

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет радіоелектроніки та телекомунікації
(повне найменування інституту, назва факультету)

Кафедра захисту інформації
(повна назва кафедри)

Пояснювальна записка

до дипломного проекту (роботи)
бакалавр
(ступінь вищої освіти)

на тему РОЗРОБКА СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ СЕРВЕРНОГО
ПРИМІЩЕННЯ ПІДПРИЄМСТВА
DEVELOPMENT OF AN INFORMATION PROTECTION SYSTEM FOR
THE ENTERPRISE'S SERVER ROOM

Виконав: студент(ка) 4 курсу, групи РТЗ-719
Спеціальності 125 Кібербезпека
(код і найменування спеціальності)

Освітня програма (спеціалізація)
Системи технічного захисту інформації,
автоматизація її обробки

КНИШ В.В.

(ПРИЗВИЩЕ та ініціали)

Керівник ЛІЗУНОВ С.І.

(ПРИЗВИЩЕ та ініціали)

Рецензент МАЛИЙ О.Ю.

(ПРИЗВИЩЕ та ініціали)

2023

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

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

ЗАТВЕРДЖУЮ
Завідувач кафедри ЗІ, к.т.н, доц.
В.О. ВОСКОБОЙНИК
“01” “06” 2023 року

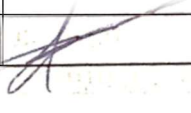
З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА

КНИША Владислава Вікторовича

(ПРИЗВИЩЕ, ім'я, по батькові)

1. Тема проєкту (роботи) Розробка системи захисту інформації серверного приміщення підприємства
development of an information protection system for the enterprise's server room
- керівник проєкту (роботи) к.т.н., доцент ЛІЗУНОВ Сергій Іванович,
(науковий ступінь, вчене звання, ПРИЗВИЩЕ, ім'я, по батькові.)
- затверджені наказом закладу вищої освіти від “04” квітня 2023 року № 95
2. Строк подання студентом проєкту (роботи) 01 червня 2023 року
3. Вихідні дані до проєкту (роботи) Розробити систему захисту інформації серверного приміщення підприємства
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Аналіз сучасного стану питання, аналіз офісного приміщення, розробка системи захисту
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень) презентація

6. Консультанти розділів проєкту (роботи)

Розділ	ПРІЗВИЩЕ, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
Розділи 1-3	ЛІЗУНОВ С.І., к.т.н. доцент		
Нормоконтроль	КОРОЛЬКОВ Р. Ю., к.т.н. ст.викл		

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

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1	Постановка завдання роботи.	1 тиждень	Завдання, ТЗ
2	Аналіз предметної області.	1 тиждень	Розділ 1
3	Дослідження офісного приміщення підприємства для реалізації завдання.	2 тиждень	Розділ 2
4	Створення системи захисту серверного приміщення	3-4 тижні	Розділ 3
5	Оформлення пояснювальної записки та відповідної документації	6-7 тиждень	Додатки
7	Нормоконтроль та рецензування.	8 тиждень	
8	Захист дипломної роботи.	9 тиждень	

Студент(ка)

(підпис) Владислав КНИШ
(Ім'я ПРІЗВИЩЕ)

Керівник проєкту (роботи)

(підпис) Сергій ЛІЗУНОВ
(Ім'я ПРІЗВИЩЕ)

РЕФЕРАТ

Пояснювальна записка до дипломної кваліфікаційної роботи бакалавра:
54 с., 14 табл., 8 рис., 24 джерела.

АДМІНІСТРАТИВНИЙ ЗАХИСТ, ЗАХИЩЕНІСТЬ ІНФОРМАЦІЇ,
ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНА СИСТЕМА, МЕРЕЖЕВИЙ
ЗАХИСТ, ПРОГРАМНИЙ ЗАХИСТ, РЕЖИМНЕ ПІДПРИЄМСТВО,
СЕРВЕРНЕ ПРИМІЩЕННЯ, СИСТЕМА БЕЗПЕКИ, ФІЗИЧНИЙ ЗАХИСТ

Об'єкт розробки – інформаційно-телекомунікаційна система «Nexus».

Предмет розробки – система безпеки інформації серверного приміщення офісу.

Мета роботи – досягнення достатнього рівня захищеності інформації в серверному приміщенні.

Розробка проводиться в рамках розгляду таких аспектів, як фізичний захист, мережевий захист, програмний захист та адміністративний захист.

В результаті проведеної роботи було створено належний фізичний, мережевий, програмний і адміністративний захист серверного приміщення режимного підприємства для забезпечення безпеки і надійності інформаційних систем. Впровадження цих заходів дозволить попередити несанкціонований доступ до серверного приміщення, зберегти цілісність і конфіденційність інформації та забезпечити відповідність вимогам нормативних актів і стандартів у сфері інформаційної безпеки.

ABSTRACT

Explanatory note to the bachelor's thesis: 54 p., 14 tables, 8 figures, 24 sources.

ADMINISTRATIVE PROTECTION, INFORMATION AND TELECOMMUNICATION SYSTEM, INFORMATION SECURITY, NETWORK PROTECTION, PHYSICAL PROTECTION, SECURE ENTERPRISE, SECURITY SYSTEM, SERVER ROOM, SOFTWARE PROTECTION

Object of development - information and telecommunication system "Nexus".

The subject of development is the information security system of the office server room.

The purpose of the work is to achieve a sufficient level of information security in the server room.

The development is carried out within the framework of consideration of such aspects as physical protection, network protection, software protection and administrative protection.

As a result of the work done, proper physical, network, software and administrative protection of the server room of a sensitive enterprise was created to ensure the security and reliability of information systems. Implementation of these measures will prevent unauthorized access to the server room, preserve the integrity and confidentiality of information and ensure compliance with the requirements of regulations and standards in the field of information security.

ЗМІСТ

Перелік скорочень.....	7
Вступ.....	8
1 Аналіз сучасного стану питання.....	9
1.1 Інформаційна безпека.....	9
1.2 Аналіз нормативно-правового забезпечення захисту інформації.....	16
1.3 Постановка задачі	18
2 Аналіз офісного приміщення.....	19
2.1 Загальні відомості про підприємство ТОВ «Nexus»	19
2.2 Аналіз підприємства	21
2.3 Обстеження об'єкту інформаційної діяльності	28
2.4 Аналіз загроз та вразливостей	35
2.5 Модель порушника	35
3 Розробка системи захисту	40
3.1 Встановлення фізичного захисту	40
3.2 Мережевий захист.....	43
3.3 Програмний захист	46
3.4 Адміністративний захист	49
Висновки	51
Перелік використаних джерел	52

ПЕРЕЛІК СКОРОЧЕНЬ

- ІТС – інформаційно-телекомунікаційна система;
- ДСТУ – Державний стандарт України;
- ОІД – об’єкт інформаційної діяльності;
- СЗІ – система захисту інформації;
- CRM (Customer relationship management) - управління відносинами з клієнтами;
- DoS (Denial-of-Service) – відмова в обслуговуванні;
- ISO (International Organization for Standardization) - міжнародна організація зі стандартизації;
- MITM (Man-in-the-Middle) – атака «людина посередні»;
- PUP (Potentially unwanted program) – потенційно небажана програма;
- SQL (Structured query language) – мова структурованих запитів;
- CIA (Confidentiality, Integrity and Availability) - конфіденційність, цілісність, доступність.

ВСТУП

У сучасному світі інформаційні технології використовуються практично в усіх сферах діяльності людей. Вони значно спрощують процеси роботи, забезпечують швидку та зручну комунікацію, зберігають інформацію і розповсюджують її. Проте, разом з тим, інформаційні технології приносять ризики, пов'язані з можливістю несанкціонованого доступу до інформації, втрати даних, впливу шкідливого програмного забезпечення та інших кіберзагроз. Особливо це стосується серверних приміщень режимних підприємств, де зберігається і обробляється важлива та конфіденційна інформація.

Більшість людей і підприємств малого бізнесу нехтують правилами безпеки, через це популярність різного роду політик безпеки росте.

Метою даної дипломної роботи є розробка системи захисту інформаційних ресурсів серверного приміщення офісного приміщення з використанням засобів системи захисту інформації (СЗІ). Розробка проводиться в рамках розгляду таких аспектів, як фізичний захист, мережевий захист, програмний захист та адміністративний захист.

Об'єкт для розробки системи: інформаційно-телекомунікаційна система «Nexus».

Предмет розробки: система безпеки інформації серверного приміщення офісу.

Мета роботи: досягнення достатнього рівня захищеності інформації в серверному приміщенні.

1 АНАЛІЗ СУЧАСНОГО СТАНУ ПИТАННЯ

1.1 Інформаційна безпека

Кібербезпека – це захист підключених до Інтернету пристроїв і служб від зловмисних атак хакерів, спамерів і кіберзлочинців. Ця практика використовується компаніями для захисту від фішингових схем, атак програм-вимагачів, крадіжки особистих даних, витоку даних і фінансових втрат.

Озирніться навколо сучасного світу, і ви побачите, що повсякденне життя більше, ніж будь-коли раніше, залежить від технологій. Переваги цієї тенденції варіюються від майже миттєвого доступу до інформації в Інтернеті до сучасних зручностей, які забезпечують технологія автоматизації розумного дому та такі концепції, як Інтернет речей.

Проте, незважаючи на райдужне сприйняття суспільством сучасних досягнень, загрози кібербезпеці, які представляють сучасні технології, є реальною небезпекою.

Кібербезпека використовувалася як загальний термін у ЗМІ для опису процесу захисту від усіх форм кіберзлочинності, від крадіжки особистих даних до міжнародної цифрової зброї, але це визначення не в змозі охопити справжню природу кібербезпеки для тих, хто не має відповідної освіти чи досвіду роботи в цифровій індустрії.

Cisco Systems, технологічний конгломерат, що спеціалізується на мережах, хмарі та безпеці, визначає кібербезпеку як «...практику захисту систем, мереж і програм від цифрових атак. Ці кібератаки зазвичай спрямовані на доступ, зміну або знищення конфіденційної інформації, вимагання грошей у користувачів, або переривання звичайних бізнес-процесів».

Чому кібербезпека важлива? У сучасному цифровому світі не можна ігнорувати кібербезпеку. Одне єдине порушення безпеки може призвести до

розкриття особистої інформації мільйонів людей. Ці порушення мають сильний фінансовий вплив на компанії, а також втрату довіри клієнтів. Отже, кібербезпека дуже важлива для захисту компаній і окремих осіб від спамерів і кіберзлочинців.

Масштаб загрози кібербезпеці

За даними Forbes, 2022 рік подарує нам низку різноманітних і жахливих викликів кібербезпеці, починаючи від збою в ланцюжку поставок і посилюючи ризики для смарт-пристроїв, аж до тривалої посухи кадрів у сфері кібербезпеки.

Згідно з журналом Cybercrime Magazine, до 2025 року кіберзлочинність коштуватиме світові 10,5 трильйонів доларів щорічно! Крім того, прогнозується, що глобальні витрати на кіберзлочинність зростатимуть майже на 15 відсотків щорічно протягом наступних чотирьох років.

Такі поняття, як пандемія, криптовалюта та зростання віддаленої роботи, об'єднуються, щоб створити середовище, багате цілями, яким можуть скористатися злочинці.

