

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи магістра

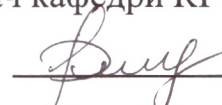
на тему:

«Методи й технології захисту клієнт-серверної мережі організації, побудованої на базі ОС Windows Server»

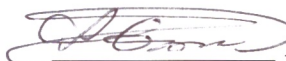
Виконав студент 2-го курсу групи КБм22-1
спеціальності 125 «Кібербезпека»

 І.С. Хімічук

Керівник старший викладач кафедри КІ та КБ

 Є.М. Трокоз

Рецензент завідувач кафедри КІ та КБ, кандидат
технічних наук, доцент

 А.А. Єфіменко

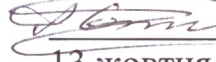
Житомир – 2023

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко
13 жовтня 2023 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Хімічук Ілля Сергійович

Тема роботи: «Методи й технології захисту клієнт-серверної мережі організації, побудованої на базі ОС Windows Server»

затверджена Наказом університету від 13 жовтня 2023 р. № 572/с

Термін здачі студентом закінченої роботи 27 грудня 2023 р.

Вихідні дані роботи:

Предметом дослідження є методи й технології захисту клієнт-серверної мережі організації, побудованої на базі ОС Windows Server.

Об'єктом дослідження є процес захисту клієнт-серверної мережі організації.

Обладнання та програмне забезпечення:

1. Маршрутизатор Cisco 7201
2. Комутатор Cisco Catalyst 2960
3. Операційні системи Cisco IOS, Windows 10, Windows Server 2019

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	О.С. Головня	16.10.2023	16.10.2023
2	О.С. Головня	31.10.2023	31.10.2023
3	О.С. Головня	10.11.2023	10.11.2023

Студент _____ І.С. Хімічук
Керівник _____ Є.М. Трокоз

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	16 жовтня 2023 – 16 жовтня 2023	Виконано
2	Пошук та аналіз інформації стосовно методів захисту клієнт-серверних мереж	27 жовтня 2023 – 1 листопада 2023	Виконано
3	Дослідження принципів побудови мереж організацій та аналіз важливості захисту локальних мереж	3 листопада 2023 – 4 листопада 2023	Виконано
4	Аналіз потенційних загроз та вразливостей	5 листопада 2023 – 7 листопада 2023	Виконано
5	Аналіз методів й технологій захисту клієнт-серверних мереж	9 листопада 2023 – 12 листопада 2023	Виконано
6	Огляд наявного проєкту мережі та аналіз доцільності використаного обладнання	13 листопада 2023 – 14 листопада 2023	Виконано
7	Аналіз моделі загроз та моделі порушника	17 листопада 2023 – 19 листопада 2023	Виконано
8	Складання списку рекомендованих методів та заходів для захисту	21 листопада 2023 – 26 листопада 2023	Виконано
9	Підготовка демонстрації базового налаштування мережі	27 листопада 2023 – 29 листопада 2023	Виконано
10	Складання рекомендацій з розгортання AD на сервері	31 листопада 2023 – 2 грудня 2023	Виконано
11	Написання пояснювальної записки	6 грудня 2023 – 11 грудня 2023	Виконано
12	Підготовка доповіді та презентації	18 грудня 2023 – 22 грудня 2023	Виконано
13	Отримання відгуку та рецензії на кваліфікаційну роботу	25 грудня 2023 – 26 грудня 2023	Виконано
14	Захист	27 грудня 2023	Виконано

Студент _____ Хімічук І.С.

Керівник _____ Трокоз Є.М.

АНОТАЦІЯ

Кваліфікаційна робота містить 63 сторінки, 50 ілюстрацій, 7 таблиць, список використаних джерел з 21 найменувань.

Метою роботи є процес дослідження методів й технологій захисту клієнт-серверної мережі організації, побудованої на базі ОС Windows Server.

В ході дослідження проведено аналіз принципів побудови та важливості захисту клієнт-серверних мереж організацій. Найбільшу увагу в дослідженні було приділено аналізу методів та технологій захисту таких мереж. Також було проведено детальний аналіз потенційних загроз та вразливостей, що можуть виникнути в умовах сучасності. Додатково проведено огляд проєкту мережі змодульованого підприємства та надано рекомендації щодо використаного обладнання. Надано рекомендації власникам організацій щодо методів та заходів захисту їх мереж.

Також було продемонстровано базові налаштування мережі. Надано рекомендаційні поради як правильно налаштовувати й автоматизувати розгортання Active Directory на сервері організації. Проведено детальний аналіз налаштувань системи захисту мережі в Active Directory.

Ключові слова: МЕТОДИ Й ТЕХНОЛОГІЇ, ЗАХИСТ ІНФОРМАЦІЇ, КОМП'ЮТЕРНІ МЕРЕЖІ, ЗАГРОЗИ МЕРЕЖІ, КЛІЄНТ–СЕРВЕРНА МЕРЕЖА, КОРИСТУВАЧ, ОБЛІКОВИЙ ЗАПИС, WINDOWS SERVER, ACTIVE DIRECTORY.

ANNOTATION

The qualification work contains 63 pages, 50 illustrations, 7 tables, a list of used sources from 21 titles.

The purpose of the work is the process of researching methods and technologies for protecting the client-server network of an organization built on the basis of the Windows Server OS.

In the course of the study, an analysis of the principles of construction and the importance of protecting client-server networks of organizations was carried out. The greatest attention in the research was paid to the analysis of methods and technologies of protection of such networks. A detailed analysis of potential threats and vulnerabilities that may arise in modern conditions was also conducted. In addition, an overview of the network project of the modular enterprise was conducted and recommendations were provided regarding the equipment used. Recommendations are given to the owners of organizations regarding methods and measures to protect their networks.

Basic network settings were also demonstrated. Recommendations are provided on how to correctly configure and automate the deployment of Active Directory on the organization's server. A detailed analysis of the settings of the network protection system in Active Directory was carried out.

Keywords: METHODS AND TECHNOLOGIES, INFORMATION PROTECTION, COMPUTER NETWORKS, NETWORK THREATS, CLIENT-SERVER NETWORK, USER, ACCOUNT.

ЗМІСТ

ВСТУП	9
РОЗДІЛ 1 АНАЛІЗ ПРИНЦИПІВ ПОБУДОВИ ТА ПРОБЛЕМИ ЗАХИСТУ МЕРЕЖІ ОРГАНІЗАЦІЇ	10
1.1 Принципи побудови мережі організації та важливість її захищеності ...	10
1.2 Аналіз потенційних загроз та вразливостей в умовах сучасності	14
1.3 Аналіз методів і технологій захисту клієнт–серверної мережі організації	16
РОЗДІЛ 2 АНАЛІЗ ПРОЄКТУВАННЯ ЛОКАЛЬНОЇ КЛІЄНТ–СЕРВЕРНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ	24
2.1 Аналіз обладнання та огляд проєкту мережі.....	24
2.2 Аналіз моделі загроз та моделі порушника.....	31
2.3 Рекомендовані методи та заходи для захисту клієнт–серверної мережі.	34
РОЗДІЛ 3 ПРИКЛАД НАЛАГОДЖЕННЯ СИСТЕМИ ЗАХИСТУ КЛІЄНТ– СЕРВЕРНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ	36
3.1 Демонстрація базових налаштувань мережі	36
3.2 Рекомендації з налаштування й автоматизації розгортання Active Directory на сервері	42
3.3 Аналіз налаштувань системи захисту мережі в Active Directory.....	50
ВИСНОВКИ.....	59
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	60
ДОДАТКИ.....	63

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПЗ – програмне забезпечення

HTTP – HyperText Transfer Protocol

FTP – File Transfer Protocol

DDoS – Distributed Denial-of-Service

VLAN – Virtual Local Area Network

MAC – Media Access Control

TLS – Transport Layer Security

SSL – Secure Sockets Layer

DNS – Domain Name System

NetBIOS – Network Basic Input/Output System

NAT – Network Address Translation

AD – Active Directory

ВСТУП

Захист клієнт-серверної мережі організації є критично важливою складовою в управлінні та забезпеченні безпеки даних та інфраструктури. На теперішній час виникають все більш складні загрози кібербезпеки, захист мережі від несанкціонованого доступу, витоку даних, атак з боку злоумисників та інших потенційних небезпек вкрай важливий.

Актуальність теми. Тема захисту клієнт-серверної мережі організації є надзвичайно актуальною в сучасному цифровому світі, де відбувається стрімкий технологічний розвиток і зростає кількість кіберзагроз. Організації та підприємства, незалежно від розміру та сфери діяльності, стикаються з різноманітними загрозами безпеці, які можуть привести до серйозних втрат даних, порушення працездатності систем, витрат часу та фінансових ресурсів на відновлення. Забезпечення високого рівня захисту від кіберзагроз стає основною пріоритетною задачею для організацій будь-якого типу. Актуальність теми захисту клієнт-серверної мережі організації є критично важливою, оскільки безпека даних є основою успішного функціонування сучасних підприємств та їхнього розвитку.

Метою кваліфікаційної роботи є дослідження основних методів й технологій захисту клієнт-серверної мережі на базі ОС Windows Server.

Встановлена мета обумовлює наступні завдання:

- аналіз принципів побудови мереж організацій та донесення їх важливості;
- розробити аналіз потенційних загроз та вразливостей, методів й технологій захисту клієнт-серверної мережі організації;
- надати рекомендації й продемонструвати налаштування системи захисту клієнт-серверної мережі;

Об'єктом дослідження є процес захисту клієнт-серверної мережі організації.

Предметом дослідження є методи й технології захисту клієнт-серверної мережі організації, побудованої на базі ОС Windows Server.

РОЗДІЛ 1 АНАЛІЗ ПРИНЦИПІВ ПОБУДОВИ ТА ПРОБЛЕМИ ЗАХИСТУ МЕРЕЖІ ОРГАНІЗАЦІЇ

1.1 Принципи побудови мережі організації та важливість її захищеності

Комп'ютерна мережа - це система, яка об'єднує комп'ютери та інші пристрої для обміну даними та ресурсами. Вона дозволяє пристроям спілкуватися між собою, обмінюватися інформацією, ресурсами та послугами. Основні компоненти комп'ютерної мережі включають:

- Пристрої: Комп'ютери, сервери, принтери, маршрутизатори, комутатори та інші пристрої, які з'єднані між собою для обміну даними.
- З'єднання: Кабельні з'єднання (Ethernet, оптоволокло тощо) або бездротові технології (Wi-Fi), які дозволяють передавати дані між пристроями.
- Програмне забезпечення: Програми та протоколи, які регулюють спілкування між пристроями та керують обміном даними.

Принципи побудови комп'ютерної мережі включають:

- Топологію: Це структура або організація з'єднання пристроїв в мережі (наприклад, зіркова, шина, кільцева топологія).
- Протоколи: Це правила та процедури, які визначають способи обміну даними між пристроями у мережі (наприклад, TCP/IP, HTTP, FTP).
- Забезпечення безпеки: Заходи для захисту даних та мережі від несанкціонованого доступу, атак та витоку інформації.

Переваги використання комп'ютерних мереж включають:

1. Обмін ресурсами:

- *Спільний доступ до даних:* Комп'ютерні мережі дозволяють користувачам обмінюватися файлами та даними, забезпечуючи спільний доступ до інформації з різних пристроїв.
- *Спільне використання принтерів та інших пристроїв:* Мережі дають можливість кільком користувачам використовувати один принтер або інші спільні ресурси.

2. Комунікація:

– *Легкість спілкування*: Використання електронної пошти, миттєвих повідомлень, відеоконференцій тощо полегшує комунікацію між користувачами мережі, навіть якщо вони знаходяться далеко один від одного.

– *Обмін інформацією*: Мережі дозволяють швидкий обмін даними, документами, мультимедійними файлами тощо.

3. Централізоване управління:

– *Централізована обробка даних*: Системи управління дозволяють керувати ресурсами та даними з централізованої точки, спрощуючи контроль та адміністрування мережі.

– *Забезпечення безпеки*: Централізована система дозволяє керувати заходами безпеки, моніторингом та захистом даних.

4. Ефективність:

– *Економія часу та ресурсів*: Спільне використання ресурсів, таких як принтери, файлові сервери тощо, зменшує зайві витрати часу та коштів на додаткове обладнання.

– *Підвищення продуктивності*: Мережі дозволяють швидше отримувати доступ до інформації та ресурсів, що сприяє підвищенню продуктивності праці.

5. Масштабованість:

– *Розширення мережі*: Комп'ютерні мережі легко розширюються шляхом додавання нових пристроїв або розширення функціональності, що дає можливість враховувати зростання потреб організації.

Комп'ютерні мережі є невід'ємною частиною сучасного світу та використовуються в різних галузях - від підприємств та організацій до особистого використання. Вони допомагають полегшити спілкування, роблять робочі процеси більш ефективними та дають доступ до безлічі ресурсів та інформації[1].

Отже захищеність мережі організації є критично важливою, оскільки це стосується захисту конфіденційності, цілісності та доступності даних, що обробляються та зберігаються в цій мережі. Незахищена мережа може стати джерелом ризиків для організації, таких як витік чутливої інформації, кібератаки,

втрата даних або зупинка бізнес-процесів. Детальніше про важливість захисту мережі організації в таблиці 1.1:

Таблиця 1.1 – Важливість захисту мережі організації

Поняття	Опис
<i>Конфіденційність даних</i>	Захищеність мережі дозволяє захищати конфіденційні дані організації від несанкціонованого доступу. Це може бути особиста інформація клієнтів, фінансові дані, інтелектуальна власність тощо.
<i>Цілісність даних</i>	Захист мережі також забезпечує цілісність даних, що означає захист від будь-яких спроб модифікації або внесення змін в інформацію несанкціонованими особами.
<i>Доступність</i>	Захищена мережа гарантує доступність інформації для тих, хто має на це право, уникнення зупинки роботи систем та запобігання втратам даних через кібератаки або інші загрози.
<i>Захист від кіберзагроз</i>	З розвитком технологій зростає загроза кібератак, які можуть призвести до крадіжок даних, блокування систем, вимагання викупу (рансомвари) та інших негативних наслідків для організації.

Продовження таблиці 1.1 – Важливість захисту мережі організації

Поняття	Опис
<i>Законодавчі вимоги та відповідності</i>	Багато секторів мають законодавчі вимоги стосовно захисту даних, такі як GDPR в Європі або HIPAA в США для медичної сфери. За невиконання цих вимог організація може потрапити під великі штрафи та втратити довіру клієнтів.
<i>Довіра та репутація</i>	Порушення безпеки даних може пошкодити репутацію організації та втратити довіру клієнтів або партнерів, що може сильно вплинути на бізнес.
<i>Ефективне управління ризиками</i>	Захист мережі дозволяє організаціям ефективно управляти ризиками, виявляти потенційні загрози та вчасно реагувати на них.

Загалом, захищеність мережі організації є ключовою для забезпечення безпеки даних, бізнес-процесів та репутації. Вона вимагає комплексного підходу, який включає технічні заходи захисту, процедури управління ризиками, свідомість персоналу та постійне вдосконалення систем безпеки.

Комплексний підхід до захисту мережі в організації вимагає ретельного поєднання різноманітних заходів та стратегій. Технічні заходи включають в себе використання передових інструментів та технологій, таких як брандмауери, антивірусне програмне забезпечення, системи аналізу та моніторингу безпеки, які активно виявляють потенційні загрози та вразливості мережі[2].

Однак технічні заходи самі по собі не є достатніми. Управління ризиками – це не менш важлива складова захисту мережі. Це включає в себе ретельний аналіз

потенційних загроз, оцінку вразливостей та ризиків, розробку стратегій мінімізації цих ризиків та прийняття заходів для запобігання можливим загрозам.

Свідомість персоналу щодо питань безпеки – ще один ключовий аспект. Технічні заходи можуть бути обійдені через людський фактор, тому навчання співробітників правилам та процедурам безпеки, усвідомлення можливих загроз, відомостей про соціальний інжиніринг, фішинг-атаки та інші види атак стають критично важливими для загального захисту мережі.

Проте без постійного вдосконалення систем безпеки, яке включає в себе аналіз результатів аудитів, реакцію на зміни у вимогах та технологіях, оновлення заходів та стратегій захисту, жодна система захисту не може бути повністю ефективною в умовах постійно змінюючогося ландшафту кіберзагроз.

Отже, суцільний підхід до захисту мережі включає в себе технічні рішення, управління ризиками, освіту персоналу та постійне вдосконалення систем безпеки, щоб забезпечити високий рівень захищеності мережі організації.

1.2 Аналіз потенційних загроз та вразливостей в умовах сучасності

Аналіз потенційних загроз та вразливостей в умовах сучасності має ключове значення для ефективного захисту систем та даних від кіберзагроз, і розгляд цих аспектів може включати в себе багато важливих та актуальних тем для дослідження.

Сучасний цифровий світ постійно стикається з різноманітними кіберзагрозами, які є серйозними загрозами для інформаційної безпеки та функціонування підприємств і організацій у всьому світі. Ці загрози включають в себе різноманітні типи хакерських атак, розповсюдження шкідливих програм, фішинг, рейдерство даних, а також нові форми кіберзагроз, які постійно змінюються та вдосконалюються.

Хакерські атаки: Хакерські атаки охоплюють широкий спектр технік, таких як DDOS-атаки (атаки на відмову в обслуговуванні), витік даних, атаки на вразливості програмного забезпечення, SQL-ін'єкції, кросс-сайт скриптинг тощо.

Вони можуть призвести до порушення роботи мережі, втрати конфіденційної інформації та суттєвих фінансових втрат.

Шкідливе програмне забезпечення: Різновиди шкідливих програм, таких як віруси, черв'яки, троянські програми, рансомвари, стали важливими загрозами для безпеки даних. Вони можуть викрасти інформацію, пошкодити файли, заблокувати доступ до систем або навіть вимагати викуп за дешифрування.

Вразливості в інформаційних системах та мережах визначають точки, які можуть бути використані для потенційних атак. Це може включати в себе недоліки в програмному забезпеченні, відсутність оновлень, слабкі паролі, використання застарілих технологій, недостатню кількість контролю за доступом до систем тощо[4].

Програмні вразливості: Регулярне виявлення та патчінг вразливостей в програмному забезпеченні важливо для запобігання експлуатації цих недоліків з метою злому чи розповсюдження шкідливого ПЗ.

Аутентифікація та управління доступом: Слабкі паролі, відсутність двофакторної аутентифікації або недостатній контроль за доступом можуть стати вразливостями, що дозволяють несанкціонованим особам отримати доступ до системи.

Особливо важливою є постійна оцінка та виправлення вразливостей, оскільки кіберзлочинці постійно шукають нові методи використання вразливостей для вторгнень у системи.

Використання застарілих технологій: Застосування застарілих версій програмного забезпечення або операційних систем, які не отримують регулярних оновлень та патчів безпеки, може стати вразливістю для атак.

Недостатній моніторинг та аналіз безпеки: Відсутність ефективних систем моніторингу та аналізу активності в мережі може перешкоджати вчасному виявленню потенційних загроз.

Згідно зі статистичними даними, наданими різними дослідницькими організаціями, такими як Центр забезпечення кібербезпеки (Cybersecurity and Infrastructure Security Agency - CISA) у США, високий рівень кіберзагроз

підтверджується ростом кількості виявлених кібератак у всьому світі протягом останніх років. Наприклад, аналізи показують зростання кількості хакерських атак на протязі останніх п'яти років, з проникненням в мережі більше 50% підприємств у всьому світі.

Інші дослідження свідчать про те, що більшість відомих вразливостей в програмному забезпеченні може бути експлуатована невдовзі після їх виявлення, що робить важливим актуальне та швидке усунення вразливостей.

