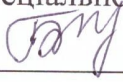


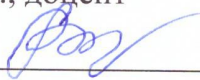
Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА
до випускної кваліфікаційної роботи бакалавра
на тему:
«Проект системи захисту гетерогенної інформаційно-комунікаційної мережі
організації»

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

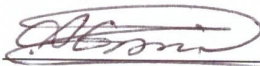
 Максим Бацманов

Керівник, професор кафедри КІ та КБ,
Д.Т.Н., доцент

 Володимир Воротніков

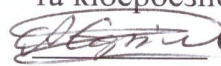
Рецензент, завідувач кафедри КІ та КБ,

К.Т.Н., доцент

 Андрій Єфіменко

Житомир – 2022

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

ЗАТВЕРДЖУЮ
Завідувач кафедри
комп'ютерної інженерії
та кібербезпеки
 Єфіменко А. А.
«06» березня 2022 р.

ЗАВДАННЯ
на випускню кваліфікаційну роботу

Студента **Бацманова Максима Олександровича**

Тема роботи: **Проект системи захисту гетерогенної інформаційно-комунікаційної мережі організації**

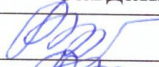
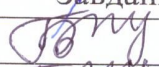
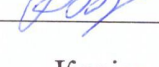
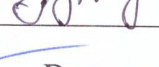
затверджена Наказом по університету від **1 березня 2022 р. № 128с**

Термін здачі студентом закінченої роботи – **10 червня 2022 р.**

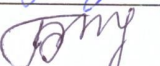
Вихідні дані для роботи:

1. Проект узагальненої топології мережі
2. Проект спрощеної топології ІКМ та узагальнена схема адресації
3. Результати проведення налаштувань інформаційно-комунікаційної мережі
4. Тестування роботи інформаційно-комунікаційної мережі

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Воротніков В.В.	 06.03.2022	 06.03.2022
2	Воротніков В.В.	 20.04.2022	 20.04.2022
3	Воротніков В.В.	 11.05.2022	 11.05.2022

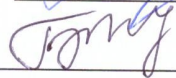
Керівник  Володимир Воротніков

Студент  Максим Бацманов

Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	6 березня 2022 – 7 березня 2022	Виконано
2	Пошук, огляд та аналіз літературних джерел	8 березня 2022 – 11 березня 2022	Виконано
3	Аналіз (сучасних) технологій захисту інформаційно-комунікаційних мереж.	12 березня 2022 – 16 березня 2022	Виконано
4	Аналіз сучасних технологічних рішень захисту інформації провідних виробників комунікаційного обладнання	17 березня 2022 – 19 березня 2022	Виконано
5	Розробка проекту захищеної гетерогенної інформаційно-комунікаційної мережі	20 березня 2022 – 24 березня 2022	Виконано
6	Розробка проекту інформаційно-комунікаційної мережі	25 березня 2022 – 30 березня 2022	Виконано
7	Розробка проекту системи адресації інформаційно-комунікаційної мережі	1 квітня 2022 – 4 квітня 2022	Виконано
8	Розробка додаткових засобів захисту інформаційно-комунікаційної мережі	5 квітня 2022 – 9 квітня 2022	Виконано
9	Розробка підсистеми захисту інформаційно-комунікаційної мережі	10 квітня 2022 – 13 квітня 2022	Виконано
10	Обґрунтування вибору та налагодження обладнання захищеної інформаційно-комунікаційної мережі	14 квітня 2022 – 18 квітня 2022	Виконано
11	Базове налаштування підсистеми захисту інформаційно-комунікаційної мережі	19 квітня 2022 – 22 квітня 2022	Виконано
12	Тестування роботи захищеної інформаційно-комунікаційної мережі	23 квітня 2022 – 24 квітня 2022	Виконано
13	Написання пояснювальної записки	25 квітня 2022 – 29 квітня 2022	Виконано
14	Підготовка презентації та виступу	30 квітня 2022 – 31 квітня 2022	Виконано
15	Отримання відгуку керівника та рецензії на кваліфікаційну роботу	6 червня 2022 – 7 червня 2022	Виконано
16	Захист	27 червня 2022	Виконано

Керівник  Володимир Воротніков

Студент  Максим Бацманов

АНОТАЦІЯ

Дипломний проект складається зі вступу, чотирьох розділів, висновків, переліку посилань, додатків і має 96 сторінок основного тексту, 27 рисунків, 3 таблиці, 16 сторінок додатків. Список використаних джерел містить 35 найменувань і займає 3 сторінки. Загальний обсяг роботи склав 112 сторінок.

Метою проекту є розробка системи захисту гетерогенної інформаційно-комунікаційної мережі організації.

В першому розділі наведено теоретичні основи побудови захищених інформаційно-комунікаційних мереж, а саме базові принципи та підходи до організації захисту інформаційно-комунікаційної мережі організації. Проведено аналіз технологій захисту інформаційно-комунікаційних мереж та сучасних технологічних рішень захисту інформації провідних виробників комунікаційного обладнання.

У другому розділі розроблено проект захищеної гетерогенної інформаційно-комунікаційної мережі організації, зокрема розроблено проект, схеми адресації, підсистеми базового захисту та додаткових засобів захисту інформаційно-комунікаційної мережі.

В третьому розділі проведено вибір та налагодження обладнання захищеної інформаційно-комунікаційної мережі, а саме: налаштування базового функціонування мережі, засобів базового захисту маршрутизаторів, GRE та mGRE-тунелів, протоколу NHRP, протоколу маршрутизації EIGRP та протоколу безпеки IPSec.

Ключові слова: ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНА МЕРЕЖА, СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ЗАХИСТ ІНФОРМАЦІЇ, VPN-МЕРЕЖА.

					КІК.КР.Б – 125 – 2 – ПЗ		
Змн.	Арк.	№ докум.	Підпис	Дата	Проект системи захисту гетерогенної інформаційно-комунікаційної мережі організації Піп Арк Акрушів Державний університет «Житомирська політехніка» Група КБ-2		
Розроб		Бацманов М.О.		20.06			
Керівник		Воротніков В.В.		20.06			
Реценз.		Єфіменко А.А.		20.06			
Н. Контр.		Воротніков В.В.		20.06			
Зав. каф.		Єфіменко А.А.		20.06			

ЗМІСТ

ВСТУП	10
РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ ЗАХИЩЕНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ МЕРЕЖ.....	12
1.1 Базові принципи та підходи до організації захисту інформаційно-комунікаційної мережі організації.	12
1.2 Аналіз технологій захисту інформаційно-комунікаційних мереж.	21
1.3 Аналіз сучасних технологічних рішень захисту інформації провідних виробників комунікаційного обладнання.	41
РОЗДІЛ 2 РОЗРОБКА ПРОЕКТУ ЗАХИЩЕНОЇ ГЕТЕРОГЕННОЇ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ МЕРЕЖІ.	49
2.1 Розробка проекту інформаційно-комунікаційної мережі.	49
2.2 Розробка схеми адресації інформаційно-комунікаційної мережі.	52
2.3 Розробка підсистеми базового захисту інформаційно-комунікаційної мережі.	55
2.4 Розробка додаткових засобів захисту інформаційно-комунікаційної мережі.	61
РОЗДІЛ 3 ОБГРУНТУВАННЯ ВИБОРУ ТА НАЛАГОДЖЕННЯ ОБЛАДНАННЯ ЗАХИЩЕНОЇ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ МЕРЕЖІ.....	62
3.1 Обґрунтування вибору апаратного та програмного забезпечення	62
3.2 Базове налагодження апаратного та програмного забезпечення.	66
3.3 Базові налаштування безпеки маршрутизаторів	68
3.4 Налаштування додаткових засобів захисту інформаційно-комунікаційної мережі	77
3.5 Тестування роботи захищеної інформаційно-комунікаційної мережі	81
ВИСНОВКИ.....	92
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	93
ДОДАТКИ.....	96

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ІВК	–	інфраструктура відкритих ключів
ІКМ	–	інформаційно-комунікаційна мережа
ЛКМ	–	локальна комп'ютерна мережа
МЕ	–	міжмережевий екран
НСД	–	несанкціонований доступ
ОС	–	операційна система
ПБ	–	політика безпеки
ПЗ	–	програмне забезпечення
ТЗІ	–	технічний захист інформації
EIGRP	–	Enhanced Interior Gateway Routing Protocol
DMVPN	–	Dynamic Multipoint VPN
GRE	–	Generic Routing Encapsulation
L2F	–	Layer 2 Forwarding
L2TP	–	Layer 2 Tunneling Protocol
NTP	–	Network Time Protocol
PPTP	–	Point-to-Point Tunneling Protocol
VPN	–	Virtual Private Network

ВСТУП

Сучасний розвиток інформаційних технологій і, зокрема, мережі Internet, призводить до необхідності захисту інформації, переданої в рамках розподіленої корпоративної мережі, що використовує мережі відкритого доступу. При використанні своїх власних фізичних каналів доступу ця проблема так гостро не постає, тому що в цю мережу не має доступу ніхто зі сторонніх. Однак вартість таких каналів досить висока, тому не кожна компанія дозволить собі використовувати їх. У зв'язку з цим, мережа Internet є найбільш доступною. Internet є незахищеною мережею, тому доводиться знаходити способи захисту конфіденційних даних, переданих по незахищеній мережі.

Безпека інформаційної взаємодії локальних комп'ютерних мереж та окремих комп'ютерів через відкриті мережі, наприклад, через інтернет, потребує якісного рішення двох завдань:

- захист підключених до відкритих каналів зв'язку локальних мереж та окремих комп'ютерів від несанкціонованих дій зі сторони зовнішнього середовища;
- захист інформації в процесі передачі по відкритим каналам зв'язку.

Метою дипломного проекту є побудова захищеної гетерогенної інформаційно-комунікаційної мережі організації.

Об'єктом дипломного проекту є процес створення захищеної гетерогенної інформаційно-комунікаційної мережі.

Предметом дослідження є використання технології DMVPN та графічних симуляторів мережі GNS3 та eNSP для побудови захищеної гетерогенної інформаційно-комунікаційної мережі організації.

Для дослідження вказаної мети необхідно вирішити наступні взаємозалежні задачі:

- розробити проект гетерогенної інформаційно-комунікаційної мережі;
- розробити проект системи адресації інформаційно-комунікаційної мережі;

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						10
Зм.	Лист	№ документу	Підпис	Дата		

- провести налагодження базового функціонування мережі;
- провести налагодження необхідних протоколів та технологій на обладнанні захищеної гетерогенної інформаційно-комунікаційної мережі .

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						11
Зм.	Лист	№ документа	Підпис	Дата		

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ ЗАХИЩЕНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ МЕРЕЖ

1.1 Базові принципи та підходи до організації захисту інформаційно-комунікаційної мережі організації.

1.1.1 Загрози інформації в інформаційно-комунікаційних мережах

Розвиток нових інформаційних технологій, загальна комп'ютеризація та різке збільшення кількості інформаційно-комунікаційних мереж призвели до того, що інформаційна безпека не тільки стає обов'язковою, вона ще й є однією з характеристик інформаційних систем. Фактор безпеки інформаційних ресурсів і послуг при розробці та експлуатації сучасних ІКМ відіграє першорядну роль.

При організації систем захисту потрібно керуватися рядом принципів, які забезпечать якісний захист та протидію від існуючих загроз.

Метою захисту інформації в ІКМ є процес протидії впливу на інформаційні ресурси та послуги, якщо даний вплив виконується з метою порушення конфіденційності, цілісності та доступності, а саме знищення, крадіжка, зниження ефективності функціонування або несанкціонований доступ [2, 9].

Побудова надійного та ефективного захисту інформаційної системи неможливе без попереднього аналізу можливих загроз безпеки системи. Цей аналіз повинен складатися з наступних етапів :

- виявлення характеру інформації, яка зберігається в системі;
- оцінку цінності інформації, яка зберігається в системі;
- побудова моделі зловмисника;
- визначення та класифікація загроз інформації в системі (несанкціоноване зчитування, несанкціонована модифікація і т.д.);

Під загрозою безпеки інформаційним ресурсам розуміють дії, які можуть призвести до спотворення, несанкціонованого використання або навіть до руйнування інформаційних ресурсів керованої системи, а також програмних і апаратних засобів [5,6].

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						12
Зм.	Лист	№ документа	Підпис	Дата		

Загрози інформаційним ресурсам та послугам можна класифікувати за наступними критеріями (рисунок 1):

- інформаційної безпеки (загрози конфіденційності даних і програм; загрози цілісності даних, програм, апаратури; загрози доступності даних; загрози відмови від виконання операцій).
- по компонентах інформаційних систем, на які загрози націлені (інформаційні ресурси та послуги, персональні дані, програмні засоби, апаратні засоби, програмно-апаратні засоби;);
- за способом здійснення (випадкові, навмисні, дії природного та техногенного характеру);
- за розташуванням джерела загроз (внутрішні та зовнішні.).



Рисунок 1.1 – Класифікація базових загроз інформаційним ресурсам в сучасних інформаційно-комунікаційних мережах

Всі загрози безпеки, спрямовані проти програмних і технічних засобів інформаційної системи, впливають на безпеку інформаційних ресурсів і призводять до порушення основних властивостей інформації, яка зберігається і обробляється в інформаційній системі. Як правило, загрози інформаційній безпеці розрізняються за способом їх реалізації [5].

Дослідження і аналіз численних випадків впливів на інформацію і несанкціонованого доступу до неї показують, що їх можна розділити на випадкові і навмисні.

Якщо розглядати класичну систему організації впливу на ІКМ, то всі загрози поділяються на випадкові, чи ненавмисні та навмисні. Джерелом ненавмисних загроз інформаційних систем можуть бути вихід з ладу апаратних чи програмних засобів, неправильні дії працівників або її користувачів, ненавмисні помилки в програмному та програмно-апаратному забезпеченні і т.д. Такі загрози можуть нанести значний збиток. Однак більш значними з точки зору ефективності функціонування ІКМ є навмисні загрози, які, на відміну від випадкових, мають на меті завдання збитків інформаційній системі або користувачам. Навмисні загрози можуть бути реалізовані шляхом довготривалої масованої атаки несанкціонованими запитами або вірусами, тощо. Наслідки наступні: руйнування (втрата) інформації, модифікація (зміна інформації на помилкову, яка коректна за формою і змістом, але має інший сенс) і ознайомлення з нею сторонніх осіб. Ціна вказаних подій може бути досить високою [5,6].

Для вирішення поставленої задачі і створення ефективної системи безпеки інформації, розроблення та вдосконалення існуючих методів захисту доцільно навести найбільш повну класифікацію загроз і шляхів їх реалізації в ІКМ.

Можна виділити актуальні загрози безпеці, які спрямовані проти інформаційних ресурсів у сучасних інформаційно-комунікаційних системах та мережах [14, 15]:

- протиправне збирання і використання інформації;
- порушення технології обробки інформації;
- впровадження в апаратні і програмні вироби компонентів, що реалізують функції, не передбачені документацією на ці вироби;
- розробка і поширення програм, що порушують нормальне функціонування інформаційних та інформаційно-телекомунікаційних систем, у тому числі систем захисту інформації;

- радіоелектронний вплив з метою виведення з ладу, пошкодження чи руйнування засобів і систем обробки інформації, телекомунікації зв'язку;
- вплив на парольно-ключові системи захисту автоматизованих систем обробки і передачі інформації;
- витік інформації технічними каналами;
- впровадження електронних пристроїв для перехоплення інформації в технічні засоби обробки, зберігання і передачі інформації з каналів зв'язку, а також у службові приміщення органів державної влади, підприємств, установ та організацій усіх форм власності;
- знищення, пошкодження, руйнування чи розкрадання машинних та інших носіїв інформації;
- перехоплення інформації в мережах передачі даних та лініях зв'язку, дешифрування цієї інформації і нав'язування хибної інформації;
- використання несертифікованих вітчизняних і закордонних інформаційних технологій, засобів захисту інформації, засобів інформатизації, телекомунікації зв'язку при створенні і розвитку інформаційної інфраструктури України;
- несанкціонований доступ до інформації, що знаходиться в банках і базах даних;
- порушення законних обмежень на поширення інформації.

1.1.2 Організаційні заходи захисту інформації

Сучасна технологія забезпечення безпеки зв'язку рекомендує всю роботу по захисту інформації з врахуванням розглянутих стратегій протидіючої сторони проводити по наступних напрямках [10,15]:

- вдосконалення організаційних і організаційно-технічних заходів;
- блокування несанкціонованого доступу до оброблюваної та інформації, що передається;
- блокування несанкціонованого отримання інформації з допомогою технічних засобів.

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						15
Зм.	Лист	№ документу	Підпис	Дата		

На сьогодні успішно розвиваються не тільки методи і засоби закриття інформації, але і проводиться активна робота протилежного напрямку, спрямована на несанкціонований доступ і перехоплення цінної комерційної інформації. Тому користувачів технічних засобів забезпечення безпеки зв'язку в першу чергу цікавлять практичні рекомендації по заходах захисту інформації і протидії несанкціонованому доступу. Під організаційними заходами захисту розуміють заходи загального характеру, які обмежують доступ до цінної інформації стороннім особам, незалежно від особливостей методів передачі і каналів витоку інформації. Будь-яка робота по забезпеченню безпеки зв'язку в комунікаційних каналах повинна починатися з таких організаційних заходів захисту [15]:

- встановлення персональної відповідальності за забезпеченням захисту інформації.
- обмеження доступу в приміщення, де проходить підготовка і обробка інформації.
- доступ до обробки, збереження і передачі конфіденційної інформації тільки перевіреним посадовим особам.
- призначення конкретних зразків технічних засобів для обробки цінної інформації і подальша робота тільки на них.
- збереження магнітних носіїв, жорстких копій і реєстраційних матеріалів в закритих міцних шафах (бажано в сейфах).
- виключення перегляду сторонніми особами змісту оброблюваної інформації за рахунок невідповідного встановлення дисплея, клавіатури, принтера і т.д.
- постійний контроль пристроїв виводу цінної інформації на фізичні носії.
- збереження цінної інформації на зовнішніх носіях тільки в засекреченому вигляді.
- використання криптографічного закриття при передачі по каналах зв'язку цінної інформації.

– знищення фізичних носіїв або матеріалів, що можуть містити фрагменти цінної інформації.

– заборона ведення переговорів про безпосередній зміст цінної інформації особам, які зайняті її обробкою.

– чітка організація робіт і контроль виконання.

Враховувати специфіку каналу обліку і методу передачі або обробки інформації дозволяють організаційно-технічні заходи, які при цьому не вимагають для своєї реалізації нестандартних прийомів і обладнання, а саме [8]:

– організація електроживлення обладнання, що обробляє цінну інформацію, від окремого джерела живлення і від загальної електромережі через стабілізатор напруги (мережний фільтр) або мотор-генератор (бажаніше).

– обмеження доступу сторонніх осіб всередину в приміщення, в якому знаходиться обладнання, шляхом встановлення механічних запорів або замків.

– при обробці і вводі-виводі інформації використовувати для відображення дисплеї, а для реєстрації — принтери.

– при відправці в ремонт технічних засобів обов'язкове знищення всієї інформації, що містяться на них.

– розміщення обладнання для обробки цінної інформації на віддалі не менше 2,5 м від пристроїв освітлення, конденсації, зв'язку, металевих труб, теле - і радіоапаратури, а також іншого обладнання, що використовується для обробки цінної інформації.

– встановлення клавіатури і друкарських пристроїв на м'які прокладки з метою зниження відходу інформації по акустичному каналу.

– при обробці цінної інформації на персональному комп'ютері, крім випадку передачі цієї інформації по мережі, відключення комп'ютера від локальної мережі або мережі віддаленого доступу.

– знищення інформації після її використання або передачі.

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						17
Зм.	Лист	№ документу	Підпис	Дата		

1.1.3 Технічні засоби захисту інформації

Одним з напрямків захисту інформації в інформаційних системах є технічний захист інформації. У свою чергу, питання ТЗІ розбиваються на два великих класи завдань: захист інформації від несанкціонованого доступу і захисту інформації від витоку технічними каналами. Під НСД звичайно мається на увазі доступ до інформації, що порушує встановлену в інформаційній системі політику розмежування доступу. Під технічними каналами розглядаються канали сторонніх електромагнітних випромінювань і наведень, акустичні канали, оптичні канали та ін..

Захист від НСД може здійснюватися в різних складових інформаційної системи [10]:

- прикладне й системне ПЗ;
- апаратна частина серверів і робочих станцій;
- комунікаційне устаткування й канали зв'язку;
- периметр інформаційної системи.

Для захисту інформації на рівні прикладного й системного ПЗ використовуються:

- системи розмежування доступу до інформації;
- системи ідентифікації й аутентифікації;
- системи аудита й моніторингу;
- системи антивірусного захисту.

Для захисту інформації на рівні апаратного забезпечення використовуються:

- апаратні ключі;
- системи сигналізації;
- засоби блокування пристроїв і інтерфейсів вводу-виводу інформації.

У комунікаційних системах використовуються наступні засоби мережевого захисту інформації:

- міжмережеві екрани (Firewall);

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						18
Зм.	Лист	№ документу	Підпис	Дата		

- системи виявлення вторгнень (IDS - Intrusion Detection System);
- засоби створення віртуальних приватних мереж (VPN - Virtual Private Network).

Але про ці засоби мова піде дещо пізніше.

Для захисту периметра інформаційної системи створюються:

- системи охоронної й пожежної сигналізації;
- системи цифрового відеоспостереження;
- системи контролю й керування доступом.

Захист інформації від її витоку технічними каналами зв'язку забезпечується наступними засобами й заходами:

- використанням екранованого кабелю й прокладкою проводів і кабелів в екранованих конструкціях;
- установкою на лініях зв'язку високочастотних фільтрів;
- побудовою екранованих приміщень ("капсул");
- використанням екранованого устаткування;
- установкою активних систем зашумлення.

З метою оцінки стану технічного захисту інформації, що обробляється або циркулює в автоматизованих системах, комп'ютерних мережах, системах зв'язку, і підготовки обґрунтованих висновків для прийняття відповідних рішень звичайно проводиться експертиза в сфері технічного захисту інформації.

Організація захисту за допомогою технічних засобів:

Блокування несанкціонованого отримання інформації за допомогою технічних засобів є досить складним завданням, а його вирішення вимагає суттєвих матеріальних затрат. Тому перед тим, як прийняти конкретні заходи, необхідно проаналізувати стан справ і врахувати наступні рекомендації [3]:

- найнадійнішим методом обмеження електромагнітного випромінювання є повне екранування приміщення, в якому знаходяться засоби обробки і передачі цінної інформації. Екранування здійснюється сталевими або алюмінієвими листами або листами із спеціальної пластмаси товщиною не менше 2 мм з надійним заземленням.

– при обробці цінної інформації основним джерелом високочастотного електромагнітного випромінювання є дисплей персонального комп'ютера. Необхідно пам'ятати, що зображення з його екрану можна приймати на віддалі кількох сотень метрів. Повністю нейтралізувати відхід інформації з екрану можна, лише використовуючи генератор шуму. Для обробки особливо важливої інформації рекомендується використання плазмових або рідкокристалічних дисплеїв.

– джерелом потужного низькочастотного випромінювання є друкуючий пристрій. Для блокування відходу інформації в цьому випадку рекомендується використати зашумлення або термодрук чи струменевий принтер.

– в багатьох випадках існують небезпечні наводки на провідники, що виходять за межі приміщення, яке підлягає охороні. Необхідно слідкувати, щоб всі з'єднання обладнання із “зовнішнім світом” здійснювалися через електричну розв'язку.

– дуже небезпечні спеціально внесені в схему обладнання обробки і зв'язку мікропередавачі або радіомаяки (закладки). Тому, після повернення обладнання з ремонту необхідно переконатися, що в ньому немає подібних закладок. Не рекомендується обробляти цінну інформацію на випадкових персональних комп'ютерах.

При виборі технічних засобів захисту інформації потрібно враховувати наступні фактори [15]:

– режим шифрування-дешифрування повинен бути простим і зручним для санкціонованого користувача.

– ефективність і надійність алгоритму шифрування не повинна залежати від змісту інформації, що передається.

– не варто віддавати перевагу тим системам, в яких криптографічні алгоритми є комерційною таємницею організації-розробника. Набагато краще, коли алгоритм відомий до деталей і відповідає деякому стандарту, а необхідний рівень стійкості визначається, наприклад, довжиною ключа.

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						20
Зм.	Лист	№ документа	Підпис	Дата		

Оптимальне вирішення складної проблеми забезпечення безпеки зв'язку можливе лише при комплексному підході з використанням, як організаційних, так і технічних заходів. Досягнення сучасної мікроелектроніки, обчислювальної техніки і методів криптографічного перетворення дозволяють оптимістично дивитись на перспективи забезпечення безпеки зв'язку. Цьому сприяє і основна тенденція розвитку сучасних систем зв'язку — перехід до цифрових методів обробки інформації, які забезпечують безпеку зв'язку за рахунок високої стійкості криптографічного перетворення.

1.2 Аналіз технологій захисту інформаційно-комунікаційних мереж.

1.2.1 Технології та специфіка побудови віртуальних приватних мереж.

Завдяки розвитку криптографічних технологій з'явився спосіб вирішити завдання захисту інформації в сучасному мережевому середовищі за рахунок використання технології захищених віртуальних приватних мереж (Virtual Private Network - VPN), що надійно шифрують інформацію, передану по дешевим відкритим мережам, включаючи Internet. Відкрита мережа може служити основою для одночасного співіснування безлічі віртуальних мереж, кількість яких визначається пропускною здатністю відкритих каналів зв'язку [7].

Компанія Check Point Software Technologies, яка не без підстави вважається законодавцем моди в області VPN і ME (наприклад, за даними незалежних консалтингових і аналітичних агентств Dataquest і IDC компанія Check Point захопила 52% світового ринку VPN-рішень і 41% ME), дає наступне визначення: "VPN - це технологія, яка об'єднує довірені мережі, вузли і користувачів через відкриті мережі, яким немає довіри". Можна зустріти і такі загальні підходи до визначення VPN:

- VPN – це захист трафіку, заснований на криптографії;
- VPN – це засіб комунікації, так як гарантія захисту доступу до внутрішніх ресурсів з будь-якої точки світу ініціює застосування інформаційних систем для віддаленого доступу;

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						21
Зм.	Лист	№ документу	Підпис	Дата		

VPN – це засіб впливу на стратегію розвитку комунікаційних систем корпорації: замість того, щоб вкладати величезні кошти в будівництво власних виділених ліній, ви практично сьогодні ж можете отримати надійно захищені канали зв'язку від комунікаційних провайдерів. Під VPN розуміють потоки даних одного підприємства, які існують в публічній мережі з комутацією пакетів і в достатній мірі захищені від впливу потоків даних інших користувачів цієї публічної мережі. Іншими словами, VPN - це деяка імітація мережі, побудованої на виділених каналах. Якщо публічна мережа надає такий сервіс, то в ній одночасно співіснують кілька VPN, які поділяють спільні комутатори та фізичні канали зв'язку.

Мережі VPN вирішують завдання підключення корпоративного користувача до віддаленої мережі і з'єднання декількох ЛКМ.

Маркетингове трактування товару має на увазі, як мінімум, дві його сутності: споживчу і фізичну. Споживча сутність VPN - «віртуальний захищений тунель, або шлях», за допомогою якого можна організувати віддалений захищений доступ через відкриті канали Internet до серверів баз даних, Web-, FTP- і поштових серверів. Фізична сутність технології VPN визначається тим, що вона може захистити трафік будь-яких інформаційних інтранет- і екстранет-систем, аудіо-та відеоконференцій, систем електронної комерції і т.п. (Але VPN, як будь-яка розподілена система, в її "фізичній сутності" є складним комплексом, який потребує цілого ряду взаємодоповнюючих засобів і систем захисту. Її здатність шифрувати дані є необхідною, але далеко не достатньою умовою для побудови дійсно надійного захисту [7].

Мета VPN-технологій полягає в максимальному ступені відокремлення потоків даних одного підприємства від потоків даних всіх інших користувачів публічної мережі. Таким чином, основними завданнями технологій VPN є забезпечення в публічній мережі гарантованої якості обслуговування для потоків даних користувача, а також захист їх від можливого несанкціонованого доступу або руйнування.

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						22
Зм.	Лист	№ документу	Підпис	Дата		

Захищеність від потоків даних інших підприємств трактується по-різному. Зазвичай її розуміють в двох відношеннях – в відношенні щодо параметрів пропускної здатності і в відношенні щодо конфіденційності даних [7].

1) Пропускна здатність VPN. Звичайно, кожне підприємство хоче, щоб віртуальні канали якомога більше були схожі на реальні виділені лінії, пропускна спроможність яких завжди в розпорядженні користувачів підприємства. Звідси випливають такі вимоги до VPN:

- користувачам повинні надаватися деякі гарантії якості обслуговування в віртуальних каналах VPN – середня пропускна здатність, максимально допустимий рівень пульсації, рівні затримок кадрів;

- користувачі повинні мати інструменти для контролю дійсних параметрів пропускної здатності віртуальних каналів.

Сьогодні для різних типів мереж з комутацією пакетів існують різні можливості отримання гарантій якості обслуговування.

2) Конфіденційність. Можливість НСД до даних, що передаються по публічній мережі, дуже хвилює мережевих адміністраторів, які звикли до використання виділених каналів або телефонних мереж для передачі корпоративних даних. Наявність зломисників в Internet представляє постійну загрозу для корпоративних серверів, до даних яких можна спробувати підключитися з будь-якого домашнього комп'ютера.