Як працює кібербезпека? Кібербезпека охоплює технології, процеси та методи захисту комп'ютерних систем, даних і мереж від атак. Щоб найкраще відповісти на питання «що таке кібербезпека» і як працює кібербезпека, потрібно розділити її на низку піддоменів:

Безпека програми. Безпека додатків охоплює реалізацію різних засобів захисту в програмному забезпеченні та службах організації від різноманітних загроз. Цей піддомен вимагає від експертів з кібербезпеки написання безпечного коду, розробки безпечних архітектур додатків, впровадження надійної перевірки введених даних тощо, щоб мінімізувати ймовірність несанкціонованого доступу або модифікації ресурсів додатків.

Хмарна безпека. Хмарна безпека стосується створення захищених хмарних архітектур і програм для компаній, які використовують

постачальників хмарних послуг, як-от Amazon Web Services, Google, Azure, Rackspace тощо.

Управління ідентифікацією та безпека даних. Цей субдомен охоплює дії, інфраструктури та процеси, які забезпечують авторизацію та автентифікацію законних осіб в інформаційних системах організації. Ці заходи передбачають впровадження потужних механізмів зберігання інформації, які захищають дані, незалежно від того, перебувають вони в процесі переходу або знаходяться на сервері чи комп'ютері. Крім того, цей піддомен ширше використовує протоколи автентифікації, як двофакторні, так і багатофакторні.

Мобільна безпека. Мобільна безпека сьогодні є великою справою, оскільки все більше людей покладаються на мобільні пристрої. Цей субдомен захищає організаційну та особисту інформацію, що зберігається на мобільних пристроях, таких як планшети, стільникові телефони та ноутбуки, від різних загроз, таких як несанкціонований доступ, втрата або крадіжка пристрою, зловмисне програмне забезпечення, віруси тощо. Крім того, мобільна безпека використовує автентифікацію та навчання для посилення безпеки.

Безпека мережі. Безпека мережі охоплює апаратні та програмні механізми, які захищають мережу та інфраструктуру від збоїв, несанкціонованого доступу та інших зловживань. Ефективна безпека мережі захищає активи організації від широкого спектру загроз зсередини та ззовні організації.

Аварійне відновлення та планування безперервності бізнесу. Не всі загрози є людськими. Субдомен DR BC охоплює процеси, сповіщення, моніторинг і плани, розроблені для того, щоб допомогти організаціям підготуватися до підтримки роботи своїх критично важливих для бізнесу систем під час і після будь-яких інцидентів (масові збої електроенергії, пожежі, стихійні лиха), а також відновлення та відновлення втрачених операцій і системи після інциденту.

Навчання користувачів. Знання — це сила, і обізнаність персоналу щодо кіберзагроз є цінною в головоломці кібербезпеки. Навчання бізнес-персоналу основам комп'ютерної безпеки має вирішальне значення для підвищення обізнаності щодо найкращих галузевих практик, організаційних процедур і політики, моніторингу та звітування про підозрілу та шкідливу діяльність. Цей субдомен охоплює курси, програми та сертифікати, пов'язані з кібербезпекою.

Що таке кібербезпека та типи кіберзагроз. Кіберзлочин визначається як будь-яка несанкціонована діяльність із залученням комп'ютера, пристрою чи мережі. Існує три загальновизнані класифікації кіберзлочинів: злочини за допомогою комп'ютера, злочини, де комп'ютер сам є мішенню, і злочини, де комп'ютер є випадковим, а не безпосередньо пов'язаним із злочином.

Ось список поширених кіберзагроз:

- кібертероризм: ця загроза є політично обґрунтованою атакою на комп'ютери та інформаційні технології з метою заподіяння шкоди та створення широкомасштабних соціальних розладів;
- зловмисне програмне забезпечення: ця загроза включає програми-вимагачі, шпигунські програми, віруси та черв'яки. Він може інсталиювати шкідливе програмне забезпечення, блокувати доступ до ресурсів вашого комп'ютера, порушувати роботу системи або приховано передавати інформацію з вашого сховища даних;
- трояни: подібно до легендарного троянського коня з міфології, ця атака змушує користувачів думати, що вони відкривають нешкідливий файл. Натомість, як тільки троян встановлено, він атакує систему, як правило, встановлюючи бекдор, який дозволяє отримати доступ кіберзлочинцям;
- ботнети: Ця особливо огидна атака передбачає широкомасштабні кібератаки, які здійснюються дистанційно керованими пристроями, зараженими шкідливим програмним забезпеченням. Подумайте про це як про

низку комп'ютерів під контролем одного кіберзлочинця. Що ще гірше, скомпрометовані комп'ютери стають частиною ботнет-системи;

- рекламне програмне забезпечення: ця загроза є різновидом шкідливого програмного забезпечення. Його часто називають програмним забезпеченням, що підтримується рекламою. Вірус рекламного програмного забезпечення — це потенційно небажана програма (PUP), яка встановлюється без вашого дозволу та автоматично генерує небажану онлайн-рекламу;

- SQL-ін'єкція: атака структурованої мови запитів вставляє шкідливий код на сервер, що використовує SQL;

- фішинг: хакери використовують фальшиві повідомлення, особливо електронну пошту, щоб змусити одержувача відкрити її та виконати інструкції, які зазвичай просять надати особисту інформацію. Деякі фішингові атаки також встановлюють зловмисне програмне забезпечення;

- атака «людина посередині»: атаки MITM передбачають введення хакерів у онлайн-транзакцію двох осіб. Потрапивши в систему, хакери можуть фільтрувати та викрадати потрібні дані. Атаки MITM часто відбуваються в незахищених публічних мережах Wi-Fi;

- відмова в обслуговуванні: DoS — це кібератака, яка заповнює мережу або комп'ютер величезною кількістю процесів «рукоятискання», що фактично перевантажує систему та робить її нездатною відповідати на запити користувачів.

Оскільки витрати даних, хакерство та кіберзлочинність досягають нових висот, компанії все більше покладаються на експертів з кібербезпеки для виявлення потенційних загроз і захисту цінних даних. Тому цілком зрозуміло, що очікується, що ринок кібербезпеки зросте з 217 мільярдів доларів США у 2021 році до 345 мільярдів доларів США до 2026 року, опублікувавши зведений річний темп зростання (CAGR) у 9,7% з 2021 по 2026 рік.

Переваги кібербезпеки. Сучасна галузь кібербезпеки в першу чергу зосереджена на захисті пристроїв і систем від зловмисників. Хоча біти та байти, що стоять за цими зусиллями, важко уявити, набагато простіше розглянути наслідки. Без фахівців з кібербезпеки, які невтомно працюють, було б майже неможливо користуватися багатьма веб-сайтами через постійні спроби атак типу «відмова в обслуговуванні». Уявіть, що у вас немає доступу до спільноти експертів і сертифікованих професіоналів Simplilearn — більше ніяких підказок, підказок і порад, які допоможуть вам досягти ваших професійних цілей!

Без надійного захисту від кібербезпеки було б легко знищити такі необхідні сучасні елементи, як електромережі та очисні споруди, які забезпечують безперебійну роботу світу.

Простіше кажучи, кібербезпека є критично важливою, оскільки вона допомагає зберегти спосіб життя, який ми звикли пізнати та насолоджуватися ним.

Міфи про кібербезпеку. Потрібно добре усвідомлювати, що кількість кібератак продовжує зростати. У сучасну епоху технологій організації та окремі особи повинні захищати себе від більшості видів загроз. На жаль, існує кілька помилкових уявлень про кібербезпеку, які все ще стримують багатьох людей від вжиття необхідних заходів для захисту особистої конфіденційної інформації.

Ось кілька поширених міфів про кібербезпеку, які варто знати.

- самих паролів достатньо, щоб захистити вас: не слід покладатися лише на паролі, щоб зберегти дані в безпеці. Хоча надійні паролі важливі, кіберзлочинці все одно можуть знайти способи їх зламати. Тому необхідно впроваджувати надійні заходи кібербезпеки, мати багаторівневий захист;

- видалення файлу з комп'ютера: після видалення даних із комп'ютера файл переміщується до кошика, а потім очищається. Навіть після

видалення даних вони залишаються на жорсткому диску, наприклад, у папці тимчасових файлів;

– рішення для шифрування не варті того: деякі організації дотримуються думки, що програмне забезпечення для шифрування — це те, без чого вони можуть обійтися. Це помилкова думка, що шифрування дозволить уникнути витоку даних. Шифрування відіграє важливу роль у захисті від кіберзлочинців і атак програм-вимагачів;

– малий і середній бізнес не є ціллю: це міф, що лише великі компанії не є захищеними, лише ці компанії є ціллю кіберзлочинців. Відповідно до звіту про розслідування витоку даних за 2021 рік, 61% усіх малих і середніх підприємств повідомили про принаймні одну кібератаку протягом року. Оскільки ці компанії мають менш надійні заходи безпеки. Тому необхідно захищати компанії від кіберзлочинів.

Безпека будь-якої організації починається з трьох принципів: конфіденційність, цілісність, доступність. Це називається CIA, яке слугує галузевим стандартом комп'ютерної безпеки з часів перших мейнфреймів.

Конфіденційність: принципи конфіденційності стверджують, що лише авторизовані сторони можуть отримати доступ до конфіденційної інформації та функцій. Приклад: військова таємниця.

Цілісність: принципи цілісності стверджують, що лише авторизовані люди та засоби можуть змінювати, додавати або видаляти конфіденційну інформацію та функції. Приклад: користувач вводить невірні дані в базу даних.

Доступність: принципи доступності стверджують, що системи, функції та дані мають бути доступними на вимогу відповідно до узгоджених параметрів на основі рівнів обслуговування.

1.2 Аналіз нормативно-правового забезпечення захисту інформації

Основним документом є Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». Він включає в себе наступні ключові пункти:

- предмет регулювання Закону: закон регулює відносини, що виникають під час створення, використання та захисту інформації в інформаційно-телекомунікаційних системах;
- основні принципи захисту інформації: закон визначає основні принципи захисту інформації, включаючи принципи законності, багаторівневого захисту, комплексного захисту, системності та неперервності захисту інформації.

Закон визначає суб'єктів відносин у сфері захисту інформації, включаючи:

- власників інформації;
- користувачів інформації;
- операторів інформаційно-телекомунікаційних систем;
- органи державної влади;
- органи місцевого самоврядування та інші.

Також, закон визначає права та обов'язки суб'єктів відносин у сфері захисту інформації.

Організація захисту інформації в інформаційно-телекомунікаційних системах: Закон регулює організацію захисту інформації в інформаційно-телекомунікаційних системах.

Відповідальність за порушення законодавства про захист інформації: Закон встановлює відповідальність за порушення законодавства про захист інформації.

Специфічні заходи захисту інформації, вказані в Законі України «Про захист інформації в інформаційно-телекомунікаційних системах»:

- організаційні заходи: включає в себе розробку та впровадження політики захисту інформації, проведення аудиту захисту інформації, проведення навчання з питань захисту інформації, та інше;
- технічні заходи: включає в себе використання спеціальних технічних засобів захисту інформації, використання криптографічних засобів захисту інформації, використання засобів контролю доступу до інформації, та інше;
- криптографічний захист – визначає, як саме здійснюється криптографічний захист інформації в інформаційно-телекомунікаційних системах;
- захист інформації від витоку через технічні канали витоку визначає, що захист інформації від витоку через технічні канали витоку інформації здійснюється за допомогою спеціальних технічних засобів.

Відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», суб'єкти, які беруть участь у захисті інформації, мають наступні обов'язання:

- власники мають забезпечити захист інформації в системах, які вони володіють. Це включає в себе розробку та впровадження політики захисту інформації, забезпечення організаційних та технічних заходів захисту інформації, забезпечення криптографічного захисту інформації, та інше;
- оператори інформаційно-телекомунікаційних систем мають забезпечити захист інформації в системах, які вони оперують. Це включає в себе забезпечення організаційних та технічних заходів захисту інформації, забезпечення криптографічного захисту інформації, та інше;
- користувачі інформаційно-телекомунікаційних систем мають дотримуватися правил захисту інформації в системах, які вони використовують. Це включає в себе дотримання політики захисту інформації, дотримання організаційних та технічних заходів захисту інформації, дотримання правил криптографічного захисту інформації, та інше.

1.3 Постановка задачі

Задача базується на аналізі проблеми вразливостей малих організацій, які не приділяють увагу захисту інформації, що обробляється в їх ІТС. Відповідно до виконаного аналізу та вимог нормативних документів у спеціальній частині необхідно виконати наступні задачі:

- ознайомитись з особливостями підприємства;
- проаналізувати фізичні характеристики об'єкту;
- проаналізувати логічну характеристику об'єкту;
- проаналізувати види інформації та особливості взаємодії інформації на об'єкті;
- обрати профіль захищеності;
- розробити основні елементи політики безпеки.

2 АНАЛІЗ ОФІСНОГО ПРИМІЩЕННЯ

2.1 Загальні відомості про підприємство ТОВ «Nexus»

Підприємство «Nexus» - ІТ компанія, яка займається створенням програмних продуктів на замовлення, внесенням коригувань в існуючі програмні продукти і тестуванням в режимі «бета» з залученням реальних користувачів.

Таблиця 2.1 – Штат підприємства «Nexus»

№	Посада	Роль в системі	Кількість працівників на посаді	Рівень кваліфікації	Стаж на підприємстві
1	Директор	Адміністратор	1	Високий	7
2	Заступник директора	Користувач	1	Високий	5
3	Директор HR-відділу	Користувач	1	Високий	5
4	HR-менеджер	Користувач	2	Середній	5
5	Тімлід	Користувач	3	Високий	4
6	Розробник	Користувач	10	Високий	4
7	Акаунт-менеджер	Користувач	2	Високий	5
7	Прибиральниця		1	Низький	3

В обов'язки директора входить регулювання всіх економічних і податкових процесів компанії, таких як оплата податків, виплати і

регулювання заробітних плат. Окрім цього в обов'язки директора входить вирішення позаштатних ситуацій.

Заступник директора виконує функції коректора між рядовим складом компанії і директором, вирішуючи власноруч проблеми, які не потребуються прямого втручання керівника компанії.

Директор HR-відділу і HR-менеджери займаються підбором та прийомом на роботу персоналу.

Тімліди відповідають за вірну роботу команд розробників, включаючи строки проектів, правки, тощо.

Акаунт менеджер відповідає за пошук клієнтів і всі взаємодії з ними. Деякі взаємодії проходять при участі тімлідів.

Структура підприємства зображена на рисунку 2.1

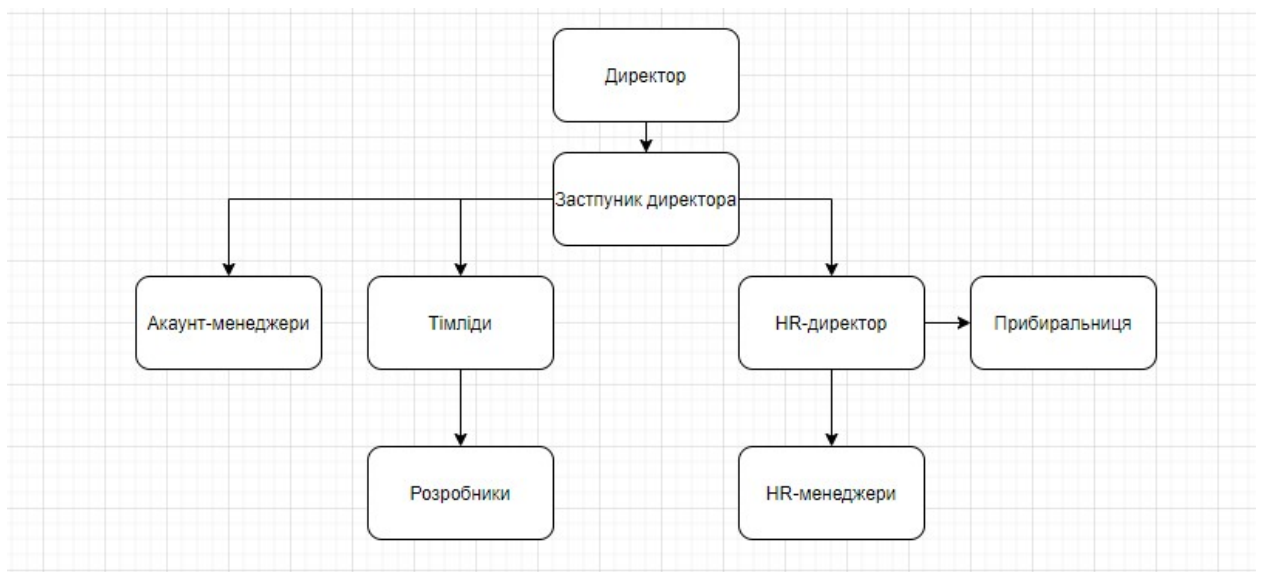


Рисунок 2.1 — Схема структури підприємства

2.2 Аналіз підприємства

Прикладна програма (додаток) — це комп'ютерна програма, призначена для виконання конкретного завдання, відмінного від роботи самого комп'ютера, яке зазвичай використовується кінцевими користувачами.[2] Прикладами є текстові процесори, та бухгалтерське програмне забезпечення. Збірний іменник відноситься до всіх додатків разом.[3] Іншими основними класифікаціями програмного забезпечення є системне програмне забезпечення, пов'язане з роботою комп'ютера, і службове програмне забезпечення.

Програми можуть бути в комплекті з комп'ютером та його системним програмним забезпеченням або опубліковані окремо і можуть бути закодовані як власні, з відкритим кодом або проекти.[4] Термін «додаток» часто відноситься до програм для мобільних пристроїв, таких як телефони.

В інформаційних технологіях додаток (додаток), прикладна програма або прикладне програмне забезпечення — це комп'ютерна програма, призначена для допомоги людям виконувати певну діяльність. Залежно від діяльності, для якої вона була розроблена, програма може маніпулювати текстом, числами, звуком, графікою та комбінацією цих елементів. Деякі пакети програм зосереджені на одному завданні, наприклад обробці текстів; інші, звані інтегрованим програмним забезпеченням, включають кілька додатків.[5]

Написане користувачем програмне забезпечення адаптує системи відповідно до конкретних потреб користувача. Програмне забезпечення, написане користувачами, включає шаблони електронних таблиць, макроси текстового процесора, наукове моделювання, аудіо, графіку та сценарії анімації. Навіть фільтри електронної пошти – це свого роду програмне

забезпечення для користувача. Користувачі самі створюють це програмне забезпечення і часто не помічають, наскільки воно важливе.

Однак розмежування між системним програмним забезпеченням, таким як операційні системи та прикладним програмним забезпеченням, не є точним і іноді є об'єктом суперечок.[6] Наприклад, одне з ключових питань у антимонопольному процесі «Сполучені Штати проти корпорації Microsoft» полягало в тому, чи є веб-браузер Microsoft Internet Explorer частиною її операційної системи Windows чи окремою частиною прикладного програмного забезпечення. Як інший приклад, суперечки щодо імен GNU/Linux частково викликані розбіжностями щодо відносин між ядром Linux та операційними системами, побудованими на цьому ядрі. У деяких типах вбудованих систем програмне забезпечення та програмне забезпечення операційної системи можуть бути нерозрізненими для користувача, як у випадку програмного забезпечення, що використовується для керування відеоманітофоном, DVD-програвачем або мікрохвильовою піччю. Наведені вище визначення можуть виключати деякі програми, які можуть існувати на деяких комп'ютерах у великих організаціях.

Існує багато різних і альтернативних способів класифікації програмного забезпечення. З юридичної точки зору, прикладне програмне забезпечення в основному класифікується з підходом «чорного ящика» щодо прав його кінцевих користувачів або передплатників (з можливими проміжними та багаторівневими рівнями підписки).

Програмні програми також класифікуються за мовою програмування, на якій написаний або виконаний вихідний код, а також з урахуванням їх призначення та результатів.

За правами власності та користування. Прикладне програмне забезпечення зазвичай розрізняють між двома основними класами: програмним забезпеченням із закритим кодом проти програмного

забезпечення з відкритим кодом, а також серед безкоштовних або запатентованих програмних програм.

Власне програмне забезпечення знаходиться під виключним авторським правом, а ліцензія на програмне забезпечення надає обмежені права на використання. Принцип відкрито-закритого стверджує, що програмне забезпечення може бути «відкрите лише для розширення, але не для модифікації». Такі програми можуть отримати доповнення лише від сторонніх розробників.

Безкоштовне програмне забезпечення з відкритим вихідним кодом запускається, розповсюджується, продається або розширюється для будь-яких цілей, і, будучи відкритим, має змінюватися або змінюватися таким же чином.

Програмні програми FOSS, випущені за безкоштовною ліцензією, можуть бути безстроковими, а також безоплатними. Можливо, власник, володар або третя сторона, яка застосовує будь-які права (авторське право, торгова марка, патент або *ius in re aliena*) мають право додавати винятки, обмеження, згасання часу або дати закінчення терміну дії ліцензійних умов використання.

Програмне забезпечення, що є публічним надбанням, є різновидом FOSS, яке є безкоштовним і - відкрито або зарезервовано - може запускатися, поширюватися, змінюватися, змінюватися, повторно публікуватися або створюватися в похідних роботах без будь-якого посилання на авторські права і, отже, відкликання. Його навіть можна продати, але без передачі суспільного надбання іншим суб'єктам. Загальнодоступне програмне забезпечення може бути випущене на підставі юридичної заяви про (не)ліцензування, яка забезпечує виконання цих умов на невизначений термін (на все життя або назавжди).

За допомогою мови кодування. З моменту розробки та майже повсюдного впровадження Інтернету з'явилася важлива відмінність між веб-

додатками, написаними за допомогою HTML, JavaScript та інших веб-технологій, які зазвичай вимагають підключення до Інтернету та використання веб-переглядача. Більш традиційні рідні програми, написані будь-якими мовами, доступними для конкретного типу комп'ютера. У комп'ютерній спільноті точилися суперечливі дебати щодо веб-додатків, які замінюють нативні програми для багатьох цілей, особливо на мобільних пристроях, таких як смартфони та планшети. Веб-програми дійсно значно зросли в популярності для деяких видів використання, але переваги програм роблять їх навряд чи скоро зникнуть, якщо взагалі взагалі зникнуть. Крім того, вони можуть бути доповнювальними і навіть інтегрованими.[9][10][11]

За призначенням і виходом. Прикладне програмне забезпечення також можна розглядати як горизонтальне або вертикальне.[12][13] Горизонтальні програми є більш популярними і поширеними, оскільки вони загального призначення, наприклад, текстові процесори або бази даних. Вертикальні додатки – це нішеві продукти, розроблені для певного типу галузі, бізнесу або відділу в організації. Інтегровані пакети програмного забезпечення намагатимуться впоратися з кожним конкретним можливим аспектом, наприклад, виробничого чи банківського працівника, чи бухгалтерії, чи обслуговування клієнтів.

