

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій
(повне найменування інституту, назва факультету)

Кафедра інформаційної безпеки та наноелектроніки
(повна назва кафедри)

Пояснювальна записка

до дипломного проекту (роботи)

бакалавр

(ступінь вищої освіти)

на тему Система захисту інформації серверного приміщення
режимного підприємства

Виконав: студент 4 курсу, групи БК-810

Спеціальності 125 Кібербезпека

(код і назва напрямку підготовки, спеціальності)

Освітня програма (спеціалізація)

Безпека інформаційних та комунікаційних
систем

КРИВОШЕЄВ Д.М.

(ПРИЗВИЩЕ та ініціали)

Керівник РОМАНЕНКО С.М.

(ПРИЗВИЩЕ та ініціали)

Рецензент МОРОЗ Г.В.

(ПРИЗВИЩЕ та ініціали)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій
Кафедра інформаційної безпеки та наноелектроніки
Ступінь вищої освіти: бакалавр
Спеціальність 125 Кібербезпека
Освітня програма (спеціалізація) Безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖУЮ
Завідувач кафедри ІБтаН, к.ф-м.н.
_____ Андрій КОРОТУН
“ ____ ” _____ 2024 року

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

КРИВОШЕЄВА Дениса Миколайовича
(ПРИЗВИЩЕ, ім'я, по батькові)

1. Тема проєкту (роботи): Система захисту інформації серверного приміщення режимного підприємства
керівник проєкту (роботи) канд. фіз.-мат. наук, доцент РОМАНЕНКО Сергій Миколайович

(науковий ступінь, вчене звання, ПРИЗВИЩЕ, ім'я, по батькові)

затверджені наказом закладу вищої освіти від « 03 » травня 2024 року № 192

2. Строк подання студентом проєкту (роботи): _____

3. Вихідні дані до проєкту (роботи): розробити систему захисту інформації серверного приміщення режимного підприємства

4.ЗМІСТ розрахунково-пояснювальної записки (перелік питань, що їх потрібно розробити): Теоретичні відомості,
Канали витоку інформації, Концепція Системи захисту інформації,
Види закладних пристроїв та їх пошук, Центр управління безпеки,
Різновид фахівців, Відомості про серверну кімнату,
Завдання до Дипломного Проєкту, Розробка СЗІ серверного приміщення,
Основні відомості про об'єкт в якому знаходиться серверна кімната,
Відомості про приміщення, Програмний захист серверів, Основні рекомендації мінімізування впливу вразливостей

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, кількість слайдів, плакатів): Презентація у програмі Microsoft Power Point (15 слайдів)

6. Консультанти розділів проєкту (роботи)

Розділ	ПРИЗВИЩЕ, ініціали та посада консультанта	Підпис, дата	
		завдання видав	Прийняв виконане завдання
1-3	РОМАНЕНКО С.М., доцент каф. ІБтаН	 03.03.2024	 03.06.2024
нормконтроль	КОРОЛЬКОВ Р.Ю., доцент каф. ІБтаН		07.06.2024

7. Дата видачі завдання « 03 » березня 2024 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1	Ознайомлення з темою та визначення ключових аспектів Дипломного проєкту	1 тиждень	Виконано
2	Аналіз загальної інформації щодо інформації про серверне приміщення.	1 тиждень	Виконано
3	Формулювання та написання вступу.	2 тиждень	Виконано
4	Проектування системи безпеки	3-5 тиждень	Виконано
5	Аналіз отриманих результатів та формування висновків Дипломного проєкту.	5-6 тиждень	Виконано
6	Здача на перевірку та підпис кваліфікаційної роботи керівнику.	6 тиждень	Виконано
7	Проходження перевірки на плагіат та нормоконтроль кваліфікаційної роботи.	6 тиждень	Виконано
8	Допуск завідувачем кафедри до захисту кваліфікаційної роботи.	8 тиждень	
9	Захист кваліфікаційної роботи.	9 тиждень	

Студент(ка)

(підпис)

Денис КРИВОШЕЄВ

(Ім'я ПРИЗВИЩЕ)

Керівник проєкту (роботи)

(підпис)

Сергій РОМАНЕНКО

(Ім'я ПРИЗВИЩЕ)

АНОТАЦІЯ

Пояснювальна записка до дипломної кваліфікаційної роботи бакалавра:

59 с., 14 рис., 16 джерел.

ІНФОРМАЦІЯ, КАНАЛ, КІБЕРІНЦИДЕНТ, КОМАНДИ, ОБ'ЄКТ, ПІДПРИЄМСТВО, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, СЕРВЕР, ЦІЛІСНІСТЬ.

Об'єкт дослідження – серверна кімната режимного підприємства. У ході роботи необхідно проаналізувати канали витоку інформації та мінімізувати їх вплив на приміщення та сервери.

Мета роботи – освоєння теоретичних основ і отримання практичних навичок в області проєктування безпеки обраної кімнати, використовуючи знання, набуті під час навчання.

Дипломний проєкт складається з двох розділів. У першому розглядаються теоретичні відомості та завдання до роботи, в другому - практична реалізація, що має декілька етапів:

- ознайомлення з об'єктом;
- мінімізація вразливостей;
- складення рекомендацій що до забезпечення максимальної захищеності.

ABSTRACT

Explanatory note to the bachelor's thesis: 59 pages, 14 figures, 16 sources.

INFORMATION, CHANNEL, CYBER INCIDENT, TEAMS, OBJECT,
ENTERPRISE, SOFTWARE, SERVER, INTEGRITY.

The object of study is the server room of a secure enterprise. In the course of the work, it is necessary to analyze the channels of information leakage and minimize their impact on the premises and servers.

The purpose of the work is to master the theoretical foundations and gain practical skills in the field of security design for the selected room, using the knowledge gained during study.

The diploma project consists of two sections. The first section deals with theoretical information and the work assignments, and the second with practical implementation, which has several stages:

- familiarization with the object;
- minimizing vulnerabilities;
- making recommendations on how to ensure maximum security.

ЗМІСТ

Перелік скорочень	7
Вступ.....	8
1 Теоретичні відомості.....	9
1.1 Канали витоку інформації	9
1.2 Концепція Системи захисту інформації.....	11
1.3 Види закладних пристроїв та їх пошук	19
1.4 Центр управління безпеки	21
1.5 Різновид фахівців	23
1.6 Системний захист	26
1.7 Завдання до дипломного проекту	37
2 Розробка СЗІ серверного приміщення.....	38
2.1 Основні відомості про об'єкт в якому знаходиться серверна кімната.....	38
2.2 Відомості про приміщення.	40
2.3 Програмний захист серверів.....	51
2.4 Основні рекомендації мінімізування впливу вразливостей	55
Висновки	57
Перелік джерел посилання	58

ПЕРЕЛІК СКОРОЧЕНЬ

ІзОД	– Інформація з обмеженим доступом
ІТ АС	– Інформаційно-телекомунікаційна автоматизована система
ІТС	– Інформаційно-телекомунікаційна система
КВІ	– Канал(ли) витоку інформації
НСД	– Несанкціонований доступ
ОІД	– Об'єкт інформаційної діяльності
ПЕМВіН	– Побічні електромагнітні випромінювання і наведення
ПЗ	– Програмне Забезпечення
РСО	– Режимно-секретний орган
СЗІ	– Система захисту інформації
ТЗЗІ	– Технічні засоби захисту інформації
SIEM	– Security information and event management (Безпека інформації та управління подіями)
IDS	– Intrusion Detection System (Система виявлення вторгнень)
IPS	– Intrusion Prevention System (Система запобігання вторгненням)
GSM	– Groupe Special Mobile (Глобальна система мобільного зв'язку)
TMS	– Threat Management Systems (Системи управління загрозами)
LAN	– Local area network (Локальна комп'ютерна мережа)
WAN	– Wide area network (Глобальна мережа)
WAF	– Web application framework (Каркас вебзастосунків)
RFI	– Radio frequency interference (Інтерфейс радіочастотних перешкод)
GPS	– Global Positioning System (Система глобального позиціювання)
SSL	– Secure Sockets Layer (Рівень захищених сокетів)
TLS	– Transport Layer Security (Захист на транспортному рівні)
КПП	– Контрольно пропускний пункт

ВСТУП

Сучасний розвиток інформаційних технологій невід'ємно пов'язаний із зростанням важливості та складності питань кібербезпеки. У міру того, як технології продовжують інтегруватися у всі аспекти нашого життя, зростає потреба в забезпеченні захисту інформації та систем від потенційних загроз. Однією з ключових аспектів у забезпеченні безпеки є вивчення та розуміння потенційних загроз і слабких місць в інформаційних системах.

Кіберзлочинці стають все більш витонченими у своїх методах, використовуючи новітні техніки для отримання доступу до конфіденційної інформації. Це підкреслює необхідність постійного вдосконалення методів захисту та аналізу ризиків. У цьому контексті, вивчення вразливостей та потенційних загроз є критично важливим для забезпечення належного рівня захисту інформаційних систем.

В цьому дипломному проекті досліджується питання витоку інформації на прикладі серверного приміщення режимного підприємства. Метою є не лише освоєння теоретичних аспектів безпеки, а й отримання практичних навичок у проектуванні та аналізі можливих вразливостей інформаційних систем використовуючи знання, отримані під час навчання.

Дослідження в рамках цього проекту спрямоване на підвищення рівня обізнаності з питань кібербезпеки. Це включає в себе розгляд сучасних методів атак, таких як фішинг, малваре, атаки на мережі та соціальна інженерія. Крім того, проект зосереджується на вдосконаленні навичок управління інформаційною безпекою в комп'ютерних системах, що є необхідним для створення ефективного технічного захисту інформації [1].

В кінці роботи зроблено висновки по виконаній роботі, в яких зазначено, яким чином було мінімізовано вплив вразливостей на ОІД.

1 ТЕОРЕТИЧНІ ВІДОМОСТІ

1.1 Канали витоку інформації

Канал витоку інформації - це ланцюжок, що веде від джерела конфіденційних даних до зломисника. Цим ланцюжком може йти несанкціонований витік або перехоплення інформації, що охороняється в ІТС [2].

Технічні КВІ прийнято ділити на наступні типи [3] :

- радіоканали (електромагнітні випромінювання радіодіапазона), витік інформації через електромагнітні випромінювання від комп'ютерів, телефонів, інших електронних пристроїв. Перехоплення сигналів мобільного зв'язку, Wi-Fi, Bluetooth для безпроводної периферії (клавіатури, миші, монітори);

- акустичні канали (розповсюдження звукових коливань в будь-якому звукопровідному матеріалі), наприклад підслуховування через стіни, двері, вікна, вентиляційні отвори, використання спеціальних пристроїв, таких як спрямовані мікрофони, стетоскопи [3];

- електричні канали (небезпечні напруги і струми в різних струмопровідних комунікаціях), зломисники можуть наводити паразитні сигнали на лінії електропередач, щоб спотворити або перехопити інформацію, що передається;

- оптичні та опто-електричні канали (електромагнітні випромінювання в інфрачервоній, видимій і ультрафіолетовій частини спектру). Спостереження через вікна, двері, інші отвори. Використання оптичних приладів, таких як біноклі, телескопи. Опто-електричні канали створюються в оптичних волокнах;

- матеріально-речовинні канали (папір, фото, магнітні носії, відходи і т.д.). Співробітники або інші особи, які мають доступ до конфіденційної інформації, можуть використовувати її без дозволу або розкривати її стороннім особам. Використання нейро-лінгвістичного програмування або соціальної інженерії у напрямку працівників для отримання конфіденційної інформації. Фішингові атаки, в яких атакувальник представляється відомими або довіреними особами для

отримання доступу. Невірне використання чи недостатня освіта персоналу з питань безпеки. Порушення правил обробки конфіденційної інформації працівниками.

Утворенню технічних КВІ сприяють певні обставини і причини технічного характеру. До них можна віднести недосконалість елементної бази і схемних рішень (конструкторських, технологічних), експлуатаційний знос елементів пристроїв (зміна характеристик, аварійний вихід із строю), а також зловмисні дії (зміна характеристик, створення аварійних ситуацій, блокування засобів захисту). Знання цих небезпек сприяє кращому вдосконаленню та аналізу небезпек для створення необхідного рівня безпеки в режимному приміщенні [1].

Аналізуючи основні небезпеки, у фізичному плані, можна виділити наступні небезпеки:

- пожежа: електрообладнання, перегрів, коротке замикання, некоректне використання електрообладнання можуть призвести до виникнення пожежі;
- затоплення: водяні потоки можуть спричинити затоплення приміщення, що може призвести до пошкодження обладнання;
- електропостачання: перебої в електропостачанні, напругові піки чи коротке замикання можуть призвести до виходу обладнання з ладу.

В технічному плані можна виділити наступний перелік небезпек:

- здійснення фізичного вторгнення або неправомірний доступ до серверного приміщення;
- використання неправомірних методів отримання доступу, таких як використання фіктивних ідентифікаторів або викрадення карток доступу;
- атаки на мережеві ресурси, спрямовані на отримання конфіденційної інформації. Використання шкідливих програм, вірусів, троянських коней тощо для отримання доступу до серверних даних;
- використання недостатньо захищених акаунтів для отримання доступу до конфіденційної інформації. Порушення політик доступу або використання слабких паролів.

1.2 Концепція системи захисту інформації

Сама СЗІ повинна відповідати головним критеріям захищеності інформації згідно НД ТЗІ 2.5-004-99.

НД ТЗІ 2.5-004-99: Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу

Цей нормативний документ, також відомий як НД ТЗІ 2.5-004-99, встановлює критерії оцінки захищеності інформації, що обробляється в комп'ютерних системах, від несанкціонованого доступу. Він використовується для сертифікації комп'ютерних систем в Україні та є важливим документом для фахівців з кібербезпеки та розробників програмного забезпечення.

Основні положення НД ТЗІ 2.5-004-99:

- класифікація комп'ютерних систем: системи класифікуються за рівнем захищеності на 4 рівні: Д, К, С, Т.
- критерії оцінки: для кожного рівня захищеності визначено набір критеріїв, які повинні бути виконані системою.
- методи оцінки: визначено методи оцінки відповідності системи критеріям захищеності.
- документація: вимоги до документації, яка повинна надаватися для сертифікації системи.



Рисунок 1.1 – Критерії захисту інформації [4]

Конфіденційність, цілісність, доступність, спостережність та гарантійність - це основні критерії захисту інформації, які визначаються для забезпечення безпеки даних та забезпечення їхньої відповідності до встановлених стандартів і вимог.

- конфіденційність: цей критерій вказує на необхідність забезпечення обмеженого доступу до інформації лише для авторизованих користувачів. Це означає, що конфіденційна інформація повинна бути захищена від несанкціонованого доступу або розголошення;

- цілісність: цей критерій вказує на необхідність збереження інформації у незмінному стані та захист від несанкціонованої модифікації. Іншими словами, інформація повинна бути збережена у своєму первісному, незмінному вигляді;

- доступність: цей критерій вказує на необхідність забезпечення доступу до інформації авторизованим користувачам в момент їхньої потреби. Це означає, що інформація повинна бути доступною для користувачів, які мають на це права, і відсутність непередбачуваних перешкод у доступі до неї;

- спостережність: цей критерій вказує на необхідність забезпечення можливості відслідковувати дії користувачів з інформацією та системами, що її обробляють. Це означає, що системи повинні мати засоби моніторингу та журналювання, які дозволяють виявляти та реагувати на потенційні загрози;

- гарантійність: цей критерій вказує на необхідність надання впевненості щодо достовірності та надійності інформації та систем, що її обробляють. Це означає, що інформація та системи повинні працювати з високою точністю та надійністю, а також забезпечувати захист від несправностей та відновлювати роботу в разі виникнення проблем.

Ще однією важливою частиною створення СЗІ є кількісна та якісна оцінки безпеки інформації та захищеності даних. Кількісний аналіз полягає у вимірюванні рівня загроз, вразливостей та ефективності заходів безпеки за допомогою кількісних показників, таких як кількість виявлених загроз, час реакції на інциденти та витрати на заходи безпеки. З іншого боку, якісний аналіз

зосереджується на оцінці ефективності заходів безпеки на основі їхньої якості, відповідності стандартам та здатності відповісти на реальні загрози.

Кількісні методи оцінки можуть включати розрахунок імовірності виникнення інциденту безпеки, обчислення середнього часу реагування на загрозу та визначення показників ефективності заходів безпеки, таких як коефіцієнт виявлення атак чи частота виявлення вразливостей. З іншого боку, якісні оцінки дозволяють аналізувати рівень забезпеченості системи заходами безпеки, якість їхнього впровадження та відповідність стандартам безпеки, таким як ISO 27001.

Обидва підходи мають свої переваги та недоліки і використовуються в залежності від конкретних потреб та умов. Кількісна оцінка може надати конкретні числові дані для прийняття рішень, тоді як якісна оцінка дозволяє краще зрозуміти взаємозв'язок між заходами безпеки та потенційними загрозами. Використання обох підходів у поєднанні допомагає забезпечити комплексний підхід до забезпечення безпеки інформації від кіберінцидентів.

Кіберінциденти є серйозною загрозою для сучасного цифрового світу, відображаючи широкий спектр подій, що стосуються безпеки та конфіденційності в Інтернеті та комп'ютерних мережах. Ці інциденти можуть бути спровоковані широким колом загроз, включаючи хакерські атаки, віруси, шкідливі програми, фішингові атаки, кібершпигунство та кібертероризм. Поняття кіберінциденту охоплює будь-яку незвичайну подію або інцидент в інформаційних технологіях, яка порушує звичний порядок функціонування системи чи мережі. Це може бути спроба несанкціонованого доступу до системи, втрата чи викрадення конфіденційної інформації, а також поширення вірусів чи інших шкідливих програм. Аналіз кіберінцидентів включає в себе вивчення їхніх причин, наслідків та методів протидії. Це дозволяє розуміти та прогнозувати потенційні загрози для безпеки в Інтернеті та розробляти ефективні заходи захисту. Аналіз також включає в себе вивчення модусу операції зловмисників, їхніх мотивів та стратегій, що допомагає розробляти кращі методи захисту в майбутньому. Цим, технічно, займається цифрова криміналістика. Цифрова криміналістика, або digital forensics, є галуззю криміналістики, яка спеціалізується на зборі, аналізі та інтерпретації

електронних доказів з метою розслідування кіберзлочинів та комп'ютерних інцидентів. Вона використовує широкий спектр методів і технологій для виявлення, аналізу та реконструкції цифрових доказів, що містяться на електронних пристроях, таких як комп'ютери, мобільні телефони, планшети та носії інформації. Застосування цифрової криміналістики охоплює такі аспекти, як відновлення видалених файлів, аналіз інтернет-активності, розкриття криптографічних захистів, виявлення слідів злому комп'ютерних систем та розслідування кібератак. Вона також може використовуватися для попередження злочинів шляхом аналізу потенційних загроз та виявлення вразливостей в інформаційних системах.

Основні завдання цифрової криміналістики включають ідентифікацію цифрових доказів НСД, їх збір, зберігання, аналіз і презентацію в суді. Для досягнення цих цілей фахівці з цифрової криміналістики використовують спеціалізовані програмні та апаратні засоби, а також володіють глибокими знаннями з областей кібербезпеки, комп'ютерної науки, математики та права.

Загально світовою спільнотою прийнято розраховувати оцінку безпеки на основі ризику, або так званого кіберризик. Кіберризик - це потенційна загроза, яка виникає з можливості несанкціонованого доступу, втрати, пошкодження чи розголошення інформації через використання комп'ютерних мереж та інтернету. Умовно ми можемо висловити це логічною формулою 1.1

$$\text{Величина Ризика} = \text{Ймовірність Події} \quad (1.1)$$

Однією з ключових складових управління ризиками в інформаційній безпеці є цілі аналізу ризиків. Ці цілі можуть варіюватися залежно від специфіки організації та її цілей. Однак, загальні цілі аналізу ризиків включають:

- ідентифікація загроз: ця ціль передбачає визначення потенційних загроз для інформаційних ресурсів та даних, які можуть виникнути внаслідок небажаних подій або дій з боку злоумисників;

- оцінка потенційних втрат: під час оцінки ризиків важливо визначити можливі наслідки випадків, пов'язаних із загрозами, і визначити їх вплив на організацію;

- визначення вразливостей: з'ясування потенційних точок вразливості в інформаційній інфраструктурі організації, які можуть бути використані зловмисниками для реалізації загроз;

- розробка стратегій мінімізації ризиків: на основі результатів аналізу ризиків визначаються стратегії та заходи для зменшення можливостей виникнення ризикованих ситуацій;

- моніторинг та аналіз ефективності заходів: постійне спостереження за станом інформаційної безпеки, виявлення нових загроз та визначення їх впливу на організацію.

Одним із ключових етапів управління ризиками є аналіз ризиків, який може бути кількісним або якісним. Кількісний аналіз ризиків ґрунтується на вимірюванні ймовірності виникнення загроз та потенційних збитків, що можуть виникнути в результаті цих загроз. Він передбачає математичні розрахунки для визначення значимості ризиків. Якісний аналіз ризиків, з іншого боку, базується на експертному оцінюванні ризиків шляхом оцінки їх ймовірності та впливу на організацію без використання конкретних числових даних. Для кількісного аналізу ризиків широко використовуються поняття Single Loss Expectancy (SLE) та Annual Loss Expectancy (ALE). SLE - це середня вартість збитків, які можуть виникнути в результаті конкретної загрози у випадку її реалізації. ALE - це середній річний збиток, який очікується внаслідок цієї загрози.

Розрахунок SLE виконується шляхом множення вартості втрати одного інциденту (AssetValue) на ймовірність виникнення цього інциденту(EF), тобто

$$SLE=AssetValue*EF \quad (1.2)$$

ALE розраховується, враховуючи SLE та ймовірність виникнення цієї загрози протягом року(ARO), тобто:

$$ALE=SLE*ARO \quad (1.3)$$

Приклади якісного аналізу ризиків в ІБ можуть включати в себе різноманітні сценарії та методики, орієнтовані на ідентифікацію та оцінку потенційних загроз і вразливостей. Один із таких прикладів - використання матриць ризиків, які дозволяють систематизувати та візуалізувати рівень ризиків за різними параметрами, такими як ймовірність виникнення події та її вплив на бізнес-процеси.

Ще одним прикладом є методика "SWOT-аналізу", яка дозволяє ідентифікувати сильні та слабкі сторони системи управління ризиками, а також можливості та загрози, що виникають з зовнішнього середовища. Основними частинами обробки ризиків є рівень ризику, його оцінка та можливість залишкового ризику.

Рівень ризику, або "level of risk", визначає ступінь загрози, яку представляють потенційні загрози для інформаційної системи та організації в цілому. Вимірюється цей рівень на основі ймовірності виникнення загрози та потенційного впливу цієї загрози на бізнес-процеси та ресурси організації.

Оцінка ризику, або "risk assessment", є процесом ідентифікації, аналізу та оцінки ризиків, які можуть вплинути на інформаційну систему. Цей процес включає в себе оцінку потенційних загроз, визначення вразливостей, оцінку відповідних контролів та прийняття рішення щодо прийняття або уникнення ризику.

Залишковий ризик, або "residual risk", відображає рівень ризику, який залишається після впровадження заходів з управління ризиками. Це оцінка ризику після застосування контрольних заходів для зменшення або усунення загроз. Залишковий ризик може залишатися на прийнятному рівні або вимагати додаткових заходів для мінімізації.

Захист інформації від витoku через технічні канали включає в себе ряд методів та засобів, які можуть бути як пасивними, так і активними. Усі ці заходи спрямовані на зниження рівня акустичних або віброакустичних сигналів до певного співвідношення сигналу та завади, встановленого відповідними нормами. Пасивні методи захисту передбачають підвищення звукоізоляції огорожувальних

конструкцій, таких як металопластикові вікна, ущільнювачі дверей або акустичні фільтри у повітроводи. З іншого боку, активні заходи спрямовані на створення активної акустичної або віброакустичної завади, яка знижує співвідношення сигналу до нормованого рівня. Наприклад для захисту провідних телефонних ліній передбачає використання різних методів та засобів для запобігання несанкціонованому доступу і перехопленню інформації через ці лінії. Одним з ефективних заходів є екранування ліній за допомогою оплітки або фольги, які повинні бути заземлені відповідно до встановлених норм для уникнення струмів, що протікають по екрану. Сам термін Екранування приміщення — це важливий аспект забезпечення безпеки та конфіденційності інформації, що проводиться за допомогою різних технічних методів та матеріалів з метою мінімізації зовнішніх електромагнітних впливів на приміщення або обмеження виходу електромагнітних хвиль з нього. Один з методів екранування — використання спеціальних матеріалів, що мають властивості електромагнітного екранування.

Практично прийнято мінімізувати площу контуру, який утворюється прямим і зворотним проведенням лінії, наприклад, шляхом скручування ліній у біфіляри. Лінії, що виготовлені з екранованого проведення або коаксіального кабелю, також повинні відповідати вимогам мінімізації площі контуру лінії, особливо якщо протікає зворотний струм по оплітці. Методи захисту провідних телефонних ліній поділяються на пасивні та активні. Пасивний захист передбачає використання фільтрів та інших пристроїв для перешкодження прослуховуванню приміщень через телефонні лінії, що перебувають у режимі відбою. Ці пристрої можуть бути встановлені безпосередньо на лінії або вбудовані в телефонні апарати. Окрім цього, широко використовуються різноманітні індикаторні пристрої, які працюють на основі аналізу параметрів телефонних ліній. Пристрої для встановлення активної загороджувальної перешкоди мають на меті захистити телефонні лінії від різних видів пристроїв для прослуховування. Це досягається шляхом введення додаткових сигналів (загороджувальної перешкоди) у лінію та зміни стандартних параметрів телефонної лінії, таких як постійна складова напруги та струм у ній, у всіх режимах роботи, зазвичай в межах, які не порушують її нормальне функціонування. Для

повного пригнічення всіх видів випромінювань, які генеруються технічними засобами аудіозапису, необхідно фільтрувати випромінювання в лінійних проводах, які виходять з пристрою, і проводах мікрофона, а також забезпечити достатнє екранування внутрішньої схеми технічного засобу аудіозапису. Екранування та фільтрація всіх проводів, що виходять з пристрою, можливі лише при значних модифікаціях конструкції технічного засобу аудіозапису та зміні його електричних параметрів. Загалом, для захисту технічного засобу аудіозапису необхідно виконати наступні заходи:

- захистити ланцюг мікрофона;
- захистити ланцюг дзвінка;
- захистити двопровідну лінію телефонної мережі.

ТЗЗІ є складними системами або пристроями, що виконують захисні функції в більшій мірі активного плану. Вони мають численні переваги, такі як висока надійність, можливість створення комплексних систем захисту, гнучке реагування на спроби несанкціонованого доступу та традиційність використовуваних методів. Наприклад системи для захисту від навмисного силового впливу, який може бути як до усієї системи, загальна мережа живлення, так і локальні пристрої або їх порти, у випадку портів особливою небезпекою є USB-killer. USB-Killer - це шкідливий пристрій, який призначений для знищення електронних пристроїв шляхом подачі великої напруги через порт USB, але деякі сучасні моделі здатні навіть спотворити і більш глибокі компоненти пристрою, материнські плати, процесори, накопичувачі та інше. Системи ТЗЗІ також мають недоліки, включаючи високу вартість, потребу у регулярному обслуговуванні та можливість видачі фіктивних тривог.

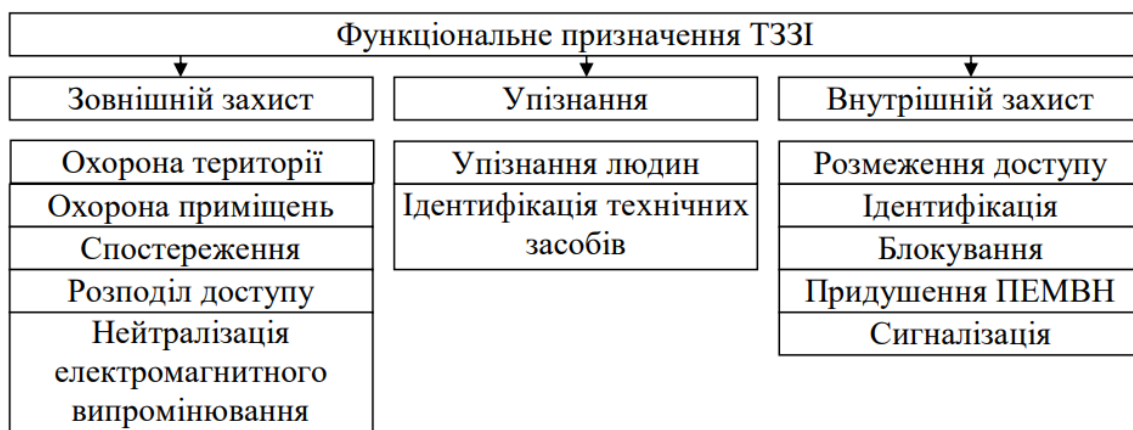


Рисунок 1.2 – Класифіковане призначення ТЗЗІ [5]

Системна класифікація ТЗЗІ може бути проведена з урахуванням таких критеріїв, як функція захисту, складність пристрою та спряженість з обчислювальною технікою. Ці критерії допомагають у здійсненні відповідних інтерпретацій і визначенні кращих підходів до захисту інформації від витіку технічними каналами.

1.3 Види закладних пристроїв та їх пошук

Закладні пристрої, такі як радіозакладки, мобільні телефони або бездротові камери, можуть бути використані для шпигунства, незаконного перехоплення даних або навіть для проведення кримінальних дій.

Наприклад закладним пристроєм може стати мобільний телефон працівника на якому може бути встановлено шпигунське ПЗ Pegasus.

Pegasus - це шпигунське програмне забезпечення, розроблене ізраїльською компанією NSO Group. Воно здатне непомітно заражати мобільні телефони та інші пристрої, що працюють під управлінням iOS та Android, і збирати широкий спектр особистої інформації.

Можливості Pegasus:

- перехоплення дзвінків та повідомлень: Pegasus може записувати телефонні дзвінки, текстові повідомлення, електронні листи та інші комунікації;
- доступ до фотографій та відео: Pegasus може отримувати доступ до фотографій, відео та інших файлів, що зберігаються на пристрої;
- відстеження місцезнаходження: Pegasus може відстежувати місцезнаходження пристрою в режимі реального часу;
- включення мікрофона та камери: Pegasus може включати мікрофон та камеру пристрою для запису звуку та відео без відома користувача;
- викрадення даних: Pegasus може викрадати паролі, банківські дані та інші конфіденційні дані з пристрою.

Pegasus зазвичай поширюється через заражені посилання або SMS-повідомлення. Коли користувач відкриває посилання, або натискає на SMS-повідомлення, Pegasus непомітно завантажується на його пристрій. Після зараження Pegasus може працювати в фоновому режимі, невідомий користувачеві. Через це пристрій може стати не тільки засобом витоку інформації, але й перейти в режим радіозакладки, або віддалено атакуючим пристроєм який у випадку знаходження у режимному приміщенні з засобами бездротової мережі може почати розповсюдження шкідливого ПЗ.

Пошук закладних пристроїв в режимному приміщенні - це важлива процедура для забезпечення безпеки та конфіденційності важливої інформації. Процес пошуку закладних пристроїв включає в себе використання спеціалізованих технічних засобів та методів для виявлення наявності таких пристроїв. Серед цих засобів можуть бути радіочастотні детектори, спектральні аналізатори, термальні камери, напрямні антени і приймачі сигналів, аналізатори сигналу мобільного зв'язку та ручні радіочастотні детектори.

Виявлення закладних пристроїв в режимному приміщенні вимагає високої кваліфікації та досвіду у використанні спеціалізованого обладнання. Оператори повинні бути здатні розрізняти сигнали, визначати їх джерело та локалізувати потенційно небезпечні пристрої.

Успішний пошук закладних пристроїв може врятувати важливу інформацію від несанкціонованого доступу, запобігти негативним наслідкам для безпеки та

конфіденційності. Тому ця процедура відіграє ключову роль у забезпеченні безпеки режимних приміщень та захисту важливої інформації.

Існує кілька пристроїв, які можуть використовуватися для пошуку радіозакладок та інших подібних пристроїв в приміщенні. Ось деякі з них:

- радіочастотні детектори: ці пристрої призначені для виявлення радіочастотних сигналів у визначеному діапазоні частот. Вони можуть виявляти радіозакладки, мобільні телефони, бездротові камери тощо.

- спектральні аналізатори: ці пристрої аналізують радіочастотний спектр на наявність сигналів різних частот. Вони можуть виявляти радіозакладки, перешкоди інших пристроїв, а також здатні виявляти зміни в спектрі сигналу, що може свідчити про діяльність шпигунських пристроїв.

- термальні камери: термальні камери можуть використовуватися для виявлення нагрітих пристроїв, таких як бездротові камери або передавачі, які можуть виділяти тепло;

- напрямні антени і приймачі сигналів: ці пристрої можуть використовуватися для визначення напрямку, з якого приходить сигнал, що допомагає виявити місце розташування радіозакладки або іншого пристрою;

- аналізатори сигналу GSM/3G/4G: ці пристрої спеціалізуються на виявленні та аналізі сигналів мобільного зв'язку, що може допомогти виявити діючі мобільні телефони або інші пристрої, які можуть використовуватися для шпигунства або незаконного перехоплення даних;

- ручні радіочастотні детектори: ці пристрої компактні і можуть бути використані для швидкого сканування приміщень або предметів для виявлення радіозакладок або інших бездротових пристроїв.

1.4 Центр управління безпеки

Важливою частиною системи безпеки є SOC. Security Operations Center (SOC)

- це центр управління безпекою, який забезпечує моніторинг, виявлення, аналіз та реагування на інциденти і загрози інформаційної безпеки в реальному часі. SOC є

централізованою частиною інформаційної безпеки організації і може використовувати різноманітні технології та інструменти для забезпечення безпеки.

Основні функції SOC включають:

- моніторинг безпеки: спостереження за мережею, системами та застосунками на предмет аномальної активності та потенційних загроз;
- виявлення загроз: аналіз інцидентів та виявлення потенційно шкідливої активності або атак на інформаційні системи;
- реагування на інциденти: вживання заходів для ліквідації виявлених загроз і захисту інформаційних ресурсів;
- аналіз інцидентів: проведення ретроспективного аналізу інцидентів для виявлення причин їх виникнення та розроблення стратегій запобігання подібним інцидентам у майбутньому;
- керування інцидентами: координація реагування на інциденти та співпраця з іншими відділами організації та зовнішніми сторонами, включаючи правоохоронні органи та постачальників послуг безпеки.

SOC може використовувати різноманітні інструменти і технології, такі як системи моніторингу подій та інцидентів (SIEM), наприклад ось деякі ключові аспекти їх взаємодії:

- збір та агрегування даних: SIEM збирає дані про безпеку з різних джерел, таких як мережеві пристрої, сервери, кінцеві точки та програмні додатки. Ці дані потім агрегуються та нормалізуються, щоб забезпечити єдиний погляд на безпеку інформаційної системи;
- аналіз та кореляція даних: SIEM використовує аналітику та правила кореляції для виявлення підозрілих активностей, які можуть свідчити про кіберзагрозу. Ці правила можуть бути засновані на відомих атаках, поведінці користувачів або інших факторах ризику;
- повідомлення про інциденти та реагування: коли SIEM виявляє підозрілу активність, він може генерувати попередження та сповіщати SOC про потенційну кіберзагрозу. SOC може потім розслідувати інцидент, вжити відповідних заходів та вжити заходів для стримування атаки;

- автоматизація та оркестрація: SIEM та SOC можуть бути інтегровані з іншими системами кібербезпеки, такими як брандмауери, системи запобігання вторгненням (IPS) та системи розвідки загроз (TI). Це дозволяє автоматизувати відповіді на інциденти, такі як блокування IP-адрес, ізоляція заражених систем або оновлення антивірусних баз даних;

- безперервне вдосконалення: SIEM та SOC постійно оновлюються новою інформацією про загрози та вразливості. Ця інформація використовується для вдосконалення правил кореляції, аналітики та методів реагування на інциденти.

У той же час системи SIEM включають в себе Системи виявлення вторгнень (IDS/IPS), системи управління загрозами (TMS), системи аналізу великих даних (Big Data Analytics) та інші, для забезпечення безпеки організації. Відповідно до розміру та потреб організації, SOC може бути розгорнутим як внутрішній відділ компанії або використовувати послуги зовнішніх постачальників безпеки.

1.5 Різновид фахівців

Згідно з розвитком серверів з'явилась необхідність для захисту їх як у фізичному плані, так і у програмному. У програмному випадку з'явилась необхідність у фахівцях кібербезпеки однієї з трьох основних "команд". [6]

Red Team (червона команда) – це фахівці які комплексно імітують реальні атаки з метою оцінки захищеності, в плані кібербезпеки, систем. Вони можуть бути як найнятими зі сторони, так і співробітниками вашої організації, але у всіх випадках їхня роль однакова - імітувати дії зловмисників і намагатися проникнути у вашу систему.

Поряд із "червоними командами" в кібербезпеці існує й низка інших. Так, наприклад, "синя команда" (Blue Team) працює разом із червоною, але її діяльність спрямована на підвищення безпеки інфраструктури системи зсередини, і в більшості випадків відповідальна за фізичну безпеку.

Основні завдання синьої команди включають:

- виконання постійного моніторингу стану інфраструктури та аналіз подій з метою виявлення аномальних або підозрілих активностей;
- проведення аудиту та сканування систем для виявлення потенційних вразливостей, які можуть бути використані зловмисниками;
- вчасне реагування на події безпеки та швидке усунення виявлених загроз для запобігання можливим інцидентам;
- забезпечення безпеки приміщень, обладнання та інфраструктури системи шляхом впровадження відповідних фізичних заходів захисту;
- проведення аналізу ефективності існуючих заходів безпеки та розробка рекомендацій щодо покращення рівня захисту інфраструктури;
- організація тренінгів та навчання персоналу з питань інформаційної безпеки для запобігання внутрішнім загрозам;
- розробка та впровадження політик, процедур та стандартів безпеки, спрямованих на підвищення рівня захисту інфраструктури.

"Пурпурова команда" (Purple Team) є сполучною ланкою, допомагаючи двом іншим командам у розробці стратегії нападу і заходів захисту. В більшій мірі фахівці пурпурної команди є свого роду головним над іншими командами, бо більшість представників цього напрямку відповідальні за остаточні рішення з приводу безпеки.

Також є неосновні (похідні від основних команд) напрями розробників інформаційної безпеки, це жовта та помаранчева команди, наприклад жовта команда в сфері кібербезпеки виконує ряд важливих фахових задач, спрямованих на виявлення потенційних загроз та захист інформаційних ресурсів. Ось деякі з основних фахових завдань жовтої команди в кібербезпеці:

- моніторинг та аналіз відхилень: жовта команда відстежує та аналізує аномальну активність в мережі та системах, виявляючи відхилення від норми, що можуть вказувати на можливі загрози безпеці;
- виявлення потенційних загроз: жовта команда використовує різноманітні інструменти та техніки для виявлення потенційних загроз та атак, таких як

аномальна активність користувачів, підозрілі мережеві пакети, незвичайна конфігурація систем тощо;

- аналіз загроз: жовта команда аналізує виявлені потенційні загрози, оцінює їх серйозність та потенційні наслідки для систем та даних організації.

- реагування на інциденти: жовта команда співпрацює з іншими командами кібербезпеки для реагування на виявлені загрози та інциденти, проводить детальний аналіз подій та вживає необхідні заходи для їх ліквідації;

- вдосконалення процесів та заходів безпеки: жовта команда допомагає у вдосконаленні процесів та заходів безпеки, шляхом виявлення слабких місць, розробки та впровадження нових технологій та практик, а також навчання персоналу щодо попередження та виявлення загроз;

- виявлення потенційних слабкостей в системах і мережах організації: це включає аналіз коду програмного забезпечення, виявлення вразливостей в мережевих протоколах та ідентифікацію можливих шляхів атаки;

- вирішення інцидентів безпеки: помаранчева команда відповідає за реагування на інциденти безпеки, виявлення та виправлення вразливостей, а також захист систем та даних від потенційних загроз;

- виконання тестів на проникнення: це включає моделювання атак і намагання взлому систем та мереж, щоб виявити потенційні слабкості та вразливості, які можуть бути використані зловмисниками;

- розробка та впровадження стратегій безпеки: помаранчева команда працює над розробкою та впровадженням стратегій, які допомагають організаціям захищати свої системи та дані від різних загроз;

- навчання та наведення усвідомленості про кібербезпеку: помаранчева команда надає навчальні програми та проводить тренінги для персоналу організації з питань кібербезпеки, щоб збільшити загальний рівень обізнаності та підвищити ступінь захищеності;

- виявлення та аналіз потенційних загроз: помаранчева команда аналізує дані щодо кіберзагроз та намагається виявити та відвернути можливі атаки з боку зловмисників.

1.6 Системний захист

Основною концепцією безпеки на програмному рівні є Кільця захисту (англ. "rings of protection") - це концепція в області комп'ютерних систем, яка використовується для визначення рівнів привілеїв та доступу до ресурсів на операційних системах та архітектурі процесорів.

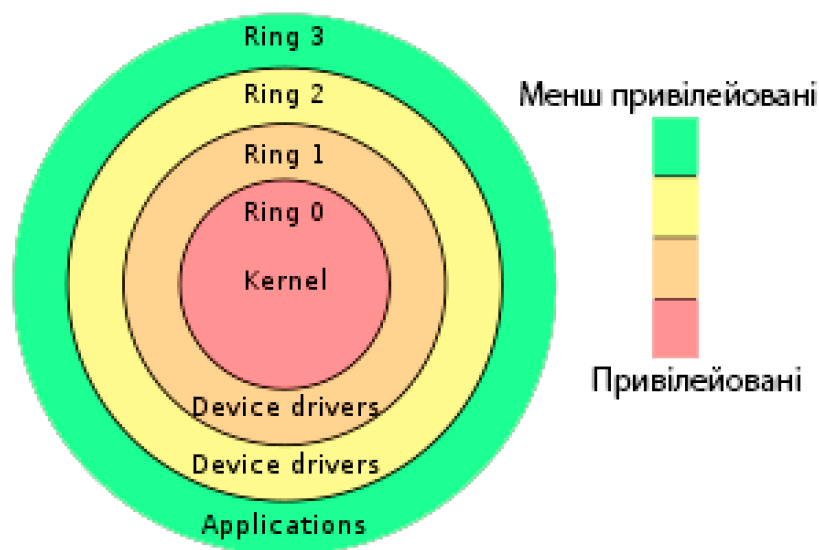


Рисунок 1.3 – Структурна ієрархія [7]

Ця концепція базується на ідеї, що системний рівень має бути розділений на декілька "кілець" або рівнів захисту, кожен з яких має свої права доступу та привілеї. Основні рівні кілець захисту зазвичай включають чотири рівні.

Кінець (Ring 0 або Level 0). Це найвищий рівень привілеїв, також відомий як "режим ядра" або "супервізорський режим". На цьому рівні знаходиться ядро операційної системи, яке має повний доступ до апаратних ресурсів комп'ютера та може виконувати привілейовані операції, такі як керування пам'яттю та обробка переривань. У багатьох операційних системах, таких як Windows, Linux, і macOS, "Ring 0" використовується для запуску ядра операційної системи і виконання

операцій, які вимагають прямого доступу до апаратного забезпечення, такого як керування процесором, пам'яттю, введенням/виведенням (I/O), таймерами та іншими системними ресурсами. Оскільки рівень 0 має повний доступ до апаратних ресурсів, він відповідає за забезпечення безпеки, стабільності та ефективності роботи системи.

Використання "Ring 0" важливо для забезпечення надійності та безпеки операційної системи, оскільки він забезпечує виконання критичних операцій та обробку переривань з мінімальними затримками та втратами продуктивності. Однак, такий високий рівень привілеїв також може створити проблеми безпеки, якщо недостатньо захищений від зловживань або атак.

Системний рівень (Ring 1 або Level 1). Цей рівень не так привілеєвий, як рівень 0, але все ще надає певні привілеї. Деякі операційні системи використовують рівень 1 для виконання деяких операцій, які не потребують повного доступу до апаратури. У цьому режимі виконуються окремі компоненти операційної системи, які не потребують такого ж рівня привілеїв, що і ядро операційної системи. Наприклад, виконання підсистеми управління пам'яттю або драйвера пристрою може здійснюватися на рівні Ring 1.

Основні характеристики рівня 1 включають:

- обмежений доступ до апаратних ресурсів: програми на рівні 1 мають обмежений доступ до апаратних ресурсів порівняно з ядром операційної системи на рівні 0;

- забезпечення надійності: рівень 1 використовується для виконання програм, які мають обмежений доступ до критичних системних ресурсів, щоб запобігти можливим проблемам безпеки та забезпечити надійність операційної системи;

- управління ресурсами: програми на рівні 1 використовуються для управління обмеженим набором ресурсів, таких як пам'ять або пристрої вводу-виводу.

Користувацький рівень (Ring 2 або Level 2). Цей рівень має обмежений доступ до апаратних ресурсів і використовується для виконання користувацьких

програм. У Ring 2 зазвичай знаходяться драйвери пристроїв та інші системні програми, які мають вищий рівень привілеїв порівняно зі звичайними користувачами, але нижчий рівень привілеїв порівняно з ядром операційної системи. Це означає, що програми на рівні 2 можуть виконувати деякі привілейовані операції, такі як керування пристроями або взаємодія з ядром, але вони не мають безпосереднього доступу до апаратного забезпечення або можливості виконання найбільш привілейованих операцій, які можуть виконувати ядро в режимі Kernel Mode (рівень 0 або Ring 0).

Більш ключовими відмінностями між Ring 1 та Ring 2 можна виділити наступні деталі:

- рівень привілеїв: Ring 1 (або Level 1) зазвичай має вищий рівень привілеїв, ніж Ring 2 (або Level 2). У рівні 1 зазвичай виконується ПЗ, що потребує привілеїв вищого рівня, наприклад, драйвери пристроїв. Рівень 2 може бути використаний для виконання менш критичних завдань або додаткових рівнів безпеки;

- потреби в системних ресурсах: у рівні 1 зазвичай розміщуються операції, які потребують прямого доступу до апаратних ресурсів, таких як операції з ядром операційної системи. Рівень 2 може бути використаний для розміщення менш критичних операцій або операцій, які не потребують безпосереднього доступу до апаратних ресурсів;

- керування пам'яттю: у рівні 1 зазвичай використовується власна таблиця сторінок, яка дозволяє неперервно використовувати адресний простір ядра. У рівні 2 можуть використовуватися власні таблиці сторінок, але зазвичай вони менш потужні або обмежені;

- контроль доступу: у рівні 1 зазвичай здійснюється більший контроль доступу до апаратних ресурсів і системних операцій, таких як переривання і виклики системного програмування. У рівні 2 може бути менше обмежень на доступ до апаратних ресурсів, але все ще може бути здійснений контроль доступу для забезпечення безпеки системи.

Користувацький рівень (Ring 3 або Level 3). Цей рівень є найнижчим рівнем привілеїв в архітектурі комп'ютерних систем. У цьому режимі виконуються

звичайні користувацькі програми та процеси, і вони мають обмежений доступ до апаратного забезпечення комп'ютера та системних ресурсів. Користувацькі програми виконуються відокремлено одна від одної і від операційної системи.

На рівні 3 процеси не мають можливості напряму взаємодіяти з апаратним забезпеченням або виконувати привілейовані операції, такі як зміна режиму роботи процесора або керування пам'яттю. Замість цього вони взаємодіють з операційною системою, яка дозволяє їм виконувати потрібні завдання через системні виклики. Ці рівні дозволяють забезпечити відокремленість та ізоляцію між різними частинами операційної системи та програмами, що допомагає запобігти несанкціонованому доступу до ресурсів та забезпечити безпеку системи.

З приводу обрання основної операційної системи для серверу виділяють дві найбільш популярні FreeBSD та Red Hat Enterprise Linux.

FreeBSD – це вільна операційна система типу Unix, що базується на 4.4 BSD-Lite з доповненнями з Berkeley Software Distribution (BSD). Вона розроблена командою FreeBSD і доступна безкоштовно для будь-яких цілей, включаючи комерційне використання. FreeBSD – це вільна операційна система, що означає, що її можна вільно використовувати, вивчати, модифікувати та розповсюджувати. Код FreeBSD повністю відкритий, що дозволяє користувачам бачити, як працює система, і вносити зміни відповідно до своїх потреб. FreeBSD відома своєю стабільністю і надійністю. FreeBSD має багато вбудованих функцій безпеки, що робить її безпечним вибором для серверів та інших критичних систем. FreeBSD може бути налаштована для роботи на широкому спектрі апаратних платформ для роботи. FreeBSD може використовуватися для різних цілей, включаючи:

- сервери: FreeBSD – це популярний вибір для серверів, завдяки своїй стабільності, безпеці та гнучкості;
- робочі станції: FreeBSD може використовуватися як настільна операційна система, як для домашнього, так і для ділового використання;
- вбудовані системи: FreeBSD може використовуватися в вбудованих системах, таких як маршрутизатори, брандмауери та мережеві пристрої зберігання;

- хмарні середовища: FreeBSD може використовуватися в хмарних середовищах, таких як Amazon Web Services (AWS) та Google Cloud Platform (GCP).

Недоліки FreeBSD:

- складність: FreeBSD може бути складною для новачків, адже вона потребує певного розуміння Unix-систем;

- невелика спільнота: спільнота FreeBSD не така велика, як спільнота Linux, тому може бути складніше знайти допомогу та підтримку;

- недоступність деяких програм: деякі програми не доступні для FreeBSD, або доступні лише у версіях з обмеженою функціональністю.

Проте є й інший більш популярний дистрибутив, це Red Hat Enterprise Linux (RHEL) є однією з провідних комерційних дистрибуцій операційної системи Linux у світі. Розроблена компанією Red Hat, ця операційна система відзначається високою стабільністю, безпекою та підтримкою великого спектру апаратного забезпечення. Однією з ключових особливостей RHEL є його спрощена система керування пакунками, що базується на інструменті RPM (Red Hat Package Manager). Це дозволяє адміністраторам ефективно керувати програмним забезпеченням та його залежностями, забезпечуючи стабільну та надійну роботу системи. Безпека є однією з головних переваг RHEL. Компанія Red Hat активно використовує систему SELinux (Security-Enhanced Linux), яка надає розширені можливості контролю доступу до системних ресурсів та управління привілегіями користувачів.

RHEL також відомий своєю довготривалою підтримкою та циклом життя продукту. Кожна версія RHEL отримує підтримку протягом 10 років, що дозволяє користувачам спокійно планувати оновлення та забезпечує стабільну роботу системи протягом тривалого періоду. Завдяки відкритому коду та активній спільноті розробників, RHEL постійно вдосконалюється та оновлюється, надаючи користувачам найновіші технології та функціонал. Ця операційна система заслужено вважається однією з найнадійніших та потужних платформ для корпоративних середовищ у сфері IT.

Також є необхідним згадати про Alpine Linux - це легковаговий і мінімалістичний дистрибутив Linux, який в основному використовується у сферах,

де вимагається висока ефективність та мінімальне споживання ресурсів. Вона є в своїй більшості операційною системою яку використовують в Docker-контейнерах, засновуючись на принципі “Збери усе самостійно”. Основні особливості Alpine Linux включають наступне:

- мінімалістичний обсяг: Alpine Linux має невеликий обсяг, що робить його ідеальним вибором для використання у віртуальних середовищах та контейнерах. Більшість компонентів, які можуть бути знайдені в інших дистрибутивах, можуть бути додані за допомогою пакетного менеджера apk;

- ефективне використання ресурсів: Alpine Linux оптимізований для мінімізації споживання пам'яті, процесорного часу та мережевого трафіку, що робить його ідеальним для використання в ролі веб-серверів, мережесих маршрутизаторів та інших високопродуктивних застосунків;

- вбудована безпека: Alpine Linux поставляється зі зв'язком libc (musl) та іншими компонентами, що допомагають у забезпеченні безпеки системи. Крім того, Alpine Linux відомий своєю активною командою розробників, яка швидко реагує на виявлені уразливості та публікує оновлення безпеки.

У випадку необхідності автоматизованого контролю Docker-контейнерів використовують K8S, або Kubernetes, це відкрита система з оркестрації контейнерів. Вона призначена для автоматизації розгортання, масштабування та управління контейнеризованими програмами.

Іншими словами, Kubernetes допомагає керувати контейнерами. Контейнери – це стандартизовані одиниці ПЗ, які включають код, бібліотеки та інші залежності, необхідні для роботи програми. Вони полегшують розгортання та масштабування програм, оскільки їх можна легко переміщати між різними середовищами.

Kubernetes допомагає з такими завданнями, як:

- запуск контейнерів;
- масштабування контейнерів вгору або вниз залежно від потреб;
- відновлення контейнерів у разі їх збою;
- розподіл ресурсів між контейнерами;
- забезпечення балансування навантаження для контейнерів.

Використання Kubernetes може допомогти організаціям швидше розробляти, розгортати та масштабувати свої програми. Це також може допомогти підвищити ефективність використання ресурсів та зробити програми більш стійкими до помилок.

Ще однією особливістю використання K8S та Docker в цілому це можливість у моніторингу CVE, що допомагає швидше орієнтуватись в плані безпеки у тому чи іншому контейнері. Наприклад 28 березня 2024 року німецький розробник Андрес Фройнд оприлюднив звіт про виявлену лазівку (бекдор) у нових версіях бібліотеки стиснення liblzma (частина архіватора xz). Ця лазівка давала зломисникам можливість віддаленого доступу через SSH до систем, де використовувалися ці версії. Виявлена лазівка в бібліотеці стиснення liblzma продемонструвала високий рівень майстерності та ретельне планування з боку зломисника. Деталі приховування лазівки:

Зломисник, який діяв під псевдонімом Jia Tan, протягом двох років брав участь у розробці xz, здобувши довіру мейнтейнерів та доступ до репозиторію з можливістю внесення комітів. Для приховування лазівки було вжито низки кроків:

Зломисник зробив понад 700 комітів, лише невелика частина з яких поступово підготувала код для лазівки.

Вихідний код, що містив лазівку та інтегрувався до бібліотеки, не був включений до основного репозиторію Github. Натомість він був прихований у tar-архівах двох останніх релізів, які зазвичай використовувалися мейнтейнерами дистрибутивів.

Цей метод приховування полягав у тому, що існував тег релізу та архів, який нібито генерувався з репозиторію на момент створення тегу. Однак до цього архіву було додано незначну модифікацію, якої не було присутньо в самому репозиторію. Ця модифікація була прихована за допомогою конфігураційної магії autoconf, яку рідко хто досліджує. Вона спрацьовувала лише під час конфігурування вихідного коду для створення Debian-пакета або RPM-пакета, що зазвичай робили мейнтейнери дистрибутивів. У цьому випадку з тестових файлів витягувалися певні фрагменти коду та вбудовувалися до бібліотеки. Важливо зазначити, що код

лазівки замінював кілька функцій в бібліотеці, які працювали з символьними таблицями бібліотек під час їхнього завантаження. Для приховування назв цих функцій вживалися спеціальні заходи такі як обфускація та перейменування. Сам термін обфускація коду означає процес навмисного ускладнення читабельності програмного коду, роблячи його важким для розуміння для людей, але зберігаючи його функціональність. Існує багато різних методів обфускації коду, деякі з найпоширеніших включають:

- зміна імен змінних і функцій: це робить код незрозумілим для людей, які не знайомі з оригінальними іменами;
- видалення зайвих коментарів і пробілів: це робить код більш щільним і складним для читання;
- вставка псевдокоду: це додає до коду зайвий код, який не впливає на його функціональність, але робить його ще більш складним для розуміння;
- шифрування коду: це робить код нечитабельним без ключа дешифрування.

Обфускація коду може використовуватися з кількох причин:

- ускладнення реверс-інжинірингу: обфускація коду може ускладнити зловмисникам розуміння того, як працює код, що може ускладнити їм його зламування;
- запобігання маніпуляціям з кодом: обфускація ускладнює модифікацію коду зловмисниками, що може запобігти внесенню шкідливих змін або використанню додатків у спосіб, який не був передбачений розробниками.



Рисунок 1.4 – Приклад коду до обфускації



Рисунок 1.5 – Приклад коду після обфускації

Після публікації дослідів вразливість отримала номер CVE-2024-3094.

Саме тому використання Docker поліпшує процес виправлення програмних небезпек через те що виправлення вразливостей в одному контейнері ніяк не завадить праці іншого або основної операційної системи.

Для розділення між закритим типом мережі (LAN) та інтернет доступною (WAN) використовують демілітаризовану зону (англ. Demilitarized Zone, скор. DMZ або ДМЗ) — сегмент мережі, що містить загальнодоступні сервіси та відокремлює їх від приватних. Як загальнодоступний може виступати, наприклад, вебсервіс: сервер, що його забезпечує, який фізично розміщений у локальній мережі (Інтернет), повинен відповідати на будь-які запити із зовнішньої мережі (Інтернет), при цьому інші локальні ресурси (наприклад, файлові сервери, робочі станції) необхідно ізолювати від зовнішнього доступу.

Мета ДМЗ — надати додатковий рівень безпеки в локальній мережі, який дозволяє мінімізувати збитки в разі атаки на один із загальнодоступних сервісів: зовнішній зловмисник має прямий доступ тільки до обладнання в ДМЗ.

З приводу шифрування даних ситуація стрімко змінюється через розвиток технологій та всебіч збільшення впровадження штучного інтелекту у повсякденне

життя. Цей процес зумовлює появу нових викликів та можливостей, які потребують ретельного аналізу та адаптації існуючих методів захисту інформації.

З одного боку, розвиток штучного інтелекту відкриває нові горизонти для вдосконалення алгоритмів шифрування. Завдяки машинному навчанню та аналізу великих даних стає можливим розробляти більш стійкі та ефективні методи кодування, стійкі до атак з боку злочинців. З іншого боку, штучний інтелект може використовуватися й для розробки нових методів дешифрування. Зловмисники, які мають доступ до потужних обчислювальних ресурсів та алгоритмів машинного навчання, можуть знаходити слабкі місця в системах шифрування та отримувати доступ до конфіденційної інформації.

Важливо зазначити, що вплив штучного інтелекту на шифрування даних не є однозначним. Ця технологія може використовуватися як для посилення, так і для ослаблення систем захисту інформації. Тому важливо постійно вдосконалювати методи шифрування, враховуючи нові можливості та ризики, які з'являються з розвитком штучного інтелекту.

Ось деякі ключові аспекти, які слід враховувати при аналізі впливу штучного інтелекту на шифрування даних. Збільшення доступних обчислювальних ресурсів може призвести до того, що зловмисникам буде легше зламувати шифри за допомогою методів грубої сили. Нові алгоритми машинного навчання можуть використовуватися для розробки більш ефективних методів дешифрування. Зловмисники можуть використовувати штучний інтелект для збору та аналізу даних про користувачів та системи, щоб знаходити слабкі місця в системах шифрування. Важливо розробляти методи захисту даних, які стійкі до атак з боку штучного інтелекту.

Зв'язківець супротивника про дешифрування AES-256 українськими підрозділами РЕР. Переклад-цитуювання: “Публікую з дозволу командира: Через колег з інтелектуальних підрозділів наших силових відомств було отримано таблиці частот, які противник слухає. ... І найголовніше: противник має доступ до семантики шляхом Дешифрації AES-256. Якщо раніше інформація про те, що AES-256 можливо дешифрувати в адекватні терміни була тільки непрямою, тепер отримано підтвердження. ЗСУ (змінено) мають дані підрозділів, які працювали на

станціях: Motorola, Kirisun, Hytera, Lira, Комбат. Найцікавіше, що одна з частот у цьому списку була в роботі один раз і дуже нетривалий час, незважаючи на це супротивник отримав достатню кількість зразків сигналу і за термін менше ніж тиждень зумів розкрити ключ.”



Рисунок 1.6 – Скріншот коментарів досягнень сил РЕБ ЗСУ зв’язківцем зі сторони ВС РФ

Тому не слід нехтувати впровадженню та розвитку шифрування. Використання власних та закритих шифрів допомагає збільшувати шанси на те, що конфіденційна інформація буде розкрита ще до того як її власник дізнається про її розкриття або витік.

1.7 Завдання до дипломного проекту

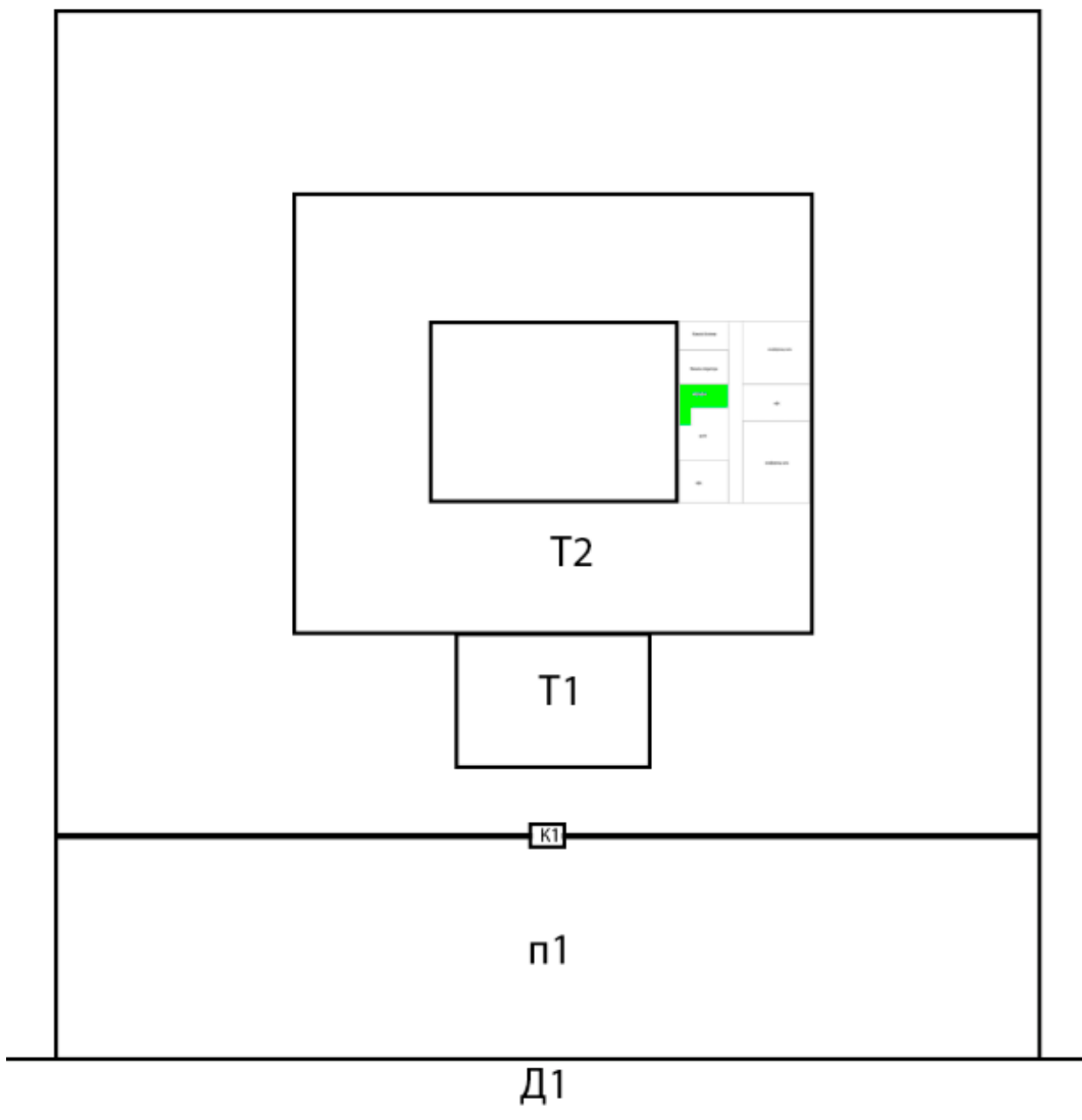
У процесі виконання дипломного проекту необхідно спроектувати план серверного приміщення. Це завдання є критично важливим, оскільки серверне приміщення є однією з ключових частин інформаційної інфраструктури будь-якої організації. Воно містить всі ключові компоненти, такі як сервери, мережеве обладнання, системи зберігання даних та інші важливі пристрої, що забезпечують функціонування ІТ АС. При проектуванні системи захисту інформації серверного приміщення передбачається використання сучасних методів захисту інформації, впровадження політик щодо використання інформаційних ресурсів, та використання мобільних пристроїв. щоб забезпечити надійну охорону даних від витоку, несанкціонованого доступу та інших загроз які можуть виникнути у будь-який час роботи. Тому проектування серверного приміщення повинно враховувати всі аспекти безпеки та стабільності. Для того щоб спроектувати СЗІ серверного приміщення необхідно виконати наступні дії:

- розробка комплексу заходів протидії витоку на фізичному рівні;
- розробка комплексу заходів протидії витоку на технічному рівні;
- створити перелік рекомендацій для підтримки мінімізації витоку через КВІ;
- зробити загальні висновки що до створеного проекту СЗІ.

Ці дії є базовими необхідностями для забезпечення стабільності та захищеності інформації. Проектування та впровадження СЗІ сприяє підвищенню рівня захищеності інформаційних ресурсів підприємства, забезпечуючи безперебійну роботу критично важливих систем та збереження конфіденційної інформації.

2 РОЗРОБКА СЗІ СЕРВЕРНОГО ПРИМІЩЕННЯ

2.1 Основні відомості про об'єкт в якому знаходиться серверна кімната



Д1 (дорожнє полотно); П1 (Паркувальна зона);

К1 (КПП); Т1 (Будівля 1); Т2 (Будівля 2);

Серверна кімната.

Рисунок 2.1 – Загальний вигляд зони будівель.

Загальний рівень доступу проходить у наступні етапи. Між переходами з T1 до T2 також існує внутрішній КПП. Обладнання для резервного живлення має загальне підключення, і тому серверна кімната не має необхідності у доповненій системи аварійного живлення так як вона вже йде по лінії безперервного живлення. Серверна кімната розміщена на 4-му поверсі.

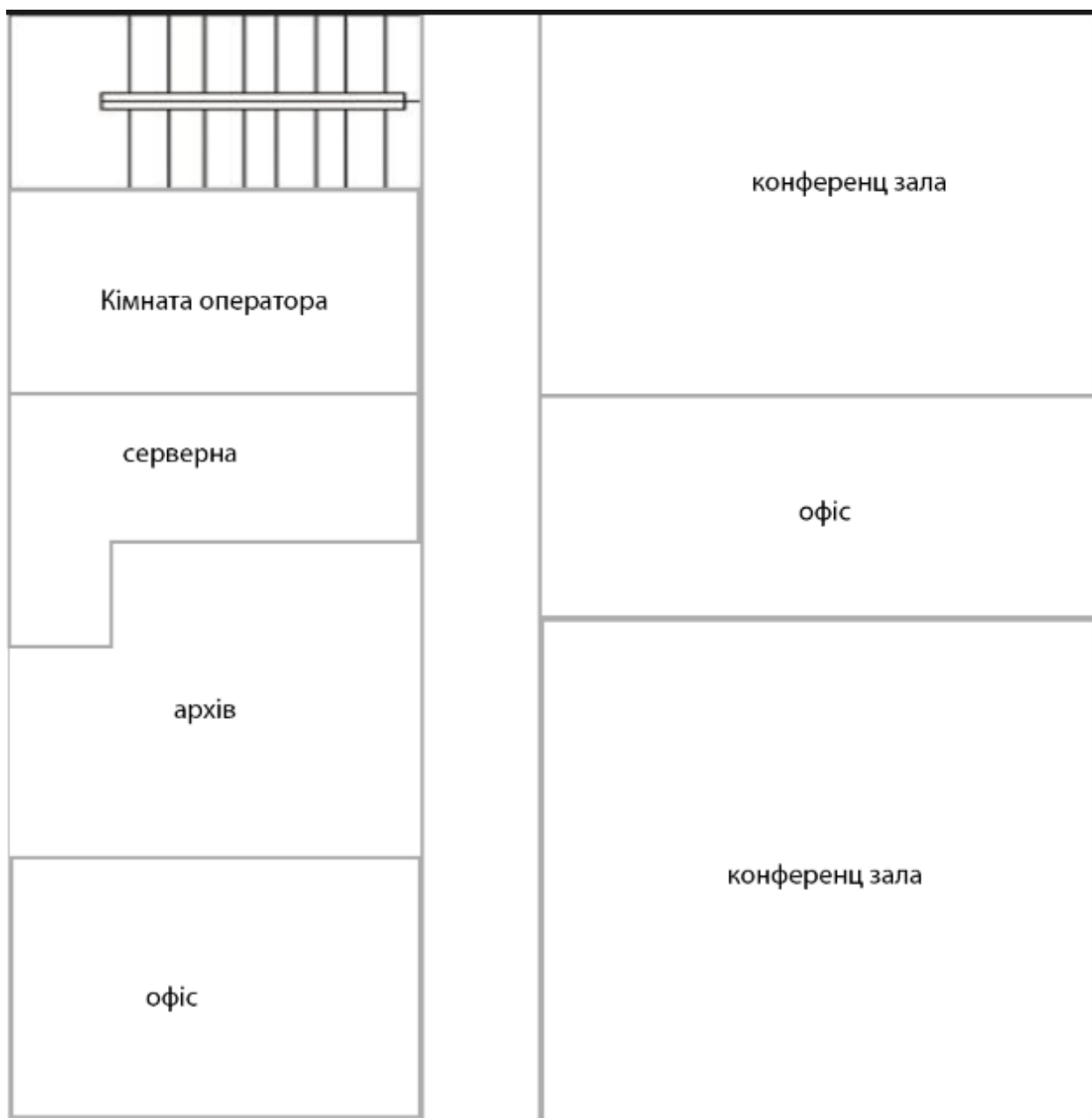


Рисунок 2.2 – Вигляд відносно інших кімнат

2.2 Відомості про приміщення

Загальні відомості про кімнату:

- 2 серверні шафи;
- 1 кондиціонер;
- 1 камера відео спостереження;
- 1 робочий стіл.

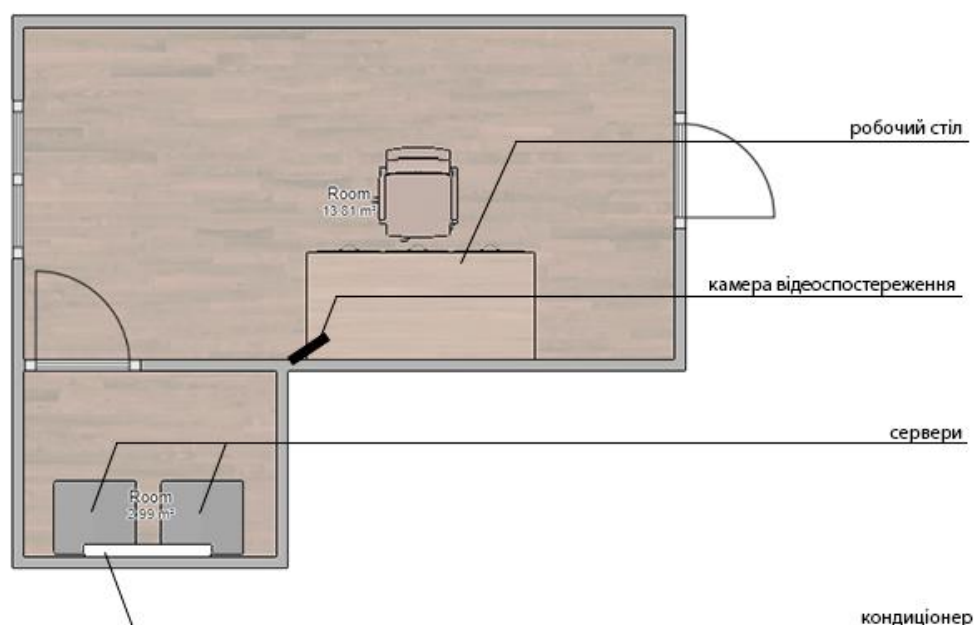
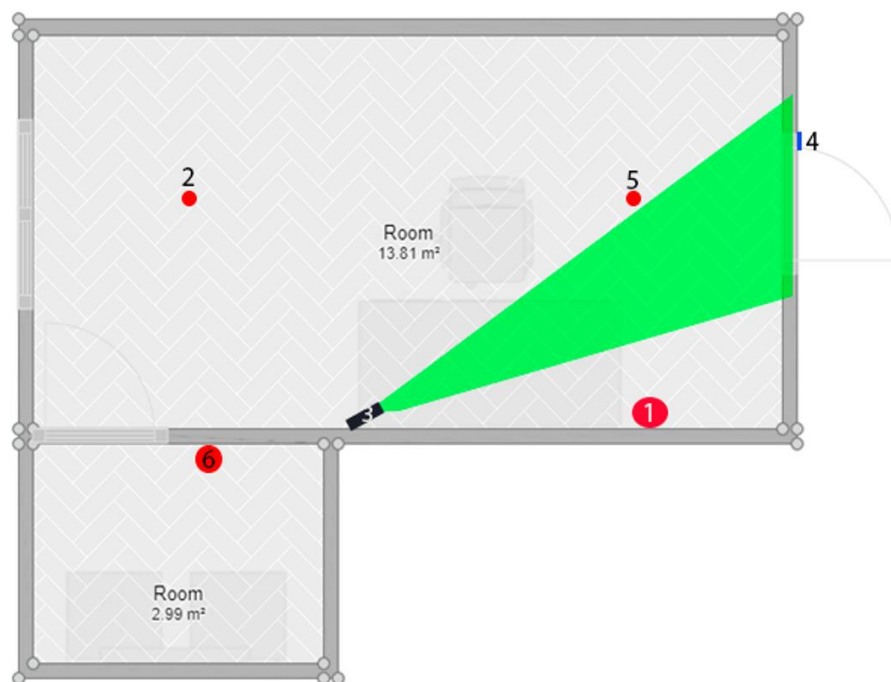


Рисунок 2.3 – Серверна кімната

Доступ до серверного приміщення. Було вирішено зробити обмежений фізичний доступ до серверного приміщення. Для цього було обрано системи контролю доступу, такі як біометричні сканери відбитку пальця (4), система відеоспостереження (3), системи вогнезахисту (2, 5) та вогнегасник порошкового типу (1), система CO2 (6) була обрана як найкращий метод для знешкодження полум'я через те, що кімната герметизується. Мобільні пристрої заборонено

проносити вище 2-го поверху об'єкту, тому що телефон у першу чергу радіо-пристрій який у свою чергу, може бути радіозакладкою.



- 1– вогнегасник порошкового типу; 2, 5 – системи вогнезахисту; 3 – система відеоспостереження; 4 – біометричні сканери відбитку пальця;
6 – система CO2.

Рисунок 2.4 – Безпека приміщення

До серверної кімнати мають доступ адміністратор першої, другої та третьої зміни, у робочий та післяробочий час. Прохід та відчинення кімнати досягається завдяки ключу, та сканеру відбитку пальців за для захисту від НСД. Використання в якості захисної системи від зчитування інформації через вікна було обрано зеркальну плівку яку наклеюють на зовнішню сторону вікна направлену на вулицю, але це має один недолік - це одноразове застосування. Зеркальні плівки можуть бути ефективними лише при денному світлі. У вечірні чи нічні години, коли в освітленні приміщення буде більше світла, вони можуть втратити свою ефективність, тому в якості активної системи захисту було обрано електрохромне скло. Це спеціальний тип скла, який може змінювати свою прозорість від прозорого до непрозорого за допомогою електричного струму. Це досягається

завдяки спеціальному покриттю скла, яке містить електромагнітні компоненти, здатні реагувати на електричний струм.

Камера відеоспостереження (3) розташована таким чином, щоб не мати візуального доступу до робочого столу адміністратора де може бути ІзОД, але мати візуальний доступ до дверей. Робітникам дозволено використовувати тільки провідні периферійні пристрої. Монітор повинен бути повернутий відносно стіни в сторону дверей, щоб уникнути небажаного показу інформації на екрані двері повинні бути завжди зачинені та відчинятись тільки після ховання секретної інформації.

Внутрішня частина кімнати з серверами оброблена вогнетривким бетоном та використано мідну сітку у якості екранувального матеріалу стін, стелі, та полу кімнати. У приміщенні весь час знаходиться обслуговуючий персонал, тому у разі виникнення пожежі у кімнаті з серверами у першу чергу ввімкнеться тривога, у персоналу буде 10 секунд щоб натиснути кнопку затримки, яка дасть час до запуску системи CO₂, системний адміністратор повинен натиснути кнопку хвилинної затримки, яка надасть можливість підбігти персоналу, оцінити рівень небезпеки, та у випадку необхідності використати вогнегасник. Оператор також може відключити систему CO₂ якщо у випадку пожежі її використання недоцільне, або у неї немає потреби у даній ситуації. У випадку якщо персонал буде відсутній, через 10 секунд після вмикання сирени зачиняться двері кімнати з серверами, та запусниться система CO₂.

Контроль навколишнього середовища:

Червоний – герметизаційний модуль для спліт системи, у разі пожежі він перекриє можливість проходження повітря по спліт системі для збільшення її ефективності;

- помаранчевий – система електронадходження;
- синій – система пожежної безпеки;
- блакитний – спліт система;
- фіолетовий – лінія LAN;
- жовтий – система опалення.

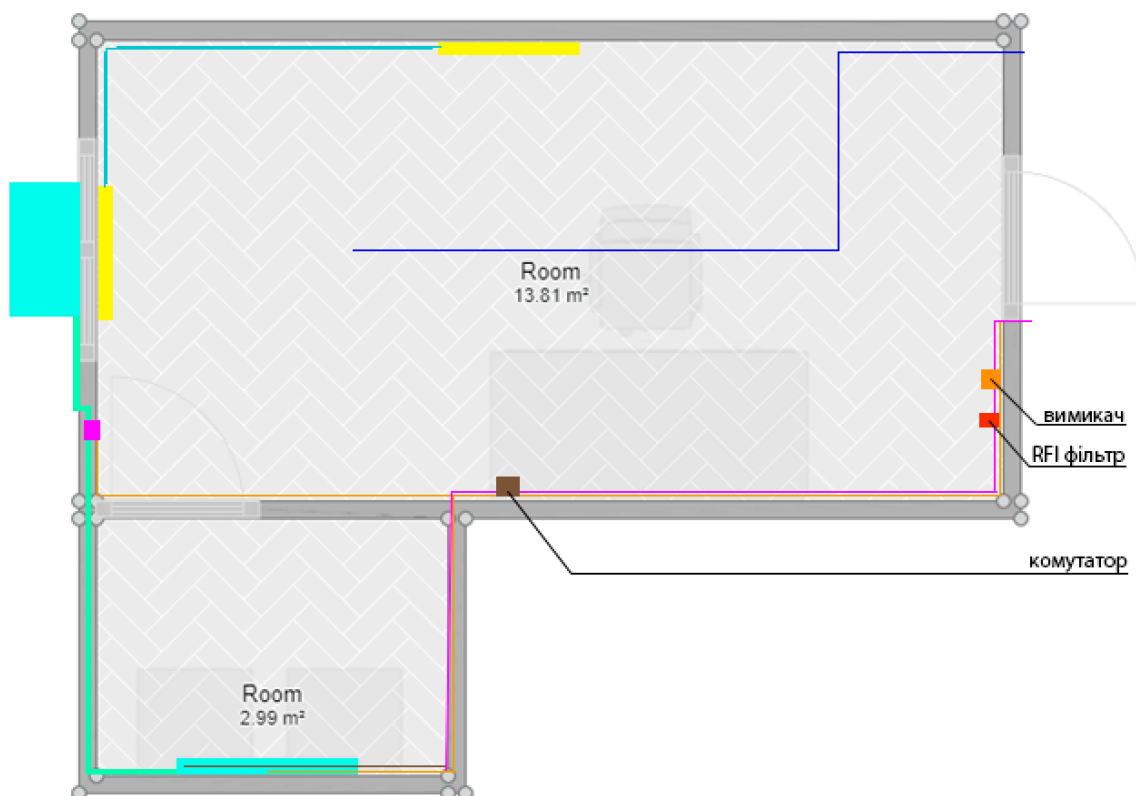


Рисунок 2.5 – Системи інженерних мереж

На рисунку також зображено комутатор який об'єднує дві LAN лінії від серверів в одну. Також слід зазначити що починаючи від комутатора і у напрямку двері та подальшому розгалуженні використовуються екранувальні матеріали (обплетення з фольги) та фільтри (RFI, вимикач), щоб зменшити електромагнітне випромінювання і сприяти максимальній ізоляції сигналів.

Розглянемо математичний приклад ефективності екранування. Відповідно до [8] основними під час екранування треба враховувати наступні фізичні явища, які відбуваються під час екранування алюмінієвим матеріалом або сталевим:

- загасання за рахунок відбиття;
- поглинаюче загасання;
- загасання спричинене багаторазовим відбиттям.

Загасання за рахунок відбиття є явищем у фізиці, зокрема в оптиці та радіофізиці, коли інтенсивність електромагнітної хвилі зменшується внаслідок відбиття від поверхонь або перешкод. Коли хвиля досягає межі двох середовищ з

різними характеристиками, частина її енергії може бути відбита назад в перше середовище, а інша частина може пройти через межу і продовжувати поширюватися в другому середовищі. Формулу можемо схарактеризувати наступним чином

$$R = 20 * \log \left| \frac{Z_0 + Z_M}{2Z_2} * \frac{Z_0 + Z_M}{2Z_0} \right| [\text{дБ}] \quad (2.1)$$

де Z_0 - імпеданс середовища (діелектрик);

Z_M - імпеданс матеріалу.

Поглинаюче загасання - це процес зменшення інтенсивності електромагнітної хвилі, коли вона проходить через матеріал, який поглинає частину її енергії. Її формула виглядає наступним чином

$$A = 20 * \log e^{\frac{\tau}{\delta}} [\text{дБ}] \quad (2.2)$$

$$\delta = \sqrt{\frac{2}{\omega \mu \sigma}} \quad (2.3)$$

де τ – товщина матеріалу;

δ - глибина проникнення;

σ – питома провідність, для алюмінію має значення $3.56e+007$ См/м і $6.993e+006$ См/м для сталі;

μ - магнітна проникність, яка має значення $4\pi * 10^{-7}$ Гн/м ;

ω - кругова частота хвиль, яка вираховується за допомогою $2\pi * f$.

Розрахуємо приклад, нехай маємо екрановану кімнату з алюмінієвими стінами товщиною 2 мм. В якості джерела було використано сигнал частотою 5 ГГц.

Отже базуючись на формулі (2.3), кругова частота хвиль $\omega = 2\pi * (5 * 10^9)$ та товщина матеріалу $t = 2 * 10^{-3}$ м.

$$\omega = 3.142 * 10^{10}$$

$$\mu = 1.257 * 10^{-6}$$

$$\sigma = 3.904 * 10^3$$

$$\delta = \sqrt{\frac{2}{(3.142*10^{10})*(1.257*10^{-6})*(3.904*10^3)}} = 1.139*10^{-4} \text{ м}$$

В результаті отримаємо що $\delta = 1.139*10^{-4}$ м, а повний розрахунок поглинаючого загасання має наступний вигляд

$$A = 20 * \log e^{\frac{2*10^{-3}}{1.139*10^{-4}}} = 152.498 \text{ [дБ]}$$

Загасання спричинене багаторазовим відбиттям, є явищем, при якому сигнал втрачає свою потужність або інтенсивність через численні відбиття від різних поверхонь або об'єктів на своєму шляху. Формула цього загасання має наступний вигляд

$$M = 20 * \log \left| 1 - \left(\frac{Z_0 - Z_M}{Z_0 + Z_M} \right)^2 * e^{-\frac{2\tau}{\delta}} * e^{-j\frac{2\tau}{\delta}} \right| \text{ [дБ]}$$

де Z_0 - імпеданс середовища (діелектрик);

Z_M - імпеданс матеріалу;

δ - глибина проникнення.

З технічної точки зору, базуючись на результатах експериментів [8], показано що при екрануванні алюмінієвим листом товщиною 1мм, ефективність екранування склала 80 дБ в широкому частотному діапазоні.

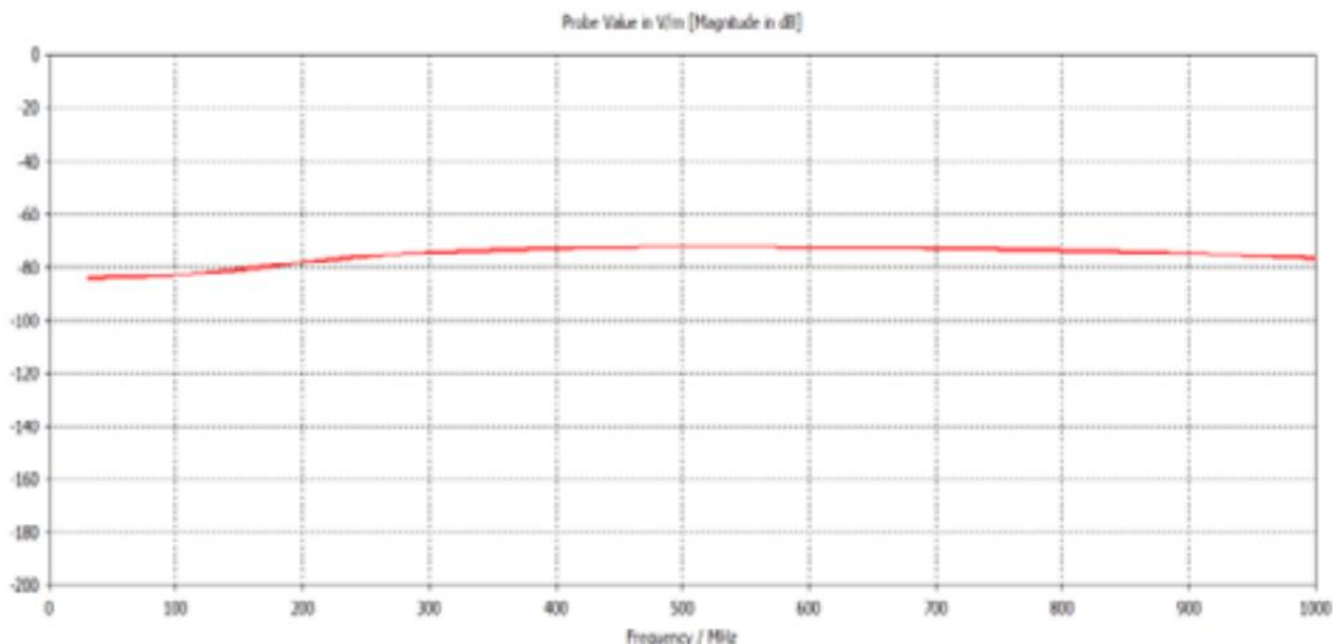


Рисунок 2.6 – Ефективність екранування алюмінієвим матеріалом [8]

А при екрануванні об'єкту металевим матеріалом, ефективність екранування була 200 дБ в широкому частотному діапазоні.

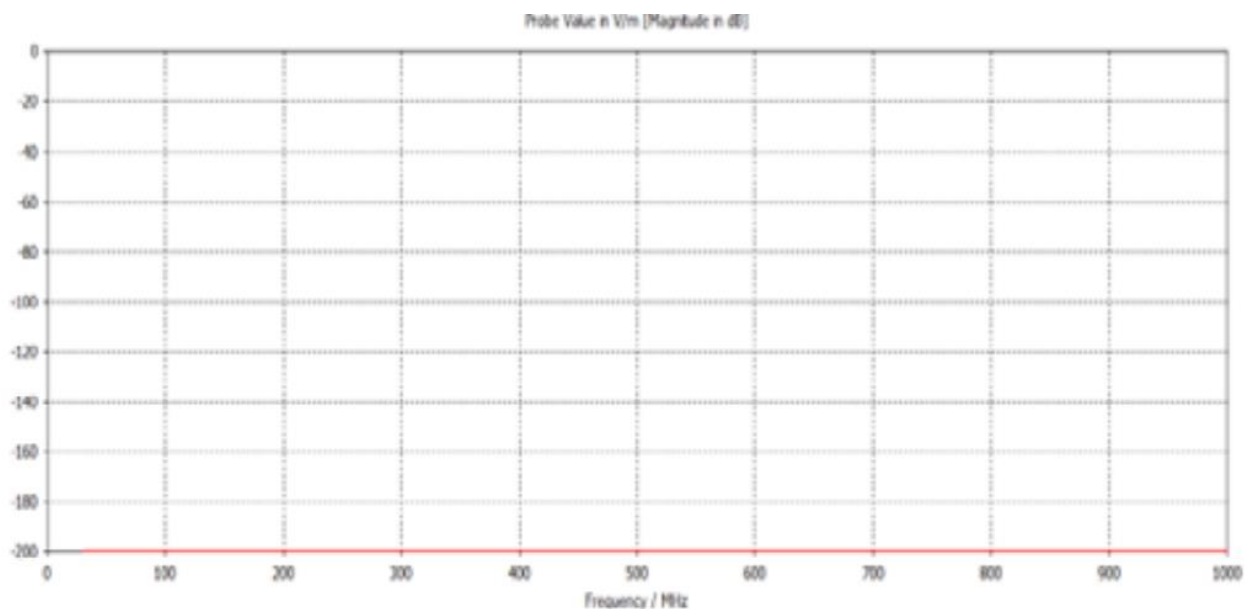


Рисунок 2.7 – Ефективність екранування сталевим матеріалом [8]

Це показує що використання алюмінієвих та сталевих матеріалів дуже добре екранує поверхні, які необхідно захистити, або максимально мінімізувати вплив від ПЕМВіН.

Точки заземлення у великій кімнаті:

- Верхній лівий кут;
- Верхній правий кут;
- Нижній лівий кут;
- Нижній правий кут.

Точки заземлення у меншій кімнаті :

- Верхній лівий кут;
- Верхній правий кут.

Схема розташування заземлення:

- централізована заземлююча шина. Розміщено біля вимикача та RFI фільтра біля комутатора, щоб зручно об'єднати всі заземлюючі провідники.

Основний заземлюючий контур:

- прокладений провідник від централізованої заземлюючої шини до основного заземлюючого контуру будівлі (найближча точка входу у заземлюючий контур).

Вибір місць розташування заземлюючих точок та централізованої заземлюючої шини обґрунтований кількома ключовими принципами:

- ефективність заземлення. Розташування заземлюючих точок у кожному куті кімнат забезпечує рівномірний розподіл заземлюючих провідників, що зменшує ризик виникнення зон з високим потенціалом. Центральне розташування заземлюючої шини дозволяє зменшити довжину заземлюючих провідників, що знижує опір заземлюючої системи і забезпечує кращу ефективність;

- зручність обслуговування. Розміщення централізованої заземлюючої шини поблизу вимикача та RFI фільтра спрощує доступ для технічного обслуговування та перевірки системи. Всі заземлюючі провідники зібрані в одному місці, що полегшує контроль та тестування;

- механічна стійкість. Кути кімнат є найбільш захищеними від механічних пошкоджень місцями. Це знижує ризик пошкодження заземлюючих провідників під час експлуатації приміщення. Використання куточків також мінімізує перешкоди для обслуговуючого персоналу;

- електрична ізоляція. Використання куточків для заземлення зменшує ризик електричних перешкод і забезпечує стабільність електричного потенціалу у всій мідній сітці. Заземлюючі провідники, прокладені вздовж стін, захищені від випадкових пошкоджень і впливу електромагнітних завад.

- безпека персоналу. Центральне розташування заземлюючої шини та точок заземлення зменшує ризик виникнення небезпечних ситуацій для обслуговуючого персоналу. Це забезпечує легкий доступ до основних компонентів системи заземлення в разі необхідності швидкого відключення чи перевірки.

Таким чином, у вас буде ефективна та надійна система заземлення для сталевих листів в кімнаті з серверами, що забезпечить електробезпеку та захист від електромагнітних завад.

Серверні кабелі мають лише локальний (без доступу до інтернет-мережі) характер, це зменшує можливість виникнення атак мережевого формату як, наприклад, атака на відмову в обслуговуванні. Для захисту від небажаних ситуацій з системами живлення такі як, наприклад, стрибки, або спади напруги було вирішено використати вимикач з необхідними для цього фільтрами, та мережевий RFI фільтр для блокування небажаного впливу височастотного шуму, який може виникати від різноманітних джерел. Відповідно до військового стану, безперебійники з батареєю повинні відповідати вимогам стійкості до електромагнітних перешкод, міцності та надійності в умовах екстремального навантаження та впливу шкідливих факторів. У воєнному середовищі, де можуть бути періодичні перебої у живленні або можливість ворожого втручання у електромережі, безперебійні живлення стають важливим засобом забезпечення неперервності роботи комунікаційних систем, важливих електронних приладів та систем безпеки. Вони забезпечують стабільне живлення, навіть у випадку великих напруг, технічних неполадок чи втрати електромережі. Безперебійники з батареєю

відіграють також критичну роль у забезпеченні безпеки та надійності важливих інформаційних систем в умовах, де можуть виникнути технічні або ворожі загрози як наприклад вихід з ладу систем резервного живлення через пошкодження. Вони є невід'ємною частиною воєнного обладнання та інфраструктури, що забезпечує стійкість та надійність функціонування систем у будь-яких умовах.

З технічної точки зору не слід виключати засоби РЕБ які можуть бути ефективним методом захисту серверної кімнати від незаконного перехоплення інформації та забезпечення безпеки даних. Ось кілька способів використання РЕБ для захисту серверної кімнати:

- блокування радіосигналів. РЕБ може бути використаний для блокування радіосигналів, які використовуються для бездротового зв'язку або спілкування між пристроями. Це може включати Wi-Fi, Bluetooth, GSM, GPS та інші радіочастотні технології. Блокування цих сигналів унеможливить зловмисникам використовувати бездротові пристрої для несанкціонованого доступу до серверної кімнати. РЕБ може бути використаний для захисту серверної кімнати шляхом блокування радіосигналів, що можуть бути використані для вибухів або інших атак фізичної безпеки;

- захист від шпигунського знаряддя. РЕБ може бути ефективним захистом від шпигунського знаряддя, такого як безпілотні літальні апарати (дрони), які можуть бути використані для зйомки або перехоплення конфіденційної інформації з серверної кімнати.

Для блокування основних типів бездротового зв'язку для серверної кімнати рекомендовано використовувати радіочастотний блокуючий пристрій, який здатний блокувати різні типи сигналів. Основні типи бездротового зв'язку, які потрібно блокувати, включають WiFi, Bluetooth, GSM (мобільний зв'язок), 3G, 4G і 5G.

Для цього можна використовувати радіочастотний блокуючий пристрій, який працює на відповідних частотах для кожного типу зв'язку:

- WiFi: Частоти 2,4 ГГц і 5 ГГц;
- Bluetooth: Частота 2,4 ГГц;

- GSM, 3G, 4G: Частоти, що залежать від регіону, але зазвичай в діапазоні 800 МГц - 2,6 ГГц;

- 5G: Частоти 600 МГц - 6 ГГц (включаючи 3,5 ГГц, 5 ГГц і вище).

Радіочастотний блокуючий пристрій повинен мати можливість перехоплення сигналів на цих частотах і блокування їх, щоб забезпечити безпеку в серверній кімнаті. Важливо також врахувати, що використання радіочастотних блокуючих пристроїв може вимагати дозволу або ліцензії в деяких країнах, тому важливо перевірити місцеві правила і регуляції.

Зазвичай для цегляної стінки коефіцієнт затухання може бути приблизно в діапазоні 5 дБ на кожні 25 см стіни, тобто якщо у нас умовно стіна 50 см в товщину та сигнал з потужністю 40 дБ, то ми маємо наступні розрахунки

$$40 \text{ дБ} - 10 \text{ дБ} = 30 \text{ дБ}$$

Отже, загальне затухання сигналу через цегляну стінку для заданих умов дорівнює 30 дБ.

Для спліт-систем обрано прецизійний промисловий кондиціонер, поліетиленові труби з встановленням спеціальних водовідштовхувальних манжетів на точки сполучення труб для мінімізації можливості створення конденсації та максимального уникнення витоку інформації через віброакустичний канал.

У якості системи опалення було вирішено використовувати ізольовану систему опалення з використанням батарей та труб з можливістю електронагріву та насосної циркуляції, у якості труб було вирішено використовувати пластикові труби, усі ці фактори мінімізують наступні небезпеки :

- витік інформації через об'єднану систему опалення акустичним каналом;
- затоплення приміщення через вихід з ладу труб або системи циркуляції рідини.

Також на кожну батарею було повішено кожух з мідної сітки яка не тільки використовується в якості екранування, але й ще дуже добре проводить тепло що

відносно інших засобів екранування мінімально впливає на ефективність опалення приміщення та підтримки необхідного рівня вологості в приміщенні.

Також для захисту персоналу в ОІД використовуються шумоізоляційні двері, а у випадку кімнати з серверами ще й можливістю герметизації приміщення, що дозволяє більш комфортно працювати персоналу та у випадку пожежі більш ефективно зупиняти полум'я. Шумові характеристики повнорозмірних серверних шаф можуть значно відрізнятися в залежності від моделі, виробника та конкретних характеристик обладнання в середині. Типово повнорозмірний серверний шкаф може виділяти високий рівень шуму, залежно від обладнання та режиму його роботи що може згубно позначитися на стані працівників.