Загалом, аналіз потенційних загроз та вразливостей в умовах сучасності відображає постійну необхідність оцінки та вдосконалення захисту інформаційних систем для запобігання кібератак та забезпечення надійного функціонування організаційних мереж та даних.

Отже бачимо, що різні фактори можуть сприяти ризикам безпеки, пов'язаним із мережами. Більш детальна інформація про деякі поширені вразливості наведена в таблиці 1.2, що знаходиться в Дотаку В:

1.3 Аналіз методів і технологій захисту клієнт–серверної мережі організації

Аналіз ризиків у сфері кібербезпеки є ключовою складовою стратегії захисту інформації. Оцінка ризиків у кібербезпеці полягає в усвідомленні потенційних загроз для інформаційної безпеки та визначенні ймовірності та впливу цих загроз на організацію. Один із підходів — це використання моделей загроз та вразливостей.

Моделі загроз та вразливостей створюють рамки для ідентифікації та аналізу потенційних кіберзагроз. SWOT-аналіз (аналіз сильних і слабких сторін, можливостей та загроз), матриці RACI (відповідальність, нагляд, консультація, інформування) та інші методи дозволяють визначити і оцінити загрози, зокрема, їхні можливі наслідки та імовірність виникнення.

Модель загроз визначає різні вектори загроз, такі як хакерські атаки, витоки даних, соціальний інженеринг тощо. Вразливості ж вказують на можливі слабкі місця в системі, через які ці загрози можуть бути реалізовані. Аналізуючи ці два аспекти, організація може розробити стратегії захисту та плани мінімізації ризиків.

Ці методи допомагають не тільки ідентифікувати потенційні загрози, а й визначати, які конкретні заходи захисту потрібно розглянути для запобігання цим загрозам. Особливо в умовах постійно зростаючого спектру кіберзагроз, ретельний аналіз ризиків та використання моделей загроз та вразливостей стають фундаментальною частиною стратегії захисту в сфері кібербезпеки[6].

Управління ризиками в інформаційній безпеці є критично важливим процесом для будь-якої організації, оскільки дозволяє визначити та зменшити вплив можливих загроз на інформаційні активи. Це включає в себе розробку стратегій та методів для виявлення, оцінки та управління ризиками, а також розробку та впровадження планів мінімізації ризиків.

Організації повинні розробляти стратегії управління ризиками, що відображають їхню спроможність виявляти та ефективно реагувати на ризики в інформаційній безпеці. Ці стратегії мають включати планування, аналіз, контроль та моніторинг ризиків усередині організації. Це допомагає ідентифікувати потенційні загрози та визначити їхній вплив на системи та даних.

Після ідентифікації ризиків необхідно розробити плани мінімізації ризиків. Ці плани включають в себе заходи з попередження та реагування на можливі загрози, що може включати в себе технічні засоби захисту, політики безпеки, процедури аварійного відновлення тощо. Вони мають бути ретельно розроблені та впроваджені для зменшення впливу ризиків на організацію.

Управління ризиками є важливим аспектом для забезпечення безпеки інформаційних систем. Воно допомагає організаціям ідентифікувати, аналізувати та керувати ризиками, забезпечуючи вчасну реакцію на потенційні загрози. Організації, які ефективно використовують стратегії управління ризиками, можуть бути краще підготовлені до захисту своїх активів та зменшення можливих втрат через кіберзагрози.

Захист від кіберзагроз стає все більшою проблемою в цифровій епісі, де зростаюча складність технологій надає нові можливості зловмисникам для втручання в інформаційні системи організацій. Огляд стратегій та методів захисту

від потенційних загроз включає в себе використання технічних та організаційних заходів з метою запобігання кібератак.

Технічні заходи захисту включають у себе широкий спектр інструментів та технологій, спрямованих на запобігання кіберзагрозам. Серед них:

1. *Брандмауер (Firewall)*: Контролюють трафік, що входить і виходить з мережі, для блокування небажаних підключень та захисту від зовнішніх атак.

2. *Антивірусне програмне забезпечення*: Виявляє, блокує та видаляє шкідливі програми, віруси та загрози.

3. *Системи виявлення вторгнень (Intrusion Detection Systems - IDS) та системи запобігання вторгнень (Intrusion Prevention Systems - IPS)*: Моніторять мережевий трафік для виявлення та блокування ненормальної або шкідливої активності.

4. *Шифрування даних*: Захищає дані від несанкціонованого доступу, забезпечуючи їхню конфіденційність.

Організаційні заходи включають у себе політики, процедури та практики, спрямовані на забезпечення безпеки в інформаційній сфері:

1. *Політики безпеки*: Розробка та впровадження внутрішніх політик безпеки, що включають в себе вимоги щодо паролів, прав доступу та інші обмеження.

2. *Навчання та усвідомлення персоналу*: Постійне навчання персоналу з правил безпеки, організація тренінгів та імітаційних вправ для підвищення усвідомленості стосовно потенційних кіберзагроз.

3. *Регулярні оновлення та патчі безпеки*: Забезпечення актуальності програмного забезпечення, включаючи операційні системи та програми, через регулярні оновлення та встановлення патчів безпеки.

Загально кажучи, комбінація технічних та організаційних заходів захисту є ключем до ефективного запобігання кібератакам. Регулярне оновлення технічних заходів безпеки, спільно з удосконаленням організаційних процесів, дозволяє зберегти важливі дані та мережеві ресурси в безпеці[5].

Людський фактор у контексті кібербезпеки теж грає ключову роль у забезпеченні безпеки інформації. Важливість освіти та усвідомлення персоналу про ризики, а також усвідомлення впливу людського фактору на безпеку інформації, визначає ефективність заходів захисту та методів зменшення ризиків.

Освічений персонал, який розуміє загрози та ризики в кіберпросторі, є першою лінією оборони в будь-якій організації. Правильно організована та систематична освіта з питань кібербезпеки надає співробітникам знання, як уникати соціального інженерінгу, фішингу, та інших шахрайських схем.

Люди можуть стати слабкою ланкою у захисті інформації через помилки, невідповідальне поведження або недостатнє усвідомлення про безпеку. Часто кіберзагрози можуть виникнути через необережність працівників: використання слабких паролів, натискання на посилання в сумнівних електронних листах тощо.

Методами зменшення впливу людського фактору на безпеку інформації можуть бути:

1. *Тренінги та освіта:* Проведення регулярних тренінгів та навчання персоналу правилам кібербезпеки.
2. *Формування безпечної культури:* Створення атмосфери в організації, де безпека інформації є пріоритетом, що сприяє збереженню даних.
3. *Використання технологій для підвищення безпеки:* Впровадження двофакторної аутентифікації, шифрування електронної пошти та даних, що може допомогти унеможливити чи послабити вплив людських помилок на безпеку.

Працівники, що освідчені та усвідомлюють ризики, можуть стати ключовими сторонами в уникненні кіберзагроз. Невідповідальне поведження чи недостатнє усвідомлення загроз може призвести до серйозних наслідків для безпеки організації. Щоб зменшити вплив людського фактору на безпеку інформації, важливо не лише надавати освіту та інструкції щодо кібербезпеки, але й створювати культуру безпеки, де працівники відчують відповідальність за захист інформації, інтегруючи ці принципи у щоденну роботу[7].

Додатковими заходами можуть бути:

1. *Моніторинг та аудит безпеки:* Регулярне аудитування безпекових процедур та контроль за їхнім виконанням для виявлення слабких місць та недоліків у системі.

2. *Постійне вдосконалення:* Постійне вдосконалення політик та процедур безпеки відповідно до змін у кіберзагрозах та технологіях.

3. *Стимулювання безпечної поведінки:* Введення системи стимулів або нагород для працівників, які дотримуються політик безпеки.

Аналіз сучасних тенденцій та новацій у сфері кібербезпеки включає в себе огляд інноваційних підходів, розвитку та потенційних викликів для захисту інформації. Детальніша інформація про це наведена в таблиці 1.3

Таблиця 1.3 – Інноваційні підходи, розвиток та потенційні виклики

Поняття		Опис
<i>Сучасні тенденції у кібербезпеці</i>	<i>Штучний інтелект та машинне навчання</i>	Використання AI для виявлення аномальної поведінки в мережі та автоматизації процесів захисту від кіберзагроз
	<i>Розширена реальність та блокчейн</i>	Впровадження технологій AR для навчання персоналу у сфері кібербезпеки та використання блокчейну для створення безпечних та недоступних для змін даних

Продовження таблиці 1.3 – Інноваційні підходи, розвиток та потенційні виклики

Поняття		Опис
	<i>Інтернет речей (IoT)</i>	Збільшення кількості підключених пристроїв вимагає нових підходів до захисту даних та мережевої інфраструктури
<i>Напрями розвитку у сфері кібербезпеки</i>	<i>Проактивний підхід до захисту</i>	Перехід від реактивних заходів до передбачення та запобігання кіберзагрозам
	<i>Кіберзахист у хмарних сервісах</i>	Розробка більш ефективних методів захисту даних, які зберігаються у хмарних сервісах
	<i>Захист від соціального інжинірингу</i>	Підвищення уваги до атак, які спираються на маніпулювання людським фактором
<i>Потенційні виклики для захисту інформації</i>	<i>Розширення атак</i>	Зростання обсягу та складності кіберзагроз, таких як розповсюдження розумних вірусів та швидка еволюція технік атак

Продовження таблиці 1.3 – Інноваційні підходи, розвиток та потенційні виклики

Поняття		Опис
	<i>Кібербезпека в медичній сфері</i>	Підвищення потенційних загроз для медичних пристроїв та медичної інфраструктури
	<i>Проблеми приватності та відповідності</i>	Ростуть вимоги до забезпечення конфіденційності та дотримання нормативних вимог у зберіганні та обробці даних

Нові технології вимагають постійного вдосконалення методів захисту та усвідомлення потенційних загроз для ефективного захисту інформації у цифровому світі.

Також важливою складовою для створення надійних та безпечних інформаційних систем у кібербезпеці є стандарти та нормативи. Роль відповідності стандартам та нормативам полягає у створенні основи для реалізації ефективних заходів безпеки та створенні структурованого підходу до захисту інформації.

Стандарти як основа безпечних практик:

1. Нормативне регулювання: Стандарти і нормативи у кібербезпеці встановлюють мінімальні вимоги щодо захисту інформації, які повинні дотримуватися організаціями для забезпечення безпеки своїх систем та даних.

2. Структурований підхід: Вони надають структурований підхід до визначення, впровадження та управління заходами з кібербезпеки, що допомагає організаціям систематично підходити до захисту інформації.

Важливість відповідності стандартам:

1. Забезпечення якості заходів безпеки: Відповідність стандартам дозволяє перевірити ефективність та якість заходів безпеки, забезпечуючи відповідність найвищим стандартам безпеки.

2. Міжнародна взаємодія: Стандарти у кібербезпеці встановлюють загальні принципи та підходи, що сприяє спільному розумінню та співпраці між організаціями на міжнародному рівні.

Вплив стандартів на безпечну практику:

1. Підвищення довіри: Відповідність стандартам і нормативам у кібербезпеці сприяє підвищенню довіри як серед внутрішніх, так і серед зовнішніх зацікавлених сторін.

2. Зменшення ризику: Виконання встановлених стандартів та нормативів допомагає зменшити ризик втрати даних чи порушення безпеки.

Стандарти та нормативи у кібербезпеці виступають як основа для впровадження ефективних заходів безпеки. Відповідність цим стандартам допомагає організаціям підвищити безпеку інформації, створити структурований підхід до захисту даних та забезпечити довіру серед зацікавлених сторін. Ретельне виконання стандартів та нормативів у кібербезпеці є важливою складовою для успішного захисту інформації та забезпечення стійкості організаційних систем.

РОЗДІЛ 2 АНАЛІЗ ПРОЄКТУВАННЯ ЛОКАЛЬНОЇ КЛІЄНТ–СЕРВЕРНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ

2.1 Аналіз обладнання та огляд проєкту мережі

Для гарного функціонування мережі слід обирати надійне обладнання, саме такими є прилади корпорації Cisco.

Слід обирати оптимальне обладнання, що має адаптованість під модернізацію модулями. Слід звернути увагу на ключові технології, необхідні для мережі, такі як підтримка GigabitEthernet та Ethernet (FastEthernet).

Рекомендовано обирати, наприклад, комутатори серії Cisco Catalyst 2960. Cisco Catalyst 2960 – це серія комутаторів, які належать до лінійки мережевого обладнання Cisco Catalyst. Вони широко використовуються в бізнес-середовищах для створення локальних мереж (LAN) через їхню надійність, продуктивність та розширені можливості управління[3].



Рисунок 2.1 – Комутатор Cisco Catalyst 2960

Отримавши свій дебют на ринку у 2003 році, модель Cisco Catalyst 2960 відразу ж здобула популярність через свою надійність і здатність забезпечувати високу швидкість передачі даних в локальних мережах. Однією з ключових характеристик цієї серії є підтримка технології Power over Ethernet (PoE), яка дозволяє живлення пристроїв через Ethernet-кабель, що дозволяє підключати пристрої, такі як IP-телефони, точки доступу Wi-Fi і безперервно живлені мережеві камери.

Деякі ключові особливості і можливості Cisco Catalyst 2960:

1. Швидкість передачі даних: Підтримка швидкостей Gigabit Ethernet забезпечує високу продуктивність для передачі даних в мережі.

2. Управління мережею: Ці комутатори оснащені рядом інструментів управління мережею, таких як Cisco Smart Install, Cisco Smart Configuration, що спрощують управління мережею.

3. Безпека мережі: Вони підтримують різноманітні механізми безпеки, такі як Access Control Lists (ACLs), Virtual LANs (VLANs), і захист від атак, що робить мережу більш захищеною.

4. Підтримка IPv6: Комутатори підтримують новий протокол IPv6, що стає все більш важливим у зв'язку з вичерпанням адрес IPv4.

5. Економія енергії: Технологія Cisco EnergyWise дозволяє ефективно керувати енергоспоживанням у мережі.

Ця серія комутаторів призначена для різноманітних сегментів ринку, від невеликих бізнесів до великих підприємств, де потрібна надійна та ефективна мережа з можливістю розширення та управління.

Маршрутизатор слід обирати з серії Cisco 7200.

Cisco 7200 – це серія маршрутизаторів, що відносяться до високопродуктивного обладнання Cisco для побудови мереж на рівні провайдера або корпоративного рівня. Вони були розроблені з метою забезпечення високої швидкості обробки пакетів, гнучкості конфігурації та розширення можливостей.



Рисунок 2.2 – Маршрутизатор Cisco 7201

Основні особливості та можливості маршрутизаторів Cisco 7200:

1. Висока продуктивність: Ці маршрутизатори підтримують високі швидкості обробки пакетів, що робить їх ефективними для мереж з великим обсягом трафіку.

2. Модульність та гнучкість: Вони мають модульну архітектуру, що дозволяє розширювати їхні можливості за допомогою різноманітних модулів, таких як модулі вводу/виводу (I/O), модулі інтерфейсів та інші.

3. Підтримка різноманітних інтерфейсів: Маршрутизатори цієї серії підтримують широкий спектр інтерфейсів, включаючи Ethernet, T1/E1, T3/E3, POS (Packet-over-SONET), ATM (Asynchronous Transfer Mode) та інші.

4. Можливості маршрутизації: Cisco 7200 підтримують різноманітні протоколи маршрутизації, такі як BGP (Border Gateway Protocol), OSPF (Open Shortest Path First), EIGRP (Enhanced Interior Gateway Routing Protocol) і RIP (Routing Information Protocol).

5. Забезпечення безпеки мережі: Ці маршрутизатори мають ряд вбудованих заходів безпеки, які допомагають управляти доступом та захищати мережевий трафік.

6. Віртуалізація мережі: Вони можуть використовуватися для створення віртуальних мереж (VRF - Virtual Routing and Forwarding) для розділення трафіку між різними логічними мережами на одному фізичному пристрої.

Маршрутизатори Cisco 7200 широко використовуються у великих компаніях, провайдерах послуг, дата-центрах та інших організаціях, де потрібні високі швидкості обробки даних, гнучкість конфігурації та надійність мережі. Їхні можливості і функціональність роблять їх популярними для різних великих мережевих інфраструктур.

Провівши аналіз бачимо, що мережу було розроблено за допомогою схеми офісного приміщення, що дозволило візуально показати, як приблизно будуть розташовані пристрої у реальній організації.

На рисунку видно, що мережа складається з серверної та трьох приміщень для роботи за персональними комп'ютерами.

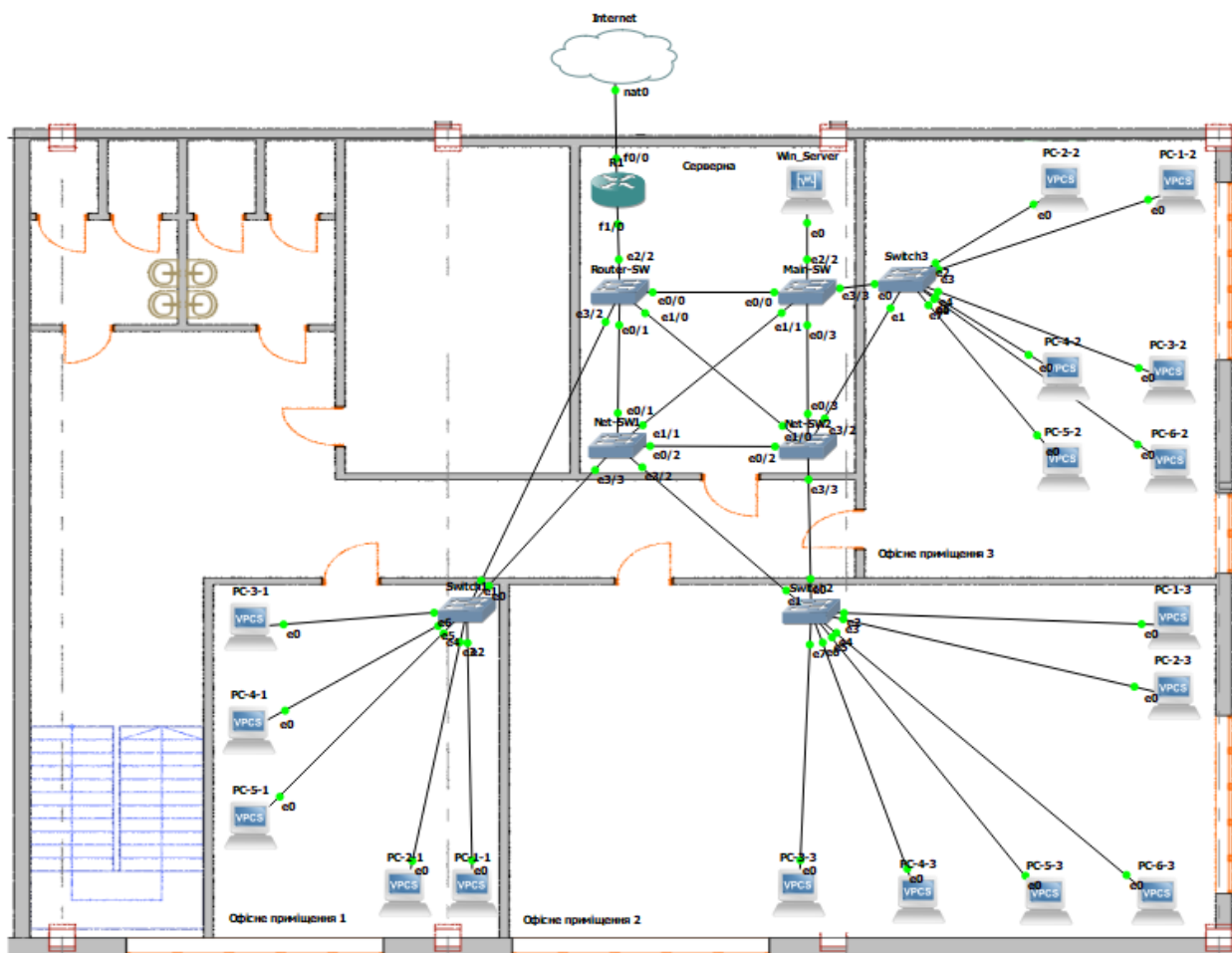


Рисунок 2.3 – Проект мережі

У загальному в мережі використано маршрутизатор Cisco 7200 та комутатори Cisco Catalyst 2960 в кількості семи одиниць. Мережа містить п'ять підмереж.