Існує багато типів прикладного програмного забезпечення [14]:

- набір програм складається з кількох програм, об'єднаних разом. Зазвичай вони мають пов'язані функції, функції та користувацькі інтерфейси і можуть взаємодіяти один з одним, напр. відкривати файли один одного. Бізнес-додатки часто поставляються в комплектах, напр. Microsoft Office, LibreOffice та iWork, які об'єднують текстовий процесор, електронну таблицю тощо; але люкси існують для інших цілей, напр. графіка або музика;
- корпоративне програмне забезпечення відповідає потребам процесів і потоків даних цілої організації в кількох відділах, часто у великому

розподіленому середовищі. Приклади включають системи планування ресурсів підприємства, системи управління відносинами з клієнтами (CRM), механізми реплікації даних та програмне забезпечення для управління ланцюгом поставок. Департаментальне програмне забезпечення — це підтип корпоративного програмного забезпечення, зосередженого на менших організаціях або групах у великій організації. (Приклади включають управління витратами на відрядження та службу підтримки ІТ);

- програмне забезпечення інфраструктури підприємства надає загальні можливості, необхідні для підтримки систем корпоративного програмного забезпечення. (Приклади включають бази даних, сервери електронної пошти та системи для керування мережами та безпекою);

- платформа додатків як послуга (aPaaS) — це служба хмарних обчислень, яка пропонує середовища розробки та розгортання служб додатків;

- програмне забезпечення для інформаційних працівників дозволяє користувачам створювати інформацію та керувати нею, часто для окремих проектів у відділі, на відміну від управління підприємством. Приклади включають управління часом, управління ресурсами, аналітичні інструменти, інструменти для співпраці та документації. Текстові процесори, електронні таблиці, клієнти електронної пошти та блогів, персональна інформаційна система та окремі медіаредактори можуть допомогти у виконанні багатьох завдань інформаційного працівника;

- програмне забезпечення для доступу до вмісту використовується переважно для доступу до вмісту без редагування, але може включати програмне забезпечення, яке дозволяє редагувати вміст. Таке програмне забезпечення задовольняє потреби окремих осіб і груп у споживанні цифрових розваг і опублікованого цифрового контенту. (Приклади включають медіапрогравачі, веб-браузери та довідкові браузери);

- освітнє програмне забезпечення пов'язане з програмним забезпеченням для доступу до вмісту, але має вміст або функції, адаптовані для використання викладачами чи студентами. Наприклад, він може надавати оцінки (тести), відстежувати прогрес за матеріалами або включати можливості спільної роботи;
- програмне забезпечення для моделювання моделює фізичні або абстрактні системи для дослідницьких, навчальних або розважальних цілей;
- програмне забезпечення для розробки медіа створює друковані та електронні засоби масової інформації для використання іншими, найчастіше в комерційних або освітніх умовах. Це включає графічне програмне забезпечення, програмне забезпечення для настільних видавництв, програмне забезпечення для розробки мультимедіа, редактори HTML, редактори цифрової анімації, цифрові аудіо- та відеокomпозиції та багато інших [15];
- програмне забезпечення для розробки продуктів використовується при розробці апаратних і програмних продуктів. Це включає в себе комп'ютерне проектування (CAD), комп'ютерну інженерію (CAE), засоби редагування та компіляції комп'ютерної мови, інтегровані середовища розробки та інтерфейси програмістів прикладних програм;
- програмне забезпечення для розваг може посилатися на відеоігри, заставки, програми для відображення фільмів або відтворення записаної музики та інші види розваг, які можна відчувати за допомогою комп'ютерного пристрою.

Опис програмного забезпечення та його локалізація на комп'ютерах підприємства «Nexus» представлено в таблиці 2.2.

Таблиця 2.2 – Програмне забезпечення в інформаційній системі підприємства

№	Назва ПО	Тип	Ліцензія	Призначення	Термін дії	Встановлено
1	Windows 10	Системне	Commercial	Операційна система	Безстроковий	PC1...PC19
2	Microsoft Word	Прикладне	Commercial	Редактор тексту	Безстроковий	PC1...PC19
3	Microsoft Excel	Прикладне	Commercial	Редактор таблиць	Безстроковий	PC1...PC5, PC18, PC19
4	Adobe Photoshop	Прикладне	Commercial	Графічний редактор	Безстроковий	PC6...PC9
5	Adobe Illustrator	Прикладне	Commercial	Редактор ілюстрацій	Безстроковий	PC6...PC9
6	Visual Studio	Прикладне	Commercial	Інтегроване середовище розробки	Безстроковий	PC10...PC17
7	Visual Studio Code	Прикладне	Commercial	Редактор коду	Безстроковий	PC10...PC17

Система складається з 19 персональних комп'ютерів, 2 принтерів, 3 комутаторів, 2 роутерів.

На рисунку 2.2 зображено схему інформаційної системи підприємства.

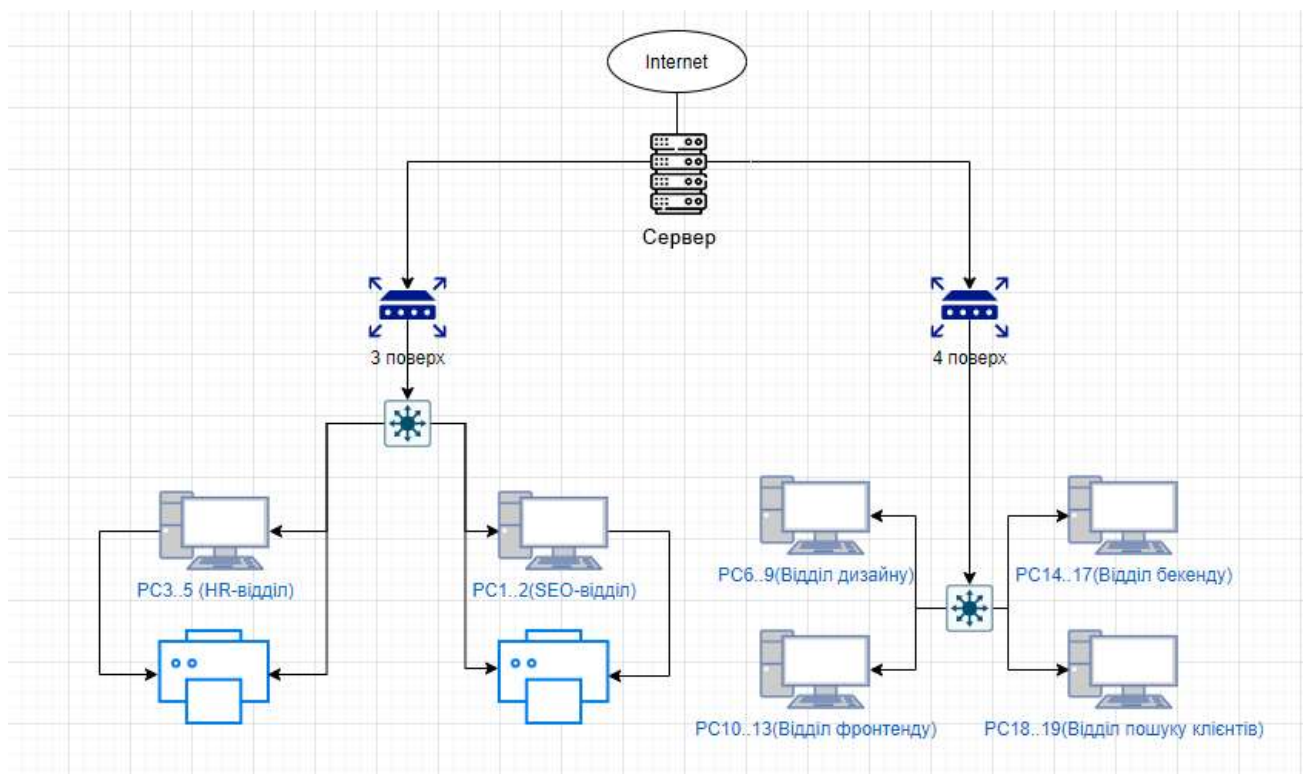


Рисунок 2.2 — Схема інформаційної системи підприємства

2.3 Обстеження об'єкту інформаційної діяльності

Приміщення компанії, є об'єктом інформаційної діяльності (ОІД), що досліджується в кваліфікаційній роботі. Об'єкт інформаційної діяльності розташований на 3-4 поверсі.

Контрольована зона (далі КЗ) обмежена зовнішніми стінами будівлі з усіх сторін, знизу - підлогою, під якою розташовані інші офіси та магазини, а зверху - стелею.

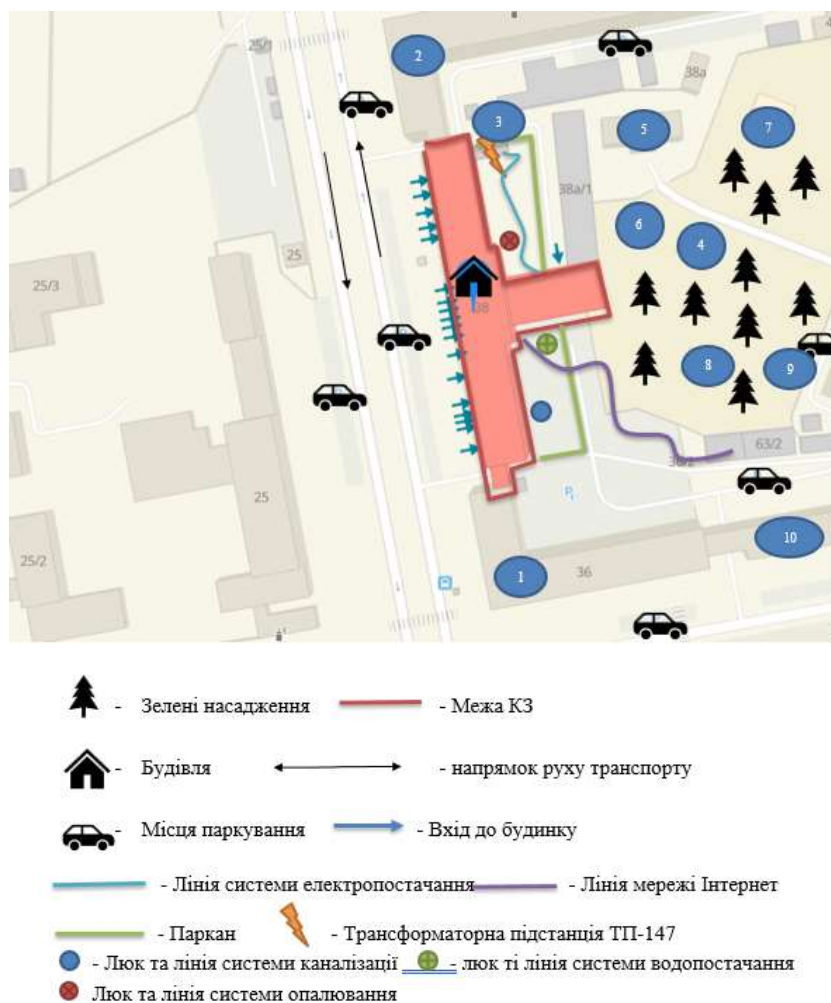


Рисунок 2.3 — Схема ситуаційного плану ОІД

Стіни будинку зроблені із цеглини з залізобетонним перекриттям.

Територія позаду будинку огорожена невисоким парканом із шлагбаумом, асфальтована, деякі ділянки зроблені бруківкою, є місця для

паркування авто для резидентів, платні та безкоштовні, які вказані на Рисунку 2.3

До даного будинку підключені наступні комунікації:

- електропостачання - від трансформаторної підстанції через підземні комунікації до розподільного щитка, який розташований на стіні всередині будинку біля кімнати охорони;
- каналізація та водопостачання - підключені до міських магістралей та заходять до підвального приміщення даного будинку;
- система опалення - централізована, труби стояку йдуть з 0 поверху до приміщень на 1 поверсі, а потім до офісів вище.

