використовуючи інструкції, доступні в Інтернеті, легко може зробити імітатор "далласовської таблетки", де зберігається код завжди на зворотному боці. Безконтактні картки або брелоки, що широко використовуються в системах контролю доступу, трохи складніше підробити, але вони також не захищені від цього. Сьогодні існують картки з високим рівнем захисту (використовуються потужні криптографічні схеми, де ключі для шифрування може призначати сам користувач), але в стандартних СКУД такі рішення, поки що практично не використовуються. Біометричні ознаки складніше підробити. Зазвичай там, де потрібний високий рівень захисту від зламу, одночасно використовуються декілька ідентифікаторів: картка і код, відбиток пальця і картка або код.

При втраті механічного ключа рекомендується замінити замок або лицьову панель. У випадку електронних ідентифікаторів втрачений "ключ" просто виключається зі списку дозволених, що набагато простіше і дешевше.

При виборі типу ідентифікатора необхідно враховувати, що у системі може бути одна точка входу (наприклад, турнікет на вході в будівлю), а користувачів може бути сотні. У цьому випадку вартість ідентифікатора, помножена на кількість, може перевищити вартість всього обладнання. І якщо

врахувати, що їх втрачають і ламають, це заплановані витрати на майбутнє. Бажано, щоб обрані ідентифікатори були широко доступні на ринку (тобто вони виробляються не єдиним у світі підприємством та мають аналоги). Це гарантує можливість докуповувати необхідну кількість ключів через кілька років.

У Bluetooth технології використовується радіочастотні діапазони 2,4 ГГц і підтримують швидкість передачі даних від 1 до 3 Мбіт/с. Загальна мета Bluetooth – забезпечення простоїв, бездротової комунікації по між різними пристроями. У сьогоденні Bluetooth-технологія використовується у різних сферах, враховуючи автомобільну промисловість, медичне приладобудування, промислову автоматизацію, мобільні пристрої та інше [7,8].

Магнітні картки – це є найбільш поширений варіант. Існують картки з низько-коерцитивною та високо-коерцитивною магнітною смугою та записом на різні доріжки.

Карти Віганда – названі на честь вченого, який відкрив магнітний сплав з прямокутною петлею гістерезису. Усередині карти розташовані відрізки дроту з цього сплаву, які при русі поряд із ними зчитувальною головкою, дозволяють зчитувати інформацію. Ці картки є більш тривалими, але і дорожчими, ніж магнітні. Один з недоліків – це код на карті записаний при виготовленні один раз і назавжди.

Картки з штрих-кодом – на картку наноситься штриховий код. Існує складніший варіант – штрих-код закривається матеріалом, прозорим лише у інфрачервоному світлі, зчитування відбувається в ІЧ-діапазоні.

Ключ-брелок "Touch memory" – металева таблетка, всередині якої розташований чіп ПЗУ. При дотику таблетки до зчитувача з пам'яті таблетки передається унікальний код ідентифікатора до контролера.

Та сама картка може відкривати як одні двері, так і служити "ключем" для кількох дверей. Для тимчасових працівників і відвідувачів оформляються тимчасові або одноразові "пропуски" – картки з обмеженим строком дії.

Пристрій, призначений для зчитування інформації з ідентифікатора та передачі цієї інформації до контролера системи контролю доступу (СКУД). Залежно від принципів роботи ідентифікатора змінюється й технологія зчитування коду. Для "далласовської таблетки" це два електричні контакти, виконані у вигляді лузи, для картки proximity це вже достатньо складний електронний пристрій, а для зчитування, наприклад, рисунку радужної оболонки ока, в склад зчитувача входить мініатюрна відеокамера.

Біометричні зчитувачі на сьогоднішній день все ще дуже дорогі, тому їх застосування повинно бути обґрунтовано реальною потребою. Крім того, вони мають деякі недоліки, тобто, відносно тривалий час ідентифікації (від десятих долей до одиниць секунд), та вони не розраховані при використанні на вулиці.

Зчитувачі відбитків пальців викликають деякий дискомфорт у людей, хоча, жоден з сучасних дактилоскопічних зчитувачів не зберігає відбитки пальців. Надійність розпізнавання людини за біометричними ознаками ще не досягає стовідсоткової точності, що також може створити певні незручності.

Серце системи контролю та управління доступом (СКУД) - це пристрій, призначений для обробки інформації з зчитувачів ідентифікаторів, прийняття рішень та керування виконавчими пристроями. За способом управління контролери СКУД поділяються на три класи: автономні, централізовані (мережеві) та комбіновані. Вони є основною складовою системи. Саме контролер приймає рішення про те, чи допустити особу до вказаних дверей. Контролер зберігає коди ідентифікаторів у своїй пам'яті разом зі списком прав для кожного з них. Коли ви надаєте ідентифікатор, зчитаний з нього код порівнюється зі збереженим у пам'яті, на основі чого приймається рішення про відкриття або не відкриття дверей чи воріт [9].

Оскільки контролер виконує такі важливі функції, його необхідно розміщувати в захищеному місці, зазвичай всередині приміщення, вхід до якого він охороняє. Інакше всі ідентифікатори будуть зайвими – зловмисник знайде

проводи від електрозамка і відкриє його, незважаючи на будь-які "розумові здібності" контролера (рисунок 1.2).

Рисунок 1.2 – Контролер

Для роботи контролера потрібне електроживлення, тому дуже важливо, щоб він міг працювати навіть у разі відключення електрики (а таке відключення може бути організоване зловмисником). Професійні контролери, як правило, мають власний акумулятор, який забезпечує їх роботу протягом кількох годин або навіть кількох днів. Якщо застосовується простий автономний контролер без власного блоку живлення, то краще не живити його від звичайного адаптера для електронних іграшок, підключеного до розетки [10].

Якщо завдання СКУД полягає в обмеженні доступу через звичайні двері, то виконавчим пристроєм буде електрично керований замок або защіпка. Защіпки є недорогими, легко встановлюються на більшість дверей і, оскільки зазвичай встановлюються в дверному косяку, не потребують гнучкого підведення живлення до самої двері. За стійкістю до в злому це найгірший варіант, тому рекомендується використовувати електричні защіпки там, де ймовірність в злому зі сторони зловмисника є мінімальною – зазвичай це двері всередині офісу. На ніч двері, обладнані електричною защіпкою, зазвичай запираються механічним ключем.

Варто зазначити, що електричні защіпки, так само як і інші типи замків, можуть бути відкритими при подачі напруги (тобто двері відкриються при живленні замка) або закритими при напрузі. Останні відкриваються, як тільки з них знімається живлення. Згідно з вимогами пожежної безпеки, всі двері, які використовуються для виходу в разі пожежі, повинні бути обладнані замками, що закриваються при напрузі (рисунок 1.3).

Рисунок 1.3 – Електронний замок

Електромагнітні замки також не є ідеальним варіантом запорного пристрою, але вони також відносно недорогі та у деяких випадках дуже зручні для установки. Якщо це можливо, їх краще встановлювати з внутрішньої сторони дверей. Майже всі вони належать до групи замків, що закриваються при напрузі, тобто придатні для установки на шляхах евакуації під час пожежі.

Електромеханічні замки існують у різних типах. Зазвичай можна вибрати досить стійкий до в злому замок (механічно міцний, з потужним засувом). Недоліки полягають у трохи вищій ціні, а також у необхідності гнучкого підведення живлення до самої двері. Більшість таких замків мають механічний перезаряд, тобто якщо на замок подали відкриваючий імпульс, навіть невеликої тривалості, двері будуть відкритими, поки їх не відкриють і знову не закриють.

Такі пристрої для обмеження проходу використовуються лише на підприємствах. Турнікети існують у двох основних типах: з поясом і повно розмірні. Різниця зрозуміла з назви. При правильній настройці всієї системи турнікет дійсно дозволяє пропустити за однією карткою лише одну особу. Завдяки цьому, а також завдяки високій пропускній здатності (прохід вимагає мінімум часу), вони є незамінними на вході в велике підприємство, де, крім того, використовується система обліку робочого часу (рисунок 1.4).

Рисунок 1.4 – Турнікет

Автономні системи дешевші, простіші в експлуатації (часто установка і налаштування такої системи доступні навіть недосвідченій особі) і за ефективністю іноді не гірше. Автономні системи відрізняються від мережевих тим, що вони не вміють створювати звіти про події, передавати інформацію про події на інший поверх і керуватися дистанційно [11].

При цьому автономні системи не потребують прокладання сотень метрів кабелю, пристроїв зв'язку з комп'ютером, а також самого комп'ютера. Це все пряма економія грошей, зусиль і часу при встановленні системи.

Щодо стійкості до зламу, "автономники" не поступаються мережевим системам, оскільки елементи, відповідальні за це - ідентифікатори, зчитувачі, запірні пристрої - в обох випадках можуть використовуватися ті самі. Звичайно,

є деякі винятки. При виборі автономної системи з високими вимогами до стійкості до в злому слід звернути увагу на наступні речі:

– зчитувач повинен бути відокремлений від контролера, щоб зовнішні ланцюги, за допомогою яких можливе відкриття замка, було недоступним, отже слід використовувати зчитувач в проти зламному виконанні;

– контролер повинен мати резервне джерело живлення на випадок тимчасового відключення мережі або навмисного вимкнення.

Деякі автономні системи мають функцію копіювання бази даних ключів. Це може бути корисним, якщо у вас є декілька дверей, в які входять ті самі люди, приблизно сотні або більше. Також, при великій кількості користувачів рекомендується використання контролера з розширеним індикатором, оскільки керування таким пристроєм є більш наочним і зручним. Різниця в ціні по відношенню до контролера зі світлодіодним і звуковим індикатором повністю оправдовується під час експлуатації.

Повністю завершений пристрій, призначений для обслуговування, зазвичай, одного контрольного пункту. Зустрічаються різноманітні варіації: контролери поєднані зі зчитувачем, контролери вбудовані в електромагнітний замок та інші. Автономні контролери розраховані на застосування різних типів зчитувачів. Зазвичай, автономні контролери призначені для обслуговування невеликої кількості користувачів, зазвичай до п'ятисот.

У мережевій системі всі контролери з'єднані між собою через комп'ютер, що надає багато переваг для великих систем, але це зовсім не потрібно для "домашньої" СКУД. Відносна вартість одного контрольного пункту в мережевій системі завжди вища. Крім того, для керування такою системою потрібен принаймні один кваліфікований спеціаліст. Проте, незважаючи на ці недоліки, мережеві системи є незамінними для великих об'єктів (офіси, виробничі підприємства), оскільки керувати навіть з десятком дверей, на яких встановлені автономні системи, стає головною болючою точкою. При потребі контролю над подіями, які відбувалися у минулому, або оперативний

додатковий контроль у реальному часі, тоді у мережевій системі працівник на прохідній може на моніторі бачити фотографію людини, яка щойно пред'явила свій ідентифікатор, що забезпечує захист від передачі карток іншим людям [12].

Забезпечуючи тісну взаємодію з іншими підсистемами безпеки (охоронною сигналізацією, відеоспостереженням), у мережевій системі з одного місця можна не тільки контролювати події на всій захищуваній території, але і централізовано керувати правами користувачів, швидко вносячи або видаляючи ідентифікатори. Всі мережеві системи мають можливість організувати декілька робочих місць, розподіливши функції керування між різними людьми та службами.

Слід звернути увагу на те, яку СУБД (систему управління базами даних) використовує розглянута СКУД. Якщо система невелика (кілька дверей, один комп'ютер, кілька сотень користувачів), то досить використовувати так звані "пласкі" СУБД, такі як Paradox, Access та подібні. Такі СУБД не вимагають великих ресурсів комп'ютера і є простими у використанні. Мережеві контролери використовують СКУД для створення будь-якого рівня складності. При цьому адміністрація отримує велику кількість додаткових можливостей. Крім простого дозволу або заборони проходу, зазвичай є такі можливості:

– отримання звіту присутності або відсутності співробітників на роботі;

– можливість миттєво дізнатися, де знаходиться конкретний співробітник;

– автоматичне ведення обліку робочого часу;

– отримання звіту про те, хто і куди ходив за будь-який період часу;

– можливість створити графік проходу співробітників, тобто хто, куди і в який час може ходити;

– можливість вести базу даних співробітників, в яку вноситься вся необхідна інформація про співробітників, включаючи їх фотографії;

– можливість розширення функціональності СКУД [13].

Точка проходу, обладнана спеціальними функціями. Особа, яка не пройшла через точку проходу, позначену як прохідна, не зможе потрапити в

будь-яке приміщення об'єкта. Зазвичай, саме час проходу через прохідну враховується при обрахунку робочого часу.

Фотоідентифікація (Photo ID) – це можливість виведення фотографії власника ідентифікатора (з бази даних) на екран комп'ютера, вона використовується на прохідних як додатковий захист від несанкціонованого проходу. Рішення про прохід може прийматися як автоматично, так і з підтвердженням від контролера на прохідній.

Кнопка "RTE" (Request To Exit) призначена для примусового дозволу перетину точки проходу, іншими словами, відкривання виконавчого пристрою, де факт відкриття фіксується в пам'яті контролера, але невідомо, хто саме пройшов. Такі кнопки встановлюються для забезпечення непошкодженого виходу з приміщень.

1.2 Принцип функціонування системи контролю та управління

Кожен співробітник, клієнт або відвідувач компанії отримує ідентифікатор (електронний ключ), тобто пластикову картку або брелок з індивідуальним кодом, що міститься в ньому. "Електронні ключі" видаються в результаті реєстрації вказаних осіб за допомогою засобів системи. Паспортні дані, фото та інші відомості про власника "електронного ключа" вносяться до персональної "електронної картки". Персональна "електронна картка" власника та код його "електронного ключа" пов'язуються один з одним та заносяться до спеціально організованих комп'ютерних баз даних [14,15].

Біля входу в будівлю або у контрольоване приміщення встановлюються зчитувачі, що зчитують код з карток та інформацію про права доступу власника картки, і передають цю інформацію до контролера системи.

У системі кожному коду ставиться у відповідність інформація про права власника картки. На основі порівняння цієї інформації та ситуації, коли була

пред'явлена картка, система приймає рішення: контролер відкриває або блокує двері (замки, турнікети), переводить приміщення в режим охорони, включає сигнал тривоги та інше.

Усі факти пред'явлення карток і пов'язані з ними дії (проходи, тривоги та інше) фіксуються в контролері і зберігаються в комп'ютері. Інформація про події, спричинені пред'явленням карток, використовується для подальшого отримання звітів щодо обліку робочого часу, порушень трудової дисципліни та інших. На підприємствах можна виділити чотири характерні точки контролю доступу: прохідні, офісні приміщення, приміщення особливої важливості та в'їзди/виїзди автотранспорту. Залежно від поставленої перед вами задачі, ви можете обрати відповідну систему контролю та управління доступом.

Невелика система контролю та управління доступом дозволить запобігти доступ небажаних осіб і точно вказати співробітникам ті приміщення, до яких вони мають право доступу.

Складніша система дозволить, крім обмеження доступу, призначити кожному співробітникові індивідуальний графік роботи, зберегти та потім переглянути інформацію про події за день. Системи можуть працювати в автономному режимі або під керуванням комп'ютера.

Комплексні системи контролю та управління доступом дозволяють вирішити питання безпеки та дисципліни, автоматизувати кадровий та бухгалтерський облік, створити автоматизоване робоче місце охоронця.

1.3 Класифікація систем контролю та управління доступом

Класифікація системи КУД за способом бувають:

– автономні - для управління однією або кількома точками управління без передачі інформації до центральної панелі та без контролю з боку оператора;

– централізовані (мережеві) - для управління точками управління з обміном інформацією з центральною панеллю та контролем та управлінням системою з боку оператора;

– універсальні - що включають функції як автономних, так і мережевих систем, які працюють в мережевому режимі під керуванням центрального пристрою управління і переходять в автономний режим при виникненні відмов у мережевому обладнанні, в центральному пристрої або при обриві зв'язку [16].