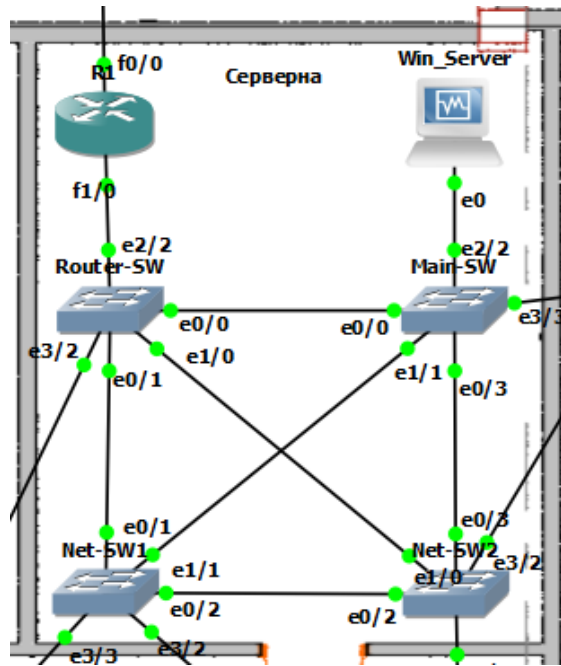


Рисунок 2.4 – Основна(серверна) частина мережі

Основна частина мережі складатиметься з двох VLAN-ів. З VLAN 50 менеджменту та VLAN 100 сервера. VLAN 50 складається з чотирьох комутаторів.

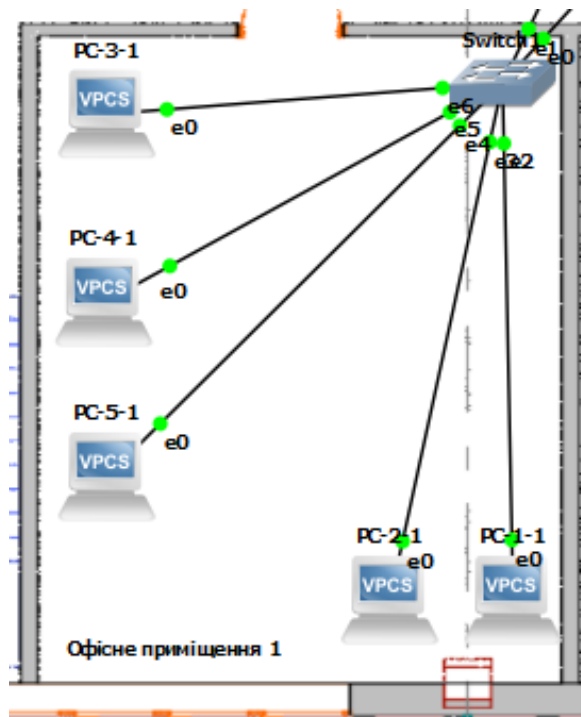


Рисунок 2.5 – Офісне приміщення 1

Перше офісне приміщення складається з одного влану (10). VLAN 10 включає в себе один комутатор та п'ять персональних комп'ютерів.

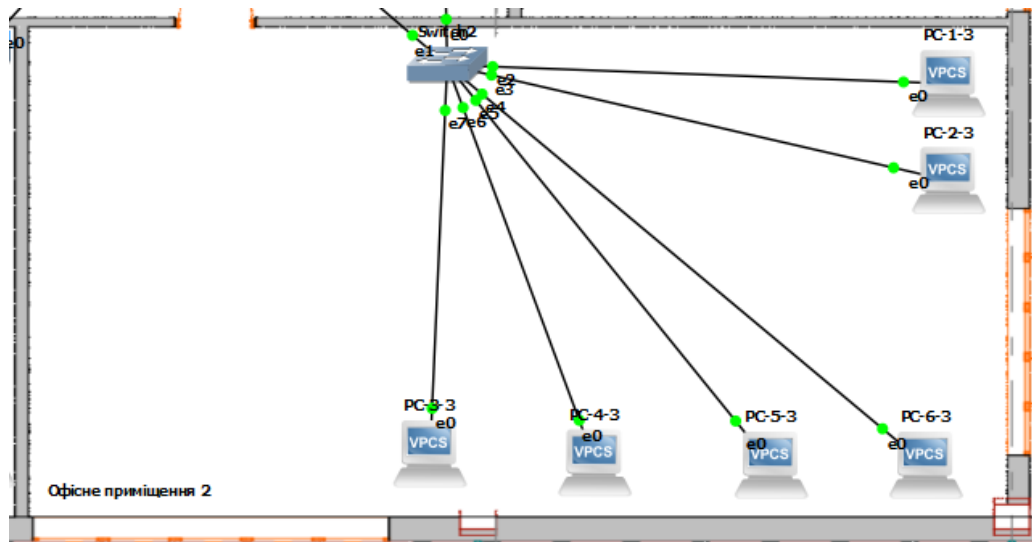


Рисунок 2.6 – Офісне приміщення 2

Друге офісне приміщення складається з одного влану (20). VLAN 20 включає в себе один комутатор та шість персональних комп'ютерів.

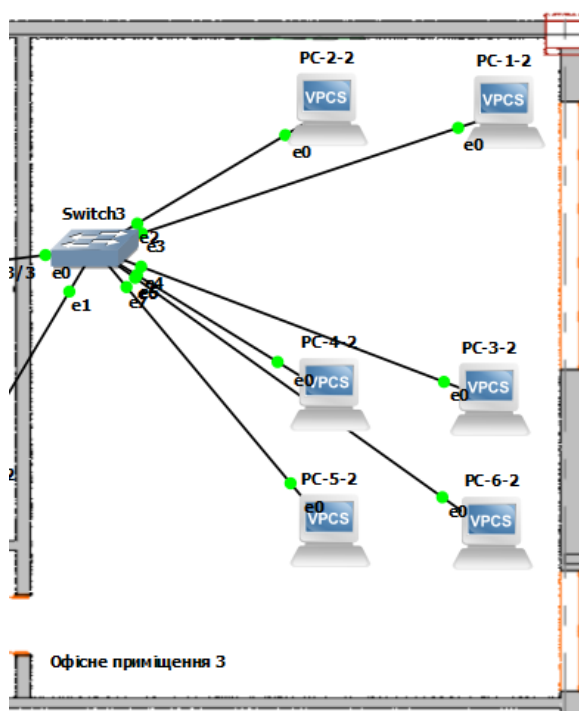


Рисунок 2.7 – Офісне приміщення 3

Третє офісне приміщення складається з одного влану (30). VLAN 30 включає в себе один комутатор та шість персональних комп'ютерів.

Отже, усі віртуальні мережі першого, другого та третього приміщення мають схожу структуру і складаються з одного комутатору та по п'ять–шість персональних комп'ютерів відповідно.

Основна частина складається з чотирьох комутаторів, на яких виконано DHCP налаштування та сервер, на якому адреса задана статичним методом.

Також в мережі налаштовано RIPv2 та SSH.

Таблиця 2.1 – Адресація підмережі VLAN 10

Призначення	IP-адреса
Адреса мережі	192.168.10.0
Маска префіксу	255.255.255.0
Інверсна маска	0.0.0.255
Мінімальна адреса	192.168.10.1
Максимальна адреса	192.168.10.254
Кількість доступних адрес	254

Таблиця 2.2 – Адресація підмережі VLAN 20

Призначення	IP-адреса
Адреса мережі	192.168.20.0
Маска префіксу	255.255.255.0
Інверсна маска	0.0.0.255
Мінімальна адреса	192.168.20.1
Максимальна адреса	192.168.20.254
Кількість доступних адрес	254

Таблиця 2.3 – Адресація підмережі VLAN 30

Призначення	IP-адреса
Адреса мережі	192.168.30.0
Маска префіксу	255.255.255.0
Інверсна маска	0.0.0.255
Мінімальна адреса	192.168.30.1
Максимальна адреса	192.168.30.254
Кількість доступних адрес	254

2.2 Аналіз моделі загроз та моделі порушника

Модель загроз – це структурований підхід до визначення та класифікації потенційних загроз для інформаційної системи або організації. Ця модель допомагає ідентифікувати, розуміти та оцінювати загрози, які можуть виникнути та спричинити ризики для безпеки даних, інфраструктури, а також операцій організації[9].

Етапи побудови моделі загроз:

1. *Ідентифікація активів:* Спочатку визначаються всі активи (інформація, обладнання, програмне забезпечення тощо), які підлягають захисту. Це можуть бути дані, пристрої, мережі, аплікації та будь-які інші ресурси, які мають важливе значення для організації.

2. *Визначення загроз:* Загрози - це потенційні події або ситуації, які можуть викликати шкоду або завдати втрат організації. Вони можуть бути природними (наприклад, природні лиха), технічними (хакерські атаки, віруси), людськими (соціальний інженеринг, неправильне використання співробітниками даних) або відповідати технічній політиці та процедурам безпеки.

3. *Оцінка вразливостей:* Визначення потенційних слабких місць (уразливостей) в інформаційній системі або процесах, які можуть бути використані загрозами для здійснення атаки або завдання шкоди.

4. *Оцінка ризику:* Цей етап включає аналіз можливих наслідків загроз та їх ймовірності виникнення. Ризик оцінюється на основі потенційної шкоди та ймовірності її виникнення.

5. *Розробка стратегій захисту:* Після оцінки ризику розробляються стратегії та плани захисту для мінімізації можливих наслідків загроз.

Важливі аспекти моделі загроз:

1. *Константна оцінка:* Модель потребує постійного оновлення і перегляду, оскільки загрози постійно змінюються і еволюціонують.

2. *Широта охоплення:* Модель має охоплювати різні типи загроз, від технічних до соціальних.

3. *Реалістичність*: Модель повинна бути побудована на реальних загрозах, які можуть впливати на конкретну організацію.

Модель загроз є важливим інструментом для підвищення кібербезпеки, оскільки вона дозволяє оцінювати потенційні ризики та розробляти стратегії захисту, щоб забезпечити безпеку активів організації чи системи[10].

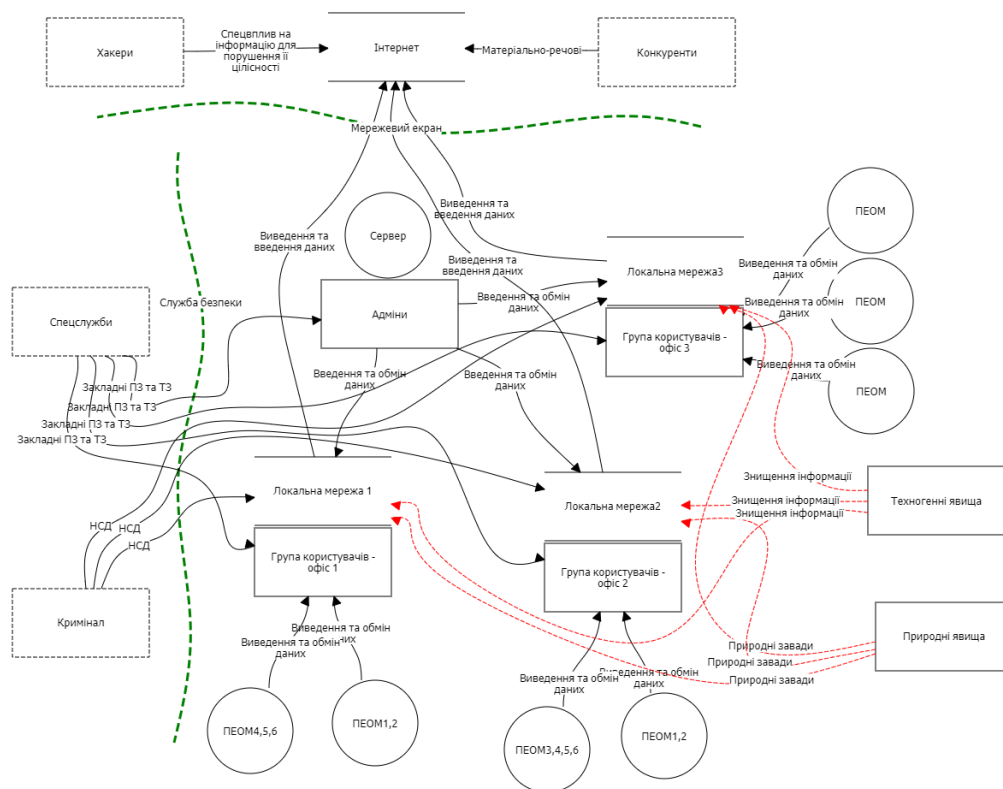


Рисунок 2.8 – Модель загроз

Також слід розуміти хто саме і чому загрожує мережі. Для цього складається модель порушника.

Модель порушника – це концептуальний інструмент, що використовується для визначення та розуміння потенційних загроз, які можуть бути створені або використані зловмисниками або атакувальниками для атаки на інформаційну систему, мережу чи організацію.

Елементи моделі порушника:

1. *Профіль порушника*: Це опис характеристик та властивостей потенційного атакувальника. Включає в себе технічні знання, рівень доступу, мети або мотивації, ресурси та можливості для здійснення атак.
2. *Методи та інструменти атаки*: Це перелік технік, інструментів, програм або методів, які порушник може використовувати для здійснення атак.

Включає в себе типи атак (наприклад, деніал сервісу, введення в оману, витік даних) та технічні засоби для їх виконання.

3. *Мотивація зловмисника*: Це фактор, який визначає, чому порушник може зацікавитися атакою на систему або організацію. Мотиви можуть бути фінансові, політичні, ідеологічні або просто намагання отримати доступ до конфіденційної інформації.

4. *Ступінь доступу*: Це рівень привілеїв чи доступу, який атакувальник може мати або отримати до системи чи мережі. Він може бути обмеженим або повним, в залежності від зазначених цілей та методів атаки.

Побудова моделі порушника:

1. *Збір інформації про загрози*: Це включає в себе аналіз відомостей про типи загроз, відомі атаки, вразливості системи та можливі наслідки.

2. *Аналіз потенційних сценаріїв*: На основі зібраної інформації створюються сценарії, що описують можливі атаки, враховуючи профіль, методи та мотивації атакувальника.

3. *Оцінка ризику*: Оцінюється потенційний вплив атаки, ймовірність виникнення та рівень пошкодження, що може бути завдано системі або організації.

4. *Розробка заходів захисту*: На основі аналізу створюються стратегії та заходи безпеки для запобігання або зменшення наслідків можливих атак.

Модель порушника допомагає ідентифікувати та розуміти характеристики потенційних загроз, що може бути використано для побудови ефективних заходів безпеки та захисту інформаційних систем чи мереж від атак.

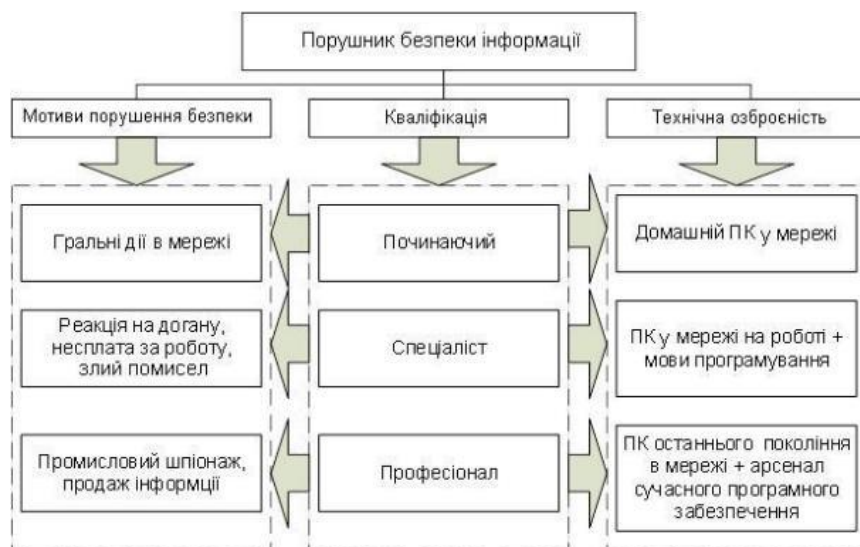


Рисунок 2.9 – Модель порушника

2.3 Рекомендовані методи та заходи для захисту клієнт–серверної мережі

Захист клієнт-серверної мережі вимагає комплексного підходу та розгляду різних аспектів, щоб забезпечити безпеку та надійність всієї інфраструктури. Проаналізувавши інформацію з попередніх розділів можна надати більш чіткі поради по захисту мережі власникам організацій. Ось деякі рекомендовані методи та заходи для захисту клієнт-серверної мережі:

1. *Сегментація мережі*: Розділення мережі на сегменти або зони для обмеження доступу та вирішення внутрішньої безпеки. Використання VLAN або мережевих фаєрволів для ізоляції чутливих даних.

2. *Централізоване керування доступом*: Впровадження централізованої системи управління доступом для керування правами доступу до ресурсів на основі ролей та політик безпеки.

3. *Жорстке відстеження системних подій*: Використання систем моніторингу та аналізу журналів подій для виявлення аномальних дій або змін в системі, що можуть вказувати на атаку.

4. *Резервне копіювання та відновлення даних*: Регулярне створення резервних копій даних та розробка планів відновлення для випадків аварійного втрати даних.

5. *Використання SSL/TLS*: Встановлення захищених з'єднань для взаємодії клієнтів і серверів, забезпечуючи шифрування даних під час передачі через мережу.

6. *Використання віртуальних приватних мереж (VPN)*: Застосування VPN для захищеної та шифрованої передачі даних через публічну мережу. VPN створює захищене тунельне з'єднання між відправником та отримувачем, перекриваючи потенційно небезпечну публічну мережу.

7. *Системи виявлення вторгнень (IDS/IPS)*: Розгортання систем виявлення вторгнень для надання спеціалізованого моніторингу та захисту від атак, які можуть пройти через брандмауер чи антивірус.

8. *Автоматичне оновлення та патчі:* Налаштування автоматичного оновлення підключених пристроїв для запобігання експлуатації відомих уразливостей.

9. *Захист від DDoS атак:* Використання спеціалізованих сервісів чи обладнання для виявлення та фільтрації трафіку, який може бути спрямований на мережу для збоїв.

10. *Шифрування даних у спокійному режимі:* Встановлення шифрування даних на зберігання чутливої інформації на серверах. Це означає, що дані зберігаються у зашифрованому вигляді за допомогою спеціальних алгоритмів шифрування. Важливо використовувати сильні алгоритми шифрування, такі як AES (Advanced Encryption Standard) або RSA (Rivest-Shamir-Adleman), які забезпечують високий рівень безпеки.