Заземлення іде від трансформаторної підстанції до розподільного щита. Безпосередньо в офісі заземлення немає.

Таблиця 2.3 – Характеристика будівель та споруд

№	Найменування	К-ть поверхів	Відстань до ОІД, м
1	Кобзар	6	18
2	Житловий будинок	4	21
3	Трансформаторна підстанція ТП-147	1	5
4	Житловий будинок	2	5
5	Житловий будинок	5	20
6	Житловий будинок	7	25
7	Житловий будинок	7	20
8	Житловий будинок	7	21
9	Житловий будинок	6	29
10	Житловий будинок	4	30

КЗ розташована в офісному будинку, комунікації, а саме труби системи опалення, лінія електропостачання та лінія комп'ютерної мережі виходять за межі КЗ. Інформація про навколишні будинки та споруди приведена у Таблиці 2.4.

Таблиця 2.4 - Прилеглі вулиці відносно ОІД

Назва	Опис
Вулиця 1	Відносно ОІД вулиця розташована на заході. Автомобільний трафік становить 150 - 230 машин на годину.
Вулиця 2	Відносно ОІД вулиця розташована на сході. Автомобільний трафік становить 20 - 50 машин на годину.
Вулиця 3	Відносно ОІД вулиця розташована на півдні. Автомобільний трафік становить 100 - 180 машин на годину.

Опис генерального плану:

- площа ОІД: 89м²;
- висота стелі — 3м. Поверх — 3-ій;
- стеля (матеріал бетон, товщина — 0,5м.), підлога (матеріал бетон+ламінат, товщина 1м.), стіни (матеріал цегла + гіпсокартон, товщина 0,6м);
- вікно (кількість — 12 шт, матеріал пластик (полівінілхлорид або ПВХ)), розміри: 3м х 1,5м. Вікна виходять на двір. Сектор прямої видимості — це ближні жилі будинки та проспект;
- лінія електропостачання іде до поверхового щитка ЩО-1, а звідти — до основного електрощита;
- сигналізація підключена ПКП біля КПП;
- лінія комп'ютерної мережі — оптичний кабель: Wi-Fi роутер підключений до мережевого обладнання провайдеру;
- система опалення — горизонтальна.



Рисунок 2.4 — Генеральний план (3 поверх)

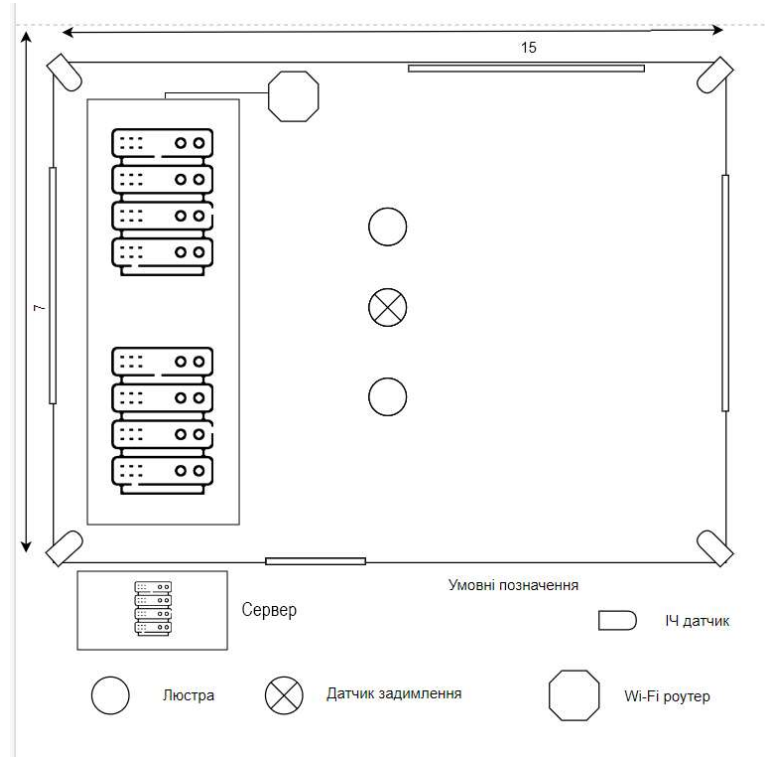
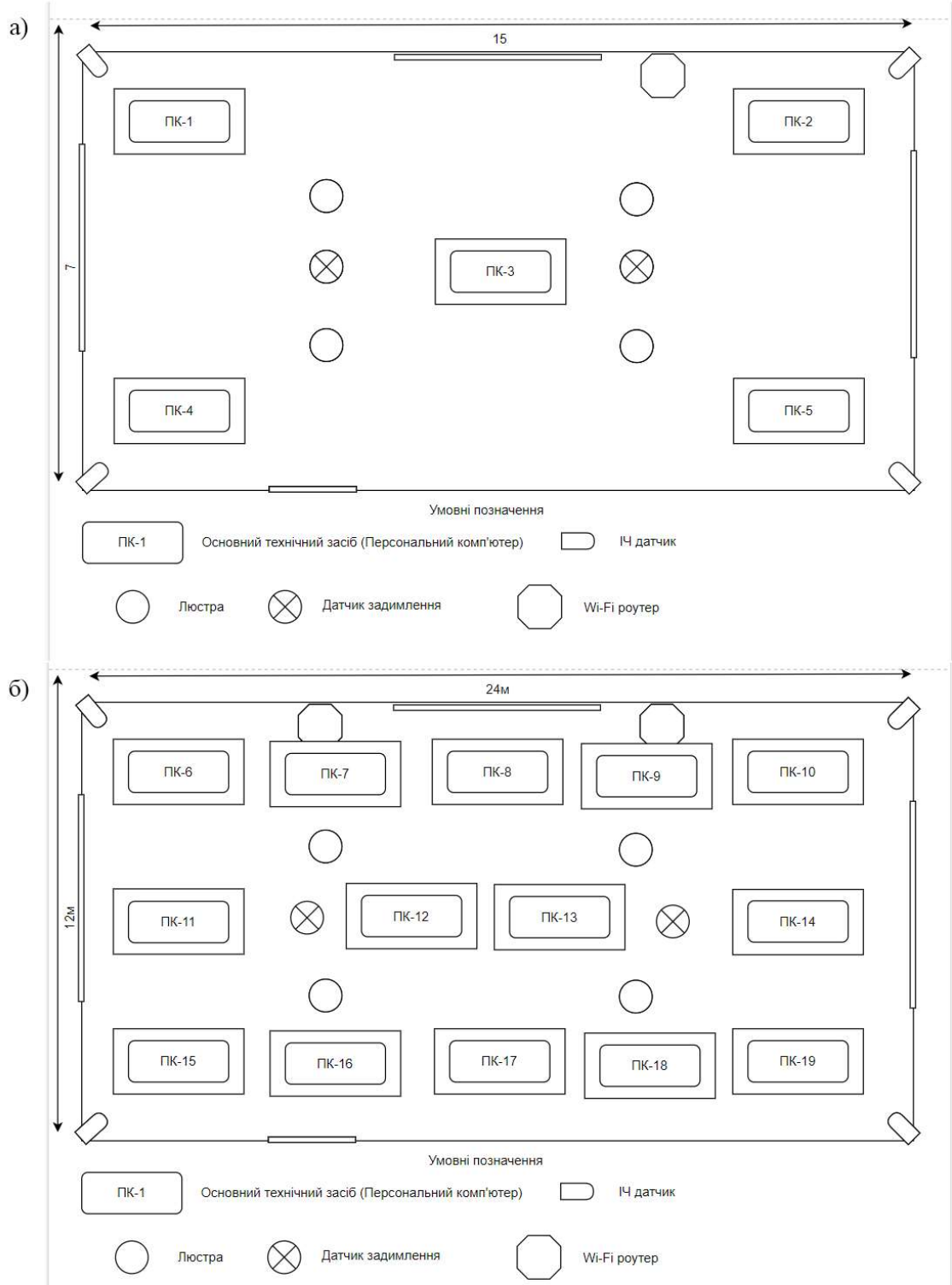


Рисунок 2.5 — Серверне приміщення



а) офіс на 3 поверсі, б) офіс на 5 поверсі

Рисунок 2.6 — Генеральний план

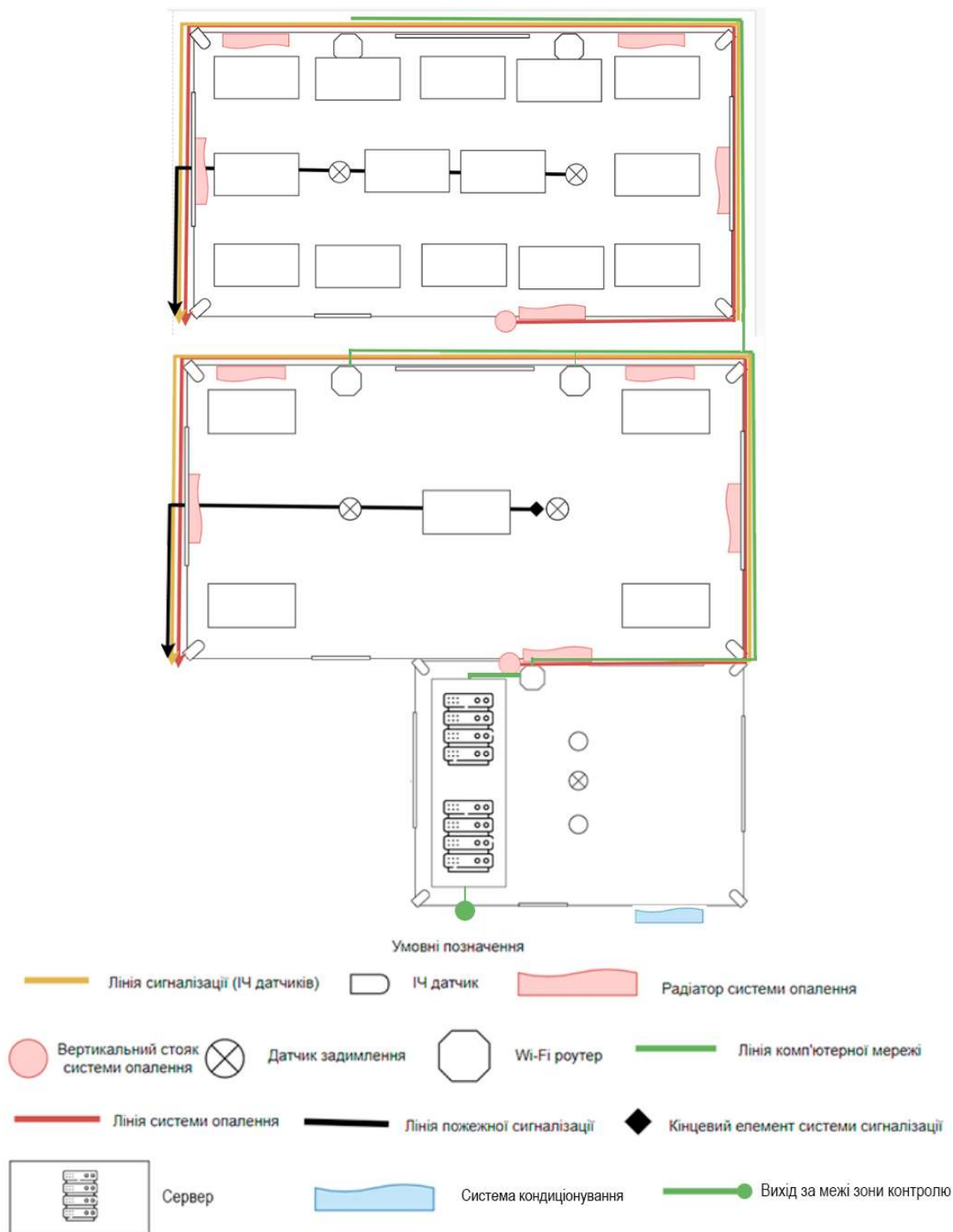


Рисунок 2.7 — Генеральний план. Схеми ліній комп'ютерної мережі, системи сигналізації та системи опалення

Режим КЗ забезпечується таким чином:

- у робочий час забезпечується співробітниками охоронної організації та системою контролю управління доступом. Чергові знаходяться біля контрольно-пропускного пункту, біля входу у будівлю;
- у неробочий час забезпечується силами охорони з використанням засобів відеоспостереження, решіток на вікнах, вхідними металопластиковими дверями, які закриваються на ключ. Також застосовується автономна сигналізація приміщень всього будинку, яка підключена до приймально-контрольного пристрою, який знаходиться біля чергових ПКП. Чергові мають тривожну кнопку, яка застосовується для виклику наряду представників охоронної організації. Сигналізація КЗ входить до складу системи сигналізації усієї будівлі.

