

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

ПОЯСНЮВАЛЬНА ЗАПИСКА

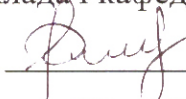
до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми інформаційної безпеки
офісного приміщення»

Виконала: студентка 4-го курсу групи КБ-21-2
спеціальності 125 «Кібербезпека»



Ярославна ПРИСЯЖНЮК

Керівник: старший викладач кафедри КІ та КБ



Єлизавета ТРОКОЗ

Рецензент: доцент кафедри КІ та КБ, кандидат технічних
наук



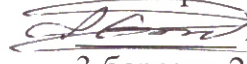
Олексій ШЕЛУХА

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Освітній рівень: бакалавр
Спеціальність 125 «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко
3 березня 2025 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студентка: Присяжнюк Ярославна Вікторівна

Тема роботи: «Проект підсистеми інформаційної безпеки офісного приміщення»

затверджена Наказом університету від 3 березня 2025 р. № 80/с

Термін здачі студентом закінченої роботи 18 червня 2025 р.

Вхідні дані до роботи: процеси забезпечення інформаційної безпеки організації, методи та засоби організації інформаційної безпеки організацій.

Обладнання та програмне забезпечення:

1. ОС Windows10 Education
2. Пакет прикладних програм Microsoft Office 2019
3. AutoCad 2019
4. GNS3 v2.2.42
5. OWASP Threat Dragon
6. Cisco Packet Tracer
7. Oracle VM VirtualBox 7.0.14

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

Розділ	Прізвище, ініціали та посади консультанта	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Трокоз Є.М.	30.03.2025	30.03.2025
2	Трокоз Є.М.	05.04.2025	05.04.2025
3	Трокоз Є.М.	18.05.2025	18.05.2025
4	Трокоз Є.М.	09.06.2025	09.06.2025

Студентка Ярославна ПРИСЯЖНЮК

Керівник проєкту Єлизавета ТРОКОЗ

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітки
1	Аналіз отриманого завдання та уточнення поставлених завдань	05.03.2025	Виконано
2	Аналіз літературних джерел	14.03.2025	Виконано
3	Аналіз об'єкта дослідження	27.03.2025	Виконано
4	Постановка задачі дослідження	01.04.2025	Виконано
5	Складання планів приміщення	03.04.2025	Виконано
6	Аналіз характеристик об'єкта	12.04.2025	Виконано
7	Розрахунок структурної моделі та параметрів адресації	18.04.2025	Виконано
8	Вибір технології для реалізації	21.04.2025	Виконано
9	Розробка захищеної КМ	29.04.2025	Виконано
10	Налаштування мережі	06.05.2025	Виконано
11	Адміністрування мережі	15.05.2025	Виконано
12	Перевірка працездатності	19.05.2025	Виконано
13	Оформлення пояснювальної записки	01.06.2025	Виконано
14	Оформлення презентації	12.06.2025	Виконано
15	Захист	18.06.2025	Виконано

Студентка Ярославна ПРИСЯЖНЮК

Керівник проєкту Єлизавета ТРОКОЗ

АНОТАЦІЯ

Завданням на кваліфікаційну роботу була розробка проєкту підсистеми інформаційної безпеки офісного приміщення.

Пояснювальна записка до кваліфікаційної роботи на тему «Проєкт підсистеми інформаційної безпеки офісного приміщення» складається зі вступу, чотирьох розділів, висновку, списку використаної літератури та додатку.

Текстова частина викладена на 90 сторінках друкованого тексту.

Пояснювальна записка має 3 додатки. Список використаних джерел містить 16 найменувань і займає 2 сторінки. В роботі наведено 122 рисунки. Загальний обсяг роботи – 135 сторінок.

У першому розділі розглянуто теоретичні відомості, які будуть використовуватися при розробці кваліфікаційного проєкту.

У другому розділі наведено результати обстеження фізичних та інформаційних ресурсів підприємства. Наведено характеристики об'єкта та його складових.

У третьому розділі наведено опис фізичної та логічної топології спроектованої мережі, розроблено таблицю IP-адресації, спроектовано служби та сервіс, описано передбачуваний захист мережі. Створено модель порушника та модель загроз, а також наведено вибір обладнання для побудови локальної мережі.

У четвертому розділі проведено налаштування та тестування роботи спроектованої локальної мережі організації. Налаштовано захист мережі.

Висновок містить в собі підсумки кваліфікаційної роботи.

Ключові слова: ЗАХИСТ ІНФОРМАЦІЇ, ІНФОРМАЦІЯ, БЕЗПЕКА, ОБ'ЄКТ, АНАЛІЗ, ЛОКАЛЬНА КОМП'ЮТЕРНА МЕРЕЖА, ЗАГРОЗА, ПІДСИСТЕМА, ПІДМЕРЕЖА, КОРИСТУВАЧ, ДОСТУП, SSH, IPV4.

					ККІКБ.КР.Б – 125 – 38 – ПЗ				
Змн.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми інформаційної безпеки офісного приміщення	Літ.	Арк.	Аркушів	
Розроб.		Присяжнюк Я.В.		16.06.25					
Керівник		Трокоз Є.М.		16.06.25			4	135	
Реценз.		Шелуха О.О.		16.06.25		ФІКТ, Гр. КБ-21-2			
Н. контр.		Трокоз Є.М.		16.06.25					
Затверд.		Єфіменко А.А.		16.06.25					

ANNOTATION

The task of the qualification work was the development of a project for the information security subsystem of an office premises.

The explanatory note to the qualification work titled "Project of the Information Security Subsystem of an Office Premises" consists of an introduction, four chapters, a conclusion, a list of references, and an appendix.

The textual part is presented on 90 pages of printed text. The explanatory note includes 3 appendices. The list of references contains 16 sources and occupies 2 pages. The work includes 122 figures. The total volume of the work is 135 pages.

The first chapter reviews the theoretical information that will be used in the development of the qualification project.

The second chapter presents the results of the survey of the physical and information resources of the enterprise. It provides the characteristics of the object and its components.

The third chapter provides a description of the physical and logical topology of the designed network, includes an IP addressing table, designs services and functionalities, and describes the intended network protection. A threat model and an intruder model are developed, and the selection of equipment for building the local network is provided.

The fourth chapter presents the configuration and testing of the designed local area network of the organization. This chapter also includes the results of the network's performance in case of attacks.

The conclusion summarizes the outcomes of the qualification work.

Keywords: INFORMATION PROTECTION, INFORMATION SECURITY, OBJECT, ANALISYS, LOCAL AREA NETWORK, THREAT, SUBSYSTEM, SUBNET, USER, ACCESS, SSH, IPv4.

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП	9
РОЗДІЛ 1. ОГЛЯД ПОНЯТТЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. ОСНОВНІ АСПЕКТИ	10
1.1 Інформація та її властивості	10
1.2 Захист інформації та його основні завдання.....	11
1.3 Рівні доступу до інформації	13
1.4 Кібератаки та їхні види	14
РОЗДІЛ 2. ОБСТЕЖЕННЯ ФІЗИЧНОГО СЕРЕДОВИЩА.....	16
2.1 Характеристика об'єкта	16
2.2 Характеристика складових об'єкта.....	17
2.3 Обстеження середовища користувачів та інформаційних потоків	20
2.4 Аналіз технологій обробки інформації в наявній системі	22
2.5 Інформація, що планується до обробки.....	23
2.6 Технології обробки інформації.	24
РОЗДІЛ 3. РОЗРОБКАМОДЕЛІ ПОРУШНИКА ТА МОДЕЛІ ЗАГРОЗ, ПРОЄКТУВАННЯ ТОПОЛОГІЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ	26
3.1 Розробка імовірного прогнозу та моделі порушника	26
3.2 Розробка імовірної моделі загроз.....	33
3.3 Основні аспекти менеджменту інформаційної безпеки, пов'язані з персоналом	37
3.4 Розробка топології мережі	40
3.5 Розробка схеми адресації мережі	43
3.6 Вибір обладнання та ОС пристроїв для розробленого проєкту мережі.....	44

РОЗДІЛ 4. ПОБУДОВА, НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ

СПРОЄКТОВАНОЇ ЛОКАЛЬНОЇ МЕРЕЖІ	48
4.1 Побудова та налагодження спроектованої локальної мережі	48
4.2 Тестування роботи побудованої локальної мережі	72
4.3 Налаштування та тестування захисту мережі	79
4.4 Додатковий захист мережі	85
ВИСНОВКИ	87
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	88
ДОДАТКИ	90

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

IP – Internet Protocol – інтернет протокол

IPv4 – Internet Protocol version 4

SSH – Secure Shell – протокол захищеного віддаленого доступу

OSPF – Open Shortest Path First – протокол маршрутизації

DHCP – Dynamic Host Configuration Protocol – протокол динамічної конфігурації вузла

STP – Spanning Tree Protocol

RPVST – Rapid Per-VLAN Spanning Tree

DNS – Domain Name System – система доменних імен

LAN – Local Area Network – мережа локального простору

WAN – Wide Area Network – мережа широкого простору

ПК – Персональний комп'ютер

ОС – Операційна система

ПЗ – Програмне забезпечення

IOS – Internetwork Operating System – міжмережева операційна система

АС – автоматизована система

ІТС – інформаційно-телекомунікаційна система

ПЕОМ – персональна електронно-обчислювальна машина

ОІД – об'єкт інформаційної діяльності

ІЗОД – із обмеженим доступом

		Присяжнюк Я.В.			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		8

ВСТУП

Інформаційні системи, побудовані на базі комп'ютерних мереж, забезпечують обробку даних; організацію доступу користувачів до даних; передачу результатів обробки даних користувачеві; використання додаткових додатків і ресурсів мережі.

Актуальність теми. Сучасні компанії генерують та обробляють значну кількість конфіденційної інформації: фінансові звіти, персональні дані співробітників, інформацію про клієнтів та партнерів. Захист цих даних є критично важливим для запобігання їх витоку або несанкціонованого доступу.

Таким чином, забезпечення інформаційної безпеки офісного приміщення є не лише питанням технологій, але й стратегічним підходом до управління ризиками, який впливає на довгострокову стабільність та успішність бізнесу.

Метою кваліфікаційного проєкту є розробка проєкту підсистеми інформаційної безпеки офісного приміщення.

Завданням на кваліфікаційний проєкт є:

- обстеження фізичного середовища об'єкта;
- обстеження середовища користувачів та інформаційних потоків;
- складання моделі порушника та моделі загроз;
- розробка структурної моделі комп'ютерної мережі;
- вибір сучасних технологій та комунікаційних пристроїв для реалізації мережі;
- розробка, налагодження мережі та налаштування захисту мережі.

Об'єктом дослідження випускної кваліфікаційної роботи є процеси забезпечення інформаційної безпеки організації.

Предметом дослідження є методи та засоби організації інформаційної безпеки організацій.

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1. ОГЛЯД ПОНЯТТЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. ОСНОВНІ АСПЕКТИ

1.1 Інформація та її властивості

Інформація – це відомості про щось незалежно від форми їх подання[3].

Сучасна наука розглядає два типи інформації:

- об’єктивна – властивості матеріальних об’єктів та явищ, які передаються іншим об’єктам та відображаються в їх структурі;
- суб’єктивна, яка відображає зміст об’єктивної інформації, сформована свідомістю людини за допомогою слів, образів і відчуттів та зафіксована будь-якому матеріальному носієві.

У побутовому розумінні, інформація – це відомості про оточуючий світ та процеси, що в ньому відбуваються, які сприймаються людиною або спеціальним пристроєм.

Інформація має певні властивості. Наприклад, з практичної точки зору, вони визначаються таким чином:

- цінність інформації – визначається можливістю забезпечення досягнення мети, поставленої їй отримувачем;
- достовірність – відповідність отриманої інформації реальності навколишнього світу;
- актуальність – відповідність цінності та достовірності отриманої інформації поточному часу

З точки зору захисту інформації нас цікавлять такі її властивості, які підлягають захисту. До них відноситься:

- конфіденційність – властивість інформації бути захищеною від несанкціонованого ознайомлення;
- цілісність – властивість інформації бути захищеною від несанкціонованої зміни або знищення;
- доступність – властивість інформації бути захищеною від несанкціонованого блокування.

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		10

Іноді ще визначають таку властивість інформації, як спостережність – властивість весь час (на усіх етапах обробки та передавання) знаходитись під контролем системи захисту.

1.2 Захист інформації та його основні завдання

Інформаційно-телекомунікаційною системою називають організаційно-технічну систему, що реалізує певну сукупність технологій обробки та передавання даних шляхом їх кодування у формі фізичних сигналів[3].

Комп'ютерна система, згідно з визначенням[16] – це сукупність програмно-апаратних засобів, яку подають на оцінювання. Під оцінюванням розуміють експертне оцінювання захищеності інформації в цих програмно-апаратних засобах. Таке оцінювання є складовою частиною експертизи на відповідність чинним нормативним документам та стандартам.

Під обчислювальною системою розуміють сукупність програмно-апаратних засобів, призначених для обробки інформації. Обчислювальна система поєднує технічні засоби обробки та передавання інформації, а також методи і алгоритми обробки даних, реалізовані у вигляді відповідного програмного забезпечення.

Автоматизована система – це організаційно-технічна система, що реалізує інформаційну технологію та поєднує в собі: обчислювальну систему, фізичне середовище, персонал та інформацію, що обробляється.

Основне правило захисту інформації: жодна система захисту не може довгий час протистояти цілеспрямованим діям озброєного сучасними технологіями кваліфікованого порушника.

Метою захисту інформації є унеможливлення або суттєве утруднення реалізації загроз для інформації, що є власністю держави, сприяння реалізації законних інтересів громадян, юридичних осіб, державних органів, здійсненню ними своїх завдань і функцій, загроз, реалізація яких може нанести державі, суспільству або особі політичні, економічні, моральні та інші збитки.

		Присяжнюк Я.В.			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

Виходячи з мети, можна сформулювати основні завдання захисту інформації[14]:

- захист інформації з обмеженим доступом від витоку;
- протидія технічним розвідкам;
- захист інформації з обмеженим доступом від несанкціонованих дій під час її обробки та зберігання;
- захист інформації від спеціальних впливів;
- захист цілісності та доступності відкритої інформації.
- керування доступом користувачів до інформаційних ресурсів з метою захисту від неправомірного випадкового або навмисного втручання у роботу системи і несанкціонованого (із перевищенням наданих повноважень) доступу до програмних і апаратних ресурсів із боку персоналу та/або сторонніх осіб;
- захист даних, що передаються каналами зв'язку;
- реєстрування, збереження і надання даних про події, що відбувалися у системі і мали відношення до безпеки;
- контроль роботи користувачів системи з боку адміністраторів, обов'язкове повідомлення адміністратора безпеки про спроби несанкціонованого доступу до ресурсів системи;
- контроль і підтримка цілісності критичних ресурсів системи захисту і середовища виконання прикладних програм;
- забезпечення замкненості програмного середовища із метою захисту від безконтрольного впровадження у систему потенційно небезпечних програм і засобів подолання системи захисту;
- керування засобами захисту.

Основні засоби протидії загрозам безпеки в комп'ютерних системах поділяються на: правові (законодавчі), морально-етичні, організаційні(адміністративні), фізичні, технічні.

До правових засобів захисту відноситься законодавчо-права база, на якій ґрунтуються інші засоби. Зокрема, в Україні це закони "Про інформацію",

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

"Про технічний захист інформації", "Про державну таємницю", нормативні документи Державної служби спеціального зв'язку та захисту інформації, які регламентують правила обробки інформації.

До морально-етичних засобів протидії відноситься дотримання норм поведінки, що традиційно склались або складаються в інформаційному суспільстві країни та світу.

Організаційні (адміністративні) засоби захисту – це засоби організаційного характеру, що таким чином регламентують процес функціонування системи обробки даних, використання її ресурсів, діяльність персоналу, а також порядок взаємодії користувачів з системою, щоб унеможливити або максимально ускладнити здійснення загроз безпеки інформації.

Фізичні засоби захисту ґрунтуються на використанні різного роду механічних, електро- або електронно-механічних пристроїв, спеціально призначених для створення фізичних перешкод на можливих шляхах проникнення потенційних порушників, їх доступу до компонентів системи та інформації, що захищається, а також засоби візуального спостереження, зв'язку і охоронної сигналізації.

Технічні (апаратно-програмні) засоби захисту базуються на використанні різних електронних пристроїв і спеціального програмного забезпечення, що входять до складу автоматизованої системи і виконують, самостійно або в комплексі з іншими засобами, функції захисту інформації.

1.3 Рівні доступу до інформації

Аналіз властивостей[3], які потребують захисту, показує, що з цієї точки зору, є два види інформації:

- відкрита, тобто така, яка призначена для ознайомлення усіх бажаючих, наприклад, газети, журнали, телевізійне та радіомовлення, інформаційні сайти, реклама тощо;
- інформація з обмеженим доступом, тобто така, ознайомитися з якою можна лише з санкції її власників або розпорядників.

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

Згідно з Державним стандартом України, інформація з обмеженим доступом – це така інформація, права доступу до якої обмежено існуючими правилами та нормами.

Згідно із Законом України "Про державну таємницю", державною таємницею є вид інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України, та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою.

Ступінь секретності інформації – це категорія, яка характеризує важливість таємної (секретної) інформації, ступінь обмеження доступу до неї та рівень її охорони державою.

Законом передбачається чотири ступені секретності (в порядку зменшення секретності):

- особливої важливості (детальні дані перепису населення, стратегічні плани Генерального штабу Збройних сил України; стратегічні політичні плани уряду тощо);
- цілком таємно (детальні тактико-технічні дані передової військової техніки та технологія їх виробництва, плани розгортання військ; стратегічні плани парламентських партій та фракцій тощо);
- таємно (технологія виробництва військової техніки та її компонентів, стратегічні та тактичні плани військ та армійських підрозділів тощо);
- для службового користування (ДСК) (фінансова звітність підприємства, дані про заробітну платню його працівників, про структуру постачання, можуть бути також дані про збут).

1.4 Кібератаки та їхні види

Кібератака[3] — сукупність узгоджених щодо мети, змісту та часу дій або заходів — так званих кіберакцій, спрямованих на певний об'єкт впливу з метою

		Присяжнюк Я.В.			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

порушення конфіденційності, цілісності, доступності, спостережності і/або авторства інформації, що циркулює в ньому, з урахуванням її уразливості, а також порушення роботи ІТ-систем і мереж зазначеного об'єкта.

Більш детально розглянемо класифікацію кібератак:

- за метою впливу на об'єкт атаки(порушення цілісності (integrity) або конфіденційності (confidentiality) інформації, її захищеності від несанкціонованого доступу (authentication), а також на порушення живучості (survivability) системи та надійності (availability) її функціонування);
- за принципом впливу на об'єкт атаки(використання прихованих каналів; застосування прав суб'єкта системи до об'єкта);
- за характером впливу на об'єкт атаки(активні та пасивні);
- за способом впливу на об'єкт атаки, зокрема на систему дозволів (захоплення привілеїв), а також безпосередній доступ до даних, програм, служб, каналів зв'язку з використанням привілеїв.
- за засобами впливу на об'єкт атаки (використання або стандартного ПЗ, або спеціально розроблених програм);
- за об'єктом атаки(на систему в цілому; на дані і програми, що містяться на зовнішніх або внутрішніх пристроях системи, а також у каналах передавання даних; на процеси і підпроцеси системи за участю користувачів);
- за станом об'єкта(безпосередньо під час атаки інформація в ньому може зберігатися, передаватися або оброблятися);
- за використовуваною системою захисту; за кількістю атакувальників; за джерелами атак; за розміщенням атакуючого об'єкта відносно атакованого; за наявністю зв'язку з атакованим об'єктом; за рівнем еталонної моделі OSI об'єкта, на який здійснюється вплив.

Висновки до першого розділу

В даному розділі було детально розглянуто поняття інформації та її видів. Розкрито поняття захисту інформації та його основних завдань. Проаналізовано рівні доступу до інформації. Також розглянуто поняття про кібератаки та їхні види.

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		15

РОЗДІЛ 2. ОБСТЕЖЕННЯ ФІЗИЧНОГО СЕРЕДОВИЩА

2.1 Характеристика об'єкта

ІТС розміщена у 16 приміщеннях адміністративної будівлі, що знаходиться за адресою: м. Житомир, майдан Путятинський, буд.2. Об'єкт розташований в центрі міста, оточений з трьох сторін спорудами різного призначення і відомчої приналежності. Схема розташування будівлі наведена на рис.2.1.

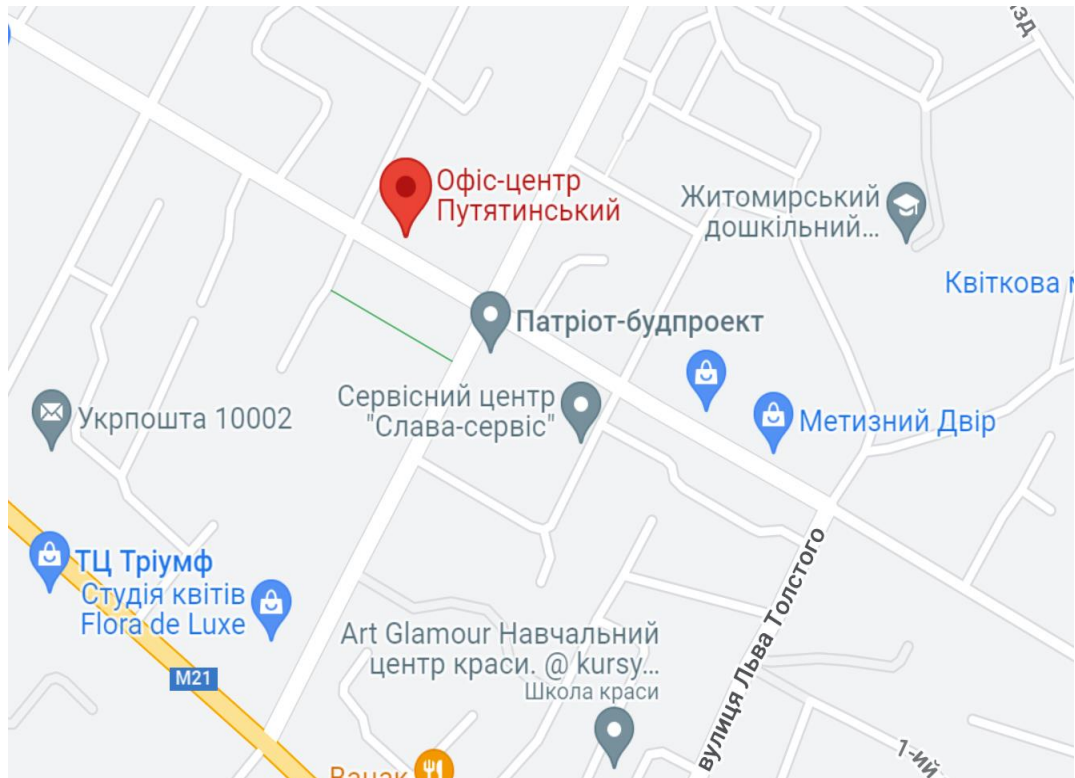


Рисунок 2.1 – Схема розташування будівлі

З боку вулиці розміщується сквер з зонами відпочинку на відстані 15м. Зліва від об'єкту розташована висотна адміністративна будівля, в якій розміщені різні державні підприємства. Праворуч від об'єкту на відстані 45–50 м розташований дев'ятиповерховий житловий будинок, нижні поверхи якого займають магазини та салон краси.

Прямо перед будівлею через парковку на відстані близько 100 м розташовано житлові будинки середньої поверховості.

		Присяжнюк Я.В.			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз С.М.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

2.2 Характеристика складових об'єкта

Нижче наведено детальний опис та характеристику фізичних складових об'єкта дослідження.

Висота стель (м): $h - 3$ м

- підвісний гіпсолітовий, зазор $h - 0,3$ м

Перекриття, товщина (мм) :

- залізобетонні перекриття;
- паркет: штучний паркет.

Стінні перегородки:

- глухі стаціонарні офісні перегородки в основі яких лежить алюмінієвий каркас;
- інші матеріали: двосторонній гіпсокартон на металевому каркасі.

Стіни зовнішні цегляні:

- товщина (см) – 90;
- фасад:вентильований, скло;
- цеглина: керам. порожниста;
- акустична штукатурка: наявна;
- інші матеріали: з внутрішньої сторони стіни оброблені гіпсокартоном.

Вікна:

- розмір отвору: 200x80 см;
- кількість отворів: 3;
- наявність плівок (призначення, тип, марка) відсутні;
- тип вікна (п`ятикамерний склопакет з енергозберігаючим склом.): товщина скла 70 мм;
- наявність захисних решіток : відсутні.

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

Двері:

- розмір отвору: 220x180 см;
- двері: 220x180 см двостулкові;
- тип: металеві з «холодним» профілем для внутрішніх дверей, та з «теплим» для зовнішніх.

Система електроживлення (освітлення):

- мережа: 220 В/50 Гц;
- автономний агрегат електроживлення: автономно-трансформаторна підстанція і дизель-генератор;
- наявність підстанції на контрольованій території: відсутній;
- тип світильників і їх кількість: люмінесцентна лампа (4 шт.)(36Вт) розміром (595 мм x 595 мм).

Система заземлення: є

Системи сигналізації (тип):

- пожежна (датчики задимлення) – 30 шт.;
- охоронна (акустичні детектори) - 8 шт.

Система вентиляції (тип): припливно-витяжна, отвір 365x500мм.

Система опалювання:

- центральне : будинкова котельня;
- наявність екранів на батареях: декоративне укриття.

Електрика:

- тип розеток: (євророзетка);
- тип проводки – двопровідні лінії.

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		18

Інші дротяні (провід) лінії:

- радіотрансляція (місцева, міська): відсутній;
- Оргтехніка: ПЕОМ в повній конфігурації – 1 шт на кожне робоче місце;
- Спеціальні технічні засоби захисту інформації: відсутні.

Схема розміщення ІТС представлена на рис.2.2, допоміжних технічних засобів: ліній електроживлення ОІД, системи охоронної та пожежної сигналізації ОІД наведена на рис.2.3. Ситуаційний план приміщення представлений на рис.2.4.

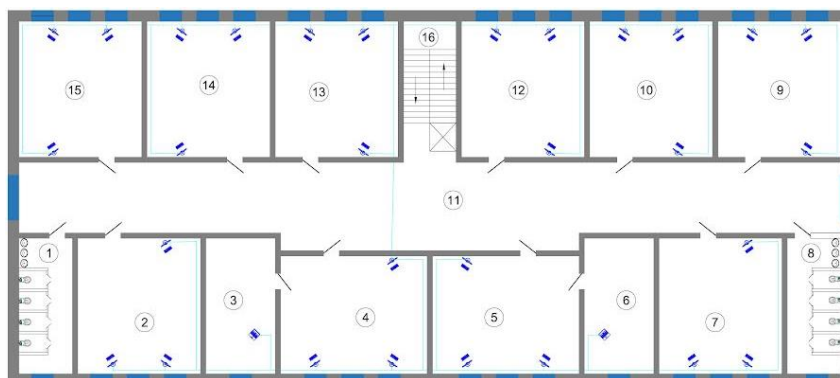
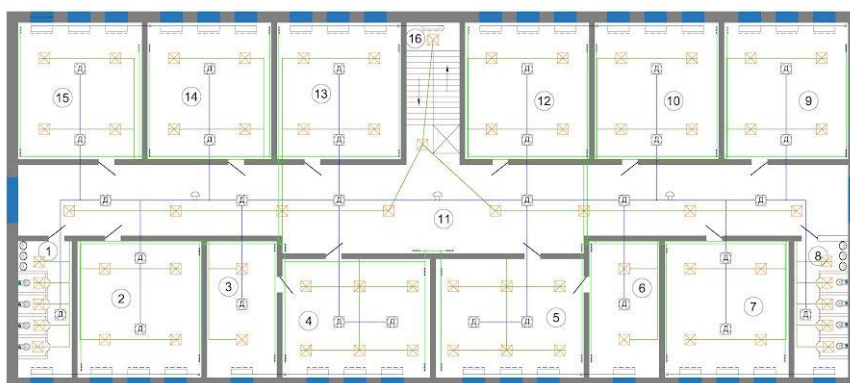


Рисунок 2.2 – Схема розташування ІТС в офісному приміщенні



Умовні позначення

	Радіатор опалення		Розетка внутрішня
	Система пожежної сигналізації		Система центрального теплого опалення
	Система електропостачання (освітлення)		Датчик задимлення
	Система електропостачання (розетки)		Стояк центрального опалення
	Лампа люмінесцентна		Сповісник пожежної тривоги

Рисунок 2.3 – Схема допоміжних технічних засобів офісного приміщення

		Присяжнюк Я.В.			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз С.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

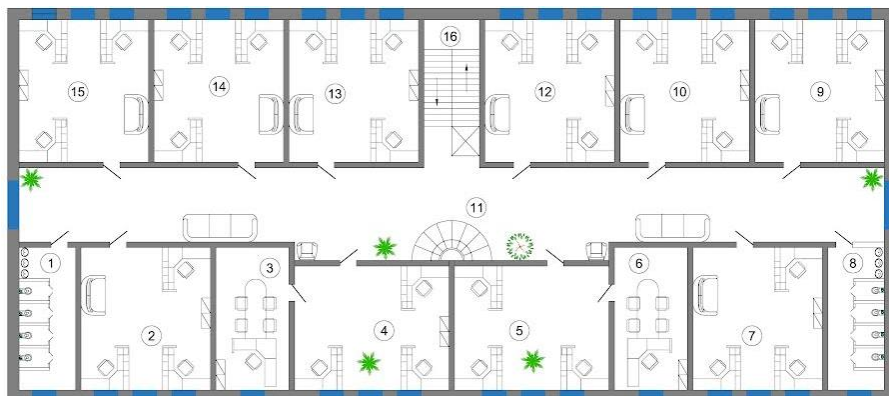


Рисунок 2.4 – Ситуаційний план приміщення

Таблиця 2.1

Реплікація приміщень

Позначення	Назва приміщення	Площа, м ²
1	Туалет, жіночий	6,5
2	Відділ кадрів	20
3	Кабінет директора	11
4	Відділ економічної безпеки	22
5	Відділ охорони	22
6	Кабінет начальника охорони	11
7	Фінансовий відділ	20
8	Туалет, чоловічий	6,5
9	Проектний відділ	20
10	Бухгалтерія	20
11	Коридор	50
12	Відділ маркетингу	20
13	Відділ інженерних вишукувань	20
14	ІТ-відділ	20
15	Договірно-плановий відділ	20
16	Сходова площадка	15

2.3 Обстеження середовища користувачів та інформаційних потоків

Відповідно до рівня повноважень щодо доступу до інформації, характеру робіт, які виконуються у процесі функціонування ІТС, доступ до ІТС матимуть:

- Користувачі ІТС[4] – особи, які працюють з інформацією (читають, редагують, друкують тощо). Користувачами ІТС є директор, заступник директора з економічної безпеки, технічний директор, персонал бухгалтерії, маркетингу, кадрів,

відділу економічної безпеки, фінансового відділу, проектного відділу, відділу інженерних вишукувань, ІТ відділу, договірно-планового відділу, начальник служби охорони.

- Технічний персонал – системний адміністратор, персонал обчислювального центру.
- Користувачі ІТС матимуть доступ до наступних видів інформації:
- Відкрита інформація загального користування;
- Інформація з обмеженим доступом, що має гриф «конфіденційно», «суворо конфіденційно».
- Схема інформаційних потоків підприємства з використанням моделі «граф-розгалуджене дерево» наведено на рис.2.5.

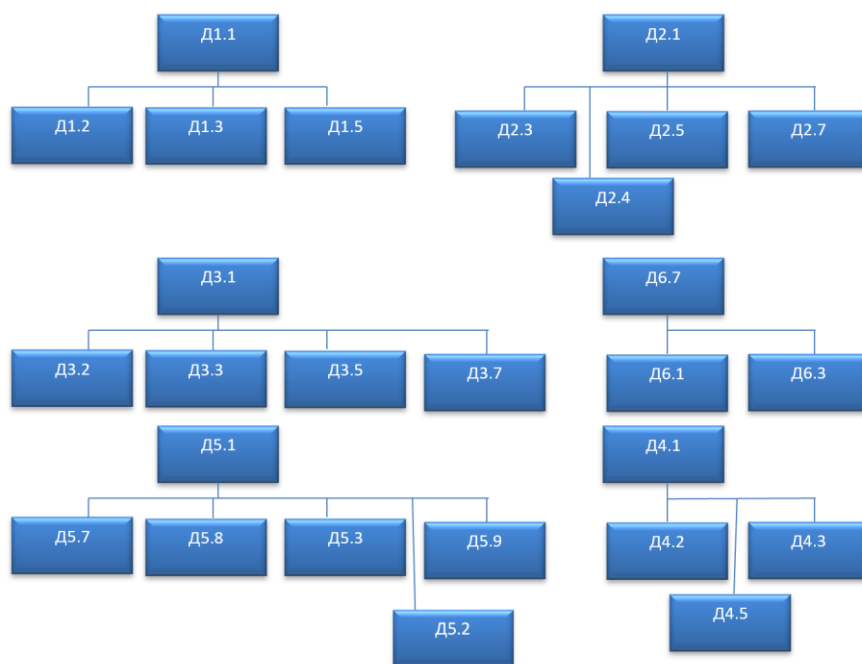


Рисунок 2.5 – Схема інформаційних потоків

- 1 – директор;
- 2 – комерційний директор, технічний директор;
- 3 – заступник директора з економічної безпеки;
- 4 – відділ кадрів;
- 5 – відділ економічної безпеки;
- 6 – начальник служби охорони;

7 – бухгалтерія, відділ маркетингу, фінансовий відділ, договірно-плановий відділ;

8 - проєктанти, інженери, геодезисти;

9 - IT відділ;

Д1 – Відомості стратегічного характеру

Д2 – Ділова інформація

Д3 – Відомості по фінансам

Д4 – Відомості економічного характеру

Д5 – Відомості технічного характеру

Д6 – Відомості про стан режиму безпеки

2.4 Аналіз технологій обробки інформації в наявній системі

Обчислювальна система є локальною мережею, яка складається з 32 АС класу «2» (ПЕОМ)[13], що знаходяться по одному на кожне робоче місце офісних приміщень. Крім цього, для забезпечення функціонування ІТС використовується 2 комутатори та 1 маршрутизатор. Склад і характеристика складових ІТС наведені у табл. 2.2. Схема наявної мережі на рис.2.6.

