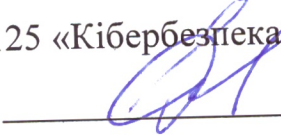


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

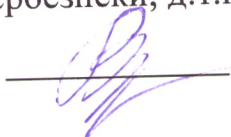
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи магістра
на тему: «Методи та засоби побудови підсистеми
захисту інтранет-мережі організації, побудованої з
використанням обладнання виробників Cisco та
MikroTik»

Виконав студент 2-го курсу, групи ЗКБм-22-1
Спеціальності 125 «Кібербезпека»

 В.О. Семеняк
Керівник доцент кафедри комп'ютерної
інженерії та кібербезпеки, к.пед.н., доцент

 О.С. Головня
Рецензент професор кафедри комп'ютерної
інженерії та кібербезпеки, д.т.н., доцент

 В.В. Воротніков

Житомир 2023

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

ЗАТВЕРДЖУЮ

Завідувач кафедри
комп'ютерної інженерії
та кібербезпеки

 Єфіменко А. А.
«13» 10 2023 р.

ЗАВДАННЯ

на випускн у кваліфікаційну роботу

Студент Семеняк Віктора Олександровича

Тема роботи: Методи та засоби побудови підсистеми захисту інтранет-мережі організації, побудованої з використанням обладнання виробників Cisco та MikroTik

затверджена Наказом по університету від 13 жовтня 2023 р. № 573/С

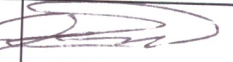
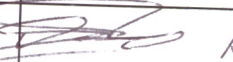
Термін здачі студентом закінченої роботи – «11» грудня 2023 р.

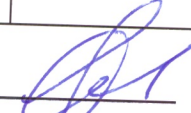
Вихідні дані для роботи:

1. Процеси захисту інформації в інтранет-мережі.
2. Методи та засоби побудови підсистеми захисту інтранет-мережі організації.

Обладнання та програмне забезпечення:

1. Образи мережевого обладнання Cisco та MikroTik.
2. ОС Windows.
3. Емулятор GNS3.
4. Програма віртуалізації VirtualBox.

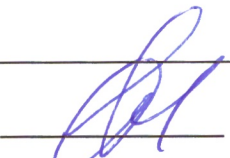
Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Єфіменко А.А.	 13.10.23	
2	Єфіменко А.А.	 13.10.23	
3	Єфіменко А.А.	 13.10.23	

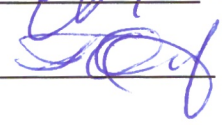
Студент  В.О. Семеняк

Керівник  О.С. Головня

Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	1 жовтня 2023 – 4 жовтня 2023	Виконано
2	Аналіз основ побудови захищених ІКМ	5 жовтня 2023 – 8 жовтня 2023	Виконано
3	Аналіз технологій захисту ІКМ	9 жовтня 2023 – 12 жовтня 2023	Виконано
4	Розробка проекту інтранет-мережі	13 жовтня 2023 – 15 жовтня 2023	Виконано
5	Розробка схеми адресації інтранет-мережі	16 жовтня 2023 – 20 жовтня 2023	Виконано
6	Розробка підсистем захисту інтранет-мережі	21 жовтня 2023 – 31 жовтня 2023	Виконано
7	Базове налагодження апаратного та програмного забезпечення	1 листопада 2023 – 10 листопада 2023	Виконано
8	Налаштування безпеки маршрутизаторів. Тестування роботи захищеної інтранет-мережі	11 листопада 2023 – 20 листопада 2023	Виконано
10	Оформлення пояснювальної записки	21 листопада 2023 – 6 грудня 2023	Виконано
11	Отримання відгуку керівника та рецензії на кваліфікаційну роботу		Виконано
12	Оформлення презентації та підготовка доповіді		Виконано
13	Захист		Виконано

Студент  В.О. Семеняк

Керівник  О.С. Головня

АНОТАЦІЯ

Випускна кваліфікаційна робота на тему «Методи та засоби побудови підсистеми захисту інтранет-мережі організації, побудованої з використанням обладнання виробників Cisco та MikroTik» складається зі вступу, трьох розділів, висновків, переліку посилань, додатків і має 57 сторінок основного тексту, 19 рисунків, 15 таблиць, 10 сторінок додатків. Список використаних джерел містить 12 найменувань і займає 1 сторінку. Загальний обсяг роботи – 66 сторінок.

Метою проекту є розробка підсистеми захисту інтранет-мережі організації, побудованої з використанням обладнання виробників Cisco та MikroTik.

У проекті вирішено задачу захисту інформації, яка функціонує в інтранет-мережі організації для обладнання провідних виробників мережевого обладнання Cisco та MikroTik.

У проекті проаналізовано теоретичні основи побудови віртуальних захищених мереж, розроблено проект захищеної інтранет-мережі, обґрунтовано вибір реального обладнання виробників Cisco та MikroTik, проведено налагодження захищеної інтранет-мережі мережі та проведено тестування її роботи.

Можливі напрямки розвитку цієї роботи пов'язані з використанням досліджень у побудові захищених гетерогенних мереж з використанням мережевого обладнання різних виробників та їх мережевої взаємодії між собою в одній захищеній інтранет-мережі.

Ключові слова: ЗАХИСТ ІНФОРМАЦІЇ, ІНТРАНЕТ-МЕРЕЖА, ПІДСИСТЕМА ЗАХИСТУ, ОБЛАДНАННЯ CISCO, ОБЛАДНАННЯ MIKROTIK, ВІРТУАЛЬНА ЗАХИЩЕНА МЕРЕЖА, МЕРЕЖЕВА ВЗАЄМОДІЯ.

ABSTRACT

The final qualification work on the topic «Methods and tools for building a security subsystem for an organisation's intranet network, built using equipment from Cisco and MikroTik» consists of an introduction, four chapters, conclusions, a list of references, appendices and has 56 pages of main text, 19 figures, 15 tables, 10 pages of appendices. The list of references includes 12 titles and occupies 1 page. The total volume of the work is 65 pages.

The aim of the project is to develop a security subsystem for an organisation's intranet network, built using equipment from Cisco and MikroTik.

The project solves the problem of protecting information that operates in the organisation's intranet network for equipment from leading network equipment manufacturers Cisco and MikroTik.

The project analyses the theoretical foundations of building virtual secure networks, develops a secure intranet project, justifies the choice of real equipment from Cisco and MikroTik, sets up the secure intranet of the network and tests its operation.

Possible directions for the development of this work are related to the use of research in the construction of secure heterogeneous networks using network equipment from different manufacturers and their network interaction with each other in one secure intranet network.

Keywords: INFORMATION SECURITY, INTRANET NETWORK, SECURITY SUBSYSTEM, CISCO EQUIPMENT, MIKROTIK EQUIPMENT, VIRTUAL SECURE NETWORK, NETWORK INTERACTION.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ.....	8
ВСТУП.....	9
1. ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ ПІДСИСТЕМИ ЗАХИСТУ ІНТРАНЕТ-МЕРЕЖІ.....	10
1.1. Технології побудови віртуальних приватних мереж	10
1.2. Використання алгоритму шифрування 3DES у побудові захищених приватних мереж	21
1.3. Огляд можливостей захисту операційної системи Cisco IOS.....	24
1.4. Огляд можливостей захисту операційної системи RouterOS.....	28
2. РОЗРОБКА ПРОЕКТУ ПІДСИСТЕМИ ЗАХИСТУ ІНТРАНЕТ- МЕРЕЖІ	32
2.1. Розробка топології інтранет-мережі.....	32
2.2. Розробка системи адресації інтранет-мережі	34
2.3. Розробка базових та додаткових засобів захисту інтранет- мережі.....	40
3. ОБГРУНТУВАННЯ ВИБОРУ ОБЛАДНАННЯ ТА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, НАЛАШТУВАННЯ ТА ПЕРЕВІРКА РОБОТИ ЗАХИЩЕНОЇ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ МЕРЕЖІ	42
3.1. Обґрунтування вибору обладнання та програмного забезпечення.....	42
3.2. Налагодження базових засобів міжмережевої взаємодії	43
3.3. Налагодження засобів захисту	47
3.4. Тестування роботи захищеної інтранет-мережі	49
ВИСНОВКИ	54
ПЕРЕЛІК ПОСИЛАНЬ.....	55
ДОДАТКИ	57

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ІМ – Інтранет-мережа

РС – Робоча станція

ПЗ – Програмне забезпечення

ЗІ – Захист інформації

ОЦ – Обчислювальний центр

ЕОМ – Електронна обчислювальна машина

МЗ – Мережа зв'язку

VPN – Віртуальна захищена мережа

OSI – Модель взаємодії відкритих систем

ВСТУП

Актуальність теми. Останнім часом у світі відбуваються якісні зміни в процесах управління на всіх рівнях, обумовлені інтенсивним упровадженням сучасних інформаційних технологій. Паралельно зростає небезпека несанкціонованого втручання в роботу інформаційних і телекомунікаційних систем, причому вагомість можливих наслідків такого втручання для суспільства зростає настільки, що найбільш розвинені держави, їх фінансові і промислові структури стали якоюсь мірою “заручниками” своїх інформаційних систем.

Поряд із традиційним способом захисту інформації особливу актуальність у даний час набуває безпека інформаційних технологій, у першу чергу пов’язаних з передачею інформації в локальних мережах, які мають доступ до глобальної мережі Інтернет.

Мета випускної кваліфікаційної роботи – розробка підсистеми захисту інтранет-мережі організації, побудованої з використанням обладнання виробників Cisco та MikroTik.

Об’єкт дослідження – процеси захисту інформації в інтранет-мережі.

Предмет дослідження – методи та засоби побудови підсистеми захисту інтранет-мережі організації.

Визначена мета обумовлює наступні **завдання**:

- розглянути технології побудови віртуальних приватних мереж та використання алгоритму шифрування 3DES у побудові захищених приватних мереж;
- розглянути можливості захисту операційних систем Cisco IOS та RouterOS;
- розробити топологію, систему адресації, базові та додаткові засоби захисту інтранет-мережі;
- обґрунтувати вибір обладнання та програмного забезпечення;
- налагодити базові засоби міжмережевої взаємодії;
- протестувати роботу захищеної інтранет-мережі.

1. ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ ПІДСИСТЕМИ ЗАХИСТУ ІНТРАНЕТ-МЕРЕЖІ

1.1. Технології побудови віртуальних приватних мереж

Технології побудови віртуальних приватних мереж органічно вписуються в бізнес компаній, що мають розподілену філіальну структуру: банки і страхові компанії, роздрібні мережі, промислові холдинги. Об'єднуватися можуть як локальні, так і територіально розподілені корпоративні мережі. Інформація в них передається по загальнодоступних каналах, тому потенційно можливе порушення конфіденційності, цілісності та доступності інформації. Одним з ефективних підходів до захисту інформації від наведених загроз є технологія VPN.

VPN (Віртуальна приватна мережа, англ. *Virtual Private Network*) – це логічна мережа, створена поверх інших мереж, на базі загальнодоступних або віртуальних каналів інших мереж. Безпека передавання пакетів через загальнодоступні мережі може реалізуватися за допомогою шифрування, внаслідок чого створюється закритий для сторонніх канал обміну інформацією. VPN дозволяє об'єднати, наприклад, декілька географічно віддалених мереж організації в єдину мережу з використанням для зв'язку між ними непідконтрольних каналів [2].

Суть цієї технології в тому, що при підключенні до VPN сервера за допомогою спеціального програмного забезпечення поверх загальнодоступної мережі у вже встановленому з'єднанні організується зашифрований канал, що забезпечує високий рівень захисту каналу передачі інформації. Використання технології VPN доцільно для захисту корпоративної мережі від дії вірусів, зловмисників, а також від інших загроз, які є результатом помилок в конфігурації або адміністрування мережі [5].

Можна виділити три основні технології захисту інформації що перетворюють накладену корпоративну мережу, побудовану на базі мережі

загального користування, у захищену віртуальну приватну мережу: шифрування, аутентифікація та контроль доступу.

Тільки реалізація всіх цих трьох властивостей дозволяє захистити інформаційні ресурси корпорації та фізично незахищені канали зв'язку від несанкціонованого доступу та витоку інформації [11].

Як приклад створення віртуальної мережі можна навести використання інкапсуляції протоколу PPP в будь-який інший протокол IP (ця реалізація називається PPTP – Point-to-Point Tunneling Protocol) або Ethernet (PPPoE).

VPN складається з двох частин: “внутрішня” (підконтрольна) мережа, яких може бути декілька, і “зовнішня” мережа, через яку проходять інкапсульовані з'єднання (зазвичай використовується мережа Інтернет) [16].

Підключення до VPN віддаленого користувача робиться за допомогою сервера доступу, який підключений як до внутрішньої, так і до зовнішньої (загальнодоступною) мережі. При підключенні віддаленого користувача (або при встановленні з'єднання з іншою захищеною мережею) сервер доступу вимагає проходження процесу ідентифікації, а потім процесу аутентифікації. Після успішного проходження обох процесів, віддалений користувач (віддалена мережа) наділяється повноваженнями для роботи в мережі, тобто відбувається процес авторизації.

VPN з'єднання завжди складається з каналу типу точка-точка, також відомого під назвою тунель. Тунель створюється в незахищеній мережі, якою найчастіше виступає Інтернет. З'єднання точка-точка має на увазі, що воно завжди встановлюється між двома вузлами. Кожен вузол відповідає за шифрування даних до того, як вони потраплять в тунель і розшифровку цих даних після того, як вони покинуть тунель.

Хоча VPN-тунель завжди встановлюється між двома точками, кожен вузол може встановлювати додаткові тунелі з іншими вузлами. Для прикладу, коли трьом віддаленим станціям необхідно зв'язатися з одним і тим же офісом, буде створено три окремих VPN-тунелів до цього офісу. Для усіх тунелів вузол на стороні офісу може бути одним і тим же. Це можливо

завдяки тому, що вузол може шифрувати і розшифровувати дані від імені усієї мережі.

В цьому випадку VPN-вузол називається VPN-шлюзом, а мережа за ним – доменом шифрування (encryption domain). Використання шлюзів зручне з кількох причин. По-перше, усі користувачі повинні пройти через один пристрій, який полегшує завдання управління політикою безпеки і контролю вхідного та вихідного трафіку мережі. По-друге, персональні тунелі до кожної робочої станції, до якої користувачеві потрібно отримати доступ, дуже швидко стануть некерованими (оскільки тунель – це канал типу точка-точка).

