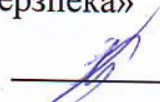


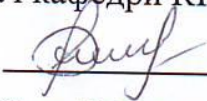
Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми захисту клієнт-серверної
мережі організації на базі ОС Windows»

Виконав студент 4-го курсу групи КБ-2
спеціальності 125 «Кібербезпека»

 Хімічук І.С.
Керівник старший викладач кафедри КІ та КБ

 Байлюк Є.М.

Рецензент доцент кафедр КІ та КБ, к.пед.н.

 Головня О.С.

Житомир – 2022

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

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної

інженерії та кібербезпеки

 Андрій Єфіменко

1 березня 2022 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Хімічук Ілля Сергійович

Тема роботи: «Проект підсистеми захисту клієнт-серверної мережі організації на базі ОС Windows»

затверджена Наказом університету від 1 березня 2022 р. № 128/с

Термін здачі студентом закінченої роботи 23 червня 2022 р.

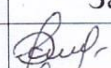
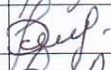
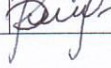
Вихідні дані роботи:

1. Об'єктом дослідження є процес захисту об'єктів
2. Предметом дослідження є підсистема захисту клієнт-серверної мережі

Обладнання та програмне забезпечення:

1. Інженерний план приміщення
2. Маршрутизатор Cisco 7201
3. Комутатор Cisco Catalyst 2960
4. 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	Байлюк Є.М.	 06.03.2022	06.03.2022
2	Байлюк Є.М.	 20.04.2022	20.04.2022
3	Байлюк Є.М.	 11.05.2022	11.05.2022

Студент

Керівник

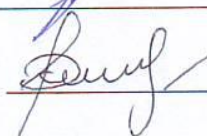
Хімічук І.С.

Байлюк Є.М.

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	6 березня 2022 – 7 березня 2022	Виконано
2	Пошук та аналіз інформації стосовно безпеки, загроз ІКС	8 березня 2022 – 11 березня 2022	Виконано
3	Аналіз методів захисту клієнт-серверної мережі	12 березня 2022 – 16 березня 2022	Виконано
4	Розробка проєкту мережі організації	17 березня 2022 – 20 березня 2022	Виконано
5	Складання моделі загроз	21 березня 2022 – 25 березня 2022	Виконано
6	Проектування підсистеми захисту клієнт-серверної мережі	26 березня 2022 – 2 квітня 2022	Виконано
7	Розробка політики безпеки клієнт серверної мережі	3 квітня 2022 – 6 квітня 2022	Виконано
8	Налаштування пристроїв мережі	7 квітня 2022 – 12 квітня 2022	Виконано
9	Налаштування й розгортання AD та налаштування підсистеми захисту мережі	13 квітня 2022 – 19 квітня 2022	Виконано
10	Тестування й аналіз роботи системи	20 квітня 2022 – 24 квітня 2022	Виконано
11	Написання пояснювальної записки	25 квітня 2022 – 29 квітня 2022	Виконано
12	Підготовка доповіді та презентації	30 квітня 2022 – 31 квітня 2022	Виконано
13	Отримання відгуку та рецензії на кваліфікаційну роботу	6 червня 2022 – 7 червня 2022	Виконано
14	Захист	23 червня 2022	Виконано

Студент  Хімічук І.С.

Керівник  Байлюк Є.М.

АНОТАЦІЯ

Кваліфікаційна робота складається з проекту підсистеми захисту клієнт-серверної мережі організації на базі ОС Windows та пояснювальної записки до нього. Пояснювальна записка містить 78 сторінок, 91 ілюстрацію.

Метою роботи є розробка проекту підсистеми захисту клієнт-серверної мережі на базі ОС Windows.

В роботі було обґрунтовано актуальність захисту клієнт-серверної мережі організації. Проаналізовано можливі загрози та наведено можливі засоби та методи захисту мережі від них. Також в роботі було обґрунтовано вибір мережевих пристроїв Cisco, надана основна інформація про використовувані комутатори та маршрутизатор. З обраних пристроїв, комп'ютерів та сервера на базі Windows Server 2019, розроблено та налагоджено проєкт мережі та проєкт її захисту. Схема була накладена на план приміщення, що дало змогу візуально продемонструвати, як приблизно будуть розподілені пристрої в реальній організації. Наведено модель загроз, опис політики безпеки, розгортання Active Directory на базі Windows Server. Також наведено результати тестування працездатності системи.

Ключові слова: ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНА СИСТЕМА, ЗАХИСТ ІНФОРМАЦІЇ, КОМП'ЮТЕРНІ МЕРЕЖІ, ЗАГРОЗИ МЕРЕЖІ, КЛІЄНТ-СЕРВЕРНА МЕРЕЖА, КОРИСТУВАЧ, ОБЛІКОВИЙ ЗАПИС, WINDOWS SERVER, ACTIVE DIRECTORY.

					КІК.КР.Б – 125 – 24 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми захисту клієнт–серверної мережі організації на базі ОС Windows.	Літ.	Арк.	Аркушів
Розроб.		Хімічук І.С..		20.06.22				
Керівник		Байлюк Є.М.		20.06.22				
Реценз.		Головня О.С.		20.06.22				
Затверд.		Єфіменко А.А.		20.06.22	ФІКТ, Гр. КБ-2			

ANNOTATION

The qualifying work consists of the project of the subsystem of protection of the client-server network of the organization based on Windows OS and the explanatory note to it. The explanatory note contains 78 pages, 91 illustrations.

The purpose of this work is to develop a project of the client-server network security subsystem based on Windows.

The urgency of protection of the client-server network of the organization is substantiated in the work. Possible threats are analyzed and possible means and methods of network protection from them are given. The paper also substantiates the choice of Cisco network devices, provides basic information about the switches and router used. From selected devices, computers and servers based on Windows Server 2019, designed and configured network design and security project. The scheme is superimposed on the plan of the room, which allows to demonstrate how approximately the devices will be distributed in the real organization. The threat model, security policy description, Active Directory deployment based on Windows Server are given. The results of system performance testing are also presented.

Keywords: INFORMATION AND COMMUNICATION SYSTEM, INFORMATION PROTECTION, COMPUTER NETWORKS, NETWORK THREATS, CLIENT-SERVER NETWORK, ACTIVITIES, USED BY USER

		<i>Хімічук І.С.</i>			<i>КІК.КР.Б – 125 – 24 – ПЗ</i>	<i>Арк.</i>
		<i>Байлюк Є.М.</i>				<i>5</i>
<i>Змн.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		

ЗМІСТ

ВСТУП	8
РОЗДІЛ 1 ОБҐРУНТУВАННЯ НЕОБХІДНОСТІ ЗАХИСТУ МЕРЕЖІ ОРГАНІЗАЦІЇ.....	9
1.1 Роль безпеки інформаційно–комунікаційних систем	9
1.2 Аналіз можливих загроз клієнт–серверній мережі на базі ОС Windows	12
1.3 Засоби та методи захисту клієнт–серверної мережі організації на базі ОС Windows.....	17
РОЗДІЛ 2 ПРОЄКТ ПІДСИСТЕМИ ЗАХИСТУ КЛІЄНТ–СЕРВЕРНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ	24
2.1 Розробка проєкту мережі організації	24
2.2 Розробка моделі загроз організації.....	30
2.3 Розробка проєкту підсистеми захисту клієнт–серверної мережі.....	31
2.4 Розробка політики безпеки клієнт–серверної мережі організації.....	33
РОЗДІЛ 3 НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ ПІДСИСТЕМИ ЗАХИСТУ КЛІЄНТ–СЕРВЕРНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ	37
3.1 Налаштування пристроїв мережі.....	37
3.2 Налаштування й автоматизація розгортання Active Directory на базі Windows Server 2019	44
3.3 Налаштування підсистеми захисту клієнт–серверної мережі на базі ОС Windows.....	57
3.4 Тестування підсистеми захисту	67
ВИСНОВКИ.....	75
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	76
ДОДАТКИ.....	79

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПЗ – програмне забезпечення

ІС – інформаційна система

ІКС – інформаційно-комунікаційна система

КСЗІ – комплексна система захисту інформації

MAC – Media Access Control

NAT – Network Address Translation

AD – Active Directory

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Сьогодні інформаційні технології розвиваються дуже швидко, проте люди не завжди замислюються над цінністю інформації. Тому її крадіжка – це одна з головних цілей кіберзлочинців. З інформацією, отриманою під час атаки, злочинці можуть заволодіти вашими логінами, паролями, документами, коштами та іншим.

Актуальність теми. Отже, система захисту клієнт серверної мережі зараз важлива, як ніколи раніше, тому що всі організації збирають, обробляють та зберігають величезні обсяги даних на комп'ютерах та інших пристроях. Більшість цих даних може бути конфіденційними, для них несанкціонований доступ або викриття зовсім недопустимі. Кібератаки стають все серйознішими та витонченішими, компаніям та організаціям потрібно вжити відповідних заходів для гідної відсічі та забезпечення якісного захисту конфіденційної інформації.

Метою кваліфікаційної роботи є розробка проекту підсистеми захисту клієнт–серверної мережі організації на базі ОС Windows.

Встановлена мета обумовлює наступні завдання:

- обґрунтувати необхідність розробки системи захисту клієнт–серверної мережі організації
- розробити проєкт системи захисту клієнт–серверної мережі
- налагодити та протестувати систему захисту клієнт–серверної мережі

Об'єктом дослідження є процес захисту інформації мережі.

Предметом дослідження є дослідження системи захисту клієнт–серверної мережі організації.

У процесі виконання кваліфікаційної роботи було розроблено проєкт підсистеми захисту клієнт–серверної мережі організації на базі ОС Windows.

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 ОБҐРУНТУВАННЯ НЕОБХІДНОСТІ ЗАХИСТУ МЕРЕЖІ ОРГАНІЗАЦІЇ

1.1 Роль безпеки інформаційно–комунікаційних систем

Захист інформації є однією з серйозних та важливих проблем. Протягом усієї історії людства шляхи вирішення цієї проблеми повністю залежали від рівня розвитку технологій. У нашому інформаційному суспільстві технологія відіграє роль активатора цієї проблеми – комп'ютерні злочини стали візитівкою сьогодення.

Комп'ютерними злочинами називають ті, які пов'язані з втручанням у роботу комп'ютера, та злочини, у вчиненні яких комп'ютери використовуються як необхідні технічні засоби.

Серед причин комп'ютерних злочинів та пов'язаних з ними розкрадань інформації можна виділити такі:

- швидкий перехід від традиційних паперових технологій зберігання та передачі інформації до електронних при одночасному відставанні від технологій захисту інформації, записаної на машинних носіях;
- широке використання локальних мереж, створення глобальних мереж та розширення доступу до інформаційних ресурсів;
- постійне ускладнення програмного забезпечення, що значно знижує їхню надійність та збільшує кількість вразливостей.

Сьогодні ніхто не може назвати точну цифру загальної шкоди від комп'ютерних злочинів, але експерти сходяться на думці, що відповідні суми вимірюються мільярдами доларів. Серед основних чинників можна назвати такі:

- збитки, спричинені ситуацією, коли працівники організації, що неспроможні виконувати свої обов'язки через непрацездатність системи (мережі);
- вартість викрадених та скомпрометованих даних;
- витрати на відновлення системи, на перевірку її цілісності, на усунення вразливостей тощо

Також слід враховувати морально–психологічні наслідки для користувачів, персоналу і власників ІС та інформації. Що ж до порушення безпеки критичних додатків у державному і військовому управлінні, атомній енергетиці, медицині, космічній галузі та фінансах, то воно може мати серйозні наслідки для

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

навколишнього середовища, економіки й безпеки держави, здоров'я і навіть людського життя.

Економічні та правові питання, приватна та комерційна таємниця, національна безпека – усе це зумовлює необхідність захисту інформації та ІС [10].

Відповідно до *Закону України «Про захист інформації в інформаційно–комунікаційних системах»* захист інформації є сукупністю організаційно–технічних заходів й правових норм, спрямованих на запобігання заподіяння шкоди інтересам власника інформації або осіб, які користуються інформацією.

Останнім часом фахівці використовують кілька концепцій визначення захищеності інформації в ІС. Такими поняттями є *захист інформації в комп'ютерних системах*, *захист інформації в комп'ютерних системах і мережах*, *захист інформації в автоматизованих системах*, *захист інформації в інформаційно–комунікаційних системах*. Часто ці поняття використовують як синоніми, проте слід зазначити: останніми роками вони зазнали деякої еволюції.

Ще кілька років тому більш поширювалося поняття *захист інформації в комп'ютерних системах і мережах*, а в офіційних документах перевагу надавали поняттю *захист інформації в автоматизованих системах*.

Нині в Україні загальноприйнятим є поняття *захист інформації в інформаційно–комунікаційних системах*.

Під інформаційно–комунікаційною системою (ІКС) розуміємо організаційно–технічну систему, що виконує функції інформаційної системи, тобто такої організаційно–технічної системи, що реалізує певну технологію (або сукупність технологій) обробки інформації, та (або) комунікаційної системи – технічної системи, що реалізує певну технологію (або сукупність технологій) передачі даних шляхом їхнього кодування у вигляді фізичних сигналів [1].

Далі зупинимося на термінах, які безпосередньо пов'язані із питаннями інформаційної безпеки в ІКС. Перше питання, яке виникає, – що саме ми захищаємо і яка мета цього захисту. Навіть швидко розглядаючи дану тему, можна впевнитися, що захист інформації без чітко визначених цілей захисту не має сенсу.

Ціллю захисту має бути збереження цінності інформаційних ресурсів для їхнього власника. Виходячи з цього, переконуємося, що прямі заходи захисту спрямовані не так на самі інформаційні ресурси, як на збереження певних технологій їх створення, оброблення, зберігання, пошуку та надання користувачам. Ці технології повинні враховувати особливості інформації, що роблять її цінною, а

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

також дозволяти користувачам різних категорій працювати з інформаційними ресурсами (створювати, знаходити, копіювати, узагальнювати, порівнювати, модифікувати, перетворювати, знищувати тощо).

Насамперед слід розуміти, що не впровадження інформаційно–комунікаційної системи дозволяє користувачам різних категорій отримувати доступ до тих чи інших інформаційних ресурсів, а фактори, до яких відноситься *Закони України*. З усього цього впливає найважливіше для визначення ролі захисту інформації поняття – політика безпеки.

Політика безпеки інформації – це сукупність законів, правил, обмежень, рекомендацій, інструкцій тощо, які регулюють обробку інформації в ІКС. Отже, саме політика інформаційної безпеки визначає застосування тих чи інших заходів захисту, які дозволяють забезпечити безпеку інформації.

Інформаційна безпека — це стан інформації, в якому властивості інформації, визначені політикою безпеки. Багаторічний досвід захисту в ІКС дозволяє визначити головні властивості інформації, збереження яких дозволяє заберегти цінність інформаційних ресурсів. Цими властивостями є конфіденційність, цілісність і доступність інформації [9].

Конфіденційність – властивість інформації, завдяки якій лише авторизовані користувачі мають змогу її отримувати (тобто ознайомлюватися з інформацією).

Цілісність – властивість інформації, яка дає можливість лише авторизованим користувачам її модифікувати.

Доступність – властивість інформації, завдяки якій авторизовані користувачі можуть використовувати її згідно з правилами, встановленими політикою безпеки, не очікуючи довше заданого (короткого) періоду часу. Тобто, інформаційний ресурс має необхідний користувачу вигляд, перебуває у тому місці, де він потрібен користувачу, і тоді, коли це йому потрібно.

Термін *доступність* використовується не тільки, коли йдеться про інформаційні ресурси, а й про ІКС у цілому, про її компоненти або окремі ресурси. Наприклад, коректно вживати цей термін до сервера, сегмента мережі, служби електронної пошти тощо.

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		11

1.2 Аналіз можливих загроз клієнт–серверній мережі на базі ОС Windows

Операційна система Windows не є в повній мірі безпечною. Не зважаючи на свою популярність, вона має ряд вразливостей та недоліків. Одним із основних недоліків якраз і є її популярність. Мільйони людей використовують цю ОС, і саме тому вона викликає особливу увагу зловмисників, що постійно намагаються знайти в ній вразливості і створюють для неї купу шкідливого програмного забезпечення.

Windows має закритий код, що не дає змоги виправити якусь проблему чи недолік самотужки, і в той же час користувачі мають повний доступ адміністратора до облікових записів. Таким чином, при виникненні якоїсь загрози в зоні ризику опиняється вся система.

Розглянемо докладніше, що може спричинити порушення інформаційної безпеки в мережі та проти чого, власне, застосовують заходи захисту інформації [4].

Несприятливий вплив – вплив, що призводить до знецінення інформаційних ресурсів.

Загроза – будь–які обставини, що призводять до порушення політик безпеки інформації та нанесять збитків мережі. Тобто, загроза – це будь–який потенційно можливий несприятливий вплив.

Загроз, очікуючих користувачів при підключенні комп'ютера до мережі, дуже багато. Це лише основні з них:

- *Злам комп'ютера* зазвичай проводиться з метою захоплення контролю над операційною системою і отримання доступу до даних;
- *Пошкодження системи* найчастіше організовується, щоб порушити працездатність (викликати відмову в обслуговуванні – «Denial of Service») будь–яких сервісів або комп'ютера (найчастіше сервера) цілком, а іноді – навіть всієї мережевої системи організації;
- *Крадіжка даних* через неправильно налаштовані права доступу, при передачі даних або системному зламі дозволяє отримати доступ до конфіденційної

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

захищеної, інформації з усіма звідси впливаючими неприємними наслідками для власника цих даних;

- *Знищення даних* має на меті порушити або навіть зупинити працездатність систем, комп'ютерів, серверів або всієї організації.

- Потрапляння в інформаційну систему *шкідливого програмного забезпечення*: вірусів, троянських програм, мережних хробаків, клавіатурних шпигунів, рекламних систем, що є актуальною проблемою для ОС Windows.

- *Атаки порушників* (хакерів).

- *BotNet* – це комп'ютерна мережа, що складається з деякої кількості хостів, із запущеними ботами — автономним програмним забезпеченням.

- *DdoS* – атака на відмову в обслуговуванні, розподілена атака на відмову в обслуговуванні – напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам, для яких комп'ютерна система була призначена.

- *Фішинг* – вид шахрайства, метою якого є виманювання персональних даних у клієнтів онлайн-аукціонів, сервісів з переказу або обміну валюти, інтернет-магазинів тощо.

Більш детально про *шкідливе програмне забезпечення*:

- *Комп'ютерний вірус* – це вид шкідливого програмного забезпечення, яке здатне поширювати свої копії з метою інфікування та пошкодження даних на пристрої жертви. Віруси можуть потрапити на комп'ютер з інших вже інфікованих пристроїв через носії інформації (CD, DVD тощо) або через Інтернет-мережу.

- *Троянська програма*. Типова троянська програма зазвичай «маскується» під будь-яку корисну утиліту (або може бути захована в якій-небудь програмі), а якщо користувач через незнання запусить її на виконання, то така програма починає контролювати комп'ютер, відкриваючи автору троянської програми

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

доступ до даних (так званий «backdoor» – «чорний хід»), викрадаючи та пересилаючи йому набрані з клавіатури паролі та ін.

– *Мережевий хробак* – це програма зі шкідливим кодом, яка атакує комп'ютери в мережі та поширюється через неї. Активний мережевий черв'як може знижувати продуктивність пристрою жертви, видаляти файли або навіть вимикати певні програми. Якщо на комп'ютері було виявлено загрозу такого типу, інфіковані файли рекомендується негайно видалити, оскільки вони можуть містити шкідливий код.

– *Клавіатурні шпигуни* – це програми, що реєструють натиснення клавіш на комп'ютері. Принцип їх дії простий – все натискання на клавіші перехоплюються програмою, і отримані дані записуються в окремий файл, який далі може бути відісланий з мережі на комп'ютер зломщика.

– *Рекламні системи* – це вид шкідливого програмного забезпечення, яке відображає не бажану рекламу на пристрої користувача. Дана загроза, як правило, інсталиється під час завантаження легітимних додатків. Хоча іноді рекламне програмне забезпечення може бути безпечним, деякі спливаючі вікна здатні не тільки відображати рекламу, але й збирати дані про конкретного користувача для відображення оголошень відповідно до його запитів у браузері. У цих випадках рекламне ПЗ може перенаправляти користувача на шкідливі веб-сайти та небезпечні сторінки через різні посилання, піддаючи ризику інфікування комп'ютерними вірусами та іншими загрозами.

Всі вище перераховані терміни слід узагальнити терміном *атака*.

Атака – це спроба реалізації загрози. Якщо атака є успішною (здійснено подолання засобів захисту), це називають *проникненням*. Наслідком успішної атаки є порушення безпеки інформації в системі, яке називають *компрометацією*.

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

Іноді використовують інше тлумачення термінів, що не є зовсім коректним. Наприклад, часто замість терміну *загроза* вживають термін *атака*. Однак потрібно розрізняти атаку, яка є дією, тобто спробою реалізувати певну загрозу, та загрозу, яка робить потенційно можливим здійснення несприятливого впливу. Атака – це здебільшого цілеспрямований вплив, як правило, умисний. Загрози можуть бути випадковими, хоча втрати від цього не стають меншими. Тому захищати інформацію потрібно також від загроз, а не лише від атак.

Важливо, що за комплексного підходу до захисту інформації має розглядатися не лише вплив, спрямований на інформаційні ресурси, але й будь-який інший вплив, що може завдати шкоди мережі. Це узагальнюється твердженням про необхідність захисту не так інформації, як насамперед технології її обробки [3].

Уразливість системи – стан нездатності системи протистояти реалізації певної загрози, сукупності загроз.

Вади захисту – причини, умови і обставини, наявність які призводять до порушення нормалізованого функціонування системи або інформаційної політики безпеки. Найчастіше вадами захисту вважаються особливості побудови програмних (а іноді й апаратних) засобів захисту, що при певних обставинах відключають їх здатність протистояти загрозам і виконувати свої функції. Таким чином, робимо висновки, що вади захисту є окремим випадком уразливості системи.

Порушник – фізична особа (необов'язково користувач системи), яка порушує системну політику безпеки. Іноді використовують термін *зловмисник*, чим наголошують умисність здійсненого ним порушення, тоді як порушник може здійснювати порушення ненавмисно (наприклад, через необережність або недостатню обізнаність).

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

Досить розповсюджений термін *хакер* є доволі неоднозначним, тому його не використовують як синонім терміну *порушник*.

Модель політики безпеки – загальний формалізований чи неформалізований опис політики безпеки. Модель безпеки використовується при проектуванні системи визначення механізмів і алгоритмів захисту, а також під час аналізу захищеності системи для перевірки й доведення коректності та достатності реалізованих механізмів.

Модель загроз – загальний формалізований чи неформалізований опис методів і засобів здійснення загроз [13].

Модель порушника – загальний формалізований чи неформалізований опис порушника. Моделі загроз і є основою для розроблення політики безпеки і проектування будь-яких систем захисту.

Захищена комп'ютерна система – комп'ютерна система, що здатна забезпечувати захист оброблюваної інформації від визначених загроз. Цей термін частіше вживають до обчислювальних систем або їхніх складових (програмних продуктів, окремих програмно-апаратних пристроїв). Іноді його застосовують до мереж, але слід розуміти, що будь-яка сучасна мережа має бути захищеною (навіть домашній комп'ютер із одним користувачем). Інакше її використання дуже швидко призведе до втрат інформації [2].

Спостережність – властивість мережі, що фіксує діяльність користувачів і процесів, використання пасивних об'єктів, а також однозначно встановлює ідентифікатори причетних до певних подій користувачів і процесів із метою запобігання порушенню політики безпеки і (або) забезпеченню відповідальності за певні дії. Це дуже важлива властивість обчислювальних систем та мереж, яка досягається реалізацією засобів *реєстрації* або *аудита*.

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

1.3 Засоби та методи захисту клієнт–серверної мережі організації на базі ОС Windows

Коли комп'ютери не були об'єднані в мережі або підключені до Інтернету, про безпеку даних можна було особливо не піклуватися. Досить було забезпечити *фізичний захист* комп'ютера і контролювати доступ сторонніх користувачів до пристроїв запису [7].

Після об'єднання комп'ютерів в мережі все змінилося – без серйозного захисту тепер уже не обійтися, інакше і операційна система, і дані, що зберігаються на комп'ютері або передаються по мережі, можуть стати легкою здобиччю зловмисників, причому так, що користувачі, які працюють на цьому комп'ютері нічого не помітять.

Під *захистом інформації в мережі* розуміється діяльність, спрямована на забезпечення безпеки інформації, яка обробляється в мережі, що дозволяє запобігти реалізації загроз або унеможливити її та зменшити ймовірність завдання збитків від реалізації загроз [8].

Захист інформації в мережі полягає у створенні системи технічних і нетехнічних заходів та в підтримці її працездатного стану.

Система таких заходів має назву – комплексна система захисту інформації.

Отримуємо, що *комплексна система захисту інформації* (КСЗІ) – це сукупність організаційних, інженерних і програмно–апаратних засобів, що забезпечують захист інформації в мережі [12].

Отже, захист інформації в мережі формально зводиться до створення і обслуговування КСЗІ. Слід зазначити, що навіть домашній комп'ютер з одним користувачем має якусь КСЗІ, проте недокументовану. Операційна система обов'язково повинна мати засоби контролю цілісності компонентів самої ОС і файлової системи. Найчастіше користувачем встановлюється антивірусний засіб і хоча б зрідка виконуються дії з оновлення його бази даних (або просто видаляється застаріла програма і встановлюється нова). Час від часу ним робляться резервні копії найцінніших файлів.

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

Зрештою, якщо користувач має вихід в Інтернет, він мусить вживати додаткових заходів безпеки.

Важливо знати, що підключення до Інтернету є найкритичнішим із міркувань безпеки системи. Якщо без такого підключення користувач може працювати роками, не застосовуючи специфічних заходів безпеки, то при наявності доступу в Інтернет йому, фактично, необхідно створити КСЗІ. У доповнення до антивірусного ПЗ ця система повинна включати в себе настроєні певним чином засоби міжмережної фільтрації (наприклад, персональний брандмауер), реєстрації подій, а, можливо, і виявлення вторгнень. Потрібно також періодично вживати заходів на кшталт оновлення програмного забезпечення, встановлення виправлень, оновлення антивірусних баз тощо.

Що стосується мереж, які використовують у державних органах і установах, підприємствах різної форми власності, то для них створення КСЗІ є життєво необхідним. У багатьох випадках обов'язковість створення КСЗІ визначається чинним законодавством.

Основні заходи безпеки при роботі в мережі досить прості [5]. Їх можна сформулювати у вигляді наступного набору правил:

- вимикайте комп'ютер, коли ви ним не користуєтесь.
- своєчасно оновлюйте операційну систему. У будь-якій ОС періодично впливають так звані «уразливості», що значно знижують захист комп'ютера. Наявність вразливостей потрібно уважно відстежувати, щоб вчасно вживати заходів для їх усунення.