У той же час загрози перехоплення пакетів, шляхом проходження по публічній мережі передачі даних багато фахівців вважають перебільшеними. Дійсно, пакети йдуть тільки через комутатори і маршрутизатори провайдерів публічних мереж, а в мережі сторонніх організацій і приватних осіб не заходять. Провайдерами публічних мереж з комутацією пакетів виступають найчастіше ті ж організації, які надають традиційні види телекомунікаційних сервісів - виділені канали та телефонні мережі. Таким чином, загроза перехоплення пакетів по шляху проходження виходить швидше від самих провайдерів, співробітників яких можуть підкупити конкуренти. Від двох типів загроз: входу у внутрішні сервери підприємства і перехоплення даних по дорозі – існують такі засоби захисту, як

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						23
Зм.	Лист	№ документу	Підпис	Дата		

міжмережеві екрани і рогоху-сервери для відображення загроз першого виду і засоби освіти захищеного каналу для другого. VPN-технології забезпечують [7, 19]:

- захист (конфіденційність, автентичність і цілісність) передаючої по мережах інформації;
- захист внутрішніх сегментів мережі від НСД з боку мереж загального користування;
- контроль доступу в захищений периметр мережі;
- приховування внутрішньої структури захищуваних сегментів мережі;
- ідентифікацію та аутентифікацію користувачів мережевих об'єктів;
- централізоване управління політикою корпоративної мережевої безпеки і налаштуваннями VPN-мережі;
- криптографічний захист даних, переданих по каналах зв'язку мереж загального користування між захищеними сегментами мережі;
- безпечний доступ користувачів VPN до ресурсів мереж загального користування.

Інтерес користувачів до даної технології обумовлений наступними факторами:

- низькою вартістю експлуатації за рахунок використання мереж загального користування замість власних або орендованих ліній зв'язку;
- практично необмеженою масштабованістю;
- простотою зміни конфігурації і нарощування корпоративних мереж;
- "прозорістю" для користувачів і додатків.

Для керівника, що приймає рішення про встановлення тих чи інших засобів або систем, важлива і фінансова сутність застосування VPN. При правильному виборі VPN:

- забезпечуються захищені канали зв'язку і захищений трафік для окремих додатків за ціною доступу в Internet, що в кілька разів дешевше власних ліній;
- не потрібно змінювати топологію мереж при встановленні VPN, переписувати програми, навчати користувачів, тобто витратити додаткові кошти;

– забезпечується масштабованість: VPN не створить проблем росту, що збереже вже зроблені раніше інвестиції в інфраструктуру безпеки.

Як правило, побудова VPN для розподілених компаній навіть з невеликою кількістю (5-10) віддалених підрозділів (філій) є досить трудомістким завданням, складність якої обумовлюється наступними основними причинами:

- 1) гетерогенністю використовуваних апаратно-програмних платформ;
- 2) різноманітністю завдань (захищений обмін між головним офісом та філіями, офісом і мобільними або віддаленими співробітниками, сегментами внутрішньої мережі компанії);
- 3) необхідністю побудови централізованої системи управління всією корпоративною VPN;
- 4) наявністю вузької смуги пропускання і відверто поганою якістю існуючих каналів зв'язку, особливо з регіональними підрозділами і т.д.

Складність побудови корпоративних VPN посилюється ще й тим, що, як правило, корпоративні замовники висувають до VPN досить жорсткі вимоги за наступними критеріями [11,19]:

- масштабованості застосовуваних технічних рішень;
- інтегровності з вже існуючими засобами;
- легальності використовуваних алгоритмів та рішень;
- пропускної здатності мережі, що захищається;
- стійкості застосовуваних криптоалгоритмів;
- уніфікованості VPN-рішення;
- загальної сукупної вартості побудови корпоративної VPN.

Однією з вимог є забезпечення масштабованості конкретної VPN. Багаторічний досвід показує, що найбільш успішно для цього застосовуються програмні VPN-агенти, які:

- можуть забезпечити захист трафіку на всіх типах комп'ютерів – робочих станціях, серверах і шлюзах (на виході з ЛКМ у відкриті мережі);
- працюють на всіх популярних ОС.

Друга складова масштабованості - централізоване, цілісне і оперативне управління VPN. Значення цих понять у даному контексті такі:

1) централізоване – конфігурування VPN відбувається в одному місці на одній робочій станції;

2) цілісне – вся VPN створюється як єдине ціле, оскільки абсолютно неприпустима ситуація, коли різні вузли мають несумісну політику безпеки або включаються в VPN не одночасно;

3) оперативне – створена в центрі "конфігурація VPN" повинна автоматично за лічені секунди бути розіслана на всі вузли VPN. Для великих систем неприйнятно, щоб оператор послідовно, нехай і віддалено, конфігурувати всі 300 VPN-сайтів або передавав їм конфігурації на флеш-носіях.

1.2.2 Політики безпеки у віртуальних приватних мережах

Важливим питанням при створенні VPN є те, що в кожній ЛКМ повинні використовуватися еквівалентні політики безпеки. VPN по суті створює одну велику мережу з групи незалежних раніше мереж. Тому безпека VPN дорівнюватиме безпеці найменш захищеної ЛКМ - якщо хоча б одна ЛКМ дозволяє здійснити незахищений доступ по комутованих лініях, то під загрозою опиняться всі ресурси VPN.

Відповідно до загальноприйнятого визначення, безпека даних означає їх конфіденційність, цілісність і доступність. Стосовно до завдань VPN критерії безпеки можуть бути визначені наступним чином.

– конфіденційність – гарантія того, що в процесі передачі по захищеним каналам VPN дані не можуть бути переглянуті ніким, крім легальних відправника і одержувача.

– цілісність – гарантія збереження незмінності переданих даних під час проходження по захищеному каналу VPN.

– доступність – гарантія того, що засоби, які виконують функції VPN, постійно доступні легальним користувачам. Доступність засобів VPN - це комплексний показник, що залежить від кількох факторів: надійності реалізації, якості обслуговування, а також ступеня захищеності самого засобу від зовнішніх атак.

Існує три основних варіанти створення VPN [7]:

1) Захищені канали. МЕ шифрує весь трафік, який передається віддаленому хосту (хост – це комп'ютер, який має унікальний IP-адресу) або мережі, і розшифровує весь трафік, прийнятий від них. Трафік між хостами в VPN, зв'язаними захищеними каналами, передається вільно, як ніби між ними немає МЕ. Насправді трафік маршрутизується МЕ VPN. Його обробка проксі-серверами (проху-сервер, або сервер повноважень, або сервер-посередник, на жаль, на сьогодні немає єдиного терміну цього засобу) чекає директив з мережі, пересилає запит до віддаленого серверу, розташованого за межами захисної системи, отримує від нього повідомлення у відповідь і передає його за призначенням, в такому випадку аутентифікація не потрібна. Будь-які два хоста всередині VPN, пов'язані захищеними каналами, можуть вільно обмінюватися даними між собою, і надавати всі сервіси TCP/IP, які у них є. Захищені канали часто використовуються для з'єднання географічно розділених мереж, що належать одній організації, кожна з яких має своє власне підключення до Internet через провайдера, в одну віртуальну мережу безпечним способом.

2) Приватні канали. Трафік між МЕ і віддаленим хостом шифрується так само, як і для захищеного каналу. Але трафік між віддаленими хостами, пов'язаними приватними каналами, не передається вільно, а повинен бути оброблений проксі-сервером МЕ і з'єднання аутентифіковане, як того вимагає звичайна політика доступу для проксі-сервера. Цей вид каналу забезпечує аутентифікацію відправника трафіку і конфіденційність даних, але в даному випадку дві мережі забезпечують наявність двох різних периметрів безпеки, і можуть використовуватися тільки ті сервіси, для яких сконфігурована передача

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						27
Зм.	Лист	№ документу	Підпис	Дата		

проксі-сервера в МЕ. Приватні канали часто використовуються для організації зв'язку між мережами різних організацій, які не хочуть надавати повного доступу до їхніх мереж, і вимагають конфіденційності трафіку між ними.

3) Проміжні канали. Ці канали використовуються для проміжної передачі зашифрованого трафіку між хостами, розташованими за МЕ і входять до складу іншої VPN. Це дозволяє МЕ, що знаходиться між двома іншими VPN, бути сконфігурованим так, що він тільки передає зашифровані дані. Він не розшифровує трафік і навіть не знає ключа шифрування. Йому треба лише знати адреси хостів по обидві сторони МЕ, що беруть участь в організації цього каналу, щоб визначити, які зашифровані пакети пропускати. Така архітектура дозволяє використовувати проміжний МЕ як маршрутизатор.

Використовуючи тільки що наведені поняття каналів VPN, наведемо приклади деяких політик безпеки (ПБ) з використанням каналів Internet для побудови VPN.

– Висока ПБ. Для VPN, що використовують Internet, МЕ організації повинні працювати в режимі приватного каналу, шифрувати трафік VPN і вимагати використання проксі-серверів МЕ для обмеження доступу до сервісів з боку віддалених хостів VPN. Також повинні бути засоби, що забезпечують швидке створення резервного каналу для передачі в разі тимчасової неможливості передачі через Internet.

– Низька-середня ПБ. Для VPN, що використовують Internet, МЕ організації повинні працювати в режимі захищеного каналу, шифрувати трафік VPN і не вимагати використання проксі-серверів для його обробки.

– Середня-висока ПБ. VPN між ЛКМ не повинні використовувати Internet для передачі критичного до оперативності передачі трафіку. Якщо рівень надійності, що надається Internet, недостатній для забезпечення необхідного рівня сервісу, для передачі даних повинні використовуватися інші способи.

1.2.3 Засоби захисту інформації, що доповнюють віртуальні приватні мережі

Сучасні VPN-мережі будуються на основі міжнародних стандартів протоколу IPSec і досягнень в області інфраструктури відкритих ключів (Public Key Infrastructure, PKI або IBK).

Основне завдання VPN – захист трафіку. Це завдання виключно складне вже на криптографічному рівні, оскільки VPN повинна задовольняти великій кількості вимог. У першу чергу мати надійну криптографію, що гарантує від прослуховування, зміни, відмови від авторства (це визначається протоколом IPSec), мати надійну систему управління ключами, захищати від атак методом повтору сеансу протоколу (replay attack) і перевіряти, чи "живий" абонент в даний момент (це забезпечується прийнятим в 1998 р. протоколом IKE). Застосування стандартних протоколів IPSec / IKE в VPN-системах сьогодні практично обов'язкове. В іншому випадку жоден замовник не зможе бути впевненим, що постачальник VPN створив криптографічно цілісну і надійну систему. Крім того, в майбутньому вона виявиться несумісна з VPN, застосовуваними контрагентами корпорації, що врешті-решт призведе до певних проблеми.

Жоден криптозахист, побудований на відкритій криптографії, не може існувати без IBK, в завдання якої входить [19]:

- створення і підпис сертифікатів, що вимагає наявності ієрархічної системи нотаріусів, так як користувач VPN повинен отримувати свій сертифікат за місцем роботи, а не їздити за ним, наприклад, в центральний офіс або в якусь іншу організацію;
- передача сертифікатів на електронний носій користувача (смарт-карта, e-token, дискета) та публікація їх на сервері сертифікатів з тим, щоб будь-який учасник VPN міг легко отримати сертифікат свого партнера;
- реєстрація фактів компрометації і публікація "чорних" списків відкликаних сертифікатів.

1.2.4 Стандартні протоколи створення віртуальних приватних мереж

1.2.4.1 Рівні захищених каналів

При побудові VPN однією з найбільш гострих є проблема сумісності. Кінцеві точки тунелю VPN повинні використовувати одні й ті ж методи взаємної аутентифікації, шифрування даних і генерації секретних ключів. Природне вирішення цієї проблеми - підтримка кожним VPN-пристроєм деякого набору стандартних технологій і протоколів захисту даних, щоб при встановленні захищеного з'єднання два вузли мережі в результаті переговорного процесу змогли знайти загальну технологію і загальний протокол. Особливо це важливо при організації екстрамережі, коли недостатньо прийняти якийсь стандарт захисту даних в рамках одного підприємства.

В даний час процес стандартизації технологій VPN ще не досяг того рівня, при якому користувачі спокійно можуть набувати VPN-продукти різних виробників, не піклуючись про їх сумісності. Але значна частина роботи в цьому напрямі вже виконана. В кінці 1998 р. була прийнята нова версія системи стандартів IPSec, які, швидше за все, будуть домінувати в Internet і приватних IP-мережах при організації VPN.

Важливою характеристикою стандартів захищеного каналу є рівень моделі взаємодії відкритих систем OSI, на якому працюють протоколи даного стандарту (рисунки 1.2). Модель OSI, розроблена Міжнародною організацією по стандартизації (International Standards Organization - ISO), визначає сім рівнів, на яких комп'ютерні системи взаємодіють один з одним, починаючи з рівня фізичного середовища передачі даних і закінчуючи рівнем прикладних програм, що використовуються для комунікацій.

Захищений канал можна побудувати на основі системних засобів, реалізованих на різних рівнях стека комунікаційних протоколів (рисунки 1.2). Звичайно, можливий і такий варіант, коли програма самостійно, без звернення до системних засобів, забезпечує конфіденційність і цілісність переданих їм даних. Але, оскільки в цьому випадку від прикладного програміста потрібні додаткові

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						30
Зм.	Лист	№ документу	Підпис	Дата		

витрати зусиль, такий варіант рідко зустрічається на практиці, хіба що для вирішення вельми специфічних завдань.

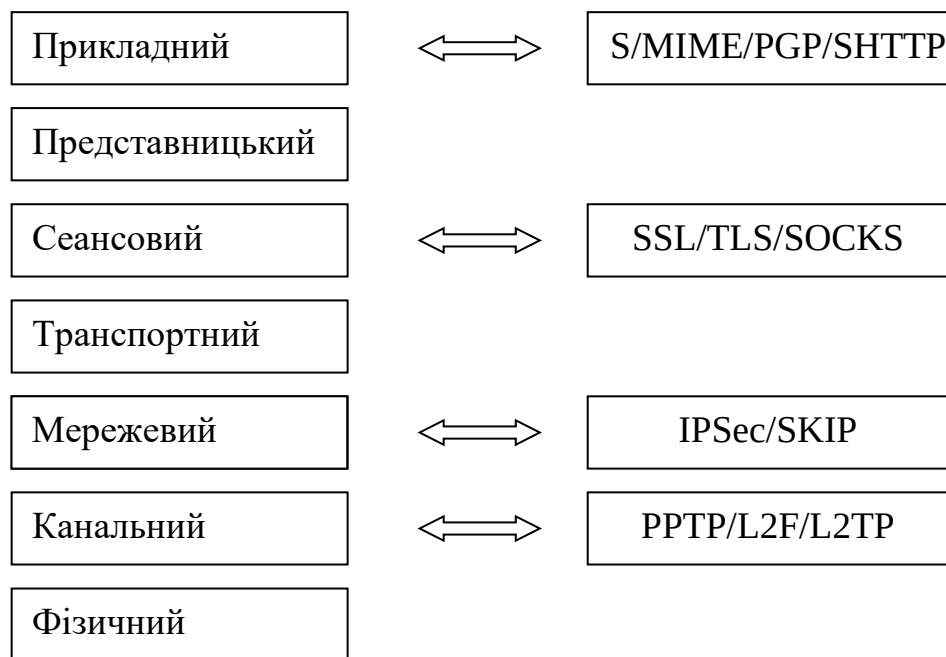


Рисунок 1.2 – Рівні захищених каналів

Що ж стосується системних засобів підтримки захищених каналів, то вони вбудовуються в різні рівні, починаючи з прикладного. На прикладному рівні зустрічається багато версій відомих протоколів, які відрізняються від своїх стандартних реалізацій наявністю тих чи інших засобів захисту переданих даних (наприклад, протоколи S / MIME (Secure Multipurpose Internet Mail Extension) або PGP (Pretty Good Privacy), що захищають дані електронної пошти) . Недоліком такого підходу є вузька область дії - протокол захищає тільки цілком певну мережеву службу - файлову, гіпертекстову або поштову. Тому для кожної служби необхідно розробляти відповідну захищену версію протоколу і виконувати цю роботу при розробці нової служби. Інший недолік - необхідність переписування програм, які користуються відповідними мережевими службами: у додатки повинні бути вбудовані явні виклики функцій захищених версій протоколу.

Найбільш відомим протоколом захищеного каналу, що працюють на сеансовому рівні, є протокол Secure Socket Layer (SSL) і його нова реалізація - Transport Layer Security (TLS). Зниження рівня протоколу зробило його набагато

більш універсальним засобом захисту. Тепер єдиним протоколом захисту можуть скористатися будь-які програми та будь-які протоколи прикладного рівня. Правда, при цьому як і раніше необхідно їх переписувати, щоб вбудувати в них виклики функцій протоколу SSL.

Чим нижче по стеку розташовані засоби захищеного каналу, тим простіше їх зробити прозорими для додатків і прикладних протоколів. Найбільш відомим стандартним засобом захисту мережевого рівня є протокол IPSec. Проте в цьому випадку програми обмежені використанням цілком певного протоколу мережевого рівня, наприклад, протокол IPSec застосуємо тільки в IP-мережах.

Протокол захищеного каналу може працювати також і на канальному рівні моделі OSI. До таких протоколів відноситься, наприклад, протокол PPTP (Point-to-Point Tunneling Protocol). Як і у випадку захищеного каналу мережевого рівня, тут також забезпечується прозорість засобів захисту для додатків і служб прикладного рівня. Перевагою такого підходу є незалежність засобів захисту від застосовуваного протоколу транспортування пакетів мережевого рівня.

1.2.4.2 Захист даних на канальному рівні

До протоколів побудови VPN даного рівня відносяться [7]:

- протокол PPTP (Point-to-Point Tunneling Protocol), розроблений Microsoft спільно з компаніями Ascend Communications, 3Com/Primary Access, Ecl-Telematics і US Robotics;
- протокол L2F (Layer-2 Forwarding) компанії Cisco Systems;
- протокол L2TP (Layer-2 Tunneling Protocol), який об'єднав обидва вищеназваних протоколи.

Однак ці протоколи, на відміну від IPSec, не можна назвати повнофункціональними (наприклад, PPTP не визначає метод шифрування).

Протоколи PPTP, L2F і L2TP об'єднує те, що вони представляють собою протоколи тунелювання канального рівня, які інкапсулюють кадри канального протоколу до протоколу мережевого рівня. За допомогою останнього дані потім

передаються по складовій мережі. Крім того, ці протоколи близькі також і тим, що їх головна область застосування - рішення задачі захищеного багатопроTOCOLьного віддаленого доступу до ресурсів КС через публічну мережу, в першу чергу через Internet. Оскільки практично будь-яке клієнтське ПЗ використовує сьогодні для віддаленого доступу стандартний протокол каналного рівня PPP, то і протоколи PPTP, L2F і L2TP засновані на інкапсуляції кадрів PPP в пакети мережевого рівня. В такій якості використовується перш за все IP, але можливе застосування і інших мережевих протоколів, таких як IPX або DECnet.

Хоча всі три протоколи часто відносять до протоколів освіти захищеного каналу, строго кажучи, цьому визначенню відповідає тільки PPTP, що забезпечує як тунелювання, так і шифрування даних. Протоколи L2F і L2TP є тільки протоколами тунелювання, а функції захисту даних (шифрування, аутентифікація, цілісність) в них не підтримуються. Передбачається, що при їх застосуванні захист тунельованих даних буде виконуватися за допомогою деякого третього протоколу, наприклад, IPSec.

Протокол PPTP - наскрізний тунельний протокол, який був представлений в робочу групу PPP Extensions IETF в якості претендента на стандартний протокол створення захищеного каналу, проте в якості стандарту так і не був затверджений. Це було пов'язано з тим, що компанія Cisco Systems приблизно в той же час представила IETF свій протокол L2F, тому було вирішено не віддавати перевагу жодному з цих протоколів, а створити якийсь об'єднаний варіант, який отримав назву L2TP. Незважаючи на відсутність статусу стандарту Internet, протокол PPTP отримав практичне поширення, в основному завдяки зусиллям компанії Microsoft, що реалізувала його у своїх операційних системах (ОС) Windows NT. Деякі виробники ME і шлюзів VPN також підтримують PPTP.

Протокол PPTP ніяк не міняє протокол PPP, але надає для нього новий транспортний засіб. В рамках цього протоколу визначається архітектура клієнт / сервер, призначена для поділу функцій, які існують в поточних серверах мережевого доступу (NAS, Network Access Server) і для підтримки VPN. Сервер мережі PPTP (PNS) повинен працювати під управлінням операційної системи

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						33
Зм.	Лист	№ документа	Підпис	Дата		

(ОС) загального призначення, а клієнт - концентратор доступу до РРТР (РАС), працює на платформі віддаленого доступу. РРТР визначає протокол управління викликами, який дозволяє серверу управляти віддаленим комутованим доступом через телефонні мережі загального користування (PSTN) чи цифрові канали ISDN або ініціалізувати вихідні комутовані з'єднання. РРТР використовує механізм загальної маршрутної інкапсуляції (Generic Routing Encapsulation, GRE) для передачі пакетів PPP, забезпечуючи при цьому контроль потоків і мережевих заторів. Безпека даних у РРТР може забезпечуватися за допомогою протоколу IPSec.

Протокол РРТР дозволяє створювати захищені канали для обміну даними по різних протоколах - IP, IPX або NetBEUI. Дані цих протоколів, які надходять в глобальну мережу упаковані в кадри PPP, потім інкапсулюються за допомогою протоколу РРТР в пакети протоколу IP, за допомогою якого переносяться в зашифрованому вигляді через мережу TCP / IP. Приймаючий вузол витягує з пакетів IP кадри PPP, а потім обробляє їх стандартним способом, тобто витягує з кадру PPP вихідний пакет IP, IPX або NetBEUI і відправляє його по ЛКМ.

Протокол L2F – протокол естафетної передачі на другому рівні, який був розроблений компанією Cisco Systems. Він забезпечує тунелювання протоколів канального рівня (тобто фреймів High - Level Data Link Control [HDLC], async HDLC або Serial Line Internet Protocol [SLIP]) з використанням протоколів більш високого рівня, наприклад IP. За допомогою таких тунелів можна розділити місце розташування RAS, до якого підключається користувач, використовуючи місцеві комутовані лінії зв'язку, і точки, де відбувається безпосередня обробка протоколу віддаленого доступу (SLIP, PPP) і користувач отримує доступ в мережу. Ці тунелі дають можливість використовувати додатки, що вимагають віддалений доступу з приватними адресами IP, IPX і AppleTalk через протокол SLIP / PPP по існуючій інфраструктурі Internet. Підтримка таких багатопрокольних додатків віртуального віддаленого доступу дуже вигідна кінцевим користувачам і незалежним постачальникам послуг, оскільки дозволяє розділити на всіх витрати на засоби доступу і базову інфраструктуру і дає можливість здійснювати доступ

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						34
Зм.	Лист	№ документу	Підпис	Дата		

через місцеві лінії зв'язку. Крім того, такий підхід захищає інвестиції, зроблені в існуючі програми, що працюють не по протоколу IP, надаючи захищений доступ до них і в той же час підтримуючи інфраструктуру доступу до Internet.

Протокол L2TP – єдиний стандартний протокол (розроблений компаніями Cisco і Microsoft (в рамках IETF)), який отримав назву тунельного протоколу другого рівня. Протокол L2TP має такі властивості.

- він прозорий для кінцевих систем: ні віддаленій кінцевій системі, ні корпоративному серверу не потрібне додаткове спеціальне ПЗ, щоб користуватися цим сервісом;
- аутентифікація забезпечується за допомогою PPP CHAP/ PAP або за допомогою інших протоколів перед стартом сесії PPP. Можуть також використовуватися такі системи, як TACACS +, RADIUS (Remote Authentication Dial-In User Service), токени доступу і одноразові паролі. Аутентифікація виконується в КС незалежно від провайдера Internet;
- адресація кінцевого вузла здійснюється за тією ж схемою, що й при прямому дзвінку на RAS КС. Адреса призначається не провайдером, а з КС;
- авторизація, як і при прямому дзвінку, також управляється з КС;
- облік виконується як провайдером (з метою оплати), так і користувачем (з метою аудиту та повернення оплати).

1.2.4.3 Захист даних на мережевому рівні

Протокол IPSec. Можливість побудови VPN на обладнанні і ПЗ різних виробників досягається впровадженням деякого стандартного механізму. Таким механізмом виступає протокол Internet Protocol Security (IPSec). Він описує всі стандартні методи VPN і визначає методи ідентифікації при ініціалізації тунелю, методи шифрування в кінцевих точках тунелю та механізми обміну та управління ключами шифрування між цими точками. Правда, цей протокол орієнтований виключно на IP-протокол.

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						35
Зм.	Лист	№ документу	Підпис	Дата		

IPSec називають в стандартах Internet системою, що відповідає дійсності. Це система відкритих стандартів, яка має на сьогодні чітко окреслене ядро і в той же час дозволяє досить просто доповнювати її новими протоколами, алгоритмами і функціями. Цьому сприяє її відкрита побудова, що включає всі нові досягнення в області криптографії. Восени 1998 р. були прийняті переглянуті специфікації RFC на всі основні компоненти IPSec, а спільна робота цих компонентів описана в стандарті RFC 2401 "Security Architecture for the Internet Protocol". У порівнянні з першими версіями стандартів IPSec, прийнятих в 1996 р., переглянуті в 1998 р. специфікації стали більш конкретними.

IPSec вирішує такі основні завдання встановлення і підтримання захищеного з'єднання [20]:

- аутентифікацію користувачів або комп'ютерів при ініціації захищеного з'єднання;
- шифрування і аутентифікацію переданих даних між кінцевими точками з'єднання;
- автоматичне постачання кінцевих точок секретними ключами, необхідними для роботи протоколів аутентифікації і шифрування даних.

Для вирішення поставлених завдань система IPSec використовує протоколи трьох типів:

- протокол обміну ключами Internet IKE (Internet Key Exchange), призначений для початкового етапу встановлення з'єднання і визначає спосіб ініціалізації захищеного каналу, а також процедури обміну та управління секретними ключами в рамках захищеного з'єднання, методи шифрування та ін;
- протокол АН (Authentication Header), який забезпечує цілісність і аутентифікацію джерела даних в переданих пакетах, а також опціонально - захист від помилкового відтворення пакетів (в заголовку АН дані пакета не шифруються);
- протокол ESP (Encapsulation Security Payload), що забезпечує шифрування, аутентифікацію та цілісність переданих даних, і опціонально – захист від

помилкового відтворення пакетів (дані і заголовок шифруються відповідно до цього протоколу).

Для шифрування даних в IPSec може бути застосований будь-який симетричний алгоритм шифрування, що використовує секретні ключі. Перевірка цілісності та аутентифікація даних виконуються за допомогою обчислення хеш-коду даних.

Для вирішення завдання безпечного управління та обміну криптографічними ключами між віддаленими пристроями використовується протокол IKE (тоді як IPSec кодує і підписує пакети). Протокол IKE автоматизує обмін ключами і встановлює безпечне з'єднання. Крім того, IKE дозволяє змінювати ключ для вже встановленого з'єднання, що підвищує конфіденційність переданої інформації.

IKE є комбінацією декількох протоколів - ISAKMP, Oakley і SKEME. Справа в тому, що загальні правила управління безпечними сполуками (в стандартах IPSec "безпечна асоціація" або "контекст безпеки" - Security Association, SA) в IP-мережах визначає протокол ISAKMP. Однак він задасть тільки послідовність етапів встановлення безпечної асоціації, формати пакетів, за допомогою яких асоціація встановлюється і розривається, формулює вимоги до процедур аутентифікації сторін та обміну секретними ключами, але самі протоколи аутентифікації сторін та обміну ключами в ньому детально не визначені. Тому розробники протоколу IKE доповнили загальні правила і процедури протоколу ISAKMP процедурами аутентифікації і обміну ключами, взятими з протоколів Oakley і SKEME. Через те, що протокол IKE використовує для управління асоціаціями алгоритми та формати протоколу ISAKMP, ці назви іноді використовують як синоніми.

Автентичність сторін в IKE встановлюється одним із двох способів. Перший спосіб передбачає виконання протоколу аутентифікації типу "запит-відповідь" з використанням хеш-функції із загальним секретним ключем (наприклад, MD5). У другому способі використовуються сертифікати відкритих ключів стандарту X.509. Кожна зі сторін підписує свій сертифікат своїм секретним ключем і

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						37
Зм.	Лист	№ документу	Підпис	Дата		

передає ці дані протилежній стороні. Якщо перевірка підписаного сертифіката іншою стороною дає позитивний результат, то це засвідчує той факт, що сторона, яка надала дані, дійсно володіє відповідним секретним ключем. Але, для посвідчення автентичності сторони потрібно ще впевнитися в автентичності самого сертифіката, і для цього сертифікат повинен бути підписаний не тільки його власником, а й деякою третьою стороною, що видала сертифікат і викликає довіру. Ця сторона називається сертифікаційним центром (перекладі англійського Certificate Authority, CA), і її відкритий ключ повинен бути відомий всім вузлам, що використовують її сертифікати для посвідчення особистостей один одного. В межах однієї організації ця проблема не викликає великих складнощів. Досить в усі вузли попередньо ввести відкритий ключ єдиного на підприємстві сервера сертифікатів, який виконує роль засвідчуючого центру для всіх вузлів і користувачів комп'ютерної мережі даного підприємства. Однак при взаємодії вузлів різних організацій, які в загальному випадку використовують сертифікати, видані різними сертифікаційними центрами, проблема стає досить складною. Повинна існувати ієрархія сертифікаційних центрів, на чолі якої знаходяться кілька сертифікаційних центрів, відкриті ключі яких всім відомі. Крім того, необхідний автоматичний протокол перевірки автентичності сертифіката. З його допомогою послідовно перевіряється справжність підписів сертифікаційних центрів аж до того, публічний ключ якого відомий стороні, яка виконує аутентифікацію. В цілому таку ієрархічну систему видачі та посвідчення сертифікатів в публічних мережах називають ІВК [20].