За кількістю контрольованих точок доступу системи КУД бувають:

– малої ємності (менше 16 точок);

– середньої ємності (не менше 16 і не більше 64 точок);

– великої ємності (64 точки і більше).

За функціональними характеристиками системи КУД бувають 3 видів:

– системи з обмеженими функціями;

– системи з розширеними функціями;

– багатофункціональні системи.

У системи будь-якого класу можуть бути введені спеціальні функції, які визначаються додатковими вимогами замовника. За видом об'єктів контролю системи КУД можуть бути:

– для контролю доступу до фізичних об'єктів;

– для контролю доступу до інформації.

Засоби КУД класифікуються за стійкістю до надзвичайних ситуацій та визначаються трьома рівнями стійкості до руйнування та неруйнівного впливу:

– нормальний;

– підвищений;

– високий.

ППУ (перешкод жувальні пристрої управління) та ПВІО (пристрої введення ідентифікаційних ознак) класифікуються за стійкістю до руйнувального впливу. Стійкість ППУ встановлюється за такими параметрами:

– стійкість до злому;

– кулестійкість;

– стійкість до вибуху.

Стійкість ПВІО встановлюється за стійкістю зчитувача до злому. Для ППУ з підвищеною та високою стійкістю додатково встановлюються 5 класів за показниками стійкості (1-й клас - найнижчий).

За стійкістю до неруйнівного впливу засоби та системи КУД залежно від їх функціонального призначення класифікуються за наступними параметрами:

– стійкість до відкриття;

– стійкість до маніпулювання;

– стійкість до спостереження;

– стійкість до копіювання (для ідентифікаторів);

– стійкість захисту засобів обчислювальної техніки.

Основні компоненти мережевої багатофункціональної системи контролю доступу показані на малюнку (рисунок 1.5).

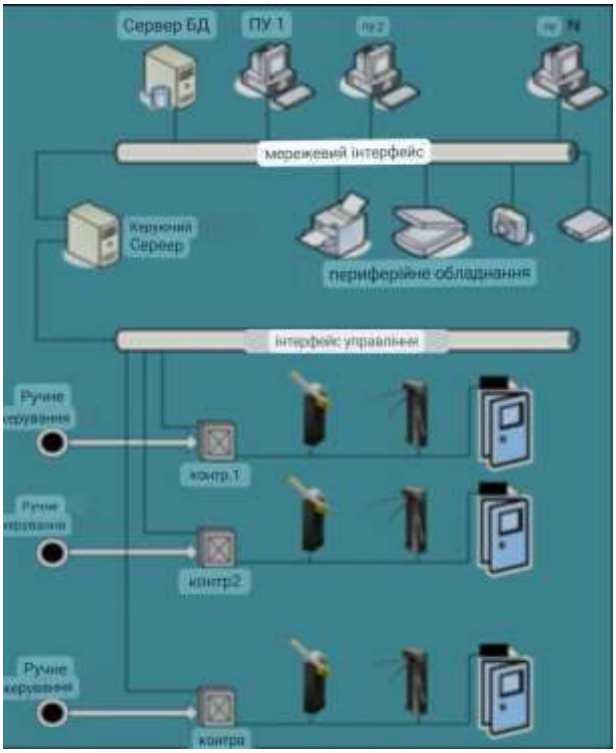


Рисунок 1.5 – Компоненти мережної багатофункціональної системи контролю доступу

На малюнку зображено найбільш загальний варіант СКУД. Всі процеси в системі контролюються керуючим сервером. Керуючий сервер підключений до сервера бази даних, пультів управління ПУ 1 - ПУ N, периферійного обладнання, такого як принтери для друку звітів або пластикових карт, модеми, сканери, фотокамери, по мережі. З іншого боку, керуючий сервер контролює стан всіх контролерів, а отже, усього обладнання для ідентифікації та ПВІО. Зв'язок здійснюється за допомогою певних протоколів, які відрізняються від виробника до виробника, як правило, через інтерфейси RS-232 і RS-485. Контролери пов'язані з виконавчими пристроями (шлагбаумами, турнікетами, електромеханічними замками і т.д.) та пристроями ідентифікації (проксиміті зчитувачами, ключами touch memory, біометричними ідентифікаторами).

Передбачене ручне керування системами здійснюється за допомогою пультів, які зазвичай розташовуються на точках входу на об'єкт. Ця схема може змінюватися в залежності від виробника обладнання.

Робота системи відбувається наступним чином. Вхідний пристрій, наприклад, підходить до пристрою ідентифікації (турнікету) і ідентифікується в системі, прикладаючи картку проксиміті (ключ touch memory), введенням коду або використанням біометричних даних до зчитувача, який зазвичай знаходиться поруч з турнікетом (на малюнку зчитувачі не показані). Далі контролер відділення, отримавши інформацію від зчитувача, перевіряє унікальний ідентифікатор у пам'яті бази даних, а також надсилає запит до керуючого сервера, який, у свою чергу, звертається до сервера бази даних. Якщо такий ідентифікатор існує в системі, то контролер замикає реле або сухі контакти, підключені до конкретного турнікету, і відчиняє його, а керуючий сервер передає інформацію на ПК служби. Крім того, на екрані пульта управління, прикріпленого до відповідної точки входу, відображається інформація про власника ідентифікатора (посада, рівень доступу, фотографія тощо), ця інформація призначена для працівників служби охорони, які контролюють дану точку входу. Крім того, інформація про вхід працівника або

гостя в дану годину фіксується в журналі подій системи. При виході працівника процес відбувається аналогічним чином, тільки з іншого боку входу.

Для отримання принципової схеми простіших систем контролю доступу достатньо виключити частину обладнання з наведеної схеми (наприклад, можна залишити лише контролер відділення, турнікет зі зчитувачем і пульт управління, така комбінація реалізує схему автономної однорівневої системи контролю доступу) [17].

Найпростішою системою контролю доступу є добре відомий домофон. В деяких випадках він інтегрується з системою відеоспостереження, у такому випадку користувач отримує відеодомофон.

1.4 Постановка задачі

Розробити і впровадити систему контролю доступу на основі Bluetooth технології в юридичному офісі з метою запобігання витоку конфіденційної інформації та забезпечення безпеки даних клієнтів.

У юридичному офісі інформація про клієнтів та конфіденційні дані є надзвичайно важливими та чутливими. Щоб забезпечити безпеку цих даних, потрібна система контролю доступу, яка обмежує фізичний доступ до приміщень та пристроїв, що містять ці дані.

Bluetooth технологія виявляється досить надійним та зручним рішенням для систем контролю доступу. Головною перевагою є відсутність необхідності використовувати фізичні ключі або картки доступу, що можуть бути загублені або скомпрометовані. Замість цього, користувачі матимуть змогу використовувати свої мобільні пристрої з підтримкою Bluetooth для отримання доступу до визначених зон офісу.

З метою з'ясування вимог до рішення проблеми системи контролю доступу від витоку інформації на основі Bluetooth-технологій потрібно вирішити такі завдання:

- аналіз потреб та вимог юридичного офісу щодо СКД;
- розробка СКД на основі Bluetooth технології;
- визначення рівнів та зон доступу в офісі відповідно до потреб безпеки;
- встановлення Bluetooth-сумісних замків та датчиків доступу в приміщеннях офісу;
- впровадження СКД в юридичному офісі з відповідним навчанням персоналу та розподілом необхідних пристроїв.

2 ПРОЄКТУВАННЯ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ НА ОСНОВІ BLUETOOTH-ТЕХНОЛОГІЇ

2.1 Аналіз інформаційної безпеки офісу

При розробці проєктних рішень системи контролю доступу на основі Bluetooth-технології було обрано офіс - юридичного агентства «Воля»

Розглянемо план офісу юридичного агентства «Воля» (рисунок 2.1).

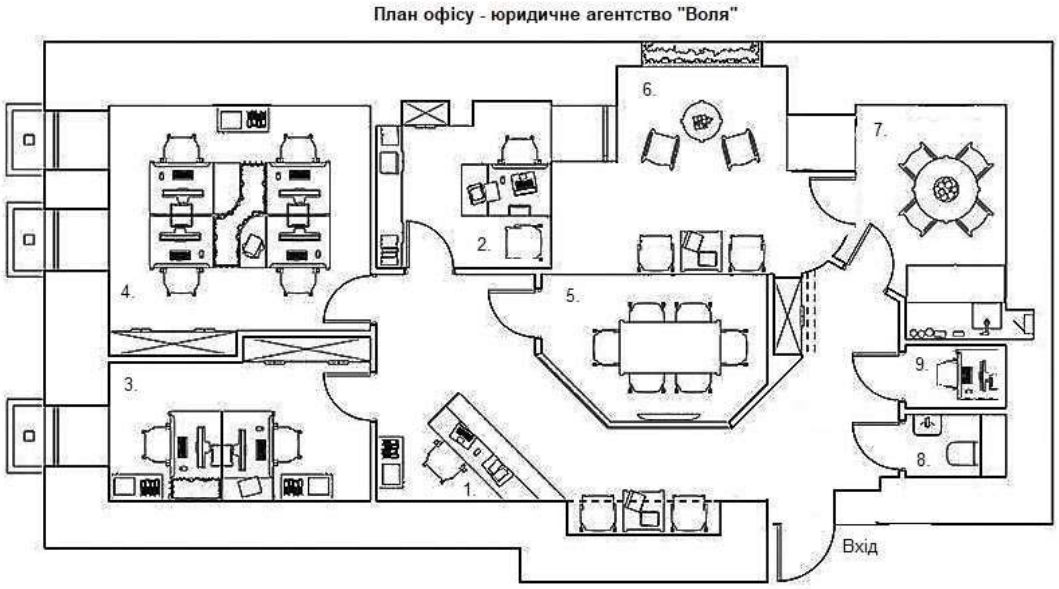


Рисунок 2.1 – План офісу

Офіс юридичного агентства «Воля» складається з дев’яти приміщень:

- куток консультанта, хол (1);
- кімната керівника (2);
- кімната спеціалістів (бухгалтер, кадровик) (3);
- кімната юристів (4);
- конференц-зал (5);
- кімната відпочинку (6);
- кухня (7);
- вбиральня (8);

– серверна (9).

Проведемо повний аналіз, за наявністю секретності документів у кожному приміщені офісу. За даними отриманими від керівництва офісу.

Куток консультанта в юридичному офісі є робочим місцем, де він займається організаційними та адміністративними завданнями. Тут можна знайти різні електронні пристрої та обладнання, які сприяють ефективності його роботи. Консультант має особистий ноутбук для виконання різноманітних завдань, включаючи обробку даних, складання листів, підготовку документів та розкладу зустрічей; телефон, що дозволяє здійснювати телефонні дзвінки, переговори з клієнтами та іншими особами. У разі потреби в обміні документами, секретар має доступ до факсу або використовує програмне забезпечення. Консультант відповідає за вхід клієнтів. Консультант працює з клієнтами та різними видами інформації які потребують захисту це:

– службова інформація це електронна пошта, інтернет переписка, протоколи зустрічей;

– юридичні документи це договори, листи, судові рішення;

– дані клієнтів це імена, адреси, контактні дані, заяви, довідки.

В кімнаті керівника знаходиться ноутбук, який обробляє юридичні дані, готує юридичні документи; телефон, який дозволяє здійснювати дзвінки, відправляти повідомлення та керувати різними аспектами комунікації в офісі, а також інформації на флешках і т.д., яка зберігається у спеціальному сейфі. Керівник юридичного офісу займається різними видами інформації які потребують захисту це:

– конфіденційна інформація це справи клієнтів, документи про власність, конфіденційні листи, договори, електроні листи, угоди з партнерами;

– юридичні документи це документи досудового розслідування, кримінальні справи, свідчення свідків, висновки експертів;

– корпоративна інформація це кадрова інформація, внутрішні інструкції, копії документів, угоди про не розголошення;

– персональні дані це дані клієнтів, імена, адреса, договори;

– конкурентна інформація це плани розвитку бізнесу, фінансові угоди.

Кімнату спеціалістів розділяють бухгалтер та кадровик. Бухгалтер в юридичному офісі займається фінансовими аспектами діяльності організації, тут є різні електронні пристрої та обладнання, які сприяють обробці фінансової інформації та веденню бухгалтерського обліку.

Це комп'ютер для виконання різних завдань, таких як облік фінансових операцій, розрахунок заробітної плати та оподаткування. Також бухгалтер використовує спеціалізоване програмне забезпечення для ведення бухгалтерського обліку, обробки фінансових транзакцій, складання звітів і аналізу фінансової інформації, часто використовує електронні таблиці, наприклад, Microsoft Excel або Google Sheets.

Бухгалтер використовує системи електронного документообігу для зберігання та обробки фінансових документів, таких як рахунки, квитанції, договори тощо, займаються різними видами інформації що потребують захисту це:

– конфіденційна інформація це фінансові документи, бухгалтерські документи, банківські виписки;

– персональні дані співробітників це платіжні дані, платіжні реквізити, бюджет офісу;

– інформаційна безпека це податкова декларація, звіти, виписки.

Кадровик у юридичному офісі здійснює роботу з персоналом, зберігає документи та виконує різні адміністративні завдання. Кадровик користується комп’ютером, телефоном, принтером для виконання різних завдань, введення кадровик записів, складання звітів. Зберігає велику кількість документів, такі як: трудові договори, заяви, персональні файли співробітників. Кадровик працює з різними видами інформації які потребують захисту це:

– персональні дані співробітників це трудові договори, резюме персоналу, контактні дані, адреса;

– системи кадрового обліку це звіти та статистика, угоди працевлаштування, резюме.

Юристи використовують комп'ютери для проведення досліджень, написання правових документів, складання договорів та аналізу юридичної інформації, мають доступ до спеціалізованого юридичного програмного забезпечення, яке допомагає в управлінні документами, проведенні досліджень, створенні шаблонів документів, до юридичних баз даних, електронних журналів, судової практики та інших джерел юридичної інформації для досліджень та оновлення своїх знань, а також використовують електронну пошту, месенджери та інші комунікаційні засоби для спілкування з клієнтами, колегами та іншими сторонами, що стосуються юридичних питань.

Юристи користуються сканерами та принтерами для створення копій та друкування юридичних документів та надання звітів клієнтам або судовим органам, а також мають цифрові архіви для зберігання та керування документами, що дозволяє швидкий доступ до раніше створених документів та інформації у офісі. Вони працюють з різними видами інформації, що потребують захисту:

– конфіденційна клієнтська інформація це справи клієнтів, свідчення свідків, докази, розмови адвокат клієнт, електроні документи;

– юридичні документи це юридичні дослідження та договори, декларації, конфіденційні листи, документи про власність, копії даних;

Конференц-зал у юридичному офісі є місцем для зустрічей, нарад, презентацій та інших комунікаційних заходів. В цьому приміщенні розташовані різні електронні пристрої, які допомагають забезпечити ефективну комунікацію та обмін інформацією.

У серверній кімнаті є обладнання та інфраструктура, які забезпечують функціонування і збереження даних в офісі. Основні компоненти, що знаходитися в серверній кімнаті: сервери, мережеві пристрої, система резервного живлення, контроль доступу. Ці компоненти допомагають

забезпечити безпеку, надійність та доступність даних в офісі, а серверна кімната є центральним місцем для їх розміщення та управління.

Кімната відпочинку в юридичному офісі є приміщеннями, де співробітники можуть розслабитися, відпочити і зарядитися енергією. Вона часто призначені для надання комфорту та зручності під час перерв у роботі.

Кухня в юридичному офісі є спільним приміщенням, де співробітники готують їжу, щоб пообідати і відпочити під час робочого дня. Кухня обладнана різними зручностями та електронними приладами, щоб забезпечити зручність і комфорт працівників. Загальною метою є створення безпечного середовища в кухні офісу.

