Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Система контролю та управління доступом для підвищення рівня інформаційної безпеки підприємства
Назва теми

КРКБ. 190103.19.01.04 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, Джиган О.Р. (Ініціали, прізвище)

Керівник — Підпис, дата 02.06.23, Тітова В.Ю. (Ініціали, прізвище)

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

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

7 06 2023р.

Хмельницький, 2023

Форма	Зона	Позиц	Позначення	Найменування	Кільк.	Прим.
А4		1	КРКБ.190103.19.01.04 ПЗ	Система контролю	66	
				та управління доступом		
				для підвищення рівня		
				інформаційної безпеки		
				підприємства		
				Пояснювальна записка		
А4		2	КРКБ.190103.19.01.04 Е8	Схема розміщення	1	
				відеоспостереження		
А4		3	КРКБ.190103.19.01.04 Е8	Схема розміщення датчиків	1	
				руху і розбиття скла		
А4		4	КРКБ.190103.19.01.04 Е8	Модель загроз і модель	1	
				порушника		

Зм.	Арк.	№ Докум.	Підп.	Дата	КРКБ.190103.19.01.04 ВП		
Розробив		Джиган О. Р.		7.06.21	Система контролю та управління доступом для підвищення рівня інформаційної безпеки підприємства Відомість проекту	Літера	Аркуш	Аркушів
Перев.		Тітова В. Ю.		7.06.21		н	1	1
Н. контр.		Мостовий С.В.		7.06.21		ХНУ, КБ-19-1		
Затв.		Кльоц Ю.П.		7.06.21				

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

Джиган О. Р.

Прізвище, ім'я, по батькові студента

1. Тема роботи *Система контролю та управління доступом для підвищення рівня інформаційної безпеки підприємства*

Керівник роботи *к.т.н., доцент Тітова В. Ю.*

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

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

2. Строк подання студентом роботи на кафедру

3. Вихідні дані до проекту (роботи) *Завдання кваліфікаційної роботи полягає у створенні системи, що забезпечує контроль доступу до цих зон та підвищує загальний рівень безпеки підприємства. Проблеми, які необхідно вирішити, включають несанкціонований доступ до приміщень, можливість витоку конфіденційної інформації та відсутність ефективної системи контролю доступу для співробітників. Вимоги до системи полягають у її надійності, швидкості реагування, простоті використання та здатності інтегруватися з існуючими пристроями та інфраструктурою підприємства.*

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити) *дослідити предметну область, існуючі рішення та провести аналіз наявних проблем , вимог та потреб підприємства. Спроектувати і розробити систему контролю та управління доступом, розробити модель загроз та модель порушника. Провести оцінку ефективності впровадженої системи контролю та управління доступом, а також оцінку рівня інформаційної безпеки підприємства.*

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень): *«Схема розміщення відеоспостереження», «Схема розміщення датчиків руху і розбиття скла», «Модель загроз і модель порушника».*

6. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання _____ 2023р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) кваліфікаційної роботи	Термін виконання етапів проекту (роботи)	Примітка
1	Вибір і затвердження теми кваліфікаційної роботи	Лютий	–
2	Аналіз об`єкта дослідження	Березень	–
3	Проектування та розробка загальної архітектури і структури системи	Березень	–
4	Постановка задачі	Квітень	–
5	Реалізація запропонованого рішення та тестування системи; аналіз результатів і оцінювання прийнятих рішень	Квітень	–
6	Написання тексту пояснювальної записки та розробка графічних матеріалів	Квітень\Травень	–
7	Остаточне коригування кваліфікаційної роботи з урахуванням зауважень керівника	Травень	–
8	Оформлення пояснювальної записки згідно вимог	Травень	–
9	Оформлення графічної частини	Травень	–

Студент _____ Джиган О.Р.
Підпис Ініціали, прізвище

Керівник проекту (роботи) _____ Тітова В.Ю.
Підпис Ініціали, прізвище

прийняв

Примітка

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Система контролю та управління доступом для підвищення рівня інформаційної безпеки підприємства».

Автор роботи: Джиган Олександр Русланович.

Керівник роботи: Тітова Віра Юріївна.

Пояснювальна записка: 66 с., 1 додаток, 23 рис., 40 джерел.

Графічна частина: 12 презентаційних слайдів.

Метою кваліфікаційної роботи є проектування та розробка системи управління та контролю доступом, яка дозволить підвищити рівень інформаційної безпеки підприємства.

У кваліфікаційній роботі була спроектована архітектура системи, що включала в себе використання пристроїв Ajax Systems, таких як хаб, датчики руху, датчики розбиття скла, датчики відкриття дверей, датчик протікання, систему оповіщення та біометричний пристрій для автентифікації працівників.

У процесі реалізації системи була врахована безпека, і були вжиті заходи для запобігання можливим загрозам та забезпечення захисту під час впровадження системи контролю та управління доступом.

Завершальним етапом роботи була оцінка ефективності впровадженої системи, де проведено аналіз результатів впровадження та визначено, наскільки система контролю та управління доступом спромоглася підвищити рівень інформаційної безпеки на підприємстві.

07.06.2023

О.Р.
зище

О.
зище

ANNOTATION

Course project: «Access control and management system to increase the level of information security of the enterprise».

Author of the work: Dzhyhan O. R.

Supervisor: Titova V. Y.

Amount - 66 pages, 1 application, 23 figures, 40 sources.

Graphic part: 12 presentation slides.

The purpose of the qualification work is to design and develop a management and access control system that will allow to increase the level of information security of the enterprise.

The qualification work designed a system architecture that included the use of Ajax Systems devices such as a hub, motion sensors, glass break sensors, door opening sensors, a leak sensor, an alert system and a biometric device for employee authentication.

In the process of implementing the system, security was taken into account, and measures were taken to prevent possible threats and ensure protection during the implementation of the access control and management system.

The final stage of the work was the evaluation of the effectiveness of the implemented system, where the implementation results were analyzed and the extent to which the access control and management system managed to increase the level of information security at the enterprise was determined.

07.06.2023

ЗМІСТ

ВСТУП

Інформаційна безпека є однією з найважливіших проблем, з якою стикаються сьогодні багато компаній. Несанкціонований доступ до конфіденційної інформації може призвести до серйозних наслідків, таких як втрата даних, шкода діловій репутації або фінансові втрати. Однак забезпечення належного рівня захисту може бути складним завданням, особливо якщо в компанії багато співробітників і використовується багато різних інформаційних систем.

Розробка та впровадження ефективних заходів безпеки інформації є одним із головних пріоритетів будь-якої організації, яка володіє інформаційними ресурсами та покладається на їх успішне функціонування. Сьогодні, з широким розповсюдженням комп'ютерної техніки та популяризацією Інтернет-технологій, інформаційна безпека стає все більш актуальною проблемою, яка повинна вирішуватися на всіх рівнях від окремого пристрою до всієї мережі.

Однією з основних загроз інформаційній безпеці є незаконний доступ. Несанкціонований доступ до інформації може призвести до її втрати або знищення та поставити під загрозу конфіденційність і цілісність даних. Тому вирішення проблеми контролю та управління доступом до інформації стало надзвичайно актуальним для забезпечення її безпеки.

Одним з найбільш ефективних і поширених заходів є використання систем контролю та управління доступом. Ці системи можуть обмежувати доступ до конфіденційної інформації, контролювати поведінку користувачів і мережевих ресурсів, а також встановлювати права доступу до різних ресурсів для різних користувачів. Використання таких систем підвищує рівень інформаційної безпеки та знижує ризик несанкціонованого доступу до інформації.

Крім того, відкриті мережі та погано захищені пристрої можуть призвести до несанкціонованого доступу до конфіденційної інформації, що призведе до серйозних збитків для бізнесу. Загальновідомо, що одним із ключових способів запобігти цьому є наявність систем контролю та управління доступом.

Така система дозволяє забезпечити безпеку проти несанкціонованого доступу до різноманітних ресурсів, таких як приміщення, комп'ютерні системи, бази даних, електронні документи тощо. Крім того, система контролю та управління доступом дозволяє встановлювати і контролювати рівень доступу різних користувачів до різних ресурсів, що допомагає забезпечити конфіденційність даних і підвищує рівень інформаційної безпеки.

Однак, вибір системи контролю та управління доступом є важливим етапом впровадження такої системи. Необхідно враховувати багато факторів, таких як розмір підприємства, типи ресурсів, що необхідно захистити, кількість користувачів і їхніх рівнів доступу, а також бюджет і доступність різних рішень.

Сьогодні багато компаній використовують системи контролю та управління доступом як засіб забезпечення безпеки інформації. Ці системи дозволяють обмежувати доступ до певних ресурсів та контролювати взаємодію користувачів з інформацією на підприємстві. Однак, не всі підприємства використовують такі системи через їх складність і високу вартість.

Саме тому розробка системи контролю та управління доступом є важливою задачею, яка може забезпечити не тільки високий рівень інформаційної безпеки, але й допомогти підприємству ефективніше управляти своїми ресурсами та знизити витрати на підтримку безпеки інформації.

Моя робота має на меті допомогти підприємствам забезпечити безпеку своїх даних та інформації, зменшити витрати на їхнє захист та уникнути можливих витоків даних.

1 ТЕОРЕТИЧНІ АСПЕКТИ СИСТЕМ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ

1.1 Аналіз предметної області і виявлення наявних проблем і завдань

Життя всіх людей тісно пов'язане із необхідністю регулярної взаємодії з різними компаніями. Підприємства виробляють товари, надають послуги та наймають людей працювати. Що стоїть за терміном «підприємство» та які типи підприємств є в Україні?

Відповідно до статті 62 ГК України «підприємство» - це самостійний господарюючий суб'єкт, зареєстрований компетентним органом державної влади або органом місцевого самоврядування з метою задоволення суспільних та особистих потреб шляхом систематичного здійснення виробництва, наукових досліджень, торгівлі та інших видів господарської діяльності у порядку, встановленому Господарським кодексом України та іншими законами. Основним завданням компанії є задоволення потреб ринку у своїх товарах чи послугах з метою отримання прибутку. Термін "компанія" відноситься до певної організаційної форми корпоративного управління, яка діє як незалежна організація [3].

Українські компанії можуть бути створені для господарювання, не пов'язаної з торгівлею, або, навпаки, для зайняття підприємницькою діяльністю.

Законодавством України передбачені такі види компаній за формами власності:

- приватні підприємства;
- підприємства колективної власності;
- комунальні підприємства;
- державні підприємства;
- підприємства зі змішаною формою власності;
- спільні комунальні підприємства.

Якщо статутний капітал компанії становить 100% іноземної участі, така компанія вважається іноземною. Якщо статутному капіталі щонайменше 10% іноземної участі, компанія вважається компанією з іноземними інвестиціями.

Залежно від формування статутного капіталу та способу реєстрації в Україні передбачено корпорації та унітарні компанії.

Унітарні товариства утворюються одним засновником, який займається формуванням статутного капіталу, придбанням майна, затвердженням статуту та розподілом доходів товариства. Усі муніципальні та державні підприємства вважаються унітарними. Крім того, до унітарних підприємств належать усі підприємства, відкриті на приватній власності засновника, власності громадського об'єднання чи релігійної організації.

При реєстрації корпорацій зазвичай беруть участь два або більше засновників, які діють відповідно до підписаного договору. Термін «корпорація» включає всі організаційно відокремлені підрозділи, створені у формі товариства або компанії, заснованої на приватних активах декількох осіб [6].

Предметною областю моєї роботи виступає ІТ-компанія.

Сьогодні ІТ-структури набувають все більшої популярності, і легко зрозуміти чому. Це бізнес, який дозволяє примножити ваші фінансові можливості за короткий проміжок часу з мінімальними ризиками та втратами. Найбільш поширеними сьогодні є ІТ-компанії, які надають послуги з розробки, підтримки та вдосконалення програмного забезпечення.

У трендах прості моделі своїх конструкцій. Роботодавці шукають приміщення, закуповують необхідне для роботи обладнання та наймають людей для виконання роботи. Здається, що рішення дуже просте, і з ним не повинно виникнути проблем. Але це стосується лише тих випадків, коли кількість людей еквівалентна, яку може контролювати одна особа – у нашому випадку це власник цієї компанії [7].

Але які наслідки для того, хто має необхідні знання та розуміння безпеки

та вирішує відкрити власну IT-компанію?

По-перше, це пожежна безпека.

Офісне середовище є надто звичайним робочим місцем для людей з усіх верств суспільства. Оскільки багато людей проводять свій день в офісі, важливо враховувати пожежну безпеку на робочому місці, особливо в офісі.

Важливою частиною пожежної безпеки є пожежна безпека. Основною причиною пожеж в офісах є електророзподілення, на яке, як було показано, припадає 31% усіх пожеж в офісах. Переконавшись, що всі працівники знають, як запобігти пожежі та що робити у разі пожежі, можна не тільки заощадити компанії багато грошей, але й врятувати життя та запобігти травмам [6].

Загальні небезпеки пожежі:

Вас може здивувати, що багато пожеж в офісах мають схожі причини. Знання типових небезпек пожеж може допомогти запобігти пожежам.

Ось основні небезпеки, про які слід знати в офісних будівлях:

– Електричне обладнання, як-от копіювальні апарати, не обслуговується належним чином або не перевіряється PAT (збої в електриці є основною причиною пожеж);

– Неналежне зберігання паперу, карток та інших легкозаймистих матеріалів, як-от В. під столами або поблизу електричного обладнання;

– Нещасні випадки, спричинені використанням електрообладнання без нагляду, наприклад тостерів, на кухні команди.

Усі робочі місця повинні пройти оцінку пожежної безпеки (FSA), яку іноді просто називають «оцінкою ризику». Оцінки ризиків не пояснюються, вони оцінюють ризик. У сфері пожежної безпеки наполегливо рекомендується, щоб компетентна, досвідчена та обізнана особа проводила оцінку ризику від імені відповідальної особи.

Оскільки щороку в нежитлових будівлях виникає понад 22 000 пожеж, важливо, щоб оцінки ризиків були оновленими та регулярно переглядалися.

Цікаво, що лише 4950 з цих пожеж виникли внаслідок підпалів; решта були класифіковані як «випадкові» [8].

Звичайно, для більшості з нас ми не знаємо, як визначити небезпеку пожежі, оцінити ризики та усунути їх, тому ми рекомендуємо вам знайти когось, хто може допомогти з цією проблемою. Це частина відповідальної людини.

Повідомлення інформації, що міститься в оцінці пожежної безпеки, усім співробітникам має вирішальне значення для забезпечення дотримання оцінки ризику під час надзвичайної ситуації та забезпечення того, щоб працівники знали, що робити щодня, щоб зменшити ризик пожежі.

Працюючи в компанії Sheep.Fish, навіть не детально аналізуючи систему захисту, я помітив, що компанія чомусь не належним чином поставилася до захисту підприємства.

Але проаналізувавши, можу сказати, що хоча офіс компанії знаходиться в офісному центрі, це не повністю захищає саму компанію, тому що офіс має окремий вхід, який можна закрити лише на ключ. Щоб потрапити в офіси, вам потрібно пройти через окремі вхідні двері в офісному центрі, а потім через передні двері в самому офісі, тому я був здивований, що жодні з дверей не мали сканера відбитків пальців, щоб ідентифікувати персонал і запобігти доступу до приміщення, призначені для сторонніх осіб.

Компанія має два офіси - відділ продажів, де працюють менеджери з продажу, і головний офіс, де працюють розробники, дизайнери, тестувальники, менеджери та офісні працівники.

Жоден із сайтів не має системи ідентифікації співробітників, що ставить під загрозу безпеку конфіденційних даних і самого підприємства, оскільки всередині компанії кожен співробітник оснащений робочим пристроєм, який, крім того, що він дорогий, включений у розробку проекту. , робота, та файли загальної конфіденційної інформації. Так, усі комп’ютери захищені паролем, але я вважаю, що ризик є завжди.

Крім того, підприємство не встановило сигналізацію на території, встановило камери відеоспостереження на входах у приміщення центрального офісу та безпосередньо на самих приміщеннях.

Моєю наступною точкою дослідження були домашні системи екстреного виклику, наприклад, я помітив, що немає пристрою, який би сповіщав власників будинків про витік водопровідних труб. В офісі знаходиться величезна кількість обладнання, і найменший контакт з вологою поглинається за лічені секунди, спричиняючи не тільки вихід обладнання, але й усі дані, що містяться на обладнанні.

1.2 Огляд існуючих систем контролю та управління доступом

У цьому розділі ми розглянемо існуючі системи контролю та управління доступом.

Система контролю доступу (ACS) — це електронна система, яка керується через мережу і забезпечує доступ до мережі. Система контролю доступу розпізнає облікові дані людини та надає їй доступ до об’єкта, забезпечуючи тим самим його захист [1].

Системи контролю доступу (ACS, ACS) забезпечують безпеку, дозволяючи легкий доступ для авторизованого персоналу.

Одна з найбільш часто використовуваних електронних систем керування дверима, ACS, використовує картки, чіпи або біометричні дані для обмеження доступу авторизованого персоналу.

Організації або сфери, які вимагають високого рівня безпеки, використовують різні типи систем контролю доступу, такі як біометрія, RFID та пристрої для зчитування карток. Кожен запис можна окремо контролювати політикою компанії, якщо потрібна висока безпека. Кібербезпека також

важлива, особливо в компаніях, які мають справу з конфіденційними даними [2].

Можна побачити, що система контролю доступу – це комплексний контрольно-управлінський програмно-технічний засіб, який спрямований на обмеження та реєстрацію входу та виходу об’єктів (людей, транспортних засобів) на конкретні об’єкти через «точки контролю доступу»: двері. , ворота, стенд огляду.

Системи фізичної безпеки та контролю доступу стали обов’язковими для більшості компаній. Великим і малим компаніям потрібно захистити свої об’єкти, дані та людей. Нижче наведено приклади того, що входить до системи фізичної безпеки та контролю доступу. Приклад СКУД показано на рисунку 1.1.