За наявності шлюзу, користувач встановлює з'єднання з ним, після чого користувачеві відкривається доступ до мережі (домену шифрування).

Цікаво відмітити, що всередині домену шифрування самого шифрування не відбувається. Причина в тому, що ця частина мережі вважається безпечною і такою, що знаходиться під безпосереднім контролем в протилежність Інтернет. Це справедливо і при з'єднанні офісів за допомогою VPN-шлюзів. Таким чином гарантується шифрування тільки тієї інформації, яка передається по небезпечному каналу між офісами [11].

Окремим пунктом слід відмітити використання тунелювання при побудові VPN.

Тунелювання (tunneling) або інкапсуляція (encapsulation) – це спосіб передачі інформації через проміжну мережу. Такою інформацією можуть бути кадри (або пакети) іншого протоколу. При інкапсуляції кадр не передається в згенерованому вузлом-відправником вигляді, а забезпечується додатковим заголовком, містить інформацію про маршрут, що дозволяє інкапсульованим пакетам проходити через проміжну мережу (Internet). На кінці тунелю кадри деінкапсуються і передаються одержувачу [2].

Цей процес (що включає інкапсуляцію і передачу пакетів) і є тунелюванням. Логічна топологія транзитної мережі пересування інкапсульованих пакетів називається тунелем.

VPN-пристрій розташовується між внутрішньою мережею і Internet на кожному кінці з'єднання. Під час передачі даних через VPN, вони зникають “з поверхні” в точці відправлення і знову з'являються тільки в точці призначення. Завдяки тунелюванню приватна інформація стає недоступною для інших користувачів. Перш ніж потрапити в Internet-тунель дані шифруються, що забезпечує їх додатковий захист. Протоколи шифрування визначаються VPN-рішенням. Розглянемо протоколи які використовує VPN.

PPTP (Point-to-Point Tunneling Protocol) – тунельний протокол “точка-точка”. Протокол PPTP є розширенням протоколу PPP (Point-to-Point Protocol – протокол “точка-точка”) і використовує механізми перевірки автентичності, стиснення і шифрування цього протоколу.

Інкапсуляція. Кадр PPP поміщається в оболонку з заголовком GRE (Generic Routing Encapsulation) і заголовком IP. У заголовку IP-адреси відправника і отримувача відповідають VPN-клієнту і VPN-сервера.

L2TP (Layer Two Tunneling Protocol) – протокол тунелювання другого рівня. L2TP використовує засоби шифрування, які надаються методом IPSec. Комбінацію L2TP та IPSec називають L2TP/IPSec. Комбінація L2TP/IPSec забезпечує роботу служб VPN, що виконують інкапсуляцію і шифрування приватних даних.

Протокол L2TP встановлюється разом з протоколом TCP/IP. У залежності від параметрів, вибраних у майстрі настройки сервера маршрутизації та віддаленого доступу.

Інкапсуляція пакетів L2TP/IPSec виконується в два етапи.

1. Інкапсуляція L2TP. Кадр PPP (IP-датаграма або IPX-датаграма) поміщається в оболонку з заголовком L2TP і заголовком UDP.
2. Потім отримане L2TP-повідомлення поміщається в оболонку з заголовком і трейлером IPSec ESP (Encapsulating Security Payload), трейлером перевірки автентичності IPSec, що забезпечує цілісність повідомлення та перевірку справжності, і заголовком IP.

У заголовку IP-адреси відправника і отримувача відповідають VPN-клієнту і VPN-сервера. Повідомлення L2TP шифрується з використанням

стандарту DES (Data Encryption Standard) або 3DES за допомогою ключів шифрування, створених у процесі узгодження IKE (Internet Key Exchange – обмін ключами в Інтернеті) [24].

Всі продукти для створення VPN можна умовно розділити на дві категорії: програмні і апаратні. Програмне рішення для VPN – це, як правило, готовий додаток, що встановлюється на підключеному до мережі окремому комп’ютері.

Оскільки для побудови VPN на базі спеціалізованого програмного забезпечення потрібне створення окремої комп’ютерної системи, такі рішення зазвичай складніше для розгортання, ніж апаратні. Створення подібної системи передбачає конфігурування сервера для розпізнавання даного комп’ютера і його операційної системи, VPN-пакета, мережевих плат для кожного з’єднання і спеціальних плат для прискорення операцій шифрування.

Розгорнути апаратно VPN, безумовно легше. Для цього необхідно підключити мережеве обладнання (комутатори, концентратори, маршрутизатори), які підтримують VPN протоколи.

VPN класифікуються за багатьма параметрами. Класифікація VPN представлена на рисунку 1.1.



Рисунок 1.1 – Класифікація VPN

Розглянемо більш детально класифікацію VPN у .

За ступенем захищеності використовуваного середовища. Найбільш поширений варіант віртуальних приватних мереж є захищені мережі. З його допомогою можливо створити надійну і захищену підмережу на основі ненадійної мережі, як правило, Інтернету. Прикладом захищених VPN є: IPSec, OpenVPN і PPTP.

Довірчі використовуються у випадках, коли середовище, яке використовується, можна вважати надійним і необхідно вирішити лише завдання створення віртуальної підмережі в рамках більшої мережі. Питання забезпечення безпеки стають неактуальними. Прикладами подібних VPN рішень є: Multi-protocol label switching (MPLS) і L2TP (Layer 2 Tunnelling Protocol). (Точніше сказати, що ці протоколи перекладають завдання забезпечення безпеки на інші, наприклад L2TP, як правило, використовується в парі з IPSec).

За способом реалізації. У вигляді спеціального програмно-апаратного забезпечення. Реалізація VPN мережі здійснюється за допомогою спеціального комплексу програмно-апаратних засобів. Така реалізація забезпечує високу продуктивність і, як правило, високий ступінь захищеності.

У вигляді програмного рішення. Використовують персональний комп'ютер зі спеціальним програмним забезпеченням, що забезпечує функціональність VPN.

Інтегроване рішення: функціональність VPN забезпечує комплекс, який вирішує також задачі фільтрації мережевого трафіку, організації мережевого екрану і забезпечення якості обслуговування.

Intranet VPN використовують для об'єднання в єдину захищену мережу декількох розподілених філій однієї організації, які обмінюються даними по відкритих каналах зв'язку.

Remote Access VPN використовують для створення захищеного каналу між сегментом корпоративної мережі (центрального офісу або філією) та одиночним користувачем, який, працюючи вдома, підключається до

корпоративних ресурсів з домашнього комп'ютера, корпоративного ноутбука, смартфона або інтернет-кіоска.

Extranet VPN використовують для мереж, до яких підключаються “зовнішні” користувачі (наприклад, замовники або клієнти). Рівень довіри до них набагато нижче, ніж до співробітників компанії, тому потрібно забезпечити спеціальні “рубежі” захисту, що запобігають або обмежують доступ останніх до особливо цінної, конфіденційної інформації.

Internet VPN використовується для надання доступу до Інтернету провайдерами, звичайно у випадку якщо по одному фізичному каналу підключаються кілька користувачів.

Client/Server VPN забезпечує захист переданих даних між двома вузлами (не мережами) корпоративної мережі. Особливість даного варіанта в тому, що VPN будується між вузлами, що перебувають, як правило, в одному сегменті мережі, наприклад, між робочою станцією і сервером. Така необхідність дуже часто виникає в тих випадках, коли в однієї фізичної мережі необхідно створити декілька логічних мереж. Наприклад, коли треба розділити трафік між фінансовим департаментом та відділом кадрів, що звертаються до серверів, що знаходяться в одному фізичному сегменті. Цей варіант схожий на технологію VLAN, але замість поділу трафіку, використовується його шифрування [2].

За типом протоколу: існують реалізації віртуальних приватних мереж під TCP/IP, IPX і AppleTalk. Але на сьогоднішній день спостерігається тенденція до загального переходу на протокол TCP/IP, і абсолютна більшість VPN рішень підтримує саме його. Адресація в ньому найчастіше вибирається у відповідності зі стандартом RFC5735, з діапазону Приватних мереж TCP/IP.

За рівнем мережевого протоколу класифікуються на основі зіставлення з рівнями еталонної мережевої моделі OSI.

При об'єднанні локальних мереж в загальну VPN мережу отримується цілком працездатний загальний простір при мінімальних витратах і високій мірі захисту. Для створення такої мережі встановлюється на одному комп'ютері з кожного сегменту спеціальний VPN-шлюз, який відповідатиме

за передачу даних між філіями. Обмін інформацією в кожному відділенні здійснюється звичайним способом, проте у тому разі якщо необхідно передати дані на іншу ділянку VPN-мережі, то вони вирушають на шлюз. У свою чергу шлюз здійснює обробку даних, шифрує їх за допомогою надійного алгоритму і передає по мережі Інтернет цільовому шлюзу в іншій філії. У точці призначення дані розшифровуються і також передаються на кінцевий комп'ютер звичайним способом. Усе це проходить абсолютно непомітно для користувача і нічим не відрізняється від роботи в локальній мережі. Окрім цього VPN є чудовим способом організації доступу окремого комп'ютера в локальну мережу компанії. Уявіть собі, що ви знаходитесь у відрядженні зі своїм ноутбуком і зіткнулися з необхідністю підключитися до своєї мережі, або викачати звідти які або дані. За допомогою спеціальної програми існує можливість з'єднатися з VPN-шлюзом вашої локальної мережі і працювати так само як будь-який інший співробітник вашої компанії знаходиться в офісі.

Одними з небагатьох недоліків, які має технологія VPN, є необхідність закупівлі невеликої кількості устаткування і програмного забезпечення, а також збільшення об'ємів зовнішнього трафіку. Втім ці витрати досить невеликі і враховуючи величезну кількість переваг VPN, з ними цілком можна миритися.

На основі аналізу технологій захисту інформації корпоративних мереж найефективнішим методом захисту VPN є тунелювання з використанням протоколу IPSec [11].

IPsec (скорочення від IP Security) – набір протоколів для забезпечення захисту даних, що передаються за допомогою протоколу IP, дозволяє здійснювати підтвердження автентичності та шифрування IP-пакетів. IPsec також містить в собі протоколи для захищеного обміну ключами в мережі Інтернет.

Спочатку IPsec включав в себе три алгоритми – незалежні базові специфікації: “Архітектура безпеки IP”, “Аутентифікуючий заголовок (AH)”, “Інкапсуляція зашифрованих даних (ESP)”. Крім цього, існують декілька

алгоритмів – залежних специфікацій, що використовують протоколи MD5, SHA, DES, 3DES, AES. На рисунку 1.2 зображено архітектуру IPSec.

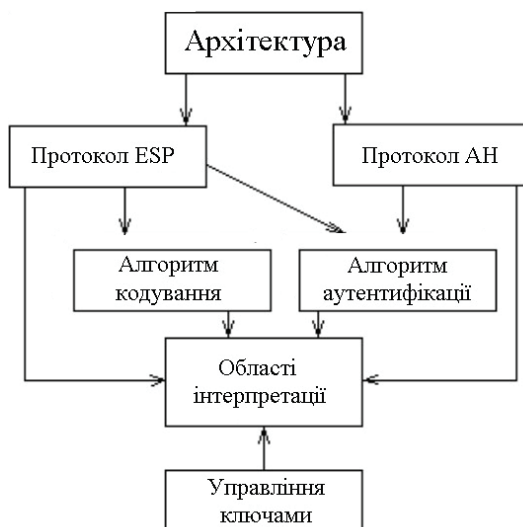


Рисунок 1.2 – Архітектура IPSec

IPSec спирається на ряд технологічних рішень і методів шифрування, але роботу IPSec в загальному можна представити у вигляді наступних послідовних процесів:

Початок процесу IPSec. Трафік, якому потрібно шифрування відповідно до політики захисту IPSec, узгодженої сторонами IPSec, починає IKE – процес.

Перша фаза IKE. IKE-процес виконує аутентифікацію сторін IPSec і веде переговори про параметри асоціацій захисту IKE, в результаті чого створюється захищений канал для ведення переговорів про параметри асоціацій захисту IPSec в ході другої фази IKE.

Друга фаза IKE. IKE-процес веде переговори про параметри асоціації захисту IPSec і встановлює відповідні асоціації захисту IPSec для пристроїв сполучених сторін.

Передача даних. Відбувається обмін даними між сполученими сторонами IPSec, який ґрунтується на параметрах IPSec і ключах, що зберігаються в базі даних асоціацій захисту.

Завершення роботи тунелю IPSec. Асоціації захисту IPSec завершують свою роботу або в результаті їх видалення, або через перевищення граничного часу їх існування [16].

IPSec діє або в тунельному, або в транспортному режимі. На рисунку 1.3 показано схему реалізації тунельного режиму. У цьому режимі вся початкова дейтаграма IP шифрується і стає корисним вантажем в новому пакеті IP з новим заголовком IP і додатковим заголовком IPSec (заголовок позначений аббревіатурою HDR). Тунельний режим дозволяє мережному пристрою (наприклад, брандмауеру PIX Firewall) виступати в ролі шлюзу IPSec або проксі – сервера, що виконує шифрування для хостів, розміщених за брандмауером. Маршрутизатор джерела шифрує пакет і передає його по тунелю IPSec. Брандмауер PIX Firewall адресата дешифрує отриманий пакет IPSec, витягує вихідну дейтаграму IP і передає її системі адресата. Головна перевага тунельного режиму полягає в тому, що не потрібно модифікувати кінцеві системи, щоб забезпечити їм можливість використання IPSec. Тунельний режим також не дозволяє аналізувати потік даних. При обміні в тунельному режимі існує можливість визначити тільки кінцеві точки тунелю, але не істинних джерела і адресата проходять через тунель пакетів, навіть якщо кінцеві точки тунелю перебувають саме в системах джерела і адресата.

У транспортному режимі шифрується тільки корисний вантаж IP, а вихідний заголовок IP залишається незмінним. Додається заголовок IPSec. Перевагою цього режиму є додавання тільки декількох байтів до кожного пакету. Крім того, пристрої відкритої мережі можуть бачити справжні адреси відправника і одержувача пакету (рис. 1.4).