При вході у офіс знаходиться хол для очікування клієнтів, він з’єднаний з кутком консультанта для кращого спілкування з клієнтами, та обладнаний зручними кріслами, тут клієнти можуть ознайомлюватися різними видами інформації, такі як: зразки заяв і договорів, публічні звіти, офіційні публікації, рекламні брошури.

У агентстві знаходяться такі електроні пристрої як: комп’ютерів - 7 шт., ноутбуків – 2 шт., принтерів – 3шт., сканерів – 4 шт., сервер – 1шт., система для відео-конференцій – 1 шт. Уся документація та обладнання потребують безпеки контролю доступу. Інформація була отримана при опитуванні керівника агентства та його персоналу. Юридичний офіс «Воля» складається з десяти працівників персоналу (табл 2.1).

Розділимо інформацію у юридичному офісі на чотири категорії: секретна інформація, конфіденційна інформація, службова інформація, загальнодоступна інформація. Секретна інформація відноситься до надзвичайно конфіденційних даних, які мають особливий статус і захищені спеціальними правилами та обмеженнями доступу. Конфіденційна інформація включає широкий спектр даних, що пов'язані з клієнтами, внутрішніми справами та діловою діяльністю офісу. Службова інформація у юридичному офісі включає дані, що стосуються внутрішньої діяльності та організації офісу [18].

Більш детальний опис видів інформації які потребують захисту у юридичному агентстві «Воля» (табл 2.2).

Таблиця 2.1 – Персонал юридичного агентства «Воля»

Персонал	Кількість осіб	Приміщення
Консультант	1	Хол
Керівник	1	Кімната керівника
Юристи	4	Кімната юристів
Бухгалтер	1	Кімната спеціалістів
Кадровик	1	Кімната спеціалістів
Адміністратор	1	Серверна
Прибиральниця	1	Приміщення офісу

В юридичному офісі існує кілька потенційних ризиків витоку інформації, особливо коли йдеться про конфіденційні дані клієнтів і юридичні документи.

Юридичний офіс може стати метою хакерів і зловмисників, які намагаються отримати доступ до конфіденційної інформації. Недостатня кібербезпека, слабкі паролі, вразливі мережеві з'єднання або недостатнє оновлення програмного забезпечення може зробити юридичний офіс легкою мішенню для кібератак. Цей офіс має велику кількість паперових документів, які можуть бути викрадені або загублені, і це може стати причиною витоку конфіденційної інформації, та недостатньо захищених фізичних копій документів. Іноді найбільш значущими загрозами є внутрішні зловживання або недбалість співробітників. Це включає неправильне використання конфіденційної інформації, незахищене зберігання даних або неправильне видалення документів [19].

Таблиця 2.2 – Види інформації у сфері агентства

Види інформації	Повний опис інформації
Секретна	1) Привілейована інформація: розмови адвокат-клієнт, листування. 2) Секрети досудового розслідування: кримінальні справи, свідчення свідків, докази, висновки експертів, письмові заяви. 3)Секрети ділової та комерційної прихованості: плани розвитку бізнесу, фінансові угоди, допомога військовим, документи ЗСУ
Конфіден-ційна	1)Інформація про клієнтів: імена, адреси, контактні дані, фінансові дані. 2)Юридична інформація: справи клієнтів, договори, судові рішення, документи про власність, додаткові декларації, конфіденційні листа, документи про власність. 3)Внутрішні документи офісу: електроні листи, внутрішня комунікація, замітки, протоколи зустрічей, файлові документи, база даних. 4)Фінансова інформація: бухгалтерські документи, платіжні реквізити, банківські виписки, бюджет офісу. 5)Комерційна інформація: бізнес плани, розробки, ринкові дослідження, угоди з партнерами.
Службова	1)Внутрішні документи і комунікації: електронна пошта, інтернет переписка, протоколи зустрічей, документи агентства, плани дій, звіти. 2)Кадрова інформація: резюме, контактна інформація, копії документів, угоди, угоди праце влаштування, угоди про нерозголошення інформації. 3)Бухгалтерські та фінансові записи: звіти, бюджети, виписки, податкова декларація, платіжні документи. 4)Технічна інформація: комп’ютерна мережа, системи безпеки, інфраструктура офісу, технічні обладнання, ліцензії програмного забезпечення.
Загального доступу	1)Законодавчі акти: закони, постанови, розпорядження, зразки заяв, зразки договорів. 2)Публічна інформація: публічні звіти, рішення судів, веб-сайти, офіційні публікації. 3)Дозвілля: брошури, газети, журнали, реклами.

2.2 Система контролю доступу

Системи контролю доступу (СКД) - це ефективний спосіб запобігання несанкціонованому проникненню недозволених осіб на територію підприємства та забезпечення контролю над доступом працівників до приміщень. Зазвичай СКД використовується як частина комплексної системи безпеки, разом з відеоспостереженням і охоронною сигналізацією.

Загалом застосування Bluetooth-технології у системі контролю доступу може допомогти забезпечити безпеку інформації і запобігти її несанкціонованому розповсюдженню.

Однією з найбільш важливих проблем в області інформаційної безпеки є захист від витоку інформації. Витік інформації стає причиною серйозних фінансових втрат, порушенням конфіденційності та приватності, та завдає шкоди репутації компанії. Щоб запобігти витоку інформації необхідно застосовувати системи контролю доступу [20].

Виділимо ступінь секретності інформації в юридичному офісі, що є особливо важливим, оскільки там зберігається конфіденційна клієнтська інформація та юридичні документи. Основні рівні секретності, які можуть застосовуватися в юридичному офісі, налічують п’ять зон.

Перша – це зона суперсекретності, яка використовується для дуже конфіденційних справ, таких як документи, пов'язані з розслідуваннями, злочинами або корпоративними секретами. Вона може бути додатково захищеною фізичною охороною, електронними системами контролю доступу та іншими високотехнологічними заходами безпеки.

Друга – це зона високої секретності, яка призначена для зберігання особливо конфіденційної інформації, такої як приватні дані клієнтів, важливі судові документи або інші чутливі матеріали. Вона може бути фізично обмеженою, забезпеченою високим рівнем безпеки та доступу тільки для обмеженого кола авторизованих працівників.

Третя – це зона обмеженого доступу, яка призначена для працівників офісу і містить конфіденційні документи та інформацію, що стосується клієнтів. Доступ до цієї зони обмежений лише авторизованим працівникам і вимагати використання ідентифікаційних карток або паролів доступу.

Четверта – це конфіденційна зона, де відпочиває персонал. У цій зоні розміщуються загальні матеріали, які можуть бути доступні для перегляду, такі як журнали, книги або публічно доступні документи.

П’ята – це відкрита зона, де знаходиться загальна інформація, доступна всім працівникам і відвідувачам офісу. На цьому рівні можуть бути розміщені загальнодоступні документи, журнали, брошури, афіші та інші не конфіденційні матеріали (рисунок 2.2).

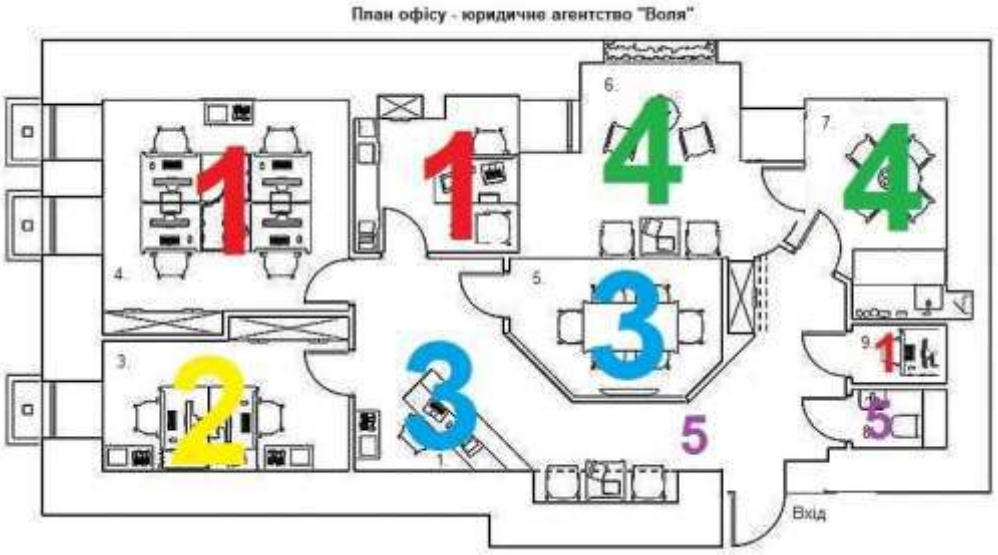


Рисунок 2.2 – Ступінь секретності інформації зон у офісі

Система контролю доступу визначає, кому дозволено входити або виходити, де їм дозволено входити або виходити, куди їм дозволено входити або виходити, а також коли їм дозволено це робити. В цьому контексті "їм" означає осіб, які мають перепустку або право доступу, тоді як тим, хто не має пропуску, не потрібно хвилюватись про питання щодо де, куди і коли входити або виходити. Система контролю доступу встановлює параметри доступу та

виконує контроль за їх дотриманням, забезпечуючи безпеку та обмежуючи доступ лише для авторизованих осіб [21].

Юридичне агентство «Воля» складається з 9 працівників усього персоналу, які мають: повний, обмежений і частково-обмежений доступ до кімнат у офісі (табл. 2.3).

Таблиця 2.3 – Режим доступу до приміщень

Персонал	Кількість	Кімнати	Доступ
1	2	3	4
Консультант	1	Куток консультанта, конференц-зал, кухня, кімната відпочинку, вбиральня, хол	Повний
		Кімната керівника, кімната юристів, серверна	Обмежений
		Кімната спеціалістів	Частково-обмежений
Керівник	1	Кімната керівника, конференц-зал, кухня, кімната відпочинку, вбиральня, хол	Повний
		Кімната юристів, серверна, кімната спеціалістів	Обмежений
		Куток консультанта	Частково-обмежений

Продовження таблиці 2.3 ,

1	2	3	4
Бухгалтер	1	Кімнати спеціалістів, конференц-зал, кухня, кімната відпочинку, вбиральня, хол	Повний
		Кімната керівника, кімната юристів, серверна	Обмежений
		Куток консультанта	Частково-обмежений
Кадровик	1	Кімнати спеціалістів, конференц-зал, кухня, кімната відпочинку, вбиральня, хол	Повний
		Кімната керівника, кімната юристів, серверна	Обмежений
		Куток консультанта	Частково-обмежений
Юристи	4	Кімната юристів, конференц-зал, кухня, кімната відпочинку, вбиральня, хол	Повний
		Кімната керівника, кімната спеціалістів, серверна	Обмежений
		Куток консультанта	Частково-обмежений
Адміністратор	1	Серверна, кухня, кімната відпочинку, вбиральня, хол	Повний
		Кімната керівника, кімната юристів, кімната спеціалістів	Обмежений
		Куток консультанта, конференц-зал	Частково-обмежений

Закінчення таблиці 2.3

1	2	3	4
Прибиральниця	1	Кухня, кімната відпочинку, вбиральня, хол	Повний
		Кімната керівника, кімната юристів, серверна, кімната спеціалістів	Обмежений
		Куток консультанта, конференц-зал	Частково-обмежений
Клієнти	-	Вбиральня, хол	Повний
		Кімната керівника, кімната юристів, серверна, кімната спеціалістів, конференц-зал, кухня, кімната відпочинку,	Обмежений
		Куток консультанта	Частково-обмежений

Загальний доступ до інформації у юридичному офісі означає, що ці дані можуть бути доступні всім співробітникам та клієнтам офісу без обмежень.

Щодо електронного контролю доступу, використаємо потужність комп’ютерів для розв'язання проблем, пов'язаних з обмеженнями, які накладаються механічними замками та ключами. Електронна система визначає, чи можна отримати доступ до захищеної області, базуючись на наданому дозволу. Якщо доступ дозволений, двері відчиняються на певний час, і ця подія буде записана в системі. Якщо доступ відхилено, двері залишаються закритими, а спроба доступу також фіксується. Система також наглядатиме за дверима і викличе тривожний сигнал, якщо двері будуть відкриті з використанням сили або залишатимуться відчиненими протягом тривалого часу. Основною точкою контролю доступу є двері, де доступ контролюється за допомогою магнітних замків та зчитувачів карток (рисунок 2.3).

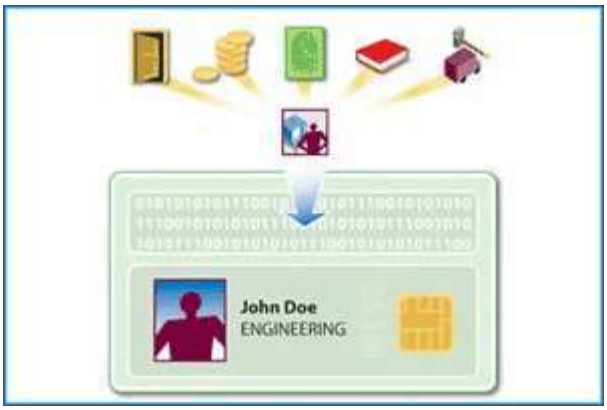


Рисунок 2.3 – Зчитувачі магнітних смуг

Взаємодія користувача з системою контролю доступу - це використання зчитувача смарткарт. Вибір зчитувача залежить від типу смарткарти, що використовується. Зчитувачі для безконтактних смарткарт, як правило, є радіопередавачами. Широкомовне поле зчитувача активує картку, яка починає передавати радіосигнал зчитувачу. Біометричні зчитувачі використовують унікальні технології і завжди потребують від користувача пред'явлення частини свого тіла, таких як відбитки пальців, геометрія руки, розпізнавання обличчя, райдужна оболонка та сітківка ока, або голосове розпізнавання за допомогою мікрофона та інше.

Просто кажучи, людина, яка має право на доступ до приміщень (перепустку), пред'являє свою смарткарту системі (підносить до безконтактного зчитувача), і двері можуть відкритися або залишитися закритими. У будь-якому випадку така подія автоматично реєструється в системі контролю доступу.

Устаткування контролю доступу від ZKTeco є ідеальним вибором для будівництва систем безпеки, як для невеликих офісів з однією точкою входу, так і для великих організацій з багатьма точками доступу, що розташовані не лише у межах однієї будівлі, а й у різних містах. Біометричні та безконтактні зчитувачі, термінали і замки ZKTeco забезпечують безпечний доступ до приватних будинків, квартир і офісів, а також забезпечують безпеку фізичної особи та підприємства. Їх можна використовувати для доступу за допомогою

безконтактних карток, кодів, відбитків пальців, образів обличчя або комбінації цих методів [22,23].

На базі обладнання ZKTeco можна побудувати типи обладнання СКД:

– термінали доступу (рисунок 2.4);

а) б)

Рисунок 2.4 – Термінали доступу:

а) термінал доступу відбитків пальців; б) термінал доступу безконтактних карт

– контролери доступу та зчитувачі (рисунок 2.5);

а) б) в) г)

Рисунок 2.5 – Контролери доступу та зчитувачі:

а) біометричний контролер; б) біометричний зчитувач; в) контролер доступу; г) зчитувач безконтактних карток

– автономні електроні замки (рисунок 2.6).

а) б)

Рисунок 2.6 – Автономні електроні замки:

а) замок відбитків пальців; б) замок безконтактних карт

Інші користування системою СКД:

– безконтактна картка, код доступу, відбиток пальця, образ обличчя, мульті ідентифікація;

– автономні-програмування пристрою біля точки проходу за допомогою майстер карти; мережеві створення мережі пристроїв доступу при керуванні програмного забезпечення; універсальні – поєднання можливостей автономних та мережевих систем;

– RS485, Ethernet, WiFi, GPRS;

– для внутрішнього застосування, для вулиці.