Таблиця 2.2

Складові ІТС

Пристрій	Характеристика	Заводський номер / рік виробництва	Кількість
Ноутбук	HP zbook g6	25486157/2019	2 шт
Системний блок	Intel i5 4x3.3 GHz + 240GB SSD	2334512 /2010	30 шт
Монітор	23"SAMSUNG 23xi (C3Z94AA)	1254945 /2017	30 шт
Пристрій	Характеристика	Заводський номер / рік виробництва	Кількість
Клавіатура	Vinga KB110BK	21668487 /2020	30 шт
Миша	Logitech Mouse M185 Swift Grey	12347856 /2018	32 шт
МФУ	Epson L3101	7689504932 /2018	10 шт
Блок безпереб. живлення	PowerWalker Vi 600 STL	2674857564739 /2016	30 шт
Модем (роутер)	Tenda AC7	36454533663 /2019	5 шт
Комутатор	TENDA S16	01-230886 /2018	2 шт
Маршрутизатор	TP-LINK TL-R4800T	0546415175/2018	5 шт

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз С.М.				22
Змн.	Арк.	№ докум.	Підпис	Дата		

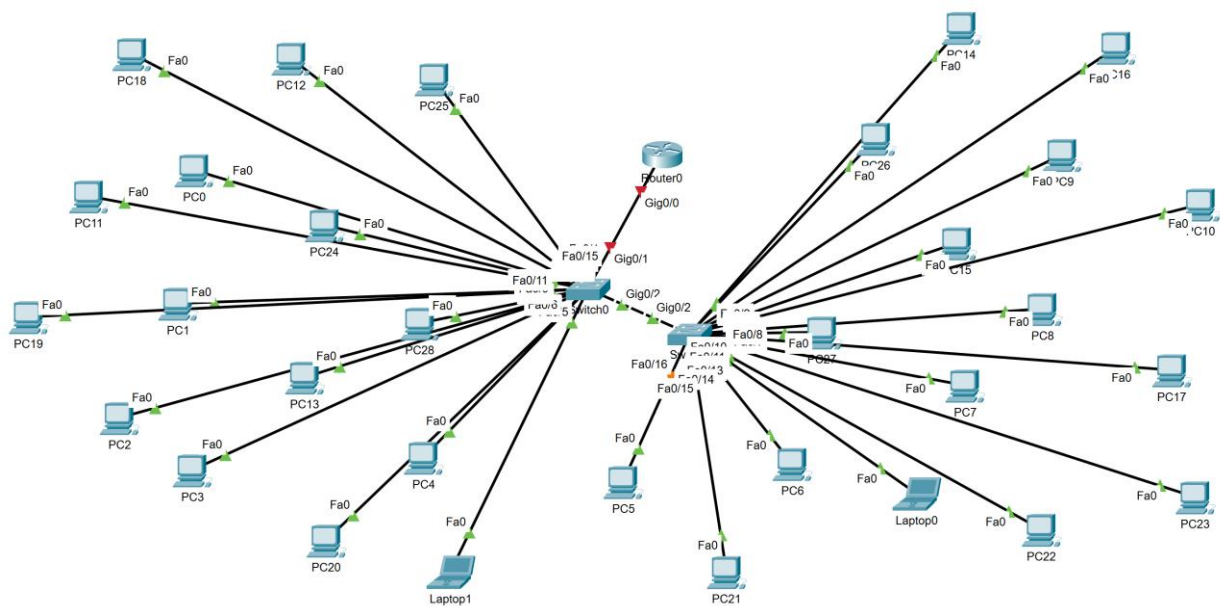


Рисунок 2.6 – Схема наявної мережі

В АС (ІТС) класу 2 встановлено наступне програмне забезпечення:

- Операційна система Windows 10 LTSC 2019;
- Пакет прикладних програм Microsoft Office 2016;
- Adobe Photoshop CS6;
- AutoCAD;
- Total Commander 9.51;
- Антивірус Avast 17.9;
- Антивірус USB Disk Security;
- ABBYY FineReader – Professional;
- Visual Studio 2019;

Для забезпечення функціонування ІТС використовується 2 комутатори, які об'єднують об'єкти АС в локальну комп'ютерну мережу, використовуючи з'єднувальні кабелі UTP категорії 5е, які не мають виходу за межі об'єкта ін-формаційної діяльності. Також наявний 1 маршрутизатор, який забезпечує доступ до мережі Інтернет.

2.5 Інформація, що планується до обробки.

Відповідно відомостей, що наведені в Акті визначення вищого ступеню доступу до інформації, яка циркулюватиме в ІТС класу «2» адміністративної будівлі

		Присяжнюк Я.В.			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз С.М.				23
Змн.	Арк.	№ докум.	Підпис	Дата		

Приватного підприємства «RaTe», матиме вищий гриф секретності «суворо конфіденційно».

За режимом доступу інформація, яка планується для обробки за допомогою ІТС, поділяється на[15]:

- Відкриту інформацію загального користування;
- Інформацію з обмеженим доступом – конфіденційна інформація (далі – ІзОД).

ІзОД буде представлена в ІТС у вигляді електронних документів створених за допомогою пакету прикладних програм Microsoft Office 2019, Adobe Photoshop CS6, AutoCAD 2021 або у роздрукованому паперовому вигляді.

Доступ до ІзОД мають зареєстровані в системі користувачі, що належать до адміністративної ланки підприємства та безпосередньо працівники відділів, що розміщені в офісних приміщеннях адміністративної будівлі даного підприємства.

2.6 Технології обробки інформації.

Відповідно відомостей, що наведені в Акті визначення вищого ступеню доступу до інформації, яка циркулюватиме в ІТС класу «2» адміністративної будівлі Приватного підприємства, матиме вищий гриф секретності «суворо конфіденційно».

За режимом доступу інформація, яка планується для обробки за допомогою ІТС, поділяється на:

- Відкриту інформацію загального користування;
- Інформацію з обмеженим доступом – конфіденційна інформація (далі – ІзОД).

ІзОД буде представлена в ІТС у вигляді електронних документів створених за допомогою пакету прикладних програм Microsoft Office 2019, Adobe Photoshop CS6, AutoCAD 2021 або у роздрукованому паперовому вигляді.

Доступ до ІзОД мають зареєстровані в системі користувачі, що належать до адміністративної ланки підприємства та безпосередньо працівники відділів, що розміщені в офісних приміщеннях адміністративної будівлі даного підприємства.

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

Висновки до другого розділу

У даному розділі було наведено розгорнуту характеристику об'єкта захисту та його основних складових, зокрема визначено фізичні, логічні й функціональні елементи, що підлягають захисту.

Розроблено ситуаційний план приміщення, схему розташування ІТС в офісному приміщенні та схему допоміжних технічних засобів. Детально розглянуто технічні особливості будівлі та розташування приміщень.

Проведено детальне обстеження середовища користувачів: визначено категорії користувачів, рівні їх доступу, характер взаємодії з інформаційними ресурсами. Особливу увагу приділено аналізу інформаційних потоків — виявлено основні джерела, напрямки руху інформації. Було змодельовано схему інформаційних потоків.

Крім того, подано повну інформацію щодо наявного технічного забезпечення, включаючи мережеві пристрої та комплектацію робочих станцій. Описано наявне програмне забезпечення робочих станцій. Спроектовано та описано схему існуючої локальної мережі організації.

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

РОЗДІЛ 3. РОЗРОБКА МОДЕЛІ ПОРУШНИКА ТА МОДЕЛІ ЗАГРОЗ, ПРОЄКТУВАННЯ ТОПОЛОГІЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

3.1 Розробка імовірного прогнозу та моделі порушника

Уразливі компоненти системи:

I - внутрішні дані

II - внутрішні прикладні програми

III - внутрішні системні модулі

IV - зовнішні дані

V - зовнішні системні модулі

VI - елементи комп'ютера та ін апаратура.

Види загроз:

A - модифікація,

B - знищення,

C - компрометація (розкриття) інформації.

Установимо відповідність ступенів ризику[11] – таблиця 3.1.

Таблиця 3.1

Ступінь ризику для різних категорій користувачів

	Елементи АС																	
	I			II			III			IV			V			VI		
Види збитків	A	B	C	A	B	C	A	B	C	A	B	C	A	B	C	A	B	C
Категорії користувачів	A	B	C	A	B	C	A	B	C	A	B	C	A	B	C	A	B	C
Інженер системних магнітних носіїв										4	4		3	3		3	3	
Користувач-операціоніст	2	2	2	1	1					2	2	2	1	1				

Продовження таблиці 3.1

Оператор системи	1	5	5		5	5		5	5	1	3	3						
Оператор периферійного обладнання											3	3		4	4		1	1
Оператор завдань											3	3		4	4			
Оператор вводу та підготовки даних	3	3	3		4	4		5	5	3	3	3		4	4		1	5
Менеджер обробки	1	5	5		5	5		5	5	1	3	3		4	4		1	5
Адміністратор баз даних	3	3	3							3	3	3						
Системний програміст		5	5		5	5	5	5	5							5	1	5
Прикладний програміст	1	1	1	2	2	2							2	2	2			
Користувач- програміст	1	1	1	2	2	2							2	2	2			
Менеджер програмного забезпечення	1	1	1	4	4	4							4	4	4			
Інженер/оператор по зв'язку		5	5															
Інженер системи							2	2	2									
Адміністратор безпеки	5	5	5	5	5	5	5	5	5	3	3	3	4	4	4	5	5	5
Системний адміністратор	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5

Далі зобразимо категорії порушників, визначених в моделі – таблиця 3.2.

Таблиця 3.2.

Категорії порушників, визначених у моделі

Позначення	Визначення категорії	Рівень за-гроз
	Внутрішні, по відношення до ІТС	
ПВ1	Технічний персонал, який обслуговує будови та приміщення (електрики, прибиральники тощо), в яких розташовані компоненти ІТС	1
ПВ2	Персонал, який обслуговує технічні засоби ІТС (інженери, техніки)	2
ПВ3	Користувачі (оператори) ІТС	2

Продовження таблиці 3.2

ПВ4	Адміністратори ІТС, співробітники служби захисту інформації	3
ПВ5	Співробітники служби безпеки установи та керівники різних рівнів	4
	Зовнішні по відношенню до ІТС	
ПЗ1	Відвідувачі (запрошені з будь-якого приводу)	1
ПЗ2	Представники організацій, що взаємодіють з питань технічного забезпечення (енерго-, водо-, теплопостачання і таке інше)	2
ПЗ3	Хакери	3
ПЗ4	Агенти конкурентів або закордонних спецслужб «під прикриттям»	4

Наступний крок – аналіз мотивів порушника. Відповідна класифікація знаходиться в таблиці 3.3.

Таблиця 3.3

Специфікація моделі порушника за мотивами порушень

Позначення	Мотив порушення	Рівень загроз
М1	Безвідповідальність	1
М2	Самоствердження	2
М3	Корисливий інтерес	3
М4	Професійний обов'язок (ПЗ4)	4

Також нам необхідно провести класифікацію за часом дії – таблиця 3.4.

Таблиця 3.4

Специфікація моделі порушника за часом дії

Позначення	Характеристика можливостей порушника	Рівень загроз
Ч1	Під час повної бездіяльності ІТС з метою відновлення та ремонту	1
Ч2	Під час призупинки компонентів ІТС з метою технічного обслуговування та модернізації	2

Ч3	Під час функціонування ІТС (або компонентів системи)	3
Ч4	Як у процесі функціонування ІТС, так і під час призупинки компонентів системи	4

І наостанок, за місцем вчинення порушення – таблиця 3.5.

Таблиця 3.5

Специфікація моделі порушника за місцем дії

Позначення	Характеристика місця дії порушника	Рівень загроз
Д1	Усередині приміщень, але без доступу до технічних засобів ІТС	1
Д2	З робочих місць користувачів (операторів) ІТС	2
Д3	З доступом у зону зберігання баз даних, архівів тощо	3
Д4	З доступом у зону керування засобами забезпечення безпеки ІТС	4

Далі виводимо два варіанти сумарного рівня загроз для окремих категорій можливих порушників:

1) внутрішній порушник «ПВ» - варіант мінімальних загроз з причини безвідповідального ставлення до виконання своїх посадових обов'язків;

2) зовнішній порушник «ПЗ4» (агент конкурентів або закордонних спецслужб «під прикриттям») - варіант максимальних загроз з причини цілеспрямованих несанкціонованих дій з метою модифікації або викрадення інформації. Зведемо все у таблицю 3.6.

Таблиця 3.6

Сумарний рівень загроз для окремих категорій порушників

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливість щодо подолання системи захисту	Можливість за часом дії	Можливість за місцем дії	Сума загроз
Директор	ПВ5	М1	К2	31	Ч3	Д3	14
	4	1	2	1	3	3	
	ПЗ4	М4	К4	34	Ч3	Д3	22
	4	4	4	4	3	3	
Комерційний директор	ПВ5	М1	К2	31	Ч3	Д3	14
	4	1	2	1	3	3	
	ПЗ4	М4	К4	34	Ч3	Д3	22
	4	4	4	4	3	3	
Заступник директора з комерційної безпеки	ПВ5	М1	К2	31	Ч3	Д3	14
	4	1	2	1	3	3	
	ПЗ4	М4	К4	34	Ч3	Д3	22
	4	4	4	4	3	3	
Проектант	ПВ2	М1	К2	31	Ч4	Д3	13
	2	1	2	1	4	3	
	ПЗ4	М4	К4	34	Ч4	Д3	23
	4	4	4	4	4	3	

Продовження таблиці 3.6

Інженер	ПВ2	М1	К2	31	Ч4	Д3	13
	2	1	2	1	4	3	
	ПЗ4	М4	К4	34	Ч4	Д3	23
	4	4	4	4	4	3	
Геодезист	ПВ2	М1	К2	31	Ч4	Д3	13
	2	1	2	1	4	3	
	ПЗ4	М4	К4	34	Ч4	Д3	23
	4	4	4	4	4	3	
Системний адміністратор	ПВ4	М1	К4	31	Ч4	Д4	17
	3	1	4	1	4	4	
	ПЗ4	М4	К4	34	Ч4	Д4	24
	4	4	4	4	4	4	
Бухгалтер	ПВ3	М1	К2	31	Ч3	Д3	12
	2	1	2	1	3	3	
	ПЗ4	М4	К4	34	Ч3	Д3	22
	4	4	4	4	3	3	
Працівник служби безпеки	ПВ4	М1	К1	31	Ч4	Д3	13
	3	1	1	1	4	3	
	ПЗ4	М4	К4	34	Ч4	Д3	23
	4	4	4	4	4	3	
Начальник служби безпеки	ПВ5	М1	К4	31	Ч4	Д3	17
	4	1	4	1	4	3	
	ПЗ4	М4	К4	34	Ч4	Д3	23
	4	4	4	4	4	3	

		Присяжнюк Я.В.			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				31
Змн.	Арк.	№ докум.	Підпис	Дата		

Закінчення таблиці 3.6

Маркетолог	ПВ3	М1	К1	31	Ч3	Д2	10
	2	1	1	1	3	2	
	ПЗ4	М4	К4	34	Ч3	Д2	21
	4	4	4	4	3	2	
Працівник відділу кадрів	ПВ3	М1	К1	31	Ч3	Д2	10
	2	1	1	1	3	2	
	ПЗ4	М4	К4	34	Ч3	Д2	21
	4	4	4	4	3	2	
Діловод	ПВ3	М1	К1	31	Ч3	Д3	11
	2	1	1	1	3	3	
	ПЗ4	М4	К4	34	Ч3	Д3	22
	4	4	4	4	3	3	

Також створимо модель внутрішнього порушника політики безпеки інформації – таблиця 3.7.

Таблиця 3.7

Модель внутрішнього порушника політики безпеки інформації

Категорія порушника «ПВ»	Мотив порушень	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Директор	М1	К2	31	Ч3	Д3	14
Комерційний директор	М1	К2	31	Ч3	Д3	14

Заступник директора з комерційної безпеки	М1	К2	З1	Ч3	Д3	14
Проектант	М1	К2	З1	Ч4	Д3	13
Інженер	М1	К2	З1	Ч4	Д3	13
Геодезист	М1	К2	З1	Ч4	Д3	13
Системний адміністратор	М1	К4	З1	Ч4	Д4	17
Бухгалтер	М1	К2	З1	Ч3	Д3	12
Діловод	М1	К1	З1	Ч3	Д3	11
Працівник служби безпеки	М1	К1	З1	Ч4	Д3	13
Начальник служби безпеки	М1	К4	З1	Ч4	Д3	17
Маркетолог	М1	К1	З1	Ч3	Д2	10
Працівник відділу кадрів	М1	К1	З1	Ч3	Д2	10

Аналіз останньої таблиці показує, що найбільшу загрозу, що має відношення до проблеми захисту інформації, становить адміністратор ІТС.

Тому організація роботи цієї особи повинна бути найбільш контрольованою, оскільки вона є основним потенційним порушником безпеки інформації. Таким чином представлено побудову моделі порушника та досліджено її особливості формування.

3.2 Розробка імовірної моделі загроз

Перейдемо до моделювання імовірних загроз[11].

Для складання імовірної моделі загроз було використано ПЗ OWASP Threat Dragon.

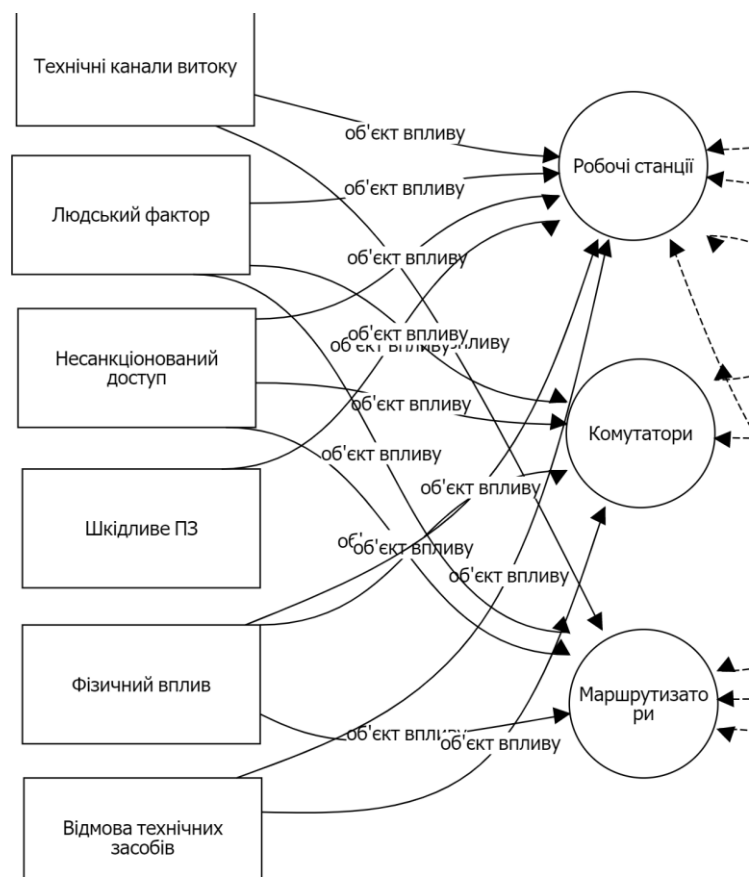


Рисунок 3.1 – Візуалізація об'єктів впливу

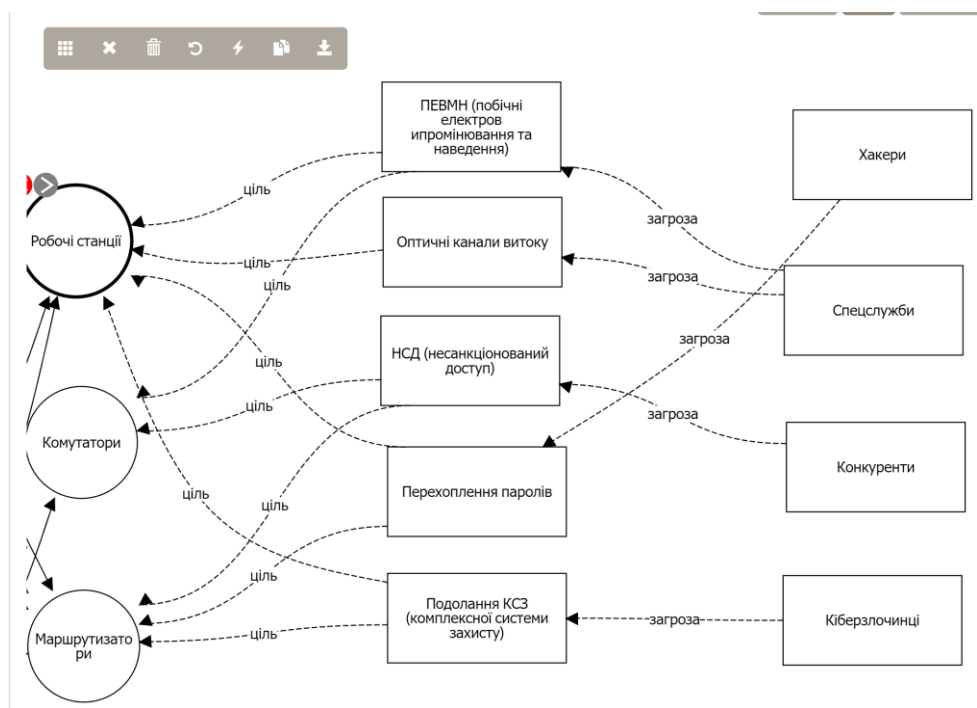


Рисунок 3.2 – Візуалізація суб'єктів, об'єктів та загроз

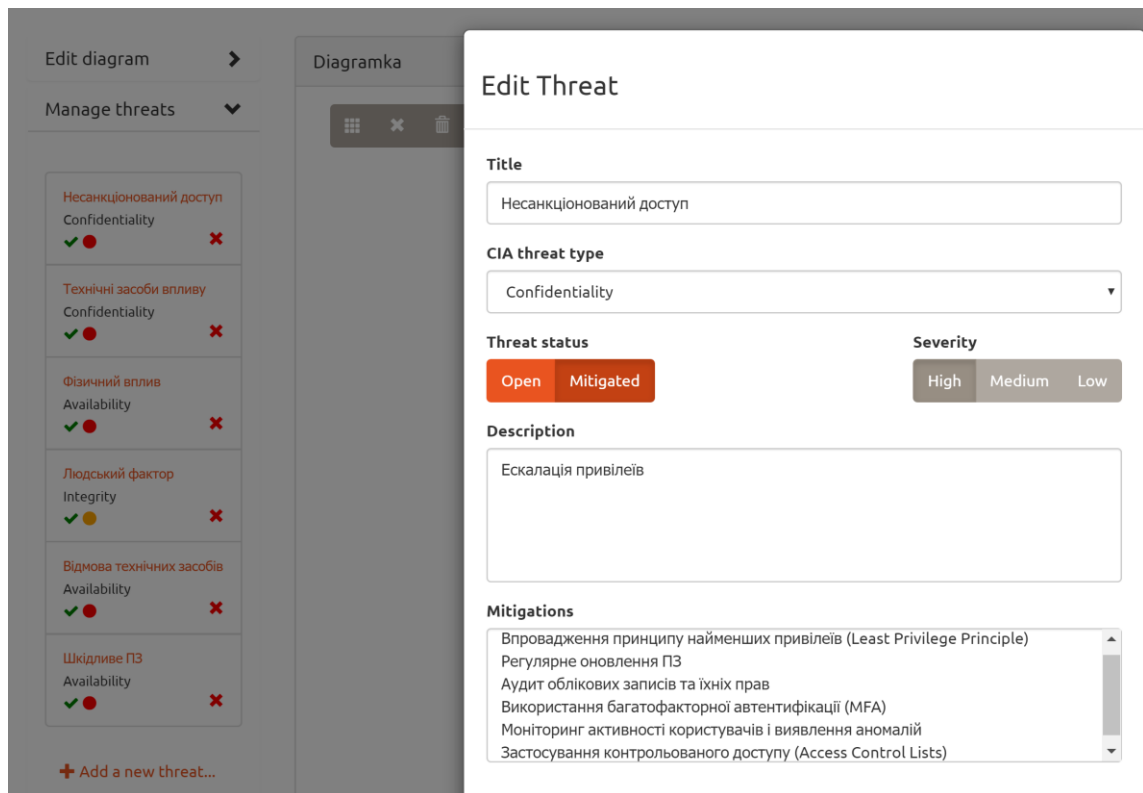


Рисунок 3.3 – Приклад опрацювання потенційної загрози, засобами спеціального ПЗ

Розглянемо більш детально кожну загрозу та шляхи її запобігання.

- Несанкціонований доступ (ескалація привілеїв) :
 - впровадження принципу найменших привілеїв (Least Privilege Principle);
 - регулярне оновлення ПЗ;
 - аудит облікових записів та їхніх прав;
 - використання багатофакторної автентифікації (MFA);
 - моніторинг активності користувачів і виявлення аномалій;
 - застосування контрольованого доступу (Access Control Lists).
- Технічні засоби впливу (копіювання інформації з носіїв, несанкціоноване відеоспостереження):
 - обмеження фізичного доступу до критичних систем;
 - екранування і захист технічних каналів передачі даних;
 - виявлення та блокування несанкціонованих пристроїв (наприклад, USB, бездротових модулів);
 - шифрування переданих і збережених даних;

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				35
Змн.	Арк.	№ докум.	Підпис	Дата		

- політики контролю використання мобільних пристроїв і знімних носіїв;
- проведення аудиту і тестування на предмет наявності побічних каналів витоку.

- Фізичний вплив (природні явища, стихійні лиха, збій електропостачання, крадіжка обладнання):

- розміщення обладнання в дата-центрах із захистом від пожеж, затоплень, землетрусів та інших стихійних лих;

- використання джерел безперебійного живлення (UPS) та резервних генераторів;

- регулярне тестування систем аварійного живлення;

- встановлення фізичних засобів захисту: контроль доступу, камери відеоспостереження, охорона;

- інвентаризація та маркування обладнання з можливістю відстеження;

- встановлення сигналізації та систем сповіщення про несанкціонований доступ;

- забезпечення резервного копіювання та зберігання копій у захищених географічно віддалених локаціях;

- розробка та тестування планів реагування на надзвичайні ситуації (Disaster Recovery Plan, DRP);

- страхування критичного обладнання від фізичних ризиків.

- Людський фактор (розголошення паролів, помилки в налаштуванні):

- проведення регулярного навчання персоналу з інформаційної безпеки;

- впровадження політик створення складних паролів і заборони їх розголошення;

- використання багатофакторної автентифікації (MFA);

- аудит і контроль змін у конфігураціях систем (change management);

- Впровадження принципу поділу обов'язків та обмеження прав доступу;

- моніторинг активності користувачів і виявлення підозрілої поведінки;

- регулярне тестування безпеки (наприклад, пентести або аудит налаштувань).

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

- Відмова технічних засобів (перебої в електропостачанні, збої в мережі):
 - використання джерел безперебійного живлення (UPS) та резервних генераторів;
 - побудова відмовостійкої IT-інфраструктури (redundancy) — дублювання критичних елементів;
 - застосування систем автоматичного перемикавання на резервні канали зв'язку;
 - регулярне технічне обслуговування та моніторинг стану обладнання;
 - виявлення та усунення "вузьких місць" у мережевій інфраструктурі;
 - використання надійного мережевого обладнання з підтримкою протоколів резервування (наприклад, VRRP, STP);
 - тестування планів аварійного відновлення (Disaster Recovery Testing);
 - оперативне сповіщення про інциденти та централізований журнал подій.
- Шкідливе ПЗ (зараження ПК вірусами):
 - використання сучасного антивірусного та антималварного ПЗ з регулярним оновленням сигнатур;
 - обмеження прав користувачів на встановлення ПЗ (принцип найменших привілеїв);
 - сегментація мережі для мінімізації поширення шкідливого ПЗ;
 - регулярне оновлення операційної системи та прикладного ПЗ;
 - проведення навчання користувачів щодо фішингу та безпечної поведінки в мережі;
 - резервне копіювання критичної інформації для запобігання втратам у разі зараження.

3.3 Основні аспекти менеджменту інформаційної безпеки, пов'язані з персоналом

Перейдемо до огляду основних аспектів менеджменту інформаційної безпеки, пов'язаних з персоналом[12].

1. Попередня перевірка.

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

Перед прийняттям на роботу працівника, слід здійснити перевірку його інформаційного середовища та історії працевлаштування. Це допоможе зменшити ризики пов'язані із зловживанням працівником доступом до конфіденційної інформації.

Конкретні механізми реалізації цієї політики можуть включати:

- Збір інформації про кандидата. Такі як резюме, інтерв'ю, рекомендації, документи, що підтверджують освіту та досвід роботи.
- Перевірка документів для забезпечення правдивості інформації, яку надав кандидат, можуть бути перевірені його документи, такі як дипломи про освіту, сертифікати і тд.
- Перевірка досвіду роботи. А саме: зв'язок з попередніми роботодавцями кандидата та запит про перевірку його робочих місць.
- Перевірка відсутності конфлікту інтересів. Може включати дослідження можливих конфліктів інтересів, які можуть виникнути між інформаційною безпекою та іншими обов'язками кандидата.
- Перевірка кримінального минулого (запит в правоохоронні органи)
- Перевірка комп'ютерної грамотності. Може включати перевірку знань кандидата щодо інформаційної безпеки.

2. Угоди про нерозголошення.

Угоди про нерозголошення (NDA) відповідають за забезпечення захисту конфіденційної інформації. Ці угоди підписуються усіма співробітниками, які мають доступ до конфіденційної інформації, та підтверджують їхнє зобов'язання не розголошувати цю інформацію третім сторонам.

Конкретні механізми реалізації цієї політики можуть включати:

- Підготовка: розроблення тексту NDA, який має чітко визначити обов'язки та права сторін, визначити обсяг інформації, що підпадає під дію угоди про нерозголошення, та строк дії угоди.
- Підписання: угоду підписують всі співробітники, які мають доступ до конфіденційної інформації. Підписання може здійснюватися як при прийомі на роботу, так і при зміні обов'язків.

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

- Пояснення вимог: після підписання угоди про нерозголошення, необхідно пояснити всім співробітникам вимоги, що містяться в угоді. Це можна зробити шляхом проведення навчання, презентацій або інших форм навчання.

- Моніторинг виконання: необхідно забезпечити моніторинг виконання угоди про нерозголошення. Це може здійснюватись шляхом проведення аудиту або регулярного перегляду діяльності співробітників.

- Відповідальність за порушення: необхідно передбачити відповідальність за порушення угоди про нерозголошення. Це може включати штрафи, розірвання контракту, інші санкції та правову відповідальність.

- Актуальність: угода про нерозголошення може потребувати оновлення, наприклад, якщо змінюється обсяг конфіденційної інформації, що підпадає під дію угоди, або коли змінюється структура компанії.

3. Тренінги для персоналу.

Навчання персоналу стандартам безпеки допомагає знизити ризик витоку конфіденційної інформації та інших проблем, пов'язаних зі зловживанням позицією. Це може бути включено в процеси навчання нових співробітників або проводитися регулярно з усіма працівниками.

Конкретні механізми реалізації цієї політики можуть включати:

- Оцінка потреб у навчанні: керівництво повинно з'ясувати, які знання та навички щодо безпеки необхідні персоналу, який має доступ до конфіденційної інформації.

- Розробка програми навчання: за допомогою отриманих даних про потреби персоналу в навчанні, слід розробити програму навчання, яка містить відповідні інструкції та курси.

- Проведення навчання: навчання може бути проведене в формі онлайн-курсів, семінарів, тренінгів або воркшопів, в залежності від типу та розміру підприємства.

- Оцінка ефективності: після проведення навчання необхідно оцінити його ефективність, щоб переконатися, що співробітники зрозуміли стандарти безпеки та вміють їх застосовувати на практиці.

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		39

- Регулярність навчання: з метою забезпечення постійної відповідності до стандартів безпеки, навчання може бути проведене регулярно з періодичністю, що визначається рівнем ризику витоку інформації.

Ці механізми можуть бути реалізовані за допомогою внутрішньогонавчального центру підприємства, або за допомогою зовнішніх постачальників навчання, таких як курси з безпеки в Інтернеті.

4. Контроль доступу.

Контроль доступу до конфіденційної інформації, який забезпечує, що тільки люди з необхідним рівнем доступу мають доступ до цієї інформації.

Конкретні механізми реалізації цієї політики можуть включати:

- Встановлення системи авторизації та аутентифікації користувачів із різними рівнями доступу до інформації. Це може включати використання паролів, біометричних методів аутентифікації та інших технічних засобів.

- Розроблення та впровадження політики доступу до інформації, яка визначає рівень доступу користувачів до різних видів інформації, а також процедури контролю доступу до цієї інформації.

- Встановлення контролю над зовнішніми пристроями, які підключаються до комп'ютерних систем, таких як USB-накопичувачі, з метою запобігання витоку даних.

- Встановлення механізмів моніторингу та аналізу доступу до інформації для виявлення можливих порушень інформаційної безпеки та вчасного реагування на них.

3.4 Розробка топології мережі

При проектуванні мережі ми намагалися дотримуватися ієрархічної моделі мережі[8], яка має багато переваг:

- спрощується розуміння організації мережі;
- модель має модульність, що означає простоту нарощування потужностей саме там, де необхідно;
- легше знайти та ізолювати проблему;

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

- підвищена відмовостійкість за рахунок дублювання пристроїв та/або з'єднань;
- розподіл функцій із забезпечення працездатності мережі з різних пристроїв.

Відповідно до цієї моделі, мережа розбивається на три логічні рівні:

- ядро мережі (Core layer: високопродуктивні пристрої, головне призначення - швидкий транспорт);
- рівень поширення (Distribution layer: забезпечує застосування політик безпеки, QoS, агрегацію та маршрутизацію у VLAN, визначає широкомовні домени);
- рівень доступу (Access-layer: як правило, L2 комутатори, призначення: підключення кінцевих пристроїв, маркування трафіку для QoS, захист від кілець у мережі (STP) та широкомовних штормів, забезпечення живлення для PoE пристроїв).

Відповідно до проведеного обстеження, спроектовано вдосконалену локальну мережу організації. Розгорнута схема мережі наведена в додатках.

Ядро мережі складається з двох маршрутизаторів (рис.3.4), з'єднаних між собою високошвидкісними каналами зв'язку вита пара GigabitEthernet та чотирьох комутаторів, з'єднаних між собою високошвидкісними агрегованими каналами зв'язку вита пара FastEthernet. Єдиним призначенням центрального рівня є швидка комутація трафіка[6].

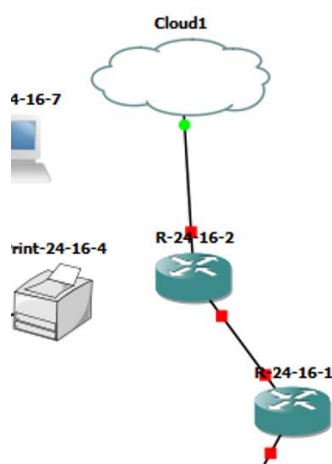


Рисунок 3.4 – Ядро мережі

		Присяжнюк Я.В.			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз С.М.				41
Змн.	Арк.	№ докум.	Підпис	Дата		

Рівень поширення створений на базі з десяти комутаторів, що під'єднані до ядра мережі за допомогою витієї пари GigabitEthernet (використовуючи статичне агрегування для покращення роботи з'єднання).

Рівень доступу представлений кінцевим устаткуванням користувачів, що забезпечує функціонування рівня.

Особливістю з'єднань комутаційного обладнання є те, що для забезпечення високої продуктивності роботи мережі використовуються високошвидкісні лінії зв'язку Gigabit Ethernet. Кінцеві вузли під'єднані до комутаційного обладнання за допомогою ліній Fast Ethernet на витій парі[9]. Приклад такого підключення наведений на рис.3.5.

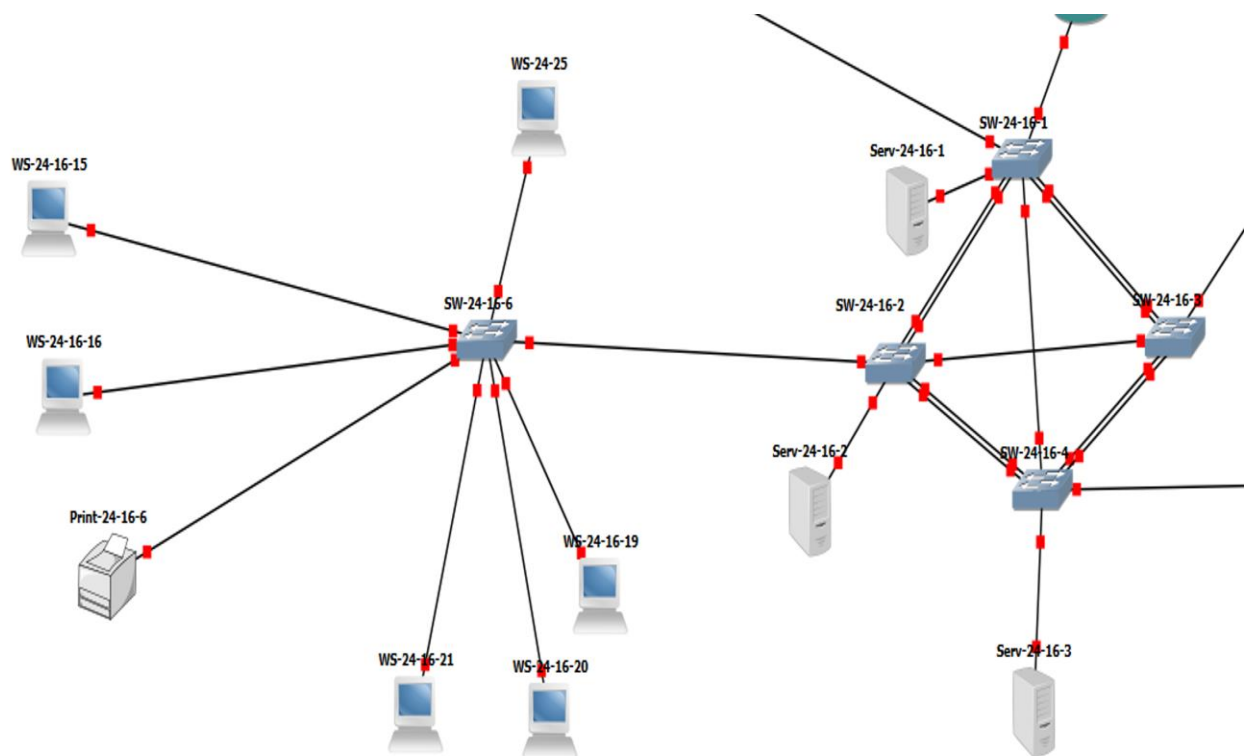


Рисунок 3.5 – Приклад з'єднання

Загалом для побудови даної мережі організації використано два маршрутизатори та десять комутаторів.