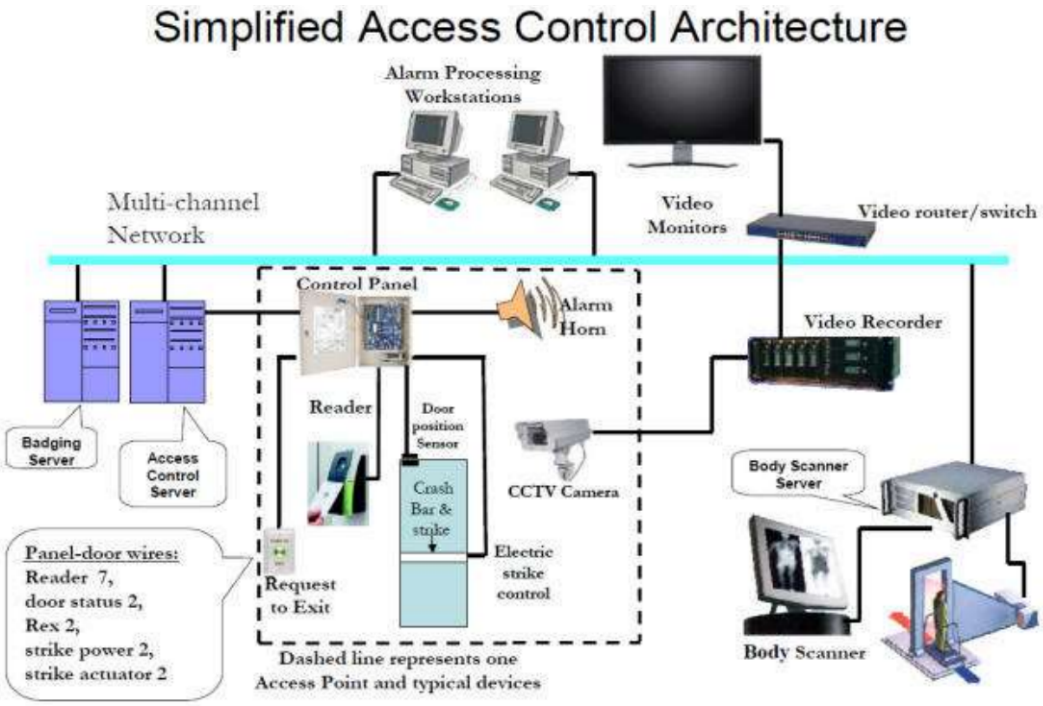


Рисунок 1.1 – Архітектура СКУД

Розглянемо основні компоненти.

Сервер системи контролю доступу (ACS) запускає програмне забезпечення. Він може містити багато серверів на одній машині або може бути розподілений між кількома машинами. Цей сервер відповідає за надання доступу та відстеження трафіку в безпечних зонах. Також підтримується база даних власників облікових

даних та їхніх рівнів доступу. Взаємодійте з панелями ACS, щоб завантажити певні дані на кожну панель для локального флеш-пам’яті.

Сервер може взаємодіяти з панеллю СКУД кількома способами.

Якщо панель оснащена картою Ethernet, зв’язок може базуватися на TCP/IP [3] тощо. Якщо панель оснащена багатоточковим інтерфейсом RS-485, сервер (через конвертер RS-232 в RS-485) буде спілкуватися з кожною панеллю по послідовній шині, опитувати кожну панель і обробляти дані панелі. Сервер ACS також може надавати хости за запитом панелей, які не мають останньої інформації. Сервери ACS планують оновити панелі, але до того часу будуть розміщені співробітники [11].

Відеомаршрутизатори/комутатори забезпечують можливість моніторингу будь-якої камери або мультиплексного зображення на клієнтських робочих станціях системи. Цифрові відеореєстратори зазвичай увімкнені та записують події циклічно. Тривалість циклу залежить від вимог замовника.

Великі корпоративні системи мають багато камер і, можливо, багато записуючих пристроїв. Реєстратори зазвичай розподіляються на обмежену кількість камер на основі їх ємності пам’яті, але вони повинні бути в одній IP-мережі, щоб події можна було викликати та відтворювати за потреби для кожної області [17].

Панель управління забезпечує шлюз між пунктами управління (шлюзи, КПП) і сервером СКУД.

Панель зберігає облікові дані користувача у флеш-пам’яті на випадок, якщо зв’язок між панеллю та сервером стає недоступним. Панель працюватиме в автономному режимі, поки з'єднання не буде відновлено.

Існують різні типи панелей та інтерфейсів для підключення панелей до сервера.

Деякі панелі використовують для зв'язку з сервером протокол Ethernet, інші використовують шину RS-485.

Проте сигнали з блокпостів досить стандартні.

Зазвичай панелі контролюють 2 контрольно-пропускні пункти (двері), але є також панелі зі слотами розширення, які можна розширити до кількох дверей.Типове підключення панелі до дверей показано на рисунку 1.2.

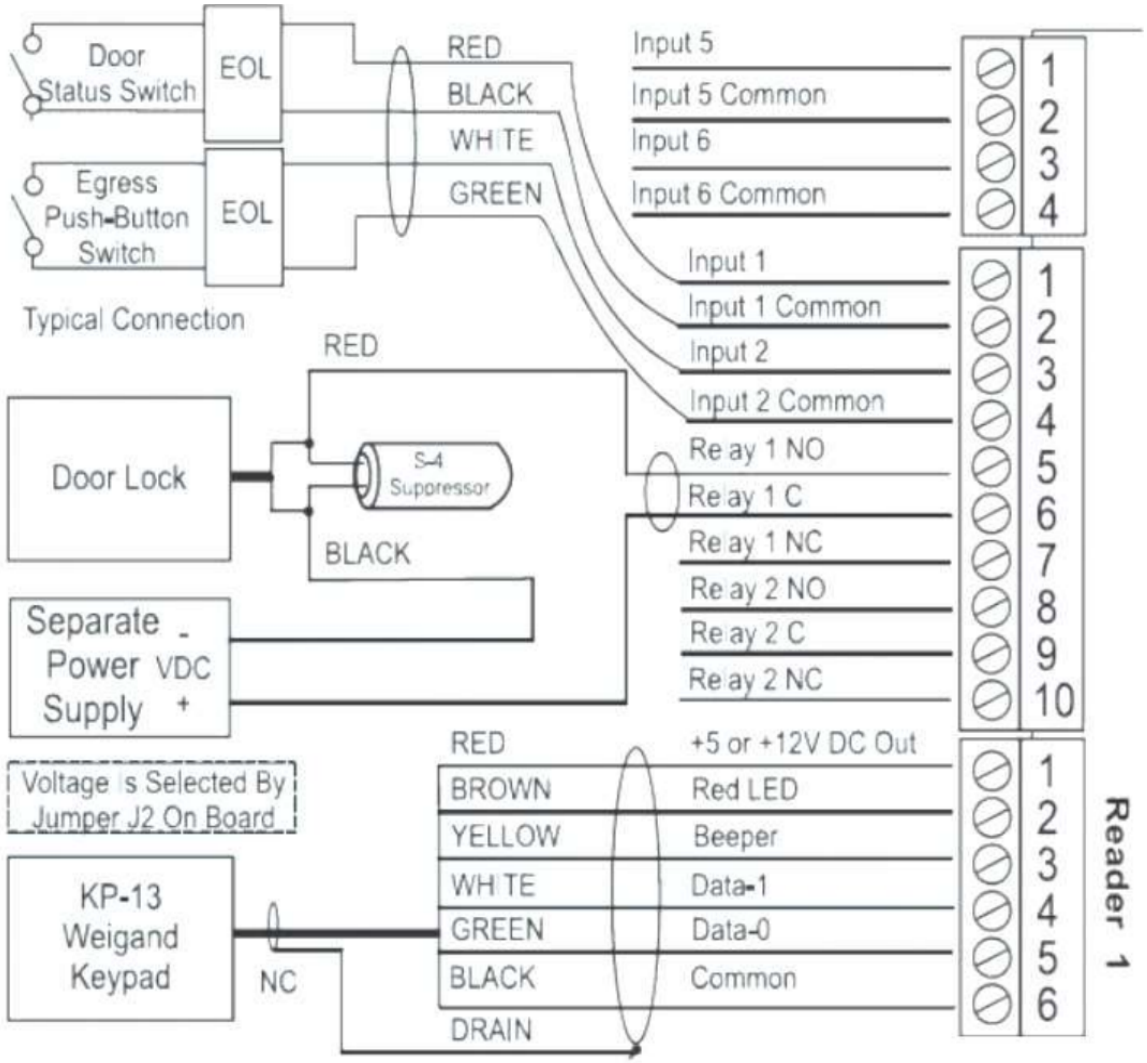


Рисунок 1.2 - Типове з'єднання панелі з дверима

Обладнання дверей складається з пристрою зчитування карток, перемикача положення дверей, кнопки запиту на вихід і електрозамка дверей. Існує багато типів рідерів із різними технологіями.

Зчитувач використовує котушку для створення магнітного поля. Коли картку наближають до пристрою зчитування, магнітне поле створює електричне поле в обмотках карти, живлячи процесор картки, і пакети даних, що містять

інформацію користувача, передаються від карти до пристрою зчитування. Приклади зчитувачів показано на рисунку 1.3.

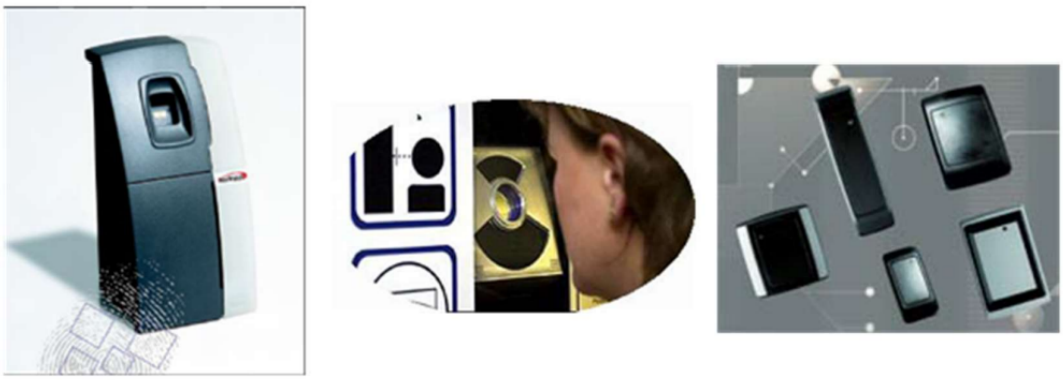


Рисунок 1.3 - Приклади зчитувачів

Перемикачі положення дверей (рисунок 1.4) зазвичай є магнітними перемикачами. Поки дві частини вимикача знаходяться близько одна до одної, вимикач закритий, інакше він розімкнений.

Рисунок 1.4 - Перемикач положення дверей

Електричний замок — це електромагнітний пристрій, який відкриває замок так, що двері можна штовхнути, не повертаючи ручку. Вхідна напруга 12 або 24 В

постійного струму. У деяких випадках використовуються магнітні замки, щоб під час подачі напруги двері утримувалися рамою замка магнітом (рисунок 1.5).

Рисунок 1.5 - Електричний замок

Запит на відмову/вихід — це миттєвий перемикач.

При натисканні ланцюг замикається і сигналізує панелі про відмикання дверей, забезпечуючи вихід із безпечної зони (рисунок 1.6).

Рисунок 1.6 - Запит на вихід/вхід

Таким чином, контроль доступу використовується, щоб ідентифікувати особу, яка виконує роботу, аутентифікувати її, а потім надати цій особі лише ключі від дверей або робочих станцій, до яких їй потрібно отримати доступ.

Існує три типи систем контролю доступу: дискреційний контроль доступу (DAC), обов'язковий контроль доступу (MAC) і рольовий контроль доступу (RBAC).

Розглянемо дискреційний контроль доступу (DAC).

Дискреційний контроль доступу – це система контролю доступу, яка надає особам, які приймають рішення, відповідальність за прийняття рішення про те, кому дозволено відвідувати певне місце, фізично чи цифрово.

DAC є системою з найменшими обмеженнями порівняно з іншими системами, оскільки вона, по суті, дозволяє кожному повністю контролювати будь-які об’єкти, якими вони володіють, і програми, пов’язані з цими об’єктами. Недоліком дискреційного контролю доступу є те, що він надає кінцевому користувачеві повний контроль для налаштування рівня безпеки та прав доступу, встановлених для інших користувачів. Дані кінцевих користувачів успадковуються в інших програмах, які вони використовують, що може призвести до впровадження 19 типів зловмисного програмного забезпечення в підприємство без відома кінцевого користувача [14].

Розглянемо обов'язковий контроль доступу (MAC).

Обов'язковий контроль доступу частіше використовується в організаціях, які вимагають більшої уваги до конфіденційності та класифікації даних (наприклад, у військових відомствах). MAC не дозволяє власнику мати право голосу в організації, яка має доступ до підрозділу чи об’єкта, лише власник має право керування доступом. MAC зазвичай класифікує всіх кінцевих користувачів і призначає їм теги, які дозволяють їм отримати доступ через систему безпеки зі встановленими правилами безпеки.

Контроль доступу на основі ролей (RBAC) RBAC, також відомий як контроль доступу на основі правил або ролей, є найпопулярнішою системою контролю доступу. RBAC користується великим попитом не лише вдома, а й у діловому світі.

У системі RBAC права доступу призначаються системними адміністраторами та суворо залежать від ролі принципала в бізнесі чи організації, при цьому більшість прав базується на обмеженнях, визначених їхніми посадовими обов’язками.

1.3 Аналіз принципів побудови систем контролю та управління доступом

Контроль доступу є однією зі складових комплексної концепції, процесу забезпечення безпеки підприємства [18].

Сучасна система контролю та управління доступом до мережі (ACMS) може забезпечити необхідний рівень захисту даних, що складаються з тисяч точок доступу та десятків тисяч користувачів. Крім того, ці системи є основою для побудови комплексної системи безпеки.

Якісний аналіз і проектування необхідні для успішної розробки інформаційних систем. Фундаментальні аспекти системного моделювання та рішення визначаються на початковому етапі, і успіх проекту значною мірою залежить від цих аспектів.

Послідовність розробки моделі АСУ є структурою, яка може бути розширена відповідно до типу та призначення інформаційної системи.

Етап визначення функціональних вимог може супроводжуватися багатьма проблемами через складність чітко визначених завдань, які залежать від ІС, різні погляди на майбутнє функціонування системи та недостатнє знання замовниками можливостей сучасного комп’ютера22. Системи та ідеї автоматизації процесів.

Побудова функціональної моделі повинна вирішити більшість цих проблем.

Тому існує нагальна потреба у розробці методики проектування СКУД.

Принцип побудови системи контролю та управління доступом на підприємстві базується на використанні технологій, що забезпечують захист інформації від несанкціонованого доступу.

Для підвищення рівня інформаційної безпеки підприємства можна прийняти наступні принципи побудови системи контролю та управління доступом:

– принцип моделі для наслідування, тут системи контролю та управління доступом повинні базуватися на моделі для наслідування, яка забезпечує доступ на основі ролі користувача в організації. Це дозволяє надавати різні рівні доступу різним користувачам залежно від їхніх ролей і дозволів;

– принцип двофакторної автентифікації, в даному принципі системи контролю та управління доступом повинні передбачати використання двофакторної автентифікації для підтвердження особи користувача. Це знижує ризик несанкціонованого доступу до системи за допомогою вкрадених логінів і паролів;

– принцип аналізу ризиків, тут системи контролю та управління доступом повинні базуватися на аналізі ризиків та ідентифікації потенційних загроз для інформації та об’єктів на підприємстві. Це дає змогу вчасно виявити потенційні загрози та вжити необхідних заходів для безпеки;

– принципи контролю доступу на рівні даних, даний принцип говорить про те, що системи контролю та управління доступом повинні базуватися на принципах контролю доступу на рівні даних, щоб забезпечити захист персональних даних та об’єктів від несанкціонованого доступу;

– принципи керування правами доступу, а тут системи контролю та керування доступом повинні надавати можливість керувати правами доступу, дозволяючи адміністраторам встановлювати та змінювати права доступу користувачів відповідно до їхніх ролей та дозволів. Це дозволяє контролювати доступ користувачів і зменшити ризик несанкціонованого доступу;

– принцип аудиту та моніторингу, в даному пункті системи контролю та управління доступом повинні забезпечувати можливість перевірки та моніторингу доступу користувачів до інформації та об’єктів підприємства. Це дозволяє виявити несанкціонований доступ і вжити необхідних заходів для забезпечення безпеки;

– принцип запобігання вторгненням, системи контролю та управління доступом повинні забезпечувати захист від вторгнення, що гарантує, що

інформація та об’єкти на підприємстві захищені від несанкціонованого доступу із зовнішніх джерел;

– принципи захисту від внутрішніх загроз, тут системи контролю та управління доступом повинні забезпечувати захист від внутрішніх загроз, щоб гарантувати, що інформація та об’єкти підприємства захищені від несанкціонованого доступу його співробітників [16].

Застосування цих принципів допоможе підвищити рівень інформаційної безпеки підприємства, забезпечити контроль і управління доступом користувачів до інформації та об’єктів підприємства, знизити ризик несанкціонованого доступу. Важливо також пам’ятати, що системи контролю та управління доступом повинні постійно підтримуватися та оновлюватися відповідно до змін у внутрішньому та зовнішньому середовищі підприємства, а також повинні бути інтегровані з іншими системами безпеки на підприємстві, такими як системи виявлення вторгнень.