Для юридичного агентства «Воля» оберемо системи контролю доступу ZKTeco, що базується на різних пристроях, таких як контролери та зчитувачі, а також автономні електронні замки. Ці системи призначені для обмеження доступу сторонніх осіб до приміщень. Щоб увійти в контрольовану зону, потрібно мати ідентифікатор користувача, яким може бути безконтактна карта, відбиток пальця, код доступу або образ обличчя. Система порівнює пред'явлений ідентифікатор з базою ключів, яка зберігається в пам'яті системи. Якщо ідентифікатор співпадає з одним з ключів у базі, система відкриває замок для доступу до контрольованої зони. Крім того, система може надавати користувачам різні гнучкі права доступу, використовуючи такі параметри, як часові зони, групи доступу і комбінації розблокування. Це дозволяє

забезпечити точний та контрольований доступ до різних зон і приміщень для різних користувачів.

Для забезпечення безпечного пропуску використовуються контролери доступу, які знаходяться всередині приміщення. При вході встановлюється зчитувач, який передає ідентифікатор користувача для порівняння на контролері. Інтелектуальні IP контролери доступу дозволяють створювати комплексні системи безпеки, які інтегруються з відеоспостереженням, охоронною та пожежною сигналізацією (рисунок 2.7).

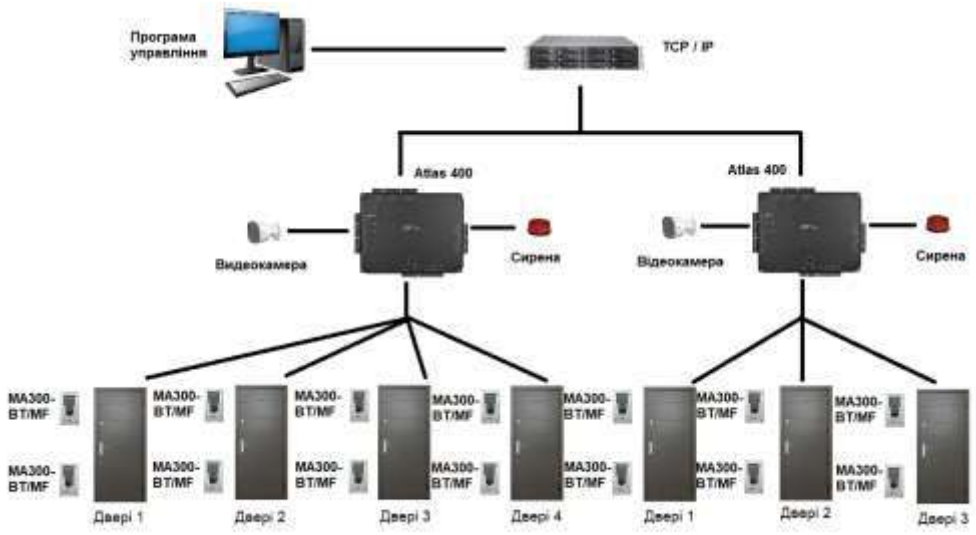


Рисунок 2.7 – Побудова СКУД на базі контролерів доступу

Автономний електронний замок є оптимальним рішенням для обмеження доступу до окремих дверей. Його встановлення займає мінімум часу, і замок живиться від пальчикових батарейок. Вхід у приміщення здійснюється за допомогою ідентифікатора користувача, а вихід можна здійснити шляхом натискання ручки замка вниз. В комплекті поставки вже міститься все необхідне для використання безконтактної картки або відбитка пальця для доступу користувача.

Одним з основних компонентів СКУД є електронні замки, один з них розташований на вхідних дверях офісу. Ці замки управляються з

використанням різних методів доступу за допомогою технології Bluetooth це - картки доступу, біометричні дані (відбитки пальців), пін-коди. Що забезпечує контроль над тим, хто має дозвіл на вхід до приміщення (рисунок 2.8).

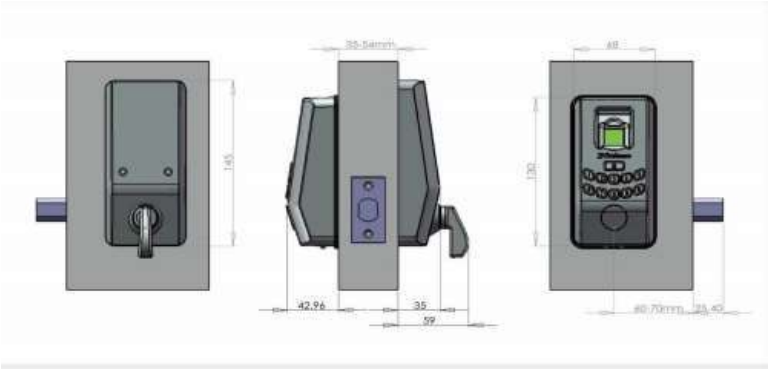


Рисунок 2.8 – Побудова СКУД на базі автономних електронних замків

2.3 Захист інформації за допомогою різних пристроїв

Система контролю доступу від витоку інформації – це є сукупність заходів, що спрямовані на захист конфіденційної інформації від несанкціонованого доступу. Один з цих заходів – це є забезпечення фізичної безпеки об'єкта, який містить конфіденційну інформацію [24,25].

Для вирішення проблем пов’язаних із захистом інформації підготовлене віповідне обладнання, яке необхідне для реалізації системи контролю доступу на основі Bluetooth-технологій розмістимо у цьому офісі це - комп’ютер, сервер, контролери, зчитувачі з відбитком пальця, зчитувачі карт, камери відеоспостереження, розумні замки, електроні замки, сигналізація.

Детально опишемо місцезнаходження приладів СКУД у приміщені юридичного офісу (рисунок 2.9-2.10).

Система відеоспостереження у офісі, складається з цифрових камер, обладнаних датчиками руху, моніторів і записувачів. Камери цифрові, з різними конструктивними особливостями. Вони застосовуються як для

внутрішніх, так і для зовнішніх приміщень. Системи можуть працювати цілодобово, записувати за рухом або на заданий графік. Камери можуть бути видимими або прихованими залежно від потреби. Зйомки можуть відстежуватися віддалено через IP-камери та системи моніторингу, або записані для зберігання [26].

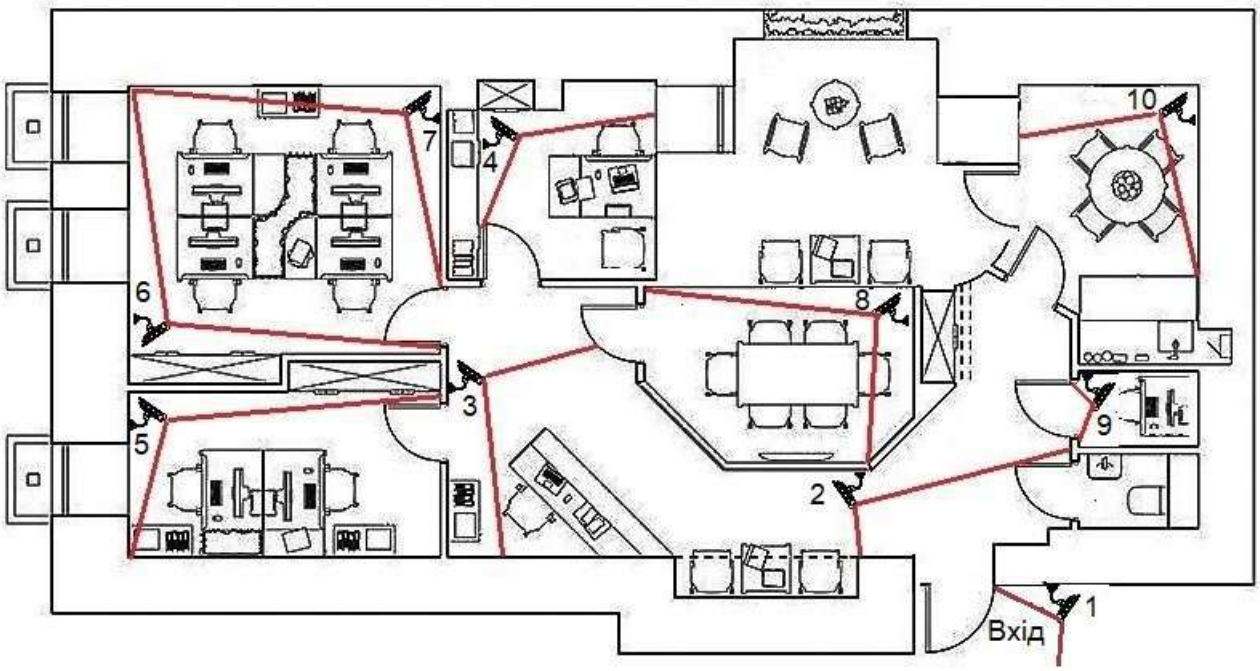


Рисунок 2.9 – Відеоспостереження у офісі

Додатковою складовою СКУД є система контролю та моніторингу, яка включає в себе десять камер відеоспостереження. Це дозволяє в реальному часі відслідковувати активність людей та забезпечення конфіденційності інформації у офісі, а також записувати відео або фотографувати для аналізу безпеки.

На плані юридичного офісу позначимо схематично обладнання для захисту інформації.

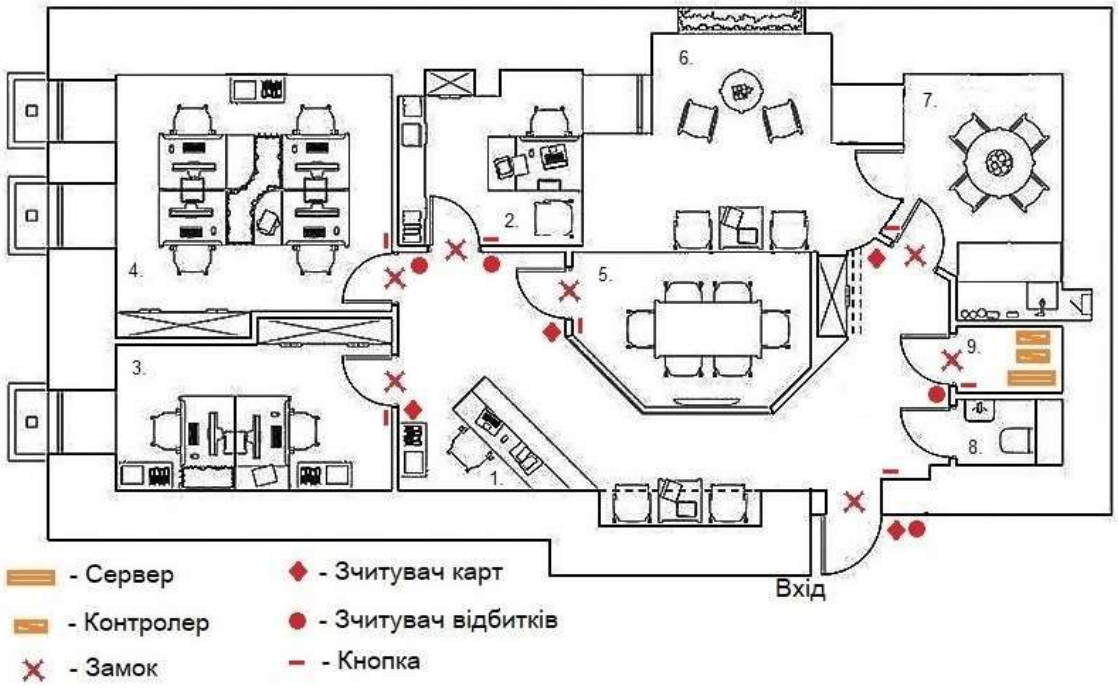


Рисунок 2.10 – Схематичне позначення пристроїв

Вхід у офіс надійно охороняється, тобто обладнаний камерою відеоспостереження №1, яка встановлена на стіні з права біля вхідних дверей. Та надійний електричний смарт-замком, що вмонтований у двері, та зчитувач відбитку пальців, який розміщений на стіні з права від дверей. При вході у офіс знаходиться кнопка дзвінка, мелодія якого, повідомляє консультанта про прихід клієнтів. За допомогою камерами відеоспостереження консультант відкриє двері використовуючи технологією Bluetooth у смартфоні. У холі на стіні навпроти вхідних дверей також розміщена камера відеоспостереження №2 на висоті 2.5 метрів, для максимального огляду входу та виходу офісу.

За місцем роботи консультанта ведеться відеоспостереження, камера №3 розташована на стіні, між кімнатами юристів та спеціалістів, на висоті 2.5 метрів, для кращого спостереження, та забезпечення захисту інформації консультанта та клієнтів. Вхід у зону консультанта має третій ступінь секретності інформації, тому вхід у цю зону частково-обмежений, що забезпечує безпечне зберігання інформації проектів, клієнтів та іншої конфіденційної інформації.

Для захисту інформації, у кабінеті керівника є камера відеоспостереження №4, яка розташована на стіні, у лівому куту навпроти дверей у кабінет на висоті 2.5 метрів, охоплюючи спектр бачення всієї кімнати, також є сейф з надійним кодовим замком, електронний смарт-замок вмонтований у двері кімнати, яким можна керувати на відстані, та сканер відбитку пальців що знаходиться на стіні при вході у кімнату. Кабінет керівника відноситься до першого ступеня секретності інформації, тому вхід обмежений.

Кімната спеціалістів обладнана камерою відеоспостереження №5, яка знаходиться в правому верхньому куті на висоті 2.5 метрів. Bluetooth смарт-замок вмонтований у двері кімнати спеціалістів. Кімната спеціалістів має другий рівень доступу тому вхід обмежений.

Кімната юристів обладнана двома камерами відеоспостереження. Камера №6 розміщена у верхньому лівому куті на висоті 2.5 метрів, а камера №7 – у верхньому правому куті на висоті 2.5 метрів, від вхідних дверей, для кращого огляду всієї кімнати, та захисту конфіденційної інформації. Вхід у кімнату захищений Bluetooth смарт-замком який вмонтований у двері та зчитувачем відбитків пальців розміщеним на стіні біля дверей. Ця кімната має перший ступінь секретності інформації, тому вхід у неї – обмежений.

У конференц-залі встановлена одна відеокамера №8, розміщена в лівому куті навпроти дверей на висоті 2.5 метрів, для спостереження захисних дій під час конференцій та засідань. Вхід у це приміщення захищений Bluetooth смарт-замком, який вмонтований у двері, та має третій ступінь секретності інформації тому вхід частково-обмежений.

Серверна, обладнана камерою відеоспостереження №9, яка розміщена в лівому верхньому куті від дверей на висоті 2.5 метрів, для постійного контролю у приміщені, та надійними Bluetoth смарт-замком, вмонтованими у двері, та зчитувачем відбитків пальців який розташований на стіні з права біля дверей. Тут знаходиться важливе обладнання для безпеки інформації тому ступінь захисту інформації перший, вхід - обмежений.

Кухня та кімната відпочинку об’єднані між собою звичайними дверима. Кімната відпочинку без відеоспостереження для спокійного відпочинку у обідню перерву, тому камера відеоспостереження №10 тільки у кухні розміщена у куті паралельно входу. Вхід у зону відпочинку обладнаний Bluetooth замком, що вмонтований у двері, для швидкого та зручного доступу у приміщення. Тут четвертий ступінь захисту інформації, тому вхід частковий тільки для персоналу.

Вбиральня обладнана пожежною сигналізацією, яка розміщена на потолку, від можливого випадку пожежі, та створення безпечного та комфортного середовища у вбиральні. Тут працівники можуть виконувати особисті гігієнічні процедури з максимальною безпекою та приватністю. Кімната вбиральні має п’ятий ступінь захисту інформації, вхід вільний для персоналу та клієнтів.