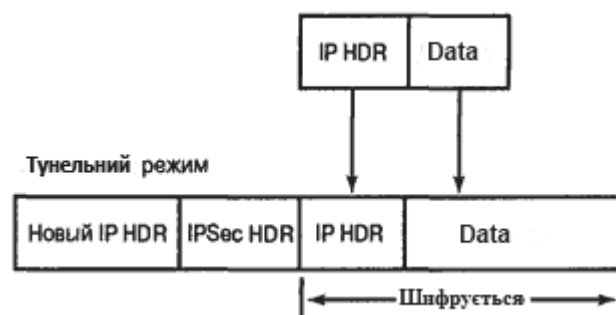


Рисунок 1.3 – Схема реалізації тунельного режиму

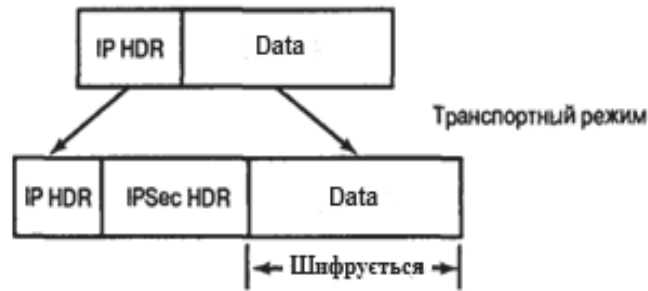


Рисунок 1.4 – Схема реалізації транспортного режиму

Це дозволяє використовувати спеціальні можливості проміжних мереж (наприклад, гарантована якість сервісу), засновані на інформації в заголовку IP. Однак заголовок рівня 4 шифрується, що обмежує можливості аналізу пакету. На жаль, передача заголовка IP у відкритому вигляді в транспортному режимі дозволяє порушнику в певній мірі виконати аналіз потоку даних. Наприклад, порушник може з'ясувати, скільки пакетів було передано сторонами IPsec, що діють в транспортному режимі. Але порушник може дізнатися тільки про те, що пакети IP пересилалися. Він не зможе визначити, чи були вони повідомленням електронної пошти або якимось іншим додатком, якщо використовувався протокол ESP [16].

Перетворення IPsec. Як видно, перетворення IPsec задає один протокол захисту IPsec (AH або ESP) з відповідними алгоритмами і режимом. Перетворення AH пропонує механізм аутентифікації корисного вантажу, а перетворення ESP-метод корисного шифрування вантажу. На рисунку 1.5 наведені можливі комбінації перетворень.

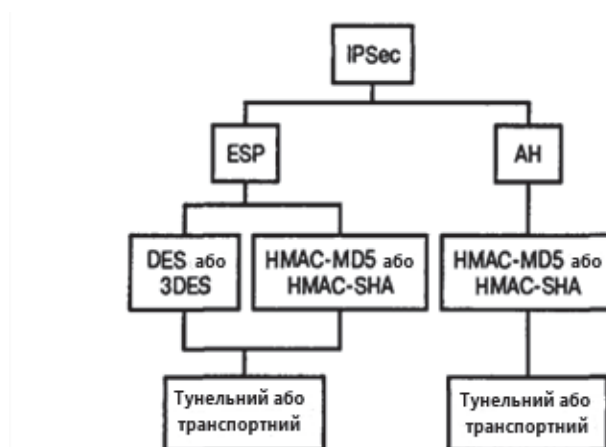


Рисунок 1.5 – Комбінації перетворень IPsec

Отже, протокол IPsec домінує в більшості реалізацій віртуальних приватних мереж. В даний час на ринку представлені як програмні реалізації (наприклад, протокол реалізований в операційній системі Windows2000 компанії Microsoft), так і програмно-апаратні реалізації IPsec – це рішення Cisco, Nokia. Незважаючи на велику кількість різних рішень, всі вони досить добре сумісні один з одним.

1.2. Використання алгоритму шифрування 3DES у побудові захищених приватних мереж

Triple DES (3DES) – симетричний блоковий шифр, створений в 1978 році на основі алгоритму DES, з метою усунення головного недоліку останнього – малої довжини ключа (56 біт), який може бути зламаний методом повного перебору ключа. Швидкість роботи 3DES в 3 рази нижче, ніж у DES, але криптостійкість набагато вище – час, необхідний для криптоаналізу 3DES, може бути в мільярд разів більше, ніж час, потрібний для розтину DES. 3DES використовується частіше, ніж DES, який легко зламується за допомогою сучасних технологій (в 1998 році організація Electronic Frontier Foundation, використовуючи спеціальний комп'ютер DES Cracker, розкрила DES за 3 дні). 3DES є простим способом усунення недоліків DES. Алгоритм 3DES побудований на основі DES, тому для його реалізації можливо використовувати програми, створені для DES [13].

Використання алгоритму 3DES у побудові захищеної приватної мережі представлено на рисунку 1.6.



Рисунок 1.6 – Використання алгоритму 3DES

У побудові захищеної приватної мережі 3DES зазвичай використовується наступним чином: за допомогою загального секретного ключа шифруються відкриті дані на одному маршрутизаторі, отримані зашифровані дані передаються на другий маршрутизатор, де вони розшифровуються за допомогою загального секретного ключа, внаслідок чого отримуються відкриті дані.

3DES виконує 3 рази алгоритм DES, довжина ключа DES дорівнює 64 біта, а довжина 3DES в 3 рази більше, тобто дорівнює 192 бітів. Для DES 64-розрядний ключ ділився на 8 байтів, в кожному байті використовується тільки 7 бітів, тому насправді довжина ключа дорівнює 56 бітів, а не 64, тому довжина ключа 3DES насправді дорівнює 168, а не 192 біта.

Існує 3 типи алгоритму 3DES:

1. DES-EEE3: Шифрується три рази з трьома різними ключами (операції шифрування-шифрування-шифрування).

2. DES-EDE3: 3DES операції шифрування-розшифрування-шифрування з трьома різними ключами.

3. DES-EEE2 і DES-EDE2: Як і попередні, за винятком того, що на першому і третьому кроці використовується однаковий ключ.

3DES представляє собою блочний шифр, він шифрує дані 64-бітовими блоками. На початку алгоритму вводиться 64-бітовий блок відкритого тексту, наприкінці 64-бітовий блок шифротексту. 3DES являється симетричним алгоритмом: для шифрування та дешифрування використовуються однакові алгоритм і ключ (за виключенням невеликих розбіжностей в використанні ключа).

Ключ 3DES зазвичай представляється 192-бітовим числом, але кожний восьмий біт використовується для перевірки парності і ігнорується. Біти парності являються найменш значущими бітами байтів ключа. Ключ, який може бути будь-яким 56-бітовим числом, можна змінити в будь-який момент часу [13].

На простішому рівні алгоритм не представляє нічого більшого, ніж комбінація двох основних методів шифрування: зміщення і дифузії.

Фундаментальним блоком, на якому будується алгоритм 3DES є застосування до тексту одиначної комбінації цих методів (підстановка, а за нею перестановка), яка залежить від ключа. Такий блок називається етапом. 3DES складається з 48 етапів (потрійне використання криптоалгоритму DES: 1DES має 16 етапів, відповідно 3DES – 48 етапів), однакова комбінація методів застосовується до вхідного тексту 48 разів.

Структурна схема шифрування даних в алгоритмі DES така ж як і в 3DES, але вона використовується тричі і з різними ключами, тобто: вхідний текст (DES) $\rightarrow$ DES $\rightarrow$ вихідний текст (DES), який є вхідним для 2DES $\rightarrow$ 2DES $\rightarrow$ вихідний текст (2DES), який є вхідним для 3DES $\rightarrow$ 3DES $\rightarrow$ шифротекст алгоритму 3DES.

Після початкової перестановки блок розбивається на праву і ліву частину довжиною по 32 біти. Надалі виконується 16 етапів однакових дій, , в яких дані об'єднуються з ключем. Після 16 етапу права і ліва частини об'єднуються, перемішуються згідно кінцевої перестановки, отримується шифротекст на виході алгоритму DES, оскільки ми працюємо з 3DES, то отриманий шифротекст, виходить на початок даного алгоритму, як відкритий текст, опрацьовується за таким же принципом ще 16 разів за іншим ключем, отримуємо знову шифротекст і опрацьовуємо його ще і третій раз згідно вище сказаного також за іншим ключем. На виході отримуємо шифротекст алгоритму 3DES.

Крипостійкість 3DES з різними ключами має довжину ключа рівну 168 біт, але через атаки “зустріч посередині” (англ. meet-in-the-middle) ефективна крипостійкість складає тільки 112 біт. У варіанті DES-EDE, в якому, ефективний ключ має довжину 80 біт. У варіанті DES-EDE, в якому $K_1=K_3$, ефективний ключ має довжину 80 біт. Для успішної атаки на 3DES потрібно близько 2^{32} біт відомого відкритого тексту, 2^{113} кроків, 2^{90} циклів DES-шифрування і 2^{88} біт пам'яті [13].

3DES з трьома ключами реалізований у багатьох додатках, орієнтованих на роботу з Інтернет, у тому числі в PGP й S/mime. Потрійний DES є досить популярною альтернативою DES і використовується при управлінні ключами

в стандартах ANSI X9.17 й ISO 8732 і у PEM (Privacy Enhanced Mail). Відомих криптографічних атак, застосовних на практиці, на 3DES не існує.

Тим не менш, 3DES потроху виходить з ужитку, що замінюється новим алгоритмом AES Rijndael. Rijndael, реалізований програмно, працює в шість разів швидше, але саме тому 3DES більше підходить для апаратних реалізацій.

1.3. Огляд можливостей захисту операційної системи Cisco IOS

Компанія Cisco Systems, заснована невеликою групою вчених Стенфордського університету, в 1986 році представила свій перший продукт.

Cisco поставляє більш 80% маршрутизаторів, що є основою Internet. Сьогодні компанія є основним провайдером комп'ютерних мереж для бізнесу. Мережеві рішення Cisco забезпечують роботу об'єднаних мереж тисяч компаній, університетів, урядових агентств і служб в усьому світі. Широкий спектр рішень компанії Cisco включає побудову високопродуктивних локальних мереж; доступ до ресурсів мережі Інтернет; засоби для мобільної роботи; забезпечення зв'язку між офісами [18].

Ці рішення можуть використовуватися як в мережах малого та середнього бізнесу, так і в мережах великих компаній.

Рішення компанії Cisco для малого і середнього бізнесу складають продукти, які можуть бути розділені на п'ять категорій: маршрутизатори доступу, засоби і додатки для Інтернет/Інтранет, комутатори локальних мереж, концентратори і засоби мережного керування.

Компанія Cisco пропонує повний спектр маршрутизаторів доступу від моделей для домашнього офісу до корпоративних серверів доступу, забезпечуючи доступ до мережі Інтернет, зв'язок між офісами і віддалений доступ для мобільних користувачів. Повнофункціональні рішення компанії Cisco для мереж Інтернет/Інтранет, включаючи мережеві додатки, розроблені для надання користувачам зручного і захищеного доступу в мережу Інтернет та забезпечення з'єднань Інтранет [1].

Рішення Cisco для локальних мереж включають модульні комутатори локальних мереж, що встановлюються в стек, комутатори фіксованої конфігурації та концентратори для робочих груп і офісів малого бізнесу.

Для роботи в глобальних мережах Cisco пропонує цілий ряд рішень, забезпечують захист даних на апаратному та програмному рівні.

Ключовим елементом, що об'єднує всі рішення в єдине ціле, є програмне забезпечення Cisco IOS.

У зв'язку з тим, що в Україні вартість цифрових каналів для передачі даних досить висока, дуже мало хто замовники можуть дозволити собі підключення, наприклад, по лінії E1, і змушені задовольнятися орендою каналів зі швидкостями 64-128 Кбіт/с, а то й виділених асинхронних ліній або ліній комутованої телефонної мережі. Однак це твердження не спростовує того факту, що з розвитком мережі провайдерів в Україні і поліпшенням їх технічної бази вартість підключення та оренди цифрових каналів передачі даних буде знижуватися до рівня європейських цін на подібного роду послуги. Тому наявність достатньо дешевих, низькошвидкісних універсальних інтерфейсів (багато з яких можуть працювати як у синхронному, так і в асинхронному режимах) в маршрутизаторах дозволяє значно знизити витрати при побудові корпоративної мережі.

Основні властивості програмного забезпечення Cisco IOS для маршрутизаторів і серверів доступу ПЗ Cisco IOS пропонує такі можливості оптимізації смуги пропускання:

Маршрутизація на вимогу (dial-on-demand routing) – мінімізація витрат завдяки тому, що маршрутизатор автоматично встановлює і завершує з'єднання під час використання мереж комутації каналів (ISDN чи звичайні телефонні мережі).

Виділення на вимогу смуги пропускання (bandwidth-on-demand) – динамічне збільшення пропускної здатності за допомогою автоматичного встановлення додаткових з'єднань і балансування передачі даних по них у відповідності з заданими рівнями.

Швидка маршрутизація (Snapshot Routing) – механізм поширення інформації протоколів маршрутизації, що дозволяє використовувати динамічні протоколи маршрутизації на комутованих лініях.

Резервування смуги пропускання і пріоритетна черговість (Virtual bandwidth reservation and priority queuing) – розширює реальне використання смуги пропускання шляхом резервування пропускну здатності і пріоритизації потоків даних в залежності від типів додатків, адреси відправника або адреси одержувача.

Спуфінг протоколу IPX (IPX Protocol Spoofing) – оптимізація мереж Novell NetWare шляхом обробки службових пакетів, управляючих з'єднанням між сервером, маршрутизатором і клієнтом.

Стиснення (компресія) даних Cisco IOS – повний набір варіантів стиснення, включаючи компресію заголовків TCP/IP, компресію на рівні інтерфейсу, компресію на рівні віртуального каналу.

Кількість використовуваного в обчислювальних мережах обладнання неухильно зростає. Користувачам вже недостатньо тих можливостей, які надаються їм локальною мережею. Потрібні постійна підкачка інформації з інших локальних мереж, від віддалених користувачів, а також стійкий вихід в Internet. Але саме по собі встановлене “залізо” не дозволяє ефективно вирішувати складні питання міжмережевої взаємодії. Потрібна відповідне ПЗ. Корпорація Cisco розробила міжмережеву операційну систему, що підтримується не тільки всім обладнанням самої Cisco, але й продуктами інших провідних виробників мережевого обладнання. Виробники мережного обладнання традиційно приділяють основну увагу вдосконаленню його апаратної частини [17].

Корпорація Cisco, що випускає практично повний спектр мережевої продукції, направила значні зусилля і на розробку спеціального ПЗ, що дозволило їй різко розширити можливості свого устаткування.

Потужна міжмережева операційна система Cisco IOS (Cisco Internetwork Operating System) забезпечує дуже високий рівень мережевих можливостей, захищеності мережі, якості сервісних послуг, простоти

використання і керованості мережним устаткуванням. IOS стала тим “інтелектом”, який дозволяє маршрутизаторам ефективно вирішувати проблеми міжмережевої взаємодії. Дана операційна система стала загальним ПЗ для всіх продуктів Cisco [18].

Рішення, застосовані в Cisco IOS, виявилися настільки вдалі, що сьогодні ця операційна система встановлюється навіть на маршрутизатори таких корпорацій, як, наприклад, Compaq і Hewlett Packard. Cisco планує подальше розширення можливостей IOS і розповсюдження цієї системи на всю мережеву галузь. Корпорація збирається підтримувати можливості IOS по забезпеченню безпеки, якості сервісу, передачі голосу і мережевого адміністрування. В даний час IOS принципово відрізняється від інших аналогічних конкуруючих продуктів тим, що вона – дійсно відкрита платформа, яка призначена не тільки для продукції Cisco.

Мережева операційна система Cisco IOS дозволяє здійснювати мультипротокольную маршрутизацію (IP, IPX, AppleTalk, SNA, DECNET) і надає можливість роботи з лініями ISDN, асинхронними і синхронними виділеними лініями, X.25, лініями Frame Relay, SMDS, Switched 56; забезпечити повну безпеку на всьому шляху передачі інформації, включаючи передачу через Firewall, необхідну маршрутну аутентифікацію, загальну маршрутну інкапсуляцію GRE (generic routing encapsulation), шифрування інформації; отримати закінчену систему якісного сервісу, включаючи підтримку протоколів RSVP (Resource Reservation Protocol), WFQ (Weighted Fair Queuing), IP Multicast, SMRP (AppleTalk Simple Routing Protocol) для роботи з мультимедійними додатками (у тому числі організації настільних відеоконференцій, дистанційного навчання та спільної передачі голосу і даних); розширити можливості для Internet/Intranet доступу, що дозволяють значно знизити його вартість. Дані можливості включають: NAT (Network Address Translation), IPeXchange IPX-to-IP gateway, GRE. Також в даній операційній системі використовуються функції оптимізації мережі WAN (маршрутизація по телефону – dial-to-demand routing, Open Shortest Path First,

Snapshot маршрутизація, можливість компресії та фільтрації), що також дозволяє знизити вартість утримання мережі WAN [18].

Всі ці можливості, інтегровані в потужні апаратні маршрутизатори, дозволяють найкращим чином організувати обмін інформацією між підрозділами фірми в реальному масштабі часу.

Сьогодні актуальною версією IOS – вбудованого програмного забезпечення усього обладнання Cisco Systems, є версія 11.2 різних підверсій.

1.4. Огляд можливостей захисту операційної системи RouterOS

Mikrotiks Ltd (торгова марка MikroTik) – латвійський виробник комп'ютерного мережного обладнання. MikroTik розробляє, встановлює і продає провідні та бездротові маршрутизатори, операційні системи до них і відповідне додаткове обладнання. Компанія була заснована в 1995 році з метою продажу устаткування на ринках, що розвиваються. У 2007 році в компанії працювало понад 70 співробітників.

Одним з продуктів MikroTik є RouterOS – мережева операційна система на базі Linux. Дана операційна система призначена для установки на апаратні маршрутизатори MikroTik RouterBoard. Також дана система може бути встановлена на ПК, перетворюючи його в маршрутизатор, що надає такі послуги, як правила брандмауера, VPN сервер і клієнт, формування якісної пропускної здатності, безпроводну точку доступу і інші часто використовувані функції маршрутизації і підключення мереж. Система також може служити як Captive-портал на основі системи бездротового доступу.

Операційна система ліцензована в ескалації рівнів, в кожному релізі тим більше функцій RouterOS, чим більше номер рівня. Ліцензування платні і ескалюються відповідно до функцій релізу. Існує програмне забезпечення під назвою Winbox, яке надає складний графічний інтерфейс для операційної системи RouterOS. Програмне забезпечення також дозволяє з'єднуватися через FTP, Telnet, і SSH. Існує також API, який дозволяє створювати спеціалізовані додатки для управління та моніторингу [19].

RouterOS підтримує безліч сервісів, які можуть бути використані середнім або великим провайдером – наприклад OSPF, BGP, VPLS/MPLS. Програмне забезпечення забезпечує підтримку практично всіх мережевих інтерфейсів на ядрі Linux 2.6.16, крім бездротових, де Atheros і Prism є єдиними підтримуваними чіпсетами (станом RouterOS версії 3.x). MikroTik також працює над модернізацією програмного забезпечення, яка забезпечить повну сумісність між сервісами MikroTik і новими мережевими розробками, такими як IPv6.

Операційна система RouterOS підтримує наступні функції для роботи з протоколом TCP/IP:

Firewall і NAT – потужні налаштування фільтрації пакетів, реалізація SNAT і DNAT, можливість класифікації пакетів за MAC-адресою джерела, IP адресам, діапазонами портів, IP протоколами, інтерфейсами, вмістом та розміром пакетів.

Routing – статична маршрутизація, multi-path маршрутизація, маршрутизація на основі політик (сполучена з файрволом), реалізація наступних протоколів динамічної маршрутизації: RIP v1/v2, OSPF v2, BGP v4.

Управління якістю обслуговування QoS – можливість динамічного керування смугою пропускання. Завдання мінімальної, максимальної і Burst швидкості для IP, протоколу, підмережі, порту. Можливість вибрати тип черги. Доступні наступні можливі: PCQ, RED, SFQ, FIFO. Релізація здійснена за допомогою пакета HTB.

Можливості HotSpot – можливість побудови plug&play точок колективного користування Internet на основі вбудованих засобів HotSpot з аутентифікацією на RADIUS сервері. Створення walled-garden зон, завдання швидкості, часу роботи клієнта.

Протоколи PTP тунелів – PPTP, PPPoE і L2TP з можливостями PAP, CHAP, MSCHAPv1 і MSCHAPv2 авторизації, RADIUS аутентифікації і управління доступом, MPPE шифрування, PPPoE компресії, керування смугою пропускання і використання правил брандмауера.

Створення простих тунелів – IP2IP тунелі, EoIP (Ethernet over IP); Використання IPsec – IP security AH і ESP протоколи. MODP Diffie-Hellman групи 1,2,5. MD5 і SHA1 алгоритми кешування. DES, 3DES, AES-128, AES-192, AES-256 алгоритми шифрування. Perfect Forwarding Secrecy (PFS) MODP групи 1,2,5;

Proxy – вбудований FTP і HTTP/HTTPS кешуючий проксі сервер, прозоре DNS і HTTP проксінг. Реалізація SOCKS протоколу, можливість завдання ACL (Access Control Lists), побудова кешуючих мереж за допомогою можливості parent proxy;

DHCP – базова реалізація DHCP сервера і DHCP релея, DHCP клієнта, можливість резервування адрес, підтримка RADIUS;

Операційна система RouterOS також підтримує підтримує *VRRP, NTP, SNMP, M3P, MNDP, Tools*.

RouterOS підтримує функції для роботи на другому рівні моделі OSI:

Бездротові мережі – підтримка IEEE802.11a/b/g бездротових клієнтів і точок доступу. Створення Wireless Distribution System (WDS), віртуальних точок доступу. Реалізація 40 і 104-бітного шифрування з WEP і WPA аутентифікацією клієнтів. Можливість завдання ACL. Авторизація клієнтів на RADIUS сервері. Підтримка роумінгу й Access Point мостів.

Bridge – можливість створення мостів між інтерфейсами з фільтрацією трафіку, що проходить.

VLAN – підтримка IEEE802.1q Virtual LAN на Ethernet і бездротових інтерфейсах, множинних VLAN-ів і побудова VLAN-мостів.

Synchronous – V.35, V.24, E1/T1, X.21, DS3 (T3), протоколи PPP, Cisco HDLC, Frame Relay.

Asynchronous – serial PPP dial-in/dial-out; PAP, CHAP, MSCHAPv1 і MSCHAPv2 протоколи авторизації, RADIUS авторизація. Модемні пули до 128 портів. Можливість створення інтерфейсів з викликом на вимогу.

RouterBOARD – апаратна платформа від MikroTik, що представляє собою лінійку маршрутизаторів під управлінням операційної системи RouterOS. Різні варіанти RouterBOARD платформ дозволяють вирішувати на

їх основі різні варіанти мережевих завдань: від простої бездротової точки доступу і керованого комутатора до потужного маршрутизатора. Практично всі моделі RouterBOARD пристроїв живляться за допомогою PoE, хоча і мають роз'єм для підключення зовнішнього джерела живлення. Моделі, призначені для роботи з бездротовими технологіями, мають слот (miniPCI) для підключення радіомодулів. Більшість моделей також має роз'єм для підключення до COM-порту ПК. У бюджетних моделях або в залежності від конкретного призначення моделі, ті чи інші елементи можуть бути відсутніми.

Обладнання RouterBOARD повинно відповідати наступним вимогам: CPU і материнська плата – частота процесора 100 МГц і вище. У даному випадку підійде Intel Pentium 133 MX або аналогічний процесор з архітектурою x86. Варто відзначити, що багатопроцесорні системи в даний момент не підтримуються; RAM – мінімум 32 MB оперативної пам'яті (максимум 1GB). Рекомендується 64 MB і вище; пристрій зберігання інформації – стандартний ATA/IDE-контролер і носій з мінімум 64 MB місця. Карти флеш-пам'яті і жорсткі диски Microdrive можуть бути підключені за допомогою спеціального адаптера [19].

Висновки до першого розділу

Отже, в першому розділі випускної кваліфікаційної роботи було розглянуто загальні теоретичні відомості технологій побудови віртуальних приватних мереж; розглянуто загальні відомості протоколу забезпечення захисту даних IPSec; розглянуто теоретичні аспекти використання алгоритму шифрування 3DES у побудові захищених приватних мереж, а також проведено огляд можливостей захисту операційних систем Cisco IOS та RouterOS.

2. РОЗРОБКА ПРОЕКТУ ПІДСИСТЕМИ ЗАХИСТУ ІНТРАНЕТ-МЕРЕЖІ

2.1. Розробка топології інтранет-мережі

На даному етапі виконання випускної кваліфікаційної роботи перейдемо до процесу безпосереднього проектування топології мережі, розробки системи адресації та засобів захисту інформаційно-комунікаційної мережі.

Слід зазначити, що загальна топологія інформаційно-комунікаційної мережі буде складатися із двох складових – фізичної та логічної топологій, тому їх слід розглянути окремо.

Загальна топологія інтранет-мережі буде включати в себе три рівні: рівень ядра, рівень розподілу та рівень доступу.

Рівень ядра буде складатися із трьох маршрутизаторів, рівні розподілу та доступу будуть складатися із чотирьох маршрутизаторів. Отже, інтранет-мережі буде складатися із семи маршрутизаторів та чотирьох локальних мереж (рисунок 2.1).

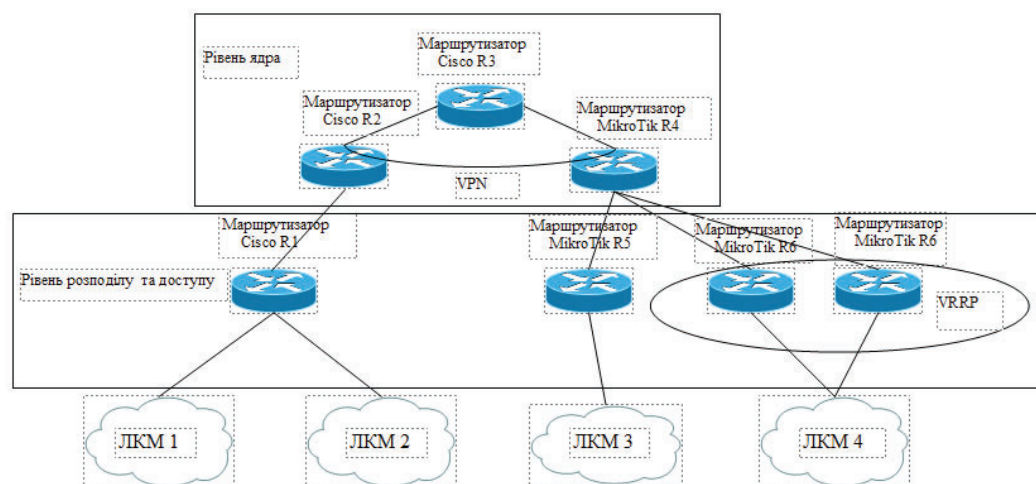


Рисунок 2.1 – Загальна топологія інформаційно-комунікаційної мережі

Фізична топологія включатиме в себе реальні фізичні зв'язки обладнання в інформаційно-комунікаційній мережі.

На рівні ядра маршрутизатори з'єднані за допомогою ліній Gigabit Ethernet на звитій парі. На рівні розподілу та доступу маршрутизатори з'єднані між собою за допомогою ліній FastEthernet на звитій парі.

Логічна топологія включатиме логічні зв'язки обладнання в інформаційно-комунікаційній мережі.

Слід зазначити, що мережа буде складатися із трьох маршрутизаторів Cisco та чотирьох маршрутизаторів MikroTik, причому на рівні доступу при використанні протоколу резервування основного шлюзу VRRP два маршрутизатори MikroTik (R6 та R7) будуть об'єднані в один VRRP-маршрутизатор. Також на рівні ядра між маршрутизатором Cisco R2 та маршрутизатором MikroTik R4 буде налаштований VPN-канал типу "Site-to-Site".

Специфіка побудови логічної топології інформаційно-комунікаційної мережі полягає в тому, що вона буде розділена на дві частини, які будуть взаємодіяти між собою завдяки функціонуванню протоколів маршрутизації RIP та OSPF. На рівні ядра на маршрутизаторі Cisco R3 буде відбуватися редистрибуція маршрутів.

Дана топологія може бути розширеною, тобто мати більше обладнання і зв'язків, але в проектуванні і реалізації захищеності мережі розглядатимуться основні принципи налагодження.

Тепер розглянемо топологію внутрішніх локальних мереж.

Перша локальна мережа має у своєму складі 130 РС. Для їх зв'язку використано 5 комутаторів на 24 порти та 1 комутатор на 16 портів.

Друга локальна мережа має у своєму складі 20 РС. Для Для їх зв'язку використано 1 комутатор на 24 порти.

Третя локальна мережа має у своєму складі 150 РС. Для їх зв'язку використано 6 комутаторів на 24 портів та 1 комутатор на 16 портів.

Четверта локальна мережа має у своєму складі 12 РС. Для їх зв'язку використано 1 комутатор на 16 портів.