3.5 Розробка схеми адресації мережі

Таблиця 3.8

Адресація пристроїв

Мережа/пристрій	Інтерфейс/Мережний адаптер/Шлюз	IP-адреса	Маска	Префікс
Маршрутизатор R-24-16-1	Інтерфейс Fa0/0	192.24.16.2	255.255.255.248	/29
	Інтерфейс Fa1/0	191.24.16.126	255.255.255.128	/25
Маршрутизатор R-24-16-2	Інтерфейс Fa0/0	192.24.16.1	255.255.255.248	/29
	Інтерфейс Fa1/0	192.24.16.9	255.255.255.248	/29
Комутатор SW-24-16-1	Інтерфейс Vlan 1	191.24.16.1	255.255.255.128	/25
	Шлюз за замовчуванням	191.24.16.126	-	-
Комутатор SW-24-16-2	Інтерфейс Vlan 1	191.24.16.2	255.255.255.128	/25
	Шлюз за замовчуванням	191.24.16.126	-	-
Комутатор SW-24-16-3	Інтерфейс Vlan 1	191.24.16.3	255.255.255.128	/25
	Шлюз за замовчуванням	191.24.16.126	-	-
Комутатор SW-24-16-4	Інтерфейс Vlan 1	191.24.16.4	255.255.255.128	/25
	Шлюз за замовчуванням	191.24.16.126	-	-
Комутатор SW-24-16-5	Інтерфейс Vlan 1	191.24.16.5	255.255.255.128	/25
	Шлюз за замовчуванням	191.24.16.126	-	-
Комутатор SW-24-16-6	Інтерфейс Vlan 1	191.24.16.6	255.255.255.128	/25
	Шлюз за замовчуванням	191.24.16.126	-	-
Комутатор SW-24-16-7	Інтерфейс Vlan 1	191.24.16.7	255.255.255.128	/25
	Шлюз за замовчуванням	191.24.16.126	-	-
Комутатор SW-24-16-8	Інтерфейс Vlan 1	191.24.16.8	255.255.255.128	/25
	Шлюз за замовчуванням	191.24.16.126	-	-

Комутатор SW-24-16-9	Інтерфейс Vlan 1	191.24.16.9	255.255.255.128	/25
	Шлюз за замовчуванням	191.24.16.126	-	-
Комутатор SW-24-16-10	Інтерфейс Vlan 1	191.24.16.10	255.255.255.128	/25
	Шлюз за замовчуванням	191.24.16.126	-	-
Сервер Serv-24-16-3	Мережний адаптер	191.24.16.12	255.255.255.128	/25
	Шлюз за замовчуванням	191.24.16.126	-	-
Сервер Serv-24-16-2	Мережний адаптер	191.24.16.13	255.255.255.128	/25
	Шлюз за замовчуванням	191.24.16.126	-	-
Сервер Serv-24-16-1	Мережний адаптер	191.24.16.14	255.255.255.128	/25
	Шлюз за замовчуванням	191.24.16.126	-	-
Робоча станція WS-ADMIN	Мережний адаптер	191.24.16.15	255.255.255.128	/25
	Шлюз за замовчуванням	191.24.16.126	-	-

Для всіх інших кінцевих пристроїв було використане динамічне виділення ір-адрес (DHCP)[10].

Таблиця 3.9

Адреси підмереж

Мережа	ІР-адреса	Маска	Інверсна маска	Префікс
A	191.24.16.0	255.255.255.128	0.0.0.127	/25
B	192.24.16.0	255.255.255.248	0.0.0.7	/29
C	192.24.16.8	255.255.255.248	0.0.0.7	/29

3.6 Вибір обладнання та ОС пристроїв для розробленого проєкту мережі

В мережі використовуються однакові комутатори моделі Cisco WS-C2960X-24TS-L[5] (рис.3.5).



Рисунок 3.6 – Комутатор Cisco WS-C2960X-24TS-L

WS-C2960X-24TS-L — це комутатор Cisco серії Catalyst 2960-X, який призначений для середніх і великих корпоративних мереж. Він має 24 порти Gigabit Ethernet, що забезпечує швидке і стабільне з'єднання для великої кількості пристроїв. Комутатор підтримує технологію Cisco StackWise, що дозволяє об'єднувати кілька пристроїв у стек і керувати ними як одним, підвищуючи масштабованість і надійність мережі.

Пристрій оснащений енергоефективними функціями, які допомагають знизити споживання електроенергії, що особливо важливо для компаній, які прагнуть зменшити витрати на експлуатацію. WS-C2960X-24TS-L також підтримує багаті можливості управління і безпеки, такі як VLAN, Quality of Service (QoS) і захист від атак, що гарантує безперебійність роботи мережі і захист від загроз.

Ще однією перевагою цього комутатора є його компактний і надійний корпус, який легко інтегрується у стандартні серверні шафи. Це робить його зручним рішенням для організацій, яким потрібен стабільний, гнучкий і простий у налаштуванні мережевий пристрій, здатний забезпечити швидкий обмін даними та підтримувати сучасні IT-завдання.

Орієнтовна вартість 45 000 грн[13].



Рисунок 3.7 – Маршрутизатор Cisco ISR4321/K9

		Присяжнюк Я.В.			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				45
Змн.	Арк.	№ докум.	Підпис	Дата		

Cisco ISR 4321/K9[5] — це маршрутизатор із серії Cisco Integrated Services Routers (ISR) 4000, призначений для малих і середніх офісів. Він забезпечує базову продуктивність маршрутизації до 50 Мбіт/с (з можливістю розширення до 100 Мбіт/с через ліцензії) та підтримує широкий спектр мережевих функцій, таких як статична і динамічна маршрутизація (OSPF, EIGRP, BGP), фільтрація трафіку (ACL), QoS, VPN, DHCP, SNMP та інші.

Має два гігабітні Ethernet-порти, один слот для модуля розширення (NIM) і один слот сервісного модуля (SM), що дозволяє масштабувати пристрій відповідно до потреб мережі. Працює на сучасній операційній системі Cisco IOS XE. Підходить для побудови надійної внутрішньої мережі з розділенням підмереж, маршрутизацією між VLAN, або підключенням до зовнішнього провайдера через інший маршрутизатор.

Орієнтовна вартість з ліцензією SEC 100 000 грн[13].

Висновки до третього розділу

У даному розділі було складено й обґрунтовано імовірний прогноз дій потенційного порушника, з урахуванням рівня його технічної підготовки, мотивації, доступу до ресурсів та можливих цілей атак. На основі цього сформовано модель порушника, яка дозволила класифікувати можливі типи зловмисників — як зовнішніх, так і внутрішніх — та визначити ймовірні сценарії їхнього впливу на інформаційну систему.

Паралельно було розроблено й проаналізовано модель загроз, в якій охоплено широкий спектр ризиків: від витоку конфіденційної інформації й несанкціонованого доступу до деструктивних дій, пов'язаних із виведенням системи з ладу або її компрометацією. Загрози систематизовано за джерелами, вразливими місцями та потенційними наслідками, що дозволило визначити пріоритетні напрямки захисту.

Окрему увагу приділено питанням менеджменту інформаційної безпеки, зокрема тим аспектам, що пов'язані з людським фактором. Розглянуто ролі та відпо-

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

відальність персоналу, політику доступу, правила роботи з конфіденційною інформацією, а також необхідність проведення навчання та підвищення обізнаності працівників у сфері безпеки.

У межах проєктної частини було розроблено топологію майбутньої комп'ютерної мережі. Створено детальну схему адресації для всіх підмереж, із чітким розподілом IP-адрес відповідно до призначення пристроїв, що забезпечує ефективне керування ресурсами та полегшує адміністрування мережі.

У даному розділі також наведено рекомендоване мережеве обладнання — комутатори та маршрутизатори. Для кожного з них наведено короткий опис, визначено переваги. Це забезпечує оптимальні умови для подальшої реалізації мережевої інфраструктури з належним рівнем захисту.

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

РОЗДІЛ 4. ПОБУДОВА, НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ СПРОЄКТОВАНОЇ ЛОКАЛЬНОЇ МЕРЕЖІ

4.1 Побудова та налагодження спроектованої локальної мережі

Налагодимо ір-адресацію на мережних пристроях[2]. Почнемо комутатора (рис.4.1).

```
SW-24-16-3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-24-16-3(config)#int vlan 1
SW-24-16-3(config-if)#ip address 191.24.16.3 255.255.255.128
SW-24-16-3(config-if)#no shut
SW-24-16-3(config-if)#exit
SW-24-16-3(config)#
*May 24 10:36:54.203: %LINK-3-UPDOWN: Interface Vlan1, changed state to up
*May 24 10:36:55.209: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
SW-24-16-3(config)#exit
SW-24-16-3#
```

Рисунок 4.1 – Типове налаштування комутатора

Проводимо налаштування для маршрутизатора (рис.4.2).

```
R-24-16-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R-24-16-1(config)#int fa0/0
R-24-16-1(config-if)#ip address 192.24.16.2 255.255.255.248
R-24-16-1(config-if)#no shut
R-24-16-1(config-if)#exit
R-24-16-1(config)#
*May 19 21:55:16.731: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*May 19 21:55:17.731: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R-24-16-1(config)#int fa1/0
R-24-16-1(config-if)#ip address 191.24.16.126 255.255.255.128
R-24-16-1(config-if)#no shut
R-24-16-1(config-if)#exit
R-24-16-1(config)#
*May 19 21:55:59.047: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to up
*May 19 21:56:00.047: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
R-24-16-1(config)#exit
R-24-16-1#
```

Рисунок 4.2 – Типове налаштування маршрутизатора

Після налаштування ІР-адресації на маршрутизаторах та комутаторах. Перевіримо зв'язок між мережними пристроями в кожній підмережі. Для цього використаємо відповідні команди (рис.4.3-4).

		Присяжнюк Я.В.			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

```

SW-24-16-10#ping 191.24.16.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 191.24.16.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 2/2/3 ms
SW-24-16-10#ping 191.24.16.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 191.24.16.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 2/3/7 ms
SW-24-16-10#ping 191.24.16.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 191.24.16.3, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 2/5/6 ms
SW-24-16-10#ping 191.24.16.4

```

Рисунок 4.3 – Перевірка зв'язку між комутаторами

```

SW-24-16-10#ping 191.24.16.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 191.24.16.5, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/3 ms
SW-24-16-10#ping 191.24.16.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 191.24.16.6, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 2/3/4 ms
SW-24-16-10#ping 191.24.16.7
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 191.24.16.7, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 8/9/12 ms
SW-24-16-10#ping 191.24.16.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 191.24.16.8, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 5/5/6 ms
SW-24-16-10#ping 191.24.16.9
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 191.24.16.9, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 2/2/4 ms
SW-24-16-10#ping 191.24.16.126
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 191.24.16.126, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 10/10/11 ms
SW-24-16-10#

```

Рисунок 4.4 – Перевірка зв'язку між мережними пристроями

Проведемо базові налаштування для Windows Server 2019 (рис.4.5-6).

```

PS C:\Users\Administrator> Install-WindowsFeature -Name AD-Domain-Services, DNS, DHCP, File-Services -IncludeManagementTools

```

Success	Restart Needed	Exit Code	Feature Result
True	No	Success	{Group Policy Management, Active Directory...

```

PS C:\Users\Administrator>

```

Рисунок 4.5 – Встановлення ролей на сервері

		Присяжнюк Я.В.			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		49

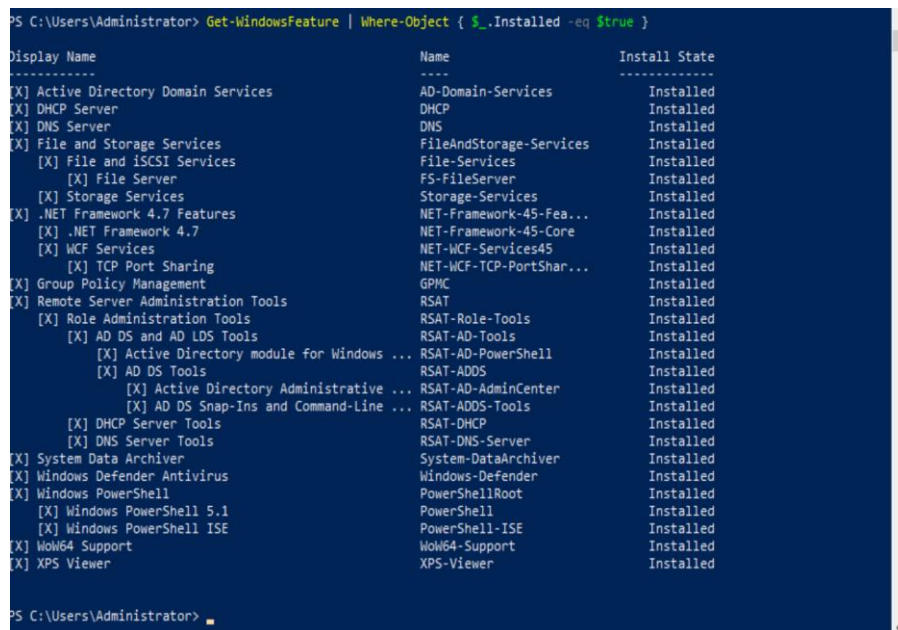


Рисунок 4.6 – Перевірка встановлених ролей

Налаштовуємо контролер домену та сеанс поточного користувача (рис.4.7-10).

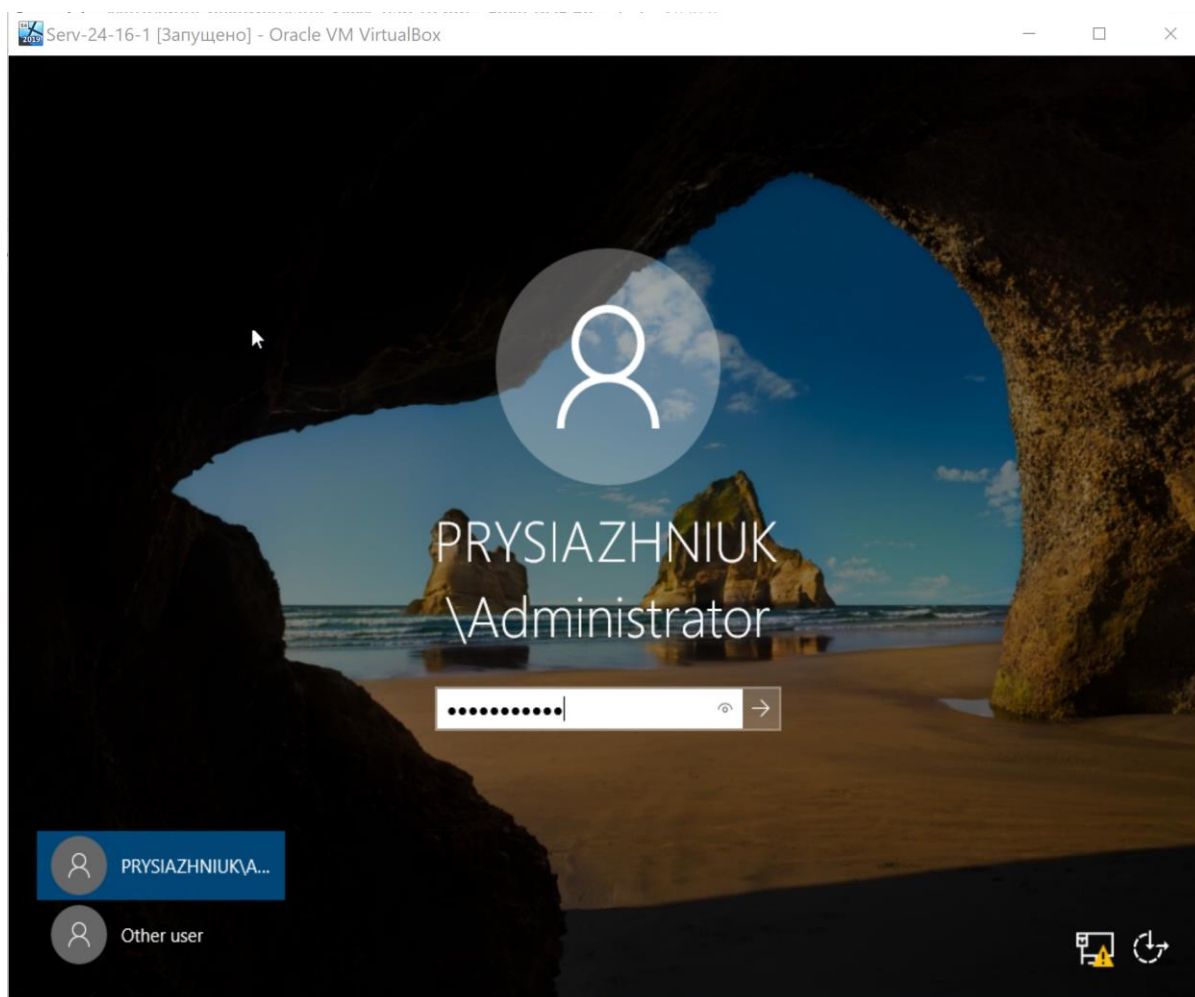


Рисунок 4.7 – Перезапуск машини після налаштувань

		Присяжнюк Я.В.			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз С.М.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

```

PS C:\Users\Administrator> nslookup prysiazhniuk.net
DNS request timed out.
    timeout was 2 seconds.
Server: UnKnown
Address: ::1

Name:   prysiazhniuk.net

PS C:\Users\Administrator>

```

Рисунок 4.8 – Перевірка відповідних налаштувань

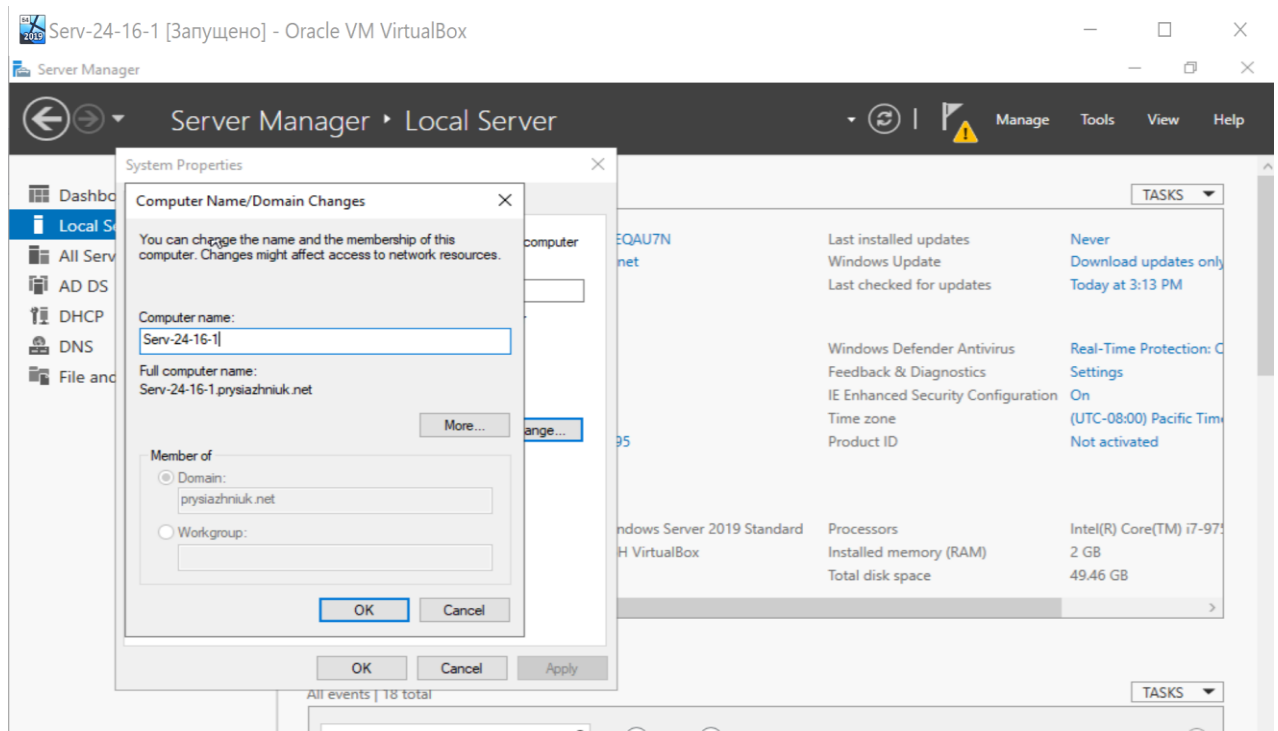


Рисунок 4.9 – Змінюємо назву сервера

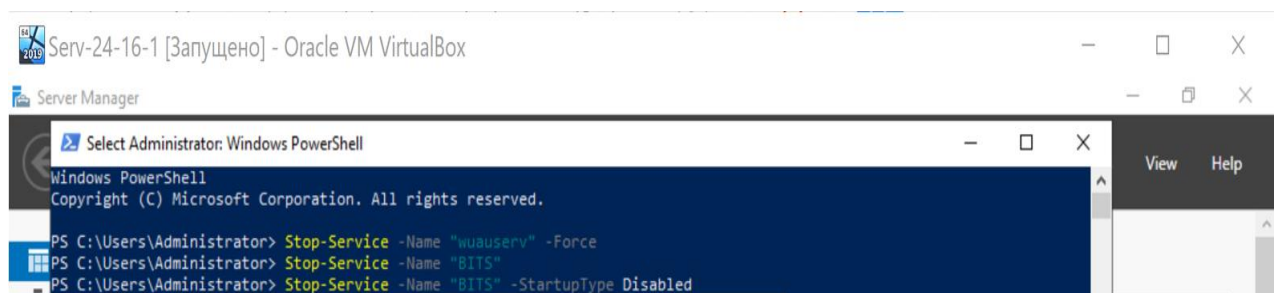


Рисунок 4.10 – Відключаємо автоматичні оновлення

Інші сервери мережі підготовлюємо до подальших налаштувань аналогічно.

Налаштуємо адресацію для серверів та робочої станції адміністратора (рис.4.11-12). На даних пристроях буде використовуватися статична адресація.

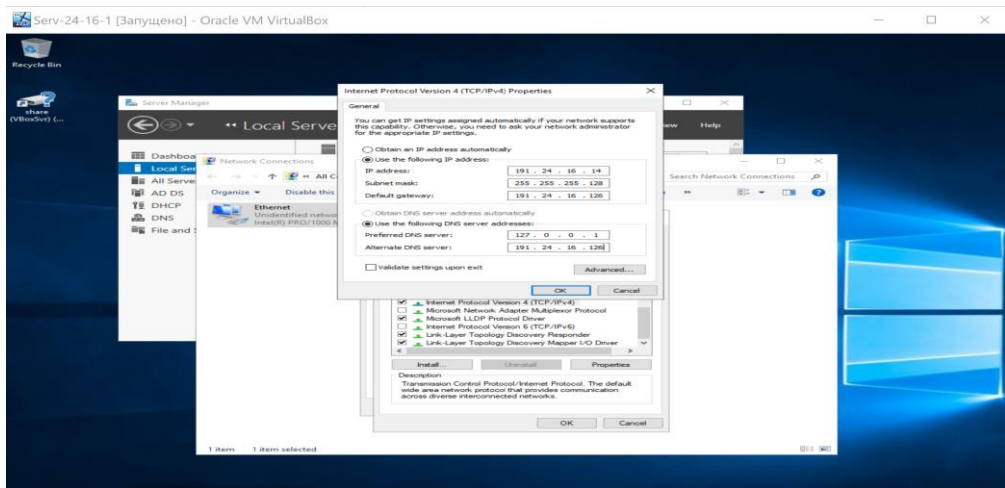


Рисунок 4.11 – Налаштування адресації на сервері (Windows Server 2019)

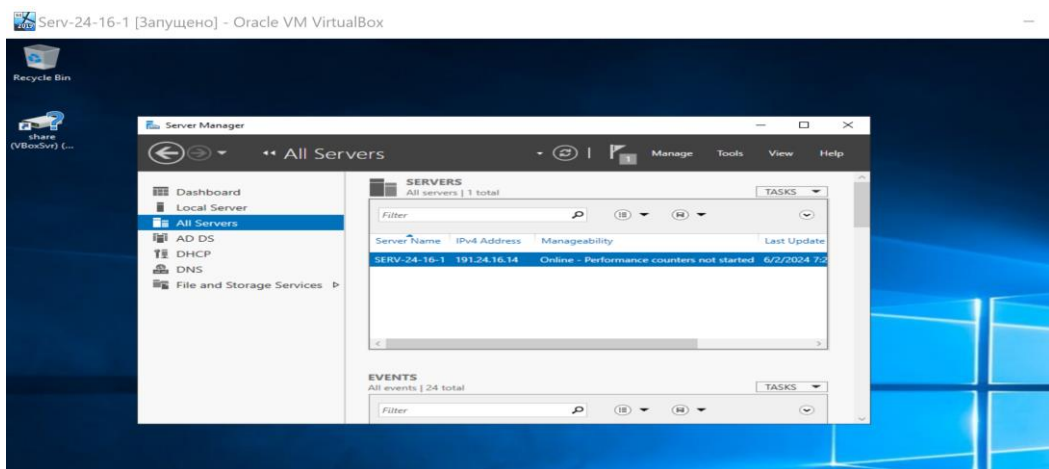


Рисунок 4.12 – Перевірка налаштування адресації на сервері (Windows Server 2019)

Також звернемо увагу на активацію DNS на Serv-24-16-1 (рис. 4.13-14).

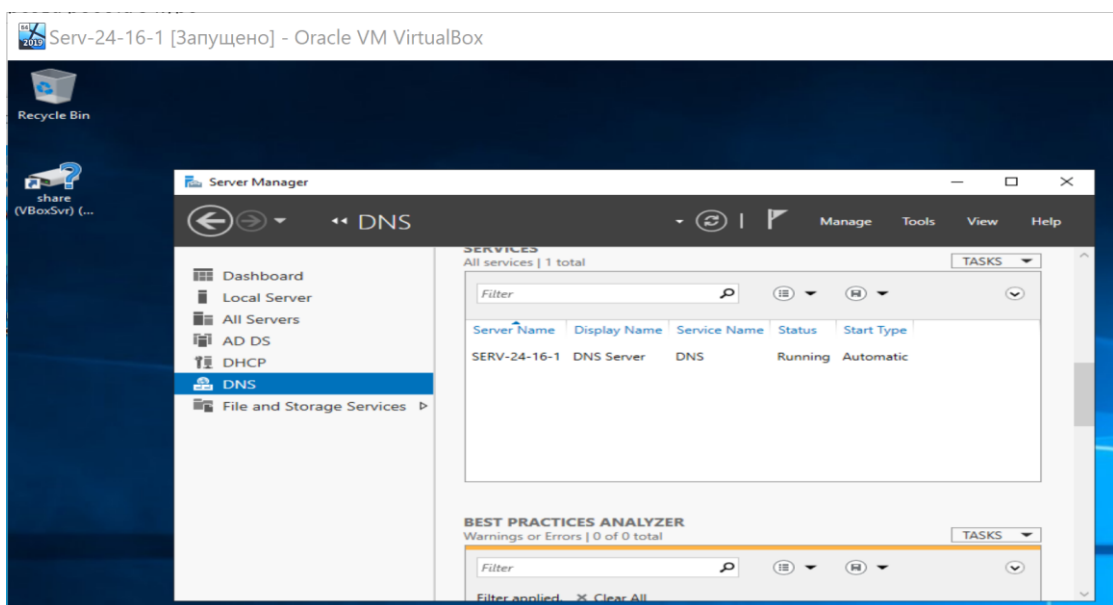


Рисунок 4.13 – Активація сервісу

		Присяжнюк Я.В.			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк. 52
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		

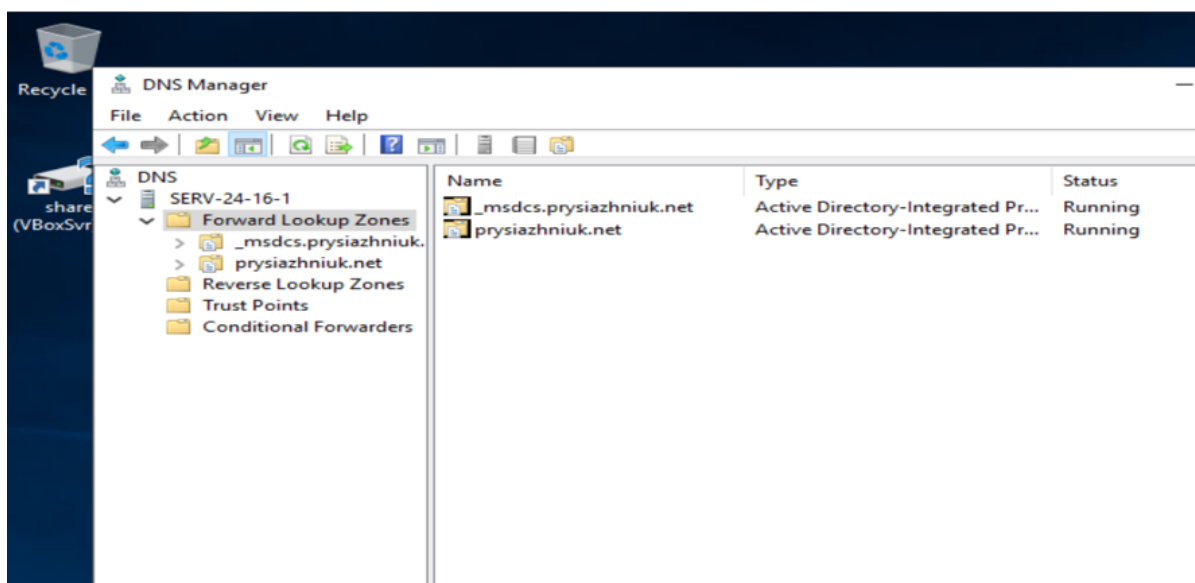


Рисунок 4.14 – Перевірка налаштувань

Проведемо налаштування адресації для робочих станцій (рис.4.15-16)

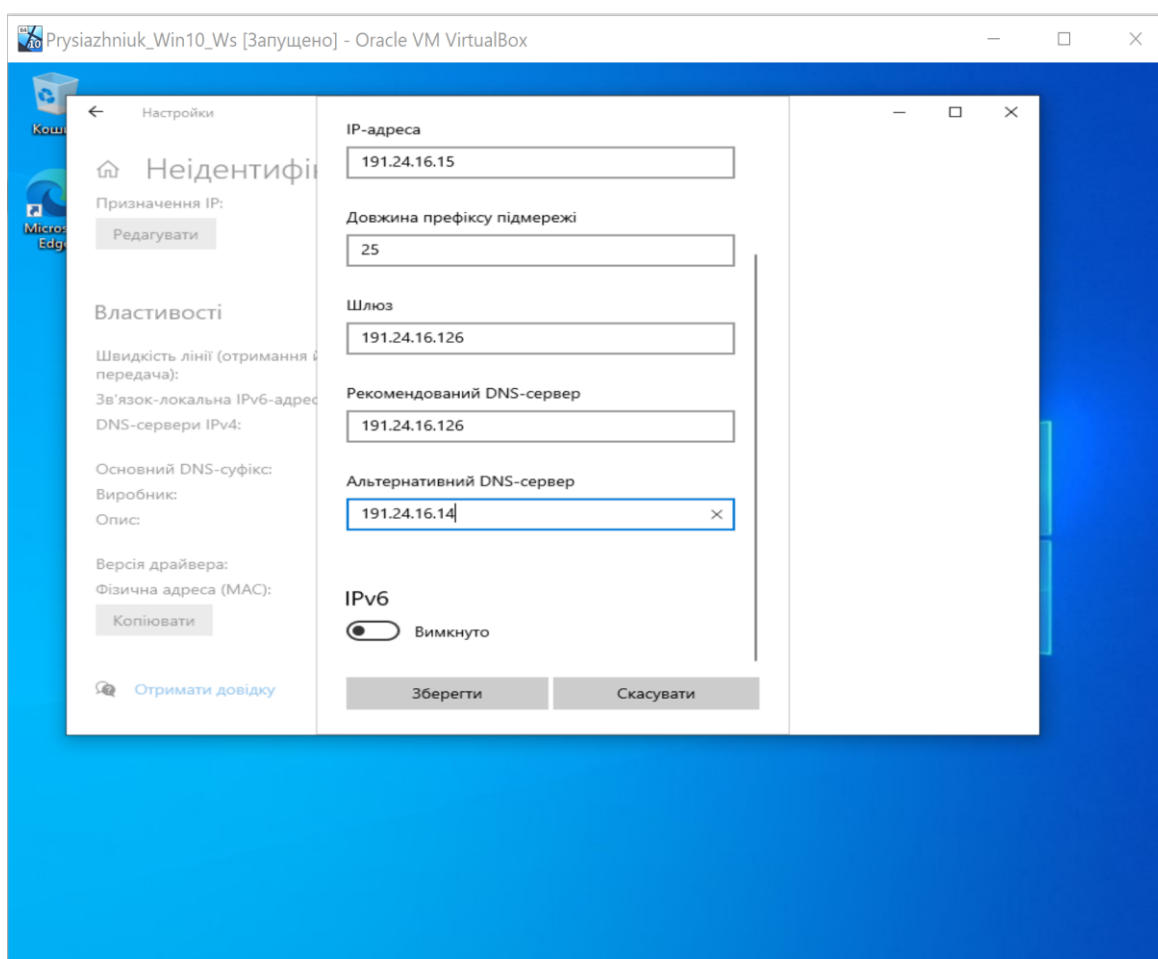


Рисунок 4.15 – Налаштування адресації на робочій станції (Windows 10)

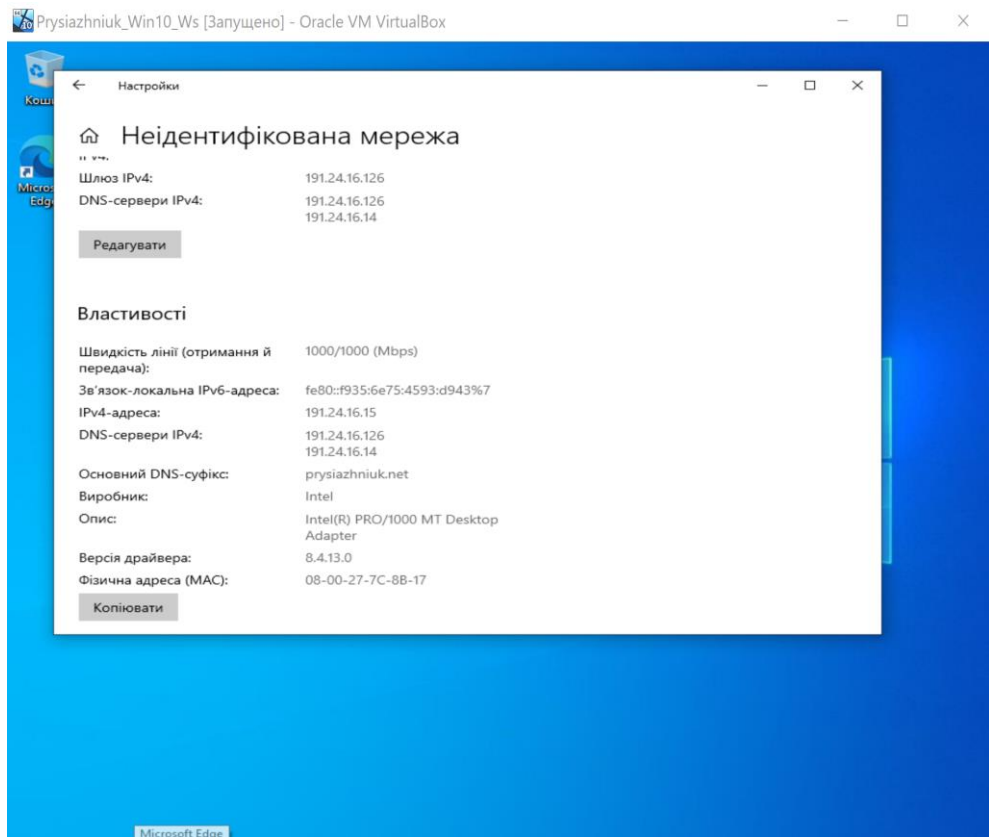


Рисунок 4.16 – Перевірка налаштування адресації на робочій станції (Windows 10)

Наступним кроком необхідно забезпечити кінцеві пристрої динамічним отримання IP-адресації. Для цього, в кожній підмережі необхідно налаштувати DHCP-сервер. В розробленій мережі ми будемо налаштовувати DHCP-pool на маршрутизаторі R-24-16-1 (рис.4.17).

```
R-24-16-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R-24-16-1(config)#ip dhcp excluded-address 191.24.16.1 191.24.16.10
^
% Invalid input detected at '^' marker.

R-24-16-1(config)#ip dhcp excluded-address 191.24.16.1 191.24.16.10
R-24-16-1(config)#ip dhcp excluded-address 191.24.16.12 191.24.16.15
R-24-16-1(config)#ip dhcp excluded-address 191.24.16.126
R-24-16-1(config)#ip dhcp pool MY-LAN
R-24-16-1(dhcp-config)#default-router 191.24.16.126
R-24-16-1(dhcp-config)#dns-server 191.24.16.14
R-24-16-1(dhcp-config)#exit
R-24-16-1(config)#exit
R-24-16-1#
```

Рисунок 4.17 – Налаштування DHCP-pool на маршрутизаторі

Перевіримо як робочої станції (кінцеві пристрої) отримують ір-адресу (рис.4.18-19).