Щоб створити ефективну систему контролю та управління доступом на підприємстві, також необхідно враховувати потреби та характеристики самого підприємства. Наприклад, велика корпорація може використовувати централізовану систему керування доступом, яка забезпечує рівномірний доступ до інформації та об’єктів на підприємстві. Невеликі підприємства можуть використовувати децентралізовану систему, де кожен відділ має власну систему контролю та управління доступом.

Важливо також враховувати різні рівні доступу користувачів до інформації та об’єктів на підприємстві, а також використання сучасних методів захисту інформації, таких як шифрування, двофакторна аутентифікація та біометрія.

Загалом, створення ефективної системи контролю та управління доступом на підприємстві є складним процесом, який вимагає глибокого розуміння потреб та особливостей підприємства, а також використання сучасних технологій та дотримання принципів інформаційної безпеки.

1.4 Постановка задачі

Метою дипломної роботи є розробка системи контролю та управління доступом для підвищення рівня інформаційної безпеки підприємства. Завдання – розробити ефективну систему захисту конфіденційної інформації та корпоративних об’єктів від несанкціонованого доступу.

Для досягнення поставленої мети, необхідно виконати наступні завдання:

– проаналізувати потреби підприємства в системі контролю та управління доступом, з'ясувати основні вимоги до функціональності та безпеки системи;

– побудувати модель потенційного порушника, яка дозволить визначити можливі загрози та вразливості системи контролю та управління доступом, та розробити заходи по їх усуненню;

– проаналізувати існуючі технології та рішення з контролю та управління доступом, зробити вибір оптимального варіанту для підприємства;

– розробити архітектуру системи контролю та управління доступом, враховуючи вимоги до безпеки та функціональності системи;

– провести аналіз ефективності розробленої системи контролю та управління доступом;

– сформулювати рекомендації щодо подальшого вдосконалення та розвитку системи контролю та управління доступом на підприємстві.

Результатом виконання дипломної роботи має стати розроблена система контролю та управління доступом, що забезпечить захист конфіденційної інформації та об'єктів підприємства від несанкціонованого доступу, зменшить ризик інцидентів зі зломом систем та дозволить забезпечити високий рівень інформаційної безпеки на підприємстві.

2 РОЗРОБКА СИСТЕМИ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ ДЛЯ ПІДПРИЄМСТВА

2.1 Аналіз вимог та потреб підприємства щодо системи контролю та управління доступом

Аналіз вимог і потреб IT-компаній щодо систем контролю та управління доступом включає розгляд основних аспектів, які необхідно враховувати для досягнення мети підвищення рівня інформаційної безпеки. Ось кілька ключових моментів, які слід враховувати під час аналізу:

– конфіденційність даних, наприклад IT-компанії часто мають конфіденційну інформацію, таку як інтелектуальна власність, важливі дані клієнтів, розробки тощо. Вимоги до системи контролю та управління доступом повинні відповідати необхідності забезпечення конфіденційності цієї інформації;

– автентифікація та авторизація, сама система повинна забезпечувати надійну автентифікацію користувача та контрольований доступ до різноманітних ресурсів і функцій системи. Це дозволить вам визначити, хто має доступ до якої інформації та які дії вони можуть виконувати;

– модель для наслідування, також IT-компанії можуть мати різні ролі та рівні доступу, наприклад системні адміністратори, розробники, тестувальники, менеджери тощо. Важливо визначити потреби рольової моделі та призначити права доступу для кожної ролі, забезпечуючи принцип найменших привілеїв;

– системні вимоги повинні включати можливість моніторингу та аудиту доступу користувачів до ресурсів і інформації. Це дозволить виявляти несанкціонований доступ і вчасно реагувати на потенційні загрози;

– масштабованість і розширюваність, тут системи контролю доступу та управління мають бути гнучкими та здатними адаптуватися до зростаючих потреб бізнесу. Він повинен підтримувати збільшення кількості користувачів,

об’єктів доступу та правил без значного впливу на продуктивність та ефективність системи;

– інтеграція з існуючими системами щоб забезпечити безперебійне функціонування та просте впровадження системи контролю та управління доступом, важливо розглянути можливість її інтеграції з існуючими системами, такими як системи ідентифікації користувачів, системи управління подіями або системи моніторингу;

– відповідність нормативним вимогам, всім IT-компаніям може знадобитися дотримуватися нормативних вимог, таких як Загальний регламент захисту даних (GDPR) або стандартів безпеки, встановлених галузевими групами. Системи контролю та управління доступом повинні відповідати цим вимогам і забезпечувати дотримання необхідних кодексів і стандартів;

– забезпечення простоти використання системою має бути легко керувати та використовувати як адміністратори, так і користувачі. Це може включати зручні для користувача інтерфейси, можливість автоматизувати певні процеси та підтримку різних типів автентифікації (наприклад, паролі, біометрія).

Аналізуючи вимоги та потреби IT-компанії, я розглядаю ці та інші аспекти в залежності від конкретних характеристик IT-компанії та конкретних потреб бізнес-процесу. Наприклад, додатково можуть з'явитися такі вимоги:

– багатофакторна автентифікація для того щоб забезпечити вищий рівень безпеки, вам може знадобитися використовувати не лише один фактор автентифікації, наприклад пароль, а комбінацію різних факторів, таких як пароль, фізичний маркер або біометричні дані;

– інтеграція з системами управління інцидентами для того щоб ефективно реагувати на потенційні інциденти безпеки, важливо, щоб системи контролю та управління доступом були інтегровані з системами управління інцидентами. Це дозволить вам швидко виявляти й реагувати на можливі порушення безпеки;

– автоматизований аналіз доступу, враховуючи що ІТ-компаніям можуть знадобитися системи контролю та керування доступом для аналізу та моніторингу активності користувачів для виявлення аномальної або підозрілої поведінки. Це допоможе вчасно виявити потенційні загрози та запобігти інцидентам безпеки;

– сумісність із існуючою інфраструктурою, це якщо ІТ-компанія використовує існуючу інфраструктуру та технологію, важливо, щоб система контролю та управління доступом була сумісна з цією існуючою інфраструктурою. Наприклад, якщо компанія використовує певні системи автентифікації або керування ідентифікацією, система контролю та управління доступом має взаємодіяти з цими системами без проблем;

– резервне копіювання та відновлення для забезпечення безпеки даних потрібен механізм резервного копіювання та відновлення. Система контролю та управління доступом повинна мати можливість створювати резервні копії конфігураційних даних і журналів і відновлювати їх у разі необхідності;

– навчання та обізнаність користувачів: люди часто є слабкою ланкою в системах контролю та управління доступом. ІТ-компаніям можуть знадобитися механізми навчання наявності та обізнаності користувачів щодо інформаційної безпеки та правил використання систем доступу.

Зробивши аналіз вимог та потреб ІТ-компанії, я можу сформулювати конкретні завдання для розробки системи контролю та управління доступом, такі як:

– розробка моделі порушника, щоб визначити типові сценарії загроз безпеці та розробити відповідні стратегії захисту;

– проектування архітектури системи контролю та управління доступом з урахуванням вимог безпеки, масштабованості, інтеграції та доступності;

– визначення набору прав доступу та ролей для різних користувачів відповідно до бізнес-процесів ІТ-компанії;

– розробка механізму автентифікації для забезпечення безпечного доступу до систем, включаючи багатофакторну автентифікацію;

– впровадити аудит доступу, який дозволить відстежувати дії користувачів, збирати журнали та аналізувати їх для виявлення потенційних загроз;

– інтеграція систем контролю та управління доступом з існуючою інфраструктурою та системами, особливо системами управління подіями та іншими рішеннями безпеки;

– розробка процедури резервного копіювання та відновлення даних для забезпечення безпеки та безперервності системи;

– навчання користувачів та поширення свідомості про безпеку інформації, що включає проведення тренінгів, створення документації та підтримку посібників;

– виконання вимог щодо регуляторної відповідності, таких як GDPR, і забезпечення дотримання стандартів безпеки, що стосуються IT-компанії.

Загальний аналіз вимог та потреб IT-компанії забезпечить розуміння основних вимог до системи контролю та управління доступом і допоможе побудувати ефективне та безпечне рішення, яке відповідає унікальним потребам підприємства.

2.2 Проектування архітектури системи контролю та управління доступом

Для того, щоб мати конкретне розуміння самої архітектури системи контролю та управління доступом підприємства, для початку розпишемо кожен її компонент по пунктах.

На основі аналізу вимог та потреб IT-компанії щодо системи контролю та управління доступом, можна спроектувати таку архітектуру:

– компонент ідентифікації та аутентифікації;

– компонент авторизації та керування правами доступу;
– компонент аудиту та моніторингу;
– компонент інтеграції та резервного копіювання;
– компонент управління інцидентами та відповіді на загрози;
– компонент адміністрування та керування;
– компонент масштабування та надійності;
– компонент інтерфейсу користувача.

Тепер розглянемо детальніше кожен компонент.

Компонент ідентифікації та аутентифікації включає в себе реалізацію механізмів автентифікації, включаючи паролі, мультифакторну автентифікацію та біометричні дані, також інтеграцію з існуючими системами автентифікації та ідентифікації і забезпечення безпеки передачі даних під час процесу автентифікації.

Компонент авторизації та керування правами доступу включає в себе визначення ролей та прав доступу для різних користувачів і груп користувачів, управління правами доступу до різних ресурсів, включаючи файли, бази даних, системи та мережеві ресурси, а також можливість гнучкого налаштування прав доступу залежно від ролей, проектів та бізнес-процесів.

Компонент аудиту та моніторингу несе в собі запис і збереження журналів активності користувачів та адміністраторів системи, аналіз журналів для виявлення підозрілої або незвичайної активності і сповіщення та відстежування інцидентів безпеки.

Компонент інтеграції та резервного копіювання повинен складатись з інтеграцій з існуючими системами керування інцидентами, ідентифікації та іншими інфраструктурами і з механізмів резервного копіювання та відновлення для забезпечення безпеки даних.

Якщо говорити про компонент управління інцидентами та відповіді на загрози, то він повинен включати розробку процедур управління інцидентами, включаючи виявлення, реагування, відновлення та аналіз, також встановлення

механізмів сповіщення та тривог для швидкого виявлення та реагування на потенційні загрози безпеки і впровадження інтеграції з системами виявлення вторгнень та системами антивірусного захисту.

Розглядаючи компонент адміністрування та керування, потрібно враховувати модуль управління конфігурацією, який дозволяє налаштовувати правила доступу, ролі користувачів та групи, а також інтерфейс для адміністраторів, що надає можливість управляти користувачами, ролями, правами доступу та іншими параметрами системи.

Дивлячись на компонент масштабування та надійності, то він повинен забезпечувати гнучкість та масштабованість системи контролю та управління доступом, щоб вона могла зростати разом з розширенням бізнесу ІТ-компанії і використання резервних копій, дублювання серверів та механізмів відновлення для забезпечення неперервності роботи системи.

Компонент інтерфейсу користувача має містити розробку зручного та інтуїтивно зрозумілого інтерфейсу для користувачів та адміністраторів системи і мати можливість налаштування особистих налаштувань та управління власним доступом до ресурсів.

Ця архітектура системи контролю та управління доступом відповідає вимогам та потребам ІТ-компанії, забезпечуючи ефективний контроль, захист та управління доступом до ресурсів, підвищуючи рівень безпеки інформації.

Ця архітектура розроблена з урахуванням особливостей ІТ-компанії і здатна відповідати її потребам у забезпеченні надійного та безпечного доступу до систем та даних.

Проектування архітектури системи контролю та управління доступом включатиме такі кроки:

– визначення основних компонентів системи, такі як ідентифікація та аутентифікація, авторизація та керування правами доступу, аудит та моніторинг, інтеграція та резервне копіювання, навчання та свідомість

користувачів, управління інцидентами та відповіді на загрози, адміністрування та керування, масштабування та надійність, інтерфейс користувача;

– визначення взаємозв'язків між компонентами та встановлення протоколів комунікації між ними;

– розробку архітектурної схеми системи, включаючи фізичну і логічну структури;

– визначення необхідних апаратних та програмних засобів для реалізації системи контролю та управління доступом;

– розробку алгоритмів та правил для забезпечення безпеки та ефективності процесу контролю та управління доступом;

– розробку інтерфейсу користувача для зручного взаємодії з системою та налаштування параметрів доступу;

– валідація та тестування розробленої системи для перевірки її ефективності, безпеки та відповідності вимогам ІТ-компанії.

Метою проектування архітектури системи контролю та управління доступом є створення комплексного комплексного рішення для забезпечення високого рівня інформаційної безпеки ІТ-компаній. Система мала відповідати потребам компанії щодо безпеки даних, захисту від несанкціонованого доступу та управління правами користувачів.

Завдання проектування архітектури системи контролю та управління доступом також включають такі не менш важливі пункти:

– розробку моделі порушника, яка в собі несе такі елементи як вивчення типових загроз та атак, які можуть бути спрямовані на ІТ-компанію, також аналіз сценаріїв атак та визначення потенційних загроз безпеці і розробку моделі порушника, яка враховує характеристики та мотивації потенційних зловмисників;

– розробку механізмів контролю та управління доступом, що має також встановлення механізмів ідентифікації та аутентифікації користувачів, включаючи використання паролів, мультифакторної автентифікації та

біометричних методів, сюди ще входить розробка системи управління ролями та правами доступу, яка дозволяє визначати рівні доступу для користувачів та груп користувачів, реалізація механізмів автоматичного призначення та зняття прав доступу в залежності від змін у ролях та робочих обов'язках користувачів та інтеграція з існуючими системами управління ідентифікацією та автентифікацією, такими як Active Directory або LDAP;

– забезпечення безпеки та конфіденційності даних, до цього входить використання шифрування для захисту передачі та збереження конфіденційних даних, розробка політик та процедур щодо управління ключами шифрування та контролю доступу до них, також встановлення механізмів захисту даних, таких як захист від несанкціонованого доступу, аудит доступу до конфіденційних даних та моніторинг змін даних;

– навчання та свідомість користувачів, оскільки вони завжди повинні бути готовими до різних ситуацій, тому цей компонент включає в себе розробку програми навчання для користувачів щодо засад безпеки, політик контролю доступу та керування правами, також забезпечення свідомості користувачів про ризики безпеки та їх відповідальність у збереженні безпеки системи та даних і проведення регулярних навчань та тренінгів щодо безпеки та правил використання системи контролю та управління доступом.

Такий підхід до проектування архітектури системи контролю доступу та управління дозволяє забезпечити повний цикл безпеки, включаючи ідентифікацію, автентифікацію, авторизацію, аудит, моніторинг, інтеграцію та навчання користувачів. Застосування цієї архітектури допоможе IT-компаніям забезпечити високу безпеку своїх систем і даних, уникаючи несанкціонованого доступу та втрат, пов’язаних із безпекою інформації.

Коли маємо розуміння по пунктах архітектури майбутньої системи контролю та управління доступом підприємства, можна спроектувати план приміщення підприємства, на якому буде застосовуватись система.

Тому, для початку я проаналізував приміщення на наявну кількість вхідних дверей, міжкімнатних дверей, а також кількість вікон. Загалом, приміщення офісу підприємства має 2 вхідних дверей, оскільки один відділ відокремлений від основного приміщення офісу, також 9 вікон, 2 міжкімнатних дверей, виходячи з цих даних, я спроектував план приміщення офісу.

Якщо говорити про стан приміщення офісу на даний момент, то як такого захисту, фактично воно не має. Двері офісу просто зачиняються лише на ключ, як одне приміщення так і друге, тобто немає пристроїв, які б дозволяли вхід до приміщень лише для працівників компанії. Тому в цьому є дуже гостра потреба, бо приміщення навіть не мають сигналізації, так, вона є на вході в офіс-центр, але вона повинна бути обов'язково окремо для приміщення підприємства.

Також я не побачив ніяких датчиків розбиття скла, датчиків руху, і тих, які б реагували на воду чи іншого типу загрози. На мою думку, це все має закладатись ще на початкових етапах, або хоча б проводити час від часу аналіз і аудит, який дозволив би удосконалювати з часом вже наявну систему.

Так, більшість приладів ніяк не відносяться по суті до системи управління і контролю доступом підприємства, але напряму впливають на забезпечення інформаційної безпеки від різних чинників. Оскільки загрози можуть виникати не лише від рук зловмисників, це можуть бути і інші типи загроз, які так чи інакше, можуть вплинути на цілісність даних.

Враховуючи всю цю інформацію, можна спроектувати схему приміщення на даному етапі (рисунок 2.1).

