

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»

Кафедра комп'ютерної інженерії та кібербезпеки

ЗВІТ З ПЕРЕДДИПЛОМНОЇ ПРАКТИКИ

студента 4-го курсу групи КІ-19-1
спеціальності 123 «Комп'ютерна інженерія»
Лавренчука Віталія Олександровича
(прізвище, ім'я та по-батькові)

Керівник:
завідувач кафедри
комп'ютерної інженерії та кібербезпеки,
кандидат технічних наук,
Сфіменко Андрій Анатолійович

Дата захисту: “__” “_____” 2023 р.

Оцінка:

Національна шкала _____

Кількість балів _____

ECTS _____

Члени комісії:

_____	_____
(підпис)	(прізвище та ініціали)

_____	_____
(підпис)	(прізвище та ініціали)

_____	_____
(підпис)	(прізвище та ініціали)

м. Житомир – 2023 рік

РЕФЕРАТ

Звіт з переддипломної практики складається зі вступу, двох розділів, висновків, списку умовних скорочень, списку використаної літератури.

Теоритична частина була викладена на 30 сторінках друкованого тексту. Список використаних джерел складається з 10 позицій та займає 1 сторінку. В роботі наведено 37 рисунків. Загалом обсяг роботи складає 30 сторінку.

У першому розділі було викладено призначення ІТ-компанії “Dual Education Ukraine”.

У другому розділі було викладено основні завдання переддипломної практики та результат їх виконання.

В третьому розділі було здійснено налагодження базових параметрів адресації, активація протоколу маршрутизації BGP та його налагодження. Налаштовано захист мережі. Перевірено працездатність мережі.

Висновок містить в собі аналіз роботи ІТ-компанії “Dual Education Ukraine.

КЛЮЧОВІ СЛОВА: DEU, ПІДТРИМКА, ОБСЛУГОВУВАННЯ РОБОЧИХ СТАНЦІЙ, ПЕРЕВІРКА ПРАЦЕЗДАТНОСТІ ПРИСТРОЇВ, НАДАННЯ КОНСУЛЬТАЦІЙ.

					ДУ «Житомирська політехніка».20.123.9.000 – ПР							
Змн.	Арк.	№ докум.	Підпис	Дата								
Розроб.		Лавренчук В.О.			Звіт з виробничої практики				Лім.	Арк.	Аркуші	
Перевір.		Єфіменко А.А.									4	
Керівник									ФІКТ Гр. КІ-19-1[1]			
Н. контр.												
Зав. каф.												

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ	3
Вступ.....	4
РОЗДІЛ 1. ВІДОМОСТІ ПРО МІСЦЕ ПРОХОДЖЕННЯ ПРАКТИКИ.....	6
1.1 ІТ-компанія “Dual Education Ukraine”	6
РОЗДІЛ 2 ЗАВДАННЯ ПРАКТИКИ.....	7
2.1. Актуальність теми	7
2.2.Теоретичні основи побудови мережі з використанням протоколу маршрутизації BGP.....	7
2.3 Windows Server та Active Directory	15
2.4. Топологія мережі	17
РОЗДІЛ 3 НАЛАГОДЖЕННЯ ОБЛАДНАННЯ	22
3.1 Налагодження обладнання мережі.....	22
3.2 Перевірка працездатності мережі	27
ВИСНОВОК.....	30
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	31

		Лавренчук В О			ДУ «Житомирська політехніка».20.123.9.000 – ПР	Арк.
		Єфіменко А.А				2
Змн.	Арк.	№ докум.	Підпис	Дата		

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

BGP – Border Gateway Protocol – Протокол Граничного Шлюзу

AS – Autonomous System – Автономна Система

ASN Autonomous System Number Номер автономної системи

eBGP – External BGP – Зовнішній Протокол Граничного Шлюзу

iBGP – Interior BGP – Внутрішній Протокол Граничного Шлюзу

		Лавренчук В О			ДУ «Житомирська політехніка».20.123.9.000 – ПР	Арк.
		Єфіменко А.А				3
Змн.	Арк.	№ докум.	Підпис	Дата		

Вступ

Для формування повного розуміння про майбутню професію потрібно використати отримані навички протягом минулих років на практиці, а саме на підприємстві, де без спеціалістів такої сфери діяльності неможливо обійтися.

Об'єктом проходження практики є **відділ програмного забезпечення ІТ-компанії “Dual Education Ukraine”**.

Предметом практики є набуття нових знань, навичок та досвіду.

Мета проходження практики полягає у закріпленні набутих за час навчання теоретичних та практичних знань у сфері програмування, комп'ютерних мереж, захисту-інформації та адміністрування систем.

Основними завданнями проходження практики у відділі програмного забезпечення ІТ-компанії **“Dual Education Ukraine”**. є :

- ознайомлення з підприємством, методами роботи та принципами виконання робіт;
- розробка макету мережі на базі протоколу маршрутизації BGP та авторизація та аутентифікація користувачів на базі Active Directory;

Метою діяльності відділу програмного забезпечення ІТ-компанії **“Dual Education Ukraine”** є адміністрування загальносистемного програмного забезпечення, забезпечення безперебійної роботи комп'ютерної інформаційної системи департаменту. Також метою є організація та підтримка електронного обміну інформацією з підприємствами, установами, організаціями, органами державної влади, місцевого самоврядування та іншими суб'єктами інформаційних відносин. Крім того забезпечення цілісності та актуальності баз даних програмних комплексів, що використовуються в департаменті, тестування та впровадження змін і доповнень до діючих програмних комплексів та підсистем. Забезпечення автоматизації робочих місць і процесів, що утворюються в департаменті, здійснення технічного обслуговування та налаштування засобів електронно-обчислювальної техніки, функціонування комп'ютерної інформаційної мережі та організаційної техніки. Впровадження систем захисту інформації, встановлення антивірусних про-

		Лавренчук В О			ДУ «Житомирська політехніка».20.123.9.000 – ПР	Арк.
		Єфіменко А.А				4
Змн.	Арк.	№ докум.	Підпис	Дата		

грам, резервування інформації, здійснення моніторингу використання працівниками програмних засобів та інформаційних ресурсів. Формування необхідних масивів даних та встановленої звітності, що забезпечується засобами спеціалізованих програмно-технологічних комплексів та підсистем, розроблених для реалізації державної політики в сфері соціального захисту населення.

		Лавренчук В О			ДУ «Житомирська політехніка».20.123.9.000 – ПР	Арк.
		Єфіменко А.А				5
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1. ВІДОМОСТІ ПРО МІСЦЕ ПРОХОДЖЕННЯ ПРАКТИКИ

1.1 ІТ-компанія “Dual Education Ukraine”

Dual Education Ukraine – організація злагодженої взаємодії всіх зацікавлених сторін, сприяння дотриманню їх прав, моніторингу якості надання освітніх послуг, об’єктивної оцінки участі всіх суб’єктів освітнього процесу у підготовці майбутніх ІТ-фахівців та їх працевлаштуванні.

Використовуючи елементи дуальної форми навчання, компанія прагне компенсувати основні недоліки традиційної інституційної освіти: розрив між теорією і практикою, освітою і виробництвом, домінування неефективних форм і методів навчання, тривалі терміни навчання і відставання від розвитку. навчальні програми від стрімких технологічних змін у сучасній ІТ-індустрії.

DEU – український центр дуальної освіти та ІТ-компанія, команда з понад 50 мислителів і творців, справжніх професіоналів і хороших людей.

		Лавренчук В О			ДУ «Житомирська політехніка».20.123.9.000 – ПР	Арк.
		Єфіменко А.А				6
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2 ЗАВДАННЯ ПРАКТИКИ

2.1. Актуальність теми

Розробка мережі на базі протоколу маршрутизації BGP та авторизація та аутентифікація користувачів на базі Active Directory є актуальною темою в сучасному світі інформаційних технологій.

BGP є протоколом маршрутизації, який використовується в глобальному Інтернеті для обміну маршрутною інформацією між провайдерами та іншими мережами. Використання BGP у внутрішніх мережах дозволяє забезпечити стійкість та надійність мережі, що є особливо важливим у великих компаніях з великою кількістю вузлів.

Авторизація та аутентифікація користувачів на базі Active Directory також є дуже важливою, оскільки забезпечує захист мережі від несанкціонованого доступу та надає можливість централізовано керувати доступом користувачів до ресурсів мережі.

Розробка мережі на базі протоколу маршрутизації BGP та авторизації та аутентифікації користувачів на базі Active Directory може бути особливо важливою для підприємств з великою кількістю вузлів та користувачів, де безпека мережі та її стійкість є критичними аспектами. Крім того, така розробка може зменшити витрати на управління мережею та забезпечити більш ефективне використання ресурсів.

2.2. Теоретичні основи побудови мережі з використанням протоколу маршрутизації BGP

Завдання практики є побудова мережі на базі протоколу маршрутизації BGP та її адміністрування з-за допомогою Active Directory. Перед тим як розпочати вивчення основного протоколу, що буде вивчатися при виконанні даного переддипломного проєкту слід познайомитись з поняттям, що тісно пов'язане з BGP, а саме автономна система(AS).

		Лавренчук В О			ДУ «Житомирська політехніка».20.123.9.000 – ПР	Арк.
		Єфіменко А.А				7
Змн.	Арк.	№ докум.	Підпис	Дата		

Автономна система (AS) в інтернеті - це система IP-мереж і маршрутизаторів, керованих одним або декількома операторами, що мають єдину політику маршрутизації з Інтернетом.

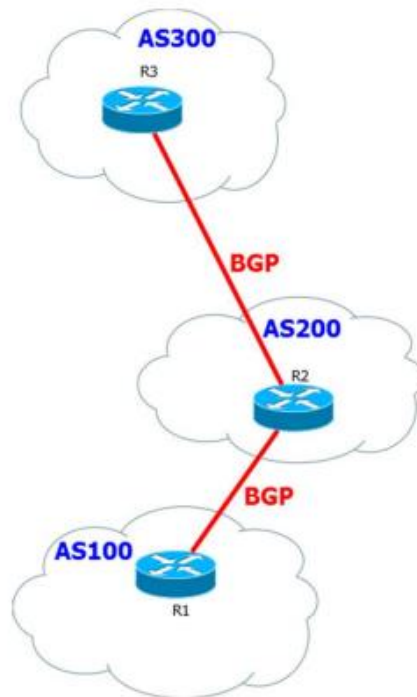


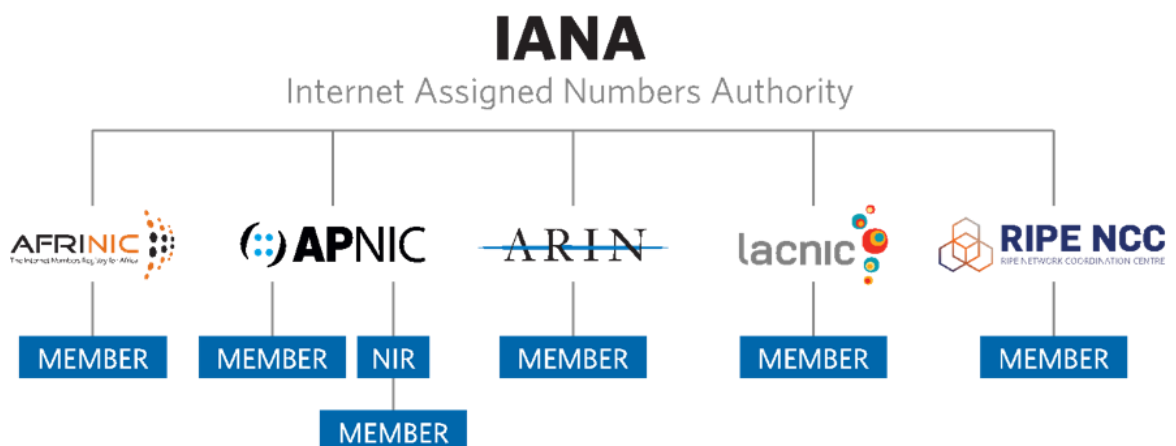
Рисунок 2.1 – Автономні системи

Спочатку визначення вимагало контролю з боку однієї сутності, як правило, інтернет провайдер (ISP) або дуже велика організація з незалежними підключеннями до декількох мереж, яка дотримується єдиної і чітко визначеної політики маршрутизації, як це було спочатку визначено в RFC 1771. Новіше визначення в RFC 1930 увійшов у користування, оскільки можуть працювати кілька організацій Протокол прикордонних шлюзів (BGP) з використанням приватних номерів AS для Інтернет-провайдер що пов'язує всі ці організації з Інтернетом. Незважаючи на те, що Інтернет-провайдер може підтримувати кілька автономних систем, Інтернет бачить лише політику маршрутизації Інтернет-провайдера. Цей Інтернет-провайдер повинен мати офіційну реєстрацію номер автономної системи (ASN).

Для використання в маршрутизації BGP кожному AS виділяється унікальний ASN. ASN важливі, оскільки ASN однозначно ідентифікує кожну мережу в Інтернеті. До 2007 р. Числа AS визначалися як 16-розрядні цілі числа, що

		Лавренчук В О			ДУ «Житомирська політехніка».20.123.9.000 – ПР	Арк.
		Єфіменко А.А				8
Змн.	Арк.	№ докум.	Підпис	Дата		

дозволяло максимум 65 536 присвоєнь. RFC 4893 введено 32-розрядні номери AS, які Орган, призначений Інтернетом (IANA) почав розподіляти до регіональний Інтернет-реєстр (RIR), хоча даний запропонований стандарт зараз замінено на RFC 6793. Ці числа записуються переважно як прості цілі числа (у позначенні, яке іноді називають "як пояснити"), від 0 до 4 294 967 295 (шістнадцяткова 0xFFFF FFFF), або у формі "asdot", яка виглядає так x.y, де x і y - це 16-розрядні числа. Номери форми 0.y - це саме старі 16-розрядні числа AS. Прийняте текстове подання автономних системних номерів визначено в RFC 5396 як "аплайн". Спеціальний 16-розрядний ASN 23456 ("AS_TRANS") було призначено IANA як заповнювач для 32-розрядних значень ASN у випадку, коли 32-розрядні ASN-маршрутизатори ("нові колонки BGP") надсилають повідомлення BGP маршрутизаторам із старим програмним забезпеченням BGP ("старі колонки BGP"), зрозуміти нові 32-розрядні ASN.



		Лавренчук В О			ДУ «Житомирська політехніка».20.123.9.000 – ПР	Арк.
		Єфіменко А.А				9
Змн.	Арк.	№ докум.	Підпис	Дата		

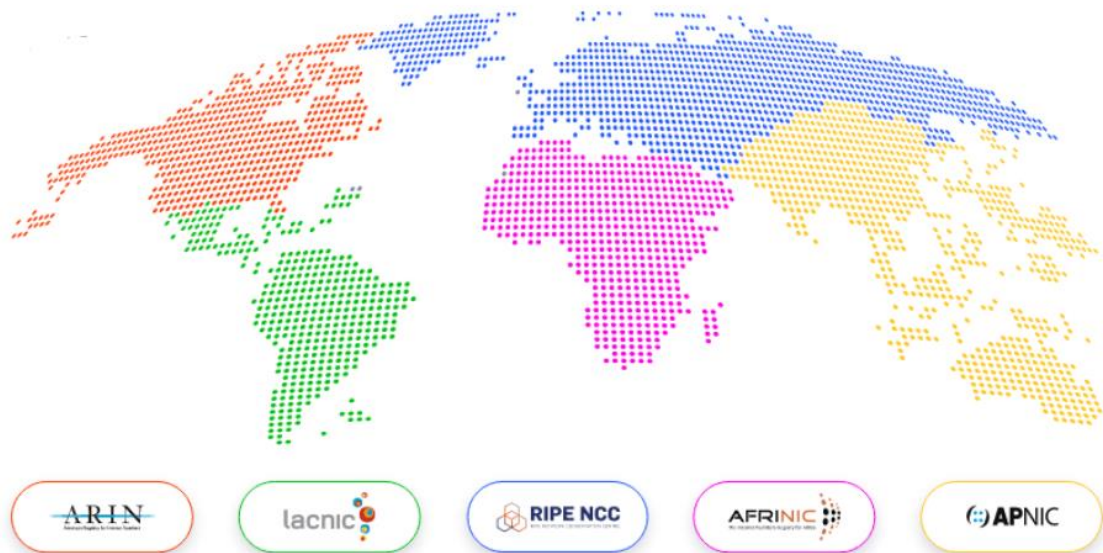


Рисунок 2.2 – Регіональні організації

Перший і останній ASN вихідних 16-розрядних цілих чисел (0 та 65 535) та останній ASN 32-розрядних чисел (4 294 967 295) зарезервовані і не повинні використовуватися операторами. ASN від 64 496 до 64 511 вихідного 16-бітового діапазону та 65 536 - 65 551 32-бітового діапазону зарезервовані для використання в документації RFC 5398. ASN 64512 - 65 534 оригінального 16-бітового діапазону AS та 4 200 000 000 - 4 294 967 294 із 32-бітового діапазону зарезервовані для приватного використання RFC 6996, тобто вони можуть використовуватися всередині, але не повинні повідомлятися глобальній мережі Інтернет. Усі інші ASN підлягають присвоєнню IANA.

Кількість унікальних автономних мереж в системі маршрутизації Інтернету перевищила 5000 в 1999 році, 30 000 в кінці 2008 року, 35 000 в середині 2010 року, 42 000 в кінці 2012 року, 54 000 в середині 2016 року і 60 000 на початку 2018 року.

Кількість виділених ASN перевищила 92000 станом на серпень 2019 року.

		Лавренчук В О			ДУ «Житомирська політехніка».20.123.9.000 – ПР	Арк.
		Єфіменко А.А				10
Змн.	Арк.	№ докум.	Підпис	Дата		

Кількість	Біти	Опис	Довідково
0	16	Зарезервовано для RPKI неділене недійсне простір ^[11]	RFC6483, RFC7607
1 - 23455	16	Загальнодоступні ASN	
23456	16	Зарезервовано для AS Pool Transition	RFC6793
23457 - 64495	16	Загальнодоступні ASN	
64496 - 64511	16	Зарезервовано для використання в документації / зразку коду	RFC5398
64512 - 65534	16	Зарезервовано для приватного користування	RFC1930, RFC6996
65535	16	Зарезервований	RFC7300
65536 - 65551	32	Зарезервовано для використання в документації та зразку коду	RFC4893, RFC5398
65552 - 131071	32	Зарезервований	
131072 - 4199999999	32	Загальнодоступні 32-розрядні ASN	
4200000000 - 4294967294	32	Зарезервовано для приватного користування	RFC6996
4294967295	32	Зарезервований	RFC7300

Рисунок 2.3 Таблиця 16-бітових і 32-бітових

Автономні системи (АС) можна згрупувати за чотирма категоріями залежно від їх підключення та операційної політики.

- **багатодомний**: АС, що підтримує зв'язки з кількома іншими АС. Це дозволяє АС залишатися підключеним до Інтернету у випадку повної відмови одного з їхніх з'єднань. Однак, на відміну від транзитної АС, цей тип АС не дозволить трафіку з однієї АС проходити на шляху до іншої АС.
- **заглушка**: АС, яка підключена лише до однієї іншої АС. Це може бути очевидною втратою номера AS, якщо політика маршрутизації мережі така ж, як і система AS вище. Однак, заглушка AS може бути вживлюючись з іншими автономними системами, що не відображається на публіці сервери маршрутного перегляду. Конкретні приклади включають приватні взаємозв'язки у фінансовому та транспортному секторах.
- **транзит**: AS, що забезпечує з'єднання через себе з іншими мережами. Тобто мережа А може використовувати мережу В, транзитну AS, для підключення до мережі С. Якщо одна AS є Інтернет-провайдером для іншої, то вона вважається транзитною AS.

- **Точка обміну Інтернетом (IX або IXP):** фізична інфраструктура, через яку постачальники послуг Інтернету або мережі доставки контенту (CDN) обмінюються Інтернет-трафіком між своїми мережами (автономні системи). IXP ASN зазвичай прозорі.

BGP (англ. Border Gateway Protocol, укр. Протокол Граничного Шлюзу) — з 1994 року єдиний протокол маршрутизації між автономними системами в глобальній мережі Інтернет, а його розширена версія MBGP (Multiprotocol BGP) використовується в MPLS-мережах ІТ-провайдерів.

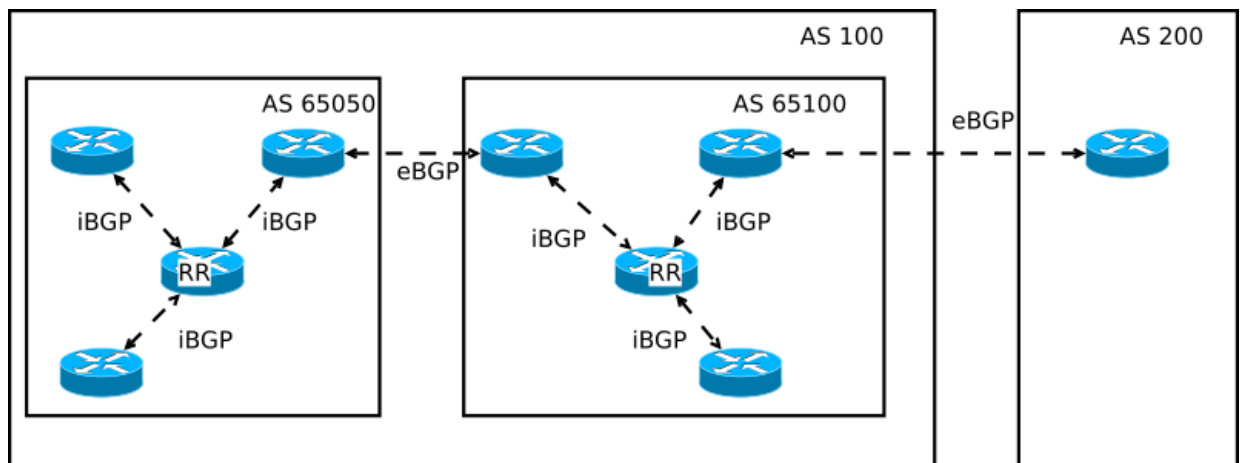


Рисунок 2.4 Топологія BGP

BGP є протоколом міждоменної маршрутизації та належить до класу дистанційно-векторних протоколів. Як протокол міждоменної маршрутизації використовується усіма інтернет-провайдерами, а також великими компаніями та організаціями, які мають власні публічні номери автономних систем (ASN) та користуються послугами більш ніж одного інтернет-провайдера (мультихомінг) або мають прямі IP-з'єднання з багатьма іншими великими компаніям, що також мають власні публічні номери автономних систем, без використання послуг інтернет-провайдерів.

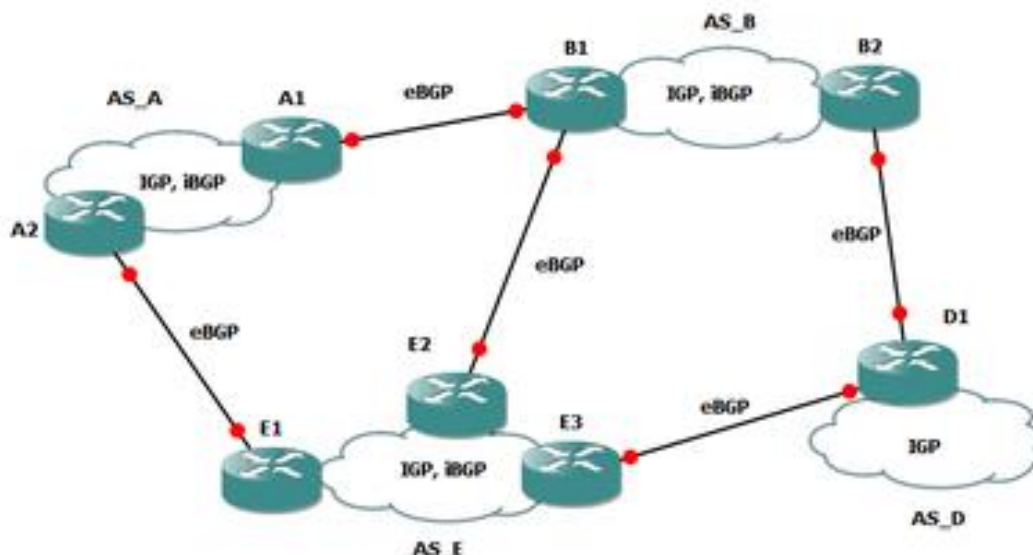


Рисунок 2.5 Автономні системи та BGP

Разом з тим немає ніяких обмежень на використання BGP в локальних мережах крім рекомендацій про приватні ASN (64512-65534), але використання BGP як протоколу внутрішньодоменної маршрутизації є недоцільним через значний час конвергенції (збіжності) у порівнянні з іншими протоколами маршрутизації, що закладено в його дизайні.

На відміну від класичного дистанційно-векторного протоколу RIP, метрикою якого є кількість хопів (відрізків шляху) між маршрутизаторами, найкращий маршрут BGP обирається по точно визначеному пріоритету атрибутів, одним із яких, але не найпріоритетнішим, є кількість хопів між автономними системами — найкоротший шлях між автономними системами (англ. shortest AS path). Тому іноді цей протокол зараховують до окремого класу шляхо-векторних протоколів.

На відміну від інших протоколів IP-маршрутизації, де маршрутизатори-сусіди знаходять один одного автоматично, BGP-сусіди мають бути прописані у конфігурації кожного маршрутизатора явно. Також BGP не має своєї власної реалізації комунікації між сусідами; для цих цілей BGP використовує протокол TCP (порт 179). BGP-сусіди періодично, за замовченням кожні 60 секунд, надсилають один одному повідомлення keepalive (чи живий?). Маршрутизатори BGP часто називають BGP-спікерами (speaker). Якщо між ними є TCP-комунікація, вони стають один одному сусідами або у BGP-термінології — BGP-пірами (peer).

		Лавренчук В О			ДУ «Житомирська політехніка».20.123.9.000 – ПР	Арк.
		Єфіменко А.А				13
Змн.	Арк.	№ докум.	Підпис	Дата		

Маршрути, отримані від сусідів з інших автономних систем, тобто по eBGP (Exterior, Зовнішній BGP) для маршрутизаторів Cisco мають адміністративну відстань (administrative distance (AD)) — 20, відповідно від сусідів з тієї ж самої АС тобто по iBGP (Interior, Внутрішній BGP) — 200.

Щоб встановити відносини сусідства, в BGP треба налаштувати вручну кожного сусіда. Коли вказується сусід локального маршрутизатора, обов'язково вказується автономна система сусіда. За цією інформацією, BGP визначає тип сусіда:

- **Внутрішній BGP сусід (iBGP-сусід)** — сусід, який знаходиться в автономній системі, що і локальний маршрутизатор. iBGP-сусіди не обов'язково мають бути безпосередньо з'єднані.
- **Зовнішній BGP сусід (eBGP-сусід)** — сусід, який знаходиться в автономній системі, відмінній від локального маршрутизатора. За замовчуванням, eBGP-сусіди мають бути безпосередньо з'єднані.

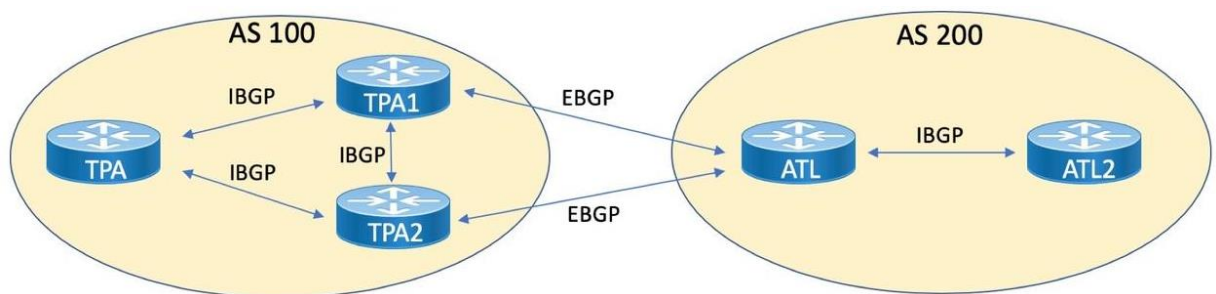


Рисунок 2.6 Типи сусідства

Тип сусіда мало впливає встановлення відносин сусідства. Більш суттєві відмінності між різними типами сусідів виявляються в процесі надсилання оновлень BGP та додаванні маршрутів до таблиці маршрутизації.

BGP виконує такі перевірки, коли формує відносини сусідства:

- Маршрутизатор повинен отримати запит на TCP-з'єднання з адресою відправника, який знайде маршрутизатор вказаним у списку сусідів (команда neighbor).
- Номер автономної системи локального маршрутизатора повинен збігатися з номером автономної системи, який вказаний на сусідньому маршрутизаторі

командою neighbor remote-as (ця вимога не дотримується при налаштуваннях конфедерацій).

- Ідентифікатори маршрутизаторів (Router ID) не повинні співпадати.
- Якщо налаштовано автентифікацію, то сусіди повинні пройти її.

Перший пункт перевірки має певну особливість: тільки один з двох маршрутизаторів IP-адреса, вказаний як адреса відправки оновлень, повинен бути вказаний в команді небагатьох інших маршрутизаторів.

BGP виконує перевірку таймерів keepalive та hold, проте розбіжність цих параметрів не впливає на встановлення відносин сусідства. Якщо таймери не збігаються, кожен маршрутизатор буде використовувати менше значення таймера hold.

Щодо станів зв'язку між сусідами, то вони бувають такими:

Таблиця 2.1

Стан	Очікування TCP?	Ініціалізація TCP?	Встановлення TCP?	Відправлено Open?	Отримано Open?	Сусід Up?
Idle	Ні					
Connect	Так					
Active	Так	Так				
Open sent	Так	Так	Так	Так		
Open confirm	Так	Так	Так	Так	Так	
Established	Так	Так	Так	Так	Так	Так

*Якщо IP-адреси із сусідом не співпали, то цей сусід буде у стані active.

2.3 Windows Server та Active Directory

Для адміністрування мережі даного проекту було використано Windows Server разом з Active Directory.

		Лавренчук В О			ДУ «Житомирська політехніка».20.123.9.000 – ПР	Арк.
		Єфіменко А.А				15
Змн.	Арк.	№ докум.	Підпис	Дата		

Windows Server є операційною системою, розробленою компанією Microsoft для користування у підприємствах та організаціях, які потребують великої мережі комп'ютерів та інфраструктури серверів. Windows Server дозволяє організувати централізоване керування ресурсами мережі та забезпечити безпеку та доступність даних для користувачів.

Active Directory (AD) - це служба директорії, яка входить до складу Windows Server та дозволяє керувати ресурсами мережі, такими як користувачі, групи, комп'ютери та додатки. AD забезпечує централізований збір, зберігання та управління інформацією про об'єкти мережі, тобто є мережевою базою даних, що містить інформацію про всі об'єкти, які належать до домену.

Однією з основних функцій AD є автентифікація та авторизація користувачів. Кожен користувач отримує унікальний ідентифікатор, що називається ім'ям користувача, яке він використовує для входу до мережі. Крім того, AD дозволяє групувати користувачів за різними ознаками, такими як роль в організації, доступ до різних ресурсів тощо.

AD також дозволяє керувати політиками безпеки, які визначають права доступу користувачів до різних ресурсів мережі. Наприклад, політика безпеки може визначати, які користувачі мають право доступу до конфіденційної інформації, які мають право використовувати певні додатки тощо.

AD також дозволяє керувати забезпеченням, аудитом та моніторингом доступу до ресурсів мережі. Це дозволяє адміністраторам в реальному часі відстежувати події, що відбуваються в мережі, та надавати допомогу користувачам у вирішенні проблем.

Крім того, AD дозволяє забезпечувати єдиний доступ до різних ресурсів мережі, таких як файли та принтери, і управляти цим доступом з централізованого місця. Це дозволяє зменшити час настройки та підтримки окремих комп'ютерів та ресурсів мережі, забезпечуючи при цьому їх ефективну роботу та безпеку.

Однією з важливих функцій AD є можливість створювати домени, які дозволяють керувати всіма об'єктами мережі з єдиного місця. Кожен домен містить інформацію про користувачів, комп'ютери, групи та інші об'єкти, які належать до

		Лавренчук В О			ДУ «Житомирська політехніка».20.123.9.000 – ПР	Арк.
		Єфіменко А.А				
Змн.	Арк.	№ докум.	Підпис	Дата		16

цього домену. Крім того, AD дозволяє створювати дерева доменів та ліси доменів, що дозволяє організовувати мережу більш складними структурами та ієрархіями.

У підсумку, Windows Server та Active Directory є потужними інструментами для керування мережевою інфраструктурою та забезпечення безпеки та доступності даних. Вони дозволяють організаціям ефективно керувати ресурсами мережі та забезпечувати безпеку та доступність даних для користувачів.

2.4. Топологія мережі

При проектуванні мережі буда використана ієрархічна структура, яка включає в себе три рівні:

- рівень ядра;
- рівень розподілу;
- рівень доступу.

Дана структура представлена на рисунку 2.7.

Також потрібно:

- виконати розробку структур автономних систем;
- визначити політики маршрутизації між автономними системами та мережами в автономній системі;
- визначити основні та резервні канали.

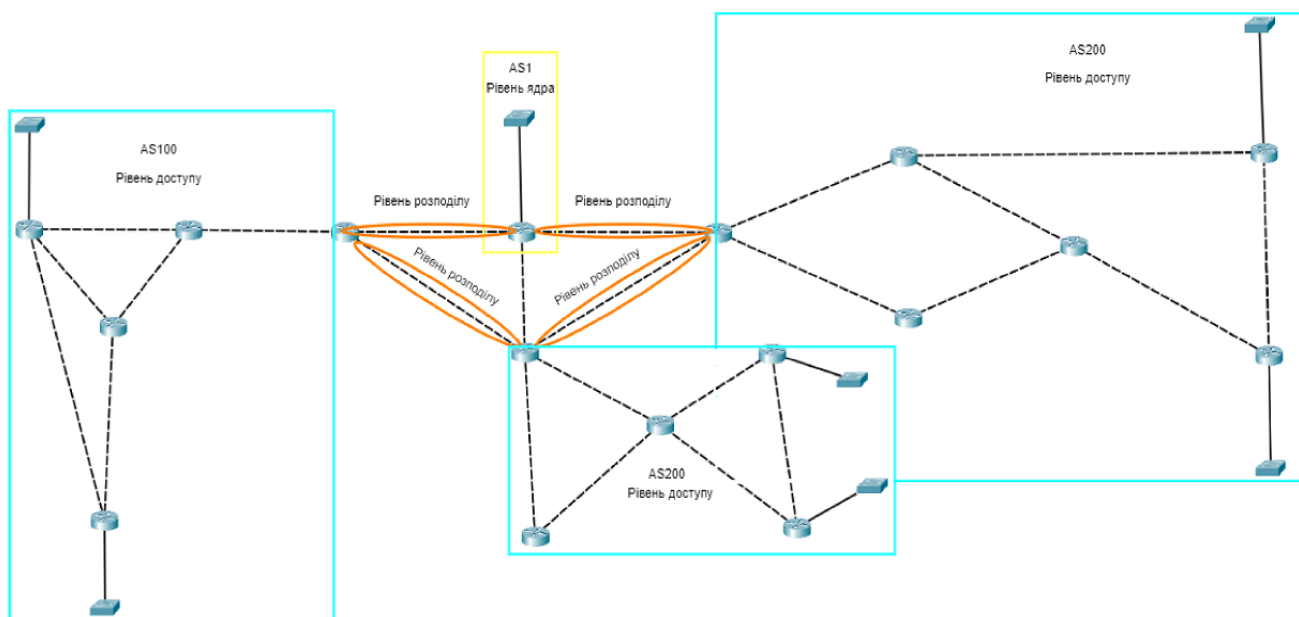


Рисунок 2.7 Топологія мережі

		Лавренчук В О			ДУ «Житомирська політехніка».20.123.9.000 – ПР	Арк.
		Єфіменко А.А				17
Змн.	Арк.	№ докум.	Підпис	Дата		

В рівні ядра знаходиться транзитна автономна система під номером 1. Вона складається з одного маршрутизатора та комутатора. AS 1(рис. 2.8) має 3 канали зв'язку з тупиковими автономними системами, а саме AS 100, AS 200 та AS 300.

Рієнь розподілу відповідає тупиковим автономним системам котрі зв'язані через граничні маршрутизатори на яких налатовуються різноманітні функції та політики захисту.

В рівні доступу знаходяться усі внутрішні маршрутизатори та інші пристрої автономної системи котрі мають зв'язок з локальними мережами AS.

При проектуванні мережі потрібно приділити достатню увагу найменуванню автономних систем та пристроїв, що в них знаходяться. Транзитна AS буде під унікальним номером (ASN - autonomous system number) 1(рис. 2.8). Наступними стнуть автономні системм з ASN 100(рис. 2.9), 200(рис. 2.10) та 300(рис. 2.11).

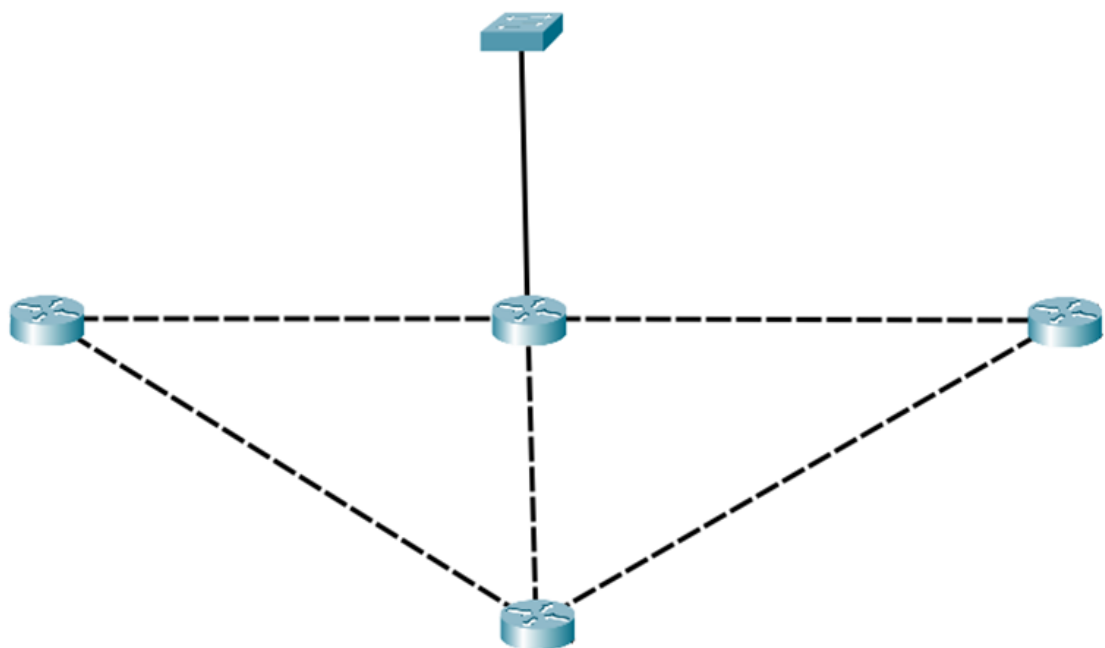


Рисунок 2.8 Автономна система AS 1

Автономна система AS 100(рис. 2.9) складається з 4 внутрішніх маршрутизаторі та 1 граничного. Найменування пристроїв обрано наступним шляхом:

- Номер пристрою нумерується зправа на ліво (R1, R2 т.д);
- Після номера пристрою вказується його належність до тієї чи іншої автономної системи (R1-AS100, R2-AS100 т.д)

AS 100 має додатковий канал зв'язу з AS 300, котрий не є оптимальним, але при виході з ладу основного каналу зв'язу з AS 1 він стане в нагоді та не зашкодить працездатності мережі. Також всередині автономної системи між внутрішніми маршрутизаторами побудовано резервні канали. R2-AS100 може пройти шлях до R5-AS100 такими шляхами:

R2-AS100 – R4-AS100 R5-AS100;

R2-AS100 – R3-AS100 R4-AS100 R5-AS100;

R2-AS100 – R3-AS100 R5-AS100;

R2-AS100 – R4-AS100 R3-AS100 R5-AS100;

Аналогічно резервні шляхи працюють й для інших пристроїв системи.

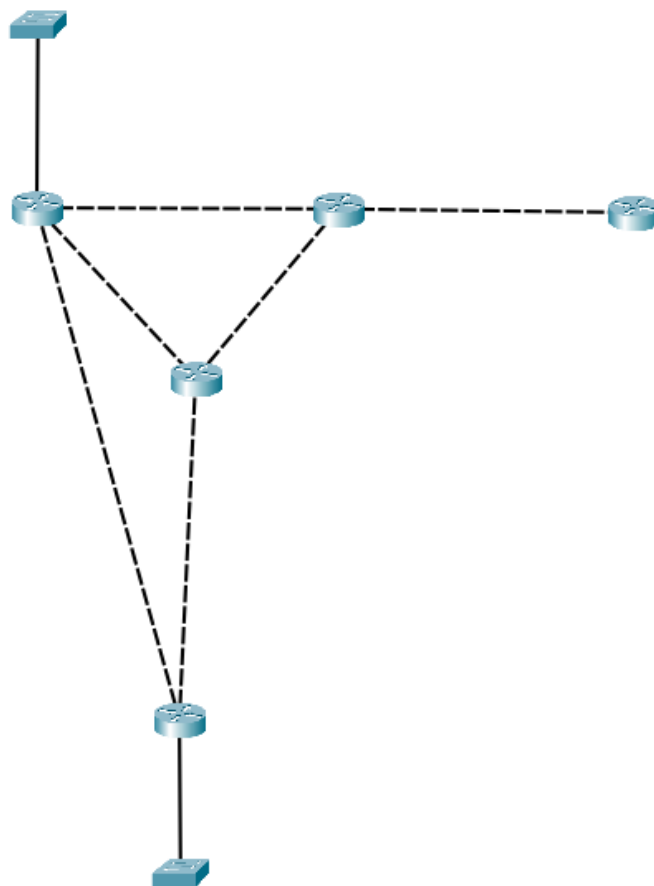


Рисунок 2.9 Автономна система AS 100

Автономна система AS 200(рис. 2.10) складається з 5 внутрішніх маршрутизаторів та 1 граничного. Найменування пристроїв обрано наступним шляхом:

- Номер пристрою нумерується зправа на ліво (R1, R2 т.д);

- Після номера пристрою вказується його належність до тієї чи іншої автономної системи (R1-AS200, R2-AS200 т.д)

AS 200 має додатковий канал зв'язку з AS 300, котрий не є оптимальним, але при виході з ладу основного каналу зв'язку з AS 1 він стане в нагоді та не зашкодить працездатності мережі. Також всередині автономної системи між внутрішніми маршрутизаторами побудовано резервні канали. R2-AS200 може пройти шлях до R6-AS200 такими шляхами:

R2-AS200 R4-AS200 R6-AS200;

R2-AS200 R5-AS200 R6-AS200;

R2-AS200 R1-AS200 R3-AS200 R4-AS200 R6-AS200;

Аналогічно резервні шляхи працюють й для інших пристроїв системи.

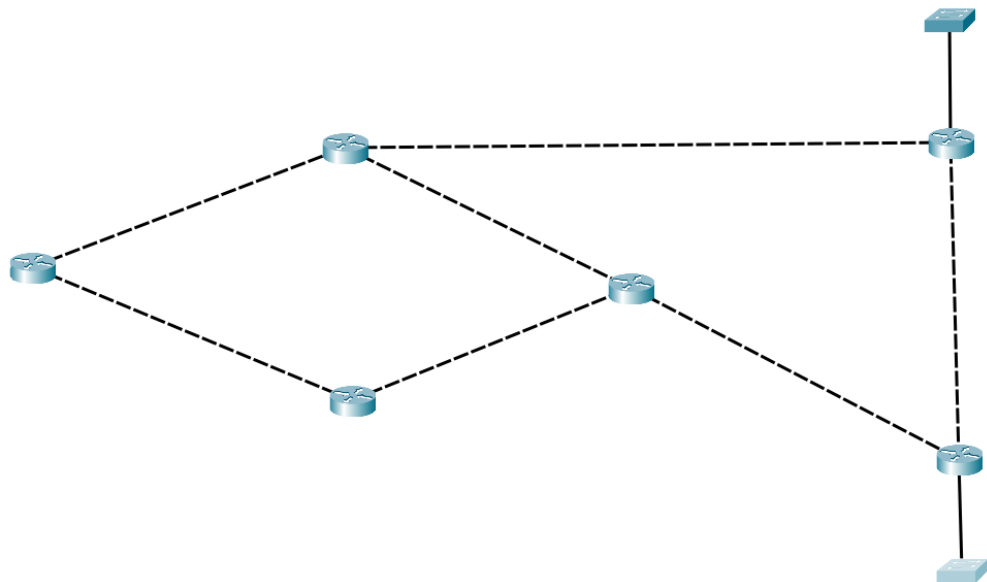


Рисунок 2.10 Автономна система AS 200

Автономна система AS 300(рис. 2.11) складається з 4 внутрішніх маршрутизаторів та 1 граничного. Найменування пристроїв обрано наступним шляхом:

- Номер пристрою нумерується зправа на ліво (R1, R2 т.д);
- Після номера пристрою вказується його належність до тієї чи іншої автономної системи (R1-AS300, R2-AS300 т.д)

AS 300 має додаткові канал зв'язку з AS 100 та AS 200. Також всередині автономної системи між внутрішніми маршрутизаторами побудовано резервні канали. R1-AS300 може пройти шлях до R5-AS300 такими шляхами:

		Лавренчук В О			ДУ «Житомирська політехніка».20.123.9.000 – ПР	Арк.
		Єфіменко А.А				20
Змн.	Арк.	№ докум.	Підпис	Дата		

R2-AS300 R3-AS300 R5-AS300;

R2-AS300 R3-AS300 R4-AS300 R5-AS300;

R2-AS300 R1-AS300 R3-AS300 R5-AS300;

R2-AS300 R1-AS300 R3-AS300 R4-AS300 R5-AS300;

Аналогічно резервні шляхи працюють й для інших пристроїв системи.

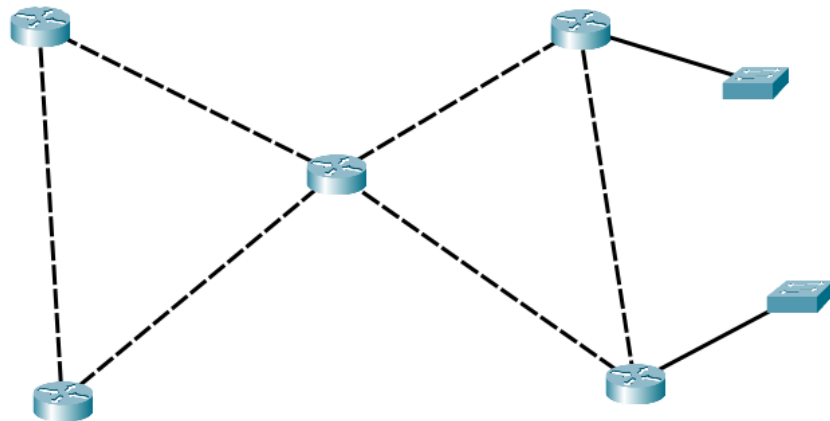


Рисунок 2.11 Автономна система AS 300

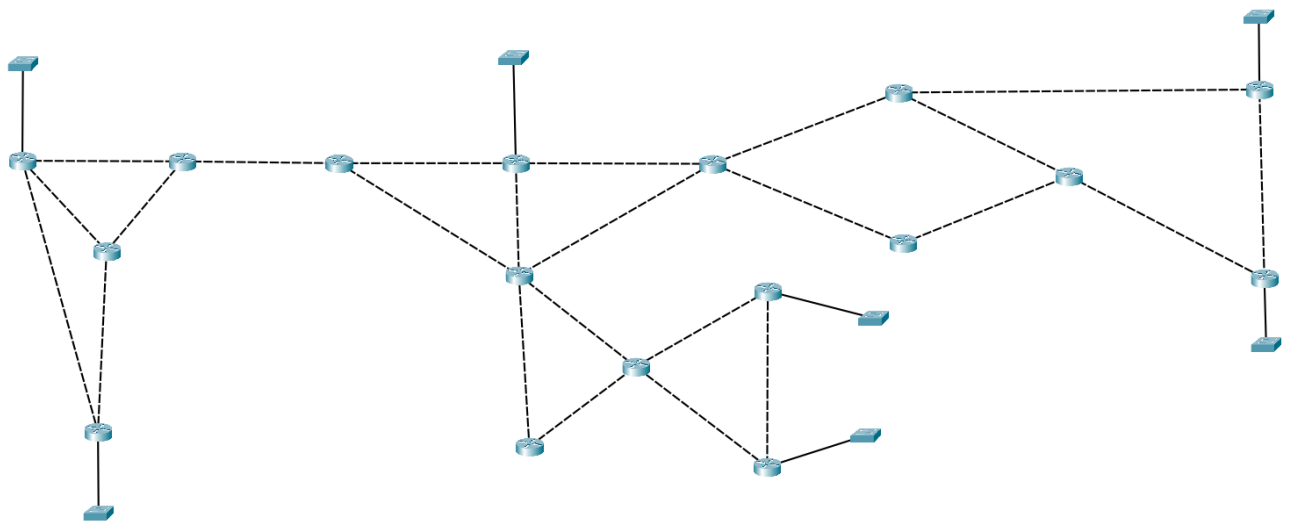


Рисунок 2.12 Загальна топологія мережі

РОЗДІЛ 3 НАЛАГОДЖЕННЯ ОБЛАДНАННЯ

3.1 Налагодження обладнання мережі

Перш за все при налаштуванні пристроїв мережі потрібно призначити їх правильні хостнейми та IP-адресаи на відповідних інтерфейсах (рис. 3.1).

```
R1-AS100(config)#int loopback 0
R1-AS100(config-if)#
*Jul 12 17:14:56.543: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
changed state to up
R1-AS100(config-if)#ip add 1.1.1.1 255.255.255.255
R1-AS100(config-if)#no sh
R1-AS100(config-if)#ex
R1-AS100(config)#int f0/0
R1-AS100(config-if)#ip add 100.100.100.1 255.255.255.252
R1-AS100(config-if)#no sh
R1-AS100(config-if)#e
*Jul 12 17:16:37.915: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state t
o up
*Jul 12 17:16:38.915: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to up
R1-AS100(config-if)#ex
R1-AS100(config)#int f1/0
R1-AS100(config-if)#ip add 10.10.10.1 255.255.255.252
R1-AS100(config-if)#no sh
R1-AS100(config-if)#
*Jul 12 17:17:15.779: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state t
o up
*Jul 12 17:17:16.779: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et1/0, changed state to up
```

Рисунок 3.1 – Налагодження інтерфейсів

Далі потрібно визначити який протокол маршрутизації буде використовуватися в автономній системі та налаштувати його (рис. 3.2).

```
R1-AS100(config-if)#router ospf 1
R1-AS100(config-router)#network 1.1.1.1 0.0.0.0 area 0
R1-AS100(config-router)#network 192.168.1.0 0.0.0.255 area 0
R1-AS100(config-router)#network 10.10.10.10 0.0.0.3 area 0
R1-AS100(config-router)#no network 10.10.10.10 0.0.0.3 area 0
R1-AS100(config-router)#network 10.10.10.0 0.0.0.3 area 0
```

Рисунок 3.2 – Налаштування динамічної маршрутизації

Наступним кроком є налаштування протоколу BGP та протоколів внутрішньої маршрутизації автономних систем(OSPF та EIGRP). В прикладі показане налаштування на граничному та внутрішньому маршрутизаторах автономної системи AS 100 (рис. 3.3-3.4).

```
R1-AS100(config-if)#router bgp 100
R1-AS100(config-router)#network 192.168.1.0 mask 255.255.255.0
R1-AS100(config-router)#neighbor 100.100.100.2 remote-as 300
R1-AS100(config-router)#do write
```

Рисунок 3.3– Налаштування BGP(граничний маршрутизатор)

		Лавренчук В О			ДУ «Житомирська політехніка».20.123.9.000 – ПР	Арк.
		Єфіменко А.А				22
Змн.	Арк.	№ докум.	Підпис	Дата		

```
R2-AS100(config-router)#router bgp 100
R2-AS100(config-router)#network 192.168.1.0 mask 255.255.255.0
R2-AS100(config-router)#neighbor 1.1.1.1 remote-as 100
R2-AS100(config-router)#neighbor 1.1.1.1 update-source loopback0
R2-AS100(config-router)#neighbor 1.1.1.1 next-hop-self
```

Рисунок 3.4 – Налаштування BGP(внутрішній маршрутизатор)

```
R1(config-router)#router ospf 300
R1(config-router)#network 30.30.30.0 0.0.0.31 area 0
R1(config-router)#network 33.33.33.33 0.0.0.0 area 0
R1(config-router)#network 203.0.0.0 0.0.1.255 area 0
```

Рисунок 3.5– Налаштування OSPF

```
R1(config)#router eigrp 200
R1(config-router)#network 20.20.20.0 0.0.0.3
R1(config-router)#network 20.20.20.4 0.0.0.3
R1(config-router)#network 20.20.20.20 0.0.0.0
R1(config-router)#network 200.0.0.0 0.0.1.255
```

Рисунок 3.6– Налаштування EIGRP

Також було налаштовано R1-AS1 як NTP-server для синхронізації внутрішнього часу усіх пристроїв мережі.

```
R1-AS1#clock set 13:00:00 July 22 2022
R1-AS1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R1-AS1(config)#ntp authentication-key 1 md5 mypass
R1-AS1(config)#ntp trusted-key 1
R1-AS1(config)#ntp authenticate
R1-AS1(config)#ntp master 3
R1-AS1(config)#service timestamps log date
R1-AS1(config)#service timestamps log datetime msec
R1-AS1(config)#logging host 80.80.80.2
R1-AS1(config)#logging trap warnings
```

Рисунок 3.7 – Налаштування NTP-server

```
R1-AS100(config)#ntp authentication-key 1 md5 mypass
R1-AS100(config)#ntp trusted-key 1
R1-AS100(config)#ntp authenticate
R1-AS100(config)#ntp update-calendar
R1-AS100(config)#ntp server 11.11.11.1
```

Рисунок 3.8– Підключення до NTP-server

Важливим кроком є налаштування протоколу SSH для безпечного віддаленого доступу до пристроїв мережі (рис. 3.9). Саме строгої аутентифікації реалізується

		Лавренчук В О			ДУ «Житомирська політехніка».20.123.9.000 – ПР	Арк.
		Єфіменко А.А				
Змн.	Арк.	№ докум.	Підпис	Дата		23

ся цілісність зв'язку. Також доступ додатково захищено за допомогою надійного шифрування.

```
R1-AS1(config)#ip domain name my.net
R1-AS1(config)#crypto key generate rsa
The name for the keys will be: R1-AS1.my.net
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R1-AS1(config)#service password-encryption
R1-AS1(config)#username admin privilege 15 password adminpass
R1-AS1(config)#aaa new-model
R1-AS1(config)#line vty 0 4
R1-AS1(config-line)#transport input ssh
R1-AS1(config-line)#logging synchronous
R1-AS1(config-line)#exec-timeout 60 0
```

Рисунок 3.9 – Налаштування SSH

Розвиток технологій не стоїть на місці і стрімко йде вгору. Не кожна людина в даний період розвитку встигає дізнатися та ознайомитись з інформацією про власну безпеку в мережі. Проте зловмисники не стоять на місці, а також вигадують, знаходять помилки в обладнаннях чи коді, і користуються цим в своїх цілях. На сьогоднішній день існує дуже багато різних атак, які здійснюють хакери для того, щоб дізнатися ту чи іншу інформацію, зламати сайти, заволодіти мережею тощо. Для того, щоб захиститися від різних типів атак, потрібно знати, як вони працюють та як налаштувати захист від них.

Самим першим кроком по захисту стало налаштування функції auto secure на маршрутизаторах мережі. В ході виконання команди налаштовуються банери, паролі до різних режимів та юзери. Результат збережено до конфігураційного файлу.

		Лавренчук В О			ДУ «Житомирська політехніка».20.123.9.000 – ПР	Арк.
		Єфіменко А.А				
Змн.	Арк.	№ докум.	Підпис	Дата		24

```

R5-AS200
R5-AS200(config)#do auto secure
--- AutoSecure Configuration ---

*** AutoSecure configuration enhances the security of
the router, but it will not make it absolutely resistant
to all security attacks ***

AutoSecure will modify the configuration of your device.
All configuration changes will be shown. For a detailed
explanation of how the configuration changes enhance security
and any possible side effects, please refer to Cisco.com for
Autosecure documentation.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.

Gathering information about the router for AutoSecure

Is this router connected to internet? [no]: n

Securing Management plane services...

Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol

```

Рисунок 3.10 – Виконання команди auto secure

Одними з головних атак на мережу від котрих потрібно налаштувати захист є MAC-spoofing та MAC-flooding. MAC-spoofing – це атака, при якій порушник обходить перевірку аутентифікації для порушення працездатності мережі. Використовується для того, щоб дізнатися про дані, програми, паролі та IP-адреси кінцевого хоста. MAC Flooding — це кібератака, під час якої зловмисник заповнює мережеві комутатори фальшивими MAC-адресами, щоб поставити під загрозу їх безпеку. MAC-spoofing: кращим захистом від даної атаки є запис в таблицю комутатора MAC адресу користувача, який підключений за даним портом. Тобто, якщо MAC адреса за даним портом зміниться, то користувач буде недоступний.

На портах комутаторів до яких приєднані робочі станції активовано функцію port security (рис. 3.11). При підміні MAC-адреси порт комутатора стане неактивним, що завадить злочинцям потрапити до мережі.

```

SW2-AS100(config)#int eth0/0
SW2-AS100(config-if)#switchport mode access
SW2-AS100(config-if)#switchport port-security
SW2-AS100(config-if)#switchport port-security mac-address 0050.7966.6806
SW2-AS100(config-if)#switchport port-security violation shutdown
SW2-AS100(config-if)#int eth0/1
SW2-AS100(config-if)#switchport mode access
SW2-AS100(config-if)#switchport port-security
SW2-AS100(config-if)#switchport port-security mac-address 0050.7966.6807
SW2-AS100(config-if)#switchport port-security violation shutdown
SW2-AS100(config-if)#int eth0/2
SW2-AS100(config-if)#switchport mode access
SW2-AS100(config-if)#switchport port-security
SW2-AS100(config-if)#switchport port-security mac-address 0050.7966.6808
SW2-AS100(config-if)#switchport port-security violation shutdown

```

Рисунок 3.11 – Налаштування функції Port Security

Для того щоб станція злочинця не могла під'єднатися до пристрою мережі через протокол SSH було створено список доступу котрий дозволяє підключення тільки однієї робочої станції, станції управління (рис. 3.12).

```

R1-AS1(config)#access-list 1 permit host 80.80.80.2
R1-AS1(config)#access-list 1 deny any
R1-AS1(config)#line vty 0 4
R1-AS1(config-line)#access-class 1 in

```

Рисунок 3.12 – Налаштування безпечного підключення по SSH

Так як в мережі використовуються протоколи динамічної маршрутизації потрібно виконати їх захистити, адже якщо злочинцям вдасться пошкодити таблицю маршрутизації потрібні пакети будуть знищені або підуть не за правильним маршрутом. Тому дуже важливо при роботі з динамічними протоколами маршрутизації використовувати аутентифікацію оновлень, бажано MD5.

```

R1-AS100(config-if)#int f1/0
R1-AS100(config-if)#ip ospf message-digest-key 1 md5 secret
R1-AS100(config-if)#ip ospf authentication message-digest

```

Рисунок 3.13 – Аутентифікація оновлень MD5 для OSPF

```

R1-AS200(config)#key chain my_passw
R1-AS200(config-keychain)#key 1
R1-AS200(config-keychain-key)#key-string strong_passw
R1-AS200(config-keychain-key)#int f0/0
R1-AS200(config-if)#ip authentication mode eigrp 200 md5
R1-AS200(config-if)#ip authentication key-chain eigrp 200 my_passw

```

Рисунок 3.14 – Аутентифікація оновлень MD5 для EIGRP

В наш час дуже розповсюджені атаки типу DDOS, особливо це стосується протоколу BGP котрий потрібно захистити для унеможливленні потрапляння у мережу некоректного трафіку. Blackhole дозволяє керувати трафіком на рівні про-

		Лавренчук В О			ДУ «Житомирська політехніка».20.123.9.000 – ПР	Арк.
		Єфіменко А.А				26
Змн.	Арк.	№ докум.	Підпис	Дата		

вайдера, до влучення в нашу AS. Він ефективний при боротьби з великими атаками на пропускну здатність каналу (найчастіше DNS Amplification). У класичній схемі метод передбачає виставлення next-hop для анонсованого маршруту на адресу ip з приватної мережі. Так як у магістральних провайдерів маршрути до приватних мереж, здебільшого, повинні бути направлені в Null0 (рис. 3.17) пакети з адресою призначення з цієї мережі автоматично відкидатимуться — потрапляти в «чорну діру» ще в мережі провайдера.

```
R1-AS1(config)#ip route 100.0.0.0 255.255.254.0 Null 0
R1-AS1(config)#ip route 200.0.0.0 255.255.254.0 Null 0
R1-AS1(config)#ip route 203.0.0.0 255.255.254.0 Null 0
```

Рисунок 3.15– Налаштування BGP Blackhole при атаці

3.2 Перевірка працездатності мережі

Спочатку потрібно перевірити зв'язок між сусідніми пристроями мережі(рис. 3.18)

```
R1-AS1#ping 11.11.11.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.11.11.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/20/24 ms
```

Рисунок 3.18 – Зв'язок з сусідніми пристроями

Далі слід перевірити чи встановилося сусідство між пристроями в протоколі BGP(рис. 3.19)

```
R1-AS300(config-router)#
*Jul 13 15:32:47.007: %BGP-5-ADJCHANGE: neighbor 100.100.100.1 Up
```

Рисунок 3.19 – Встановлення сусідства

При перевірці правильного налаштування протоколі внутрішньої та зовнішньої маршрутизації слід перевірити зв'язок між мережами автономних систем(рис. 3.20-3.22)

```
WS4-AS100> ping 203.0.0.3
84 bytes from 203.0.0.3 icmp_seq=1 ttl=58 time=128.826 ms
84 bytes from 203.0.0.3 icmp_seq=2 ttl=58 time=126.988 ms
84 bytes from 203.0.0.3 icmp_seq=3 ttl=58 time=117.607 ms
84 bytes from 203.0.0.3 icmp_seq=4 ttl=58 time=87.419 ms
84 bytes from 203.0.0.3 icmp_seq=5 ttl=58 time=79.484 ms
```

Рисунок 3.20 – Зв'язок між мережами AS 100 та AS 300

		Лавренчук В О			ДУ «Житомирська політехніка».20.123.9.000 – ПР	Арк.
		Єфіменко А.А				27
Змн.	Арк.	№ докум.	Підпис	Дата		

```
WS1-AS300> ping 200.0.1.3
84 bytes from 200.0.1.3 icmp_seq=1 ttl=57 time=150.106 ms
84 bytes from 200.0.1.3 icmp_seq=2 ttl=57 time=126.449 ms
84 bytes from 200.0.1.3 icmp_seq=3 ttl=57 time=127.266 ms
84 bytes from 200.0.1.3 icmp_seq=4 ttl=57 time=127.492 ms
84 bytes from 200.0.1.3 icmp_seq=5 ttl=57 time=132.996 ms
```

Рисунок 3.21 – Зв'язок між мережами AS 300 та AS 200

```
WS4-AS200> ping 100.0.1.4
84 bytes from 100.0.1.4 icmp_seq=1 ttl=57 time=276.685 ms
84 bytes from 100.0.1.4 icmp_seq=2 ttl=57 time=129.483 ms
84 bytes from 100.0.1.4 icmp_seq=3 ttl=57 time=123.716 ms
84 bytes from 100.0.1.4 icmp_seq=4 ttl=57 time=131.732 ms
84 bytes from 100.0.1.4 icmp_seq=5 ttl=57 time=139.795 ms
```

Рисунок 3.22 – Зв'язок між мережами AS 200 та AS 100

Наступним кроком перевіримо працездатність функції Port Security шляхом підключення станції злочинця до комутатора(рис. 3.23).

```
*Jul 21 16:42:56.932: %PORT_SECURITY-2-PSECURE VIOLATION: Security violation occurred, caused by MAC address 0050.7966.6810 on port Ethernet1/0.
*Jul 21 16:42:57.935: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0, changed state to down
SW1-AS100(config-if)#
*Jul 21 16:42:58.939: %LINK-3-UPDOWN: Interface Ethernet1/0, changed state to down
```

Рисунок 3.23 – Робота Port Security

В результаті підключення робочої станції – злочинця порт відключається та переходить у стан err-disable.

Також перевіримо чи працює віддалене підключення по протоколу SSH(рис. 3.24).

```
PS C:\Users\Student> ssh -c aes256-cbc admin@80.80.80.1
The authenticity of host '80.80.80.1 (80.80.80.1)' can't be established.
RSA key fingerprint is SHA256:JUKER4R5WDGh+EMAum8C7SLIPIWCf5Bw6krnpjwdB5k.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added '80.80.80.1' (RSA) to the list of known hosts.
Password:
Welcome!
R1-AS1>en
Password:
% Access denied
R1-AS1>en
Password:
R1-AS1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
R1-AS1(config)#
```

Рисунок 3.24 – Підключення по SSH з валідної IP-адреси 80.80.80.2

```
PS C:\Users\Student> ssh -c aes256-cbc admin@80.80.80.1
ssh: connect to host 80.80.80.1 port 22: Connection refused
```

Рисунок 3.25 – Підключення по SSH з невалідної IP-адреси 80.80.80.3

В результаті список доступу відпрацював як заплановано.

		Лавренчук В О			ДУ «Житомирська політехніка».20.123.9.000 – ПР	Арк.
		Єфіменко А.А				28
Змн.	Арк.	№ докум.	Підпис	Дата		

Наступним кроком стане перевірка журналювання подій з використанням додатку TFTPd, що була встановлена на одну з робочих станцій мережі.

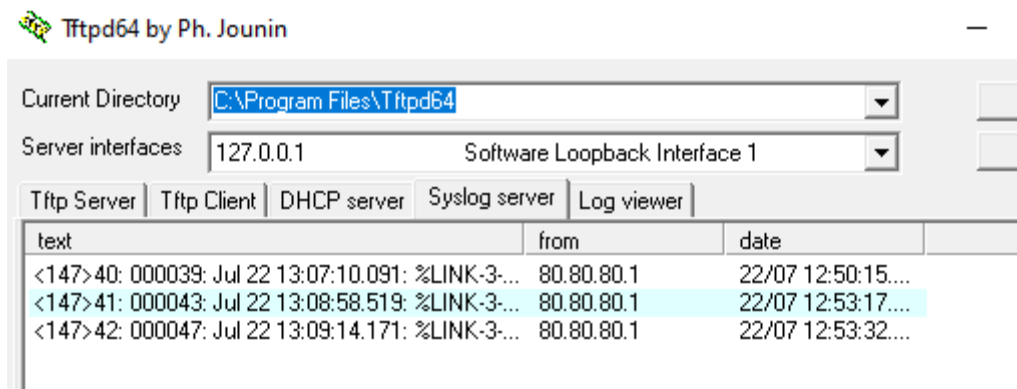


Рисунок 3.26 Перевірка журналу подій

ВИСНОВОК

Протягом проходження виробничої практики було ознайомлено з роботою як самої ІТ-компанії Dual Education Ukraine так і відділом програмного забезпечення, головною задачею якого є покращення та модернізування всієї інформаційної інфраструктури компанії, а також стежити за її працездатністю, реагувати на виникаючі проблеми. Було виконано розробку макету мережі на базі протоколу маршрутизації BGP та авторизація та аутентифікація користувачів на базі Active Directory.

В компанії посада ІТ-фахівця передбачає виконання як складних, пов'язаних з усуненням проблем з мережею, так і найпростіших обов'язків: заправляти картриджі принтера, встановлювати операційні системи та ПЗ тощо. Тому протягом проходження практики було досягнуто подібні цілі, а саме, було обслуговано близько десяти робочих станції, усунено неполадки пов'язані зі збоями комплектуючих запчастин або програмним забезпеченням. Також отримано навички по роботі з мережевими принтерами, вирішено проблеми, що виникали у працівників та встановлено нові пристрої.

Велику увагу було приділено виконанню завдань безпосередньо пов'язаних з дисципліною “Комп'ютерні мережі”.

Отже, данна практика допомогла засвоїти та відточити навички, що були отримані протягом вивчення дисциплін “Комп'ютерні мережі”, “Захист інформації в інформаційно-комунікаційних системах”, “Програмування мовою JavaScript”, “Операційні системи”. Досвід отриманий протягом даного місяця несе великий вклад в майбутнє професійне зростання в данній сфері.

		Лавренчук В О			ДУ «Житомирська політехніка».20.123.9.000 – ПР	Арк.
		Єфіменко А.А				30
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. BGP [Електронний ресурс] – Режим доступу до ресурсу: [https://ru.wikipedia.org/wiki/Border Gateway Protocol](https://ru.wikipedia.org/wiki/Border_Gateway_Protocol).
2. What is BGP? [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cloudflare.com/learning/security/glossary/what-is-bgp/>.
3. AS [Електронний ресурс] – Режим доступу до ресурсу: <https://www.techtarget.com/searchnetworking/definition/autonomous-system>.
4. What is an AS? [Електронний ресурс] – Режим доступу до ресурсу: <https://www.techopedia.com/definition/11063/autonomous-system-as>.
5. Dynamic Routing Protocols [Електронний ресурс] – Режим доступу до ресурсу: <https://community.cisco.com/t5/networking-knowledge-base/dynamic-routing-protocols-ospf-eigrp-ripv2-is-is-bgp/ta-p/4511577>.
6. Windows Server [Електронний ресурс] – Режим доступу до ресурсу: <https://www.microsoft.com/ru-ru/windows-server>.
7. Active Directory [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Active_Directory.
8. Що таке Active Directory? [Електронний ресурс] – Режим доступу до ресурсу: <https://qagroup.com.ua/publications/what-is-active-directory/>.
9. CCNAv7: Enterprise Networking, Security, and Automation [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: <https://lms.netacad.com/course/view.php?id=247980>.
10. Практичні приклади BGP [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/26634-bgptoc.html>.