Комунікаційні системи КЗ вказані у Таблиці 2.5. Вони також відображені на генеральному плані (Рисунки 2.4-2.7).

Таблиця 2.5 - Комунікаційні системи

Вид комунікації	Характеристика
Система електропостачання	від трансформаторної підстанції через підземні комунікації до розподільного щитка, який розташований на стіні всередині будинку біля входу до приміщення.
Система опалення	Централізована, труби стояку йдуть з 0 поверху до КЗ, а потім до офісів вище.
Система каналізації	Підключені до міських магістралей та заходять до підвального приміщення даного будинку
Система водопостачання	
Телефонна лінія та Інтернет	Підключені до Інтернет-провайдера «Київстар». Кабель локальної мережі являє собою неекранована вита пара (1000BASE-T) категорії 5e
Система сигналізації	Складається з датчиків руху (пасивні інфрачервоні), датчиків диму, система відеоспостереження, пропускні електронні пункти. Адмініструється службою безпеки власника будівлі.

2.4 Аналіз загроз та вразливостей

На цьому етапі проводиться аналіз моделі ризику, тобто будується модель загрози та модель порушника, припускаючи можливі наслідки реалізації загрози. Він також визначає перелік ключових загроз, на які спрямований ССІР.

Цей етап базується на нормативному документі ДСТУ ISO/IEC 27005: 2015 – Впровадження інформаційних технологій. спосіб захисту. Управління ризиками інформаційної безпеки з урахуванням специфіки підприємства.

Аналіз загроз і вразливостей включає наступні етапи:

- модель порушника;
- модель загроз;
- оцінка ризиків і їх наслідків.

2.5 Модель порушника

Зовнішні порушення включають людей за межами бізнесу. Це можуть бути конкуруючі компанії та крадіжки, які супроводжують або, люди, які не мають доступу до ISD, але мають доступ до приміщень, де розташовані компоненти ІТС, і можуть використовувати ISD, наприклад, прибиральники, електрики тощо.

Внутрішні правопорушники включають тих, хто фізично підключений до каналів зв'язку або інших компонентів мережі передачі даних, користувачів АУ та тих, хто безпосередньо залучений до операцій ІТС.

У таблиці 2.6 наведено категорії правопорушників, використані для створення моделі. Модель злочинця дає специфікації для різних показників:

- за мотивами здійснення порушень;
- за рівнем кваліфікації та обізнаності щодо ІТС;
- за показником можливостей використання засобів ІТС для реалізації загроз;
- за часом та місцем дії.

Профіль порушника визначає сукупність цих характеристик.

Таблиця 2.6 – категорії порушників

Рейтингова оцінка	Опис
0	Не становить загрози
1	Незначний
2	Низький
3	Середній
4	Високий

За результатами аналізу характеристик оброблюваної інформації категорії порушників, які мають потенціал для порушення конфіденційності та цілісності інформації, вважаються найбільш небезпечними.

Таблиця 2.7 - Категорії порушників. Внутрішні по відношенню до ІТС.

Позначення	Визначення категорії	Рівень загроз
ПВО	Директор	0
ПВ1	HR-менеджер	2
ПВ2	Розробник	3
ПВ3	Тімліди	4

Таблиця 2.8 - Категорії порушників. Зовнішні по відношенню до ІТС

Позначення	Визначення категорії	Рівень загроз
ПЗ0	Кандидати на вакансію	1
ПЗ1	Комунальні служби, служби з питань благоустрою	1
ПЗ2	Вахтери, сантехнік, електрик, прибиральниці	1

Таблиця 2.9 - Специфікація моделі порушника за мотивами здійснення порушень

Позначення	Мотив порушення	Рівень загроз
M1	Халатність, некваліфікованість	1
M2	Самоствердження	1
M3	Корисний інтерес	1

Таблиця 2.10 - Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІТС

Позначення	Рівень кваліфікації	Рівень загроз
K1	Низький рівень знань, вміння працювати з компонентами ІТС	1
K2	Середній рівень знань, має практичний досвід з роботи з компонентами ІТС та їх обслуговування	2

Таблиця 2.11 - Специфікація моделі порушника за показником можливостей

Позначення	Характеристика можливостей порушника	Рівень загроз
30	Не має навичок	0
31	Підглядання за робочим процесом	1
32	Взлом, підбір паролю до облікових записів	2

Таблиця 2.12 – Специфікація моделі порушника за часом дії

Позначення	Час дії	Рівень загроз
Ч1	Під час призупинення використання компонентами ІТС	2
Ч2	Під час ремонту компонентів ІТС	1
Ч3	Під час роботи компонентів ІТС	1
Ч4	У будь-який час, маючи доступ до інформації у хмарному сховищі (до обл. зап.)	2

Таблиця 2.13

Специфікація моделі порушника за місцем дії

Позначення	Час дії	Рівень загроз
МД1	Робочі місця робітників	2
МД2	У приміщенні, де розташовані ІТС	2
МД3	У будь-якому місці, маючи доступ до інформації у хмарному сховищі	2

Профілі порушників всіх категорій наведено у таблиці 2.14, у колонці «Сума загроз» наведено рейтингову оцінку загроз порушника з відповідними характеристиками.

Таблиця 2.14 - Профілі порушників

Посада	Кат. пор.	Мотив поруш.	Можл ивості	Рів.обіз. ІТС	Час	Місце	Сума загроз
Директор	ПВ0	МІ	30	К2	ЧЗ	МД1	6
	0	1	0	2	1	2	
HR-менеджер	ПВ1	МІ	31	К2	ЧЗ	МД1	8
	1	1	1	2	1	2	
Розробники	ПВ2	МІ	32	К2	ЧЗ	МД1	11
	3	1	2	2	1	2	
Тімліди	ПВ3	МІ	32	К2	ЧЗ	МД1	12
	4	1	2	2	1	2	
Відвідувачі	ПЗ0	МЗ	31	К1	Ч1	МД2	8
	2	1	1	1	1	2	
Комунальні служби	ПЗ1	МЗ	31	К1	ЧЗ	МД2	7
	1	1	1	1	1	2	
прибиральниці, сантехник, електрик, вахтери	ПЗ2	МЗ	31	К1	ЧЗ	МД2	7
	1	1	1	1	1	2	

Найбільшу загрозу представляють внутрішні робітники організації, а саме HR-менеджери, розробники та тімліди, оскільки вони мають безпосередній доступ до системи ІТС та працюють з її компонентами, та мають достатню компетенцію і мотиви.

3 РОЗРОБКА СИСТЕМИ ЗАХИСТУ

3.1 Встановлення фізичного захисту

Поглянемо на загальну схему серверного приміщення із встановленою системою захисту (рисунок 3.1)

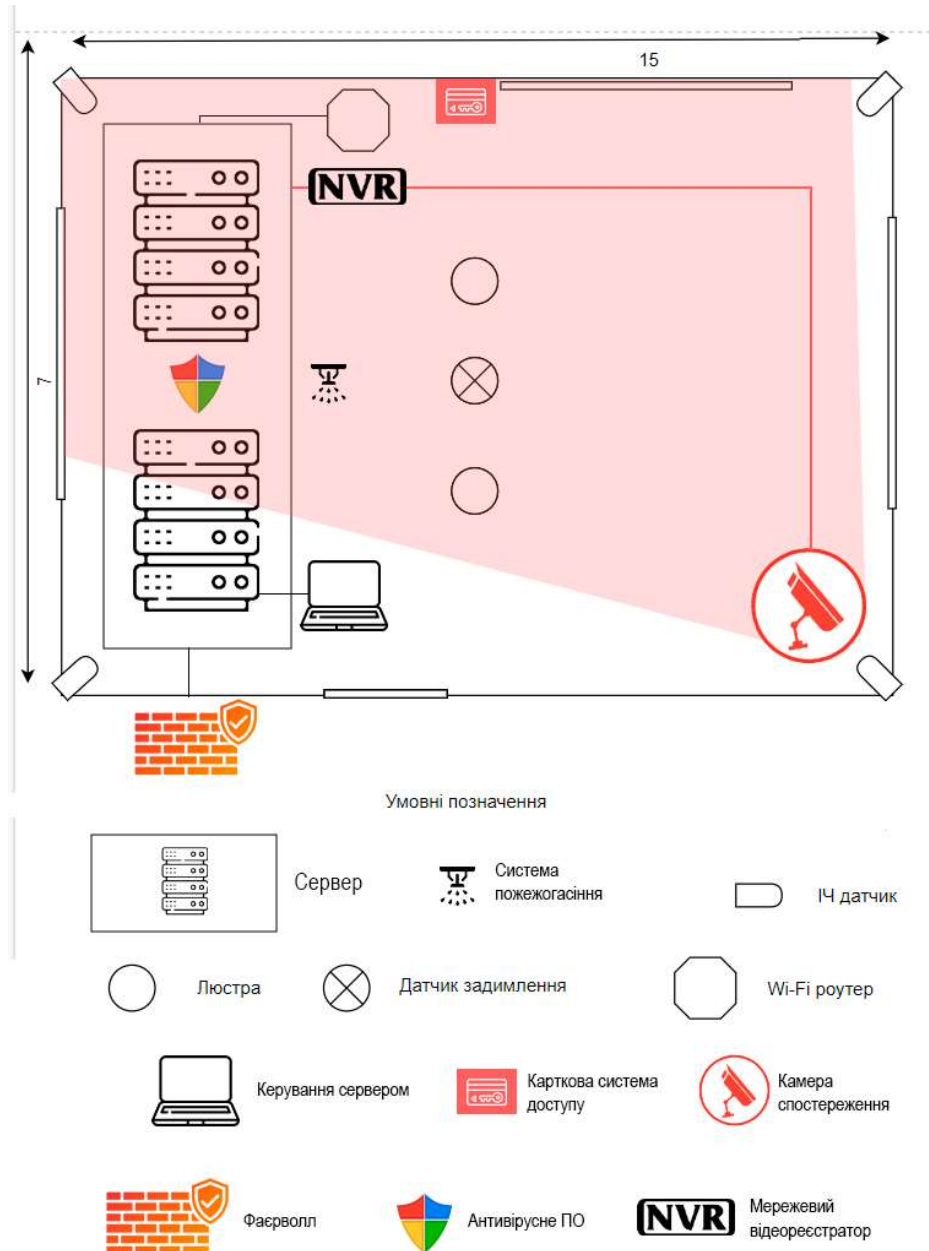


Рисунок 3.1 – план системи захисту серверного приміщення

Перше, що потрібно виконати – це встановити системи контролю доступу. Це один з основних способів забезпечення фізичного захисту серверного приміщення. Системи контролю доступу включає в себе карткову систему. Використання різних видів систем контролю доступу забезпечує більш повний і надійний захист від несанкціонованого доступу.