Після перевірки автентичності сторін протокол ІКЕ використовує алгоритм Діффі-Хеллмана, за допомогою якого сторони визначають розділюючий секретний ключ, який буде використовуватися в безпечній асоціації протоколами АН або ESP. У цього ключа є час життя – якщо він закінчується, то дана асоціація примусово розривається і встановлюється нова, для якої заново визначається інший секретний ключ. Крім секретного ключа, на цій стадії сторони можуть погодити і інші параметри асоціації.

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						38
Зм.	Лист	№ документу	Підпис	Дата		

1.2.5 Міжмережеві екрани

Ряд завдань щодо відображення найбільш ймовірних загроз для внутрішніх мереж здатні вирішувати міжмережеві екрани. У сфері комп'ютерних мереж міжмережевий екран є бар'єром, що захищає від спроб злоумисників вторгнутися у внутрішню мережу для того, щоб скопіювати, змінити або стерти інформацію або скористатися пам'яттю або обчислювальною потужністю працюючих у цій мережі комп'ютерів. Міжмережевий екран повинен забезпечувати безпечний доступ до зовнішньої мережі та обмежити доступ зовнішніх користувачів до внутрішньої мережі.

Міжмережевий екран (МЕ) - це система міжмережевого захисту, що дозволяє розділити загальну мережу на дві частини або більше і реалізувати набір правил, що визначають умови проходження пакетів з даними через кордон з однієї частини загальної мережі в іншу. Як правило, ця межа проводиться між корпоративною (локальною) мережею підприємства і глобальною мережею Internet, хоча її можна провести і всередині корпоративної мережі підприємства. МЕ пропускає через себе весь трафік, приймаючи для кожного пакета що проходить рішення - пропускати його або відкинути. Для того щоб МЕ міг здійснити це, йому необхідно визначити набір правил фільтрації [8, 16].

Зазвичай міжмережеві екрани захищають внутрішню мережу підприємства від "вторгнень" з глобальної мережі Internet, проте вони можуть використовуватися і для захисту від "нападів" з корпоративної інтранет мережі, до якої підключена локальна мережа підприємства. Жоден міжмережевий екран не може гарантувати повного захисту внутрішньої мережі при всіх можливих обставин. Однак для більшості комерційних організацій встановлення міжмережевого екрану є необхідною умовою забезпечення безпеки внутрішньої мережі. Головний аргумент на користь застосування міжмережевого екрану полягає в тому, що без нього системи внутрішньої мережі наражаються на

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						39
Зм.	Лист	№ документу	Підпис	Дата		

небезпеку з боку слабо захищених служб мережі Internet, а також зондування і атак з яких-небудь інших хост - комп'ютерів зовнішньої мережі.

При підключенні корпоративної або локальної мережі до глобальних мереж адміністратор мережевої безпеки має вирішувати наступні завдання [8]:

- захист корпоративної або локальної мережі від несанкціонованого доступу з боку глобальної мережі;
- приховування інформації про структуру мережі та її компонентів від користувачів глобальної мережі,
- розмежування доступу в мережу, що захищається з глобальної мережі та з мережі, що захищається в глобальну мережу.

Необхідність роботи з віддаленими користувачами вимагає встановлення жорстких обмежень доступу до інформаційних ресурсів мережі, що захищається. При цьому часто виникає потреба в організації у складі корпоративної мережі кількох сегментів з різними рівнями захищеності:

- вільно доступні сегменти (наприклад, рекламний WWW-сервер);
- сегмент з обмеженим доступом (наприклад, для доступу співробітникам організації з віддалених вузлів);
- закриті сегменти (наприклад, локальна фінансова мережа організації).

Для захисту корпоративної або локальної мережі застосовуються такі основні схеми організації міжмережевих екранів:

- міжмережевий екран – фільтруючий маршрутизатор;
- міжмережевий екран на основі двопортового шлюзу;
- міжмережевий екран на основі екранованого шлюзу;
- міжмережевий екран – екранована підмережа.

1.3 Аналіз сучасних технологічних рішень захисту інформації провідних виробників комунікаційного обладнання.

1.3.1 Провідні виробники комунікаційного обладнання

Рівень шкідливого трафіку в сучасних інформаційно-комунікаційних мережах постійно зростає і захист мережевого периметра стає більш важливим. Постійні атаки різного роду з різних джерел змушують замислитися про безпеку мережі. Перед багатьма операторами зв'язку та організаціями постає питання про вибір надійного комунікаційного обладнання для забезпечення захисту. Найчастіше необхідно не просто пристрій безпеки, а всеосяжне, надійне рішення, інтегроване в поточну інфраструктуру. Такі, необхідні для безпеки, рішення, пропонують такі виробники комунікаційного обладнання:

- 1) Cisco Systems;
- 2) Huawei Technologies;
- 3) Juniper Networks;
- 4) Ruby Tech;
- 5) Alcatel-Lucent;
- 6) Extreme Networks та ін..

Провідними компаніями, що займають найбільшу долю ринку комунікаційного обладнання є Cisco Systems та Huawei Technologies.

Компанія Huawei була заснована в 1987 році зі статутним капіталом у 5680 доларів США. За минулі роки щорічний обсяг продажів компанії перевищив 20 млрд доларів США, а офіси компанії працюють у більш ніж 140 країнах світу. Компанія заснована в економічній зоні Шеньчжень, Китай. На нинішній день компанія увійшла в десятку найбільших світових постачальників телекомунікаційного обладнання.

Huawei Technologies – один з лідерів у сфері розробки і виробництва телекомунікаційного обладнання, систем і комплексних мережевих рішень, що на даний час обслуговує 35 з 50 провідних світових операторів, поряд з одним

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						41
Зм.	Лист	№ документу	Підпис	Дата		

мільярдом користувачів по всьому світу. Перелік продукції, що випускається включає рішення для мереж мобільного зв'язку, обладнання широкосмугового доступу, рішення для IP мереж, оптичних мереж, додаткові послуги зв'язку і термінали. Huawei Technologies володіє всіма перевагами у сфері довгострокового розвитку і надає конкурентоспроможні рішення зв'язку своїм клієнтам. Компанія Huawei офіційно присутня в Україні з 2000 року. Саме тоді в Києві було відкрито українське представництво всесвітнього гіганта, де на сьогоднішній день працює близько 100 осіб. Обладнання Huawei встановлено у найбільших гравців місцевого телекомунікаційного ринку – компаній МТС, «Київстар», «Українські Радіосистеми» (ТМ Beeline), «Голден Телеком», «CST-Інвест» (CDMA-оператор), «Велтон Телеком» і «Телесистеми України».

В даний час широкосмугові та інтелектуальні мережі зв'язку, в яких переважає пакетна передача даних, розвиваються в напрямку інтеграції з IP-мережами і оптичними мережами, що надають більш уніфіковану платформу підтримки для мереж зв'язку наступного покоління. Компанія пропонує на вигідних умовах широкий спектр обладнання передачі даних Huawei, включаючи маршрутизатори низької і середньої продуктивності, маршрутизатори рівня ядра мережі, мультисервісні шлюзи управління (MSCG), комутатори LAN і системи мережевого управління.

Cisco Systems – світовий лідер в області мережевих технологій, що змінюють способи людського спілкування, зв'язку, співпраці. Сьогодні мережі стали найважливішим елементом бізнесу, освіти, державного управління та домашніх комунікацій. IP-рішення Cisco можна з повним правом назвати фундаментальною основою цих мереж.

Компанія Cisco Systems була заснована в 1984 році невеликою групою вчених із Стенфордського університета. З самого початку інженери Cisco стали лідерами з розробки мережевих технологій, заснованих на інтернет-протоколі. Сьогодні, компанія Cisco розробляє кращі в галузі продукти та рішення в базових для неї галузях (комутація і маршрутизація), а також у сфері сучасних технологій, до яких відносяться [25]:

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						42
Зм.	Лист	№ документу	Підпис	Дата		

- IP-комунікації
- мережева безпека
- Бездротові мережі LAN
- Мережі зберігання (SAN)
- Домашні мережі
- Відеосистеми

Компанія Cisco була ініціатором багатьох історичних змін в сфері технологій, і сьогодні вона продовжує цю традицію. Зараз, коли галузь високих технологій знову переживає період великих змін, Cisco зберігає лідируючі позиції в різних сегментах, таких як маршрутизація, комутація, уніфіковані комунікації, бездротовий зв'язок і безпека. Компанія стала каталізатором переходу всієї галузі на IP-технології. Послуги та рішення Cisco використовуються для створення комп'ютерних мереж, що дозволяють приватним особам, компаніям і навіть цілим країнам підвищити продуктивність праці, поліпшити якість надаваних послуг, зміцнити конкурентоспроможність [24].

Ресурси Cisco – це самий великий в галузі портфель апаратних засобів, що використовуються для будівництва інформаційних мереж і надання доступу до них, плюс операційна система Cisco IOS (призначена для підтримки мережевих послуг і додатків), досвід проектування і розгортання мереж, а також система технічної підтримки і професійних послуг з обслуговування та оптимізації мережевої роботи. Унікальність Cisco в тому, що вона здатна - самостійно або разом з партнерами - надати всі перераховані вище ресурси.

1.3.2 Характеристика мережевих продуктів компанії Huawei Technologies

Маршрутизатори компанії Huawei серії AR для підприємств являють собою маршрутизатори наступного покоління, корпоративного класу і засновані на фірмовій Універсальній Платформі Маршрутизації (VRP), яка в повній мірі користується перевагами накопиченої підприємством інформації в таких областях, як передача даних, мережа бездротового доступу і базова мережа. AR

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						43
Зм.	Лист	№ документу	Підпис	Дата		

об'єднує в собі маршрутизацію, комутацію, послуги 3G, послуги передачі голосу і функції безпеки. Такий маршрутизатор використовує багатоядерний процесор CPU і неблоковану структуру комутації, забезпечує провідну в галузі швидкодію і розширення системи, відповідаючи майбутнім вимогам сервісного обслуговування. AR пропонує комплексне рішення для корпоративних мереж, виконує швидке багатоканальне обслуговування і зберігає інвестиції клієнтів.

Маршрутизатори серії AR не тільки підтримують бездротовий режим WLAN, UMTS, LTE, але також і дротовий режим оптоволокна і мідного дроту, що забезпечує споживачеві гнучкість методів доступу до мережі.

Маршрутизатор AR з'єднаний з основною інформаційною системою від стороннього виробника за допомогою відкритої платформи послуг (OSP) для забезпечення уніфікованого спілкування корпоративних користувачів. Клієнти, агенти, що представляють стороннього виробника постачальники та виробники, у міру необхідності, можуть удосконалити і використовувати маршрутизатори AR.

Маршрутизатор AR виконує різні голосові функції для інформаційних мереж підприємств, забезпечуючи гнучкість та ефективність комунікацій.

У період обслуговування маршрутизатор AR гарантує безпечну роботу корпоративних мереж. Крім того, він забезпечує комплексний механізм захисту безпеки, що включає контроль доступу користувачів, розпізнавання пакетів інформації та активний захист від спроб порушення захисту. Такий механізм захищає капіталовкладення клієнтів.

У міру зростання підприємства зростають і вимоги корпоративних користувачів до служб розгортання. Маршрутизатор AR надає USB-диск для розгортання пристроїв і здійснення функцій авто-налаштування для служби розгортання.

Корпоративні користувачі зацікавлені в простому управлінні послугами. Маршрутизатор AR надає функції iТес, NQA, NetStream для спрощення управління послугами.

Маршрутизатори AR1200 функціонують як вихідні маршрутизатори філій підприємства, і забезпечують методи гнучкого доступу для підтримки віддалених

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						44
Зм.	Лист	№ документу	Підпис	Дата		

мережевих з'єднань. AR1200 відповідає різним вимогам до доступу, включаючи виділену лінію, Ethernet, xDSL і WLAN. Це економить витрати на розгортання і використання, а також має високу оцінку серед замовників.

Маршрутизатори AR2200 і AR3200 надають інтерфейсні плати 24GE для впровадження доступу GE з високою щільністю портів. Така інтерфейсна плата сприяє зручності роботи в мережі та її техобслуговування, а також захищає капіталовкладення клієнтів.

В якості голосового шлюзу для корпоративних мереж AR3200 функціонує як місцева АТС з протоколом IP (IP PBX) або як SIP-шлюз.

Вбудована в маршрутизатори офісна АТС (PBX) підтримує основний шифр підприємства, інтерактивну систему розпізнавання голосових повідомлень IVR і систему інформаційного запиту про рахунок, що зміцнює репутацію підприємства і підвищує ефективність корпоративного зв'язку. AR розташований в Центральному офісі, щоб встановлювати інтелектуальне автоматичне з'єднання. Якщо стався збій в роботі мережі WAN, то в якості запасної мережі для дзвінків використовується телефонна комутувана мережа загального користування PSTN. Таким чином, забезпечується надійність зв'язку між центральним офісом і локальними філіями.

AR з'єднують в собі служби голосового зв'язку, факс і Ір-послуги. Надаючи послуги передачі голосу для корпоративних користувачів, AR функціонують як SIP-шлюз філії і перетворює телефонні сигнали в VoIP-сигнали. Інтерфейси каналу вихідного зв'язку маршрутизатора AR з'єднані з мережею IMS / NGN з метою отримання будь-яких мультимедійних даних, контрі надходять будь-який час, наприклад, від телефонів, мобільних телефонів і комп'ютерів.

Маршрутизатори AR надають безпечний доступ для встановлення зв'язку між корпоративними філіями і між філіями і центральним офісом, а також надають партнерам доступ до корпоративних ресурсів. Такі канали, як мережі VPN по протоколах GRE і IPSEC, встановлені між центральним офісом і філіями і забезпечують безпечний доступ до інформації і передачу даних. AR виконують швидке розгортання каналу і аутентифікацію філій. Використання такого каналу

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						45
Зм.	Лист	№ документу	Підпис	Дата		

дозволяє партнерам отримувати доступ до корпоративних ресурсів і користуватися ними спільно. Також маршрутизатори AR надає користувачам послугу аутентифікації і авторизації.

Оскільки вони є обладнанням PE мережі MPLS, маршрутизатори AR розташовуються в центральному офісі та філіях підприємства. Різні види послуг поділяються на категорії за допомогою мережі MPLS L3 VPN. Маршрутизатори AR здійснюють гнучке розгортання, швидку розводку і безпечну передачу послуг VPN, а також підтримують обслуговування підприємств по мережах.

1.3.3 Характеристика мережевих продуктів компанії Cisco Systems

Продукти компанії Cisco оснащені вбудованими функціями безпеки, які забезпечують безпеку всієї мережі. Захист мережевих ресурсів стає прозорим, масштабованим і керованим компонентом будь-якої корпоративної інфраструктури. Cisco пропонує простий і масштабований шлях міграції до безпечних мережевих з'єднань для послуг IP. Крім базових принципів побудови безпечної мережі, відомих під назвою SAFE Blueprint, Cisco пропонує найсучасніші методи багаторівневої захисту критично важливих бізнес-процесів від внутрішніх і зовнішніх загроз.

В свою чергу компанія Cisco Systems пропонує ряд наступних рішень з інформаційної безпеки. У лінійку систем інформаційної безпеки цього виробника входять [11, 24]:

- ідентифікація та управління безпекою
- інтегровану мережева безпека
- технологія Cisco DMVPN

1) Мережеві послуги Cisco з ідентифікацією (Identity Based Networking Services – IBNS) представляють собою інтегроване рішення, до складу якого входить декілька продуктів Cisco, що забезпечують аутентифікацію, контроль доступу та дотримання встановлених для користувачів правил (user policies) в інтересах захисту мережевих з'єднань і ресурсів. Рішення Cisco IBNS не тільки підвищує загальний рівень безпеки, але і дозволяє більш економічно керувати

змiнами в масштабi всiєї органiзацiї. В результатi з'являється possibilitь оптимiзацiї управлiння великими мережами, пiдвищення продуктивностi i скорочення поточних витрат.

Пропонуючи пiдприємствам безпечну структуру IBNS для управлiння мобiльностю користувачiв i скорочення витрат, пов'язаних з доступом до мережевих ресурсiв, Cisco дозволяє пiдприємствам пiдвищити продуктивнiсть працi i скоротити поточнi витрати.

Рiшення Cisco IBNS дає цiлий ряд переваг: iнтелектуальнi possibiliti для бiльш гнучкої i мобiльної роботи з групами користувачiв, поєднання аутентифiкацiї, контролю доступу i призначених для користувача правил (user policies) для захисту мережевих з'єднань i ресурсiв, а також пiдвищення безпеки та гнучкостi доступу до бездротових й провiдних мереж, що дозволяє пiдприємствам швидко створювати мiжфункцiональнi i проектнi групи, надавати безпечний доступ партнерам i легше створювати безпечнi мережевi з'єднання для переговорних кiмнат i конференц-залiв.

2) Iнтеграцiя IP-послуг, а також функцiй маршрутизацiї та безпеки дозволяє компанiям створювати надiйну основу для подальшого розвитку своїх додаткiв i послуг. Замовники повиннi захищати критично важливи данi i системи i в той же час робити їх доступними для користування. Щоб вирiшити це протирiччя, компанiя Cisco розробила цiлий ряд нових платформ маршрутизацiї i допрацювала програмнi засоби, призначенi для пiдтримки безпечних IP-послуг.

Для малих вiддалених офiсiв i мобiльних співробітників створений новий широкосмуговий Ethernet-маршрутизатор Cisco 831 i новий широкосмуговий ADSL-маршрутизатор Cisco 837. Разом з Ethernet-маршрутизатором Cisco SOHO 91 i ADSL-маршрутизатором Cisco SOHO 97 вони будуть пiдтримувати високу продуктивнiсть, економiчность i надiйность мережевих з'єднань. Вбудованi функцiї мiжмережевих екранiв з урахуванням станiв (integrated stateful firewall) i послуги вiртуальних приватних мереж (VPN), а також шифрування з апаратним прискоренням i засоби управлiння дозволяють маршрутизаторам Cisco 831 i 837 надiйно пiдтримувати сучаснi високоякiснi послуги з передачi даних, голосу та вiдео. Широкосмуговi маршрутизатори Cisco SOHO 91 i 97 призначенi для пiдтримки простого i безпечного доступу в малих офiсах. Вони iдеально

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						47
Зм.	Лист	№ документу	Підпис	Дата		

підходять для широкосмугового середовища і також володіють вбудованими функціями міжмережевих екранів і віртуальних приватних мереж, а також найсучаснішими функціями управління, що дозволяє значно скоротити вартість володіння.

Платформи маршрутизації Cisco підтримують нові сучасні послуги безпеки, реалізовані на рівні операційної системи Cisco IOS, інтегровані з послугами IP-мереж і дозволяють передавати в віртуальних приватних мереж голос і відео з операторською якістю. До числа таких послуг відносяться: розширена функціональність QoS, сучасні функції маршрутизації на вимогу (on-demand meshing) і аварійне підхоплення IPSec з урахуванням станів. Все це дозволяє підвищувати надійність голосового зв'язку по каналах VPN. Додаткові послуги Cisco IOS для протоколу IPSec включають інтегровану підтримку шифрування за стандартом AES (Advanced Encryption Standard) і прозорість трансляції мережесих адрес (Network Address Translation - NAT), що підвищує можливості міжмережевої взаємодії.

3) Для побудови територіально розподілених мереж на поточний момент в більшості випадків використовуються віртуальні шифровані мережі поверх інтернету. Традиційний підхід побудови подібних мереж за допомогою простого шифрування трафіку методом IPsec в тунельному режимі вкрай не ефективний на рахунок складності настройки, неможливості використання динамічних протоколів маршрутизації, не працездатності multicast трафіку, і дуже поганої масштабованості. Додавання нових сайтів в таких мережах часто вимагає перенастроювання всіх вузлів, коригування величезного числа ACL, статичних маршрутів і т.д.

Для усунення вище сказаних недоліків компанія Cisco в своїх маршрутизаторах пропонує технологію Cisco DMVPN (Dynamic Multipoint VPN).

Детальна інформація про дану технологію наведена в 2 розділі дипломного проекту.

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						48
Зм.	Лист	№ документа	Підпис	Дата		

РОЗДІЛ 2 РОЗРОБКА ПРОЕКТУ ЗАХИЩЕНОЇ ГЕТЕРОГЕННОЇ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ МЕРЕЖІ.

2.1 Розробка проекту інформаційно-комунікаційної мережі.

Комп'ютерна мережа представляє собою набір вузлів – комп'ютерів та маршрутизаторів, що об'єднуються лініями зв'язку. Лінії зв'язку включають кабельні системи та мережеве обладнання. Для організації взаємодії в мережі використовуються прикладні програми, які мають клієнт-серверну архітектуру (Web-сервери і браузері, мережеві СУБД і т.д.).

Доцільність створення комп'ютерної мережі обумовлюється наступним [18]:

- можливістю використання територіально розподіленого програмного забезпечення, інформаційних баз даних і баз знань, які перебувають у різних користувачів;
- можливістю організації розподіленої обробки даних шляхом залучення ресурсів багатьох обчислювальних машин;
- оперативному перерозподілу навантаження між комп'ютерами, включеними в мережу і ліквідації пікового навантаження за рахунок перерозподілу її з урахуванням часових поясів;
- спеціалізацією окремих машин на роботі з унікальними програмами, які потрібні ряду користувачів мережі;
- колективізації ресурсів, особливо дорогого периферійного обладнання, яким економічно недоцільно укомплектовувати кожен ЕОМ.

Основні вимоги, що пред'являються до сучасних комп'ютерних мереж:

- простота експлуатації та доступу користувача до мережі;
- відкритість – можливість підключення різнотипних ЕОМ;
- розвиток – можливість нарощування ресурсів мережі і абонентів;
- автономність – робота користувача на своїй ЕОМ не повинна обмежуватися тим, що ЕОМ включена в мережу;

- інтегрованість – можливість обробки і передачі інформації різного виду: символної, графічної та ін.;
- захищеність – можливість запобігання несанкціонованого доступу до мережі;
- невеликий час відповіді забезпечує ефективну роботу користувача в діалоговому режимі відповідно до призначення мережі;
- безперервність роботи – можливість відключення і підключення компонентів мережі без переривання її роботи;
- завадостійкість – здатність достовірно передавати інформацію в умовах перешкод;
- висока надійність і прийнятна вартість послуг мережі.

Проаналізувавши вищесказані вимоги, можна зробити висновок, що до задач проектування інформаційно-комунікаційної мережі відносять наступні питання:

- 1) Проектування на апаратному рівні – вибір відповідного мережевого обладнання, проектування та монтаж кабельної системи, настройка інтелектуального обладнання;
- 2) Вибір транспортних протоколів котрі будуть використовуватися в мережі і підтримуватись всіма вузлами мережі. Задачі маршрутизації. Адресація вузлів мережі;
- 3) Проектування логічної структури мережі;
- 4) Проектування системи безпеки.

В даному розділі проведемо проектування на апаратному рівні, а саме оберемо яке обладнання нам потрібне розробку проекту інформаційно-комунікаційної мережі.

Мережа складається з Hub-маршрутизатора та Spoke-маршрутизаторів, які підключені до мережі Internet через порти FastEthernet. Між маршрутизаторами організована зовнішня незахищена мережа. Далі до кожного з маршрутизаторів підключені комутатори до яких підключена необхідна кількість робочих станцій.

Загальна топологія мережі зображена на рисунку 2.1.

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						50
Зм.	Лист	№ документа	Підпис	Дата		

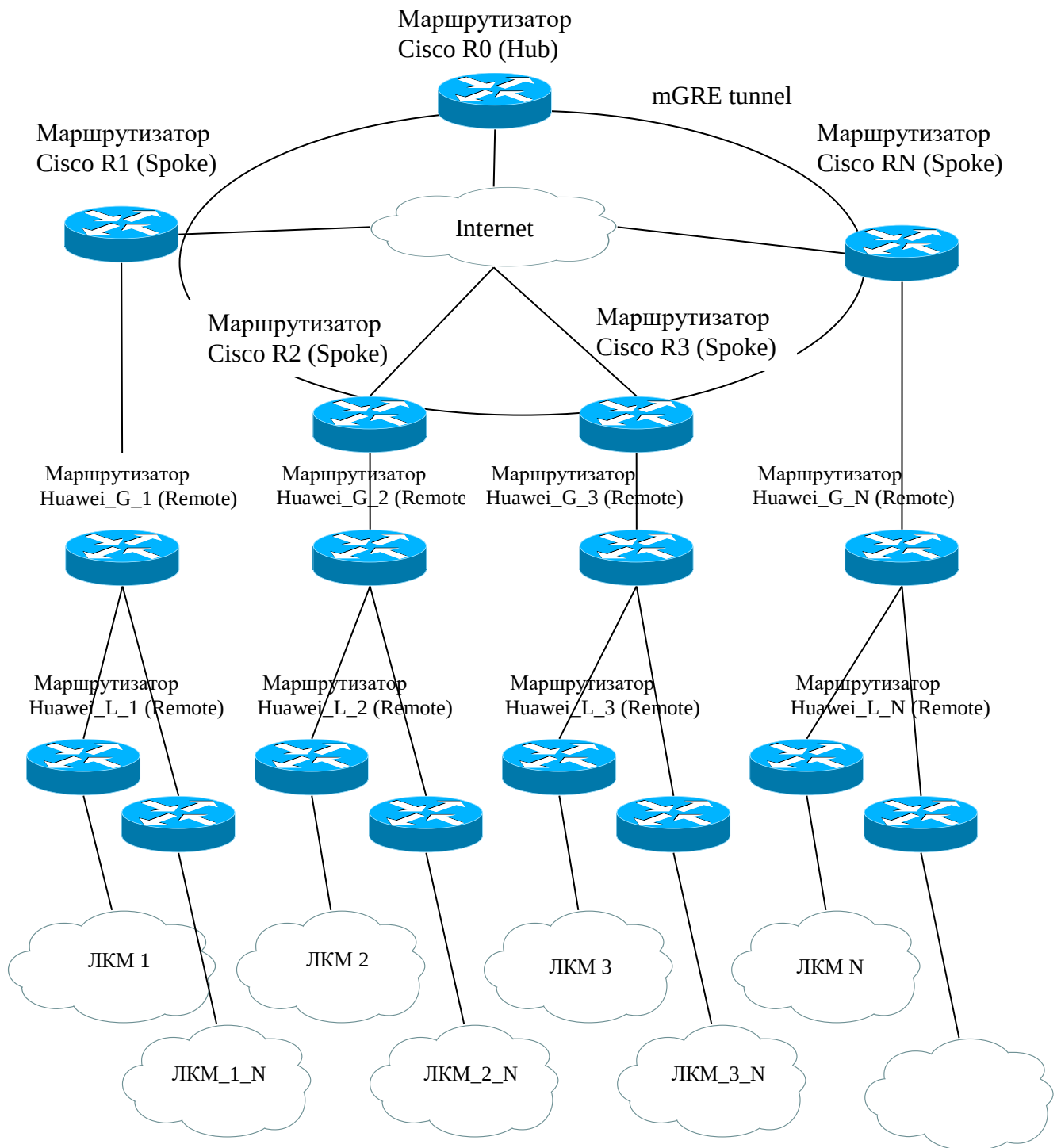


Рисунок 2.1 – Проект узагальненої топології мережі

Для даного дипломного проекту, проведемо налагодження лише частини мережі, зображеної на рисунку 2.1. Вибір частини мережі для проектування зумовлений тим, що інша, випущена з уваги частина мережі, схожа на обрану

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						51
Зм.	Лист	№ документа	Підпис	Дата		

частину та налаштовується аналогічно. Отже схема топології мережі, яку будемо проектувати наведена на рисунку 2.2.

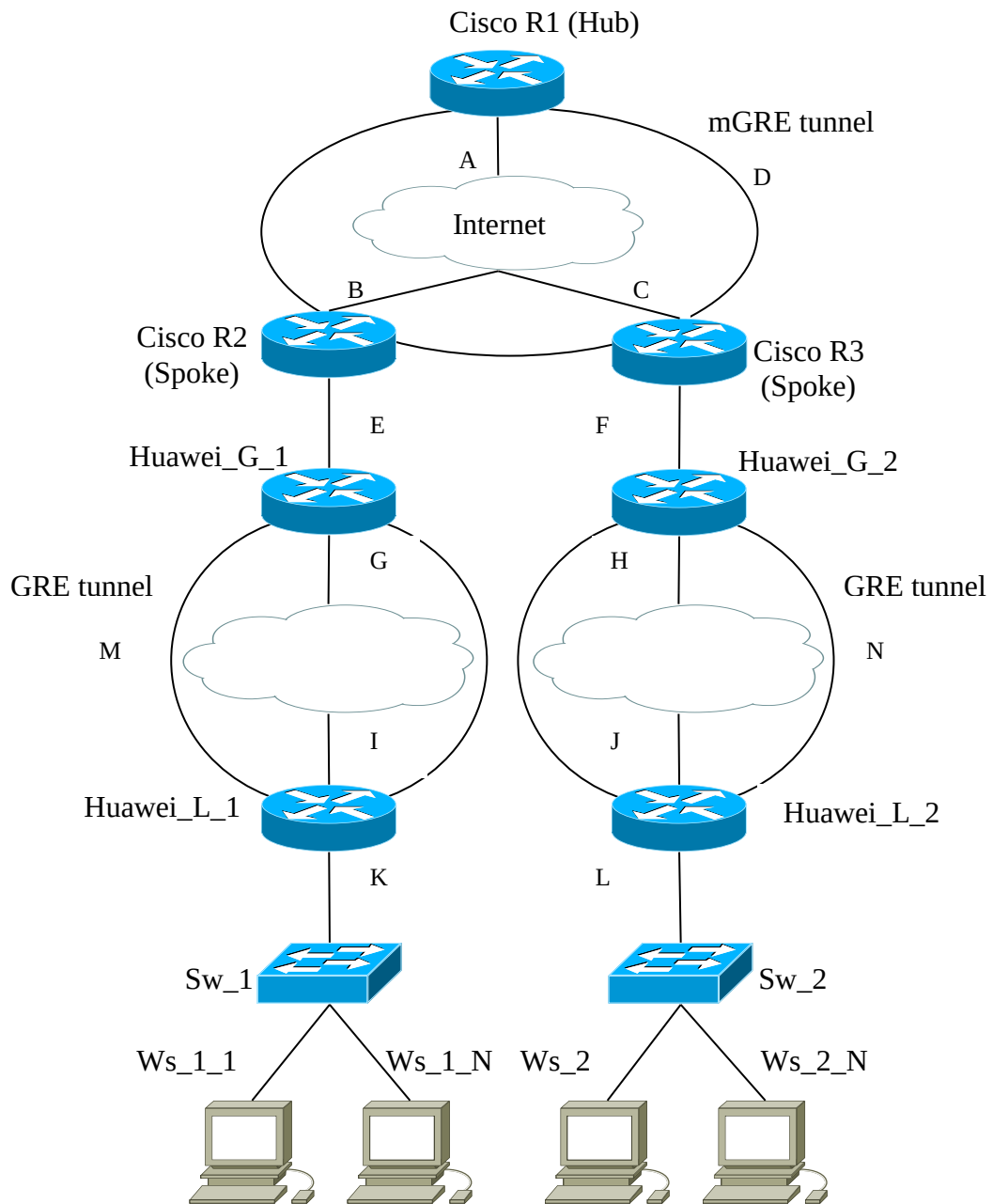


Рисунок 2.2 – Проект спрощеної топології мережі

Перейдемо до вибору адресації мереж вибраної топології.

2.2 Розробка схеми адресації інформаційно-комунікаційної мережі.

Для адресації маршрутизаторів між собою необхідно по 2 адреси в кожній підмережі. Тому доцільно використовувати адреси з масками 255.255.255.252. Всього таких під мереж буде 9.

Також, ще буде дві підмережі, в яких буде по 29 та 125 робочих станцій.

Отож узагальнена схема адресації вузлів мережі представлена в таблиці 2.1, а детальні схеми фізичної та логічної адресації вузлів мережі наведені в таблицях 2.2 та 2.3 відповідно.

Таблиця 2.1 – Узагальнена схема адресації мережі для спрощеного проекту

Підме режа	IP адреса мережі	Маска	Використовувані пристрої	Діапазон IP адрес вузлів
A	192.83.15.0	255.255.255.252	маршрутизатори	192.83.15.1- 192.83.15.2
B	192.83.35.0	255.255.255.252	маршрутизатори	192.83.35.1- 192.83.35.2
C	192.83.55.0	255.255.255.252	маршрутизатори	192.83.55.1- 192.83.55.2
D	10.83.5.0	255.255.255.248	маршрутизатори	10.83. 5.1- 10.83. 5.3
E	10.83.35.0	255.255.255.252	маршрутизатори	10.83.35.1- 10.83.35.2
F	10.83.55.0	255.255.255.252	маршрутизатори	10.83.55.1- 10.83.55.2
G	105.83.35.0	255.255.255.252	маршрутизатори	105.83.35.1- 105.83.35.2
H	105.83.55.0	255.255.255.252	маршрутизатори	105.83.45.1- 105.83.45.2
I	105.83.45.0	255.255.255.252	маршрутизатори	105.83.55.1- 105.83.55.2
J	105.83.65.0	255.255.255.252	маршрутизатори	105.83.65.1- 105.83.65.2
K	10.83.50.0	255.255.255.224	маршрутизатор	10.83.50.1
			робочі станції	10.83.50.2- 10.83.50.30
L	10.83.50.0	255.255.255.128	маршрутизатор	10.83.70.1
			робочі станції	10.83.70.2- 10.83.70.126

M	11.83.35.0	255.255.255.252	маршрутизатори	11.83.35.1- 11.83.35.2
N	11.83.55.0	255.255.255.252	маршрутизатори	11.83.55.1- 11.83.55.2

Таблиця 2.2 – Детальна схема фізичної адресації вузлів мережі для спрощеного проекту

Пристрій	Фізичний інтерфейс	Мережа	IP – адреса інтерфейсу	Маска підмережі	Шлюз
Dyn_83_5_1	Fa 0/0	192.83.15.0	192.83.15.1	255.255.255.252	-----
	Fa 0/1	10.83.15.0	10.83.15.1	255.255.255.252	10.83.15.2
Dyn_83_5_2	Fa 0/0	192.83.35.0	192.83.35.1	255.255.255.252	-----
	Fa 0/1	10.83.35.0	10.83.35.1	255.255.255.252	-----
Dyn_83_5_3	Fa 0/0	192.83.55.0	192.83.55.1	255.255.255.252	-----
	Fa 0/1	10.83.55.0	10.83.55.1	255.255.255.252	-----
Huawei_G_1	GE0/0/0	10.83.35.0	10.83.35.2	255.255.255.252	-----
	GE0/0/1	105.83.35.0	105.83.35.1	255.255.255.252	-----
Huawei_G_2	GE0/0/0	10.83.55.0	10.83.55.2	255.255.255.252	-----
	GE0/0/2	105.83.35.0	105.83.35.1	255.255.255.252	-----
Huawei_L_1	GE0/0/0	105.83.45.0	105.83.45.1	255.255.255.224	-----
	GE0/0/1	10.83.50.0	10.83.50.1	255.255.255.224	10.83.50.1
Huawei_L_2	GE0/0/0	105.83.65.0	105.83.65.1	255.255.255.252	-----
	GE0/0/1	10.83.70.0	10.83.70.1	255.255.255.128	10.83.70.1

Таблиця 2.3 – Детальна схема логічної адресації вузлів мережі для спрощеного проекту

Пристрій	Логічний інтерфейс	Мережа	IP – адреса інтерфейсу	Маска підмережі	Шлюз
Dyn_83_5_1	Tunnel 0	10.83.5.0	10.83.5.1	255.255.255.248	-----
Dyn_83_5_2	Tunnel 0	10.83.5.0	10.83.5.2	255.255.255.248	-----
Dyn_83_5_3	Tunnel 0	10.83.5.0	10.83.5.3	255.255.255.248	-----
Huawei_G_1	Tunnel 0/0/0	11.83.35.0	11.83.35.1	255.255.255.252	-----
Huawei_G_2	Tunnel 0/0/0	11.83.55.0	11.83.55.1	255.255.255.252	-----
Huawei_L_1	Tunnel 0/0/0	11.83.35.0	11.83.35.2	255.255.255.252	-----
Huawei_L_2	Tunnel 0/0/0	11.83.55.0	11.83.55.2	255.255.255.252	-----

2.3 Розробка підсистеми базового захисту інформаційно-комунікаційної мережі.

Маршрутизатор - це "перша лінія оборони" нашої мережі, яка безпосередньо підключена до Internet. Вони часто застосовуються в якості ключових елементів в системах захисту мереж (наприклад, firewall для фільтрації пакетів та обмеження проходження певного IP-трафіку). В даному дипломному проєкті, ми використовуємо обладнання фірм Cisco Systems та Huawei Technologies, які завдяки різній реалізації своїх "фірмових" операційних систем, можуть набути властивостей, необхідних нам як адміністраторам мережі.

Перед тим як вводити в дію кожен маршрутизатор, забезпечимо його захист, тобто зробимо все можливе для запобігання його використання не за призначенням як зловмисниками так і співробітниками підприємства.

Наша мережа розділена на декілька порівняно невеликих ділянок, кожен з яких можна розглядати окремо від інших.

- Ядро мережі відповідає за високошвидкісну передачу мережевого трафіку; первинне призначення пристрою, що входить в ядро мережі, полягає в комутації пакетів.

- На рівні розподілу (розподіл шару) відбувається підсумовування маршрутів і агрегація трафіку.

- Рівень доступу відповідає за формування мережевого трафіку, виконує контроль точок входу в мережу і надає інші служби прикордонних пристроїв.

Перед ядром мережі поставлена одна чітко сформульована задача - комутація пакетів (перемикання пакетів). Подібно двигуну, що працює на межі своїх можливостей, пристрої ядра не повинні відчувати ні найменшого недоліку в "паливі" і функціонувати в режимі пікової продуктивності. Можна сказати, що саме в ядрі мережі зосереджена вся її обчислювальна потужність. Нижче наведено дві основні стратегії, що дозволяють досягти максимальної продуктивності ядра мережі.

- У ядрі не повинні реалізовуватися мережеві правила.
- Кожен пристрій ядра повинен володіти можливістю доступу до кожного пункту призначення мережі.

Будь-яка форма реалізації мережевих правил повинна бути винесена за межі ядра мережі. Найбільш вдалим прикладами такої реалізації є фільтрація пакетів і маршрутизація за правилами. Навіть у тому випадку, коли пристрої ядра можуть фільтрувати і передавати пакети з високою швидкістю, ці функції мають бути винесені за межі ядра. Основне завдання ядра мережі - комутація пакетів, і все, що забирає обчислювальні ресурси пристроїв ядра або збільшує затримку комутації пакетів, має розглядатися як загроза продуктивності всієї мережі.

Крім цього, слід уникати збільшення складності конфігурації маршрутизаторів ядра. Посудіть самі: одна справа - допустити помилку при реалізації мережевих правил на рівні доступу до мережі, що може призвести до втрати з'єднання з певною групою користувачів, і зовсім інша - помилитися при внесенні змін до мережеві правила маршрутизаторів ядра, що може викликати вихід з ладу всієї мережі.

Пристрої ядра повинні володіти достатньою інформацією про маршрути для проведення інтелектуальної комутації пакета, призначеного для будь-якого кінцевого пристрою мережі; маршрутизатори ядра не повинні використовувати стандартні маршрути для досягнення внутрішніх пунктів призначення. Слід зазначити: сказане вище зовсім не означає, що маршрутизатор ядра повинен володіти відомостями про маршрут до кожної окремої підмережі. Для зменшення розмірів таблиці маршрутизації ядра можуть і повинні використовуватися сумарні маршрути. Стандартні ж маршрути слід використовувати для досягнення зовнішніх пунктів призначення, таких, наприклад, як вузли в Internet.

Для безпеки пристроїв ядра, будемо використовувати технологію Cisco DMVPN - динамічна багатоточкова віртуальна приватна мережа (DMVPN) – рішення на основі Cisco IOS Software для створення масштабованих віртуальних приватних мереж (VPN), захищених на рівні IP-протоколу. Вона використовує централізовану архітектуру для полегшення впровадження та управління

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						56
Зм.	Лист	№ документа	Підпис	Дата		

розгортанням, яке необхідне для розмежування контролю доступу різних груп користувачів і співробітників: у тому числі мобільних, комутованих і користувачів зовнішніх мереж. Також, вона дозволяє філіальним структурам підприємств підтримувати зв'язок один з одним безпосередньо, використовуючи Інтернет. При цьому між сайтами не потрібно підтримувати постійне підключення до VPN. Це дозволяє звести до мінімуму розгортання захищених каналів VPN і покращує продуктивність мережі за рахунок скорочення часу затримки і коливань під час оптимізації використання смуги пропускання.

Технологія DMVPN базується на наступних базових принципах:

- топологія Hub & Spoke;
- віртуальна L2 підмережа на базі point-to-multipoint інтерфейсів mGRE;
- шифрування проходжуваного GRE трафіку за допомогою IPsec;
- використання динамічної маршрутизації.

Технологія mGRE (multipoint GRE) базується на змінній GRE інкапсуляції з додаванням додаткових 4-ох байтів, а також технології NHRP (Next hop resolution protocol). На відміну від класичного point-to-point GRE – віртуальний інтерфейс mGRE працює аналогічно інтерфейсу point-to-multipoint Frame Relay. Тим самим дозволяючи в рамках однієї L2 мережі об'єднати багато пристроїв. NHRP в свою чергу є супутнім механізмом, що дозволяє встановити відповідність між реальними фізичними IP адресами маршрутизаторів, і їх віртуальними тунельними адресами. Маршрутизатори можуть виступати в ролі NHRP серверів, і NHRP клієнтів. Першими є Hub-маршрутизатори. Вони вибудовують динамічну таблицю відповідності реальних і віртуальних адрес у міру реєстрації Spoke-маршрутизаторів. І поширюють цю інформацію по всіх Spoke-маршрутизаторах.

Шифрування проходжуваних GRE пакетів реалізується за допомогою IPsec.

Основна мета побудови мережі на базі віртуальних інтерфейсів GRE – отримати можливість використовувати протоколи динамічної маршрутизації для поширення інформації про маршрути та здійснення відмовостійкості. В даному випадку Cisco настійно рекомендує протокол EIGRP. Основні принципи настройки класичні: не розтягувати процес маршрутизації ширше DMVPN хмаринки, використовувати по можливості режим Stub в spoke-вузлах з метою

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						57
Зм.	Лист	№ документу	Підпис	Дата		

виключення проходження транзитного трафіку через них, використовувати суммарізацію маршрутів.

Логічно DMVPN може бути реалізований в 2-х варіантах:

– Spoke-to-spoke deployment. У цьому випадку на всіх маршрутизаторах віртуальні інтерфейси налаштовуються у режимі mGRE. В результаті з точки зору передачі даних ми отримуємо full mesh мережу, в якій unicast трафік між spoke-вузлами йде безпосередньо по динамічно встановлюються канали. Для побудови динамічного тунелю spoke використовує отриману від hub-сайту NHRP таблицю. При цьому постійно підтримуються і беруть участь в динамічній маршрутизації тільки тунелі до Hub-вузлів.

В результаті ми маємо систему з наступними перевагами:

- простота і наочність налаштування;
- ефективна масштабованість. Додавання нового вузла – проста типова процедура;
- повноцінна full mesh топологія з точки зору передачі даних при помірному обсязі службового трафіку.

До загальних переваги DMVPN належать:

- підтримка протоколів маршрутизації, що забезпечує резервування каналів передачі даних і можливість балансування навантаження мережевого трафіку;
- спрощене управління VPN за допомогою єдиного multipoint-тунелю, взаємодія з багатьма віддаленими офісами (point-to-multipoint, broadcast);
- підтримка Multicast-трафіку з деякими обмеженнями (тільки Hub маршрутизатор може реплікувати Multicast-потік на Site-маршрутизатори).

Недоліком DMVPN є :

- часта Spoke-to-Spoke взаємодія, може стати результатом постійної ініціалізації IKE-сесій між Spoke-маршрутизаторами і, в результаті, негативно позначитися на пропускній здатності каналу передачі даних.

Перед рівнем розподілу мережі поставлено три чітко сформульовані завдання.

- Ізоляція наслідків зміни топології.
- Управління розміром таблиці маршрутизації.

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						58
Зм.	Лист	№ документу	Підпис	Дата		

- Агрегація мережевого трафіку.

Для досягнення цих цілей використовуються дві основні стратегії, що реалізуються на рівні розподілу.

- Підсумовування маршрутів.
- Мінімізація числа каналів, що з'єднують рівень розподілу з ядром мережі.

Рівень розподілу відповідає за агрегацію мережевого трафіку. Агрегація досягається за рахунок об'єднання трафіку, що надходить по великому числу низькошвидкісних каналів передачі інформації, що пов'язують рівень розподілу з пристроями рівня доступу, в декілька широкосмугових каналів, що зв'язують рівень розподілу з ядром мережі. Подібна стратегія породжує в мережі ефективні точки підсумовування і зменшує кількість маршрутів, яке повинні приймати до уваги маршрутизатори ядра при ухваленні рішення про комутації пакетів. Більш докладно значимість такого підходу розглядається в розділі 3, "Надмірність в ієрархічних мережах".

Перед рівнем доступу мережі поставлено три основні завдання.

- Формування мережевого трафіку.
- Контроль доступу до мережі.
- Виконання інших функцій прикордонних пристроїв.

Пристрої рівня доступу з'єднують високошвидкісні канали локальних мереж з каналами глобальної мережі, несучими трафік на рівень розподілу. Пристрої рівня доступу є видимою частиною мережі, саме вони асоціюються у більшості замовників з поняттям "мережа".

Слід обов'язково переконатися в тому, що трафік, сформований на рівні доступу мережі, не перевантажує канал, що з'єднує рівень доступу з рівнем розподілу. Незважаючи на те що це завдання вирішується головним чином на етапі визначення пропускної здатності каналу передачі інформації, вона має відношення до розташування пари "сервер-служба" та фільтрації пакетів. Трафік, не призначений для вузла за межами локальної мережі, не повинен передаватися пристроєм рівня доступу.

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						59
Зм.	Лист	№ документа	Підпис	Дата		

На рівні доступу в нашій мережі будуть функціонувати маршрутизатори компанії Huawei, і для забезпечення їх надійного функціонування, будемо використовувати GRE тунелі та протокол IKE.

Тунелі GRE загалом конфігуруються між джерельним маршрутизатором і маршрутизатором призначення, так що пакети, призначені для пересилання крізь тунель (вже форматовані із інкапсуляцією даних у заголовок “звичайного” пакету, визначеного протоколом), інкапсулюються з новим заголовком (заголовком GRE) і поміщаються в тунель з адресою призначення до кінцевого пункту тунелю (нового наступного стрибка). Коли пакет досягає кінцевий пункт тунелю, заголовок GRE видаляється і пакет пересилається до призначення, як вказано в заголовку оригінального IP-пакету.

IKE (Internet Key Exchange) - стандартний протокол IPsec, що використовується для забезпечення безпеки взаємодії у віртуальних приватних мережах. Призначення IKE - захищене узгодження та доставка ідентифікованого матеріалу для асоціації безпеки (SA).

IPSec SA можна налаштувати вручну. Однак, коли кількість вузлів в мережі збільшується, то важко виконувати ручну конфігурацію і забезпечувати безпеку мережі. У цьому випадку, ми будемо використовувати IKE протокол для автоматичного налаштування SA і обміну ключами.

IKE має механізм самозахисту, тому він може безпечно поширювати ключі, ідентифікатори аутентифікації і створювати IPSec SA навіть в незахищених мережах.

Механізми захисту IKE:

Обмін та спільний розподіл ключів Діффі-Хеллмана (DH). Обидві сторони зв'язку можуть обмінюватися даними без передачі загального ключа і знайти спільний ключ розрахунковим шляхом. Передумовою для шифрування є те, що обидві сторони повинні мати ключ. Заслуга IKE в тому, що даний протокол ніколи не передає загальний ключ безпосередньо по незахищених мережах, а обчислює загальний ключ шляхом обміну серією даних. Навіть якщо третя

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						60
Зм.	Лист	№ документу	Підпис	Дата		

сторона (наприклад, хакер) фіксує всі обміни даними, що використовуються для розрахунку загального ключа, третя сторона не може з'ясувати реальний ключ.

Після того, як генерується загальний ключ, особисті дані передаються в зашифрованому вигляді.

2.4 Розробка додаткових засобів захисту інформаційно-комунікаційної мережі.

Для забезпечення додаткової безпеки маршрутизаторів, була розроблена підсистема захисту, яка включає наступні елементи:

- парольний доступ для підключення по консолі;
- парольний доступ для підключення по телнету;
- забезпечення захисту для паролів в конфігурації;
- запобігання поширення інформації про користувачів;
- запобігання поширення інформації про маршрутизатор на сусідні пристрої:
- запобігання атак на сервіс NTP;
- перешкоджання використанню маршрутизаторів для smurf атак;
- виявлення і видалення "завислих" сесій, звільняючи використовувані VTY;
- відкидання IP пакетів, в яких включена опція source routing.

Таким чином зловмисник не зможе отримати назад відповідь на надісланий пакет, якщо він використовував підроблену IP адресу.

Також додатковими засобами є налаштування Radius сервера, DHCP сервера та парольного доступу по ssh до маршрутизаторів Huawei.

Отже при виконанні даного розділу було розроблено проекти узагальненої та спрощеної топології інформаційно-комунікаційної мережі та визначена необхідна кількість маршрутизаторів комутаторів та робочих станцій.

Також було розроблено проекти узагальненої та детальної фізичної та логічної схем адресації мережі для спрощеного проекту та проект підсистеми захисту інформаційно-комунікаційної мережі.

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						61
Зм.	Лист	№ документа	Підпис	Дата		

РОЗДІЛ 3 ОБГРУНТУВАННЯ ВИБОРУ ТА НАЛАГОДЖЕННЯ ОБЛАДНАННЯ ЗАХИЩЕНОЇ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ МЕРЕЖІ.

3.1 Обґрунтування вибору апаратного та програмного забезпечення

3.1.1 Обґрунтування вибору апаратного забезпечення

В даній частині дипломного проекту необхідно обрати та обґрунтувати свій вибір мережевого обладнання для побудови захищеної інформаційно-комунікаційної мережі.

Для початку визначимо, які типи обладнання будемо використовувати при побудові топології мережі, яку будемо проектувати:

- маршрутизатори Cisco – підтримка протоколів маршрутизації EIGRP та RIP version 2, наявність портів FastEthernet.
- маршрутизатори Huawei – підтримка протоколу маршрутизації RIP, наявність портів FastEthernet/GigabitEthernet;
- комутатори – з оптимальною кількістю портів, що здатні забезпечити з'єднання між маршрутизатором робочими станціями без перенавантаження мережі, підтримка мереж Ethernet;
- робочі станції – ПК з підтримкою операційної системи Windows XP.

Враховуючи вимоги до обладнання обираємо наступні пристрої:

- маршрутизатори Cisco 3925 Security Bundle w/SEC license PAK;
- Маршрутизатор AR3260 Routers AR0M0036SA00
- комутатори Linksys Gigabit 5-Port Workgroup Switch;
- комутатори Cisco 24 port 10/100/1000;

Детальні характеристики кожного з пристроїв наведені в додатку А.

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						62
Зм.	Лист	№ документа	Підпис	Дата		

3.1.2 Обґрунтування вибору програмного забезпечення

Обране апаратне забезпечення компаній Cisco Systems та Huawei Technologies передбачає використання операційні системи Cisco IOS та VRP відповідно. Розглянемо переваги кожної з них.

Програмне забезпечення Cisco IOS (Internetwork Operating System) Software – це операційна система, що забезпечує функціонування активного мережевого обладнання Cisco, на основі якого побудовано багато великих корпоративних мереж. Ця операційна система підтримує [12, 13]:

- Широкий спектр мережевих протоколів;
- Інтеграцію даних, голосу та відео у рамках єдиної IP мережі;
- Механізми забезпечення якості обслуговування (QoS);
- Засоби забезпечення безпеки;
- Багатоадресні розсилки (IP multicast);
- Засоби управління.

Cisco IOS підтримує маршрутизовані протоколи, до яких відносяться: IP версії 4, IP версії 6, IPX, AppleTalk, OSI, SNA, DECnet, VINES, XNS та ін.. Крім цього вона дозволяє проводити настройку практично всіх відомих протоколів маршрутизації, таких як: RIP, IGRP, EIGRP, OSPF, IS-IS, BGP, протоколів маршрутизації багатоадресного трафіку і ін..

Програмне забезпечення Cisco IOS підтримує багато механізмів мережевої безпеки, таких як міжмережеві екрани, системи виявлення мережевих атак, віртуальні приватні мережі (VPN - Virtual Private Network) та ін.. Основні механізми забезпечення мережевої безпеки включають в себе:

- списки контролю доступу (ACL) для пакетної фільтрації трафіку;
- засоби безпечного адміністрування, які підтримують протоколи SSH, SNMPv3 і HTTPS, що забезпечують шифрування каналів управління, та інструменти управління і моніторингу SDM і Autosecure;

– централізовану аутентифікацію, авторизацію і облік адміністративної діяльності, віддаленого доступу і підключень до мережі за допомогою протоколів RADIUS і TACACS +;

– стек протоколів IPSec;

– Cisco IOS Firewall - контекстний міжмережевий екран, який забезпечує контроль трафіку на прикладному рівні (CBAC - Context-based Access Control), виявлення мережевих атак, в тому числі атак типу "відмова в обслуговуванні" (DoS - Denial of Service), блокування Java-апплетів і підтримку VPN.

За час свого існування Cisco IOS кілька разів істотно модернізувалася, і її удосконалення триває і зараз. У переважній більшості сучасних пристроїв застосовується Cisco IOS версій 11 або 12. Причому для кожної моделі пристрою існує унікальний варіант Cisco IOS, який зберігається у вигляді архівного двійкового файлу з розширенням .bin.

Починаючи з версії 12.3, програмне забезпечення Cisco IOS, поставляється у вигляді наступних восьми основних пакетів:

- 1) IP Base - пакет початкового рівня;
- 2) IP Voice - забезпечує підтримку IP телефонії, VoIP, VoFR;
- 3) Advanced Security - підтримує Cisco IOS Firewall, IDS, SSH, IPSec VPN, 3DES;
- 4) Enterprise Base - підтримує різні маршрутизовані протоколи та мережі IBM;
- 5) SP Services - додатковий модуль до IP Voice для підтримки NetFlow, SSH, ATM, VoATM, MPLS;
- 6) Enterprise Services - додатковий модуль до Enterprise Base, призначений для підтримки Service Provider (SP) Services, а також повну підтримку мереж IBM;
- 7) Advanced IP Services - додатковий модуль до SP Services, що включає підтримку Advanced Security і IPv6;
- 8) Advanced Enterprise Services - включає в себе максимальні можливості Cisco IOS Software.

Чотири перші пакета призначені для мереж, в яких здійснюється передача даних з інтеграцією голосу, забезпечується безпека і використовуються різні

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						64
Зм.	Лист	№ документу	Підпис	Дата		

маршрутизовані протоколи (IP, IPX, AppleTalk та ін.). Три додаткових модуля призначені для розширення функцій перших чотирьох пакетів. Пакет Advanced Enterprise Services об'єднує всі функції попередніх, забезпечуючи максимальну функціональність Cisco IOS.

Мережева операційна платформа VRP розроблена компанією Huawei для обладнання передачі даних – серії маршрутизаторів Quidway, магістрального комутатора ATM Radium, серії LAN-комутаторів Quidway S і сервера доступу Quidway A8010. Мережева операційна платформа VRP є інтелектуальною власністю компанії Huawei. Для забезпечення користувачів гнучкими і різноманітними рішеннями, VRP має можливість функціонувати на будь-якій платформі апаратного забезпечення. Мережева операційна платформа здатна до постійного вдосконалення і забезпечує максимальний захист капіталовкладень користувачів. Основним елементом платформи VRP є послуги IP, на базі яких формується структура, що володіє 300 різними характеристиками. Крім великого числа можливостей платформа забезпечує широкий масштаб застосування, базуючись на побажаннях і вимогах замовників.

За допомогою стека протоколів TCP/IP, платформа VRP реалізує функції різноманітних протоколів на рівні каналів даних, на мережевому рівні і на прикладному рівні. Операційна система об'єднує такі технології передачі даних як маршрутизацію, QoS, VPN, безпека і голос поверх IP (VoIP). Платформа VRP забезпечує мережеве обладнання відмінною функцією передачі даних, заснованої на технології передачі IP-пакетів – TurboEngine. До архітектури VRP входять: IP voice services - мовні послуги IP, System services - системні служби, Routing policy management - управління маршрутизацією, Configuration management - управління конфігурацією, Command line - командний рядок, IP forwarding engine - пересилання IP пакетів, Fast forwarding - швидка пересилання, IP security and firewall - IP безпеку і брандмауер, Web mgmt - управління через web-інтерфейс

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						65
Зм.	Лист	№ документу	Підпис	Дата		

- Технологія передачі IP-пакетів TurboEngine: включає послуги передачі пакетів IP, швидкісну передачу пакетів IP, QoS, маршрутизацію, безпеку і брандмауер.
- Взаємодія WAN (глобальна мережа): підтримує послуги PPP/MP, SLIP, HDLC/SDLC, X.25, Frame Relay, LAPB, ISDN і Ethernet.
- Протокол маршрутизації: підтримує протоколи RIP, OSPF, BGP, IGRP і EIGRP.
- IP послуга: підтримує послуги ARP/Proху ARP, NAT, DNS, DHCP relay, VLAN, SNA, VoIP і VPN.
- Управління конфігурацією: інтерфейс командного рядка, запис аварійних повідомлень, виведення інформації про налагодження, управління SNMP.

3.2 Базове налагодження апаратного та програмного забезпечення.

Проведемо базові налаштування елементів мережі:

Налаштування зовнішніх інтерфейсів маршрутизаторів

Dyn_83_5_1(config)#interface f0/0

Dyn_83_5_1(config-if)# ip address 192.83.15.1 255.255.255.252

Dyn_83_5_1(config-if)# no shutdown

Dyn_83_5_2(config)#interface f0/0

Dyn_83_5_2(config-if)# ip address 192.83.35.1 255.255.255.252

Dyn_83_5_2(config-if)# no shutdown

Dyn_83_5_3(config)#interface f0/0

Dyn_83_5_3(config-if)# ip address 192.83.55.1 255.255.255.252

Dyn_83_5_3(config-if)# no shutdown

[Huawei_Global_1]interface GigabitEthernet0/0/1

[Huawei_Global_1-GigabitEthernet0/0/1]ip address 105.83.35.1 30

[Huawei_Global_2]interface GigabitEthernet0/0/2

[Huawei_Global_2-GigabitEthernet0/0/2]ip address 105.83.55.1 30

[Huawei_Local_1]interface GigabitEthernet0/0/0

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						66
Зм.	Лист	№ документа	Підпис	Дата		

[Huawei_Local_1-GigabitEthernet0/0/0]ip address 105.83.45.1 30

[Huawei_Local_2]interface GigabitEthernet0/0/0

[Huawei_Local_2-GigabitEthernet0/0/0]ip address 105.83.65.1 30

Налаштування внутрішніх інтерфейсів маршрутизаторів

Dyn_83_5_2(config)#interface f0/1

Dyn_83_5_2(config-if)# ip address 10.83.35.1 255.255.255.252

Dyn_83_5_2(config-if)# no shutdown

Dyn_83_5_3(config)#interface f0/1

Dyn_83_5_3(config-if)# ip address 10.83.55.1 255.255.255.252

Dyn_83_5_3(config-if)# no shutdown

[Huawei_Global_1]interface GigabitEthernet0/0/0

[Huawei_Global_1-GigabitEthernet0/0/0]ip address 10.83.35.2 30

[Huawei_Global_2]interface GigabitEthernet0/0/0

[Huawei_Global_2-GigabitEthernet0/0/0]ip address 10.83.55.2 30

[Huawei_Local_1]interface GigabitEthernet0/0/1

[Huawei_Local_1-GigabitEthernet0/0/1]ip address 10.83.50.1 27

[Huawei_Local_2]interface GigabitEthernet0/0/1

[Huawei_Local_2-GigabitEthernet0/0/1]ip address 10.83.70.1 25

У даному дипломному проєкті на маршрутизаторах Dyn_83_5_1-
Dyn_83_5_3 прописані статичні маршрути до мереж зовнішніх інтерфейсів інших
маршрутизаторів.

Налаштування статичних маршрутів на на hub та spoke-маршрутизаторах:

Dyn_83_5_1(config)# ip route 192.83.35.0 255.255.255.252 192.83.15.2

Dyn_83_5_1(config)# ip route 192.83.55.0 255.255.255.252 192.83.15.2

Dyn_83_5_2(config)# ip route 192.83.15.0 255.255.255.252 192.83.35.2

Dyn_83_5_2(config)# ip route 192.83.55.0 255.255.255.252 192.83.35.2

Dyn_83_5_3(config)# ip route 192.83.35.0 255.255.255.252 192.83.55.2

Dyn_83_5_3(config)# ip route 192.83.55.0 255.255.255.252 192.83.55.2

Проведемо налаштування протоколу маршрутизації RIP на
маршрутизаторах Huawei:

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						67
Зм.	Лист	№ документа	Підпис	Дата		

```
[Huawei_Global_1]rip
```

```
[Huawei_Global_1-rip-1]network 10.0.0.0
```

```
[Huawei_Global_1-rip-1]network 105.0.0.0
```

Наведені параметри налаштування маршрутизації RIP тільки на маршрутизаторі Huawei_Global_1, оскільки на інший маршрутизаторах команди налаштування аналогічні.

3.3 Базові налаштування безпеки маршрутизаторів

3.3.1 Налаштування mGRE-тунелів, протоколу NHRP, та протоколу маршрутизації EIGRP на маршрутизаторах Cisco

Проведемо налаштування multipoint GRE-тунелів:

В використовуваній нами топології, а саме «Зірка» (hub-n-spoke) будемо використовувати multipoint GRE (mGRE) тунель, який дозволяє термінувати на собі кілька GRE-тунелів. mGRE-тунель також дозволяє одному GRE-інтерфейсу підтримувати кілька IPsec-тунелів і спрощує кількість і складність налаштувань, в порівнянні з GRE-тунелями.

Крім того, mGRE-інтерфейс дозволяє використовувати динамічно призначені IP-адреси на spoke-маршрутизаторах.

Для адресації тунелів виділена мережа 10.83.5.0/29, всі тунелі знаходяться в одній мережі. На hub-маршрутизаторі і spoke-маршрутизаторах mGRE-тунелі налаштовуються аналогічно (отже приведемо приклад тільки для для hub-маршрутизатора).

Створення тунельного інтерфейсу:

```
Dyn_83_5_1 (config) # interface Tunnel0
```

Задання IP-адреси на інтерфейсі:

```
Dyn_83_5_1(config-if) # ip address 10.83.5.1 255.255.255.248
```

Так як GRE додає додаткові заголовки до IP-пакету, необхідно змінити значення MTU на інтерфейсі:

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						68
Зм.	Лист	№ документу	Підпис	Дата		

Dyn_83_5_1(config-if) # ip mtu 1416

В якості адреси відправника в пакеті, що виходить з mGRE-інтерфейсу буде використовуватися IP-адреса фізичної інтерфейсу, а адреса одержувача буде вивчена динамічно за допомогою протоколу NHRP.

Налаштування відповідності між тунельним інтерфейсом і фізичним:

Dyn_83_5_1(config-if) # tunnel source FastEthernet 0/0

Включення mGRE-тунелю:

Dyn_83_5_1(config-if) # tunnel mode gre multipoint

Завдання ключа, який ідентифікує тунель, але його можна і не задавати:

Dyn_83_5_1(config-if) # tunnel key 555

Проведемо налаштування NHRP протоколу. Next Hop Resolution Protocol (NHRP) – клієнт-серверний протокол перетворення адрес, що дозволяє всім хостам, які знаходяться в NBMA (Non Broadcast Multiple Access)-мережі, динамічно вивчити NBMA-адреси (фізичні адреси) один одного звертаючись до next-hop-серверу (NHS). Після цього хости можуть обмінюватися інформацією один з одним безпосередньо.

У мережі DMVPN:

- Hub-маршрутизатор буде працювати як NHS, а spoke-маршрутизатори будуть клієнтами;

- Hub-маршрутизатор зберігає та обслуговує базу даних NHRP, в якій зберігаються відповідності між фізичними адресами та адресами mGRE-тунелів spoke-маршрутизаторів;

- На кожному spoke-маршрутизаторі hub-маршрутизатор статично вказаний як NHS і задано відповідність між фізичною адресою та адресою mGRE-тунелю hub-маршрутизатора;

- При включенні кожен spoke-маршрутизатор реєструється на NHS і, при необхідності, може вимагати у сервера інформацію про адреси інших spoke-маршрутизаторів для побудови spoke-to-spoke тунелів;

- Network ID - характеристика локальна для кожного маршрутизатора. Різні інтерфейси можуть брати участь в різних NHRP сесіях; це просто розмежувач

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						69
Зм.	Лист	№ документу	Підпис	Дата		

того, що сесія NHRP на одному інтерфейсі не та що на іншому. Відповідно, абсолютно не обов'язково, щоб Network ID збігалися на різних маршрутизаторах.

Налаштування на hub- та spoke-маршрутизаторах відрізняються, то приведемо приклади кожного з них:

Налаштування NHRP на hub-маршрутизаторі:

Включення NHRP на інтерфейсі:

```
Dyn_83_5_1 (config) # interface Tunnel0
```

```
Dyn_83_5_1 (config-if) # ip nhrp network-id 555
```

Hub-маршрутизатор буде автоматично додавати відповідності між адресами spoke-маршрутизаторів:

```
Dyn_83_5_1 (config-if) # ip nhrp map multicast dynamic
```

Налаштування аутентифікації, але її можна і не використовувати:

```
Dyn_83_5_1 (config-if) # ip nhrp authentication zhenya
```

Налаштування NHRP на spoke-маршрутизаторах:

Включення NHRP на інтерфейсі:

```
Dyn_83_5_3 (config) # interface Tunnel0
```

```
Dyn_83_5_3 (config-if) # ip nhrp network-id 555
```

Адреса тунельного інтерфейсу hub-маршрутизатора вказується як next-hop-сервер:

```
Dyn_83_5_3 (config-if) # ip nhrp nhs 10.83.5.1
```

Статична відповідність між адресою mGRE-тунелю і фізичною адресою hub-маршрутизатора (перша адреса - адреса тунельного інтерфейсу, друга - адреса зовнішнього фізичного інтерфейсу):

```
Dyn_83_5_3 (config-if) # ip nhrp map 10.83.5.1 192.83.15.1
```

Адреса зовнішнього фізичного інтерфейсу hub-маршрутизатора вказується як одержувач multicast-пакетів від локального маршрутизатора:

```
Dyn_83_5_3 (config-if) # ip nhrp map multicast 192.83.15.1
```

Налаштування аутентифікації:

```
Dyn_83_5_3 (config-if) # ip nhrp authentication zhenya
```

Налаштування прапора «не унікальності» ір-адреси тунелю в базі nhrp на hub-маршрутизаторі (його також можна не використовувати):

Dyn_83_5_3 (config-if) # ip nhrp registration no-unique

Якщо зміниться зовнішня адреса spoke-маршрутизатора і цієї команди не буде, то hub-маршрутизатор не відновить свою базу nhrp через помилку: unique address registered already

Перевіримо роботу mGRE-тунелю та протокола NHRP за допомогою команди show ip interface brief

```
Dyn_83_5_1#show ip int brief
Interface      IP-Address      OK? Method Status      Prot
o0c01
FastEthernet0/0      192.83.15.1      YES manual up          up
FastEthernet0/1      10.83.15.1       YES manual up          up
Tunnel0             10.83.5.1        YES manual up          up

Dyn_83_5_2#show ip int brief
Interface      IP-Address      OK? Method Status      Prot
o0c01
FastEthernet0/0      192.83.35.1      YES manual up          up
FastEthernet0/1      10.83.35.1       YES manual up          up
Tunnel0             10.83.5.2        YES manual up          up

Dyn_83_5_3#show ip int brief
Interface      IP-Address      OK? Method Status      Prot
o0c01
FastEthernet0/0      192.83.55.1      YES manual up          up
FastEthernet0/1      10.83.55.1       YES manual up          up
Tunnel0             10.83.5.3        YES manual up          up
```

Рисунок 3.1 – Результат виконання команди show ip interface brief на маршрутизаторах

Проведемо перевірку NHRP на hub- та spoke-маршрутизаторах (Dyn_83_5_1 та Dyn_83_5_2 відповідно) за допомогою команд: show ip nhrp nhs (інформація про NHS), show ip nhrp brief, show ip nhrp (детальна інформація про інші маршрутизатори отримана по NHRP:), show ip nhrp multicast (одержувач multicast-трафіку), show ip nhrp summary (сумарна інформація про записи NHRP), show ip nhrp traffic (статистика по пакетах NHRP)

```

Dyn_83_5_1#show ip nhrp brief
      Target      Via      NBMA      Mode  Intfc  Claimed
10.83.5.2/32      10.83.5.2      192.83.35.1  dynamic  Tu0    <    >
10.83.5.3/32      10.83.5.3      192.83.55.1  dynamic  Tu0    <    >
Dyn_83_5_1#
Dyn_83_5_1#show ip nhrp
10.83.5.2/32 via 10.83.5.2, Tunnel0 created 00:12:54, expire 01:47:05
      Type: dynamic, Flags: authoritative registered
      NBMA address: 192.83.35.1
10.83.5.3/32 via 10.83.5.3, Tunnel0 created 00:10:25, expire 01:49:34
      Type: dynamic, Flags: authoritative registered
      NBMA address: 192.83.55.1
Dyn_83_5_1#
Dyn_83_5_1#show ip nhrp multicast
      I/F      NBMA address
Tunnel0      None      Flags: dynamic
Tunnel0      None      Flags: dynamic
Dyn_83_5_1#
Dyn_83_5_1#show ip nhrp summary
IP NHRP cache 2 entries, 496 bytes
      0 static  2 dynamic  0 incomplete
Dyn_83_5_1#
Dyn_83_5_1#show ip nhrp traffic
Tunnel0
      Sent: Total 4
            0 Resolution Request  2 Resolution Reply  0 Registration Request
            2 Registration Reply  0 Purge Request  0 Purge Reply
            0 Error Indication
      Rcvd: Total 9
            2 Resolution Request  0 Resolution Reply  7 Registration Request
            0 Registration Reply  0 Purge Request  0 Purge Reply
            0 Error Indication

```

Рисунок 3.2 – Перевірка NHRP на Dyn_83_5_1

```

Dyn_83_5_2#show ip nhrp nhs
Legend:
  E=Expecting replies
  R=Responding

Tunnel0:
  10.83.5.1      RE
Dyn_83_5_2#
Dyn_83_5_2#
Dyn_83_5_2#show ip nhrp brief
      Target      Via      NBMA      Mode  Intfc  Claimed
10.83.5.1/32      10.83.5.1      192.83.15.1  static  Tu0    <    >
10.83.5.3/32      10.83.5.3      192.83.55.1  dynamic  Tu0    <    >
Dyn_83_5_2#
Dyn_83_5_2#show ip nhrp
10.83.5.1/32 via 10.83.5.1, Tunnel0 created 00:12:00, never expire
      Type: static, Flags: authoritative used
      NBMA address: 192.83.15.1
10.83.5.3/32 via 10.83.5.3, Tunnel0 created 00:02:13, expire 01:52:55
      Type: dynamic, Flags: router
      NBMA address: 192.83.55.1
Dyn_83_5_2#
Dyn_83_5_2#show ip nhrp multicast
      I/F      NBMA address
Tunnel0      192.83.15.1      Flags: static
Dyn_83_5_2#
Dyn_83_5_2#show ip nhrp summary
IP NHRP cache 2 entries, 496 bytes
      1 static  1 dynamic  0 incomplete
Dyn_83_5_2#
Dyn_83_5_2#show ip nhrp traffic
Tunnel0
      Sent: Total 5
            1 Resolution Request  0 Resolution Reply  4 Registration Request
            0 Registration Reply  0 Purge Request  0 Purge Reply
            0 Error Indication
      Rcvd: Total 2
            0 Resolution Request  1 Resolution Reply  0 Registration Request
            1 Registration Reply  0 Purge Request  0 Purge Reply
            0 Error Indication
Dyn_83_5_2#

```

Рисунок 3.3– Перевірка NHRP на Dyn_83_5_2

Проведемо налаштування маршрутизації. В якості протоколу маршрутизації будемо використовувати EIGRP, для цього то необхідно:

- включити EIGRP для мереж mGRE-інтерфейсів;
- вимкнути автоматичне підсумовування мереж за класовою ознакою;
- налаштувати EIGRP на mGRE-інтерфейсі.

1) Включення EIGRP для мереж mGRE-інтерфейсів:

```
Dyn_83_5_1(config)#router eigrp 1
```

```
Dyn_83_5_1(config-router)#network 10.10.10.0 0.0.0.255
```

2) Відключення автоматичного сумування мереж:

```
Dyn_83_5_1(config-router)#no auto-summary
```

3) Налаштування EIGRP на mGRE-інтерфейсах

Для роботи в мережі DMVPN необхідно додатково налаштувати EIGRP.

На hub-маршрутизаторі необхідно відключити правило розщеплення горизонту (split horizon), інакше EIGRP не буде анонсувати маршрути, вивчені через mGRE-інтерфейс назад в цей же інтерфейс:

```
Dyn_83_5_1 (config-if) # no ip split-horizon eigrp 1
```

За замовчуванням EIGRP буде підставляти IP-адреса hub-маршрутизатора в якості next-hop для маршрутів які він анонсує, навіть коли анонсує маршрути назад через той же інтерфейс, на якому вони були вивчені. Для мережі DMVPN необхідно щоб EIGRP використовував в якості next-hop адреси spoke-маршрутизаторів. Тому на hub-маршрутизаторі необхідно відключити це правило:

```
Dyn_83_5_1 (config-if) # no ip next-hop-self eigrp 1
```

При використанні DMVPN у великих мережах час збіжності мережі може збільшуватися. Для того щоб уникнути можливих проблем з маршрутизацією, на маршрутизаторах необхідно змінити hold time (за замовчуванням 15 секунд):

```
Dyn_83_5_1 (config-if) # ip hold-time eigrp 1 35
```

Якщо на одному з маршрутизаторів цей параметр змінений, то сусіди цього маршрутизатора будуть використовувати цей таймер. Для того щоб маршрутизатор сам використовував певне значення таймера, необхідно змінити таймер на відповідному інтерфейсі сусіда.

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						73
Зм.	Лист	№ документу	Підпис	Дата		

Перевіримо роботу EIGRP, для цього використаємо команди `show ip eigrp neighbors` та `show ip route` отримаємо

```
Dyn_83_5_1#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address                Interface      Hold Uptime    SRTT    RTO    Q    Seq
                               (sec)                (ms)          Cnt  Num
1   10.83.5.3                Tu0            11 00:01:44    652    5000    0    10
0   10.83.5.2                Tu0            12 00:01:49    624    5000    0    12
```

Рисунок 3.4 – Сусіди для Dyn_83_5_1

3.3.2 Налаштування протоколу безпеки IPSec на маршрутизаторах Cisco

Умовно налаштування IPsec можна розбити на дві фази:

Перша фаза – налагодження IKE:

Аутентифікація по pre-shared key. У політиці з аутентифікацією по pre-shared key, метод аутентифікації змінений, тому що за замовчуванням використовується аутентифікація за сертифікатами. Інші параметри використовують значення за замовчуванням.

Створюємо політику isakmp:

```
Dyn_83_5_1 (config) # crypto isakmp policy 20
```

```
Dyn_83_5_1 (config-isakmp) # authentication pre-share
```

Так як адреса реєр заздалегідь невідома і може бути отримана динамічно, то при налаштуванні pre-shared key необхідно вказувати шаблонну адресу (wildcard address).

Налаштування isakmp pre-shared key:

```
Dyn_83_5_1 (config) # crypto isakmp key 0 isakmpkey address 0.0.0.0 0.0.0.0
```

Друга фаза – налагодження IPsec-профілю:

Так як hub-маршрутизатор не знає заздалегідь IP-адреси spoke-маршрутизаторів, то для другої фази IPsec потрібна динамічна crypto map (dynamic crypto map), але для тунельних інтерфейсів еквівалентом dynamic crypto map є IPsec-profile:

– застосовується на тунельному інтерфейсі;

– після застосування будь-який трафік, що виходить з тунельного інтерфейсу ініціює створення IPsec-тунелю (немає необхідності використовувати ACL, як у звичайній crypto map);

– source і destination адреси тунельного інтерфейсу використовуються для створення IPsec-тунелю. Адреси можуть бути прописані в налаштуваннях інтерфейсу або отримані динамічно за допомогою NHRP.

Отже створюємо transform set:

```
Dyn_83_5_1 (config) # crypto ipsec transform-set DMVPN-TR esp-des
```

Так як mGRE-інтерфейс забезпечує створення тунелю, то IPsec можна перевести в транспортний режим (за замовчуванням використовується тунельний режим):

```
Dyn_83_5_1 (cfg-crypto-trans) # mode transport
```

Створюємо IPSec-профіль:

```
Dyn_83_5_1 (config) # crypto ipsec profile DMVPN
```

```
Dyn_83_5_1 (config-profile) # set transform-set DMVPN-TR
```

Застосуємо IPsec-профіль на mGRE-інтерфейсі:

```
Dyn_83_5_1 (config) # interface Tunnel0
```

```
Dyn_83_5_1 (config-if) # tunnel protection ipsec profile DMVPN
```

3.3.3 Налаштування GRE-тунелів та протоколу IKE маршрутизаторах Huawei

Для налаштування GRE- тунелю на маршрутизаторах Huawei, необхідно виконати наступні кроки:

1) Створити інтерфейс тунелю на маршрутизаторі;

```
[Huawei_Global_1] interface tunnel 0/0/0
```

2) Визначити адресу джерела тунелю, як IP-адресу інтерфейсу, який посилає пакет;

```
[Huawei_Global_1-Tunnel0/0/0] tunnel-protocol gre
```

```
[Huawei_Global_1-Tunnel0/0/0] source 105.83.35.1
```

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						75
Зм.	Лист	№ документа	Підпис	Дата		

3) Визначити адресу призначення тунельню, як IP-адресу інтерфейсу, який приймає пакет;

[Huawei_Global_1-Tunnel0/0/0] destination 105.83.45.1

4) Налаштувати мережеву адресу інтерфейсу тунелю для того, щоб тунель для підтримки протоколу динамічної маршрутизації;

[Huawei_Global_1-Tunnel0/0/0] ip address 11.83.35.1 30

5) Налаштувати статичний маршрут для того, щоб трафік між мережами передавався через GRE- тунель.

[Huawei_Global_1] ip route-static 10.83.50.0 255.255.255.252 11.83.35.2

Для налаштування протоколу IKE на маршрутизаторах Huawei, необхідно виконати наступні кроки:

1) Налаштувати локальний ідентифікатор хоста і IKE peer:

[Huawei_Global_1]ike local-name huawei01

[Huawei_Global_1]ike peer Huawei_Local_1 v1

[Huawei_Global_1-ike-peer-Huawei_Local_1]exchange-mode aggressive

*[Huawei_Global_1-ike-peer-Huawei_Local_1]pre-shared-key ciphers
%%\$%%\$}H"z!S,^u*;!(AQmOU4+,.2n%\$%%\$*

[Huawei_Global_1-ike-peer-Huawei_Local_1]local-id-type name

[Huawei_Global_1-ike-peer-Huawei_Local_1]remote-name huawei02

[Huawei_Global_1-ike-peer-Huawei_Local_1]remote-address 105.83.45.1

2) Налаштувати правила ACL, для щоб дані потоку були захищені:

[Huawei_Global_1-acl-adv-3101]acl number 3101

*[Huawei_Global_1-acl-adv-3101]rule 5 permit ip source 10.83.35.0 0.0.0.3
destination 10.83.50.0 0.0.0.31*

3) Налаштувати пропозиції безпеки:

[Huawei_Global_1]ipsec proposal tran1

[Huawei_Global_1-ipsec-proposal-tran1] encapsulation-mode tunnel

[Huawei_Global_1-ipsec-proposal-tran1] transform esp

[Huawei_Global_1-ipsec-proposal-tran1] esp encryption-algorithm des

[Huawei_Global_1-ipsec-proposal-tran1] esp authentication-algorithm sha1

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						76
Зм.	Лист	№ документу	Підпис	Дата		

[Huawei_Global_1-ipsec-proposal-tran1] quit

4) Налаштувати політики безпеки: прийняття ACL правила та пропозицію безпеки:

[Huawei_Global_1] ipsec policy map1 10 isakmp

[Huawei_Global_1-ipsec-policy-isakmp-map1-10] ike-peer Huawei_Local_1

[Huawei_Global_1-ipsec-policy-isakmp-map1-10] proposal tran1

[Huawei_Global_1-ipsec-policy-isakmp-map1-10] security acl 3101

[Huawei_Global_1-ipsec-policy-isakmp-map1-10] quit

5) Застосувати політику безпеки на інтерфейсі:

[Huawei_Global_1-GigabitEthernet0/0/1]ipsec policy map1

3.4 Налаштування додаткових засобів захисту інформаційно-комунікаційної мережі

Для забезпечення додаткової безпеки маршрутизаторів, була розроблена підсистема захисту, яка включає наступні елементи:

- парольний доступ для підключення по консолі:

line con 0

login

password [пароль]

- парольний доступ для підключення по телнету:

line vty 0 4

login

password [пароль]

- забезпечення захисту для паролів в конфігурації:

service password-encryption

- запобігання поширення інформації про користувачів:

no service finger

- запобігання поширення інформації про маршрутизатор на сусідні пристрої:

no cdp running

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						77
Зм.	Лист	№ документу	Підпис	Дата		

no cdp enable

- запобігання атак на сервіс NTP:

ntp disable

- перешкоджання використанню маршрутизаторів для smurf атак:

no ip directed-broadcast

- виявлення і видалення "завислих" сесій, звільняючи використовувані VTU:

service tcp-keepalives-in

- відкидання IP пакетів, в яких включена опція source routing. Таким чином зломисник не зможе отримати назад відповідь на надісланий пакет, якщо він використовував підроблену IP адресу:

no ip source-route

- захищення від флуду, що дозволити працювати важливим процесам:

scheduler allocate

- парольний доступ по ssh на маршрутизаторах Huawei:

Створення локальної пари ключів на SSH_server:

[Huawei_Global_1]rsa local-key-pair create

Налаштування VTU користувача інтерфейсу:

[Huawei_Global_1]user-interface vty 0 4

[Huawei_Global_1-ui-vty0-4]authentication-mode aaa

[Huawei_Global_1-ui-vty0-4]protocol inbound ssh

Налаштування двох локальних користувачів:

[Huawei_Global_1]aaa

[Huawei_Global_1-aaa]local-user z1password simple z1

[Huawei_Global_1-aaa]local-user z1 service-type ssh

[Huawei_Global_1-aaa]local-user z1 privilege level 15

[Huawei_Global_1-aaa]local-user z2 password cipher z2

[Huawei_Global_1-aaa]local-user z2 service-type ssh

[Huawei_Global_1-aaa]local-user z2 privilege level 15

- Створення SSH користувача з ім'ям z1 і конфігурування режиму аутентифікації з паролем для цього користувача:

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						78
Зм.	Лист	№ документа	Підпис	Дата		

[Huawei_Global_1]ssh user z1 authentication-type password

Створення SSH користувача з ім'ям SSH z2 і конфігурування режиму аутентифікації RSA для користувача:

[Huawei_Global_1]ssh user z2 authentication-type rsa

Створення пари локальних ключів на клієнті:

[Huawei_Local_1]rsa local-key-pair create

Надсилання відкритого ключа RSA, згенерованого на клієнті, на сервер:

[Huawei_Global_1]rsa peer-public-key zhenya

Enter "RSA public key" view, return system view with "peer-public-key end".

[Huawei_Global_1-rsa-public-key]public-key-code begin

Enter "RSA key code" view, return last view with "public-key-code end".

[Huawei_Global_1-rsa-key-code]3047

[Huawei_Global_1-rsa-key-code] 0240

*[Huawei_Global_1-rsa-key-code] E3A7DD2A 41619DB8 87C393E6
37F8EC7F FE3CCC99*

*[Huawei_Global_1-rsa-key-code] 648127E9 5CB55853 682B6769 6A1A29AC
F14C4B6C*

*[Huawei_Global_1-rsa-key-code] BB42D341 FFACE436 72629F6D
83BA629D 820EB648*

[Huawei_Global_1-rsa-key-code] FED5D523

[Huawei_Global_1-rsa-key-code] 0203

[Huawei_Global_1-rsa-key-code] 010001

[Huawei_Global_1-rsa-key-code]public-key-code end

[Huawei_Global_1-rsa-public-key]peer-public-key end

Прийняття відкритого ключа RSA для z2

[Huawei_Global_1]ssh user z2 assign rsa-key zhenya

Включення сервісу stelnet на SSH сервері

[Huawei_Global_1]stelnet server enable

[Huawei_Global_1]ssh user z1 service-type stelnet

[Huawei_Global_1]ssh user z2 service-type stelnet

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						79
Зм.	Лист	№ документу	Підпис	Дата		

Включення аутентифікації на SSH клієнті для першого входу в систему:

[Huawei_Local_1] ssh client first-time enable

– налаштування Radius сервера

Команди налаштування Radius сервера для маршрутизаторах Cisco:

Спочатку налагодимо маршрутизатор для аутентифікації на зовнішньому сервері:

Dyn_83_5_1 (config)#aaa new-model

Dyn_83_5_1 (config)#aaa authentication login default radius

Dyn_83_5_1 (config)#radius-server host 10.83.15.2 auth-port 1812 acct-port 1813

Dyn_83_5_1 (config)#radius-server key zhenya

Для входу в привілейований режим виконаємо наступні налаштування на маршрутизаторі:

Dyn_83_5_1 (config)#line vty 0 4

Dyn_83_5_1 (config-line)#privilege level 15

Dyn_83_5_1 (config-line)#exit

Dyn_83_5_1 (config)#

Команди налаштування Radius сервера для маршрутизаторах Huawei:

1) Налаштування шаблону Radius сервера, схеми аутентифікації та схеми обліку

Створення шаблону Radius сервера з ім'ям shiva.

[RouterA] radius-server template shiva

Налаштування IP-адрес і портів сервера.

[RouterA-radius-shiva] radius-server authentication 129.7.66.66 1812

[RouterA-radius-shiva] radius-server accounting 129.7.66.66 1813

Налаштування ключа та кількості ретрансляцій на сервері.

[RouterA-radius-shiva] radius-server shared-key it-is-my-secret

[RouterA-radius-shiva] radius-server retransmit 2

[RouterA-radius-shiva] quit

Налаштування перевірки автентичності схеми 1 з режимом аутентифікації Radius.

[RouterA] aaa

[RouterA-aaa] authentication-scheme 1

[RouterA-aaa-authen-1] authentication-mode radius

[RouterA-aaa-authen-1] quit

Налаштування схеми обліку 1 з режимом обліку Radius.

[RouterA-aaa] accounting-scheme 1

[RouterA-aaa-accounting-1] accounting-mode radius

[RouterA-aaa-accounting-1] quit

2) Застосування схеми аутентифікації 1, схеми обліку 1 та Radius шаблону до домену Huawei

[RouterA-aaa] domain huawei

[RouterA-aaa-domain-huawei] authentication-scheme 1

[RouterA-aaa-domain-huawei] accounting-scheme 1

[RouterA-aaa-domain-huawei] radius-server shiva

3.5 Тестування роботи захищеної інформаційно-комунікаційної мережі

На даному етапі дипломного проектування вже побудовано схему ІКМ, розроблено систему адресації на налагоджено підсистеми захисту та обладнання яке використовується в інформаційно-комунікаційній мережі.

Отже проведемо перевірку налаштувань, встановлених в розділі 3.2 даного дипломного проекту.

Для початку проглянемо таблиці маршрутизації кожного з маршрутизаторів:

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						81
Зм.	Лист	№ документа	Підпис	Дата		

```

Dyn_83_5_1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

    192.83.15.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.83.15.0/30 is directly connected, FastEthernet0/0
R       192.83.15.0/24 [120/10] via 10.83.5.3, 00:00:20, Tunnel0
                    [120/10] via 10.83.5.2, 00:00:21, Tunnel0
    192.83.55.0/24 is variably subnetted, 2 subnets, 2 masks
S       192.83.55.0/30 [1/0] via 192.83.15.2
R       192.83.55.0/24 [120/10] via 10.83.5.2, 00:00:21, Tunnel0
    10.0.0.0/8 is variably subnetted, 6 subnets, 3 masks
R       10.83.70.0/30 [120/10] via 10.83.5.3, 00:00:02, Tunnel0
C       10.83.15.0/30 is directly connected, FastEthernet0/1
C       10.83.5.0/29 is directly connected, Tunnel0
R       10.83.50.0/27 [120/4] via 10.83.5.2, 00:00:01, Tunnel0
R       10.83.55.0/30 [120/1] via 10.83.5.3, 00:00:02, Tunnel0
R       10.83.35.0/30 [120/1] via 10.83.5.2, 00:00:06, Tunnel0
    11.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
R       11.0.0.0/8 [120/10] via 10.83.5.3, 00:00:08, Tunnel0
                    [120/10] via 10.83.5.2, 00:00:07, Tunnel0
D EX    11.83.55.0/30 [170/297308416] via 10.83.5.3, 00:16:46, Tunnel0
D EX    11.83.35.0/30 [170/297308416] via 10.83.5.2, 00:19:17, Tunnel0
    192.83.35.0/24 is variably subnetted, 2 subnets, 2 masks
S       192.83.35.0/30 [1/0] via 192.83.15.2
R       192.83.35.0/24 [120/10] via 10.83.5.3, 00:00:12, Tunnel0
    105.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
D EX    105.83.55.0/30 [170/297308416] via 10.83.5.3, 00:16:52, Tunnel0
D EX    105.83.45.0/30 [170/297308416] via 10.83.5.2, 00:19:24, Tunnel0
D EX    105.83.35.0/30 [170/297308416] via 10.83.5.2, 00:19:24, Tunnel0
R       105.0.0.0/8 [120/2] via 10.83.5.3, 00:00:18, Tunnel0
                    [120/2] via 10.83.5.2, 00:00:17, Tunnel0
D EX    105.83.65.0/30 [170/297308416] via 10.83.5.3, 00:16:58, Tunnel0

```

Рисунок 3.5 – Таблиця маршрутизації Dyn_83_5_1

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						82
Зм.	Лист	№ документу	Підпис	Дата		

```

Dyn_83_5_2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

    192.83.15.0/24 is variably subnetted, 2 subnets, 2 masks
S       192.83.15.0/30 [1/0] via 192.83.35.2
D EX    192.83.15.0/24 [170/297308416] via 10.83.5.2, 00:19:52, Tunnel0
    192.83.55.0/24 is variably subnetted, 2 subnets, 2 masks
S       192.83.55.0/30 [1/0] via 192.83.35.2
R       192.83.55.0/24 [120/10] via 10.83.5.1, 00:00:19, Tunnel0
    10.0.0.0/8 is variably subnetted, 6 subnets, 3 masks
D EX    10.83.70.0/30 [170/297308416] via 10.83.5.3, 00:17:08, Tunnel0
R       10.83.15.0/30 [120/1] via 10.83.5.1, 00:00:06, Tunnel0
C       10.83.5.0/29 is directly connected, Tunnel0
R       10.83.50.0/27 [120/3] via 10.83.35.2, 00:00:02, FastEthernet0/1
D EX    10.83.55.0/30 [170/297308416] via 10.83.5.3, 00:17:20, Tunnel0
C       10.83.35.0/30 is directly connected, FastEthernet0/1
    11.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
D EX    11.0.0.0/8 [170/297308416] via 10.83.5.2, 00:20:15, Tunnel0
D EX    11.83.55.0/30 [170/310108416] via 10.83.5.3, 00:17:55, Tunnel0
S       11.83.35.0/30 [1/0] via 10.83.35.2
    192.83.35.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.83.35.0/30 is directly connected, FastEthernet0/0
R       192.83.35.0/24 [120/10] via 10.83.5.1, 00:00:22, Tunnel0
    105.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
D EX    105.83.55.0/30 [170/310108416] via 10.83.5.3, 00:18:02, Tunnel0
R       105.83.45.0/30 [120/2] via 10.83.35.2, 00:00:20, FastEthernet0/1
R       105.83.35.0/30 [120/1] via 10.83.35.2, 00:00:21, FastEthernet0/1
D EX    105.0.0.0/8 [170/297308416] via 10.83.5.2, 00:20:25, Tunnel0
D EX    105.83.65.0/30 [170/310108416] via 10.83.5.3, 00:18:06, Tunnel0

```

Рисунок 3.6 – Таблиця маршрутизації Dyn_83_5_2

```

Dyn_83_5_3#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

    192.83.15.0/24 is variably subnetted, 2 subnets, 2 masks
S       192.83.15.0/30 [1/0] via 192.83.55.2
D EX    192.83.15.0/24 [170/297308416] via 10.83.5.3, 00:08:52, Tunnel0
    192.83.55.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.83.55.0/30 is directly connected, FastEthernet0/0
R       192.83.55.0/24 [120/10] via 10.83.5.1, 00:00:17, Tunnel0
    10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
S       10.83.70.0/30 [1/0] via 10.83.55.2
R       10.83.15.0/30 [120/1] via 10.83.5.1, 00:00:22, Tunnel0
C       10.83.5.0/29 is directly connected, Tunnel0
C       10.83.55.0/30 is directly connected, FastEthernet0/1
D EX    10.83.35.0/30 [170/297308416] via 10.83.5.2, 00:01:11, Tunnel0
D EX    10.83.50.0/30 [170/297308416] via 10.83.5.2, 00:17:08, Tunnel0
    11.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
D EX    11.0.0.0/8 [170/297308416] via 10.83.5.3, 00:09:01, Tunnel0
S       11.83.55.0/30 [1/0] via 10.83.55.2
D EX    11.83.35.0/30 [170/310108416] via 10.83.5.2, 00:01:40, Tunnel0
    192.83.35.0/24 is variably subnetted, 2 subnets, 2 masks
S       192.83.35.0/30 [1/0] via 192.83.55.2
R       192.83.35.0/24 [120/10] via 10.83.5.1, 00:00:00, Tunnel0
    105.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
R       105.83.55.0/30 [120/1] via 10.83.55.2, 00:00:19, FastEthernet0/1
D EX    105.0.0.0/8 [170/297308416] via 10.83.5.3, 00:09:08, Tunnel0
R       105.83.65.0/30 [120/2] via 10.83.55.2, 00:00:21, FastEthernet0/1
D EX    105.83.45.0/30 [120/2] via 10.83.5.2, 00:18:06, Tunnel0
D EX    105.83.35.0/30 [120/1] via 10.83.5.2, 00:20:25, Tunnel0

```

Рисунок 3.6 – Таблиця маршрутизації Dyn_83_5_3

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						83
Зм.	Лист	№ документу	Підпис	Дата		

```

<Huawei_Global_1>display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
      Destinations : 24          Routes : 24

Destination/Mask    Proto    Pre  Cost           Flags NextHop          Interface
-----
 10.83.5.0/29       RIP      100   1             D   10.83.35.1          GigabitEthernet0/0/0
 10.83.15.0/30      RIP      100   2             D   10.83.35.1          GigabitEthernet0/0/0
 10.83.35.0/30      Direct   0     0             D   10.83.35.2          GigabitEthernet0/0/0
 10.83.35.2/32      Direct   0     0             D   127.0.0.1           GigabitEthernet0/0/0
 10.83.35.3/32      Direct   0     0             D   127.0.0.1           GigabitEthernet0/0/0
 10.83.50.0/30      Static   60    0             RD  11.83.35.2          Tunnel0/0/0
 10.83.55.0/30      RIP      100  10             D   10.83.35.1          GigabitEthernet0/0/0
 10.83.70.0/30      RIP      100  10             D   10.83.35.1          GigabitEthernet0/0/0
 11.0.0.0/8         RIP      100  10             D   10.83.35.1          GigabitEthernet0/0/0
 11.83.35.0/30      Direct   0     0             D   11.83.35.1          Tunnel0/0/0
 11.83.35.1/32      Direct   0     0             D   127.0.0.1           Tunnel0/0/0
 11.83.35.3/32      Direct   0     0             D   127.0.0.1           Tunnel0/0/0
 105.0.0.0/8        RIP      100  10             D   10.83.35.1          GigabitEthernet0/0/0
 105.83.35.0/30     Direct   0     0             D   105.83.35.1         GigabitEthernet0/0/1
 105.83.35.1/32     Direct   0     0             D   127.0.0.1           GigabitEthernet0/0/1
 105.83.35.3/32     Direct   0     0             D   127.0.0.1           GigabitEthernet0/0/1
 105.83.45.0/30     RIP      100   1             D   105.83.35.2         GigabitEthernet0/0/1
 127.0.0.0/8        Direct   0     0             D   127.0.0.1           InLoopBack0
 127.0.0.1/32       Direct   0     0             D   127.0.0.1           InLoopBack0
127.255.255.255/32  Direct   0     0             D   127.0.0.1           InLoopBack0
 192.83.15.0/24     RIP      100  10             D   10.83.35.1          GigabitEthernet0/0/0
 192.83.35.0/24     RIP      100  11             D   10.83.35.1          GigabitEthernet0/0/0
 192.83.55.0/24     RIP      100  11             D   10.83.35.1          GigabitEthernet0/0/0
255.255.255.255/32  Direct   0     0             D   127.0.0.1           InLoopBack0

```

Рисунок 3.7 – Таблица маршрутизації Huawei_Global_1

```

<Huawei_Global_2>display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
      Destinations : 23          Routes : 23

Destination/Mask    Proto    Pre  Cost           Flags NextHop          Interface
-----
 10.83.5.0/29       RIP      100   1             D   10.83.55.1          GigabitEthernet0/0/0
 10.83.15.0/30      RIP      100   2             D   10.83.55.1          GigabitEthernet0/0/0
 10.83.35.0/30      RIP      100  10             D   10.83.55.1          GigabitEthernet0/0/0
 10.83.55.0/30      Direct   0     0             D   10.83.55.2          GigabitEthernet0/0/0
 10.83.55.2/32      Direct   0     0             D   127.0.0.1           GigabitEthernet0/0/0
 10.83.55.3/32      Direct   0     0             D   127.0.0.1           GigabitEthernet0/0/0
 10.83.70.0/25      Static   60    0             RD  11.83.55.2          Tunnel0/0/0
 11.0.0.0/8         RIP      100  10             D   10.83.55.1          GigabitEthernet0/0/0
 11.83.55.0/30      Direct   0     0             D   11.83.55.1          Tunnel0/0/0
 11.83.55.1/32      Direct   0     0             D   127.0.0.1           Tunnel0/0/0
 11.83.55.3/32      Direct   0     0             D   127.0.0.1           Tunnel0/0/0
 105.0.0.0/8        RIP      100  10             D   10.83.55.1          GigabitEthernet0/0/0
 105.83.55.0/30     Direct   0     0             D   105.83.55.1         GigabitEthernet0/0/2
 105.83.55.1/32     Direct   0     0             D   127.0.0.1           GigabitEthernet0/0/2
 105.83.55.3/32     Direct   0     0             D   127.0.0.1           GigabitEthernet0/0/2
 105.83.65.0/30     RIP      100   1             D   105.83.55.2         GigabitEthernet0/0/2
 127.0.0.0/8        Direct   0     0             D   127.0.0.1           InLoopBack0
 127.0.0.1/32       Direct   0     0             D   127.0.0.1           InLoopBack0
127.255.255.255/32  Direct   0     0             D   127.0.0.1           InLoopBack0
 192.83.15.0/24     RIP      100  10             D   10.83.55.1          GigabitEthernet0/0/0
 192.83.35.0/24     RIP      100  11             D   10.83.55.1          GigabitEthernet0/0/0
 192.83.55.0/24     RIP      100  11             D   10.83.55.1          GigabitEthernet0/0/0
255.255.255.255/32  Direct   0     0             D   127.0.0.1           InLoopBack0

```

Рисунок 3.8 – Таблица маршрутизації Huawei_Global_2

```

<Huawei_Local_1>display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
      Destinations : 21          Routes : 21

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
-----
 10.83.5.0/29       RIP     100   3          D    105.83.45.2       GigabitEthernet0/0/0
 10.83.15.0/30      RIP     100   4          D    105.83.45.2       GigabitEthernet0/0/0
 10.83.35.0/30      Static   60   0         RD    11.83.35.1         Tunnel0/0/0
 10.83.55.0/30      RIP     100  12          D    105.83.45.2       GigabitEthernet0/0/0
 10.83.70.0/30      RIP     100  12          D    105.83.45.2       GigabitEthernet0/0/0
 11.0.0.0/8         RIP     100  12          D    105.83.45.2       GigabitEthernet0/0/0
 11.83.35.0/30      Direct   0     0          D    11.83.35.2         Tunnel0/0/0
 11.83.35.2/32      Direct   0     0          D    127.0.0.1          Tunnel0/0/0
 11.83.35.3/32      Direct   0     0          D    127.0.0.1          Tunnel0/0/0
 105.0.0.0/8        RIP     100  12          D    105.83.45.2       GigabitEthernet0/0/0
 105.83.35.0/30     RIP     100   1          D    105.83.45.2       GigabitEthernet0/0/0
 105.83.45.0/30     Direct   0     0          D    105.83.45.1       GigabitEthernet0/0/0
 105.83.45.1/32     Direct   0     0          D    127.0.0.1          GigabitEthernet0/0/0
 105.83.45.3/32     Direct   0     0          D    127.0.0.1          GigabitEthernet0/0/0
 127.0.0.0/8        Direct   0     0          D    127.0.0.1          InLoopBack0
 127.0.0.1/32       Direct   0     0          D    127.0.0.1          InLoopBack0
127.255.255.255/32  Direct   0     0          D    127.0.0.1          InLoopBack0
 192.83.15.0/24     RIP     100  12          D    105.83.45.2       GigabitEthernet0/0/0
 192.83.35.0/24     RIP     100  13          D    105.83.45.2       GigabitEthernet0/0/0
 192.83.55.0/24     RIP     100  13          D    105.83.45.2       GigabitEthernet0/0/0
255.255.255.255/32  Direct   0     0          D    127.0.0.1          InLoopBack0

```

Рисунок 3.9 – Таблиця маршрутизації Huawei_Local_1

```

<Huawei_Local_2>display ip routing-table
Route Flags: R - relay, D - download to fib
-----
Routing Tables: Public
      Destinations : 20          Routes : 20

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
-----
 10.83.5.0/29       RIP     100   3          D    105.83.65.2       GigabitEthernet0/0/0
 10.83.15.0/30      RIP     100   4          D    105.83.65.2       GigabitEthernet0/0/0
 10.83.35.0/30      RIP     100  12          D    105.83.65.2       GigabitEthernet0/0/0
 10.83.55.0/30      Static   60   0         RD    11.83.55.1         Tunnel0/0/0
 11.0.0.0/8         RIP     100  12          D    105.83.65.2       GigabitEthernet0/0/0
 11.83.55.0/30      Direct   0     0          D    11.83.55.2         Tunnel0/0/0
 11.83.55.2/32      Direct   0     0          D    127.0.0.1          Tunnel0/0/0
 11.83.55.3/32      Direct   0     0          D    127.0.0.1          Tunnel0/0/0
 105.0.0.0/8        RIP     100  12          D    105.83.65.2       GigabitEthernet0/0/0
 105.83.55.0/30     RIP     100   1          D    105.83.65.2       GigabitEthernet0/0/0
 105.83.65.0/30     Direct   0     0          D    105.83.65.1       GigabitEthernet0/0/0
 105.83.65.1/32     Direct   0     0          D    127.0.0.1          GigabitEthernet0/0/0
 105.83.65.3/32     Direct   0     0          D    127.0.0.1          GigabitEthernet0/0/0
 127.0.0.0/8        Direct   0     0          D    127.0.0.1          InLoopBack0
 127.0.0.1/32       Direct   0     0          D    127.0.0.1          InLoopBack0
127.255.255.255/32  Direct   0     0          D    127.0.0.1          InLoopBack0
 192.83.15.0/24     RIP     100  12          D    105.83.65.2       GigabitEthernet0/0/0
 192.83.35.0/24     RIP     100  13          D    105.83.65.2       GigabitEthernet0/0/0
 192.83.55.0/24     RIP     100  13          D    105.83.65.2       GigabitEthernet0/0/0
255.255.255.255/32  Direct   0     0          D    127.0.0.1          InLoopBack0

```

Рисунок 3.10 – Таблиця маршрутизації Huawei_Local_2

Перевірка isakmp SA на Dyn_83_5_1 та за Dyn_83_5_2 допомогою команди show crypto isakmp sa:

```
Dyn_83_5_1#show crypto isakmp sa
dst          src          state          conn-id slot status
192.83.15.1  192.83.35.1  QM_IDLE        1      0 ACTIVE
192.83.15.1  192.83.55.1  QM_IDLE        2      0 ACTIVE

Dyn_83_5_1#show crypto isakmp sa det
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption

C-id  Local          Remote          I-VRF          Status Encr Hash Auth DH Lifetime
Cap.
1     192.83.15.1    192.83.35.1    ACTIVE des  sha  psk  1  23:41:52
      Connection-id:Engine-id = 1:1(software)
2     192.83.15.1    192.83.55.1    ACTIVE des  sha  psk  1  23:47:47
      Connection-id:Engine-id = 2:1(software)
```

Рисунок 3.11 – Перевірка isakmp SA на Dyn_83_5_1

```
Dyn_83_5_2#show crypto isa sa
dst          src          state          conn-id slot status
192.83.15.1  192.83.35.1  QM_IDLE        1      0 ACTIVE
192.83.35.1  192.83.55.1  QM_IDLE        2      0 ACTIVE

Dyn_83_5_2#show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption

C-id  Local          Remote          I-VRF          Status Encr Hash Auth DH Lifetime C
ap.
1     192.83.35.1    192.83.15.1    ACTIVE des  sha  psk  1  23:41:40
      Connection-id:Engine-id = 1:1(software)
2     192.83.35.1    192.83.55.1    ACTIVE des  sha  psk  1  23:47:35
      Connection-id:Engine-id = 2:1(software)
```

Рисунок 3.12 – Перевірка isakmp SA на Dyn_83_5_2

Перевіримо роботу IPsec:

Переглянемо інформацію про сгурто map на Dyn_83_5_1 та Dyn_83_5_2:

```

Dyn_83_5_1#show crypto map
Crypto Map "Tunnel0-head-0" 65536 ipsec-isakmp
  Profile name: DMVPN
  Security association lifetime: 4608000 kilobytes/3600 seconds
  PFS (Y/N): N
  Transform sets={
    DMVPN-TR,
  }

Crypto Map "Tunnel0-head-0" 65537 ipsec-isakmp
  Map is a PROFILE INSTANCE.
  Peer = 192.83.35.1
  Extended IP access list
    access-list permit gre host 192.83.15.1 host 192.83.35.1
  Current peer: 192.83.35.1
  Security association lifetime: 4608000 kilobytes/3600 seconds
  PFS (Y/N): N
  Transform sets={
    DMVPN-TR,
  }

Crypto Map "Tunnel0-head-0" 65538 ipsec-isakmp
  Map is a PROFILE INSTANCE.
  Peer = 192.83.55.1
  Extended IP access list
    access-list permit gre host 192.83.15.1 host 192.83.55.1
  Current peer: 192.83.55.1
  Security association lifetime: 4608000 kilobytes/3600 seconds
  PFS (Y/N): N
  Transform sets={
    DMVPN-TR,
  }
  Interfaces using crypto map Tunnel0-head-0:
    Tunnel0

```

Рисунок 3.13 – Інформація про crypto map на Dyn_83_5_1

```

Dyn_83_5_2#show crypto map
Crypto Map "Tunnel0-head-0" 65536 ipsec-isakmp
  Profile name: DMVPN
  Security association lifetime: 4608000 kilobytes/3600 seconds
  PFS (Y/N): N
  Transform sets={
    DMVPN-TR,
  }

Crypto Map "Tunnel0-head-0" 65537 ipsec-isakmp
  Map is a PROFILE INSTANCE.
  Peer = 192.83.15.1
  Extended IP access list
    access-list permit gre host 192.83.35.1 host 192.83.15.1
  Current peer: 192.83.15.1
  Security association lifetime: 4608000 kilobytes/3600 seconds
  PFS (Y/N): N
  Transform sets={
    DMVPN-TR,
  }

Crypto Map "Tunnel0-head-0" 65538 ipsec-isakmp
  Map is a PROFILE INSTANCE.
  Peer = 192.83.55.1
  Extended IP access list
    access-list permit gre host 192.83.35.1 host 192.83.55.1
  Current peer: 192.83.55.1
  Security association lifetime: 4608000 kilobytes/3600 seconds
  PFS (Y/N): N
  Transform sets={
    DMVPN-TR,
  }
  Interfaces using crypto map Tunnel0-head-0:
    Tunnel0

```

Рисунок 3.14 – Інформація про crypto map на Dyn_83_5_2

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						87
Зм.	Лист	№ документу	Підпис	Дата		

Перевірка IPsec SA на Dyn_83_5_2 після встановлення тунеля spoke-to-spoke:

```
Dyn_83_5_1#show crypto ipsec sa

interface: Tunnel0
Crypto map tag: Tunnel0-head-0, local addr 192.83.15.1

protected vrf: (none)
local ident (addr/mask/prot/port): (192.83.15.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (192.83.35.1/255.255.255.255/47/0)
current_peer 192.83.35.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 290, #pkts encrypt: 290, #pkts digest: 290
#pkts decaps: 285, #pkts decrypt: 285, #pkts verify: 285
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 91, #recv errors 0

local crypto endpt.: 192.83.15.1, remote crypto endpt.: 192.83.35.1
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0xA57593CC(2775946188)

inbound esp sas:
spi: 0x67A03BED(1738554349)
transform: esp-des ,
in use settings =(Transport, )
conn id: 2001, flow_id: SW:1, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4547838/2361)
IV size: 8 bytes
replay detection support: N
Status: ACTIVE

inbound ah sas:

inbound pcip sas:

outbound esp sas:
spi: 0xA57593CC(2775946188)
transform: esp-des ,
in use settings =(Transport, )
conn id: 2002, flow_id: SW:2, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4547837/2334)
IV size: 8 bytes
replay detection support: N
Status: ACTIVE

outbound ah sas:

outbound pcip sas:

protected vrf: (none)
local ident (addr/mask/prot/port): (192.83.15.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (192.83.55.1/255.255.255.255/47/0)
current_peer 192.83.55.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 207, #pkts encrypt: 207, #pkts digest: 207
#pkts decaps: 212, #pkts decrypt: 212, #pkts verify: 212
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 171, #recv errors 0

local crypto endpt.: 192.83.15.1, remote crypto endpt.: 192.83.55.1
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x6E179C48(1847041096)

inbound esp sas:
spi: 0x5EBE8620(1589544480)
transform: esp-des ,
in use settings =(Transport, )
conn id: 2003, flow_id: SW:3, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4606837/2635)
IV size: 8 bytes
replay detection support: N
Status: ACTIVE

inbound ah sas:

inbound pcip sas:

outbound esp sas:
spi: 0x6E179C48(1847041096)
transform: esp-des ,
in use settings =(Transport, )
conn id: 2004, flow_id: SW:4, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4606837/2627)
IV size: 8 bytes
replay detection support: N
Status: ACTIVE

outbound ah sas:

outbound pcip sas:
Dyn_83_5_1#
Dyn_83_5_1#
Dyn_83_5_1#
Dyn_83_5_1#
```

Рисунок 3.15 – IPsec SA на Dyn_83_5_1

```
Dyn_83_5_2#show crypto ipsec sa

interface: Tunnel0
Crypto map tag: Tunnel0-head-0, local addr 192.83.35.1

protected vrf: (none)
local ident (addr/mask/prot/port): (192.83.35.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (192.83.15.1/255.255.255.255/47/0)
current_peer 192.83.15.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 289, #pkts encrypt: 289, #pkts digest: 289
#pkts decaps: 293, #pkts decrypt: 293, #pkts verify: 293
#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.: 192.83.35.1, remote crypto endpt.: 192.83.15.1
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x67A03BED(1738554349)

inbound esp sas:
spi: 0xA57593CC(2775946188)
transform: esp-des ,
in use settings =(Transport, )
conn id: 2001, flow_id: SW:1, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4574690/2346)
IV size: 8 bytes
replay detection support: N
Status: ACTIVE

inbound ah sas:

inbound pcip sas:

outbound esp sas:
spi: 0x67A03BED(1738554349)
transform: esp-des ,
in use settings =(Transport, )
conn id: 2002, flow_id: SW:2, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4574690/2328)
IV size: 8 bytes
replay detection support: N
Status: ACTIVE

outbound ah sas:

outbound pcip sas:

protected vrf: (none)
local ident (addr/mask/prot/port): (192.83.35.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (192.83.55.1/255.255.255.255/47/0)
current_peer 192.83.55.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#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.: 192.83.35.1, remote crypto endpt.: 192.83.55.1
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x429B6F1C(1117482780)

inbound esp sas:
spi: 0xB8AF60B9(3098501305)
transform: esp-des ,
in use settings =(Transport, )
conn id: 2003, flow_id: SW:3, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4525321/2645)
IV size: 8 bytes
replay detection support: N
Status: ACTIVE

inbound ah sas:

inbound pcip sas:

outbound esp sas:
spi: 0x429B6F1C(1117482780)
transform: esp-des ,
in use settings =(Transport, )
conn id: 2004, flow_id: SW:4, crypto map: Tunnel0-head-0
sa timing: remaining key lifetime (k/sec): (4525321/2631)
IV size: 8 bytes
replay detection support: N
Status: ACTIVE

outbound ah sas:

outbound pcip sas:
Dyn_83_5_2#
Dyn_83_5_2#
Dyn_83_5_2#
Dyn_83_5_2#
Dyn_83_5_2#
Dyn_83_5_2#
```

Рисунок 3.16 – IPsec SA на Dyn_83_5_2

```
[Huawei_Global_1]display ipsec policy

=====

IPSec policy group: "map1"
Using interface: GigabitEthernet0/0/1
=====

Sequence number: 10
Security data flow: 3101
Peer name      : Huawei_Local_1
Perfect forward secrecy: None
Proposal name:  tran1
IPSec SA local duration(time based): 3600 seconds
IPSec SA local duration(traffic based): 1843200 kilobytes
Anti-replay window size: 32
SA trigger mode: Automatic
Route inject: None
Qos pre-classify: Disable
```

Рисунок 3.17 – Ipsec policy на Huawei_Global_1

```
[Huawei_Global_2]display ipsec policy

=====

IPSec policy group: "map2"
Using interface: GigabitEthernet0/0/1
=====

Sequence number: 10
Security data flow: 3101
Peer name      : Huawei_Local_2
Perfect forward secrecy: None
Proposal name:  tran1
IPSec SA local duration(time based): 3600 seconds
IPSec SA local duration(traffic based): 1843200 kilobytes
Anti-replay window size: 32
SA trigger mode: Automatic
Route inject: None
Qos pre-classify: Disable
```

Рисунок 3.18 – Ipsec policy на Huawei_Global_2

```
[Huawei_Local_1]display ipsec policy

=====

IPSec policy group: "use1"
Using interface: GigabitEthernet0/0/0
=====

Sequence number: 10
Security data flow: 3101
Peer name      : Huawei_Global_1
Perfect forward secrecy: None
Proposal name:  tran1
IPSec SA local duration(time based): 3600 seconds
IPSec SA local duration(traffic based): 1843200 kilobytes
Anti-replay window size: 32
SA trigger mode: Automatic
Route inject: None
Qos pre-classify: Disable
```

Рисунок 3.18 – Ipsec policy на Huawei_Local_1

```
[Huawei_Local_2]display ipsec policy
```

```
=====
IPSec policy group: "use2"
Using interface: GigabitEthernet0/0/0
=====
```

```
Sequence number: 10
Security data flow: 3101
Peer name      : Huawei_Global_
Perfect forward secrecy: None
Proposal name:  tran1
IPSec SA local duration(time based): 3600 seconds
IPSec SA local duration(traffic based): 1843200 kilobytes
Anti-replay window size: 32
SA trigger mode: Automatic
Route inject: None
Qos pre-classify: Disable
```

Рисунок 3.20 – Ipsec policy на Huawei_Local_2

```
<Huawei_Global_1>display ipsec proposal
```

```
Number of proposals: 1

IPSec proposal name: tran1
Encapsulation mode: Tunnel
Transform           : esp-new
ESP protocol        : Authentication SHA1-HMAC-96
                    Encryption      DES
```

Рисунок 3.21 – Ipsec proposal на Huawei_Global_1

```
<Huawei_Local_1>display ipsec proposal
```

```
Number of proposals: 1

IPSec proposal name: tran1
Encapsulation mode: Tunnel
Transform           : esp-new
ESP protocol        : Authentication SHA1-HMAC-96
                    Encryption      DES
```

Рисунок 3.22 – Ipsec proposal на Huawei_Local_1

Детальні налаштування маршрутизаторів та проведення тестування мережі відображені в додатку Б.

Отже в даному розділі дипломного проекту було проведено налагодження обладнання захищеної інформаційно-комунікаційної мережі. Спочатку було обрано та обгрунтовано вибір апаратного та програмного забезпечення, яке використовується при розробці проєкту, після чого було проведено налаштування базового функціонування мережі, засобів базового захисту маршрутизаторів,

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						90
Зм.	Лист	№ документа	Підпис	Дата		

mGRE-тунелів, протоколу NHRP, протоколу маршрутизації EIGRP та протоколу безпеки IPSec.

Завершальним етапом даного розділу є тестування роботи захищеної інформаційно-комунікаційної мережі.

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						91
Зм.	Лист	№ документа	Підпис	Дата		

ВИСНОВКИ

В результаті виконання даного дипломного проекту було отримано наступні результати:

Проведено аналіз базових принципів та підходів до організації захисту інформаційно-комунікаційної мережі організації.

Проведено аналіз технологій захисту інформаційно-комунікаційних мереж та сучасних технологічних рішень захисту інформації провідних виробників комунікаційного обладнання, таких як Huawei Technologies та Cisco Systems.

Розроблено проекти узагальненої та спрощеної топології інформаційно-комунікаційної мережі та визначена необхідна кількість маршрутизаторів комутаторів та робочих станцій.

Розроблено проекти узагальненої та детальної фізичної та логічної схем адресації мережі для спрощеного проекту та проект підсистеми захисту інформаційно-комунікаційної мережі.

Проведено вибір та налагодження обладнання захищеної інформаційно-комунікаційної мережі, а саме: налаштування базового функціонування мережі, засобів базового захисту маршрутизаторів, GRE та mGRE-тунелів, протоколу NHRP, протоколу маршрутизації EIGRP, протоколу безпеки IPSec

Розглянуто питання з основ охорони праці, а саме основні положення з організації охорони праці та техніки безпеки на підприємстві та аналіз потенційно небезпечних виробничих факторів та методи захисту від них.

Розраховано витрати та економічний ефект на створення та експлуатацію інформаційно-комунікаційної мережі.

Проведено тестування налаштованої мережі, результатом якого є правильне функціонування всіх налаштованих параметрів. Тестування проводилось за допомогою команд ping та tracert

В результаті виконання дипломного проекту отримали захищену інформаційно-комунікаційну мережу, в якій забезпечується безпечне проходження трафіку з однієї мережі в іншу через GRE та mGRE тунель.

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						92
Зм.	Лист	№ документа	Підпис	Дата		

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України «Про інформацію»: станом на 13 січня 2011р. / Верховна Рада України. – Офіц. вид. – К.: Відомості Верховної Ради. – 2011. - №32. – 313 с. – (Бібліотека офіційних видань).
2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»: станом на 19 березня 2009 р. / Верховна Рада України. – Офіц. вид. – К.: Відомості Верховної Ради. – 2009. – №33. – 485 с – (Бібліотека офіційних видань).
3. Santos, Omar. CCNA Security 210-260. Official Cert Guide / Omar Santos, John Stuppi. – Cisco Press, 2015. – 658 p.
4. Conlan J., Patrik. Cisco Network Professional. Advanced Internetworking Guide. / Patrik J. Conlan. – Wiley Publishing, 2009. – 854 p.
5. Vyncke, Eric. LAN Switch Security: What Hackers Know about Your Switches / Eric Vyncke, Christopher Paggen. – Cisco Press, 2007. – 340 p.
6. Watkins, Michael. CCNA Security. Official Exam Certification Guide / Michael Watkins, Kevin Wallace. – Cisco Press, 2008. – 638 p.
7. Wilkins, Sean. CCNP Security. SECURE 642-637. Official Cert Guide / Sean Wilkins, Franklin H. Smith III. – Cisco Press, 2011. – 738 p.
8. Бирюков А. А. Информационная безопасность. Защита и напа-дение. 2-е изд., перераб. и доп. / А. А. Бирюков. – М. : ДМК-Пресс, 2017. – 434 с.
9. Буров Є.В. Комп'ютерні мережі: Підручник. – Львів: “Магнолія плюс”, 2016. – 264 с.
10. Буров Є.В. Комп'ютерні мережі. Підручник. Том 1. / Є.В. Бу-ров, М.М. Митник. – Львів: «Магнолія 2006», 2021. – 334 с.
11. Буров Є.В. Комп'ютерні мережі. Підручник. Том 2. / Є.В. Бу-ров, М.М. Митник. – Львів: «Магнолія 2006», 2021. – 204 с.
12. Дж. Бони. Руководство по Cisco IOS / Бони Дж. – СПб.: Питер; М.: Издате-льство „Русская Редакция”, 2008. – 784 с.
13. Кулаков Ю.О. Комп'ютерні мережі / Ю.О. Кулаков, І.А. Жуков. - К.: Вид-во Нац. авіац. ун-ту "НАУ-друк", 2009. – 392 с.

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						93
Зм.	Лист	№ документу	Підпис	Дата		

14. Одом Уэнделл. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 100-101; акад. изд. / пер. с англ. Уэнделл Одом. – М. : ООО „И.Д. Вильямс”, 2015. – 896 с.
15. Одом Уэнделл. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200-101: маршрутизация и коммутация, акад. изд. / пер. с англ. Уэнделл Одом. – М. : ООО „И.Д. Вильямс”, 2015. – 736 с.
- 16.Олифер В. Г. Безопасность компьютерных сетей / В. Г. Олифер, Н. А. Олифер. – М. : Горячая линия-Телеком, 2016. – 644 с.
- 17.Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы : учебник для вузов. – 6-е изд. / В. Г. Олифер, Н. А. Олифер. – СПб. : Питер, 2020. – 1008 с.
- 18.Таненбаум Э. Компьютерные сети. 5-е изд. / Э. Таненбаум, Д. Уэзе-тролл. – СПб.: Питер, 2012. – 960 с.
- 19.Уэнстром М. Организация защиты сетей Cisco. : Пер. с англ. / М. Уэнстром. – М.: Издательский дом "Вильямс", 2005. – 768 с.
- 20.Филимонов А. Ю. Построение мультисервисных сетей Ethernet / А. Ю. Филимонов. – СПб. : БХВ-Петербург, 2007. – 592 с.
- 21.Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В. Ф. Шаньгин. – М.: ИД «ФОРУМ»: ИН-ФРА-М, 2008. – 416 с.
- 22.Єфіменко А.А. Захист інформації в інформаційно-комунікаційних системах: методичні рекомендації для виконання лаборато-рних робіт. Ч. 2 / підг. А. А. Єфіменко. – Житомир: ЖВІ, 2017. – 176 с.
- 23.Єфіменко А.А. Захист інформації в інформаційно-комунікаційних системах: методичні рекомендації для виконання лаборато-рних робіт. Ч. 1 / підг. А. А. Єфіменко. – Житомир: ЖДТУ, 2018. – 112 с.
- 24.Єфіменко А.А. Комп'ютерні мережі : методичні рекомендації для виконання лабораторних робіт. Ч. 1. / підг. А. А. Єфіменко, – Житомир: ЖДТУ, 2017. – 144 с.

- 25.Єфіменко А.А. Комп'ютерні мережі : методичні рекомендації для виконання лабораторних робіт. Ч. 2. / підг. А. А. Єфіменко, – Житомир: ЖДТУ, 2018. – 136 с.
- 26.Єфіменко А.А. Комп'ютерні мережі : методичні рекомендації для виконання лабораторних робіт. Ч. 3. / підг. А. А. Єфіменко, – Житомир: ЖДТУ, 2019. – 120 с.
- 27.Навчальний курс CCNA Routing and Switching: Introduction to Networks [Електронний ресурс] – Режим доступу: www.netacad.com.
- 28.Навчальний курс CCNA Routing and Switching: Routing and Switching Essentials [Електронний ресурс] – Режим доступу: www.netacad.com.
- 29.Навчальний курс CCNA Routing and Switching: Scaling Networks [Електронний ресурс] – Режим доступу: www.netacad.com.
- 30.Навчальний курс CCNA Routing and Switching: Connecting Networks [Електронний ресурс] – Режим доступу: www.netacad.com.
31. Навчальний курс CCNAv7: Introduction to Networks [Електрон-ний ресурс] – Режим доступу: www.netacad.com.
32. Навчальний курс CCNAv7: Switching, Routing, and Wireless Essentials [Електронний ресурс] – Режим доступу: www.netacad.com.
33. Навчальний курс CCNAv7: Enterprise Networking, Security, and Automation [Електронний ресурс] – Режим доступу: www.netacad.com.
34. Навчальний курс CCNA Security [Електронний ресурс] – Режим доступу: www.netacad.com.
35. Навчальний курс CCNA Cybersecurity Operations [Електронний ресурс] – Режим доступу: www.netacad.com.

ДОДАТКИ

					КІК.КР.Б – 125 – 2 – ПЗ	Лист
						96
Зм.	Лист	№ документу	Підпис	Дата		

Технічні характеристики обладнання



Рисунок А.1 – Маршрутизатор Cisco 3925 Security Bundle w/SEC license PAK

Таблиця А.1 – Технічні характеристики

Пам'ять, процесор	
RAM	Встановлено 1 ГБ. Можливе розширення до 2 ГБ
Флеш пам'ять	Встановлено 256 МБ. Можливе розширення до 8 ГБ
Мережа	
Технологія з'єднання	Дротова
Протокол передачі даних	Ethernet, Fast Ethernet, Gigabit Ethernet
Протоколи маршрутизації	BGP, GRE, OSPF, DVMRP, EIGRP, IS-IS, IGMPv3, PIM-SM, PIM-SSM, статична IPv4 і IPv6 маршрутизація, PBR
Особливості конфігурації	Підтримує: VPN, IPv6, MPLS, Syslog, QoS, DMVPN, WRED, CBWFQ
Відповідність стандартам	IEEE 802.3, IEEE 802.1Q, IEEE 802.1ag, IEEE 802.1ah
Інтерфейси, роз'єми	
Інтерфейси	Інтерфейси 3 мережових Ethernet порту 10Base-T/100Base-TX/1000Base-T - роз'єм RJ-45; 1 консольний порт керування - роз'єм RJ-45; 1 консольний порт керування - роз'єм міні USB тип B; 1 послідовний допоміжний порт - роз'єм RJ-45;
Фізичні характеристики	
Джерело живлення	Внутрішній блок живлення з підтримкою PoE 100 - 240 В; 47 - 63 Гц; 7,1 / 3,0 А
Габарити	133,35 x 438,15 x 476,25 мм
Вага	17,7 кг (з джерелом живлення, без модулів); 18,1 кг (з PoE, без модулів); 27,2 кг (типовий вага в повній конфігурації).



Рисунок А.2 – Маршрутизатор AR3260 Routers AR0M0036SA00

Таблиця А.4 – Технічні характеристики

Апаратні засоби	
Переадресація ємності (64 байт)	2 млн. пакетів в секунду (з SRU40), 4 млн. пакетів в секунду (з SRU80)
Комутаційна здатність	60 Гбіт
WAN порти	3GE
SIC слоти	4
WSIC слоти	2
XSIC слоти	4/6
USB 2.0 порт	2
Mini-USB порт	1
Консольний порт	1
Пам'ять	2 GB
Flash (за замовчуванням / макс)	2 GB/4 GB
Максимальна потужність	350 W(Одинарний модуль живлення)/700 W(Подвійний модуль живлення)
Змінний струм	100 V-240 V
Частота	50 Hz/60 Hz
Постійний струм	-48 V~-60 V
Розміри (висота x ширина x глибина)	130.5мм x 442 мм x 470 мм
Вага	11 Кг
Діапазон температур	0°C-40°C

Продовження таблиці А.4 – Технічні характеристики

Програмне забезпечення	
Основні функції	DHCP server/client, PPPoE server/client, PPPoA client, PPPoEoA client, NAT, Sub interface management
Голос	RTP, SIP, SIP AG, IP PBX/TDM PBX, FXO/FXS, VoIP/conference call
3G	CDMA 2000 EV-DO Rev A, WCDMA, individual 3G uplink/backup link
LAN	IEEE 802.1P, IEEE 802.1Q, IEEE 802.3, VLAN management, MAC address management, MSTP
IPv4 unicast routing	Routing policy, static route, RIP, OSPF, IS-IS, BGP
Multicast	IGMP V1/V2/V3, IGMP-Snooping V1/V2/V3, PIM SM, PIM DM, MSDP
MPLS	LDP, MPLS L3 VPN, static LSP, dynamic LSP
VPN	IPSec VPN, GRE VPN, DSVPN, SSL VPN, L2TP VPN
Захист	ACL, брандмауер, аутентифікація 802.1x, аутентифікація MAC адрес, Web аутентифікація, аутентифікація AAA, RADIUS аутентифікація, аутентифікація HWTACACS, ARP безпека, DHCP, чорний список



Рисунок А.3 – Комутатор Linksys Gigabit 5-Port Workgroup Switch

Таблиця А.3 – Технічні характеристики

Основні характеристики	
Тип пристрою	Комутатор (світч)
Виробник	Linksys
Параметри мережі	
Інтерфейси	Ethernet, Gigabit Network
Кількість базових портів	5 RJ-45 10/100/1000 Мбіт / с
MDI	всі порти підтримують MDI / MDI-X з автоматичним визначенням необхідності кросового підключення
Пропускна спроможність	до 1000 Мбіт / сек
Індикатори	електроживлення, активне з'єднання, швидкість з'єднання, FDX
Підтримувані стандарти	IEEE 802.3, 802.3u, 802.3x, 802.3ab
Сертифікати	FCC Part 15 Class A
Електроживлення вбудований	вбудований блок живлення 12 В (постійний струм), 2 А
Фізичні характеристики	
Розмір (Ш x В x Г)	186 x 48 x 154 мм
Вага	500 г
Ціна	508.40 грн



Рисунок А.4 – Комутатор Cisco 24 port 10/100/1000

Таблиця А.4 – Технічні характеристики

Основні характеристики	
Тип пристрою	Комутатор (світч)
Виробник	Cisco
Модель	WS-CE520G-24TC-K9
Параметри мережі	
Тип мережі	Gigabit Ethernet, Fast Ethernet, Ethernet
Кількість портів	24 порта Ethernet 10Base-T/1000Base-T/100Base-TX.
Розмір таблиці MAC адрес	8000
Тип комунікації	Дуплексний, напівдуплексний
Індикатори	Активне з'єднання, електроживлення
Підтримувані стандарти	IEEE 802.1Q (VLAN), IEEE 802.1X, IEEE 802.3, IEEE 802.3ab ,IEEE 802.3u
Технологія з'єднання	Провідна
Електроживлення	Джерело живлення внутрішнє. 120/230 В змінного струму, 45 Вт.
Фізичні характеристики	
Розмір (Ш x В x Г)	4.39 x 44.45 x 25.15 см
Вага	3.7 кг
Ціна	2 927.40 грн

Налаштування роботи мережі

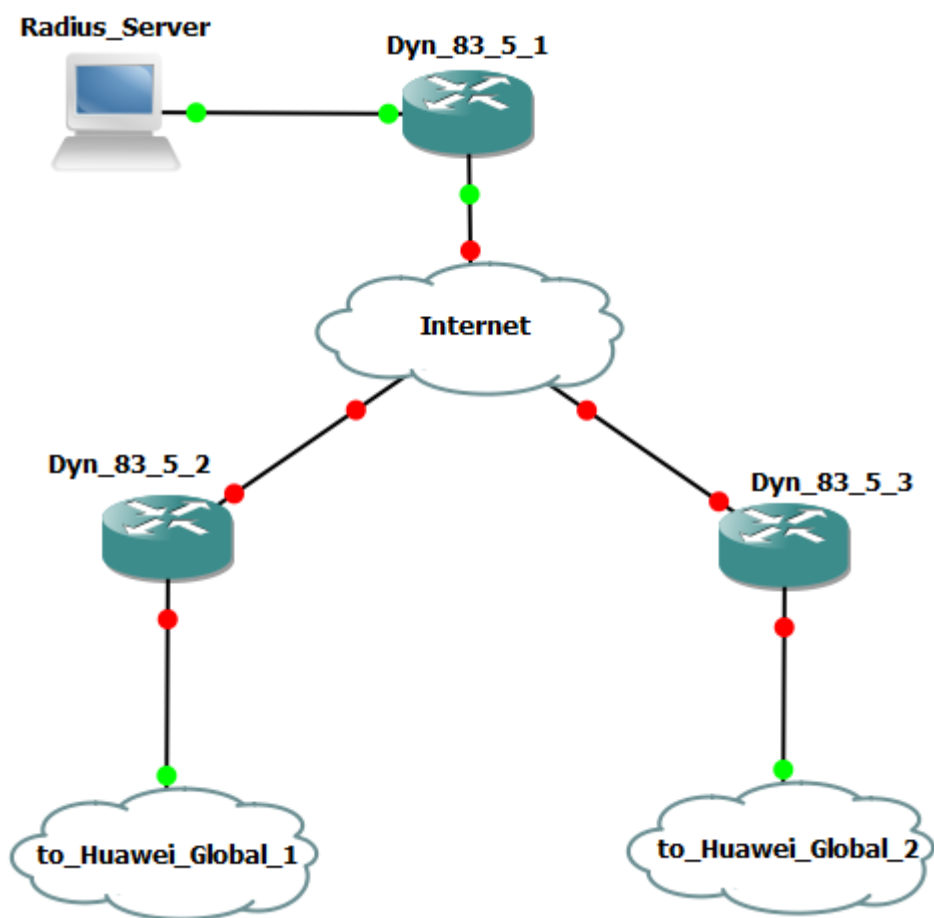


Рисунок Б.1 – Топологія мережі в програмі симуляторі GNS3

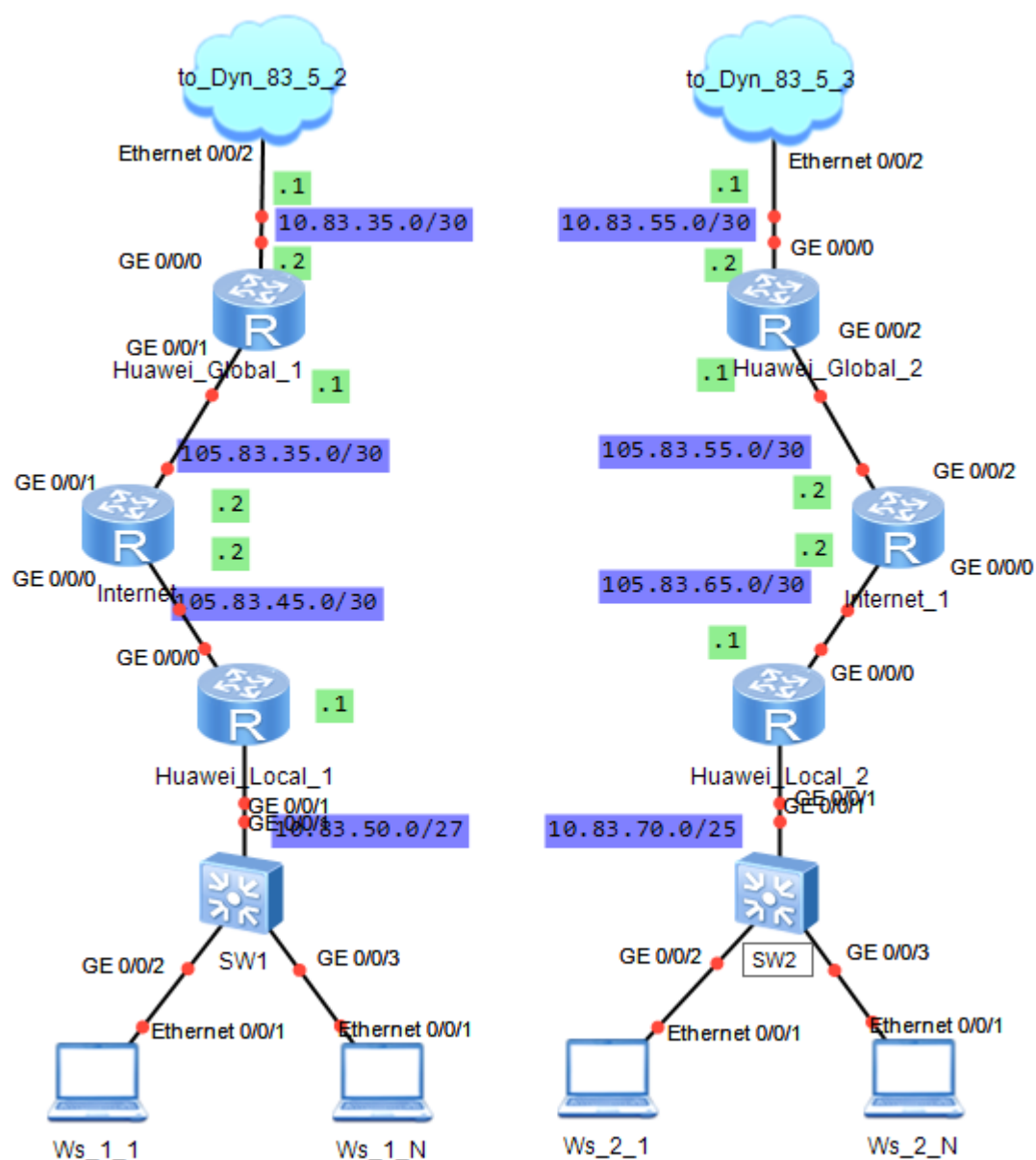


Рисунок Б.2 – Топологія мережі в програмі симуляторі eNSP

```

Dynamips(0): Dyn_83_5_1, Console port
Dyn_83_5_1#show run
Building configuration...

Current configuration : 1803 bytes
!
version 12.4
service tcp-keepalives-in
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Dyn_83_5_1
!
boot-start-marker
boot-end-marker
!
aaa new-model
!
aaa authentication login default group radius
!
aaa session-id common
memory-size iomem 5
!
ip cef
no ip domain lookup
!
!
crypto isakmp policy 10
!
crypto isakmp policy 20
authentication pre-share
crypto isakmp key isakmpkey address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set DMVPN-TR esp-des
mode transport
!
crypto ipsec profile DMVPN
set transform-set DMVPN-TR
!
interface Tunnel0
ip address 10.83.5.1 255.255.255.248
no ip redirects
ip mtu 1416
ip hold-time eigrp 1 35
no ip next-hop-self eigrp 1
ip nhrp authentication zhenya
ip nhrp map multicast dynamic
ip nhrp network-id 555
no ip split-horizon eigrp 1
tunnel source FastEthernet0/0
tunnel mode gre multipoint
tunnel key 555
tunnel protection ipsec profile DMVPN
!

```

```

Dynamips(0): Dyn_83_5_1, Console port
!
interface FastEthernet0/0
ip address 192.83.15.1 255.255.255.252
duplex auto
speed auto
ntp disable
!
interface FastEthernet0/1
ip address 10.83.15.1 255.255.255.252
duplex auto
speed auto
ntp disable
!
!
router eigrp 1
redistribute static
redistribute rip
network 10.83.5.0 0.0.0.7
default-metric 1000 250 255 1 1500
no auto-summary
!
router rip
version 2
redistribute static
redistribute eigrp 1
network 10.0.0.0
default-metric 10
!
no ip http server
no ip http secure-server
ip forward-protocol nd
ip route 192.83.35.0 255.255.255.252 192.83.15.2
ip route 192.83.55.0 255.255.255.252 192.83.15.2
!
radius-server host 10.83.15.2 auth-port 1812 acct-port 1813
radius-server key zhenya
!
no cdp run
!
line con 0
exec-timeout 0 0
password 7 083B1D
logging synchronous
login
line aux 0
line vty 0 4
privilege level 15
!
!
scheduler allocate 4000 1000
!
end

```

Рисунок Б.3 – Результат виконання команди show running-config Dyn_83_5_1

```

Dyn_83_5_2#show running-config
Building configuration...

Current configuration : 1814 bytes
!
version 12.4
service tcp-keepalives-in
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Dyn_83_5_2
!
boot-start-marker
boot-end-marker
!
aaa new-model
!
aaa authentication login default group radius
!
aaa session-id common
memory-size iomem 5
!
ip cef
no ip domain lookup
!
crypto isakmp policy 10
!
crypto isakmp policy 20
authentication pre-share
crypto isakmp key isakmpkey address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set DMVPN-TR esp-des
mode transport
!
crypto ipsec profile DMVPN
set transform-set DMVPN-TR
!
interface Tunnel0
ip address 10.83.5.2 255.255.255.248
no ip redirects
ip mtu 1416
ip nhrp authentication zhenya
ip nhrp map multicast 192.83.15.1
ip nhrp map 10.83.5.1 192.83.15.1
ip nhrp network-id 555
ip nhrp nhs 10.83.5.1
ip nhrp registration no-unique
tunnel source FastEthernet0/0
tunnel mode gre multipoint
tunnel key 555
tunnel protection ipsec profile DMVPN
!

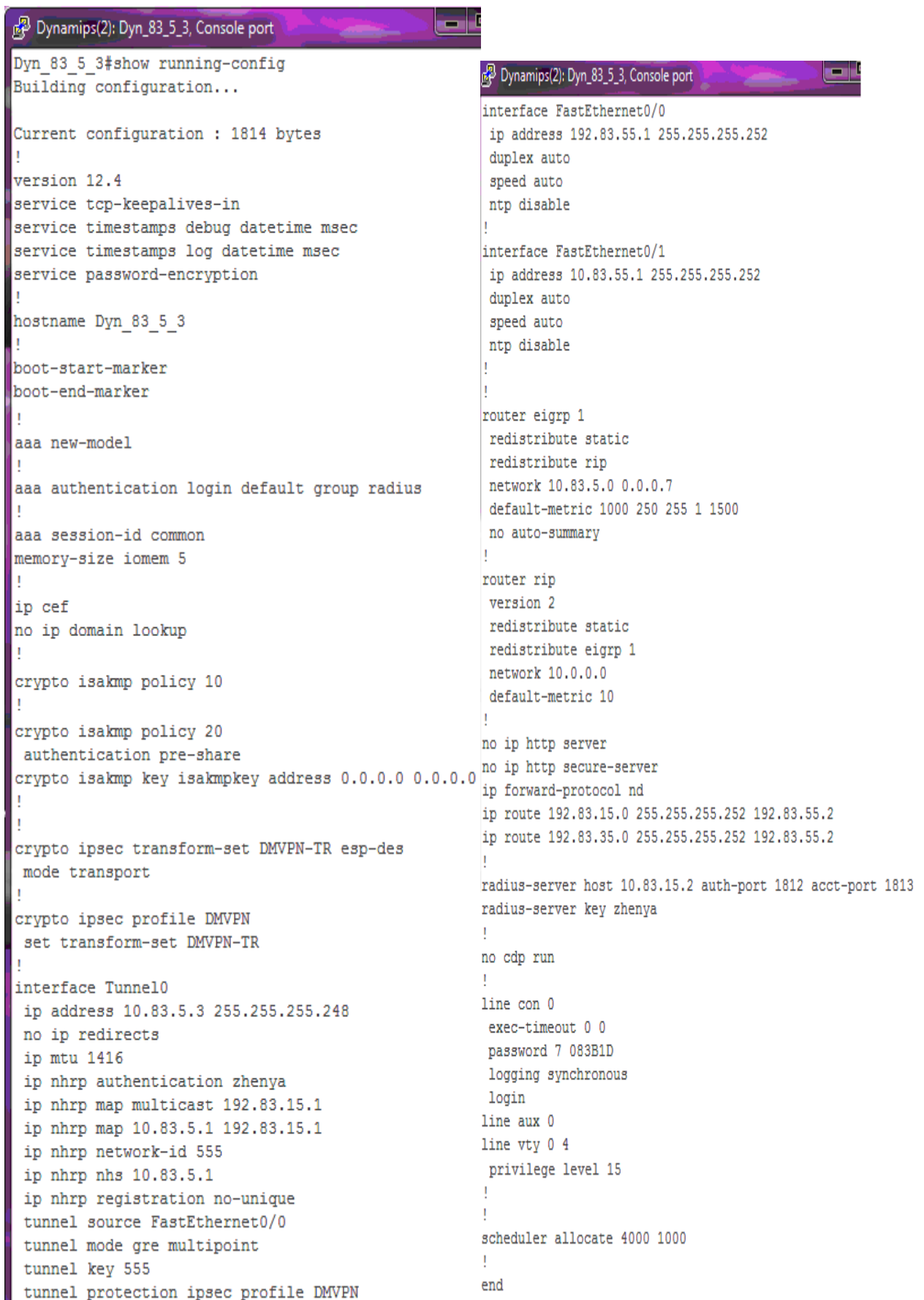
```

```

Dyn_83_5_2, Console port
interface FastEthernet0/0
ip address 192.83.35.1 255.255.255.252
duplex auto
speed auto
ntp disable
!
interface FastEthernet0/1
ip address 10.83.35.1 255.255.255.252
duplex auto
speed auto
ntp disable
!
!
router eigrp 1
 redistribute static
 redistribute rip
 network 10.83.5.0 0.0.0.7
 default-metric 1000 250 255 1 1500
 no auto-summary
!
router rip
 version 2
 redistribute static
 redistribute eigrp 1
 network 10.0.0.0
 default-metric 10
!
no ip http server
no ip http secure-server
ip forward-protocol nd
ip route 192.83.15.0 255.255.255.252 192.83.35.2
ip route 192.83.55.0 255.255.255.252 192.83.35.2
!
radius-server host 10.83.15.2 auth-port 1812 acct-port 1813
radius-server key zhenya
!
no cdp run
!
line con 0
 exec-timeout 0 0
 password 7 083B1D
 logging synchronous
 login
line aux 0
line vty 0 4
 privilege level 15
!
!
scheduler allocate 4000 1000
!
end

```

Рисунок Б.4 – Результат виконання команди show running-config Dyn_83_5_2



```
Dyn_83_5_3#show running-config
Building configuration...

Current configuration : 1814 bytes
!
version 12.4
service tcp-keepalives-in
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Dyn_83_5_3
!
boot-start-marker
boot-end-marker
!
aaa new-model
!
aaa authentication login default group radius
!
aaa session-id common
memory-size iomem 5
!
ip cef
no ip domain lookup
!
crypto isakmp policy 10
!
crypto isakmp policy 20
 authentication pre-share
crypto isakmp key isakmpkey address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set DMVPN-TR esp-des
 mode transport
!
crypto ipsec profile DMVPN
 set transform-set DMVPN-TR
!
interface Tunnel0
 ip address 10.83.5.3 255.255.255.248
 no ip redirects
 ip mtu 1416
 ip nhrp authentication zhenya
 ip nhrp map multicast 192.83.15.1
 ip nhrp map 10.83.5.1 192.83.15.1
 ip nhrp network-id 555
 ip nhrp nhs 10.83.5.1
 ip nhrp registration no-unique
 tunnel source FastEthernet0/0
 tunnel mode gre multipoint
 tunnel key 555
 tunnel protection ipsec profile DMVPN

interface FastEthernet0/0
 ip address 192.83.55.1 255.255.255.252
 duplex auto
 speed auto
 ntp disable
!
interface FastEthernet0/1
 ip address 10.83.55.1 255.255.255.252
 duplex auto
 speed auto
 ntp disable
!
!
router eigrp 1
 redistribute static
 redistribute rip
 network 10.83.5.0 0.0.0.7
 default-metric 1000 250 255 1 1500
 no auto-summary
!
router rip
 version 2
 redistribute static
 redistribute eigrp 1
 network 10.0.0.0
 default-metric 10
!
no ip http server
no ip http secure-server
ip forward-protocol nd
ip route 192.83.15.0 255.255.255.252 192.83.55.2
ip route 192.83.35.0 255.255.255.252 192.83.55.2
!
radius-server host 10.83.15.2 auth-port 1812 acct-port 1813
radius-server key zhenya
!
no cdp run
!
line con 0
 exec-timeout 0 0
 password 7 083B1D
 logging synchronous
 login
line aux 0
line vty 0 4
 privilege level 15
!
!
scheduler allocate 4000 1000
!
end
```

Рисунок Б.5 – Результат виконання команди show running-config Dyn_83_5_3

```

<Huawei_Global_1>display current-configuration
[V200R003C00]
#
sysname Huawei_Global_1
#
snmp-agent local-engineid 800007DB0300000000000000
snmp-agent
#
clock timezone Indian Standard Time minus 05:13:20
clock daylight-saving-time Day Light Saving Time repeating 12:32 9-1 12:32 11-23
#
drop illegal-mac alarm
#
stp disable
#
ike local-name huawei01
#
wlan ac-global carrier id other ac id 0
#
set cpu-usage threshold 80 restore 75
#
acl number 3101
rule 5 permit ip source 10.83.35.0 0.0.0.3 destination 10.83.50.0 0.0.0.31
#
ipsec proposal tran1
esp authentication-algorithm sha1
#
ike peer Huawei_Local_1 v1
exchange-mode aggressive
pre-shared-key cipher %K8m.Nt84DZ)e#<0'8bmE3Uw)%K8m
local-id-type name
remote-name huawei02
remote-address 105.83.45.1
#
ipsec policy map1 10 isakmp
security acl 3101
ike-peer Huawei_Local_1
proposal tran1
#
aaa
authentication-scheme default
authorization-scheme default
accounting-scheme default
domain default
domain default_admin

local-user admin password cipher %K8m.Nt84DZ)e#<0'8bmE3Uw)%K8m
local-user admin service-type http
#
firewall zone Local
priority 15
#
interface GigabitEthernet0/0/0
ip address 10.83.35.2 255.255.255.252
#
interface GigabitEthernet0/0/1
ip address 105.83.35.1 255.255.255.252
ipsec policy map1
#
interface GigabitEthernet0/0/2
#
interface NULL0
#
interface Tunnel0/0/0
ip address 11.83.35.1 255.255.255.252
tunnel-protocol gre
source 105.83.35.1
destination 105.83.45.1
#
rip 1
version 2
network 10.0.0.0
network 105.0.0.0
#
ssh client first-time enable
#
ip route-static 10.83.50.0 255.255.255.252 11.83.35.2
#
user-interface con 0
authentication-mode password
user-interface vty 0 4
user-interface vty 16 20
#
wlan ac
#
return
<Huawei_Global_1>

```

Рисунок Б.6 – Результат виконання команди display current-configuration на Huawei_Global_1

```

<Huawei_Global_2>display current-configuration
[V200R003C00]
#
sysname Huawei_Global_2
#
snmp-agent local-engineid 800007DB0300000000000000
snmp-agent
#
clock timezone Indian Standard Time minus 05:13:20
clock daylight-saving-time Day Light Saving Time repeating 12:32 9-1 12:32 11-23
#
drop illegal-mac alarm
#
stp disable
#
wlan ac-global carrier id other ac id 0
#
set cpu-usage threshold 80 restore 75
#
dhcp enable
#
ip pool 1
gateway-list 10.83.70.1
network 10.83.70.0 mask 255.255.255.128
dns-list 105.83.58.1 105.83.55.2
domain-name huawei2.com
#
acl number 3101
rule 5 permit ip source 10.83.55.0 0.0.0.3 destination 10.83.70.0 0.0.0.127
#
ipsec proposal tran1
esp authentication-algorithm sha1
#
ike peer Huawei_Local_2 v1
exchange-mode aggressive
pre-shared-key cipher %K8m.Nt84DZ)e#<0'8bmE3Uw)%K8m
local-id-type name
remote-name huawei02
remote-address 105.83.65.1
#
ipsec policy map2 10 isakmp
security acl 3101
ike-peer Huawei_Local_2
proposal tran1

#
aaa
authentication-scheme default
authorization-scheme default
accounting-scheme default
domain default
domain default_admin
local-user admin password cipher %K8m.Nt84DZ)e#<0'8bmE3Uw)%K8m
local-user admin servi
#
firewall zone Local
priority 15
#
interface GigabitEthernet0/0/0
ip address 10.83.55.2 255.255.255.252
ipsec policy map2
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
ip address 105.83.55.1 255.255.255.252
dhcp select global
#
interface NULL0
#
interface Tunnel0/0/0
ip address 11.83.55.1 255.255.255.252
tunnel-protocol gre
source 105.83.55.1
destination 105.83.65.1
#
rip 1
version 2
network 10.0.0.0
network 105.0.0.0
#
ssh client first-time enable
#
ip route-static 10.83.70.0 255.255.255.128 11.83.55.2
#
user-interface con 0
authentication-mode password
user-interface vty 0 4
user-interface vty 16 20
#
wlan ac
#
return
<Huawei_Global_2>

```

Рисунок Б.7 – Результат виконання команди display current-configuration на Huawei_Global_2

```

<Huawei_Local_1>display current-configuration
[V200R003C00]
#
sysname Huawei_Local_1
#
snmp-agent local-engineid 800007DB03000000000000
snmp-agent
#
clock timezone Indian Standard Time minus 05:13:20
clock daylight-saving-time Day Light Saving Time repeating 12:32 9-1 12:32 11-23
#
drop illegal-mac alarm
#
stp disable
#
ike local-name huawei02
#
wlan ac-global carrier id other ac id 0
#
set cpu-usage threshold 80 restore 75
#
rsa peer-public-key labnario
public-key-code begin
3047
0240
E3A7DD2A 41619DB8 87C393E6 37F8EC7F FE3CCC99 648127E9 5CB55853 682B6769
6A1A29AC F14C4B6C BB42D341 FFACE436 72629F6D 83BA629D 820EB648 FED5D523
0203
010001
public-key-code end
peer-public-key end
#
acl number 3101
rule 5 permit ip source 10.83.50.0 0.0.0.31 destination 10.83.35.0 0.0.0.3
#
ipsec proposal tran1
esp authentication-algorithm sha1
#
ike peer Huawei_Global_1 v1
exchange-mode aggressive
pre-shared-key cipher %%%$)H"z!S,^u*:l(AQmOU4+,.2n%%$
local-id-type name
remote-name huawei01
remote-address 10.83.35.1
#
ipsec policy use1 10 isakmp
security acl 3101
ike-peer Huawei_Global_1
proposal tran1
#
aaa
authentication-scheme default
authorization-scheme default
accounting-scheme default

domain default
domain default_admin
local-user z1 password cipher %%%$PJG5'PDeB:M'</;D7,10J%yc%%$
local-user z1 privilege level 15
local-user z1 ftp-directory flash:
local-user z1 service-type ssh ftp
local-user z2 password cipher %%%$@~]BTmpd7Ap-G|&L6i1MJ&u]%%$
local-user z2 ftp-directory flash:
local-user z2 service-type ssh ftp
local-user admin password cipher %%%$K8m.Nt84DZ)e#<0`8bmE3Uw)%%$
local-user admin service-type http
#
firewall zone Local
priority 15
#
interface GigabitEthernet0/0/0
ip address 105.83.45.1 255.255.255.252
ipsec policy use1
#
interface GigabitEthernet0/0/1
ip address 10.83.50.1 255.255.255.224
#
interface GigabitEthernet0/0/2
#
interface NULL0
#
interface Tunnel0/0/0
ip address 11.83.35.2 255.255.255.252
tunnel-protocol gre
source 105.83.45.1
destination 105.83.35.1
#
rip 1
version 2
network 105.0.0.0
network 10.0.0.0
#
ssh user z1 assign rsa-key labnario
ssh user z2 assign rsa-key labnario
sftp server enable
stelnet server enable
#
ip route-static 10.83.35.0 255.255.255.252 11.83.35.1
#
user-interface con 0
authentication-mode password
user-interface vty 0 4
authentication-mode aaa
protocol inbound ssh
user-interface vty 16 20
#
wlan ac
#
return
<Huawei_Local_1>
<Huawei_Local_1>

```

Рисунок Б.8 – Результат виконання команди display current-configuration на Huawei_Local_1

```

<Huawei_Local_2>display current-configuration
[V200R003C00]
#
sysname Huawei_Local_2
#
snmp-agent local-engineid 800007DB0300000000000000
snmp-agent
#
clock timezone Indian Standard Time minus 05:13:20
clock daylight-saving-time Day Light Saving Time repeating 12:32 9-1 12:32 11-23
#
drop illegal-mac alarm
#
stp disable
#
ike local-name huawei02
#
wlan ac-global carrier id other ac id 0
#
set cpu-usage threshold 80 restore 75
#
dhcp enable
#
rsa peer-public-key labnario
public-key-code begin
3047
0240
E3A7DD2A 41619DB8 87C393E6 37F8EC7F FE3CCC99 648127E9 5CB55853 682B6769
6A1A29AC F14C4B6C BB42D341 FFACE436 72629F6D 83BA629D 820EB648 FED5D523
0203
010001
public-key-code end
peer-public-key end
#
acl number 3101
rule 5 permit ip source 10.83.70.0 0.0.0.127 destination 10.83.55.0 0.0.0.3
#
ipsec proposal tran1
esp authentication-algorithm sha1
#
ike peer Huawei_Global_2 v1
exchange-mode aggressive
pre-shared-key cipher %%%H"z!S,^u*;1(AQmOU4+,.2n%%$
local-id-type name
remote-name huawei01
remote-address 10.83.55.1
#
ipsec policy use2 10 isakmp
security acl 3101
ike-peer Huawei_Global_2
proposal tran1
#
aaa
authentication-scheme default
authorization-scheme default
accounting-scheme default

domain default
domain default_admin
local-user z1 password cipher %%%$PJG5'PDeB:M'</:D7,10J%yc%%$
local-user z1 privilege level 15
local-user z1 ftp-directory flash:
local-user z1 service-type ssh ftp
local-user z2 password cipher %%%$~]BTmpd7Ap~G|&L611MJ&u]%%$
local-user z2 ftp-directory flash:
local-user z2 service-type ssh ftp
local-user admin password cipher %%%$K8m.Nc84DZ)e#<0`8bmE3Uw)%%$
local-user admin service-type http
#
firewall zone Local
priority 15
#
interface GigabitEthernet0/0/0
ip address 105.83.65.1 255.255.255.252
ipsec policy use2
#
interface GigabitEthernet0/0/1
ip address 10.83.70.1 255.255.255.128
dhcp select relay
dhcp relay server-ip 105.83.55.1
#
interface GigabitEthernet0/0/2
#
interface NULL0
#
interface Tunnel0/0/0
ip address 11.83.55.2 255.255.255.252
tunnel-protocol gre
source 105.83.65.1
destination 105.83.55.1
#
rip 1
version 2
network 10.0.0.0
network 105.0.0.0
#
ssh user z1 assign rsa-key labnario
ssh user z2 assign rsa-key labnario
sftp server enable
stelnet server enable
#
ip route-static 10.83.55.0 255.255.255.252 11.83.55.1
#
user-interface con 0
authentication-mode password
user-interface vty 0 4
authentication-mode aaa
protocol inbound ssh
user-interface vty 16 20
#
wlan ac
#
return
<Huawei_Local_2>
<Huawei_Local_2>

```

Рисунок Б.9 – Результат виконання команди display current-configuration на Huawei_Local_2

Після всіх налаштувань перевіримо працездатність мережі:

Для перевірки зв'язку будемо використовувати команди ping tracert (tracerout):

```

Dyn_83_5_1#traceroute 10.83.50.2

Type escape sequence to abort.
Tracing the route to 10.83.50.2

 0 10.83.5.2 672 msec 768 msec 788 msec
 1 10.83.35.2 784 msec 1168 msec 716 msec
 2 11.83.35.2 776 msec * 636 msec
 3 10.83.50.2 964 msec 1068 msec 1136 msec

```

Рисунок Б.10 – Маршрут слідування даних з 10.83.5.1 до 10.83.50.2

```

Dyn_83_5_1#traceroute 10.83.70.2

Type escape sequence to abort.
Tracing the route to 10.83.70.2

 0 10.83.5.3 384 msec 464 msec 544 msec
 1 10.83.55.2 840 msec 680 msec 672 msec
 2 11.83.55.2 896 msec 824 msec 776 msec
 3 10.83.50.2 1184 msec 1056 msec 1096 msec

```

Рисунок Б.11 – Маршрут прямування даних з 10.83.5.1 до 10.83.70.2

Проведемо перевірку зв'язку з робочими станціями з Hub-маршрутизатора (Dyn_83_5_1)

```

Dyn_83_5_1#ping 10.83.50.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.83.50.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 660/756/840 ms

```

Рисунок Б.12 – Наявний зв'язок та маршрут прямування даних Маршрут прямування з 10.83.5.1 до 10.83.50.2

```

Dyn_83_5_1#ping 10.83.70.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.83.70.2 timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 764/851/972 ms

```

Рисунок Б.13 – Наявний зв'язок та маршрут прямування даних Маршрут прямування з 10.83.5.1 до 10.83.70.2

No.	Time	Source	Destination	Protocol	Length	Info
383	416.640000	192.83.55.1	192.83.35.1	ISAKMP	186	Identity Protection (Main Mode)
384	417.201000	192.83.35.1	192.83.55.1	ISAKMP	146	Identity Protection (Main Mode)
385	417.533000	192.83.55.1	192.83.35.1	ISAKMP	314	Identity Protection (Main Mode)
386	417.911000	10.83.35.2	192.83.55.1	ICMP	62	Echo (ping) request id=0x6747, seq=2/512, ttl=62
387	418.052000	192.83.55.1	192.83.15.1	ESP	114	ESP (SPI=0x28671a65)
388	418.123000	192.83.35.1	192.83.55.1	ISAKMP	314	Identity Protection (Main Mode)
389	418.260000	192.83.15.1	192.83.55.1	ESP	122	ESP (SPI=0x160c6921)
390	418.453000	192.83.55.1	192.83.35.1	ISAKMP	142	Identity Protection (Main Mode)
391	418.822000	192.83.35.1	192.83.55.1	ISAKMP	110	Identity Protection (Main Mode)

Frame 383: 186 bytes on wire (1488 bits), 186 bytes captured (1488 bits)
 Ethernet II, Src: cc:09:10:e0:00:00 (cc:09:10:e0:00:00), Dst: cc:06:10:e0:00:10 (cc:06:10:e0:00:10)
 Internet Protocol Version 4, Src: 192.83.55.1 (192.83.55.1), Dst: 192.83.35.1 (192.83.35.1)
 User Datagram Protocol, Src Port: isakmp (500), Dst Port: isakmp (500)
 Internet Security Association and Key Management Protocol

Рисунок Б.14 – Перехоплений трафік за допомогою програми Wireshark

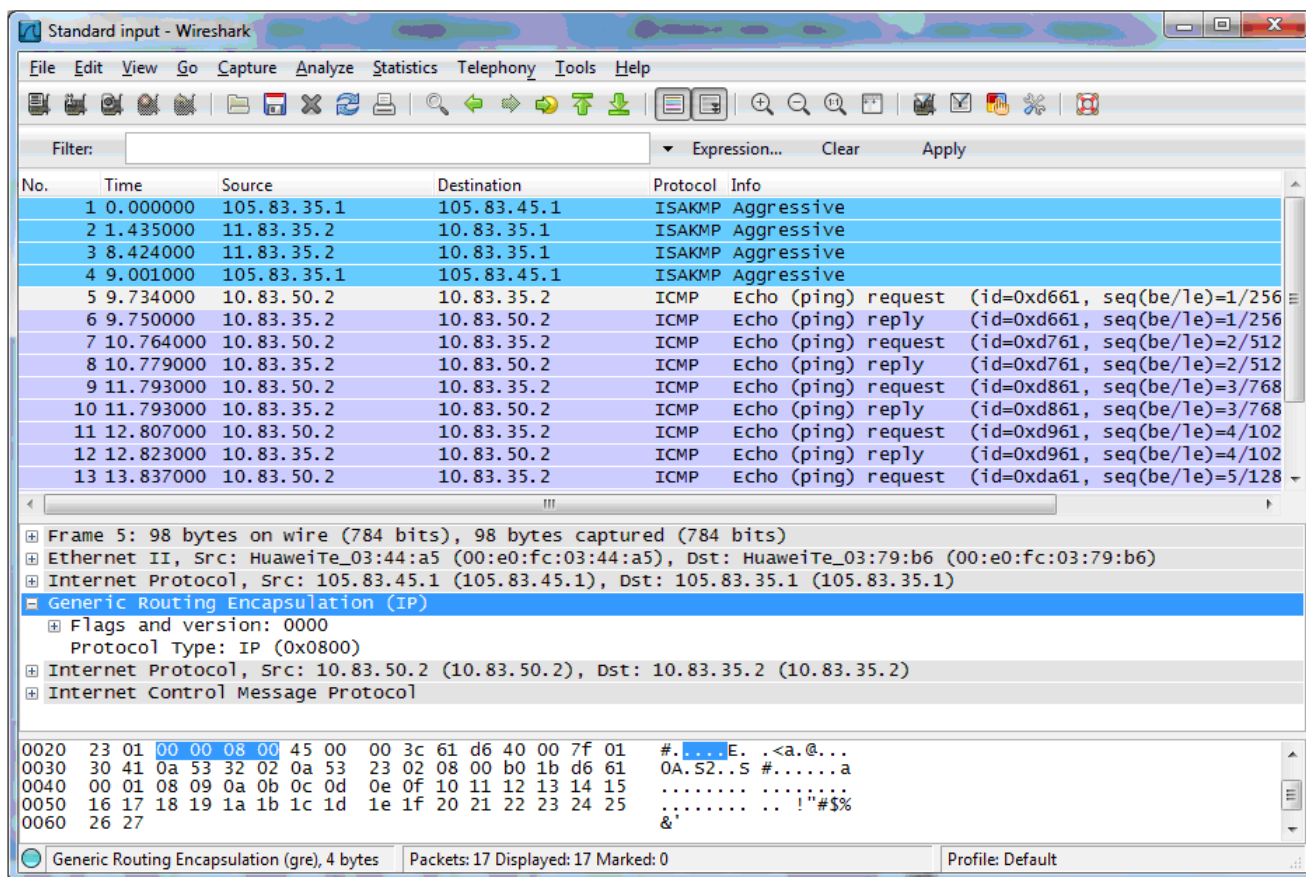


Рисунок Б.15 – Перехоплений трафік за допомогою програми Wireshark

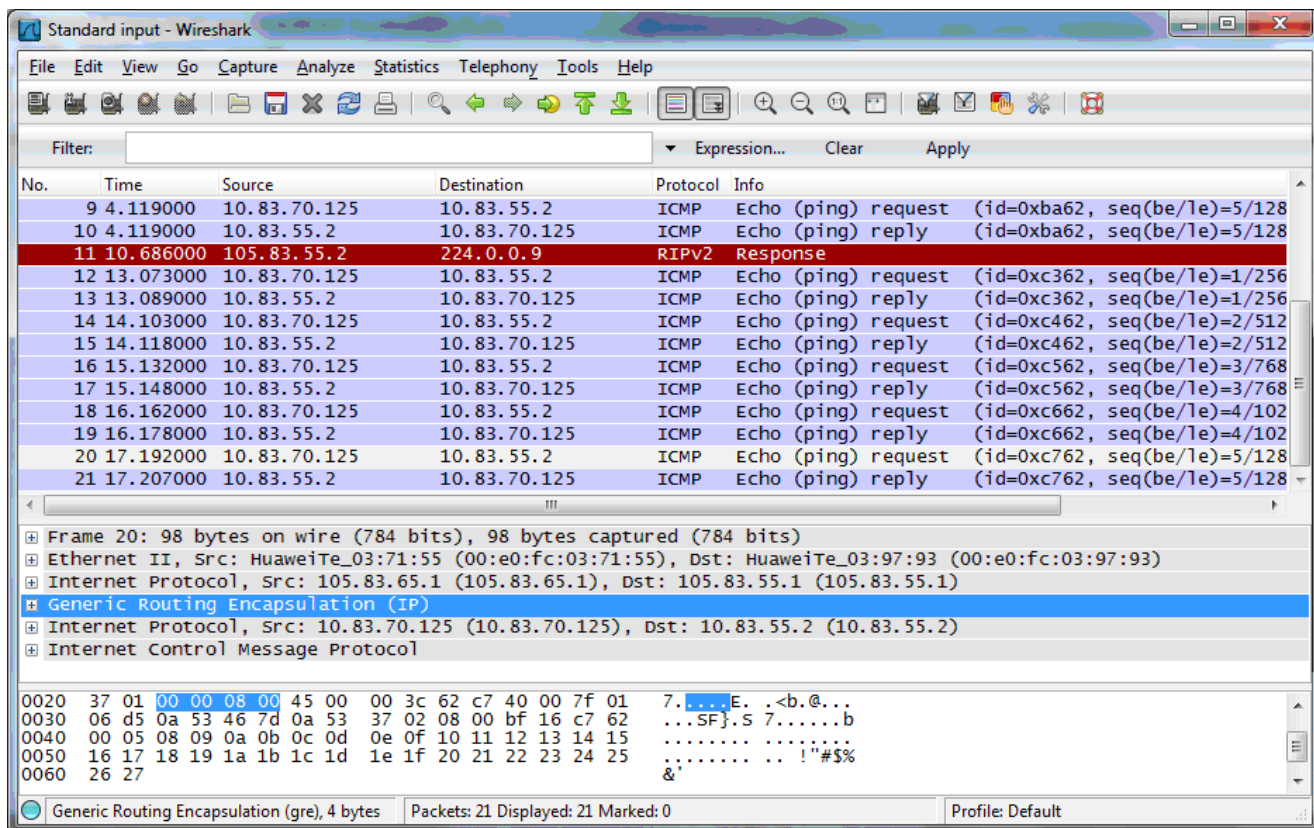


Рисунок Б.16 – Перехоплений трафік за допомогою програми Wireshark

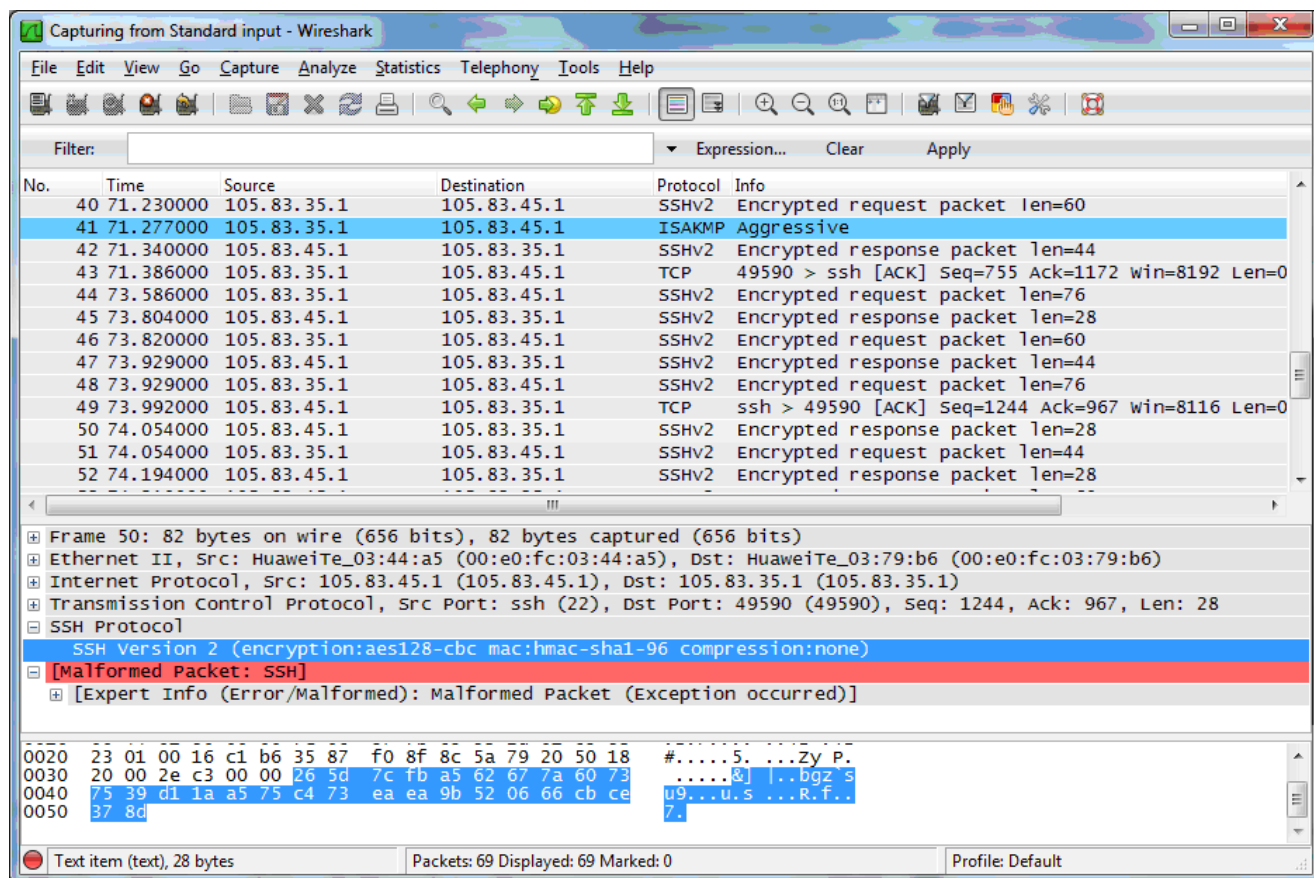


Рисунок Б.17 – перехоплений трафік за допомогою програми Wireshark