Для ОС Windows корпорацією Microsoft створено спеціальний веб-вузол Windows Update, звернувшись до якого, неважко переглянути та завантажити список оновлень, рекомендованих для вашого комп'ютера;

- використовуйте обмежений набір добре перевірених додатків, не встановлюйте самі і не дозволяйте іншим встановлювати на ваш комп'ютер програми, взяті з неперевірених джерел. Якщо додаток більше не потрібен, видаліть його;

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

– без необхідності не надавайте ресурси свого комп'ютера у загальний доступ. Якщо ж це все-таки було потрібно, обов'язково налаштуйте мінімально необхідний рівень доступу до ресурсу тільки для зареєстрованих облікових записів;

– встановіть (або включіть) на комп'ютері *персональний міжмережевий екран (брандмауер)*. Якщо мова йде про корпоративні мережі, встановіть брандмауери як на маршрутизаторах, що з'єднують вашу локальну мережу з Інтернетом, так на всіх комп'ютерах мережі;

– обов'язково встановіть на комп'ютер спеціалізоване антивірусне і «антишпигунське» програмне забезпечення. Налаштуйте його на автоматичне отримання оновлень як мінімум один раз на тиждень;

– навіть якщо ви єдиний власник комп'ютера, для звичайної роботи застосовуйте *користувацький обліковий запис*: у цьому випадку пошкодження системи, наприклад, при зараженні вірусом, буде незмірно менше, ніж якщо б ви працювали з правами адміністратора. Для всіх облікових записів, особливо адміністративних, встановіть та запам'ятайте складні паролі.

Складним вважається пароль, що містить випадкову комбінацію літер, цифр та спеціальних символів, наприклад jxglrg\$N. Зрозуміло, пароль не повинен збігатися з ім'ям вашого профілю. В операційних системах Windows складний пароль можна згенерувати автоматично, використовуючи команду NET USER з ключем /RANDOM, наприклад:

– NET USER Ім'я_Користувача /RANDOM

Пароль у вигляді випадкової послідовності символів нелегко запам'ятати, тому часто використовують таку техніку – пароль набирається в англійській розкладці російськими літерами. Наприклад, слово «Пароль» тоді виглядатиме як «Gfhjkm». Однак цей спосіб слід застосовувати з обережністю – зломщики давно мають цілі словники подібним чином перетворених слів, так що бажано вставляти у такі паролі спеціальні символи і цифри.

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

Паролі для доступу у різні системи мають бути різними. Неприпустимо використовувати один і той самий пароль для адміністрування вашого комп'ютера і для входу, наприклад, на ігровий веб-сайт;

– при роботі з електронною поштою ніколи відразу не відкривайте вкладення, особливо отримані від невідомих відправників. Збережіть вкладення на диск, перевірте його антивірусною програмою і лише потім відкрийте. Якщо є така можливість, увімкніть у вашій поштовій програмі захист від потенційно небезпечного вмісту і відключіть підтримку HTML;

– при роботі з веб-сайтами дотримуйтесь заходів розумної обережності: намагайтеся уникати реєстрації, не передавайте нікому персональні відомості про себе і уважно працюйте з Інтернет-магазинами та іншими службами, де застосовуються онлайніві способи оплати за допомогою кредитних карт або систем типу WebMoney. При проведенні оплати переконайтеся, що з'єднання захищено шифруванням за допомогою технології *Secure Sockets Layer (SSL)* – у цьому випадку адресний рядок обов'язково повинен починатися з «https://»;

– перераховані вище заходи лише підвищують загальну захищеність системи і даних, але не дають ніякої гарантії від їх пошкодження або навіть повної втрати. Тому обов'язково слід створювати резервні копії системи і даних на знімному жорсткому диску або на DVD–RW – це дозволить вам легко відновити їх у разі втрати. При цьому одну копію має сенс зберігати не вдома, наприклад, в сейфі;

– під час резервного копіювання краще використовувати утиліти для створення «образів» жорсткого диска (такі, як Norton Ghost). Резервну копію можна зняти з «системного» жорсткого диска після правильної установки на нього всіх необхідних програм і антивірусної перевірки та зберігати її на іншому жорсткому диску (мережевому або знімному), щоб у разі пошкодження системи швидко відновити її працездатність.

– виключно важливу роль грає навчання всіх користувачів основам безпечної роботи в мережах – як у домашніх, так і в корпоративних, – адже порушення правил одним користувачем ставить під загрозу всю систему захисту.

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

Отже, для роботи в мережі потрібні мережеві операційні системи, які прийнято поділяти на клієнтські та серверні. Клієнтські ОС відрізняються невеликим набором служб, але включають в себе спектр мережевих додатків. Серверні системи бувають різних типів і призначені для обслуговування тих чи інших запитів мережевих клієнтів [11].

Для організації роботи в мережах Microsoft застосовуються дві моделі: робочі групи, які використовуються при невеликій кількості комп'ютерів, та домени, що дозволяють легко об'єднувати велику кількість користувачів, робочих станцій і серверів.

Далі розглянемо основні принципи, які використовуються при побудові сучасних мережевих ОС, а також вкажемо найпростіші правила безпеки, яких обов'язково слід дотримуватися при роботі в мережі.

Принципи побудови захищених ОС:

- усі сучасні ОС є *багатокористувацькими* – вони розраховані на роботу в системі (в тому числі одночасну) декількох користувачів;
- щоб відрізнити одного користувача від іншого, застосовуються *облікові записи (accounts)* з унікальними *іменами та паролями*;
- облікові записи розрізняються *рівнем повноважень (привілеїв, прав)* – набором дій, які власник даного облікового запису може виконувати в системі.

Зазвичай облікові записи поділяють на *адміністративні*, які володіють максимальними привілеями, і *користувацькі*, набір повноважень для яких дозволяє нормально працювати в системі, але не дозволяє виконувати будь-які критичні з точки зору безпеки даних операції, наприклад, формувати розділи жорсткого диска або змінювати налаштування мережі.

У сучасних версіях ОС Windows додатково існують облікові записи з рівнем прав, середнім між адміністративним і користувацьким (учасники групи «Досвідчені користувачі»), а також котрі володіють мінімальними повноваженнями *гостьові облікові записи* (учасники групи «Гості», включаючи вбудований обліковий запис «Гість»).

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

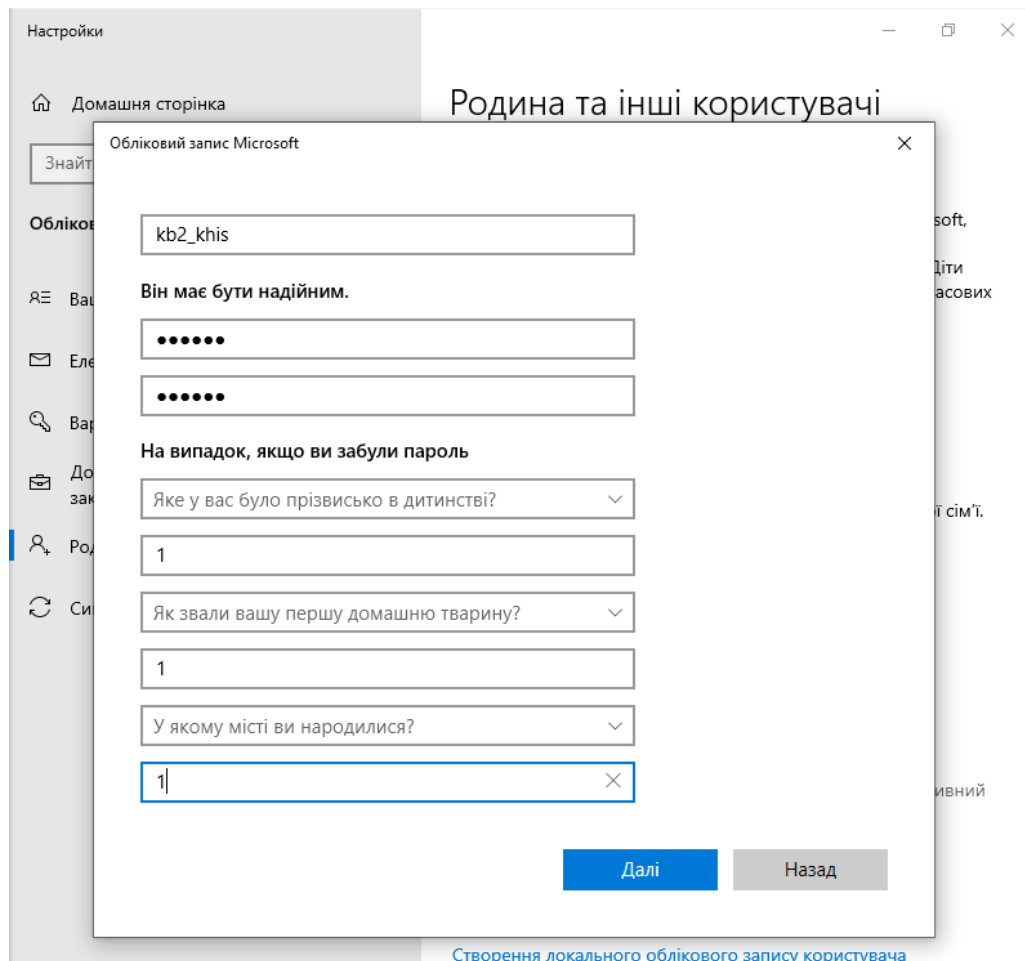


Рисунок 1.1 – Приклад створення користувача на Windows 10

Інші користувачі

Дозвольте людям, які не є членами вашої сім'ї, входити за власними обліковими записами. Це не додасть їх до вашої сім'ї.

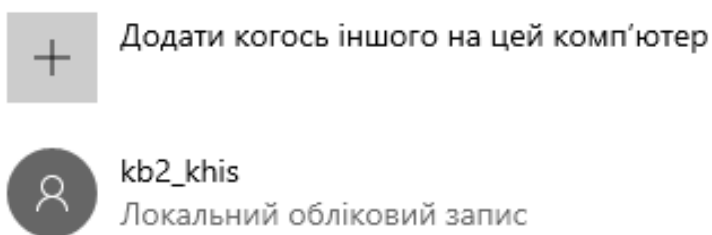


Рисунок 1.2 – Перегляд створених користувачів

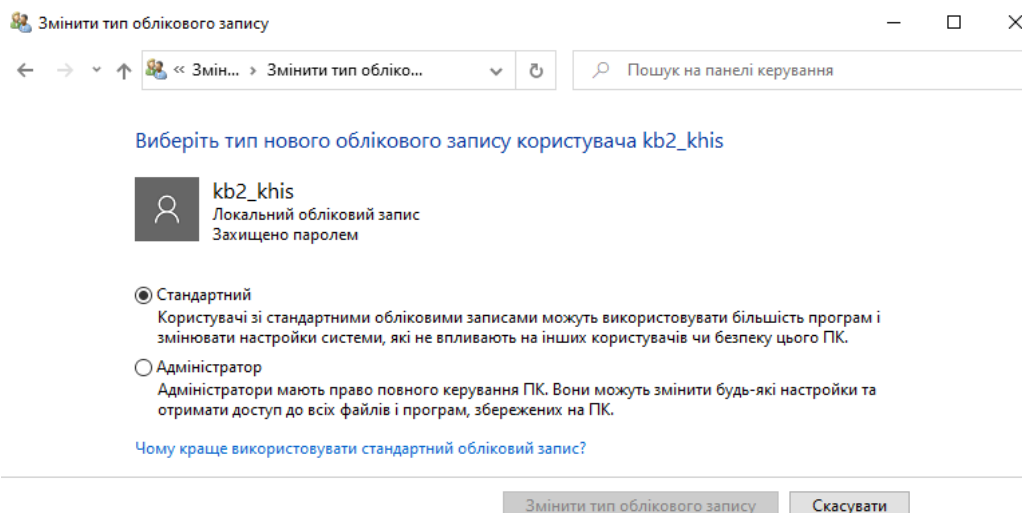


Рисунок 1.3 – Зміна типу облікового запису користувача на Windows 10

Крім того, існує два типи облікових записів – *локальні* з бази даних конкретного комп’ютера з ОС Windows та *глобальні облікові записи в домені*, які зберігаються на контролерах домену (докладніше про них буде сказано далі);

Для входу в комп’ютер обов’язково потрібно вказати ім’я та пароль облікового запису, зареєстрованої в системі. Слід підкреслити, що поняття «вхід у систему» має на увазі не лише безпосередній доступ, а й інші можливості роботи з комп’ютером, наприклад *мережевий* або *термінальний* вхід, для яких також потрібні користувацькі ім’я та пароль.

В операційних системах Windows допускається також мережевий вхід без вказівки імені та пароля (*анонімний вхід*); такі підключення використовуються при деяких взаємодіях у мережах Microsoft;

Після входу в систему (інтерактивного, мережевого та ін.) користувач отримує доступ до ресурсів того комп’ютера, у який він увійшов (наприклад, доступ до локальних файлів або каталогів). Рівень доступу при цьому визначається *списком дозволів*, тобто можливих дій, які даний користувач може здійснювати з захищеним об’єктом. Наприклад, один користувач може змінити або видалити файл, інший – тільки прочитати його, а третьому взагалі буде відмовлено в доступі до цього файлу.

РОЗДІЛ 2 ПРОЄКТ ПІДСИСТЕМИ ЗАХИСТУ КЛІЄНТ–СЕРВЕРНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ

2.1 Розробка проєкту мережі організації

Після аналізу питань із захисту безпеки інформаційно–комунікаційних систем було розроблено проєкт мережі організації, що є одним з важливих етапів роботи для подальшої її працездатності.

Для забезпечення функціонування мережі організації було обрано оптимальне обладнання корпорації Cisco, котрі мають адаптованість під модернізацію модулями. Також потрібно приділити особливу увагу технологіям, котрі необхідні для мережі, зокрема це підтримка GigabitEthernet та Ethernet (FastEthernet).

На роль комутаторів обрано Cisco Catalyst 2960 Series , що є серією комутаторів з фіксованою конфігурацією і портами Fast Ethernet і Gigabit Ethernet, що мають розширені LAN сервіси для підприємств початкового рівня і мереж віддаленого офісу. Комутатори Cisco Catalyst 2960 підтримують безпечний доступ. Крім того, вони є масштабованим рішенням для управління в міру зміни потреб бізнесу [6].



Рисунок 2.1 – Комутатор Cisco Catalyst 2960

Комутатори Cisco Catalyst 2960 підтримують “розумні функції” (створення складних списків управління доступом, розширена безпека), комбіновані гігабітні порти (мідний 10/100 / 1000BASE–T Ethernet або SFP–модуль для переходу в інше середовище – Cisco 1000BASE–SX, 1000BASE–LX, 1000BASE–ZX, 100BASE–FX,

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

100BASE-LX, CWDM SFP). Також пристрої Catalyst 2960 підтримують QoS, покроковий Rate Limiting, ACL (на базі MAC або IP адрес, портів UDP / TCP) і multicast services, можливість регулювати швидкість передачі на кожному порту з кроком 64 Кбіт, Link Aggregation для організації більш швидкісних з'єднань між комутаторами і серверами, можливість організації транкових з'єднань на кожному порту за допомогою тегів 802.1q, до 255 VLAN на комутатор, до 4000 VLAN ID і управління через Cisco Network Assistant (підтримує широкий спектр моделей комутаторів від Cisco Catalyst 2960 до Cisco Catalyst 4506).

Маршрутизатор було обрано з серії Cisco 7200.

Маршрутизатори Cisco 7200 – це обладнання провайдерського класу для інтернет-трафіку зі швидкістю до 2 мільйонів пакетів в секунду. Завдяки модульній архітектурі ці маршрутизатори дозволяють створювати масштабовані рішення, що відповідають різним вимогам до щільності, продуктивності та асортименту послуг, одночасно забезпечуючи захист інвестицій з урахуванням майбутнього розвитку мережі.



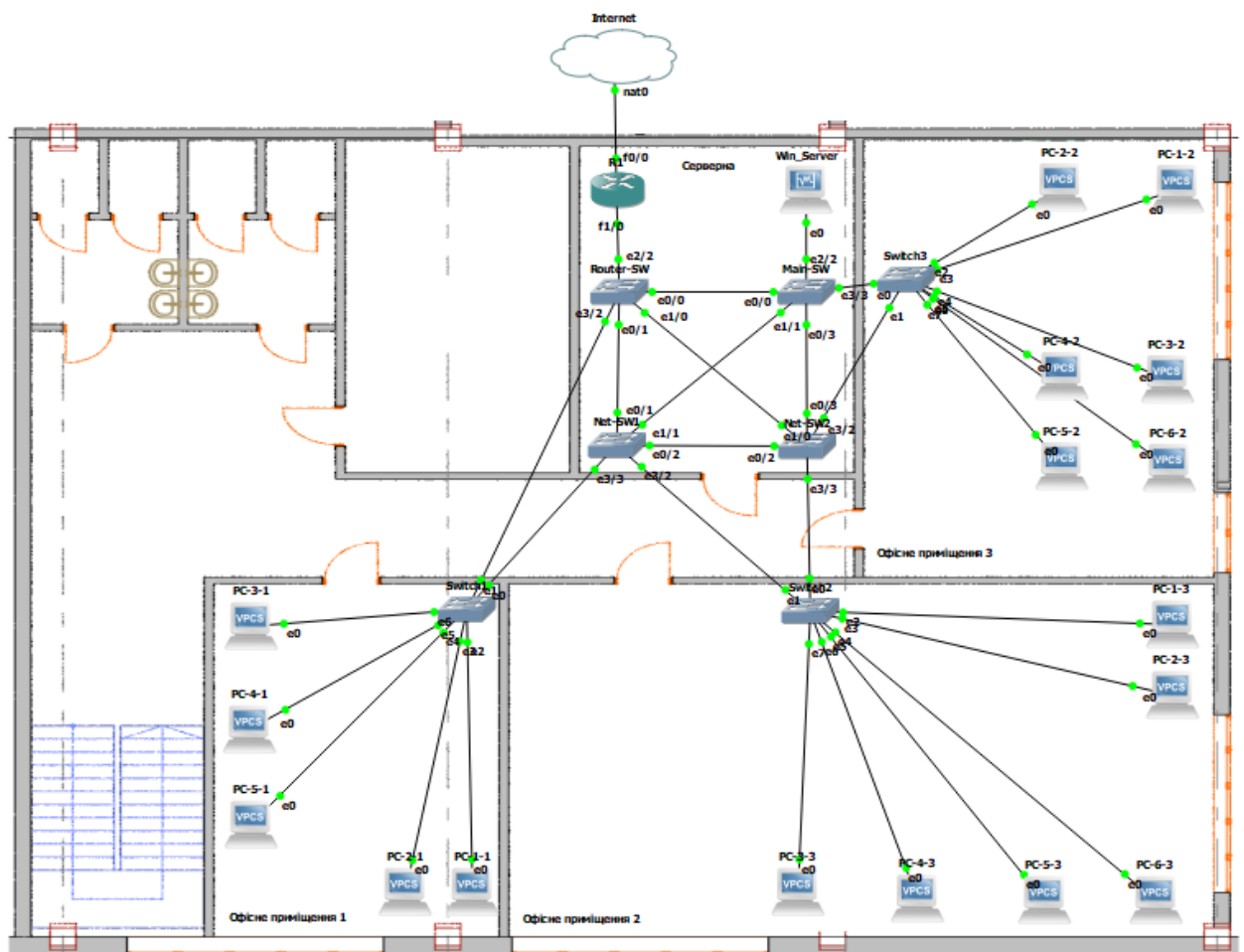
Рисунок 2.2 – Маршрутизатор Cisco 7201

Пристрої Cisco 7200 серії підтримують великий вибір модулів розширення для створення різних конфігурацій, включаючи швидкісні модулі маршрутизації (NPE-G2 Network Processing Engine), модулі інтерфейсні PA та інші.

До переваг модульних маршрутизаторів Cisco 7200 серії можна віднести апаратну підтримку VPN-шифрування (VPN Services Adapter), підтримка інтерфейсів від DS0 до OC-3, а також Fast Ethernet, Gigabit Ethernet, Packet over

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				25
Змн.	Арк.	№ докум.	Підпис	Дата		

У результаті виходить, що мережа складається з серверного та трьох офісних приміщень.



Узагальному в мережі використано один маршрутизатор та сім комутаторів. Мережа складається з п'яти підмереж.

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк С.М.				26
Змн.	Арк.	№ докум.	Підпис	Дата		

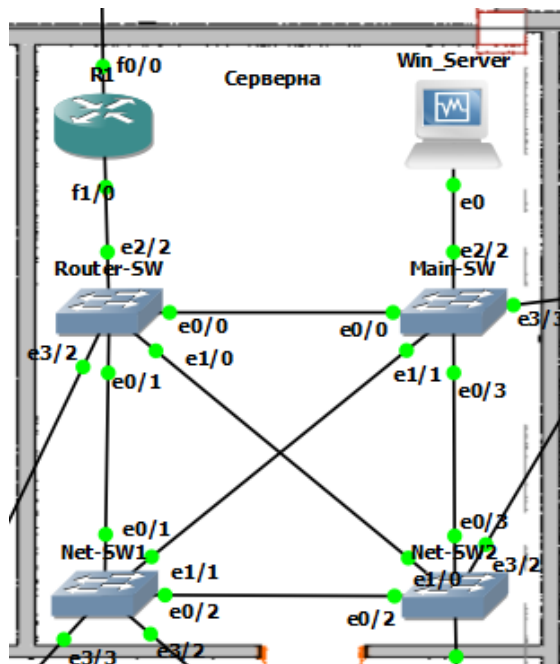


Рисунок 2.4 – Перша частина мережі

Перша частина мережі складається з двох VLAN (50, 100). З VLAN 50 менеджменту та VLAN 100 сервера. VLAN 50 складається з чотирьох комутаторів.

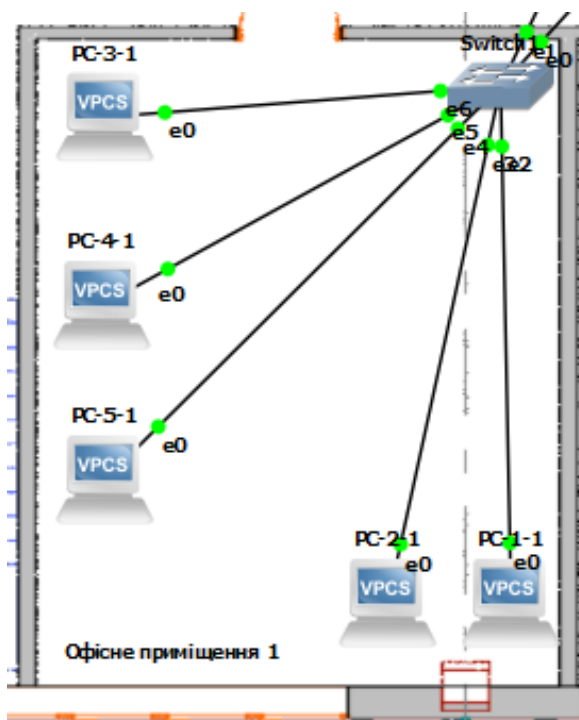


Рисунок 2.5 – Друга частина мережі

Друга частина мережі складається з одного влану (10). VLAN 10 включає в себе один комутатор та п'ять робочих станцій.

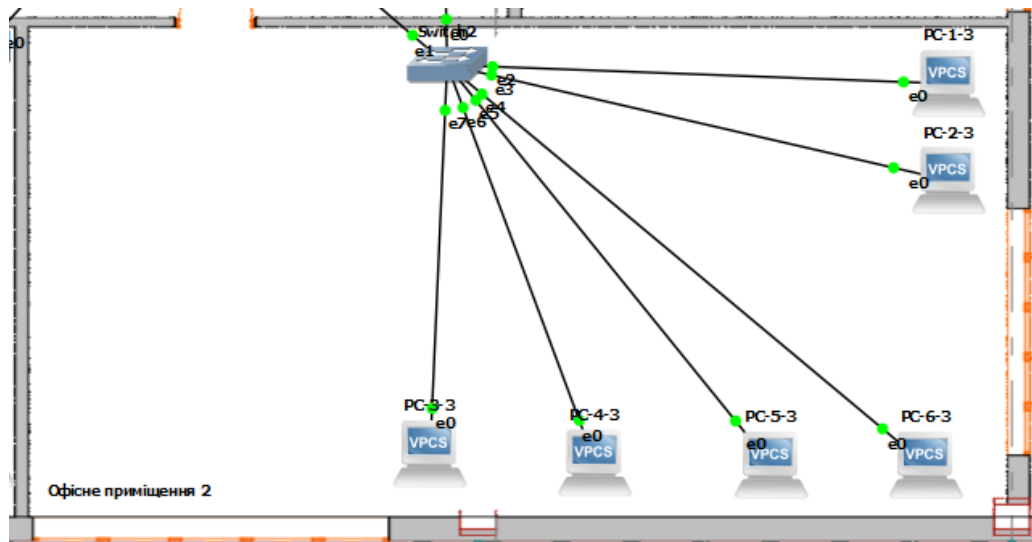


Рисунок 2.6 – Третя частина мережі

Третя частина мережі складається з одного влану (20). VLAN 20 включає в себе один комутатор та шість робочих станцій.

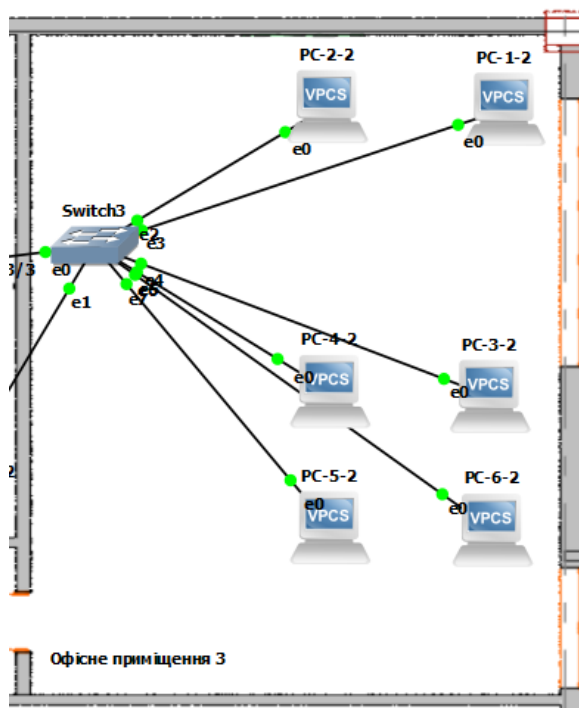


Рисунок 2.7 – Четверта частина мережі

Четверта частина мережі складається з одного влану (30). VLAN 30 включає в себе один комутатор та шість робочих станцій.

Отже, усі віртуальні мережі другої, третьої та четвертої частини мають схожу будову і включають в себе по одному комутатору та по п'ять–шість робочих станцій відповідно.

Перша частина включає в себе чотири комутатори, на яких налаштовано DHCP та сервер, на якому адреса задається статично.

Також в мережі налаштовано RIPv2 та SSH.

Таблиця 2.1 – Адресація підмережі VLAN10

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 2.1 – Адресація підмережі VLAN20

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 2.1 – Адресація підмережі VLAN30

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 Розробка моделі загроз організації

Після розробки проєкту мережі слід розробити для неї підсистему захисту, але розробити її буде набагато простіше використовуючи модель загроз цій мережі.

Визначення, що теке модель загроз, було представлено ще в першому розділі. Тут розглянемо це питання більш детально і визначимося, які загрози можуть вплинути на нашу мережу і яким чином [14].

Модель загроз повинна визначити:

- перелік можливих типів загроз, що має бути класифікованим за результатом впливу на інформацію, а саме на яку властивість інформації націлені ці загрози (конфіденційність, цілісність, доступність);
- перелік можливих способів реалізації загроз різного типу атак відносно інформаційних об'єктів ІКС.

Загрози інформації або ІКС залежать від різних чинників та є за природою об'єктивними або суб'єктивними.

У свою чергу суб'єктивні загрози поділяються на випадкові та навмисні.

Для кожної загрози необхідно визначити:

- Які властивості інформації або ІКС вона порушує;
- Які джерела її виникнення;
- Які можливі спроби її реалізації.

Серед загроз, що можуть вплинути на нашу мережу, маємо: хакерів, конкурентів, спецслужби, кримінал. Також природні та техногенні явища.