11. *Регулярні аудити безпеки:* Проведення регулярних аудитів безпеки мережі для виявлення та усунення можливих проблем безпеки. Цей процес охоплює перевірку наявних заходів безпеки, які вже застосовані в мережі, а також виявлення необхідності нових заходів або покращень.

12. *Безпека від електронної пошти:* Використання фільтрів та систем аналізу електронної пошти для виявлення та блокування шкідливих повідомлень.

Ці заходи є частиною стратегії захисту клієнт-серверної мережі і можуть бути придатними в залежності від контексту, розміру та специфікацій вашої мережевої інфраструктури[8].

Кожна організація повинна розглядати свої потреби у безпеці та використовувати комбінацію цих методів у відповідності до своєї інфраструктури та загроз, з якими вони можуть стикатися.

РОЗДІЛ 3 ПРИКЛАД НАЛАГОДЖЕННЯ СИСТЕМИ ЗАХИСТУ КЛІЄНТ–СЕРВЕРНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ

3.1 Демонстрація базових налаштувань мережі

У цьому пункті представлений приклад базового налаштування пристроїв мережі. Пристрої завчасно слід підготувати до роботи.

В роутері R1 на порті f1/0 налаштовано Sub-інтерфейси (10, 20, 30, 50, 100), для взаємодії між віртуальними локальними підмережами. Для кожного VLAN створений окремий інтерфейс, на якому задано відношення до потрібного VLAN, адресу та тип інкапсуляції.

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int f1/0.10
R1(config-subif)#des SUBNET-WORKER-1
R1(config-subif)#encapsulation dot1Q 10
R1(config-subif)#ip add 192.168.10.254 255.255.255.0
R1(config-subif)#no sh
R1(config-subif)#ex
R1(config)#int f1/0.20
R1(config-subif)#des SUBNET-WORKER-2
R1(config-subif)#encapsulation dot1Q 20
R1(config-subif)#ip add 192.168.20.254 255.255.255.0
R1(config-subif)#ex
R1(config)#int f1/0.30
R1(config-subif)#des SUBNET-WORKER-3
R1(config-subif)#encapsulation dot1Q 30
R1(config-subif)#ip add 192.168.30.254 255.255.255.0
R1(config-subif)#no sh
R1(config-subif)#ex
R1(config)#
R1(config)#
R1(config)#int f1/0.100
R1(config-subif)#des SERV-AD-SUBNET
R1(config-subif)#encapsulation dot1Q 100
R1(config-subif)#ip add 192.168.100.6 255.255.255.248
R1(config-subif)#no sh
R1(config-subif)#ex
R1(config)#int f1/0.50
R1(config-subif)#des SUBNET-MGMT
R1(config-subif)#encapsulation dot1Q 50
R1(config-subif)#ip add 192.168.50.14 255.255.255.240
R1(config-subif)#no sh
```

Рисунок 3.1 – Налаштування Sub-інтерфейсів

Для отримання адрес по протоколу DHCP, адреси шлюзів по замовчуванню вносяться у виключення. Якщо цього не зробити, це викличе дублікації IP-адрес та призведе до конфлікту.

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip dhcp excluded-address 192.168.10.254
R1(config)#ip dhcp excluded-address 192.168.20.254
R1(config)#ip dhcp excluded-address 192.168.30.254
R1(config)#ip dhcp excluded-address 192.168.100.6
R1(config)#ip dhcp excluded-address 192.168.50.14
```

Рисунок 3.2 – Виключення адрес з простору адрес DHCP

Для отримання робочими машинами IP–адрес автоматично, на підмережах працівників офісу виконується налаштування протоколу DHCP.

```
R1(config)#ip dhcp pool WORKER-1
R1(dhcp-config)#network 192.168.10.0 255.255.255.0
R1(dhcp-config)#domain-name office.local
R1(dhcp-config)#default-router 192.168.10.254
R1(dhcp-config)#dns-server 192.168.100.6
R1(dhcp-config)#ex
R1(config)#ip dhcp pool WORKER-2
R1(dhcp-config)#network 192.168.20.0 255.255.255.0
R1(dhcp-config)#domain-name office.local
R1(dhcp-config)#default-router 192.168.20.254
R1(dhcp-config)#dns-server 192.168.100.6
R1(dhcp-config)#ex
R1(config)#ip dhcp pool WORKER-3
R1(dhcp-config)#network 192.168.30.0 255.255.255.0
R1(dhcp-config)#domain-name office.local
R1(dhcp-config)#default-router 192.168.30.254
R1(dhcp-config)#dns-server 192.168.100.6
R1(dhcp-config)#ex
```

Рисунок 3.3 – Налаштування протоколу DHCP

Для доступу мережі в інтернет на інтерфейсі f0/0 виконується налаштування динамічного отримання IP–адреси.

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int f0/0
R1(config-if)#ip add dhcp
R1(config-if)#no sh
R1(config-if)#
*Jun 11 12:17:12.047: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Jun 11 12:17:13.047: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
```

Рисунок 3.4 – Налаштування DHCP

Щоб кожна підмережа мала вихід в інтернет, на кожній з них слід налаштувати механізм NAT.

NAT (Network Address Translation) – це технологія мережі, яка перетворює IP-адреси з одного діапазону на інші для передачі даних через мережу. Це дозволяє об'єднувати декілька пристроїв у мережі за допомогою одного зовнішнього IP-адреси, забезпечуючи внутрішній мережі доступ до зовнішнього Інтернету.

```

R1(config)#int f1/0.10
R1(config-subif)#ip nat inside

*Jun 11 12:25:55.955: %LINEPROTO-5-UPDOWN: Line protocol on Interface NVI0, changed state to up
R1(config-subif)#ip nat inside
R1(config-subif)#int f1/0.20
R1(config-subif)#ip nat inside
R1(config-subif)#int f1/0.30
R1(config-subif)#ip nat inside
R1(config-subif)#int f1/0.100
R1(config-subif)#ip nat inside
R1(config-subif)#ex
R1(config)#int f0/0
R1(config-if)#ip nat outside
R1(config-if)#ex
R1(config)#acc
R1(config)#access-list 1 permit 192.168.100.0 0.0.0.7
R1(config)#access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)#access-list 1 permit 192.168.20.0 0.0.0.255
R1(config)#access-list 1 permit 192.168.30.0 0.0.0.255
R1(config)#ip nat inside source list 1 int f0/0 overload
R1(config)#

```

Рисунок 3.5 – Налаштування NAT

Першочергово слід створити підмережі для юзерів, сервера та менеджменту на кожному з комутаторів.

```

Router-SW#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router-SW(config)#vlan 10
Router-SW(config-vlan)#name WORKER-1
Router-SW(config-vlan)#vlan 20
Router-SW(config-vlan)#name WORKER-2
Router-SW(config-vlan)#vlan 30
Router-SW(config-vlan)#name WORKER-3
Router-SW(config-vlan)#vlan 50
Router-SW(config-vlan)#name MGMT
Router-SW(config-vlan)#vlan 100
Router-SW(config-vlan)#name SERV-AD
Router-SW(config-vlan)#

```

Рисунок 3.6 – Створення підмереж

```

Main-SW#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Main-SW(config)#vlan 10
Main-SW(config-vlan)#name WORKER-1
Main-SW(config-vlan)#vlan 20
Main-SW(config-vlan)#name WORKER-2
Main-SW(config-vlan)#vlan 30
Main-SW(config-vlan)#name WORKER-3
Main-SW(config-vlan)#vlan 50
Main-SW(config-vlan)#name MGMT
Main-SW(config-vlan)#vlan 100
Main-SW(config-vlan)#name SERV-AD
Main-SW(config-vlan)#

```

Рисунок 3.7 – Створення підмереж

Налагодження на інших комутаторах має аналогічний вигляд.

Наступним кроком налагоджуються транкові канали на потрібних портах щоб поширити трафік по створених до цього VLAN-ах.

```

Router-SW(config)#int e2/2
Router-SW(config-if)#switchport trunk allowed vlan 10,20,30,50,100
Router-SW(config-if)#switchport trunk encapsulation dot1q
Router-SW(config-if)#switchport mode trunk
Router-SW(config-if)#
*Jun 13 10:34:07.812: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet2/2,
changed state to down
Router-SW(config-if)#
*Jun 13 10:34:12.294: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet2/2,
changed state to up
Router-SW(config-if)#int e3/2
Router-SW(config-if)#
Router-SW(config-if)#switchport trunk allowed vlan 10,20,30,50,100
Router-SW(config-if)#switchport trunk encapsulation dot1q
Router-SW(config-if)#switchport mode trunk
Router-SW(config-if)#
Router-SW(config-if)#int e0/1
Router-SW(config-if)#switchport trunk allowed vlan 10,20,30,50,100
Router-SW(config-if)#switchport trunk encapsulation dot1q
Router-SW(config-if)#switchport mode trunk
Router-SW(config-if)#
Router-SW(config-if)#int e1/0
Router-SW(config-if)#switchport trunk allowed vlan 10,20,30,50,100
Router-SW(config-if)#switchport trunk encapsulation dot1q
Router-SW(config-if)#switchport mode trunk
Router-SW(config-if)#
Router-SW(config-if)#int e0/0
Router-SW(config-if)#switchport trunk allowed vlan 10,20,30,50,100
Router-SW(config-if)#switchport trunk encapsulation dot1q
Router-SW(config-if)#switchport mode trunk

```

Рисунок 3.8 – Налаштування транкових каналів

```

Main-SW(config)#int e2/2
Main-SW(config-if)#switchport trunk allowed vlan 10,20,30,50,100
Main-SW(config-if)#switchport trunk encapsulation dot1q
Main-SW(config-if)#switchport mode trunk
Main-SW(config-if)#d
*Jun 13 10:50:28.709: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet2/2,
changed state to down
Main-SW(config-if)#du
*Jun 13 10:50:33.212: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet2/2,
changed state to up
Main-SW(config-if)#duplex full
Main-SW(config-if)#
Main-SW(config-if)#int e0/0
Main-SW(config-if)#switchport trunk allowed vlan 10,20,30,50,100
Main-SW(config-if)#switchport trunk encapsulation dot1q
Main-SW(config-if)#switchport mode trunk
Main-SW(config-if)#
Main-SW(config-if)#int e1/1
Main-SW(config-if)#switchport trunk allowed vlan 10,20,30,50,100
Main-SW(config-if)#switchport trunk encapsulation dot1q
Main-SW(config-if)#switchport mode trunk
Main-SW(config-if)#
Main-SW(config-if)#int e0/3
Main-SW(config-if)#switchport trunk allowed vlan 10,20,30,50,100
Main-SW(config-if)#switchport trunk encapsulation dot1q
Main-SW(config-if)#switchport mode trunk
Main-SW(config-if)#
Main-SW(config-if)#int e3/3
Main-SW(config-if)#switchport trunk allowed vlan 10,20,30,50,100
Main-SW(config-if)#switchport trunk encapsulation dot1q
Main-SW(config-if)#switchport mode trunk
Main-SW(config-if)#
Main-SW(config-if)#ex
Main-SW(config)#

```

Рисунок 3.9 – Налаштування транкових каналів

Налаштування транкових каналів на інших пристроях аналогічне.

```

Router-SW(config)#int vlan 50
Router-SW(config-if)#ip add 192.168.50.1 255.255.255.240
Router-SW(config-if)#no sh
Router-SW(config-if)#ex
Main-SW(config)#int vlan 50
Main-SW(config-if)#ip add 192.168.50.2 255.255.255.240
Main-SW(config-if)#no sh
Main-SW(config-if)#ex
Net-SW1(config)#int vlan 50
Net-SW1(config-if)#ip add 192.168.50.3 255.255.255.240
Net-SW1(config-if)#no sh
Net-SW1(config-if)#ex
Net-SW2(config)#int vlan 50
Net-SW2(config-if)#ip add 192.168.50.4 255.255.255.240
Net-SW2(config-if)#no sh
Net-SW2(config-if)#ex

```

Рисунок 3.10 – Налаштування підмережі менеджмент

Також слід налаштувати протокол віддаленого доступу SSH.

SSH (Secure Shell) – це криптографічний мережевий протокол, який забезпечує захищене та шифроване з'єднання між двома вузлами через ненадійну мережу, таку як Інтернет. Використовується для віддаленого доступу до систем, управління віддаленими комп'ютерами, передачі файлів та інших мережевих послуг, забезпечуючи конфіденційність та безпеку під час обміну даними.

```

R1(config)#crypto key generate rsa
The name for the keys will be: R1.office.local
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#
*Jun 13 14:11:57.711: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#service password-encryption
R1(config)#username admin privilege 15 secret Cisc0lCisc0l
R1(config)#enable secret Cisc0lCisc0l
R1(config)#line vty 0 4
R1(config-line)#transport input ssh
R1(config-line)#transport output ssh
R1(config-line)#exec-timeout 60 0

```

Рисунок 3.11 – Налаштування SSH на маршрутизаторі

```

Router-SW(config)#crypto key generate rsa
The name for the keys will be: Router-SW.office.local
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 7 seconds)

Router-SW(config)#
*Jun 13 15:12:00.343: %SSH-5-ENABLED: SSH 1.99 has been enabled
Router-SW(config)#service password-encryption
                        ^
% Invalid input detected at '^' marker.

Router-SW(config)#service password-encryption
Router-SW(config)#username admin privilege 15 secret Cisco1Cisco1
Router-SW(config)#enable secret Cisco1Cisco1
Router-SW(config)#line vty 0 4
Router-SW(config-line)#transport input ssh
Router-SW(config-line)#transport output ssh
Router-SW(config-line)#exec-timeout 60 0

```

Рисунок 3.12 – Налаштування SSH на комутаторі

Налаштування протоколу SSH на інших пристроях є аналогічним.

Для запобігання виникнення петель слід виконати налаштування протоколу RSTP на комутаторах.

RSTP (Rapid Per-VLAN Spanning Tree Plus) - це розширений протокол керування деревом протоколу Spanning Tree, який дозволяє швидше виявляти оптимальні шляхи для передачі даних в мережах Ethernet з використанням VLAN. RSTP є розширенням стандарту IEEE 802.1D Spanning Tree Protocol (STP), яке дозволяє створювати незалежні дерева для кожного VLAN, що сприяє підвищенню ефективності передачі даних у великих мережах.[12].

```

Router-SW#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router-SW(config)#span
Router-SW(config)#spanning-tree mode rapid-pvst
Router-SW(config)#

```

Рисунок 3.13 – Налаштування протоколу керування RSTP