		Присяжнюк Я.В.			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				54
Змн.	Арк.	№ докум.	Підпис	Дата		

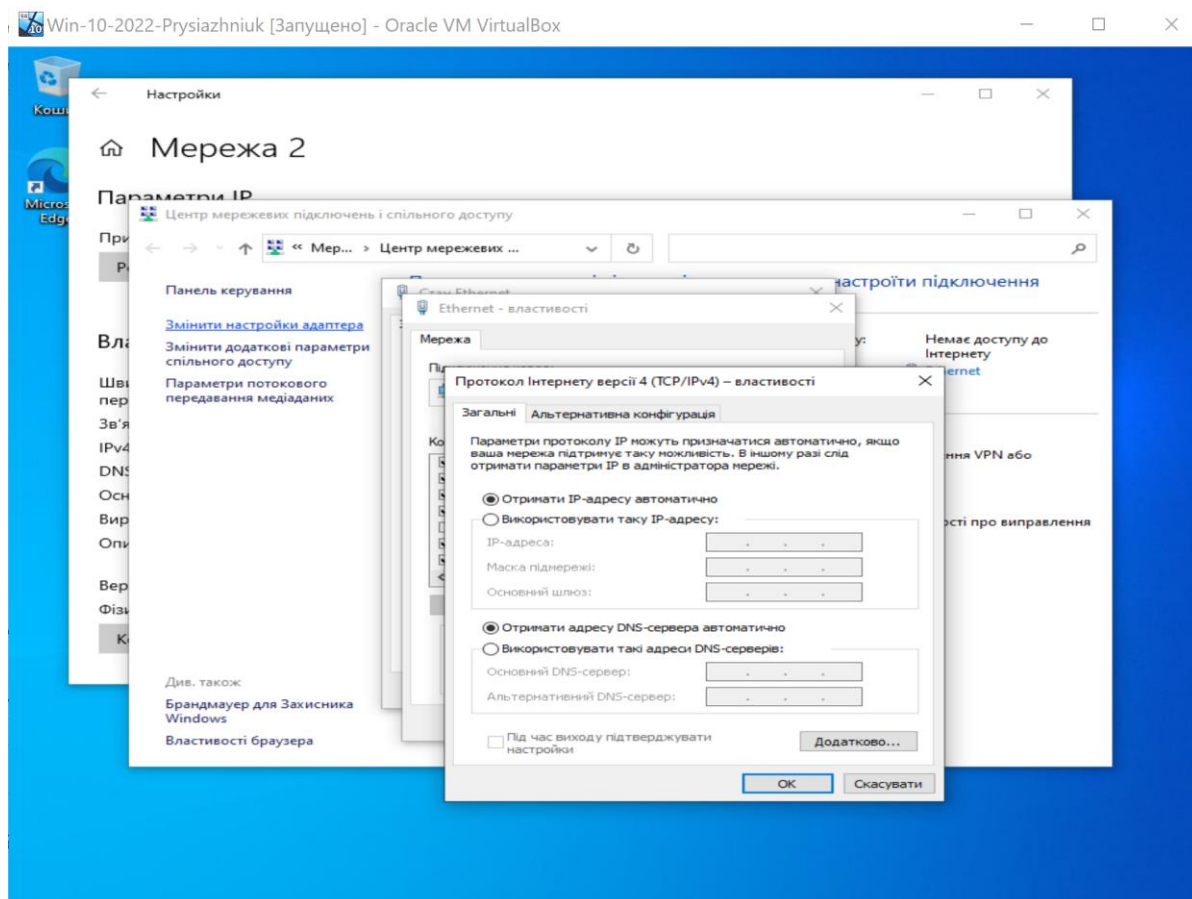


Рисунок 4.18 – Динамічне отримання ір-адреси на робочій станції



Рисунок 4.19 – Перевірка налаштувань на робочій станції

Перевіримо зв'язок між щойно налаштованими пристроями (рис.4.20-23).

		Присяжнюк Я.В.			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз С.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		55

```
Prysiazhniuk_Win10_Ws [Запущено] - Oracle VM VirtualBox
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Student> ping 191.24.16.7
Ping 191.24.16.7 with 32 bytes of data:
Reply from 191.24.16.7: bytes=32 time=3ms TTL=255
Reply from 191.24.16.7: bytes=32 time=2ms TTL=255
Reply from 191.24.16.7: bytes=32 time=2ms TTL=255
Reply from 191.24.16.7: bytes=32 time=2ms TTL=255
Ping statistics for 191.24.16.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 3ms, Average = 2ms
PS C:\Users\Student> ping 191.24.16.4
Ping 191.24.16.4 with 32 bytes of data:
Reply from 191.24.16.4: bytes=32 time=2ms TTL=255
Reply from 191.24.16.4: bytes=32 time=2ms TTL=255
Reply from 191.24.16.4: bytes=32 time=2ms TTL=255
Reply from 191.24.16.4: bytes=32 time=3ms TTL=255
Ping statistics for 191.24.16.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 3ms, Average = 2ms
PS C:\Users\Student> ping 191.24.16.3
Ping 191.24.16.3 with 32 bytes of data:
Reply from 191.24.16.3: bytes=32 time=3ms TTL=255
Reply from 191.24.16.3: bytes=32 time=3ms TTL=255
Reply from 191.24.16.3: bytes=32 time=1ms TTL=255
Reply from 191.24.16.3: bytes=32 time=6ms TTL=255
Ping statistics for 191.24.16.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 6ms, Average = 3ms
```

Рисунок 4.20 – Перевірка зв'язку між пристроями однієї підмережі

```
Prysiazhniuk_Win10_Ws [Запущено] - Oracle VM VirtualBox
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Student> ping 191.24.16.8
Ping 191.24.16.8 with 32 bytes of data:
Reply from 191.24.16.8: bytes=32 time=2ms TTL=255
Reply from 191.24.16.8: bytes=32 time=1ms TTL=255
Reply from 191.24.16.8: bytes=32 time=5ms TTL=255
Reply from 191.24.16.8: bytes=32 time=2ms TTL=255
Ping statistics for 191.24.16.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 5ms, Average = 2ms
PS C:\Users\Student> ping 191.24.16.10
Ping 191.24.16.10 with 32 bytes of data:
Reply from 191.24.16.10: bytes=32 time=5ms TTL=255
Reply from 191.24.16.10: bytes=32 time=5ms TTL=255
Reply from 191.24.16.10: bytes=32 time=5ms TTL=255
Reply from 191.24.16.10: bytes=32 time=5ms TTL=255
Ping statistics for 191.24.16.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 5ms, Maximum = 5ms, Average = 5ms
PS C:\Users\Student> ping 191.24.16.1
Ping 191.24.16.1 with 32 bytes of data:
Reply from 191.24.16.1: bytes=32 time=6ms TTL=255
Reply from 191.24.16.1: bytes=32 time=1ms TTL=255
Reply from 191.24.16.1: bytes=32 time=4ms TTL=255
Reply from 191.24.16.1: bytes=32 time=1ms TTL=255
Ping statistics for 191.24.16.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 6ms, Average = 3ms
PS C:\Users\Student> ping 191.24.16.2
```

Рисунок 4.21 – Перевірка зв'язку між пристроями однієї підмережі

```
Prysiazhniuk_Win10_Ws [Запущено] - Oracle VM VirtualBox
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Student> ping 191.24.16.2
Ping 191.24.16.2 with 32 bytes of data:
Reply from 191.24.16.2: bytes=32 time=6ms TTL=255
Reply from 191.24.16.2: bytes=32 time=15ms TTL=255
Reply from 191.24.16.2: bytes=32 time=1ms TTL=255
Reply from 191.24.16.2: bytes=32 time=3ms TTL=255
Ping statistics for 191.24.16.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 15ms, Average = 6ms
PS C:\Users\Student> ping 191.24.16.6
Ping 191.24.16.6 with 32 bytes of data:
Reply from 191.24.16.15: Destination host unreachable.
Reply from 191.24.16.15: Destination host unreachable.
Reply from 191.24.16.15: Destination host unreachable.
Reply from 191.24.16.15: Destination host unreachable.
Ping statistics for 191.24.16.6:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\Users\Student> ping 191.24.16.6
Ping 191.24.16.6 with 32 bytes of data:
Reply from 191.24.16.6: bytes=32 time=4ms TTL=255
Reply from 191.24.16.6: bytes=32 time=1ms TTL=255
Reply from 191.24.16.6: bytes=32 time=1ms TTL=255
Reply from 191.24.16.6: bytes=32 time=1ms TTL=255
Ping statistics for 191.24.16.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 4ms, Average = 1ms
PS C:\Users\Student>
```

Рисунок 4.22 – Перевірка зв'язку між пристроями однієї підмережі

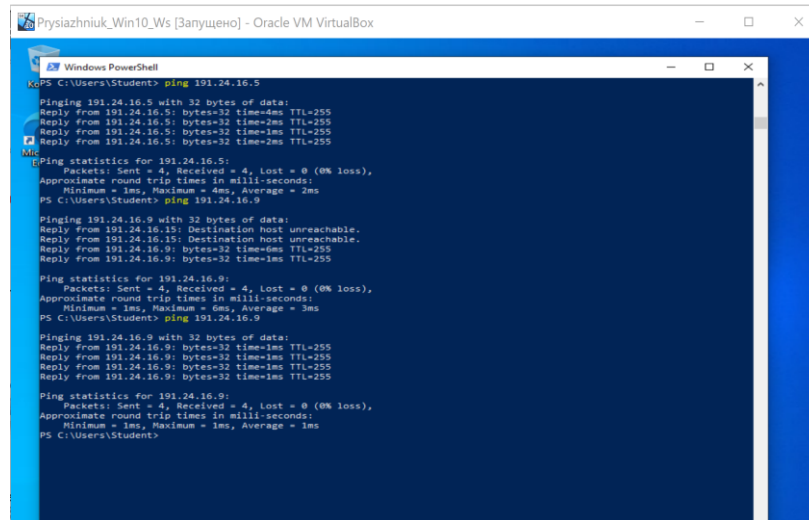


Рисунок 4.23 – Перевірка зв'язку між пристроями однієї підмережі

Наступним кроком буде налаштування зв'язку між різними підмережами. Налаштування маршрутизації виконано за допомогою динамічного протоколу маршрутизації OSPF (рис.4.24-25) та перевірка коректності цих налаштувань (рис.4.26-28).

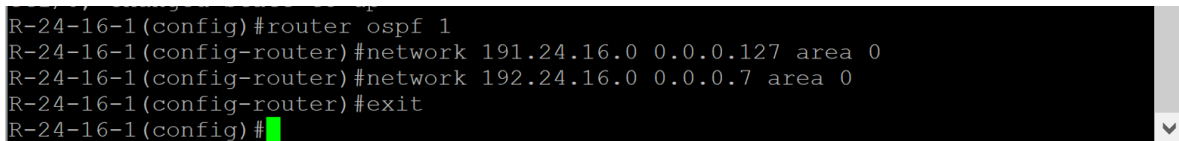


Рисунок 4.24 – Налаштування протоколу OSPF на маршрутизаторі

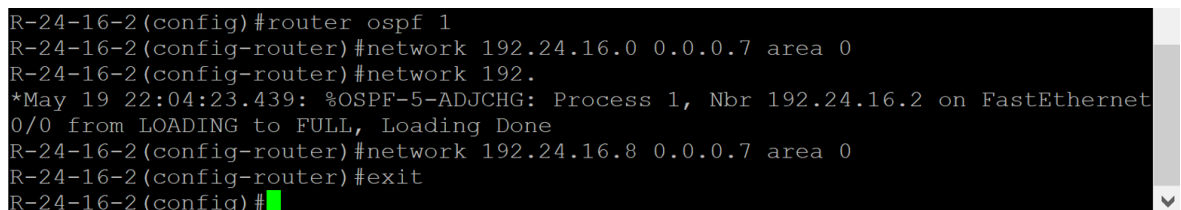


Рисунок 4.25 – Налаштування протоколу OSPF на маршрутизаторі
Перевіримо зв'язок між пристроями віддалених підмереж.

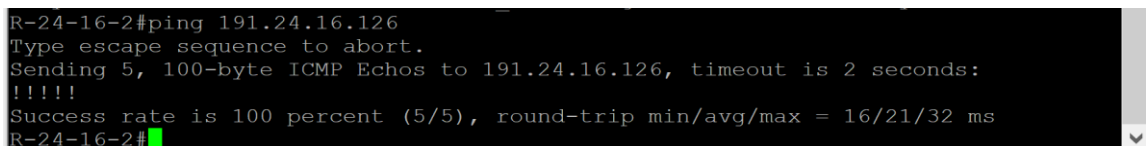


Рисунок 4.26 – Перевірка зв'язку між пристроями різних підмережі

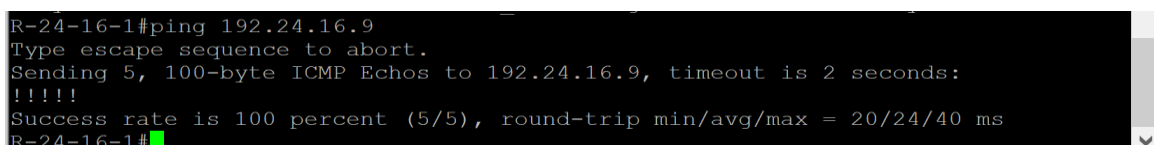


Рисунок 4.27 – Перевірка зв'язку між пристроями різних підмережі

		Присяжнюк Я.В.			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				57
Змн.	Арк.	№ докум.	Підпис	Дата		

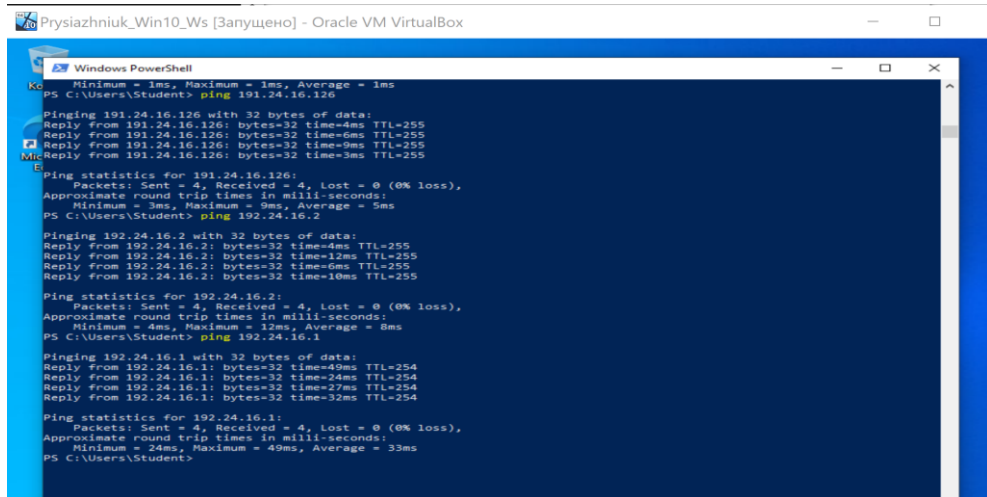


Рисунок 4.28 – Перевірка зв'язку між пристроями різних підмережі

Налагодимо агреговані канали (статична агрегація)

```
SW-24-16-4#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-24-16-4(config)#int port-channel 3
SW-24-16-4(config-if)#description AGGREGATED-LINK-TO-SW-24-16-3
SW-24-16-4(config-if)#exit
SW-24-16-4(config)#int range eth0/0, eth0/1
SW-24-16-4(config-if-range)#channel-group 3 mode on
SW-24-16-4(config-if-range)#exit
SW-24-16-4(config)#
*May 26 17:51:24.462: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel3, changed state to up
SW-24-16-4(config)#port-channel load-balance src-dst-mac
SW-24-16-4(config)#ip default-gateway 191.24.16.126
SW-24-16-4(config)#no ip domain-lookup
SW-24-16-4(config)#int port-channel 4
SW-24-16-4(config-if)#description AGGREGATED-LINK-TO-SW-24-16-2
SW-24-16-4(config-if)#exit
SW-24-16-4(config)#int range eth0/2, eth0/3
SW-24-16-4(config-if-range)#channel-group 4 mode on
SW-24-16-4(config-if-range)#exit
SW-24-16-4(config)#
*May 26 17:53:17.199: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel4, changed state to up
SW-24-16-4(config)#
```

Рисунок 4.29 – Типове налаштування комутатора

Наступним кроком буде налагодження протоколу RPVST на комутаторах. Розпочнемо з активації даного протоколу на комутаторах (рис.4.30).

```
SW-24-16-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-24-16-1(config)#spanning-tree mode rapid-pvst
SW-24-16-1(config)#ex
% Ambiguous command: "ex"
SW-24-16-1(config)#exit
SW-24-16-1#
*May 26 18:01:18.696: %SYS-5-CONFIG_I: Configured from console by console
SW-24-16-1#
```

Рисунок 4.30 – Типове налаштування комутатора

Далі встановимо пріоритети відповідно до ролей комутаторів (рис.4.31-34).

		Присяжнюк Я.В.			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				58
Змн.	Арк.	№ докум.	Підпис	Дата		

```
SW-24-16-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-24-16-1(config)#spanning-tree vlan 1 root primary
SW-24-16-1(config)#spanning-tree vlan 1 priority 28672
SW-24-16-1(config)#exit
SW-24-16-1#
```

Рисунок 4.31 – Налаштування для первинного комутатора

```
SW-24-16-2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-24-16-2(config)#spanning-tree vlan 1 root secondary
SW-24-16-2(config)#spanning-tree vlan 1 priority 36864
SW-24-16-2(config)#exit
SW-24-16-2#
```

Рисунок 4.32 – Налаштування для вторинного комутатора

```
SW-24-16-3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-24-16-3(config)#spanning-tree vlan 1 priority 45056
SW-24-16-3(config)#exit
SW-24-16-3#
```

```
SW-24-16-4#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-24-16-4(config)#spanning-tree vlan 1 priority 45056
SW-24-16-4(config)#exit
SW-24-16-4#
```

Рисунок 4.33-34 – Зміни пріоритетів для інших комутаторів

Після базової підготовки проєкту мережі переходимо до налаштувань SSH[7]. Почнемо з мережних пристроїв (рис.4.35).

Сценарій налагодження віддаленого підключення за протоколом SSH до маршрутизатора Cisco з використанням імені пристрою та імені домену та з використанням засобів локальної аутентифікації на базі механізму користувачів наведений нижче. У цьому сценарії застосовані паролі типу 5.

```
SW-24-16-7#OO
SW-24-16-7#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-24-16-7(config)#username Yasya privilege 15 secret adminerpass
SW-24-16-7(config)#username Technic privilege 1 secret technicpass
SW-24-16-7(config)#enable secret enablepass
SW-24-16-7(config)#ip domain-name prysiazhniuk.net
SW-24-16-7(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: SW-24-16-7.prysiazhniuk.net

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)

SW-24-16-7(config)#
*May 29 10:10:39.503: %SSH-5-ENABLED: SSH 1.99 has been enabled
SW-24-16-7(config)#ip ssh version 2
SW-24-16-7(config)#line vty 0 4
SW-24-16-7(config-line)#login local
SW-24-16-7(config-line)#transport input ssh
SW-24-16-7(config-line)#transport output ssh
SW-24-16-7(config-line)#logout-warning 30
SW-24-16-7(config-line)#absolute-timeout 10
SW-24-16-7(config-line)#logging synchronous
SW-24-16-7(config-line)#exit
SW-24-16-7(config)#exit
SW-24-16-7#
```

Рисунок 4.35 – Типове налаштування комутатора

Сценарій налагодження елементів захисту від атак на пристрій та налагодження підсистеми журналювання подій, пов'язаних із вдалими та невдалими спробами SSH-підключень (рис.4.36).

		Присяжнюк Я.В.			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				59
Змн.	Арк.	№ докум.	Підпис	Дата		

```

SW-24-16-7#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-24-16-7(config)#login block-for 300 attempts 3 within 3
SW-24-16-7(config)#login delay 5
SW-24-16-7(config)#login on-failure log
SW-24-16-7(config)#login on-success log
SW-24-16-7(config)#ip ssh time-out 60
SW-24-16-7(config)#ip ssh authentication-retries 5
SW-24-16-7(config)#ip ssh maxstartups 5
SW-24-16-7(config)#ip ssh logging events
SW-24-16-7(config)#exit
SW-24-16-7#
*May 29 10:13:55.361: %SYS-5-CONFIG_I: Configured from console by console
SW-24-16-7#

```

Рисунок 4.36 – Типове налаштування комутатора

По аналогії проводимо налаштування інших мережевих пристроїв. Розглянемо детально налаштування маршрутизатора (рис.4.37).

```

R-24-16-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R-24-16-1(config)#username Yasya privilege 15 secret adminerpass
R-24-16-1(config)#username Technic privilege 1 secret technicpass
R-24-16-1(config)#enable secret enablepass
R-24-16-1(config)#ip domain-name prysiazhniuk.net
R-24-16-1(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R-24-16-1.prysiazhniuk.net

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

R-24-16-1(config)#ip ssh version 2
R-24-16-1(config)#line vty 0 4
R-24-16-1(config-line)#login local
R-24-16-1(config-line)#transport input ssh
R-24-16-1(config-line)#transport output ssh
R-24-16-1(config-line)#logout-warning 30
R-24-16-1(config-line)#absolute-timeout 10
R-24-16-1(config-line)#logging synchronous
R-24-16-1(config-line)#exit
R-24-16-1(config)#login block-for 300 attempts 3 within 3
R-24-16-1(config)#login delay 5
R-24-16-1(config)#login on-failure log
R-24-16-1(config)#login on-success log
R-24-16-1(config)#ip ssh time-out 60
R-24-16-1(config)#ip ssh authentication-retries 5
R-24-16-1(config)#ip ssh maxstartups 5
R-24-16-1(config)#ip ssh logging events
R-24-16-1(config)#exit

```

Рисунок 4.37 – Типове налаштування маршрутизатора

Тепер переходимо до налаштування протоколу SSH на кінцевих пристроях. Отож розглянемо підключення з комп'ютера адміністратора до робочої станції користувача. На робочій станції потрібно встановити SSH-server та на комп'ютері адміністратора SSH-клієнт (рис.4.38-39).

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				60
Змн.	Арк.	№ докум.	Підпис	Дата		

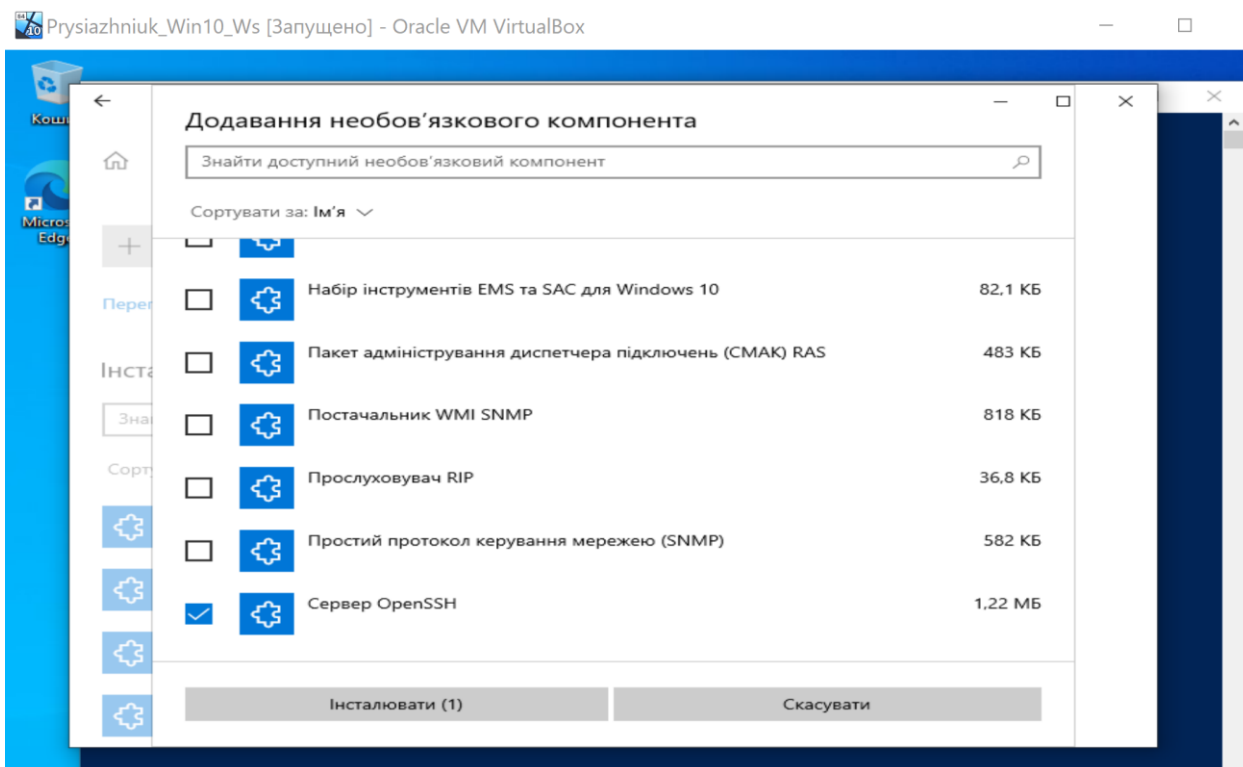


Рисунок 4.38 – Встановлюємо відповідні компоненти

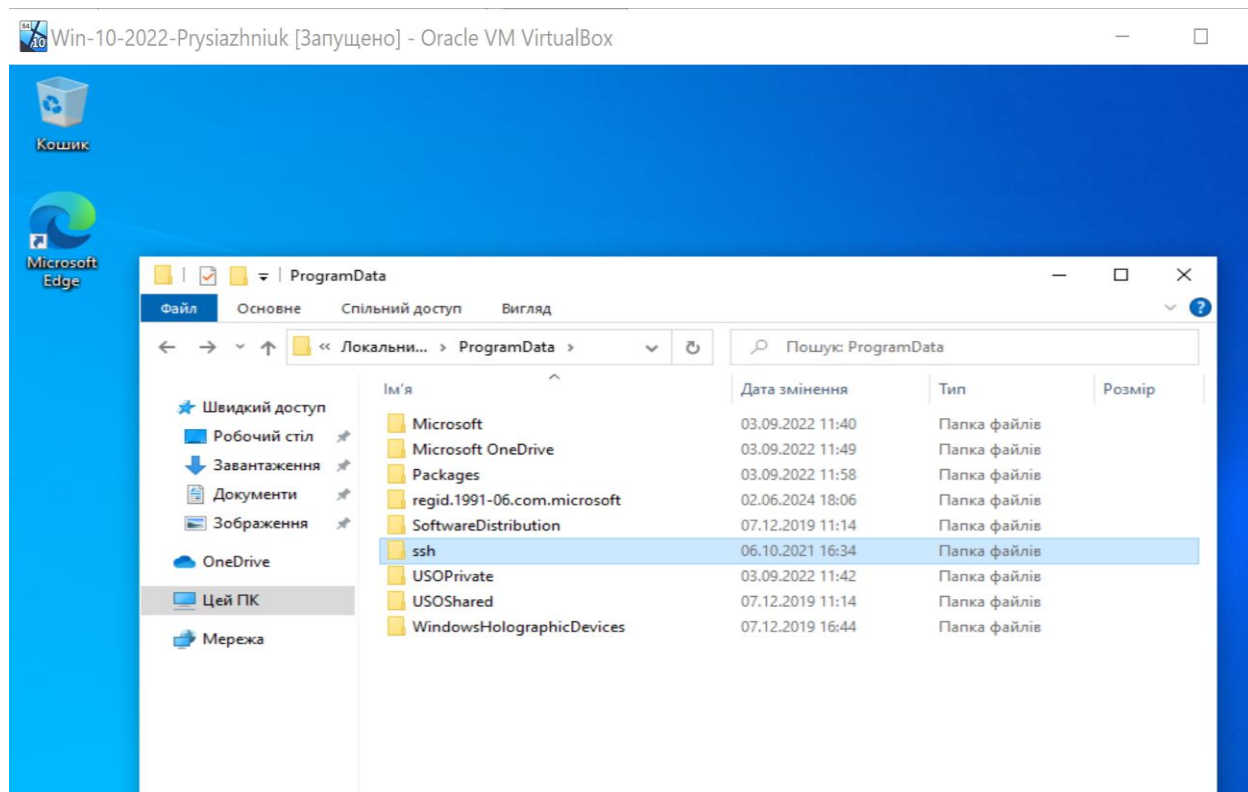


Рисунок 4.39 – Переходимо у відповідну теку, для перевірки встановлення

Далі нам треба отримати ключі. Для цього необхідно виконати кроки з рис.4.40-47.