Проаналізувавши написане вище, в програмі OWASP Threat Dragon було створено модель загроз організації.

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

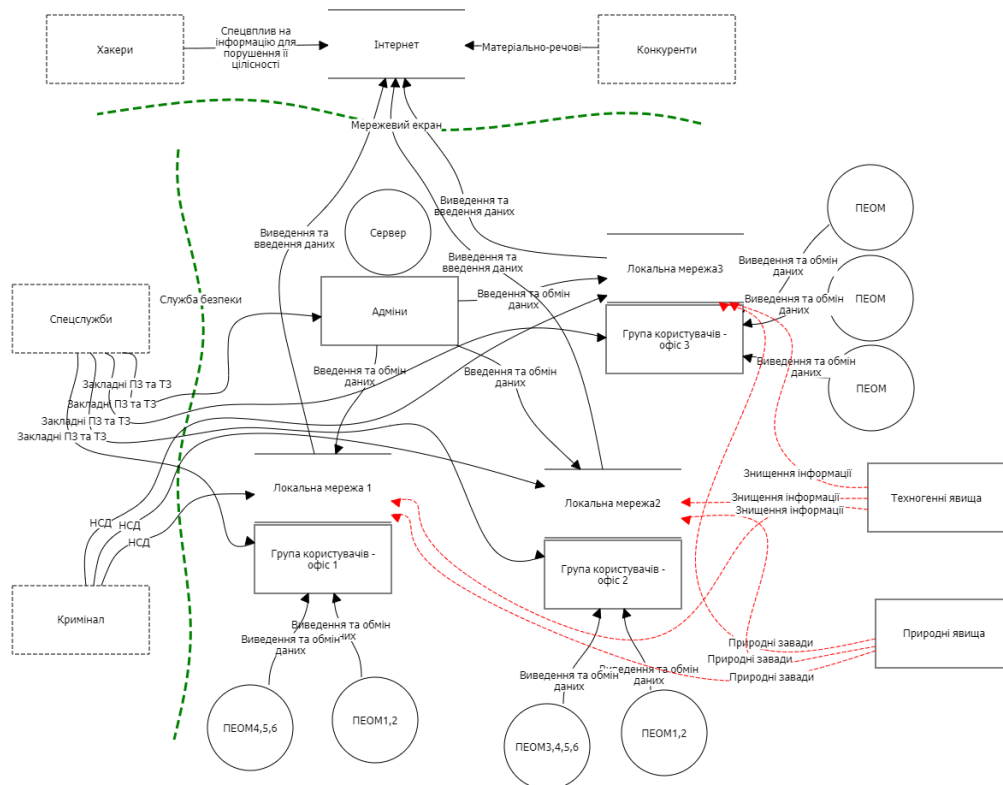


Рисунок 2.8 – Модель загроз організації

2.3 Розробка проєкту підсистеми захисту клієнт–серверної мережі

Після створення моделі загроз, з'являється уявлення від чого повинна бути захищена мережа. Це дає можливість розробити проєкт підсистеми захисту.

Отже, першим кроком буде захист пристроїв мережі, таких як комутатори, маршрутизатори та ін. Розроблений раніше проєкт мережі має багато комутаторів, що можуть стати першою ціллю для атак зловмисників.

Одною із відомих атак є *підміна DHCP-сервера*. Зловмисник підключає в мережу свій DHCP-сервер, що починає ширити користувачам невірні IP-адреси і призводить до неможливості подальшої роботи.

Також зловмисник може підмінити шлюз за замовчуванням і вказати себе. Таким чином, він отримує можливість перехоплювати трафік користувачів. Ця атака називається «Людина посередині» (Main in the Middle).

Гарне рішення захисту від атаки такого типу – налаштування функції DHCP snooping на комутаторах мережі.

Ще одна не менш поширена атака – *атака на VLAN (VLAN Hopping)*. Вона дозволяє сторонній VLAN бачити трафік атакованої VLAN. Ця атака використовує можливість комутаторів автоматично погоджувати типи портів.

Одією з можливостей захисту від цієї атаки є команда `switchport nonegotiate`, що якраз вимикає ту саму можливість автоматичного погодження портів.

Також є ще один варіант атаки з перескоком VLAN. Зловмисник використовує `native VLAN` й додає ще один тег.

Для захисту від цього типу атаки потрібно назначити на всіх портах, що є `trunk`, в якості `native`, невикористовуваний VLAN.

Також для безпеки приладів мережі можна налаштувати протокол віддаленого підключення `SSH`. Він шифрує передавані повідомлення, і у випадку їх втрати, вони не будуть ніким прочитані.

Крайнім випадком, але одним із самих ефективних, є відключення невикористовуваних портів і вмикати їх тільки за важливої потреби.

Далі розглянемо можливості захисту в `Active Directory`.

Захист `Active Directory` базується на недопуску зловмисника в домен, а у випадку проникнення, на його швидкому прибиранні.

Для виключення можливості входу зловмисника кожен користувач повинен мати особистий унікальний пароль. Паролі користувачів повинні бути складними і для більшої безпеки змінюватися особисто користувачем. Пароль адміністратора, зрозуміло, має бути в рази складнішим.

Слід попрацювати також над правилами паролів та правилами входу. Користувачі не зможуть обрати собі надто простий пароль, у пароля буде свій термін дії, та при трьох неправильних спробах входу обліковий запис користувача буде заблоковано.

В `Active Directory` можна налаштувати права, якими будуть володіти користувачі. На відміну від адміністраторів, користувачі матимуть мінімальні права, що в разі крадіжки їх облікового запису, нанесе мінімальних збитків.

Також буде налаштовано правила аудиту, що дасть можливість відслідковувати підозрілі дії за допомогою журналу подій.

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

2.4 Розробка політики безпеки клієнт–серверної мережі організації

Метою розробки політики безпеки є ефективне управління інформаційною безпекою організації, спрямована на зниження ризиків інформаційної безпеки, забезпечення безперервності діяльності установи, дотримання правил збереження інформаційних активів задля позитивних інформаційних відносин з партнерами і клієнтами, а найголовніше – захист інформації від зовнішніх та внутрішніх загроз.

Розробка політики інформаційної безпеки здійснюється з урахуванням існуючої політики безпеки, яка включає в себе: політику управління інформаційною безпекою, політику управління інцидентами інформаційної безпеки, політику безпеки інформації з обмеженим доступом [15].

Політика захисту персональних даних:

Відповідальний – системний адміністратор.

Власник документа – директор організації.

Опис. Політика захисту персональних даних складена відповідно з усіма вимогами та визначає порядок обробки та заходи щодо забезпечення безпеки персональних даних клієнт–серверної мережі.

Ціль. Ця політика застосовується у випадках, коли організація оброблює персональні дані своїх клієнтів, їх співробітників, тощо. В такому разі організація відповідає за забезпечення захисту оброблювальних персональних даних.

Область застосування. Вимоги політики захисту персональних даних поширюється на всіх працівників організації, що мають доступ до персональних даних клієнтів.

Політика. Організація гарантує збереження конфіденційності, цілісності отриманих персональних даних, а також запобігає несанкціонованому доступу до них сторонніми особами.

Працівники Організації починають роботу з інформацією, що несе персональні дані тільки у разі згоди клієнта, які зазначені у відповідних документах.

Прид час передачі інформації, що містить персональні дані (з використанням Wi-Fi каналу), працівник організації повинен користуватись електронно–

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

цифровим підписом (ЕЦП). Одержувач цих відомостей повинен використати спеціальний ключ ЕЦП, який надає доступ до них.

Працівник організації має право видалити персональні дані клієнта з інформаційних ресурсів у разі відкликання останнім згоди на обробку його даних.

Політика відповідальності.

Керівництво організації зобов'язане ознайомити своїх працівників із цією Політикою і оголосити відповідальність у разі її недотримання.

Політика безпеки обліку та зберігання носіїв інформації:

Відповідальний – системний адміністратор.

Власник документа – директор організації.

Опис. Політика безпеки обліку та зберігання носіїв інформації складається відповідно до всіх вимог та визначає порядок обліку і зберігання носіїв інформації організації.

Ціль. Ця політика призначена для ведення контролю за носіями інформації: встановлення учасників знищення, зміни та/або передачі службової інформації, визначенні місця збереження носіїв інформації.

Область застосування. Вимоги політики безпеки обліку та зберігання носіїв інформації поширюється на всіх працівників організації, які працюють з персональними даними працівників і клієнтів.

Політика.

Працівник організації приступаючи до роботи з паперовим або електронним носієм інформації повинен залишити запис в «Журналі обліку носіїв», в якому вказати своє ПІБ, назву паперового носія, номер, дату та час отримання і поставити підпис. Відповідальна особа видає працівнику вказаний носій інформації.

Працівник організації, по завершенню роботи з паперовим та/або електронним носієм інформації, повинен залишити примітку в «Журналі обліку носіїв», в якому вказати дату та час повернення і поставити підпис. Відповідальна особа приймає у працівника вказаний носій інформації і перевіряє його. У разі виявлення недостатчі паперів та/або пошкодження носіїв, відповідальна особа інформує керівництво організації.

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

Працівник організації, що отримав носій інформації, несе відповідальність за збереження цілісності і доступності носія. У разі, якщо працівник залишає своє робоче місце, він повинен повернути носій інформації відповідальній особі і залишити відмітку в «Журналі обліку носіїв».

Працівник організації повинен прийняти та повернути носій інформації відповідальній особі з 8.30 ранку до 17.30 вечора.

Відповідальна особа в проміжку з 17.30 до 18.00 повинна провести облік носіїв інформації. У разі виникнення проблем проінформувати про них керівництво організації.

Відповідальна особа за зберігання носіїв інформації має зберігати носії інформації в спеціальному сейфі, обладнаному кодовим та механічним замком. Другий ключ від замку зберігається у керівництва організації.

Друкування і розмноження документів, що містять службову інформацію, повинні відбуватися відповідно усім нормам.

Працівники організації повинні обробляти, зберігати, змінювати та передавати інформацію з обмеженим доступом тільки з використанням ліцензованого ПЗ.

Працівники організації повинні блокувати можливість контакту з носіями, на яких міститься інформація обмеженого доступу, сторонніми особами.

Політика відповідальності.

Відповідальна особа за зберігання носіїв інформації ознайомлює працівників організації з вимогами цієї Політики під розпис.

Політика забезпечення антивірусного захисту інформації:

Відповідальний – системний адміністратор.

Власник документа – директор організації.

Опис. Політика забезпечення антивірусного захисту інформації організації визначає вимоги захисту інформаційних ресурсів антивірусним ПЗ від втручання шкідливих програм, що можуть призвести до призупинення роботи організації.

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		35

Ціль. Метою цієї політики є запобігання діяльності шкідливих програм і забезпечення антивірусного захисту інформаційних ресурсів.

Область застосування. Вимоги політики забезпечення антивірусного захисту інформації стосуються всіх працівників, які працюють з інформаційними ресурсами організації.

Політика.

Системний адміністратор має встановити і налаштувати антивірусне ПЗ на комп'ютер працівника організації, а також встановити ПЗ для дистанційного контролю за КС цього працівника.

Системний адміністратор має своєчасно встановлювати оновлення антивірусного ПЗ на комп'ютер працівників організації. Встановлення оновлень повинно відбуватись в понеділок кожного тижня з 9.30 до 10 години ранку.

Працівник організації, отримавши і завантаживши файл з корпоративної пошти, має виконати перевірку цього файлу на наявність вірусів, використовуючи антивірусне ПЗ.

Працівники організації, оброблюючи інформацію з електронного носія, повинні проводити перевірку файлів на наявність вірусів.

Системний адміністратор, отримавши повідомлення в своїй КС про наявність вірусів на комп'ютері працівників організації, повинен негайно ліквідувати загрозу, провести аналіз її виникнення і встановити відповідальних за скоєння цієї загрози.

Системний адміністратор повинен встановлювати тільки ліцензоване програмне забезпечення на комп'ютери всіх працівників організації.

Політика відповідальності.

Системний адміністратор повинен проінформувати працівників організації з вимогами цієї політики і доповісти про відповідальність за недотримання цих вимог.

		Хімчук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

РОЗДІЛ 3 НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ ПІДСИСТЕМИ ЗАХИСТУ КЛІЄНТ–СЕРВЕРНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ

3.1 Налаштування пристроїв мережі

У цьому пункті представлено базове налаштування всіх пристроїв спроектованої до цього мережі. Всі пристрої були попередньо переіменовані та підготовлені до роботи.

В роутері R1 на порті FastEthernet 1/0 налаштовано Sub-інтерфейси 10, 20, 30, 50, 100. Це було зроблено для взаємодії між віртуальними локальними підмережами. Для кожного VLAN створено свій Sub-інтерфейс, на якому задано належність 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

Далі для отримання DHCP адрес було виключено адреси шлюзів по замовчуванню. Це могло б викликати дублікації IP-адрес та призвести 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 IP-адрес DHCP

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

Щоб робочі машини організації отримували IP–адреси автоматично, для підмереж працівників офісу WORKER–1, WORKER–2, WORKER–3 виконано 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 маршрутизатора було виконано дії з 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 динамічного отримання IP–адреси.

Через декілька секунд після підняття порта отримуємо адресу.

```
*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
R1(config-if)#
*Jun 11 12:17:19.007: %DHCP-6-ADDRESS_ASSIGN: Interface FastEthernet0/0 assigned DHCP address 192.168.122.212, mask 255.255.255.0, hostname R1
```

Рисунок 3.5 – Видача динамічної IP–адреси

Наступним і останнім кроком в першочерговому налаштуванні маршрутизатора буде налаштування механізму NAT на кожній підмережі, що дасть змогу отримати їм вихід в глобальну мережу інтернет.

NAT (Network Address Translation) – це механізм у мережах TCP/IP, що дає змогу змінювати IP адресу в заголовку пакета, що проходить через пристрій маршрутизації трафіку. Отримуючи пакет від локального комп'ютера,

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

маршрутизатор аналізує IP-адресу призначення. Якщо це локальна адреса, пакет пересилається іншому локальному комп'ютеру. Якщо ні, то пакет треба надіслати назовні в інтернет.

```
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 3.6 – Налаштування NAT

Після налаштування маршрутизатора, переходимо до налаштування комутаторів. Першим кроком в їх налаштуванні є створення підмереж для користувачів, для сервера та підмережі для менеджменту на кожному з них.

```
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 3.7 – Створення підмереж на Router-SW

```
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 3.8 – Створення підмереж на Main-SW

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				39
Змн.	Арк.	№ докум.	Підпис	Дата		

```

Net-SW1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Net-SW1(config)#vlan 10
Net-SW1(config-vlan)#name WORKER-1
Net-SW1(config-vlan)#vlan 20
Net-SW1(config-vlan)#name WORKER-2
Net-SW1(config-vlan)#vlan 30
Net-SW1(config-vlan)#name WORKER-3
Net-SW1(config-vlan)#vlan 50
Net-SW1(config-vlan)#name MGMT
Net-SW1(config-vlan)#vlan 100
Net-SW1(config-vlan)#name SERV-AD
Net-SW1(config-vlan)#

```

Рисунок 3.9 – Створення підмереж на Net-SW1

```

Net-SW2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Net-SW2(config)#vlan 10
Net-SW2(config-vlan)#name WORKER-1
Net-SW2(config-vlan)#vlan 20
Net-SW2(config-vlan)#name WORKER-2
Net-SW2(config-vlan)#vlan 30
Net-SW2(config-vlan)#name WORKER-3
Net-SW2(config-vlan)#vlan 50
Net-SW2(config-vlan)#name MGMT
Net-SW2(config-vlan)#vlan 100
Net-SW2(config-vlan)#name SERV-AD
Net-SW2(config-vlan)#
Net-SW2(config-vlan)#

```

Рисунок 3.10 – Створення підмереж на Net-SW1

Далі виконується налагодження транкових каналів на потрібних портах для розповсюдження трафіку по всіх створених раніше VLAN.

```

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 3.11 – Налаштування транкових каналів на маршрутизаторі Router-SW

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				40
Змн.	Арк.	№ докум.	Підпис	Дата		

```

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 3.12 – Налаштування транкових каналів на маршрутизаторі Main-SW

```

Net-SW1(config)#int e0/1
Net-SW1(config-if)#switchport trunk allowed vlan 10,20,30,50,100
Net-SW1(config-if)#switchport trunk encapsulation dot1q
Net-SW1(config-if)#switchport mode trunk
Net-SW1(config-if)#
Net-SW1(config-if)#int e1/1
Net-SW1(config-if)#switchport trunk allowed vlan 10,20,30,50,100
Net-SW1(config-if)#switchport trunk encapsulation dot1q
Net-SW1(config-if)#switchport mode trunk
Net-SW1(config-if)#
Net-SW1(config-if)#int e0/2
Net-SW1(config-if)#switchport trunk allowed vlan 10,20,30,50,100
Net-SW1(config-if)#switchport trunk encapsulation dot1q
Net-SW1(config-if)#switchport mode trunk
Net-SW1(config-if)#
Net-SW1(config-if)#int e3/2
Net-SW1(config-if)#switchport trunk allowed vlan 10,20,30,50,100
Net-SW1(config-if)#switchport trunk encapsulation dot1q
Net-SW1(config-if)#switchport mode trunk
Net-SW1(config-if)#
Net-SW1(config-if)#int e3/3
Net-SW1(config-if)#switchport trunk allowed vlan 10,20,30,50,100
Net-SW1(config-if)#switchport trunk encapsulation dot1q
Net-SW1(config-if)#switchport mode trunk
Net-SW1(config-if)#
Net-SW1(config-if)#ex
Net-SW1(config)#

```

Рисунок 3.13 – Налаштування транкових каналів на маршрутизаторі Net-SW1

		Хімчук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				41
Змн.	Арк.	№ докум.	Підпис	Дата		

```

Net-SW2(config)#int e0/2
Net-SW2(config-if)#switchport trunk allowed vlan 10,20,30,50,100
Net-SW2(config-if)#switchport trunk encapsulation dot1q
Net-SW2(config-if)#switchport mode trunk
Net-SW2(config-if)#
Net-SW2(config-if)#int e0/3
Net-SW2(config-if)#switchport trunk allowed vlan 10,20,30,50,100
Net-SW2(config-if)#switchport trunk encapsulation dot1q
Net-SW2(config-if)#switchport mode trunk
Net-SW2(config-if)#
Net-SW2(config-if)#int e1/0
Net-SW2(config-if)#switchport trunk allowed vlan 10,20,30,50,100
Net-SW2(config-if)#switchport trunk encapsulation dot1q
Net-SW2(config-if)#switchport mode trunk
Net-SW2(config-if)#
Net-SW2(config-if)#int e3/2
Net-SW2(config-if)#switchport trunk allowed vlan 10,20,30,50,100
Net-SW2(config-if)#switchport trunk encapsulation dot1q
Net-SW2(config-if)#switchport mode trunk
Net-SW2(config-if)#
Net-SW2(config-if)#int e3/3
Net-SW2(config-if)#switchport trunk allowed vlan 10,20,30,50,100
Net-SW2(config-if)#switchport trunk encapsulation dot1q
Net-SW2(config-if)#switchport mode trunk

```

Рисунок 3.14 – Налаштування транкових каналів на маршрутизаторі Net-SW2

```

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 3.15 – Налаштування підмережі менеджменту

Також було налаштовано протокол віддаленого доступу SSH.

SSH (Secure Shell) – це один з видів мережевих протоколів, який шифрує паролі і передану інформацію.

Даний протокол є універсальним рішенням, яке дає можливість передавати будь-які протоколи мережі. Він стискає дані для їх подальшого надійного шифрування і передачі, якісно захищає канал передачі даних від можливих сторонніх підключень з наступним перехопленням даних.

Для початку налагодження генеруємо ключ для SSH, зашифровуємо паролі та створюємо користувача з індивідуальним паролем і видаємо йому максимальні привілеї, задаємо пароль для привілейованого режиму.

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

```

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 3.16 – Налаштування протоколу SSH на маршрутизаторі R1

```

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 Cisc0lCisc0l
Router-SW(config)#enable secret Cisc0lCisc0l
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 3.17 – Налаштування протоколу SSH на комутаторі Router-SW

На інших пристроях мережі було виконано аналогічні попереднім налаштування протоколу SSH.

Також потрібно налаштувати протокол RPVST+ на комутаторах для того, щоб запобігти виникненню петель у мережі. Цей протокол проприетарна версія Cisco, що покращує функції відкритого протоколу STP. Для Rapid Per-VLAN Spanning Tree характерний значно менший час збіжності і більш вища стабільність [16].

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

```
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 3.18 – Налаштування протоколу RPVST+ на комутаторі Router-SW

```
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 3.19 – Налаштування протоколу RPVST+ на комутаторі Main-SW

```
Net-SW1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Net-SW1(config)#spa
Net-SW1(config)#spanning-tree mode r
Net-SW1(config)#spanning-tree mode rapid-pvst
```

Рисунок 3.20 – Налаштування протоколу RPVST+ на комутаторі Net-SW1

```
Net-SW2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Net-SW2(config)#sp
Net-SW2(config)#spanning-tree mode r
Net-SW2(config)#spanning-tree mode rapid-pvst
```

Рисунок 3.21 – Налаштування протоколу RPVST+ на комутаторі Net-SW2

3.2 Налаштування й автоматизація розгортання Active Directory на базі Windows Server 2019

В цьому підрозділі розгорнемо контроллер домена в Active Directory на Windows Server 2019. Це дасть великий обсяг можливостей на керування всіма процесами пов'язаними з користувачами та їх безпекою.

Спочатку визначимо, що ж таке Active Directory.

Active Directory – це служби каталогів, розроблені компанією Microsoft, завдяки яким адміністратор мережі отримує дуже зручний централізований засіб керування обліковими записами користувачів, груповими політиками (в тому числі політиками безпеки) і об'єктами в мережі. Завдяки вбудованому механізму реплікації, зашкодити правильно налаштованим сервісам AD становить геть не легку задачу. Також налаштувати Active Directory досить просто завдяки графічному інтерфейсу, це можна зробити використовуючи тільки мишку і впорається з цим навіть початківець.

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

Використання Active Directory є дуже гарним рішенням для організацій і майже в кожному офісі зараз можна зустріти цю технологію.

Перейдемо до розгляду дій по роботі з AD.

Без наявності Windows Server нічого не вийде, тому першочергово потрібно його встановити [20].

Після встановлення і запуску ми будемо спостерігати панель менеджера сервера, що є основним графічним засобом керування. З її допомогою ми маємо можливість керувати компонентами і сервісами на сервері. Також цю панель можна використовувати і для базових мережеских налаштувань.

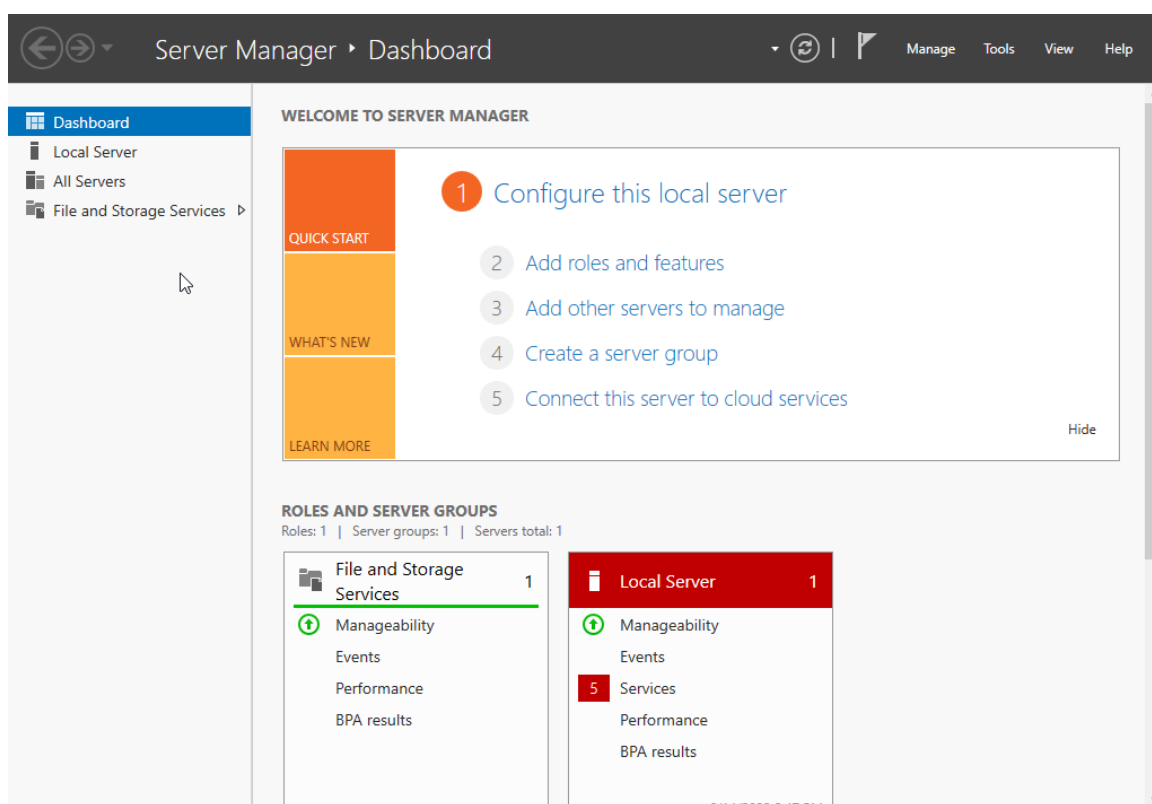


Рисунок 3.22 – Панель менеджера сервера в Windows Server 2019

Першим кроком буде зміна мережевого імені сервера, так як за замовчуванням генерується складне і незрозуміле ім'я.

Мережеве ім'я використовується як альтернатива IP-адресі і дає змогу не запам'ятовувати адресу комп'ютера, а зв'язуватись з ним по його логічній назві. З урахуванням того, що IP-адреса може змінюватись – це буде розумним рішенням.

Робочі станції організації ще можуть мати стандартно згенероване ім'я (але бажано змінити і їх), а ось для сервера це зовсім не бажано.