Офіс, обладнаний системою контролю доступу (СКУД), відзначається високим рівнем безпеки та контролю над доступом до приміщення. СКУД - це комплексна система, що включає в себе різні пристрої та технології такі як Bluetooth, для контролю та обліку вхідної та вихідної активності.

Аутентифікація користувачів у юридичному офісі важлива для забезпечення безпеки та конфіденційності інформації. Це процес перевірки ідентифікаційних даних користувача, щоб переконатися, що він є дозволеним користувачем і має доступ до необхідних ресурсів і систем [27,28].

Практичні кроки які буде використовувати персонал, для аутентифікації користувачів у юридичному офісі.

Кожен користувач буде мати унікальний ідентифікатор або обліковий запис, який містить інформацію про нього, наприклад, ім'я, посаду, електронну адресу тощо. Користувачам надаватимуться індивідуальні облікові записи з унікальними ідентифікаторами та паролями.

Застосується політика сильних паролів, яка вимагатиме від користувачів використовувати паролі, які складаються з комбінації великих і малих літер,

цифр і спеціальних символів. Регулярно нагадувати користувачам про необхідність зміни паролів і не допускати використання слабких або очевидних паролів при користувані.

Розглянемо можливість використання багатофакторної аутентифікації, що включає в себе використання двох або більше методів аутентифікації, це може бути поєднання пароля та одноразового коду, який надсилається на мобільний телефон користувача.

Встановимо рівні доступу та права для різних користувачів в залежності від їхніх обов'язків та потреб. Наприклад, адміністратор системи має повний доступ до серверної, тоді як юристам можуть бути надані обмежені права і т.п.

Використаємо систему моніторингу активності користувачів для виявлення незвичайних або підозрілих дій. Це може допомогти вчасно виявити спроби несанкціонованого доступу або порушення безпеки.

Навчимо користувачів методам безпеки, наприклад, про небезпеку використання одного й того ж пароля для різних систем, про фішингові атаки та інші загрози безпеці. Ці заходи будуть сприяти аутентифікації користувачів у юридичному офісі та безпеки їхньої інформації. Важливо регулярно переглядати та оновлювати ці заходи з урахуванням змін технологій та безпекових загроз (табл 2.4).

Таблиця 2.4 – Аутенфікації користувачів

Персонал	Приміщення	Ступінь доступу по зонах	Аутентифі-кація	Графік роботи
1	2	3	4	5
Адміністратор	Серверна	1	Відбиток пальця	8:00/17:00

Закінчення таблиці 2.4

1	2	3	4	5
Керівник	Кімната керівника	1	Відбиток пальця	8:00/17:00
Консультант	Куток консультанта	3	Картка	8:00/17:00
Юристи	Кімната юристів	1	Відбиток пальця	8:00/17:00
Бухгалтер	Бухгалтерія	2	Картка	8:00/17:00
Кадровик	Кадри	2	Картка	8:00/17:00
Прибиральниця	–	4, 5	Картка	12:00/14:00
Клієнти	–	5	–	–

2.4 Висновок

В розділі розроблена система контролю доступу від витоку інформації на основі Bluetooth-технології, що має функції контролю доступу до окремих зон офісу, а також систему відеоспостереження.

Наприклад, для обмеження доступу до важливих зон, таких як серверна кімната, кімната керівника і кімната юристів, вхід у ці приміщення на рівні «конфіденційний»:

– при вході є зчитувач відбитків пальців;

– система дозволяє забезпечити високий рівень безпеки для конфіденційної інформації та обмежити доступ лише до авторизованих осіб;

– електроні замки та зчитувачі відбитків пальців обладнані технологією Bluetooth, що досить зручно для потрапляння у приміщення;

– все приміщення обладнане камерами відеоспостереження у реальному часі що теж є важливою складовою СКУД.

Враховуючи всі ці складові, юридичне агентство, обладнане СКУД, можна описати як сучасний, безпечний та контрольований простір, де доступ до приміщення і окремих зон обмежений та контрольований. Це допомагає забезпечити захист приміщення, даних та ресурсів компанії, а також забезпечити безпеку співробітників і відвідувачів.

3 ПОЛІТИКА БЕЗПЕКИ КОРИСТУВАННЯ СИСТЕМОЮ ТА ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ

3.1 Інструкція з експлуатації системи

Для системи контролю доступу із захистом від витоку інформації на основі Bluetooth-технології я використав такі пристрої як: смарт-замок DL30Z, Bluetooth смарт-замки ML200, камери відеоспостереження ES-852O21C-S5-MI, термінали доступу MA300-BT/MF та контролери доступу Atlas 400. Далі інструкція опису кількох елементів.

DL30Z - це смарт-замок, призначений для забезпечення безпеки та зручності в будинку чи офісі, встановлюється на вхідні двері і контролюється за допомогою смартфона або іншого пристрою з підтримкою бездротового зв'язку. DL30Z підтримує бездротові протоколи Bluetooth або Wi-Fi, що дозволяє віддалено керувати замком через програму на смартфоні або іншому пристрої. Смарт-замок DL30Z забезпечує можливість створення кількох користувацьких кодів доступу. Це дозволяє різним людям мати індивідуальні коди для входу без використання ключів. DL30Z надає повідомлення на смартфон про різні події, такі як відкриття або закриття замка, зберігає журнал подій, що дозволяє переглядати історію активності замку. Завдяки підтримці бездротового зв'язку, DL30Z дозволяє керувати замком з будь-якої точки світу через Інтернет. Можливо відкрити або закрити замок, навіть перебуваючи далеко від дому. В комплект входить фізичний ключ у випадку, якщо потрібний традиційний спосіб доступу або у разі збою електроживлення. DL30Z інтегрує з смарт-пристроями, такими як системи "розумний дім" або віртуальні помічники, що дозволяє вам створити власну інтелектуальну систему безпеки.

Важливо, що конкретні характеристики та функціональність DL30Z можуть змінюватись в залежності від виробника та моделі. Рекомендується вивчення документації та специфікації конкретного пристрою для отримання точної інформації про його можливості та налаштування (рисунок 3.1) [29].

Рисунок 3.1 – Смарт-замок DL30Z

ML200 - це Bluetooth смарт-замок, який пропонує зручність та безпеку для офісних дверей, використовує бездротову технологію Bluetooth для зв'язку з мобільними пристроями та управління замком через спеціальну програму, підтримує з'єднання Bluetooth, що дозволяє керувати замком за допомогою смартфона. Для цього потрібно встановити відповідну програму та налаштувати з'єднання між замком і пристроєм. Смарт-замок ML200 зазвичай має свою мобільну програму, яка надає широкий спектр функцій. За допомогою програми можна відкривати та закривати замок, створювати тимчасові коди доступу, переглядати журнал подій та отримувати сповіщення про дії, пов'язані із замком.

ML200 дозволяє створювати унікальні коди доступу для різних користувачів, також ведеться журнал подій, для перегляду історії використання замку, та постачається з фізичним ключем, який може використовуватися у разі збою електроживлення або інших проблем бездротового з'єднання. Завдяки з'єднанню Bluetooth, ML200 дозволяє керувати замком здалеку в межах діапазону Bluetooth. Ви можете відкрити або закрити замок, перебуваючи всередині будинку або поблизу нього (рисунок 3.2) [30].

Перш ніж встановити Bluetooth смарт-замок потрібне розблокування за допомогою будь-якого методу аутентифікації перед реєстрацією нового замка.

Потім, реєстрація адміністратора перед виконанням будь-яких інших операцій в автономному режимі.

Рисунок 3.2 – Bluetooth смарт-замок ML200

Живлення замка відбувається за допомогою чотирьох лужних батарейок типу AA. Не рекомендується використовувати не лужні або акумуляторні батарейки. Не рекомендується виймати батарейки з замка під час його роботи. Замінюємо батарейки, коли замок блимає червоним світлом разом із 2-секундним звуковим сигналом після увімкнення. Замок має механічні ключі для ручного розблокування. Зберігаємо ці ключі в безпечному місці. Батарейки потрібно замінювати, коли заряд акумулятора низький, замок блимає червоним світлом разом із 2-секундними звуковими сигналами. Індикація незаконних спроб: після 5 невдалих спроб перевірки замок буде блимати червоним світлом разом із 10-секундними звуковими сигналами, і блокування перестане працювати. Micro-USB у нижній частині зовнішнього блоку це інтерфейс. Його можна зарядити за допомогою павербанка, коли замок вимкнений.

Аварійний механічний ключ використовується для відкриття дверей у випадку електронної несправності замка. У цьому випадку потрібно зсунути кришку ключа та вставити ключ для розблокування в екстреній ситуації. Замок підтримує з'єднання через Bluetooth 5.0, його можна розблокувати за допомогою смартфона, якщо Bluetooth підключено. Функція доступна лише з додатковим Smart Gateway. За допомогою встановленого Smart Gateway замок можна керувати дистанційно через додаток ZSmart. У замку присутне управління голосовим помічником, ця функція доступна лише з додатковим

Smart Gateway. Замок можна розблокувати за допомогою голосових команд через Amazon Alexa і Google Assistant [31].

ES-852O21C-S5-MI – це модель камери відеоспостереження, призначеної для забезпечення безпеки та спостереження за об'єктами. Вона має ряд функцій та характеристик, які роблять її ефективним інструментом для відеоспостереження. Камера ES-852O21C-S5-MI забезпечує високу роздільну здатність відео. Вона може записувати відео у форматі Full HD або навіть 4K Ultra HD, що дозволяє отримувати чітке та деталізоване зображення. Камера зазвичай оснащена вбудованим інфрачервоним підсвічуванням, що дозволяє знімати відео навіть в умовах низького освітлення або повної темряви. Це робить її придатною для спостереження у нічний час, зазвичай має широкий кут огляду 105°, що дозволяє охопити велику площу. Це корисно для спостереження за просторами з різними кутами та забезпечує широке покриття.

Камера зазвичай має функцію підключення до мережі, наприклад, Ethernet або бездротове з'єднання Wi-Fi, що дозволяє передавати відео та отримувати доступ до неї віддалено через мережу, що забезпечує зручність та мобільність. Ця модель включає функції аналітики відео, такі як виявлення руху, виявлення осіб або зон розмежування. Це дозволяє автоматично визначати та реагувати на певні події, спрощуючи процес моніторингу. Камера зазвичай має ступінь захисту від вологи та пилу, що дозволяє використовувати її всередині приміщень або на відкритому повітрі (рисунок 3.3).

Рисунок 3.3 – Камера відеоспостереження ES-852O21C-S5-MI

Перш ніж розпочати монтаж системи відеоспостереження, важливо врахувати деякі деталі при виборі місць для розміщення камер.

Встановимо камеру високо та розташовуємо на достатній висоті для забезпеченням широкого кута огляду та кращої якості запису. Це дозволить охопити більше зони за допомогою меншої кількості камер.

Розмістимо камеру у недоступних для зловмисників місцях, вибравши місця, важкодоступні для потенційних злочинців. Це забезпечить більшу безпеку та унеможливить «нерозумні» спроби втрутитися у роботу камер.

Уникаємо направлення камери прямо на джерела світла, оскільки це може призвести до не до експонування зображень. Краще розташовувати камери таким чином, щоб світло падало на об'єкти, які ви бажаєте спостерігати.

Незалежно від типу камери (дротової або бездротової), важливо розташовувати їх поблизу джерела живлення. Це забезпечить стабільне живлення та роботу камери.

Не рекомендується розміщення камери відеоспостереження безпосередньо під вікнами, оскільки це може призвести до переекспонування зображень через ІЧ-відображення.

Не потрібне встановлення камери у вбиральнях, та приватних місцях щоб не порушувати приватність користувачів.

Крім того, перед монтажем важливо правильно спланувати маршрут проводів та кабелів камер відеоспостереження. Заздалегідь спланувуємо маршрут, яким будуть проходити дроти камер відеоспостереження. Це особливо важливо, якщо встановлювати камери в різних місцях офісу.

Розглянемо необхідні отвори для проходу дротів та продумаємо найкоротший маршрут. Кожен кабель складається з двох проводів зі своїми роз'ємами - один для живлення, інший для підключення до відео реєстратора. Створимо єдине джерело живлення для кабелів або підключимо їх до різних розеток у офісі [32].

Підключимося до записувального пристрою, після прокладання дротів підключимо кабелі до відео реєстратора (DVR/NVR). Потім підключимо відео реєстратор до монітора для перегляду.

Останнім кроком є налаштування камер відеоспостереження, щоб мати доступ до них через смартфони, комп'ютери або планшети. Деякі виробники надають програми та програмне забезпечення для настільних комп'ютерів, які дозволяють отримати доступ до камер з будь-якого місця.

MA300-BT/MF – це термінал доступу, призначений для контролю доступу та ідентифікації користувачів, підтримує різні методи аутентифікації, включаючи безконтактні карти (RFID), біометричне сканування відбитків пальців та паролі. Це дозволяє вибрати найбільш зручний та безпечний спосіб доступу. Термінал має функцію бездротового зв'язку Bluetooth, що дозволяє йому підключатися до мобільних пристроїв, таких як смартфони або планшети. Він сумісний з різними стандартами безконтактних карток, такими як RFID або NFC, що дозволяє використовувати картки для ідентифікації користувачів. Цей термінал доступу має вбудований сенсор для сканування відбитків пальців. Він дозволяє користувачам аутентифікуватись за допомогою їх унікальних біометричних даних, зберігає журнал подій, який дозволяє відстежувати та переглядати історію доступу. Має функції керування доступом, дозволяючи налаштовувати права доступу користувачів та обмежувати доступ до певних зон або часу (рисунок 3.4) [33].

Рисунок 3.4 – Термінал доступу MA300-BT/MF

Режим реєстрації за допомогою майстер картки дозволяє реєструвати лише одного користувача кожного разу, коли ви увійшли у режим реєстрації. Під час реєстрації нового користувача, зчитувач автоматично надає мінімально вільний ID номер користувача. Крім того, ви також можете зареєструвати користувача за допомогою USB-клавіатури. У режимі очікування система переходить у режим реєстрації після піднесення майстер картки (після цього система знову повертається до режиму очікування).

Після голосової підказки «Реєстрація користувача», розташуємо палець або піднесемо карту щоб розпочати процес реєстрації. Існує два можливих варіанти. Розглянемо перший варіант, спочатку піднесемо безконтактну карту, після успішної реєстрації нової карти пристрій повідомить «ID номер користувача. Реєстрація успішна!» і можна переходити до наступного кроку. У разі помилки під час реєстрації, система повідомить "Номер карти вже існує" і повернеться в режим реєстрації, очікуючи розташування пальця або піднесення карти, після голосового повідомлення "Реєстрація. Розташуйте палець" система перейде у режим реєстрації відбитків пальця. Піднесемо один і той самий палець до сенсора тричі, при успішній реєстрації система повідомить "Успішна реєстрація. Розташуйте палець" і перейде до реєстрації наступного пальця. У разі помилки під час реєстрації, система повідомить "Розташуйте палець знову" і тоді потрібно повторити попередній крок, після реєстрації 10 відбитків та 1 картки система автоматично повернеться в режим очікування після піднесення майстер картки або після закінчення тайм-ауту.

Розглянемо другий варіант, спочатку розташуйте палець, розташуємо один і той самий палець на сенсорі три рази. При успішній реєстрації система повідомить «Номер користувача. Успішна реєстрація», після чого можна переходити до наступного кроку. У разі помилки під час реєстрації, система озвучить «Розташуйте палець ще раз» і повернеться в режим реєстрації, очікуючи розташування пальця або піднесення карти, після голосового повідомлення «Реєстрація. Розташуйте палець або піднесіть карту» система

перейде у режим реєстрації, очікуючи піднесення нової карти або розташування пальця, після успішної реєстрації безконтактної карти система повідомить «Успішна реєстрація. Розташуйте палець» і перейде в режим реєстрації відбитків пальця. У разі піднесення раніше незареєстрованого пальця та успішної реєстрації цього пальця, система повідомить «Реєстрація успішна. Розташуємо палець або піднесіть карту» для продовження реєстрації нових відбитків та карти. Після реєстрації 10 відбитків система повідомить «Піднесіть картку» для реєстрації картки, якщо вона ще не зареєстрована, система автоматично повернеться в режим очікування після реєстрації 10 відбитків та 1 картки після піднесення майстер картки або закінчення тайм-ауту.

Якщо користувачеві вже призначено певний ID номер, існують такі варіанти реєстрації відбитків або картки, після піднесення зареєстрованої карти система озвучить «Номер користувача. Реєстрація. Розташуйте палець» і перейде в режим реєстрації відбитків. Раніше зареєстровані відбитки будуть перезаписані новими, розташуйте один і той самий палець на сенсорі три рази. При успішній реєстрації система повідомить «Номер користувача. Успішна реєстрація» і буде готова до реєстрації наступного пальця, система автоматично повернеться в режим очікування після реєстрації 10 відбитків та 1 картки після піднесення майстер картки або закінчення тайм-ауту.

Atlas 400 – це контролер доступу, призначений для управління та контролю доступу користувачів до зони або приміщення. Він забезпечує безпеку та зручність управління доступом, а також пропонує різні функції для ефективної роботи. Atlas 400 має високу масштабованість, що дозволяє легко керувати великою кількістю зчитувачів та точок доступу. Це робить його придатним для використання у комплексних системах контролю доступу, таких як офісні будівлі, торгові центри та промислові об'єкти. Контролер доступу Atlas 400 підтримує різні методи аутентифікації, такі як безконтактні карти (RFID), біометричне сканування відбитків пальців або розпізнавання обличчя. Це дозволяє вибирати найбільш зручний та безпечний спосіб ідентифікації

користувачів, обмеження на доступ до певних зон, приміщень або час, що забезпечує контроль та безпеку. Контролер доступу Atlas 400 зберігає журнал подій, відстежує та аналізує активність доступу, а також забезпечує надійний аудит та моніторинг системи, має підключення до мережі, такої як Ethernet, що забезпечує віддалене керування та моніторинг системи контролю доступу. Це дозволяє адміністраторам налаштовувати параметри доступу та отримувати сповіщення про активність через мережний інтерфейс. Контролер доступу Atlas 400 може інтегруватися з іншими системами безпеки, такими як системи відеоспостереження або пожежної сигналізації. Це дозволяє створити комплексну систему безпеки, яка працює взаємодіючи та координуючи дії різних компонентів (рисунок 3.5) [34].

Рисунок 3.5 – Контролер доступу Atlas 400

Важливо, що конкретні характеристики та функціональність приладів може змінюватись в залежності від виробника та моделі. Рекомендується вивчення документації та специфікації конкретного пристрою для отримання точної інформації про його можливості та налаштування.

3.2 Економічні розрахунки

Розглянемо конкретні характеристики, функціональність та розміщення приладів СКУД у юридичному офісі.

Вартість обладнання, розрахункова вартість СКУД включає в себе вартість всього необхідного обладнання, такого як, контролери, зчитувачі, камери відеоспостереження, вхідний смарт-замок та Bluetooth замки, які ми розглянемо далі.

У приміщення офісу розташована камера відеоспостереження ES-852021 C-S5-MI з права при вході та має великий кут огляду, що дозволяє спостерігати за поведінкою можливих зловмишнеків та вчасно втрутитися у не правомірні дії доступу до офісу. Орієнтована вартість камери відеоспостереження ES-852021 C-S5-MI складає – 2 006 грн. Важливу роль відіграють смарт-замок DL30Z та зчитувач MA300-BT/MF, які гарно зарекомендували себе за характеристикою на ринку, відміно виконують свої функції для забезпечення безпеки у офісі, та мають доступну вартість для необхідного налагодження та керування системою контролю доступу. Вартість яких складає: вхідний смарт-замок DL30Z - 5 852 грн; та зчитувач MA300-BT/MF - 6 460 грн. Оскільки входом у приміщення, протягом дня, користується велика кількість персоналу та клієнтів система має вражати своєю якістю.

Зайшовши у приміщення юридичного офісу за нами спостерігає камера відео спостереження ES-852021 C-S5-MI, яка знаходиться на достатній висоті у холі, та має великий кут огляду, що забезпечує безпеку входу та виходу. Далі, з ліва по периметру, знаходиться куток консультанта, який також супроводжує оглядом камера відеоспостереження ES-852021 C-S5-MI, що знаходиться на відповідній висоті між дверима у кімнати юристів та спеціалістів, загалом осягаючи частину холу, куток консультанта та двері у конференц-зал.

Камера відеоспостереження у конференц-залі знаходиться на висоті 2.5 мертів, паралельно входу. У двері конференц-залу вмонтований надійний

Bluetooth замок ML200, та зчитувач MA300-BT/MF, якими користуються персонал юридичного офісу по безконтактних картках (RFID). Вартість Bluetooth смарт-замка ML200 - 4 598 грн, та зчитувача MA300-BT/MF - 6 460 грн, за один прилад.

Двері кімнати спеціалістів обладнані Bluetooth замок ML200, та зчитувачем MA300-BT/MF, а також кімнаті з права на стіні знаходиться камера відеоспостереження, яка має великий кут огляду, спостерігаючи за безпекою бухгалтера та кадровика і інформацією відповідного призначення.

У кімнаті юристів знаходиться, дві камери відеоспостереження розміщені паралельно одна одній, на відповідній висоті для повного огляду захисту інформації у кімнаті. Двері кімнати такаж, обладнані Bluetooth замок ML200, та зчитувачем MA300-BT/MF, якими користуються юристи у офісі для надійного та зручного входу та виходу з кімнати.

Затишна кімната, яка надійно охороняється камерою відеоспостереження та входом, де дверний Bluetooth замок ML200, зчитувачем MA300-BT/MF – це кімната керівника в якій знаходиться велика кількість конфіденційної інформації тому вхід у неї обмежений тут діє двофакторна ідентифікації за відбитком пальця, та надійного паролю, яку використовує керівник.

Однією з досить секретних, конфіденційних кімнат є серверна, де знаходиться: сервер, контролери, комп’ютер та інша техніка – це «серце» офісу. Вхід до якої спостерігає камера відео спостереження, яка знаходиться на впроти входу. Двері серверної надійно обладнані Bluetooth замок ML200, зчитувачем MA300-BT/MF, доступ до цієї кімнати охороняється біометричним доступом та надійним паролем, яким користується тільки адміністратор.

У юридичному офісі є затишна кімната для відпочинку без відеоспостереження, якою користується персонал для проведення обидної перерви, та релаксу. Кухня обладнана відповідною технікою та меблями для підготування до обіду, а також для безпеки персоналу за усім спостерігає камера відеоспостереження. Вхід у кухню забезпечений надійним Bluetooth

замком ML200 і зчитувачем MA300-BT/MF, якими користується персонал агентства за використанням безконтактних карток (RFID).

Для приміщення офісу було придбано значна кількість однакових моделей камер відеоспостереження, зчитувачем, контролерів, Bluetooth замків виробника ZKTeco.

Орієнтовна вартість за даними сайту, декількох приладів на сьогоднішній день, для створення СКУД на базі обладнання ZKTeco з використанням технології Bluetooth зведені у таблиці (табл 3.1).

Таблиця 3.1 – Обране обладнання СКУД

Найменування	Кількість	Ціна за шт. (грн.)	Сума (грн.)
Контролер «Atlas 400»	2	17 982	35 964
Зчитувач «MA300-BT/MF»	8	6 460	51 680
Камера відеоспостереження «ES-852021 C-S5-MI»	10	2 006	20 060
Вхідний smart-замок «DL30Z»	1	5 852	5 852
Bluetooth замок «ML200»	6	4 598	27 588
		Підсумок	141 144

Таким чином за результатами зведеними у таблицю, видно що орієнтована вартість приладів СКД для юридичного офісу складає 141 144 гривень, що відповідає нормальній ціновій політиці на сьогоднящній день, де

були використані прилади відомого виробника ZKTeco, які гарно зарекомендували себе на ринку У компанії повний набір обладнання для захисту підприємства від зовнішніх та внутрішніх загроз автоматизації бізнес процесів.

3.3 Політика безпеки користування системою

Основні аспекти рольової політики безпеки СКУД на основі Bluetooth технологій: аутентифікація, управління видимістю, керування спаренням, виявлення загроз.

Аутентифікація забезпечує перевірку ідентичності пристроїв, які намагаються встановити Bluetooth-з'єднання, для цього можуть використовуватися паролі, ключі або інші методи аутентифікації. Наприклад, у режимі парного з'єднання можна вимагати введення пароля, щоб забезпечити, що тільки дозволені користувачі можуть підключатися до пристрою.

Управління видимістю забезпечує контроль над видимістю Bluetooth-пристрою, де користувач може встановлювати налаштування видимості, вимкнення Bluetooth-пристрою або налаштовувати список довірених пристроїв, з якими може встановлюватися з'єднання. Це має важливу роль та може допомогти зменшити ризик несанкціонованого доступу до пристрою.

Керування спаренням забезпечує контроль над процесом спарення між Bluetooth-пристроями. Це може обмежувати автоматичне спарення, налаштовувати список довірених пристроїв, або вимагати підтвердження спарення з іншого пристрою перед його встановленням. Що дозволяє забезпечити, коли тільки дозволені пристрої можуть встановлювати з'єднання.

Виявлення загроз безпеці відповідає за виявлення та блокування загроз безпеці Bluetooth-з'єднання. Що може виявляти спроби перехоплення з'єднання, атаки "людина посередині" (man-in-the-middle), спроби встановлення

підробленого з'єднання та інші види атак. Для цього можуть використовуватися алгоритми виявлення загроз, такі як аналіз підозрілих активностей, контроль інтегритету даних та перевірка цифрових підписів [36].

Ці чотири складових спільно допомагають створити систему контролю доступу, яка забезпечує безпеку і захист від витоку інформації через Bluetooth-технологію. Крім основних складових системи контролю доступу, варто враховувати інші аспекти:

- права доступу і авторизація;
- моніторинг і виявлення вторгнень;
- оновлення програмного забезпечення;
- навчання та свідомість користувачів;
- аудит та моніторинг.

Політика безпеки інформації - це сукупність пов'язаних документів, які визначають порядок забезпечення безпеки інформації в конкретній організації і встановлюють вимоги щодо підтримки такого порядку. Розробка політики безпеки є обов'язковим і ключовим етапом при проектуванні будь-якої системи забезпечення безпеки інформації. Від правильного формування корпоративних правил і процедур залежить рівень безпеки і всіх наступних проектних рішень [36].

Політика безпеки формується на основі аналізу ризиків, які є реальними для інформаційної системи організації. Процес аналізу ризиків включає дослідження компонентів інформаційної системи компанії, які піддаються загрозам, визначення вразливих місць системи, оцінка ймовірності кожної конкретної загрози та очікувані збитки, вибір можливих методів захисту та розрахунок їх вартості. На завершальному етапі оцінюється користь від застосування запропонованих заходів захисту. Ця користь може бути як позитивною, так і негативною. [37]

Слід також зазначити, що Український стандарт з технічного захисту інформації наразі не містить достатньо конкретних нормативних та методичних

матеріалів щодо розробки політик безпеки для автоматизованих систем. Це особливо актуально для більшості організацій, які навіть не мають уявлення про поняття політики безпеки. Однак парадокс полягає в тому, що фактично в будь-якій організації завжди існують конкретні правила, які регламентують процес її функціонування, зокрема процес захисту інформації, і ці правила є політикою безпеки. Таким чином, фактично в будь-якій автоматизованій системі окремі елементи політики безпеки завжди присутні.

Створення нормативної бази повинно відбуватися відповідно до чинного законодавства. Однак, зрозуміло, що дане положення може застосовуватися до будь-якого виду діяльності. Оскільки інформаційні технології швидко розвиваються, нормативна база значно відстає від практичних потреб. Відставання законів, стандартів і відсутність методичного забезпечення стають особливо критичними.

В реальній системі обробки інформації можуть працювати системний адміністратор, менеджер баз даних і звичайні користувачі. Ролева політика безпеки (РПБ) використовується для розподілу повноважень між цими ролями, враховуючи їхні обов'язки. Системному адміністратору призначаються спеціальні повноваження, які дозволяють йому контролювати роботу системи і керувати її налаштуваннями. Менеджер баз даних має доступ до керування сервером баз даних, а права звичайних користувачів обмежені мінімально необхідним для запуску програм. Кількість ролей у системі може не відповідати кількості користувачів. Один користувач може виконувати кілька ролей одночасно або послідовно, якщо має відповідні повноваження, і кілька користувачів можуть мати доступ до однієї ролі, якщо вони виконують однакові завдання. У РПБ керування доступом здійснюється у два етапи: спочатку для кожної ролі визначається набір повноважень, які включають права доступу до об'єктів, а потім кожному користувачеві призначається список доступних йому ролей. Повноваження надаються ролям відповідно до принципу найменших привілеїв, згідно з яким кожний користувач отримує

лише мінімально необхідні повноваження для виконання своїх обов'язків. У моделі РПБ використовуються множини: множина користувачів, множина ролей, множина повноважень для доступу до об'єктів та множина сеансів роботи користувачів з системою. Для цих множин встановлюються відношення, які визначають набір повноважень, призначених кожній ролі, а також доступні ролі для кожного користувача [39].

Роль політики безпеки у юридичному офісі для керівника є вкрай важливою. Керівник проводить оцінку потенційних загроз безпеки інформації, виявляє слабкі місця і розробляє стратегію їх запобігання, а такаж визначає, хто має право на доступ до різних типів інформації в офісі. Формує застосування відповідних технічних заходів безпеки, таких як шифрування даних, паролі та використання захищених мереж. Надає персоналу достатню підготовку з питань безпеки інформації, включаючи правила щодо обробки і збереження конфіденційної інформації. Керівник вживає заходів при виявлені потенційних проблем та вжиття заходів для їх виправлення [40].

Роль адміністратора інформаційної безпеки полягає у організації циклу заходів забезпечення безпеки інформаційної системи, яка включає такі етапи: проведення аудиту інформаційної безпеки, складання звіту про виявлені вразливості, формулювання рекомендацій. Обмеження та повноваження адміністратора також визначені внутрішньою політикою та правилами юридичного офісу. Зазвичай адміністратор не надає юридичні поради та не виконує роботу, яка вимагає правової кваліфікації. Адміністратор дотримується конфіденційності і забезпечує безпеку конфіденційної інформації, що стосується клієнтів та справ офісу.

Роль консультанта в офісі надання юридичних порад та підтримки, рекомендацій що до різних правових питань, підготовки документів, таких як: контракти, угоди, листи. Однак, консультант не має права виконувати дії, які вимагають правової кваліфікації, що зарезервовані для адвокатів або юристів з повними правами, а також представляти клієнтів у суді або на переговорах,

підписувати документи або виконувати дії, які мають правові наслідки, без доручення адвоката чи керівництва офісу.

У юридичному офісі роль бухгалтера полягає в обліку та фінансовому управлінні організації. Він веде облік фінансових операцій, бухгалтерських записів, складає бюджет, контролює витрати, оплачує рахунки, а також веде облік заборгованості та розрахунки з клієнтами. Підготовляє фінансові звіти для внутрішнього та зовнішнього використання, включаючи звіти для керівництва, податкових органів та інших зацікавлених сторін. Розраховує податки, включаючи податок на прибуток, ПДВ та інші обов'язкові платежі. Не має повноважень надавати юридичні поради не втручається у питання пов’язані з правовою діяльністю.