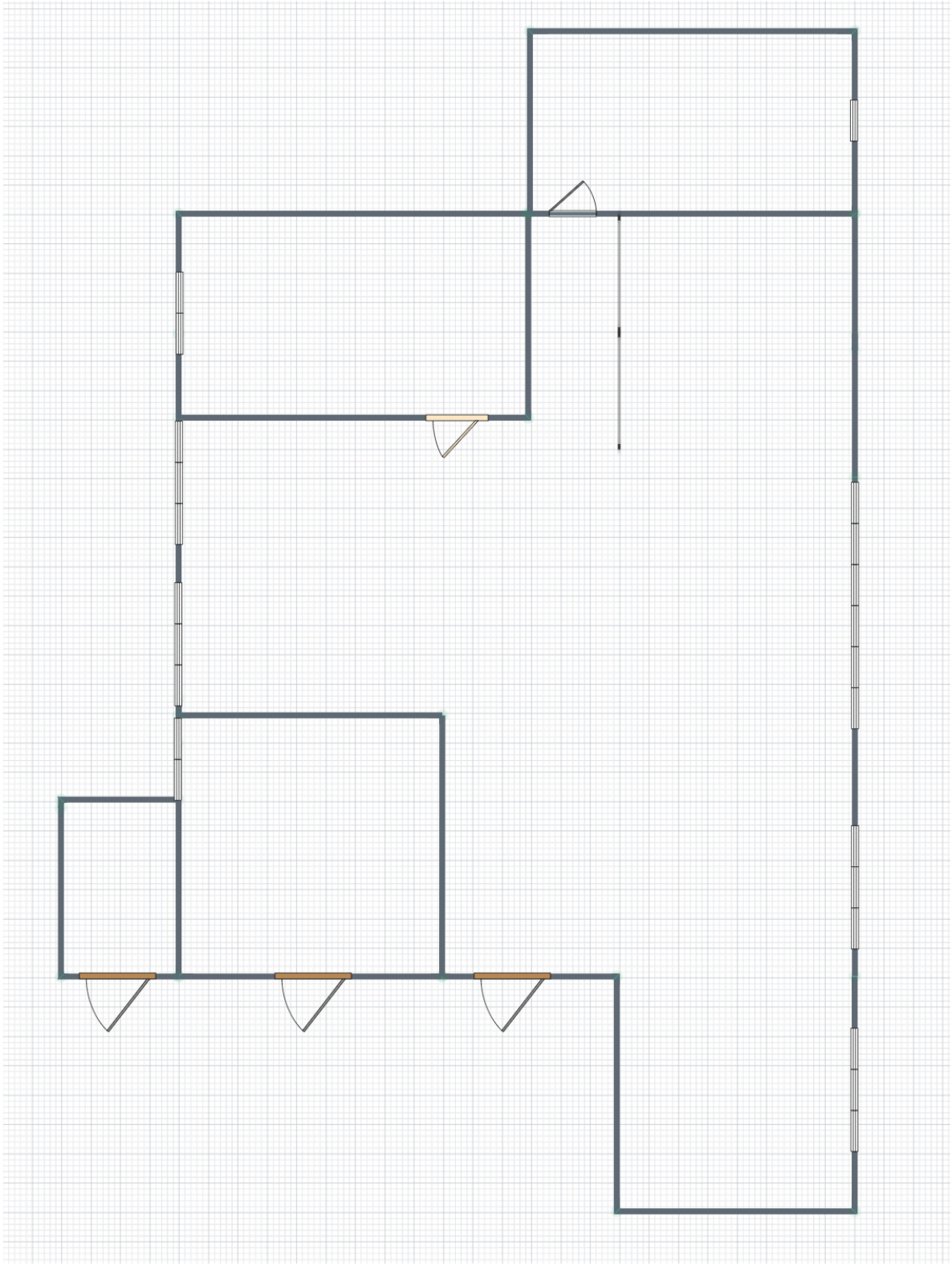


Рисунок 2.1 – Зовнішні і внутрішні стіни офісу

Тепер потрібно позначити внутрішні зони приміщення офісу підприємства (рисунок 2.2).

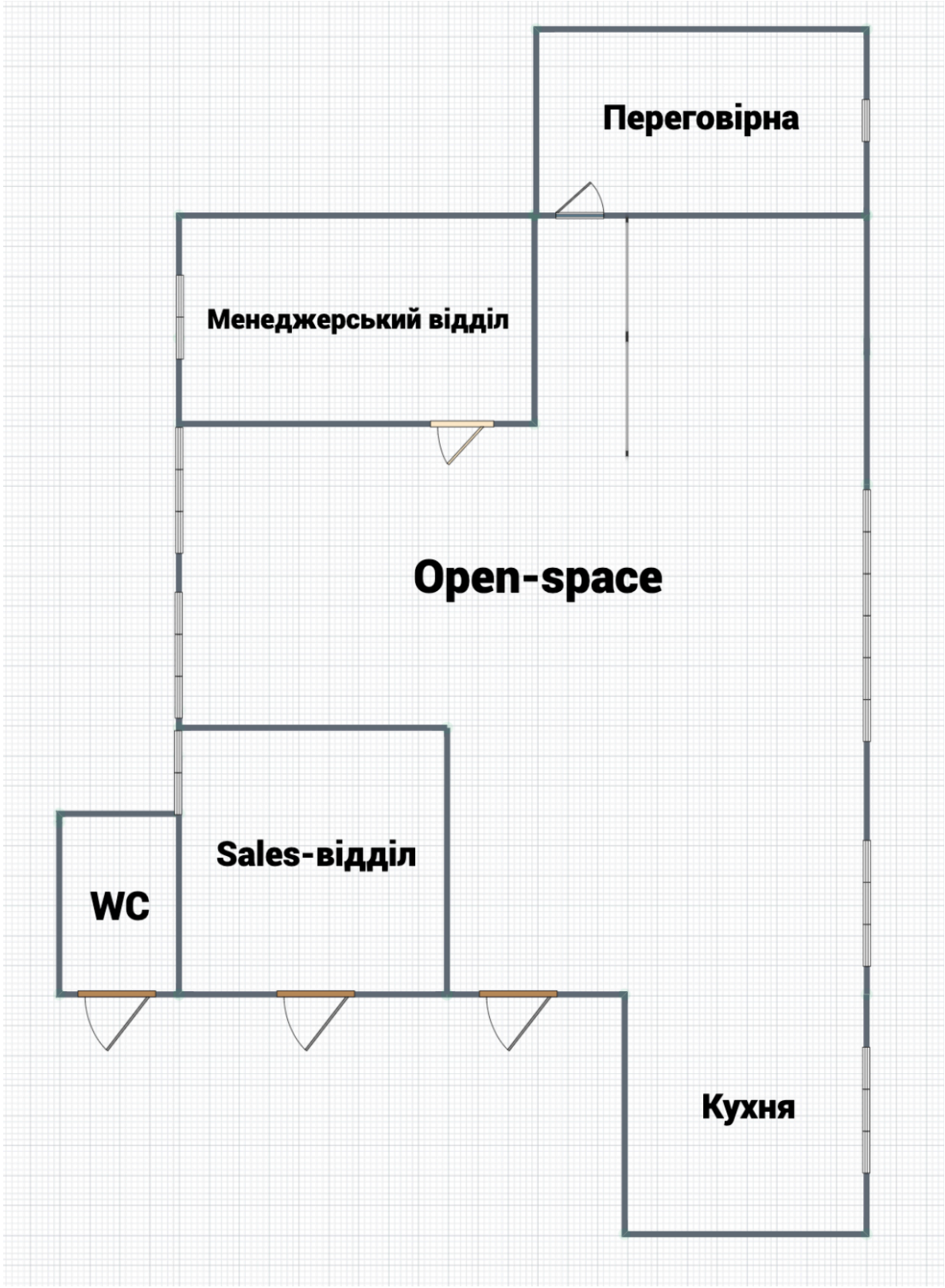


Рисунок 2.2 – Позначені внутрішні зони приміщення офісу

Коли вже візуально бачимо повний план приміщення офісу підприємства з розподіленими внутрішніми зонами та розташованими дверима і вікнами, можемо

скласти повноцінний план приміщення офісу разом з всіма елементами (рисунок 2.3).

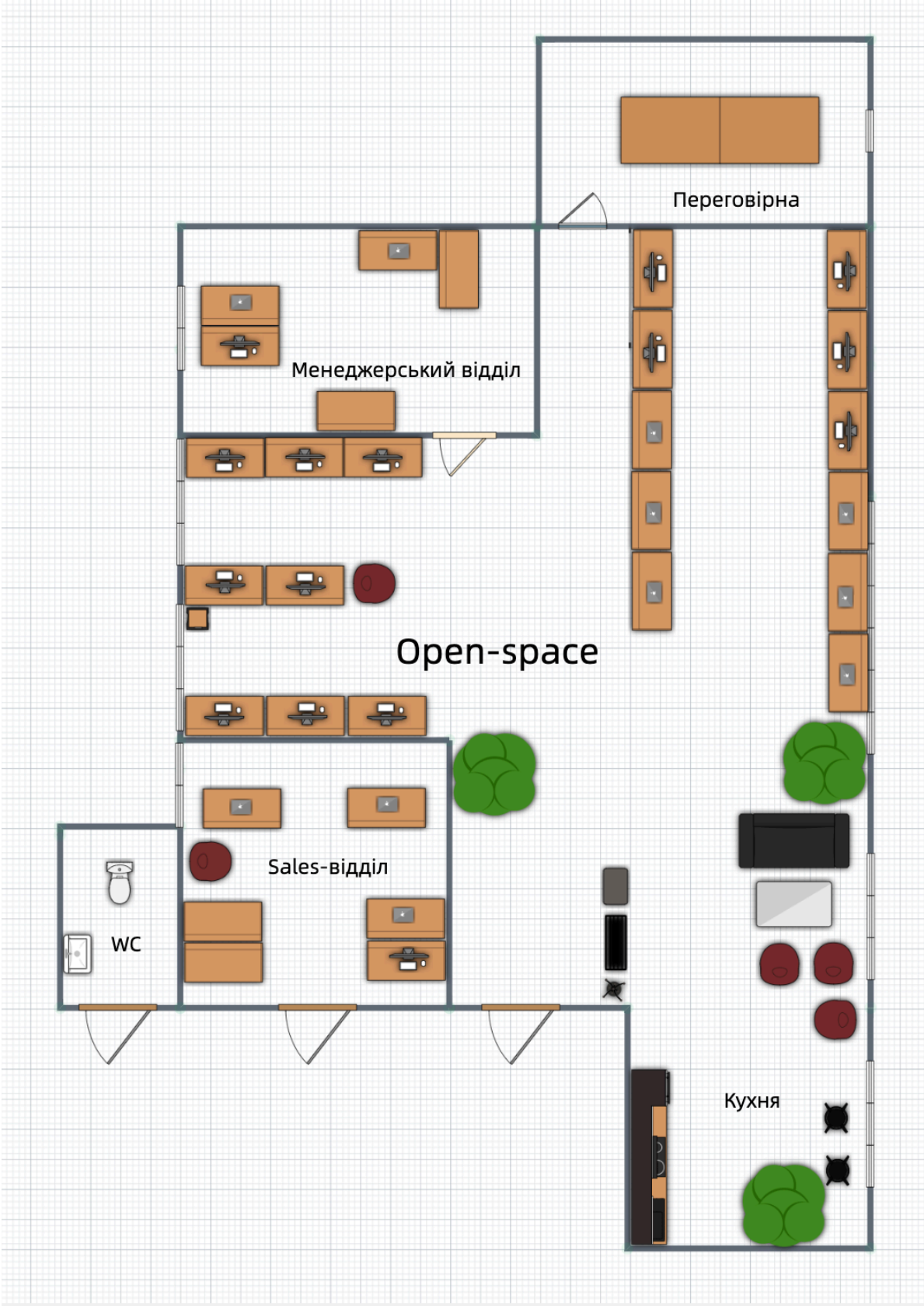


Рисунок 2.3 – Спроектований план приміщення

Тепер потрібно розмістити камери.

Взагалі для цього підприємства достатньо трьох камер відеоспостереження, тому що немає потреби стежити за робочим процесом всередині офісу, а для безпеки можна використовувати датчик руху з фото-фіксацією, тому одну камеру потрібно встановити біля входу в офіс, де можливе охоплення вхідних зон відразу двох приміщень, друга камера повинна бути встановлена на вході в офісний центр, а третя на зовнішній частині стіни приміщення і направлена на вікна офісу, оскільки вони виходять на дах будівлі, то звідти запросто можна здійснити проникнення в приміщення.

Тому щоб запобігти цьому, камеру потрібно поставити направлену в сторону саме цих вікон. Таким чином вона буде охоплювати відразу всі зони видимості, а в разі спроби проникнення зможе це зафіксувати. Це також дуже важливо, оскільки доступ до даху будівлі можна отримати дуже багатьма способами, і відстежити проникнення туди буде набагато важче. Звичайно, є охорона, але інколи вони можуть і не встежити за проникненням. Камеру, яка буде охоплювати ці зони зображено на рисунку 2.4.

Третю камеру, яка повинна розміщуватись на вході в приміщення офіс-центру, я не зображав, оскільки я маю план приміщення лише підприємства, для якого і проектується система контролю та управління доступом.

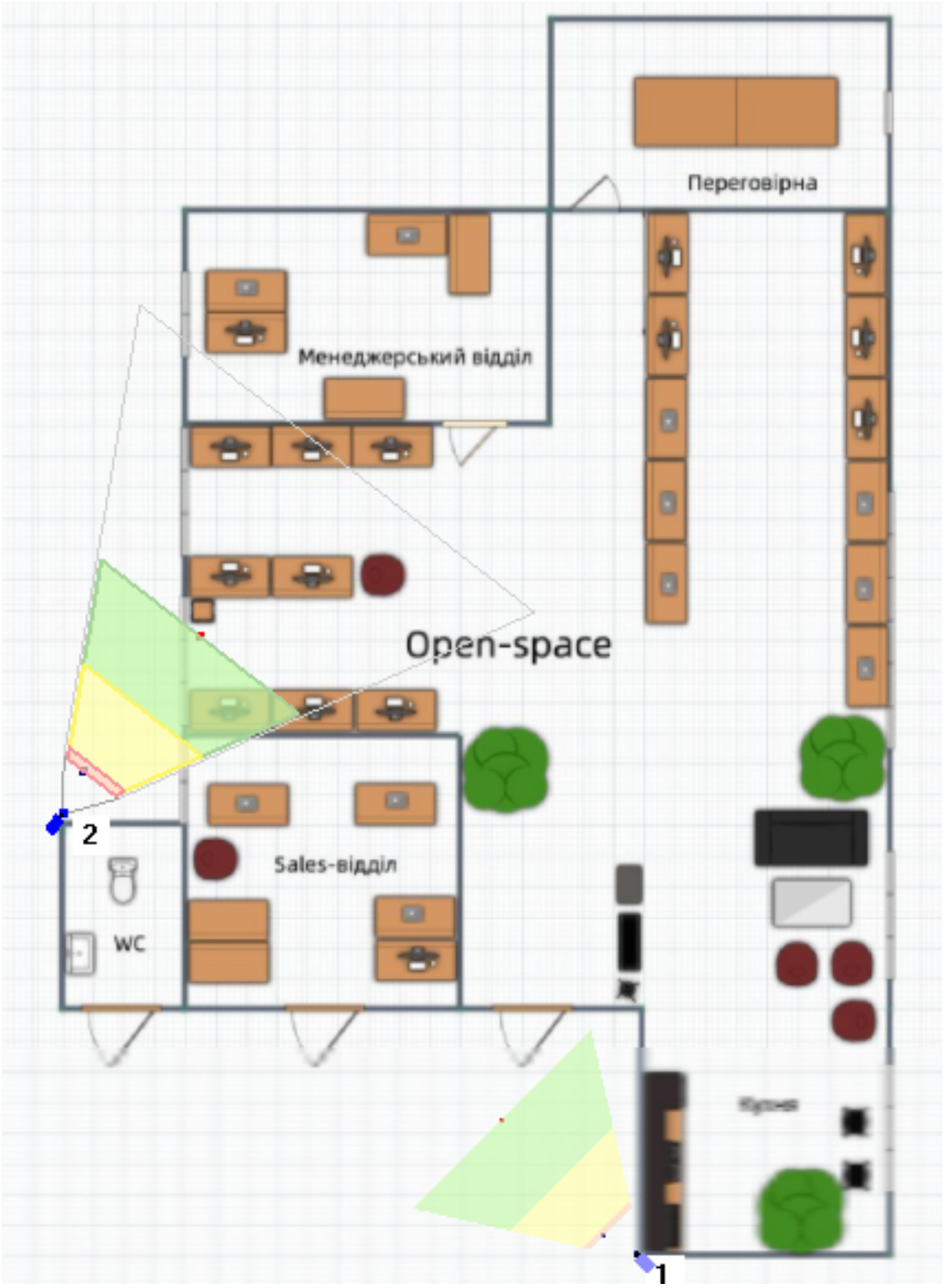


Рисунок 2.4 – Встановлені камери на приміщенні офісу

Для забезпечення пожежної безпеки, компанія вже використовує датчики пожежної сигналізації, що є плюсом на даному етапі. Датчики

розташовані рівномірно по площині стелі, у різних місцях, у всіх кабінетах, для нормального забезпечення пожежної безпеки. Модель датчика показано на рисунку 2.5.

Рисунок 2.5 – Зображення типу пожежного датчика, які використовує компанія

Для того, щоб забезпечити належну ідентифікацію і автентифікацію всіх працівників компанії, потрібно використовувати біометричний термінал доступу, нехай це буде пристрій ZKTeco X8-BT. Даний пристрій як раз відповідає потребам підприємства і забезпечить доступ до приміщення лише зареєстрованим працівникам. Модель пристрою зображена на рисунку 2.6.

Рисунок 2.6 – Біометричний термінал доступу

Даний термінал потрібно розташувати на вході у основне приміщення офісу відразу поряд з дверима, для зручності. Кнопка для виходу з приміщення відповідно буде розташована з середини приміщення також біля дверей.

Схема роботи даного терміналу представлена на рисунку 2.7.

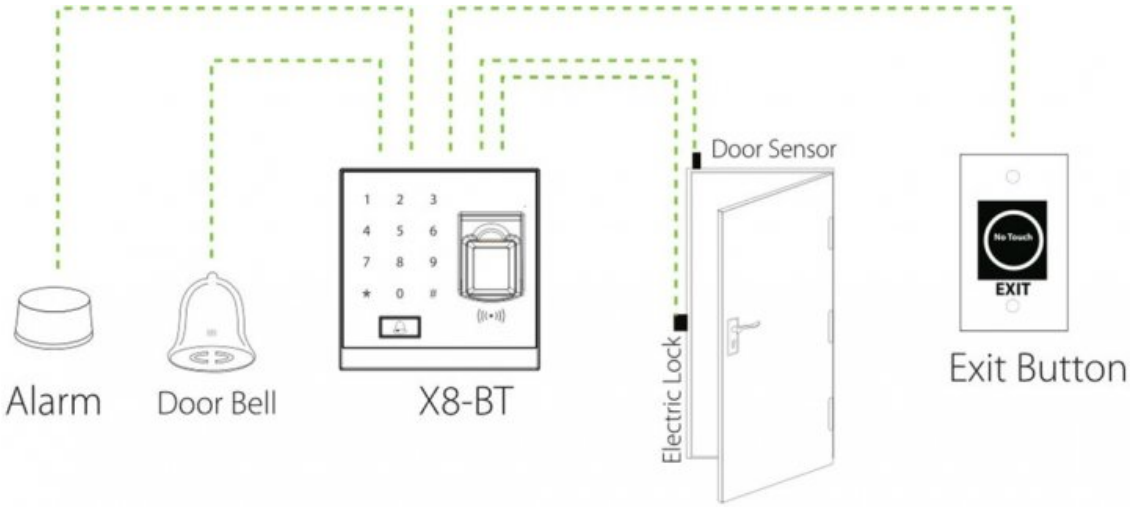


Рисунок 2.7 – Схема роботи біометричного терміналу доступу

Для вирішення інших потреб підприємства я підійшов комплексно, обравши систему захисту від компанії Ajax Systems.