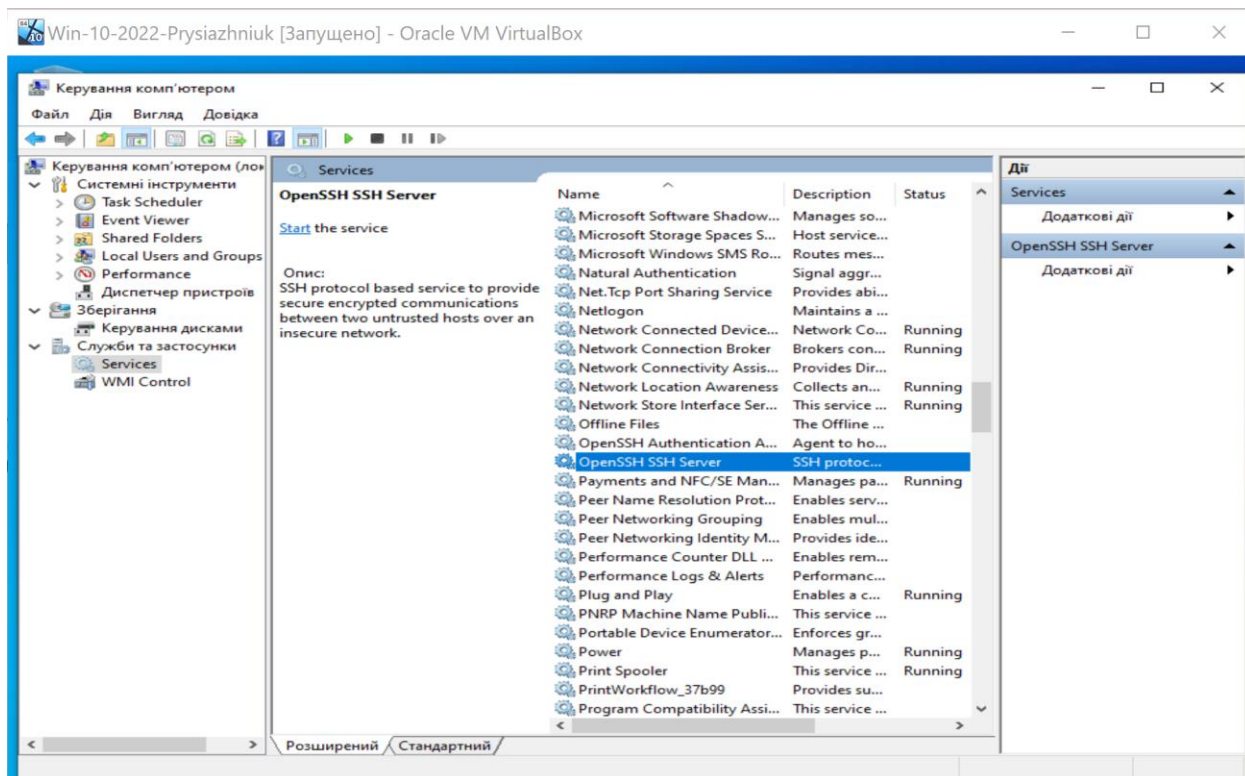


Рисунок 4.40 – Переходимо у керування комп'ютером та знаходимо відповідний сервіс

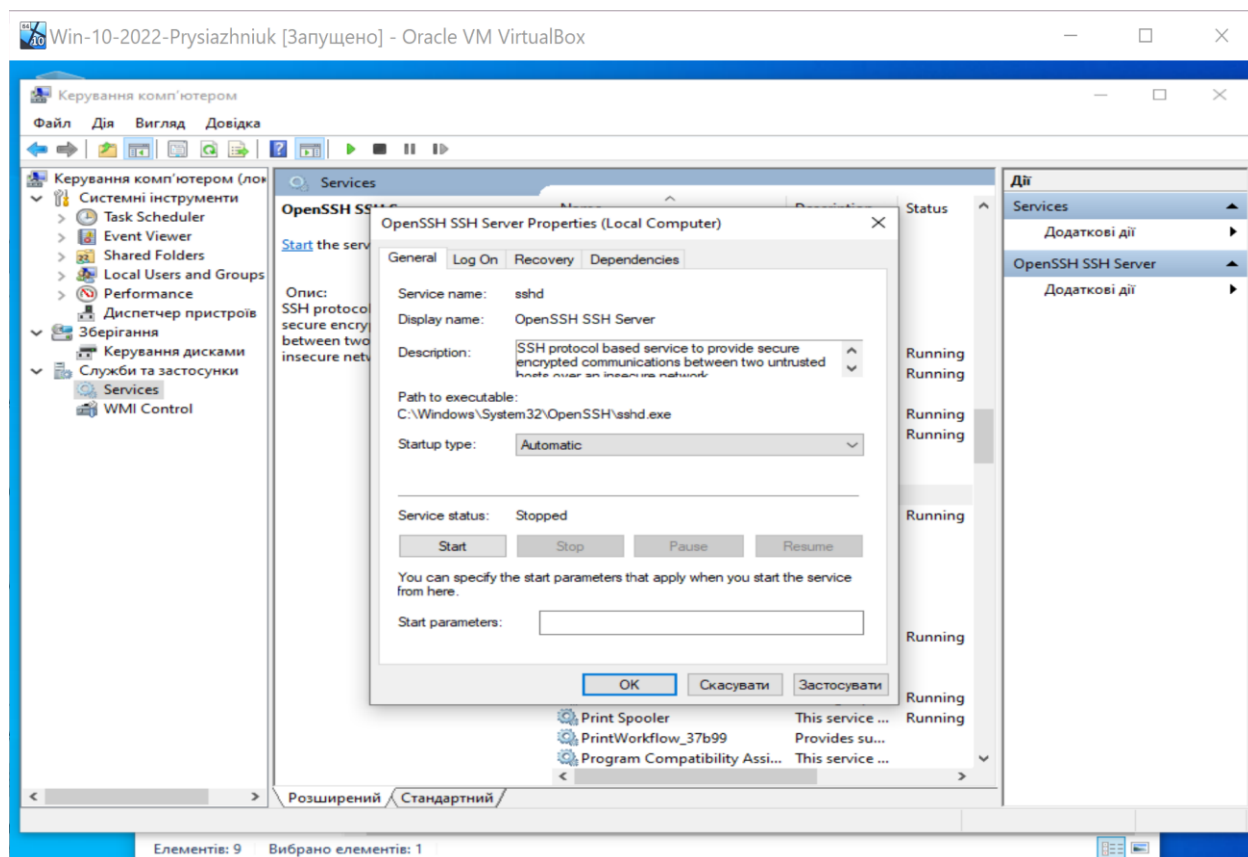


Рисунок 4.41 – Встановлюємо startup type “automatic” та натискаємо start

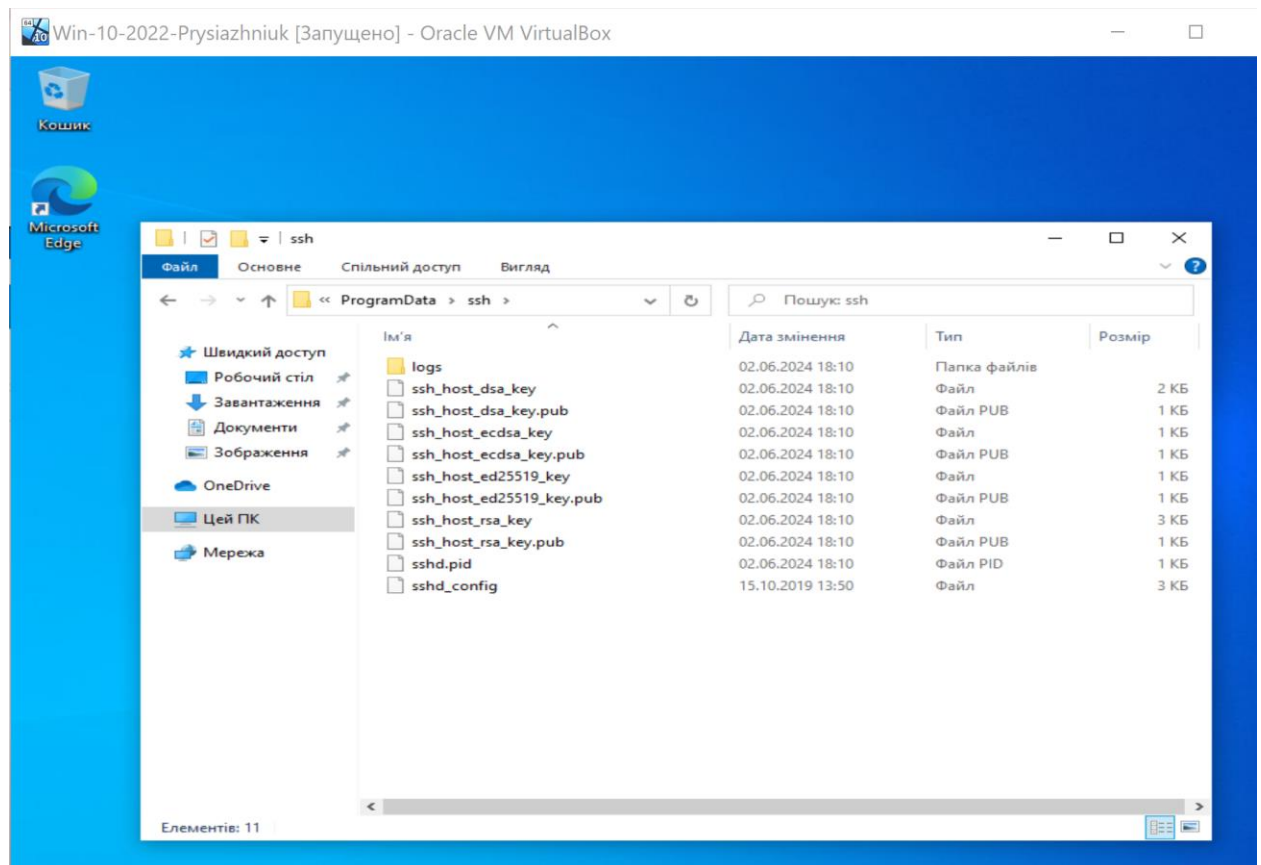


Рисунок 4.42 – Перевірка отримання ключів

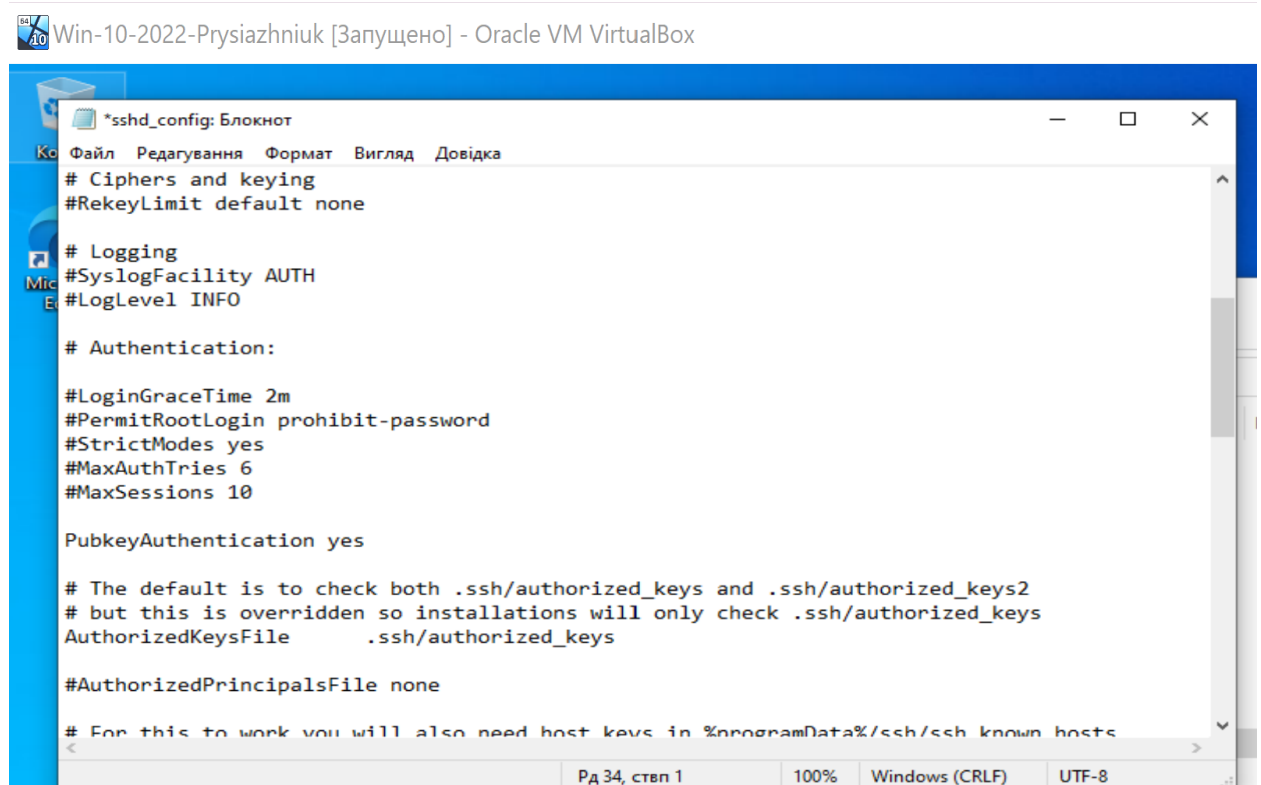


Рисунок 4.43 – Перевіряємо конфігураційний файл (PubkeyAuthentication має бути yes)

		Присяжнюк Я.В.			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз С.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		63

Всі кінцеві робочі станції мають операційну систему – Windows 10. Тому проводимо аналогічні налаштування.

Перейдемо до налаштування серверів. Операційна система для серверів, яка використовується в мережі – Windows Server 2019. Першим кроком перевіряємо чи встановлено SSH-server, як компонент системи^[7].

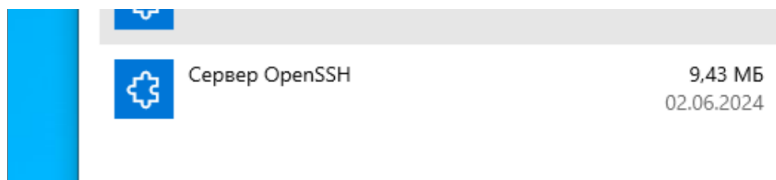


Рисунок 4.44 – Встановлюємо відповідний компонент

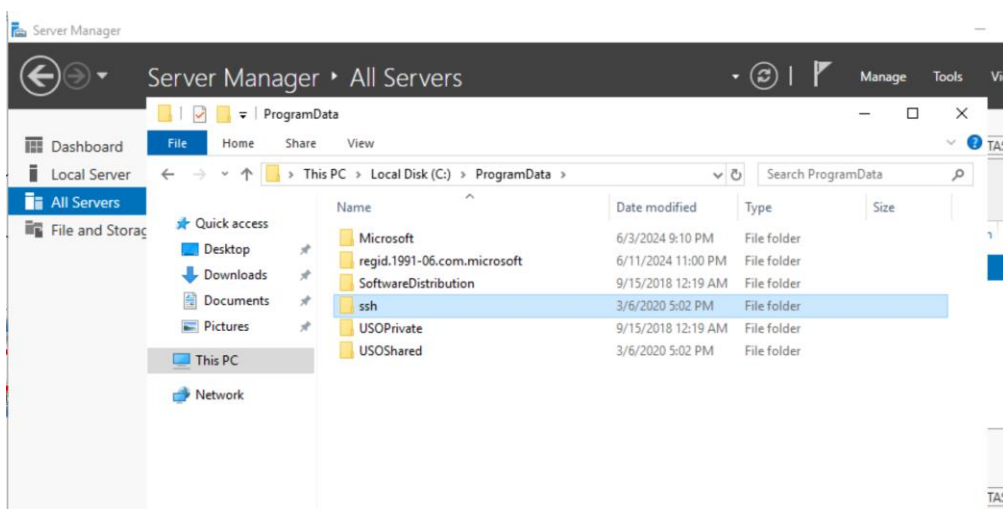


Рисунок 4.45 – Перевіряємо встановлення пакунку

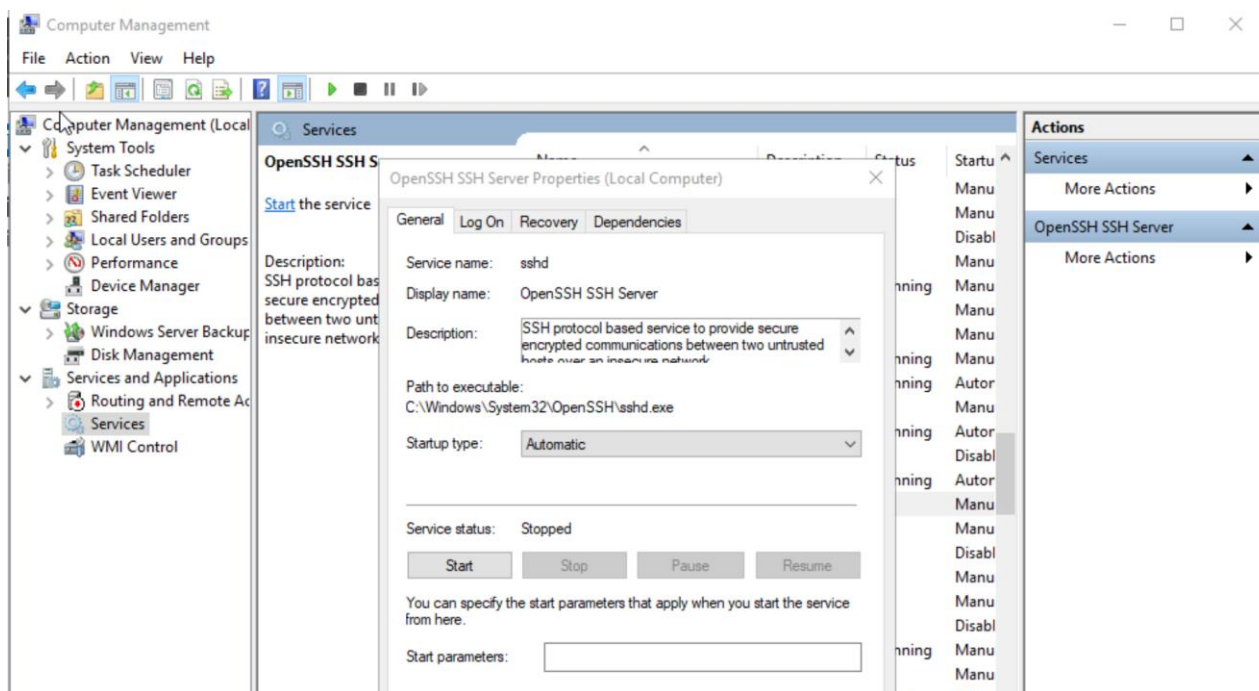


Рисунок 4.46 – Активуємо встановлений пакунок

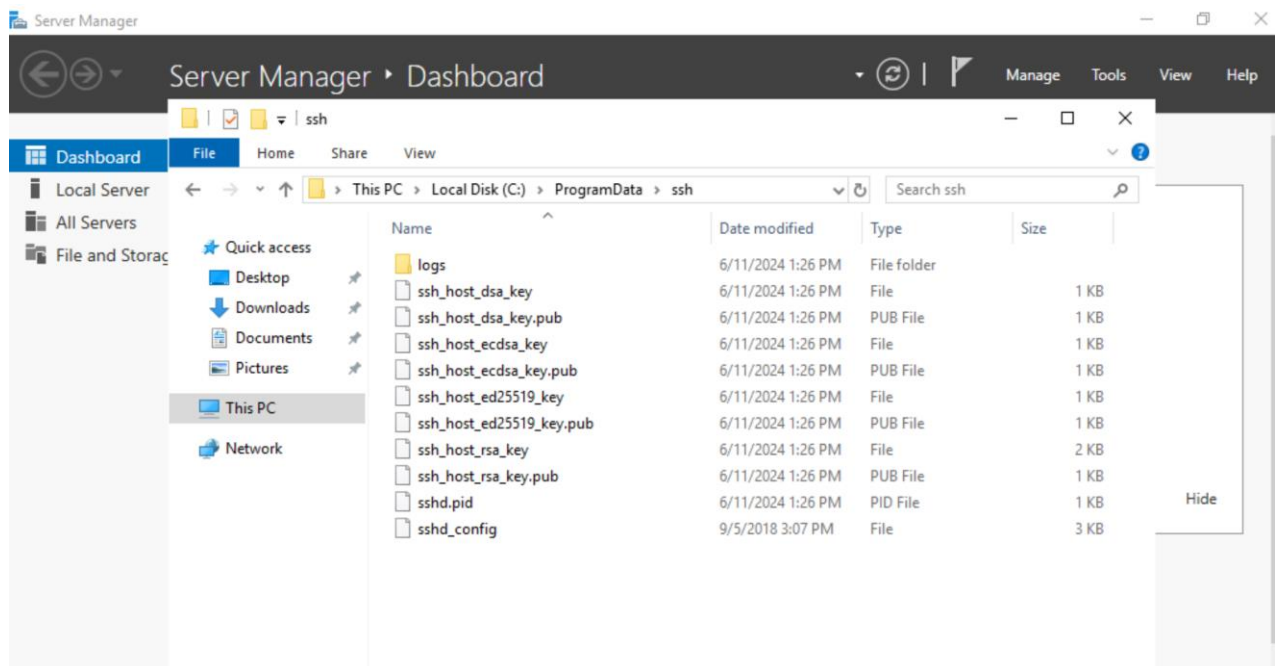


Рисунок 4.47 – Перевірка отримання ключів

Як бачимо на рис.4.48-49, ми можемо підключитися за протоколом SSH з різних робочих станцій до мережних пристроїв.

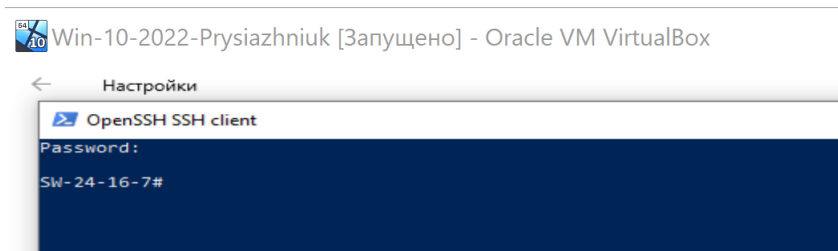


Рисунок 4.48 – Підключення по SSH до комутатора з робочої станції

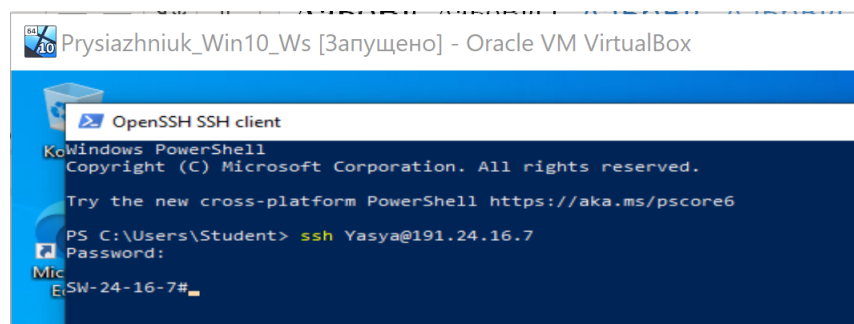


Рисунок 4.49 – Підключення по SSH до комутатора з робочої станції адміністратора

Щоб покращити безпеку мережі варто встановити списки доступу[1]. Тобто вказати ір-адреси пристроїв, які можуть виконувати таке підключення (рис.4.51).

		Присяжнюк Я.В.			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз С.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		65

```
SW-24-16-7#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-24-16-7(config)#access-list 10 permit 191.24.16.15
SW-24-16-7(config)#access-list 10 deny any
SW-24-16-7(config)#line vty 0 4
SW-24-16-7(config-line)#login local
SW-24-16-7(config-line)#transport input ssh
SW-24-16-7(config-line)#access-class 10 in
SW-24-16-7(config-line)#exit
SW-24-16-7(config)#
```

Рисунок 4.50 – Приклад створення списку доступу

Перевіримо налаштування списків доступу (рис.4.52-54).

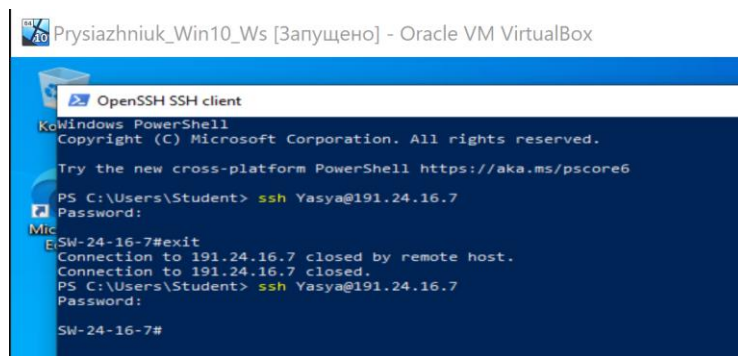


Рисунок 4.51 – Підключення з робочої станції адміністратора

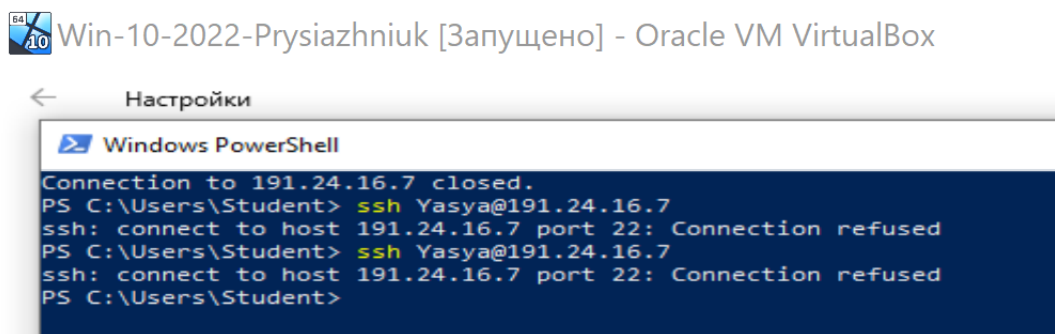


Рисунок 4.52 – Спроба підключення з робочої станції

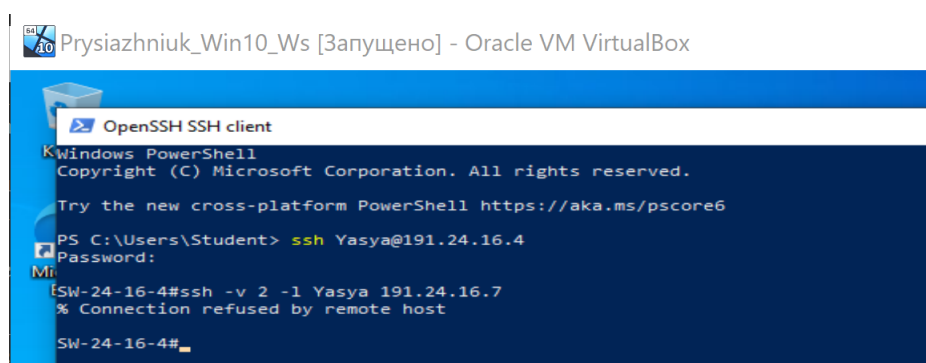


Рисунок 4.53 – Спроба підключення з іншого комутатора

Аналогічно проводимо налаштування для інших комутаторів (рис.4.54-55). Маршрутизатори налаштовуємо аналогічно. Проте варто взяти до уваги, що список дозволених ір-адрес має бути ширшим.

		Присяжнюк Я.В.			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				66
Змн.	Арк.	№ докум.	Підпис	Дата		

```

R-24-16-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R-24-16-1(config)#access-list 10 permit 191.24.16.15
R-24-16-1(config)#access-list 10 permit 191.24.16.1
R-24-16-1(config)#access-list 10 deny any
R-24-16-1(config)#line vty 0 4
R-24-16-1(config-line)#access-class 10 in
R-24-16-1(config-line)#exit
R-24-16-1(config)#

```

Рисунок 4.54 – Налаштування списку доступу для першого комутатора

```

R-24-16-2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R-24-16-2(config)#access-list 10 permit 191.24.16.15
R-24-16-2(config)#access-list 10 permit 191.24.16.126
R-24-16-2(config)#access-list 10 permit 192.24.16.2
R-24-16-2(config)#line vty 0 4
R-24-16-2(config-line)#exit
R-24-16-2(config)#access-list 10 deny any
R-24-16-2(config)#line vty 0 4
R-24-16-2(config-line)#access-class 10 in
R-24-16-2(config-line)#exit
R-24-16-2(config)#

```

Рисунок 4.55 – Налаштування списку доступу для другого комутатора

Проведемо налаштування списків доступу до серверів та робочих станцій (рис.4.56-64).

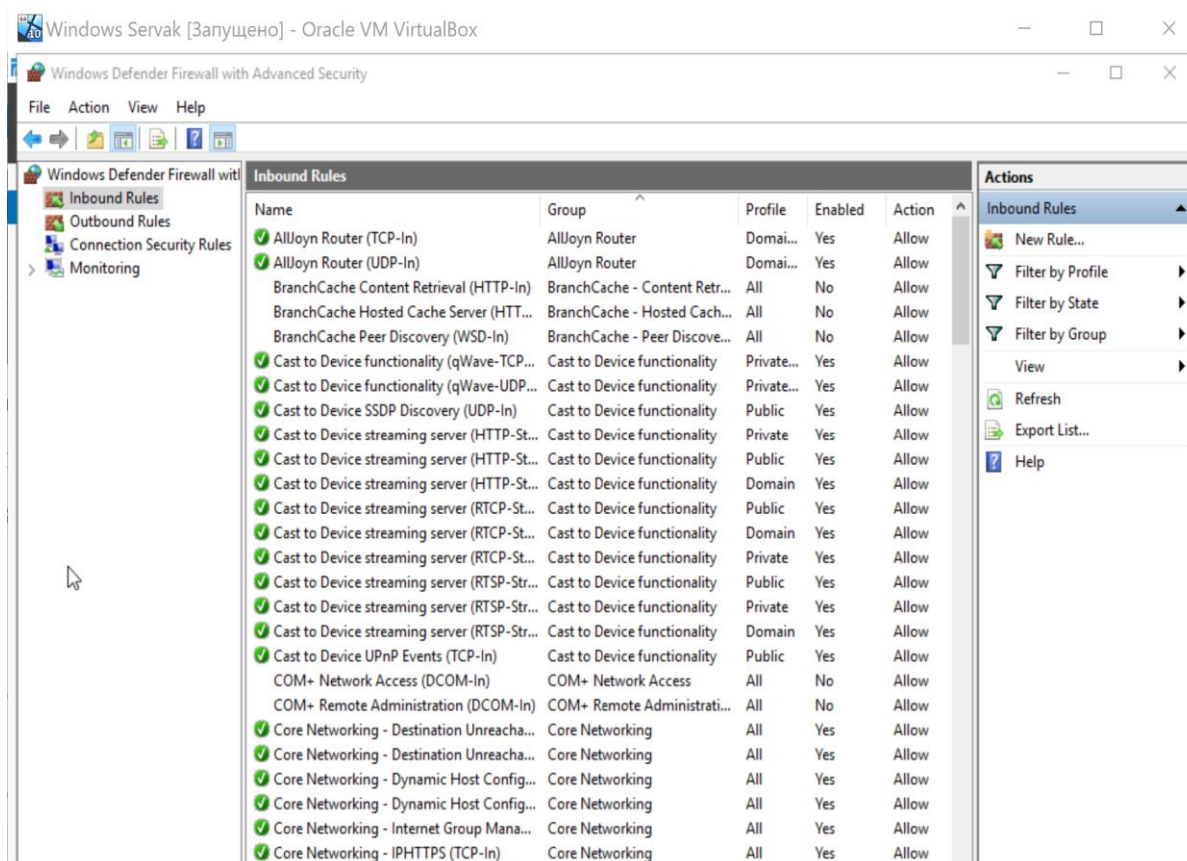


Рисунок 4.56 – Відкриваємо меню Windows Defender Firewall with Advanced Security

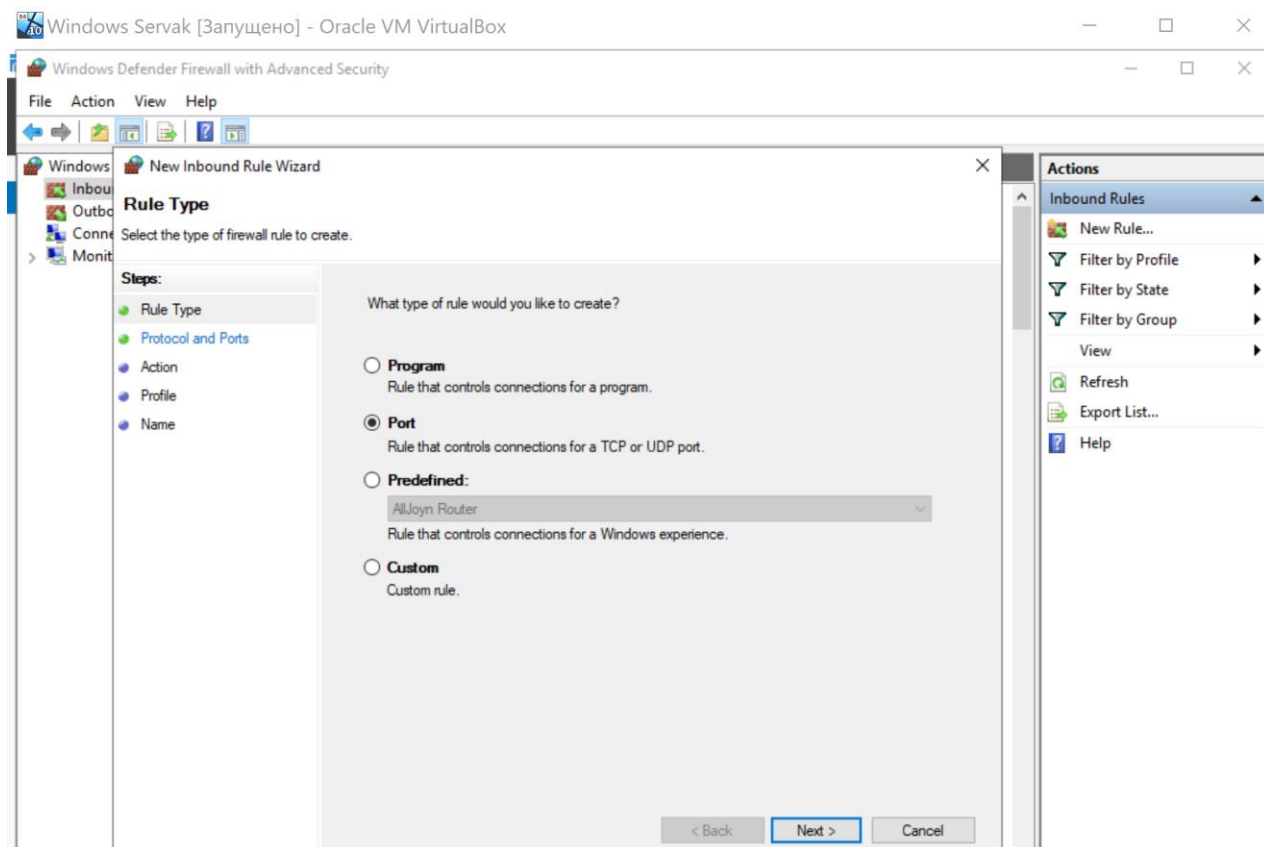


Рисунок 4.57 – Далі створюємо нове правило (port і next)

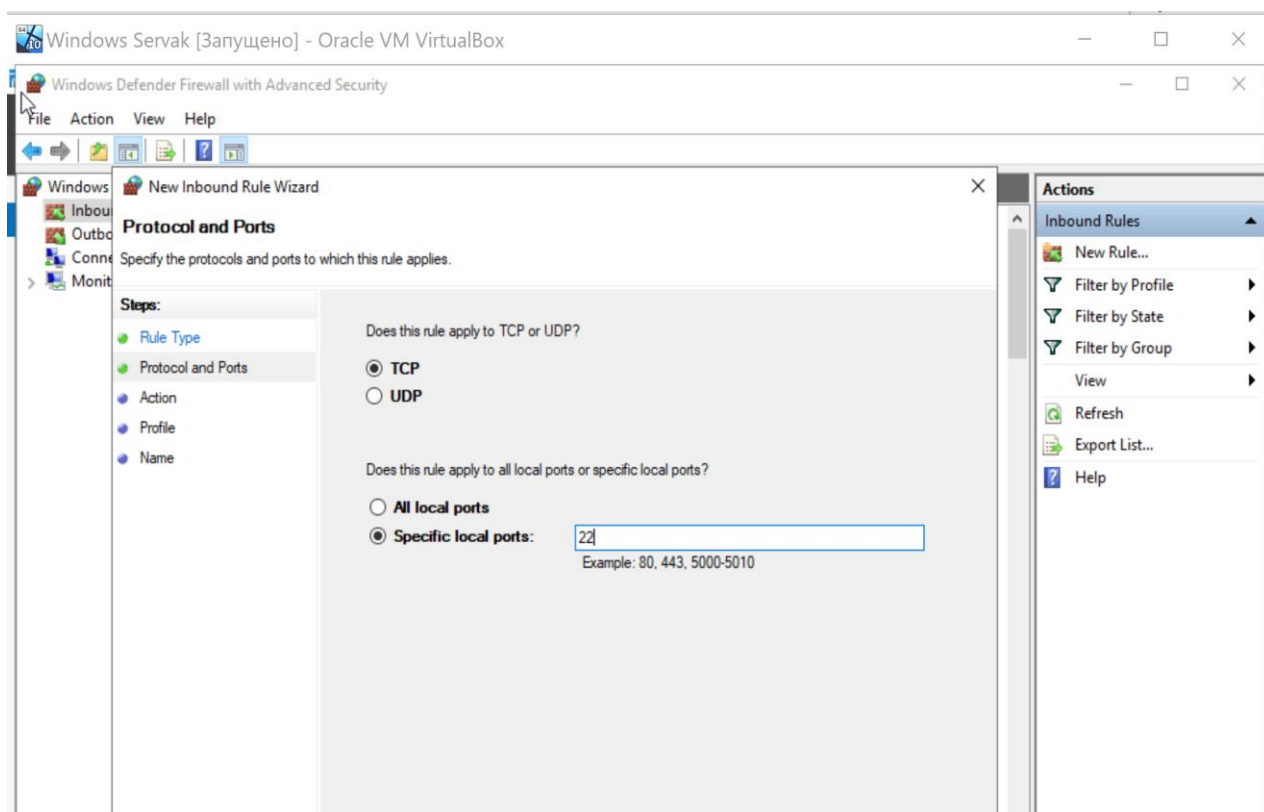


Рисунок 4.58 – Обираємо TCP та вказуємо номер порту

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		68

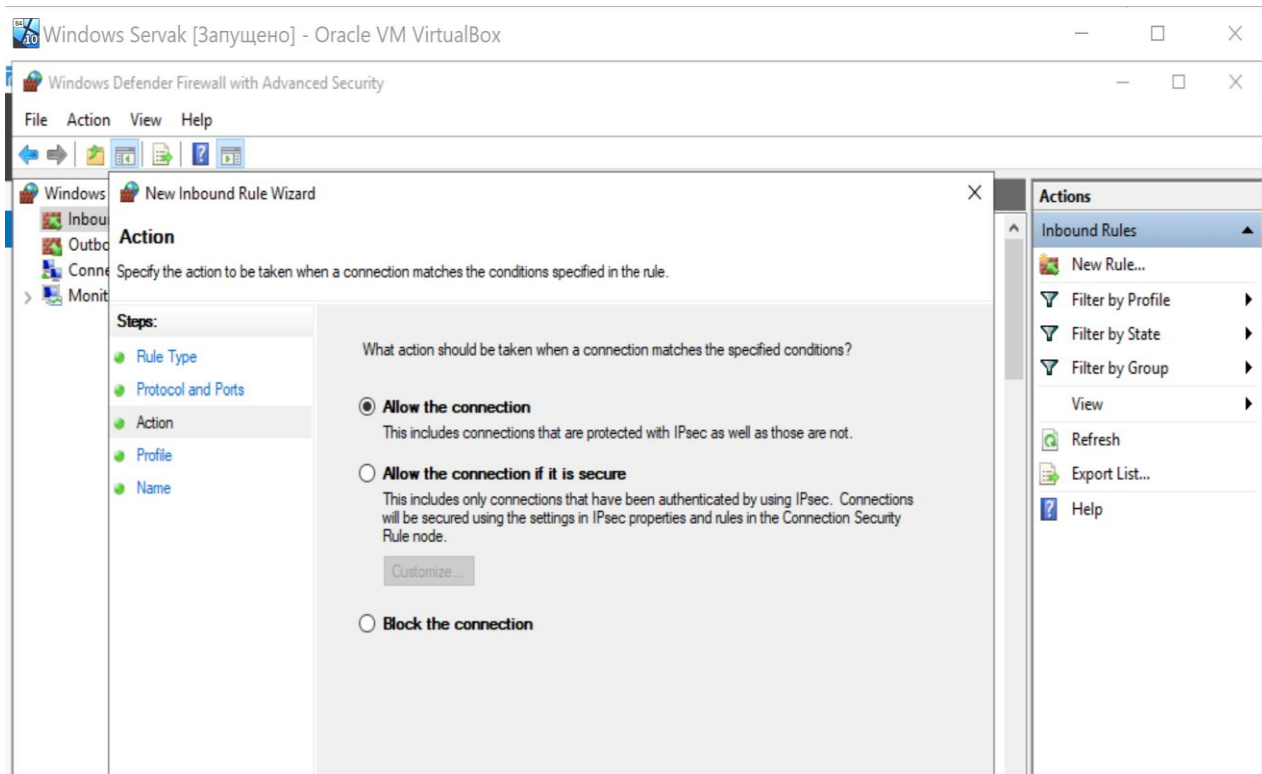


Рисунок 4.59 – Дозволяємо підключення і переходимо далі

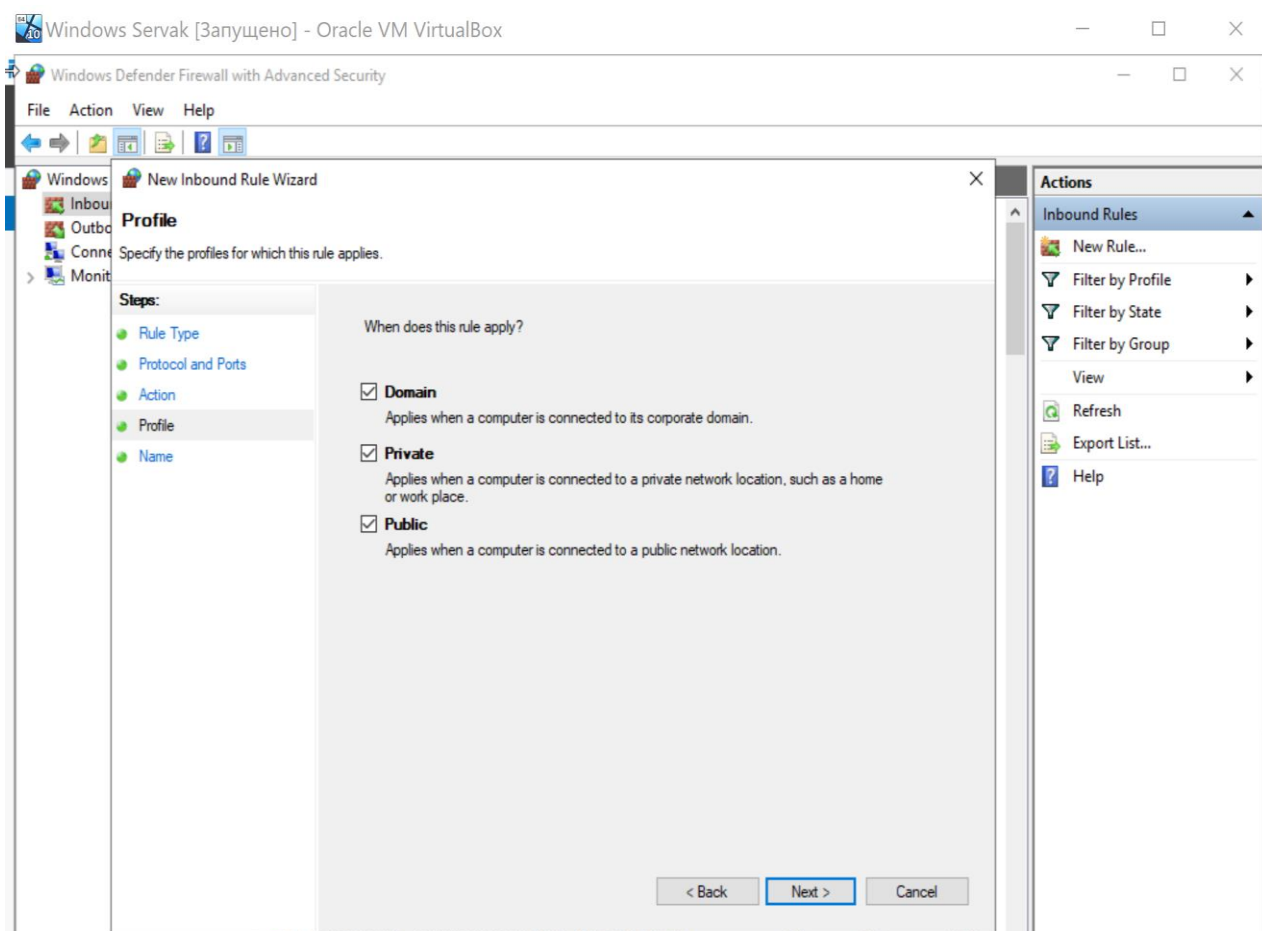


Рисунок 4.60 – Перевіряємо всі прапорці і переходимо далі

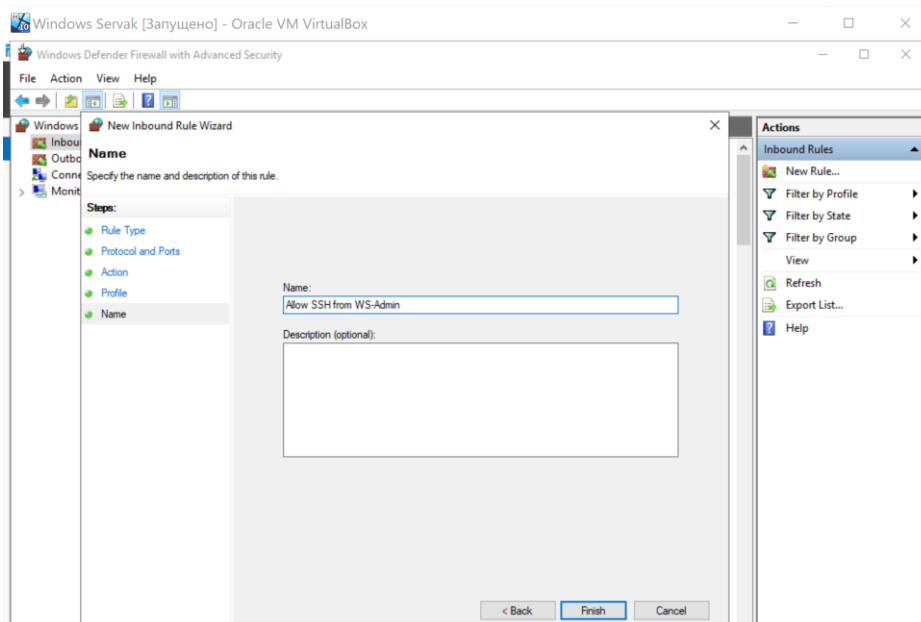


Рисунок 4.61 – Даємо назву новоствореному правилу і закінчуємо

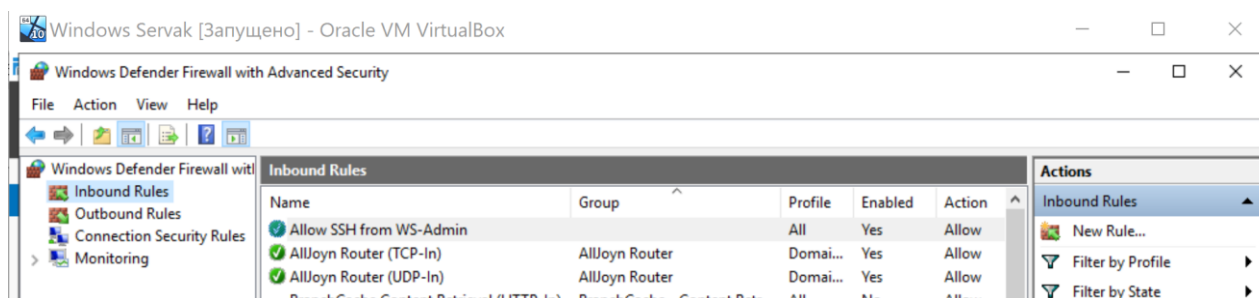


Рисунок 4.62 – Перевіряємо чи створилося правило

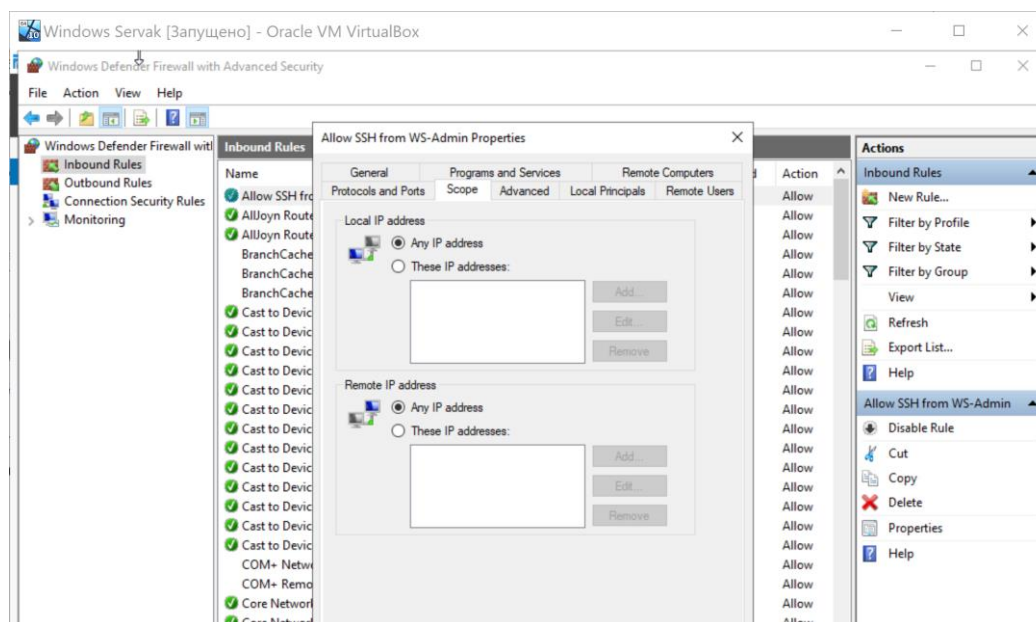


Рисунок 4.63 – Переходимо у налаштування новоствореного правила

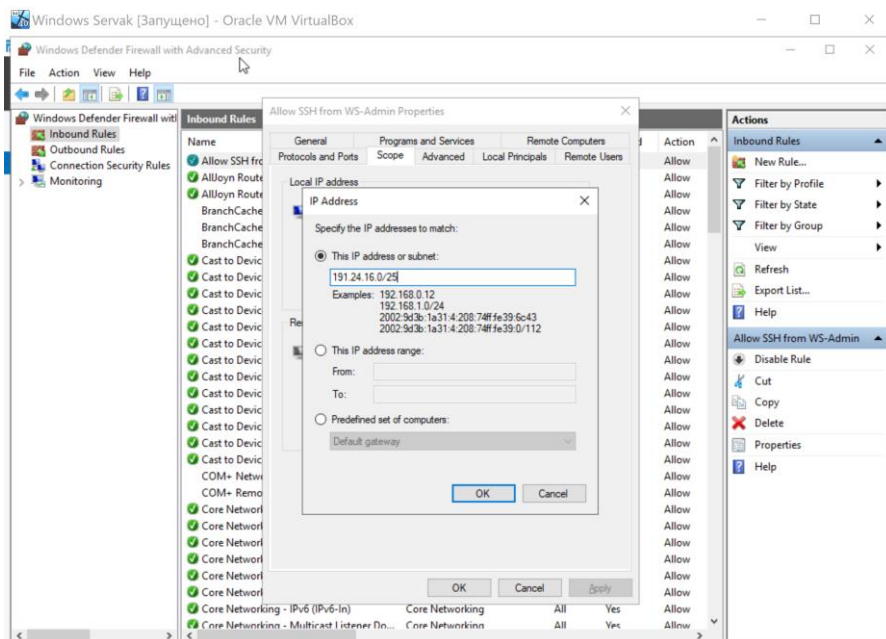


Рисунок 4.64 – Додаємо ір-адреси підмережі А

Так як доступ до серверів буде мати не лише адміністратор. Налаштування для робочих станцій з операційною системою Windows 10 буде проводитися аналогічно. Єдиною відмінністю будуть ір-адреси. Так як до робочих станцій користувачів буде мати доступ тільки адміністратор, то при налаштуванні правила ми будемо вказувати тільки одну дозовану ір-адресу (рис.4.65).

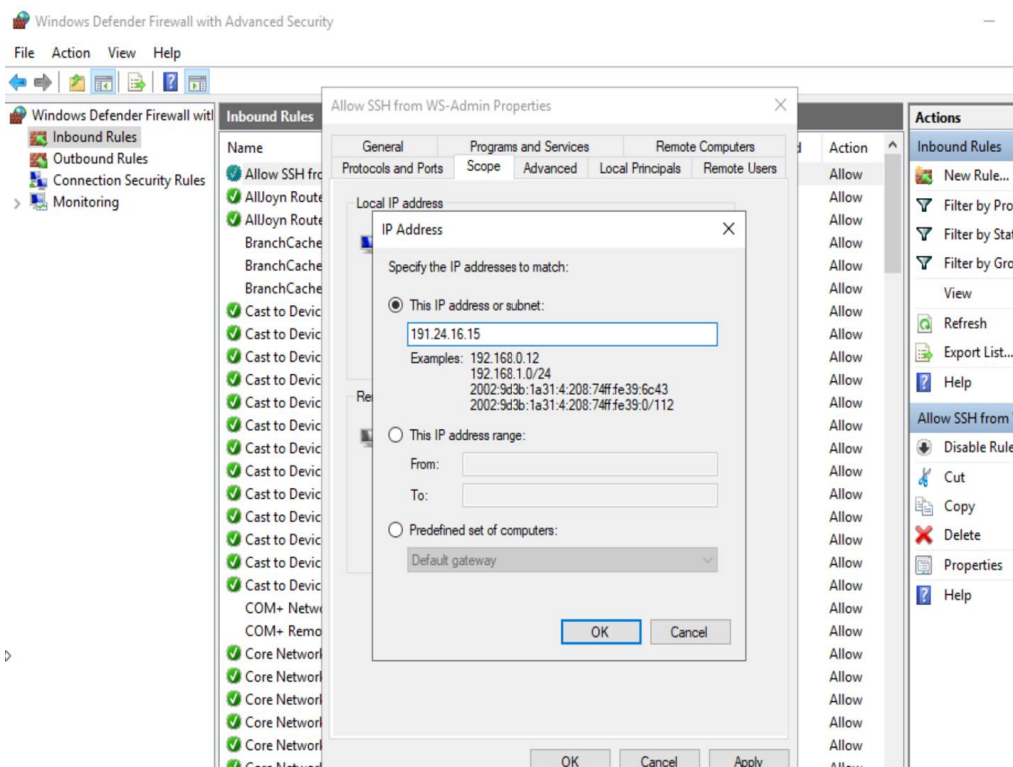


Рисунок 4.65 – Додаємо ір-адресу адміністратора

Налагодимо додаткові служби NTP (синхронізація часу в мережі) і Syslog (спосіб отримання системних повідомлень). Відповідні налаштування наведені на рис.4.66-68.

```
R-24-16-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R-24-16-1(config)#logging on
R-24-16-1(config)#logging host 191.24.16.12
R-24-16-1(config)#l
*Jun 12 18:21:01.199: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 191.24.16.12
port 514 started - CLI initiated
R-24-16-1(config)#logging userinfo
R-24-16-1(config)#logging buffered 32000
R-24-16-1(config)#logging trap warnings
R-24-16-1(config)#exit
R-24-16-1#
```

Рисунок 4.66 – Типове налаштування Syslog на маршрутизаторі

```
R-24-16-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R-24-16-1(config)#service timestamps log datetime msec
R-24-16-1(config)#ntp authenticate
R-24-16-1(config)#ntp authenticate-key 191 md5 cisco123
^
% Invalid input detected at '^' marker.

R-24-16-1(config)#ntp authentication-key 191 md5 cisco123
R-24-16-1(config)#ntp trusted-key 191
R-24-16-1(config)#ntp server 191.24.16.13
R-24-16-1(config)#ntp server 191.24.16.13 key 191
R-24-16-1(config)#ntp update-calendar
R-24-16-1(config)#exit
R-24-16-1#s
*Jun 12 18:34:58.059: %SYS-5-CONFIG I: Configured from console by console
```

Рисунок 4.67 – Типове налаштування NTP-клієнта на маршрутизаторі

```
SW-24-16-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-24-16-1(config)#service timestamps log datetime msec
SW-24-16-1(config)#ntp authenticate
SW-24-16-1(config)#ntp authentication-key 191 md5 cisco123
SW-24-16-1(config)#ntp trusted-key 191
SW-24-16-1(config)#ntp server 191.24.16.13 key 191
SW-24-16-1(config)#ntp update-calendar
SW-24-16-1(config)#exit
SW-24-16-1#
```

Рисунок 4.68 – Типове налаштування NTP-клієнта на комутаторі

Повторюємо відповідні налаштування на всіх мережних пристроях.

4.2 Тестування роботи побудованої локальної мережі

Перевірка наявності зв'язку між кінцевими пристроями, шлях пакету при передачі. Це можна здійснити за допомогою команд ping та tracer (рис.4.72-78, рис.4.79-82).

Тепер перевіримо функціонування протоколу RIPv2, за допомогою діагностичної команди (рис.4.69-71)

		Присяжнюк Я.В.			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				72
Змн.	Арк.	№ докум.	Підпис	Дата		

```

SW-24-16-1#show spanning-tree

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    28673
             Address     aabb.cc00.0a00
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    28673 (priority 28672 sys-id-ext 1)
             Address     aabb.cc00.0a00
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface                Role Sts Cost      Prio.Nbr Type
-----
Et0/0                    Desg FWD 100        128.1   Shr
Et0/1                    Desg FWD 100        128.2   Shr
Et1/0                    Desg FWD 100        128.5   Shr
Et1/3                    Desg FWD 100        128.8   Shr
Et2/0                    Desg FWD 100        128.9   Shr
Et2/1                    Desg FWD 100        128.10  Shr
Et2/2                    Desg FWD 100        128.11  Shr
Et2/3                    Desg FWD 100        128.12  Shr
Et3/0                    Desg FWD 100        128.13  Shr
Et3/1                    Desg FWD 100        128.14  Shr
Et3/2                    Desg FWD 100        128.15  Shr
Et3/3                    Desg FWD 100        128.16  Shr
Po2                      Desg FWD 56         128.65  Shr
Po1                      Desg FWD 56         128.66  Shr

SW-24-16-1#

```

Рисунок 4.69 – Перевірка функціонування протоколу RPVST на первинному комутаторі

```

SW-24-16-2#show spanning-tree

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    28673
             Address     aabb.cc00.0a00
             Cost         56
             Port         66 (Port-channel2)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    36865 (priority 36864 sys-id-ext 1)
             Address     aabb.cc00.0100
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface                Role Sts Cost      Prio.Nbr Type
-----
Et1/0                    Desg FWD 100        128.5   Shr
Et1/1                    Desg FWD 100        128.6   Shr
Et1/2                    Desg FWD 100        128.7   Shr
Et1/3                    Desg FWD 100        128.8   Shr
Et2/0                    Desg FWD 100        128.9   Shr
Et2/1                    Desg FWD 100        128.10  Shr
Et2/2                    Desg FWD 100        128.11  Shr
Et2/3                    Desg FWD 100        128.12  Shr
Et3/0                    Desg FWD 100        128.13  Shr
Et3/1                    Desg FWD 100        128.14  Shr
Et3/2                    Desg FWD 100        128.15  Shr
Et3/3                    Desg FWD 100        128.16  Shr
Po4                      Desg FWD 56         128.65  Shr
Po2                      Root FWD 56         128.66  Shr

SW-24-16-2#

```

Рисунок 4.70 – Перевірка функціонування протоколу RPVST на вторинному комутаторі

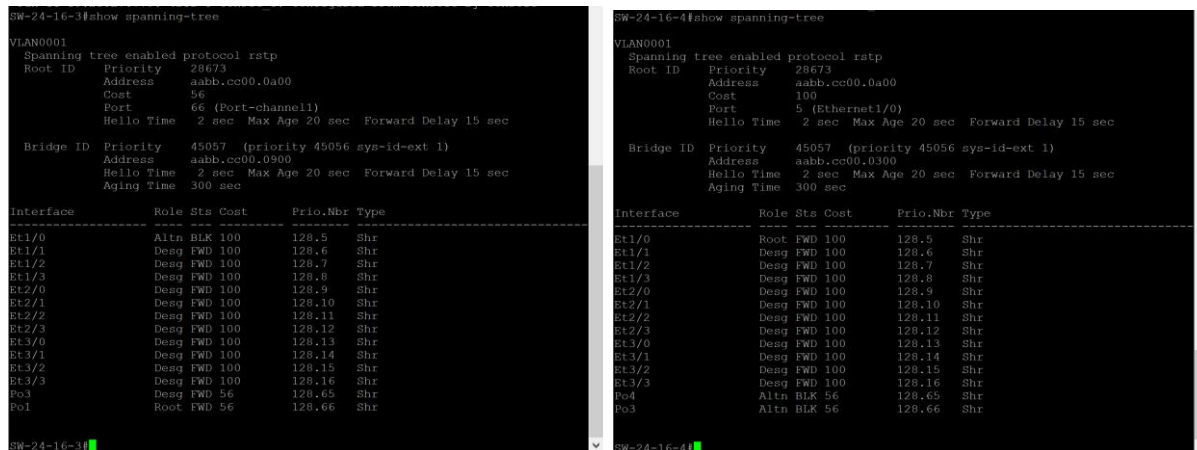


Рисунок 4.71-72 – Перевірка функціонування протоколу RPVST на комутаторах зі зміненими пріоритетами

Перевіримо налаштування протоколу віддаленого доступу SSH на пристроях мережі (рис.4.73-78).

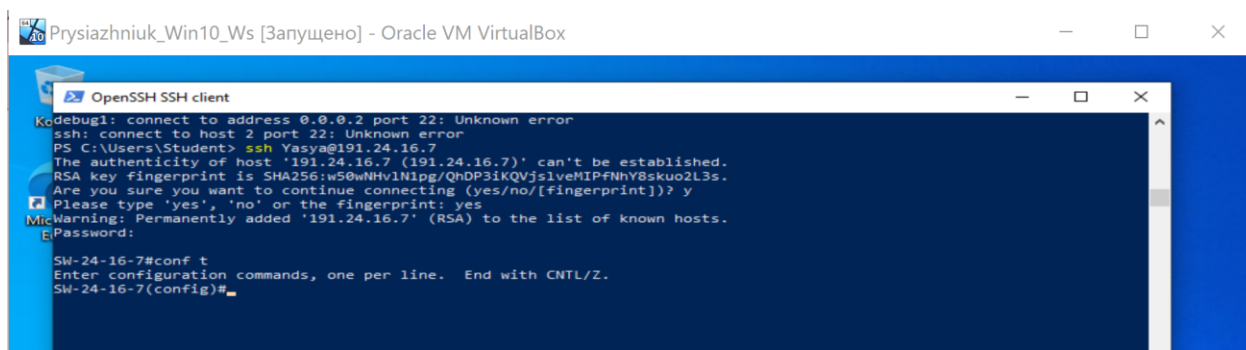


Рисунок 4.73 – Перевірка підключення до комутатора



Рисунок 4.74 – Перевірка журналювання подій на комутаторі

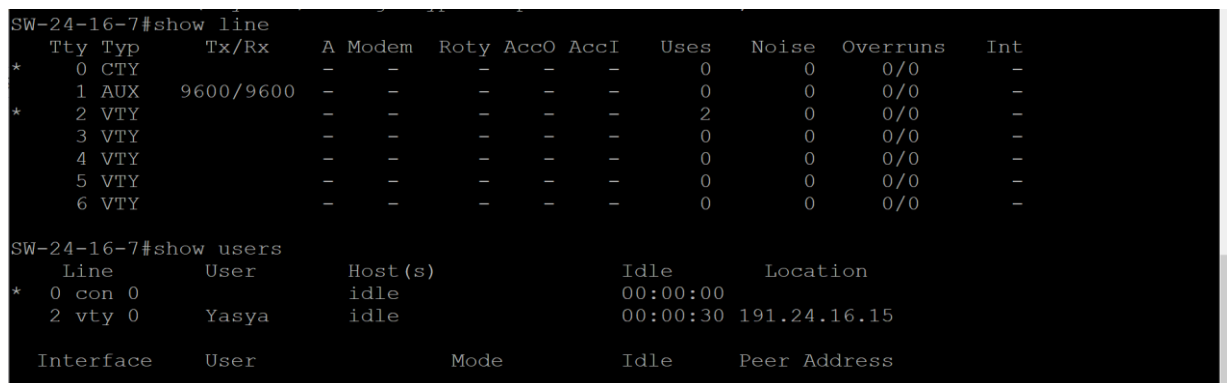


Рисунок 4.75 – Результат діагностичної команди show line на комутаторі

```

SW-24-16-7 - PuTTY
SW-24-16-7#show tcp

tty2, virtual tty from host 191.24.16.15
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled, Minimum incoming TTL 0, Outgoing TTL 255
Local host: 191.24.16.7, Local port: 22
Foreign host: 191.24.16.15, Foreign port: 65219
Connection tableid (VRF): 0
Maximum output segment queue size: 20

Enqueued packets for retransmit: 0, input: 0 mis-ordered: 0 (0 bytes)

Event Timers (current time is 0x2E96B2):
Timer           Starts      Wakeups      Next
Retrans         11         0           0x0
TimeWait        0          0           0x0
AckHold         10         3           0x0
SendWnd         0          0           0x0
KeepAlive       0          0           0x0
GiveUp          0          0           0x0
PmtuAger        0          0           0x0
DeadWait        0          0           0x0
Linger          0          0           0x0
ProcessQ        0          0           0x0

iss: 3733254754 snduna: 3733256150 sndnxt: 3733256150
irs: 60830388 rcvnxt: 60832626

sndwnd: 62845 scale: 0 maxrcvwnd: 4128
rcvwnd: 3588 scale: 0 delrcvwnd: 540

SRTT: 770 ms, RTTO: 2360 ms, RTV: 1590 ms, KRTT: 0 ms
minRTT: 0 ms, maxRTT: 1000 ms, ACK hold: 200 ms
uptime: 39470 ms, Sent idletime: 26380 ms, Receive idletime: 26325 ms
Status Flags: passive open, active open
Option Flags: Retrans timeout
IP Precedence value : 6

TCB is waiting for TCP Process (116)

```

Рисунок 4.76 – Результат діагностичної команди show tcp на комутаторі

```

SW-24-16-7 - PuTTY
TCB is waiting for TCP Process (116)

Datagrams (max data segment is 1460 bytes):
Rcvd: 16 (out of order: 0), with data: 10, total data bytes: 2237
Sent: 19 (retransmit: 0, fastretransmit: 0, partialack: 0, Second Congestion: 0), with data:
13, total data bytes: 1395

Packets received in fast path: 0, fast processed: 0, slow path: 0
fast lock acquisition failures: 0, slow path: 0
TCP Semaphore 0xF1567B38 FREE
SW-24-16-7#show ssh
Connection Version Mode Encryption Hmac State Username
0 2.0 IN aes128-ctr hmac-shal Session started Yasya
0 2.0 OUT aes128-ctr hmac-shal Session started Yasya
%No SSHv1 server connections running.
SW-24-16-7#show crypto key mypubkey rsa
% Key pair was generated at: 10:10:39 UTC May 29 2024
Key name: SW-24-16-7.prysiashniuk.net
Key type: RSA KEYS
Storage Device: not specified
Usage: General Purpose Key
Key is not exportable. Redundancy enabled.
Key Data:
30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00D96B08
DDC03EA1 BD01096F 09A4ACE4 10805AE0 FF25956F 359E223D 506DB296 C8F3E832
95C8E31D 39006648 5B352E8E 4E84DD95 FB157CDD A435C933 70DBC567 90D6F824
9F035650 02D1FA58 EA65B327 BDCABFF8 65249651 91AB0C83 6B221D21 6EA3622F
4CDFC0B3 14E69366 C8567D34 51862D8E FFDF3151 6CF5F3EC 63013800 35020301 0001
% Key pair was generated at: 10:10:40 UTC May 29 2024
Key name: SW-24-16-7.prysiashniuk.net.server
Key type: RSA KEYS
Temporary key
Usage: Encryption Key
Key is not exportable. Redundancy enabled.
Key Data:
307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00938E3A 04C4F55C
0AC6D2E7 8D08B6E0 71340CAF BACC9966 DAB74D24 FCAD5202 623CB101 91CD1748
69A44B6D AE502498 D810F4D4 0EB89E31 FF84000F F2FACAEC 30A83BFB 6551860C
84257CD5 B6FF684C B0E2B3A7 B50D0B6C FD8300E8 DDF8301E 8D020301 0001

```

Рисунок 4.77 – Результат діагностичної команди show ssh на комутаторі

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз С.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		75

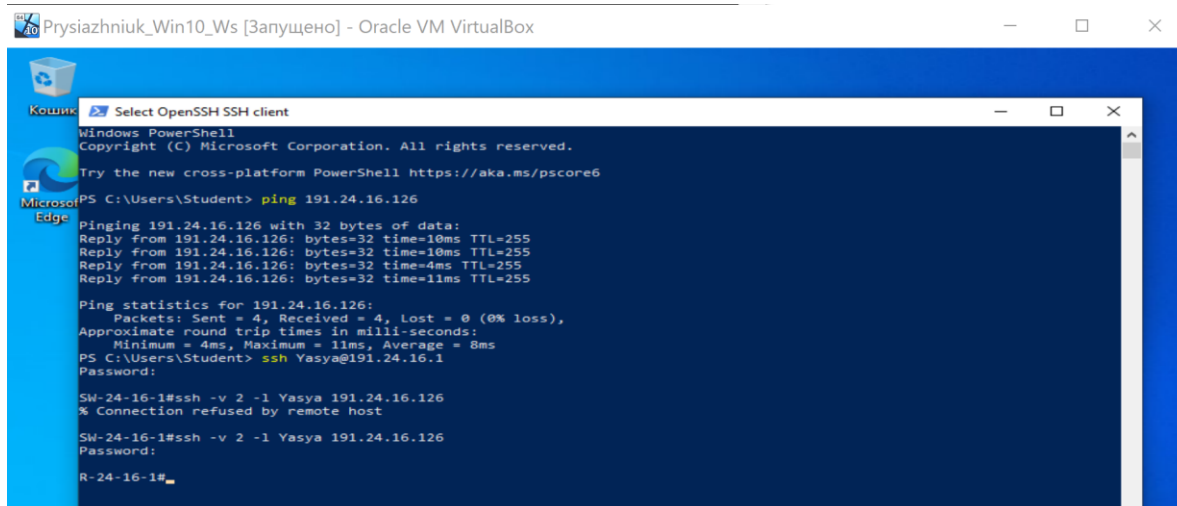


Рисунок 4.78 – Перевірка підключення за протоколом SSH до маршрутизатора

Як бачимо, підключення до маршрутизаторів має відбуватися поступово, через комутатор (рис.4.78). Також у журналі подій з'являється відповідний запис (рис.4.79).

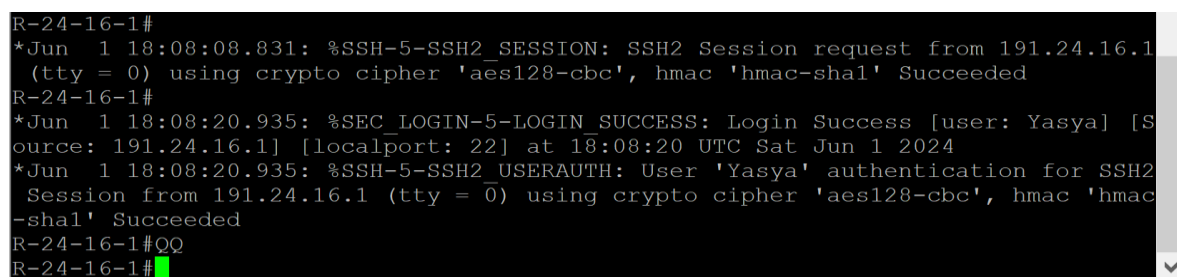


Рисунок 4.79 – Відповідне журналювання подій до маршрутизаторі

Перевіримо підключення до маршрутизатора з віддаленої підмережі (рис.4.80-81).

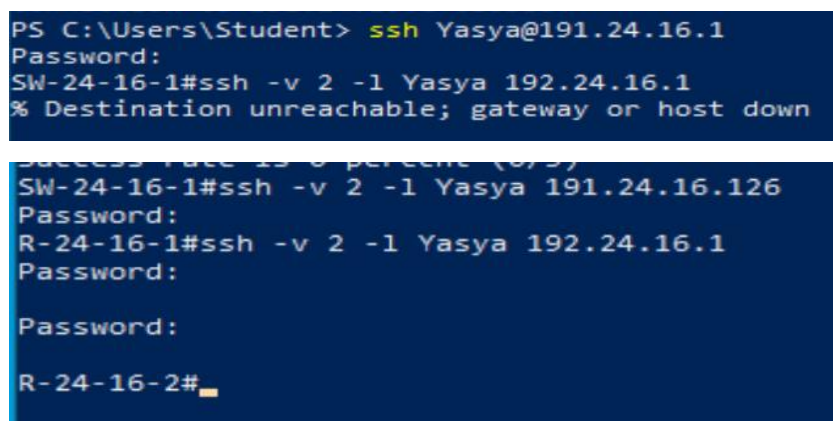


Рисунок 4.80-81 – Перевірка підключення за протоколом SSH до віддаленого маршрутизатора

Як і в попередньому прикладі ми маємо виконувати таке підключення посту-
ПОВО.

```
R-24-16-2#
*Jun  1 18:17:40.835: %SSH-5-SSH2_SESSION: SSH2 Session request from 192.24.16.2
(tty = 0) using crypto cipher 'aes128-cbc', hmac 'hmac-sha1' Succeeded
R-24-16-2#
*Jun  1 18:17:51.195: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: Yasya] [Sou
rce: 192.24.16.2] [localport: 22] [Reason: Login Authentication Failed] at 18:17
:51 UTC Sat Jun 1 2024
R-24-16-2#
*Jun  1 18:18:01.187: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: Yasya] [S
ource: 192.24.16.2] [localport: 22] at 18:18:01 UTC Sat Jun 1 2024
*Jun  1 18:18:01.187: %SSH-5-SSH2_USERAUTH: User 'Yasya' authentication for SSH2
Session from 192.24.16.2 (tty = 0) using crypto cipher 'aes128-cbc', hmac 'hmac
-sha1' Succeeded
R-24-16-2#
```

Рисунок 4.82 – Журналювання подій на маршрутизаторі

Зараз перейдемо до перевірки підключень за допомогою протокола SSH че-
рез робочі станції (рис.4.83-88).

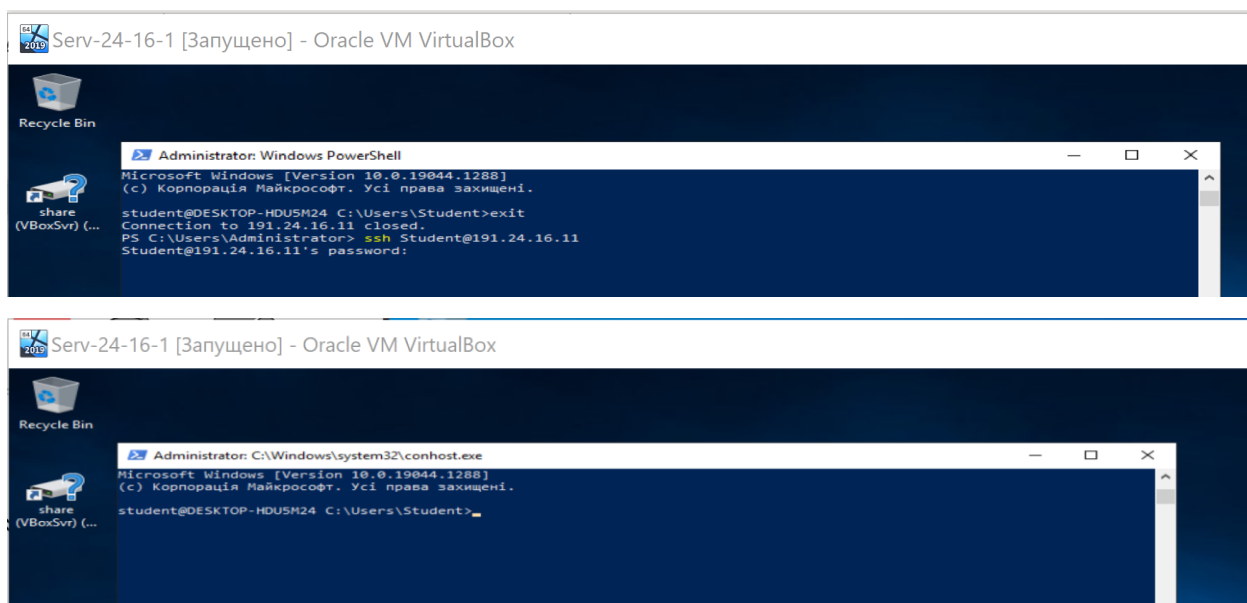


Рисунок 4.83-84 – Перевірка підключення за допомогою SSH до робочої станції

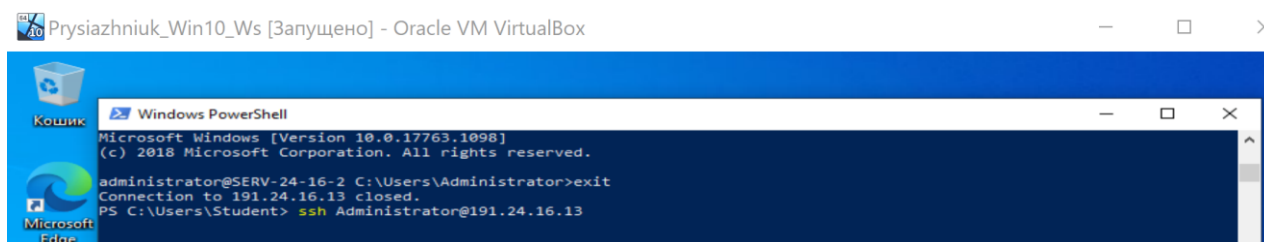


Рисунок 4.85 – Перевірка підключення за допомогою SSH до сервера

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				77
Змн.	Арк.	№ докум.	Підпис	Дата		

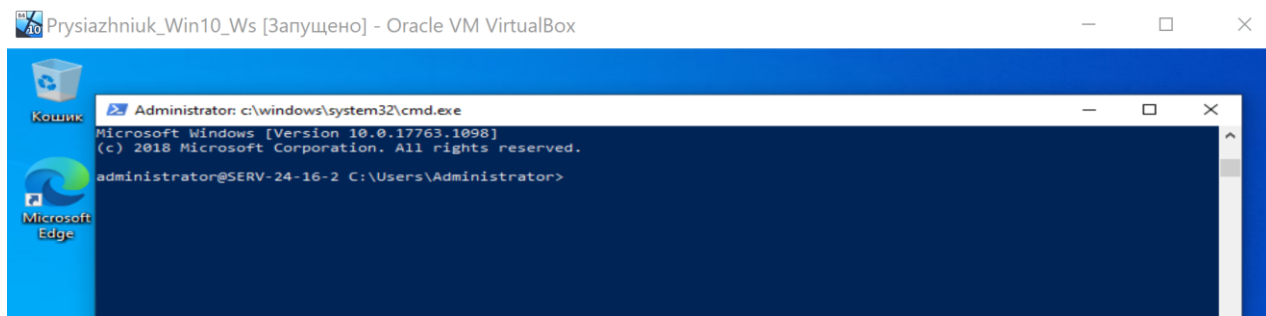


Рисунок 4.86 – Перевірка підключення за допомогою SSH до сервера

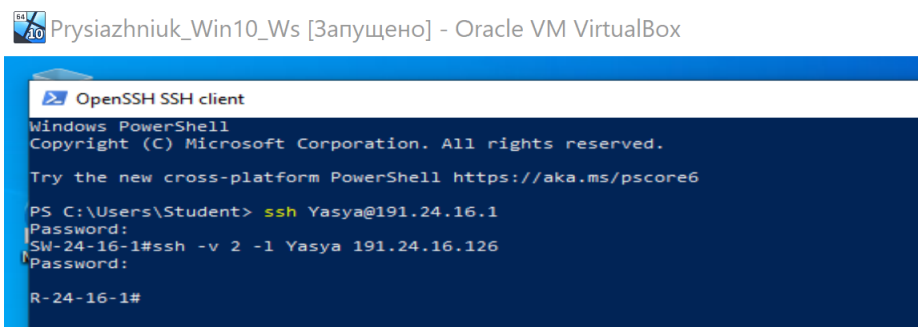


Рисунок 4.87 – Перевірка підключення до маршрутизатора R-24-16-1 після налаштування списків доступу

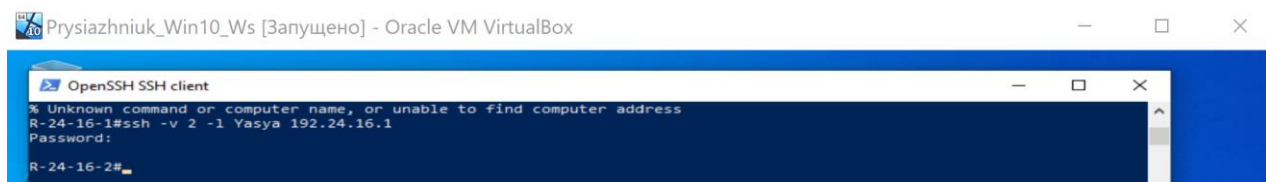


Рисунок 4.88 – Перевірка підключення до маршрутизатора R-24-16-2 після налаштування списків доступу

А зараз детально розглянемо роботу DHCP-pool, налаштованого на одному з маршрутизаторів (рис.4.89).

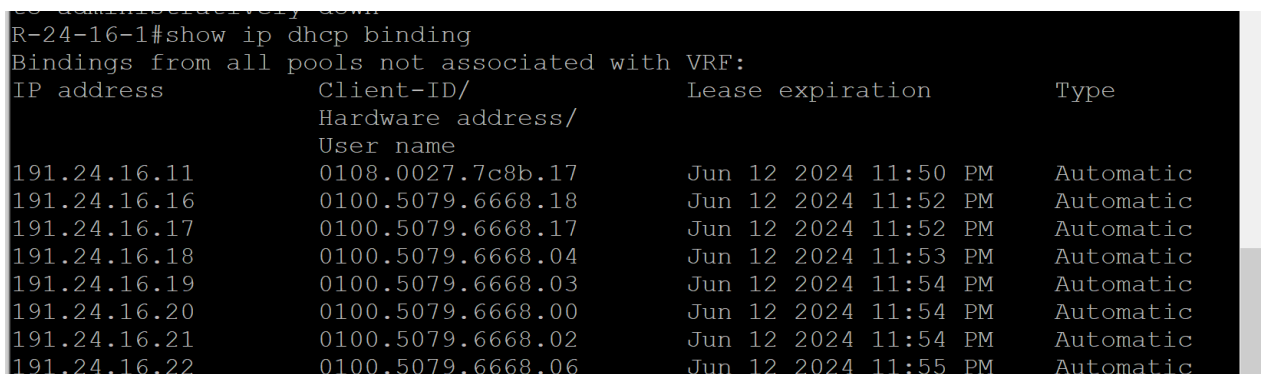


Рисунок 4.89 – Діагностична команда для маршрутизатора

Розглянемо детальніше роботу протоколу динамічної маршрутизації OSPF, за допомогою діагностичної команди (рис.4.90).

```
R-24-16-1#show ip route ospf
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

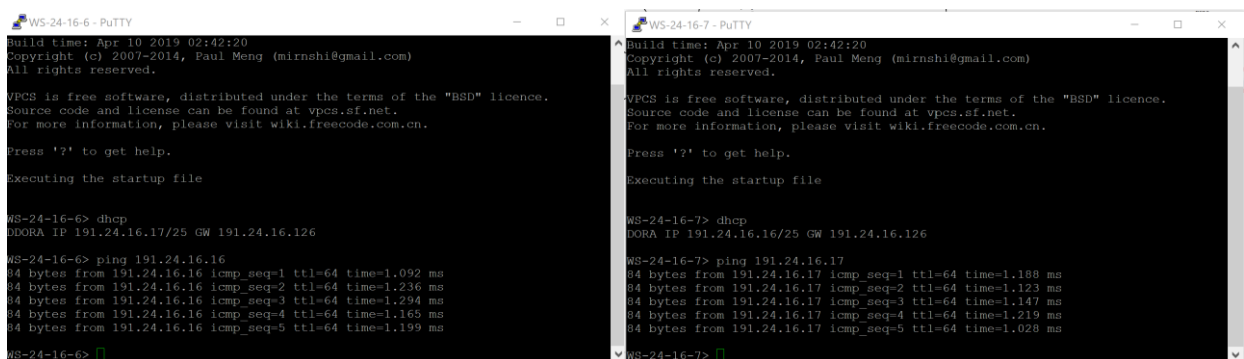
Gateway of last resort is not set

    192.24.16.0/24 is variably subnetted, 3 subnets, 2 masks
O       192.24.16.8/29 [110/2] via 192.24.16.1, 00:00:06, FastEthernet0/0
R-24-16-1#
```

Рисунок 4.90 – Діагностична команда для маршрутизатора

4.3 Налаштування та тестування захисту мережі

Першим кроком буде налаштування захисту для протидії атакам на протокол DHCP. Отож, розглянемо детально симуляцію такою атаки (рис.4.95). Для цього перевіримо нормальне функціонування мережі, а саме виділення динамічної адреси та використання її для зв'язку між пристроями мережі (рис.4.91-92). Далі нам треба під'єднати несанкціоновану робочу станцію (рис.9.93).



```
WS-24-16-6 - PuTTY
Build time: Apr 10 2019 02:42:20
Copyright (c) 2007-2014, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

WS-24-16-6> dhcp
DDORA IP 191.24.16.17/25 GW 191.24.16.126

WS-24-16-6> ping 191.24.16.16
84 bytes from 191.24.16.16 icmp_seq=1 ttl=64 time=1.092 ms
84 bytes from 191.24.16.16 icmp_seq=2 ttl=64 time=1.236 ms
84 bytes from 191.24.16.16 icmp_seq=3 ttl=64 time=1.294 ms
84 bytes from 191.24.16.16 icmp_seq=4 ttl=64 time=1.165 ms
84 bytes from 191.24.16.16 icmp_seq=5 ttl=64 time=1.199 ms

WS-24-16-6>

WS-24-16-7 - PuTTY
Build time: Apr 10 2019 02:42:20
Copyright (c) 2007-2014, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

WS-24-16-7> dhcp
DORA IP 191.24.16.16/25 GW 191.24.16.126

WS-24-16-7> ping 191.24.16.17
84 bytes from 191.24.16.17 icmp_seq=1 ttl=64 time=1.188 ms
84 bytes from 191.24.16.17 icmp_seq=2 ttl=64 time=1.123 ms
84 bytes from 191.24.16.17 icmp_seq=3 ttl=64 time=1.147 ms
84 bytes from 191.24.16.17 icmp_seq=4 ttl=64 time=1.219 ms
84 bytes from 191.24.16.17 icmp_seq=5 ttl=64 time=1.028 ms

WS-24-16-7>
```

Рисунок 4.91-92 – Нормальне функціонування мережі (динамічне виділення ір-адреси + перевірка зв'язку між робочими станціями)

Під'єднуємо робочу станцію зломисника. Атака буде проводитися за допомогою ПЗ Yersinia.

		Присяжнюк Я.В.			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		79

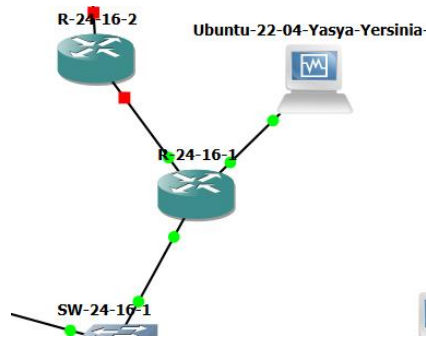


Рисунок 4.93 – Під'єднано робочу станцію зловмисника

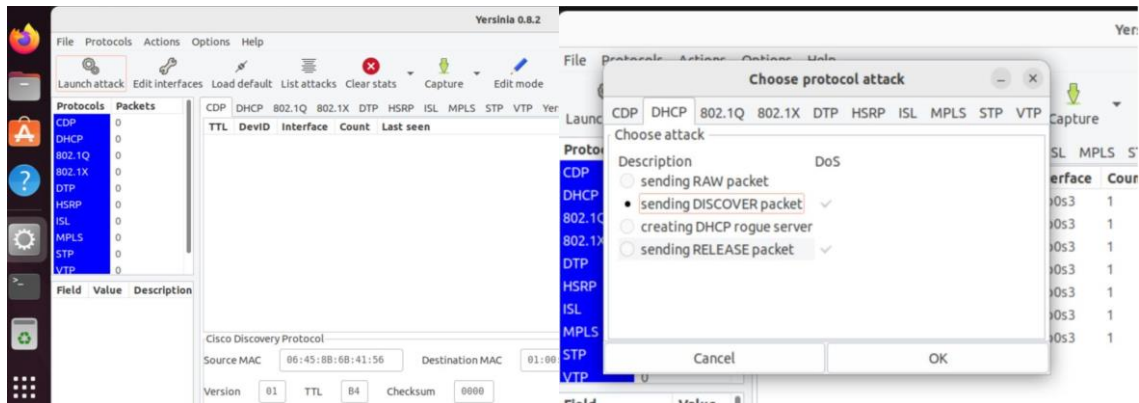


Рисунок 4.94 – Проведення атаки

На жаль, без коректно налаштованого захисту атака буде вдалою і робота мережі буде порушена (рис.4.95).

```
WS-24-16-7> ping 191.24.16.17
host (191.24.16.17) not reachable
WS-24-16-7>
```

Рисунок 4.95 – Працездатність мережі під час атаки

Отож, налаштовуємо захист від атак такого типу (рис.4.96-97).

```
SW-24-16-5#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-24-16-5(config)#ip dhcp snooping
SW-24-16-5(config)#int range e0/0-1
SW-24-16-5(config-if-range)#ip dhcp snooping trust
SW-24-16-5(config-if-range)#ip dhcp snooping limit rate 256
SW-24-16-5(config-if-range)#exit
SW-24-16-5(config)#exit
SW-24-16-5#
*Jun  2 17:52:18.559: %SYS-5-CONFIG_I: Configured from console by console
SW-24-16-5#
```

Рисунок 4.96 – Типове налаштування для комутатора (інтерфейси між мережними пристроями)

```

SW-24-16-3 - PuTTY
description AGGREGATED-LINK-TO-SW-24-16-1
!
interface Ethernet0/0
channel-group 1 mode on
ip dhcp snooping limit rate 256
ip dhcp snooping trust
!
interface Ethernet0/1
channel-group 1 mode on
ip dhcp snooping limit rate 256
ip dhcp snooping trust
!
interface Ethernet0/2
channel-group 3 mode on
ip dhcp snooping limit rate 256
ip dhcp snooping trust
!
interface Ethernet0/3
channel-group 3 mode on
ip dhcp snooping limit rate 256
ip dhcp snooping trust
!
interface Ethernet1/0
ip dhcp snooping limit rate 256
ip dhcp snooping trust
!
interface Ethernet1/1
ip dhcp snooping limit rate 256
ip dhcp snooping trust

```

Рисунок 4.97 – Приклад фрагменту конфігураційного файлу з відповідними налаштуваннями

Проведемо повторну атаку та перевіримо результат налаштувань (рис.4.98-100).

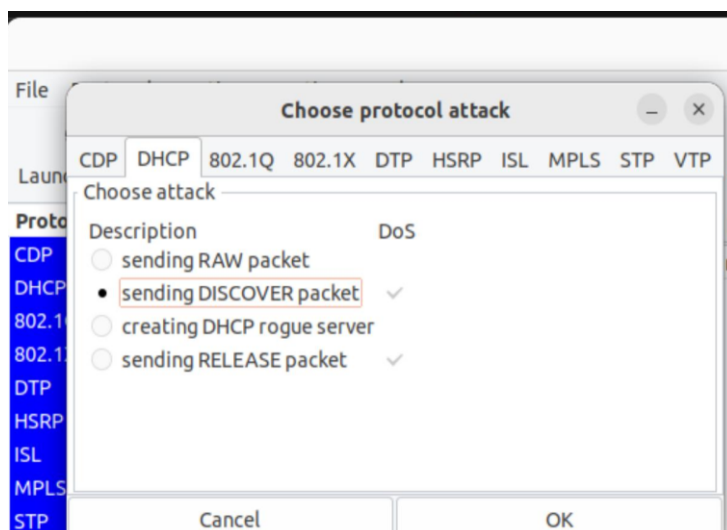


Рисунок 4.98 – Запуск повторної атаки

```

WS-24-16-7> ping 191.24.16.17
84 bytes from 191.24.16.17 icmp_seq=1 ttl=64 time=1.474 ms
84 bytes from 191.24.16.17 icmp_seq=2 ttl=64 time=1.234 ms
84 bytes from 191.24.16.17 icmp_seq=3 ttl=64 time=1.137 ms
84 bytes from 191.24.16.17 icmp_seq=4 ttl=64 time=1.141 ms
84 bytes from 191.24.16.17 icmp_seq=5 ttl=64 time=1.286 ms
WS-24-16-7> █

```

Рисунок 4.99 – Перевірка зв'язку між робочими станціями

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				81
Змн.	Арк.	№ докум.	Підпис	Дата		

```
SW-24-16-1#ping 191.24.16.126
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 191.24.16.126, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 5/8/10 ms
SW-24-16-1#
```

Рисунок 4.100 – Перевірка зв'язку між комутатором та маршрутизатором (DHCP-pool)

Далі розглянемо атаки на протоколи сімейства STP, а саме появу в мережі несанкціонованого комутатора. Налаштуємо засоби захисту комутаторів з використанням функцій безпеки Root Guard, BPDU Guard (рис.4.101).

```
SW-24-16-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-24-16-1(config)#int range e0/0-3, e1/0-2
SW-24-16-1(config-if-range)#spanning-tree guard root
SW-24-16-1(config-if-range)#
*Jun 12 17:38:14.896: %SPANTREE-2-ROOTGUARD_CONFIG_CHANGE: Root guard enabled on
port Ethernet0/0.
*Jun 12 17:38:14.896: %SPANTREE-2-ROOTGUARD_CONFIG_CHANGE: Root guard enabled on
port Ethernet0/1.
*Jun 12 17:38:14.897: %SPANTREE-2-ROOTGUARD_CONFIG_CHANGE: Root guard enabled on
port Ethernet1/0.
SW-24-16-1(config-if-range)#exit
SW-24-16-1(config)#
```

Рисунок 4.101 – Налаштування для кореневого комутатора

Налаштуємо portfast та bpduguard для інтерфейсів комутатора, які під'єднанні до робочих станцій (рис.4.102).

```
SW-24-16-9#conf
Configuring from terminal, memory, or network [terminal]? t
Enter configuration commands, one per line. End with CNTL/Z.
SW-24-16-9(config)#int range eth0/1-3, eth1/1-2
SW-24-16-9(config-if-range)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast will be configured in 5 interfaces due to the range command
but will only have effect when the interfaces are in a non-trunking mode.
SW-24-16-9(config-if-range)#spanning-tree bpduguard enable
SW-24-16-9(config-if-range)#exit
SW-24-16-9(config)#
```

Рисунок 4.102 – Типове налаштування комутатора

		Присяжнюк Я.В.			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				82
Змн.	Арк.	№ докум.	Підпис	Дата		

```

SW-24-16-8#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-24-16-8(config)#spanning-tree portfast default
%Warning: this command enables portfast by default on all interfaces. You
should now disable portfast explicitly on switched ports leading to hubs,
switches and bridges as they may create temporary bridging loops.

SW-24-16-8(config)#spanning-tree portfast bpduguard default
SW-24-16-8(config)#errdisable recovery cause bpduguard
SW-24-16-8(config)#errdisable recovery interval 60
SW-24-16-8(config)#int range e0/1-2
SW-24-16-8(config-if-range)#spanning-tree portfast disable
SW-24-16-8(config-if-range)#spanning-tree bpduguard disable
SW-24-16-8(config-if-range)#exit
SW-24-16-8(config)#int range Q
SW-24-16-8#
*Jun 12 17:55:55.897: %SYS-5-CONFIG_I: Configured from console by console
SW-24-16-8#QQ
SW-24-16-8#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-24-16-8(config)#int range e1/0-3, e0/3
SW-24-16-8(config-if-range)#spanning-tree portfast
SW-24-16-8(config-if-range)#spanning-tree bpduguard enable
SW-24-16-8(config-if-range)#spanning-tree etherchannel guard misconfig
SW-24-16-8(config)#

```

Рисунок 4.103 – Приклад налаштування інших комутаторів мережі

Далі налагоджуємо BPDU Filter на інтерфейсах, що під'єднані до кінцевих пристроїв (рис.4.104).

```

SW-24-16-8(config)#int range e1/0-3, e0/3
SW-24-16-8(config-if-range)#spanning-tree bpdufilter enable
SW-24-16-8(config-if-range)#exit
SW-24-16-8(config)#

```

Рисунок 4.104 – Приклад такого налаштування

Наступний крок – налаштування Loop Guard на інтерфейсах комутаторів, що під'єднані до інших мережних пристроїв (рис.4.105).

```

SW-24-16-8(config)#int range e0/1-2
SW-24-16-8(config-if-range)#spanning-tree guard loop
SW-24-16-8(config-if-range)#exit
SW-24-16-8(config)#

```

Рисунок 4.105 – Приклад такого налаштування

Проводимо аналогічні налаштування для інших комутаторів. А потім перевіряємо налаштування. Під'єднуємо несанкціонований комутатор до мережі (рис.4.106) та спостерігаємо реакцію порту мережевого комутатора (рис.4.107-109).

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		83

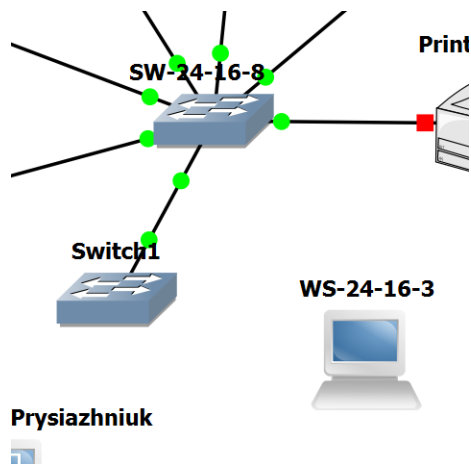


Рисунок 4.106 – Під'єднуємо нелегальний комутатор

Port	Name	Status	Vlan	Duplex	Speed	Type
Eth1/2		err-disabled	1	auto	auto	unknown

Рисунок 4.107 – Реакція порту на під'єднання комутатора

ErrDisable Reason	Timer Status
arp-inspection	Disabled
bpduguard	Enabled
channel-misconfig (STP)	Disabled
dhcp-rate-limit	Disabled
dtp-flap	Disabled
gbic-invalid	Disabled
inline-power	Disabled
l2ptguard	Disabled
link-flap	Disabled
mac-limit	Disabled
link-monitor-failure	Disabled
loopback	Disabled
oam-remote-failure	Disabled
pagp-flap	Disabled
port-mode-failure	Disabled
ppoe-ia-rate-limit	Disabled
psecure-violation	Disabled
security-violation	Disabled
sfp-config-mismatch	Disabled
storm-control	Disabled
udld	Disabled

Interface	Errdisable reason	Time left(sec)
unicast-flood	Disabled	
vmps	Disabled	
psp	Disabled	
dual-active-recovery	Disabled	
evc-lite input mapping fa	Disabled	
Recovery command: "clear	Disabled	

Timer interval: 60 seconds

Interfaces that will be enabled at the next timeout:

Interface	Errdisable reason	Time left(sec)
Eth1/2	bpduguard	29

Рисунок 4.108 – Фрагмент відповідної діагностичної команди

```

SW-24-16-2#show int e0/2 status

Port      Name      Status      Vlan      Duplex  Speed Type
Et0/2     err-disabled 1          auto     auto unknown
SW-24-16-2#
*Jun 12 19:00:19.017: %PM-4-ERR_RECOVER: Attempting to recover from bpduguard er
r-disable state on Et0/2
*Jun 12 19:00:19.017: %PM-4-ERR_RECOVER: Attempting to recover from bpduguard er
r-disable state on Et0/3
*Jun 12 19:00:19.017: %PM-4-ERR_RECOVER: Attempting to recover from bpduguard er
r-disable state on Po4
SW-24-16-2#
*Jun 12 19:00:21.022: %LINK-3-UPDOWN: Interface Ethernet0/2, changed state to up
*Jun 12 19:00:21.022: %LINK-3-UPDOWN: Interface Port-channel4, changed state to
up
*Jun 12 19:00:21.022: %LINK-3-UPDOWN: Interface Ethernet0/3, changed state to up
*Jun 12 19:00:22.028: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/
2, changed state to up
*Jun 12 19:00:22.028: %LINEPROTO-5-UPDOWN: Line protocol on Interface Port-chann
el4, changed state to up
*Jun 12 19:00:22.028: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/
3, changed state to up
SW-24-16-2#show int e0/2 status

Port      Name      Status      Vlan      Duplex  Speed Type
Et0/2     connected 1          auto     auto unknown
SW-24-16-2#

```

Рисунок 4.109 – Приклад відновлення порту на іншому комутаторі

4.4 Додатковий захист мережі

В ході проведення попереднього обстеження інформаційного середовища, виявлено, що на робочих станціях вже встановлено:

- Антивірус Avast 17.9;
- Антивірус USB Disk Security;

Дане програмне забезпечення чудово виконує його функції. Замінювати його немає необхідності, лише оновити до останніх версій.

Профілактичні рекомендації:

- Регулярні оновлення операційної системи та всіх встановлених програм дозволяють оптимізувати роботу, прибравши недосконалості попередніх версій, які можуть бути використані зловмисниками для атаки на систему.

- Використання вбудованого брандмауера (наприклад, Windows Defender) для контролю вхідного та вихідного трафіку, що може допомогти запобігти не-санкціонованому доступу.

		Присяжнюк Я.В.			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		85

- Встановлення вимог до складності паролів кінцевих користувачів (довжина, наявність символів, цифр тощо). Також своєчасне оновлення паролів.
- Включення політики блокування або обмеження використання USB-пристроїв, якщо це можливо, або використання програм для моніторингу та блокування несанкціонованих пристроїв.
- Регулярне створення резервних копій важливих даних, щоб у разі зараження можна було відновити інформацію.
- Проведення тренінгів для співробітників щодо питань інформаційної безпеки (фішинг, небезпечні вкладення в листах, небезпечні сайти тощо).

Висновки до четвертого розділу

У цьому розділі було Проведено налагодження мережі, а саме: ір-адресація, статичне агрегування, RIPv2, OSPF та DHCP. Детально реалізовано використання протоколу SSH. Також було перевірено зв'язок між пристроями мережі, виділення автоматичних IP-адрес протоколом DHCP та досліджено роботу діагностичних команд для виведення інформації про роботу налаштованих протоколів.

Налаштовано та перевірено захищений віддалений доступ до мережних та кінцевих пристроїв, серверів. Реалізовано списки доступу по протоколу SSH.

Реалізовано та протестовано захист під поширених типів атак на мережні пристрої. Проведено аналіз наявного антивірусного ПЗ на робочих станціях.

Особливу увагу приділено розробці списку профілактичних рекомендацій для посилення інформаційної безпеки.

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		86

ВИСНОВКИ

У ході виконання поставлених завдань було проведено комплексне дослідження та проєктування комп'ютерної мережі з урахуванням як технічних, так і інформаційно-безпекових аспектів. На етапі обстеження фізичного середовища об'єкта визначено просторові, інфраструктурні та електротехнічні умови для розгортання мережевого обладнання, що дозволило закласти основу для подальшого планування.

Обстеження середовища користувачів та аналіз інформаційних потоків дало змогу виявити потреби майбутніх користувачів, структуру взаємодії між ними та типи даних, що циркулюють мережею. Це дозволило перейти до побудови моделі порушника та моделі загроз, на основі яких були визначені актуальні ризики, потенційні вектори атак і слабкі місця системи, що потребують підвищеної уваги з боку захисту.

У результаті було розроблено структурну модель комп'ютерної мережі, що охоплює ключові компоненти — комутатори, маршрутизатори, сервери, точки доступу — та демонструє логічну й фізичну організацію взаємозв'язків. Після цього проведено обґрунтований вибір сучасних комунікаційних технологій і пристроїв (зокрема, Cisco ISR4321-V/K9, WS-C2960X-24TS-L), що відповідають вимогам до продуктивності, масштабованості та безпеки.

Заключний етап полягав у безпосередній розробці та налагодженні мережі. Всі дії проводились із врахуванням попередньо змодельованих загроз. Проведено не лише базові налаштування локальної мережі, а й додаткові налаштування захисту від атак на протоколи DHCP (велика кількість запитів до DHCP-pool на отримання IP-адреси), STP (під'єднання несанкціонованого комутатора).

У результаті виконаної роботи було створено ефективну, безпечну та гнучку комп'ютерну мережу, що відповідає потребам користувачів і вимогам сучасної кібербезпеки.

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				87
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Windows Server: open SSH, [електронний ресурс] – Режим доступу : https://learn.microsoft.com/uk-ua/windowsserver/administration/openssh/openssh_over-view
2. Netacad, [електронний ресурс] – Режим доступу: <https://www.netacad.com/>
3. Learn.ztu.edu.ua, [електронний ресурс] – Режим доступу: <https://learn.ztu.edu.ua/course/view.php?id=1890>.
4. Wikipedia, [електронний ресурс] – Режим доступу: <https://uk.wikipedia.org/wiki>
5. Cisco, [електронний ресурс] – Режим доступу: <http://www.cisco.com>
6. Поняття про комп'ютерні мережі [Електронний ресурс] // Київський професійно-педагогічний коледж імені Антона Макаренка. – 2019. – Режим доступу: <https://kppk.com.ua/ELLIB/ebook/Gorbenko/IKT/13/13.htm>
7. SSH – the protocol for communication, [електронний ресурс] – Режим доступу: <https://cqr.company.ua/wiki/protocols/ssh-the-protocol-for-communication/>
8. Комп'ютерні мережі: [навчальний посібник] / А. Г. Микитишин, М. М. Митник, П. Д. Стухляк, В. В. Пасічник. — Львів: «Магнолія 2006», 2013. — 256 с
9. Буров Є. Комп'ютерні мережі. 2-ге оновлене і доповн. вид. Львів: БаК, 2003. – 584 с., іл. [Навчальний посібник]
10. Кулаков Ю.О., Луцький Г.М. Комп'ютерні мережі. Підручник / За ред. Ю.С. Ковтанюка. – К.: Юніор, 2003. – 400 с. [Навчальний посібник]
11. НД ТЗІ 1.1-002-99, [електронний ресурс] – Режим доступу: https://tzi.ua/ua/nd_tz_1.1-002-99.html
12. ISO 27002, [електронний ресурс] – Режим доступу: <https://learn.ztu.edu.ua/mod/resource/view.php?id=172696&forceview=1>

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				88
Змн.	Арк.	№ докум.	Підпис	Дата		

13. StackSystem, [електронний ресурс] – Режим доступу:

<https://stack-systems.com.ua/>

14. НД ТЗІ 2.5-005-99, [електронний ресурс] – Режим доступу:

https://tzi.ua/ua/nd_tz_2.5-005-99.html

15. НД ТЗІ 1.4-001-2000, [електронний ресурс] – Режим доступу:

<https://www.tzi.com.ua/polozhennya-pro-sluzhbu-zaxistu-nformacz.html>

16. НД ТЗІ 1.1-003-099, [електронний ресурс] – Режим доступу:

https://tzi.ua/ua/nd_tz_1.1-003-99.html

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз С.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		89

ДОДАТКИ

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		90

Схема побудованої мережі

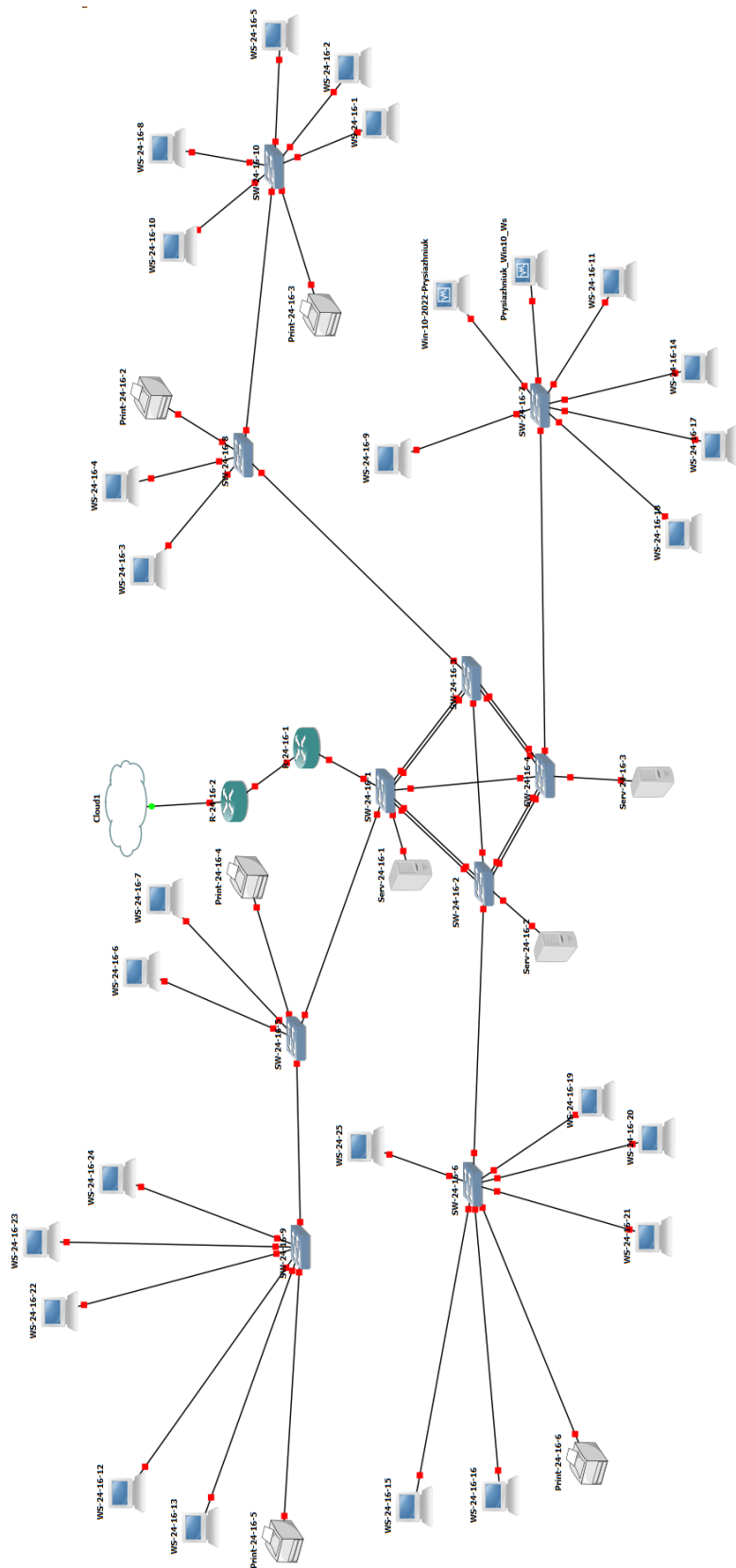


Рисунок А.1 – Схема локальної мережі

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				91
Змн.	Арк.	№ докум.	Підпис	Дата		