В юридичному офісі роль кадровика полягає в управлінні кадровими процесами та ресурсами організації. Кадровик відбирає кандидатів на вакантні посади в офісі, проводить співбесіди та здійснювати оцінку потенційних працівників. Здійснює процедури з працевлаштування, включаючи укладання контрактів, підготовку документів, пов'язаних з прийомом на роботу. Веде кадрову документацію, включаючи утримання персональних карток, заяв про відпустку, заяв про звільнення. організовує навчання та розвиток персоналу. Немає повноважень надавати юридичні поради та не втручається у питання пов’язані з правовою діяльністю.

Роль юристів у юридичному офісі є центральною, оскільки вони володіють спеціалізованою юридичною кваліфікацією та надають правову підтримку клієнтам. Роль юристів полягає у надавані юридичних порад, консультацій з різних галузь права, а також аналізу правових проблем та підготовки юридичних документів. Вони вповноважені представляти клієнтів у судових процесах, арбітражних справах та переговорах, укладають, переглядають та аналізують контракти, угоди та інші юридичні документи. Юристи не повині здійснювати будь-які дії, які суперечать етичним стандартам та професійній поведінці юристів.

Роль прибиральниці у юридичному офісі полягає в забезпеченні чистоти та порядку в приміщені агентства. Основні завдання прибиральниці включають прибирання офісних приміщень, утилізацію сміття, та підтримання чистоти, тобто: протирання поверхонь, миття підлоги, прибирання вбиральні та інших загальних приміщень. За дозволу від ролі керівника, прибиральниця має повноваження часткового входу у всі приміщення офісу, для прибирання та підтримання чистоти. Заборонено виконувати дії, які не входять у її компетенцію, такі як, втручання у юридичні або адміністративні питання офісу, виконуючи роботу, яка вимагає спеціалізованих навичок або ліцензій, які не має прибиральниця.

У відповідності за наявності штату юридичного агентства, рольова політика безпеки користування системою контролю та управління доступом (СКУД) з захистом від витоку інформації на основі Bluetooth технологій включає набір правил і заходів для забезпечення безпеки та конфіденційності використання системи. Важливо забезпечити безпеку даних електронних пристроїв шляхом використання паролів, регулярного оновлення програмного забезпечення та застосування заходів проти вторгнень та кібератак, де знаходиться конфіденційна інформація.

3.4 Висновок

Загалом, система контролю доступу від витоку інформації Bluetooth-технології поєднала технічні заходи безпеки, правила доступу, навчання користувачів та постійний моніторинг для забезпечення максимального рівня захисту від витоку інформації.

Також була провдена оцінка ефективності розробки системи контролю доступу у юридичному агентстві «Воля». За результатами оцінки було встановлено, що витрати на реалізацію системи становлять 141 144 гривень, не

враховуючи монтажних робіт. Було проведено ознайомлення з інструкцією, навчання персоналу з користуванням приладами СКУД.

Політика безпеки користування системою визначила набір правил, процедур і практик, які спрямовані на захист конфіденційності, цілісності та доступності інформації, а також на запобігання незаконного доступу до неї і інших загроз безпеци. Основна мета полягала в забезпеченні захисту конфіденційної інформації клієнтів та важливих даних офісу, забезпеченні дотримання вимог законодавства про захист персональних даних та зменшенні ризику витоку інформації. Особливо важливою була розробка охорони приватної інформації про клієнтів, яка включала конфіденційну і комерційну інформацію, юридичні документи, переписку та інші конфіденційні дані.

ВИСНОВКИ

Загальна мета цього проєкту було забезпечити надійний рівень безпеки інформаційної системи, мінімізувати ризики та захистити дані від втрати, розголошення або несанкціонованого доступу. Оцінка ризиків та економічне обґрунтування витрат допомогли визначити необхідні заходи та розподілити ресурси ефективно для досягнення цієї мети.

З метою забезпечення безпеки та запобігання витоку конфіденційної інформації в юридичному офісі, було розроблено та впроваджено систему контролю доступу на основі Bluetooth технології. Для досягнення успіху в цьому процесі було вирішено значна кількість необхідних завдань.

Першим кроком було розглянуто потреби та вимоги офісу щодо системи контролю доступу. Це включало вивчення режимів роботи, категорій доступу, обмежень та інших факторів, які впливають на безпеку даних.

На основі отриманих вимог потрібно було розробити систему контролю доступу, яка базується на Bluetooth технології. Що включало вибір необхідного обладнання, розробки програмного забезпечення та інтеграцію з існуючою інфраструктурою офісу.

Було розроблено рівні доступу та зони, які відповідають потребам безпеки офісу. Це включає обмеження доступу до певних приміщень або пристроїв залежно від ролі та повноважень користувачів.

Для реалізації системи контролю доступу необхідно було встановити Bluetooth-сумісні замки та датчики доступу в приміщеннях офісу. Це забезпечило фізичний контроль та доступ до конфіденційної інформації.

Останнім кроком було впроваджено систему контролю доступу в офісі. Це включало навчання персоналу з використання нової системи, розподіл необхідних пристроїв та налагодження процесу роботи з системою.

В цілому, впровадження системи контролю доступу на основі Bluetooth технології в юридичному офісі є важливим заходом для забезпечення безпеки

даних клієнтів та запобігання витоку конфіденційної інформації. Правильне виконання вищезазначених завдань є ключовим для успіху і ефективного функціонування системи контролю доступу.

Bluetooth технологія є зручною для користувачів офісу. Замість використання фізичних ключів або карток доступу, користувачі матимуть змогу використовувати свої мобільні пристрої з підтримкою Bluetooth для отримання доступу до визначених зон офісу. Це спростить процес контролю доступу і уникне проблем, пов'язаних з втратою або крадіжкою фізичних ключів.

Та лише дотримуючись правил захисту інформації, агентство може забезпечити безпеку своєї внутрішньої інформації. Ці правила чітко визначають, яку інформацію, де і як потрібно захищати, і їх необхідно дотримувати всім співробітникам без винятку. У межах агентства ці правила перетворюються на складну ієрархічну систему інструкцій і регламентів, які призначені для різних категорій співробітників, що займаються забезпеченням безпеки інформації.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Industrial Bluetooth. *Phoenixcontact.* URL: https://www.phoenixcontact.com/uk-ua/tekhnolohiyi/tekhnolohiyi-zvyazku/industrial-bluetooth (дата звернення: 04.04.2023).
2. Bluetooth: коротко про найважливіше. *Shop-gsm.ua.* URL: https://shop-gsm.ua/blog/istoriya-poyavleniya-i-razvitiya-bluetooth-kratko-o-samom-vazhnom/ (дата звернення: 02.05.2023)
3. Що таке система контролю доступу і навіщо вона потрібна. *Alarm - охоронні системи.* URL: https://alarm.lviv.ua/blog/shho-take-sistema-kontrolyu-dostupu-i-navishho-vona-potribna (дата звернення: 05.04.2023).
4. Основні завдання систем контролю доступу. *Ohrana.ua* URL: https://ohrana.ua/uk/stati-i-obzory/chto-takoe-skud.html (дата звернення: 02.05.2023)
5. Системи контролю доступу. *Одесса сервер.* URL: http://domofonodessa.od.ua/index.php?route=information/information&information_id=13 (дата звернення: 05.04.2023).
6. Система контролю доступу. *Expertsolution.* URL: https://expertsolution.com.ua/uk/sistema-kontrolja-dostupa--skud--dlja-gostinic?utm_source=google&utm_campaign=ua&utm_medium=cpc&gclid=Cj0KCQjw7PCjBhDwARIsANo7CglFOzPAuBxpMraJwI3sc77gnWPoJdeENeTaDw9U3E5avO0W7-wRtksaAvfdEALw_wcB (дата звернення: 02.05.2023)
7. Технологія Bluetooth. *Вікі ЦДУ* URL: https://wiki.cuspu.edu.ua/index.php/Технологія_Bluetooth (дата звернення: 05.04.2023).
8. Що таке бездротова технологія BLUETOOTH. *Helpguide.sony* URL: https://helpguide.sony.net/speaker/srs-btv5/v1/uk/contents/02/01/01/01.html (дата звернення: 02.05.2023).

9. Система контролю і управління доступом (СКУД). *Vist+it.* URL: https://vistplus.com/it-poslugi/skud/ (дата звернення: 06.04.2023).

10. Електрозамки: які є, як працюють. *Deps.* URL: https://deps.ua/ua/knowegable-base/reference-information/9239.html (дата звернення: 06.04.2023).

11. Автономні системи. *Studfiles.* URL: https://studfile.net/preview/5285785/page:6/ (дата звернення: 08.04.2023).

12. Системи контролю доступу. *Лабараторія безпеки.* URL: https://securitylab.com.ua/sistemy-kontrolya-dostupa/ (дата звернення: 08.04.2023).

13. Система управління базами даних. *Вікіпедія* URL: https://uk.wikipedia.org/wiki/Система_управління_базами_даних (дата звернення: 09.04.2023).

14. Види контролю. *Освіта.ua.* URL: https://osvita.ua/vnz/reports/management/14696/ (дата звернення: 16.04.2023).

15. Системи контролю і управління доступом від А до Я. *dep* URL: https://deps.ua/ua/knowegable-base/reference-information/7824.html (дата звернення: 21.04.2023).

16. 1Контроль доступу. *Система Електрозахисту.* URL: http://sez.net.ua/kontrol-dostupa-vraga-nuzhno-znat-v-lico-2.html (дата звернення: 16.04.2023).

17. Системи контролю та управління доступом, інтегровані системи безпеки. *Fortnet.* URL: https://access.com.ua/index.php/k2/download/instruction/item/19-content-demo-123 (дата звернення: 18.04.2023).

18. Види інформації з обмеженим доступом. *Studies.* URL: https://studies.in.ua/inf-pravo-seminar/2147-vidi-nformacyi-z-obmezhenim-dostupom.html (дата звернення: 07.05.2023).

19. Захист інформації. *Енциклопедія сучасної України.* URL: https://esu.com.ua/article-15872 (дата звернення: 07.05.2023).

20. Комплексні системи безпеки. Валтек. URL: https://valtek.com.ua/ua/system-integration/security-control-system/integrated-security-systems/information-security-system-review (дата звернення: 11.05.2023).

21. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації: навчальний посібник / С. О. Іванченко та ін. Київ : НТУУ «КПІ», 2016. 104 с.

22. Системи контролю доступу. Zkteco URL: https://zktecoua.com/ua/solutions/skud/ (дата звернення: 11.05.2023).

23. Системи контролю доступу. *Fibergroup* URL: http://fibergroup.com.ua/ua/uslugi/sistemy-bezopasnosti/sistemi-kontrolya-dostupa/ (дата звернення: 02.05.2023).

24. Гапак О. М., Балога С.І. Захист інформації в комп'ютерних системах: навч.посіб Ужгород: УжНУ 2021р 24с

25. Засоби та методи захисту інформації. *Буклiб.* URL: https://buklib.net/books/28625/ (дата звернення: 21.04.2023).

26. Встановлення відеоспостереження. *Ivipor.* URL: https://iviport.com.ua/cctv-in-the-office/ (дата звернення: 11.05.2023).

27. Що таке багатофакторна аутентифікація. *Hideez.* URL: https://hideez.com/uk-ua/blogs/news/what-is-multifactor-authentication-advantages-and-limitations-hideez (дата звернення: 02.05.2023).

28. Аутентифікація користувачів. *Studfile.* URL: https://studfile.net/preview/5392724/page:16/ (дата звернення: 02.05.2023).

29. Інтелектуальний замок. *Zkteco.* URL: https://zktecoua.com/ua/products/intellektualnyj-zamok-dl30z/ (дата звернення: 02.05.2023).

30. Кодовий замок. *Zkteco.* URL: https://zktecoua.com/ua/products/bluetooth-password-lock-ml200/ (дата звернення: 02.05.2023).

31. Посібник користувача з цифровою клавіатурою початкового рівня. *Zkteco* .URL: https://uk.manuals.plus/zkteco/ml200-entry-level-digital-keypad-smart-

lock-with-bluetooth-communication-manual#product_features (дата звернення: 21.04.2023).

32. Комплексна установка систем та камер відеоспостереження. *Itlogica.* URL: https://itlogica.com.ua/uk/services/ustanovka-sistem-videonabljudenija/ (дата звернення: 21.04.2023).

33. Біометричний термінал по відбитку пальця. *Zkteco.* URL: https://zktecoua.com/ua/products/fingerprint-reader-zkteco-ma300/ (дата звернення: 21.04.2023).

34. RFID контролер доступу. *Zkteco.* URL: https://zktecoua.com/ua/products/rfid-kontroller-dostupa-atlas400/ (дата звернення: 21.04.2023).

35. Глушков В. Інформаційна безпека (соціально-правові аспекти). Право України. 2010. № 9. С.311-313

36. Політика безпеки мережі. URL: Політика_безпеки_мережі (дата звернення: 21.04.2023).

37. Політика інформаційної безпеки. *Alcor.* URL: https://alcor-bpo.com/uk/information-security-policy/ (дата звернення: 21.04.2023).

38. Громико І. Державна домінантність визначення інформаційної безпеки України в умовах протидії загрозам. Право України. 2008. № 8. С.130-134.

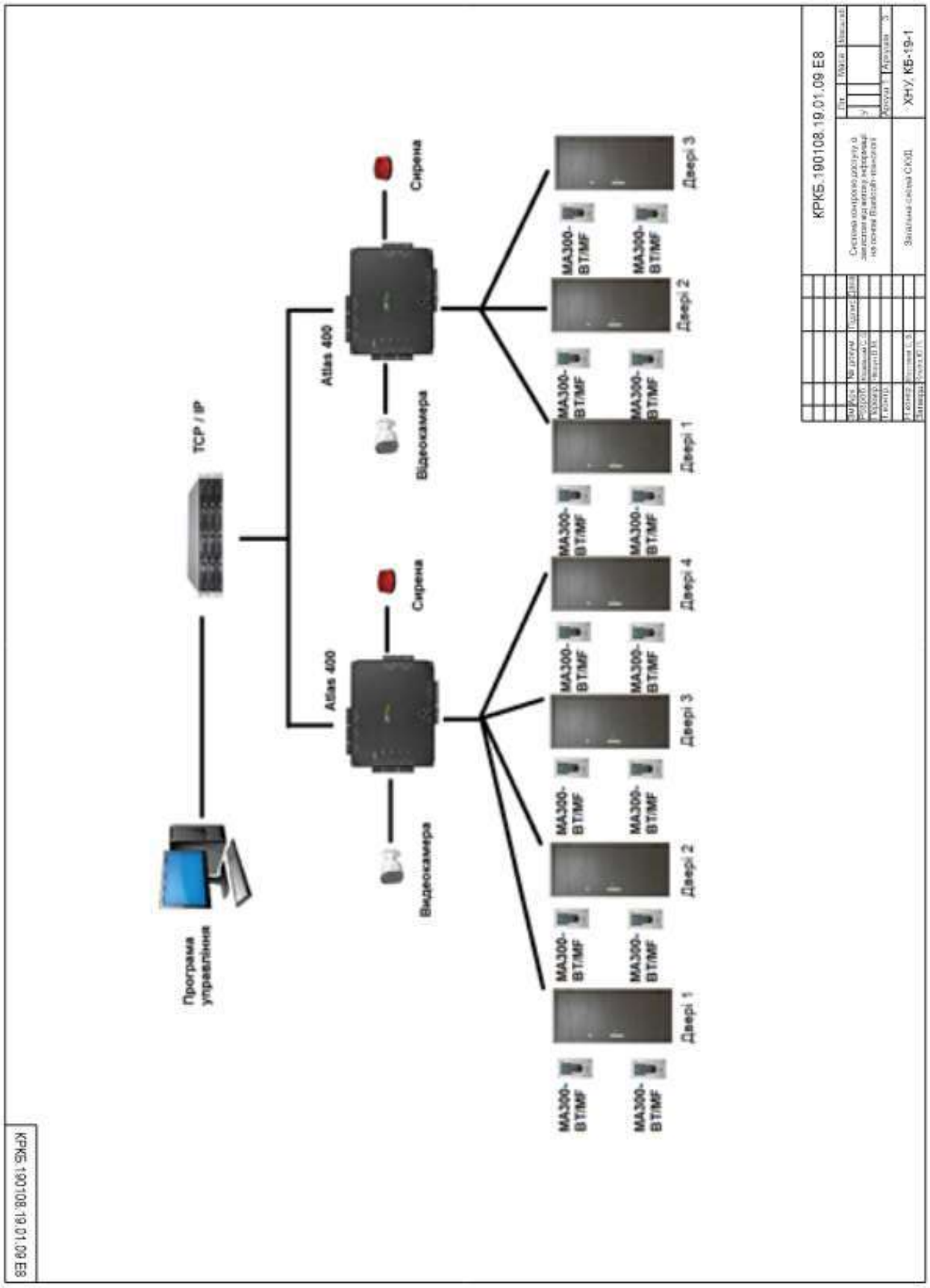
39. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: навчальний посібник. Рекомендовано МОН України для вищих юридичних навчальних закладів. К.: Кондор, 2004. – 384 с.