```

Main-SW#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Main-SW(config)#spa
Main-SW(config)#spanning-tree mode rapid-pvst
Main-SW(config)#

```

Рисунок 3.14 – Налаштування протоколу керування RSTP

3.2 Рекомендації з налаштування й автоматизації розгортання Active Directory на сервері

Active Directory (AD) - це сервіс директорії, який використовується в операційних системах Windows Server для управління ресурсами мережі, такими як комп'ютери, користувачі, групи, додатки тощо. Основна мета Active Directory полягає в тому, щоб забезпечити централізоване управління ідентифікацією та автентифікацією користувачів і ресурсів в корпоративній мережі.

Active Directory використовує модель дерева каталогів, де кожен об'єкт (користувач, комп'ютер, принтер тощо) у мережі представлений як об'єкт в дереві, що має свої атрибути та властивості. Ці об'єкти групуються в організаційні одиниці (OU), що утворюють ієрархію для полегшення керування та організації.

Active Directory використовує протоколи, такі як LDAP (Lightweight Directory Access Protocol) для доступу до даних у директорії та Kerberos для автентифікації та управління сеансами користувачів. Основна ідея полягає у тому, щоб забезпечити ефективне управління ресурсами мережі та забезпечити безпеку та доступність для користувачів і систем в мережі.

Як вже зрозуміло, для роботи з AD слід встановити Windows Server[16].

Запустивши машину зі встановленим Windows Server першою запуститься панель менеджера сервера. Вона і є першим та основним засобом керування.

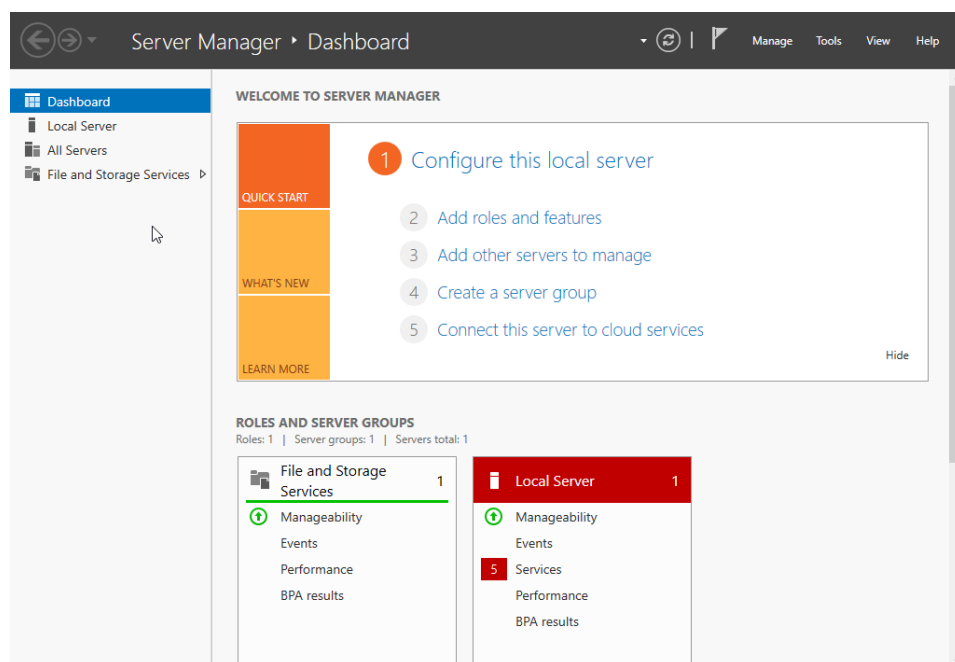


Рисунок 3.15 – Панель менеджера сервера

Слід увімкнути сервіси (ролі), а саме: «Служби домену Active Directory» та «DNS-сервер».

Служби домену Active Directory – роль, яка запускає технологію Active Directory і надає серверу роль контроллера домену. Ця роль дає змогу керувати об'єктами в мережі і створює базу даних, в якій буде зберігатись інформація про них. На цю базу і приходить запит аутентифікації користувачів при вході в обліковий запис.

DNS-сервер – це важлива частина сервісу домену Active Directory, оскільки DNS у Active Directory відіграє ключову роль у забезпеченні роботи домену AD, забезпечуючи ідентифікацію об'єктів та ресурсів, їх пошук та доступ у мережі AD.

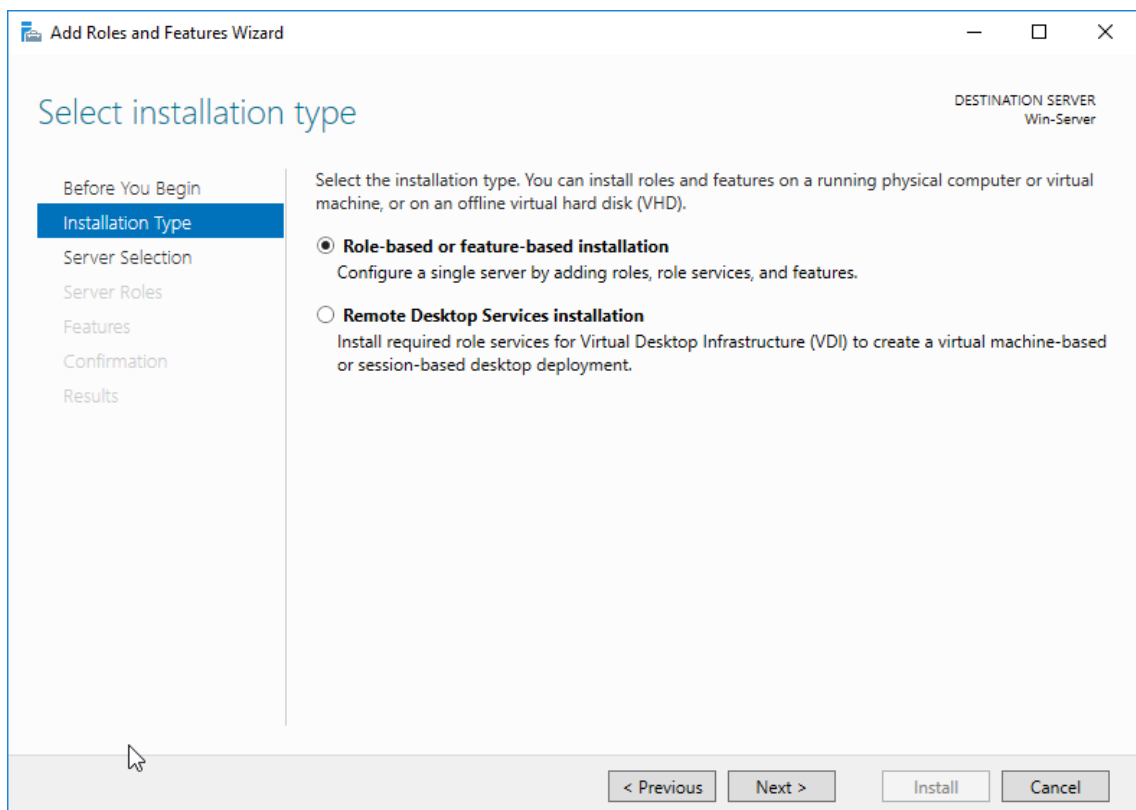


Рисунок 3.16 – Вікно додавання ролей і компонентів AD

Наступним кроком слід додати новий ліс і кореневий домен.

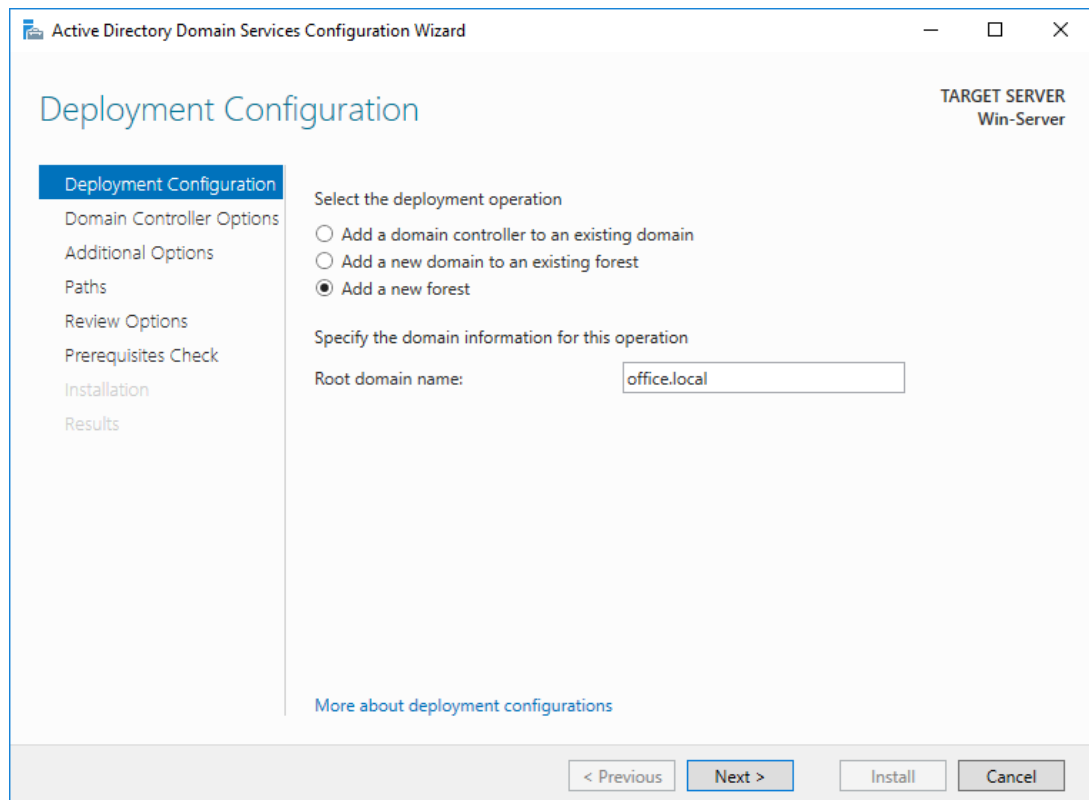


Рисунок 3.17 – Майстер налаштування домених служб AD

Наступним кроком потрібно обрати режим роботи лісу та домена, можливості контролера, та обрати пароль, що слугує для відновлення служб каталогів.

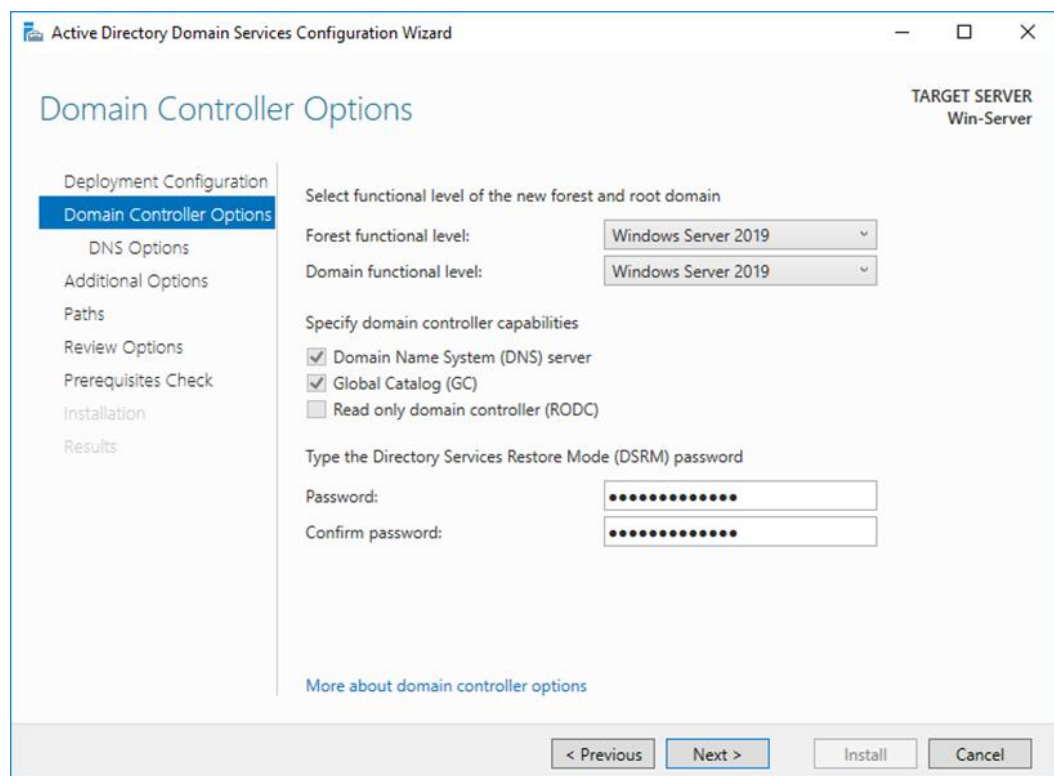


Рисунок 3.18 – Параметри контролера домена

В наступному вікні автоматично генерується NetBIOS-ім'я домену. NetBIOS (Network Basic Input/Output) – це набір програмних інтерфейсів, які дозволяють комп'ютерам у мережі взаємодіяти між собою. Є примітивнішим аналогом DNS.

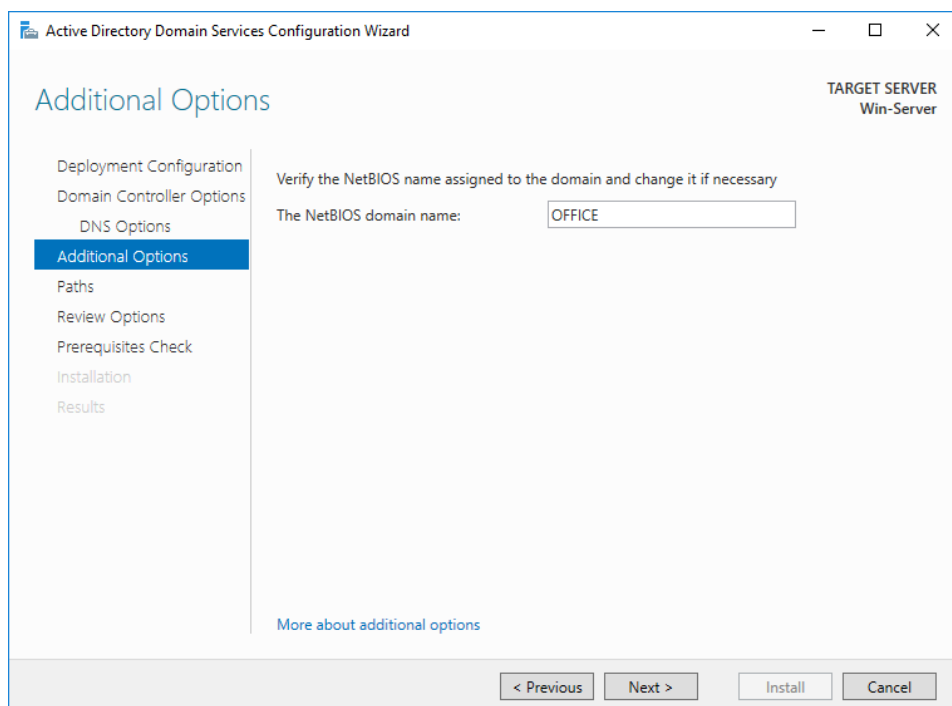


Рисунок 3.19 – Налаштування NetBIOS імені

Далі обрані налаштування проходять попередню перевірку. По завершенню перевірки, маємо змогу розпочати інсталювання. Це є останнім кроком налаштування контролера домену Active Directory.

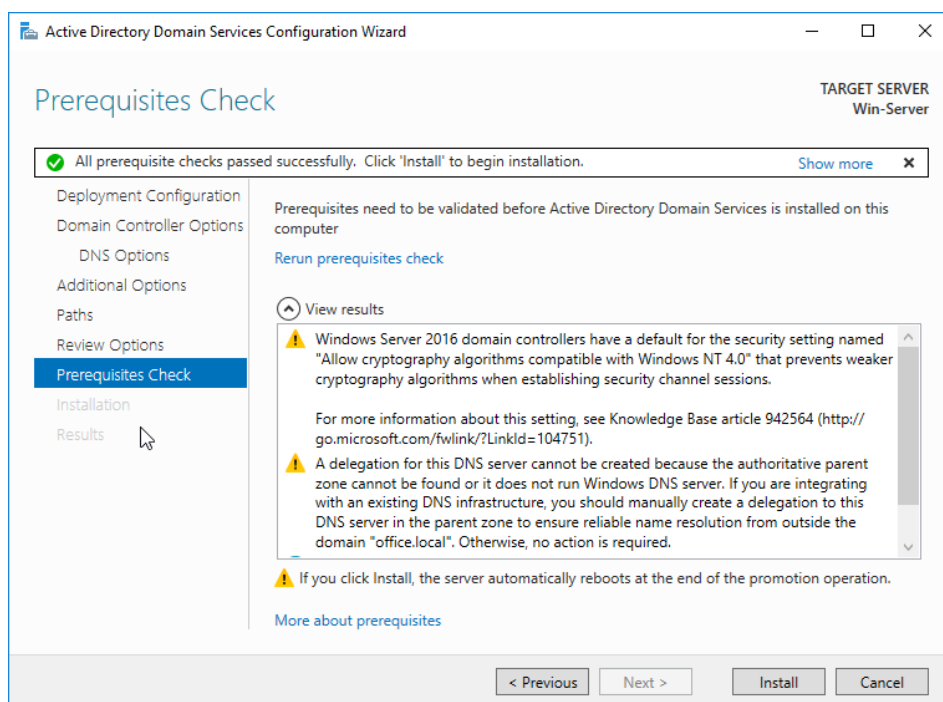


Рисунок 3.20 – Попередня перевірка вимог налаштувань

Так виглядає головне вікно керування всіма об'єктами домену в Active Directory.

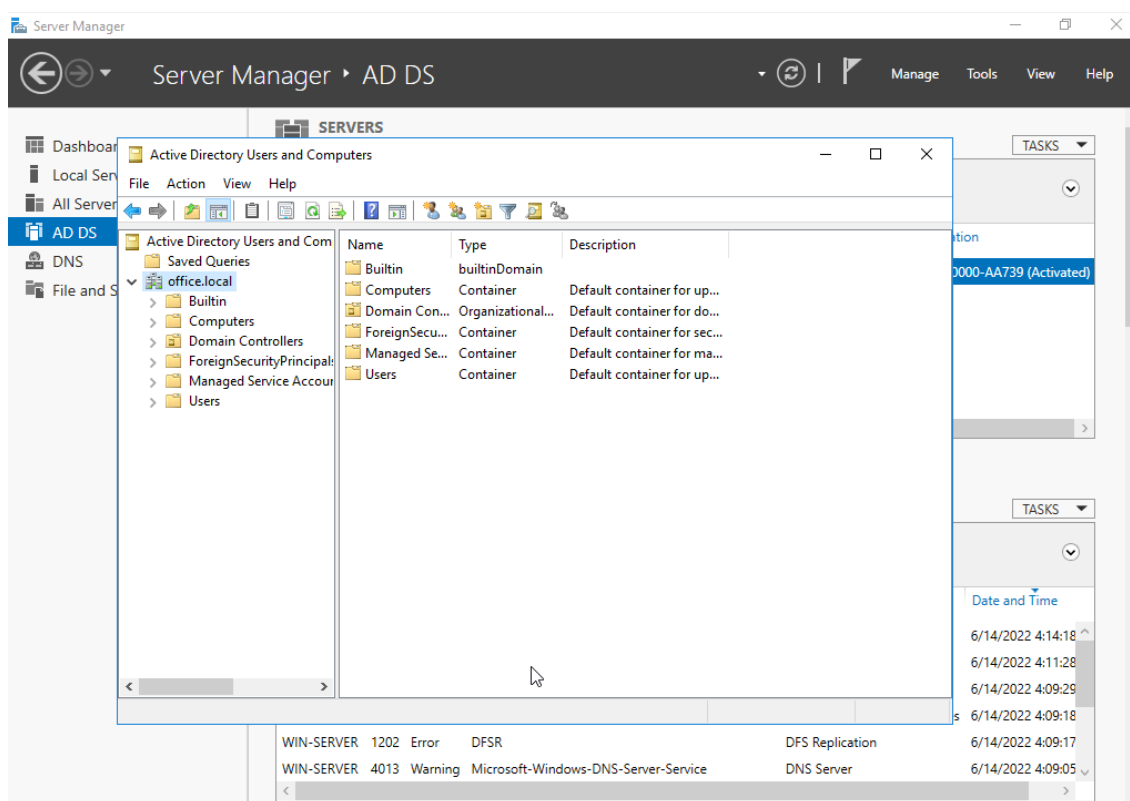


Рисунок 3.21 – Об'єкти домена

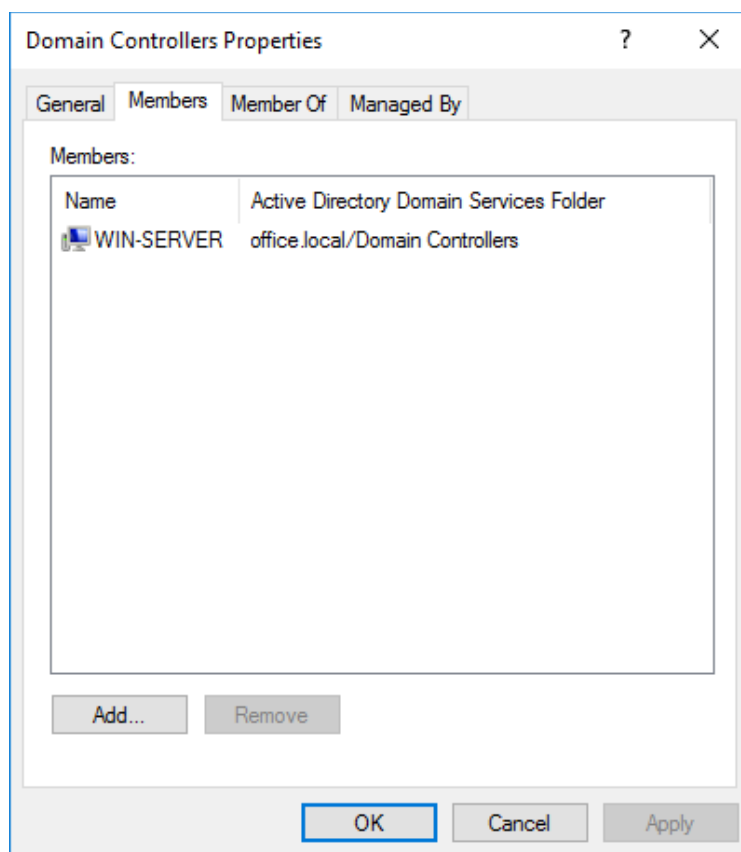
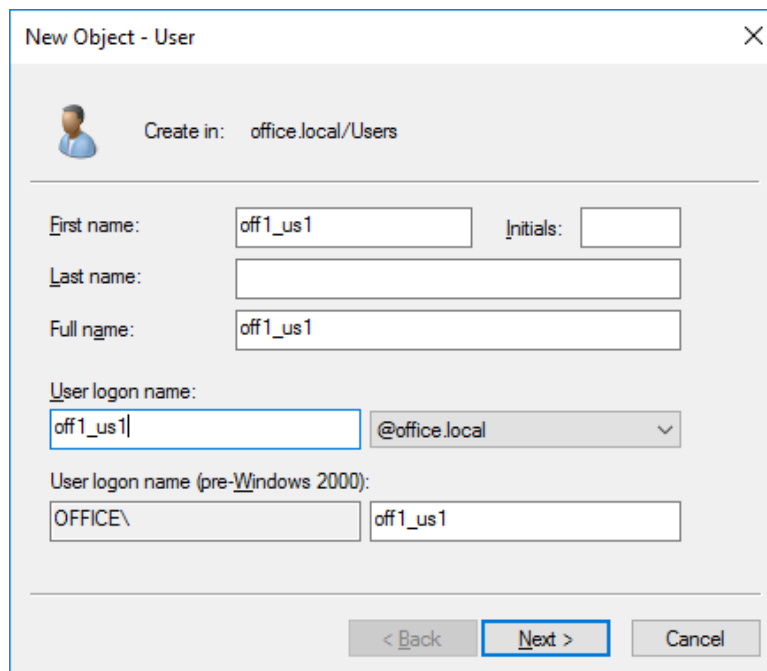


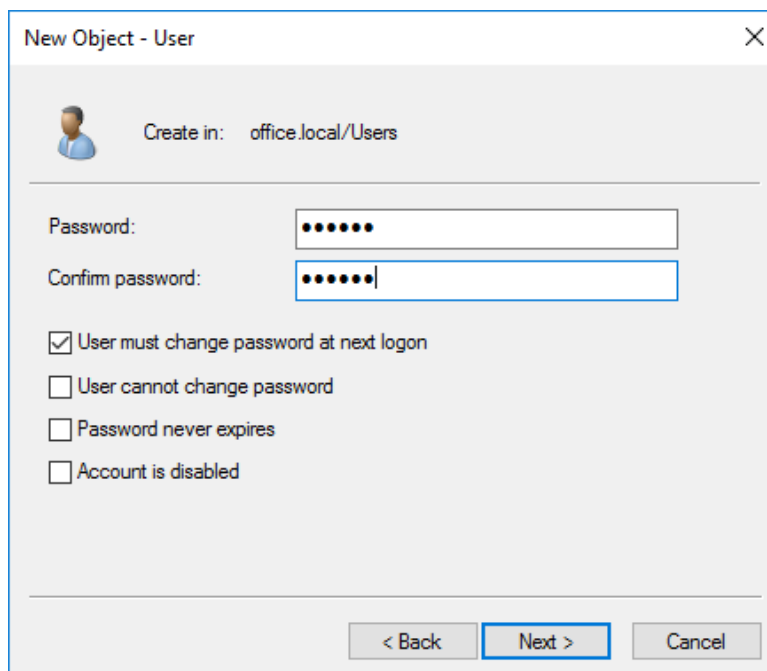
Рисунок 3.22 – Контролер домена

Створення користувачів виглядає наступним чином. В цих панелях адміністратор має змогу задавати ім'я, пароль та встановлювати певні обмеження юзеру (в подальшому все це можна буде редагувати) [15].



The screenshot shows the 'New Object - User' dialog box with the title bar 'New Object - User' and a close button. Below the title bar is a user icon and the text 'Create in: office.local/Users'. The main area contains several input fields: 'First name:' with 'off1_us1', 'Initials:' (empty), 'Last name:' (empty), 'Full name:' with 'off1_us1', 'User logon name:' with 'off1_us1' and a dropdown menu showing '@office.local', and 'User logon name (pre-Windows 2000):' with 'OFFICE\' and 'off1_us1'. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

Рисунок 3.23 – Створення користувача



The screenshot shows the 'New Object - User' dialog box with the title bar 'New Object - User' and a close button. Below the title bar is a user icon and the text 'Create in: office.local/Users'. The main area contains two password input fields: 'Password:' and 'Confirm password:', both filled with dots. Below these are four checkboxes: 'User must change password at next logon' (checked), 'User cannot change password' (unchecked), 'Password never expires' (unchecked), and 'Account is disabled' (unchecked). At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

Рисунок 3.24 – Створення користувача

Таким чином виглядають створені користувачі, що знаходяться в об'єкті Users.

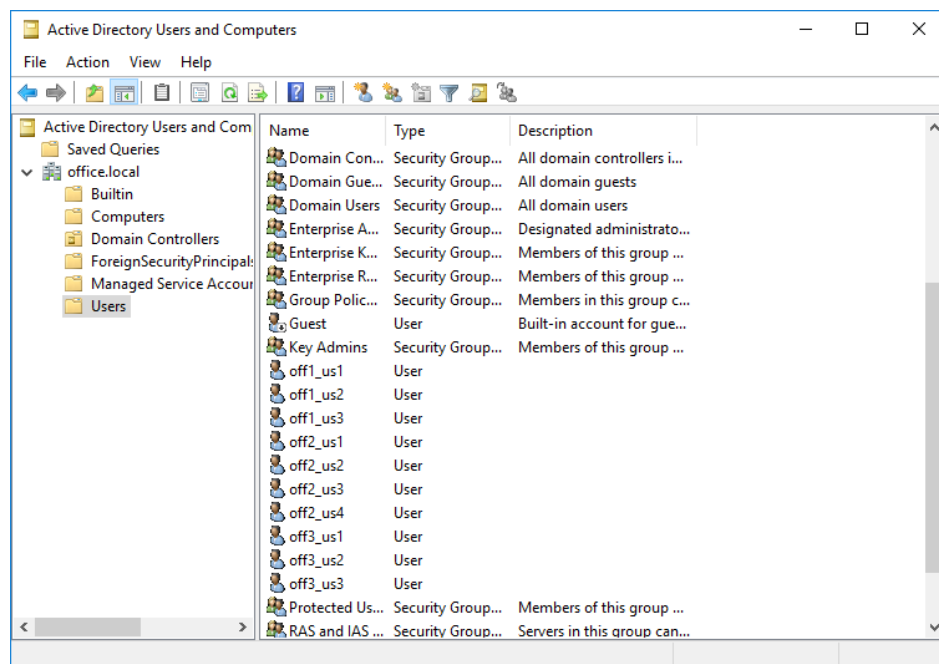


Рисунок 3.25 – Вміст об'єкту Users

Варто слідкувати за гарною структурованістю об'єктів домену. Слід створювати різні групи та об'єкти щоб компоненти не були хаотично розкидані. Це суттєво впливає на комфортність адміністрування доменом.

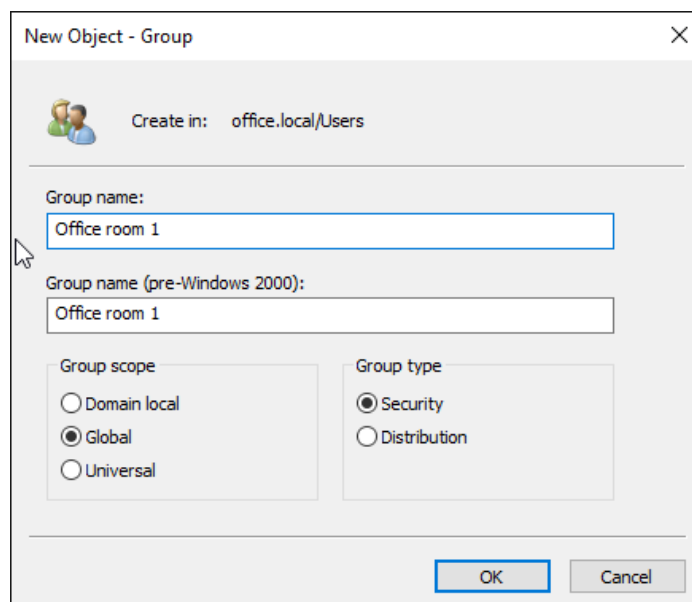


Рисунок 3.26 – Створення групи користувачів

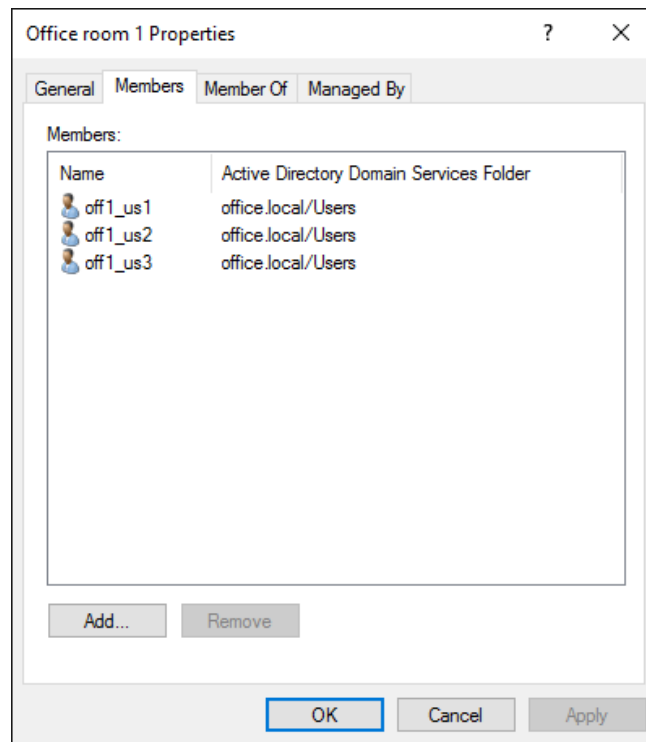


Рисунок 3.27 – Додані в групу користувачі