Технічні характеристики обладнання

Б.1 Технічні характеристики маршрутизатора Cisco ISR4321-V/K9

Параметр	Характеристика
Тип пристрою	Маршрутизатор
Технологія доступу	WAN, LAN, маршрутизація, VPN
Кількість WAN портів	2 (вбудовані Gigabit Ethernet WAN порти)
Тип WAN портів	2 x Gigabit Ethernet (RJ-45)
Протоколи	OSPF, EIGRP, BGP, RIP, IPsec VPN, MPLS, NAT, DHCP
Підтримка IPv6	Так
Наявність USB портів	2 (1 USB 3.0, 1 USB 2.0)
Підтримка USB-носіїв інформації	Так (для збереження конфігурацій, оновлення ПО)
Підтримка DLNA	Ні
Підтримка Auto-MDI/MDI-X	Так
Консольний порт	Так, RS-232(RJ-45)
Об'єм оперативної пам'яті	4 ГБ
Об'єм Flash пам'яті	16 ГБ

Управління

Параметр	Характеристика
Web-інтерфейс	Так
Підтримка SSH	Так
Підтримка SNMP	Так
NAT	Так
DHCP-сервер	Так

Експлуатаційні характеристики

Параметр	Характеристика
Робоча температура	від 0°C до 40°C
Температура зберігання	від -40°C до 70°C
Вологість при експлуатації	від 5% до 85%, без утворення конденсату
Вологість при зберіганні	від 5% до 95%, без утворення конденсату

Джерело живлення

Параметр	Характеристика
Напруга	100–240 В змінного струму (АС), 50–60 Гц

Підтримка операційних систем

Параметр	Характеристика
Підтримувані операційні системи	Cisco IOS XE (версії 16.x і вище)

Інші характеристики

Параметр	Характеристика
Габарити	44.5 x 36.5 x 4.4 см
Вага нетто	Приблизно 3.97 кг
Вага брутто	Залежить від упаковки та комплектації

Посилання на опис на сайті виробника - <http://www.cisco.com>

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		93

Б.2 Технічні характеристики комутатора Cisco Systems WS-C2960X-24TS-L

Параметр	Характеристика
Кількість портів	24
Порти введення/виводу	24 x 10/100/1000 Ethernet, 4 x SFP (оптичні)
Флеш-пам'ять	64 МБ
Монтаж у стійку	1U
Розміри Ш x Г x В	445 x 251 x 44 мм
Вага	3,2 кг
Емісії звукового тиску	43 дБ
Вимоги до живлення	100-240VAC, 1.3-0.8A, 50-60 Hz
Мінімальний обсяг ОЗУ	256 МБ
Середній час напрацювання на відмову	1500 000 год
Безпека	802.1X, ACL, Secure Shell (SSH), RADIUS, TACACS+
Діапазон відносної вологості при експлуатації	10 – 90 %
Діапазон температури зберігання	-40 до 70 °C
Діапазон температур у робочому режимі	0 до 45 °C
Висота над рівнем моря в неробочому режимі	До 12000 м
Технологія підключення	Ethernet, SFP (Small Form-factor Pluggable)
Швидкість передачі (макс)	1 Гбіт/с на порт
Швидкість передачі	До 24 Гбіт/с (сумарно)
Комутаційна здатність	216 Гбіт/с
Розмір адресної таблиці	16000 записів

		Присяжнюк Я.В.			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				94
Змн.	Арк.	№ докум.	Підпис	Дата		

Характеристики мережі	VLAN, QoS, Multicast, Spanning Tree Protocol (STP)
Стандарти мережі	IEEE 802.3, 802.3u, 802.3ab, 802.1Q, 802.1p
Протоколи управління	SNMP, RMON, CLI, Cisco IOS Software
Протокол каналу передачі	Ethernet IEEE 802.3

ДОДАТОК В

Лістинг конфігурації пристроїв

R-24-16-1

```
!  
! Last configuration change at 18:34:58 UTC Wed Jun 12 2024  
upgrade fpd auto  
version 15.2  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname R-24-16-1  
!  
boot-start-marker  
boot-end-marker  
!  
!  
logging userinfo  
logging buffered 32000  
enable secret 5 $1$ZpM5$G26c/TxTIWLgpuTFGpHio.  
!  
no aaa new-model  
no ip icmp rate-limit unreachable  
!  
!  
!  
ip dhcp excluded-address 191.24.16.1 191.24.16.10  
ip dhcp excluded-address 191.24.16.12 191.24.16.15  
ip dhcp excluded-address 191.24.16.126  
!  
ip dhcp pool MY-LAN  
network 191.24.16.0 255.255.255.128  
default-router 191.24.16.126  
dns-server 191.24.16.14
```

```

domain-name prysiazhniuk.net
!
!
!
no ip domain lookup
ip domain name prysiazhniuk.net
ip cef
login block-for 300 attempts 3 within 3
login delay 5
login on-failure log
login on-success log
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
username Yasya privilege 15 secret 5 $1$2E3/$DwAFwQtjsllc24rGzrHvi1
username Technic secret 5 $1$8P2t$X8DM.wnHe9uFvOgvVkKX/0
!
redundancy
!
!
ip tcp synwait-time 5
ip ssh maxstartups 5
ip ssh time-out 60
ip ssh authentication-retries 5
ip ssh logging events
ip ssh version 2
!
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
ip address 192.24.16.2 255.255.255.248
duplex half
!
interface FastEthernet1/0
ip address 191.24.16.126 255.255.255.128
duplex auto

```

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		96

```

speed auto
!
interface FastEthernet1/1
no ip address
shutdown
duplex auto
speed auto
!
router ospf 1
network 191.24.16.0 0.0.0.127 area 0
network 192.24.16.0 0.0.0.7 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
!
logging trap warnings
logging host 191.24.16.12
access-list 10 permit 191.24.16.1
access-list 10 permit 191.24.16.15
access-list 10 deny any
no cdp log mismatch duplex
!
!
!
control-plane
!
!
!
mgcp profile default
!
!
!
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
access-class 10 in

```

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				97
Змн.	Арк.	№ докум.	Підпис	Дата		

```

logout-warning 30
absolute-timeout 10
logging synchronous
login local
transport input ssh
transport output ssh
!
ntp authentication-key 191 md5 0822455D0A16544541 7
ntp authenticate
ntp trusted-key 191
ntp update-calendar
ntp server 191.24.16.13 key 191
!
end

```

R-24-16-2

```

Current configuration : 2033 bytes
!
upgrade fpd auto
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R-24-16-2
!
boot-start-marker
boot-end-marker
!
!
logging userinfo
logging buffered 32000
enable secret 5 $1$4Xxy$6s6btyU96mdn0byUCzznC1
!
no aaa new-model
no ip icmp rate-limit unreachable
!
!
!
!
!
!
no ip domain lookup
ip domain name prysiazhniuk.net
ip cef
login block-for 300 attempts 3 within 3
login delay 5
login on-failure log
login on-success log

```

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		98

```

no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
username Yasya privilege 15 secret 5 $1$DdXF$829kvwSE9i3m/iaqdONWh.
username Technic secret 5 $1$N8OQ$SrgMCWlizrs4o6Ey1cEf91
!
redundancy
!
!
ip tcp synwait-time 5
ip ssh maxstartups 5
ip ssh time-out 60
ip ssh authentication-retries 5
ip ssh logging events
ip ssh version 2
!
!
!
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
ip address 192.24.16.1 255.255.255.248
duplex half
!
interface FastEthernet1/0
ip address 192.24.16.9 255.255.255.248
duplex auto
speed auto
!
interface FastEthernet1/1
no ip address
shutdown
duplex auto
speed auto
!
router ospf 1
network 192.24.16.0 0.0.0.7 area 0
network 192.24.16.8 0.0.0.7 area 0

```

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				99
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
!
logging trap warnings
logging host 191.24.16.12
access-list 10 permit 191.24.16.15
access-list 10 permit 191.24.16.126
access-list 10 permit 192.24.16.2
access-list 10 deny any
no cdp log mismatch duplex
!
!
!
control-plane
!
!
!
mgcp profile default
!
!
!
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
access-class 10 in
logout-warning 30
absolute-timeout 10
logging synchronous
login local
transport input ssh
transport output ssh
!
ntp authentication-key 191 md5 094F471A1A0A464058 7
ntp authenticate
ntp trusted-key 191

```

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		100

```
ntp update-calendar
ntp server 191.24.16.13 key 191
!
end
```

SW-24-16-1

```
!
! Last configuration change at 18:55:13 UTC Wed Jun 12 2024
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-24-16-1
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
enable secret 5 $1$4NCI$PHw3Zs/M8BBxzjgDsIw.g/
!
username Yasya privilege 15 secret 5 $1$MP1.$oofGUHhO3331js6gEn5yY/
username Technic secret 5 $1$TcY.$arOximjN7F8lmKqqsXE9Z0
no aaa new-model
!
!
!
!
!
no ip icmp rate-limit unreachable
!
!
!
ip dhcp snooping
no ip domain-lookup
ip domain-name prysiazhniuk.net
ip cef
login block-for 300 attempts 3 within 3
login delay 5
login on-failure log
login on-success log
no ipv6 cef
!
!
port-channel load-balance src-dst-mac
```

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		101

```
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 1 priority 28672
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
ip ssh maxstartups 5
ip ssh time-out 60
ip ssh authentication-retries 5
ip ssh logging events
ip ssh version 2
!
!
!
!
!
!
!
!
!
!
!
!
interface Port-channel2
description AGGREGATED-LINK-TO-SW-24-16-2
!
interface Port-channel1
description AGGREGATED-LINK-TO-SW-24-16-3
!
interface Ethernet0/0
spanning-tree guard root
ip dhcp snooping limit rate 256
ip dhcp snooping trust
!
interface Ethernet0/1
spanning-tree guard root
ip dhcp snooping limit rate 256
ip dhcp snooping trust
!
interface Ethernet0/2
channel-group 2 mode on
spanning-tree guard root
ip dhcp snooping limit rate 256
ip dhcp snooping trust
!
interface Ethernet0/3
channel-group 2 mode on
spanning-tree guard root
ip dhcp snooping limit rate 256
ip dhcp snooping trust
```

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				102
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
interface Ethernet1/0
 spanning-tree guard root
 ip dhcp snooping limit rate 256
 ip dhcp snooping trust
!
interface Ethernet1/1
 channel-group 1 mode on
 spanning-tree guard root
 ip dhcp snooping limit rate 256
 ip dhcp snooping trust
!
interface Ethernet1/2
 channel-group 1 mode on
 spanning-tree guard root
 ip dhcp snooping limit rate 256
 ip dhcp snooping trust
!
interface Ethernet1/3
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
 ip address 191.24.16.1 255.255.255.128
!
 ip default-gateway 191.24.16.126
 ip forward-protocol nd
!
 no ip http server
 no ip http secure-server
!
!
!
 access-list 10 permit 191.24.16.15
 access-list 10 deny any
!
!
!

```

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		103

```

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
access-class 10 in
logout-warning 30
absolute-timeout 10
logging synchronous
login local
transport input ssh
transport output ssh
!
ntp authentication-key 191 md5 060506324F41584B56 7
ntp authenticate
ntp trusted-key 191
ntp update-calendar
ntp server 191.24.16.13 key 191
!
end

```

SW-24-16-2

```

!
! Last configuration change at 18:58:53 UTC Wed Jun 12 2024
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-24-16-2
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
enable secret 5 $1$5lUB$JLD/Kt2D9dbdKLRPg3mia/
!
username Yasya privilege 15 secret 5 $1$M1uu$Px5/HE5a9JlPq4uCI3ZmE/

```

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		104

```
username Technic secret 5 $1$hGG1$D7KR9np1hjVpR38zhdDWM1
no aaa new-model
!
!
!
!
!
no ip icmp rate-limit unreachable
!
!
!
ip dhcp snooping
no ip domain-lookup
ip domain-name prysiazniuk.net
ip cef
login block-for 300 attempts 3 within 3
login delay 5
login on-failure log
login on-success log
no ipv6 cef
!
!
errdisable recovery cause bpduguard
errdisable recovery interval 60
port-channel load-balance src-dst-mac
!
spanning-tree mode rapid-pvst
spanning-tree portfast default
spanning-tree portfast bpduguard default
spanning-tree extend system-id
spanning-tree vlan 1 priority 36864
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
ip ssh maxstartups 5
ip ssh time-out 60
ip ssh authentication-retries 5
ip ssh logging events
ip ssh version 2
!
!
!
!
!
!
!
!
!
!
```

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				105
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface Port-channel4
description AGGREGATED-LINK-TO-SW-24-16-4
!
interface Port-channel2
description AGGREGATED-LINK-TO-SW-24-16-1
!
interface Ethernet0/0
channel-group 2 mode on
spanning-tree portfast disable
spanning-tree bpduguard disable
spanning-tree guard loop
ip dhcp snooping limit rate 256
ip dhcp snooping trust
!
interface Ethernet0/1
channel-group 2 mode on
spanning-tree portfast disable
spanning-tree bpduguard disable
spanning-tree guard loop
ip dhcp snooping limit rate 256
ip dhcp snooping trust
!
interface Ethernet0/2
channel-group 4 mode on
spanning-tree portfast disable
spanning-tree bpduguard disable
spanning-tree guard loop
ip dhcp snooping limit rate 256
ip dhcp snooping trust
!
interface Ethernet0/3
channel-group 4 mode on
spanning-tree portfast disable
spanning-tree bpduguard disable
spanning-tree guard loop
ip dhcp snooping limit rate 256
ip dhcp snooping trust
!
interface Ethernet1/0
spanning-tree portfast disable
spanning-tree bpduguard disable
spanning-tree guard loop
ip dhcp snooping limit rate 256
ip dhcp snooping trust
!
interface Ethernet1/1
spanning-tree portfast disable
spanning-tree bpduguard disable
spanning-tree guard loop
ip dhcp snooping limit rate 256
ip dhcp snooping trust
!

```

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		106

```

interface Ethernet1/2
!
interface Ethernet1/3
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
ip address 191.24.16.2 255.255.255.128
!
ip default-gateway 191.24.16.126
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
access-list 10 permit 191.24.16.15
access-list 10 deny any
!
!
!
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
access-class 10 in
logout-warning 30
absolute-timeout 10
logging synchronous

```

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		107

```

login local
transport input ssh
transport output ssh
!
ntp authentication-key 191 md5 121A0C0411045D5679 7
ntp authenticate
ntp trusted-key 191
ntp update-calendar
ntp server 191.24.16.13 key 191
!
end

```

SW-24-16-3

```

!
! Last configuration change at 19:06:46 UTC Wed Jun 12 2024
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-24-16-3
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
enable secret 5 $1$Bvw0$otUWxtDZYer4wCwvtv1sa.
!
username Yasya privilege 15 secret 5 $1$okSj$f1xRjvqcuNSFmV137nQCz.
username Technic secret 5 $1$98nV$c7DaIpnvxEJWh371nvWyl/
no aaa new-model
!
!
!
!
!
no ip icmp rate-limit unreachable
!
!
!
ip dhcp snooping
no ip domain-lookup
ip domain-name prysiazhniuk.net
ip cef
login block-for 300 attempts 3 within 3

```

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		108

```
login delay 5
login on-failure log
login on-success log
no ipv6 cef
!
!
errdisable recovery cause bpduguard
errdisable recovery interval 60
port-channel load-balance src-dst-mac
!
spanning-tree mode rapid-pvst
spanning-tree portfast default
spanning-tree portfast bpduguard default
spanning-tree extend system-id
spanning-tree vlan 1 priority 45056
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
ip ssh maxstartups 5
ip ssh time-out 60
ip ssh authentication-retries 5
ip ssh logging events
ip ssh version 2
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Port-channel3
description AGGREGATED-LINK-TO-SW-24-16-4
!
interface Port-channel1
description AGGREGATED-LINK-TO-SW-24-16-1
!
interface Ethernet0/0
channel-group 1 mode on
spanning-tree portfast disable
spanning-tree bpduguard disable
spanning-tree guard loop
ip dhcp snooping limit rate 256
ip dhcp snooping trust
!
interface Ethernet0/1
channel-group 1 mode on
```

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				109
Змн.	Арк.	№ докум.	Підпис	Дата		

```

spanning-tree portfast disable
spanning-tree bpduguard disable
spanning-tree guard loop
ip dhcp snooping limit rate 256
ip dhcp snooping trust
!
interface Ethernet0/2
channel-group 3 mode on
spanning-tree portfast disable
spanning-tree bpduguard disable
spanning-tree guard loop
ip dhcp snooping limit rate 256
ip dhcp snooping trust
!
interface Ethernet0/3
channel-group 3 mode on
spanning-tree portfast disable
spanning-tree bpduguard disable
spanning-tree guard loop
ip dhcp snooping limit rate 256
ip dhcp snooping trust
!
interface Ethernet1/0
spanning-tree portfast disable
spanning-tree bpduguard disable
spanning-tree guard loop
ip dhcp snooping limit rate 256
ip dhcp snooping trust
!
interface Ethernet1/1
spanning-tree portfast disable
spanning-tree bpduguard disable
spanning-tree guard loop
ip dhcp snooping limit rate 256
ip dhcp snooping trust
!
interface Ethernet1/2
!
interface Ethernet1/3
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
!

```

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				110
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
 ip address 191.24.16.3 255.255.255.128
!
 ip default-gateway 191.24.16.126
 ip forward-protocol nd
!
 no ip http server
 no ip http secure-server
!
!
!
 access-list 10 permit 191.24.16.15
 access-list 10 deny any
!
!
!
 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
  access-class 10 in
  logout-warning 30
  absolute-timeout 10
  logging synchronous
  login local
  transport input ssh
  transport output ssh
!
 ntp authentication-key 191 md5 05080F1C22431F5B4A 7
 ntp authenticate
 ntp trusted-key 191
 ntp update-calendar
 ntp server 191.24.16.13 key 191
!
end

```

SW-24-16-4

!

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		111

```

! Last configuration change at 19:04:02 UTC Wed Jun 12 2024
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-24-16-4
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
enable secret 5 $1$ypbB$JsSsQ021g1WF3s26PJYpM0
!
username Yasya privilege 15 secret 5 $1$zT/2$LZsql0Cs9.HR1Sb5Dqgi.1
username Technic secret 5 $1$CrN3$dtc8QX33Tdn8ELBCb85M9.
no aaa new-model
!
!
!
!
!
no ip icmp rate-limit unreachable
!
!
!
ip dhcp snooping
no ip domain-lookup
ip domain-name prysiazhniuk.net
ip cef
login block-for 300 attempts 3 within 3
login delay 5
login on-failure log
login on-success log
no ipv6 cef
!
!
errdisable recovery cause bpduguard
errdisable recovery interval 60
port-channel load-balance src-dst-mac
!
spanning-tree mode rapid-pvst
spanning-tree portfast default
spanning-tree portfast bpduguard default
spanning-tree extend system-id
spanning-tree vlan 1 priority 45056
!

```

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		112

```
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
ip ssh maxstartups 5
ip ssh time-out 60
ip ssh authentication-retries 5
ip ssh logging events
ip ssh version 2
!
!
!
!
!
!
!
!
!
!
!
!
interface Port-channel4
description AGGREGATED-LINK-TO-SW-24-16-2
!
interface Port-channel3
description AGGREGATED-LINK-TO-SW-24-16-3
!
interface Ethernet0/0
channel-group 3 mode on
spanning-tree portfast disable
spanning-tree bpduguard disable
spanning-tree guard loop
ip dhcp snooping limit rate 256
ip dhcp snooping trust
!
interface Ethernet0/1
channel-group 3 mode on
spanning-tree portfast disable
spanning-tree bpduguard disable
spanning-tree guard loop
ip dhcp snooping limit rate 256
ip dhcp snooping trust
!
interface Ethernet0/2
channel-group 4 mode on
spanning-tree portfast disable
spanning-tree bpduguard disable
spanning-tree guard loop
ip dhcp snooping limit rate 256
ip dhcp snooping trust
!
interface Ethernet0/3
channel-group 4 mode on
```

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				113
Змн.	Арк.	№ докум.	Підпис	Дата		

```

spanning-tree portfast disable
spanning-tree bpduguard disable
spanning-tree guard loop
ip dhcp snooping limit rate 256
ip dhcp snooping trust
!
interface Ethernet1/0
spanning-tree portfast disable
spanning-tree bpduguard disable
spanning-tree guard loop
ip dhcp snooping limit rate 256
ip dhcp snooping trust
!
interface Ethernet1/1
spanning-tree portfast disable
spanning-tree bpduguard disable
spanning-tree guard loop
ip dhcp snooping limit rate 256
ip dhcp snooping trust
!
interface Ethernet1/2
!
interface Ethernet1/3
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
ip address 191.24.16.4 255.255.255.128
!
ip default-gateway 191.24.16.126
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
access-list 10 permit 191.24.16.15

```

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		114

```

access-list 10 deny any
!
!
!
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
access-class 10 in
logout-warning 30
absolute-timeout 10
logging synchronous
login local
transport input ssh
transport output ssh
!
ntp authentication-key 191 md5 0822455D0A16544541 7
ntp authenticate
ntp trusted-key 191
ntp update-calendar
ntp server 191.24.16.13 key 191
!
end

```

SW-24-16-5

```

!
! Last configuration change at 18:37:33 UTC Wed Jun 12 2024
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-24-16-5
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000

```

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		115

```
logging console discriminator EXCESS
enable secret 5 $1$c1M7$19X3uWOjPdZqDbBIgw.C61
!
username Yasya privilege 15 secret 5 $1$y5nF$fcc7AES9iAG1QajlkmFhh0
username Technic secret 5 $1$jSgL$k8xvFwUMy.Rz0OZNUhuAt.
no aaa new-model
!
!
!
!
!
no ip icmp rate-limit unreachable
!
!
!
ip dhcp snooping
no ip domain-lookup
ip domain-name prysiazniuk.net
ip cef
login block-for 300 attempts 3 within 3
login delay 5
login on-failure log
login on-success log
no ipv6 cef
!
!
errdisable recovery cause bpduguard
errdisable recovery interval 60
spanning-tree mode pvst
spanning-tree portfast default
spanning-tree portfast bpduguard default
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
ip ssh maxstartups 5
ip ssh time-out 60
ip ssh authentication-retries 5
ip ssh logging events
ip ssh version 2
!
!
!
!
!
!
!
!
!
```

```

!
interface Ethernet0/0
 spanning-tree portfast disable
 spanning-tree bpduguard enable
 spanning-tree bpduguard disable
 ip dhcp snooping limit rate 256
 ip dhcp snooping trust
!
interface Ethernet0/1
 spanning-tree portfast disable
 spanning-tree bpduguard enable
 spanning-tree bpduguard disable
 ip dhcp snooping limit rate 256
 ip dhcp snooping trust
!
interface Ethernet0/2
 spanning-tree portfast
 spanning-tree bpduguard enable
 spanning-tree guard loop
!
interface Ethernet0/3
 spanning-tree portfast
 spanning-tree bpduguard enable
 spanning-tree guard loop
!
interface Ethernet1/0
 spanning-tree portfast
 spanning-tree bpduguard enable
 spanning-tree guard loop
!
interface Ethernet1/1
!
interface Ethernet1/2
!
interface Ethernet1/3
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!

```

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				117
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface Vlan1
 ip address 191.24.16.5 255.255.255.128
 !
 ip default-gateway 191.24.16.126
 ip forward-protocol nd
 !
 no ip http server
 no ip http secure-server
 !
 !
 !
 access-list 10 permit 191.24.16.15
 access-list 10 deny any
 !
 !
 !
 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
 access-class 10 in
 logout-warning 30
 absolute-timeout 10
 logging synchronous
 login local
 transport input ssh
 transport output ssh
 !
 ntp authentication-key 191 md5 110A1016141D5A5E57 7
 ntp authenticate
 ntp trusted-key 191
 ntp update-calendar
 ntp server 191.24.16.13 key 191
 !
 end

```

SW-24-16-6

```

!
! Last configuration change at 18:48:37 UTC Wed Jun 12 2024
!
version 15.2
service timestamps debug datetime msec

```

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		118

```

service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-24-16-6
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
enable secret 5 $1$6NGF$DvWkk.3Iy4Jn0ibnFi0UW/
!
username Yasya privilege 15 secret 5 $1$aDGQ$/JdC0rPqnil0Gj/Dsutkk0
username Technic secret 5 $1$4RZH$7.dLPFaE3gtz/2hxGL1Xm1
no aaa new-model
!
!
!
!
!
no ip icmp rate-limit unreachable
!
!
!
!
ip dhcp snooping
no ip domain-lookup
ip domain-name prysiazhniuk.net
ip cef
login block-for 300 attempts 3 within 3
login delay 5
login on-failure log
login on-success log
no ipv6 cef
!
!
errdisable recovery cause bpduguard
errdisable recovery interval 60
spanning-tree mode pvst
spanning-tree portfast default
spanning-tree portfast bpduguard default
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
ip ssh maxstartups 5
ip ssh time-out 60
ip ssh authentication-retries 5
ip ssh logging events

```

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		119

```

ip ssh version 2
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
spanning-tree portfast disable
spanning-tree bpduguard disable
spanning-tree guard loop
ip dhcp snooping limit rate 256
ip dhcp snooping trust
!
interface Ethernet0/1
spanning-tree portfast
spanning-tree bpdufilter enable
spanning-tree bpduguard enable
!
interface Ethernet0/2
spanning-tree portfast
spanning-tree bpdufilter enable
spanning-tree bpduguard enable
!
interface Ethernet0/3
spanning-tree portfast
spanning-tree bpdufilter enable
spanning-tree bpduguard enable
!
interface Ethernet1/0
spanning-tree portfast
spanning-tree bpdufilter enable
spanning-tree bpduguard enable
!
interface Ethernet1/1
!
interface Ethernet1/2
!
interface Ethernet1/3
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!

```

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				120
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
 ip address 191.24.16.6 255.255.255.128
!
 ip default-gateway 191.24.16.126
 ip forward-protocol nd
!
 no ip http server
 no ip http secure-server
!
!
!
 access-list 10 permit 191.24.16.15
 access-list 10 deny any
!
!
!
 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
  access-class 10 in
  logout-warning 30
  absolute-timeout 10
  logging synchronous
  login local
  transport input ssh
  transport output ssh
!
 ntp authentication-key 191 md5 104D000A061843595F 7
 ntp authenticate
 ntp trusted-key 191
 ntp update-calendar
 ntp server 191.24.16.13 key 191
!

```

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		121

end

SW-24-16-7

!
! Last configuration change at 18:54:10 UTC Wed Jun 12 2024
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-24-16-7
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
enable secret 5 \$1\$hOJn\$ftO6/1yZyRdaqDP3zCx761
!
username Yasya privilege 15 secret 5 \$1\$4zBv\$0c7g..FcwgaNTo4ZHrfeY.
username Technic secret 5 \$1\$jC6\$eFbc.yEioPYP19IodWG61.
no aaa new-model
!
!
!
!
!
no ip icmp rate-limit unreachable
!
!
!
ip dhcp snooping
no ip domain-lookup
ip domain-name prysiazhniuk.net
ip cef
login block-for 300 attempts 3 within 3
login delay 5
login on-failure log
login on-success log
no ipv6 cef
!
!
errdisable recovery cause bpduguard
errdisable recovery interval 60
spanning-tree mode pvst
spanning-tree portfast default

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		122

```

spanning-tree portfast bpduguard default
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
ip ssh maxstartups 5
ip ssh time-out 60
ip ssh authentication-retries 5
ip ssh logging events
ip ssh version 2
!
!
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
spanning-tree portfast disable
spanning-tree bpduguard disable
spanning-tree guard loop
ip dhcp snooping limit rate 256
ip dhcp snooping trust
!
interface Ethernet0/1
spanning-tree portfast
spanning-tree bpdufilter enable
spanning-tree bpduguard enable
!
interface Ethernet0/2
spanning-tree portfast
spanning-tree bpdufilter enable
spanning-tree bpduguard enable
!
interface Ethernet0/3
spanning-tree portfast
spanning-tree bpdufilter enable
spanning-tree bpduguard enable
!
interface Ethernet1/0
spanning-tree portfast
spanning-tree bpdufilter enable
spanning-tree bpduguard enable
!
interface Ethernet1/1
spanning-tree portfast

```

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				123
Змн.	Арк.	№ докум.	Підпис	Дата		

```

spanning-tree bpdupfilter enable
spanning-tree bpduguard enable
!
interface Ethernet1/2
spanning-tree portfast
spanning-tree bpdupfilter enable
spanning-tree bpduguard enable
!
interface Ethernet1/3
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
ip address 191.24.16.7 255.255.255.128
!
ip default-gateway 191.24.16.126
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
access-list 10 permit 191.24.16.15
access-list 10 deny any
!
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15

```

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		124

```

logging synchronous
line vty 0 4
access-class 10 in
logout-warning 30
absolute-timeout 10
logging synchronous
login local
transport input ssh
transport output ssh
!
ntp authentication-key 191 md5 13061E010803557878 7
ntp authenticate
ntp trusted-key 191
ntp update-calendar
ntp server 191.24.16.13 key 191
!
end

```

SW-24-16-8

```

!
! Last configuration change at 18:18:12 UTC Wed Jun 12 2024
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-24-16-8
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
enable secret 5 $1$fPT7$q37LYLBKFD1IuDQkAfoR01
!
username Yasya privilege 15 secret 5 $1$1Xmb$24qzt5YR2mHVTI5lPGwGn/
username Technic secret 5 $1$Nw5H$KMY8quLa.gQR5nsc4yJr.
no aaa new-model
!
!
!
!
!
no ip icmp rate-limit unreachable
!
!
!

```

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		125

```
ip dhcp snooping
no ip domain-lookup
ip domain-name prysiazniuk.net
ip cef
login block-for 300 attempts 3 within 3
login delay 5
login on-failure log
login on-success log
no ipv6 cef
!
!
errdisable recovery cause bpduguard
errdisable recovery interval 60
spanning-tree mode pvst
spanning-tree portfast default
spanning-tree portfast bpduguard default
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
ip ssh maxstartups 5
ip ssh time-out 60
ip ssh authentication-retries 5
ip ssh logging events
ip ssh version 2
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
!
interface Ethernet0/1
spanning-tree portfast disable
spanning-tree bpduguard disable
spanning-tree guard loop
ip dhcp snooping limit rate 256
ip dhcp snooping trust
!
interface Ethernet0/2
spanning-tree portfast disable
spanning-tree bpduguard disable
spanning-tree guard loop
ip dhcp snooping limit rate 256
```

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				126
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip dhcp snooping trust
!
interface Ethernet0/3
spanning-tree portfast
spanning-tree bpdudfilter enable
spanning-tree bpduguard enable
!
interface Ethernet1/0
spanning-tree portfast
spanning-tree bpdudfilter enable
spanning-tree bpduguard enable
!
interface Ethernet1/1
spanning-tree portfast
spanning-tree bpdudfilter enable
spanning-tree bpduguard enable
!
interface Ethernet1/2
spanning-tree portfast
spanning-tree bpdudfilter enable
spanning-tree bpduguard enable
!
interface Ethernet1/3
spanning-tree portfast
spanning-tree bpdudfilter enable
spanning-tree bpduguard enable
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
ip address 191.24.16.8 255.255.255.128
!
ip default-gateway 191.24.16.126
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!

```

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				127
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
!
access-list 10 permit 191.24.16.15
access-list 10 deny any
!
!
!
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
access-class 10 in
logout-warning 30
absolute-timeout 10
logging synchronous
login local
transport input ssh
transport output ssh
!
ntp authentication-key 191 md5 110A1016141D5A5E57 7
ntp authenticate
ntp trusted-key 191
ntp update-calendar
ntp server 191.24.16.13 key 191
!
end

```

SW-24-16-9

```

!
! Last configuration change at 18:43:41 UTC Wed Jun 12 2024
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-24-16-9
!
boot-start-marker
boot-end-marker
!

```

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		128


```

!
!
!
!
interface Ethernet0/0
 spanning-tree portfast disable
 spanning-tree bpduguard disable
 spanning-tree guard loop
 ip dhcp snooping limit rate 256
 ip dhcp snooping trust
!
interface Ethernet0/1
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
!
interface Ethernet0/2
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
!
interface Ethernet0/3
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
!
interface Ethernet1/0
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
!
interface Ethernet1/1
 spanning-tree portfast
 spanning-tree bpdufilter enable
 spanning-tree bpduguard enable
!
interface Ethernet1/2
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface Ethernet1/3
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Ethernet3/0
!

```

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				130
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
 ip address 191.24.16.9 255.255.255.128
!
 ip default-gateway 191.24.16.126
 ip forward-protocol nd
!
 no ip http server
 no ip http secure-server
!
!
!
 access-list 10 permit 191.24.16.15
 access-list 10 deny any
!
!
!
 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
  access-class 10 in
  logout-warning 30
  absolute-timeout 10
  logging synchronous
  login local
  transport input ssh
  transport output ssh
!
 ntp authentication-key 191 md5 13061E010803557878 7
 ntp authenticate
 ntp trusted-key 191
 ntp update-calendar
 ntp server 191.24.16.13 key 191
!
end

```

SW-24-16-10

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		131

```

!
! Last configuration change at 18:33:03 UTC Wed Jun 12 2024
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-24-16-10
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
enable secret 5 $1$sjpN$IhgpXnjFu54H8DjNvHUj.
!
username Yasya privilege 15 secret 5 $1$GzpF$EP/ru9XRbTKUpw67WqkxU.
username Technic secret 5 $1$slIE$iOzT.41Iyige0CIB3OKHF/
no aaa new-model
!
!
!
!
!
no ip icmp rate-limit unreachable
!
!
!
ip dhcp snooping
no ip domain-lookup
ip domain-name prysiazhniuk.net
ip cef
login block-for 300 attempts 3 within 3
login delay 5
login on-failure log
login on-success log
no ipv6 cef
!
!
errdisable recovery cause bpduguard
errdisable recovery interval 60
spanning-tree mode pvst
spanning-tree portfast default
spanning-tree portfast bpduguard default
spanning-tree extend system-id
!
vlan internal allocation policy ascending

```

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		132

```

!
ip tcp synwait-time 5
ip ssh maxstartups 5
ip ssh time-out 60
ip ssh authentication-retries 5
ip ssh logging events
ip ssh version 2
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
!
interface Ethernet0/1
spanning-tree portfast disable
spanning-tree bpduguard disable
spanning-tree guard loop
ip dhcp snooping limit rate 256
ip dhcp snooping trust
!
interface Ethernet0/2
spanning-tree portfast
spanning-tree bpdufilter enable
spanning-tree bpduguard enable
!
interface Ethernet0/3
spanning-tree portfast
spanning-tree bpdufilter enable
spanning-tree bpduguard enable
!
interface Ethernet1/0
spanning-tree portfast
spanning-tree bpdufilter enable
spanning-tree bpduguard enable
!
interface Ethernet1/1
spanning-tree portfast
spanning-tree bpdufilter enable
spanning-tree bpduguard enable
!
interface Ethernet1/2
!
interface Ethernet1/3
!

```

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		133

```

interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
ip address 191.24.16.10 255.255.255.128
!
ip default-gateway 191.24.16.126
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
access-list 10 permit 191.24.16.15
access-list 10 deny any
!
!
!
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
access-class 10 in
logout-warning 30
absolute-timeout 10
logging synchronous
login local
transport input ssh
transport output ssh
!

```

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		134

ntp authentication-key 191 md5 02050D4808095E731F 7
ntp authenticate
ntp trusted-key 191
ntp update-calendar
ntp server 191.24.16.13 key 191
!

en

		Присяжнюк Я.В			ККІКБ.КР.Б – 125 – 38 – ПЗ	Арк.
		Трокоз Є.М.				135
Змн.	Арк.	№ докум.	Підпис	Дата		