На мою думку, саме ця компанія є професіоналами в своїй сфері, тому для того, щоб не витрачати час на поступове будування системи захисту, можна використати вже готове рішення. Тому для старту можна використати стартовий комплект StarterKit Cam Plus (рисунок 2.8).

Рисунок 2.8 – Вигляд стартового комплекту StarterKit Cam Plus

В даний комплект входить 4 пристрої, а саме:

– хаб, який контролює роботу пристроїв системи безпеки;

– датчик руху, що вже з перших кроків реагує на постороннього в приміщенні, яке охороняється, і робить серію фотографій;

– датчик відкриття дверей;

– брелок для ключів встановлює й знімає оселю з-під охорони.

Оскільки для повного забезпечення захисту, даного комплекту і кількості пристроїв для такого офісу буде замало, то потрібно розглянути також декілька

додаткових пристроїв. Тому я розглянув додатково ще датчики руху, оскільки в нас декілька приміщень.

Ajax Systems дає можливість використовувати датчики руху відразу з інтегрованими датчиками розбиття скла, тому використаю і дане рішення. Їх нам потрібно ще 4 одиниці. Модель даних датчиків зображено на рисунку 2.9.

Рисунок 2.9 – Вигляд датчику руху з датчиком розбиття скла

Тепер потрібно забезпечити захист від протікання води, для цього у Ajax Systems також є варіант пристрою, який забезпечить його, це бездротовий адресний датчик протікання (рисунок 2.10).

Рисунок 2.10 – Вигляд бездротового датчику протікання

Тепер, коли ми маємо розуміння, які пристрої будуть використовуватись для забезпечення захисту IT-підприємства, на мою думку, логічно, що потрібно ще додати систему оповіщення. Оскільки вже для системи керування і управління доступом, а саме для підвищення рівня інформаційної безпеки, будуть використовуватись пристрої від Ajax Systems, то і сигналізація також буде від цієї ж компанії. Наприклад, для даного підприємства чудово підійде сирена HomeSiren (рисунок 2.11).

Рисунок 2.11 – Вигляд сирени HomeSiren

Для того щоб забезпечити авторизацію та керування правами доступу працівників в системі, компанія вже використовує ресурс Colab-Team.

Colab-Team – це онлайн сервіс, який повноцінно забезпечить роботу компанії, оскільки підприємство використовує даний сервіс для ведення проектів, які розробляються, також для ведення звітності працівників по лікарняних, відпустках, навчанню, нарадах, а також відстежуванню робочого часу працівників. Звичайно, саме ця система вже забезпечує багаторівневий доступ працівникам, оскільки в компанії працюють розробники, проектні менеджери, менеджери з продажу, CEO та директор, тому важливо, щоб всі мали певний рівень доступу в системі.

Оскільки важливою складовою підвищення рівня інформаційної безпеки будь-якого підприємства звичайно є навчання та свідомість працівників, то Colab-Team також дозволяє автоматизувати даний процес. В системі є окремий розділ по навчанню працівників. Кожен новачок в компанії, в першу чергу, починаючи працювати, починає саме з ознайомлення всіх аспектів роботи ознайомлюючись з навчальним розділом. Даний розділ несе в собі інформацію по роботі з сервісом, по забезпеченню безпеки під час роботи і в загальному вводить в курс роботи в компанії. Також даний розділ має в собі навчальну інформацію по роботі на різних посадах, які займають працівники підприємства.

Даний розділ також є завжди актуальним, оскільки регулярно оновлюється для забезпечення належного захисту, але навчання працівників проводиться рідко.

Загалом, коли маємо спроектований план приміщення, рекомендоване розташування камер відеоспостереження, а також перелік пристроїв, які підвищать рівень інформаційної безпеки підприємства і забезпечать повноцінну роботу системи контролю і управління доступом, потрібно побудувати модель загроз та модель порушника.

2.3 Модель загроз та побудова моделі порушника

Під загрозою слід розуміти засіб здійснення дії, яка вважається небезпечною. Наприклад, загрози видалити інформацію з дисплеїв і перехопити випромінювання можуть призвести до втрати таємності або таємності, загрози пожежі можуть призвести до порушення цілісності та доступності інформації, загрози для каналів саботажу.

Передача інформації може призвести до втрати доступності.

Загрози для підприємства можуть бути різними в залежності від специфіки діяльності, архітектури системи та середовища. Однак нижче наведено загальну модель загроз, яку можна використовувати для аналізу ризиків безпеки

підприємства. У таблиці 2.1 описано ймовірність (висока, середня, низька) та можливі наслідки кожної загрози.

Таблиця 2.1 – Модель загроз

Загроза	Вірогідність	Наслідки
1	2	3
Вторгнення в мережу або систему	Висока	Несанкціонований доступ до конфіденційних даних, пошкодження або зміна даних, витік конфіденційної інформації, перерви в роботі системи
Фішинг (вилучення конфіденційних даних)	Середня	Крадіжка облікових даних та паролів, несанкціонований доступ до системи, втрата даних
Витік конфіденційної інформації	Висока	Втрата довіри клієнтів та партнерів, фінансові втрати, шкода репутації
Втрата або крадіжка пристроїв	Середня	Витік конфіденційних даних, втрата даних, втрата фізичного обладнання
Несанкціонований доступ до даних	Висока	Крадіжка конфіденційних даних, порушення приватності клієнтів, шкода репутації, правові наслідки
Атаки на сервери та мережеве обладнання	Висока	Пошкодження або втрата даних, зниження продуктивності мережі, перерви в роботі системи, витрати на відновлення та відновлення послуг

Закінчення таблиці 2.1

1	2	3
Недостатня свідомість щодо кібербезпеки	Середня	Підвищення ризику використання вразливостей, недостатня реагування на загрози, зростання вразливостей
Недостатня резервне копіювання даних	Середня	Втрата даних при випадку відмови обладнання, нездатність відновити важливі дані, перерва в роботі бізнесу
Недостатній контроль доступу	Середня	Несанкціонований доступ до системи, зловживання привілеями, втрата даних, порушення приватності
Недостатня фізична безпека	Середня	Крадіжка або пошкодження обладнання, незаконний доступ до приміщень, втрата даних, вплив на безпеку
Віруси та шкідливі програми	Висока	Втрата даних, пошкодження системи, перерва в роботі, фінансові втрати, втрата довіри клієнтів
Втрати через недостатній моніторинг	Середня	Невчасне виявлення атак, затримка в реагуванні, зростання наслідків і втрат
Фізичні явища	Середня	Пошкодження обладнання, приміщення офісу, втрата даних, фінансові втрати

Комплексна модель загроз ІТ-організації виявила потенційні загрози, які можуть вплинути на її безпеку та стабільність. Ці загрози варіюються від кібератак зловмисників, порушень конфіденційних даних, фізичної безпеки, слабких місць у системах і процесах, а також втручання третіх сторін.

Розуміння цих загроз і своєчасне реагування на них є важливою частиною управління ризиками. Підприємства повинні приділяти повну увагу заходам безпеки, включаючи захист інфраструктури, захист даних, контроль доступу та моніторинг системи.

Тепер, маючи побудовану модель загроз, базуючись на отриманій інформації, можна побудувати і модель порушника, оскільки це є також не менш важливим етапом при розробці системи контролю і управління доступом.

Модель порушника є важливим елементом систем контролю та управління доступом, оскільки вона допомагає ідентифікувати потенційні загрози та незвичні дії в системі. Основна мета моделі зловмисника — визначити типові сценарії поведінки, які можуть свідчити про вторгнення або порушення безпеки.

Застосування моделі порушника дозволяє системам контролю та управління доступом виявляти аномальні або підозрілі дії та реагувати на них, наприклад, несанкціонований доступ до об’єктів, спроби вторгнення в мережу, використання неавторизованих пристроїв та інші аномальні події. Тому система може вживати відповідних заходів для запобігання атакам і забезпечення безпеки інформації та ресурсів компанії.

Таким чином, модель порушника є потужним інструментом для покращення інформаційної безпеки на підприємстві, допомагаючи виявляти та усувати загрози та порушення вчасно та ефективно. Оскільки вже завчасно прописані можливі загрози і дії порушника, можна заздалегідь забезпечити належний захист від них, для того щоб уникнути інцидентів в майбутньому. Тому, для належного розуміння всіх порушень які можуть виникнути, була описана модель порушника. Модель порушника описано в таблиці 2.2.

Таблиця 2.2 – Модель порушника

Порушник	Мотивація	Навички	Методи порушення
Зовнішній зловмисник	Фінансова вигода	Високі	Кібератаки, фішинг, використання вразливостей програмного забезпечення
Конкурент	Конкурентна розвідка	Середні	Злом систем, крадіжка інтелектуальної власності, шпигунство
Недоброзичливий співробітник	Виразка незадоволення, збирання даних	Високі	Незаконне використання доступу, крадіжка даних, пошкодження систем
Екс-співробітник	Мстивість, розкриття інформації	Середні	Незаконний доступ, розкриття конфіденційної інформації
Соціальний інженер	Незаконне здобуття доступу	Високі	Фішинг, маніпулювання співробітниками, підбір паролів
Внутрішній зловмисник	Фінансова вигода, розкриття інформації	Високі	Використання недоліків в системах, злом доступу, крадіжка даних
Хакер-активіст	Політичні чи ідеологічні мотиви	Високі	Дефейс сайтів, DDoS-атаки, розкриття інформації
Зовнішній співробітник	Незадоволення, відмова в обслуговуванні		Злом систем, використання слабких паролів, фішинг

2.4 Висновки до розділу

В результаті проведеного аналізу вимог та потреб підприємства щодо системи контролю та управління доступом, а також проектування архітектури системи та побудови моделей загроз та порушника, було отримано важливі висновки, які покращують інформаційну безпеку підприємства:

– виявлені потреби підприємства у забезпеченні інформаційної безпеки є високими, оскільки воно працює з конфіденційною інформацією клієнтів та власною інтелектуальною власністю.

– розроблена архітектура системи контролю та управління доступом, яка включає в себе використання фізичних та логічних пристроїв автентифікації, а також систем відеоспостереження забезпечує вимоги підприємства та забезпечує безпеку приміщень;

– вибір підходящих пристроїв та технологій, таких як біометричні сканери, смарт-карти, системи відеоспостереження, дозволяє задовольнити потреби підприємства підвищити і забезпечити високий рівень інформаційної безпеки;

– побудована модель загроз виявила потенційні небезпеки, з якими може зіткнутися підприємство, такі як кібератаки, соціальний інженерінг, викрадення даних та інші. Це дозволяє своєчасно усвідомити ризики і розробити ефективні стратегії захисту;

– модель порушника розглядає різні варіанти потенційних зловмисників з різними намірами, такими як злам системи, несанкціонований доступ до приміщень або крадіжка даних.

Загалом, результати проведених досліджень та розробок дозволять підприємству підвищити рівень інформаційної безпеки шляхом впровадження системи контролю та управління доступом, що забезпечить захист від потенційних загроз та забезпечить надійний контроль доступу до систем та приміщень.

3 РЕАЛІЗАЦІЯ СИСТЕМИ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ НА ПІДПРИЄМСТВІ

3.1 Опис процесу реалізації системи на підприємстві

Впровадження ефективної системи контролю та управління доступом є важливим етапом у забезпеченні безпеки та захисту корпоративної інформації. Особливо це стосується IT-компаній, які обробляють цінну інформацію про компанію та дані клієнтів. Однак, враховуючи різноманітність загроз і ризиків, важливо детально і системно підходити до проектування і впровадження системи контролю доступу.

У цьому випадку наша IT-компанія, що спеціалізується на веб-розробці та розробці мобільних додатків, вирішила вдосконалити свою систему контролю та управління доступом. Відсутність пристроїв для аутентифікації співробітників, відеоспостереження та відсутність будь-яких систем безпеки в приміщеннях створюють потенційні ризики для інформаційної безпеки та можливість несанкціонованого доступу.

Тому в цьому підрозділі ми детально розглянемо процес впровадження системи контролю та управління доступом на нашому IT-підприємстві з використанням системи Ajax, яка забезпечить надійний контроль доступу та моніторинг приміщень. Ми охопимо всі етапи, від підготовки та проектування до тестування, впровадження та навчання персоналу. Цей процес допоможе забезпечити високий рівень безпеки та захисту наших організаційних і клієнтських даних.

Процес реалізації системи керування та управління доступом на підприємстві, враховуючи вимоги, спроектовану архітектуру та моделі загроз і порушника, може складатись з таких етапів:

– підготовчий етап, який включає в себе уточнення вимог та потреб підприємства щодо системи керування та управління доступом, включаючи встановлення цілей, обсягу робіт, технічних вимог та бюджету, а також Аналіз

існуючої інфраструктури та приміщень, включаючи розташування точок доступу, розміщення робочих зон та зон з обмеженим доступом;

– закупівля та підготовка обладнання, куди входить закупівля необхідних пристроїв від компанії Ajax Systems, таких як хаб, датчики руху, датчики розбиття скла, датчики відкриття, датчик протікання, система оповіщення. А також біометричний сканер відбитку пальців та камери відеоспостереження і випробування та перевірка обладнання на відповідність вимогам та його готовності до встановлення;

– встановлення обладнання, даний етап складається ще й з розміщення та підключення хаба Ajax Systems у відповідному місці, що забезпечує оптимальну покриття всіх приміщень, монтаж датчиків руху, датчиків розбиття скла, датчиків відкриття дверей та датчика протікання відповідно до спроектованої архітектури та моделі загроз. Також входить і встановлення біометричного сканера відбитку пальців у точках доступу та розміщення камер відеоспостереження в стратегічних місцях, відповідно до схеми розміщення;

– конфігурація та налаштування системи включає в себе підключення всіх пристроїв до хаба та їх налагодження для забезпечення взаємодії, Налаштування прав доступу для працівників згідно з їхніми ролями та відповідно до моделі порушника, а також налагодження параметрів системи, таких як часові розклади, відстеження тривог, запис відеозаписів;

– тестування та впровадження, куди входить проведення повного тестування системи для перевірки її працездатності та відповідності вимогам, виявлення можливих вразливостей та виправлення їх і пілотне впровадження системи на обмеженій кількості точок доступу та оцінка її ефективності та взаємодії з працівниками;

– навчання та підтримка, що складається з навчання персоналу підприємства щодо використання системи, правил безпеки та реагування на тривоги, а також Забезпечення постійної підтримки та оновлення системи, включаючи оновлення програмного забезпечення та обслуговування пристроїв.

Опис процесу впровадження такої системи управління та контролю доступу дозволить підприємству встановити надійні засоби контролю доступу, підвищити рівень інформаційної безпеки та забезпечити захист критичних ресурсів. Використання обладнання Ajax Systems, в тому числі хабів, датчиків руху, датчиків розбиття скла, відкривання дверей, датчиків витоків і камер відеоспостереження, а також біометричних сканерів відбитків пальців, забезпечить комплексний захист і моніторинг приміщень і допоможе уникнути можливих загроз і порушення.

Тепер, коли маємо чіткий план реалізації системи контролю та управління доступом на підприємстві, будемо згідно нього йти крок за кроком, щоб це було максимально ефективно.

Для підготовки було вже раніше проведено аналіз вимог та потреб підприємства, а також проведено попередню оцінку самого підприємства на теперішній рівень інформаційної безпеки. Тому тепер, потрібно лише проаналізувати існуючу інфраструктуру, а також робочі приміщення, а маючи актуальну схему приміщення підприємства, складнощів це не склало.

Далі, перед закупівлею необхідного обладнання, яке було описано на етапі проектування, потрібно провести аналіз їхньої вартості враховуючи вимоги і потреби підприємства в необхідній кількості зазначених пристроїв. Розраховану вартість необхідних пристроїв описано в таблиці 3.1.

Таблиця 3.1 – Оцінка вартості необхідних пристроїв

№ п/н	Назва	К-ть (шт)	Ціна (грн)	Сума (грн)
1	2	3	4	5
1	StarterKit Cam Plus	1	16 799	16 799
2	Сирена HomeSiren	1	1 729	1 729

Закінчення таблиці 3.1

1	2	3	4	5
3	Датчик руху і розбиття скла CombiProtect	4	2 419	9 676
4	Датчик відчинення DoorProtect Plus	1	1 549	1 549
5	LeaksProtect	5	1 379	6 895
6	Пристрій для читання відбитків пальців ZKTeco X8-BT	1	3 885	3 885
7	IP камера Hikvision DS-2CD1121-I	3	2 891	8 673
			Сума:	49 206

Після закупівлі необхідного обладнання, сміливо можна переходити до наступного етапу, а саме його встановлення і належного розміщення.

Почнемо з хаба, його було прийнято рішення встановити в переговірній, де для нього не буде ризику для заподіяння фізичної шкоди. Саме розташування показано на рисунку 3.1.