В кожній локальній мережі кількість комутаторів обиралась таким чином, щоб в них залишались вільні порти, оскільки в такому випадку буде

можливість розширення мережі та можливість агрегації каналів в даній мережі.

2.2. Розробка системи адресації інтранет-мережі

Інтранет-мережа складається із локальних мереж та мереж зв'язку, тому система адресації інтранет-мережі буде складатися із сукупності системи адресації локальних мереж та системи адресації мереж зв'язку.

Оскільки до складу інтранет-мережі входять чотири локальні мережі, то система адресації локальних мереж буде виглядати наступним чином:

Перша локальна мережа: кількість вузлів в мережі – 130, комутаторів – 6, тому, врахувавши, що ще додаємо 3 адреси – широкомовну, адресу мережі та адресу шлюзу за замовчуванням, отримаємо 139 зайнятих адреси. Дані адресації першої локальної мережі наведені у таблиці 2.1.

Таблиця 2.1 – Адресація ЛКМ №1

Призначення	IP адреса
Адреса мережі	192.93.21.0
Маска мережі	255.255.255.0/24
Інвертована маска	0.0.0.255
Мінімальна адреса	192.93.21.1
Максимальна адреса	192.93.21.254
Широкомовна адреса	192.93.21.255
Шлюз за замовчуванням	192.93.21.1
Діапазон адрес комутаторів	192.93.21.2 – 192.93.21.7
Діапазон адрес вузлів	192.93.21.8 – 192.93.21.137
Діапазон вільних адрес	192.93.21.138 – 192.93.21.254

Друга локальна мережа: кількість вузлів в мережі – 20, комутаторів – 1, тому, врахувавши, що ще додаємо 3 адреси – широкомовну, адресу мережі та адресу шлюзу за замовчуванням, отримаємо 24 зайнятих адреси. Дані адресації другої локальної мережі наведені у таблиці 2.2.

Таблиця 2.2 – Адресація ЛКМ №2

Призначення	IP адреса
Адреса мережі	193.93.21.0
Маска мережі	255.255.255.224/27
Інвертована маска	0.0.0.31
Мінімальна адреса	193.93.21.1
Максимальна адреса	193.93.21.30
Широкомовна адреса	193.93.21.31
Шлюз за замовчуванням	193.93.21.1
Адреса комутатора	193.93.21.2
Діапазон адрес вузлів	193.93.21.3 – 193.93.21.22
Діапазон вільних адрес	193.93.21.23 – 193.93.21.30

Третя локальна мережа: кількість вузлів в мережі – 150, комутаторів – 7, тому, врахувавши, що ще додаємо 3 адреси – широкомовну, адресу мережі та адресу шлюза по замовчуванню, отримаємо 160 зайнятих адреси. Дані адресації третьої локальної мережі наведені у таблиці 2.3.

Таблиця 2.3 – Адресація ЛКМ №3

Призначення	IP адреса
Адреса мережі	194.93.21.0

Маска мережі	255.255.255.0/24
Інвертована маска	0.0.0.255
Мінімальна адреса	194.93.21.1
Максимальна адреса	194.93.21.254
Широкомовна адреса	194.93.21.255
Шлюз за замовчуванням	194.93.21.1
Діапазон адрес комутаторів	194.93.21.2 – 194.93.21.8
Діапазон адрес вузлів	194.93.21.9 – 194.93.21.158
Діапазон вільних адрес	193.93.21.159 – 193.93.21.254

Четверта локальна мережа: кількість вузлів в мережі – 12, комутаторів – 1, тому, врахувавши, що ще додаємо 5 адрес – широкомовну, адресу мережі та адресу шлюзу за замовчуванням, 2 адреси інтерфейсів маршрутизаторів, тому отримаємо 16 зайнятих адреси. Дані адресації четвертої локальної мережі наведені у таблиці 2.4.

Таблиця 2.4 – Адресація ЛКМ №4

Призначення	IP адреса
Адреса мережі	195.93.21.0
Маска мережі	255.255.255.224/27
Інвертована маска	0.0.0.31
Мінімальна адреса	195.93.21.1
Максимальна адреса	195.93.21.30
Широкомовна адреса	195.93.21.31
Шлюз за замовчуванням	195.93.21.30

Діапазон адрес інтерфейсів маршрутизаторів	195.93.21.1 – 195.93.21.2
Адреса комутатора	195.93.21.3
Діапазон адрес вузлів	195.93.21.4 – 195.93.21.15
Діапазон вільних адрес	195.93.21.16 – 195.93.21.29

Для адресації мереж, що служать для зв'язку маршрутизаторів, доведеться застосувати шість мереж: 196.93.21.0, 197.93.21.0, 198.93.21.0, 199.93.21.0, 200.93.21.0, 201.93.21.0. Оскільки в кожній з цих мереж будуть з'єднуватися лише по два маршрутизатори, тобто для їх зв'язку між собою буде використано двоточкове з'єднання, то для них буде доцільно використати маску 255.255.255.252/30.

Поведемо детальну адресацію кожної мережі зв'язку. Дані адресації першої мережі зв'язку наведені у таблиці 2.5.

Таблиця 2.5 – Адресація МЗ №1

Призначення	IP адреса
Адреса мережі	196.93.21.0
Маска мережі	255.255.255.252/30
Інвертована маска	0.0.0. 1
Мінімальна адреса	196.93.21.1
Максимальна адреса	196.93.21.2
Широкомовна адреса	196.93.21.3
Діапазон адрес інтерфейсів маршрутизаторів	196.93.21.1 – 196.93.21.2

Дані адресації другої мережі зв'язку наведені у таблиці 2.6.

Таблиця 2.6 – Адресація МЗ №2

Призначення	IP адреса
Адреса мережі	197.93.21.0
Маска мережі	255.255.255.252/30
Інвертована маска	0.0.0. 1
Мінімальна адреса	197.93.21.1
Максимальна адреса	197.93.21.2
Широкомовна адреса	197.93.21.3
Діапазон адрес інтерфейсів маршрутизаторів	197.93.21.1 – 197.93.21.2

Дані адресації третьої мережі зв'язку наведені у таблиці 2.7.

Таблиця 2.7 – Адресація МЗ №3

Призначення	IP адреса
Адреса мережі	198.93.21.0
Маска мережі	255.255.255.252/30
Інвертована маска	0.0.0. 1
Мінімальна адреса	198.93.21.1
Максимальна адреса	198.93.21.2
Широкомовна адреса	198.93.21.3
Діапазон адрес інтерфейсів маршрутизаторів	198.93.21.1 – 198.93.21.2

Дані адресації четвертої мережі зв'язку наведені у таблиці 2.8.

Таблиця 2.8 – Адресація МЗ №4

Призначення	IP адреса
Адреса мережі	199.93.21.0
Маска мережі	255.255.255.254/30
Інвертована маска	0.0.0. 1
Мінімальна адреса	199.93.21.1
Максимальна адреса	199.93.21.2
Широкомовна адреса	199.93.21.3
Діапазон адрес інтерфейсів маршрутизаторів	199.93.21.1 – 199.93.21.2

Дані адресації п'ятої мережі зв'язку наведені у таблиці 2.9.

Таблиця 2.9 – Адресація МЗ №5

Призначення	IP адреса
Адреса мережі	200.93.21.0
Маска мережі	255.255.255.254/30
Інвертована маска	0.0.0. 1
Мінімальна адреса	200.93.21.1
Максимальна адреса	200.93.21.2
Широкомовна адреса	200.93.21.3
Діапазон адрес інтерфейсів маршрутизаторів	200.93.21.1 – 200.93.21.2

Дані адресації шостої мережі зв'язку наведені у таблиці 2.10.

Таблиця 2.10 – Адресація МЗ №6

Призначення	IP адреса
Адреса мережі	201.93.21.0
Маска мережі	255.255.255.254/30
Інвертована маска	0.0.0. 1
Мінімальна адреса	201.93.21.1
Максимальна адреса	201.93.21.2
Широкомовна адреса	201.93.21.3
Діапазон адрес інтерфейсів маршрутизаторів	201.93.21.1 – 201.93.21.2

Розподіл адрес по діапазону в локальних комп'ютерних мережах проводився таким чином, щоб використати необхідну кількість IP адрес, забезпечивши при цьому вільні IP адреси для можливості розширення мережі та виконання агрегації каналів.

В мережах зв'язку вільні IP адреси не потрібні, оскільки на рівні ядра вони створюють загрозу несанкціонованого підключення до мереж зв'язку.

2.3. Розробка базових та додаткових засобів захисту інтранет-мережі

Оскільки розроблювальна інтранет-мережа має ряд уразливостей як на рівні ядра, так і на рівнях розподілу та доступу, тому є необхідність у розробці базових та додаткових засобів захисту.

Як базові засоби захисту інтранет-мережі будуть налаштовані наступні засоби:

1. Налаштування протоколів маршрутизації RIP та OSPF.

2. Налаштування DHCP-серверів з підвищеним рівнем інформаційної безпеки, тобто видача IP-адрес буде проводитися по відповідним MAC-адресам DHCP-клієнтів.

3. Налаштування парольного захисту маршрутизаторів, причому довжина паролю буде не меншою за вісім символів і під час його створення будуть використані літерні, цифрові та спеціальні символи, також буде використано зміну регістру клавіатури при введенні символів.

4. Налаштування протоколу резервування основного шлюзу VRRP.

5. Відключення на маршрутизаторах непотрібних протоколів та сервісів: cdp, service tcp-small-servers, service udp-small-servers, service finger, ip http server та ip http secure-server.

Як додаткові засоби захисту інтранет-мережі будуть налаштовані наступні засоби:

1. Налаштування аутентифікації в протоколах маршрутизації.

2. Налаштування на рівні ядра віртуальної захищеної мережі типу “Site-to-Site” з використанням протоколу IPSec. При налаштуванні використаємо блочний симетричний криптографічний алгоритм 3DES з довжиною ключа 192 біта та хеш-функцію MD5 з довжиною дайджесту 128 біт.

3. Налаштування моделі AAA на маршрутизаторах. Для цього використаємо Radius-сервер для доступу до маршрутизаторів та Syslog-сервер для журналювання всіх подій на маршрутизаторах.

4. Віддалений доступ до маршрутизаторів відбуватиметься завдяки використанню протоколу SSH, при цьому проведемо заборону у використанні протоколу Telnet.

Висновки до другого розділу

Отже, в другому розділі курсового проекту було розроблено фізичку та логічну топологію інтранет-мережі, розроблено систему адресації, основні та додаткові засоби захисту інтранет-мережі.

3. ОБГРУНТУВАННЯ ВИБОРУ ОБЛАДНАННЯ ТА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, НАЛАГОДЖЕННЯ ТА ПЕРЕВІРКА РОБОТИ ЗАХИЩЕНОЇ ІНТАНЕТ-МЕРЕЖІ

3.1. Обґрунтування вибору обладнання та програмного забезпечення

Для правильного і ефективного функціонування мережі необхідно обрати якісне та надійне обладнання, саме тому було обрано мережеве обладнання провідних виробників мережевого обладнання компанію Cisco та MikroTik. В спроектованій мережі використовуються наступні типи обладнання :

1. Маршрутизатори Cisco(3 шт.);
2. Маршрутизатори MikroTik(4 шт.);
3. Комутатори :
 - 3 шт. на 16 портів ;
 - 12 шт. на 24 порти ;
4. Робочі станції (312 шт.).

Розроблювальна мережа складається з трьох рівнів – рівня ядра, рівня розподілу та рівня доступу.

На рівні ядра використовуються два маршрутизатори фірми Cisco та один маршрутизатор фірми MikroTik. Всі три маршрутизатори містять по два порти Gigabit Ethernet на звитій парі. Але в одному з маршрутизаторів ще додатково встановлено два додаткові порти Gigabit Ethernet (маємо чотири порти Gigabit Ethernet).

В якості реального обладнання для маршрутизаторів було обрано маршрутизатори Cisco CISCO7206 та MikroTik RouterBOARD 750GL. Вибір маршрутизаторів проводився за принципом мінімальної вартості кінцевого обладнання.

На рівні розподілу використовуються один маршрутизатор фірми Cisco та три маршрутизатори фірми MikroTik. Всі маршрутизатори є однотипними і містять по два порти FastEthernet на звитій парі. Але в одному з

маршрутизаторів ще додатково встановлено два додаткові порти FastEthernet (маємо чотири порти FastEthernet).

В якості реального обладнання для маршрутизаторів було обрано маршрутизатори Cisco CISCO7206 та MikroTik RouterBOARD 750GL.

На рівні доступу використовуються комутатори Cisco Linksys SD216T-EU та Cisco Linksys WS-C3750X-24P-S.

В якості програмного забезпечення мережевих пристроїв було обрано версію мережевої операційної системи Cisco IOS c7200-ik9o3s-mz.123-22 та mikrotik-5.20, що підтримує усі існуючі на сьогодні моделі мереженого обладнання фірми Cisco та MikroTik і забезпечує стабільне і надійне функціонування мережі.

В якості програмного забезпечення робочих станцій було обрано операційну систему Windows XP SP3.

Технічні характеристики всіх пристроїв приведені у додатку А.

3.2. Налашдування базових засобів міжмережевої взаємодії

Налаштування роботи мережі проводиться засобами програмного емулятора GNS3, а для налаштування роботи робочих станцій використаємо програмний емулятор VirtualBox.

Оскільки деякі команди для налагодження маршрутизаторів є ідентичними, то недоцільно їх наводити для всіх маршрутизаторів, достатньо їх показати на одному із них.

Налаштування інтерфейсів маршрутизатора Cisco відбувається наступним чином:

```
Router>enable
Router#configure terminal
Router(config)#hostname R1
R1 (config)#interface FastEthernet0/0
R1 (config-if)#ip address 192.93.21.1 255.255.255.0
R1 (config-if)#no shutdown
R1 (config-if)#exit
R1 (config)#interface FastEthernet 0/1
```

```
R1 (config-if)# ip address 196.93.21.1 255.255.255.252
R1 (config-if)#no shutdown
R1 (config-if)#exit
R1 (config)#interface FastEthernet 1/0
R1 (config-if)# ip address 193.93.21.1 255.255.255.224
R1 (config-if)#no shutdown
R1 (config-if)#exit
```

Налагодження інтерфейсів маршрутизатора MikroTik відбувається наступним чином:

```
[Admin@MikroTik] > interface enable ether2
[Admin@MikroTik] > interface enable ether3
[Admin@MikroTik] > ip address add address=199.93.21.2/30
interface=ether2
[Admin@MikroTik] > ip address add address=194.93.21.1/24
interface=ether3
```

Налагодження протоколу маршрутизації RIP з аутентифікацією на маршрутизаторі Cisco:

```
R1 (config)#router rip
R1 (config-router)#version 2
R1 (config-router)#network 192.93.21.0
R1 (config-router)#network 193.93.21.0
R1 (config-router)#network 196.93.21.0
R1 (config-router)# exit
R1 (config)# key chain priv
R1 (config- keychain)# key 1
R1 (config- keychain- key)# key-string mystr
R1 (config- keychain- key)# exit
R1 (config- keychain)# exit
R1 (config)#interface FastEthernet0/1
R1 (config-if)# ip rip authentication key-chain priv
R1 (config-if)# ip rip authentication mode md5
```

Налагодження протоколу маршрутизації OSPF з аутентифікацією на маршрутизаторі Cisco:

```
R4 (config)#router ospf 1
R4 (config-router)#network 198.93.21.0 0.0.0.3 area 0
R4 (config-router)#area 0 authentication message-digest
R4 (config-router)#exit
R4 (config)#interface FastEthernet0/1
R4 (config-if)#ip ospf message-digest-key 2 md5 mystr
R4 (config-if) ip ospf authentication message-digest
```

Налагодження редистрибуції маршрутів:

```
R3 (config)#router rip
R3(config-router)#version 2
R3(config-router)#redistribute static metric 1
R3(config-router)#redistribute ospf 1 metric 1
R3(config-router)#exit
R3 (config)#router ospf 1
R3(config-router)#redistribute static metric 200 subnets
R3(config-router)#redistribute rip metric 200 subnets
```

Налагодження протоколу маршрутизації OSPF з аутентифікацією аутентифікацією на маршрутизаторі MikroTik:

```
[Admin@MikroTik] > routing ospf interface add interface=ether2
authentication=md5 authentication-key=mystr authentication-key-id=2
[Admin@MikroTik] > routing ospf interface add interface=ether3
authentication=md5 authentication-key=mystr authentication-key-id=2
[Admin@MikroTik] > routing ospf network add network=199.93.21.0/30
area=backbone
[Admin@MikroTik] > routing ospf network add network=194.93.21.0/24
area=backbone
```

Налагодження DHCP-сервера на маршрутизаторі Cisco:

```
R1 (config)#ip dhcp pool A
R1 (dhcp-config)#host 192.93.21.2 255.255.255.0
R1 (dhcp-config)#default-router 192.93.21.1
R1 (dhcp-config)#client-identifier 0108.0027.d18f.60
R1 (dhcp-config)#client-name Win_1
R1 (dhcp-config)#exit
R1 (config)#ip dhcp excluded-address 192.93.21.2-192.93.21.7
R1 (config)#ip dhcp excluded-address 192.93.21.138-192.93.21.254
```

Налагодження DHCP-сервера на маршрутизаторі MikroTik:

```
[Admin@MikroTik] > ip pool add name=mypool ranges=194.93.21.9-
194.93.21.158
[Admin@MikroTik] > ip dhcp-server add name=serv1 interface=ether2
address-pool=mypool
[Admin@MikroTik] > ip dhcp-server network add address=194.93.21.0/24
gateway=194.93.21.1 dns-server=194.93.21.1
[Admin@MikroTik] > ip dhcp-server enable serv1
```

Налагодження протоколу VRRP на маршрутизаторі MikroTik:

```
[Admin@MikroTik] > interface vrrp add name=vrrp1 interface=ether3
[Admin@MikroTik] > ip address add address=195.93.21.30/27
interface=vrrp1
```

Створення користувача на маршрутизаторі Cisco:

```
R1 (config)#username Admin secret 0 adM_2932
```

Відключення непотрібних сервісів та протоколів на маршрутизаторі

Cisco:

```
R1 (config)#no cdp run
```

```
R1 (config)#no service tcp-small-servers
```

```
R1 (config)#no service udp-small-servers
```

```
R1 (config)#no service finger
```

```
R1 (config)#service tcp-keepalives-in
```

```
R1 (config)#service tcp-keepalives-out
```

```
R1 (config)#no ip http server
```

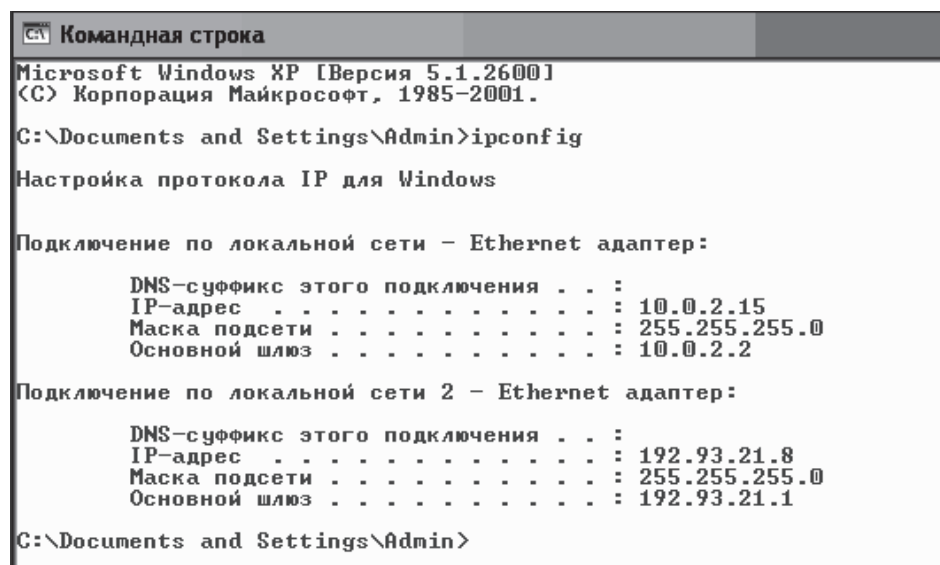
```
R1 (config)#no ip http secure-server
```

Створення нового користувача на маршрутизаторі MikroTik:

```
[admin@MikroTik] > user add name=Admin password=adM_2932  
group=full
```

```
[admin@MikroTik] > user disable admin
```

Проведемо налагодження робочих станцій. Оскільки налаштування всіх робочих станцій є однотипним, то доцільно привести налаштування лише для однієї станції Windows. Для цього присвоємо IP адресу для робочої станції Windows і для перевірки налаштування виконаємо команду *ipconfig* в командному рядку (рисунок 3.1):



```
Командная строка
Microsoft Windows XP [Версия 5.1.2600]
(C) Корпорация Майкрософт, 1985-2001.

C:\Documents and Settings\Admin>ipconfig

Настройка протокола IP для Windows

Подключение по локальной сети - Ethernet адаптер:

        DNS-суффикс этого подключения . . . : 
        IP-адрес . . . . . : 10.0.2.15
        Маска подсети . . . . . : 255.255.255.0
        Основной шлюз . . . . . : 10.0.2.2

Подключение по локальной сети 2 - Ethernet адаптер:

        DNS-суффикс этого подключения . . . : 
        IP-адрес . . . . . : 192.93.21.8
        Маска подсети . . . . . : 255.255.255.0
        Основной шлюз . . . . . : 192.93.21.1

C:\Documents and Settings\Admin>
```

Рисунок 3.1 – Присвоєння IP-адреси для робочої станції Windows

3.3. Налаштування засобів захисту

Оскільки на рівні ядра між маршрутизаторами Cisco та MikroTik налаштовано VPN-зв'язок типу "Site-to-Site", то наведемо команди його налаштування.

Для маршрутизатора Cisco:

Налаштування списку доступу для VPN:

```
R2 (config)#ip access-list extended Site_A
R2 (config-ext-nucl)#permit ip 197.93.21.0 0.0.0.3 198.93.21.0 0.0.0.3
R2 (config-ext-nucl)#exit
```

Налаштування ISAKMP POLICY:

```
R2 (config)#crypto isakmp policy 1
R2 (config-isakmp)#encryption 3des
R2 (config-isakmp)#hash md5
R2 (config-isakmp)#authentication pre-share
R2 (config-isakmp)#group 2
R2 (config-isakmp)#exit
```

Налаштування Transform-set :

```
R2 (config)#crypto isakmp key 0 kluch address 198.93.21.2
R2 (config)#crypto ipsec transform-set name esp-3des esp-md5-hmac
```

Налаштування CRYPTO MAP :

```
R2 (config)#crypto map map1 ipsec-isakmp
R2 (config-crypto-map)#set peer 198.93.21.2
R2 (config-crypto-map)#set transform-set name
R2 (config-crypto-map)#set pfs group2
R2 (config-crypto-map)#match address Site_A
R2 (config-crypto-map)#exit
R2 (config)#interface FastEthernet0/1
R2 (config-if)# crypto map map1
R2 (config-if)# exit
```

Налаштування VPN для маршрутизатора MikroTik:

```
[Admin@MikroTik] > ip ipsec proposal add name="IPSec" auth-
algorithms=md5 enc-algorithms=3des lifetime=30m lifebytes=0 pfs-
group=modp1024 disabled=no
```

```
[Admin@MikroTik] > ip ipsec peer add address=197.93.21.1 secret=kluch
generate-policy=no exchange-mode=main send-initial-contact=yes proposal-
```

*check=obey hash-algorithm=md5 enc-algorithm=3des dh-group=modp1024
lifetime=1d lifebytes=0 disabled=no*

*[Admin@MikroTik] > ip ipsec policy add src-address=198.93.21.2/32: any
dst-address=197.93.21.1/32: any protocol=all action=encrypt level=require ipsec-
protocols=esp tunnel=no sa-src-address=198.93.21.2 sa-dst-
address=197.93.21.1 proposal=IPSec disabled=no*

Налаштування Radius-сервера для маршрутизатора Cisco:

R1(config)#aaa new-model

R1(config)#aaa authentication login default radius

R1(config)#radius-server host 192.93.21.8 auth-port 1812 acct-port 1813

R1(config)#radius-server key testing123

Налаштування Radius-сервера для маршрутизатора MikroTik:

*[Admin@MikroTik] > radius add address=194.93.21.155 auth-port 1812
acct-port 1813 service=login secret=t123*

[Admin@MikroTik] > radius incoming set accept=yes port=1813

[Admin@MikroTik] > user aaa set use-radius=yes default-group=full

Налаштування Syslog-сервера для маршрутизатора Cisco:

R1(config)#int loopback 0

R1(config-if)#ip add 10.10.10.10 255.255.255.255

R1(config-if)#logging host 192.93.3.8

R1(config)#logging source-interface loopback 0

R1(config)#logging trap debugging

Налаштування Syslog-сервера для маршрутизатора MikroTik:

*[Admin@MikroTik] > system logging action add name=action1
target=remote remote=194.93.21.155*

[Admin@MikroTik] > system logging add action=action1 topics=system

Налаштування протоколу SSH для маршрутизатора Cisco:

R1(config)#crypto key generate rsa 1024

Налаштування протоколу SSH для маршрутизатора MikroTik:

[Admin@MikroTik] > ip ssh regenerate-host-key

Заборона протоколу Telnet для маршрутизатора Cisco:

R1(config)#access-list 101 deny tcp any any eq 23

Заборона протоколу Telnet для маршрутизатора MikroTik:

*[Admin@MikroTik] > ip firewall filter add chain=output action=drop
protocol=tcp src-port=23*

3.4. Тестування роботи захищеної інтранет-мережі

Отже, на даному етапі випускної кваліфікаційної роботи отримано спроектовану і нагагоджену захищену інтранет-мережу організації. Тепер буде проведено тестування роботи захищеної інтранет-мережі.

Спочатку перевіримо зв'язок між робочими станціями. Для цього виконаємо команди *ping* та *tracert* з робочої станції, що знаходиться в третій локальній мережі, до робочої станції, що знаходиться в першій локальній мережі (рисунок 3.2).

```
<C> Корпорация Майкрософт, 1985-2001.
C:\Documents and Settings\Admin>ping 192.93.21.8
Обмен пакетами с 192.93.21.8 по 32 байт:
Ответ от 192.93.21.8: число байт=32 время=104мс TTL=123
Ответ от 192.93.21.8: число байт=32 время=51мс TTL=123
Ответ от 192.93.21.8: число байт=32 время=55мс TTL=123
Ответ от 192.93.21.8: число байт=32 время=47мс TTL=123

Статистика Ping для 192.93.21.8:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь),
Приблизительное время приема-передачи в мс:
    Минимальное = 47мсек, Максимальное = 104 мсек, Среднее = 64 мсек
C:\Documents and Settings\Admin>tracert 192.93.21.8
Трассировка маршрута к 192.93.21.8 с максимальным числом прыжков 30
  1      1 ms      <1 мс      <1 мс    194.93.21.1
  2      1 ms      1 мс      <1 мс    199.93.21.1
  3      7 ms      9 мс      10 мс    198.93.21.1
  4     30 ms     31 мс     31 мс    197.93.21.1
  5     35 ms     42 мс     40 мс    196.93.21.1
  6     54 ms     51 мс     51 мс    192.93.21.8
Трассировка завершена.
```

Рисунок 3.2 – Перевірка зв'язку між робочими станціями

Проведемо перевірку роботи Radius-сервера. Для цього на Radius-сервері створимо користувача у відповідній вкладці *Users* (рис. 3.3).

```
AdminR      Password = "123R"
             User-Service-Type = Login-User,
#            Login-Host = 194.93.21.1,
#            Login-Service = ssh,
#            Login-TCP-Port = 22|
```

Рисунок 3.3 – Створення користувача Radius-сервера

Далі буде виконано підключення до маршрутизатора з робочої станції за допомогою програмного додатку PuTTY. Для цього в ній потрібно ввести логін і пароль користувача, що зберігається на Radius-сервері (рисунок 3.4).

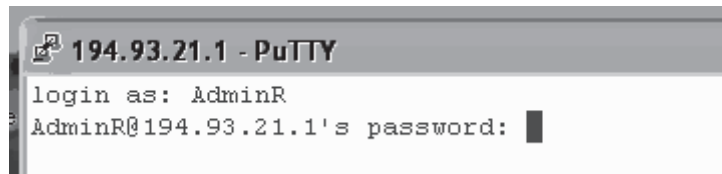


Рисунок 3.4 – Введення логину-пароллю користувача Radius-сервера

Після виконання успішного процесу аутентифікації та авторизації було отримано доступ до маршрутизатора з робочої станції з використанням логіну і пароллю Radius-сервера за допомогою протоколу SSH (рисунок 3.5).

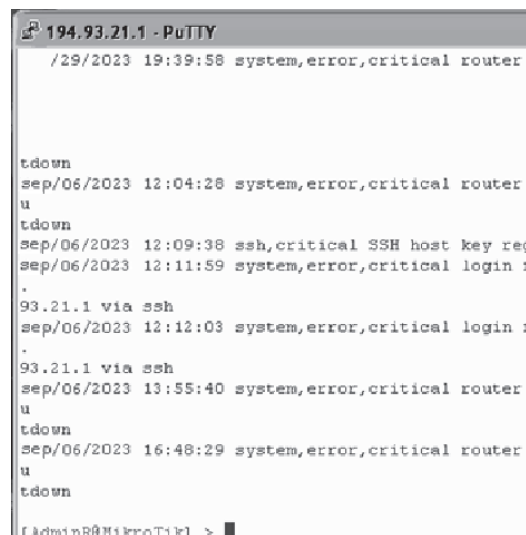


Рисунок 3.5 – Вхід на маршрутизатор з використанням Radius-сервера

Наступним кроком буде проведення перевірки роботи Syslog-сервера. Для цього на робочій станції необхідно запустити програмний додаток Kiwi_Syslog, за допомогою якого буде проводитися аудит інтранет-мережі. Результати перевірки роботи Syslog-сервера представлені на рисунку 3.6.

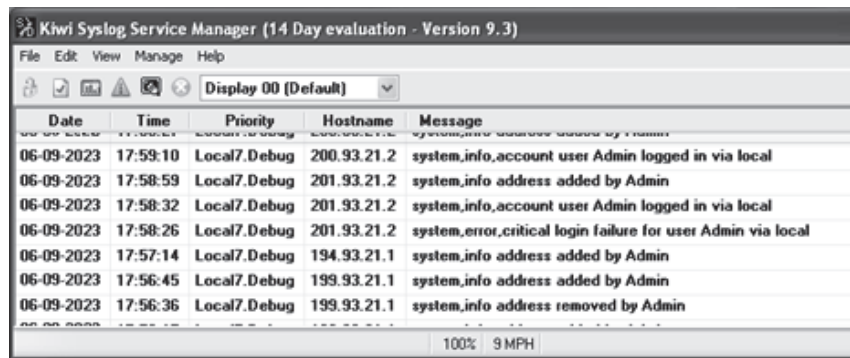


Рисунок 3.6 – Перевірка роботи Syslog-сервера

Далі проведемо перевірку роботи протоколу SSH. Спочатку спробуємо підключитися між маршрутизаторами Cisco. Результат перевірки представлений на рисунку 3.7.

```
Cisco_2#ssh -l Admin 197.93.21.2
Password:
Cisco_3>en
Password:
Cisco_3#
```

Рисунок 3.7 – Перевірка роботи протоколу SSH між маршрутизаторами Cisco

Тепер спробуємо перевірити роботи протоколу SSH між маршрутизаторами Cisco та MikroTik (рисунок 3.8).

```
Cisco_2#ssh -l Admin 198.93.21.2
[Connection to 198.93.21.2 aborted: error status 0]
Cisco_2#
*Mar 1 00:08:05.719: SSH2 CLIENT 0: hostkey algo not supported: client ssh-rsa, server ssh-dss
Cisco_2#
```

Рисунок 3.8 – Перевірка роботи протоколу SSH між маршрутизаторами Cisco та MikroTik

Як бачимо з рисунку 3.8 підключення з маршрутизатора Cisco до маршрутизатора MikroTik є невдале, оскільки SSH-сервер використовує криптографічні ключі SSH-DSS, а SSH-клієнт – SSH-RSA. Тобто в даних

реалізаціях операційних систем маршрутизаторів Cisco і MikroTik таке підключення виконати неможливо з технічної точки зору.

Проведемо спробу підключення до маршрутизатора за допомогою незахищеного протоколу TELNET. Результат підключення представлений на рисунку 3.9.

```
Cisco_2#telnet 197.93.21.2
Trying 197.93.21.2 ...
% Connection refused by remote host
Cisco_2#
```

Рисунок 3.9 – Перевірка роботи протоколу TELNET

Як бачимо з рисунку 3.9 діє блокування підключення до маршрутизаторів за допомогою протоколу TELNET.

Тепер перевіримо результат роботи протоколу VRRP на маршрутизаторах R6 та R7. Для цього виконаємо команду *interface vrrp print* на обох маршрутизаторах (рис. 3.10 – 3.11).

```
[Admin@MikroTik] > interface vrrp print
Flags: X - disabled, I - invalid, R - running, M - master, B - backup
# NAME INTER... MAC-ADDRESS URI PRI INTERVAL U U3..
0 RM vrrp21 ether3 00:00:5E:00:01:01 1 100 1s 3 ipv4
[Admin@MikroTik] >
```

Рисунок 3.10 – Перевірка роботи VRRP на маршрутизаторі R6

З рисунку 3.10 бачимо, що маршрутизатор R6 знаходиться у стані *Master*, тобто він є основним.

```
[Admin@MikroTik] > interface vrrp print
Flags: X - disabled, I - invalid, R - running, M - master, B - backup
# NAME INTER... MAC-ADDRESS URI PRI INTERVAL U U3..
0 B vrrp21 ether3 00:00:5E:00:01:01 1 100 1s 3 ipv4
[Admin@MikroTik] >
```

Рисунок 3.11 – Перевірка роботи VRRP на маршрутизаторі R7

З рисунку 3.11 бачимо, що маршрутизатор R6 знаходиться у стані *Backup*, тобто він є резервним.

Оскільки на рівні ядра між маршрутизаторами R2 та R4 було налаштовано віртуальну захищену мережу типу “Site-to-Site” з використанням протоколу IPSec, то перевіримо її роботу за допомогою програмного додатку Wireshark (рисунок 3.12).

4	10.720000	cc:01:2a:c4:00:01	cc:01:2a:c4:00:01	LOOP	60 Reply
5	11.010000	197.93.21.1	224.0.0.9	RIPv2	106 Response
6	15.055000	197.93.21.2	224.0.0.9	RIPv2	186 Response
7	16.203000	cc:00:2a:c4:00:00	CDP/VTP/DTP/PagP/UDCDP		356 Device ID: Cisco_3.lab.1
8	16.844000	197.93.21.1	198.93.21.2	ESP	150 ESP (SPI=0x03c378b5)
9	16.888000	198.93.21.2	197.93.21.1	ESP	150 ESP (SPI=0xe7689548)
10	16.908000	197.93.21.1	198.93.21.2	ESP	150 ESP (SPI=0x03c378b5)
11	16.931000	198.93.21.2	197.93.21.1	ESP	150 ESP (SPI=0xe7689548)
12	16.942000	197.93.21.1	198.93.21.2	ESP	150 ESP (SPI=0x03c378b5)
13	16.966000	198.93.21.2	197.93.21.1	ESP	150 ESP (SPI=0xe7689548)
14	16.976000	197.93.21.1	198.93.21.2	ESP	150 ESP (SPI=0x03c378b5)
15	16.999000	198.93.21.2	197.93.21.1	ESP	150 ESP (SPI=0xe7689548)
16	17.009000	197.93.21.1	198.93.21.2	ESP	150 ESP (SPI=0x03c378b5)
17	17.032000	198.93.21.2	197.93.21.1	ESP	150 ESP (SPI=0xe7689548)
18	19.999000	cc:00:2a:c4:00:00	cc:00:2a:c4:00:00	LOOP	60 Reply

Рисунок 3.12 – Перевірка роботи VPN

З рисунку 3.12 бачимо, що дані, які передаються між маршрутизаторами R2 та R4, представлені в зашифрованому вигляді, тобто віртуальна захищена мережа працює правильно.

Висновки до третього розділу

Отже, в третьому розділі впускної кваліфікаційної роботи було обґрунтовано вибір реального обладнання та програмного забезпечення; обладнання було обране серед провідних виробників мережевого обладнання фірм Cisco та MikroTik і воно повністю відповідає поставленим вимогам; також було проведено налагодження базових засобів міжмережевої взаємодії та засобів захисту; проведено тестування роботи захищеної інтранет-мережі.

ВИСНОВКИ

В результаті виконання випускної кваліфікаційної роботи було отримано наступні результати:

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

Проведено аналіз технологій захисту інтранет-мереж та сучасних технологічних рішень захисту інформації провідних виробників мережевого обладнання, таких як Cisco та MikroTik.

Розроблено проект топології інтранет-мережі та визначена необхідна кількість мережевого обладнання.

Розроблено проект системи адресації мережі та проект підсистеми захисту інтранет-мережі організації.

Проведено вибір та налагодження обладнання захищеної інтранет-мережі, а саме: налаштування базових засобів міжмережевої взаємодії та засобів захисту інтранет-мережі.

Проведено тестування налаштованої мережі, результатом якого є правильне функціонування всіх налаштованих параметрів.

При проведенні тестування нашої системи, вона показала надійну і адекватну роботу, тому вона може бути використана в реальному житті.

Спроектowana захищена інтранет-мережа повністю відповідає поставленим вимогам і в подальшому може бути розширена і допрацьована.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Боллапрагада В., Мэрфи К., Уайт Р., Структура операционной системы Cisco IOS. Для профессионалов. / В. Боллапрагада, К. Мэрфи, Р. Уайт – М., Вильямс, 2002. – 208 с.
2. Браун С. Виртуальные частные сети. Из-во Лори, McGraw-Hill Companies, 2001. / С. Браун – 508 с.
3. Галкин В., Григорьев Ю. Телекоммуникации и сети: Учеб. пособие для вузов. / В., Галкин, Ю. Григорьев – М.: Изд-во МГТУ им. Н.Э. Баумана, 2003. – 608 с.
4. ГОСТ 12.2.032-78. Робоче місце при виконанні робіт сидячи. Загальні ергономічні вимоги.
5. Грайворонський М. Безпека інформаційно-комунікаційних систем / М. Грайворонський. – К.: Видавнича група BNV, 2009 – 608 с.
6. Гук М. Аппаратные средства локальных сетей. Энциклопедия / М. Гук – СПб.: “Питер”, 2000. – 576 с.
7. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення.
8. Жітецький В., Джігірей В., Основі охорони праці. Навчальний посібник. / В. Жітецький, В. Джігірей, – Львів: Афіша, 2000. – 350 с.
9. 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).
10. 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).
11. Запечников С., Милославская Н., Толстой А. Основы построения виртуальных частных сетей: Учеб. пособие для вузов. М: Горячая линия / С. Запечников, Н. Милославская, А. Толстой – Телеком, 2003. – 249 с.

12. Кулаков Ю., Луцкий Г. Компьютерні мережі. Підручник / За редакцією Ю. Ковтанюка. – К.: Юніор, 2003. – 400 с.
13. Ленков С. Методы и средства защиты информации. В 2-х томах / С. Ленков, Д. Перегудов, В. Хорошко. – К.: Арий, 2008. – Том II. Информационная безопасность. – 344 с.
14. Малюк А., Пазизин С., Погожин Н. Введение в защиту информации в автоматизированных системах: Учеб. пособие. / А. Малюк, С. Пазизин, Н. Погожин – М.: Горячая линия – Телеком, 2005. – 147 с.
15. НД ТЗІ 1.1-002-99: Загальні положення по захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 №22.
16. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. / В. Олифер, Н. Олифер – СПб.: Питер, 2010. – 944 с.
17. Олифер В., Олифер Н. Сетевые операционные системы: Учебник для вузов. 2-е изд. / В. Олифер, Н. Олифер – СПб.: Питер, 2007. – 672 с.
18. Офіційний веб-сайт компанії Cisco Systems. URL: <http://www.cisco.com/>
19. Офіційний веб-сайт компанії MikroTik. URL: <http://mikrotik.com/>
20. Поповский В. Защита информации в телекоммуникационных сетях: Учебник: В 2 т. / В. Поповский, А. Персигов. – Харьков: ООО “Компания СМІТ”, 2006. – Т.2. – 292 с.
21. СНІП № 4-79. Природне і штучне освітлення. Норми проектування.
22. Хорев А. Способы и средства защиты информации / А. Хорев. – М.: МО РФ, 2000. – 316 с.
23. Хорошко В. Методы и средства защиты информации / В. Хорошко, А. Чекатов. – К.: Юниор, 2003. – 478 с.
24. Юдін О.К., Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних: Підручник / О. Юдін, О. Корченко, Г. Конахович – К: Вид-во ТОВ “НВП” ІНТЕРСЕРВІС”, 2009. – 716 с.

ДОДАТКИ

Додаток А – Технічні характеристики пристроїв

Таблиця А1 - Технічні характеристики комутатора Cisco Linksys SD216T-EU

Виробник	Cisco Linksys
Модель	SD216T-EU
Кількість портів	16 портів Ethernet 10Base-T/100Base-TX/1000BASE-T
Комутаційна здатність	100 Мбит/с
Протоколи	Ethernet, Fast Ethernet, Gigabit Ethernet.
Розмір таблиці MAC адрес	32000
Основні характеристики	• автоматичний MDI/MDI-X; • керування потоками даних; • автоматичне узгодження; • дуплекс; • автоматичне визначення пристроїв.
Розмір	130 x 127 x 41мм
Вага	0,5 кг
Діапазон робочих температур	0 – 40 °C
Робочий діапазон вологості	10 – 90 %

Таблиця А2 - Технічні характеристики комутатора Cisco Linksys WS-C3750X-24P-S

Виробник	Cisco Linksys
Модель	3750X
Кількість портів	24 порти Ethernet 10Base-T/100Base-TX/1000BASE-T
Комутаційна здатність	160 Гбіт/с
Протоколи	Ethernet, Fast Ethernet, Gigabit Ethernet.
Розмір таблиці MAC адрес	8000
Основні характеристики	• автоматичний MDI/MDI-X; • керування потоками даних; • автоматичне узгодження; • дуплекс; • автоматичне визначення пристроїв.
Розмір	44,5 x 445 x 460 мм
Вага	7,2кг
Діапазон робочих температур	0 – 40 °C
Робочий діапазон вологості	10 – 90 %

Таблиця А3 - Технічні характеристики маршрутизатора Cisco 7206

Тип пристрою	Маршрутизатор
Форм-фактор	Rack-mountable – модульний
Ширина x висота x глибина	42,7x43,2x13,3 см
Пам'ять RAM	1 GB DDR SDRAM
Флеш-пам'ять	256 MB
Канальний протокол	Ethernet, FastEthernet, Gigabit Ethernet
Транспортний протокол	OSPF, IGRP, RIP, IS-IS, BGP, EIGRP, HSRP
Підтримувані стандарти	IEEE 802.1Q
Інтерфейси	3 x network - Ethernet 10Base-T/100Base-TX/1000Base-T - RJ-45 1 x management - console - RJ-45 1 x serial - auxiliary - RJ-45 1 x management - Ethernet 10Base-T/100Base-TX - RJ-45 2 x USB - 4 PIN USB Тип А
Операційна система	Cisco IOS
Програмне забезпечення	Cisco IOS IP Base
Мін робоча температура	5 °C
Мак робоча температура	40 °C
Робочий діапазон вологості	5 - 85%

Таблиця А4 - Технічні характеристики маршрутизатора RouterBOAR750GL

Тип пристрою	Маршрутизатор
Форм-фактор	Rack-mountable – модульний
Ширина x висота x глибина	113x89x28 см
Швидкість центрального процесору	400MHz
Флеш-пам'ять	64 MB
Канальний протокол	Ethernet, FastEthernet, Gigabit Ethernet
Транспортний протокол	OSPF, RIP, BGP, VRRP
Підтримувані стандарти	IEEE 802.1Q
Кількість портів Gigabit Ethernet	5
Операційна система	RouterOS Level 4 license
Вага	129 г
Мін робоча температура	-30 °C
Мак робоча температура	70 °C
Робочий діапазон вологості	10 - 65%

Налаштування маршрутизатора R1:

```

Current configuration : 1842 bytes
!
version 12.4
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Cisco_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
ip domain name lab.local
no ip dhcp use vrf connected
ip dhcp excluded-address 192.93.21.2 192.93.21.7
ip dhcp excluded-address 192.93.21.138 192.93.21.254
!
ip dhcp pool Dhcp1
  host 192.93.21.8 255.255.255.0
  client-identifier 0108.0027.d18f.60
  default-router 192.93.21.1
  client-name Win_1
!
key chain priv
key 1
  key-string mystr
!
username Admin secret 5 $1$2.3A$XGkrpkMUQbWOqabaHBgeT.
!
interface Loopback0
  ip address 10.10.10.10 255.255.255.255
!
interface FastEthernet0/0
  ip address 192.93.21.1 255.255.255.0
  duplex auto
  speed auto
!
interface FastEthernet0/1
  ip address 196.93.21.1 255.255.255.0
  ip rip authentication mode md5
  ip rip authentication key-chain priv
  duplex auto
  speed auto
!
interface FastEthernet1/0
  ip address 193.93.21.1 255.255.255.224
  duplex auto
  speed auto
!

router rip
  version 2
  network 192.93.21.0
  network 193.93.21.0
  network 196.93.21.0
!

```

```

no ip http server
no ip http secure-server
ip forward-protocol nd
!
logging trap debugging
logging source-interface Loopback0
logging 192.93.21.8
access-list 101 deny tcp any any eq telnet
no cdp run
!
radius-server host 192.93.21.8 auth-port 1812 acct-port 1813
radius-server key t123
!
control-plane
!
line con 0
exec-timeout 0 0
privilege level 15
password 123
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
transport input ssh
!
end

```

Налаштування маршрутизатора R2:

```

Current configuration : 1831 bytes
!
version 12.4
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Cisco_2
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
!
ip cef
no ip domain lookup
ip domain name lab.local
!
key chain priv
key 1
  key-string mystr
!
username Admin secret 5 $1$t91K$k83Yg1G1ghs6fiUGwkG2H0
!
ip ssh version 1
!
crypto isakmp policy 1
  encr 3des
  hash md5
  authentication pre-share
  group 2
crypto isakmp key kluch address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set vpn esp-3des esp-md5-hmac
mode transport
!
crypto map vpn 1 ipsec-isakmp

```

```

set peer 198.93.21.2
set transform-set vpn
set pfs group2
match address ToMik
!
interface Loopback0
ip address 20.20.20.20 255.255.255.255
!
interface FastEthernet0/0
ip address 196.93.21.2 255.255.255.252
ip rip authentication mode md5
ip rip authentication key-chain priv
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 197.93.21.1 255.255.255.252
ip rip authentication mode md5
ip rip authentication key-chain priv
duplex auto
speed auto
crypto map vpn
!
router rip
version 2
network 196.93.21.0
network 197.93.21.0
!
no ip http server
no ip http secure-server
ip forward-protocol nd
!
ip access-list extended ToMik
permit ip 197.93.21.0 0.0.0.3 198.93.21.0 0.0.0.3
logging trap debugging
logging source-interface Loopback0
logging 192.93.21.8
access-list 101 deny tcp any any eq telnet
no cdp run
!
control-plane
!
line con 0
exec-timeout 0 0
privilege level 15
password 123
logging synchronous
login local
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login local
transport input ssh
!
end

```

Налаштування маршрутизатора R3:

```

Current configuration : 1623 bytes
!
version 12.4
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Cisco_3
!
boot-start-marker

```

```

boot-end-marker
!
no aaa new-model
memory-size iomem 5
!
ip cef
no ip domain lookup
ip domain name lab.local
!
key chain priv
key 1
    key-string mystr
!
username Admin secret 5 $1$Q.Ru$EADd7Ms2dLnRdZKqAtG/x0
!
interface Loopback0
ip address 30.30.30.30 255.255.255.255
!
interface FastEthernet0/0
ip address 197.93.21.2 255.255.255.252
ip rip authentication mode md5
ip rip authentication key-chain priv
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 198.93.21.1 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 2 md5 mystr
duplex auto
speed auto
!
!
router ospf 1
log-adjacency-changes
area 0 authentication message-digest
redistribute static metric 200 subnets
redistribute rip metric 200 subnets
network 198.93.21.0 0.0.0.3 area 0
!
router rip
version 2
redistribute static metric 1
redistribute ospf 1 metric 1
network 197.93.21.0
!
no ip http server
no ip http secure-server
ip forward-protocol nd
!
logging trap debugging
logging source-interface Loopback0
logging 192.93.21.8
access-list 101 deny tcp any any eq telnet
!
control-plane
!
line con 0
exec-timeout 0 0
privilege level 15
password 123
logging synchronous
login local
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login local
transport input ssh
!
end

```

Налаштування маршрутизатора R4:

```
# jun/04/2013 17:26:02 by RouterOS 5.20
# software id = VSZV-1YJJ
#
/ip hotspot user profile
set [ find default=yes ] idle-timeout=none keepalive-timeout=2m
/ip ipsec proposal
add auth-algorithms=md5 name=Ipsec
/system logging action
add name=action1 remote=194.93.21.155 target=remote
/tool user-manager customer
add backup-allowed=yes disabled=no login=admin password="" \
    paypal-accept-pending=no paypal-allowed=no paypal-secure-response=no \
    permissions=owner signup-allowed=no time-zone=-00:00
/ip address
add address=198.93.21.2/30 interface=ether2
add address=199.93.21.1/30 interface=ether3
add address=200.93.21.1/30 interface=ether4
add address=201.93.21.1/30 interface=ether5
add address=192.168.56.2/24 interface=ether1
/ip firewall filter
add action=drop chain=output protocol=tcp src-port=23
/ip ipsec peer
add address=197.93.21.1/32 secret=kluch
/ip ipsec policy
add dst-address=197.93.21.1/32 proposal=Ipsec sa-dst-address=197.93.21.1 \
    sa-src-address=198.93.21.2 src-address=198.93.21.2/32
/routing ospf interface
add authentication=md5 authentication-key=mystr authentication-key-id=2 \
    interface=ether2
add authentication=md5 authentication-key=mystr authentication-key-id=2 \
    interface=ether3
add authentication=md5 authentication-key=mystr authentication-key-id=2 \
    interface=ether4
add authentication=md5 authentication-key=mystr authentication-key-id=2 \
    interface=ether5
/routing ospf network
add area=backbone network=198.93.21.0/30
add area=backbone network=199.93.21.0/30
add area=backbone network=200.93.21.0/30
add area=backbone network=201.93.21.0/30
/system lcd
set contrast=0 enabled=no port=parallel type=24x4
/system lcd page
set time disabled=yes display-time=5s
set resources disabled=yes display-time=5s
set uptime disabled=yes display-time=5s
set packets disabled=yes display-time=5s
set bits disabled=yes display-time=5s
set version disabled=yes display-time=5s
set identity disabled=yes display-time=5s
set ether5 disabled=yes display-time=5s
set ether4 disabled=yes display-time=5s
set ether3 disabled=yes display-time=5s
set ether2 disabled=yes display-time=5s
set ether1 disabled=yes display-time=5s
/system logging
add action=action1 topics=system
```

Налаштування маршрутизатора R5:

```
# jun/04/2013 17:28:06 by RouterOS 5.20
# software id = X8QN-ATGL
#
/ip hotspot user profile
set [ find default=yes ] idle-timeout=none keepalive-timeout=2m
/ip pool
add name=mypool ranges=194.93.21.7-194.93.21.156
/ip dhcp-server
add address-pool=mypool disabled=no interface=ether3 name=Dhcp2
/system logging action
```

```

add name=action1 remote=194.93.21.155 target=remote
/tool user-manager customer
add backup-allowed=yes disabled=no login=admin password="" \
    paypal-accept-pending=no paypal-allowed=no paypal-secure-response=no \
    permissions=owner signup-allowed=no time-zone=-00:00
/ip address
add address=199.93.21.2/30 interface=ether2
add address=194.93.21.1/24 interface=ether3
add address=192.168.56.3/24 interface=ether1
/ip dhcp-server network
add address=194.93.21.0/24 dns-server=194.93.21.1 gateway=194.93.21.1
/ip firewall filter
add action=drop chain=output protocol=tcp src-port=23
/radius
add address=194.93.21.155 secret=t123 service=login
/radius incoming
set accept=yes port=1813
/routing ospf interface
add authentication=md5 authentication-key=mystr authentication-key-id=2 \
    interface=ether2
add authentication=md5 authentication-key=mystr authentication-key-id=2 \
    interface=ether3
/routing ospf network
add area=backbone network=199.93.21.0/30
add area=backbone network=194.93.21.0/24
/system lcd
set contrast=0 enabled=no port=parallel type=24x4
/system lcd page
set time disabled=yes display-time=5s
set resources disabled=yes display-time=5s
set uptime disabled=yes display-time=5s
set packets disabled=yes display-time=5s
set bits disabled=yes display-time=5s
set version disabled=yes display-time=5s
set identity disabled=yes display-time=5s
set ether3 disabled=yes display-time=5s
set ether2 disabled=yes display-time=5s
set ether1 disabled=yes display-time=5s
/system logging
add action=action1 topics=system
/user aaa
set default-group=full use-radius=yes

```

Налаштування маршрутизатора R6:

```

# jun/04/2013 17:29:23 by RouterOS 5.20
# software id = C7BI-SYVE
#
/interface vrrp
add interface=ether3 name=vrrp21
/ip hotspot user profile
set [ find default=yes ] idle-timeout=none keepalive-timeout=2m
/system logging action
add name=action1 remote=194.93.21.155 target=remote
/tool user-manager customer
add backup-allowed=yes disabled=no login=admin password="" \
    paypal-accept-pending=no paypal-allowed=no paypal-secure-response=no \
    permissions=owner signup-allowed=no time-zone=-00:00
/ip address
add address=200.93.21.2/30 interface=ether2
add address=195.93.21.1/27 interface=ether3
add address=195.93.21.30/32 interface=vrrp21 network=195.93.21.30
add address=192.168.56.4/24 interface=ether1
/ip firewall filter
add action=drop chain=output protocol=tcp src-port=23
/ip neighbor discovery
set vrrp21 disabled=yes
/routing ospf interface
add authentication=md5 authentication-key=mystr authentication-key-id=2 \
    interface=ether2
add authentication=md5 authentication-key=mystr authentication-key-id=2 \

```

```

interface=ether3
/routing ospf network
add area=backbone network=200.93.21.0/30
add area=backbone network=195.93.21.0/27
/system lcd
set contrast=0 enabled=no port=parallel type=24x4
/system lcd page
set time disabled=yes display-time=5s
set resources disabled=yes display-time=5s
set uptime disabled=yes display-time=5s
set packets disabled=yes display-time=5s
set bits disabled=yes display-time=5s
set version disabled=yes display-time=5s
set identity disabled=yes display-time=5s
set vrrp21 disabled=yes display-time=5s
set ether3 disabled=yes display-time=5s
set ether2 disabled=yes display-time=5s
set ether1 disabled=yes display-time=5s
/system logging
add action=action1 topics=system

```

Налаштування маршрутизатора R7:

```

# jun/04/2013 17:29:50 by RouterOS 5.20
# software id = 68SF-II2M
#
/interface vrrp
add interface=ether3 name=vrrp21
/ip hotspot user profile
set [ find default=yes ] idle-timeout=none keepalive-timeout=2m
/system logging action
add name=action1 remote=194.93.21.155 target=remote
/tool user-manager customer
add backup-allowed=yes disabled=no login=admin password="" \
    paypal-accept-pending=no paypal-allowed=no paypal-secure-response=no \
    permissions=owner signup-allowed=no time-zone=-00:00
/ip address
add address=201.93.21.2/30 interface=ether2
add address=195.93.21.2/27 interface=ether3
add address=195.93.21.30/32 interface=vrrp21 network=195.93.21.30
add address=192.168.56.5/24 interface=ether1
/ip firewall filter
add action=drop chain=output protocol=tcp src-port=23
/ip neighbor discovery
set vrrp21 disabled=yes
/routing ospf interface
add authentication=md5 authentication-key=mystr authentication-key-id=2 \
    interface=ether2
add authentication=md5 authentication-key=mystr authentication-key-id=2 \
    interface=ether3
/routing ospf network
add area=backbone network=201.93.21.0/30
add area=backbone network=195.93.21.0/27
/system lcd
set contrast=0 enabled=no port=parallel type=24x4
/system lcd page
set time disabled=yes display-time=5s
set resources disabled=yes display-time=5s
set uptime disabled=yes display-time=5s
set packets disabled=yes display-time=5s
set bits disabled=yes display-time=5s
set version disabled=yes display-time=5s
set identity disabled=yes display-time=5s
set vrrp21 disabled=yes display-time=5s
set ether3 disabled=yes display-time=5s
set ether2 disabled=yes display-time=5s
set ether1 disabled=yes display-time=5s
/system logging
add action=action1 topics=system

```