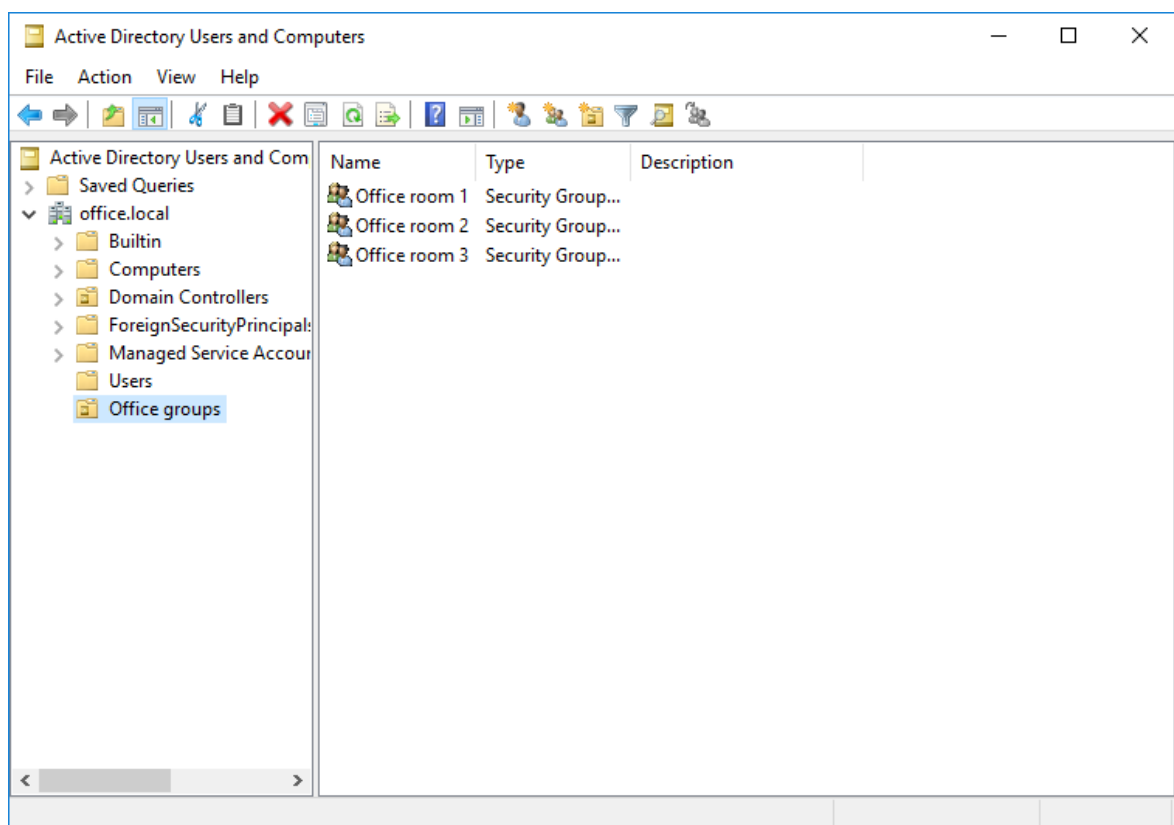


Рисунок 3.28 – Додані в новий об'єкт групи користувачів

3.3 Аналіз налаштувань системи захисту мережі в Active Directory

Active Directory (AD) надає різноманітні можливості для захисту даних та забезпечення безпеки в мережевому середовищі. Ось кілька ключових можливостей захисту даних в Active Directory представлені в таблиці 3.1:

Таблиця 3.1 – Захист даних в Active Directory

Поняття	Опис
Аутентифікація та авторизація	AD забезпечує процес аутентифікації користувачів для впевненості, що тільки авторизовані особи мають доступ до мережевих ресурсів
	Встановлення прав доступу на основі політики безпеки дозволяє контролювати, які користувачі мають доступ до конкретних об'єктів у мережі
Контроль доступу	AD надає можливість обмеження доступу до конфіденційних даних шляхом налаштування прав доступу на рівні об'єктів, папок, файлів тощо
	Встановлення ролей і груп користувачів спрощує управління правами доступу та дозволяє легко визначати, хто має доступ до певних ресурсів

Продовження таблиці 3.1 – Захист даних в Active Directory

Поняття	Опис
Шифрування даних	Active Directory може підтримувати шифрування даних для підвищення безпеки під час передачі даних через мережу або зберігання на серверах
Аудит та журналювання	Механізми аудиту дозволяють вести журнал подій та виявляти спроби несанкціонованого доступу або інші аномалії в мережі
Політика паролів	Застосування строгих політик паролів дозволяє створювати надійні паролі та змушувати користувачів періодично їх змінювати
Захист від атак	Виявлення та запобігання різноманітним атакам, включаючи перехоплення сесій, спроби несанкціонованого доступу та інші загрози
Резервне копіювання та відновлення	Резервне копіювання даних допомагає уникнути втрати інформації у випадку аварій чи втрати даних

Використання цих можливостей дозволяє підвищити безпеку і забезпечити ефективний захист даних у середовищі Active Directory. Однак важливо враховувати специфіку організації та вимоги безпеки, щоб належним чином налаштувати ці функції[17].

Найпростіший і найперший захід безпеки це надання паролю користувачам. Active Directory надає змогу адміністратору вибрати шлях або особисто надати

користувачу пароль, або довірити йому цей вибір особисто, надавши можливість обрати бажаний пароль при першому вході в мережу.

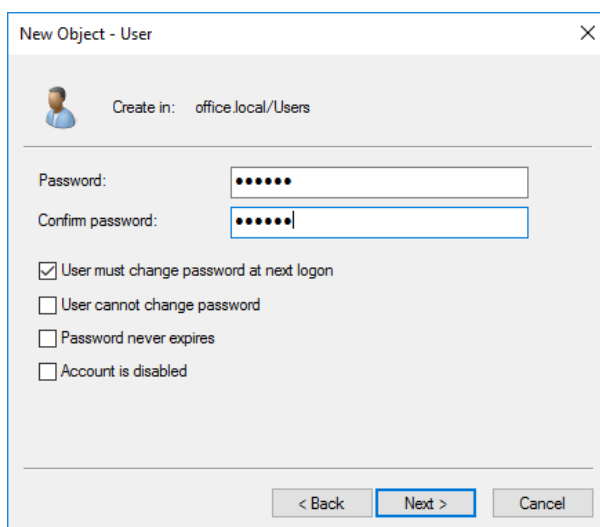


Рисунок 3.29 – Встановлення пароля користувачу

Також гарним рішенням є створення резервних облікових записів адміністратора. Як правило перший адміністраторський обліковий запис стає резервним, має найбільші права і використовується лише для спеціальних задач. Зрозуміло, що пароль в таких обліковок має бути надійним.

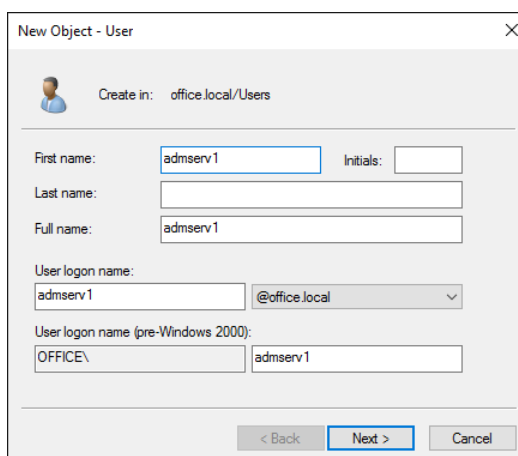


Рисунок 3.30 – Створення облікового запису адміністратора

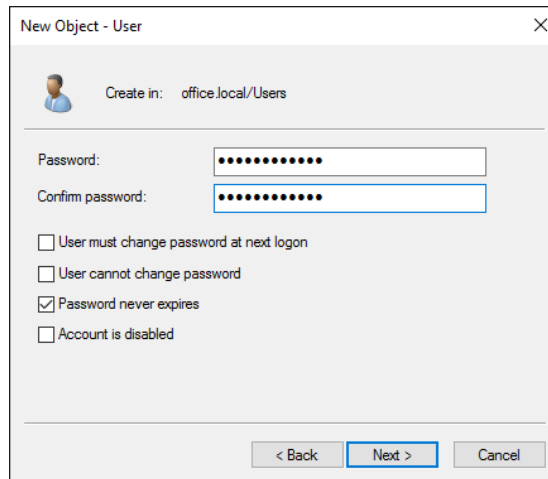


Рисунок 3.31 – Створення облікового запису адміністратора

Не слід створювати якийсь унікальний логін для резервних облікових записів адміністратора. Тоді зловмисникам буде складніше зрозуміти, що цей обліковий запис має більші права і він не стане їх першочерговою ціллю.

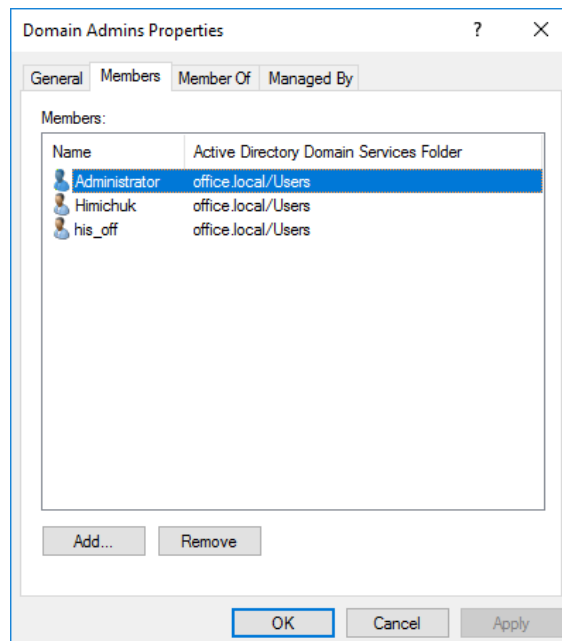


Рисунок 3.32 – Резервні записи адміністраторів

В основному всі безпекові заходи щодо користувачів налаштовуються в менеджері групових політик.

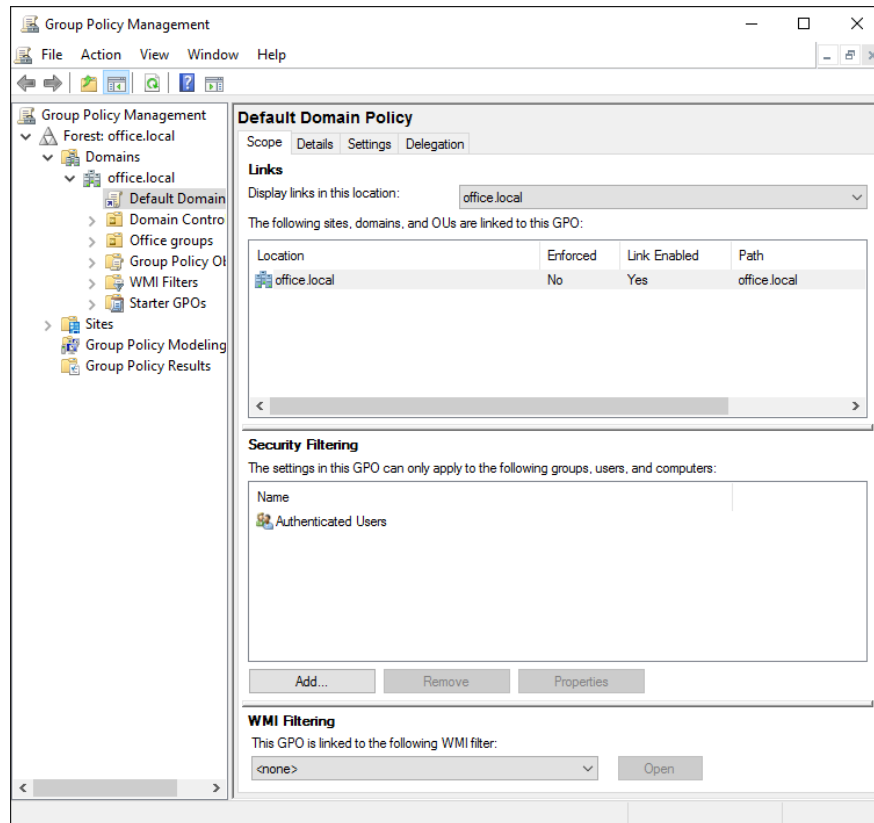


Рисунок 3.33 – Вікно менеджера групових політик

Не варто надавати звичайним користувачам занадто великі права. Це вбереже мережу від випадкових інцидентів, або не дасть зловмисникам великої користі від отримання доступу до облікового запису користувача

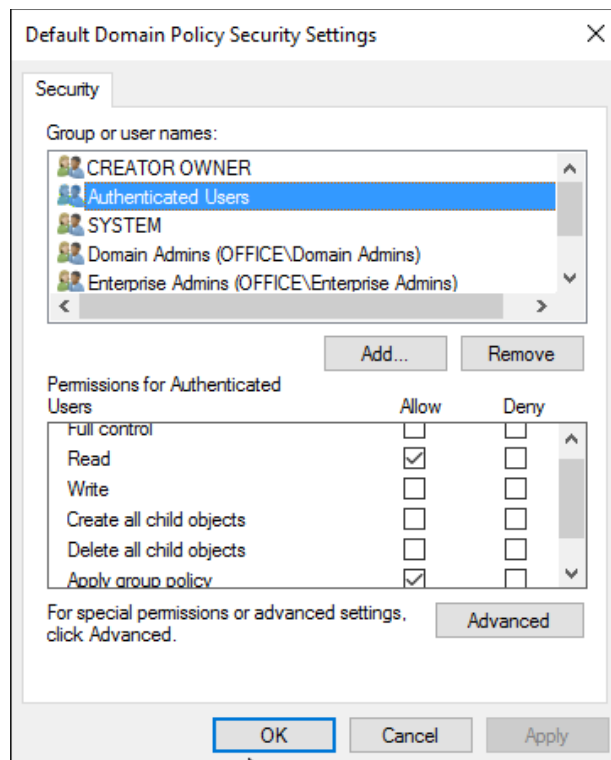


Рисунок 3.34 – Налаштування політик безпеки для користувачів

Через політики акаунтів слід налаштувати термін дії, мінімальну довжину паролів та вимоги до його складності.

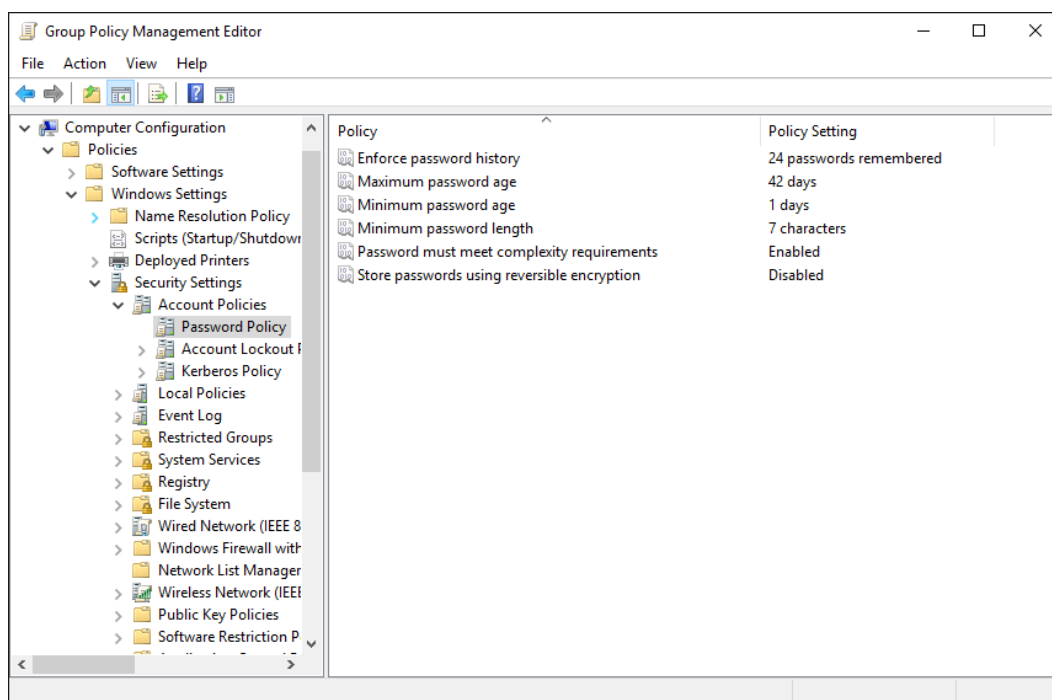


Рисунок 3.35 – Налаштування парольних політик

Також важливо налаштувати політику блокування акаунтів. Тут налаштовується час блокування, розблокування та кількість спроб входу, після яких обліковий запис буде заблоковано.

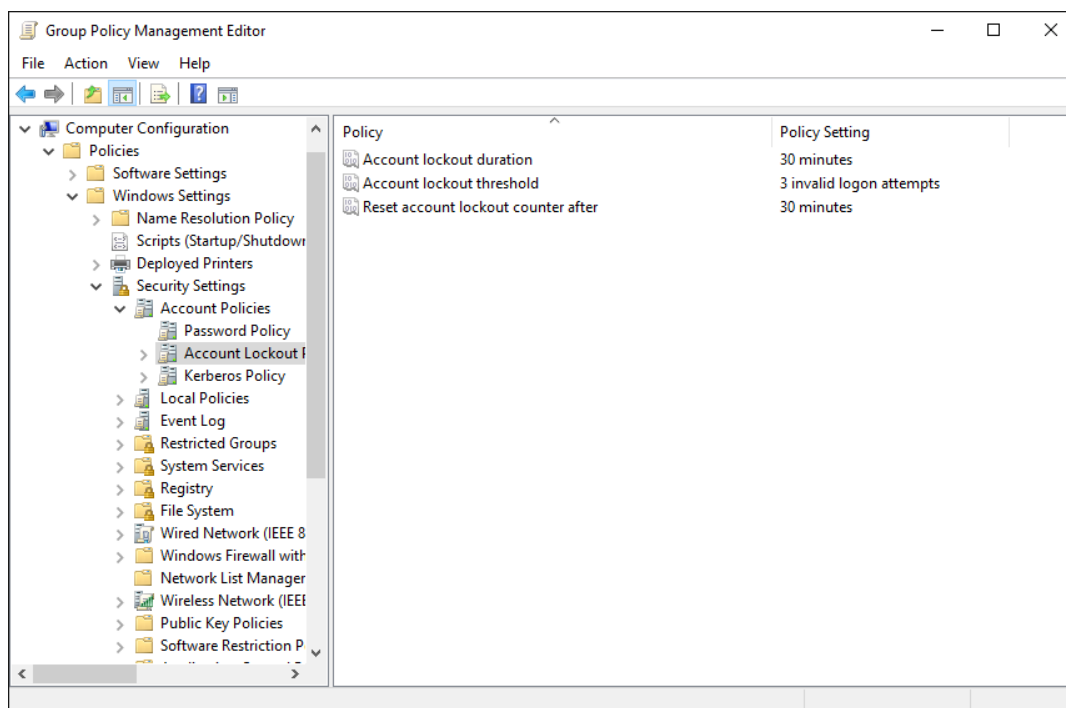


Рисунок 3.36 – Налаштування політик блокування акаунтів

Налаштування політик аудиту є не менш важливими за інші заходи безпеки, так як. дають змогу вести журналювання подій. На журналювання зазвичай виділяють достатню кількість місця.

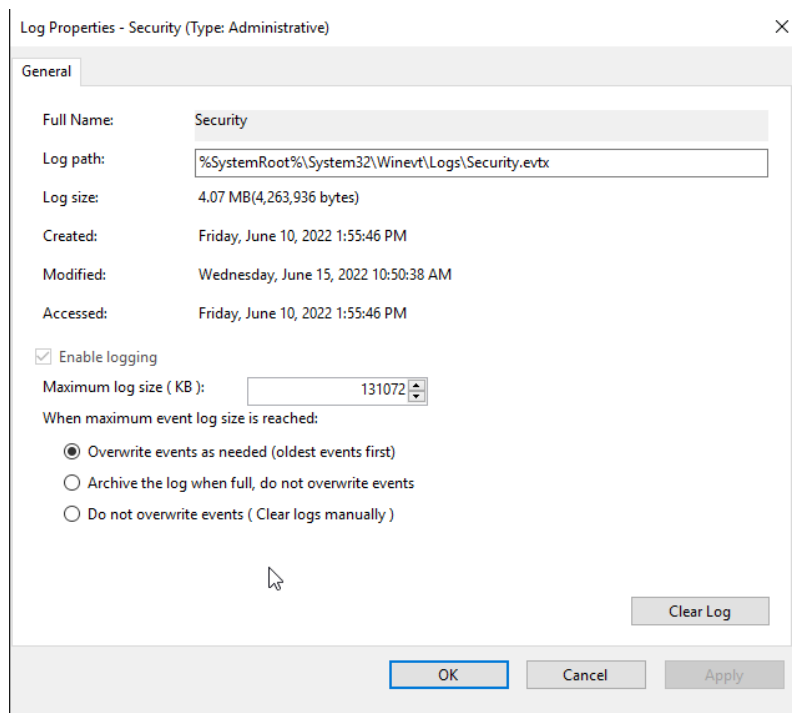


Рисунок 3.37 – Властивості журналу подій

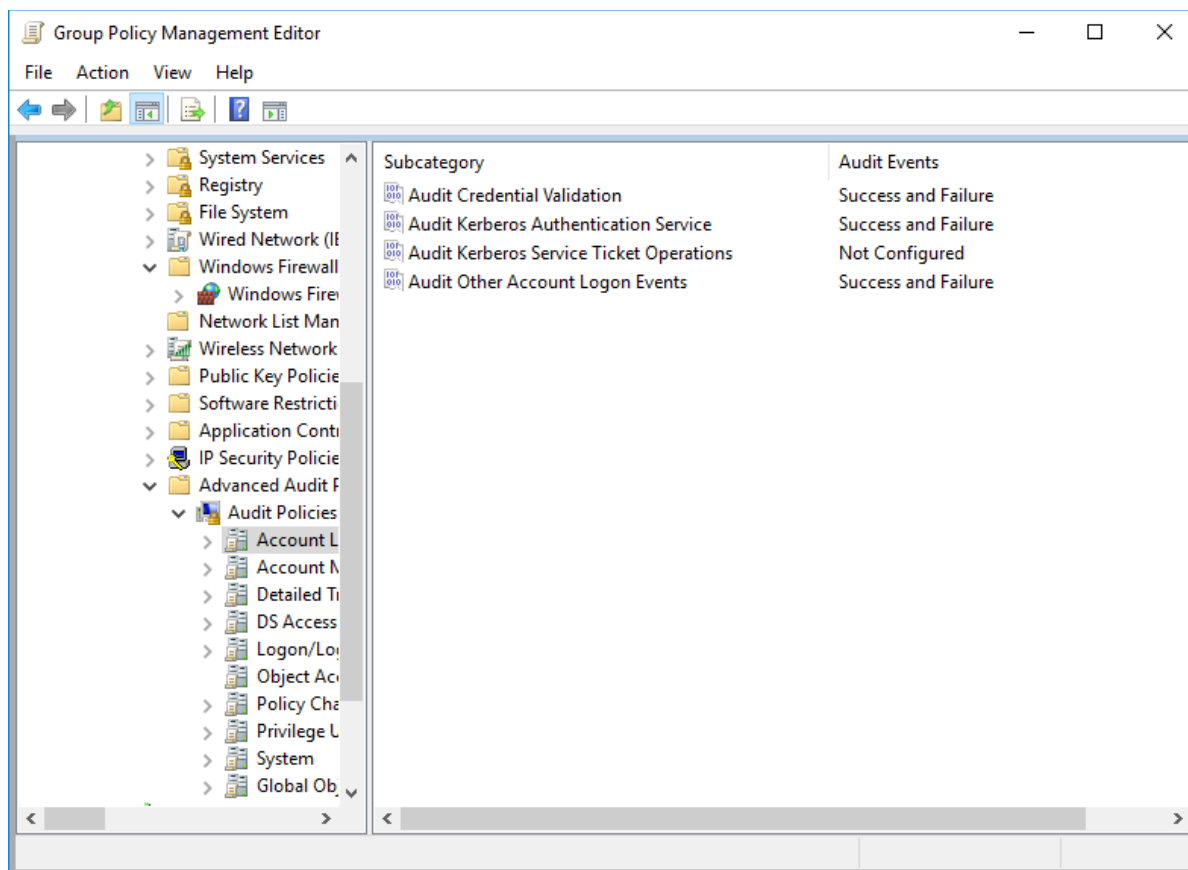


Рисунок 3.38 – Налаштування аудиту подій входу в систему

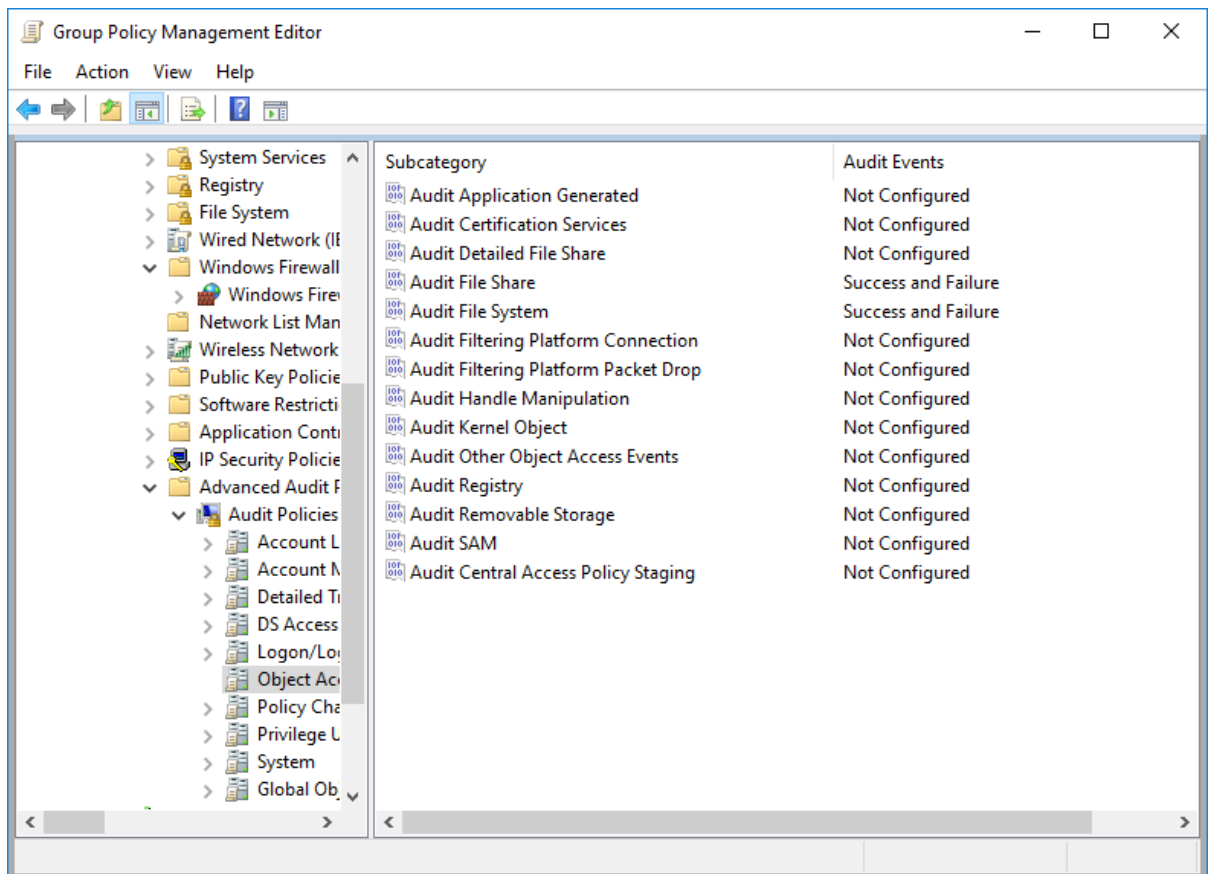


Рисунок 3.39 – Налаштування аудиту доступу до об'єктів

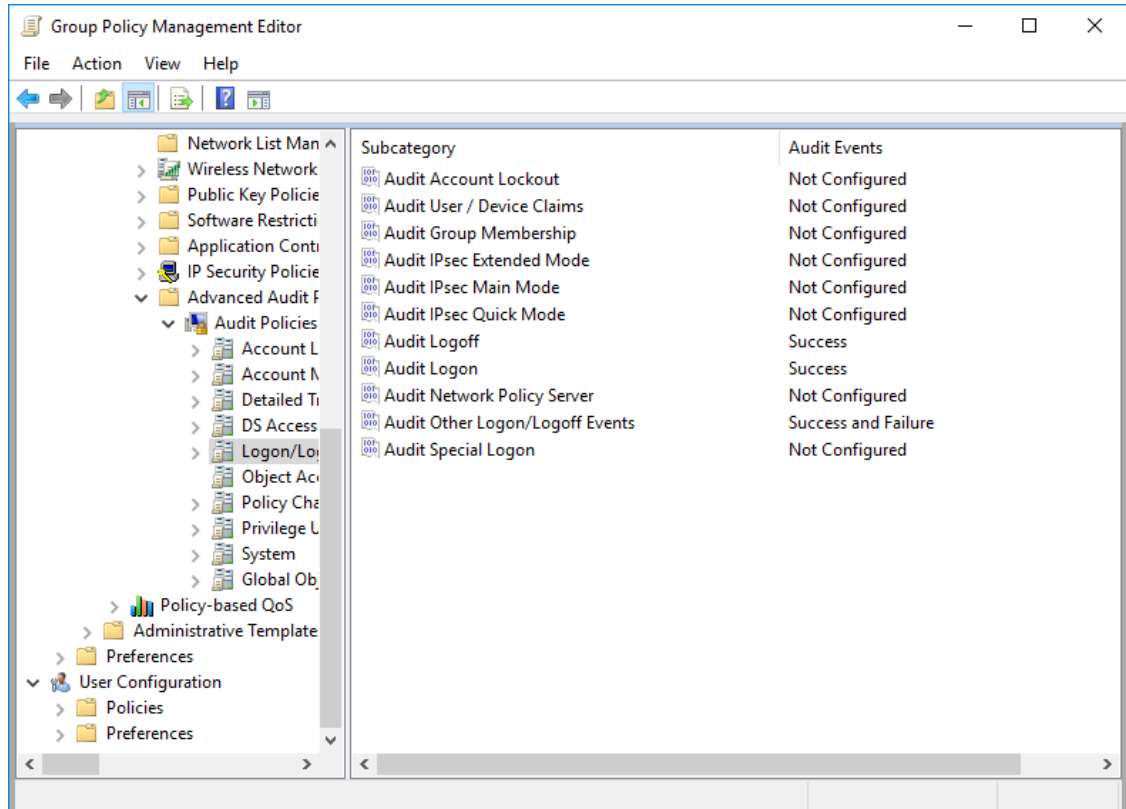


Рисунок 3.40 – Налаштування аудиту подій входу/виходу

Всі виконувані дії після правильного налаштування будуть записуватися в журнал перегляду подій.

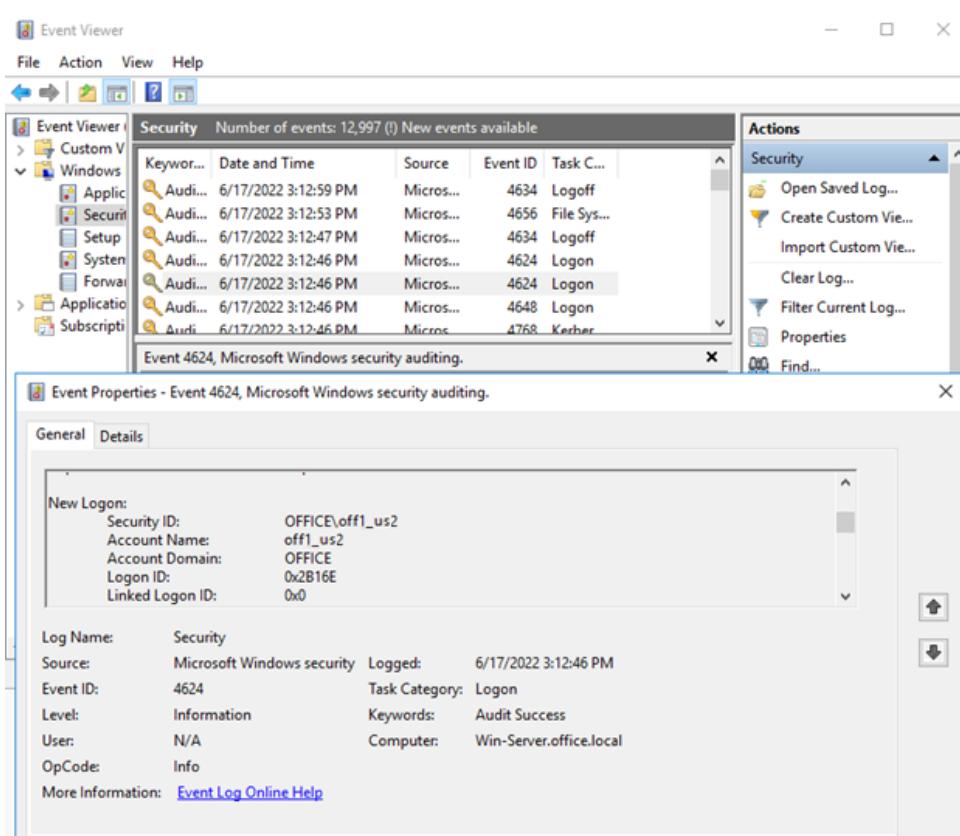


Рисунок 3.41 – Подія входу користувача записана в журнал

ВИСНОВКИ

У даній кваліфікаційній роботі було досліджено методи й технології захисту клієнт-серверної мережі організації, побудованої на базі ОС Windows Server.

У першому розділі детально розглянуто принципи згідно яких відбувається побудова мережі організації. Розписано основні компоненти з яких складається, будь-яка, комп'ютерна мережа та зазначено основні переваги її використання. Доведено важливість захисту мереж організацій шляхом аналізу потенційних загроз та вразливостей. Після проведення аналізу існуючих загроз, наведено безліч методів й технологій захисту клієнт-серверної мережі.

У другому розділі увагу було сконцентровано на аналізі проектування локальних клієнт-серверних мереж. Проведено рекомендації щодо використання обладнання з поясненням його переваг та можливостей, а потім оглянуто один із варіантів проектування мережі організації. Проаналізовано моделі загроз та моделі порушника. Як висновок до досліджень першого та другого розділів, надано рекомендовані методи та заходи власникам організацій по захисту мереж в їх організаціях.

У третьому розділі було наведено приклад налагодження системи захисту. Для розуміння основних моментів продемонстровано налагодження базових налаштувань мережі з короткими описами і правилами. Далі увага в розділі сконцентрована саме на Active Directory. Надані рекомендації з налаштування та автоматизації її розгортання з частковою демонстрацією процесу. Останнім кроком було проаналізовано теоретичні налаштування системи захисту мережі в Active Directory та надано практичний приклад, що демонструє налагодження і результат роботи системи захисту.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

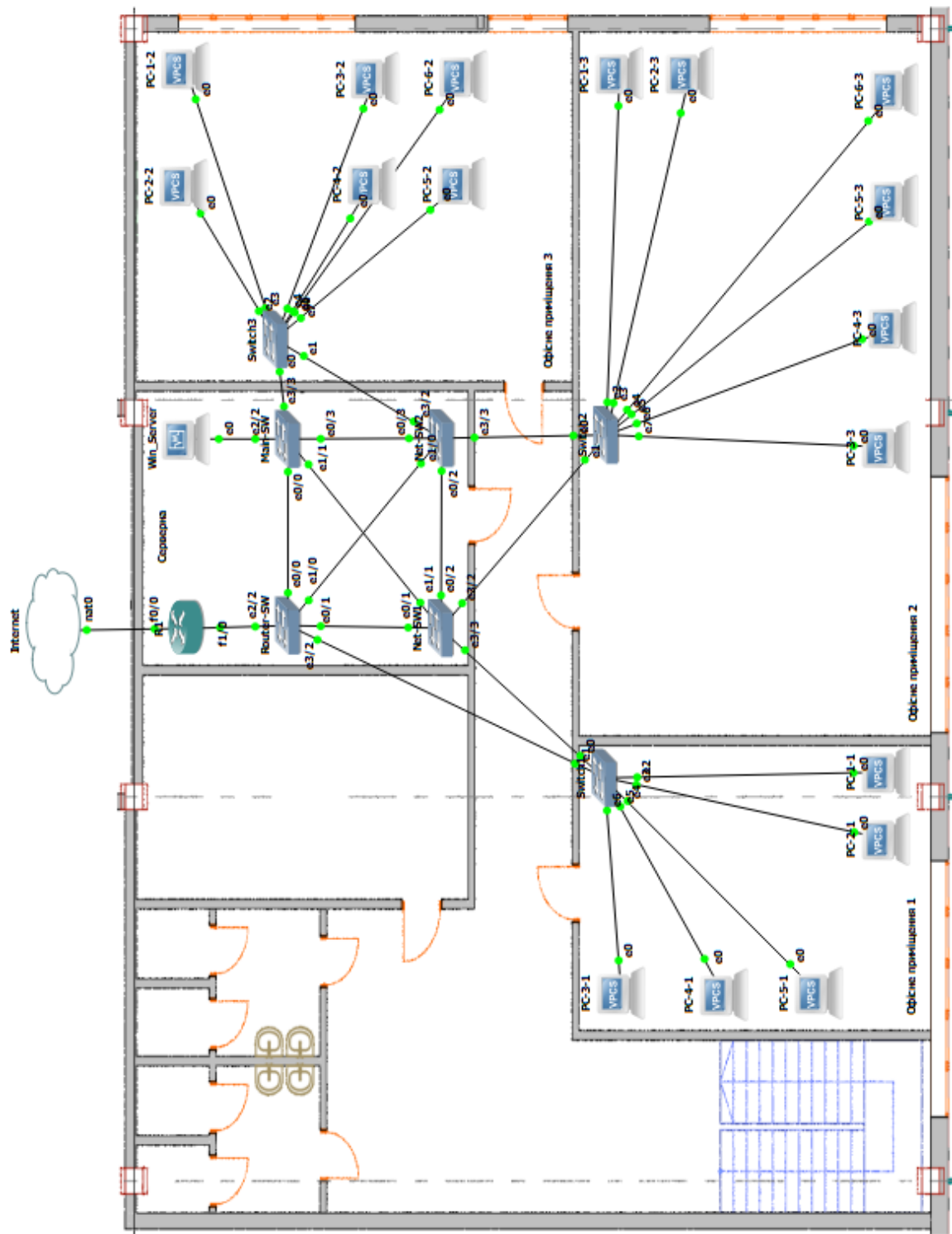
1. Основи захисту інформації в мережах [Електронний ресурс] / studfile.net, Гончарова – Режим доступу до ресурсу: <https://studfile.net/preview/9649827/page:9>
2. Безпека мережі [Електронний ресурс] – Режим доступу до ресурсу: <https://www.eset.com/ua/support/information/entsiklopediya-ugroz/bezopasnost-seti/>
3. Мережеві комутатори Cisco [Електронний ресурс] – Режим доступу до ресурсу: <https://hi-news.pp.ua/tehnka-tehnologiyi/3554-merezhev-komutatori-cisco-harakteristiki-parametri-vdguki.html>
4. Інформаційна безпека. Загрози при роботі в Інтернеті і їх уникнення [Електронний ресурс] – Режим доступу до ресурсу: <https://miyklas.com.ua/p/informatica/10-klas/informatciini-tehnologiyi-v-suspilstvi-322205/informatciina-bezpeka-navchannia-v-interneti-321523/re-0cf3c5d6-6a11-458b-b39d-889f102e9e71>
5. Технології захисту інформації [Електронний ресурс] – Режим доступу до ресурсу: <https://www.uzhnu.edu.ua/uk/infocentre/get/4186>
6. Поняття про інформаційну безпеку [Електронний ресурс] – Режим доступу до ресурсу: <https://studfile.net/preview/3740811/page:2/>
7. СУТНІСТЬ ІНФОРМАЦІЇ ТА РОЛЬ ІНФОРМАЦІЙНОЇ СИСТЕМИ В УПРАВЛІННІ ДІЯЛЬНОСТІ ОРГАНІЗАЦІЇ [Електронний ресурс] – Режим доступу до ресурсу: https://pidru4niki.com/74216/informatika/informatsiyni_sistemi_i_tehnologiyi_v_upravlinni_organizatsiyeyu
8. Мережеві служби, клієнти, сервери, ресурси. Захист при роботі у мережі [Електронний ресурс] – Режим доступу до ресурсу: <https://sites.google.com/site/kmposibnyk/lekci/tema-no9>
9. Модель загроз для інформації в ітс: мета та завдання [Електронний ресурс] – Режим доступу до ресурсу: <https://studfile.net/preview/9650054/page:7/>

10. ПОБУДОВА УЗАГАЛЬНЕНОЇ МОДЕЛІ ЗАГРОЗ ДЛЯ СИСТЕМ ІНТЕРНЕТ-БАНКІНГУ [Електронний ресурс] – Режим доступу до ресурсу: <https://ofp.cibs.ubs.edu.ua/files/1403/14vmmpum.pdf>
11. Розробка політики інформаційної безпеки [Електронний ресурс] – Режим доступу до ресурсу: <http://referatss.com.ua/work/rozrobka-politiki-informacijnoi-bezpeki-2/>
12. Configuring Rapid-PVST+ [Електронний ресурс] – Режим доступу до ресурсу: <https://www.freecnaworkbook.com/workbooks/ccna/configuring-rapid-per-vlan-spanning-tree-protocol>
13. VLAN hopping [Електронний ресурс] – Режим доступу до ресурсу: <https://sites.google.com/site/theocsic/technologies/securitynet/vlan-hopping>
14. Клієнт-серверна архітектура та ролі серверів [Електронний ресурс] – Режим доступу до ресурсу: <https://medium.com/@IvanZmerzlyi/%D0%BA%D0%BB%D1%96%D1%94%D0%B%D1%82-%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80%D0%BD%D0%B0-%D0%B0%D1%80%D1%85%D1%96%D1%82%D0%B5%D0%BA%D1%82%D1%83%D1%80%D0%B0-%D1%82%D0%B0-%D1%80%D0%BE%D0%BB%D1%96-%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80%D1%96%D0%B2-9893d8048229>
15. New Active Directory User Account [Електронний ресурс] – Режим доступу до ресурсу: <https://activedirectorypro.com/how-to-create-a-new-active-directory-user-account/>
16. AD DS Installation and Removal Wizard Page Descriptions [Електронний ресурс] – Режим доступу до ресурсу: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/ad-ds-installation-and-removal-wizard-page-descriptions#BKMK_DepConfigPage

17. Байлюк Є.М., Покотило О.А., Головня О.С., Хімічук І.С. Аналіз кібератак на Active Directory та методів підвищення рівня захищеності операційної системи Windows Server. Вісник Херсонського національного технічного університету. 2023. Вип.1. С. 123-129. – Режим доступу: https://journals.kntu.kherson.ua/index.php/visnyk_kntu/article/view/190/182

ДОДАТКИ

Проект мережі організації





Таблиця 1.2 – Поширені кіберзагрози

Поняття		Опис
<i>Несанкціонований доступ</i>	<i>Слабкі паролі</i>	Зловмисники можуть використати слабкі паролі або паролі, які легко вгадати, щоб отримати несанкціонований доступ
	<i>Атаки грубою силою</i>	Автоматизовані інструменти можуть намагатися вгадати паролі, систематично пробуючи всі можливі комбінації
<i>Перехоплення даних</i>	<i>Man-in-the-Middle</i>	Зловмисники можуть перехоплювати та маніпулювати зв'язком між клієнтом і сервером, потенційно отримуючи доступ до конфіденційних даних
	<i>Прослуховування</i>	Передача незашифрованих даних може бути перехоплена, що призведе до розкриття

		конфіденційної інформації
<i>Атаки на відмову в обслуговуванні (DoS)</i>	<i>Перевантаження сервера</i>	Потоки запитів можуть перевантажити сервер, спричиняючи його повільність або невідповідь
	<i>Розподілена відмова в обслуговуванні (DDoS)</i>	Скоординовані атаки з кількох джерел можуть посилити вплив DoS-атаки
<i>Підробка даних</i>	<i>Підробка пакетів</i>	Зловмисники можуть змінити вміст пакетів даних, що призведе до неавторизованих змін у переданій інформації
	<i>Підробка даних</i>	Маніпулювання даними для створення неправдивої інформації може мати серйозні наслідки для цілісності спілкування
<i>Неправильна конфігурація безпеки</i>	<i>Неналежний контроль доступу</i>	Неправильно налаштований контроль доступу може дозволити неавторизованим користувачам отримати доступ до

		конфіденційних ресурсів
	<i>Налаштування за замовчуванням</i>	Використання налаштувань за замовчуванням без належної зміни може виявити вразливості, добре відомі зловмисникам
<i>Зловмисне програмне забезпечення</i>	<i>Атаки на стороні клієнта</i>	Шкідливе програмне забезпечення на клієнтських пристроях може поставити під загрозу безпеку мережі, викравши облікові дані або впровадивши шкідливий код у дані, що надсилаються на сервер
	<i>Атаки на стороні сервера</i>	Зловмисне програмне забезпечення, націлене на сервери, може призвести до витоку даних, збою в роботі служби або несанкціонованого доступу

<i>Слабке шифрування</i>	<i>Незахищені протоколи</i>	використання застарілих або незахищених протоколів шифрування може полегшити зловмисникам розшифровку зашифрованих даних
	<i>Проблеми з керуванням ключами</i>	погані методи керування ключами можуть поставити під загрозу конфіденційність зашифрованих даних
<i>Недостатня реєстрація та моніторинг</i>	<i>Відсутність видимості</i>	Неадекватне ведення журналів і моніторинг ускладнюють виявлення підозрілих дій і своєчасне реагування на них
	<i>Нездатність виявити аномалії</i>	без належного моніторингу незвичайні моделі або поведінка, що вказують на атаку, можуть залишитися непоміченими
<i>Соціальна інженерія</i>	<i>Фішинг</i>	Обманом змусити користувачів розкрити

		конфіденційну інформацію за допомогою оманливих електронних листів або повідомлень може поставити під загрозу безпеку зв'язку клієнт-сервер
	<i>Маніпулювання користувачами</i>	Використання людської психології для маніпулювання користувачами, щоб змусити їх виконувати дії, які ставлять під загрозу безпеку
<i>Програмне забезпечення без виправлень</i>	<i>Застаріле програмне забезпечення</i>	Невиконання регулярних оновлень і виправлень як клієнтського, так і серверного програмного забезпечення може залишити відомі вразливості невирішеними
<i>SQL ін'єкція</i>	<i>Ін'єкційні атаки</i>	Зловмисники можуть використати погано продезінфіковані дані користувача, щоб

		ввести зловмисні SQL-запити в базу даних. Це може призвести до несанкціонованого доступу, маніпулювання даними або навіть видалення записів
<i>Міжсайтовий скриптинг (XSS)</i>	<i>Впровадження сценаріїв</i>	Шкідливі сценарії впроваджуються на веб-сторінки, які потім надаються користувачам. Ці сценарії можуть викрадати конфіденційну інформацію, наприклад облікові дані для входу, у клієнтів
<i>Міжсайтова підробка запитів (CSRF)</i>	<i>Неавторизовані запити</i>	Зловмисники обманом змушують користувачів несвідомо надсилати запити на сервер, на якому користувач пройшов автентифікацію. Це може призвести до виконання дій від імені

		користувача без його згоди
<i>Перехоплення сеансу</i>	<i>Викрадені маркери сеансу</i>	Зловмисники можуть перехопити або отримати маркери сеансу за допомогою аналізу сеансу або іншими способами та використовувати їх, щоб імітувати дійсний сеанс користувача
<i>Експлойти нульового дня</i>	<i>Невідомі вразливості</i>	Використання вразливостей, які ще не відомі постачальнику програмного забезпечення чи спільноті безпеки, може призвести до успішних атак до того, як будуть розроблені та розгорнуті виправлення
<i>Підробка DNS</i>	<i>Маніпульовані відповіді DNS</i>	Зловмисники порушують процес вирішення DNS, перенаправляючи клієнтів на шкідливі сервери. Це може призвести до несанкціонованого

		доступу або перехоплення даних
<i>Обхід брандмауера веб-додатків (WAF)</i>	<i>Обхід заходів безпеки</i>	Досвідчені зловмисники можуть знайти способи обійти WAF або інші механізми безпеки, дозволяючи їм використовувати вразливості базової програми або сервера
<i>Незахищені API</i>	<i>Слабка автентифікація</i>	API, у яких відсутні належні механізми автентифікації, можна використати для отримання несанкціонованого доступу до даних або послуг
	<i>Неправильна авторизація</i>	Неправильно налаштовані дозволи API можуть дозволити зловмисникам виконувати дії, до яких вони не повинні мати доступу
<i>Небезпечне завантаження файлів</i>	<i>Виконання зловмисних файлів</i>	Якщо функція завантаження файлів не захищена належним

		чином, зловмисники можуть завантажити зловмисні файли, які можна виконати на сервері, що призведе до різних проблем безпеки.
<i>Внутрішні загрози</i>	<i>Зловмисні інсайдери</i>	Співробітники або особи з інсайдерським доступом можуть навмисно чи ненавмисно поставити під загрозу безпеку мережі, витікаючи конфіденційну інформацію або сприяючи атакам
<i>Програми-вимагачі</i>	<i>Шифрування даних</i>	Зловмисники можуть шифрувати критично важливі дані на серверах, вимагаючи викуп за ключ дешифрування. Це може призвести до значної втрати даних і збоїв у роботі
<i>Фізична безпека</i>	<i>Несанкціонований доступ до обладнання</i>	Доступ до обладнання: фізичний доступ до серверів може призвести до

		неавторизованих модифікацій, крадіжки даних або втручання
<i>Вразливості нових технологій</i>	<i>Проблеми безпеки Інтернету речей</i>	у контексті клієнт-сервер із залученням пристроїв Інтернету речей такі вразливості, як слабка автентифікація пристрою та незахищений зв'язок, можуть становити серйозні ризики
	<i>Проблеми з безпекою блокчейну</i>	Проблеми, пов'язані зі смарт-контрактами, алгоритмами консенсусу та безпекою гаманця, можуть вплинути на безпеку клієнт-серверних програм на основі блокчейну