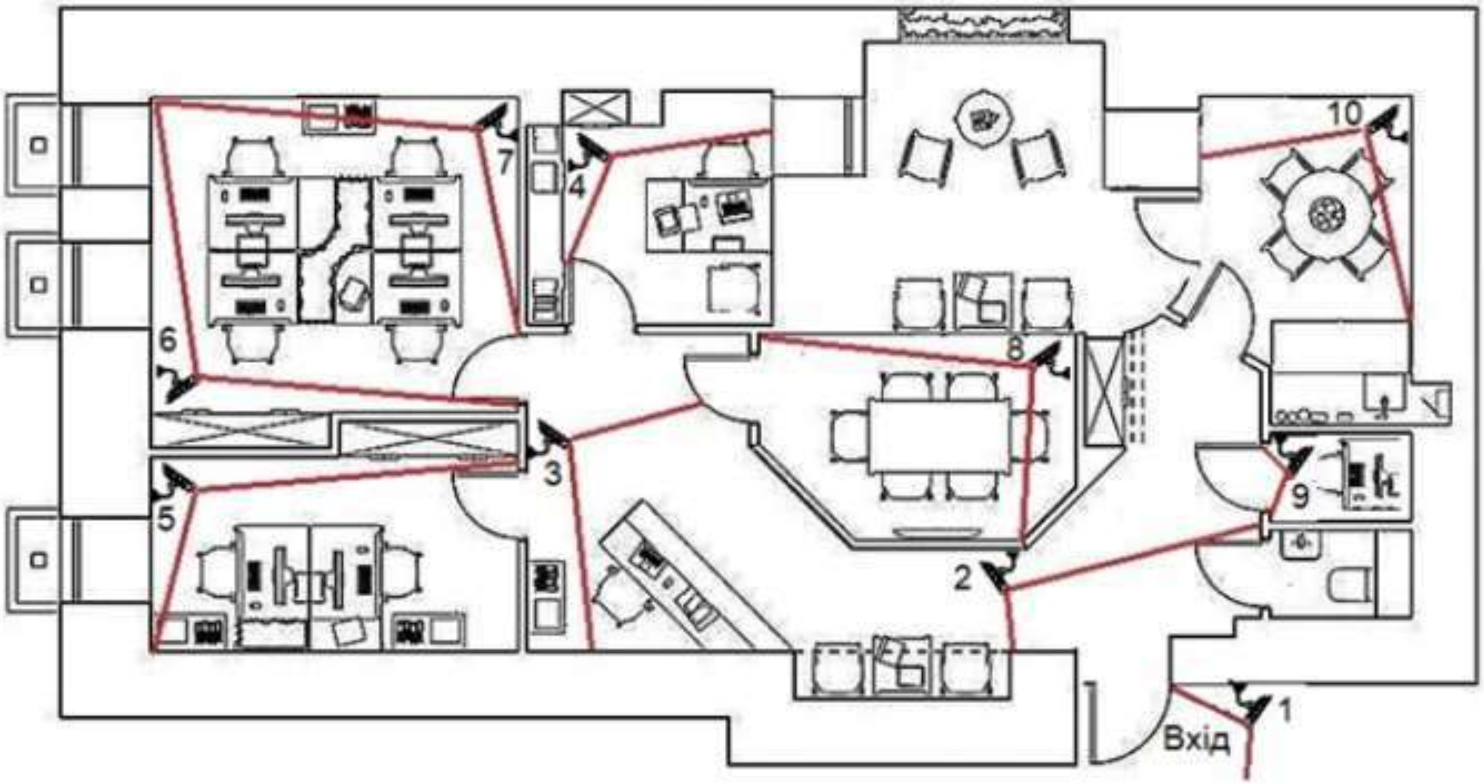
40. Куркін М. В., Понікаров В. Д., Назаренко Д. В. Контроль та захист економічної безпеки діяльності підприємств : навч. посіб. Х. ; ФОП Павленко О. Г.; ВД «ІНЖЕК», 2010. 300 с.

ДОДАТОК А

(обов’язковий)

Копія графічної частини

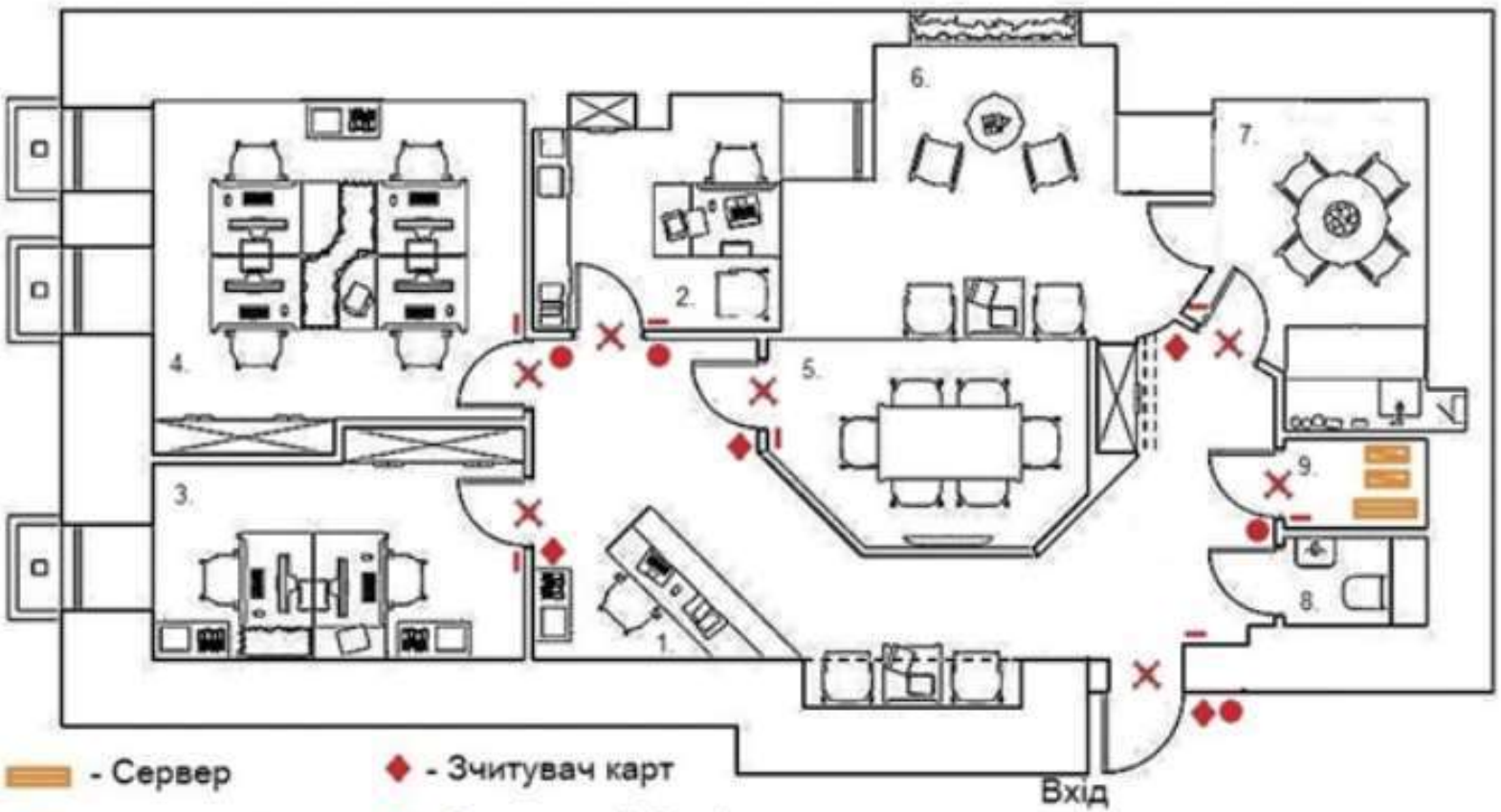




					КРКБ.190108.19.01.09 Е8		
Зм.	Арк.	№ докум.	Підпис	Дата	Система контролю доступу із захистом від витоку інформації на основі Bluetooth-технології	Літ. У	Маса / Масштаб
Розроб.	[illegible]					Аркуш 2	Аркушів 3
Керівн.	[illegible]						
Т. контр.					Схема розміщення відеоспостереження	ХНУ, КБ-19-1	
Н. контр.	[illegible]						
Затверд.	[illegible]						

КРКБ.190108.19.01.09 Е8

КРКБ.190108.19.01.09 ЕВ



					КРКБ.190108.19.01.09 ЕВ		
Змін.	Арк.	№ докум.	Підпис	Дата	Система контролю доступу з елементами ідентифікації інформації на основі Bluetooth-технології	Літ.	Маса	Масштаб
Розроб.		Кошовий С.О.				У		
Керівник		Чекун Д.В.				Аркуш 31	Аркушів 3	
Н.контр.								
Затверд.		Кошовий С.О.			Схема розміщення обладнання СКУД	ХНУ, КБ-19-1		
		Чекун Д.В.						

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «бакалавр»

Студент Медвецький Сергій Олегович

Тема Система контролю доступу із захистом від витоку інформації на основі Bluetooth-технології

Спеціальність 125 – Кібербезпека

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «бакалавр»:

кількість листів креслень 3; кількість сторінок записки 69.

1. Короткий зміст роботи та прийнятих рішень У кваліфікаційній роботі була розроблена система контролю доступу на основі Bluetooth-технології для офісу. Ця система має вбудований захист від витоку інформації. У процесі проєктування були розроблені такі компоненти: система контролю доступу, модель загроз, система відеоспостереження та система розміщення обладнання. Крім того, надані рекомендації для персоналу щодо роботи з конфіденційними даними та використання системи обладнання.

2. Висновок про відповідність кваліфікаційної роботи завданню У кваліфікаційній роботі було виконано поставлене завдання як у теоретичній, так і в практичній частині.

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі роботи наведена загальна характеристика задачі, визначені об'єкт, предмет та методи дослідження, а також сформульована мета. Зазначені задачі, що потрібно виконати для досягнення поставленої мети, проведений аналіз досліджуваної проблеми та обгрунтований підхід до її вирішення. У першому розділі розглядаються об'єкти захисту інформації та системи контролю доступу. Наступні розділи присвячені розробці системи контролю доступу на основі Bluetooth-технології із захистом від витоку інформації та розміщенню обладнання у приміщенні юридичного агентства "Воля". Також був проведений економічний розрахунок системи.

4. Позитивні сторони роботи Кваліфікаційна робота має практичну цінність. Вона полягає у розробці системи контролю доступу із захистом від витоку інформації на основі Bluetooth-технології, що забезпечує захист інформації та спрощує користування обладнанням. Завдяки цьому підприємство є захищеним від витоку інформації та вторгнення зловмисників. При проєктуванні системи контролю доступу використане сучасне обладнання фірми ZKTeco.

5. Негативні сторони роботи В системі не передбачено резервне живлення на випадок зникнення електроенергії, що є надзвичайно актуальним в сучасних умовах, тому за відсутності електроенергії не буде працювати технологія Bluetooth, стане потреба механічного режиму, що знижує ефективність захисту від вторгнень. Недостатньо деталізоване використання Bluetooth-технології в системі та захист від витоку інформації на основі Bluetooth-технології

6. Оцінка графічного оформлення та пояснювальної записки роботи Графічне оформлення кваліфікаційної роботи відповідає темі роботи та виконане з дотриманням стандартів. В цілому, графічне оформлення є якісним, а пояснювальна записка відповідає нормам оформлення.

7. Відгук про роботу в цілому Кваліфікаційна робота заслуговує позитивної оцінки, оскільки весь матеріал роботи є структурованим, чітким та послідовним. Усі розділи роботи мають логічну послідовність, що сприяє зрозумінню викладеного матеріалу в рамках теми роботи. Графічний матеріал допомагає наочно продемонструвати доцільність та ефективність прийнятих рішень для досягнення мети.

8. Інші зауваження В переліку використаних джерел наявні посилання на популярні ресурси, такі, як Вікіпендія, які не рекомендовано використовувати при написанні кваліфікаціних робіт.

9. Оцінка кваліфікаційної роботи Враховуючи всі позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що вона заслуговує оцінки «добре».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи)
Підченко Сергій Костянтинович,
завідувач кафедри ТМІТ, доктор технічних наук, професор

«7» 06 2023. (підпис)

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:
Назва: Система контролю доступу із захистом від витоку інформації на основі Bluetooth-технології

Автор: Медвецький Сергій Олегович

Спеціальність: 125 – Кібербезпека

Освітня програма: освітньо-професійна

Науковий керівник: Чешун Віктор Миколайович, к.т.н, доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою Unichek складає 94.52%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v-15.257 складає 99%.

Згідно з Положенням про дотримання академічної доброчесності в Хмельницькому національному університеті (http://www.khnu.km.ua/root/files/01/10/03/0005.pdf) така авторська робота, обсяг оригінального тексту у відсотках до загального обсягу матеріалу в якій складає 90-100 %, визнається роботою з високою унікальністю тексту.

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1. Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості, складає 5.48%, з яких 1.22% є збігами з одним джерелом, зумовленими наявністю типових фразеологічних виразів предметної області, а також формулюваннями, які утворюють загальновживані фрази.
2. Інші збіги є збігами в назвах використаних друкованих видань, розміщених в переліку джерел посилань, а також в типових складових стандартних

Керівник роботи _____ В. М. Чешун

Завідувач кафедри кібербезпеки _____ Ю. П. Кльоц

UNICHECK

Ім'я користувача:
Кафедра кібербезпеки

ID перевірки:
1015458738

Дата перевірки:
06.06.2023 14:04:33 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
06.06.2023 14:05:02 EEST

ID користувача:
100008300

Назва документа: **Медвецький**

Кількість сторінок: **69** Кількість слів: **13829** Кількість символів: **107792** Розмір файлу: **1.12 MB** ID файлу: **1015118163**

5.48%
Схожість

Найбільша схожість: **1.22%** з джерелом з Бібліотеки (ID файлу: **1015105543**)

4.4% Джерела з Інтернету	349	Сторінка 71
1.68% Джерела з Бібліотеки	76	Сторінка 72

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 1.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 8%**

	Документ		Сумарний збіг по Базі Даних	
ID: 114923 Назва: Система контролю доступу із захистом від витоку інформації на основі Bluetooth-технології Додано в БД: 2023-06-06 Автора: Медвецький С.О. Керівники: Чешун В.М, Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	83019	1292	877 (1%)	15 (1%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми