

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 захищеного мережного обміну на базі технології Get VPN»

Виконав

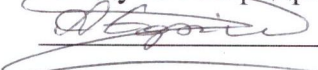
студент 4-го курсу, групи КБ-1

спеціальності 125 «Кібербезпека»

 Висоцький В.П.

Керівник,

завідувач кафедри КІ та КБ, к.т.н.

 Єфіменко А. А.

Рецензент

доцент кафедри КІ та КБ, к.т.н., доцент

 Пулеко І. В.

Житомир – 2021

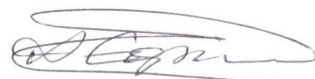
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ
СПЕЦІАЛЬНІСТЬ 125 «КІБЕРБЕЗПЕКА»

ЗАТВЕРДЖУЮ

Завідувач кафедри
комп'ютерної інженерії
та кібербезпеки

Єфіменко А. А.

«12» квітня 2021 р.



ЗАВДАННЯ

на випускню кваліфікаційну роботу

Студента **Висоцького Віктора Павловича**

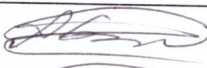
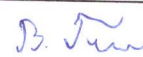
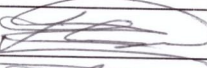
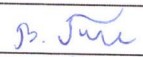
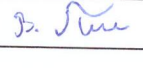
Тема роботи: проект підсистеми захищеного мережного обміну на базі технології Get VPN
затверджена Наказом по університету від «12» квітня 2021 р. № 134/С

Термін здачі студентом закінченої роботи – «22» червня 2021р.

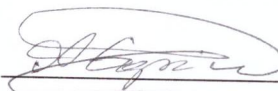
Вихідні дані для роботи:

1. Логічна топологія мережі
2. Маршрутизатори Cisco
3. Комутатори Cisco
4. Операційні системи Cisco IOS, Windows 10, Windows 7, Windows 8 Lite,
5. Графічний симулятор мереж GNS3

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосують-

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Єфіменко А.А.	2.03.21 	2.03.21 
2	Єфіменко А.А.	6.04.21 	6.04.21 
3	Єфіменко А.А.	4.05.21 	4.05.21 

Керівник

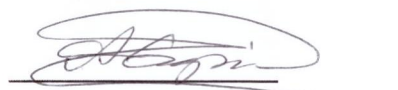


Єфіменко А.А.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	6 квітня 2021 – 7 квітня 2021	Виконано
2	Пошук, огляд та аналіз літературних джерел щодо організації гетерогенної мережі	8 квітня 2021 – 11 квітня 2021	Виконано
3	Аналіз протоколів захисту та маршрутизації	12 квітня 2021 – 16 квітня 2021	Виконано
4	Аналіз можливостей GET VPN	17 квітня 2021 – 19 квітня 2021	Виконано
5	Проектування мережної інфраструктури	20 квітня 2021 – 24 квітня 2021	Виконано
6	Проектування серверної інфраструктури	25 квітня 2021 – 30 квітня 2021	Виконано
7	Проектування сценарію тестування мережі	5 травня 2021 – 9 травня 2021	Виконано
8	Базове налагодження пристроїв мережі	10 травня 2021 – 13 травня 2021	Виконано
9	Налагодження роботи підсистем віддаленого доступу	14 травня 2021 – 30 травня 2021	Виконано
10	Тестування роботи віддаленого доступу	31 травня 2021 – 3 червня 2021	Виконано
11	Аналіз результатів тестування	4 червня 2021 – 6 червня 2021	Виконано
12	Написання пояснювальної записки	7 червня 2021 – 12 червня 2021	Виконано
13	Підготовка презентації та виступу	13 червня 2021 – 14 червня 2021	Виконано
14	Отримання відгуку керівника та рецензії на кваліфікаційну роботу	15 червня 2021 – 16 червня 2021	Виконано
15	Захист	23 червня 2021	

Керівник проекту


(підпис)

Єфіменко А.А.

(прізвище та ініціали)

Студент


(підпис)

Висоцький В. П.

(прізвище та ініціали)

АНОТАЦІЯ

Дана дипломна робота присвячена розробці та налаштуванню захищеної мережі з використанням технологій CISCO. В роботі зроблено аналіз можливостей даних технологій, а також розроблено топологію мережі, розподілено Ір адреси, створено мережевий канал на базі технології Get Vpn. Також надано опис сучасних технологій тунелювання та приведено приклад їх криптографічного захисту. Приведені приклади роботи системи.

					КІК.КБ.Б. – 125 – 02 - ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми захищеного мережного обміну на базі технології Get VPN	Літ.	Арк.	Аркушів
Розроб.		Висоцький В.П.		29.06				
Перевір.		Пулеко І. В.		29.06.21				
Керівник		Єфіменко А.А.		29.06.21				
Н. контр.		Пулеко І. В.		29.06.21				
Зав. каф		Єфіменко А.А.		29.06.21				
						«Житомирська політехніка» ФІКТ гр. КБ – 1		

ANNOTATION

This thesis is devoted to the development and configuration of a secure network using CISCO technologies. The analysis of the possibilities of these technologies is made in the work, and also the network topology is developed, Ip-addresses are distributed, the network channel base of Get Vpn technology is created. A description of modern tunneling technologies is also given and an example of their cryptographic protection is given. Examples of system operation are given.

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		2

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ	4
ВСТУП.....	5
РОЗДІЛ 1. АНАЛІЗ СУЧАСНОГО СТАНУ ТА ОБҐРУНТУВАННЯ АКТУАЛЬНОСТІ ВИКОРИСТАННЯ ЗАХИЩЕНИХ З’ЄДНАНЬ.....	7
1.1 Обґрунтування актуальності теми досліджень захисту мереж	7
1.2 Важливість інформаційних систем	11
1.3 Аналіз існуючих способів захисту мережевих з’єднань.....	15
1.4 Методи та способи передачі, захисту інформації в мережах	18
1.5 Загальний опис Virtual Private Networks.....	21
1.6. Опис технології Group Encrypted Transport VPN	25
Висновок до першого розділу	30
РОЗДІЛ 2. ПРОЕКТУВАННЯ ТА ПРИНЦИПИ СТВОРЕННЯ ЗАХИЩЕНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ GET VPN.....	31
2.1 Опис та принципи вибору топології мережі.....	31
2.2 Розробка загальної структури мережі.....	36
2.3 Структуровані кабельні системи та принципи їх вибору	39
2.4 Опис логічного проектування мережі.....	41
Висновок до другого розділу.....	44
РОЗДІЛ 3. ВИБІР ТА НАЛАГОДЖЕННЯ ОБЛАДНАННЯ, ТЕСТУВАННЯ СТВОРЕНОЇ МЕРЕЖІ.....	45
3.1 Обґрунтування вибору обладнання	45
3.2 Налаштування технології маршрутизації та захисту пристроїв.....	49
3.4 Перевірка працездатності та тестування налаштованих функцій.....	53
Висновок до третього розділу	57
ВИСНОВКИ	58
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ.....	59
ДОДАТКИ	61

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		3

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

VPN – Virtual Private Network - віртуальна приватна мережа

ПК – Персональний комп'ютер

PPTP – Point to Point Tunneling Protocol L2TP – Layer 2 Tunneling Protocol

NAT - Network Address Translation — перетворення мережевих адрес

PAT - Port Address Translation

IP – Internet Protocol

OSPF - Open Shortest Path First

ISAKMP – Internet Security Association and Key Management Protocol - Інтернет протокол асоціацій безпеки та керування ключами

IKE – Internet Key Exchange

WAN - широкопasmова мережа

LAN - Local Area Network

CAM - Content-Addressable Memory

MAC - Media access control

STP - Spanning Tree Protocol

ARP - Address Resolution Protocol

BPDU - Bridge Protocol Data Unit

TCP - transmission control protocol

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		4

ВСТУП

Сьогодні дослідження побудови ефективних комп'ютерних мереж займають дуже ключову роль у нашому житті. Напрямки застосування нових інформаційних технологій на базі електронно-обчислювальної техніки і розвинутих засобів комунікацій в управлінській діяльності підприємств світу та країн різноманітні – від забезпечення найпростіших функцій службового листування до системного аналізу і підтримки складних задач прийняття рішень. Оскільки люди починають використовувати технології для спілкування, завжди існував чіткий розподіл між мережами. Публічна мережа, подібно до загальнодоступної комунікаційної системи та Інтернету, - це велика колекція не пов'язаних між собою аналогів, які більш-менш вільно обмінюються інформацією між собою. Люди, які мають доступ до загальнодоступної мережі, можуть мати або не мати нічого спільного, і будь-яка особа в цій мережі може спілкуватися лише з невеликою частиною своїх потенційних користувачів. Приватна мережа складається з комп'ютерів, що належать приватній організації, які спеціально діляться даними з один одного. Їх запевняють, що вони будуть єдиними, хто використовує мережу, і що дані, передані між ними, бачитимуть лише інші в групі. Типова корпоративна локальна мережа (локальна мережа) або широкосмугова мережа - це деякі приклади приватної мережі. Межа між приватною та публічною мережею завжди проводилася на маршрутизаторі шлюзу, де компанія встановить брандмауер, щоб не допустити злоумисників із загальнодоступних мереж до їх приватної мережі або не дати власним внутрішнім користувачам переглядати публічну мережу, коли компанії могли дозволити своїм локальним мережам працювати як окремі, ізольовані острови. Кожне відділення може мати власну локальну мережу зі своєю схемою імен, електронною поштою та навіть своїм улюбленим мережевим протоколом - жоден з яких не може бути сумісним з іншими установами офісів. Однак, коли все більше ресурсів компанії переходило на комп'ютери, ці офіси потребували взаємозв'язку. Традиційно це робилося за допомогою орендованих телефонних ліній різної швидкості. Використовуючи орендовані лінії, компанія може бути впевнена, що

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		5

зв'язок завжди доступний і приватний. Однак орендовані телефонні лінії можуть коштувати дорого. Зазвичай вони виставляються на основі фіксованої щомісячної плати плюс витрати на пробіг. Якщо компанія має офіси в іншій країні, ці витрати можуть бути непомірними.

Об'єкт дослідження дипломної роботи - процес створення мережі. Для розуміння місця технологій Get Vpn в мережі, зображено структурну схему типової організації.

Предмет дослідження даної роботи – технологія захищеного між мережного обміну GET VPN.

Завдання – створення системи кіберзахисту в режимі реального часу. За останні 10 років кібернетичні атаки досить помітно розвинулися і змінили свій типовий вигляд та алгоритм проведення. Завдяки розповсюдженій практиці використання базових видів захисту, як антивірус та фаєрвол, інформаційні системи стали менш-вразливими до типових атак, таких як: атака з допомогою вірусів, DDOS-атаки, ARP-спуфінг і так далі. Тож при побудові сучасних мереж використовуються все більш різноманітні засоби та топології, а також засоби тунелювання.

Результатом роботи - має бути повністю розроблений і налаштований проект мережі.

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		6

РОЗДІЛ 1. АНАЛІЗ СУЧАСНОГО СТАНУ ТА ОБҐРУНТУВАННЯ АКТУАЛЬНОСТІ ВИКОРИСТАННЯ ЗАХИЩЕНИХ З'ЄДНАНЬ

1.1 Обґрунтування актуальності теми досліджень захисту мереж

У наш час кіберпростір стикається з різними типами кіберзагроз та атак. Кібербезпека стосується захисту кіберпростору від кіберзагроз. Нещодавно все було комп'ютеризовано з використанням кібернетики. Різні технології, такі як хмарні обчислення, смартфони, техніки Інтернету речей тощо. Конфіденційність, безпека та економічні втрати збільшуються через кібератаки. Основна мета хакера полягає в отриманні незаконного доступу до комп'ютерної інформації, програмного забезпечення, інтелектуальної власності або базової мережі користувачів. Кіберзагрози створюють багато соціально-економічних, екологічних, етичних, національних та міжнародних проблем. Сьогодні людина може надсилати та отримувати будь-яку форму даних, електронною поштою чи аудіо чи відео, лише натисканням кнопки, але чи замислювався він коли-небудь про те, наскільки надійно його ідентифікатор даних безпечно передається або надсилається іншій людині будь-який витік інформації. Відповідь полягає в кібербезпеці. Оскільки комп'ютери та мережеві системи зростають у сучасному світі, потреба у зростанні та потужній безпеці комп'ютерів та мереж також стає все більш необхідною та важливою. Збільшення системи комп'ютерних мереж спричинило багато мереж різного роду інтернет-загроз, і завдяки цьому впливу можна помітити, що потреба в підвищеній безпеці мережі є життєво важливою і важливою в кожній організації. Захист може включати ідентифікацію, автентифікацію та авторизацію та камеру спостереження для захисту цілісності, доступності, підзвітності та автентичності комп'ютерного обладнання або мережевого обладнання. Не існує встановленої процедури проектування захищеної мережі. Безпека мережі повинна бути розроблена з урахуванням потреб однієї організації, а не будь-якої іншої. Наприклад, невелика юридична компанія дозволить отримати доступ до інформації про справи для уповноважених користувачів на зовнішній стороні мережі, і в той же час забезпечити, щоб повний доступ до Інтернету завжди був доступний для

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		7

співробітників всередині мережі, в інших випадках отримати доступ до матеріалів справи з офісу або в дорозі. Сьогодні Інтернет - це інфраструктура, яка швидко зростає у повсякденному житті. У сучасному технічному середовищі багато новітніх технологій змінюють обличчя людини. Але завдяки цим новітнім технологіям ми не можемо захистити нашу приватну інформацію дуже ефективно, і тому в наші дні кіберзлочини зростають з кожним днем. Сьогодні понад 60 відсотків загальної кількості комерційних транзакцій здійснюється в Інтернеті, тож це поле вимагало високої якості захисту для прозорих та найкращих транзакцій. Отже, кібербезпека стала останнім випуском. Сфера кібербезпеки не обмежується лише захистом інформації в ІТ-галузі, а й різними іншими сферами, такими як кіберпростір тощо. Навіть новітні технології, такі як хмарні обчислення, мобільні обчислення, електронна комерція, мережеві банкінги тощо, також потребують високого рівня безпеки. Оскільки ці технології містять важливу інформацію про людину, їх безпека стала необхідною справою. [2]. Підвищення кібербезпеки та захист критично важливих інформаційних інфраструктур мають важливе значення для безпеки та економічного добробуту кожної країни. Зробити Інтернет безпечнішим (та захистити його користувачів) стало невід'ємною частиною розвитку нових послуг, а також державної політики. Боротьба з кіберзлочинністю потребує комплексного та безпечного підходу. Враховуючи, що лише технічні заходи не можуть запобігти будь-якому злочину, надзвичайно важливо, щоб правоохоронні органи могли ефективно розслідувати та переслідувати кіберзлочини. Сьогодні багато держав та урядів вводять суворі закони щодо кібер-цінних паперів, щоб запобігти втраті важливої інформації. Кожна людина також повинна навчитися цій кібербезпеці та врятувати себе від цих все більших кіберзлочинів. Кіберзлочинність - це термін будь-якої незаконної діяльності, яка використовує комп'ютер як основний засіб вчинення та крадіжки. Зростаючий перелік кіберзлочинів включає злочини, які стали можливими завдяки комп'ютерам, такі як вторгнення в мережі та розповсюдження комп'ютерних вірусів, а також комп'ютерні варіанти наявних злочинів, таких як викрадення особистих даних, переслідування, знущання та тероризм, які стати такою ж основною проблемою для людей і націй. Зазвичай

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		8

загальнолюдською мовою кіберзлочинність може бути визначена як злочин, скоєний за допомогою комп'ютера та Інтернету з метою встановлення особистості особи, продажу контрабанди, переслідування жертв або зриву операцій із зловмисними програм. Оскільки щодня технології відіграють головну роль у житті людини, кіберзлочини також збільшуватимуться разом із технологічним прогресом. Тут згадано нижче деякі з тенденцій, які мають величезний вплив на кібербезпеку.

1. Веб-сервери зберігається загроза атак на веб-програми для вилучення даних або розповсюдження шкідливого коду. Кіберзлочинці розповсюджують свій зловмисний код через законні веб-сервери, які вони скомпрометували. Але атаки на викрадення даних, багато з яких привертають увагу ЗМІ, також є великою загрозою. Тепер нам потрібно більше акцентувати увагу на захисті веб-серверів та веб-додатків. Веб-сервери - особливо найкраща платформа для викрадення даних цими злочинцями. Отже, завжди потрібно використовувати безпечніший браузер, особливо під час важливих операцій, щоб не стати жертвою цих злочинів.