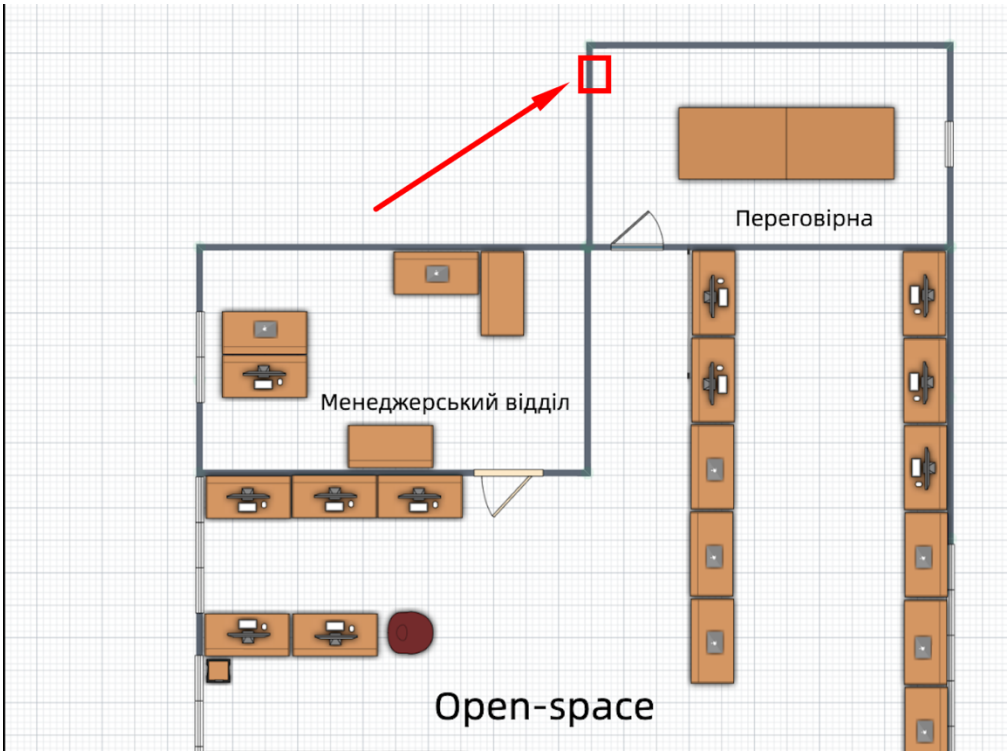


Рисунок 3.1 – Розташування хабу керування

Далі, потрібно розташувати сирену HomeSiren, вона буде розташована над вхідними дверима в головне приміщення офісу. Розташування сирени показано на рисунку 3.2.

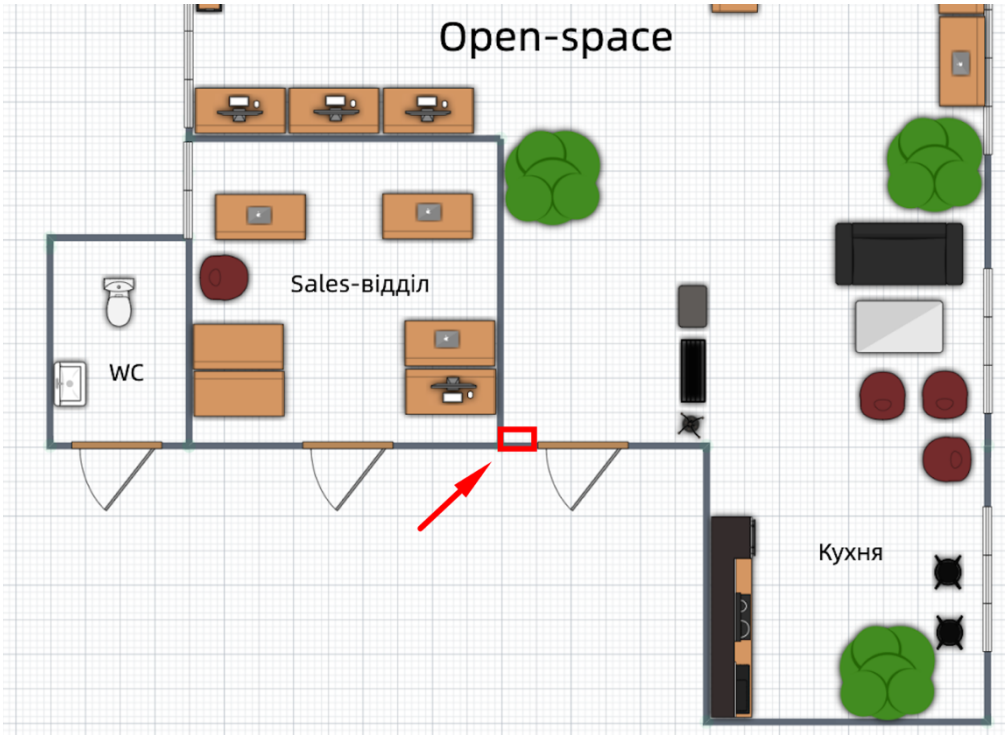


Рисунок 3.2 – Розташування системи оповіщення

Тепер, для ідентифікації і автентифікації працівників, а також для обмеження доступу до приміщення стороннім особам, потрібно встановити пристрій зчитування відбитку пальців, він буде розташовуватись на стіні зліва від вхідних дверей. Розташування пристрою для зчитування відбитку пальців показано на рисунку 3.3.

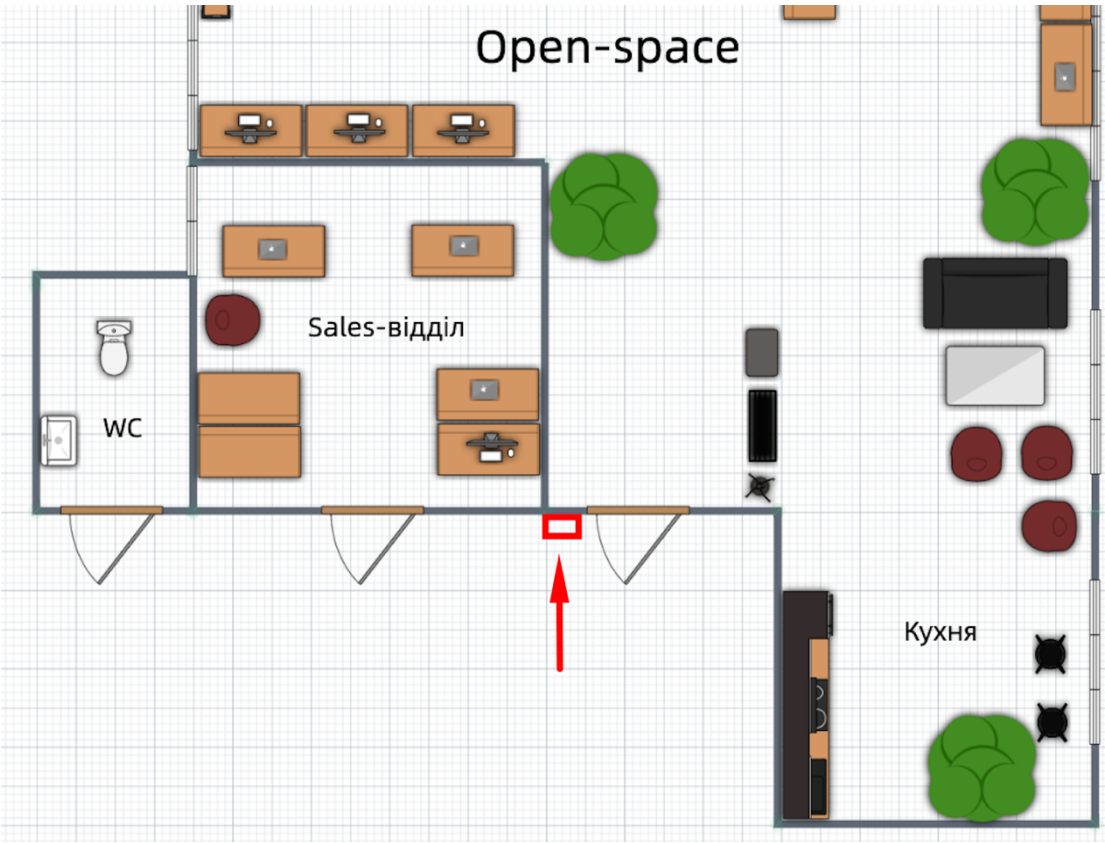


Рисунок 3.3 – Розташування пристрою зчитування відбитку пальців

На даному етапі, потрібно тепер зайнятись розміщенням датчиків протікання. Вони повинні бути розташовані обов'язково в туалеті, а також в приміщеннях, де є система опалення, тому було прийнято рішення розмістити по одному датчику в кожному приміщенні.

Оскільки передбачено, що данні датчики кріпляться на підлогу, а якщо це приміщення ванної або туалету, то потрібно розташовувати їх біля умивальника, що було реалізовано і в цьому випадку. Також датчики були розміщені під батареями опалення, тому що саме там є ризик протікання в разі чого (рисунок 3.4).

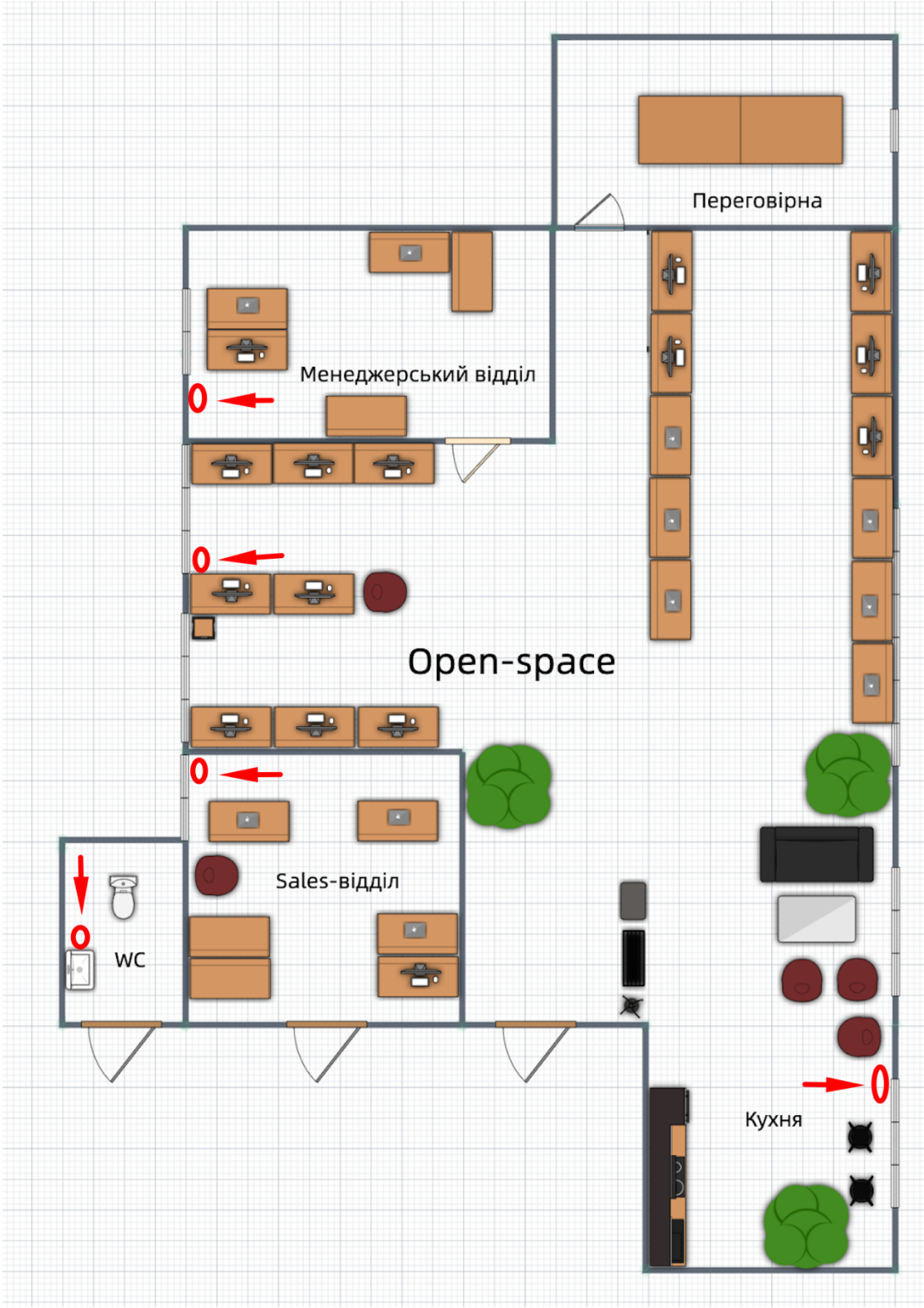


Рисунок 3.4 – Розташування датчиків протікання в приміщеннях

Тепер потрібно розмістити датчики руху і розбиття скла, оскільки було прийнято рішення комплексно підійти до вирішення цієї потреби, то 4 датчика

забезпечать функціональність реагування на рух і на розбиття скла. Їх саме тому буде розміщено в кожному приміщенні, оскільки наприклад в приміщенні менеджерського та sales-відділів, є доступ до даху офіс-центру, тому там є гостра потреба забезпечити належний захист від проникнення (рисунок 3.5).

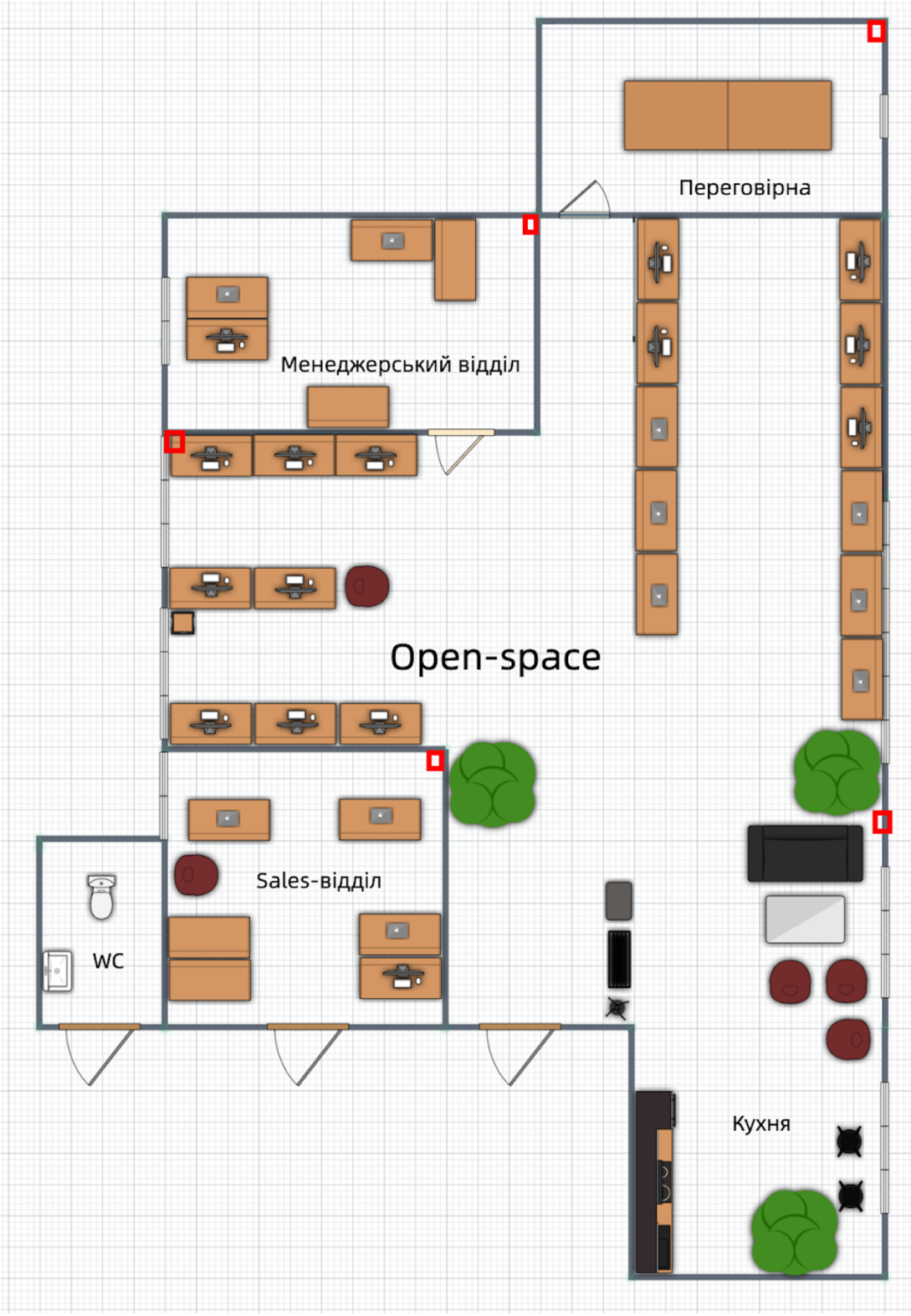


Рисунок 3.5 – Розташування всіх датчиків руху і розбиття скла

На зображенні показано розміщення всіх датчиків руху з додатковою функцією реагування на розбиття скла, а також датчик руху, що йде в комплекті StarterKit Cam Plus, який розміщений на центральній стіні опен-спейсу, бо в ньому ще є і фотофіксація, тому важливо, щоб він охоплював саме основне приміщення підприємства.

Ну і коли всі датчики розміщені в потрібних місцях, лишається розмістити лише датчики відчинення, які будуть розміщені на вхідних дверях в головні приміщення, тобто в sales-відділ і головне приміщення підприємства.

Розташування камер я показав ще на етапі проектування майбутньої системи контролю та управління доступом, додам лише, що для забезпечення належного відеоспостереження було використано камери від компанії Hikvision моделі DS-2CD1121-I. Оскільки на мою думку, саме ця компанія є лідером по якості систем відеоспостереження. Модель даної камери зображена на рисунку 3.6.