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				45
Змн.	Арк.	№ докум.	Підпис	Дата		

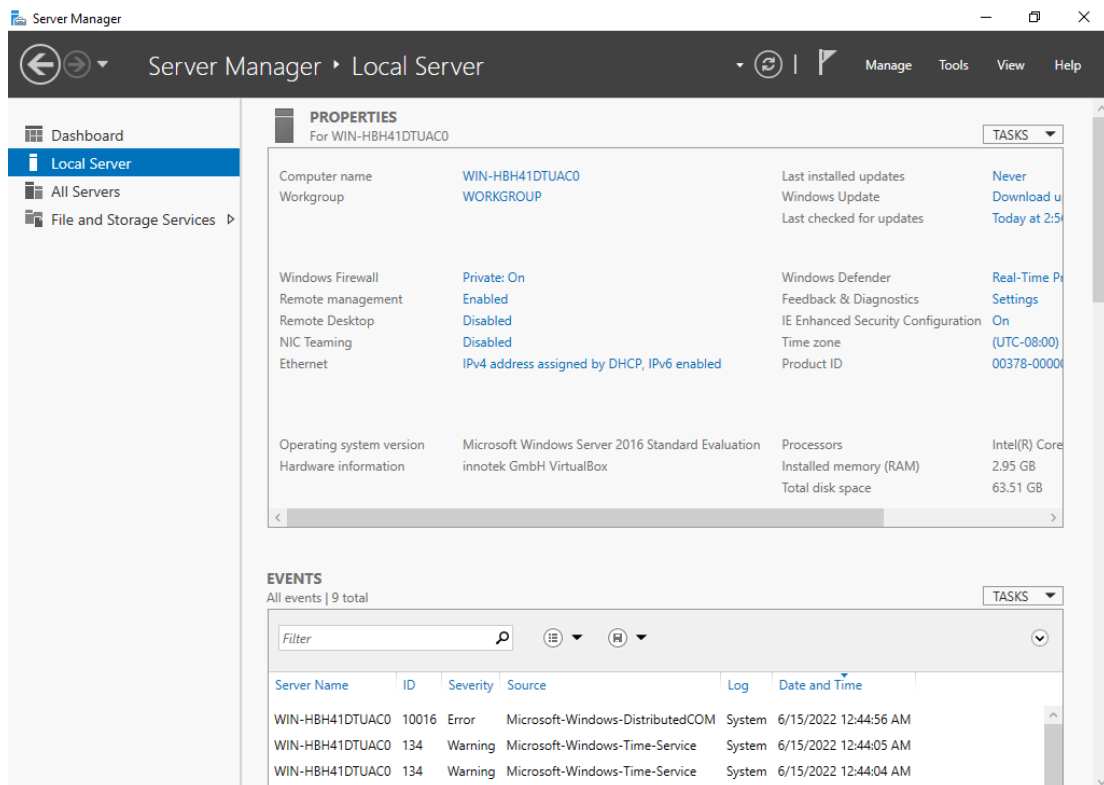


Рисунок 3.23 – Властивості сервера

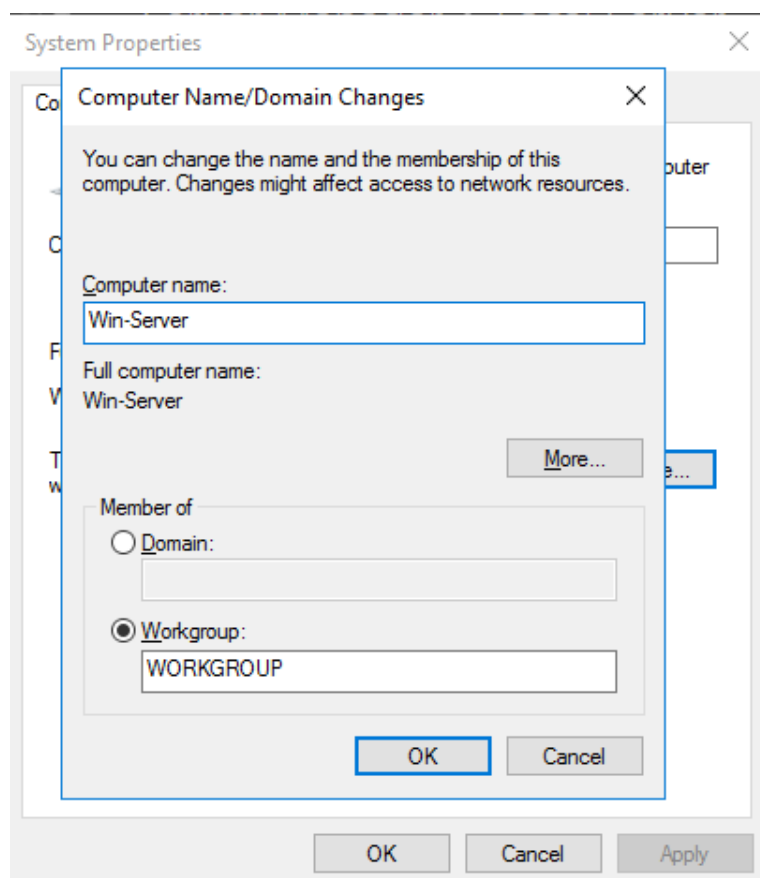


Рисунок 3.24 – Зміна мережевого імені комп'ютера

Після виконаних дій зі зміни імені треба перезапустити машину.

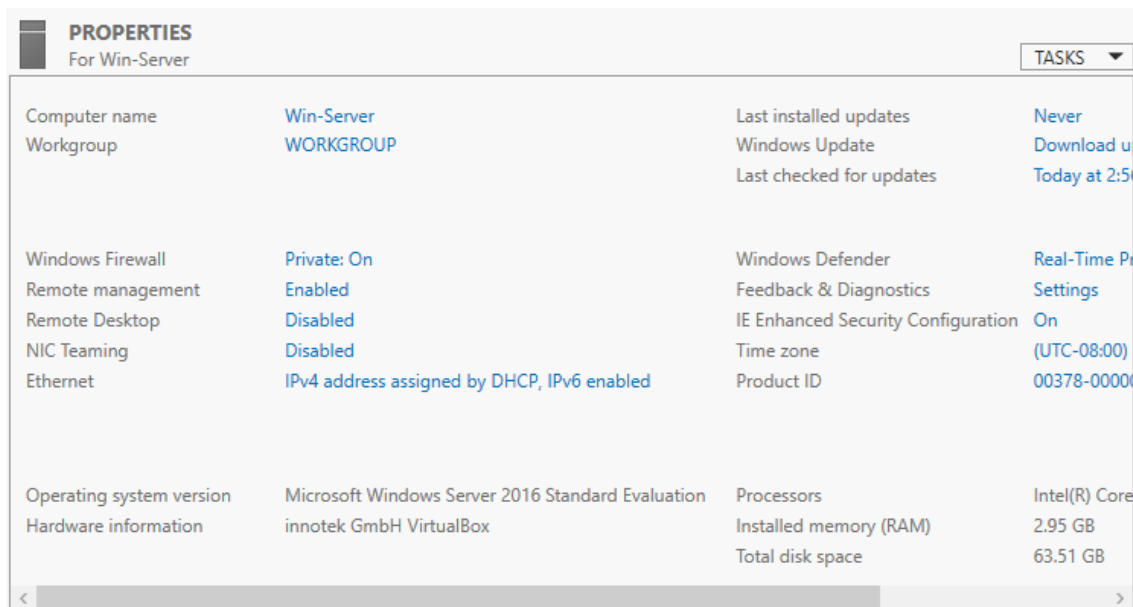


Рисунок 3.25 – Змінене мережеве ім'я у властивостях сервера

Після зміни імені слід задати статичну IP-адресу серверу або підняти службу DHCP. Так як DHCP було налаштовано на маршрутизаторі R1 раніше, задано статичну адресу.

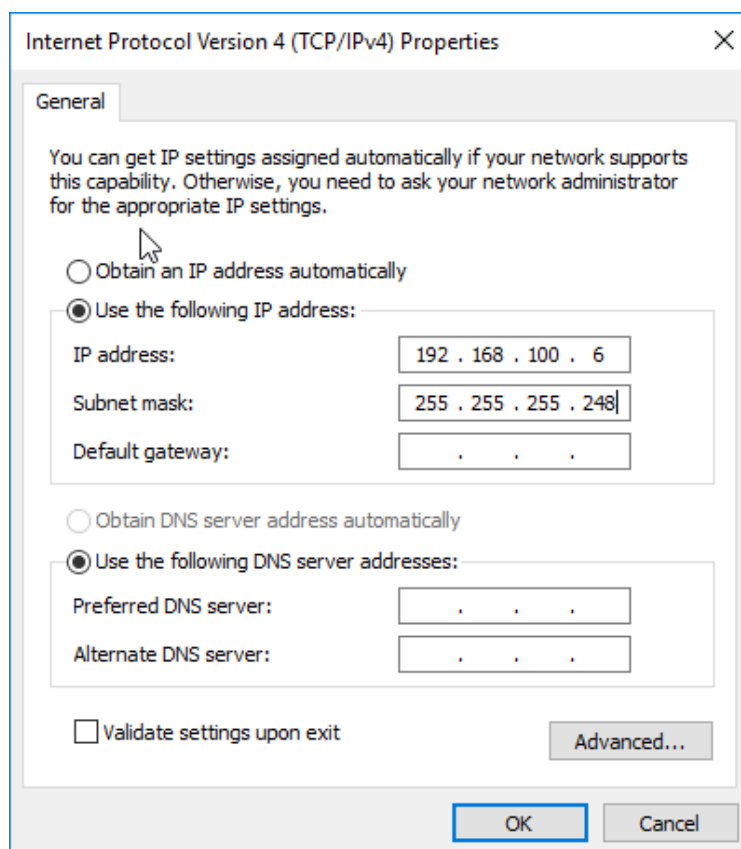


Рисунок 3.26 – Задання IP-адреси на сервері

З базовими налаштуваннями сервера закінчено. Далі було ввімкнено сервіси (ролі) на Windows Server.

А саме: «Служби домену Active Directory» та «DNS–сервер».

Служби домену AD – роль, що і підіймає технологію Active Directory на сервері і задає йому роль контролера домену. Саме ця роль дає можливість адміністратору керувати об'єктами в мережі і створює базу даних, в якій буде зберігатись інформація про них. На цю базу і приходить запит на аутентифікацію користувача при спробі входу в обліковий запис.

Використання DNS–сервера є також обов'язковим, так як він зберігає всі DNS–записи [18].

У ролі DNS–сервера можна використовувати як саму машину сервера, так і якусь окрему. Для масштабних організацій більш правильним буде використовувати для DNS–сервера окрему машину.

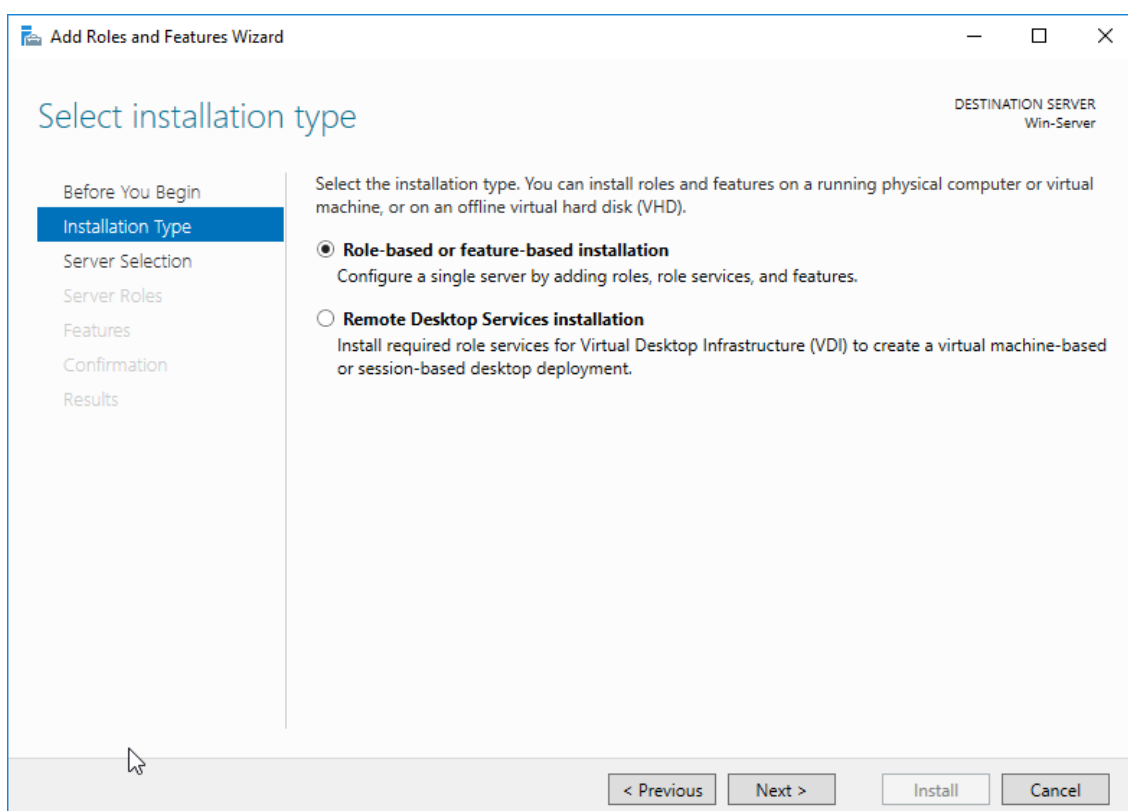


Рисунок 3.27 – Вікно додавання ролей і компонентів у Windows Server

Після вибору всіх ролей і компонентів буде запропоновано подивитися на весь перелік інструментів, що будуть встановлені.

По закінченню встановлення отримуємо можливість налаштовувати контроллер. Переходимо в конфігурацію розгортання та додаємо новий ліс і кореневий домен. У нашому випадку – office.local.

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

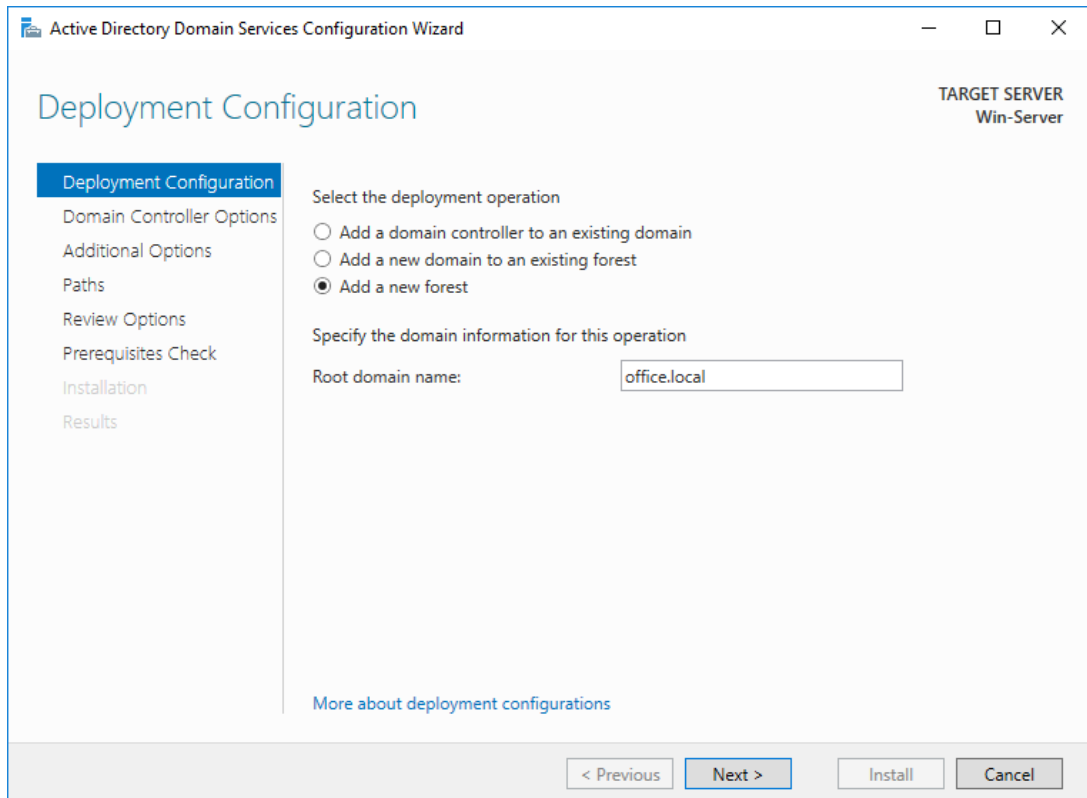


Рисунок 3.28 – Вікно майстра налаштування домених служб AD

Переходимо в параметри контролера домена, де можемо обрати режим роботи лісу та домена, можливості контролера, та ввести пароль для відновлення служб каталогів.

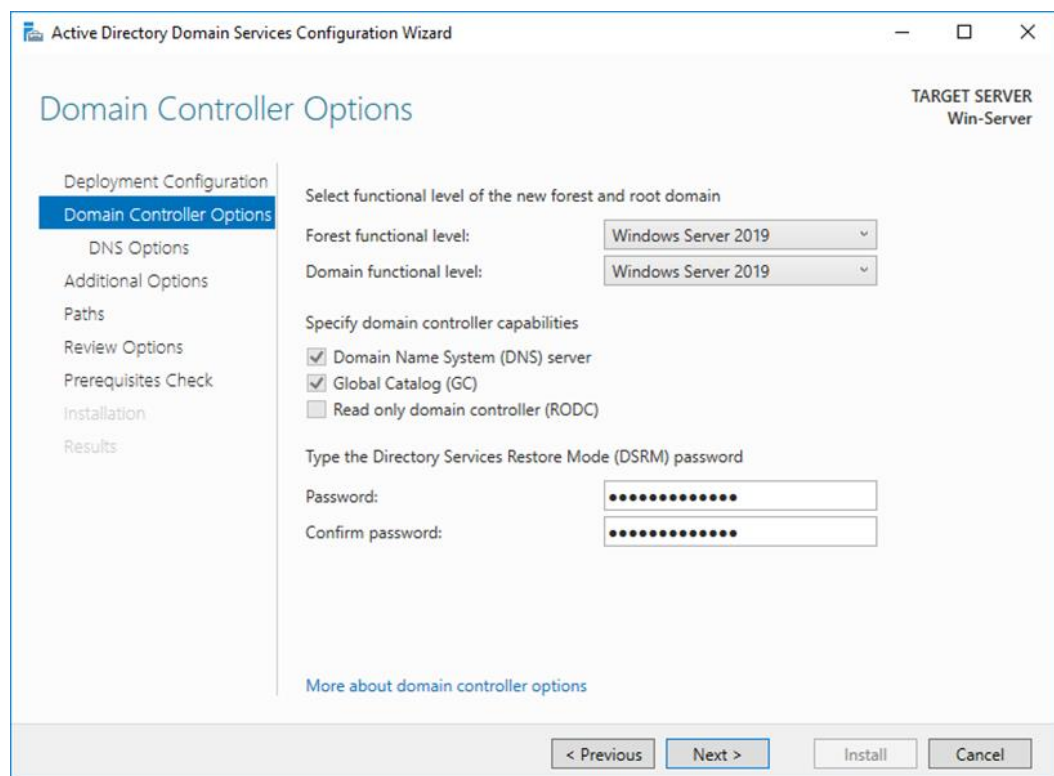


Рисунок 3.29 – Параметри контролера домена(змінити картинку)

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				49
Змн.	Арк.	№ докум.	Підпис	Дата		

Далі переходимо в додаткові налаштування, де автоматично згенерувалося NetBIOS-ім'я. NetBIOS (Network Basic Input/Output) – старіший і примітивніший аналог DNS, який також використовується для дозволу доменних імен в мережі.

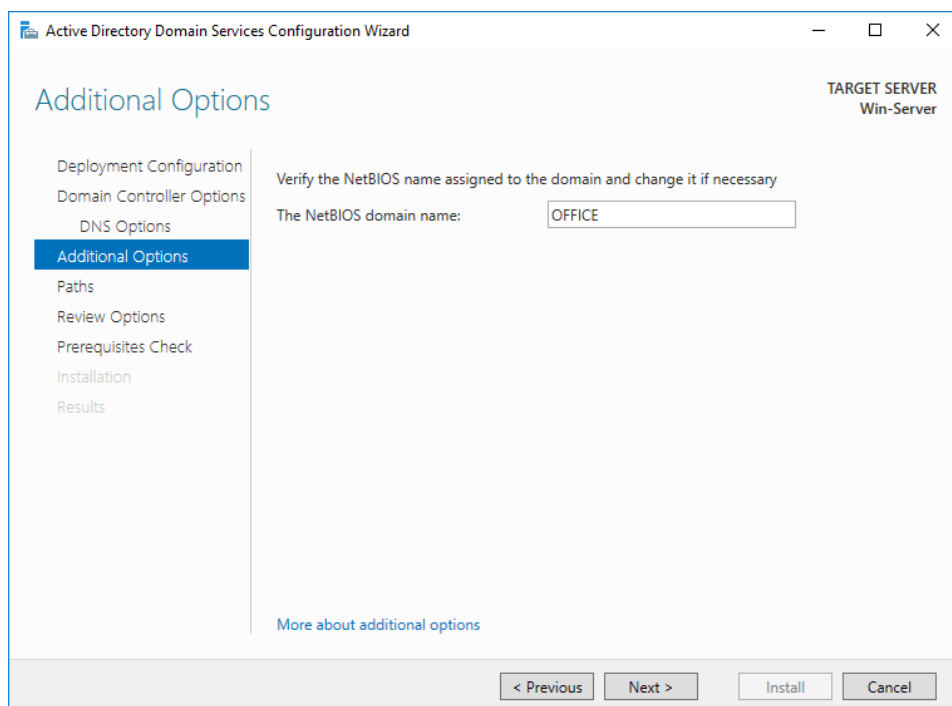


Рисунок 3.30 – Налаштування імені домена NetBIOS

Потрапляємо на попередню перевірку налаштувань. Пройшовши перевірку, можемо почати встановлення і після цього налаштування контролеру домена AD завершено.

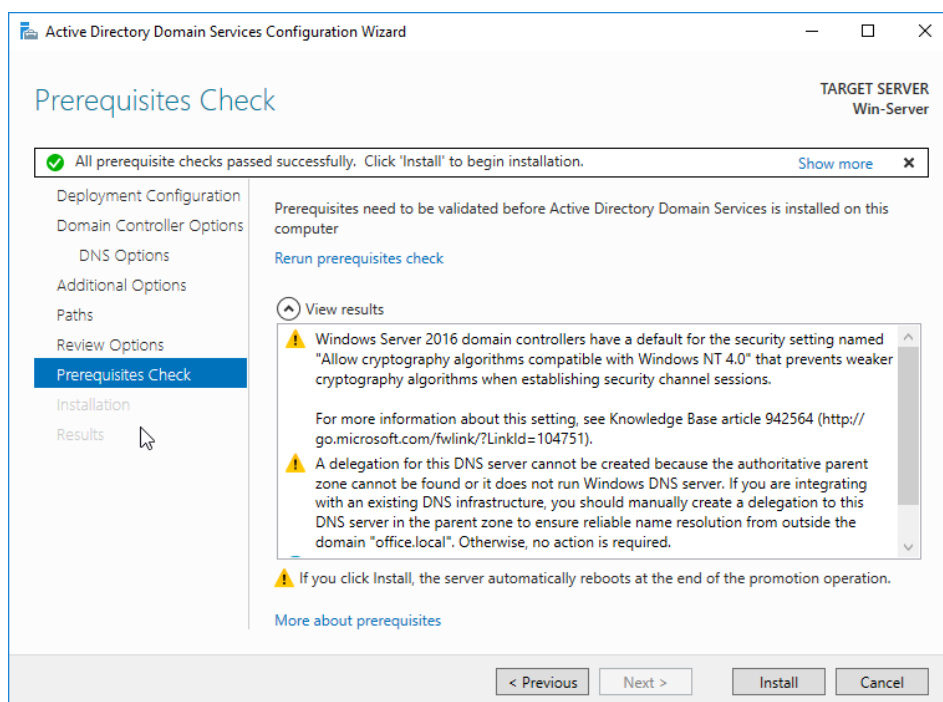


Рисунок 3.31 – Попередня перевірка вимог налаштувань

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

Після встановлення всіх налаштувань комп'ютер перезапускається, і ми бачимо, що тепер він у домені office.local.

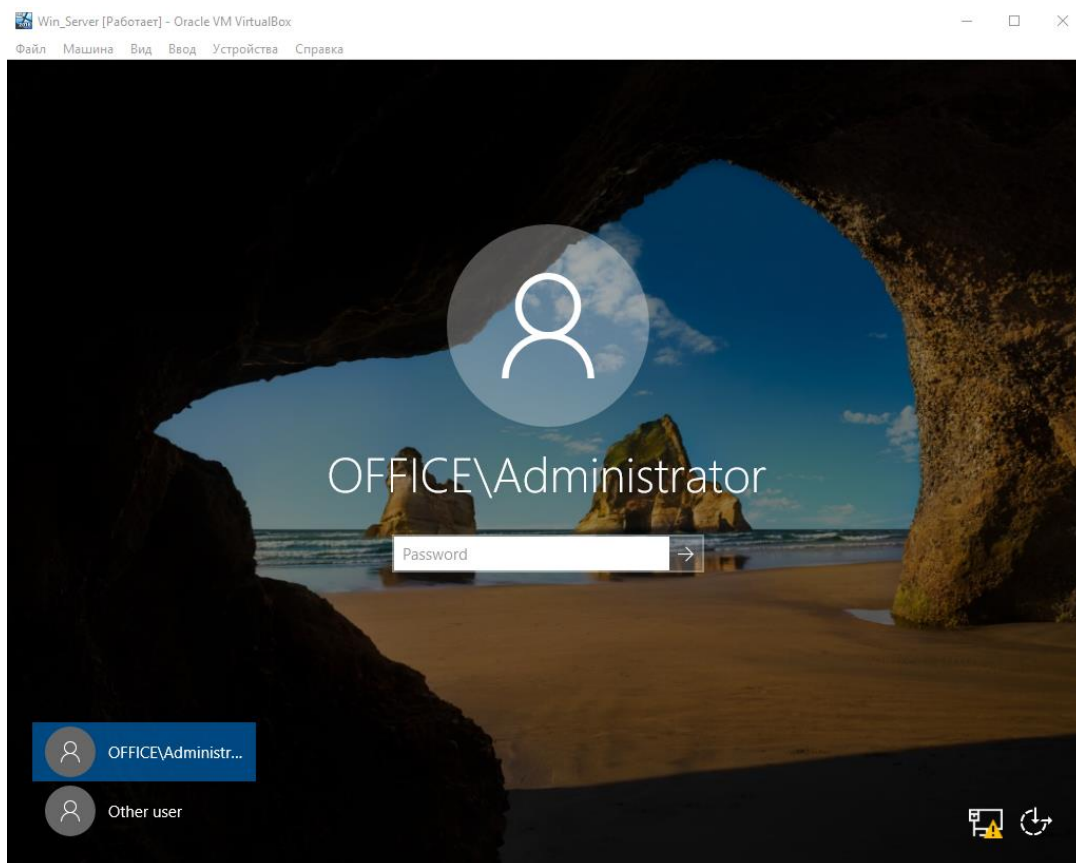


Рисунок 3.32 – Екран входу після перезапуску

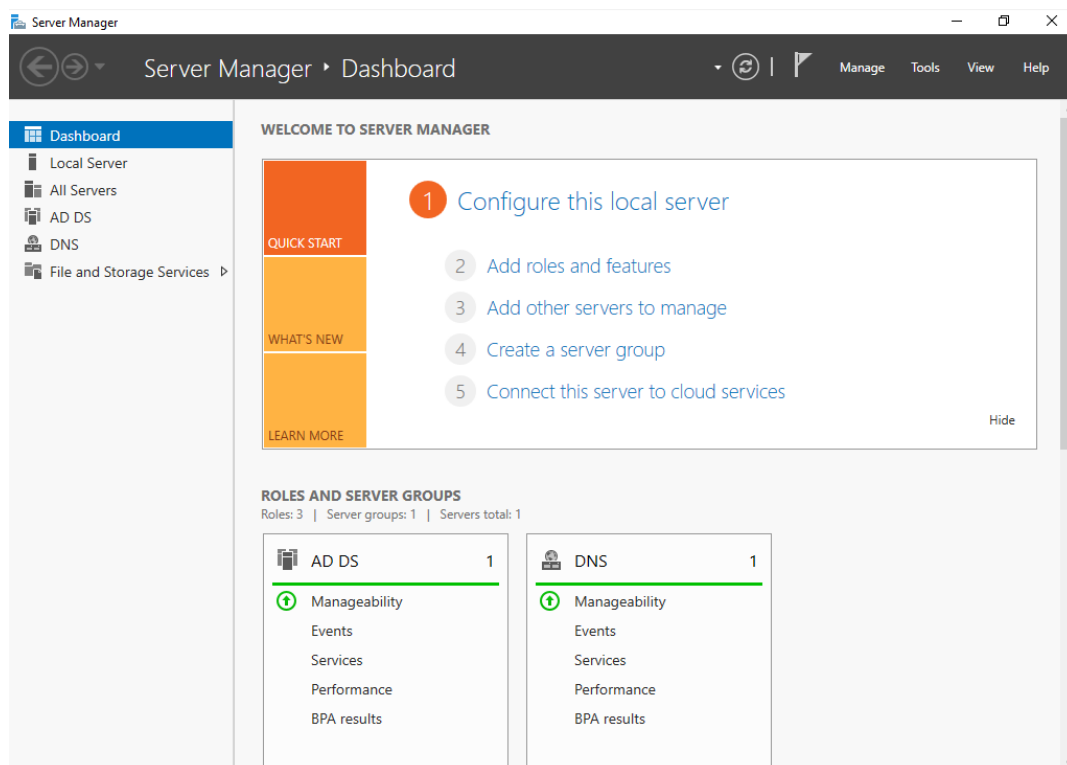


Рисунок 3.33 – Панель менеджера серверів після налаштувань AD

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				51
Змн.	Арк.	№ докум.	Підпис	Дата		

Переходимо у вікно «Користувачі і Компютери Active Directory». В ньому знаходяться всі об'єкти домену. Тут можна додавати, видаляти та редагувати їх.