2. Хмарні обчислення та їхні послуги. Сьогодні всі малі, середні та великі компанії повільно застосовують хмарні сервіси. Іншими словами, світ повільно рухається до хмар. Ця остання тенденція представляє великий виклик для кібербезпеки, оскільки трафік може обходити традиційні пункти перевірки. Окрім того, із збільшенням кількості програм, доступних у хмарі, також потрібно буде вдосконалювати засоби управління веб-додатками та хмарними службами, щоб запобігти втраті цінної інформації. Незважаючи на те, що хмарні сервіси розробляють власні моделі, все ще виникає багато питань щодо їх безпеки. Хмара може надавати величезні можливості, але завжди слід зазначити, що по мірі еволюції хмари та збільшення її загрози безпеки.

3. АРТ та цілеспрямовані атаки - це абсолютно новий рівень засобів кіберзлочинності. Роками можливості мережевої безпеки, такі як веб-фільтрація або IPS, відігравали ключову роль у виявленні таких цілеспрямованих атак (переважно після початкового компромісу). Оскільки зловмисники стають сміливішими та застосовують більш розмиті методи, мережева безпека повинна інтегруватися з іншими службами безпеки, щоб виявляти атаки. Отже, потрібно вдосконалити

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		9

наші методи безпеки, щоб запобігти появі нових загроз у майбутньому.

4. Мобільні мережі Сьогодні ми можемо підключитися до будь-кого в будь-якій частині світу. Але для цих мобільних мереж безпека дуже серйозна проблема. У наші дні брандмауери та інші заходи безпеки стають пористими, оскільки люди використовують такі пристрої, як планшети, телефони, ПК тощо, які знову вимагають додаткових цінних паперів, крім тих, що присутні в застосованих додатках. Ми завжди повинні думати про проблеми безпеки цих мобільних мереж. Подальші мобільні мережі дуже схильні до цих кіберзлочинів, тому слід бути обережними у випадку їхніх проблем безпеки.

5.Новий Інтернет-протокол IPv6 - це новий Інтернет-протокол, який замінює IPv4 (старіша версія), який є основою наших мереж загалом та Інтернету в цілому. Захист IPv6 - це не лише питання перенесення можливостей IPv4. Хоча IPv6 є оптовою заміною для надання більшої кількості IP-адрес, є деякі дуже фундаментальні зміни в протоколі, які потрібно враховувати в політиці безпеки. Тому завжди краще якомога швидше перейти на IPv6, щоб зменшити ризики, пов'язані з кіберзлочинністю.

6. Шифрування коду - це процес кодування повідомлень (або інформації) таким чином, що підслуховувачі чи хакери не можуть його прочитати. У схемі шифрування повідомлення або інформація зашифровуються за допомогою алгоритму шифрування, перетворюючи їх у нечитабельний текст шифру. Зазвичай це робиться із використанням ключа шифрування, який вказує, як кодувати повідомлення. [5]. Шифрування на самому початковому рівні захищає конфіденційність даних та їх цілісність. Але більше використання шифрування приносить більше проблем у кібербезпеці. Шифрування також використовується для захисту даних при передачі, наприклад, дані, що передаються через мережі (наприклад, Інтернет, електронна комерція), мобільні телефони, бездротові мікрофони, бездротові домофони тощо. Отже, зашифрувавши код, можна дізнатися, чи є витік інформації. По мірі того, як ми стаємо більш соціальними у світі, який стає все більш зв'язаним, компанії повинні знаходити нові способи захисту особистої інформації. Соціальні медіа відіграють величезну роль у кібербезпеці та

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		10

внесе великий внесок у особисті кіберзагрози. Прийняття соціальних мереж серед персоналу стрімко зростає, а також загроза нападу. Оскільки соціальні медіа чи сайти соціальних мереж майже щодня використовуються більшістю з них, це стало величезною платформою для кіберзлочинців для злову приватної інформації та крадіжки цінних даних. У світі, де ми швидко відмовляємося від своєї особистої інформації, компанії повинні гарантувати, що вони так само швидко виявляють загрози, реагують у режимі реального часу та уникають будь-яких порушень. [17]. Оскільки ці соціальні медіа легко привертають увагу людей, хакери використовують їх як приманку для отримання необхідної інформації та даних. Отже, люди повинні вживати відповідних заходів, особливо у роботі з соціальними мережами, щоб запобігти втраті своєї інформації. Здатність окремих людей ділитися інформацією з мільйонною аудиторією є основним викликом, який соціальні медіа ставлять перед бізнесом. Окрім надання кому-небудь повноважень розповсюджувати комерційно конфіденційну інформацію, соціальні медіа також надають таку ж силу розповсюдженню неправдивої інформації, яка може бути настільки ж шкідливою. Швидке поширення неправдивої інформації через соціальні мережі є одним із нових ризиків. Хоча соціальні медіа можуть бути використані для кіберзлочинів, ці компанії не можуть дозволити собі припинити використання соціальних медіа, оскільки вони відіграють важливу роль у публічності компанії. Натомість вони повинні мати рішення, які повідомлятимуть їх про загрозу, щоб виправити її до нанесення реальної шкоди. Однак компанії повинні це розуміти і усвідомлювати важливість аналізу інформації, особливо в соціальних розмовах, та пропонувати відповідні рішення щодо безпеки, щоб не триматися подалі від ризиків. Потрібно обробляти соціальні медіа, використовуючи певні політики та правильні технології. [4].

1.2 Важливість інформаційних систем

Інформаційні системи відіграють життєво важливу роль у загальній діяльності будь-якої організації. Вони надають своїм користувачам багато переваг, від простої обробки транзакцій на операційному рівні до складних завдань, таких як

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		11

прийняття важливих та конкурентних рішень на стратегічному рівні організації. Можна виділити кілька ролей, які відіграють інформаційні системи в організації, але О'Брайен та Маракас визначили три основні ролі, які відіграють інформаційні системи у бізнесі. Це такі; Інформаційні системи підтримують бізнес-процеси та операції. По-друге, вони підтримують прийняття рішень співробітниками та менеджерами і, нарешті, підтримують стратегії досягнення конкурентних переваг. Ці три основні ролі охоплюють будь-які інші ролі, які відіграють інформаційні системи в організації. Інформаційні системи багато в чому підтримують бізнес-процеси та операції організації. Наприклад, в готелі реєстрація заїзду та виїзду з готелю здійснюється за допомогою комп'ютерів та програмного забезпечення, що полегшує роботу, відмінюючи традиційний спосіб використання зошитів та паперу для запису такої інформації. Тепер клієнти можуть навіть зробити власні бронювання через веб-сайт готелів замість відвідування зробити це особисто в готелі, що може призвести до тиску на персонал офісу. Зараз розроблені системи для легкого та швидкого збору інформації про клієнтів. Зараз завдяки інформаційним системам різні підрозділи організації працюють легко. Відділ ведення домашнього господарства готелю тепер може повідомити адміністрацію про те, які номери вже готові до використання, а які ні, без особистої взаємодії персоналу в результаті інформаційних систем. Управління організацією тепер стало більш об'єднаним з добре інтегрованими інформаційними системами. Інформаційні системи також допомагають співробітникам та менеджерам бізнесу приймати обґрунтовані рішення. Це пов'язано з тим, що інформаційні системи мають можливість аналізувати дані, зібрані як в рамках організації, так і із зовнішніх джерел, на корисну інформацію, яка може бути використана працівниками та менеджерами в процесі прийняття рішень. Прийняття рішень є невід'ємною частиною управління і відбувається на всіх функціях і на всіх рівнях. Рішення краще приймати, коли доступна точна інформація, яка допомагає тому, хто приймає рішення, приймати об'єктивне рішення. Типи інформаційних систем, такі як Інформаційна система управління (MIS), Системи підтримки рішень (DSS) та Виконавчі інформаційні системи (EIS), спеціально розроблені, щоб до-

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		12

помогти керівництву організації у процесі прийняття рішень. Тезесистеми формують типові звіти та графіки з таких питань, як тенденція замовлень, аналіз споживачів, прибутковість продукції, готові позиції та прогнози запасів, звіти про аварії та відсутніх, звіти про оцінку роботи та багато іншого. Менеджери та співробітники використовують ці звіти та графіки як основу для своїх рішень. Наприклад, рішення щодо того, які страви, які потрібно додати або вилучити з меню готелю, може приймати менеджер з питань харчування та напоїв після типового аналізу, який приймається за допомогою системи підтримки рішень. Нарешті, інформаційні системи також підтримують стратегії для конкурентних переваг. Конкуренція в сучасному бізнесі надзвичайно важлива, і що стане важливим, це те, як швидко компанії можуть перетворити свої масиви інформації, яку вони збирають, у знання, щоб вони могли надавати послуги та продукти, які відповідають їх конкурентам. Стратегічні інформаційні системи можуть допомогти забезпечити госпітальні операції за допомогою інноваційних засобів, необхідних їм для надання продуктів та послуг, що дасть їм порівняльну перевагу над конкурентами. Промисловість, конкурентні переваги можуть призвести до збільшення продажів приміщень (завдяки ефективним системам бронювання та організаційних веб-сайтів), зниженню вартості товарів (завдяки зменшенню експлуатаційних витрат та менш дорогим каналам розподілу), поінформованості про бренд (завдяки ефективним рекламним кампаніям, націленим на відповідного замовника та доставлених через відповідний економічно ефективний засіб), хороші взаємовідносини з клієнтом та організацією (шляхом ведення бази даних про клієнтів та їх потреби) та прийняття своєчасних ефективних рішень. Усі приватні особи, компанії та, загалом, усі організації постійно збирають дані, багато з яких для них взагалі не мають значення. Однак доступні інші дані, які дозволяють їм краще зрозуміти своє власне середовище та себе. Ці дані - те, що ми знаємо як інформацію - дозволяють їм приймати більш точні рішення. З цієї причини потрібна сума інформація в потрібний момент є ключовим фактором для кожної організації. Менеджери компаній приймають рішення, готують плани та контролюють діяльність своєї компанії, використовуючи інформацію, яку вони можуть

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		13

отримати або з офіційних джерел, або за допомогою неформальних каналів, таких як особисті розмови, телефонні дзвінки, соціальні контакти тощо. [12]. За цих обставин менеджери теоретично повинні мати можливість визначити та отримати тип інформації, яка їм потрібна. Однак це не те, що відбувається на практиці; швидше, спосіб виконання менеджерами своєї роботи залежить від наявної інформації, до якої вони мають доступ. Тому більшість рішень прийняті за відсутності абсолютних знань, або через те, що інформація недоступна, або через те, що доступ до неї буде дуже дорогим. Незважаючи на труднощі з отриманням інформації, керівники потребують відповідної інформації, на якій базуватимуть свої функції планування, контролю та прийняття рішень. Хоча терміни дані та інформація іноді використовуються без розбору, вони мають різне значення. Дані - це не випадкові символи, що представляють символ значення атрибутів або подій. Отже, дані - це факти, події та операції, що зберігаються відповідно до узгодженого коду. Дані - це факти, отримані в результаті зчитування, спостереження, обчислення, вимірювання тощо. Суми та інші деталі організації наприклад, рахунки-фактури, чеки, квитанції тощо. Дані отримуються автоматично, що є результатом рутинної процедури, такої як виставлення рахунків або процеси вимірювання. Процес роздумів та розуміння інформації - це те, що дозволяє повідомленням мати різне значення для різних людей. Цей процес також означає, що дані, проаналізовані, узагальнені або оброблені для отримання повідомлень, стануть інформацією лише в тому випадку, якщо одержувач розуміє їх значення. Щоб дані трансформувались в інформацію, має існувати усвідомлення того, що людина отримуючи повідомлення, він використовуватиме його для свого навчання, посади в організації та знайомства з мовою та розрахунками, що використовуються в повідомленні. [6]. Хоча всі менеджери потребують інформації, вони не всі потребують інформації одного типу. Вид необхідної інформації буде залежати від ряду факторів: їх рівня в ієрархії, роботи, яку вони виконують, конфіденційності, терміновості тощо. Дійсно, корисність інформації є суперечливим моментом, і те, що для однієї людини є інформацією, для іншого це дані. Наприклад, в організації, коли інформація передається з одного організаційного рівня на ін-

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		14

ший, її значення може суттєво змінитися, адже що на одному ієрархічному рівні це розглядається як важлива інформація, тоді як на іншому рівні це просто дані.

1.3 Аналіз існуючих способів захисту мережевих з'єднань

Системна та мережева технологія - ключова технологія для широкого спектру застосувань. Безпека має вирішальне значення до мереж та додатків. Хоча, мережна безпека є найважливішою вимогою для нових мереж, існує значний брак безпеки методів, які можна легко реалізувати. Існує "розрив у спілкуванні" між розробниками технологій безпеки та розробниками мереж. Дизайн мережі добре розроблений процес, який базується на відкритих системах Модель інтерфейсу (OSI). Модель OSI має кілька переваг при проектуванні мереж. Вона пропонує модульність, гнучкість, простота використання та стандартизація протоколів. Протоколи різні шари можна легко комбінувати для створення стеки, які дозволяють модульну розробку. реалізація окремих шарів може бути змінена пізніше без внесення інших коригувань, дозволяючи гнучкість у розвитку. На відміну від мережі дизайн, безпечний дизайн мережі - це не дуже добре розроблений процес. Не існує методології керувати складністю вимог безпеки. Розглядаючи мережеву безпеку, вона повинна бути такою підкреслив, що вся мережа захищена. Безпека мережі стосується не лише безпеки в комп'ютерах на кожному кінці ланцюг спілкування. При передачі даних файл канал зв'язку не повинен бути вразливим Атакувати. Можливий хакер може націлити на каналу зв'язку, отримати дані, розшифрувати їх та повторно вставте помилкове повідомлення. Захист мережі це так само важливо, як захист комп'ютерів і шифрування повідомлення. Кілька механізмів безпеки розроблено таким чином, що їх можна використати на певному рівні моделі мережевого рівня OSI. [1].

Безпека на рівні додатків

Заходи безпеки, що використовуються на цьому рівні, специфічні для конкретного застосування. Різні типи додатків потребують окремих заходів безпеки. Для того, щоб забезпечити захист рівня додатків, програми потрібно моди-

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		15

фікувати. Вважається, що розробити криптографічно обґрунтований протокол програми дуже складно, а його правильна реалізація ще складніша. Отже, механізми захисту рівня додатків для захисту мережевих комунікацій переважно є лише рішеннями, заснованими на стандартах, які використовуються протягом певного часу. Прикладом протоколу захисту прикладного рівня є Secure Multipurpose Internet Mail Extensions (S / MIME), який зазвичай використовується для шифрування повідомлень електронної пошти. Безпека на транспортному рівні - заходи безпеки на цьому рівні можуть бути використані для захисту даних за один сеанс зв'язку між двома хостами. Найпоширенішим використанням протоколів захисту транспортного рівня є захист трафіку сеансів HTTP та FTP.

Безпека транспортного рівня (TLS) і рівень захищеного сокета (SSL) - найпоширеніші протоколи, що використовуються для цієї мети.

Мережевий рівень - заходи безпеки на цьому рівні можуть застосовуватися до всіх додатків; таким чином, вони не є специфічними для застосування. Усі мережеві комунікації між двома хостами або мережами можуть бути захищені на цьому рівні, не змінюючи жодної програми. У деяких середовищах протокол захисту мережевого рівня, такий як Інтернет-протокол

Безпека (IPsec) забезпечує набагато краще рішення, ніж елементи керування транспортного або прикладного рівня, через труднощі додавання елементів керування до окремих програм. Однак протоколи безпеки на цьому рівні забезпечують меншу гнучкість зв'язку, яка може знадобитися деяким програмам. До речі, механізм захисту, призначений для роботи на вищому рівні, не може забезпечити захист даних на нижчих шарах, оскільки нижчі шари виконують функції, вищі шари не знають. Отже, може знадобитися розгортання безлічі механізмів безпеки для підвищення безпеки мережі. [10].

У наступних розділах ми обговоримо механізми безпеки, що застосовуються на різних рівнях мережевої архітектури OSI для досягнення мережевої безпеки. При розробці захищеної мережі слід зазначити наступне :

1. Доступ - авторизованим користувачам надається означає спілкуватися з та з певної мережі.

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		16

2. Конфіденційність - інформація в мережі залишається приватною.
3. Аутентифікація – забезпечення того, що користувачі - це ті, за кого вони себе видають.
4. Цілісність - переконайтеся, що повідомлення не було модифіковано під час транспортування.

Розроблено ефективний план мережевої безпеки з розумінням питань безпеки, потенціалу зловмисників, необхідний рівень безпеки та фактори, які робили мережу вразливою до атак інструменти - це шифрування, механізми автентифікації, виявлення вторгнень, управління безпекою та брандмауери. [2]. Підприємства у всьому світі використовуючи комбінацію деяких з цих інструментів. "Інтранети" одночасно підключені до Інтернету та розумно захищений від нього. Інтернет сама архітектура призводить до вразливостей в мережі. Інтернет дуже допомагає у розробці нової безпеки технології та підходи до мереж з доступ до Інтернету та сама інтернет-безпека. Типи атак через Інтернет потрібно також вивчити, щоб мати можливість виявляти та охороняти проти них. Системи виявлення вторгнень є встановлюється на основі типів атак більшості загальновживані. Вторгнення в мережі складаються з пакети, які вводяться для створення проблем для наступні причини:

- марно споживати ресурси
- перешкоджати роботі будь-яких системних ресурсів
- Отримати системні знання, які можуть бути експлуатована в пізніших атаках

Контроль доступу та захист паролем. Поняття імені користувача та пароля було основним способом захисту нашої інформації. Це може бути одним із перших заходів щодо кібербезпеки. [19]. Аутентифікація даних. Документи, які ми отримуємо, завжди повинні бути автентифіковані перед завантаженням, тобто їх слід перевірити, чи вони походять із надійного та надійного джерела та чи не змінюються. Автентифікація цих документів зазвичай здійснюється за допомогою антивірусного програмного забезпечення, що є в пристроях. Таким чином, хороше антивірусне програмне забезпечення також має важливе значення для захисту при-

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		17

строїв від вірусів. Сканери шкідливих програм. Це програмне забезпечення, яке зазвичай сканує всі наявні в системі файли та документи на наявність зловмисного коду чи шкідливих вірусів. Віруси, хробаки та троянські коні - приклади шкідливого програмного забезпечення, яке часто об'єднують у групи та називають шкідливим програмним забезпеченням. Брандмауери. Брандмауер - це програмне забезпечення або апаратне забезпечення, яке допомагає відсіяти хакерів, віруси та хробаків, які намагаються дістатися до вашого комп'ютера через Інтернет. Усі повідомлення, що надходять або виходять з Інтернету, проходять через наявний брандмауер, який перевіряє кожне повідомлення та блокує повідомлення, які не відповідають зазначеним критеріям безпеки. Тому брандмауери відіграють важливу роль у виявленні шкідливого програмного забезпечення. Антивірусне програмне забезпечення Антивірусне програмне забезпечення - це комп'ютерна програма, яка виявляє, запобігає та вживає заходів для роззброєння або видалення шкідливих програм, таких як віруси та хробаки. [20]. Більшість антивірусних програм включають функцію автоматичного оновлення, яка дозволяє програмі завантажувати профілі нових вірусів, щоб вона могла перевірити наявність нових вірусів, як тільки їх виявлять. Антивірусне програмне забезпечення є обов'язковою та необхідною мірою для кожної системи.

1.4 Методи та способи передачі, захисту інформації в мережах

На даний момент основний функціонал передачі інформації в мережах, а також можливість їх з'єднання забезпечують безліч протоколів. Маршрутизацію в даній роботі забезпечить протокол OSPF (Open Shortest Path First), адже це чи не найпопулярніший маршрутизації стану каналу. Цей відкритий стандарт, тому його можна запускати на маршрутизаторах, що виробляються різними постачальниками, що на відміну від EIGRP, власного протоколу Cisco, який можна запускати лише на пристроях Cisco. OSPF є безкласовим і підтримує такі функції, як VLSM, ручне підведення підсумків маршрутів, поступове оновлення, рівномірне балансування навантаження тощо. Як метрику OSPF використовує єдиний параметр - вартість інтерфейсу. OSPF

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		18

використовує багатоадресні адреси 224.0.0.5 та 224.0.0.6 для зв'язку між маршрутизаторами з підтримкою OSPF. Адміністративна відстань за замовчуванням для маршрутів OSPF - 110. Маршрутизаторам, на яких запущено OSPF, потрібно встановити взаємозв'язок сусідів перед обміном оновленнями маршрутизації. Оскільки OSPF є протоколом маршрутизації стану зв'язку, сусіди не обмінюються таблицями маршрутизації; натомість вони обмінюються інформацією про мережеву топологію. Потім кожен маршрутизатор OSPF запускає алгоритм SFP для обчислення найкращих маршрутів і додає їх до таблиці маршрутизації. Оскільки кожен маршрутизатор знає всю топологію мережі, шанс виникнення циклу маршрутизації є мінімальним. Маршрутизатори OSPF зберігають інформацію про маршрутизацію та топологію у трьох таблицях:

- таблиця сусідів - зберігає інформацію про сусідів OSPF.
- таблиця топології - зберігає структуру топології мережі.
- таблиця маршрутизації - зберігає найкращі маршрути.

Функція клієнта SSH - це програма, яка працює над протоколом SSH для забезпечення автентифікації пристрою та шифрування. Клієнт SSH забезпечує безпечне, зашифроване з'єднання з будь-яким пристроєм, на якому запущений сервер SSH. Це з'єднання забезпечує зашифроване вихідне з'єднання.

Завдяки автентифікації та шифруванню клієнт SSH забезпечує захищений зв'язок через незахищену мережу. SSH - це недороге програмне рішення для утримання сторонніх поглядів від даних в мережі. Це не вирішує всі проблеми конфіденційності та безпеки, але ефективно ліквідує декілька з них. Його основними особливостями є:

- Безпечний протокол клієнт / сервер для шифрування та передачі даних через мережу
- Аутентифікація (розпізнавання) користувачів за паролем, хостом або відкритим ключем, плюс необов'язкова інтеграція з іншими популярними системами автентифікації, включаючи Kerberos, SecurID, PGP, TIS Gauntlet

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		19

- Можливість додавати захист до небезпечних мережових програм, таких як Telnet, FTP, та багато інших програм та протоколів на основі TCP / IP
- Майже повна прозорість для кінцевого користувача
- Реалізації для більшості операційних систем [11].

CDP - це протокол виявлення пристроїв, який працює на рівні 2 (рівень каналу передачі даних) на всіх пристроях, виготовлених Cisco (маршрутизатори, мости, сервери доступу та комутатори), і дозволяє програмам управління мережею виявляти пристрої Cisco, які є сусідами вже відомих пристроїв. За допомогою CDP програми для керування мережею можуть дізнатися тип пристрою та адресу агента простого мережевого протоколу управління сусідніх пристроїв, на яких працюють прозорі протоколи нижчого рівня. Ця функція дозволяє програмам надсилати запити SNMP на сусідні пристрої. CDP працює на всіх носіях, які підтримують протокол доступу до підмереж. Оскільки CDP працює лише на рівні каналу передачі даних, дві системи, які підтримують різні протоколи мережевого рівня, можуть дізнатися одна про одну. Кожен налаштований CDP пристрій надсилає періодичні повідомлення на адресу багатоадресної розсилки, рекламуючи принаймні одну адресу, за якою він може отримувати повідомлення. Це також містить інформацію про час життя або про час утримання, тобто проміжок часу, коли приймаючий пристрій зберігає інформацію CDP перед тим, як її відкинути. Кожен пристрій також прослуховує повідомлення, надіслані іншими пристроями, щоб дізнатись про сусідні пристрої. Протоколи виявлення рівня 2 розроблені для спільного використання інформації між безпосередньо підключеними пристроями. Вони надсилають Інформацію про конкретний пристрій (наприклад, роль пристрою, стан інтерфейсу, призначена IP-адреса, версія операційної системи, живлення, Можливості Ethernet, дуплексність, конфігурація VLAN тощо) до сусідів. Ці протоколи корисні під час роботи в мережі обслуговування та процес усунення несправностей, коли адміністратор намагається знайти джерело проблеми та ізолювати його. Протокол виявлення Cisco

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		20

(CDP) був першим із цього сімейства виявлення рівня каналу передачі даних протоколів. Використання CDP обмежене для пристроїв Cisco лише завдяки патентована природі. [3].

1.5 Загальний опис Virtual Private Networks

Опис даної технології краще всього буде почати з пояснення самої суті слова «мережа. Це, мабуть, найменш складний для нас термін для визначення та розуміння, оскільки загально прийняте визначення є досить суперечливим і загально визнаним у всій галузі. Мережа складається з будь-якої кількості пристроїв які можуть спілкуватися за допомогою довільного методу. До таких пристроїв належать комп'ютери, принтери, маршрутизатори тощо, і можуть бути в географічно різноманітних місцях. Методів, за допомогою яких вони можуть спілкуватися, безліч, оскільки існує незліченна кількість специфікацій електронної сигналізації, а також протоколів каналів передачі даних, транспорту та прикладного рівня. Для простоти, давайте просто погодьмося, що «мережа» - це сукупність пристроїв, які можуть певним чином спілкуватися та можуть успішно передавати та отримувати дані між собою. Термін "приватний" є досить простим і нерозривно пов'язаний з поняттям "віртуалізація", що стосується VPN, які ми обговоримо за мить. У найпростіших визначеннях "приватний" означає, що зв'язок між двома (або більше) пристроями є, певним чином, таємницею - що пристрої, які не беруть участі в "приватному" характері зв'язку, не є приватними щодо переданого вмісту, і що вони насправді зовсім не знають про приватні стосунки. Відповідно, конфіденційність та безпека даних (цілісність даних) також є важливими аспектами VPN, які потрібно враховувати при розгляді будь-якої конкретної VPN впровадження. Іншим способом вираження цього визначення поняття "приватне" є його антонім "публічний". „Публічний” об'єкт - це той, що є відкритим доступом, і ним керують в умовах та обмеженнях загального державного ресурсу, часто через державну адміністративну установу. За контрактом, "приватним" об'єктом є той, де доступ обмежений певним набором об'єктів, і треті сторони не можуть отримати доступ. Як правило, приватним ресурсом управляють суб'єкти, які мають ексклю-

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		21

живне право доступу. Приклади цього типу приватної мережі можна знайти в будь-якій організаційній мережі, яка не підключена до Інтернету або будь-якої іншої зовнішньої організаційної мережі. Ці мережі є приватними через те, що немає зовнішнього підключення, а отже, і зовнішніх мережевих комунікацій. Інший важливий аспект "конфіденційності" у VPN полягає в її технічному визначенні, як опис конфіденційності системи адресації та маршрутизації, що означає, що адресація, що використовується в рамках спільноти VPN, що представляє інтерес, є окремою та окремою від адреси базової спільної мережі, від інших спільнот VPN. Те саме справедливо для системи маршрутизації, що використовується в мережі VPN, і системи базової спільної мережі. Схема маршрутизації та адресації у VPN, для всіх намірів та цілей, повинна бути самодостатньою, але це перероджується у філософську дискусію щодо контексту терміна "VPN". Крім того, варто вивчити відмінності між "одноранговою" та "накладеною" моделями побудови VPN. «Віртуалізація» - це аспект, подібний до того, що ми коротко описали вище як «приватний», проте сценарій дещо змінений - приватне спілкування зараз ведеться через мережеву інфраструктуру, спільну для якої використовує не одна організація. Таким чином, приватний ресурс фактично побудований за допомогою основи логічного розділення деякого базового загального спільного ресурсу, а не за допомогою основи дискретних та виділених фізичних схем та служб зв'язку. Відповідно, "приватна" мережа не має відповідної "приватної" фізичної системи зв'язку. Натомість "приватна" мережа - це віртуальне творіння, яке не має фізичного аналога. Віртуальний зв'язок між двома (або більше) пристроями пов'язаний з тим, що пристрої, які не беруть участь у віртуальних зв'язках, не знайомі з вмістом даних, і що вони також взагалі не знають про приватні стосунки між віртуальними однопітками. Наприклад, спільною мережевою інфраструктурою може бути глобальний Інтернет, і кількість організацій або інших користувачів, які не беруть участь у віртуальній мережі, може буквально нараховувати тисячі або мільйони. Раніше організації або підприємства фізично встановлювали лінії на великі відстані, щоб забезпечити безпечну передачу даних. Однак ця система непрактична для кожного підприємства та повсякденних користувачів через

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		22

вартість, простір та час, необхідні для таких установок. В останні роки, з експоненціальним зростанням Інтернету, ландшафт телекомунікацій докорінно змінився, і Інтернет став частиною майже всіх аспектів розвиненого світу, включаючи освіту, банківську справу, бізнес та політику. За останні два десятиліття громадський Інтернет виявився вразливим для зловмисників, які шукають конфіденційну інформацію. Найновішим рішенням цієї проблеми стала віртуальна приватна мережа на основі IP (IPVPN). Віртуальну приватну мережу (VPN) можна визначити як спосіб забезпечення безпечного зв'язку між членами групи за допомогою використання загальнодоступної телекомунікаційної інфраструктури, збереження конфіденційності за допомогою протоколу тунелювання та процедур безпеки. Системи VPN надають користувачам ілюзію повністю приватної мережі. Віртуальну приватну мережу IP (IPVPN) можна визначити як реалізацію VPN, яка використовує загальнодоступні або спільні ресурси мережі IP для емуляції характеристик приватної мережі на основі IP. Основною метою VPN є надання підприємствам тих самих можливостей, або навіть кращих, як у приватних мережах, але з набагато меншими витратами. Підприємства отримують вигоду від VPN у зниженні вартості, збільшенні масштабованості та збільшенні продуктивності праці, не порушуючи при цьому безпеку. VPN повинна забезпечувати автентифікацію, контроль доступу, конфіденційність та цілісність даних для забезпечення безпеки даних. Можливо, найсильніша мотивація VPN спирається на економіку комунікацій. Колекція віртуальних мереж, реалізована поверх загальної фізичної комунікаційної інфраструктури, дешевша, ніж побудова еквівалентного збору дискретних мереж, кожна для одного клієнта. Ще одним інтересом VPN є, звичайно, можливість перетворювати деякі частини мережа організації, практично невидима для зовнішніх спостерігачів. Цей аспект конфіденційності комунікацій може відігравати важливу роль для організацій. Залежно від рівня безпеки, якого вимагає організація, може бути достатньо простого абстрагування розсуду та загрози мережі VPN. Однак для більш високих рівнів захисту користувачів потрібні відповідні вимоги до сильної безпеки доступу та передачі даних у мережі, і слід застосовувати додаткові механізми. Абстракція VPN також цікава для забезпе-

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		23

чення спілкування в закритих групах. VPN також можна розглядати як підтримку тієї ж функціональності багатоадресної комунікації, але в контрольованому та безпечному середовищі. Можна також подумати про використання багатоадресного зв'язку в мережі VPN, що виглядає як дворівневий груповий зв'язок. Застосуваність VPN в цій галузі є багатообіцяючою. Ще однією важливою мотивацією VPN є властивість розділити мережеві ресурси. За допомогою розділення ресурсів можна надати якісь гарантії якості обслуговування додаткам. Мережеві ресурси можуть бути зарезервовані або надані не на основі VPN. Мережеві ресурси можуть включати буфери в маршрутизаторах, онлайніві посилання пропускну здатності тощо, і навіть адресний простір можна розглядати як спільний ресурс (залежно від того, як реалізовані VPN, адресні простори можуть перекриватися). Із визначення та мотивації VPN можна перелічити кілька вимог до побудови VPN. Будь-яка VPN має мінімальний набір можливостей і може мати додаткові функції відповідно до вимог користувача. Основним моментом є те, що для того, щоб VPN працював, має бути можливість зіставити користувацькі послуги з відповідними можливостями мережевої інфраструктури. Для визначення VPN необхідний адміністративний механізм для призначення членства у VPN. Хост може належати до однієї або декількох мереж VPN, а також до глобальної мережі Інтернет. Бажана можливість динамічної зміни членства в хості. Про додавання нових хостів до VPN (наприклад, користувач, що набирає номер) слід сигналізувати провайдеру у випадку корпоративного VPN. Взагалі це слід робити прозоро для членів VPN. Тим не менше, VPN може бути проінформована про додавання та видалення користувачів через проблеми безпеки або управління групами. Набір членів VPN може бути визначений, пропонує один підхід. Що стосується безпеки, то від VPN можуть знадобитися різні можливості, що залежать від послуги користувача. Мінімальна здатність, яку вимагає VPN, полягає в тому, щоб гарантувати певний вид ізоляції між віртуальною мережею та зовнішнім світом, що впливає з визначення VPN. Залежно від рівня необхідного захисту може бути визначена підключеність користувача, включаючи різноманітні механізми захисту, як IPSec. Безпека може вимагатися дискретно хостами кінцевих

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		24

користувачів, або VPN може застосовувати надзвичайну політику безпеки. VPN може надавати підтримку QoS. Це можна зробити двома різними способами: користувачі можуть сигналізувати про свої вимоги QoS за допомогою RSVP (або іншого методу сигналізації), біти пріоритету IP або що-небудь інше, або VPN може внутрішньо призначати вимоги QoS для відображення в інфраструктурі передачі. Щоб гарантувати QoS, інфраструктура може явно підтримувати запити QoS, або вона може проектуватися таким чином, що вона послідовно забезпечує адекватне QoS (з певним рівнем довіри).

1.6. Опис технології Group Encrypted Transport VPN

Сьогодні високоінтегровані та широкомасштабні мережеві мережі потребують безпечного транспортного рішення, що забезпечує миттєве з'єднання між сайтами без шкоди для якості обслуговування або додавання складності та накладних витрат на загальну мережу. У відповідь на цю потребу Cisco представила інноваційне розширене рішення шифрування - Cisco IOS GET VPN - що використовує безтунельний підхід VPN, заснований на революційній технології Cisco Group Encrypted Transport (GET VPN). Технологія GET VPN пропонує глобальним корпоративним мережам можливість масштабувати голосові, відео та передачі даних із підвищеною мережевою ефективністю. -до будь-якого зашифрованого підключення та високомасштабованого мережевого середовища. Cisco GETVPN пропонує революційне рішення для безтунельних, конфіденційних та конфіденційних комунікацій. Груповий зашифрований транспортний VPN (GETVPN) вводить концепцію довіреної групи для усунення тунельних точка-точка і пов'язаної з ними маршрутизації накладання. Усі члени групи (ГМ) мають спільну асоціацію безпеки (SA), також відому як група SA. Це дозволяє ГМ дешифрувати трафік, зашифрований будь-яким іншим ГМ. (Зверніть увагу, що IPsec CE діє як GM.) У мережах GETVPN немає необхідності узгоджувати точкові IPsec-тунелі між членами групи, оскільки GETVPN є безтунельним. Отже, GETVPN не є технологією VPN від точки до точки для підключення до віддалених місцеположень. GDOI - це протокол керування груповими ключами, який використовується для надання

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		25

набору ключів IPSec групі пристроїв IOS, які називаються Group Members (GM), які хочуть безпечно спілкуватися, GDOI запускається між GM та сервером ключів (KS). Ці ключі періодично оновлюються на всіх пристроях за допомогою процесу, який називається rekey. За допомогою GETVPN ви можете спростити миттєвий зв'язок гілок та забезпечити низьку затримку, увімкнувши постійний прямий зв'язок між сайтами, не вимагаючи транспорту через центральний хаб. За допомогою GETVPN ви можете максимізувати свою мережеву безпеку, і вона забезпечує шифрування мереж MPLS, зберігаючи при цьому мережевий інтелект, такий як підключення до повної мережі, природний шлях маршрутизації та якість обслуговування (QoS). За допомогою GETVPN ви можете дотримуватися державного регулювання та законів про конфіденційність, і це допомагає вам забезпечити дотримання вимог безпеки та внутрішнього регулювання, шифруючи весь трафік глобальної мережі. [3].GETVPN надасть вам гнучкість управління та усуне складне однорангове керування ключами за допомогою групових ключів шифрування.

GETVPN забезпечує такі ключові переваги:

1. Миттєве широкомасштабне підключення будь-до-будь-якого IP за допомогою групової парадигми безпеки IPsec.
2. Використовує переваги базової інфраструктури маршрутизації IP VPN і не вимагає накладання маршрутизації контрольної площини.
3. Легко інтегрується з інфраструктурами багатоадресного передавання без проблем реплікації багатоадресної передачі
4. Спостерігається в традиційних рішеннях IPsec на основі тунелів.
5. Зберігає IP-адресу джерела та адресу призначення під час шифрування та інкапсуляції IPsec.

процес. Тому GETVPN дуже добре інтегрується з такими функціями, як QoS та інженерія трафіку.

Рішення GETVPN базується як на відкритих стандартах, так і на запатентованій Cisco інноваційній технології, яка допомагає використовувати потужність базових MPLS / спільних IP-мереж. На додаток до використання існуючого IKE, IPsec та

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		26

багатоадресні технології, рішення GETVPN спирається на наступні основні будівельні блоки для забезпечення необхідна функціональність:

- GDOI
- Ключові сервери (KS)
- Кооперативні (COOP) KS
- Члени групи (ГМ)
- Збереження заголовка тунелю IP
- Групова асоціація безпеки
- Механізм Rekey [9].

Розуміння протоколу GDOI

Протокол групового домену інтерпретації (GDOI), використовується для розподілу набору криптографічних ключів та політик до групи пристроїв. GDOI визначається як домен інтерпретації протоколу управління ключами асоціації Інтернет-безпеки (ISAKMP) для групового управління ключами. У моделі управління групою протокол GDOI працює між членом групи та контролером групи або сервером ключів (GC / KS) та управляє асоціаціями безпеки групи (GSA) та груповими ключами для набору учасників безпеки. ISAKMP визначає дві фази переговорів. GDOI - це протокол фази 2, захищений асоціацією безпеки фази ISAKMP. GDOI представляє два різні ключі шифрування:

Ключ шифрування ключа (КЕК) - використовується для захисту площини управління. КЕК - це назва ключа, що використовується членами групи для розшифровки повідомлень повторного введення з GC / KS. Цей ключ є частиною ключа шифрування ключа асоціації безпеки .

Ключ шифрування трафіку (ТЕК) - використовується для захисту площини даних. ТЕК - це назва ключа, що використовується учасниками групи для шифрування або дешифрування зв'язку між іншими членами групи. Цей ключ є частиною ключа шифрування транспорту.

Як і у випадку зі стандартним IPsec, усі ключі мають термін служби, і їх потрібно повторно ввести. Ключі, що розподіляються через GDOI, є груповими

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		27

ключами і використовуються всією групою. Як засіб шифрування у данній технології використовується криптографічний стандарт AES. Шифрування AES було створено Національним інститутом стандартів і технологій США у 2001 році і має на меті запропонувати специфікацію електронного шифрування даних. Розробниками AES є два бельгійські криптографи: Джоан Дімен та Вінсент Ріймен. Відомо, що дует запропонував свій блок-шифр Національному інституту стандартів і технологій під час відбору AES. Для того, щоб вибрати безпечний AES, NIST розглянув три різні блок-шифри з сімейства шифрів Rijndael. Усі вибрані три шифри склали 128 біт, але довжина їх ключів становила 128, 192 та 256 біт. Врешті-решт було обрано блок-шифр, розроблений Ріджменом та Даменом. Цей AES був вперше прийнятий у Сполучених Штатах, але з часом він став загальносвітовим. AES характеризується як симетричний блок-шифр, іншими словами він використовує той самий ключ для шифрування та дешифрування. До того, як AES був прийнятий, застосовувався стандарт шифрування даних (DES), який все більше вразливий до атак грубої сили. Ось чому NIST оголосив, що існує невідкладна потреба у кращому та більш розвиненому заміні DES. Отже, AES став використовуватися як кращий, новіший і вдосконалений алгоритм шифрування. Спочатку AES передбачалося використовувати для захисту секретної інформації на державному рівні. Відомо, що його легко застосувати як в апаратному, так і в програмному забезпеченні, в результаті він широко використовується для захисту від різних методів кібератаки, включаючи грубу силу. [8]. На сьогодні AES можуть безкоштовно використовувати державні та приватні організації у своїх комерційних та некомерційних програмах. Проте неурядові організації стикаються з певними обмеженнями, накладеними експортним контролем США. На сьогоднішній день кожен може отримати доступ до криптографії AES лише за секунди. В Інтернеті є Інтернет-інструменти та джерела, оскільки AES має коріння з відкритим кодом. Розширений стандарт шифрування (AES) використовується для захисту даних від несанкціонованого доступу та для їх шифрування. Для цього використовується ключ криптографічного процесу різної довжини. Це позначено як AES-128, AES-192 або AES-256 залежно від довжини.

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		28

Спочатку цей процес був запроваджений Американським національним інститутом стандартів і технологій і може використовуватися в США для шифрування документів з максимальним рівнем безпеки. Цей метод шифрування будь-якого типу даних вважається особливо безпечним та ефективним. Він використовується в численних протоколах і технологіях передачі, наприклад, захист WPA2 мереж WiFi використовує розширений стандарт шифрування, а також стандарт SSH або IPsec. За допомогою технології передачі голосу за IP (VoIP) процес AES часто використовується для захисту користувачів та даних сигналізації. Сьогодні Advanced Encryption Standard постійно інтегрований в апаратне забезпечення багатьох пристроїв. Це забезпечує більш швидке та ефективне шифрування та дешифрування, ніж це було б можливо завдяки чистим програмним рішенням. AES користується величезною популярністю, оскільки переваги говорять самі за себе. Наприклад, цей стандарт шифрування можна вільно використовувати, не вимагає ліцензійних зборів і не підпадає під патентні обмеження. До цього додаються порівняно низькі вимоги до сховища та обладнання. Алгоритм шифрування нескладний та елегантний у програмуванні та простий у реалізації. Стандарт розширеного шифрування використовує алгоритм Рієндаеля в поєднанні з симетричними блоковими шифрами як метод шифрування. Довжини блоків визначені за визначенням і складають 128 біт. Те саме стосується фіксованих довжин ключів; на додаток до 128 біт вони також можуть містити 192 або 256 біт. Ви можете зашифрувати свої тексти за допомогою AES-шифрування в Інтернеті та вибрати довжину ключа (128, 192 та 256 біт). Такі інструменти забезпечують шифрування AES середнім користувачем, але ці онлайн-програми дуже непридатні для використання урядом та організацією. Якщо вам потрібні професійні рішення AES для вашої організації, вам слід розглянути можливість зв'язку з постачальником послуг. Шифрування AES має три різні блокові шифри: AES-128 (128 біт), AES-192 (192 біт) і AES-256 (256 біт). Ці блокові шифри названі на честь довжини ключа, яку вони використовують для шифрування та дешифрування. Всі ці шифри шифрують і дешифрують дані в 128-бітових блоках, але вони використовують різні розміри криптографічних ключів. [14].

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		29

Висновок до першого розділу

В даному розділі було описано та проаналізовано основні мережеві технології, що були використані в проекті. Детально розглянуті основні поняття створення захищених мереж, а також показано переваги використання технології Get vpn. Визначено основні складові частини мережевого обміну та проаналізовано актуальність данної роботи.

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		30

РОЗДІЛ 2. ПРОЕКТУВАННЯ ТА ПРИНЦИПИ СТВОРЕННЯ ЗАХИЩЕНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ GET VPN

2.1 Опис та принципи вибору топології мережі

Класифікація мережі на основі основних ролей

Однорангова мережа

Перший тип мережі, який ми розглянемо, називається Peer-to-Peer. У цьому виді У мережі немає такого поняття, як сервер, і хости мережі не мають певної ролі. Вони надають послуги мережі, а також вони споживають послуги мережі. У рівному мережі ми можемо мати хостів, які виконуватимуть різноманітні різні ролі. Наприклад, один комп'ютер може мати підключений до нього принтер, який спільно використовується в мережі. Інший на комп'ютері може бути встановлений великий жорсткий диск, і кожен може розміщувати на ньому файли жорсткий диск. Отже, у цій ситуації у нас є хости, які одночасно забезпечують та споживають мережу послуги. По суті, вони функціонують одночасно і як клієнт, і як сервер. Головна перевага однорангової мережі - це простота установки. Нам залишається лише ділитися наші ресурси в мережі. Це також дуже недорого, оскільки нам не потрібно купувати сервер апаратне та програмне забезпечення. Звичайно, є певні недоліки однорангової мережі. Спочатку з усіх, однорангова мережа не дуже масштабована, що означає, що чим більше вона стає, тим більше складніше ним керувати. Це тому, що їм бракує централізованого контролю. Однорангові мережі зазвичай застосовуються в невеликих організаціях, які використовують обмежену кількість комп'ютерів. В ситуації, коли в мережі більше 10 комп'ютерів, слід розглянути використання централізованої серверної мережі.

Мережа Клієнт - Сервер

Іншою класифікацією в категорії хост-ролей є мережа клієнтського сервера. У клієнта серверна мережа, на відміну від однорангової мережі, хостам мережі при-

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		31

значені певні ролі їх. У нас є певні системи, певні хости, яким призначено бути серверами. Сервер забезпечує мережеві ресурси. У мережі клієнт-сервер ми також маємо клієнтів або робочі станції. Сервер забезпечує ресурси, а клієнт використовує ресурси. З одноранговим мережа однолітків у всіх була однаковою або схожою операційною системою, але на клієнтському сервері робочі станції мережевих клієнтів мають загальні зручні операційні системи, такі як Windows XP, Vista, 7, MacOS або Linux. Сервери мали б спеціально оптимізовану операційну систему як Server 2003 або Server 2008. Ці операційні системи призначені для забезпечення мережі ресурсів і не призначені для завдань типу клієнта. Головна перевага цього типу мережа полягає в тому, що вона дуже масштабована. Це означає, що дуже легко збільшити розмір в мережі, дуже легко додати більше клієнтів і дуже легко додати більше серверів. Клієнт серверні мережі також набагато легше підтримувати. Це тому, що послуги централізовані. Якщо ми знаємо, де знаходяться всі послуги, ми знаємо, де шукати, коли у нас є якісь проблеми з ними. Резервне копіювання також набагато простіше. Ми можемо налаштувати, щоб користувачі зберігали свої дані на сервер. Таким чином, замість того, щоб створювати резервні копії окремих робочих станцій, нам потрібно лише це робити зробити резервну копію одного місця - сервера. Є деякі недоліки. Операційні системи для серверів є досить дорогими (звичайно, винятком є Linux). Інша справа, що цей тип Мережа вимагає багато планування. Ми повинні вирішити, які сервери будуть розміщені на яких послугах, де вони будуть розміщені в мережі тощо.

Класифікація мережі на основі географічного розташування

Локальна мережа (LAN)

Перший вид мережі, що базується на географії, - це локальна мережа або локальна мережа. Місцева територіальна мережа знаходиться на невеликій географічній території. Приклад локальної мережі це буде мережа всередині певної компанії або мережа у нас вдома. Це може мати, наприклад, кілька поверхів, але в деяких випадках всі вони будуть з'єднані мережевим середовищем шляху. Це також може бути кілька будівель, і вони можуть бути якимось чином зв'язані між собою. Ми можемо мати кілька будівель, наприклад, містечко. Це все ще локальна мережа оскі-

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		32

льки мережа управляється однією організацією та віддаленою розділення господарів порівняно невелике. Це називається міжмережею, але воно все ще є локальним зональної мережі.

Столична мережа (MAN)

Metropolitan Area Network охоплює фізичну область, більшу за локальну мережу, але меншу за WAN, наприклад місто. ЛЮДИНА може бути власністю та нею керувати одна організація, така як урядовий орган або велика корпорація, але ним зазвичай користуються багато людей і організації. Це встановлюється за допомогою різних взаємозв'язків між глобальною мережею та локальною мережею. MAN має багато додатків, він найчастіше використовується в банках, онлайн-бронювання систем та у багатьох військових службах. MAN може забезпечити підключення до Інтернету або кабельне телебачення для локальних мереж у столичному регіоні.

Персональна мережа (PAN)

PAN - це комп'ютерна мережа, організована навколо окремо взятої людини. Він використовується для спілкування між комп'ютерними пристроями, включаючи телефони та персональний цифровий помічник, поруч із тілом людини. Персональні мережі зазвичай включають мобільний комп'ютер, стільниковий телефон та / або портативний обчислювальний пристрій, такий як КПК або Pad.

ПАН можна використовувати для зв'язку між самими персональними пристроями (внутрішньоособисте спілкування), або для підключення до мережі вищого рівня та Інтернету (посилання вгору). ПАН можуть бути побудовані за допомогою кабелів або бездротового зв'язку. USB та FireWire технології часто пов'язують дротовий PAN, тоді як бездротові PAN зазвичай використовують Bluetooth, IrDA, бездротовий USB, Z-Wave та ZigBee. Bluetooth PAN також називають піконетами.

Персональні мережі загалом охоплюють діапазон менше 10 метрів (близько 30 футів).

Класифікація мережі на основі топологій мережі

Топологія мережі - це розміщення різних взаємопов'язаних елементів на комп'ютері мережі. Топологія може бути фізичною або логічною. Добре знати

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		33

про топології мережі оскільки різні типи мережевих стандартів можуть використовувати один тип фізичної топології, але використовувати зовсім іншу логічну топологію. Фізична топологія відноситься до способу комп'ютерна мережа фізично підключена.

Топологія шини

Багато мережевих стандартів, з якими ми будемо працювати, використовуватимуть топологію шини, фізично чи логічно. На топології шини всі дані надходять по центральному проводу. Кожен хост, підключений до цього дроту, може безпосередньо спілкуватися з будь-яким іншим хостом підключений до дроту. Сьогодні ми не побачимо багато мереж, які все ще використовують фізичну шину топологія більше. Однак ми знайдемо багато мереж, які все ще функціонують логічно як автобус.

Топологія кільця

У топології кільцевої мережі немає центрального сполучного середовища. Натомість ми маємо точку для точкових з'єднань між мережевими хостами. Кожен господар пов'язаний зі своїми двома сусідами. На відміну від топології шини, з кільцевою топологією дана робоча станція або хост можуть лише спілкуватися безпосередньо лише з двома іншими хостами в мережі. Дані, на які адресовано хости, крім сусідів, передаватимуться наступному підключеному хосту, поки він не досягне одержувач хосту. Таким чином, інформація може передаватися будь-якому хосту в мережі. Це може бути не прямим з'єднанням, тому що йому, можливо, доведеться переходити від хоста до хоста до хосту, перш ніж він врешті-решт з'явиться його призначення.

Топологія зірок

Топологія зірки використовує центральний сполучний пристрій. Усі хости в мережі підключаються до центральний приєднувальний пристрій з мережевим кабелем, і це фізична топологія. Однак, через різні протоколи він насправді може працювати як топологія кільця або шини. Якщо один хосту потрібно надіслати дані якомусь іншому хосту, він надішле інформацію на центральний з'єднувальний пристрій. Потім центральний сполучний пристрій копіює інформацію та

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		34

пересилає його до відповідного хоста. Спосіб роботи центрального приєднувального пристрою залежить від стандарту мережі що ми використовуємо. Деякі пристрої копіюють ці дані та надсилають їх усім хостам (концентратору). Кожен Потім хост перегляне цю інформацію та перевірить, чи адресовано їй. Якщо пакета немає адресований конкретному хосту, він скине пакет. Таким чином лише правильний одержувач прочитає інформацію в пакеті. Інші мережеві технології працюватимуть зовсім по-іншому. Центральний пристрій буде запам'ятати, який хост підключений до якого порту на центральному пристрої (комутатор). Тому що Центральний пристрій знає, який хост підключений до якого порту, він буде надсилати дані безпосередньо на правий одержувач пакета.

У даному дипломному проекті використовується топологія «Зірка». Вона обрана так як дозволяє легко підключати робочі станції до мережі, діагностувати та локалізувати несправності шляхом простого відключення абонентів від мережі. Недоліком топології є підвищена витрата кабелю, а але у даному випадку це несуттєво так як сумарна довжина кабелю невелика і не потребує суттєвих витрат.

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		35

2.2 Розробка загальної структури мережі

Для реалізації описаних функцій було вирішено створити проект типової мережі. При проектуванні мережі було вирішено розділити її на два можливі підрозділи та налаштувати відповідні можливості пристроїв. Слід відзначити, що данна мережа має досить легкі можливості моніторингу недоліків та можливих відхилень.

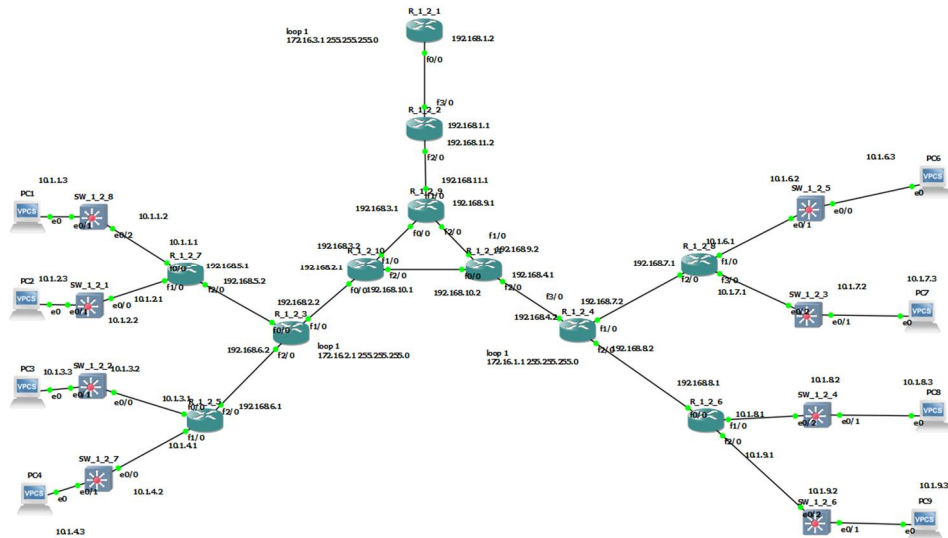


Рисунок 2.1 – Загальна топологія мережі

Розглянемо кожну підмережу. Підмережа А та В складається із двох комутаторів SW_1_2_8 SW_1_2_1 по 16 портів та по 12 ПК.

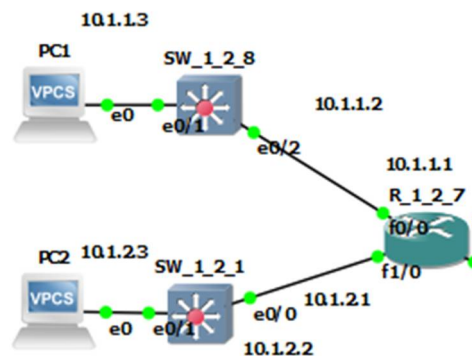


Рисунок 2.2 – Підмережа А, В

Підмережа С та D складаються із 2 комутаторів на 16 портів до кожного із яких підключено по 14 ПК.

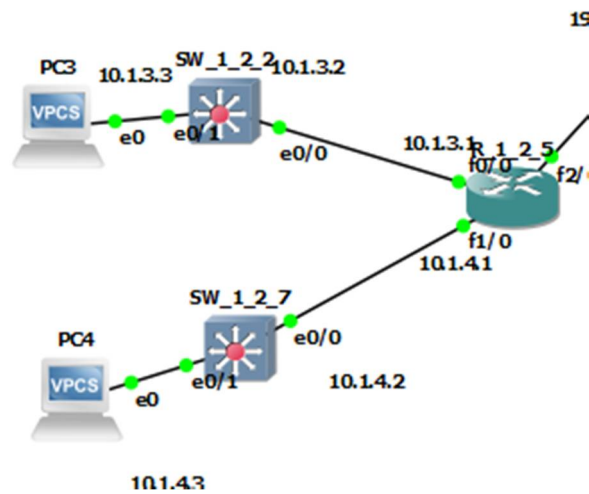


Рисунок 2.3 – Підмережа С та D

Підмережа Е складається із комутатора на 16 портів та 10 ПК.

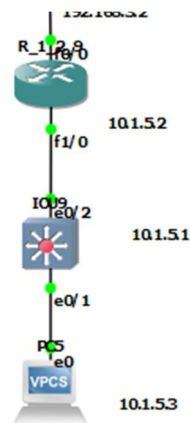


Рисунок 2.4 – Підмережа Е

Наступні підмережі F та G мають по комутатору (SW_1_2_5, SW_1_2_3) що підключені до маршрутизатора R_1_2_8. Кожна підмережа складається із 10 ПК.

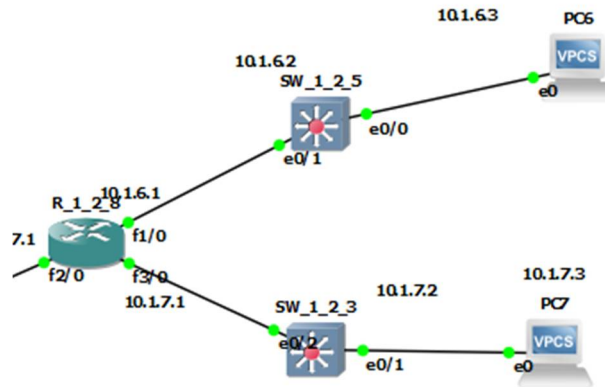


Рисунок 2.5 – Підмережа F,G

Наступні підмережі F та G мають по комутатору (SW_1_2_4, SW_1_2_6) що підключені до маршрутизатора R_1_2_6. Кожна підмережа складається із 10 ПК.

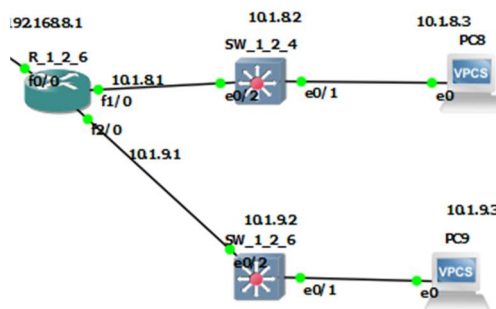


Рисунок 2.6 – Підмережа H, I

2.3 Структуровані кабельні системи та принципи їх вибору

В якості середовища передачі інформації в локальних мережах найчастіше використовуються: коаксіальний кабель, виті пари провідників і оптоволоконні середовища. Симплексний, напівдуплексний та повний дуплекс називаються діалоговими режимами, і вони визначають напрямок, в якому дані можуть протікати через мережеві носії: Симплексний режим дозволяє односторонню передачу даних через мережу, при цьому для передачі сигналу використовується повна пропускна здатність кабелю. Односторонній зв'язок мало корисний для локальних мереж, що робить його в кращому випадку незвичним для мережевих реалізацій.

Набагато більш поширеним є напівдуплексний режим, який забезпечує передачу та прийом у мережі, але не одночасно. Багато мереж налаштовано для напівдуплексного зв'язку. Переважним діалоговим режимом для мережевого зв'язку є повнодуплексний режим. Щоб використовувати повний дуплекс, як мережева карта, так і концентратор або комутатор повинні підтримувати повний дуплекс. Пристрої, налаштовані на повний дуплекс, можуть одночасно передавати та приймати. Це означає, що мережеві карти 100 Мбіт / с теоретично можуть передавати зі швидкістю 200 Мбіт / с, використовуючи повнодуплексний режим.

Кабелі з витою парою існують дуже давно. Спочатку він був створений для передачі голосу і широко використовувався для телефонної комунікації. Сьогодні, крім телефонного зв'язку, кручена пара є найбільш широко використовуваним середовищем для роботи в мережі. Популярність виті пари можна пояснити тим, що вона легша, гнучкіша і легша в монтажі, ніж коаксіальний або волоконно-оптичний кабель. Це також дешевше, ніж інші засоби масової інформації, і може досягти більшої швидкості, ніж його коаксіальна конкуренція. Ці фактори роблять виту пару ідеальним рішенням для більшості мережевих середовищ. Сьогодні використовуються два основних типи кабелів із витою парою: неекранована вита пара (UTP) та екранована вита пара (STP). UTP набагато частіше, ніж STP, і використовується для більшості мереж. Екранована вита пара використовується в середовищах, в яких необхідний більший опір ЕМІ та ослабленню. Однак більший

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		39

опір має свою ціну. Додатковий екран, а також необхідність заземлення цього екрану (для чого потрібні спеціальні з'єднувачі) можуть значно збільшити вартість кабельної установки STP.

Коаксіальний кабель, або коаксіальний, як його прийнято називати, існує довгий час. Він досяг успіху як у передачі телевізійного сигналу, так і в реалізації мережі. Коаксіальна конструкція виконана з мідним сердечником у центрі, який несе сигнал, пластиковою ізоляцією, плетеним металевим екраном та зовнішнім пластиковим покриттям. Коаксіальний кабель сконструйований таким чином, щоб додати опір загасанню (втрата сили сигналу, коли сигнал проходить через відстань), перехресні перешкоди (погіршення сигналу, спричинене сигналами від інших кабелів, що проходять поруч з ним). У мережі використовуються два типи коаксіальних коаксіальних коаксіальних конусів, також відомих як thinnet, і товстих коаксіальних коаксіальних коаксіальних каналів, також відомих як thicknet. І те, і інше вже не користується особливою популярністю, але найімовірніше ви зіткнетеся з тонкими коаксіальними. Товстий коаксіал використовувався головним чином для магістрального кабелю. Він міг проходити через простори пленуму, оскільки він забезпечував значний опір ЕМІ та перехресним перешкодам і міг пролягати довжиною до 500 метрів. Товстий коаксіальний пристрій забезпечує швидкість до 10 Мбіт / с, що занадто повільно для сучасних мережевих середовищ.

Багато в чому волоконно-оптичний носій усуває недоліки носіїв на основі міді. Оскільки волоконно-оптичні носії використовують світлопропускання замість електронних імпульсів, такі загрози, як ЕМІ, перехресні перешкоди та загасання, не стають питаннями. Волокно добре підходить для передачі даних, відео та передачі голосу. Крім того, оптоволоконний кабель є найбільш безпечним серед усіх кабельних носіїв. Той, хто намагається отримати доступ до сигналів даних по волоконно-оптичному кабелю, повинен фізично зачепити носій. Враховуючи склад кабелю, це є особливо складним завданням. На жаль, незважаючи на переваги волоконних носіїв перед мідними, вони все ще не користуються популярністю кабелів із крученою парою. Помірно складні процедури монтажу та об-

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		40

слуговування волокна часто вимагають кваліфікованих техніків зі спеціальними інструментами. Крім того, вартість рішення на основі волокон обмежує кількість організацій, які можуть дозволити його впровадити. Іншим часом прихованим недоліком впровадження волоконного рішення є вартість модернізації існуючого мережевого обладнання. Волокно несумісне з більшістю електронного мережевого обладнання. Це означає, що вам доведеться придбати мережеве обладнання, сумісне з волокном. 100BaseTX відомий як мережевий дизайн Fast Ethernet і є одним із трьох стандартів 802.3u. Як випливає з назви, 100BaseTX передає мережеві дані зі швидкістю до 100 Мбіт / с - швидкістю, на якій сьогодні працює більшість локальних мереж. 100BaseTX найчастіше реалізується за допомогою UTP-кабелю, але він може використовувати STP; тому він страждає від тих самих обмежень на відстань у 100 метрів, що й інші мережі на базі UTP. 100BaseTX використовує UTP-кабель категорії 5, і, як і 10BaseT, він використовує незалежні шляхи передачі та прийому, тому може підтримувати повнодуплексну роботу. Без сумніву, 100BaseTX є найпоширенішим стандартом Fast Ethernet. Через популярність даного стандарту, а також технічні можливості проектування було вирішено використати даний мережевий дизайн у запропонованій мережі для забезпечення зв'язку між її сегментами.

2.4 Опис логічного проектування мережі

Інтернет-протокол (IP) є одним з важливих протоколів у TCP / IP. Цей протокол визначає хости та маршрутизує дані між ними через Інтернет. Перше покоління IP, яке широко застосовується, - це IPv4. Уявляючи, що в наші дні мобільні телефони, настільні комп'ютери, андроїди та величезна кількість інших Інтернет-пристроїв підключені до Інтернету. Для комунікації між пристроями було вирішено використати дане покоління протоколу IP, адже IPv4 продемонстрував надійність, сумісність з широким спектром протоколів, програм та легку реалізацію.

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		41

Таблиця 2.1 – Опис мережевих з'єднань

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Маршрутизатор R_1_2_1	Fa0/0	Комутатор SW_1	Fa6/1
	Gig1/0	Маршрутизатор R_1_2_4	Gig3/0
Маршрутизатор R_1_2_2	Fa0/0	Комутатор SW_1	Fa7/1
	Gig1/0	Маршрутизатор R_1_2_4	Gig1/0
Маршрутизатор R_1_2_3	Fa0/0	Комутатор SW_1	Fa 8/1
	Se2/0	Маршрутизатор R_1_2_4	Se2/0
Маршрутизатор R_1_2_4	Gig3/0	Маршрутизатор R_1_2_1	Gig1/0
	Gig1/0	Маршрутизатор R_1_2_2	Gig1/0
	Se2/0	Маршрутизатор R_1_2_3	Se2/0
	Fa0/0	Комутатор SW_1	Eth2/1
Маршрутизатор R_1_2_4	Gig3/0	Маршрутизатор R_1_2_1	Gig1/0
	Gig1/0	Маршрутизатор R_1_2_2	Gig1/0
	Se2/0	Маршрутизатор R_1_2_3	Se2/0
	Fa0/0	Комутатор SW_1	Eth2/1
Маршрутизатор R_1_2_4	Gig3/0	Маршрутизатор R_1_2_1	Gig1/0
	Gig1/0	Маршрутизатор R_1_2_2	Gig1/0
	Se2/0	Маршрутизатор R_1_2_3	Se2/0
	Fa0/0	Комутатор SW_1	Eth2/1
	Se2/0	Маршрутизатор R_1_2_3	Se2/0
	Fa0/0	Комутатор SW_1	Eth2/1
Маршрутизатор R_1_2_4	Gig3/0	Маршрутизатор R_1_2_1	Gig1/0
	Gig1/0	Маршрутизатор R_1_2_2	Gig1/0
	Se2/0	Маршрутизатор R_1_2_3	Se2/0
	Fa0/0	Комутатор SW_1	Eth2/1
Маршрутизатор R_1_2_4	Gig3/0	Маршрутизатор R_1_2_1	Gig1/0
	Gig1/0	Маршрутизатор R_1_2_2	Gig1/0
	Se2/0	Маршрутизатор R_1_2_3	Se2/0
	Fa0/0	Комутатор SW_1	Eth2/1
Маршрутизатор R_1_2_4	Gig3/0	Маршрутизатор R_1_2_1	Gig1/0
	Gig1/0	Маршрутизатор R_1_2_2	Gig1/0

	Se2/0	Маршрутизатор R_1_2_3	Se2/0
	Fa0/0	Комутатор SW_1	Eth2/1
Маршрутизатор R_1_2_4	Gig3/0	Маршрутизатор R_1_2_1	Gig1/0
	Gig1/0	Маршрутизатор R_1_2_2	Gig1/0
	Se2/0	Маршрутизатор R_1_2_3	Se2/0
	Fa0/0	Комутатор SW_1	Eth2/1
Комутатор S_W_2	Eth2/1	Маршрутизатор R_1_2_4	Fa0/0
	Eth0/1	Робоча станція PC_6	Fa0
	Eth1/1	Робоча станція PC_7	Fa0
Робоча станція PC_0	Fa0	Комутатор SW_1_2_1	Fa 0/1
Робоча станція PC_1	Fa0	Комутатор SW_1_2_1	Fa1/1
Робоча станція PC_2	Fa0	Комутатор SW_1_2_1	Fa2/1
Робоча станція PC_3	Fa0	Комутатор SW_1_2_1	Eth0/1

Для мережі провайдера та між підключенням брандмауера та маршрутизаторами IP адреси були розподілені таким чином щоб забезпечити найлегшу можливість налаштування необхідних функцій.

R_1_2_1 – R_1_2_2 – 192.168.1.0 /30

R_1_2_7 – R_1_2_9 – 192.168.2.0 /30

R_1_2_9 – R_1_2_10 – 192.168.3.0 /30

R_1_2_10 – R_1_2_11 – 192.168.4.0 /30

R_1_2_10 – R_1_2_3 – 192.168.5.0 /30

R_1_2_3 – R_1_2_7 – 192.168.6.0 /30

R_1_2_3 – R_1_2_5 – 192.168.7.0 /30

R_1_2_11 – R_1_2_4 – 192.168.8.0 /30

R_1_2_4 – R_1_2_8 – 192.168.9.0 /30

R_1_2_4 – R_1_2_6 – 172.12.10.0 /30

Розрахунок IP адрес для підмереж наведені у наступній таблиці, а також у додатках.

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		43

Таблиця 2.2 – Адресація підмережі А

Призначення	IP-адреса
Адреса мережі	192.168.1.0
Маска мережі	255.255.255.0
Інвертована маска	0.0.0.255
Мінімальна адреса	192.168.1.1
Максимальна адреса	192.168.1.254
Широкомовна адреса	192.168.1.255
Шлюз по замовчуванню	192.168.1.1
Діапазон адрес комутаторів	192.168.1.2
Діапазон адрес майбутніх ПК	192.168.1.3-192.168.1.15
Діапазон вільних адрес	192.168.1.16 - 192.168.1.254

Висновок до другого розділу

В даному розділі було створено мережу з використанням GNS3. Було розподілено проект на під мережі, показано етапи логічного проектування, вибір кабельного обладнання , а також обґрунтовано вибір саме такої моделі створення мережі. За допомогою таблиць було надано опис мережевих з'єднань та розподіл IP адрес.

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		44

РОЗДІЛ 3. ВИБІР ТА НАЛАГОДЖЕННЯ ОБЛАДНАННЯ, ТЕСТУВАННЯ СТВОРЕНОЇ МЕРЕЖІ

3.1 Обґрунтування вибору обладнання

Існує багато компаній, що розвивають мережеву продукцію та створюють необхідне обладнання для мережевого доступу та взаємодії. Cisco Systems, технологічна компанія, що працює у всьому світі, і є найбільш відомою завдяки своїм комп'ютерним мережевим продуктам, була заснована в 1984 році та має головний офіс у Сан-Хосе, штат Каліфорнія. Cisco Systems, Inc. розробляє, виробляє та продає мережі, засновані на Інтернет-протоколах, та інші продукти, пов'язані з індустрією комунікацій та інформаційних технологій в Америці, Європі, Близькому Сході, Африці, Азіатсько-Тихоокеанському регіоні, Японії та Китаї. Він забезпечує інфраструктурні платформи, включаючи мережеві технології комутації, маршрутизації, бездротового зв'язку та продукти центрів обробки даних, які розроблені для спільної роботи з надання мережевих можливостей, транспортування та / або зберігання даних. Компанія також пропонує продукти для співпраці, що включають уніфіковані комунікації, Cisco TelePresence та конференції, а також Інтернет речей та програмне забезпечення для аналітики. Крім того, він надає продукти безпеки, такі як мережева безпека, безпека хмар та електронної пошти, управління ідентифікацією та доступом, вдосконалений захист від загроз та уніфіковані продукти управління загрозами; та продукти для хмарного та системного управління. Крім того, компанія пропонує широкий спектр послуг та варіантів підтримки для своїх клієнтів, включаючи технічну підтримку та розширені послуги. Він обслуговує підприємства різного розміру, державні установи, уряди та постачальників послуг. Компанія продає свою продукцію та послуги безпосередньо, а також через системні інтегратори, постачальників послуг, інших торгових посередників та дистриб'юторів. Cisco Systems, Inc. має стратегічні альянси з Internet2 для надання можливостей та програмних рішень наступного покоління; і Tele2 Iot на платформі управління підключеннями 2CONTROL. Через те, що обладнання Cisco забезпечує високо захищені зв'язки, машинне навчання та безпеку, керовані

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		45

ну хмарою, забезпечує сьгоднішні потреби та масштаби з високим рівнем рентабельності інвестицій, було вирішено використати обладнання саме цієї компанії для запропонованої мережі. Маршрутизатори інтегрованих служб серії Cisco 4000 забезпечують маршрутизацію, хостинг, безпеку, комутацію та видимість програм - і все це на єдиній надійній платформі.

Маршрутизатор Cisco ISR (Integrated Services Routers) 4000 серії включає в себе моделі Cisco ISR4300 і Cisco ISR4400 підсерії. Ці пристрої відрізняються високою продуктивністю від 50 Мбіт / с до 2 Гбіт / с, вбудованими WAN портами Gigabit Ethernet і SFP портами. Функціональність платформи Cisco ISR4300 і Cisco ISR4400 можна розширити за допомогою інтерфейсних модулів NIM. Платформа підтримує 2 або 3 слота розширення, в залежності від моделі. Обсяг пам'яті DRAM в 4GB з можливістю розширення до 16GB дозволяє справлятися із завданнями з високою швидкістю. Моделі Cisco ISR4400 підтримують функцію резервного живлення. Маршрутизатор Cisco ISR4300 і Cisco ISR4400 підтримують роботу протоколів NAT, IPSec VPN сервіси, RIP v1 / v2, EIGRP, OSPF, BGP, PBR, PfR, IPv4 і IPv6 адресацію. Маршрутизатор Cisco ISR4000 серії надають замовникам призначені для користувача послуги найвищої якості, високу масштабованість архітектури, захист інвестицій і мінімальні витрати на установку.

Для використання у проекті було вирішено взяти маршрутизатор Cisco ISR4431.



Рисунок 3.7 – Маршрутизатор Cisco ISR4431

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		46

Основні характеристики	
технологія доступу	Ethernet
Типи WAN-підключення	L2TP, PPPoE, PPTP, Динамічний IP, Статичний IP
Кількість LAN портів	3
Тип LAN портів	10/100 / 1000Base-TX
Кількість портів SFP	2 шт
Протоколи Ethernet	IEEE 802.3, IEEE 802.3ab, IEEE 802.3u
Апаратна складова	
Об'єм оперативної пам'яті	4096 МБ
Обсяг Flash пам'яті	4096 МБ
Web-інтерфейс	+
Брандмауер (Firewall)	+
VPN	+
Габарити	438.15 x 44.6 x 438.15 мм
Вага нетто	6.2 кг

Сімейство Catalyst 9200 Series забезпечує кращі в своєму класі функції, такі як високий рівень безпеки корпоративного рівня, відмовостійкість і простота ІТ-інфраструктури, що робить їх зручними. Комутатор Catalyst 9200L-24PXG-2Y є основоположним будівельним блоком для архітектури цифрової мережі Cisco, допомагає спростити складність, оптимізувати ІТ і скоротити експлуатаційні витрати за рахунок використання інтелектуальних засобів, автоматизації та людського досвіду, які жоден інший постачальник не може надати, незалежно від того, де ви знаходитесь. Безпека: Краще в своєму класі портфолію безпеки засноване на Talos, Trustworthy Solutions, шифруванні MACsec і сегментації. Отримайте розширені функції безпеки, які захищають цілісність вашого обладнання, програмного забезпечення і всіх даних, що проходять через комутатор. Стійкість: 9200L-24PXG-2Y забезпечує відмовостійкість на рівні підприємства за допомогою бло-

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		47

ків живлення і вентиляторів FRU, модульних каналів зв'язку, холодних виправлень і постійного PoE, що допомагає підтримувати безперебійну роботу вашого бізнесу. Простота IT: отримаєте простий веб-інтерфейс або ініціалізацію Cisco DNA Center в поєднанні з відкритими API-інтерфейсами Cisco IOS XE і можливість програмування технології UADP ASIC. Комутатор Catalyst 9200L-24PXG-2Y забезпечує просте управління вже зараз і захист інвестицій для майбутніх інновацій.



Рисунок 3.8 – Комутатор Cisco Catalyst 9200L

Основні характеристики	
Сукупні лінки 10/100/1000 або PoE + мідні порти	24 порти з повним PoE + (порти 8 мГіг до 10G, 16 портів до 1G)
Конфігурація висхідної лінії зв'язку	2x 25G фіксованих лінки
Основне джерело змінного струму за замовчуванням	PWR-C5-600WAC
Пропускна здатність	80 Гбіт / с
Обсяг DRAM пам'яті	2 ГБ
Обсяг Flash пам'яті	4 ГБ
Комутаційна потужність	292 Гбіт / с
Швидкість пересилання	229,16 Mpps

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		48

3.2 Налаштування технології маршрутизації та захисту пристроїв

Даний проект було виконано у середовищі GNS 3. GNS3 - це графічний симулятор мережі, який дозволяє емуляцію складної мережі. Можливо, ви знайомі з VMWare або Virtual PC які використовуються для емуляції різних операційних систем у віртуальному середовищі. Ці програми дозволяють запускати операційні системи такі як Windows XP Professional або Ubuntu Linux у віртуальному режимі середовища на вашому комп'ютері. GNS3 дозволяє використовувати той самий тип емуляцій за допомогою операційних систем Cisco Internetwork. Через можливість інтерпритації та налаштування необхідних функцій, а також показ налаштованого функціоналу, було обрано саме цей симулятор мережі.

Для початку налаштуємо інтерфейси, для подальшої можливості роботи з пристроєм. Для прикладу було показано налаштування на R_1_2_9.

```
R_1_2_9#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R_1_2_9(config)#int f 0/0
R_1_2_9(config-if)#ip address 192.168.3.1 255.255.255.0
R_1_2_9(config-if)#no sh
R_1_2_9(config-if)#ex
R_1_2_9(config)#
*Jun 16 20:37:00.683: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.1 on FastEthernet0/0 from LOADING to FULL, Loading Done
R_1_2_9(config)#int f 2/0
R_1_2_9(config-if)#ip address 192.168.9.1 255.255.255.0
R_1_2_9(config-if)#no sh
R_1_2_9(config-if)#ex
R_1_2_9(config)#ex
*Jun 16 20:37:33.195: %LINK-3-UPDOWN: Interface FastEthernet2/0, changed state to up
*Jun 16 20:37:34.195: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet2/0, changed state to up
R_1_2_9(config)#int f 1/0
R_1_2_9(config-if)#ip address 192.168.11.1 255.255.255.0
R_1_2_9(config-if)#no sh
R_1_2_9(config-if)#exit
```

Рисунок 3.9 – Налаштування інтерфейсів

Для забезпечення парольного доступу для різних видів підключень (ліній) та доступу у привілейований режим було використано наступні команди.

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		49

```

R_1_2_9(config)#enable password adminpass
R_1_2_9(config)#line console 0
R_1_2_9(config-line)#password mypass1
R_1_2_9(config-line)#login
R_1_2_9(config-line)#exit
R_1_2_9(config)#line aux 0
R_1_2_9(config-line)#password mypass2
R_1_2_9(config-line)#login
R_1_2_9(config-line)#exit
R_1_2_9(config)#line vty 0 15
R_1_2_9(config-line)#password mypass3
R_1_2_9(config-line)#login
R_1_2_9(config-line)#exit
R_1_2_9(config)#

```

```

R_1_2_9(config)#username adminer privilege 15 secret adminerpass
R_1_2_9(config)#username adminer privilege 1 secret technicpass

```

Рисунок 3.10 – Налаштування парольного доступу

Завдяки автентифікації та шифруванню клієнт SSH забезпечує захищений зв'язок через незахищену мережу.

```

R_1_2_9(config)#$generate rsa usage-keys label MySSH-keys modulus 1024
The name for the keys will be: MySSH-keys

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R_1_2_9(config)#
*Jun 17 22:53:09.399: %SSH-5-ENABLED: SSH 1.99 has been enabled
R_1_2_9(config)#ip ssh version 2
R_1_2_9(config)#ip ssh time-out 60
R_1_2_9(config)#ip ssh authentication-retries 5
                                     ^
% Invalid input detected at '^' marker.

R_1_2_9(config)#ip ssh authentication-retries 5
R_1_2_9(config)#ip
*Jun 17 22:54:07.043: %OSPF-4-FLOOD_WAR: Process 1 re-originates LSA ID 192.168.
3.1 type-2 adv-rtr 192.168.11.1 in area 0
R_1_2_9(config)#ip ssh maxstartups 5
R_1_2_9(config)#line vty 0 4
R_1_2_9(config-line)#login local
R_1_2_9(config-line)#transport input ssh
R_1_2_9(config-line)#transport output ssh
R_1_2_9(config-line)#exit
R_1_2_9(config)#exit
R_1_2_9#

```

Рисунок 3.11 – Налаштування клієнту SSH

На маршрутизаторах було налаштовано протокол CDP.

```

R_1_2_9(config)#cdp timer 30
R_1_2_9(config)#cdp holdtime 90
R_1_2_9(config)#cdp advertise-v2
R_1_2_9(config)#cdp run
R_1_2_9(config)#exit

```

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		50

```
Global CDP information:
  Sending CDP packets every 30 seconds
  Sending a holdtime value of 90 seconds
  Sending CDPv2 advertisements is enabled
```

Рисунок 3.12 – Налаштування таймерів CDP
на маршрутизаторах було налаштовано функцію Port Security.

```
SW_1_2_5(config)#int e 0/1
SW_1_2_5(config-if)#switchport mode access
SW_1_2_5(config-if)#switchport port-security maximum 3
SW_1_2_5(config-if)#switchport port-security violation restrict
SW_1_2_5(config-if)#switchport port-security aging type inactivity
SW_1_2_5(config-if)#switchport port-security aging time 60
SW_1_2_5(config-if)#exit

SW_1_2_5(config)#int e 0/0
SW_1_2_5(config-if)#switchport mode access
SW_1_2_5(config-if)#switchport port-security
SW_1_2_5(config-if)#switchport port-security mac-address 00:50:79:66:68:04
SW_1_2_5(config-if)#switchport port-security violation shutdown
^
% Invalid input detected at '^' marker.

SW_1_2_5(config-if)#switchport port-security violation shutdown
```

Рисунок 3.13 – Налаштування функції Port Security
Маршрутизацію забезпечить протокол OSPF

```
R_1_2_9(config)#router ospf 1
R_1_2_9(config-router)#network 192.168.11.0 0.0.0.255 area 0
R_1_2_9(config-router)#network 192.168..0 0.0.0.255 area 0
*Jun 16 20:38:28.435: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.11.2 on FastEtherne
t1/0 from LOADING to FULL, Loading Done
R_1_2_9(config-router)#network 192.168.9.0 0.0.0.255 area 0
R_1_2_9(config-router)#network 192.168.3.0 0.0.0.255 area 0
```

Рисунок 3.14 – Налаштування протоколу маршрутизації

3.3 Налаштування технології захищених з'єднань Get Vpn

Звичним чином налаштовуємо crypto isakmp policy. Для шифрування будемо ви-
користовувати AES 256.

```
R_1_2_1(config)#crypto isakmp policy 10
R_1_2_1(config-isakmp)#encryption aes 256
^
% Invalid input detected at '^' marker.

R_1_2_1(config-isakmp)#encryption aes 256
R_1_2_1(config-isakmp)#authentication pre-share
R_1_2_1(config-isakmp)#group 2
R_1_2_1(config-isakmp)#exit
R_1_2_1(config)#crypto isakmp key VPN address 192.168.2.2
R_1_2_1(config)#crypto isakmp key VPN address 192.168.4.2
```

Рисунок 3.15 – Налаштування crypto isakmp policy

		Висоцький В.П.				Арк.
						51
Змн.	Арк.	№ докум.	Підпис	Дата		

Визначаємо, що шифрувати

```
R_1_2_1(config)#crypto ipsec transform-set tset esp-aes esp-md5-hmac
R_1_2_1(cfg-crypto-trans)#exit
R_1_2_1(config)#crypto ipsec profile GET-PROF
R_1_2_1(ipsec-profile)#set transform-set tset
R_1_2_1(ipsec-profile)#set security-association lifetime seconds 3600
R_1_2_1(ipsec-profile)#exit
```

Рисунок 3.16 – Налаштування типу шифрування

Створюємо gdoi - групу. Далі, задаємо ідентифікатор групи. Повинен бути однаковий у всіх. Налаштовуємо аутентифікацію. Далі задаємо, яким способом оновлювати ключі, unicast або multicast. Оскільки в GET VPN-решт тунелів безліч, то і таких записів вийде дуже багато. Тому Cisco рекомендує максимально сумаризувати ACE. Наприклад в нашому випадку найкраще записати Тут все значно простіше, фактично нам потрібно вказати, якої групи ми належимо (за допомогою identity number) і KS цієї групи.

```
R_1_2_1(config)#access-list 150 permit ip 172.16.0.0 0.0.255.255 172.16.0.0 0.0.0.0
```

```
R_1_2_1(config)#crypto gdoi group GET-GROUP
R_1_2_1(config-gdoi-group)#identity number 100
R_1_2_1(config-gdoi-group)#server local
R_1_2_1(gdoi-local-server)#sa
*Jun 17 17:03:07.219: %CRYPTO-6-GDOI_ON_OFF: GDOI is ON
R_1_2_1(gdoi-local-server)#sa ipsec 1
R_1_2_1(gdoi-sa-ipsec)#profile GET-PROF
R_1_2_1(gdoi-sa-ipsec)#match address ipv4 150
R_1_2_1(gdoi-sa-ipsec)#exit
R_1_2_1(gdoi-local-server)#address ipv4 172.16.3.1
R_1_2_1(gdoi-local-server)#exit
```

Рисунок 3.17 – Налаштування gdoi – групи та ACL

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		52

```

R_1_2_3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R_1_2_3(config)#crypto isakmp policy 10
R_1_2_3(config-isakmp)# encr aes 256
R_1_2_3(config-isakmp)# authentication pre-share
R_1_2_3(config-isakmp)# group 2
R_1_2_3(config-isakmp)#crypto isakmp key VPN address 172.16.3.1
R_1_2_3(config)#
R_1_2_3(config)#crypto gdoi group GET-GROUP
R_1_2_3(config-gdoi-group)# identity number 100
R_1_2_3(config-gdoi-group)# server address ipv4 172.16.3.1
R_1_2_3(config-gdoi-group)#exit
R_1_2_3(config)#crypto map cmap 10 gdoi
% NOTE: This new crypto map will remain disabled until a valid
        group has been configured.
R_1_2_3(config-crypto-map)#set group GET-GROUP
R_1_2_3(config-crypto-map)#exit
R_1_2_3(config)#int f 1/0
R_1_2_3(config-if)#crypto map cmap
R_1_2_3(config-if)#
*Jun 17 17:05:06.011: %CRYPTO-5-GM_REGSTER: Start registration to KS 172.16.3.1
for group GET-GROUP using address 192.168.2.2
R_1_2_3(config-if)#
*Jun 17 17:05:06.043: %CRYPTO-6-GDOI_ON_OFF: GDOI is ON
R_1_2_3(config-if)#
*Jun 17 17:05:06.783: %GDOI-5-GM_REGS_COMPL: Registration to KS 172.16.3.1 compl
ete for group GET-GROUP using address 192.168.2.2

```

Рисунок 3.18 – Налаштування клієнта Get Vpn

3.4 Перевірка працездатності та тестування налаштованих функцій

Почнемо перевірку налаштованих функцій. Спочатку перевіримо парольний доступ для різних видів підключень (ліній) та доступу у привілейований режим.

```

line con 0
  exec-timeout 0 0
  privilege level 15
  password mypass1
  logging synchronous
  login
  stopbits 1
line aux 0
  exec-timeout 0 0
  privilege level 15
  password mypass2
  logging synchronous
  login
  stopbits 1
line vty 0 4
  password mypass3
  login
line vty 5 15
  password mypass3
  login

```

Рисунок 3.19 – Тестування парольного доступу

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		53

Перевіримо налаштування SSH та можливість віддаленого підключення до пристроїв.

```
R_1_2_3#
R_1_2_3#ssh -l adminer 192.168.3.1

Password:

Password:

R_1_2_9#
```

Рисунок 3.20 – Тестування протоколу SSH

Введемо команди для перевірки налаштувань протоколу CDP

```
R_1_2_9#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID         Local Intrfce   Holdtme    Capability   Platform   Port ID
R_1_2_11          Fas 2/0        147        R            7206VXR    Fas 1/0
R_1_2_10          Fas 0/0        145        R            7206VXR    Fas 1/0
R_1_2_2           Fas 1/0        136        R            7206VXR    Fas 2/0

R_1_2_9# show cdp traffic
CDP counters :
  Total packets output: 1377, Input: 688
  Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
  No memory: 0, Invalid packet: 0, Fragmented: 0
  CDP version 1 advertisements output: 0, Input: 0
  CDP version 2 advertisements output: 1377, Input: 688
```

Рисунок 3.21 – Тестування налаштувань протоколу CDP

Налаштовані функції захисту маршрутизаторів буде показано на наступних рисунках.

```
SW_1_2_5#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
              (Count)          (Count)          (Count)
-----
Et0/0        1                1                0                Shutdown
Et0/1        3                1                0                Restrict
-----
Total Addresses in System (excluding one mac per port)  : 0
Max Addresses limit in System (excluding one mac per port) : 4096
```

```
SW_1_2_5#show port-security int e 0/0
Port Security          : Enabled
Port Status            : Secure-up
Violation Mode         : Shutdown
Aging Time             : 0 mins
Aging Type             : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses  : 1
Total MAC Addresses    : 1
Configured MAC Addresses : 1
Sticky MAC Addresses   : 0
Last Source Address:Vlan : 0050.7966.6804:1
Security Violation Count : 0
```

Рисунок 3.22 – Тестування налаштувань Port Security

Останніс кроком перевірки працездатності мережі буде перевірка основної функції Get-Vpn.

```
R_1_2_1#show run | sec crypto
crypto isakmp policy 10
  encr aes 256
  authentication pre-share
  group 2
crypto isakmp key VPN address 192.168.2.2
crypto isakmp key VPN address 192.168.4.2
crypto ipsec transform-set tset esp-aes esp-md5-hmac
crypto ipsec profile GET-PROF
  set transform-set tset
crypto gdoi group GET-GROUP
  identity number 100
  server local
  rekey retransmit 10 number 2
  sa ipsec 1
  profile GET-PROF
  match address ipv4 150
  replay counter window-size 64
  address ipv4 172.16.3.1
```

Рисунок 3.23 – Перевірка налаштувань KS сервера

```
R_1_2_3#show run | sec crypto
crypto isakmp policy 10
  encr aes 256
  authentication pre-share
  group 2
crypto isakmp key VPN address 172.16.3.1
crypto gdoi group GET-GROUP
  identity number 100
  server address ipv4 172.16.3.1
crypto map cmap 10 gdoi
  set group GET-GROUP
crypto map cmap
```

Рисунок 3.24 – Перевірка налаштувань клієнта

		Висоцький В.П.				Арк.
						55
Змн.	Арк.	№ докум.	Підпис	Дата		

```

R_1_2_4#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id status
172.16.3.1   192.168.4.2   GDOI_IDLE     1001 ACTIVE
IPv6 Crypto ISAKMP SA

```

Рисунок 3.25 – Перевірка тунелю

```

R_1_2_3#ping 172.16.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/39/76 ms

```

Рисунок 3.26 – Перевірка зв'язку

```

R_1_2_3#trace 172.16.1.1 source 172.16.2.1
Type escape sequence to abort.
Tracing the route to 172.16.1.1

 0 172.16.2.1 72 msec 60 msec 60 msec
R_1_2_3#

```

Рисунок 3.27 – Перевірка передачі трафіку по каналу

```

R_1_2_3#show crypto ipsec sa
interface: FastEthernet1/0
  Crypto map tag: cmap, local addr 192.168.2.2

protected vrf: (none)
local ident (addr/mask/prot/port): (172.16.0.0/255.255.0.0/0/0)
remote ident (addr/mask/prot/port): (172.16.0.0/255.255.0.0/0/0)
current_peer 0.0.0.0 port 848
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
  #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

local crypto endpt.: 192.168.2.2, remote crypto endpt.: 0.0.0.0
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet1/0
current outbound spi: 0x63A31697(1671632535)
PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0x63A31697(1671632535)
    transform: esp-aes esp-md5-hmac ,
    in use settings = {Tunnel, }
    conn id: 1, flow_id: SW:1, sibling_flags 80000040, crypto map: cmap
    sa timing: remaining key lifetime (sec): (3473)
    IV size: 16 bytes

```

Рисунок 3.28 – Перевірка крипто-перетворення при передачі трафіку

		Висоцький В.П.				Арк.
						56
Змн.	Арк.	№ докум.	Підпис	Дата		

Висновок до третього розділу

В даному розділі було налаштовано основні функції мережі, функції захисту пристроїв та захищеного між мережного зв'язку з використанням технології Get Vpn. За допомогою функцій моніторингу було перевірено налаштовані можливості, а такої протестовано зв'язок та захист з'єднань. Також було надано опис мережевого обладнання та принципи його вибору.

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		57

ВИСНОВКИ

Була створена система кіберзахисту в режимі реального часу. За останні 10 років кібернетичні атаки досить помітно розвинулися і змінили свій типовий вигляд та алгоритм проведення. Завдяки розповсюдженій практиці використання базових видів захисту, як антивірус та фаєрвол, інформаційні системи стали менш-вразливими до типових атак, таких як: атака з допомогою вірусів, DDOS-атаки, ARP-спуфінг і так далі. Тож при побудові сучасної мережі використано різноманітні засоби захисту, а також тунелювання. Для розуміння місця технологій Get Vpn в мережі, було зображено структурну схему типової організації. В результаті данної роботи було створено повністю розроблений і налаштований проєкт мережі.

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		58

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. IPsec and IKE Administration Guide [Електронний ресурс], - Режим доступу: <https://docs.oracle.com/cd/E19683-01/816-7264/index.html>
2. Haseeb Niazi, Nipul Shah, Biao Zhou, Varun Sethi Shashi Shastry, Rudresh Veerapaji - Group Encrypted Transport VPN (GETVPN) Design and Implementation Guide , 2019p - 317стр.
3. Network Security Baseline – [Електронний ресурс], - Режим доступу: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/Baseline_Security/securebasebook.pdf
4. International Journal of Scientific Research and Review . R. Sri Devi, Dr. M. Mohankumar - AN EMPIRICAL STUDY ON CYBER SECURITY THREATS AND ATTACKS , 2005p - 214стр.
5. Ahmed A. Jaha, Fathi Ben Shatwan, and Majdi Ashibani - Proper Virtual Private Network (VPN) Solution :Createspace Independent Pub, 2008 p. - 92 стор.
6. Charlie Scott, Paul Wolfe and Mike Erwin, - Virtual Private Networks Second Edition , 1999 p.
7. Fatemeh Soleimani Roozbahani - Security Solutions against Computer Networks Threats:Pearson Education, 2009 p. - 1152 стор.
8. Luís Henrique M. K. Costa, Otto Carlos M. B. - An Introduction to Virtual Private Networks:Towards D-VPNs, 2015p - 712стр.
9. An Introduction to Computer Networks [Електронний ресурс], - Режим доступу: <http://intronetworks.cs.luc.edu/current/ComputerNetworks.pdf>
10. Fundamental Principles of Network Security [Електронний ресурс], - Режим доступу: <http://www.people.vcu.edu/~gasaunde/NetworkSecurityWhitepaper.pdf>
11. Network Security: History, Importance, and Future [Електронний ресурс], - Режим доступу: <http://www.aimt.edu.in/wp-content/uploads/2016/12/Network-Security.pdf>
12. Introduction to Management Information Systems [Електронний ресурс], - Режим доступу:

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		59

<http://www.repositori.uji.es/xmlui/bitstream/handle/10234/46625/s63.pdf?sequence=1&isAllowed=y>

13. David Barnet, David Groth, Jim McBee - Cabling: The Complete Guide to Network Wiring, Third Edition. San Francisco, M.:Cisco Press,2012 p. - 368 стор.
14. Cabling, Connectors, andEthernet Standards [Електронний ресурс], - Режим доступу : https://access.itxlearning.com/data/cmdata/NETPLUSN10004/Books/ec2_netplus004c02.pdf
15. NETWORK SECURITY [Електронний ресурс], - Режим доступу : https://www.theseus.fi/bitstream/handle/10024/47351/Sulaimon_Adeniji.pdf?sequence=1
16. Configuring Cisco Discovery Protocol [Електронний ресурс], - Режим доступу: https://www.cisco.com/c/en/us/td/docs/wireless/mwr_2941_dc/software_config/guide/3_3/2941_33_Config_Guide/cdp.pdf
17. Configuring Port Security [Електронний ресурс], - Режим доступу: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/port_sec.pdf
18. Quick Comparison: IPSEC vs DMVPN vs EasyVPN vs GETVPN[Електронний ресурс], - Режим доступу: <https://www.routexp.com/2017/08/quick-comparison-ipsec-vs-dmvpn-vs.html>
19. Richard Deal- The Complete Cisco VPN Configuration Guide/ Richard Deal– M.: Cisco Press, 2005 - 1032стр.
20. Sheila Frankel - Guide to Ssl Vpns/ Sheila Frankel, Paul Hoffman, Angela Orebaugh- M.:Createspace Independent Pub, 2008 p. - 92 стор.