Для контролю доступу необхідно визначити перелік осіб, яким дозволено вхід в серверне приміщення. Це дозволить знизити ризик доступу до обладнання людей, які не мають відповідних дозволів або знань.

Щоб контролювати та слідкувати за активністю в серверному приміщенні, рекомендується вести журнал входу та виходу. Якщо вхід та вихід не контролюється автоматичною системою, такий журнал допоможе встановити, хто і коли входив та виходив з приміщення.

Разом із цим система відеоспостереження є важливою частиною забезпечення фізичного захисту серверного приміщення. Вони дозволяють моніторити діяльність всередині та навколо приміщення, що може допомогти виявити і запобігти несанкціонованому доступу. Розташування камери відображено на рисунку 3.1.

Для забезпечення ефективної роботи систем відеоспостереження необхідно регулярно перевіряти та обслуговувати відеокамери. Це може включати перевірку якості зображення, правильної роботи всіх функцій камери, а також її фізичного стану.

Забезпечення належного зберігання та шифрування з камер є важливим аспектом управління відеоспостереженням. Це не тільки допомагає захистити конфіденційність інформації, але і гарантує, що записи не можуть бути змінені або видалені без належного дозволу.

Систему відеонагляду включає в себе камеру, мережевий відеореєстратор (NVR) та власне сервер із системою зберігання даних. Камери передають дані через Ethernet до NVR, після обробки яким (саме на ньому відбувається шифрування даних), матеріал потрапляє на сховище до серверу.

Сервер зберігає відео на RAID-масиві із жорстких дисків, щоб забезпечити надійність зберігання.

Для забезпечення фізичного захисту одну із ключових ролей грає встановлення датчиків диму в серверному приміщенні - це критично важливий елемент протипожежної безпеки. В серверному приміщенні встановлено автоматичні системи гасіння пожежі (рисунок 3.1). Ці системи миттєво активуються при виявленні пожежі і здатні швидко і ефективно припинити розповсюдження вогню без шкоди для обладнання.

Не менш важливо регулярно перевіряти систему протипожежного захисту на належну роботу. Це може включати тестування датчиків диму та температури, перевірку газових систем гасіння пожежі, а також перевірку регулярного обслуговування та підтримки цих систем.

Для забезпечення оптимальних умов для роботи серверного обладнання потрібно встановити систему кондиціонування та вентиляції, спеціально адаптовані для серверних приміщень. Ці системи допомагають підтримувати стабільну температуру та вологість, які є критично важливими для довготривалої і надійної роботи серверів. Регулювання температури та вологості відповідно до технічних вимог обладнання важливо для забезпечення його надійної роботи. Занадто висока температура може призвести до перегріву і виходу обладнання з ладу, в той час як висока вологість може призвести до корозії та інших проблем.

Необхідно проводити періодичні перевірки та обслуговування систем кондиціонування та вентиляції, щоб вони працювали ефективно і надійно. Це включає в себе перевірку фільтрів, вентиляторів, компресорів та інших компонентів на предмет зносу, пошкодження або неправильної роботи. Час від часу можуть знадобитися професійне обслуговування або ремонт.

Таким чином, виконання цих заходів забезпечить надійний фізичний захист серверного приміщення і гарантує безперебійну роботу серверу.

3.2 Мережевий захист

Найпростіший спосіб забезпечити захист даних в мережі – це шифрування даних. Воно забезпечує конфіденційність та цілісність переданих даних, захищаючи інформацію від несанкціонованого доступу та зловживання. Використання таких протоколів безпеки, як SSL (Secure Sockets Layer), TLS (Transport Layer Security) або IPSec (Internet Protocol Security), дозволяє шифрувати мережевий трафік на різних рівнях мережевої моделі OSI. Ці протоколи забезпечують також аутентифікацію сторін, участь у якій вони беруть, та забезпечують інтегральність переданих даних. Найпростішим та досить надійним методом стане використання алгоритму RSA для захисту даних.

RSA (Rivest-Shamir-Adleman) – це криптосистема з відкритим ключем, яка використовується для шифрування і цифрового підпису даних. Це одна з найбільш широко використовуваних криптосистем і вона є основою для багатьох протоколів безпеки в Інтернеті, таких як SSL і TLS.

Алгоритм RSA включає наступні дії:

- генерація ключів, яка включає вибір двох великих простих чисел p і q , а потім обчислення їх добутку $n = p * q$. Цей добуток n використовується як модуль для обох ключів – відкритого та закритого. Обчислюється функція Ейлера $\varphi(n) = (p-1) * (q-1)$. Вибирається ціле число e таке, що $1 < e < \varphi(n)$ і e та $\varphi(n)$ є взаємно простими числами (тобто їх найбільший спільний дільник дорівнює 1). Це число e стане частиною відкритого ключа. Обчислюється число d таке, що $(d * e) \% \varphi(n) = 1$. Це число d стане частиною закритого ключа. Відкритий ключ RSA складається з пари чисел (e, n) , а закритий ключ – з пари (d, n) ;
- шифрування повідомлення M (даних), для якого використовується відкритий ключ. Повідомлення перетворюється в числове представлення m

(для цього можна використати багато різних методів). Потім обчислюється шифртекст c за формулою $c = m^e \bmod n$;

– для дешифрування шифртексту c використовується закритий ключ. Обчислюється оригінальне повідомлення m за формулою $m = c^d \bmod n$.

RSA є дуже безпечним виключно завдяки труднощам розкладання великих чисел на прості множники.

Також для записту мережевого захисту необхідне використання файрволів та систем виявлення вторгнень. Файрволи є важливим компонентом мережевої безпеки. Файрволи використовуються для контролю мережевого трафіку, що проходить через них, за допомогою встановлення визначених правил безпеки. Особливо він потрібен для фільтрації вхідних та вихідних даних за межами контрольованої зони. Ці правила можуть бути налаштовані на основі типу протоколу, IP-адреси, портів та інших параметрів.

В основі файрволів лежать такі принципи:

- базовий фільтр пакетів: фільтрує пакети на основі заголовків IP, портів, протоколу тощо;
- фільтрація на рівні додатку: визначає, які види мережевого трафіку можуть проходити через файрвол на основі конкретних додатків або служб;
- файрволи зі станом: вони відстежують активні мережеві з'єднання та фільтрують пакети на основі стану з'єднання;
- файрволи також можуть включати додаткові функції, такі як VPN для захищеного з'єднання мережі та IPS (система запобігання вторгненням), що надає додатковий рівень захисту.

Системи виявлення вторгнень (IDS) працюють, аналізуючи мережевий трафік та виявляючи активність, яка відповідає відомим шаблонам зловмисного поведіння, або є ненормальною. Існують два основних типи IDS:

- системи виявлення вторгнень на основі сигнатур (Signature-Based IDS): ці системи працюють, порівнюючи мережевий трафік з відомими шаблонами або «сигнатурами» зловмисних дій;
- системи виявлення вторгнень на основі аномалій (Anomaly-Based IDS): вони використовують машинне навчання та статистичний аналіз для встановлення «нормального» поведінки мережі та виявлення відхилень від цієї норми;
- обидві системи мають свої переваги та недоліки: системи на основі сигнатур добре виявляють відомі загрози, але можуть пропустити нові або невідомі атаки. Системи на основі аномалій можуть виявити нові атаки, але мають більш високий рівень помилкових сигналів.

Всі ці інструменти, коли вони правильно налаштовані та використовуються разом, можуть становити міцну оборону від різноманітних мережевих загроз.

Політики обмеження доступу мають на меті забезпечити контроль над тим, хто має доступ до мережі і серверів, а також над тим, що вони можуть робити з наявними ресурсами. Вони можуть включати аутентифікацію користувача, контроль доступу на основі ролей (Role-Based Access Control, RBAC) та атрибутний контроль доступу (Attribute-Based Access Control, ABAC).

Аутентифікація користувачів є першим кроком в системі обмеження доступу. Вона забезпечує перевірку ідентичності користувача, що намагається отримати доступ до системи.

Аутентифікація може включати:

- пароль або PIN-код;
- мобільний телефон або інший фізичний токен;
- біометричні дані, такі як відбитки пальців або сканування сітківки ока.

Найдешевшою та досить надійною системою є саме парольний доступ, який і було обрано в якості ідентифікатора користувача.

Контроль доступу на основі ролей (RBAC). RBAC є моделлю обмеження доступу, в якій права та обов'язки присвоюються користувачам на основі їх ролі в системі. Це означає, що дозволи контролюються на рівні групи, а не на рівні окремого користувача, що спрощує управління правами доступу в більших системах.

Атрибутний контроль доступу (ABAC). ABAC є більш гнучкою моделлю обмеження доступу, в якій права доступу можуть бути налаштовані на основі багатьох різних атрибутів, включаючи атрибути користувача, атрибути ресурсу, атрибути дій та атрибути середовища. Наприклад, правила можуть бути налаштовані таким чином, що користувач може отримати доступ до певного ресурсу лише під час робочих годин та лише з певної мережі.

Принцип мінімальних привілеїв. Принцип мінімальних привілеїв, також відомий як принцип найменшого привілею, означає, що користувачам та системам надаються лише ті права доступу, які їм безпосередньо потрібні для виконання їх роботи. Це зменшує ризик, що якщо обліковий запис користувача буде скомпрометовано, зловмисник зможе використати його для отримання широкого доступу до системи.

Узагальнено, всі ці політики обмеження доступу допомагають забезпечити, що тільки авторизовані користувачі мають доступ до ваших серверів та мережі, і що вони можуть виконувати лише ті дії, до яких у них є дозвіл.

3.3 Програмний захист

Цей пункт описує основні механізми, які сприяють захисту від шкідливого програмного забезпечення, а також політики та процедури, які допомагають забезпечити цей захист.

Для забезпечення оптимального захисту від потенційних загроз, необхідно систематично оновлювати всі встановлені програми та операційні системи. Це означає, що повинні бути встановлені всі доступні оновлення та патчі безпеки, які випускаються розробниками. Ці патчі зазвичай містять виправлення помилок, зміни для поліпшення стабільності та, що найважливіше, усунення вразливостей, що можуть бути використані зловмисниками для атаки на систему.

Антивірусне програмне забезпечення є одним з ключових інструментів для захисту комп'ютерної системи від різноманітних цифрових загроз. Його основна функція – виявлення, блокування та видалення шкідливого програмного забезпечення, що може включати віруси, троянські програми, шпигунське ПЗ, рекламне ПЗ та інше.

Встановлення антивірусного ПЗ має сенс лише в тому випадку, якщо воно регулярно оновлюється. Оновлення антивірусного ПЗ включають нові вірусні сигнатури, що дозволяє йому виявляти та боротися з найновішими загрозами. Вірусні сигнатури - це унікальні характеристики шкідливого програмного забезпечення, які дозволяють антивірусному ПЗ впізнавати та боротися з шкідливим кодом.

Більшість антивірусних програм пропонує автоматичні оновлення, що можуть бути налаштовані так, щоб вони виконувались регулярно без потреби вручну перевіряти наявність нових оновлень. Регулярні оновлення гарантують, що система захищена від найновіших відомих загроз.

Нарешті, важливо відмітити, що антивірусне ПЗ має бути лише частиною більш загальної стратегії безпеки, яка також має включати видалення невикористовуваного програмного забезпечення, регулярне оновлення всіх програм та систем, використання складних паролів та двофакторної автентифікації.

Контроль доступу є сукупністю процесів, політик і технологій, які забезпечують захист даних та ресурсів комп'ютерної системи від несанкціонованого доступу. Цей контроль допомагає забезпечити

конфіденційність, цілісність і доступність інформації, а також запобігти можливим загрозам, таким як злам, витік даних або зловживання правами доступу.

Політики контролю доступу визначають права доступу до конкретних ресурсів і системних функцій. Це означає, що організація визначає, які користувачі мають доступ до певних даних, програм або інших ресурсів, і які дії вони можуть виконувати з цими ресурсами. Політики контролю доступу можуть базуватися на ролях користувачів, типах даних, групах користувачів або контексті використання.

Першим кроком у встановленні ефективного контролю доступу є аналіз потреб організації. Це означає визначення, які ресурси потрібно захищати, хто повинен мати доступ до цих ресурсів і які дії можуть бути виконані з цим доступом. Наприклад, в банку можуть бути різні рівні доступу для клієнтів, працівників, адміністраторів системи та керівників.

Після визначення потреб організації, розробляються політики контролю доступу. Це документи, які описують правила і обмеження для доступу до ресурсів. Політики можуть включати такі елементи, як призначення ролей, принципи надання дозволів, правила аутентифікації та авторизації, аудит доступу і процедури управління ідентифікацією.

Після розробки політик контролю доступу, їх необхідно застосувати на рівні операційної системи або програмного забезпечення. Це означає, що правила та обмеження, встановлені в політиках, повинні бути впроваджені в систему і забезпечуватися їх строге дотримання. Наприклад, операційна система може мати механізми аутентифікації, які перевіряють ідентифікацію користувача перед наданням доступу, а також механізми авторизації, які перевіряють права доступу користувача до ресурсів.

Ефективний контроль доступу включає також процес моніторингу та аудиту. Це дозволяє відстежувати дії користувачів і перевіряти, чи дотримуються політики контролю доступу. Журнали аудиту дозволяють виявляти потенційні загрози та викриті порушення безпеки, а також

допомагають виконати розслідування випадків несанкціонованого доступу або витоку даних.

Узагалі, ефективний контроль доступу є ключовим аспектом безпеки комп'ютерних систем і даних. Він допомагає забезпечити, що тільки авторизовані користувачі мають доступ до ресурсів і виконують дії, які відповідають їх ролям і правам. Правильно розроблені політики контролю доступу і їх впровадження на рівні операційної системи допомагають зменшити ризики несанкціонованого доступу, зламу і витоку даних.

3.4 Адміністративний захист

Для розподілення адміністративного захисту серверного приміщення використовується принцип найменшого привілею та принцип розділення обов'язків. Основною метою такого захисту є забезпечення безпеки фізичного доступу до серверного приміщення та контроль за ним.

Директор (Адміністратор):

- має повний контроль над серверним приміщенням та його ресурсами;
- забезпечує встановлення та дотримання політик безпеки;
- відповідає за надання доступу до серверного приміщення відповідним співробітникам;
- має повний доступ до всіх системних налаштувань і конфіденційних даних.

Заступник директора та директор HR-відділу (Користувачі):

- мають обмежений доступ до серверного приміщення для виконання своїх обов'язків;
- відповідають за адміністрування та управління користувачами в межах своєї відповідальності;

- не мають повного контролю над сервером і обмежені в правах доступу до критичних системних компонентів.

HR-менеджер, Тімлід, Розробники та Акаунт-менеджери (Користувачі):

- мають доступ до серверного приміщення в обмеженому режимі, що відповідає їх ролям та обов'язкам;

- забезпечують доступ до серверних ресурсів, необхідних для виконання своїх професійних завдань;

- мають обмежені права доступу до системних компонентів і конфіденційних даних, що не стосуються їх роботи.

Прибиральниця:

- не має доступу до серверного приміщення або комп'ютерних систем;

- її виключна відповідальність полягає в забезпеченні чистоти та порядку у приміщенні, включаючи зону серверів.

Для забезпечення адміністративного захисту серверного приміщення також можуть бути застосовані наступні заходи:

- встановлення системи контролю доступу, такої як електронний ключ або карта доступу, для обмеження фізичного доступу лише до авторизованих співробітників;

- встановлення відеоспостереження для контролю за входом та перебуванням у приміщенні;

- використання біометричних систем ідентифікації (наприклад, сканерів відбитків пальців) для забезпечення ще більшої безпеки доступу;

- проведення регулярних навчань і нагляду за співробітниками, щоб вони дотримувалися процедур безпеки та не розголошували конфіденційну інформацію;

- важливо забезпечити, щоб доступ до серверного приміщення та систем був розподілений за необхідністю, а обов'язки та права кожного співробітника відповідали його ролі та потребам організації.

ВИСНОВКИ

Встановлення фізичного захисту серверного приміщення є необхідною складовою для забезпечення безпеки і надійності інформаційних систем режимного підприємства. Всі ці заходи сприяють зменшенню ризиків несанкціонованого доступу до серверного приміщення і збереженню цілісності і конфіденційності інформації.

Мережевий захист є ключовим аспектом безпеки серверного приміщення. В ході дослідження було досліджено різні методи і технології, такі як мережеві брандмауери, системи виявлення вторгнень (IDS).

Програмний захист є необхідною складовою для забезпечення безпеки серверного приміщення. Ці заходи дозволяють ефективно захищати серверне приміщення від шкідливого програмного забезпечення і неправомірного доступу.

Адміністративний захист є важливою складовою безпеки серверного приміщення. В ході дослідження було досліджено різні аспекти адміністративного захисту, такі як регулярні навчання персоналу, створення політики безпеки, регулярні аудити і відстеження подій. Впровадження цих заходів дозволяє підтримувати високий рівень безпеки і забезпечувати відповідність інформаційних систем режимного підприємства вимогам нормативних актів і стандартів.

В результаті проведеної роботи було створено належний фізичний, мережевий, програмний і адміністративний захист серверного приміщення режимного підприємства для забезпечення безпеки і надійності інформаційних систем. Впровадження цих заходів дозволить попередити несанкціонований доступ до серверного приміщення, зберегти цілісність і конфіденційність інформації та забезпечити відповідність вимогам нормативних актів і стандартів у сфері інформаційної безпеки.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” від 05.07.1994 №80-VI // Відомості Верховної Ради України. -
2. Статистика кібератак на малі підприємства за 2021 рік [Електронний ресурс]. - Режим доступу <https://www.fundera.com/resources/small-business-cyber-security-statistics#>
3. Інформація щодо ІТ компаній, які ведуть бізнес на території України [Електронний ресурс]. - Режим доступу <https://jobs.dou.ua/ratings/>
4. Закон України «Про інформацію» від 02.10.1992 № 2657-XII // Відомості Верховної Ради України. - 1992. - № 48. [Електронний ресурс]. - Режим доступу <https://zakon.rada.gov.ua/laws/show/2657-12>
Класифікація “інформації в законодавстві України”.
5. Закон України “Про захист персональних даних” від 01.06.2010 № 2297-VI// Відомості Верховної Ради України. - 2010. - № 5. [Електронний ресурс]. - Режим доступу <https://zakon.rada.gov.ua/laws/show/2297-17>.
6. Закон України “Про доступ до публічної інформації” від 13.01.2011 № 2939- VI // Відомості Верховної Ради України. - 2011. - № 32. [Електронний ресурс]. - Режим доступу <https://zakon.rada.gov.ua/laws/show/2939-17>.
7. Статистика кібератак на підприємства [Електронний ресурс]. - Режим доступу <https://techexpert.ua/cyber-attacks-number-statistics/>
8. 1994. - № 80. [Електронний ресурс]. - Режим доступу <http://zakon4.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80>
9. ДСТУ ISO/IEC 27002:2015 [Електронний ресурс] // ДСТУ. - 2015. - Режим доступу до ресурсу: <http://online.budstandart.com/ua/catalog/doc-page.html?id doc=66911>.

10. ДСТУ ISO/IEC 27005:2017 [Електронний ресурс] // ДСТУ. - 2017.
- Режим доступу до ресурсу: <http://online.budstandart.com/ua/catalog/doc-page.html?id doc=66912>.
11. НД ТЗІ 3.7-003 - Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно - телекомунікаційній системі. - [Чинний від 08.11.2005] - К. ДССЗІ, 2005. - №125 - (Нормативний документ системи технічного захисту інформації).
12. НД ТЗІ 1.4-001 - Типове положення про службу захисту інформації в автоматизованій системі. - [Чинний від 04.12.2000] - К. : ДСТСЗІ СБУ, 2000.
- №53 - (Нормативний документ системи технічного захисту інформації).
13. НД ТЗІ 2.5-004 - Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. - [Чинний від 28.04.1999] - К. ДСТСЗІ СБУ, 1999. - №22 - (Нормативний документ системи технічного захисту інформації).
14. НД ТЗІ 2.5-005 - Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. - [Чинний від 28.04.2000] - К. : ДСТСЗІ СБУ, 2000.
- №22- (Нормативний документ системи технічного захисту інформації).
15. НД ТЗІ 1.6-005 - Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці. - [Чинний від 15.04.2013] - К. : ДССЗІ, 2013. - №125 - (Нормативний документ системи технічного захисту інформації).
16. Етапи створення КСЗІ [Електронний ресурс] -
Режим доступу до ресурсу: <http://www.vaas.gov.ua/news/zaxist-informacijnix-sistem-vazhlive-zavdannya-sogodennya/>.
17. Методичні вказівки до виконання економічної частини дипломного проекту зі спеціальності 125 Кібербезпека/Упоряд. Д. П. Пілова.

Дніпро: Національний технічний університет «Дніпровська політехніка», 2019.

18. Методичні рекомендації до виконання дипломних робіт (проектів) бакалаврів та магістрів спеціальностей 125 Кібербезпека / О.В. Герасіна, Д.С.Тимофеев, О.В. Кручинін, Ю.А.Мілінчук Дніпро: НТУ «ДП», 2020. 47 с.

19. НД ТЗІ 2.5-004 - Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. - [Чинний від 28.04.1999] - К. ДСТСЗІ СБУ, 1999. - №22 - (Нормативний документ системи технічного захисту інформації).

20. НД ТЗІ 2.5-005 - Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. - [Чинний від 28.04.2000] - К. : ДСТСЗІ СБУ, 2000. - №22- (Нормативний документ системи технічного захисту інформації).

21. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.2-004-99. — Київ: ДСТСЗІ СБ України, 1999. — 55 с.

22. Інформація щодо середньої заробітної плати спеціаліста з кібербезпеки. [Електронний ресурс]. - Режим доступу <https://ua.trud.com/ua/salary/2/67683.html>

23. Актуальні ціни на електроенергію [Електронний ресурс]. - Режим доступу <https://yasno.com.ua/b2c-tariffs>

24. Середня заробітна плата спеціаліста з кібербезпеки [Електронний ресурс]. - Режим доступу <https://ua.trud.com/ua/salary/2/67682.html>