2.3 Програмний захист серверів

Програмний захист включає захист даних на серверах і під час передачі за допомогою шифрування. Використання SSL/TLS [16. TLS/SSL] для захисту мережевого трафіку та антивіруси для усунення вразливостей безпеки. Та найголовніше - власний дистрибутив операційної системи, у нашому випадку це Лінукс. Для доступу до файлової системи було обрано Kerberos як надійний метод захисту та розгалуження доступу до серверу. Kerberos - це протокол мережевої аутентифікації, який дозволяє користувачам отримати доступ до різних ресурсів мережі, таких як файли, принтери та інші служби, без необхідності повторно вводити свій пароль. Принцип роботи Kerberos базується на використанні зашифрованих "квитків", які підтверджують ідентифікацію користувача.



Рисунок 2.8 – Схема роботи протоколу Kerberos

Основні складові Kerberos:

- клієнт. Користувач, який намагається отримати доступ до мережевого ресурсу;
- служба. Ресурс (наприклад, файловий сервер або додаток), до якого користувач намагається отримати доступ;
- Центр автентифікації (KDC): Центральний сервер, який використовується для автентифікації користувачів та видачі квитків. KDC складається з двох компонентів;
 - Служба авторизації (AS): Перший крок автентифікації. Клієнти звертаються до AS для отримання тимчасового квитка автентифікації (TGT);
 - Служба квитків (TGS): Клієнти використовують TGT для отримання квитка доступу до конкретної служби. Токен автентифікації (Ticket): Зашифрований об'єкт, який використовується для підтвердження ідентичності користувача перед отриманням доступу до мережевого ресурсу;

Процес роботи Kerberos може бути узагальнений наступним чином, користувач намагається отримати доступ до мережевого ресурсу та відправляє

запит до AS для отримання TGT. AS перевіряє ідентичність користувача, створює TGT та відправляє його користувачеві. Після отримання TGT, користувач відправляє запит до TGS для отримання квитка доступу до конкретної служби. TGS перевіряє TGT, створює квиток доступу та відправляє його користувачеві. Користувач використовує квиток доступу для отримання доступу до мережевого ресурсу. Квитки автоматично оновлюються або видаляються після закінчення строку дії. Основна перевага Kerberos полягає в тому, що він дозволяє уникнути передачі паролю через мережу, що робить його більш безпечним для автентифікації користувачів у розподілених середовищах.

У якості каналу передачі даних було використано VPN для безпечного з'єднання з серверами. Також базовим принципом безпеки серверів вважається у першу чергу заміна порту SSH (22), через який відбувається віддалене адміністрування, на інший та перекривання усіх інших невикористовуваних портів. Тестування безпеки проводити тільки з використанням “снэпшоту” програмного середовища, застарілих та відсутності секретних даних.

Використання принципу найменших привілеїв (Least Privilege Principle). Це означає, що кожен користувач, або програма має мати доступ лише до тих ресурсів і функцій, які необхідні для виконання їхніх завдань. Воно дозволяє обмежити можливість атак та зменшити ризик витоку даних або компрометації системи. Використання системи виявлення та запобігання вторгнень (Intrusion Detection and Prevention System, IDPS). IDPS дозволяє виявляти та реагувати на спроби несанкціонованого доступу до системи або аномальну активність, таку як атаки ззовні чи внутрішні порушення безпеки. Це може включати моніторинг мережевого трафіку, аналіз системних журналів та виявлення змін у конфігураціях системи.

Інше рішення для розподілу ієрархії доступу користувачів до інформації в системі - це використання системи контролю доступу на рівні файлової системи. Наприклад, використання Access Control Lists (ACLs) для точного контролю доступу до файлів і каталогів на сервері. Це дозволяє налаштувати деталізовані правила доступу для кожного користувача або групи користувачів, забезпечуючи

потрібний рівень безпеки. Використання веб-застосункових брандмауерів (WAF) допомагає захистити веб-додатки від різноманітних атак, включаючи SQL-ін'єкції, крос-сайт скриптинг (XSS), крадіжки сесій та інші вразливості. Ці інструменти працюють на рівні веб-проксі, аналізуючи HTTP-запити та відповіді, щоб виявляти та блокувати потенційно шкідливий трафік. Вони можуть фільтрувати вхідні дані, перевіряти їх на відповідність заздалегідь визначеним шаблонам та правилам безпеки, а також блокувати атаки в реальному часі. Більше того, WAF може забезпечувати контроль доступу до веб-додатків, обмежуючи права доступу користувачів на основі їхніх ролей та привілеїв. Це дозволяє захистити конфіденційні дані, запобігти несанкціонованому доступу та забезпечити виконання вимог регуляторів у сфері безпеки даних. Крім того, за допомогою аналізу великих обсягів трафіку WAF може виявляти аномальні або підозрілі дії, що допомагає у виявленні інцидентів безпеки та вчасному реагуванні на них. Таким чином, використання WAF є важливою складовою стратегії безпеки веб-додатків та дозволяє підвищити рівень захищеності та надійності веб-сервісів. Для захисту від витоку конфіденційної інформації використовують DLP (Data Loss Prevention) системи - це комплексні рішення, спрямовані на запобігання втраті конфіденційної інформації в організації. Основна мета DLP систем полягає в ідентифікації, моніторингу та контролі за потоками даних у всій організації, що дозволяє уникнути непередбачених витоків даних.

Основні функції DLP систем включають:

- ідентифікація конфіденційної інформації: DLP системи визначають чутливі дані, такі як особиста інформація клієнтів, фінансові дані, інтелектуальна власність тощо;
- моніторинг потоків даних: DLP системи встановлюють контроль за потоками даних у всіх точках організації, включаючи мережевий трафік, електронну пошту, файли на серверах тощо;
- блокування або зашифрування даних: При виявленні конфіденційної інформації, DLP системи можуть блокувати її передачу, зашифровувати або

використовувати інші методи захисту для запобігання неправомірному доступу до даних;

- попередження про порушення політик безпеки: DLP системи можуть генерувати сповіщення та повідомлення про порушення внутрішніх політик безпеки, дозволяючи адміністраторам вчасно реагувати на можливі загрози;

- аналіз та звітність: DLP системи надають можливість аналізувати потоки даних, виявляти тенденції та патерни втрати даних, а також створювати звіти для внутрішнього аудиту та виконання регуляторних вимог;

Застосування DLP систем дозволяє підвищити рівень безпеки організації, запобігти фінансовим втратам, зберегти репутацію компанії та виконувати вимоги законодавства щодо захисту персональних даних і конфіденційної інформації. Також великим значенням є програмна оптимізація на випадок необхідності негайного вимкнення серверу у випадку дронової або ракетної небезпеки, тому що у випадку початку роботи РЕБ, яке потенційно може буди розташоване поблизу ОІД, може викликати програмний збій в роботі пристрою.

Окрім стандартного шифрування протоколом Нідгема — Шредера яке використовує Kerberos, є необхідність, згідно з статтею 8 в ЗУ «Про захист інформації в інформаційно-комунікаційних системах» яка вимагає використання державно сертифікованих або розроблених в державі засобів шифрування для захисту інформації.

2.4 Основні рекомендації мінімізування впливу вразливостей

Згідно з останніми тенденціями у світі, більшість компанії починають віддавати перевагу фахівцям «червоної команди», тому у близькій перспективі весь прогрес прийде до переваги фахівців цього напрямку для тестування програмної безпеки на відповідність актуальності системи безпеки. Рекомендовано проводити

регулярні тестування особового персоналу на предмет актуальності знань та проводити необхідне навчання за для покращення освіти.

Слідкувати за останніми технологічними розробками та вдосконалювати системи захисту відповідно до змін у загрозах. Згідно з цим проводити регулярне тестування захисту від ПЕМВіН для перевірки ефективності заходів та виявлення нових вразливостей.

Використовувати за можливості пропрієтарні роз'єми для периферійних пристроїв та критичних кабелів живлення та передачі інформації, та ні в якому разі не використовувати периферію з посередковим підключенням.

Використовувати тільки ліцензійне ПЗ або ПЗ власного виробництва.

Регулярно створювати резервні копії даних в ІТС і перевіряти їх відновлення. Це забезпечить можливість відновлення інформації у випадку спроби фізичного знищення або пошкодження в моменти НСД.

Проводити систематичні аудити безпеки, виявляти та виправляти можливі вразливості та аномалії в ІТ АС. РСО має мати політики безпеки інформації для всього персоналу для захисту від НСД.

Таким чином можна мінімізувати явища витоку інформації у серверному приміщенні.

ВИСНОВКИ

У даному дипломному проєкті було проведено детальне проектування комплексної системи захисту інформації для серверного приміщення режимного підприємства. Було розглянуто загальні відомості про серверну кімнату, включаючи наявне обладнання та розташування. Для забезпечення фізичного захисту приміщення було запропоновано комплекс заходів, таких як: система контролю доступу з біометричними сканерами відбитків пальців, відеоспостереження, вогнезахисні системи та система гасіння пожежі на основі CO₂. Також було передбачено екранування стін, стелі та підлоги за допомогою мідної сітки для захисту від витоку інформації через електромагнітні канали. Крім того, було наголошено на важливості регулярного тестування безпеки, навчання персоналу, використання ліцензійного програмного забезпечення, створення резервних копій даних та проведення аудитів безпеки.

Таким чином, запропонований комплекс заходів забезпечить всебічний захист інформації в серверному приміщенні, мінімізуючи ризики витоку даних через фізичні, програмні та організаційні канали витоку інформації. Дотримання цих рекомендацій допоможе підприємству підвищити рівень інформаційної безпеки та захистити свої конфіденційні дані та критичну інфраструктуру.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Про захист інформації в інформаційно-телекомунікаційних системах [Електронний ресурс] : Закон України від 05.07.1994 р. № 80/94-ВР : станом на 4 квіт. 2024 р. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/80/94-vr#Text> (дата звернення: 07.06.2024). – Назва з екрана.

2. Збірник наукових праць ВІТІ [Електронний ресурс]: Збірник наукових праць Військового інституту телекомунікацій та інформатизації / гол. ред. А.О. Свида. – К.: ВІТІ, 2013. – Вип. 2. – Режим доступу: https://www.viti.edu.ua/files/zbk/2013/8_2_2013.pdf. (дата звернення: 14.04.2024). – Назва з екрана.

3. Учасники проєктів Вікімедіа. Канали витоку інформації – Вікіпедія [Електронний ресурс] / Учасники проєктів Вікімедіа // Вікіпедія. – Режим доступу: https://uk.wikipedia.org/wiki/Канали_витоку_інформації (дата звернення: 19.04.2024). – Назва з екрана.

4. Data integrity // Wikipedia. – Режим доступу: https://en.wikipedia.org/wiki/Data_integrity (дата звернення: 07.06.2024).

5. Про затвердження Порядку підключення об'єктів телекомунікацій до системи фіксації показників обсягу трафіка [Електронний ресурс]: Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України: [прийнятий 29 листопада 2013 р. № 215: станом на 29 листопада 2013 р.]. – Режим доступу: <https://zakon.rada.gov.ua/rada/show/v0215519-13#Text>

6. The Difference Between Red, Blue, and Purple Teams. Unsupervised Learning. Режим доступу: <https://danielmiessler.com/p/red-blue-purple-teams/> (дата звернення: 20.04.2024). – Назва з екрана.

7. Operating system privilege rings in most modern hardware platforms and operating systems // ResearchGate. – Режим доступу: https://www.researchgate.net/figure/Operating-system-privilege-rings-in-most-modern-hardware-platforms-and-operating-systems_fig1_339759698 (дата звернення: 07.06.2024).

8. Kovar S., Valouch J., Urbancokova H. Calculation of Shielding Effectiveness of Materials for Security Devices. // MATEC Web of Conferences. – 2017. – Vol. 125. – Режим доступу: <https://www.matec->

conferences.org/articles/matecconf/pdf/2017/39/matecconf_csc2017_02036.pdf (дата звернення: 24.04.2024).

9. 7 types of information leaks and how to prevent them // Agility PR Solutions. – Режим доступу: <https://www.agilitypr.com/pr-news/public-relations/7-types-of-information-leaks-and-how-to-prevent-them/> (date of access: 26.04.2024).

10. Contributors to Wikimedia projects. Electromagnetic warfare - Wikipedia [Електронний ресурс] / Contributors to Wikimedia projects // Wikipedia, the free encyclopedia. – [Б. м.], 2002. – Режим доступу: https://en.wikipedia.org/wiki/Electromagnetic_warfare (date of access: 01.05.2024). – Назва з екрана.

11. Contributors to Wikimedia projects. ISO/IEC 27001 - Wikipedia [Електронний ресурс] / Contributors to Wikimedia projects // Wikipedia, the free encyclopedia. – [Б. м.], 2013. – Режим доступу: https://en.wikipedia.org/wiki/ISO/IEC_27001 (date of access: 01.05.2024). – Назва з екрана.

12. Staff D. R. NIST Cybersecurity Framework Adoption Hampered By Costs, Survey Finds [Електронний ресурс] / Dark Reading Staff // Dark Reading | Security | Protect The Business. – Режим доступу: <https://www.darkreading.com/cyberattacks-data-breaches/nist-cybersecurity-framework-adoption-hampered-by-costs-survey-finds> (date of access: 09.05.2024). – Назва з екрана.

13. Information security management systems [Електронний ресурс] // European and International Standards | Genorma. – Режим доступу: <https://genorma.com/en/topics/standards-on-cybersecurity/standards/7> (date of access: 20.05.2024). – Назва з екрана.

14. What is a Container? | Docker [Електронний ресурс] // Docker. – Режим доступу: <https://www.docker.com/resources/what-container/> (date of access: 07.06.2024). – Назва з екрана.

15. What is Cybersecurity Risk? Definition & Factors to Consider in 2024 [Електронний ресурс] // SecurityScorecard. – Режим доступу: <https://securityscorecard.com/blog/what-is-cybersecurity-risk-factors-to-consider/> (date of access: 20.05.2024). – Назва з екрана.

16. How to Secure your LAN Network | Tufin [Електронний ресурс] // Tufin. – Режим доступу: <https://www.tufin.com/blog/how-to-secure-your-lan> (date of access: 20.05.2024). – Назва з екрана.