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		60

Додатки

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		61

Таблиця 2.2 – Адресація під мережі В

Призначення	IP-адреса
Адреса мережі	192.168.2.0
Маска мережі	255.255.255.0
Інвертована маска	0.0.0.255
Мінімальна адреса	192.168.2.1
Максимальна адреса	192.168.2.254
Широкомовна адреса	192.168.2.255
Шлюз по замовчуванню	192.168.2.1
Діапазон адрес комутаторів	192.168.2.2
Діапазон адрес майбутніх ПК	192.168.2.3-192.168.2.15
Діапазон вільних адрес	192.168.2.16 - 192.168.2.254

Таблиця 2.4 – Адресація під мережі D

Призначення	IP-адреса
Адреса мережі	192.168.4.0
Маска мережі	255.255.255.0
Інвертована маска	0.0.0.255
Мінімальна адреса	192.168.4.1
Максимальна адреса	192.168.4.254
Широкомовна адреса	192.168.4.255
Шлюз по замовчуванню	192.168.4.1
Діапазон адрес комутаторів	192.168.4.2
Діапазон адрес майбутніх ПК	192.168.4.3-192.168.4.15
Діапазон вільних адрес	192.168.4.16 - 192.168.4.254

Таблиця 2.3 – Адресація підмережі С

Призначення	ІР-адреса
Адреса мережі	192.168.3.0
Маска мережі	255.255.255.0
Інвертована маска	0.0.0.255
Мінімальна адреса	192.168.3.1
Максимальна адреса	192.168.3.254
Широкомовна адреса	192.168.3.255
Шлюз по замовчуванню	192.168.3.1
Діапазон адрес комутаторів	192.168.3.2
Діапазон адрес майбутніх ПК	192.168.3.3-192.168.3.15
Діапазон вільних адрес	192.168.3.16 - 192.168.3.254

Таблиця 2.5 – Адресація підмережі Е

Призначення	ІР-адреса
Адреса мережі	192.168.5.0
Маска мережі	255.255.255.0
Інвертована маска	0.0.0.255
Мінімальна адреса	192.168.5.1
Максимальна адреса	192.168.5.254
Широкомовна адреса	192.168.5.255
Шлюз по замовчуванню	192.168.5.1
Діапазон адрес комутаторів	192.168.5.2
Діапазон адрес майбутніх ПК	192.168.5.3-192.168.5.15
Діапазон вільних адрес	192.168.5.16 - 192.168.5.254

Таблиця 2.6 – Адресація підмережі F

Призначення	IP-адреса
Адреса мережі	192.168.6.0
Маска мережі	255.255.255.0
Інвертована маска	0.0.0.255
Мінімальна адреса	192.168.6.1
Максимальна адреса	192.168.6.254
Широкомовна адреса	192.168.6.255
Шлюз по замовчуванню	192.168.6.1
Діапазон адрес комутаторів	192.168.6.2
Діапазон адрес майбутніх ПК	192.168.6.3-192.168.6.15
Діапазон вільних адрес	192.168.6.16 - 192.168.6.254

Таблиця 2.7 – Адресація підмережі G

Призначення	IP-адреса
Адреса мережі	192.168.7.0
Маска мережі	255.255.255.0
Інвертована маска	0.0.0.255
Мінімальна адреса	192.168.7.1
Максимальна адреса	192.168.7.254
Широкомовна адреса	192.168.7.255
Шлюз по замовчуванню	192.168.7.1
Діапазон адрес комутаторів	192.168.7.2
Діапазон адрес майбутніх ПК	192.168.7.3-192.168.7.15
Діапазон вільних адрес	192.168.7.16 - 192.168.7.254

Конфігураційні файли пристроїв мережі

R_1_2_1#show run

Building configuration...

Current configuration : 1742 bytes

!

upgrade fpd auto

version 12.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname R_1_2_1

!

boot-start-marker

boot-end-marker

!

logging message-counter syslog

!

no aaa new-model

ip source-route

no ip icmp rate-limit unreachable

ip cef

!

!

!

!

no ip domain lookup

no ipv6 cef

!

multilink bundle-name authenticated

!

!

!

archive

log config

hidekeys

!

!

crypto isakmp policy 10

encr aes 256

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		65

```

authentication pre-share
group 2
crypto isakmp key VPN address 192.168.2.2
crypto isakmp key VPN address 192.168.4.2
!
!
crypto ipsec transform-set tset esp-aes esp-md5-hmac
!
crypto ipsec profile GET-PROF
set transform-set tset
!
crypto gdoi group GET-GROUP
identity number 100
server local
rekey retransmit 10 number 2
sa ipsec 1
profile GET-PROF
match address ipv4 150
replay counter window-size 64
address ipv4 172.16.3.1
!
!
!
ip tcp synwait-time 5
!
!
!
!
interface Loopback1
ip address 172.16.3.1 255.255.255.0
ip ospf 1 area 0
!
interface Loopback3
no ip address
!
interface FastEthernet0/0
ip address 192.168.1.2 255.255.255.0
duplex half
!
router ospf 1
log-adjacency-changes
network 172.16.1.0 0.0.0.255 area 0

```

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		66

```

network 172.16.2.0 0.0.0.255 area 0
network 192.168.1.0 0.0.0.255 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
access-list 150 permit ip 172.16.0.0 0.0.255.255 172.16.0.0 0.0.255.255
no cdp log mismatch duplex
!
!
control-plane
!
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
!
End
hostname R_1_2_2
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!

```

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		67

```

no aaa new-model
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
archive
log config
  hidekeys
!
!
ip tcp synwait-time 5
!
!
interface FastEthernet0/0
ip address 192.168.2.1 255.255.255.0
duplex half
!
interface FastEthernet1/0
ip address 192.168.3.1 255.255.255.0
duplex half
!
interface FastEthernet2/0
ip address 192.168.11.2 255.255.255.0
duplex half
!
interface FastEthernet3/0
ip address 192.168.1.1 255.255.255.0
duplex half
!
router ospf 1
  log-adjacency-changes

```

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		68

```

network 192.168.1.0 0.0.0.255 area 0
network 192.168.2.0 0.0.0.255 area 0
network 192.168.3.0 0.0.0.255 area 0
network 192.168.4.0 0.0.0.255 area 0
network 192.168.11.0 0.0.0.255 area 0

```

!

```
ip forward-protocol nd
```

```
no ip http server
```

```
no ip http secure-server
```

!

!

!

```
no cdp log mismatch duplex
```

!

!

!

!

!

!

```
control-plane
```

!

!

!

!

!

!

!

```
gatekeeper
```

```
shutdown
```

!

!

```
line con 0
```

```
exec-timeout 0 0
```

```
privilege level 15
```

```
logging synchronous
```

```
stopbits 1
```

```
line aux 0
```

```
exec-timeout 0 0
```

```
privilege level 15
```

```
logging synchronous
```

```
stopbits 1
```

```
line vty 0 4
```

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		69

```

login
!
End

hostname R_1_2_9
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
enable password adminpass
!
no aaa new-model
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
archive
log config
hidekeys
!
!
ip tcp synwait-time 5
!
!
interface FastEthernet0/0
ip address 192.168.3.1 255.255.255.0
duplex half
!
interface FastEthernet1/0
ip address 192.168.11.1 255.255.255.0
duplex half

```

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		70

```

!
interface FastEthernet2/0
 ip address 192.168.9.1 255.255.255.0
 duplex half
!
interface FastEthernet3/0
 no ip address
 shutdown
 duplex half
!
interface FastEthernet4/0
 no ip address
 shutdown
 duplex half
!
router ospf 1
 log-adjacency-changes
 network 10.1.5.0 0.0.0.255 area 0
 network 192.168.3.0 0.0.0.255 area 0
 network 192.168.9.0 0.0.0.255 area 0
 network 192.168.11.0 0.0.0.255 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
no cdp log mismatch duplex
 cdp timer 30
 cdp holdtime 90
!
!
control-plane
!
!
gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 0 0

```

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		71

```

privilege level 15
password mypass1
logging synchronous
login
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
password mypass2
logging synchronous
login
stopbits 1
line vty 0 4
password mypass3
login
line vty 5 15
password mypass3
login
!
End

```

```

hostname R_1_2_10
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!
no aaa new-model
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!

```

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		72

```

!
archive
log config
hidekeys
!
!
!
!
!
ip tcp synwait-time 5
!
!
!
!
interface FastEthernet0/0
ip address 192.168.2.1 255.255.255.0
duplex half
!
interface FastEthernet1/0
ip address 192.168.3.2 255.255.255.0
duplex half
!
interface FastEthernet2/0
ip address 192.168.10.1 255.255.255.0
duplex half
!
interface FastEthernet3/0
no ip address
shutdown
duplex half
!
interface FastEthernet4/0
no ip address
shutdown
duplex half
!
router ospf 1
log-adjacency-changes
network 192.168.2.0 0.0.0.255 area 0
network 192.168.3.0 0.0.0.255 area 0
network 192.168.10.0 0.0.0.255 area 0
!

```

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		73

```

ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
no cdp log mismatch duplex
!
!
!
!
!
!
!
control-plane
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
!
End

hostname R_1_2_11
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!

```

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		74

```

no aaa new-model
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
!
archive
log config
hidekeys
!
!
!
!
!
ip tcp synwait-time 5
!
!
!
!
interface FastEthernet0/0
ip address 192.168.10.2 255.255.255.0
duplex half
!
interface FastEthernet1/0
ip address 192.168.9.2 255.255.255.0
duplex half
!
interface FastEthernet2/0
ip address 192.168.4.1 255.255.255.0
duplex half
!
interface FastEthernet3/0
no ip address
shutdown

```

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		75

```

duplex half
!
router ospf 1
log-adjacency-changes
network 192.168.4.0 0.0.0.255 area 0
network 192.168.9.0 0.0.0.255 area 0
network 192.168.10.0 0.0.0.255 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
no cdp log mismatch duplex
!
!
control-plane
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
!
End

hostname R_1_2_3
!
boot-start-marker

```

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		76

```

boot-end-marker
!
logging message-counter syslog
!
no aaa new-model
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
!
archive
log config
hidekeys
!
!
crypto isakmp policy 10
encr aes 256
authentication pre-share
group 2
crypto isakmp key VPN address 172.16.3.1
!
!
crypto gdoi group GET-GROUP
identity number 100
server address ipv4 172.16.3.1
!
!
crypto map cmap 10 gdoi
set group GET-GROUP
!
!
!
ip tcp synwait-time 5
!

```

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		77

```

!
!
!
interface Loopback1
 ip address 172.16.2.1 255.255.255.0
 ip ospf 1 area 0
!
interface FastEthernet0/0
 ip address 192.168.5.2 255.255.255.0
 duplex half
!
interface FastEthernet1/0
 ip address 192.168.2.2 255.255.255.0
 duplex half
 crypto map cmap
!
interface FastEthernet2/0
 ip address 192.168.6.2 255.255.255.0
 duplex half
!
interface FastEthernet3/0
 no ip address
 shutdown
 duplex half
!
router ospf 1
 log-adjacency-changes
 network 172.16.1.0 0.0.0.255 area 0
 network 172.16.3.0 0.0.0.255 area 0
 network 192.168.2.0 0.0.0.255 area 0
 network 192.168.5.0 0.0.0.255 area 0
 network 192.168.6.0 0.0.0.255 area 0
!
 ip forward-protocol nd
 ip route 172.16.2.0 255.255.255.0 172.16.3.1
 no ip http server
 no ip http secure-server
!
!
!
 no cdp log mismatch duplex
!

```

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		78

```

!
!
!
!
!
control-plane
!
!
!
!
!
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
!
End

hostname R_1_2_4
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!
no aaa new-model
ip source-route

```

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		79

```

no ip icmp rate-limit unreachable
ip cef
!
!
!
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
!
archive
log config
  hidekeys
!
!
crypto isakmp policy 10
  encr aes 256
  authentication pre-share
  group 2
crypto isakmp key VPN address 172.16.3.1
!
!
crypto gdoi group GET-GROUP
  identity number 100
  server address ipv4 172.16.3.1
!
!
crypto map cmap 10 gdoi
  set group GET-GROUP
!
!
!
ip tcp synwait-time 5
!
!
!
!
interface Loopback1
  ip address 172.16.1.1 255.255.255.0
  ip ospf 1 area 0

```

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		80

```

!
interface FastEthernet0/0
  no ip address
  duplex half
!
interface FastEthernet1/0
  ip address 192.168.7.2 255.255.255.0
  duplex half
!
interface FastEthernet2/0
  ip address 192.168.8.2 255.255.255.0
  duplex half
!
interface FastEthernet3/0
  ip address 192.168.4.2 255.255.255.0
  duplex half
  crypto map cmap
!
router ospf 1
  log-adjacency-changes
  network 172.16.2.0 0.0.0.255 area 0
  network 172.16.3.0 0.0.0.255 area 0
  network 192.168.4.0 0.0.0.255 area 0
  network 192.168.7.0 0.0.0.255 area 0
  network 192.168.8.0 0.0.0.255 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
no cdp log mismatch duplex
!
!
!
!
!
!
!
control-plane
!
!

```

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		81

```

!
!
!
!
!
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
login
!
End

hostname R_1_2_7
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!
no aaa new-model
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
no ip domain lookup
no ipv6 cef
!

```

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		82

```

multilink bundle-name authenticated
!
!
archive
log config
hidekeys
!
!
crypto isakmp policy 100
encr aes
authentication pre-share
group 5
lifetime 3600
crypto isakmp key cisco address 192.168.1.2
!
!
crypto gdoi group GDOI
identity number 1234
server address ipv4 192.168.1.2
!
!
crypto map CRYPTO 10 gdoi
set group GDOI
!
!
!
ip tcp synwait-time 5
!
!
!
!
interface FastEthernet0/0
ip address 10.1.1.1 255.255.255.0
duplex half
!
interface FastEthernet1/0
ip address 10.1.2.1 255.255.255.0
duplex half
!
interface FastEthernet2/0
ip address 192.168.5.1 255.255.255.0
duplex half

```

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		83

```

crypto map CRYPTO
!
interface FastEthernet3/0
no ip address
shutdown
duplex half
!
router ospf 11
log-adjacency-changes
!
router ospf 1
log-adjacency-changes
network 10.1.1.0 0.0.0.255 area 0
network 10.1.2.0 0.0.0.255 area 0
network 192.168.5.0 0.0.0.255 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
no cdp log mismatch duplex
!
!
!
!
!
!
!
control-plane
!
!
!
!
!
!
!
gatekeeper
shutdown
!
!
line con 0

```

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		84

```

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
login
!
End

hostname R_1_2_5
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!
no aaa new-model
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!

```

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		85

```

!
archive
log config
hidekeys
!
!
!
!
!
ip tcp synwait-time 5
!
!
!
!
interface FastEthernet0/0
ip address 10.1.3.1 255.255.255.0
duplex half
!
interface FastEthernet1/0
ip address 10.1.4.1 255.255.255.0
duplex half
!
interface FastEthernet2/0
ip address 192.168.6.1 255.255.255.0
duplex half
!
interface FastEthernet3/0
no ip address
shutdown
duplex half
!
router ospf 1
log-adjacency-changes
network 10.1.3.0 0.0.0.255 area 0
network 10.1.4.0 0.0.0.255 area 0
network 192.168.6.0 0.0.0.255 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!

```

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		86

```

!
no cdp log mismatch duplex
!
!
!
!
!
!
control-plane
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
!
End

hostname R_1_2_8
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!
no aaa new-model
ip source-route
no ip icmp rate-limit unreachable
ip cef
!

```

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		87

```

!
!
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
archive
log config
hidekeys
!
!
ip tcp synwait-time 5
!
!
!
!
interface FastEthernet0/0
no ip address
shutdown
duplex half
!
interface FastEthernet1/0
ip address 10.1.6.1 255.255.255.0
duplex half
!
interface FastEthernet2/0
ip address 192.168.7.1 255.255.255.0
duplex half
!
interface FastEthernet3/0
ip address 10.1.7.1 255.255.255.0
duplex half
!
router ospf 1
log-adjacency-changes
network 10.1.6.0 0.0.0.255 area 0
network 10.1.7.0 0.0.0.255 area 0
network 192.168.7.0 0.0.0.255 area 0

```

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		88

```

!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
no cdp log mismatch duplex
!
!
control-plane
!
!
!
!
!
!
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
!
End

hostname R_1_2_6
!
boot-start-marker
boot-end-marker
!

```

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		89

```

logging message-counter syslog
!
no aaa new-model
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
archive
log config
  hidekeys
!
!
ip tcp synwait-time 5
!
!
!
!
interface FastEthernet0/0
ip address 192.168.8.1 255.255.255.0
duplex half
!
interface FastEthernet1/0
ip address 10.1.8.1 255.255.255.0
duplex half
!
interface FastEthernet2/0
ip address 10.1.9.1 255.255.255.0
duplex half
!
interface FastEthernet3/0
no ip address
shutdown

```

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		90

```

duplex half
!
router ospf 1
log-adjacency-changes
network 10.1.8.0 0.0.0.255 area 0
network 10.1.9.0 0.0.0.255 area 0
network 192.168.8.0 0.0.0.255 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
no cdp log mismatch duplex
!
!
control-plane
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
!
end

```

		Висоцький В.П.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		91