Рисунок 3.6 – Вигляд камери відеоспостереження Hikvision DS-2CD1121-I

Дана камера є купольного типу, має можливість спостереження з різних кутів і забезпечить належне відеоспостереження, яке до цього було взагалі відсутнім.

Далі, коли абсолютно всі пристрої розташовані в потрібних місцях, враховуючи вимоги та потреби підприємства, а також модель загроз, дані пристрої потрібно підключити до хаба і провести належну конфігурацію і налаштування всіх пристроїв, для забезпечення нормального функціонування як єдиної системи. Не менш важливим моментом на цьому етапі є те, що потрібно провести налаштування прав доступу для працівників згідно з їхніми ролями та відповідно до моделі порушника.

Враховуючи те, що підприємство вже має систему, яку використовує для роботи і забезпечення різного рівня доступу, потрібно провести аналіз наявної системи, а також зробити чистку акаунтів звільнених співробітників, якщо такі є, щоб унеможливити ризик витоку конфіденційної інформації через екс-працівників.

Тепер коли проведено всі налаштування, аналіз та конфігурації, потрібно провести тестування впровадженої системи контролю та управління доступом. Зробити це потрібно в першу чергу спираючись на модель загроз і модель порушника, проаналізувати додаткові можливі загрози інформаційної безпеки підприємства та протестувати захист від цих загроз впровадженою системою.

В разі якщо все ж таки будуть знайдені якісь вразливості, їх потрібно буде виправити завчасно, щоб потім в майбутньому підприємство з ними більше не стикалось.

Після повного впровадження, а також тестування і аналізу системи контролю та управління доступом, потрібно провести навчання працівників підприємства щодо використання системи, правил безпеки та реагування на тривоги і проводити його регулярно. Що не менш важливим є те, що потрібно також забезпечити постійну підтримку і оновлення системи, що включатиме і обслуговування пристроїв, а також оновлення програмного забезпечення.

3.2 Забезпечення безпеки під час впровадження системи

Забезпечення безпеки під час впровадження вже розробленої і спроектованої системи контролю та управління доступом на підприємстві включає ряд кроків, які максимально забезпечують захист інформації та ресурсів компанії. Тому нижче наведено список цих кроків:

– фізична безпека;
– захист мережі та комунікацій;
– автентифікація та авторизація;
– моніторинг і аудит;
– навчання та свідомість персоналу.

Ці кроки сприяють ефективній і безпечній реалізації системи контролю та управління доступом на підприємстві. Врахування фізичної безпеки, захисту мережі, автентифікації та авторизації, моніторингу та аудиту, а також навчання персоналу дозволяє забезпечити надійну захищеність інформації та активів компанії під час впровадження системи контролю доступу.

Тепер давайте розглянемо детальніше кожен крок, для забезпечення належної безпеки під час впровадження системи контролю та управління доступом.

Фізична безпека включає в себе такі кроки як розташування обладнання, бо важливо встановити хаб та інші пристрої контролю доступу в безпечному місці, яке обмежує фізичний доступ несанкціонованих осіб. Наприклад, можна встановити хаб в захищеному серверному приміщенні або в місці з обмеженим доступом для зовнішніх осіб. Також сюди входить захист обладнання оскільки протягом процесу встановлення необхідно впровадити заходи для захисту обладнання, такі як встановлення фізичних замків на шафи або кабельні траси, щоб запобігти несанкціонованому доступу до них.

Захист мережі та комунікацій складається з встановлення захищеної мережі з використанням файрволу, віртуальних приватних мереж (VPN) та

інших захисних механізмів допоможе уникнути несанкціонованого доступу до системи контролю доступу через мережу. А також потрібне забезпечення шифрування даних, що передаються між пристроями контролю доступу, хабом та іншими компонентами системи, дозволяє захистити ці дані від перехоплення та несанкціонованого доступу.

Автентифікація та авторизація являє собою використання пристроїв біометричної автентифікації, наприклад, сканерів відбитків пальців, дозволяє підвищити рівень безпеки шляхом використання унікальних фізичних характеристик користувачів. Також потрібно вимагати від користувачів встановлення сильних паролів для своїх облікових записів, які використовуються для доступу до системи контролю доступу.

Моніторинг і аудит включає в себе встановлення камер відеоспостереження в ключових зонах підприємства допомагає контролювати доступ та виявляти потенційні загрози, а також забезпечення регулярного аудиту доступу до системи контролю доступу дозволяє виявляти незвичайну активність та спроби несанкціонованого доступу.

Навчання та свідомість персоналу складається з забезпечення навчання персоналу щодо користування системою контролю доступу, правил безпеки та процедур реагування на можливі загрози допомагає створити свідоме середовище безпеки на підприємстві. Сюди також входить створення культури безпеки та посилення свідомості персоналу щодо важливості дотримання правил безпеки та політик доступу є необхідною частиною забезпечення безпеки системи.

Дані всі кроки спрямовані на достатнє забезпечення безпеки під час впровадження системи контролю та управління доступом на підприємстві. Оскільки загалом є дуже багато чинників, які справді можуть вплинути в загальному на процес реалізації системи.

3.3 Оцінка ефективності впровадженої системи

Після впровадження системи контролю та управління доступом, була проведена оцінка ефективності впровадженої системи, основні аспекти що впливають на ефективність системи включають:

– завдяки використанню пристроїв Ajax Systems, встановленню датчиків руху, датчиків розбиття скла, датчиків відкриття дверей та датчика протікання, система контролю доступу може ефективно виявляти та реагувати на спроби несанкціонованого доступу. Це дозволяє забезпечити високий рівень безпеки приміщень та обладнання;

– використання сканера відбитків пальців для автентифікації працівників забезпечує високий рівень ідентифікації та унікальності доступу. Це допомагає уникнути проблем, пов'язаних з втратою або недостатньо сильними паролями;

– встановлення двох камер відеоспостереження дозволяє контролювати приміщення і виявляти підозрілу або незвичайну активність. Це створює додатковий рівень безпеки і дозволяє швидко реагувати на потенційні загрози;

– завдяки впровадженій системі оповіщення, адміністратори та відповідальні особи отримують сповіщення про виникнення подій або незвичайну активність. Це дозволяє швидко реагувати на можливі загрози та вживати відповідних заходів безпеки;

– Система контролю доступу може збирати дані про активність користувачів, виявлені загрози та події. Це надає можливість проводити аналіз, виявляти вразливості та вдосконалювати систему безпеки на основі зібраних даних.

Загалом, впроваджена система контролю та управління доступом, з урахуванням використання пристроїв Ajax Systems, біометричної автентифікації, камер відеоспостереження та інших заходів безпеки, виявляється ефективною в захисті підприємства від несанкціонованого доступу, реагуванні на загрози та забезпеченні безпеки інформації та активів. Проте,

важливо пам'ятати, що безпека є постійним процесом, і система потребує постійного оновлення та аналізу для забезпечення найвищого рівня захищеності.

3.4 Висновки з результатів реалізації системи

В ході реалізації системи контролю та управління доступом на підприємстві були проведені всі необхідні етапи, що включали опис процесу реалізації системи, забезпечення безпеки під час впровадження та оцінку ефективності впровадженої системи.

Процес реалізації системи був детально продуманий та ефективно виконаний. Було проведено аналіз вимог і потреб підприємства, що дозволило визначити необхідні компоненти та функціонал системи. Архітектура системи була спроектована з урахуванням потреб безпеки та забезпечення вимог підприємства.

Особлива увага була приділена забезпеченню безпеки під час впровадження системи контролю та управління доступом. Були використані пристрої від компанії Ajax Systems, такі як датчики руху, датчики розбиття скла, датчики відкриття дверей, датчик протікання та система оповіщення. Також був використаний сканер відбитку пальців для біометричної автентифікації працівників. Ці пристрої забезпечили виявлення потенційних загроз і збільшили рівень безпеки приміщення.

Впроваджена система контролю та управління доступом показала високу ефективність. За допомогою використаних пристроїв та забезпечення безпеки, підприємство змогло контролювати доступ працівників до приміщення, зменшити ризик несанкціонованого доступу та забезпечити захист важливої інформації. Оцінка ефективності показала, що система відповідає вимогам підприємства та сприяє забезпеченню безпеки і контролю доступу на всіх

рівнях. Впровадження системи контролю та управління доступом дозволило підприємству покращити свою інформаційну безпеку та забезпечити надійний контроль доступу до приміщення.

Система ефективно виявляє загрози та автоматично реагує на них, сповіщаючи відповідні відділи або керівництво підприємства. Застосування біометричної автентифікації сприяє точному ідентифікуванню працівників і запобігає несанкціонованому доступу. Крім того, система контролю та управління доступом значно спрощує процес управління правами доступу та адміністрування системи.

Впроваджена система має позитивний вплив на загальну безпеку підприємства, запобігаючи несанкціонованому доступу до ресурсів та мінімізуючи ризик витоку конфіденційної інформації. Результати оцінки ефективності підтверджують успішне впровадження системи та покращення інформаційної безпеки на підприємстві.

Отже, реалізація системи контролю та управління доступом на даному підприємстві була успішною і мала значний позитивний вплив на безпеку та захист інформації. Вона стала надійним і ефективним інструментом управління доступом, що дозволяє підприємству ефективно боротися з загрозами та забезпечувати контроль над ресурсами. Результати реалізації системи свідчать про її успішність і важливість для підвищення загальної інформаційної безпеки на підприємстві.

ВИСНОВКИ

Виконання кваліфікаційної роботи було успішним і зайняло кілька етапів. На кожному етапі були враховані вимоги та потреби підприємства з метою покращення рівня безпеки і контролю доступу до приміщення.

Аналіз предметної області існуючих систем контролю та управління доступом дозволив виявити проблеми та завдання, що потребують вирішення. Застосування принципів побудови систем контролю та управління доступом стало основою для постановки задачі і проектування архітектури системи.

Аналіз вимог та потреб підприємства був проведений з урахуванням їх специфіки і визначив необхідні компоненти та функціонал системи контролю та управління доступом. Побудова моделі загроз і моделі порушника допомогли визначити потенційні небезпеки і врахувати їх при реалізації системи.

Опис процесу реалізації системи контролю та управління доступом на підприємстві був детально пророоблений, включаючи планування приміщення, підбір пристроїв та впровадження системи. Забезпечення безпеки під час впровадження системи було високим пріоритетом, і були використані відповідні пристрої та заходи для забезпечення фізичної та інформаційної безпеки.

Оцінка ефективності впровадженої системи контролю та управління доступом свідчить про її успішність. Застосування відповідних пристроїв і процедур дозволило забезпечити надійний контроль доступу та зменшити ризик несанкціонованого доступу до приміщення. Підприємство зазнало покращення своєї інформаційної безпеки і здатне ефективно впоратися з потенційними загрозами і порушниками.

В цілому, реалізація системи контролю та управління доступом на підприємстві виявилася успішною і відповідає вимогам та потребам підприємства. Застосування відповідних технологій та процедур дозволило

забезпечити підвищену інформаційну безпеку і зменшити ризики несанкціонованого доступу. Реалізована система є надійним інструментом для захисту цінної інформації та забезпечення контролю над доступом на підприємстві.

Додатково, впроваджена система контролю та управління доступом сприяє поліпшенню загальної безпеки приміщення підприємства. Завдяки використанню різних пристроїв, таких як датчики руху, датчики розбиття скла, датчики відкриття дверей, датчик протікання, система оповіщення та біометричний пристрій для автентифікації працівників, система здатна вчасно виявляти потенційні загрози та несанкціонований доступ.

Крім того, використання камер відеоспостереження дозволяє забезпечувати візуальний контроль за подіями в приміщенні, а це значно підвищує ефективність системи безпеки. Камери можуть фіксувати незвичайні дії або порушення, що дозволяє оперативно реагувати на них та приймати відповідні заходи для запобігання можливим проблемам.

Завдяки процесу реалізації системи контролю та управління доступом, вдалому проектуванню архітектури системи та врахуванню моделі загроз та порушника, підприємство здобуло надійну інфраструктуру безпеки. Ця система стала необхідним інструментом для підприємства, оскільки вона забезпечує не тільки захист важливих даних, але й контроль над доступом працівників та гостей до різних зон приміщення.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Базавлук Я. І. Аналіз поняття "підприємство" : thesis. 2015. URL: http://essuir.sumdu.edu.ua/handle/123456789/44148 (дата звернення: 14.03.2023).

2. Батечко О., Цимбаленко Н. В. Інформаційна безпека підприємства : thesis. 2016. URL: https://er.knutd.edu.ua/handle/123456789/4464 (дата звернення: 23.04.2023).

3. Біометричні технології: навч. посіб./ Р.Ю. Царьов, Т. М. Лемеха. Одеса: ОНАЗ ім. О.С. Попова, 2016. 140 с.

4. Види реєстрації компаній [Електронний ресурс] : [Вебсайт]. – Електронні дані. – Режим доступу: https://uk.economy-pedia.com/11040318-business (дата звернення: 13.03.2023) – Назва з екрана.

5. Виявлення та блокування засобів негласного отримання інформації на об'єктах інформаційної діяльності. Навчальній посібник/ О.А. Лаптєв, В.А. Савченко, Г.В. Шуклін. К.:ДУТ, 2020. 126 с.

6. Відеоспостереження [Електронний ресурс] : [Вебсайт]. – Електронні дані. – Режим доступу: https://uk.wikipedia.org/wiki/Відеоспостереження (дата звернення: 19.03.2023) – Назва з екрана.

7. Захист інформації від несанкціонованого доступу : thesis / А. М. Куліш та ін. 2013. URL: http://essuir.sumdu.edu.ua/handle/123456789/31765 (дата звернення: 11.04.2023).

8. Здолбіцька Н., Здолбіцький А., Семенко О. Системи електронної ідентифікації і управління доступом користувачів. Комп’ютерно-інтегровані технології: освіта, наука, виробництво. 2019. № 36. С. 103–108. URL: https://doi.org/10.36910/6775-2524-0560-2019-36-5 (дата звернення: 23.05.2023).

9. Інформаційна безпека: навчальний посібник / [Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв та ін.]; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. – Львів: Видавництво Львівської політехніки, 2019. – 580 с.

10. Інформаційна безпека: питання правового регулювання: монографія/ А.Ю. Нашинець-Наумова. Київ: Видавничий дім «Гельветика», 2017. 168 с.

11. Комплексна безпека інформаційних мережевих систем. Навчальний посібник/ А.Г. Микитишин, М.М. Митник, П.Д. Стухляк. Львів, «Магнолія 2006», 2016. 256 с.

12. Крилова В. А., Мирошник А. Н. Розробка методів оцінки ефективності систем захисту інформації в розподілених комп'ютерних системах. Інформаційно-керуючі системи на залізничному транспорті. 2015. № 2. URL: https://doi.org/10.18664/ikszt.v0i2.51946 (дата звернення: 17.05.2023).

13. Кубрак М. О. Система захисту інформаційно-комунікаційних мереж : thesis. 2021. URL: http://ir.stu.cn.ua/123456789/22643 (дата звернення: 22.04.2023).

14. Методологія захисту інформації. Аспекти кібербезпеки: підручник/ Г.М. Гулак К.: Видавництво НА СБ України, 2020. 256 с.

15. Мехед Д. Б. Захист інформації на підприємстві. Вісник Чернігівського державного технологічного університету. Серія "Технічні науки". 2014. № 2 (73). С. 143–148.

16. НД ТЗІ 3.3-001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації

17. Олійник О. Державна інформаційна політика та інформаційна безпека України: політико-правові аспекти. Право України. 2005. № 5. С. 108–110.

18. Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України: аналітична доповідь/ Д.Г. Бобро, С.П. Іванюта, С.І. Кондратов, О.М. Суходоля/ за заг. ред. О. М. Суходолі. К.: НІСД, 2019. 224 с.

19. Організаційно-правові основи захисту службової інформації: навч. посіб./І.П. Касперський, С. О. Князєв, О. І. Матяш та ін. Київ: Нац. акад. СБУ, 2017. 120 с.

20. Основи інформаційної безпеки. Конспект лекцій./ Б.А. Заплотинський. КІІВіП НУ “ОЮА”, кафедра інформаційно-аналітичної та інноваційної діяльності, 2017. 128 с.

21. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України: монограф./ О. П. Єрменчук. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2018. 180 с.

22. Політики безпеки. Навчальний посібник для студентів вищих навчальних закладів/ Козачок В.А., Гайдур Г.І., Гахов С.О., Хмелевський Р.М., Чумак Н.С. Київ: ДУТ ННІЗІ, 2020. 167 с.

23. Проєктування та монтаж локальних комп’ютерних мереж: [навчальний посібник]/ І. М. Журавська. Миколаїв : Видавництво ЧДУ ім. Петра Могили, 2016. 396 с.

24. Системи відеоспостереження: лабораторний практикум [Електронний ресурс]: навч.посіб./ В. М. Бакіко, В. Б. Швайченко. Київ : КПІ ім. Ігоря Сікорського, 2021. режим доступу: https://ela.kpi.ua/bitstream/123456789/41124/1/SV_lab_praktykum.pdf

25. Системи електроживлення підприємств зв’язку: Навчальний посібник/ А.Ф. Кадацький, О.П. Русу. Одеса: ОНАЗ ім. О.С.Попова, 2016. 76 с.

26. Сучасні методи забезпечення надійності персоналу: навчальний посібник у схемах і таблицях/ З.Б. Живко. Львів: ЛьвДУВС, 2019. 128 с.

27. Тертишник В. М. Система технічного захисту інформації на підприємстві : thesis. 2021. URL: http://ir.stu.cn.ua/123456789/22665 (дата звернення: 05.05.2023).