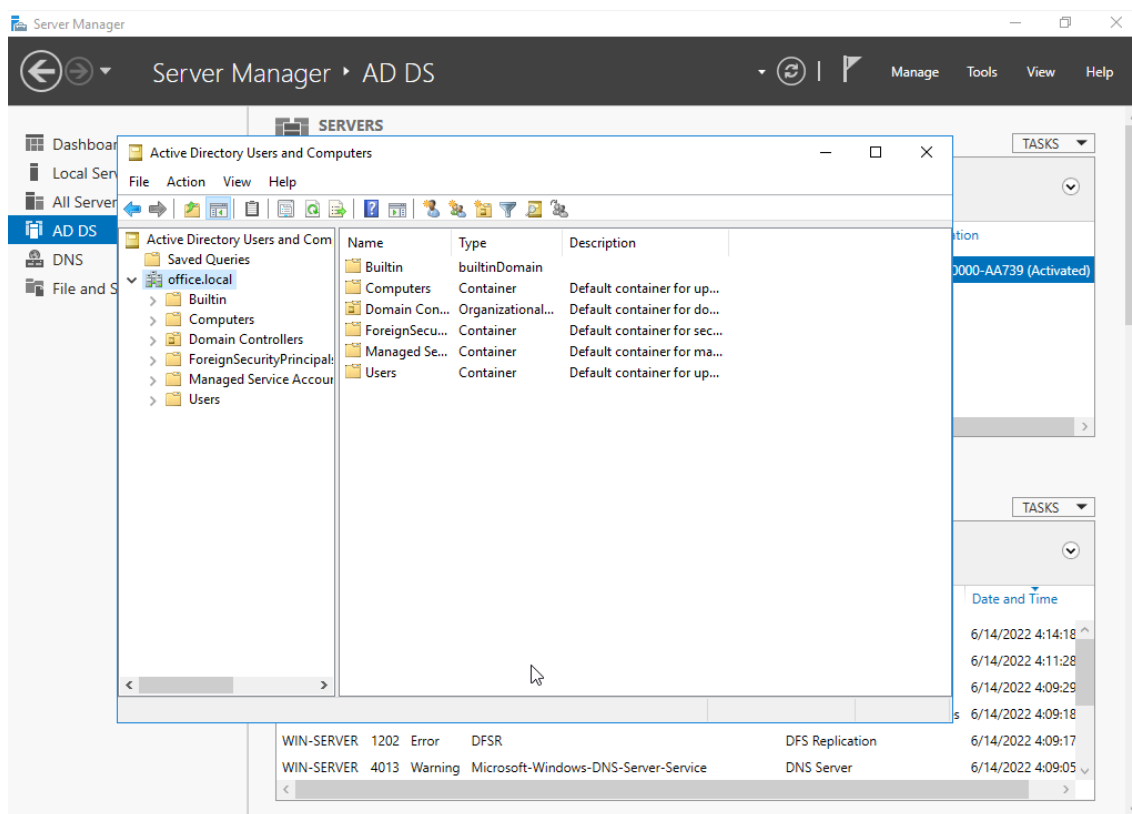


Рисунок 3.34 – Об'єкти домена

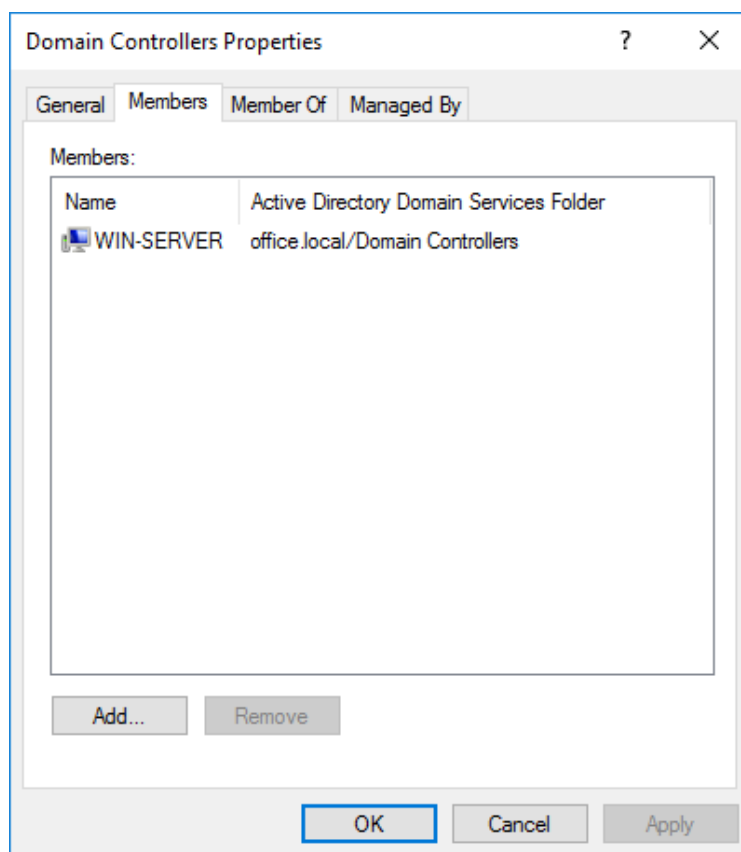


Рисунок 3.35 – Контролер домена

У папці Users було проведено додавання нових облікових записів для працівників організації на прикладі створення користувача off1_us1 [19].

Рисунок 3.36 – Додавання нового користувача

Після того як ми визначилися з ім'ям облікового запису та ім'ям, під яким буде виконуватись вхід, нам потрібно задати користувачу особистий пароль, що повинен відповідати паролівній політиці домена. Також можна вибрати дії з паролем для цього користувача: користувач має змінити пароль при першому вході, користувач ніколи не може змінювати пароль...

Рисунок 3.37 – Задання пароля користувачу

		Хімічук І.С.		
		Байлюк Є.М.		
Змн.	Арк.	№ докум.	Підпис	Дата

На фінальному етапі створення відображаються обрані раніше налаштування.

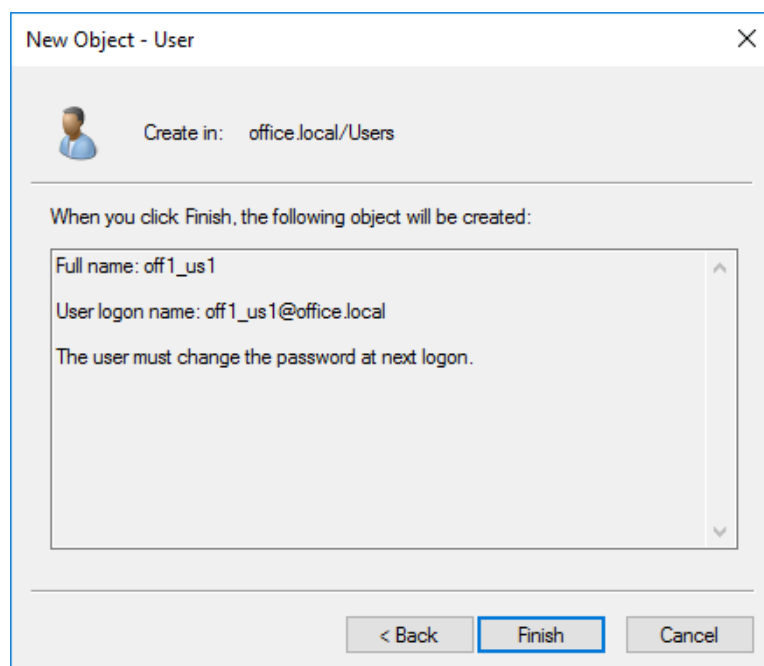


Рисунок 3.38 – Останній етап створення користувача

У результаті було створено десять нових користувачів.

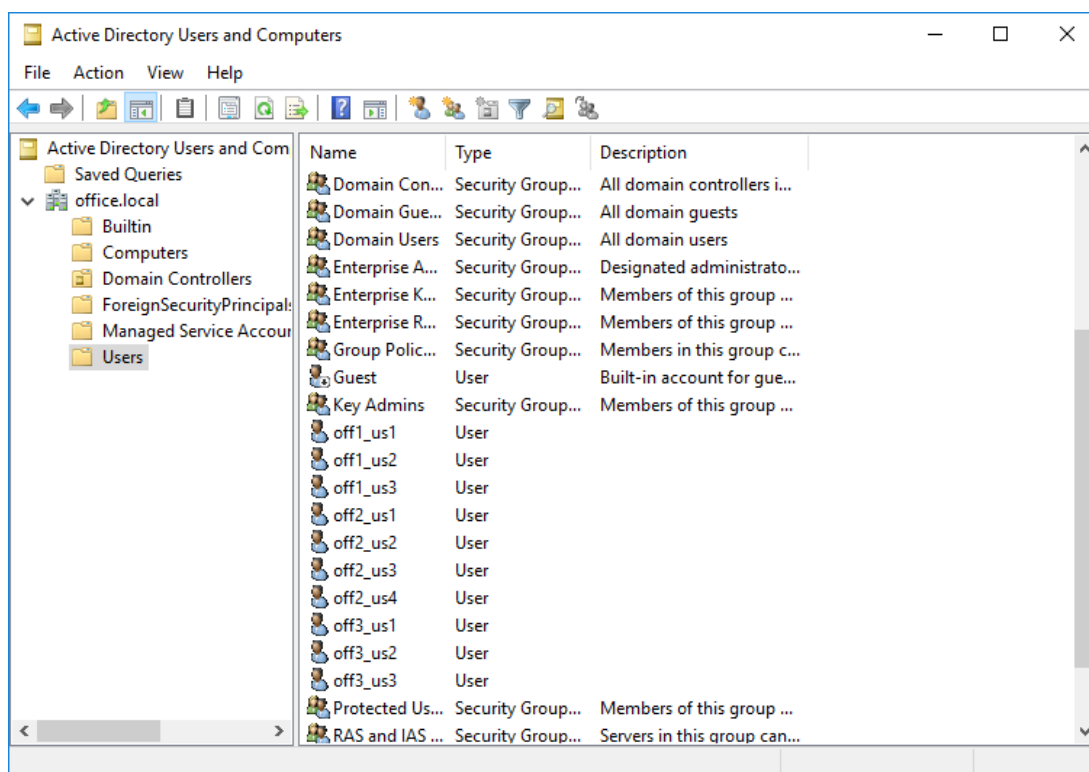


Рисунок 3.39 – Створені користувачі

Так як працівники будуть розміщені в різних офісних приміщеннях і облікові записи названі відповідно до цих приміщень, доцільно буде створити три окремих групи для них. Далі додаємо в ці групи потрібних користувачів.

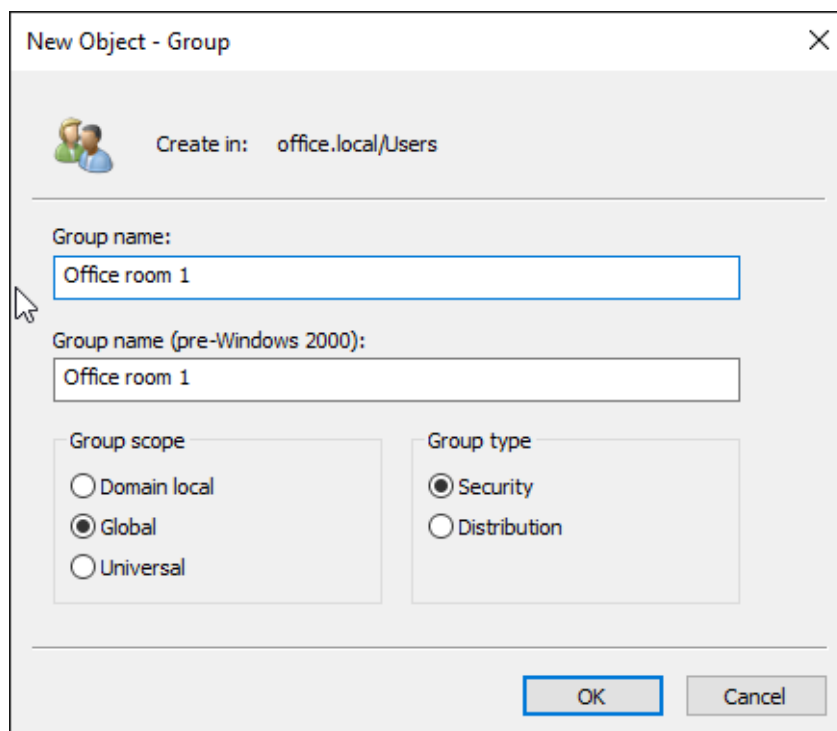


Рисунок 3.40 – Створення нової групи користувачів

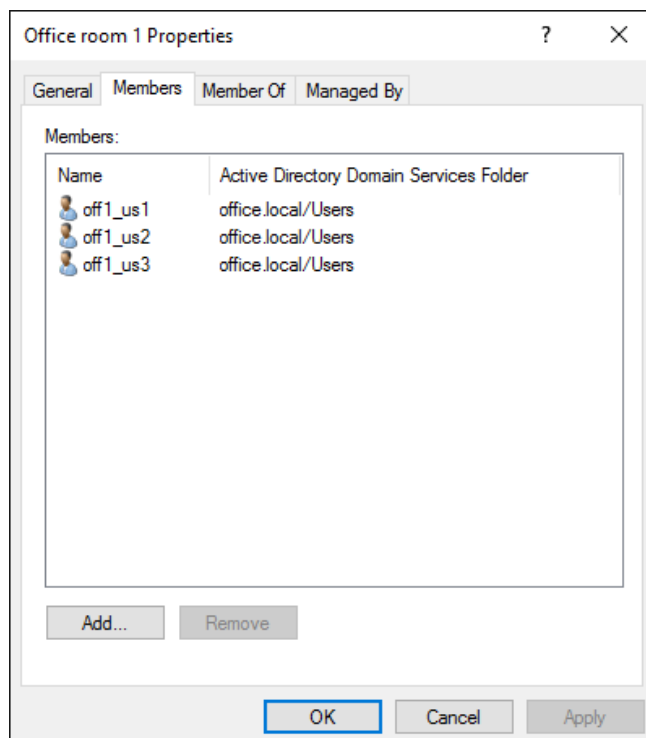


Рисунок 3.41 – Додані в групу користувачі

Для доданих груп користувачів створюємо новий об'єкт «Office groups» і додаємо їх в нього.

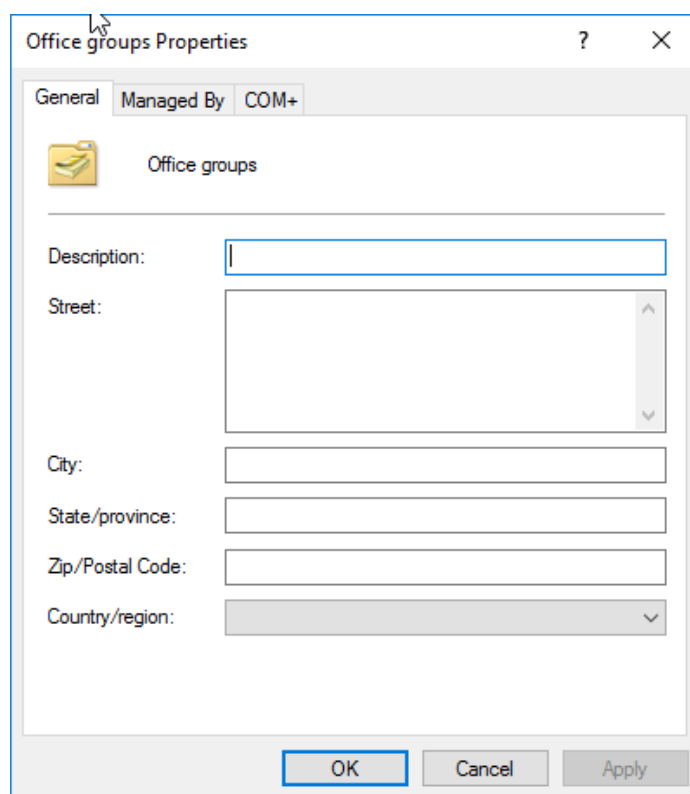


Рисунок 3.42 – Створений новий об'єкт Office groups

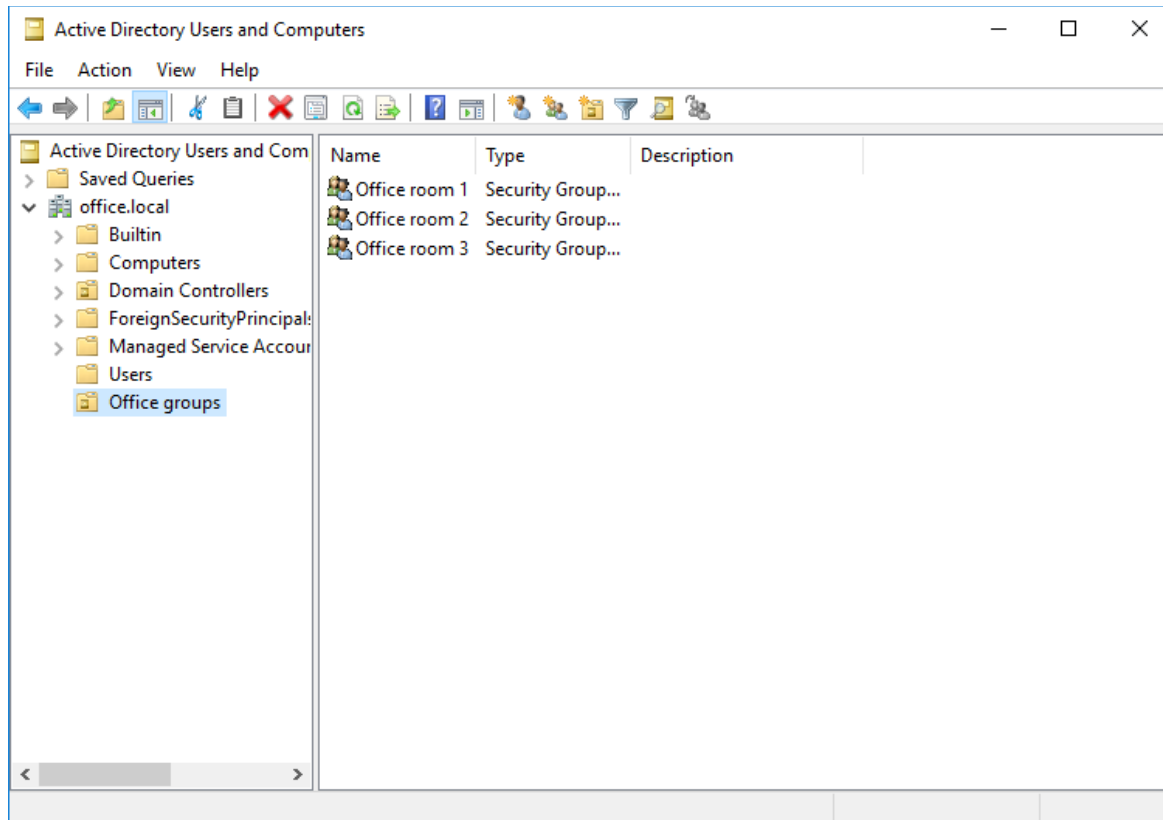


Рисунок 3.43 – Додані в об'єкт групи користувачів

3.3 Налаштування підсистеми захисту клієнт–серверної мережі на базі ОС Windows

Після налаштування пристроїв мережі та розгортання Active Directory, переходимо до налаштування підсистеми захисту клієнт–серверної мережі, що була розроблена в другому розділі.

Як зазначалось раніше, на комутатори може бути реалізована атака підміни DHCP–сервера.

Найкращим захистом від цього є вмикання на всіх комутаторах функції DHCP snooping і подальше вказання довірених (truth) портів.

```
Main-SW#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Main-SW(config)#ip dhcp sn
Main-SW(config)#ip dhcp snooping vlan 10,20,30,50,100
Main-SW(config)#ip dhcp snooping trust e0/0, e0/3, e1/1, e2/2, e3/3
```

Рисунок 3.44 – Налаштування DHCP snooping

Ще розглядалася атака на VLAN (VLAN Hopping). Вона використовує можливість комутаторів автоматично погоджувати типи портів. Отже, вимикаємо цю можливість командою switchport nonegotiate.

```
Main-SW#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Main-SW(config)#int e0/1
Main-SW(config-if)#switchport nonegotiate
```

Рисунок 3.45 – Налаштування команди switchport nonegotiate на інтерфейсі e0/1

Також ця атака має інший варіант, коли зловмисник використовує підключення до native VLAN і додає ще один тег [17].

Для уникнення такого сценарію, на всіх транкових портах назначаємо в якості native невикористовуваний VLAN.

```
Main-SW#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Main-SW(config)#int e0/0
Main-SW(config-if)#switchport trunk native vlan 999
Main-SW(config-if)#int e0/3
Main-SW(config-if)#switchport trunk native vlan 999
Main-SW(config-if)#int e1/1
Main-SW(config-if)#switchport trunk native vlan 999
Main-SW(config-if)#int e2/2
Main-SW(config-if)#switchport trunk native vlan 999
Main-SW(config-if)#int e3/3
Main-SW(config-if)#switchport trunk native vlan 999
Main-SW(config-if)#
```

Рисунок 3.46 – Назначення в ролі native невикористовуваний VLAN 999

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				57
Змн.	Арк.	№ докум.	Підпис	Дата		

У кінці налаштування захисту на пристроях для максимальної безпеки слід вимкнути невикористовувані порти. Це виключить можливість підключення до пристроїв зловмисного засобу.

```
Main-SW#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Main-SW(config)#int range e0/1-2, e1/0, e1/2-3, e2/0-1
Main-SW(config-if-range)#sh
Main-SW(config-if-range)#int e2/3
Main-SW(config-if)#sh
Main-SW(config-if)#int range e3/0-2
Main-SW(config-if-range)#sh
```

Рисунок 3.47 – Вимкнення невикористовуваних портів на комктаторі Main-SW

Тепер перейдемо до налаштування захисту в Active Directory.

Почнемо з самого простого і при створенні нового користувача, при задаванні йому паролю, поставимо галочку в пункті user must change password at next logon. Працівник отримує від адміністратора пароль, по якому вперше заходить в систему і одразу при вході змінює пароль на свій особистий, який буде відповідати нормам політики домена. Такий підхід забезпечує максимальну безпеку, адже навіть адміністратор не буде знати пароль користувача.

Рисунок 3.48 – Дозвіл працівнику змінити свій пароль при першому вході

Далі створюємо резервні облікові записи для адміністратора. Це робиться на випадок виникнення проблем з основним записом. Рекомендується в подальшому використовувати ці записи, а резервним буде саме головний. Також для цих користувачів задається постійний пароль.

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				58
Змн.	Арк.	№ докум.	Підпис	Дата		

New Object - User

Create in: office.local/Users

First name: admserv1 Initials:

Last name:

Full name: admserv1

User logon name: admserv1 @office.local

User logon name (pre-Windows 2000): OFFICE\ admserv1

< Back Next > Cancel

Рисунок 3.49 – Створення нового облікового запису адміністратора

New Object - User

Create in: office.local/Users

Password:

Confirm password:

☐ User must change password at next logon

☐ User cannot change password

☒ Password never expires

☐ Account is disabled

< Back Next > Cancel

Рисунок 3.50 – Задання паролю запису адміністратора

New Object - User

Create in: office.local/Users

When you click Finish, the following object will be created:

Full name: admserv1

User logon name: admserv1@office.local

The password never expires.

< Back Finish Cancel

Рисунок 3.51 – Останній етап створення користувача

		Хімічук І.С.		
		Байлюк Є.М.		
Змн.	Арк.	№ докум.	Підпис	Дата

КІК.КР.Б – 125 – 24 – ПЗ

Арк.

59

Додаємо створених користувачів в групу адміністраторів домену

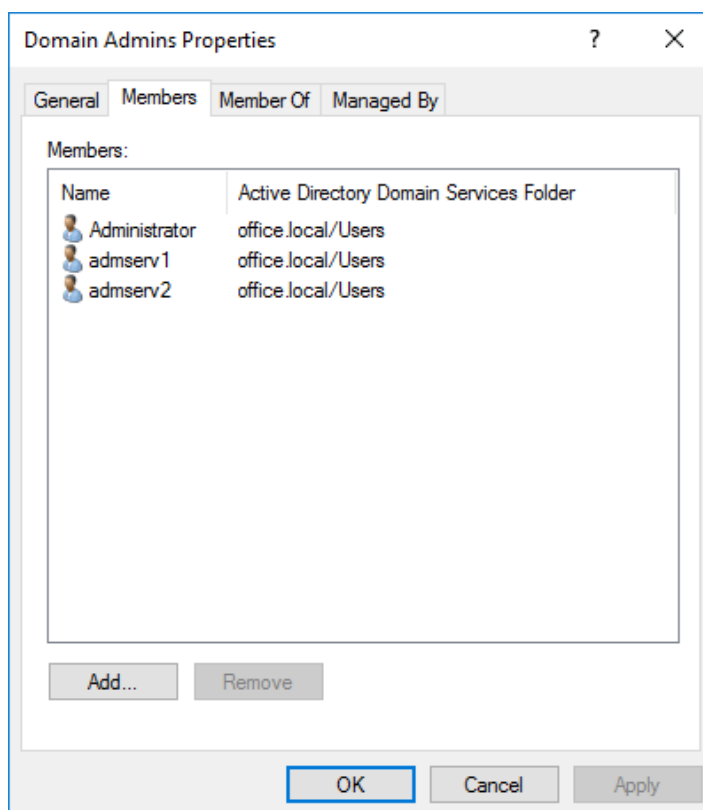


Рисунок 3.52 – Додані користувачі в групу адміністраторів домену

Гарним рішенням буде перейменування облікових записів адміністраторів, на якісь звичайні ім'я. Ці дії виконуються для того, щоб в разі отримання злоумисником переліку користувачів, він не зрозумів, хто має права адміністратора.

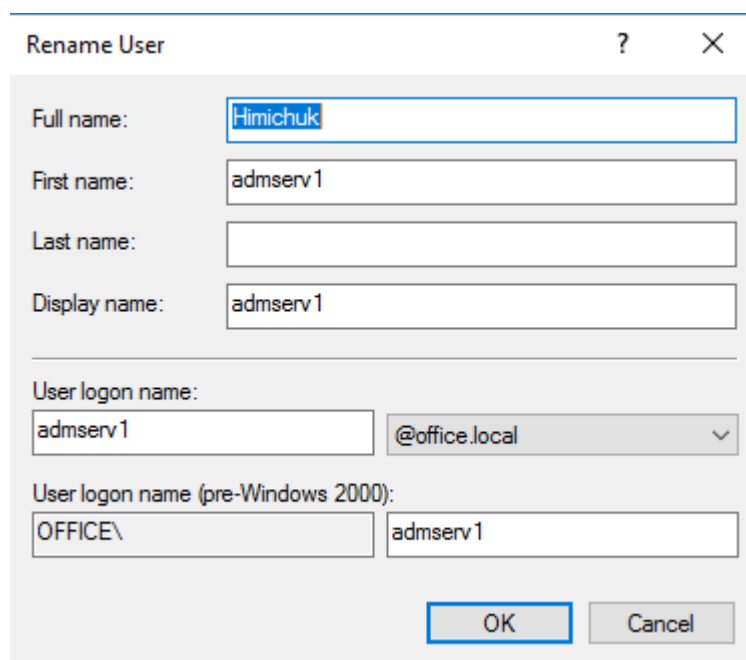


Рисунок 3.53 – Перейменування облікового запису адміністратора

		Хімичук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				60
Змн.	Арк.	№ докум.	Підпис	Дата		

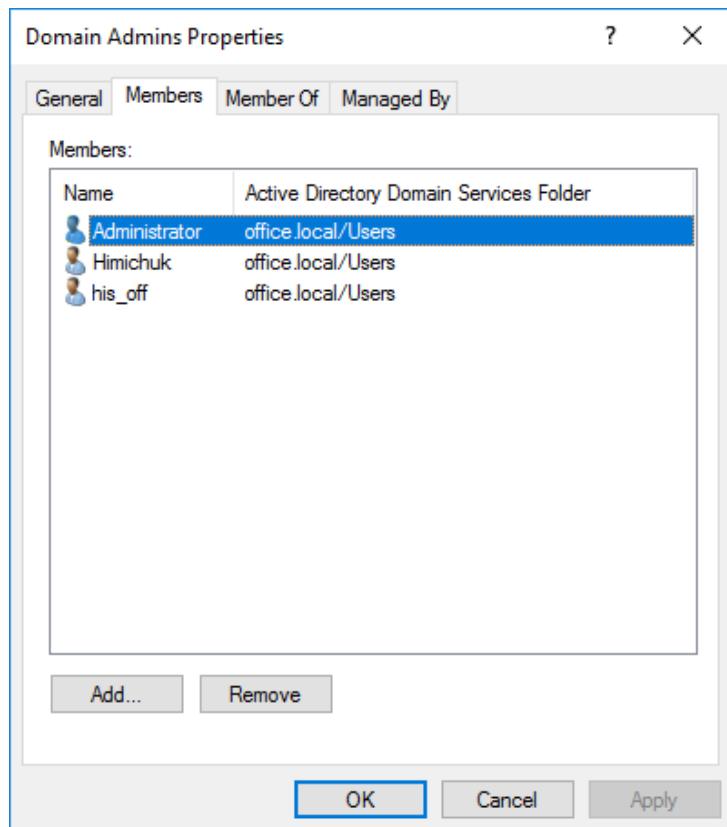


Рисунок 3.54 – Перейменовані записи адміністраторів

Наступним кроком буде налаштування групових політик. Для цього відкриваємо вікно менеджера групових політик.

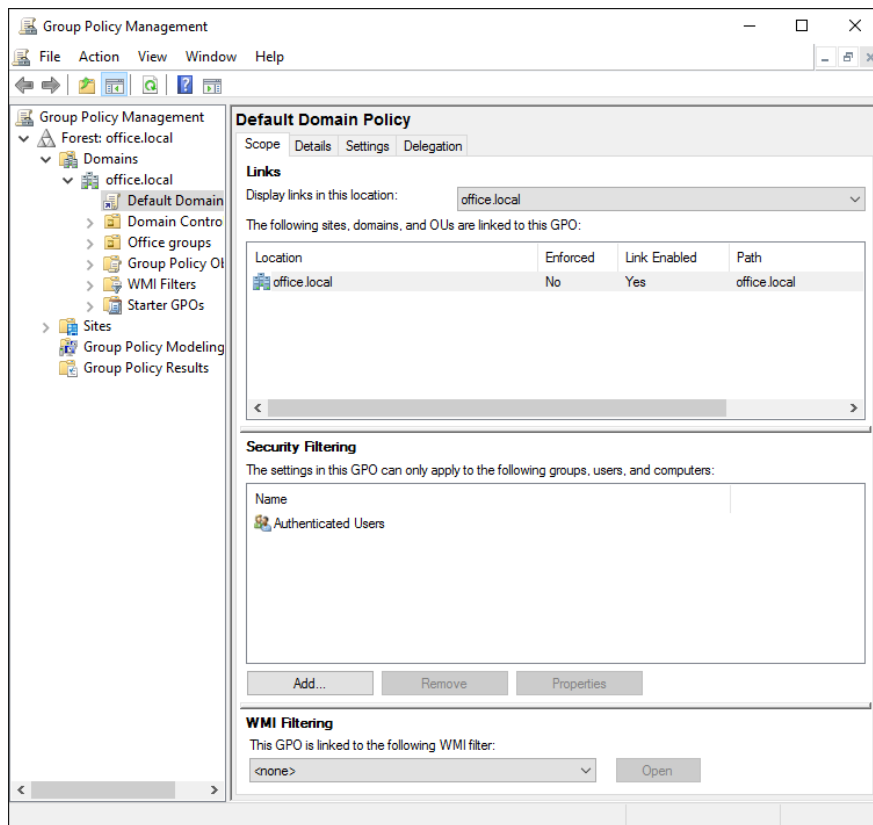


Рисунок 3.55 – Вікно менеджера групових політик

		Хімичук І.С.		
		Байлюк Є.М.		
Змн.	Арк.	№ докум.	Підпис	Дата

КІК.КР.Б – 125 – 24 – ПЗ

Арк.

61

Заходимо в налаштування політики безпеки домену і виставляємо для адміністратора домену всі можливі дозволи, а для авторизованих користувачів навпаки – мінімальні. Без прав адміністратора звичайні користувачі не зможуть встановлювати програми та вносити зміни в налаштування робочих машин.

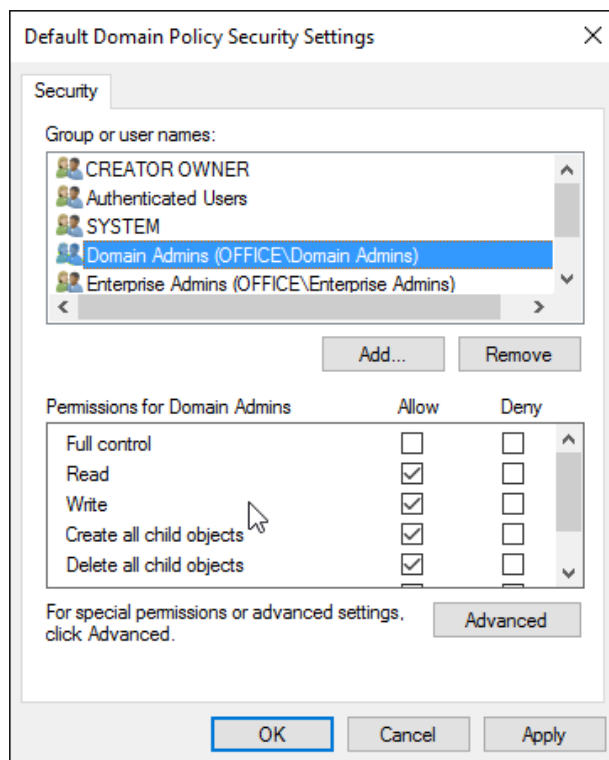


Рисунок 3.56 – Налаштування політик безпеки для адміністраторів

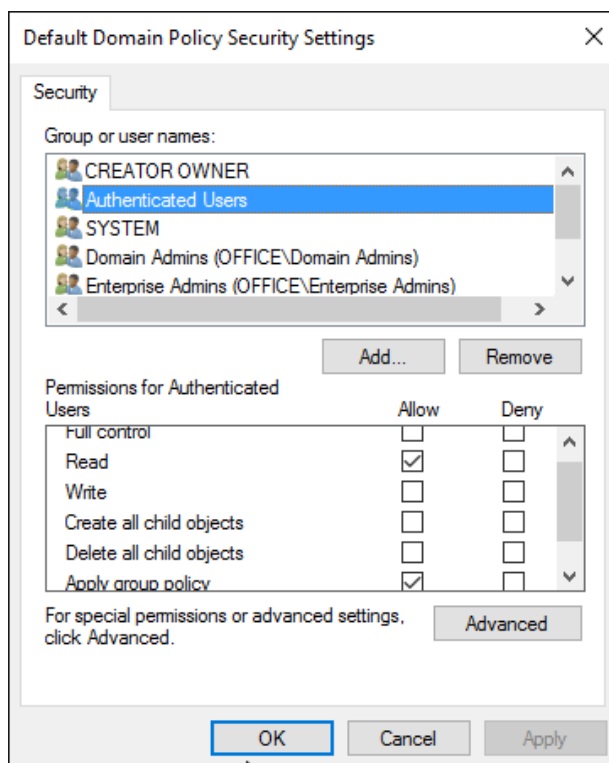


Рисунок 3.57 – Налаштування політик безпеки для користувачів

Далі налаштовуємо політики акаунтів. Переходимо у вкладку політик відносно паролів. Тут налаштовується термін дії паролів, мінімальна довжина паролю та параметри стосовно його складності.

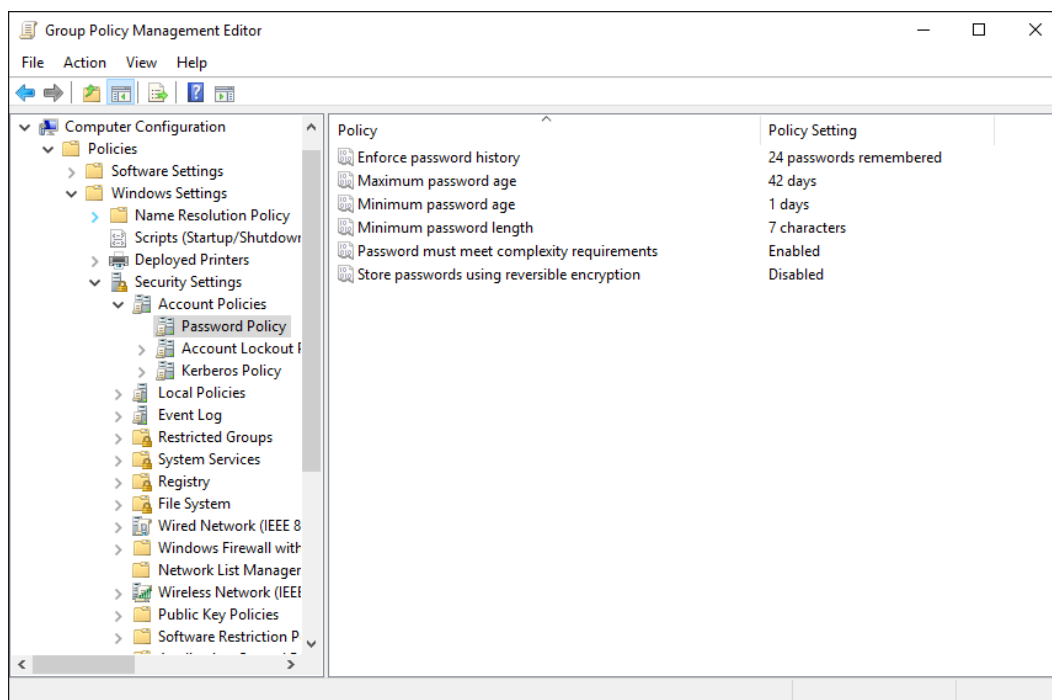


Рисунок 3.58 – Налаштування парольних політик

Наступним кроком налаштовуємо політику блокування акаунтів. Тут задаємо час блокування, розблокування та кількість спроб входу, після яких обліковий запис буде заблоковано.

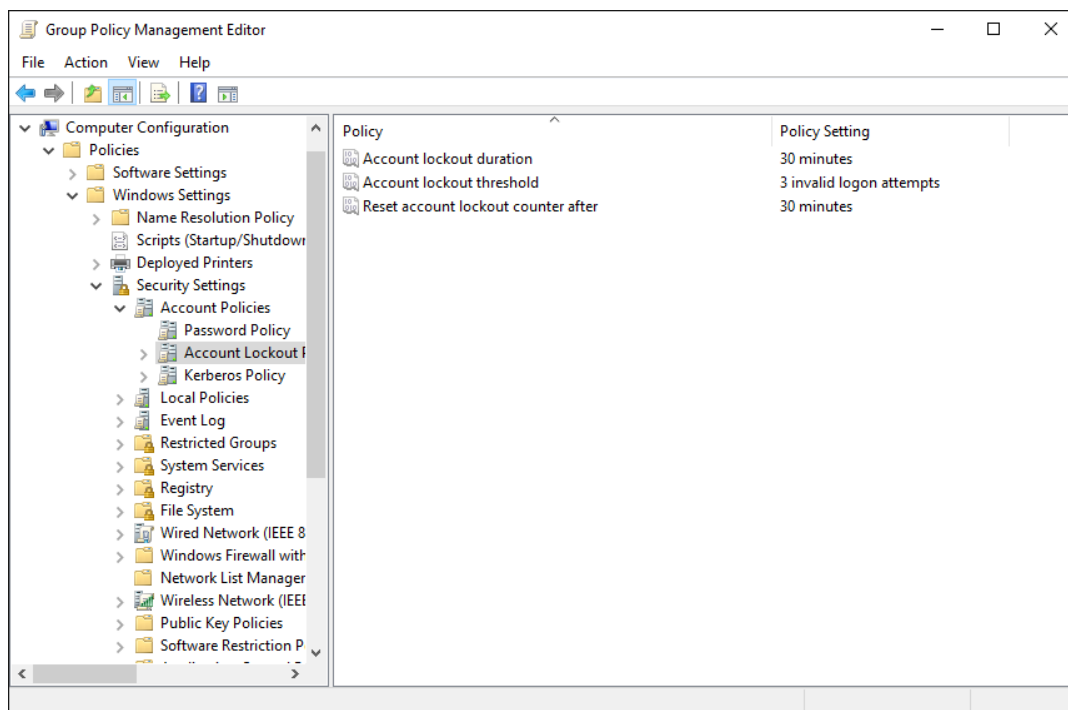


Рисунок 3.59 – Налаштування політик блокування акаунтів

Після налагоджень політик безпеки переходимо в налаштування політик аудиту. Налаштовані політики аудиту дають змогу записувати події, що відбуваються в домені в спеціальний журнал, та таким чином відслідковувати можливі дії порушника.

Першочергово виділяємо більше місця журналу безпеки, в який будуть записані всі налаштовані дії.

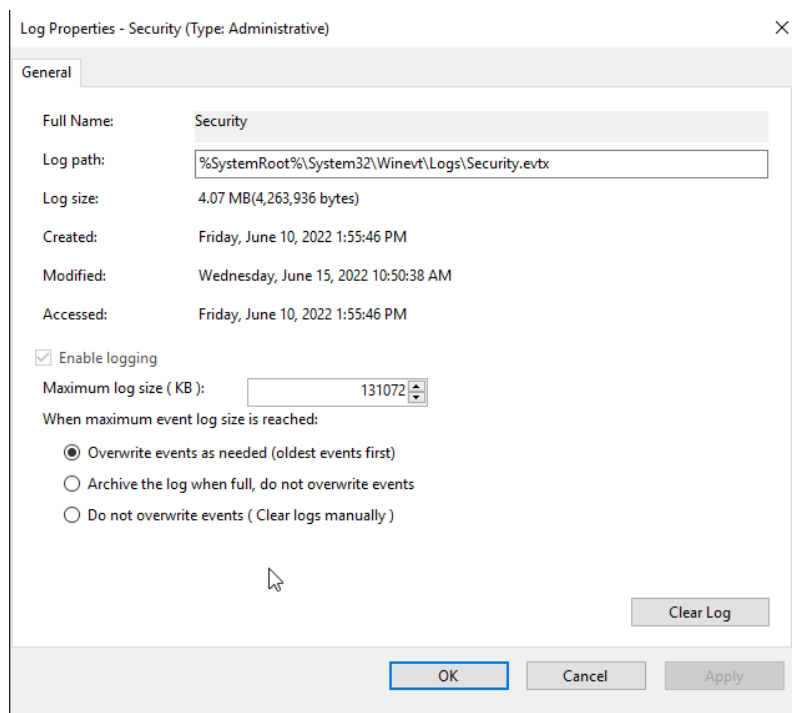


Рисунок 3.60 – Властивості журналу безпеки

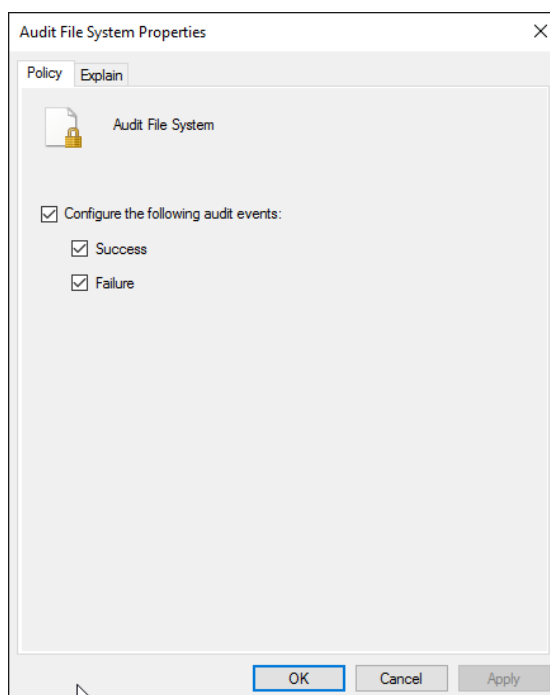


Рисунок 3.61 – Вмикання подій аудиту

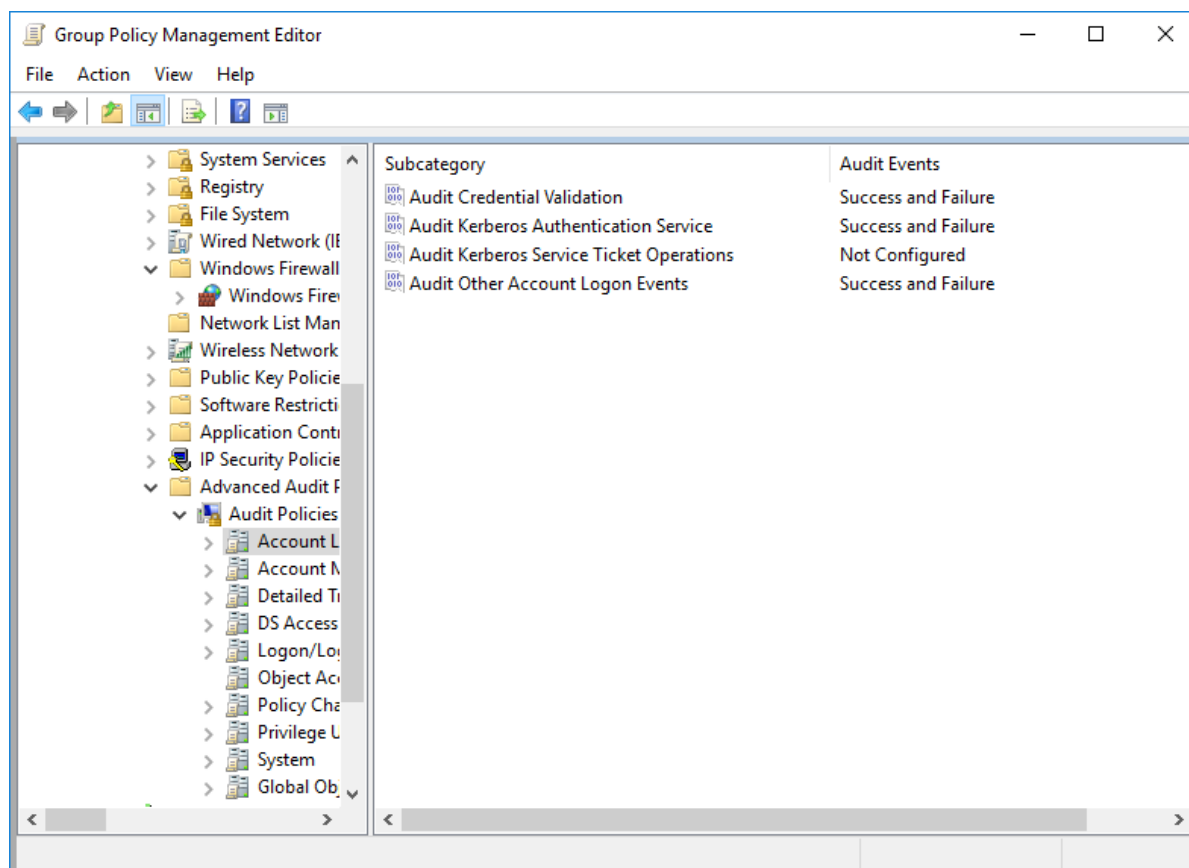


Рисунок 3.62 – Налаштування аудиту подій входу в систему

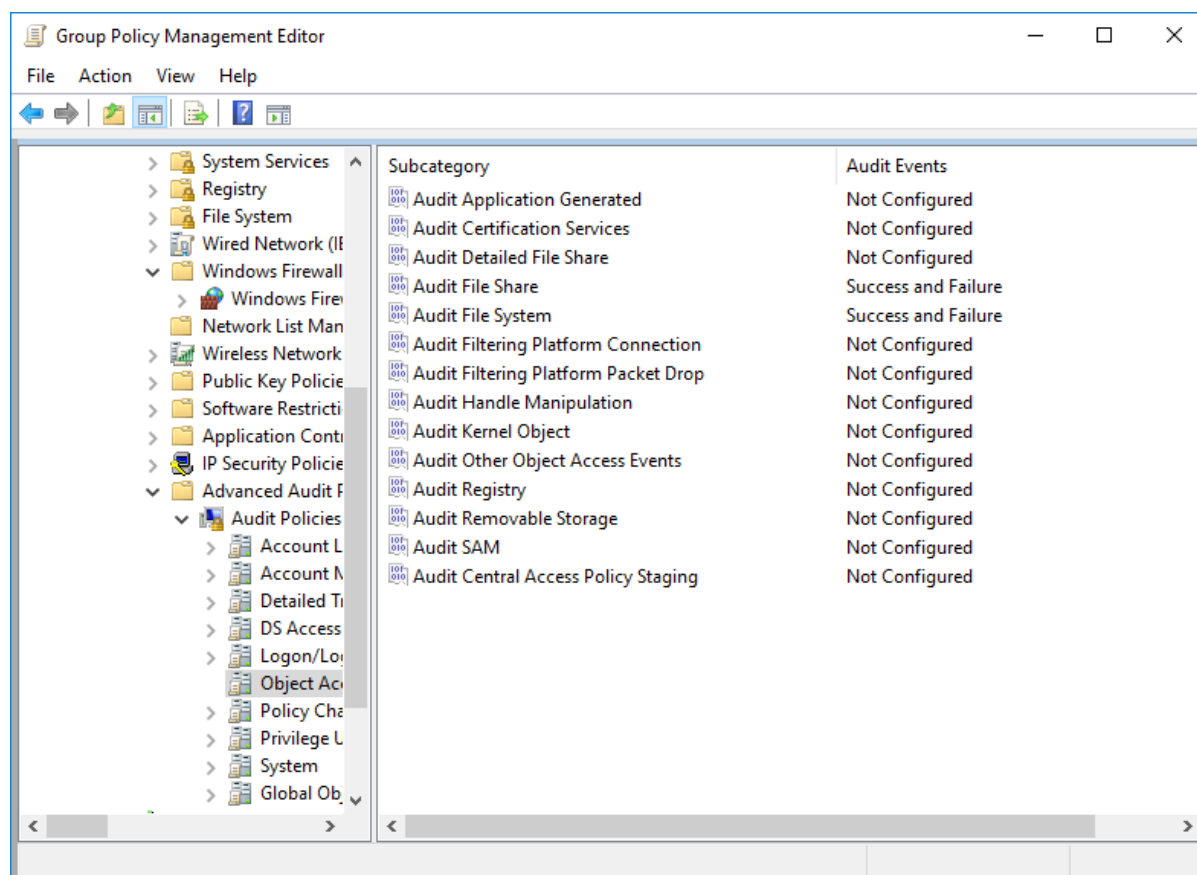


Рисунок 3.63 – Налаштування аудиту доступу до об'єктів

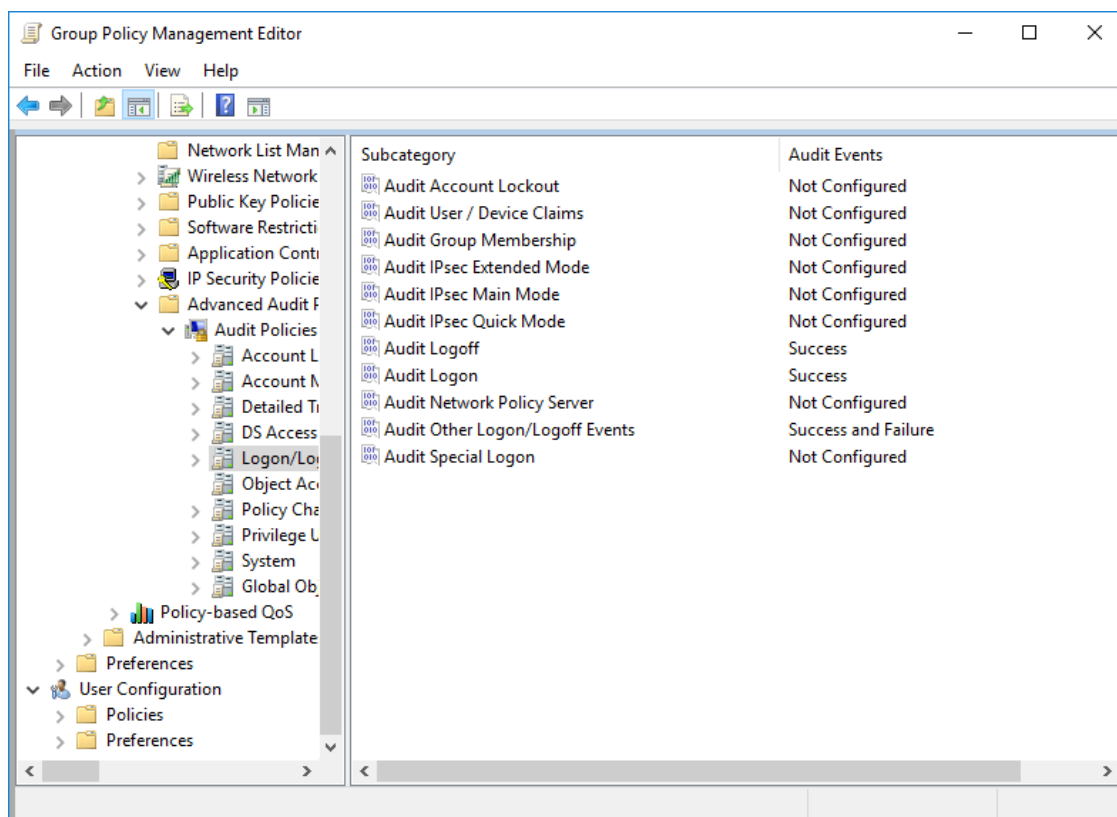


Рисунок 3.64 – Налаштування аудиту подій входу/виходу

Після налаштування політик аудиту можемо спостерігати всі виконувані дії, записані в журнал перегляду подій.

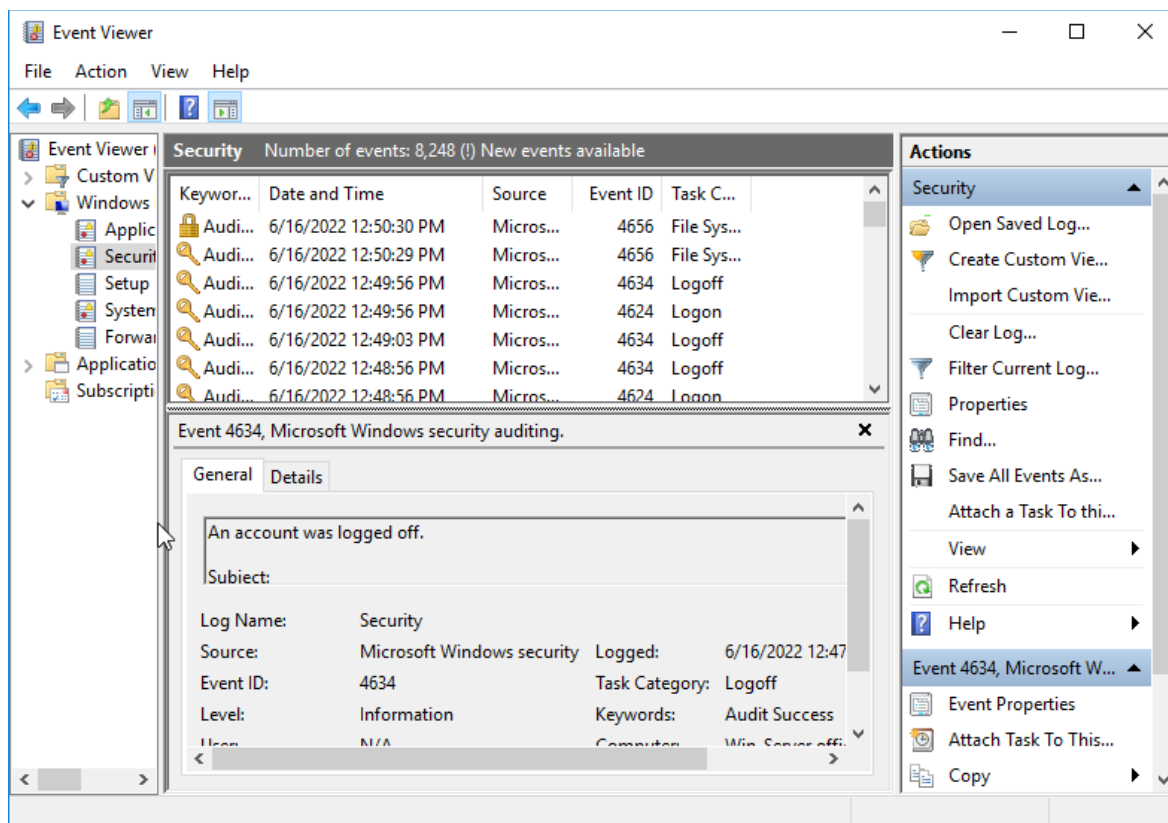


Рисунок 3.65 – Журнал перегляду подій

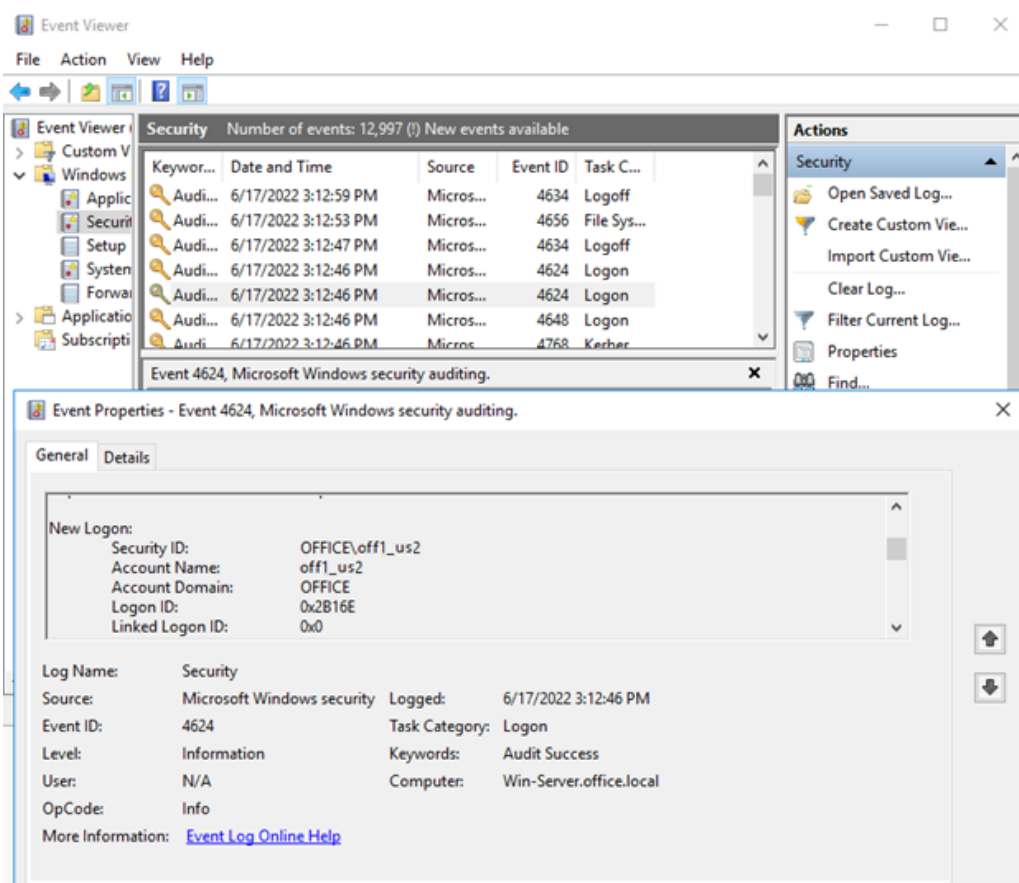


Рисунок 3.66 – Подія входу користувача

3.4 Тестування підсистеми захисту

По завершенню всіх налаштувань пристроїв мережі, налаштувань та розгортання Active Directory на Windows Server 2019, налаштувань підсистеми захисту клієнт–серверної мережі треба протестувати працездатність всієї системи.

Перше, що треба зробити – це додати комп'ютери в домен. Ця операція проводиться на самому комп'ютері, що вже підключений в мережу, у вікні зміни імені комп'ютера чи домену. За замовчуванням вибрано, що комп'ютер є учасником робочої групи. Нам потрібно, щоб комп'ютер був учасником не групи, а домену, тому переставляємо галочку. Тепер маємо можливість ввести ім'я домену і після підтвердження, буде запропоновано ввести ім'я.

Це все буде робити системний адміністратор при підключенні комп'ютера в мережу за допомогою свого облікового запису, але в нашому випадку підійшов і запис користувача.

		Хімчук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		67

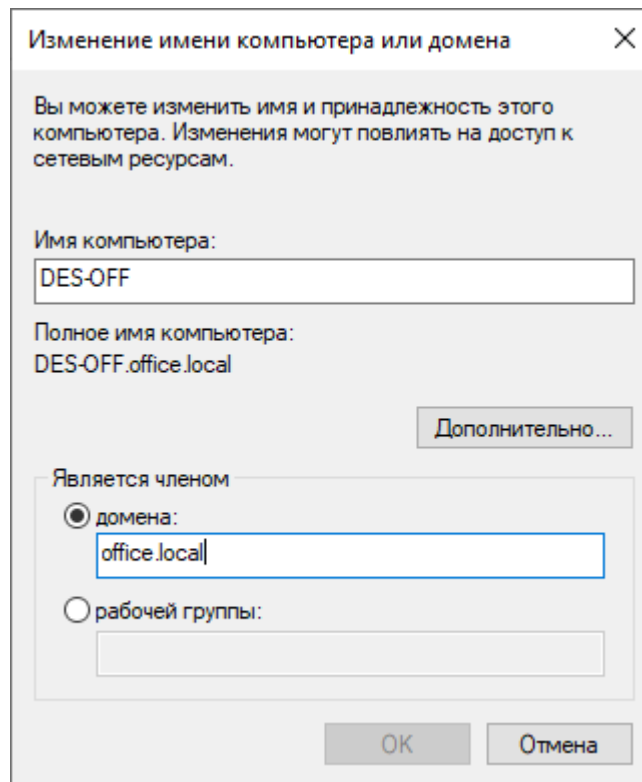


Рисунок 3.67 – Додавання комп'ютера в домен

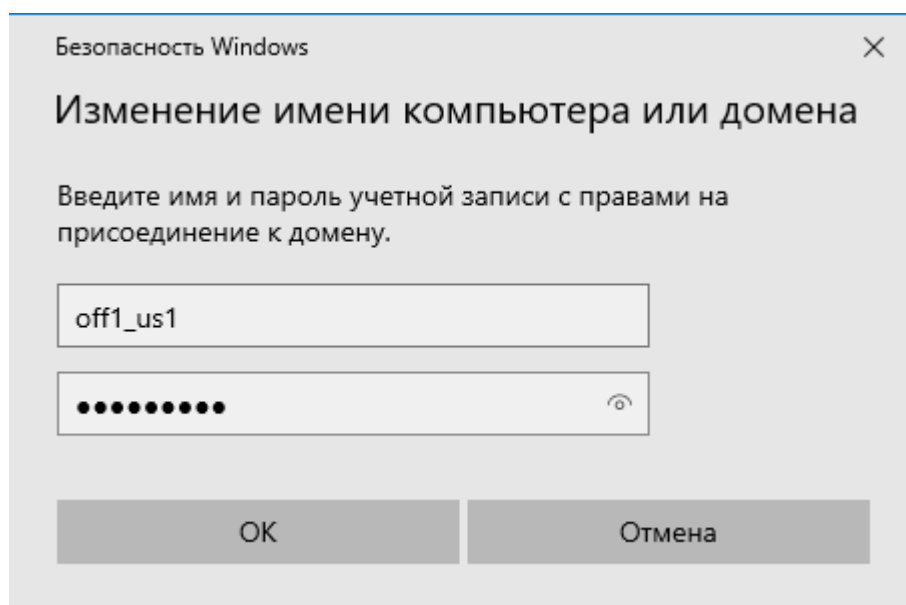


Рисунок 3.68 – Введення даних запису з правами на підключення

Додавання було успішним, і тепер нам запропоновано увійти під обліковим записом користувача домену.

Виконуємо вхід під записом off1_us2.

Так як при створенні запису була поставлена галочка на зміну паролю при першому вході, працівник має ввести пароль, отриманий ним від адміністратора та свій новий унікальний пароль з його повторним підтвердженням.

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		68

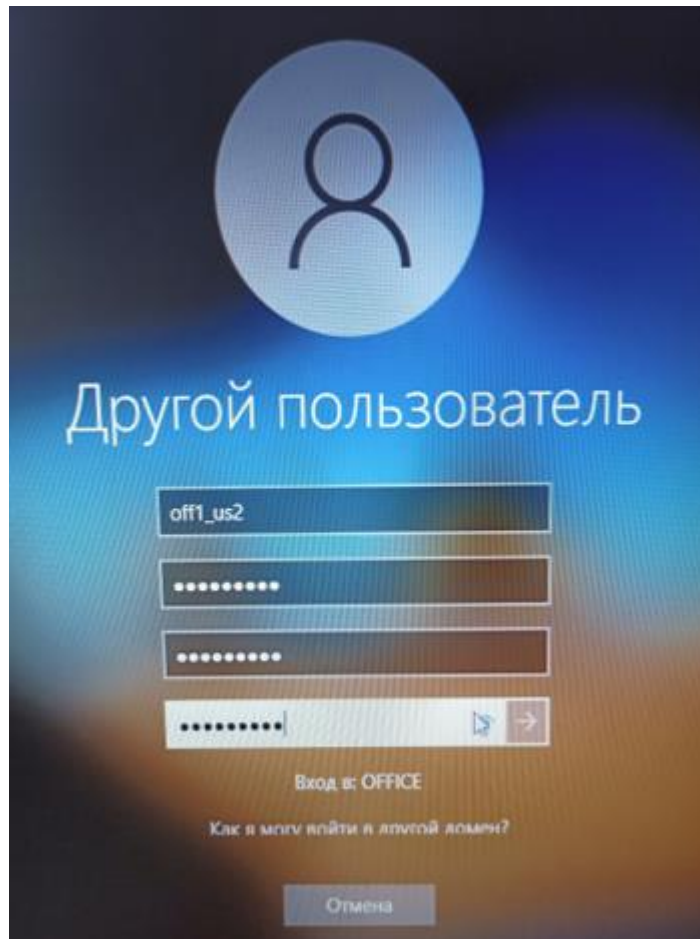


Рисунок 3.69 – Зміна паролю при першому вході

Після виконання вище перерахованих дій показується повідомлення про успішну зміну паролю і починається вхід в систему під обліковим записом.

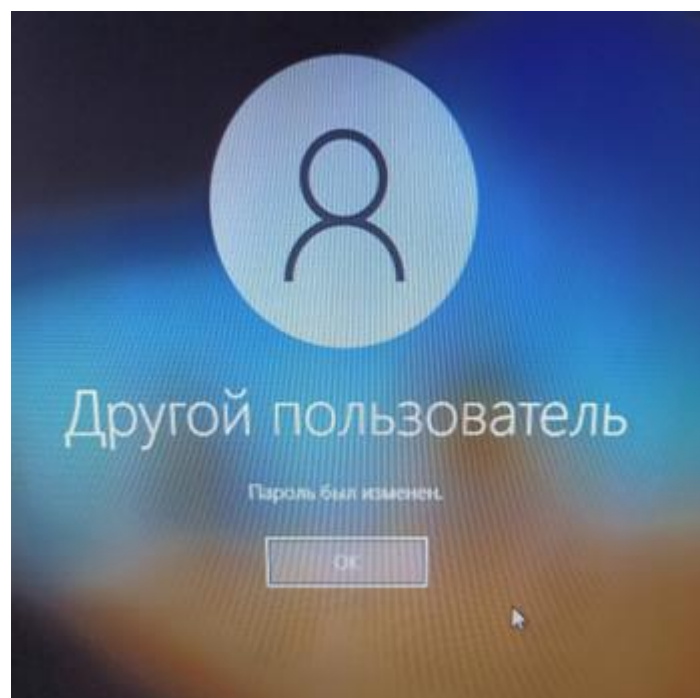


Рисунок 3.70 – Повідомлення про успішну зміну паролю

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				69
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 3.71 – Вхід в систему під обліковим записом off1_us2

Додамо ще один комп'ютер та зайдемо на ньому в обліковий запис off3_us3. Для нього виконуються аналогічні з off1_us2 дії.

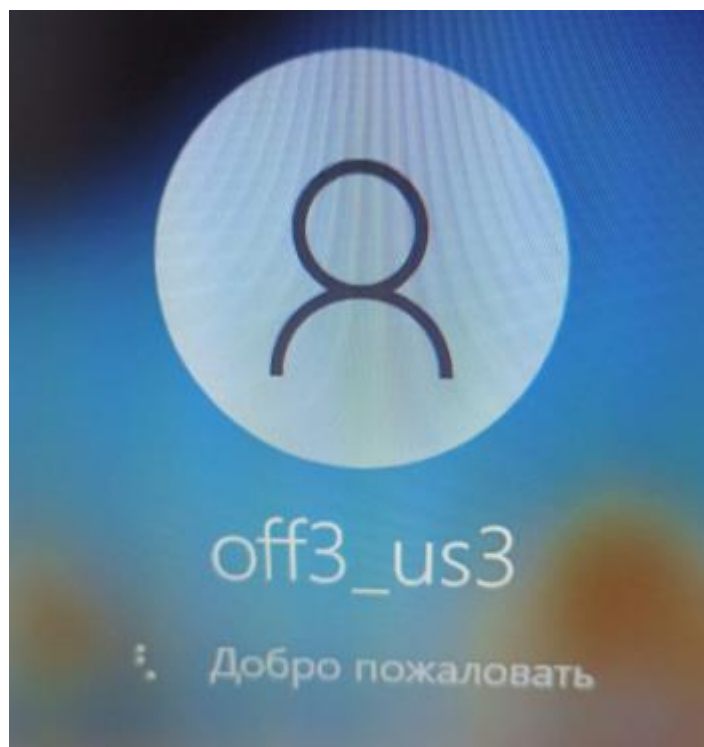


Рисунок 3.72 – Вхід в систему під обліковим записом off3_us3

Коли користувачами було здійснено вхід, підключені в домен комп'ютери, відображаються в Active Directory в об'єкті комп'ютери. Бачимо, що підключено два компютера. З назви розуміємо, що перший ком'пютер належить до першого офісу, а другий до третього.

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				70
Змн.	Арк.	№ докум.	Підпис	Дата		

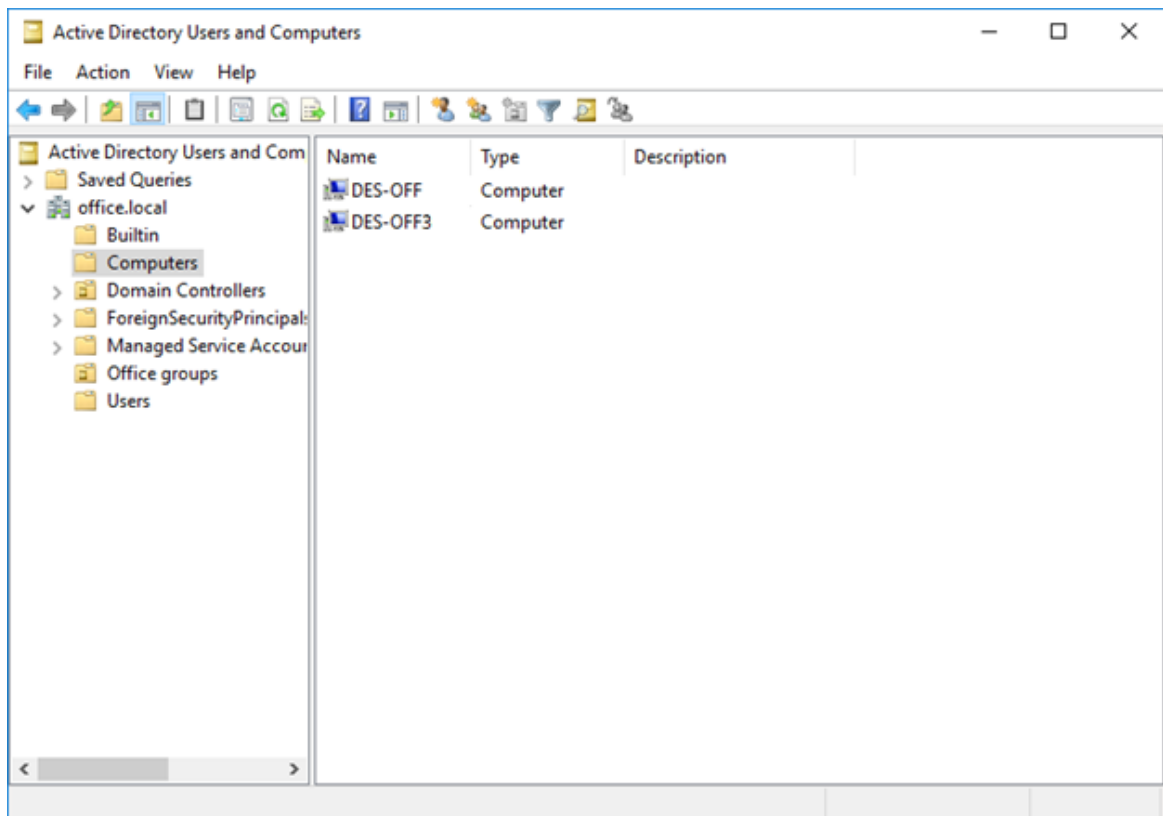


Рисунок 3.73 – Підключені в домен комп'ютери

Далі було проведено спробу увійти, використовуючи невірний пароль. Як бачимо, без особистого паролю нічого не вийде і після третьої спроби обліковий запис блокується.



Рисунок 3.74 – Реакція на використання невірного паролю

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				71
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 3.75 – Блокування облікового запису

Ось як ці події бачить адміністратор. У властивостях облікового запису з'явилося повідомлення про те, що він заблокований.

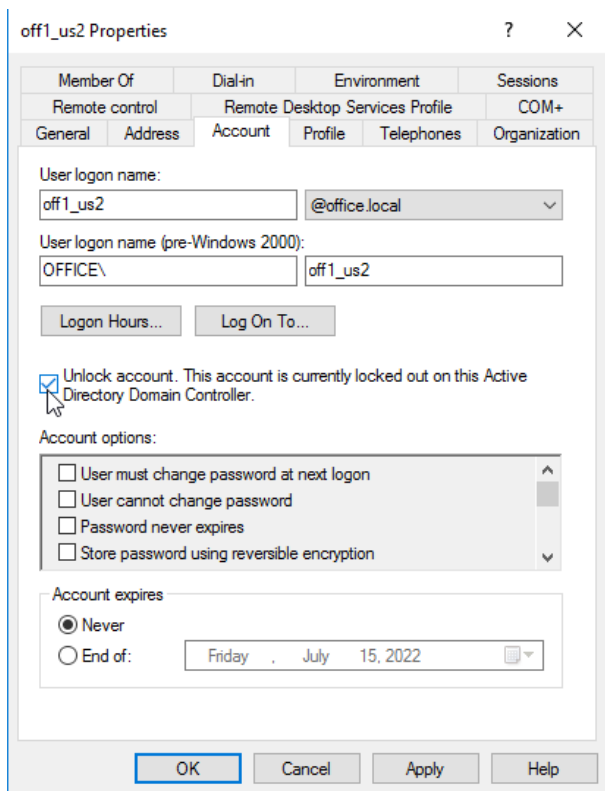


Рисунок 3.76 – Повідомлення про заблокування облікового запису

		Хімічук І.С.		
		Байлюк Є.М.		
Змн.	Арк.	№ докум.	Підпис	Дата

КІК.КР.Б – 125 – 24 – ПЗ

Арк.

72

Тепер при першому вході в обліковий запис користувача off2_us1 спробуємо при зміні паролю ввести менший за сім символів, що не відповідає парольній політиці, налаштованій раніше.

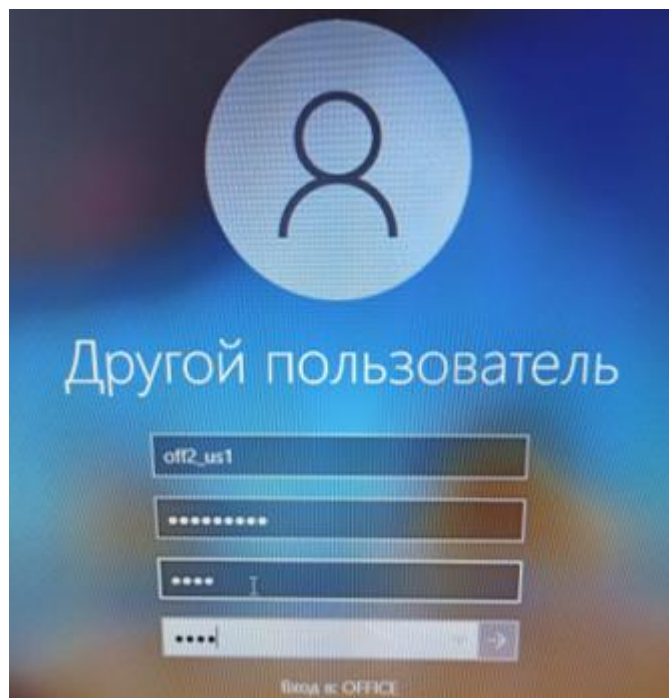


Рисунок 3.77 – Зміна паролю при першому вході

Отримуємо повідомлення про те, що пароль не може бути змінений, тому що не відповідає політиці безпеки домену.

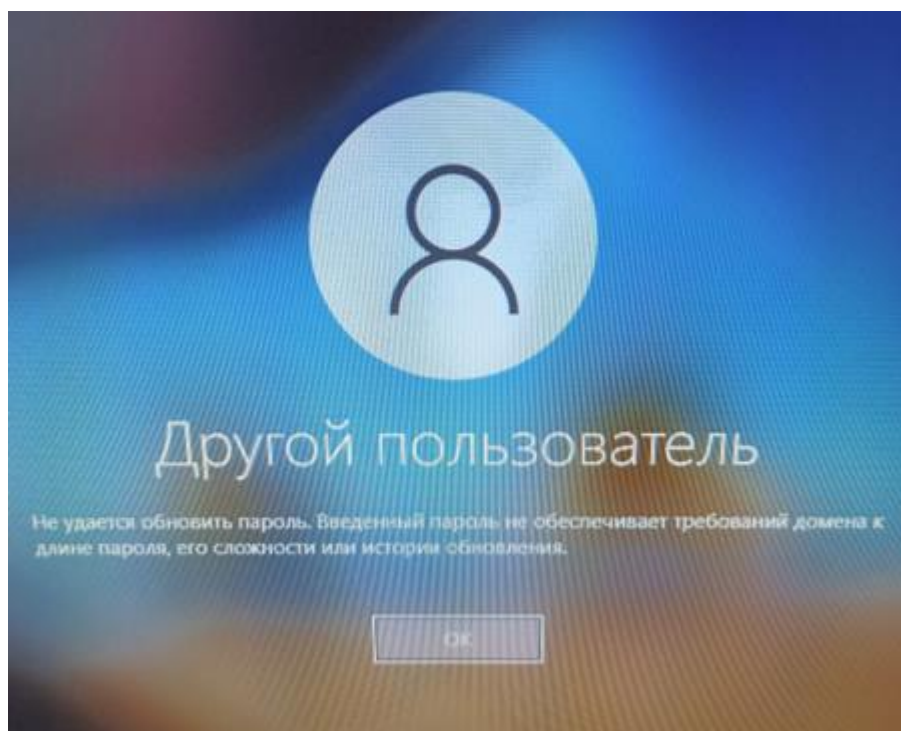


Рисунок 3.78 – Помилка зміни паролю

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				73
Змн.	Арк.	№ докум.	Підпис	Дата		

Також можна перевірити, що відбудеться при вході в систему під неіснуючим користувачем.

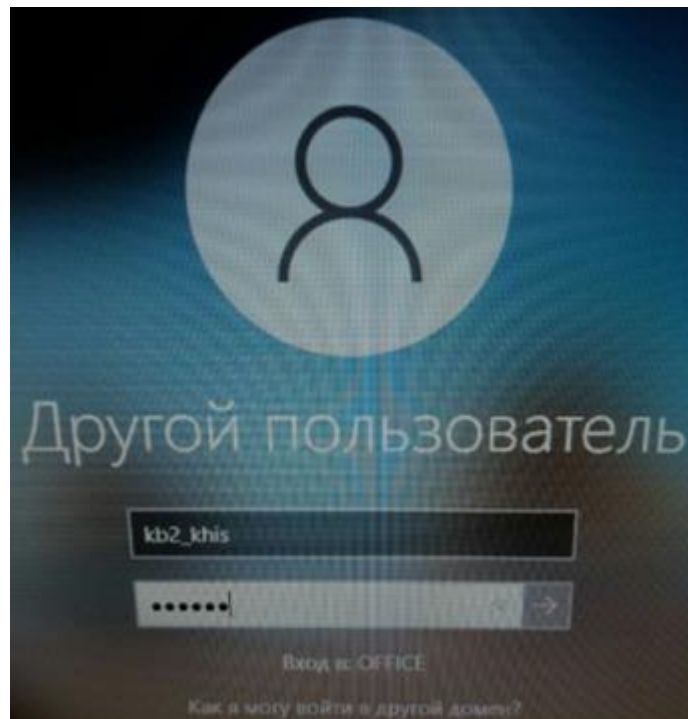


Рисунок 3.79 – Вхід під неіснуючим користувачем

Вхід невдалий, а користувач отримує попередження про неможливість входу з використанням цих облікових даних. Також система припускає, що цей обліковий запис може відноситися до іншого домену. Пропонується перевірити підключення комп'ютера до мережі організації та повторити спробу.

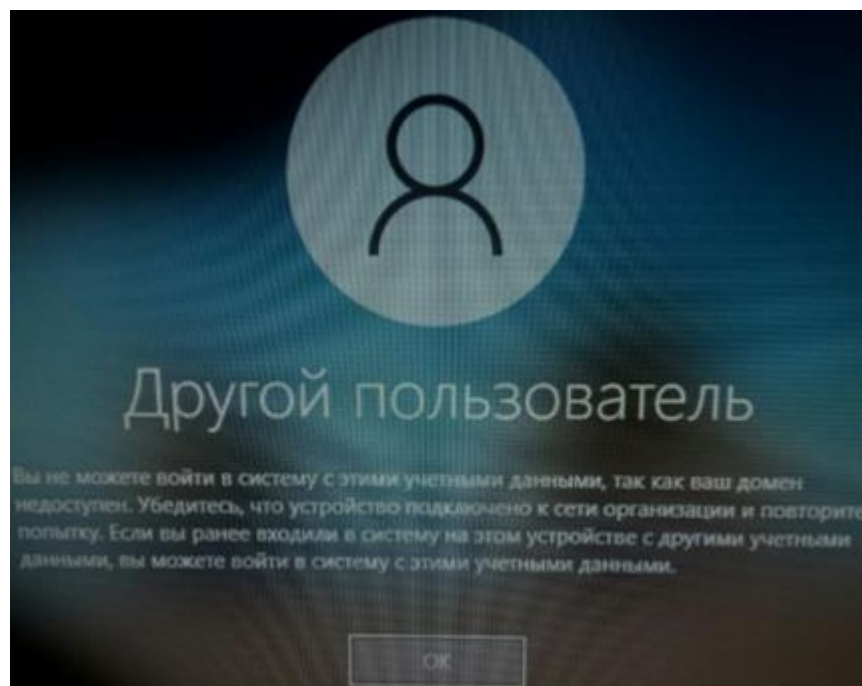


Рисунок 3.80 – Помилка входу в систему

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				74
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

У даній кваліфікаційній роботі розроблено проєкт підсистеми захисту клієнт–серверної мережі організації на базі ОС Windows.

У першому розділі було обґрунтовано необхідність захисту клієнт–серверної мережі організації. Розглянуті роль безпеки інформаційно–комунікаційних систем, можливі загрози та методи захисту мережі організації.

У другому розділі було приділено багато часу проєктуванню підсистеми захисту клієнт серверної мережі. Було обрано потрібні мережеві пристрої та з їх використанням розроблено проєкт мережі. На розроблений проєкт мережі було складено модель загроз відповідно всім нормам. Також було розроблено проєкт підсистеми захисту клієнт–серверної мережі та розроблено політику безпеки цієї мережі.

У третьому розділі було проведено налаштування пристроїв раніше розробленої мережі та підключено до неї сервер на базі Windows Server 2019. Після цього проведено налаштування й автоматизацію розгортання Active Directory на сервері, створено облікові записи працівникам. По завершенню налаштувань пристроїв мережі та сервера було реалізовано підсистему захисту мережі шляхом налагодження на мережевих пристроях захисту від атак зловмисників та налаштуванням різних політик в Active Directory.

Розроблений проєкт був реалізований в середовищі емуляції GNS3 та потім перевірений на реальному обладнанні. Даний проєкт можна використовувати для створення малих організацій на базі ОС Windows, а зважаючи на гнучкі налаштування пристроїв Cisco та Active Directory, мережу завжди можна буде розширювати за потреби.

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				75
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Інформаційна безпека інформаційно комунікаційних систем [Електронний ресурс] / Режим доступу до ресурсу: https://dut.edu.ua/uploads/l_488_73227512.pdf
2. Безпека інформаційних систем [Електронний ресурс] – Режим доступу до ресурсу: https://pidru4niki.com/74227/informatika/bezpeka_informatsiynih_sistem
3. Основи захисту інформації в мережах [Електронний ресурс] / studfile.net, Гончарова – Режим доступу до ресурсу: <https://studfile.net/preview/9649827/page:9>
4. Інформаційна безпека [Електронний ресурс] – Режим доступу до ресурсу: https://ua-referat.com/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0
5. Безпека мережі [Електронний ресурс] – Режим доступу до ресурсу: <https://www.eset.com/ua/support/information/entsiklopediya-ugroz/bezopasnost-seti/>
6. Мережеві комутатори Cisco [Електронний ресурс] – Режим доступу до ресурсу: <https://hi-news.pp.ua/tehnka-tehnologiyi/3554-merezhev-komutatori-cisco-harakteristiki-parametri-vguki.html>
7. Інформаційна безпека. Загрози при роботі в Інтернеті і їх уникнення [Електронний ресурс] – Режим доступу до ресурсу: <https://miyklas.com.ua/p/informatika/10-klas/informatciini-tehnologiyi-v-suspilstvi-322205/informatciina-bezpeka-navchannia-v-interneti-321523/re-0cf3c5d6-6a11-458b-b39d-889f102e9e71>
8. Технології захисту інформації [Електронний ресурс] – Режим доступу до ресурсу: <https://www.uzhnu.edu.ua/uk/infocentre/get/4186>
9. Поняття про інформаційну безпеку [Електронний ресурс] – Режим доступу до ресурсу: <https://studfile.net/preview/3740811/page:2/>
10. СУТНІСТЬ ІНФОРМАЦІЇ ТА РОЛЬ ІНФОРМАЦІЙНОЇ СИСТЕМИ В УПРАВЛІННІ ДІЯЛЬНОСТІ ОРГАНІЗАЦІЇ [Електронний ресурс] – Режим

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				76
Змн.	Арк.	№ докум.	Підпис	Дата		

доступу

до

ресурсу:

[https://pidru4niki.com/74216/informatika/informatsiyni sistemi i tehnologiyi v upravlinni organizatsiyeyu](https://pidru4niki.com/74216/informatika/informatsiyni_sistemi_i_tehnologiyi_v_upravlinni_organizatsiyeyu)

11. Мережеві служби, клієнти, сервери, ресурси. Захист при роботі у мережі [Електронний ресурс] – Режим доступу до ресурсу: <https://sites.google.com/site/kmposibnyk/lekciitema-no9>

12. ПРИНЦИПИ ТА ПОРЯДОК РОЗРОБКИ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ [Електронний ресурс] – Режим доступу до ресурсу: <https://openarchive.nure.ua/bitstream/document/861/1/460-469.pdf>

13. Модель загроз для інформації в ітс: мета та завдання [Електронний ресурс] – Режим доступу до ресурсу: <https://studfile.net/preview/9650054/page:7/>

14. ПОБУДОВА УЗАГАЛЬНЕНОЇ МОДЕЛІ ЗАГРОЗ ДЛЯ СИСТЕМ ІНТЕРНЕТ-БАНКІНГУ [Електронний ресурс] – Режим доступу до ресурсу: <https://ofp.cibs.ubs.edu.ua/files/1403/14vmmpum.pdf>

15. Розробка політики інформаційної безпеки [Електронний ресурс] – Режим доступу до ресурсу: <http://referatss.com.ua/work/rozrobka-politiki-informacijnoi-bezpeki-2/>

16. Configuring Rapid-PVST+ [Електронний ресурс] – Режим доступу до ресурсу: <https://www.freecnaworkbook.com/workbooks/ccna/configuring-rapid-per-vlan-spanning-tree-protocol>

17. VLAN hopping [Електронний ресурс] – Режим доступу до ресурсу: <https://sites.google.com/site/theocsic/technologies/securitynet/vlan-hopping>

18. 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%BD%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->

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				77
Змн.	Арк.	№ докум.	Підпис	Дата		

[%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80%D1%96%D0%B2-9893d8048229](https://active-directorypro.com/how-to-create-a-new-active-directory-user-account/)

19. New Active Directory User Account [Електронний ресурс] – Режим доступу до ресурсу: <https://active-directorypro.com/how-to-create-a-new-active-directory-user-account/>

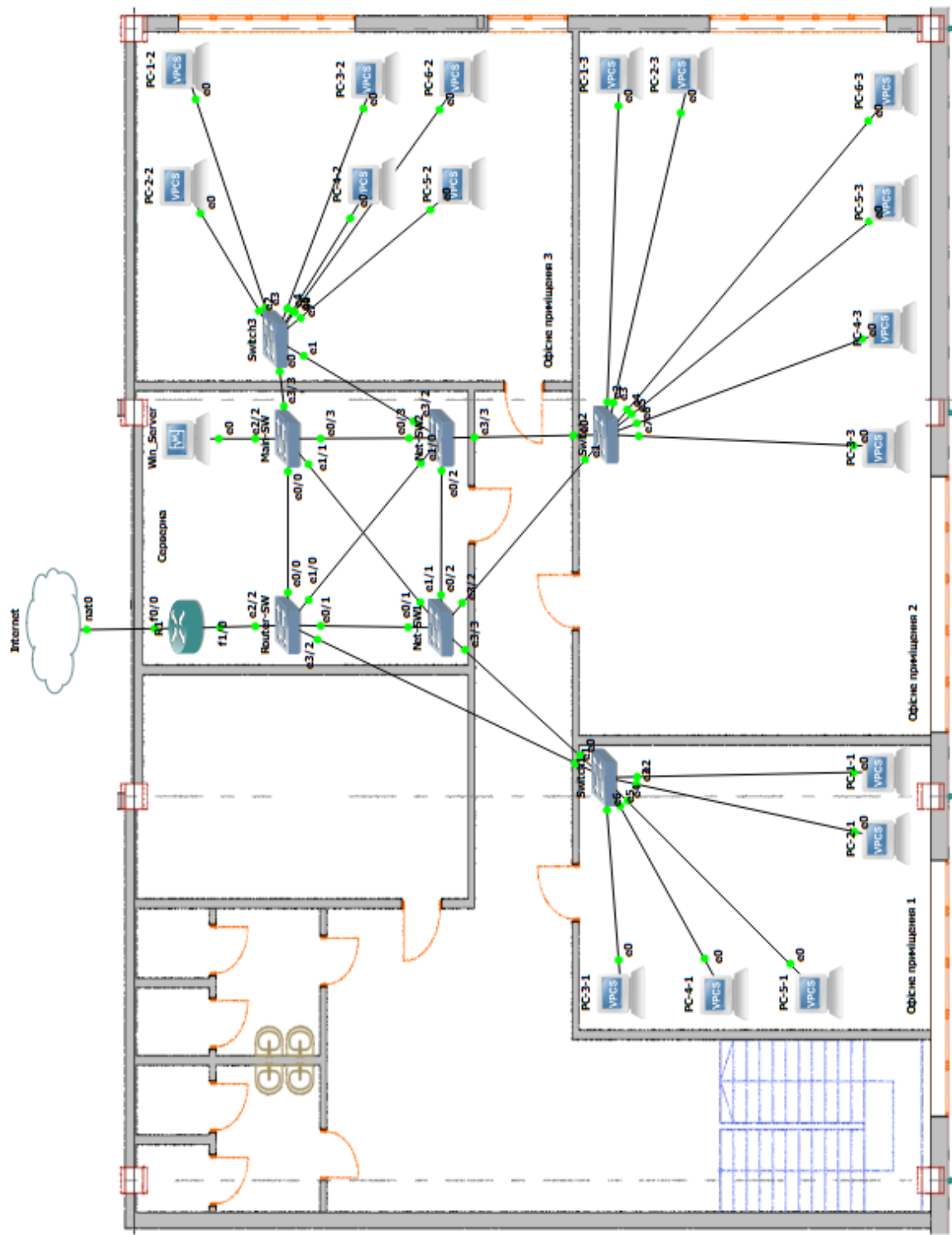
20. AD DS Installation and Removal Wizard Page Descriptions [Електронний ресурс] – Режим доступу до ресурсу: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/ad-ds-installation-and-removal-wizard-page-descriptions#BKMK_DepConfigPage

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				78
Змн.	Арк.	№ докум.	Підпис	Дата		

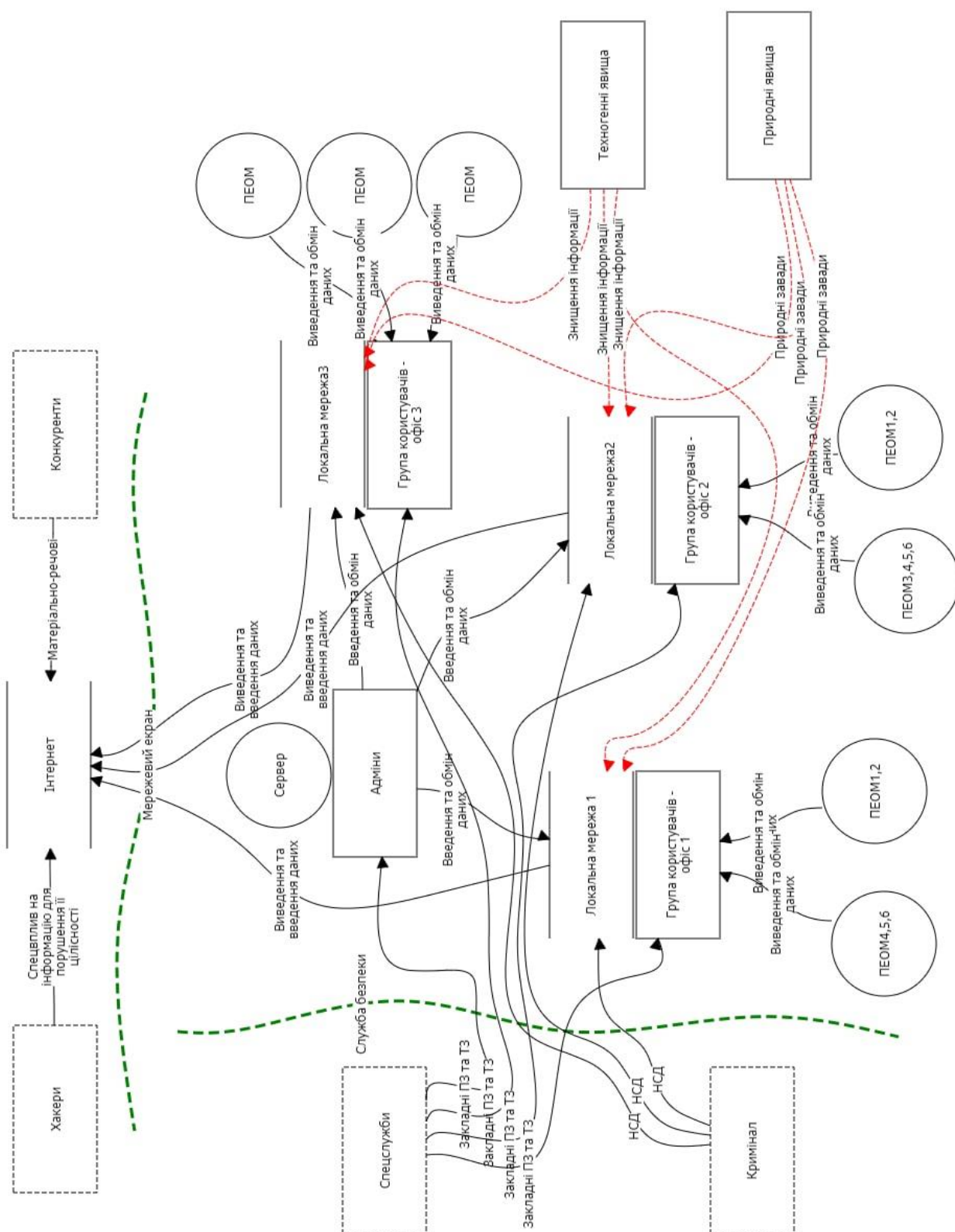
ДОДАТКИ

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				79
Змн.	Арк.	№ докум.	Підпис	Дата		

Проект мережі організації



Модель загроз організації



Лістинг конфігурацій всіх пристроїв мережі

```

R1#show run
Building configuration...

Current configuration : 2951 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
enable secret 5
$1$3u/B$rhCirvioOTeqV/lrUPBjZ0
!
no aaa new-model
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
!
ip dhcp excluded-address 192.168.10.254
ip dhcp excluded-address 192.168.20.254
ip dhcp excluded-address 192.168.30.254
ip dhcp excluded-address 192.168.100.6
ip dhcp excluded-address 192.168.50.14
!
ip dhcp pool WORKER-1
 network 192.168.10.0 255.255.255.0
 domain-name office.local
 dns-server 192.168.100.6
 default-router 192.168.10.254
!
ip dhcp pool WORKER-2
 network 192.168.20.0 255.255.255.0
 domain-name office.local
 default-router 192.168.20.254
 dns-server 192.168.100.6
!
ip dhcp pool WORKER-3
 network 192.168.30.0 255.255.255.0
 domain-name office.local
 default-router 192.168.30.254
 dns-server 192.168.100.6
!
!
no ip domain lookup
ip domain name office.local
no ipv6 cef
!
multilink bundle-name authenticated
!
!
username admin privilege 15 secret 5
$1$YJOS$j2Obzdx/CWd/3cjp12qu9.
archive
 log config
  hidekeys
!
!
!
ip tcp synwait-time 5
!
!
!
interface FastEthernet0/0
 ip address dhcp
 ip nat outside
 ip virtual-reassembly
 duplex half
!
interface FastEthernet1/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet1/0.10
 description SUBNET-WORKER-1
 encapsulation dot1Q 10
 ip address 192.168.10.254 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
interface FastEthernet1/0.20
 description SUBNET-WORKER-2
 encapsulation dot1Q 20
 ip address 192.168.20.254 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
interface FastEthernet1/0.30
 description SUBNET-WORKER-3
 encapsulation dot1Q 30
 ip address 192.168.30.254 255.255.255.0

```

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				82
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip nat inside
ip virtual-reassembly
!
interface FastEthernet1/0.50
description SUBNET-MGMT
encapsulation dot1Q 50
ip address 192.168.50.14 255.255.255.240
!
interface FastEthernet1/0.100
description SERV-AD-SUBNET
encapsulation dot1Q 100
ip address 192.168.100.6 255.255.255.248
ip nat inside
ip virtual-reassembly
!
interface FastEthernet1/1
no ip address
shutdown
duplex auto
speed auto
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip nat inside source list 1 interface
FastEthernet0/0 overload
!
access-list 1 permit 192.168.100.0 0.0.0.7
access-list 1 permit 192.168.10.0 0.0.0.255
access-list 1 permit 192.168.20.0 0.0.0.255
access-list 1 permit 192.168.30.0 0.0.0.255
no cdp log mismatch duplex
!
!
!
control-plane
!
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0

```

```

privilege level 15
logging synchronous
stopbits 1
line vty 0 4
exec-timeout 60 0
login
transport input ssh
transport output ssh
!
end

Router-SW#show run
Building configuration...

Current configuration : 2383 bytes
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname Router-SW
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops
6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
no aaa new-model
no ipv6 cef
ipv6 multicast rpf use-bgp
no ip icmp rate-limit unreachable
!
no ip domain-lookup
ip cef
!
!
ip dhcp snooping vlan 10,20,30,50,100
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
vlan internal allocation policy ascending
!

```

		Хімічук І.С.			KIK.KP.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip tcp synwait-time 5
!
!
!
interface Ethernet0/0
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 10,20,30,50,100
switchport mode trunk
duplex auto
!
interface Ethernet0/1
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 10,20,30,50,100
switchport mode trunk
duplex auto
!
interface Ethernet0/2
shutdown
duplex auto
!
interface Ethernet0/3
shutdown
duplex auto
!
interface Ethernet1/0
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 10,20,30,50,100
switchport mode trunk
duplex auto
!
interface Ethernet1/1
shutdown
duplex auto
!
interface Ethernet1/2
shutdown
duplex auto
!
interface Ethernet1/3
shutdown
duplex auto
!
interface Ethernet2/0
shutdown
duplex auto
!
interface Ethernet2/1
shutdown
duplex auto
!
interface Ethernet2/2
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 10,20,30,50,100
switchport mode trunk
duplex auto
!
interface Ethernet2/3
shutdown
duplex auto
!
interface Ethernet3/0
shutdown
duplex auto
!
interface Ethernet3/1
shutdown
duplex auto
!
interface Ethernet3/2
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 10,20,30,50,100
switchport mode trunk
duplex auto
!
interface Ethernet3/3
shutdown
duplex auto
!
interface Vlan1
no ip address
shutdown
!
interface Vlan50
ip address 192.168.50.2 255.255.255.240
!
!
no ip http server
!
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0

```

		Хімічук І.С.			KIK.KP.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				6
Змн.	Арк.	№ докум.	Підпис	Дата		

```

privilege level 15
logging synchronous
line vty 0 4
login
!
end

Main-SW#show run
Building configuration...

Current configuration : 2383 bytes
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname Main-SW
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops
6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
no aaa new-model
no ipv6 cef
ipv6 multicast rpf use-bgp
no ip icmp rate-limit unreachable
!
no ip domain-lookup
ip cef
!
!
ip dhcp snooping vlan 10,20,30,50,100
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
!
!

```

```

interface Ethernet0/0
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 10,20,30,50,100
switchport mode trunk
duplex auto
!
interface Ethernet0/1
shutdown
duplex auto
!
interface Ethernet0/2
shutdown
duplex auto
!
interface Ethernet0/3
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 10,20,30,50,100
switchport mode trunk
duplex auto
!
interface Ethernet1/0
shutdown
duplex auto
!
interface Ethernet1/1
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 10,20,30,50,100
switchport mode trunk
duplex auto
!
interface Ethernet1/2
shutdown
duplex auto
!
interface Ethernet1/3
shutdown
duplex auto
!
interface Ethernet2/0
shutdown
duplex auto
!
interface Ethernet2/1
shutdown
duplex auto
!
interface Ethernet2/2
switchport trunk encapsulation dot1q
switchport trunk native vlan 999

```

		Хімічук І.С.			KIK.KP.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

```

switchport trunk allowed vlan 10,20,30,50,100
switchport mode trunk
duplex auto
!
interface Ethernet2/3
shutdown
duplex auto
!
interface Ethernet3/0
shutdown
duplex auto
!
interface Ethernet3/1
shutdown
duplex auto
!
interface Ethernet3/2
shutdown
duplex auto
!
interface Ethernet3/3
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 10,20,30,50,100
switchport mode trunk
duplex auto
!
interface Vlan1
no ip address
shutdown
!
interface Vlan50
ip address 192.168.50.2 255.255.255.240
!
!
no ip http server
!
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login

```

```

!
end

Net-SW1#show run
Building configuration...

Current configuration : 2383 bytes
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname Net-SW1
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops
6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
no aaa new-model
no ipv6 cef
ipv6 multicast rp use-bgp
no ip icmp rate-limit unreachable
!
no ip domain-lookup
ip cef
!
!
ip dhcp snooping vlan 10,20,30,50,100
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
!
!
interface Ethernet0/0
shutdown
duplex auto
!

```

		Хімічук І.С.			KIK.KP.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface Ethernet0/1
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 10,20,30,50,100
switchport mode trunk
duplex auto
!
interface Ethernet0/2
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 10,20,30,50,100
switchport mode trunk
duplex auto
!
interface Ethernet0/3
shutdown
duplex auto
!
interface Ethernet1/0
shutdown
duplex auto
!
interface Ethernet1/1
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 10,20,30,50,100
switchport mode trunk
duplex auto
!
interface Ethernet1/2
shutdown
duplex auto
!
interface Ethernet1/3
shutdown
duplex auto
!
interface Ethernet2/0
shutdown
duplex auto
!
interface Ethernet2/1
shutdown
duplex auto
!
interface Ethernet2/2
shutdown
duplex auto
!
interface Ethernet2/3
shutdown
duplex auto
!
interface Ethernet3/0
shutdown
duplex auto
!
interface Ethernet3/1
shutdown
duplex auto
!
interface Ethernet3/2
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 10,20,30,50,100
switchport mode trunk
duplex auto
!
interface Ethernet3/3
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 10,20,30,50,100
switchport mode trunk
duplex auto
!
interface Vlan1
no ip address
shutdown
!
interface Vlan50
ip address 192.168.50.2 255.255.255.240
!
!
no ip http server
!
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
end

Net-SW2#show run

```

		Хімічук І.С.			KIK.KP.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

Building configuration...

Current configuration : 2383 bytes

```
!  
version 15.1  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
service compress-config  
!  
hostname Net-SW2  
!  
boot-start-marker  
boot-end-marker  
!  
!  
logging discriminator EXCESS severity drops  
6 msg-body drops EXCESSCOLL  
logging buffered 50000  
logging console discriminator EXCESS  
!  
no aaa new-model  
no ipv6 cef  
ipv6 multicast rpf use-bgp  
no ip icmp rate-limit unreachable  
!  
no ip domain-lookup  
ip cef  
!  
!  
ip dhcp snooping vlan 10,20,30,50,100  
!  
!  
spanning-tree mode pvst  
spanning-tree extend system-id  
!  
!  
!  
vlan internal allocation policy ascending  
!  
ip tcp synwait-time 5  
!  
!  
!  
interface Ethernet0/0  
shutdown  
duplex auto  
!  
interface Ethernet0/1  
shutdown  
duplex auto  
!
```

```
interface Ethernet0/2  
switchport trunk encapsulation dot1q  
switchport trunk native vlan 999  
switchport trunk allowed vlan 10,20,30,50,100  
switchport mode trunk  
duplex auto  
!  
interface Ethernet0/3  
switchport trunk encapsulation dot1q  
switchport trunk native vlan 999  
switchport trunk allowed vlan 10,20,30,50,100  
switchport mode trunk  
duplex auto  
!  
interface Ethernet1/0  
switchport trunk encapsulation dot1q  
switchport trunk native vlan 999  
switchport trunk allowed vlan 10,20,30,50,100  
switchport mode trunk  
duplex auto  
!  
interface Ethernet1/1  
shutdown  
duplex auto  
!  
interface Ethernet1/2  
shutdown  
duplex auto  
!  
interface Ethernet1/3  
shutdown  
duplex auto  
!  
interface Ethernet2/0  
shutdown  
duplex auto  
!  
interface Ethernet2/1  
shutdown  
duplex auto  
!  
interface Ethernet2/2  
shutdown  
duplex auto  
!  
interface Ethernet2/3  
shutdown  
duplex auto  
!  
interface Ethernet3/0  
shutdown  
duplex auto
```

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
interface Ethernet3/1
shutdown
duplex auto
!
interface Ethernet3/2
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 10,20,30,50,100
switchport mode trunk
duplex auto
!
interface Ethernet3/3
switchport trunk encapsulation dot1q
switchport trunk native vlan 999
switchport trunk allowed vlan 10,20,30,50,100
switchport mode trunk
duplex auto
!
interface Vlan1
no ip address
shutdown
!
interface Vlan50
ip address 192.168.50.2 255.255.255.240
!
!
no ip http server
!
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
end

```

		Хімічук І.С.			КІК.КР.Б – 125 – 24 – ПЗ	Арк.
		Байлюк Є.М.				11
Змн.	Арк.	№ докум.	Підпис	Дата		