28. Технічний захист інформації [Електронний ресурс] : [Вебсайт]. – Електронні дані. – Режим доступу: https://tzi.ua/ua/tz.html (дата звернення: 18.04.2023) – Назва з екрана.

29. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник/ С.О. Іванченко, О.В Гавриленко, О.А Липський, А.С. Шевцов. К.: ІСЗЗІ НТУУ «КПІ», 2016. 104 с.

30. Data and Information Leakage Prevention Within the Scope of Information Security/ Barbara Hauer/ December 2015IEEE Access 3:1-1. DOI:10.1109/ACCESS.2015.2506185

31. Design and Implementation of a Computerized User Authentication System for E-Learning/ Z. Faizal Khan, Sultan Refa Alotaibi. iJET Vol. 15, No. 9, 2020 pp. 4-18. https://doi.org/10.3991/ijet.v15i09.12387

32. Fundamentals of Information Systems Security / Editors : David Kim, Michael G. Solomon. Burlington, Massachusetts: Jones & Bartlett Learning, 2018. 548 p.

33. Information leakage analysis of software: How to make it useful to IT industries?/ Kushal Anjaria, Arun Mishra/ - Faculty of Computers and Information Technology, Future University in Egypt. Production and hosting by Elsevier B.V., 2017 pp. 10-18. https://doi.org/10.1016/j.fcij.2017.04.002

34. Information Security. Foundations, technologies and applications/ Editors : Ali Ismail Awad, Michael Fairhurst. The Institution of Engineering and Technology, 2018. 418 p.

35. One-Time-Username: A Threshold-based Authentication System/ Abdulrahman Alhothailya, Arwa Alrawaisa, Chunqiang Hua, Wei Li. - Procedia Computer Science 129 (2018), Elsevier Ltd. pp. 427-431. https://doi.org/10.1016/j.procs.2018.03.019

36. Policy Management Engine (PME): A policy-based schema to classify and manage sensitive data in cloud storages/ Faraz Fatemi Moghaddam, Philipp Wieder, RaminYahyapour. Journal of Information Security and Applications, Volume 36, October 2017. pp. 11-19. https://doi.org/10.1016/j.jisa.2017.07.003

37. Research on Behavior-Based Data Leakage Incidents for the Sustainable Growth of an Organization/ Jawon Kim, Jaesoo Kim, Hangbae Chang. Sustainability 2020, 12, 6217. pp. 1-14. doi:10.3390/su12156217

38. The Access Control Technologies Handbook – Prepared by Space and Naval Warfare Systems Center Atlantic, 2015. 53 p.

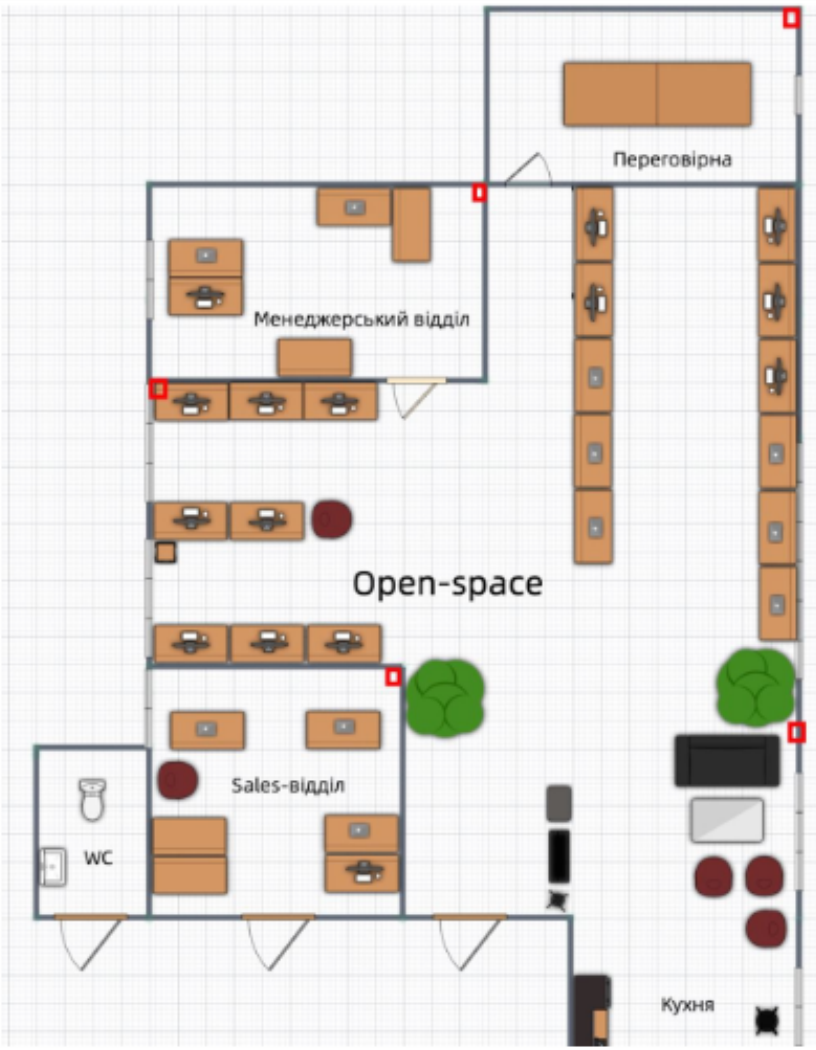
39. TSQM: Trust-based Secure Query Method in Anonymous Communication System/ Xiaohuan Liua, Fengyin Lia, Jiguo Yua, Can Cui. Procedia Computer Science 129 (2018), Elsevier Ltd. pp. 394-399. https://doi.org/10.1016/j.procs.2018.03.014.

40. Yanko A., Vyhivskyi R. Система захисту комп'ютерної мережі. Системи управління, навігації та зв'язку. Збірник наукових праць. 2022. Т. 2, № 68. С. 91–94. URL: https://doi.org/10.26906/sunz.2022.2.091 (дата звернення: 15.05.2023).

ДОДАТОК А

Копія графічної частини

КРКБ.190103.19.01.04 Е8



						КРКБ.190103.19.01.04 Е8	
Зм.	Арк.	№ докум.	Підпис	Дата	Система контролю та управління доступом для підвищення інформаційної безпеки підприємства	Літ.	Маса	Масштаб
Розроб.		Данець О. Я.				У		
Перевір.		Тітов В. Ю.						
Т.контр.						Аркуш 2	Аркушів 3	
Н.контр.		Москвін С. Б.			Схема розміщення датчиків руху і розбиття скла	ХНУ, КБ-19-1		
Затверд.		Кульц Ю. П.						

КРКБ.190103.19.01.04 Е8

Загроза	Вірогідність	Наслідки
Вторгнення в мережу або систему	Висока	Несанкціонований доступ до конфіденційних даних, пошкодження або зміна даних, витік конфіденційної інформації, перерви в роботі системи
Фішинг (вилучення конфіденційних даних)	Середня	Крадіжка облікових даних та паролів, несанкціонований доступ до системи, втрата даних
Витік конфіденційної інформації	Висока	Втрата довіри клієнтів та партнерів, фінансові втрати, шкода репутації
Втрата або крадіжка пристроїв	Середня	Витік конфіденційних даних, втрата даних, втрата фізичного обладнання
Несанкціонований доступ до даних	Висока	Крадіжка конфіденційних даних, порушення приватності клієнтів, шкода репутації, правові наслідки
Атаки на сервери та мережеве обладнання	Висока	Пошкодження або втрата даних, зниження продуктивності мережі, перерви в роботі системи, витрати на відновлення та відновлення послуг
Недостатня свідомість щодо кібербезпеки	Середня	Підвищення ризику використання вразливостей, недостатня реагування на загрози, зростання вразливостей

Загроза	Вірогідність	Наслідки
Недостатня резервне копіювання даних	Середня	Втрата даних при випадку відмови обладнання, нездатність відновити важливі дані, перерва в роботі бізнесу
Недостатній контроль доступу	Середня	Несанкціонований доступ до системи, зловживання правцівеями, втрата даних, порушення приватності
Недостатня фізична безпека	Середня	Крадіжка або пошкодження обладнання, незаконний доступ до приміщень, втрата даних, вплив на безпеку
Віруси та шкідливі програми	Висока	Втрата даних, пошкодження системи, перерва в роботі, фінансові втрати, втрата довіри клієнтів
Втрати через недостатній моніторинг	Середня	Невчасне виявлення атак, затримка в реагуванні, зростання наслідків і втрат
Фізичні явища	Середня	Пошкодження обладнання, приміщення офісу, втрата даних, фінансові втрати

Порушник	Мотивація	Навички	Методи порушення
Зовнішній зловмисник	Фінансова вигода	Високі	Кібератаки, фішинг, використання вразливостей програмного забезпечення
Конкурент	Конкурентна розвідка	Середні	Злом систем, крадіжка інтелектуальної власності, шпигунство
Недобросовісний співробітник	Вирівка незадоволення, збирання даних	Високі	Незаконне використання доступу, крадіжка даних, пошкодження систем
Екс-співробітник	Мстивість, розкриття інформації	Середні	Незаконний доступ, розкриття конфіденційної інформації
Соціальний інженер	Незаконне здобуття доступу	Високі	Фішинг, маніпулювання співробітниками, підбір паролів
Внутрішній зловмисник	Фінансова вигода, розкриття інформації	Високі	Використання недоліків в системах, злом доступу, крадіжка даних
Хакер-активіст	Політичні чи ідеологічні мотиви	Високі	Дефейс сайтів, DDoS-атаки, розкриття інформації
Зовнішній співробітник	Незадоволення, відмова в обслуговуванні		Злом систем, використання слабких паролів, фішинг

						КРКБ.190103.19.01.04 Е8	
Змі	Арк	№ докум.	Підпис	Дата			
Розроб.		Данець О. Я.			Система контролю та управління доступом для підвищення інформаційної безпеки підприємства	Літ	Маса / Масштаб
Перевір.		Гітов В. Ю.				У	
Т.контр.						Аркуш 3	Аркушів 3
Н.контр.		Мотовня С. Б.			Модель загроз і модель порушника	ХНУ, КБ-19-1	
Затверд.		Кальц Ю. Л.					

РІШЕННЯ ЕКСПЕРТНОЇ 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 та управління доступом для підвищення рівня інформаційної безпеки підприємства

Автор: Джиган Олександр Русланович

Спеціальність: 125 – Кібербезпека

Освітня програма: освітньо-професійна

Науковий керівник: Тітова Віра Юріївна, 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 91.87%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v-15.257 складає 99%.

Згідно з Положенням про систему забезпечення академічної доброчесності у ХНУ (https://khmnu.edu.ua/wp-content/uploads/normatyvni-dokumenty/polozhennya/pro-systemu-zabezpechennya-akademichnoyi-dobrochesnosti.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. Максимальний обсяг збігу з одним джерелом, визначений системою виявлення збігів/ ідентичності/схожості, складає 1.07%, що зумовлено текстовим наповненням рамок, яке є стандартним.
2. Інші збіги є збігами в назвах використаних друкованих видань, розміщених в переліку джерел посилань, наявністю типових фразеологічних виразів предметної області, а також формулюваннями, які утворюють загальновживані фрази.

Керівник роботи _____ В.Ю. Тітова

Завідувач кафедри кібербезпеки _____ Ю. П. Кльоц

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ

Направляється студент Джиган Олександр Русланович на захист дипломного проєкту (роботи)
(прізвище, ім'я, по батькові)

за спеціальністю 125 - Кібербезпека

На тему: Система контролю та управління доступом для підвищення рівня інформаційної безпеки підприємства

Дипломний проєкт (робота), рецензія, довідка про перевірку на плагіат додаються.

Декан факультету ____________ Олег САВЕНКО
(підпис) (ім'я, прізвище)

ДОВІДКА УСПІШНОСТІ

Джиган О. Р. за період навчання на факультеті інформаційних технологій з 2019 по 2023 роки повністю виконав навчальний план спеціальності з таким розподілом оцінок за:
національною шкалою: відмінно 13,64 %, добре 54,55 %, задовільно 31,82 %.
шкалою ЄКТС: A 11,43 %, B 40,00 %, C 17,14 %, D 20,00 %, E 11,43 %.

Методист факультету ____________ ____________
(підпис) (ім'я, прізвище)

ВИСНОВОК КЕРІВНИКА ДИПЛОМНОГО ПРОЄКТУ (РОБОТИ) ТА ОБГРУНТУВАННЯ ОЦІНКИ

Студент Джиган О.Р. на належному рівні виконав поставлене завдання та за свою роботу заслуговує оцінки „відмінно".

Оцінка дипломного проєкту (роботи) відмінно // А, (500)

Керівник дипломного проєкту ____________ Попов В.Ю.
(підпис) (ім'я, прізвище)

"5" 06 2023 р.

ВИСНОВОК КАФЕДРИ ПРО ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ)

Дипломний проєкт (роботу) розглянуто. Студент Джиган О. Р. допускається до захисту цього проєкту (роботи) в екзаменаційній комісії.

Завідувач кафедри кібербезпеки
(назва)

Юрій Клots
(підпис, ім'я, прізвище)

"7" 06 2023 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітньо-кваліфікаційного рівня «бакалавр»

Студент Джиган Олександр Русланович
Тема: «Система контролю та управління доступом для підвищення рівня інформаційної безпеки підприємства»
Галузь знань 12 «*Інформаційні технології*» Спеціальність 125 «*Кібербезпека*» Освітня програма «Кібербезпека»

Обсяг дипломної роботи освітньо-кваліфікаційного рівня «бакалавр»: кількість листів креслень 3; кількість сторінок записки 67;

1. Короткий зміст КР та прийнятих рішень Кваліфікаційна робота присвячена дослідженню питань, пов'язаних з розробкою та впровадженням системи контролю та управління доступом для підприємства з метою підвищення рівня інформаційної безпеки. Для досягнення цієї мети було проведено дослідження різних систем контролю та управління доступом, їх переваг та недоліків, а також методів їх впровадження в підприємство. Робота має на меті допомогти підприємствам забезпечити безпеку своїх даних та інформації, зменшити витрати на їхнє захист та уникнути можливих витоків даних.

2. Висновок про відповідність КР завданню Кваліфікаційна робота у повній мірі відповідає поставленому завданню як в теоретичній так і у практичній частині роботи.

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі обґрунтовується актуальність теми роботи, її зв'язок з галуззю знань «Інформаційні технології» та спеціальністю «Кібербезпека», формулюється мета та основні завдання кваліфікаційної роботи. У першому розділі було проведено аналіз існуючих систем контролю та управління доступом, що дозволило виявити проблеми та завдання, що потребують вирішення; застосування принципів побудови систем контролю та управління доступом стало основою для постановки задачі і проєктування архітектури системи. У другому розділі було проаналізовано вимоги та потреби підприємства з урахуванням специфіки, визначено необхідні компоненти та функціонал системи контролю та управління доступом, побудовано модель загроз і модель порушника. У третьому розділі наведено опис процесу реалізації системи контролю та управління доступом на підприємстві, включаючи планування приміщення, підбір пристроїв та впровадження системи, проведено оцінку ефективності впровадженої системи контролю та управління доступом.

4. Позитивні сторони кваліфікаційної роботи полягають у тому що, застосування відповідних пристроїв і процедур дозволило забезпечити надійний контроль доступу та зменшити ризик несанкціонованого доступу до приміщення. Підприємство зазнало покращення своєї інформаційної безпеки і здатне ефективно впоратися з потенційними загрозами і порушниками.В цілому, реалізація системи контролю та управління доступом на підприємстві виявилася успішною і відповідає вимогам та потребам підприємства. Застосування відповідних технологій та процедур дозволило забезпечити підвищену інформаційну безпеку і зменшити ризики несанкціонованого доступу. Реалізована система є надійним інструментом для захисту цінної інформації та забезпечення контролю над доступом на підприємстві.

5. Негативні сторони проекту: -

6. Оцінка графічного оформлення та пояснювальної записки роботи. Графічне оформлення виконане відповідно до теми кваліфікаційної роботи із дотриманням усіх стандартів. У загальному графічне оформлення виконане на достатньому технічному рівні. Пояснювальна записка відповідає нормам для її оформлення та вимогам

7. Відгук про роботу в цілому В загальному кваліфікаційна робота заслуговує позитивної оцінки. Весь матеріал кваліфікаційної роботи структурований, чіткий та послідовний. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики кваліфікаційної роботи. У пояснювальній записці багато наглядних пояснень. Графічний матеріал дозволяє наочно побачити доцільність та ефективність рішень, які були прийняті за основу для досягнення поставленої задачі проектування.

8. Інші зауваження -

9. Оцінка дипломної роботи Розглянувши позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що робота заслуговує оцінки «відмінно/ А (4,75)».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) декан факультету інформаційних технологій, д.т.н., професор Савенко Олег Станіславович

« 5 » червня 2023 . _____ (підпис)

UNICHECK

Ім'я користувача:
Кафедра кібербезпеки

ID перевірки:
1015445156

Дата перевірки:
05.06.2023 23:17:33 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
05.06.2023 23:18:38 EEST

ID користувача:
100008300

Назва документа: **Джиган**

Кількість сторінок: **66** Кількість слів: **11717** Кількість символів: **92203** Розмір файлу: **13.28 MB** ID файлу: **1015105543**

8.13%
Схожість

Найбільша схожість: **1.92%** з джерелом з Бібліотеки (ID файлу: **1011466175**)

6.4% Джерела з Інтернету	531	Сторінка 68
4.11% Джерела з Бібліотеки	115	Сторінка 71

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: 6%**

	Документ		Сумарний збіг по Базі Даних	
ID: 114872 Назва: Система контролю та управління доступом для підвищення рівня інформаційної безпеки підприємства Додано в БД: 2023-06-05 Автора: Джиган О.Р. Керівники: Тітова В.Ю. Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	72282	1095	2915 (4%)	43 (4%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми