МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ АЕРОНАВІГАЦІЇ,
ЕЛЕКТРОНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ ТА РАДІОЕЛЕКТРОННИХ СИСТЕМ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри

_____ Роман ОДАРЧЕНКО
“_____”_____2022 р.

КВАЛІФІКАЦІЙНА РОБОТА

(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ МАГІСТР

Тема: «Оптимізація інтрамережі підприємства»

Виконавець: _____ Ілля МАЗУРЕНКО
(підпис)

Керівник: _____ Ірина КОЗЛЮК
(підпис)

Консультанти з окремих розділів пояснювальної записки:

Консультант розділу «Охорона праці» _____ Батир ХАЛМУРАДОВ
(підпис)

Консультант розділу «Охорона навколишнього середовища»
_____ Євгеній БОВСУНОВСЬКИЙ
(підпис)

Нормоконтролер: _____ Денис БАХТІЯРОВ
(підпис)

Київ 2022

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет аеронавігації, електроніки та телекомунікацій
Кафедра телекомунікаційних та радіоелектронних систем
Спеціальність 172 «Телекомунікації та радіотехніка»
Освітньо-професійна програма «Телекомунікаційні системи та мережі»

ЗАТВЕРДЖУЮ
Завідувач кафедри

Роман ОДАРЧЕНКО
“_____”_____2022 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

Мазуренка Іллі Олександровича
(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема кваліфікаційної роботи: «Оптимізація інтрамережі підприємства» затверджена наказом ректора від «07» вересня 2022 р. №1321/ст

2. Термін виконання роботи: з 05.09.2022 р. по 30.11.2022 р.

3. Вихідні дані до роботи: інтрамережа підприємства

4. Зміст пояснювальної записки: загальна характеристика інтрамережі, аналіз підходів до побудови захищеної інтрамережі підприємства, проєкт захищеної інтрамережі підприємства в віртуальному середовищі EVE-NG

5. Перелік обов'язкового графічного (ілюстративного) матеріалу: проєкт захищеної інтрамережі підприємства в віртуальному середовищі EVE-NG, налаштування комутаційного обладнання інтрамережі підприємства

6. Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1	Розробити деталізований зміст розділів кваліфікаційної роботи	05.09.2022-06.09.2022	Виконано
2	Вступ	07.09.2022-10.09.2022	Виконано
3	Загальна характеристика інтрамережі	12.09.2022-05.10.2022	Виконано
4	Аналіз підходів до побудови захищеної інтрамережі підприємства	06.10.2022-15.10.2022	Виконано
5	Проєкт захищеної інтрамережі підприємства в віртуальному середовищі EVE-NG	17.10.2022-05.11.2022	Виконано
6	Охорона праці	07.11.2022-12.11.2022	Виконано
7	Охорона навколишнього середовища	14.11.2022-19.11.2022	Виконано
8	Усунення недоліків та захист кваліфікаційної роботи	21.11.2022-30.11.2022	Виконано

7. Консультанти з окремих розділів

Розділ	Консультант (посада, П.І.Б.)	Дата, підпис	
		Завдання видав	Завдання прийняв
Охорона праці	к.м.н., проф. Батир ХАЛМУРАДОВ		
Охорона навколиш-нього середовища	к.т.н., доц. Євгеній БОВСУНОВСЬКИЙ		

8. Дата видачі завдання: “22" серпня 2022 р.

Керівник кваліфікаційної роботи _____ Ірина КОЗЛЮК
(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ Ілля МАЗУРЕНКО
(підпис випускника) (П.І.Б.)

РЕФЕРАТ

Кваліфікаційна робота «Оптимізація інтрамережі підприємства» містить 103 сторінки, 28 рисунків, 5 таблиць, 46 використаних джерел.

АВТОМАТИЧНА ТЕЛЕФОННА СТАНЦІЯ, VIRTUAL LOCAL AREA NETWORK, FIRST HOP REDUNDANCY PROTOCOL, VIRTUAL PRIVATE NETWORK, ARCHITECTURE FOR VOICE, VIDEO AND INTEGRATED DATA, VIRTUAL ROUTER REDUNDANCY PROTOCOL.

Мета кваліфікаційної роботи - створення оптимізованої схеми захищеної інтрамережі підприємства, готової до впровадження в компанії з реальними умовами.

Об'єктом дослідження – процес побудови корпоративної інтрамережі мережі підприємства.

Предметом дослідження – корпоративна інтрамережа підприємства.

Методи дослідження – порівняльний аналіз, теоретичні знання та практичні надбання в галузі комп'ютерних мереж та програмного забезпечення

Наукова новизна отриманих результатів – набули подальшого розвитку методи моделювання корпоративних мереж.

Практичне значення отриманих результатів – розглянуто принципи архітектури та життєвий цикл побудови мережі. Взято до уваги питання відмовостійкості та живучості апаратного комплексу, що використовується у віртуальному середовищі. Створено тестову схему мережі для компанії середнього розміру. Схема може бути адаптована і розгорнута для множини типових середніх компаній. Віртуальна лабораторія EVE-Ng розгортається серед операційної системи Windows.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ

АТС – Автоматична телефонна станція.

VLAN – Virtual Local Area Network (Віртуальна локальна мережа).

FHRP – First Hop Redundancy Protocol (Протокол резервування першого переходу).

VPN – Virtual Private Network (Віртуальна приватна мережа).

AVVID – Architecture for Voice, Video and Integrated Data (Архітектура для голосу, відео та інтегрованих даних).

VRRP – Virtual Router Redundancy Protocol (Протокол резервування віртуального маршрутизатора).

SDC – Software-Defined Camera (Програмно-визначена камера).

VoIP – Voice over IP (Голос через IP).

TLS – Transport Layer Security (Протокол захисту транспортного рівня).

SRTP – Secure Real-time Transport Protocol (Безпечний протокол передачі даних в реальному часі).

ВСТУП

Актуальність теми. Основою інфраструктури сучасних підприємств є інтрамережі передачі даних, що надають транспорт для передачі інформації між різними програмами інформаційних систем.

Останнім часом мультисервісні мережі змінюються спеціалізованим мережам. Для забезпечення потреб вимог до мультисервісної корпоративної інтрамережі, безперервно зростають, як до середовища передачі інформації для виконання різних додатків. Високе значення має час реакції, він потребує належної організації корпоративної мережі та додатків. Робота в реальному часі стала життєвою необхідністю і однією з головних вимог, що висуваються до корпоративних мереж та додатків.

Але при цьому гарантувати гарний час реакції та належну інформаційну безпеку особливо важко - цьому перешкоджає різноманітність потоків даних та їхня висока інтенсивність, потреба здійснювати пошук даних в базах великого обсягу, невисока швидкість глобальних ліній зв'язку між підрозділами, уповільнення швидкості взаємодії у шлюзах, що узгоджують неоднорідні компоненти різних підмереж.

Підтримка роботи установ, що користуються цією мережею – одна з головних цілей корпоративної інтрамережі. Користувачами корпоративної мережі є працівники цього підприємства. Така мережа включає відділення у різних регіонах по всій Україні, будучи складовою мережею, що включає сегменти глобальної і локальної мережі.

Таким чином, актуальність теми дипломної роботи обумовлена необхідністю створення надійної, захищеної та повнофункціональної корпоративної інтрамережі підприємства [1-30].

Мета кваліфікаційної роботи - створення оптимізованої схеми захищеної інтрамережі підприємства, готової до впровадження в компанії з реальними умовами.

Для досягнення поставленої мети вирішуються такі наукові завдання.

1. аналіз принципів архітектури та життєвого циклу побудови мережі;
2. аналіз відмовостійкості та живучості апаратного комплексу, що використовується у віртуальному середовищі;

3. створення тестової схеми мережі для компанії середнього розміру;
4. впровадження засобів інформаційної безпеки з подальшою оптимізацією роботи мережі.

Об'єктом дослідження – процес побудови корпоративної інтрамережі мережі підприємства.

Предметом дослідження – корпоративна інтрамережа підприємства.

Методи дослідження: порівняльний аналіз, теоретичні знання та практичні надбання в галузі комп'ютерних мереж та програмного забезпечення

Наукова новизна отриманих результатів. Набули подальшого розвитку методи моделювання корпоративних мереж.

Практичне значення отриманих результатів.

Розглянуто принципи архітектури та життєвий цикл побудови мережі. Взято до уваги питання відмовостійкості та живучості апаратного комплексу, що використовується у віртуальному середовищі. Створено тестову схему мережі для компанії середнього розміру. Схема може бути адаптована і розгорнута для множини типових середніх компаній. Віртуальна лабораторія EVE-Ng розгортається серед операційної системи Windows.

РОЗДІЛ 1
ЗАГАЛЬНА ХАРАКТЕРИСТИКА ІНТРАМЕРЕЖІ

1.1. Корпоративна мережа як об'єкт дослідження

Корпоративна мережа - це складний комплекс взаємопов'язаних та узгоджено функціонуючих апаратних та програмних компонентів, що забезпечує передачу інформації між різними віддаленими програмами та системами, що використовуються на підприємстві. Через наявність кількох центрів обробки даних корпоративні мережі належать до децентралізованих (або розподілених) обчислювальних систем [1].

Корпоративну мережу необхідно розглядати з різних боків: структурної, функціональної та системно-технічної.

Зі структурної точки зору корпоративна мережа - мережа змішаної топології, що містить кілька локальних обчислювальних мереж. Корпоративна мережа об'єднуватиме філії ЛПЗ, створюючи спільний інформаційно-корпоративний простір. З цього погляду корпоративна мережа відбиває структуру підприємства.

З функціональної точки зору корпоративна мережа - це ефективне середовище передачі актуальної інформації, необхідної для вирішення завдань.

З системно-технічної точки зору корпоративна мережа є цілісною структурою, що складається з взаємопов'язаних і взаємодіючих рівнів, представлених на рис. 1.1.

Таким чином, з системно-технічної точки зору корпоративна мережа - це складна система, що надає користувачам та програмам набір корисних роботі послуг та сервісів, загальносистемних та спеціалізованих додатків, що володіє набором корисних якостей і властивостей, і містить служби, що гарантує нормальне функціонування корпоративної мережі [1].

Рис. 1.1. Ієрархія рівнів корпоративної мережі [9]

Роль корпоративних мереж в створенні і розвитку IT- інфраструктури. В даний час IT-інфраструктура будь-якого підприємства - це його ключова інфраструктура, незалежно від виду діяльності. Для впровадження інформаційних технологій транспортну базу організують корпоративні мережі передачі.

Сучасна корпоративна мережа - це не тільки мережа передачі даних, а складний комплекс, який здатний надавати різні послуги з прогнозованими характеристиками.

Завдяки корпоративним мережам результативно вирішуються завдання ключових процесів. Таких як:

• швидкий доступ до інформаційних масивів загального інформаційного простору;

• аналіз стану і управління бізнес-процесами з єдиного аналітичного центру;

• обмін інформаційними і розрахунковими документами;

• безперервне автоматизоване спостереження (моніторинг) та управління ресурсами інфокомунікаційної системи з єдиного центру [1].

1.2. Особливості проєктування корпоративних мереж

Основна мета проєктування корпоративних мереж полягає в тому, щоб визначити структуру, склад апаратно-програмних засобів та організацію корпоративної мережі. І при заданих обмеженнях на витрати на її проєктування, впровадження та обслуговування вони виконуватимуть основні вимоги до якості інформаційних послуг, що надаються мережею. І будується це на основі характеристик корпоративних інформаційних потоків підприємства, параметрів споживачів та виробників інформації. При проєктуванні корпоративної мережі мережеві адміністратори та мережеві інтегратори намагаються забезпечити виконання таких вимог [2]:

- розширюваність – можливість простої інтеграції окремих компонентів мережі (користувачів, додатків, служб, комп'ютерів).
- масштабованість - можливість додавання нових вузлів та протяжність зв'язків, а також продуктивності вузлів та мережевого обладнання;
- продуктивність - забезпечення необхідних значень параметрів продуктивності мережевих вузлів та каналів зв'язку (швидкість передачі даних, час реакції, затримка передачі та її варіація);
- керованість - забезпечення можливостей централізованого управління, планування розвитку мережі та моніторингу стану мережі;
- надійність - забезпечення безперебійної роботи вузлів мережі та каналів зв'язку, узгодженості, збереження та доставки даних без змін та помилок вузлу призначення;
- безпека - забезпечення захисту даних від несанкціонованого доступу.

Враховуючи масштабність, використання глобальних зв'язків, високий ступінь різнорідності проєктування корпоративних мереж є процесом, що важко формалізується. На сьогоднішній день відсутні універсальні методики проєктування корпоративних мереж. Тому потрібно сформулювати деякі типові етапи виконання мережевих проєктів.

Процес проєктування корпоративної мережі складається з наступних етапів: [2]

1. Аналіз вимог . На цьому етапі формулюються основні цілі підприємства (оперативний прийом замовлень, скорочення виробничого циклу, підвищення продуктивності праці тощо). Аналізуються існуючі аналогічні системи, обґрунтовується потреба у проєктах системи.

2. Розробка бізнес-моделі підприємства. Бізнес-модель або функціональна модель виробництва викладає основні, адміністративні та допоміжні бізнес-процеси підприємства, ієрархічні взаємини та інформаційні потоки між підрозділами. Також передає структуроване відображення функцій виробничої системи, інформації середовища та об'єктів, що пов'язують ці функції.

3. Розробка технічної моделі корпоративної мережі (структурний синтез). Технічна модель представляє собою сукупність технічних засобів, необхідних для реалізації проєкту корпоративної мережі. На даному етапі визначаються технічні параметри компонентів мережі, такі як повний функціональний набір необхідних програмних та апаратних засобів, але без конкретизації обладнання (марок та моделей).

4. Розробка фізичної моделі корпоративної мережі (параметричний синтез). Фізична модель корпоративної мережі представляє докладний опис програмних і технічних засобів, їх кількості, технічних параметрів і способів взаємодії. Таким чином, це конкретизація технічної моделі мережі, в якій вибрані протоколи, конкретні мережні пристрої та інші мережеві технічні засоби. Вибираються вони відповідно до технічних параметрів, що задаються в технічній моделі. Параметри, структурна схема та алгоритми функціонування мережі як результати виконання даного етапу використовуються для подальшого аналізу.

5. Моделювання та оптимізація корпоративної мережі. Моделювання проводиться на даному етапі з метою оцінки характеристик функціонування корпоративної мережі та їхньої оптимізації.

6. Встановлення та налагодження корпоративної мережі. На цьому етапі мається на увазі управління конфігуруванням, координування поставок від субпідрядників, інсталяцію та налагодження обладнання, навчання персоналу.

7. Тестування корпоративної мережі. на цьому етапі повинні проводитись необхідні випробування, описані у контракті з інтегратором.

8. Супровід та експлуатація корпоративної мережі. Останній етап не має чітко визначених часових кордонів, він передбачає безперервний процес [2].

Параметри якості корпоративної мережі. В даний час вимоги корпоративних користувачів і корпоративних додатків до пропускної спроможності мережі, що постійно зростають, призвели до появи нових високошвидкісних технологій і нових механізмів якості обслуговування, що враховують різні характеристики трафіку: відносна швидкість передачі даних і чутливість до затримок, втрат і спотворень пакетів. Розглянемо основні параметри якості корпоративної мережі [2]:

- пропускна спроможність мережі - інтегральний параметр характеризує обсяг інформації, що передається мережею за одиницю часу;
- реакція на характеристики профілю трафіку - параметр, що характеризує зміни навантаження на мережу в залежності від характеристик профілю трафіку.

Наприклад, зміна числа спотворених або втрачених пакетів, пропускної здатності при пульсуючій або плавній зміні трафіку; кількість спотворених чи втрачених пакетів (згідно з експертними оцінками, для протоколу TCP 1-5% втрачених пакетів знаходиться в межах норми, граничне значення при якому мережа практично не працює - 40% втрачених чи спотворених пакетів); [3]

- час доставки - час подвійного ходу (у прямому та зворотному напрямку). Цей параметр може змінюватися в діапазоні від 0 до 2000 MS , впливаючи на продуктивність роботи одного потоку; [3]
- нерівномірність часу доставки пакетів - параметр, що впливає роботу окремих додатків, наприклад, програми, керуючі технічним об'єктом у часі чи передають мультимедійну інформацію.

1.3. Трирівнева ієрархічна модель

Під час проєктування корпоративної мережі весь процес розробки було розбито на 3 частини, так як комп'ютерні мережі зручно представляти у вигляді трирівневої ієрархічної моделі, що містить такі рівні [4]:

- рівень ядра;

- рівень розподілу;
- рівень доступу.

Рівень ядра призначений для високошвидкісної передачі мережевого трафіку та швидкісної комутації пакетів. Тому на мережевих пристроях цього рівня не вводяться додаткові технології (списки доступу або маршрутизація за правилами), які відповідають за маршрутизацію та фільтрацію пакетів.

Рівень ядра чи базовий рівень представимо кількома філіями підприємства, які у різних містах. Маршрутизатори цих вузлів – маршрутизатори ядра – з'єднані між собою, утворюючи кільцеве ядро мережі з надмірними шляхами. Цей рівень призначений для оперативної та надійної комутації великих обсягів трафіку. На базовому рівні трафік передається разом для кількох користувачів. Тут обробляються великі обсяги трафіку, тому важливо враховувати швидкість і затримки. Зазвичай використовують швидкодіючі мережі Multi-Gigabit Ethernet і Gigabit Ethernet [4].

За допомогою протоколу Ethernet до кожного з маршрутизаторів підключається через комутатор маршрутизатор і група серверів, які разом утворюють демілітаризовану зону та забезпечують доступ до Інтернету. Група корпоративних серверів також підключається до кожного вузлового маршрутизатора. Кожен із маршрутизаторів ядра за допомогою технології глобальних мереж, наприклад Frame Relay, з'єднаний віртуальними каналами з маршрутизаторами інтрамережі інших філій підприємсва.

Frame Relay ("Передача кадрів") - технологія передачі даних, що активно застосовується в інтрамережах мережах різного масштабу. Основний принцип цієї технології полягає у створенні кількох віртуальних каналів одним фізичним, що кожному віртуального каналу резервується гарантована смуга пропускання. Цей принцип дає ряд істотних переваг перед виділеними цифровими каналами, і перед протоколами X.25 і TCP/IP [5].

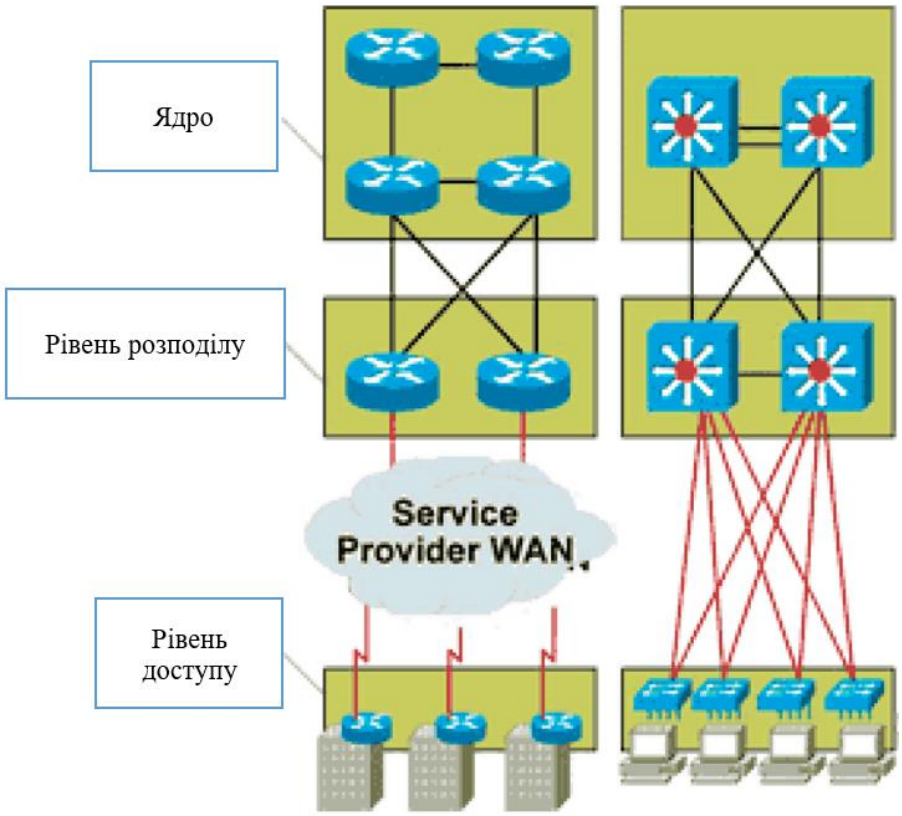

Рис. 1.2. Трирівнева Модель [11]

Рівень розподілу використовується для підсумовування маршрутів. Підсумовування проводиться для зменшення мережевого трафіку на верхніх рівнях мережі. Воно і є об'єднання декількох мереж в одну велику загальну. Основними функціями рівня розподілу є фільтрація, маршрутизація та доступ до регіональних мереж. Якщо потрібно, то й визначення правил доступу пакетів до рівня ядра. На рівні розподілу необхідно встановлювати найшвидший спосіб обробки запитів до служб, як метод файлового звернення до сервера. Маршрутизатор рівня розподілу з'єднані з маршрутизаторами ядра. На рівні доступу здійснюється контроль доступу до мережі та формується мережевий трафік. В основному використовуються мережі 100-Mbps Fast Ethernet та 1000-Mbps Gigabit Ethernet [5].

Маршрутизатори рівня доступу служать для підключення до глобальної обчислювальної мережі окремих користувачів (сервери доступу) або окремих локальних мереж. На цьому рівні реалізовано управління користувачами і робітниками групами під час звернення до ресурсів об'єднаної мережі. Іноді рівень доступу називають рів-

нем настільних систем. Найбільша частина необхідних користувачам мережевих ресурсів має бути доступна локально. На рівні розподілу виконується перенаправлення трафіку до віддалених служб. Швидкість мережі – Ethernet 100 Mbps або 1000-Mbps Ethernet [5-6].

Найпростішим комутуючим обладнанням рівня доступу є комутатори робочих груп. У свою чергу, до них приєднуються автоматизовані робочі місця працівників організації (АРМи). Через велику кількість АРМів у мережі комутатори рівня робочих груп необхідно поділити на два рівні. Комутатори робочих груп верхнього (другого) рівня об'єднуються в єдину мережу за допомогою комутаторів будівель, які в рамках одного кампуса з'єднуються в кільце оптоволоконними лініями зв'язку.

Проєктована мережа повинна відповідати вимогам надмірності та структурованості. Надмірність робить мережу стійкою до порушень каналів передачі даних та їх неполадок, підвищує надійність системи, проте збільшує трудомісткість адміністрування мережі.

1.4. Структура мережі

Територіальні комп'ютерні мережі служать для обміну даними між філіями підприємства, які у різних регіонах країни. Вони мають велику довжину і вимагають великих витрат. У їх вартість входять кабелі, робота з прокладання, витрати на комутаційне обладнання, проміжну підсилювальну апаратуру, що забезпечує необхідну смугу пропускання каналу та експлуатаційні витрати на підтримку в робочому стані [7].

Глобальна мережа не може бути повністю створена для підприємства, тому пропонується проміжний варіант: корпоративна мережа підприємства використовує обладнання громадської глобальної мережі, їх послуги, але частину доповнює своїми власними. Наприклад, оренда каналів зв'язку, з урахуванням якої створити власну територіальну мережу [7].

Локальні та глобальні мережі складається з периферійних підмереж та магістралі, яка пов'язує ці підмережі. Структуру великої локальної мережі наведено на рис.

1.3, вона складається з підмереж, об'єднаних магістраллю, що включають два кільця FDDI і чотири маршрутизатори. Кожна підмережа може мати ієрархічну структуру, утворену своїми маршуртизаторами, комутаторами, концентраторами і мережевими адаптерами. всі ці комунікаційні пристрої пов'язані розгалуженою кабельною системою. Така мережа може бути розташована біля декількох районів міста [7].

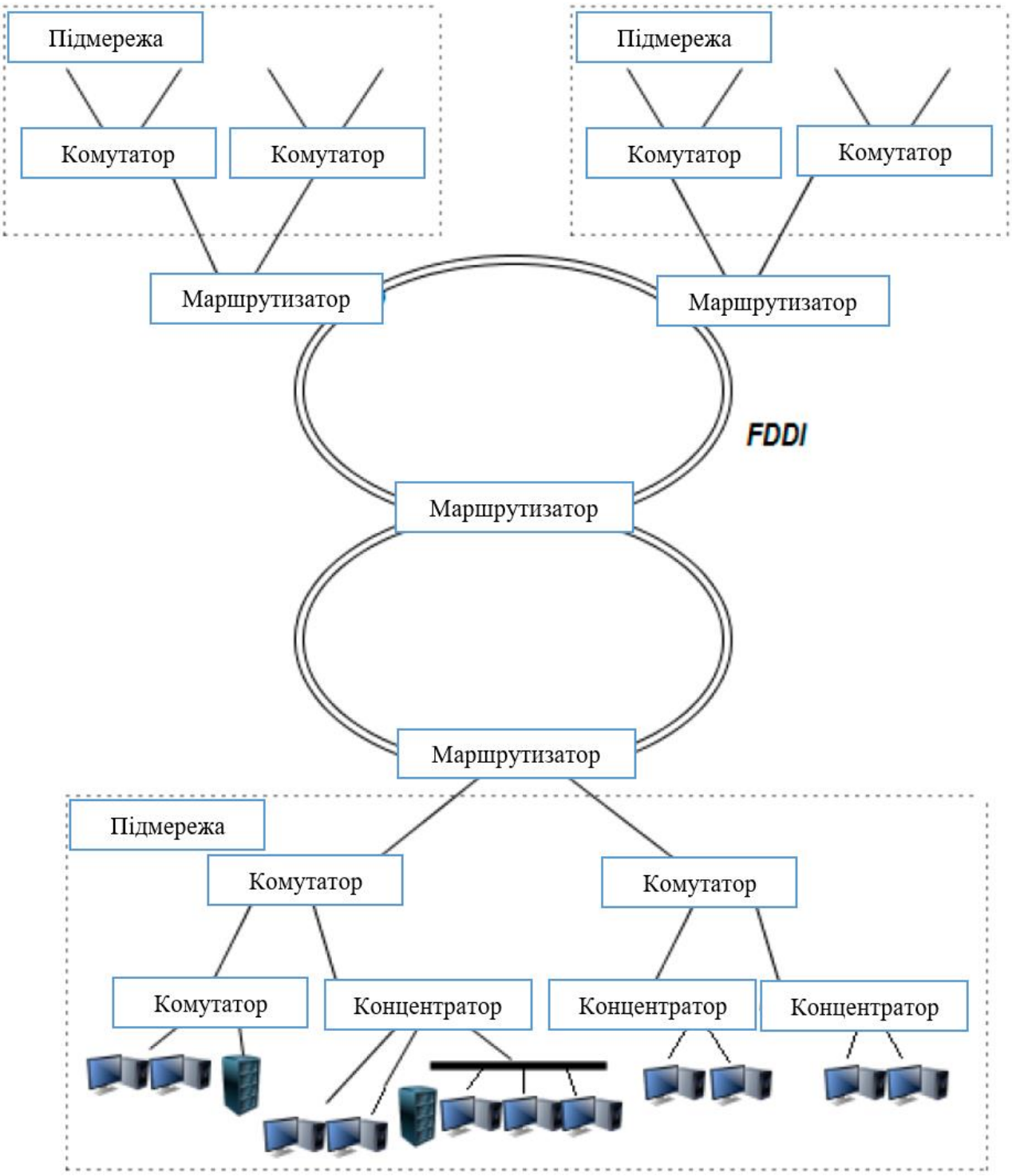

Рис. 1.3. Структура локальною мережі

Глобальна мережа з'єднує локальні мережі, розташовані на великій відстані одна від одної. Вона має ієрархічну структуру з високошвидкісною магістраллю, повільнішими периферійними мережами та каналами доступу локальних мереж до глобальних.

Структура глобальної комп'ютерної мережі наведено на рис. 1.4. В основі лежать канали зв'язку, що не комутуються, які з'єднують комутатори глобальної мережі. Комутатори називають центрами комутації пакетів (ЦКП).

У місцях, де потрібне відгалуження або з'єднання потоків даних або магістральних мереж, встановлюються комутатори. Вибір такого місця розташування комутаторів визначається також можливістю обслуговування комутаторів кваліфікованим персоналом, наявністю виділених каналів зв'язку в даному пункті, надійністю мережі, що визначається надмірними зв'язками між комутаторами.

Кінцеві вузли глобальної мережі показано на рис. 1.4. Основні типи кінцевих вузлів глобальної мережі: комп'ютери (К), локальні мережі, маршрутизатори (R), мультиплексори (MUX), що використовуються для одночасної передачі по комп'ютерній мережі даних і голосу (або зображення). Пристрої типу DTE (Data Terminal Equipment) перетворять користувальницьку інформацію в дані для передачі по лінії зв'язку та здійснюють зворотне перетворення. Локальна мережа відокремлена від глобального маршрутизатора або віддаленого мосту.

Тут використовуються такі позначення: S (switch) – комутатори, К – комп'ютери, R (router) – маршрутизатори, MUX (multiplexor) – мультиплексор, UNI (User-Network Interface) – «інтерфейс користувач – мережа» та NNI (Network-Network Interface) – «інтерфейс мережа – мережа». Офісна АТС – PBX, чорні квадратики – пристрої DCE.

Під час передачі даних через глобальну мережу мости і маршрутизатори працюють відповідно до тієї ж логіки, що і при з'єднанні локальних мереж. Мости будують таблицю MAC-адрес на підставі трафіку, що проходить, і за інформацією в цій таблиці приймають рішення - надавати кадри в віддалену мережу або ні.

Маршрутизатори приймають рішення на підставі номера пакету будь-якого протоколу мережного рівня (наприклад, IP або IPX). Якщо пакет потрібно передати

наступному маршрутизатору по глобальній мережі, упаковують його в кадр цієї мережі, доповнюють відповідною апаратною адресою наступного маршрутизатора і посилають у глобальну мережу [8].

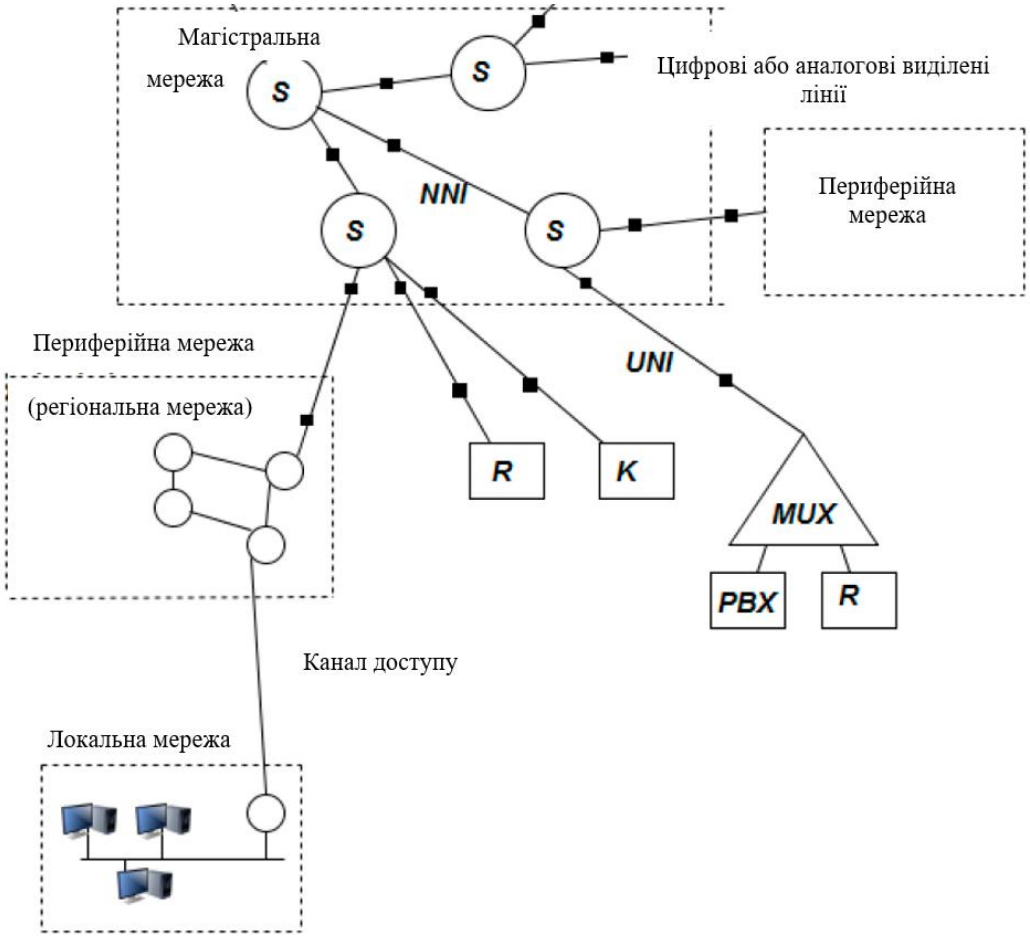

Рис. 1.4. Структура глобальною мережі

Так як кінцеві вузли глобальної мережі повинні передавати дані по каналу зв'язку конкретного стандарту, кожен пристрій типу DTE необхідно оснастити пристроєм типу DCE (Data Circuit terminating Equipment) який забезпечує необхідний протокол фізичного рівня заданого каналу. Залежно від типу каналу для зв'язку з каналами глобальних мереж використовуються DCE трьох основних типів: модеми для роботи з виділеними і комутованими аналоговими каналами, пристрої DSU/CSU для роботи з цифровими виділеними каналами мереж технології TDM і термінальні адаптери (TA) для роботи з цифровими каналами мереж ISDN Пристрої DTE та DCE узагальнено називають обладнанням, що розміщується на території абонента глобальної мережі – Customer Premises Equipment, CPE.

При використанні WAN дуже важливі послуги, що надаються мережею, і правильне визначення інтерфейсу взаємодії з мережею. Кінцеве обладнання та програмне забезпечення повинні коректно сполучатися з відповідним обладнанням та програмним забезпеченням. Забезпеченням WAN, тому у глобальній мережі суворо прописано та стандартизовано інтерфейс «користувач-мережа» (UNI - User-to-Network Interface). Це необхідно для того, щоб користувачі могли без проблем підключатися до мережі за допомогою комунікаційного обладнання будь-якого виробника, який дотримується стандарту UNI даної технології (наприклад, X.25).

Протоколи взаємодії комутаторів усередині глобальної мережі, які називають інтерфейсом «мережа-мережа» (Network-to-Network Interface, NNI), стандартизуються не завжди. Якщо організація створює глобальну мережу, вона має мати свободу дій, щоб вирішувати, як взаємодіяти внутрішнім вузлам мережі між собою. Тому внутрішній інтерфейс, у разі його стандартизації, має назву «мережа-мережа», а не «комутатор-комутатор», підкреслюючи, що він повинен використовуватися в основному при взаємодії двох територіальних мереж різних операторів, але, якщо стандарт NNI приймається, то відповідно до нього організується взаємодія всіх комутаторів мережі, а не лише прикордонних [8-9].

РОЗДІЛ 2
АНАЛІЗ ПІДХОДІВ ДО ПОБУДОВИ ЗАХИЩЕНОЇ ІНТРАМЕРЕЖІ ПІДПРИЄМСТВА

2.1. Постановка цілей і завдань кваліфікаційної роботи

Мета кваліфікаційної роботи - створення оптимізованої схеми захищеної інтрамережі підприємства, готової до впровадження в компанії з реальними умовами. Захистити від усіх можливих загроз неможливо. Загроза існує завжди і можна лише більшою чи меншою мірою захиститись від неї. Розроблена схема буде надійною і закриє більшість вразливих зон. Для розробки буде використовуватись віртуальна лабораторія Eve-ng розгорнута на операційній системі Windows 11 Professional. Командлет, який використовується в налаштуванні емульованого обладнання, стандартний. Емулюватиметься в більшості обладнання, що надається компанією Cisco. Функціонал розробленої схеми буде доступний у розумінні та матиме ешелонований захист. Завдання, які вирішує створена мережа:

- захищене функціонування;
- своєчасна реакція на несанкціонований доступ;
- надійність функціоналу, що надається;
- відмовостійкість і живучість;
- наявність сучасних практик;
- універсальність;

Задоволення юридичних вимог. Вимоги до інтрамережі, що проєктується:

- розробка на операційній системі Windows 11 Professional. Продукт буде спрямовано реалізації у СНД просторі, у якому переважає використання операційної системи Windows 10-11. Це полегшить процес впровадження;

- розробка у віртуальній лабораторії Eve-ng. Eve-ng є мало кому відомою системою моделювання. Розробники цього продукту впроваджують найкращі рішення у галузі розробки мереж у віртуальному просторі. Можливо, у майбутньому вони зможуть скласти конкуренцію великим компаніям;
- використання сертифікатів реального обладнання емулювання. Це дозволяє зіткнутися з низкою проблем, що зустрічаються в реальних умовах, що дозволяє наблизити проєктовану систему до реальних умов;
- використання стандартного командлет для налаштування обладнання, що дозволяє адаптувати розроблену схему в багатьох компаніях.

Мережа і її топологія. В наш час важко уявити людину, яка не чула про інтернет або їм не користувався. Інтернет впевненою роблю зайшов в наші життя і міцно закріпився у них. Одним із важливих аспектів можна виділити Мережу.

Класифікація обчислювальних середовищ за територіальною поширеністю:

- **BAN(Body Area Network)** - нижня комп'ютерна мережа) - мережа носимих смарт-пристроїв, що носяться на тілі людини;
- **PAN(Personal Area Network)** - персональна мережа, що використовується для взаємодії різноманітних пристроїв одного власника;
- **LAN (Local Area Network)** - локальні мережі із замкнутою інфраструктурою, що може обслужити від маленької компанії, що базується у кількох приміщеннях, до цілих промислових підприємств, суть цієї мережі - це її закритість і допуск лише її співробітників із виділеними їм правами досутпа;
- **CAN (Campus Area Network)** - Об'єднання кількох близько розташованих локальних мереж;
- **MAN (Metropolitan Area Network)** - Мережі одного або декількох міст, що складаються з безлічі локальних мереж;
- **WAN (Wide Area Network)** - Глобальна мережа, що покриває великі географічні об'єкти [10].

Мережева топологія – це структура нашої мережі (графа), вершинами якого є обчислювальні пристрої та ребрами – інформаційні чи фізичні зв'язки між вершинами [10-12].

Класифікація по мережевим топологіям [12]:

- повнозв'язкова - у такій топології кожен обчислювальний пристрій безпосередньо пов'язаний з усіма іншими;
- шина - у такій топології всі обчислювальні пристрої підключені до однієї магістралі, але в кінцях знаходяться термінатори. Вся передача даних здійснюється через магістраль;
- зірка – у цій мережевий топології всі обчислювальні пристрої підключені до одного концентратору, вся передача даних здійснюється через концентратор;
- кільце - обчислювальні пристрої з'єднані безпосередньо між собою в одному напрямку. Дані в такий мережі йдуть по одному напрямку, а кожний обчислювальний пристрій приймає лише призначену ньому інформацію. Реалізується це все на підставі маркера, що дає в певний момент часу використовувати мережу лише певному обчислювальному пристрою, дана топологія вважається вразливою, оскільки вихід із ладу одного обчислювального пристрою призведе до порушення функціонування всієї мережі;
- дерево – дана топологія являє собою зіркову ієрархію, коли від одного обчислювального пристрою відходить кілька інших від яких у свою чергу відходять інші і таким чином виходить чітка ієрархія з топологією зірка, що нагадує дерево;
- Fat Tree (товсте дерево) - ефективна для створення високопродуктивної мережі, в якій відбувається потовщення для отримання більш високої пропускної здатності;
- змішана - така топологія включає безліч інших топологій і використовується при проєктуванні великих мереж для досягнення максимального ефекту при підборі різних типів топологій під конкретні завдання;

- децентралізація – дана мережева топологія передбачає кілька вузлів, що мають різні маршрути з'єднання у разі виходу їх ладу будь-якого компонента чи ділянки обчислювальної мережі.

За типом середовища передачі:

- дротові;
- бездротові.

Також можна виділити класифікацію за типами операційних систем (Windows, Cisco, Unix), за швидкістю передачі даних, за необхідності постійної підтримки з'єднання і т.д.

2.2. Компоненти мережі

Далі ознайомимося з основними компонентами, які можуть входити до складу мережі, частина інших буде розглянута далі [13-14].

Маршрутизатор - з'явився він вже давно разом з розвитком інтернету, під маршрутизатором розуміється фізичний мережевий пристрій (комп'ютер, обчислювальний пристрій і т.д.) який використовується для передачі інформації в локальній мережі, між різними мережами і інтернетом. Маршрутизатор також виконує роль DHCP, розподіляючи приватні IP-адреси між пристроями мережі. Таблиця маршрутизації – те, на що потім спирається маршрутизатор при побудові маршруту передачі пакетів у мережі. Таблиця маршрутизації може бути оновлена динамічно і статично, коли людина сама прописує маршрути та інтерфейси, при динамічному оновленні таблиця маршрутизації заповнюється самостійно з урахуванням протоколу, із яким взаємодіє.

Комутатор (Switch) - це фізичний мережевий пристрій, що дозволяє з'єднувати різні ділянки мережі для передачі пакетів між ними, раніше роль комутатора відігравав концентратор. Концентратор або хаб – це мережний пристрій, до якого підключені обчислювальні пристрої, але який не має технічного обладнання для аналізу даних та прийняття рішення. З комутаторами все набагато легше вони мають можливість адресної відправки MAC-адресами підключених обчислювальних пристроїв.

Згодом таблиця з адресами заповнюється і комутатор розуміє, куди відправляти пакет. На підставі чого можна впевнено сказати, що мережеві комутатори використовують канальний рівень моделі OSI. У мережних комутаторів бувають свої режими роботи:

- з проміжним зберіганням та передачею. Комутатор аналізує та перевіряє пакет, тим самим бере його на короткострокове зберігання, а потім переконавшись у його справжності та відсутності загрози для системи відправляє одержувачу;
- наскрізний режим – менш безпечний, але швидше, у якому комутатор лише пропускає крізь себе пакети, не перевіряючи їх вміст та не перевіряючи контрольну суму;
- безфрагментарний – в даному режимі зчитується MAC – адреса та перевіряються перші 64 байти даних, після чого пакет спокійно відправляється одержувачу, пов'язано це з тим, що більшість помилок міститься саме в цих перших байтах.

Комутатори також можна розділити по смузі пропускної здатності на асиметричні та симетричні, перші мають на одному пристрої порти з різною пропускною здатністю, другі мають однакову пропускну здатність.

Сервер це комп'ютер здатний на різноманітні маніпуляції з даними: зберігання, обробка, переправка і т.д. також є можливість надання послуг, коли на сервері крутиться певне програмне забезпечення. Сервера можна класифікувати по-різному, за обсягом аудиторії, що обслуговується: робочі групи, локальні підприємства, промислові компанії, міста і т.д. Також можна класифікувати за типом завдань: Web-сервери, Сервери баз даних, Сервери друку, Проксі-сервери, Файлові сервери, DHCP-сервери, сервери віддаленого доступу, принт-сервери. У результаті отримуємо комп'ютер, здатний вирішувати безліч різнопланових завдань.

DMZ (демілітаризована зона) – це сегмент мережі, функції якого спрямовані на забезпечення безпеки мережі. DMZ можна встановити на різні сегменти мережі, але в більшості випадків використовується на комутаторі, суть даної технології полягає у

створенні бар'єру між зовнішньою та локальною мережею. Досягається це з використанням міжмережевих екранів, що фільтрують трафік, що надходить до них. Для досягнення більшого ефекту встановлюється два або більше міжмережевих екранів, щоб якщо один вийде з ладу, інший міг забезпечити безпечну працездатність мережі. На різних міжмережевих екранах можуть використовувати різні правила фільтрації, при установці DMZ на сервер можна налаштувати доступ лише з певного вузла до певного компонента сервера [15].

IP-телефонія – це технологія, яка використовує IP мережу для здійснення комунікації абонентів. Якщо в мережі використовується звернення на станції провайдерів і для здійснення дзвінка не потрібен вихід у мережу, то для здійснення дзвінка по IP-телефону необхідний прямий вихід у мережу.

Voip-шлюзи – це фізичні пристрої, що дозволяють телефонним апаратам, офісним станціям та АТС мати вихід в IP-мережу.

Існує кілька видів IP- телефонії [15]:

- на кожному з комп'ютерів є спеціальне програмне забезпечення, яке має вихід у мережу та зв'язок здійснюється через нього, також при такому способі можна мати можливість виклику абонента з ТМЗК у такому разі буде надіслано запит на проксі-сервер, який у свою чергу з використанням інтегрованих шлюзів знайде необхідного нам абонента та відкриє з ним канал зв'язку;
- клієнт має телефонний апарат з використанням ТМЗК відправляє запит до провайдера IP-телефонії, проходить автентифікацію на основі PIN-коду, потім провайдер знаходить проксі сервер абонента з яким ми хочемо відкрити канал зв'язку, і з проксі сервера провайдера відправляється запит на сервер, а далі та використанням інтегрованих шлюзів встановлюється контакт;
- використовується на телефонах з Voip-шлюзом. Абонент, бажаючий з'єднається з іншим абонентом, відправляє виклик, який обробляє провайдер, потім пересилає в ТМЗК, який визначать, до кого проксі серверу відноситься запитуваний абонент, знаходячи його створює канал за допомогою

інтегрованого шлюзу. При зворотному з'єднанні запитуваний абонент обробляє адресу (телефон), що викликає, відправляє це запит у ТМЗК, який знаходить прикріплений до номера проксі сервер і за допомогою інтегрованих шлюзів відкриває канал зв'язку.

У результаті ми маємо безліч плюсів IP- телефонії [15]:

- низьке навантаження на канали передачі, дані передаються в цифровому форматі та при передачі стискаються;
- низька ціна - для здійснення дзвінка нам необхідно лише мати підключення в мережі і нам відкриваються дзвінки у будь-які точки світу;
- функціональність - можливість реалізувати те, що в телефонній мережі або не реалізується, або дуже дорого;
- безпека – всі дані, що передаються по каналах IP-телефонії, шифруються та ідентифікуються потоком у отримувача.

Cisco ASA – фізичний мережевий пристрій, що використовується для досягнення безпеки мережі, що має функції міжмережевого екрану та VPN, що дозволяє створювати правила фільтрації, та захист внутрішніх віртуальних мереж. Використовується на багатьох підприємствах від малого до великого, творцем і дистриб'ютором даного продукту є компанія Cisco. Ходить багато суперечок що краще використовувати Cisco ASA або Cisco маршрутизатор, на маршрутизаторі можна легко налаштувати міжмережевий екран, а також VPN, в свою чергу Cisco ASA підтримує технологію маршрутизації і здатний динамічно розподіляти адреси і вести адресну таблицю.

2.3. Основні положення при проєктуванні захищеної інтрамережі

Високий темп розвитку технологій у сфері інформаційної безпеки є постійною проблемою для організацій. Швидке поширення ботнетів, зростаюча витонченість мережевих атак, тривожне зростання організованої злочинності та шпигунства в Інтернеті, крадіжка особистих даних та даних, більш інноваційні інсайдерські атаки та поява нових форм загроз у мобільних системах є прикладами різноманітних та складних реальних загроз, які формують сучасні проблеми.

Як ключовий фактор, що дає уявлення для клієнтів про надійність продукту, мережі повинні розроблятися та впроваджуватися з урахуванням міркувань безпеки для забезпечення конфіденційності, цілісності та доступності даних та системних ресурсів, що підтримують ключові бізнес-функції.

Досягнення відповідного рівня безпеки більше не є питанням розгортання точкових продуктів, обмежених мережевими периметрами. Сьогодні складність та витонченість загроз потребують загальносистемного підходу та взаємодії з усіма учасниками ланцюжка. З цією метою підприємства, що працюють з даними, що мають високий рівень ризику, використовують підхід глибокого захисту, де кілька рівнів захисту стратегічно розташовані по всій мережі, але в рамках єдиної стратегії. Інформація про події та стан справ спільно використовується для більшої наочності, а дії у відповідь координуються в рамках загальної стратегії контролю [15-18].

Багато компаній використовують модульні конструкції, які прискорюють розгортання і полегшують впровадження нових рішень та технологій у міру розвитку потреб бізнесу. Така модульність продовжує термін корисного використання наявного обладнання, захищаючи грошові вкладення. У той же час ці проєкти включають набір інструментів для полегшення повсякденних операцій, що скорочує загальні оперативні витрати.

Cisco Security Control Framework (SCF). У даний час є найбільш популярними практики Cisco, вони включають [18-19]:

- сучасні рішення завдань безпеки мережі;
- серйозні практики з побудови мережі;
- надійні системи захисту;
- надання якісного обладнання;
- систему підтримки і ведення наданого обладнання;
- цілісну структуру системи;
- документовану базу наданого продукту та високий функціонал товару.

Cisco SCF – це система безпеки, спрямована на забезпечення доступності мережі та послуг, а також безперервності бізнесу. Загрози безпеки - це рухома ціль, і

SCF призначений для вирішення поточних векторів загроз, а також відстеження нових загроз, що розвиваються з використанням кращих загальних практик і комплексних рішень. Cisco SAFE використовує SCF для створення мережевих конструкцій, які забезпечують доступність мережі та сервісу, а також безперервність бізнесу. Cisco SCF керує вибором продуктів і можливостей безпеки та спрямовує їх розгортання по всій мережі, де вони найкраще покращують видимість та контроль [20].

SCF передбачає наявність політики безпеки, розробленої в результаті оцінки загроз і ризиків, а також відповідно до бізнес-цілей та завдань. Передбачається, що політики та керівні принципи безпеки визначають прийнятне та безпечне використання кожної служби, пристрою та системи у навколишньому середовищі. Політика безпеки повинна також визначати процеси та процедури, необхідні для досягнення бізнес-цілей та завдань. Сукупність процесів та процедур визначає операції безпеки. Для успіху бізнесу дуже важливо, щоб політика безпеки, керівні принципи та операції не перешкоджали, а скоріше розширювали можливості організації для досягнення її цілей та завдань.

Успіх політики безпеки зрештою залежить від того, наскільки вона підвищує видимість та контроль. Простіше кажучи, безпеку можна визначити як функцію видимості та контролю. Без жодної видимості немає контролю, а без будь-якого контролю немає і безпеки. Тому основну увагу SCF приділяє підвищенню видимості та контролю. У контексті SAFE SCF керує вибором та розгортанням платформ та можливостей для досягнення бажаного ступеня видимості та контролю.

SCF визначає шість дій безпеки, які допомагають забезпечити дотримання політик безпеки та покращити видимість та контроль. Видимість підвищується за рахунок дій по ідентифікації, моніторингу і кореляції. Контроль покращується за рахунок дій по зміцненню, ізоляції та примусовому застосуванню.

На підприємстві існують різні місця у мережі, такі як центр обробки даних, кампус та філія. Безпечні ділянки отримані із застосування SCF до кожної точки мережі. Результатом є виявлення технологій та найкращих загальних практик, які найкраще задовольняють кожній з шести ключових дій щодо забезпечення видимості та контролю. Таким чином, безпечні реалізації включають різні технології і можливості по

всій мережі, щоб отримати видимість мережевої активності, забезпечити дотримання мережної політики і усунути аномальний трафік. В результаті елементи мережної інфраструктури, такі як маршрутизатори та комутатори, використовуються як всепроникні, принципові точки моніторингу політики та забезпечення її дотримання.

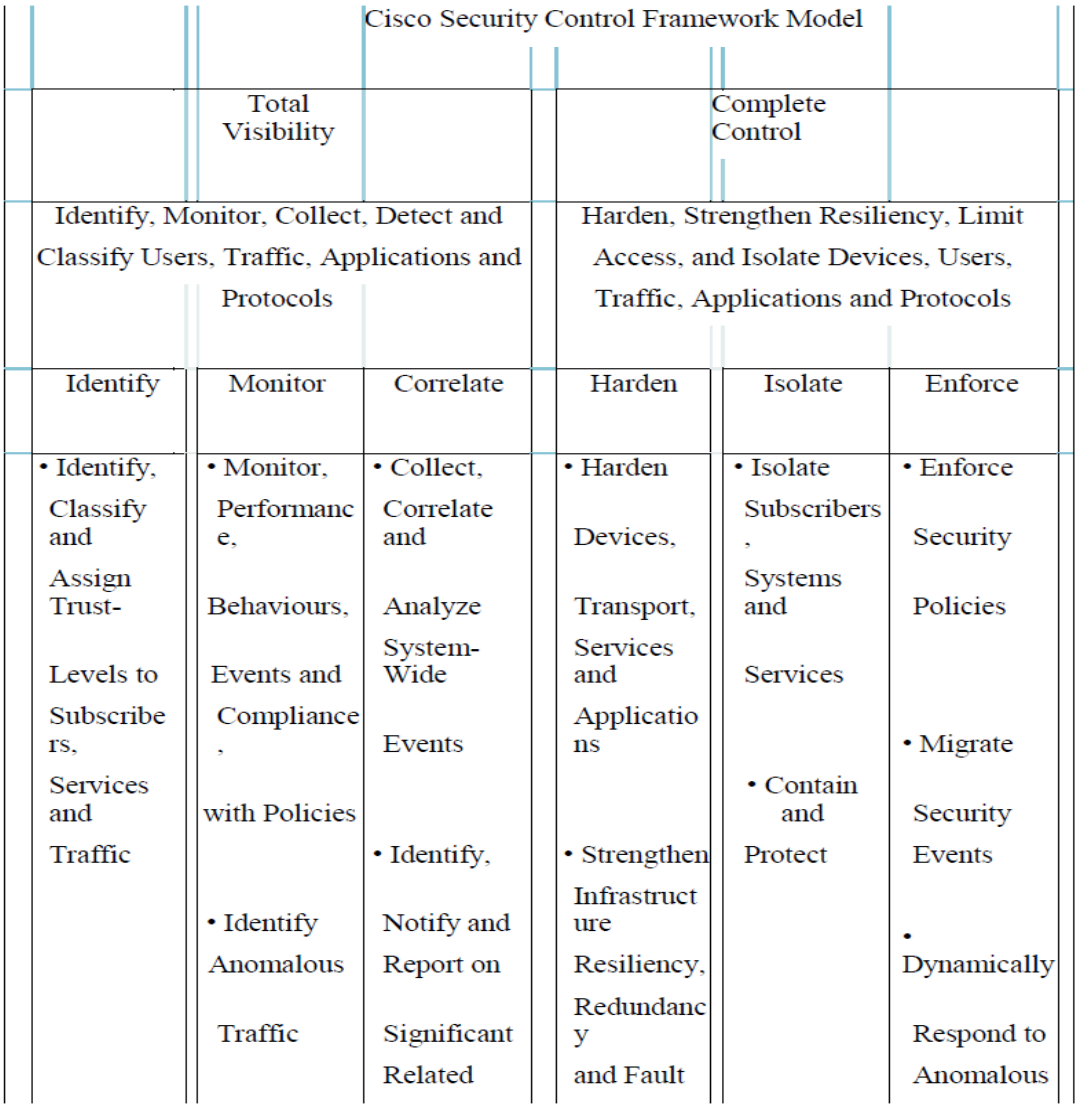

Рис. 2.1. Модель контролю

2.4. Життєвий цикл проєктованої архітектури інтрамережі підприємства

Оскільки потреби бізнесу та безпеки постійно змінюються, сучасні практики проєктування захищених мереж виступають за постійний огляд та коригування впровадження відповідно до змінних вимог. І тому можна використовувати цикл архітектури [20].

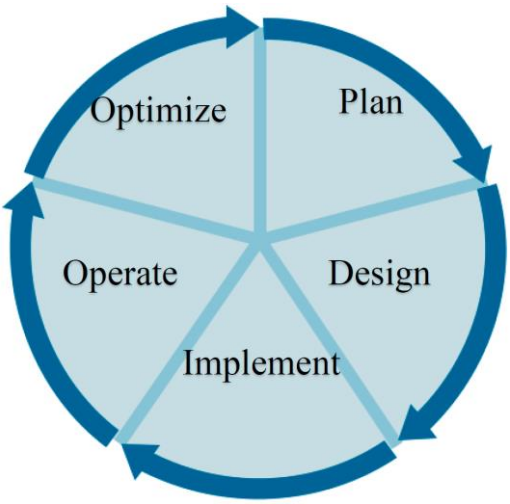

Рис. 2.2. Цикл архітектури

Цикл починається з планування, яке має включати оцінку загроз та ризиків, спрямовану на виявлення активів та поточного стану безпеки. Планування має також включати аналіз прогалин для виявлення сильних та слабких сторін існуючої архітектури.

Після початкового планування цикл продовжується розробкою та відбором середовищ, можливостей і передових практик, необхідних для усунення розриву та задоволення майбутніх потреб. Це призводить до детального проєктування з урахуванням технічних та бізнесових вимог. Реалізація слідує за проєктом. Це включає розгортання і підготовку середовищ і можливостей. Розгортання зазвичай виконується окремі фази, що вимагає послідовності виконання плану. Як тільки нова реалізація буде впроваджена, її необхідно буде підтримувати та експлуатувати. Це включає управління і моніторинг інфраструктури, а також розвідку безпеки для пом'якшення загроз. Нарешті, оскільки вимоги до бізнесу та безпеки постійно змінюються, необхідно проводити регулярні оцінки для виявлення та усунення можливих прогалин. З цією метою може бути використана інформація, отримана під час повсякденних операцій та оцінок [21].

Цей процес є ітераційним, і кожна ітерація призводить до реалізації, що більш підходить для задоволення мінливих потреб бізнесу та політики безпеки.

Принципи архітектури побудови захищених мереж. Процес побудови захищеної мережі є досить серйозним процесом, що вимагає всеосяжного підходу у своїй

реалізації, а також використання кращих практик для досягнення мети. На даний момент одними з найкращих практик має Cisco. Далі розглянемо принципи на які повинні спиратися люди при побудові захищеної мережі [22].

Захист-в-глибину. У сучасних практиках безпека вбудована на всю мережу, наслідуючи глибокий підхід захисту та забезпечуючи конфіденційність, цілісність. та доступність даних, додатків, кінцевих точок та самої мережі. Для покращення видимості та контролю багатий набір технологій та можливостей забезпечення безпеки розгортається на кількох рівнях, але в рамках загальної стратегії [22].

Модульність і гнучкість. Креслення наслідують модульне проєктування, де всі компоненти описуються функціональними ролями, а не точковими платформами. Загальна мережна інфраструктура поділена на функціональні модулі, кожен з яких є особливим PIN-кодом, таким як кампус і центр обробки даних. Функціональні модулі потім поділяються на керовані і деталізовані функціональні шари, і блоки (наприклад, рівень доступу, блок прикордонного розподілу), кожен з яких виконує певну роль у мережі [22].

Модульні конструкції забезпечують додаткову гнучкість при розгортанні, дозволяючи поетапно впроваджувати модулі відповідно до бізнес-потреб організації. Факт, що компоненти описуються функціональними ролями, а не точковими платформами, полегшує вибір найкращих платформ для даних ролей і їх можливу заміну по мірі розвитку технологій та потреб бізнесу. Нарешті, модульність конструкції також прискорює впровадження нових послуг та ролей, продовжуючи термін корисного використання існуючого обладнання та захищаючи попередні капіталовкладення.

Доступність і відмовостійкість послуг. Схеми проєктування включають кілька рівнів надмірності для усунення окремих точок збою і максимізації доступності мережної інфраструктури. Це включає використання надлишкових інтерфейсів, резервних модулів, резервних пристроїв і топологічно надлишкових шляхів. Крім того, в конструкції також використовується широкий набір функцій, призначених для підвищення стійкості мережі до атак та збоїв у роботі мережі [22].

Нормативні вимоги. При проєктуванні мережі вкладається таке поняття, як базовий рівень безпеки, вбудований як невід'ємна частина мережевої інфраструктури.

Базовий рівень безпеки включає багатий набір методів і функцій забезпечення безпеки, зазвичай необхідних нормативними актами і стандартами, що полегшує досягнення відповідності нормативним вимогам [22].

Перевірка реалізації. Сучасні практики включають набір інструментів для аналізу та перевірки функціонування та забезпечення дотримання гарантій по всій мережі, забезпечуючи поточне уявлення про стан безпеки мережі та допомагаючи оцінити відповідність політикам безпеки, стандартам та правилам [22].

Глобальний обмін інформацією і співробітництво. Багато компаній, що зарекомендували себе, активно використовують можливості обміну інформацією та спільної роботи, доступні на продуктах і платформах різних організацій. Інформація про реєстрацію та події, що генерується пристроями в мережі, централізовано збирається, відстежується та корелюється для забезпечення максимальної видимості. Зміни у відповідь і заходи щодо пом'якшення наслідків координуються централізовано для посилення контролю [22].

2.5. Аксіоми безпеки

Мережеві середовища створюються з безлічі пристроїв, служб та інформації, конфіденційність, цілісність та доступність яких можуть бути порушені. Правильний захист мережі та її сервісів потребує розуміння цих мережевих активів та їх потенційних загроз. Кожен сегмент мережі можна вважати як ціль компрометації даних користувача, тому розглянемо мережеві компоненти як цілі. Далі ми дізнаємося про різні сегменти мережі, ознайомимося з їх призначенням, дізнаємося з ролі та застосування у функціонуванні безпечної мережі, а також розберемо їх слабкі сторони [23].

Цілі компонентів мережевої інфраструктури. Мережева інфраструктура складається не тільки з маршрутизаторів і комутаторів, але і з великої кількості вбудованих пристроїв, включаючи, але не обмежуючись ними, брандмауери, системи запобігання вторгненням, балансувальники навантаження та пристрої прискорення додатків. Всі ці інфраструктурні пристрої можуть зазнавати атак, спрямованих безпосередньо на них або опосередковано впливають на доступність мережі. Можливі атаки

включають несанкціонований доступ, підвищення привілеїв, розподілена відмова в обслуговуванні (DDoS), переповнення буфера, атаки потоку трафіку та багато іншого.

Як правило, пристрої мережної інфраструктури надають кілька механізмів доступу, включаючи консольний та віддалений доступ на основі таких протоколів, як Telnet, rlogin, HTTP, HTTPS та SSH. Зміцнення цих пристроїв має вирішальне значення для запобігання несанкціонованому доступу та компрометації. Передова практика включає використання захищених протоколів, відключення невикористовуваних служб, обмеження доступу до необхідних портів та протоколів, а також примусову автентифікацію, авторизацію та облік [24].

Однак інфраструктурні пристрої не всі однакові. Дуже важливо зрозуміти їх унікальні характеристики та природу, щоб правильно закріпити їх. Основна мета маршрутизаторів і комутаторів-забезпечити можливість підключення, тому стандартні конфігурації зазвичай дозволяють прохід трафіку без обмежень.

Крім того, на пристроях можуть бути включені деякі стандартні служби, які можуть не знадобитися для даного середовища. Це дає можливість для експлуатації, і слід зробити належні кроки, щоб вимкнути непотрібну послугу.

Зокрема, в обов'язки маршрутизаторів входить вивчення та розповсюдження інформації про маршрут і, зрештою, пересилання пакетів найбільш відповідними шляхами. Успішні атаки на маршрутизатори-це ті, які здатні вплинути або порушити одну, або кілька цих основних функцій шляхом компрометації самого маршрутизатора, його сеансів роботи або інформації про маршрутизації. Через їхню природу маршрутизатори третього рівня можуть бути націлені на віддалені мережі. Рекомендації щодо безпеки маршрутизаторів включають зміцнення пристроїв, фільтрацію пакетів, обмеження членства в протоколі маршрутизації та контроль поширення та вивчення інформації про маршрутизацію.

На відміну від маршрутизаторів, завдання комутаторів полягає у забезпеченні підключення до локальної мережі, тому вони вразливіші для атак другого рівня, які найчастіше відбуваються всередині організації. Поширені атаки на комутовані середовища включають широкомовні шторми, повені MAC і атаки, призначені для використання обмежень на підтримуючі протоколи, такі як протокол дозволу адрес ARP,

протокол динамічної конфігурації хоста DHCP і протокол сполучного дерева STP. Рекомендації щодо безпеки комутаторів включають зміцнення пристроїв, обмеження широкомовних доменів, безпеку SPT, перевірку ARP, захист від спуфінгу, відключення портів, що не використовуються, і дотримання рекомендацій VLAN.

Брандмауери, балансувальники навантаження та вбудовані пристрої в цілому також схильні до несанкціонованого доступу та компрометації, отже, їх зміцнення має вирішальне значення. Як і будь-які інші пристрої інфраструктури, вбудовані пристрої мають обмежені ресурси та можливості, і в результаті вони також потенційно вразливі до атак на виснаження ресурсів. Такі атаки призначені для виснаження обчислювальної потужності або пам'яті пристрою. Це може бути досягнуто шляхом перевищення пропускної здатності пристрою з точки зору кількості підключень за секунду, максимальної кількості підключень або кількості пакетів за секунду. Атаки також можуть бути спрямовані на аналіз протоколів та пакетів з використанням спотворених пакетів або маніпуляцій із протоколами. Рекомендації щодо безпеки варіюються залежно від характеру вбудованого пристрою.

Мережеві сервіси. Мережеві комунікації залежать від низки служб, включаючи, але не обмежуючись ними, систему доменних імен (DNS), протокол мережного часу (NTP) та DHCP. Порушення роботи таких служб може призвести до часткової або повної втрати зв'язку, а їх маніпуляції можуть бути платформою для крадіжки даних, відмови в обслуговуванні (DoS), зловживання послугами та іншої шкідливої діяльності. В результаті все більша кількість та різноманітність атак постійно націлюються на інфраструктурні сервіси [24].

DNS забезпечує взаємодію між зручними для користувача доменними іменами та логічними IP-адресами. Оскільки доступ до більшості служб в інтернеті та інтрамережах здійснюється за їх доменними іменами, а не за IP-адресами, порушення роботи DNS, швидше за все, призведе до втрати підключення. DNS-атаки можуть бути орієнтовані як на сервери імен, так і на клієнти, також відомі як розпізнавачі. Деякі поширені атаки включають атаки посилення DNS, отруєння кешу DNS та захоплення доменних імен. Атаки посилення DNS зазвичай складаються з повені

серверів імен не запитаними відповідями, часто у відповідь рекурсивні запити. Отруєння кешу DNS полягає в зловмисній зміні або введенні записів DNS в кеш сервера, які часто використовуються для фішингу та атак типу "людина в середині". Викрадення доменного імені належить до незаконного акту, коли хтось краде контроль за доменним ім'ям у його законного власника.

Рекомендації щодо зниження рівня ризику включають виправлення та аналіз DNS-серверів, брандмауери, використовуючи для керування DNS-запитів і трафіку в зоні реалізації ІПС, щоб виявляти та блокувати по DNS-атаках і т.д.

NTP, який використовується для синхронізації часу між комп'ютерними системами по IP-мережі, використовується для цілого ряду програм, заснованих на часі, таких як автентифікація користувачів, ведення журналу подій, планування процесів і т. д. Служба NTP може зазнавати різних атак, починаючи від недоброякісних серверів NTP, вставлення неприпустимої інформації NTP, до DoS на серверах NTP. Найкращі методи безпеки NTP включають використання однорангової аутентифікації NTP, використання списків контролю доступу, а також зміцнення пристроїв і т.п. буд.

DHCP - це найбільш широко розгорнутий протокол для динамічного налаштування систем по IP-мережі. Дві з найпоширеніших атак DHCP - це встановлення шахрайських DHCP-серверів та заміна адрес DHCP. Шахрайські DHCP-сервери використовуються для надання дійсним користувачам невірних відомостей про конфігурацію, щоб запобігти їх доступу до мережі. Крім того, шахрайські DHCP-сервери використовуються для атак man-in-the-middle (MITM), де дійсним клієнтам надається IP-адреса скомпрометованої системи як шлюз за умовчанням [24-16]. Підміна адрес DHCP - це ще один поширений тип атаки. Він складається з вичерпання пулу IP-адрес, доступних DHCP-серверу протягом певного періоду часу, і досягається шляхом трансляції підроблених DHCP-запитів однією або декількома скомпрометованими системами в локальній мережі. Рекомендації щодо захисту від DHCP-сервера включає загартовування та використання функцій безпеки DHCP для комутаторів, таких як DHCP snooping та безпеки портів і т.д.

Кінцеві точки - це цілі. Кінцева точка мережі - це будь-яка система, яка підключається до мережі та взаємодіє з іншими об'єктами через інфраструктуру. Сервери,

настільні комп'ютери, ноутбуки, мережеві системи зберігання даних, IP-телефони, мобільні пристрої з підтримкою мережі та IP-відеосистеми – це приклади кінцевих точок. Через величезну різноманітність апаратних платформ, операційних систем і додатків кінцеві точки представляють одну з найскладніших проблем з погляду безпеки. Оновлення та виправлення різних компонентів кінцевих точок зазвичай доступні з різних джерел та в різний час, що ускладнює підтримка систем в актуальному стані. У доповнення до різноманітності платформ та програмного забезпечення портативні системи, такі як ноутбуки та мобільні пристрої, часто використовуються в гарячих точках Wi-Fi, готелях, будинках співробітників та інших середовищах поза корпоративним контролем. Частково через проблеми безпеки, згадані вище, кінцеві точки є найбільш вразливими і успішно скомпрометованими пристроями [27].

Список загроз кінцевих точок настільки ж широкий і різноманітний, як і величезна різноманітність доступних платформ та програмного забезпечення. Прикладами поширених загроз для кінцевих точок є шкідливі програми, черв'яки, ботнети та спам електронною поштою. Шкідливе програмне забезпечення - це ПЗ, призначене для надання несанкціонованого доступу та/або крадіжки даних у жертви. Шкідливі програми, як правило, купуються за допомогою електронних листів, що містять троянську програму, або при перегляді скомпрометованого веб-сайту. Реєстратори ключів та шпигунські програми є прикладами шкідливих програм, призначених для запису поведінки користувачів та крадіжки особистої інформації, такий як номери кредитних карток та соціального страхування. Черв'яки — це ще одна форма шкідливого програмного забезпечення, яка може автоматично поширюватися по мережі. Ботнети – це одна з найшвидших форм шкідливого програмного забезпечення, яка здатна компрометувати дуже велику кількість систем для спаму електронної пошти, DoS на вебсерверах та іншої шкідливої діяльності. Ботнети зазвичай економічно мотивовані і управляються організованою кіберзлочинністю. Спам електронною поштою складається з небажаної електронної пошти, що часто містить шкідливі програми або є частиною фішинг-афери.

Забезпечення безпеки кінцевих точок вимагає приділити пильну увагу кожному з компонентів системи і, що не менш важливо, забезпечення обізнаності кінцевих користувачів. Кращі практики включають підтримку кінцевих точок в актуальному стані з останніми оновленнями, виправленнями; зміцнення операційної системи та додатків; впровадження програмного забезпечення endpoint security; забезпечення безпеки веб-трафіку та трафіку електронної пошти; а також постійне інформування кінцевих користувачів про поточні загрози та заходи безпеки.

Мережева інфраструктура - ціль для атаки. Цілі сегменти Мережі можуть бути об'єктом таких атак, як крадіжка сервісу, зловживання сервісом, DoS, MITM і втрата даних. Крадіжка сервісу відноситься до несанкціонованого доступу та використання мережевих ресурсів; хорошим прикладом є використання відкритих бездротових точок доступу неавторизованими користувачами [27].

Зловживання мережевими послугами обходиться організаціям мільйони доларів на рік і полягає у використанні мережевих ресурсів не за призначенням; наприклад, особисте використання співробітниками корпоративних ресурсів. Мережі також можуть піддаватися DoS-атакам, призначеним для порушення роботи мережевих служб, та атак MITM, які використовуються для крадіжки особистих даних.

Мережеві атаки відносяться до найважчих для боротьби, оскільки вони зазвичай використовують переваги внутрішньої характеристики в тому, як працює мережа. Мережеві атаки можуть працювати лише на рівні 2 чи більше.

Атаки рівня 2 часто використовують переваги довірчої структури певних протоколів рівня 2, таких як STP, ARP та CDP. Деякі інші атаки 2 рівня можуть бути націлені на певні характеристики транспортного носія, такі як бездротовий доступ. Деякі атаки рівня 2 можуть бути пом'якшені за допомогою найкращих практик на комутаторах, маршрутизаторах та бездротових точках доступу.

Атаки на основі рівня 3 використовують IP-транспорт і можуть містити маніпулювання протоколами маршрутизації. Прикладами таких атак є розподілені DoS (DDoS), проломи захисту, диверсія трафіку. DDoS працює, змушуючи десятки або сотні машин одночасно відправляти хибні дані на цільову IP-адресу. Мета такої атаки полягає не тільки у тому, щоб відключити певний хост, але й у тому, щоб зробити всю

мережу несприйнятливою. Інші часті атаки рівня 3 полягають у введення невірних відомостей про маршрут у процес маршрутизації, щоб навмисно перенаправити трафік, обмежений цільовою мережею. Трафік може бути перенаправлений у чорну дірку, роблячи цільову мережу недосяжною, або в систему, налаштовану для роботи як MITM. Найкращі методи захисту від мережевих атак рівня 3 включають захист пристроїв, фільтрацію від спуфінгу, захист протоколу маршрутизації, мережеву телеметрію, брандмауери і системи запобігання вторгнень [27].

Програми - цілі для атак. Програми кодуються людьми і тому схильні до численних помилок. Необхідно подбати про те, щоб комерційні та загальнодоступні програми мали останні виправлення безпеки. Програми громадського надбання, а також спеціально розроблені програми також вимагають перевірки коду, щоб переконатися, що ці програми не становлять жодних ризиків для безпеки, викликаних поганим програмуванням. Це може включати в себе такі сценарії, як спосіб очищення введення користувача, як програма виконує виклики іншим програмам або самій операційній системі, рівень привілеїв, на якому виконується додаток, ступінь довіри, яку додаток має до навколишніх систем, та метод, що використовується додатком для передачі даних по мережі [27].

Погане програмування може призвести до переповнення буфера, ескалації привілеїв, вгадування облікових даних сеансу, ін'єкції SQL, атак міжсайтових сценаріїв і т. д . несанкціоновану команду. Ескалація привілеїв зазвичай відбувається через відсутність засобів контролю за примусовою авторизацією. Використання передбачуваних облікових даних Користувача або ідентифікаційних даних сеансу полегшує захоплення сеансу та атаки на уособлення користувача. Ін'єкція SQL-це поширена атака у веб-середовищах, що використовують backend SQL і де введення користувача не є належним чином очищеним. Простіше кажучи, атака полягає у маніпулюванні введенням даних для запуску виконання створеного оператора SQL. Міжсайтові сценарії - це ще одна поширена форма атаки, яка полягає у впровадженні шкідливого коду на веб-сторінки і тому, що він виконується після перегляду іншими користувачами. Міжсайтові сценарії можливі на веб-сайтах, де користувачі можуть розміщувати контент і які не можуть належним чином перевірити дані, що вводяться користувачем.

Середовища програм можуть бути захищені за допомогою програмного забезпечення endpoint security та зміцнення операційної системи, в якій розміщується програма. Брандмауери, системи запобігання вторгненням та XML-шлюзи також можуть використовуватися для пом'якшення атак на основі додатків.

2.6. Проєктування захищеної мережі

Eve-ng у своїх проєктах використовує найсучасніші та найпросунутіші практики по роботі з мережевим обладнанням, законодавцями моди є Cisco. Проєкти Eve-ng були створені відповідно до принципів архітектури та відповідно до аксіом безпеки. За більш витончених атак точкові рішення безпеки вже не є ефективними. Сьогоднішнє середовище потребує більш високого ступеня поширення, яке може бути досягнуто лише за допомогою інфраструктурної розвідки безпеки та спільної роботи. З цією метою схеми проєктування Eve-ng використовують різні форми мережевої телеметрії, присутні на мережному обладнанні, пристроях безпеки та кінцевих точках, щоб отримати послідовне та точне уявлення про мережну активність. В рамках моніторингу, аналізу та кореляції подій збираються, аналізуються та корелюються дані реєстрації та відомості про події, що генеруються маршрутизаторами, комутаторами, брандмауерами, системами запобігання вторгненням та програмним забезпеченням для захисту кінцевих точок. Архітектура також використовує сумісність між платформами безпеки, такими як системи запобігання вторгнень, брандмауери та програмне забезпечення для захисту кінцевих точок [28].

Мережеве обладнання визначає сім дій безпеки, які допомагають забезпечити дотримання політик безпеки та покращити видимість та контроль. Видимість підвищується за рахунок дій з ідентифікації, моніторингу та кореляції. Надаючи інформацію про безпеку та спільну роботу на рівні всієї інфраструктури, проєктовані безпечні мережі можуть ефективно пропонувати наступне:

- поліпшена архітектура побудови – на рівні всієї інфраструктури забезпечує цільне бачення топологій мережі, шляхів атаки та ступеня ушкодження;

- ідентифікація загроз - збирання та відстеження тенденцій, кореляція та протоколювання інформації про події допомагають визначити наявність загроз безпеці, прихід до компромісів та виявлення витоків даних;
- підтвердження дій - маючи можливість відстежувати атаку, коли вона проходить через мережу, і маючи видимість на кінцевих точках, архітектура може підтвердити успіх чи невдачу атаки;
- зменшення кількості помилкових спрацьовувань - кінцева точка і доступність (цілісність) системи допомагають визначити, чи справді ціль вразлива для цієї атаки;
- зменшення обсягу інформації про події - кореляція подій різко скорочує кількість подій, заощаджуючи дорогоцінний час оператора безпеки та дозволяючи йому зосередитися на найважливішому;
- визначення ступеня серйозності інциденту-покращена видимість кінцевої точки та мережі дозволяє архітектурі динамічно збільшувати або зменшувати ступінь серйозності інциденту залежно від ступеня вразливості мети та контексту атаки;
- скорочення часу відгуку - наявність видимості по всій мережі дозволяє визначити шляхи атаки та визначити найкращі місця для застосування заходів для пом'якшення наслідків.

Eve-ng використовує спільні для всієї інфраструктури можливості розвідки та спільної роботи, для контролю та пом'якшення добре відомих атак та атак нульового дня. Відповідно до проєктів, що використовуються в найкращих практиках, побудова безпечної мережі, системи захисту від вторгнень, брандмауери, контроль доступу до мережі, програмне забезпечення для захисту кінцевих точок, а також системи моніторингу та аналізу працюють разом для ідентифікації та динамічного реагування на атаки. Як частина контролю та стримування загроз, ці проєкти мають можливість ідентифікувати джерело загрози, візуалізувати її шлях атаки, а також пропонувати і навіть динамічно застосовувати у відповідь дії. Можливі дії у відповідь включають ізоляцію скомпрометованих систем, обмеження швидкості, фільтрацію пакетів і багато іншого.

Контроль покращується за рахунок дій "затримати", "ізолювати" та "примусити". Наведемо деякі з цілей проєктів EVE-Ng:

- адаптивна реакція на загрози в реальному часі; вихідні загрози динамічно ідентифікуються і можуть бути заблоковані в режимі реального часу;
- послідовне охоплення застосування політики - заходи щодо пом'якшення наслідків та стримування можуть бути застосовані в різних місцях мережі для поглибленого захисту;
- мінімізація наслідків атаки - дії у відповідь можуть бути динамічно ініційовані відразу ж після виявлення атаки, мінімізуючи шкоду;
- єдина політика та управління безпекою - єдина платформа управління політикою та безпекою спрощує контроль та адміністрування, а також знижує операційні витрати.

Корпоративні інтрамережі створюються за допомогою маршрутизаторів, комутаторів та інших мережних пристроїв, які підтримують роботу програм та служб. Тому правильний захист цих мережевих пристроїв має важливе значення для продовження бізнес-операцій. Мережева інфраструктура не тільки часто використовується як платформа для атак, але і всі частіше стає безпосередньою ціллю шкідливої діяльності. З цієї причини необхідно вжити необхідних заходів для забезпечення безпеки, надійності та доступності мережної інфраструктури. Eve-ng передбачає можливість використання її віртуальної лабораторії та надає рекомендовані конструкції для підвищення безпеки та найкращі практики для захисту областей управління та управління інфраструктурою. Ця архітектура закладає міцний фундамент, на якому згодом можуть бути побудовані досконаліші методи та прийоми.

Найкращі практики та рекомендації щодо проєктування представлені в наступних областях [29]:

- доступ до інфраструктурних пристроїв;
- стійкість та живучість пристрою;
- інфраструктура маршрутизації;
- комутаційна інфраструктура;
- застосування мережевої політики;

- мережева телеметрія;
- мережеве управління.

Проєктна схема відповідає модульній схемі, в якій вся мережева інфраструктура поділена на функціональні модулі, кожен з яких представляє собою свою область дії. Функціональні модулі потім поділяються більш керовані і деталізовані функціональні верстви, і блоки, кожен із яких виконує певну роль мережі.

Захист мережевої інфраструктури. Розглянемо найкращі методи забезпечення безпеки самої мережної інфраструктури. Це включає встановлення базової лінії безпеки для захисту області управління і контролю, а також створення міцної основи, на якій згодом можуть бути побудовані більш досконалі методи і прийоми.

Нижче перераховані ключові області базової безпеки:

- доступ до інфраструктурних пристроїв;
- інфраструктура маршрутизації;
- стійкість і живучість пристрої;
- мережева телеметрія;
- застосування мережевої політики;
- комутаційна інфраструктура.

Наведемо поширені види атак на мережеву інфраструктуру:

- відмова в обслуговуванні (DoS);
- розподілені DoS (DDoS);
- несанкціонований доступ;
- перехоплення сеансу;
- атака "людина-в-середині" (MITM);
- підвищення привілеїв;
- вторгнення;
- боти;
- атаки по протоколу маршрутизації;
- атаки на сполучне дерево.

Доступ до пристроїв інфраструктури. Захист інфраструктури мережі вимагає забезпечення доступу до цих пристроїв інфраструктури. Якщо доступ до інфраструктурного пристрою порушено, то може бути порушена безпека та керування всією мережею. Отже, дуже важливо встановити відповідні заходи контролю для запобігання несанкціонованому доступу до інфраструктурних пристроїв.

Пристрої мережної інфраструктури часто надають цілу низку різних механізмів доступу, включаючи консольні та асинхронні з'єднання, а також віддалений доступ на основі таких протоколів, як Telnet, rlogin, HTTP та SSH [29]. Деякі механізми зазвичай включені за замовчуванням із мінімальною безпекою, пов'язаною з ними. З цієї причини кожен пристрій інфраструктури повинен бути ретельно перевірений та налаштований таким чином, щоб забезпечити включення лише підтримуваних механізмів доступу та їх належний захист.

Основні заходи щодо забезпечення як інтерактивного, так і управлінського доступу до інфраструктурного пристрою полягають у наступному [30]:

- обмеження доступності пристроїв - обмежити доступні порти та обмежити дозволені комунікатори та дозволені методи доступу;
- юридичне обґрунтування - відображення юридичного обґрунтування, розробленого разом із юридичним консультантом компанії для інтерактивних сесій;
- аутентифікація доступу - переконайтеся, що доступ надається лише автентифікованим користувачам, групам та службам;
- авторизація дій - обмеження дій та уявлень, дозволених будь-яким конкретним користувачем, групою або сервісом;
- забезпечення конфіденційності даних - захист локально збережених конфіденційних даних від перегляду та копіювання;
- журнал та обліковий запис для всього доступу - запис того, хто звертався до пристрою, що сталося та коли для аудиту.

Захист локальних паролей. Паролі, як правило, повинні підтримуватися та контролюватись централізованим AAA-сервером. Однак у багатьох пристроях інфраструктури інформацію можна зберігати на локальному рівні. Деякі локальні паролі та

секретна інформація можуть знадобитися, наприклад, для локального резервного копіювання у разі відсутності серверів AAA, спеціальних імен користувачів, секретних ключів та іншої інформації про паролі.

Глобальне шифрування пароля, локальне шифрування пароля користувача та `enable secret` - це функції, доступні в Cisco IOS для захисту конфіденційної інформації, що локально зберігається:

Увімкніть автоматичне шифрування паролів за допомогою глобальної команди `service password-encryption`. Після налаштування всі паролі автоматично шифруються, включаючи паролі локально визначених користувачів.

Визначте локальний пароль увімкнення за допомогою команди `enable secret global`. Увімкнення має бути доступно оброблено за допомогою протоколу AAA, такого як TACACS+. Локально налаштований пароль включення буде використовуватися як резервний механізм після налаштування AAA.

Визначте рядок із паролем за допомогою команди `password line` для кожного рядка, який ви плануєте використовувати для адміністрування системи. Зверніть увагу, що такі паролі використовуються для початкового налаштування та не діють після налаштування AAA. Також зверніть увагу на те, що деякі пристрої можуть мати більше 5 VTYs.

Зверніть увага, що алгоритм шифрування, використовуваний командою `service password-encryption` є шифром Vigenere, який можна легко змінити. Отже, ця команда найперше корисна для утримання несанкціонованих осіб від перегляду паролів у конфігураційному файлі.

Впровадження банерів повідомлень. Рекомендується, щоб у всіх інтерактивних сеансах був представлений банер з юридичним повідомленням, щоб користувачі були повідомлені про політику безпеки і про те, що вони підкоряються їй. У деяких юрисдикціях цивільне чи кримінальне переслідування зловмисника, який вривається в систему, простіше або навіть потрібне, якщо подано законний банер з повідомленням, що інформує несанкціонованих користувачів про те, що їхня діяльність факти-

чно не законна. У деяких юрисдикціях також може бути заборонено контролювати діяльність неавторизованого користувача, якщо він не був про це повідомлений та не дав згоду [30].

Вимоги до юридичного повідомлення є складними та різняться у кожній юрисдикції та ситуації. Навіть у межах юрисдикції юридичні думки різняться, і це питання слід обговорити з вашим власним юрисконсультом, щоб переконатися, що воно відповідає вимогам компанії, місцевим та міжнародним правовим вимогам. Це часто має вирішальне значення для забезпечення належних дій у разі порушення безпеки.

У співпраці з юридичним консультантом компанії заяви, які можуть бути включені до банеру юридичного повідомлення, включають:

- сповіщення про тому, що доступ до системі і її використання дозволені лише спеціально уповноваженим персоналом, та повідомлення про те, хто може надати цей дозвіл;
- повідомлення про те, що несанкціонований доступ та використання системи є незаконними та можуть підлягати цивільному або кримінальному покаранню;
- повідомлення про те, що доступ та використання системи можуть реєструватися або контролюватись без додаткового повідомлення, а отримані журнали можуть використовуватись як докази в суді;
- додаткові конкретні повідомлення, які вимагають місцеві закони.

З точки зору інформаційної безпеки, а не юридичної, банер юридичного повідомлення не повинен містити жодної конкретної інформації про пристрій, такий як його ім'я, модель, програмне забезпечення, місцезнаходження, оператор або власник, оскільки цей вид інформації може бути корисним для зловмисника [28].

Безпечний адміністративний доступ. Дотримуйтесь цих рекомендацій для забезпечення безпечного адміністративного доступу:

- включити доступ по SSH за наявності небезпечного телнет з'єднання. Використовувати із мінімальним розміром модуля 768 біт;
- уникайте доступу до протоколу HTTP. Якщо можна використовувати HTTPS;

- вимкніть непотрібні лінії доступу. Відключені порти, які не будуть використовуватися з командою `no exec`;
- у кожному рядку, що використовується, явно визначте протоколи, дозволені для вхідних і вихідних сеансів. Обмеження вихідних сеансів запобігає використанню системи як проміжного вузла для інших атак. Однак слід зазначити, що вихідне з'єднання Telnet може знадобитися для управління інтегрованими модулями, такими як мережевий модуль Cisco IPS для маршрутизаторів Cisco ISR;
- використовуйте базові ACL для керування джерелами, з яких буде дозволено сеанси. Джерелом зазвичай є підмережа, в якій знаходяться адміністратори. Також варто використовувати ACL із розширеними списками, для налаштування типу протоколу, використовуваного між вузлами;
- зарезервуйте останній VTY. Налаштувати доступ-класу, використовувати лише на безпечному устаткуванні;
- встановити очікування та часу очікування сеансу - встановити очікування та часу очікування сеансу в кожну лінію. Увімкніть TCP `keepalives` для виявлення та закриття завислих сеансів.

Найкращі практики використання маршрутизації. Маршрутизація є однією з найважливіших частин інфраструктури, яка підтримує роботу мережі, і тому дуже важливо вжити необхідних заходів для її захисту. Існують різні способи скомпрометувати маршрутизацію – від запровадження нелегітимних оновлень до DoS, спеціально розроблених для порушення маршрутизації. Атаки можуть бути орієнтовані на пристрої маршрутизації, пірингові сеанси або інформацію про маршрутизацію.

Найкращі практики з проєктування використовують такі заходи для ефективного захисту площини маршрутизації:

- обмежити членство в протоколі маршрутизації - обмежити сеанси маршрутизації довіреними одноранговими вузлами, перевірити походження та цілісність оновлень маршрутизації;

- контроль розповсюдження маршруту - застосування фільтрів маршрутів для забезпечення поширення тільки дійсної інформації про маршрут. Управління обміном інформацією про маршрутизації між одноранговими вузлами маршрутизації та між процесами перерозподілу;
- контроль статусу сеансів - необхідно вести журнал логів, що містить інформацію про поточний сеанс і проведені зміни в його ході.

Обмеження членства в протоколі маршрутизації. Багато протоколів динамічної маршрутизації, зокрема протоколи внутрішніх шлюзів, реалізують механізми автоматичного виявлення однорангових вузлів, що полегшують розгортання та налаштування маршрутизаторів. За умовчанням ці механізми працюють у припущенні, що це однорангові вузли мають бути довіреними, що дозволяє встановлювати сеанси пірингу з фіктивних маршрутизаторів і вводити помилкові дані маршрутизації. На щастя, Cisco IOS надає низку рекомендованих функцій, призначених для обмеження сеансів маршрутизації довіреними одноранговими вузлами, які допомагають перевірити походження та цілісність оновлень маршрутизації:

- увімкніть перевірку справжності сусідів, щоб забезпечити справжність сусідніх маршрутів та цілісність їх оновлень маршрутизації. Доступно для BGP, IS-IS, OSPF, RIPv2 та EIGRP. Використовуйте автентифікацію алгоритму дайджесту повідомлень версії 5 (MD5), а не небезпечну автентифікацію за звичайним текстом. Щоб нормально функціонувати, автентифікація сусідів має бути включена обох кінцях сеансу маршрутизації;
- використовуйте команду пасивного інтерфейсу за промовчанням при включенні маршрутизації в діапазонах мережі, що відповідають великому числу інтерфейсів. Команда "`passive-interface default`" змінює логіку конфігурації на пасивну за умовчанням, запобігаючи поширенню оновлень маршрутизації на інтерфейсі, якщо тільки інтерфейс явно не налаштований за допомогою команди "`no passive-interface`". Це дозволяє вибірково включити поширення оновлень маршрутизації за інтерфейсами, які, як очікується, будуть частиною процесу маршрутизації;

- при використанні BGP увімкніть перевірку безпеки TTL, також відому як узагальнений механізм безпеки TTL (GTSM, RFC 3682). Перевірка безпеки TTL запобігає атакам DoS на основі маршрутизації, несанкціонованого пірингу та скидання сеансів, запущених із систем, не підключених безпосередньо до тієї ж підмережі, що й маршрутизатори-жертви. Для правильної роботи перевірка безпеки TTL має бути налаштована на обох кінцях сеансу BGP.

Фільтрування поширення маршрутів. Фільтрація маршрутів є ще одним важливим інструментом для забезпечення безпеки інфраструктури маршрутизації. Більшість протоколів маршрутизації допускають налаштування фільтрів маршрутів, які запобігають поширення приватних маршрутів по всій мережі. З точки зору безпеки ці фільтри корисні, оскільки вони допомагають гарантувати, що приватні ділянки мережі не відображаються у загальнодоступному просторі мережі.

Фільтрування маршрутів може бути розділена на дві форми:

- фільтрування маршрутної інформації, що передається між вузлами маршрутизації;
- фільтрування маршрутної інформації, що передається між процесами маршрутизації в одному маршрутизаторі внаслідок перерозподілу.

Реалізувати фільтрацію однорангових префіксів по краях дозволяє контролювати вхідні фільтри по краях. Це дозволить гарантувати, що в мережу буде введено лише очікувані маршрути. Баланс між вищим контролем та пов'язаним з ним операційним навантаженням.

Розгортайте фільтри на краях, звідки може бути введена неправильна інформація про маршрутизацію, наприклад на краю глобальної мережі. Управління вхідними оновленнями маршрутизації на кордоні глобальної мережі не лише пом'якшує введення фіктивних маршрутів у філіях, але й запобігає перетворенню філії з подвійним доступом на транзитну мережу.

Якщо потрібно перерозподіл маршрутів, застосуйте фільтри перерозподілу, щоб суворо контролювати, які маршрути оголошуються. Реалізація фільтрів перерозподілу маршрутів допомагає стримувати наслідки потенційної ін'єкції неприпустимих маршрутів, запобігає циклам та допомагає підтримувати стабільність мережі.

Також необхідно застосування фільтрів маршрутів на тупикових маршрутизаторах та віддалених місцях з тупиковими мережами, дані фільтри дозволять запобігти розповсюдженню неприпустимої інформації про маршрут.

Ведення журналу змін стану. Часті зміни стану з'єднання та скидання є загальними симптомами проблем мережного підключення та стабільності мережі, які мають бути досліджені. Ці симптоми можуть також вказувати на атаки, що продовжуються, на інфраструктуру маршрутизації. Реєстрація змін стану сеансів – це хороша практика, яка допомагає виявити такі проблеми та полегшує усунення несправностей. У більшості протоколів маршрутизації ведення журналу повідомлень про зміну стану увімкнено за замовчуванням. Якщо цей параметр увімкнено, то кожного разу, коли сеанс маршрутизатора змінюється або зазнає скидання, маршрутизатор генерує повідомлення журналу. Якщо увімкнено системний журнал, повідомлення надсилається на сервер системного журналу. В іншому випадку воно зберігається у внутрішньому буфері маршрутизатора [30].

Ведення журналу повідомлень про зміну стану в BGP за промовчанням вимкнено; Щоб увімкнути його, використовуйте команду маршрутизатора BGP “`log-neighbor-changes`”. За замовчуванням стан журналу EIGRP та OSPF змінюється. Якщо його вимкнено, його можна ввімкнути за допомогою команди “`EIGRP log-neighbor-changes router`” для EIGRP та команди “`log-adjacency-changes router`” для OSPF.

2.7. Рекомендації по відмовостійкості і живучості пристроїв

Маршрутизатори та комутатори можуть піддаватися атакам, спрямованим на те, щоб опосередковано вплинути на доступність мережі. Можливі атаки включають DoS, засновані на несанкціонованих та санкціонованих протоколах, розподілені DoS,

атаки переповнення, рекогносцировку, несанкціонований доступ та багато іншого. Розглянемо найкращі практики, призначені для збереження стійкості та живучості маршрутизаторів і комутаторів, допомагаючи мережі підтримувати доступність навіть під час виконання атаки:

- вимкнення непотрібних служб;
- використання ACL для захисту інфраструктури;
- управління навантаженнями маршрутизаторів (CoPP);
- безпека портів;
- надмірність.

Вимкнення непотрібних служб. Щоб полегшити розгортання, маршрутизатори та комутатори виходять із коробки зі списком включених служб, які вважаються підходящими для більшості мережевих середовищ. Однак, оскільки не всі мережі мають однакові вимоги, деякі з цих служб можуть бути не потрібні і тому можуть бути вимкнені.

Відключення цих непотрібних служб має дві переваги: це допомагає зберегти системні ресурси та усуває потенціал експлойтів безпеки на відключених службах [28].

Розглянь кілька загальних рекомендацій:

- ідентифікація відкритих портів - використовуйте команду "`show control-plane host open-ports`", щоб побачити, які порти UDP/TCP прослуховує маршрутизатор, та визначити, які служби необхідно відключити;
- глобальні служби відключені за умовчанням - якщо це не потрібно явно, переконайтеся, що finger, identification (identd), а також невеликі сервери TCP та UPD залишаються відключеними на всіх маршрутизаторах та комутаторах;
- глобальні служби включені за замовчуванням - якщо явно не потрібно, BOOTP, IP-подібна маршрутизація та PAD-служби мають бути відключені глобально на всіх маршрутизаторах;

- IP-спрямоване мовлення - переконайтеся, що направлене мовлення залишається відключеним на всіх інтерфейсах;
- вимкнення CDP - вимкніть CDP на інтерфейсах, де служба може становити небезпеку. Наприклад, на зовнішніх інтерфейсах, таких як ті, що знаходяться на межі інтернету, і тільки для даних портів у кампусі та філії доступу;
- зовнішні порти та доступ - якщо не потрібно, відключіть MOP, IP-перенаправлення та проксі - ARP на всіх інтерфейсах доступу та зовнішніх інтерфейсах. Це зазвичай включає лінії доступу в філіях, а також зовнішні порти, такі як ті, що знаходяться на кордоні Інтернет.

Використання ACL для захисту інфраструктури. Списки контролю доступу для захисту інфраструктури (IACL) – це метод контролю доступу, який захищає мережну інфраструктуру від внутрішніх та зовнішніх атак. IACLs (Infrastructure access control list) - це метод, заснований на розширених ACL, спочатку розроблених інтернет-провайдерами (ISP) для захисту своїх мережевих інфраструктур, але згодом вони отримали широке поширення во багатьох підприємствах бажаючих захистити свою інфраструктуру [26-30].

У двох словах, IACL - це розширені ACL, призначені для явного дозволу трафіку управління, пов'язаного з обладнанням інфраструктури, таким як маршрутизатори та комутатори, в той же час забороняючи будь-який інший трафік, який не повинен проходити через задану інфраструктуру. Наприклад, IACL, розгорнутий на піринговому краї провайдера, налаштований для явного дозволу сеансів BGP від відомих однорангових вузлів, водночас забороняючи будь-який інший трафік, призначений до пірінгового маршрутизатора провайдера, а також до іншого адресного простору інфраструктури.

ACL найбільш корисні при розгортанні на краях мережі, де інфраструктура стає доступною для внутрішніх чи зовнішніх користувачів. Також на адміністративних кордонах, де трапляються обладнання чи посилання під іншим управлінням. На підприємстві ACL можуть бути розгорнуті на багатьох краях мережі:

- WAN edge - захист базової інфраструктури від можливих загроз, що виходять із віддалених філій та місць розташування партнерів;
- доступ до кампуса/філії - захист інфраструктури від можливих атак, що виходять із локальних мереж;
- прикордонні фільтри інтернету можуть бути сконструйовані таким чином, щоб функціонувати як IACL для захисту інфраструктури від зовнішніх небезпек.

Хоча існує загальна структура для побудови IACL, фактичні записи ACL сильно відрізнятимуться залежно від навколишнього середовища. IACL, побудований без належного розуміння протоколів і задіяних пристроїв, може зрештою виявитися неефективним і навіть привести до повної відкритості для проведення хакерських атак на мережу. За цією причиною кращий підхід до побудови IACL - почати з ACL виявлення, щоб ідентифікувати трафік і не контролювати доступ. IACL повинен застосовуватися тільки тоді, коли протоколи та порти, які використовуються інфраструктурою надійні та зрозумілі.

РОЗДІЛ 3
ПРОЄКТ ЗАХИЩЕНОЇ ІНТРАМЕРЕЖІ ПІДПРИЄМСТВА В ВІРТУАЛЬНОМУ СЕРЕДОВИЩІ EVE-NG

3.1. Розгортання і встановлення

У цьому розділі кваліфікаційної роботи необхідно спроєктувати захищену інтрамережу. Мережа проєктуватиметься у віртуальній лабораторії Eveng і матиме всі необхідні параметри та функції для впровадження в офісах середнього та малого бізнесу. До складу компанії входитиме центральний офіс, що бере на себе основну частину навантаження і дві філії, що знаходяться у різних містах. Центральний офіс розташований на першому поверсі, складається з 10 приміщень та надає 30 робочих місць. Філія виконуватиме завдання з надання послуг, що надаються компанією в області. Має менш розширений спектр послуг, на відміну від центрального та надає 10 робочих місць.

Наша робота буде виконуватися на платформі Windows 11 Professional. Перейдемо до встановлення та налагодження нашої віртуальної лабораторії. Для початку нам необхідно завантажити платформу WMware Workstation, в якій ми будемо розгортати віртуальний сервер eve-ng. Завантажуємо образ безкоштовної версії eve-ng. Також нам буде необхідно встановити низку додаткового ПЗ:

- Putty;
- Plink;
- Ultravnc_wrapper.bat;
- Wireshark_wrapper.bat;
- Wireshark;
- UltraVnc (Viewer, Server);
- Qemu;
- FileZilla.

Після встановлення всіх додаткових компонентів необхідно розгорнути саму віртуальну машину. Після установки необхідно правильно налаштувати віртуальну машину, після правильно виконаних всіх дій ми побачимо вітальне вікно eve-ng.

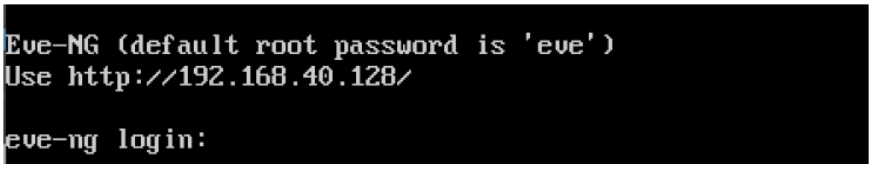

Рис. 3.1. Вікно автентифікації в eve-ng

Адреса 192.168.40.128 буде використана для входу до віртуальної лабораторії eve-ng. Зайдемо до віртуальної лабораторії.

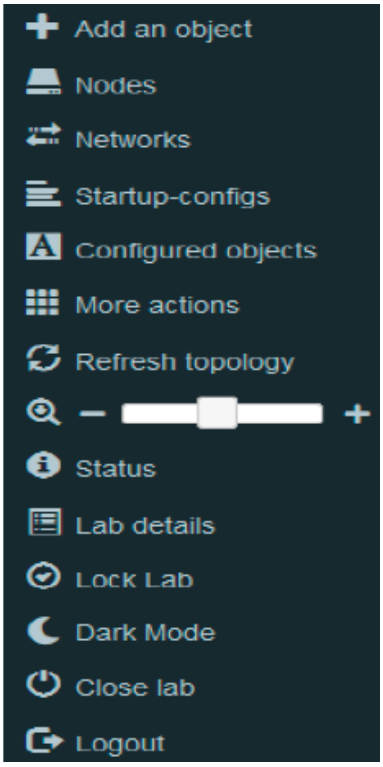

Рис. 3.2. Вкладка eve-ng

Оскільки ми віртуалізуватимемо компоненти мережі, з урахуванням їх усіх реальних особливостей. Нам доведеться встановити сертифікати на всі компоненти мережі, які ми будемо використовувати. Деякі сертифікати можна знайти у відкритому доступі, але більшість потрібно купувати за гроші. Компоненти мережі, що використовуються нами, будуть мати всі параметри реального обладнання.

Після встановлення всіх можливих сертифікатів та налагодження їх роботи можна перейти до проєктування мережі. Оскільки у відкритому доступі є мало сертифікатів, обходимося тим, що маємо, а точніше: Cisco IOL, Cisco Vios, Cisco Asa, Zentyal.

Проєктована система складатиметься з мережевого простору головного офісу та філії. Дані мережні простори матимуть можливість повноцінно взаємодіяти між собою, а також з ресурсами ззовні. Основні методи, що використовуються для захисту мережевого простору: різні види паролів, ASA, Vlan, Acl, GRE, IPSec.

3.2. Налаштування маршрутизації між офісами

Проєктування системи розпочнемо із створення роутера для філії компанії. Створюємо та називаємо його BranchRT. Команда "`hostname BranchRT`" дозволяє нам це здійснити [29].

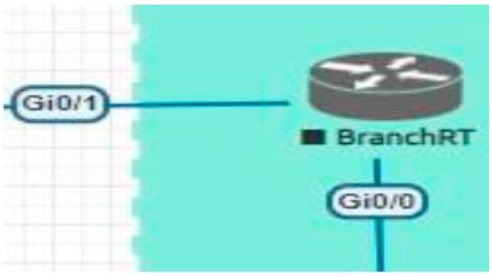

Рис. 3.2. Роутер філії

Далі перейдемо до налаштування роутера BranchRT. Зв'язок усередині філії відбуватиметься через інтерфейс Gi0/0, в адресному просторі 10.10.10.200 з маскою 255.255.255.0. Команда "`int Gi0/0`" дозволяє нам зайти на необхідний інтерфейс, а за допомогою "ip address адресного простору" встановити необхідну адресу, також команда "`no sh`" дозволяє включити вибраний інтерфейс.

Після налаштування мережі всередині філії необхідно налаштувати зв'язок з головним офісом. Зв'язок між головним офісом та філією буде здійснюватись через ISP (Інтернет-провайдер). Заходимо на інтерфейс Gi0/1 та встановлюємо адресу роутеру 172.168.112.2 з маскою 255.255.255.252 для виходу в мережу.

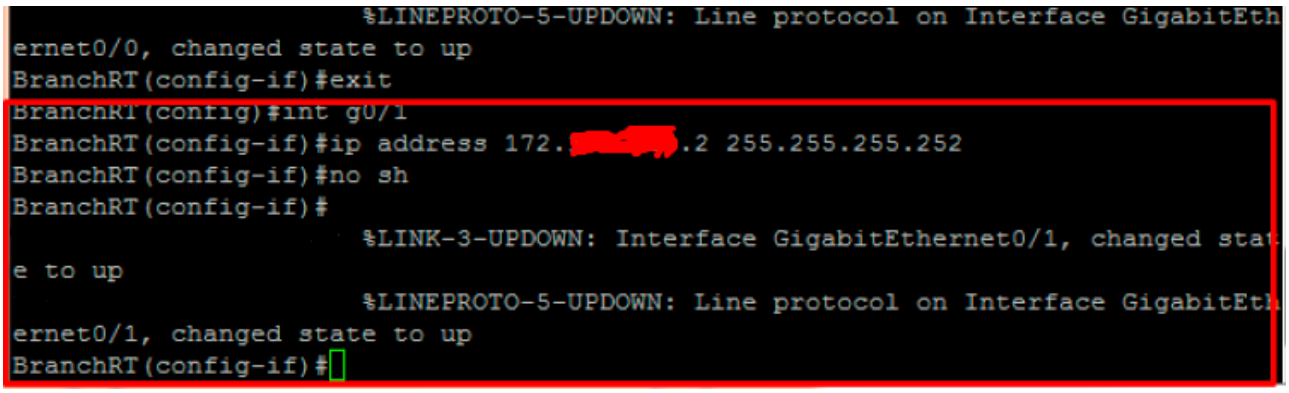

Рис. 3.3. Налаштування роутера BranchRT

Встановимо адресу ISP для взаємодії з філією. Використовуючи інтерфейс Gi0/1 та адресу 172.***.***.1 з маскою 255.255.255.252.

Для взаємодії між ISP та прикордонним роутером головного офісу BorderRT використовуватиметься адресний простір 40.0.1.0 з маскою 255.255.255.0. Заходимо на інтерфейс Gi0/0 і встановлюємо адресу.

40.0.1.1 з маскою 255.255.255.0, і піднімаємо його.

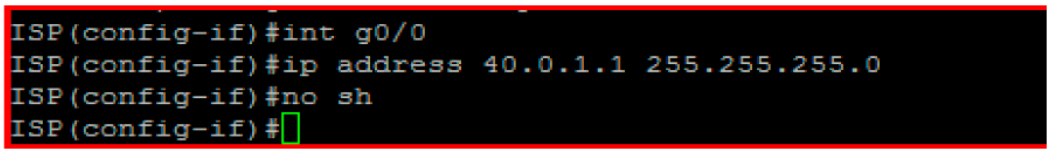

Рис. 3.4. Налаштування ISP

Далі перейдемо до налаштування прикордонного роутера головного офісу BorderRT.

BorderRT буде взаємодіяти з ISP в адресному просторі 40.0.1.0./24, а з внутрішньою мережею компанії через 30.0.1.0/24. Для налаштування вихід у мережу зайдемо на інтерфейс Gi0/0 та встановимо адресу 40.0.1.2 з маскою 255.255.255.0.

Для встановлення доступу у внутрішню мережу зайдемо на інтерфейс Gi0/1 та встановимо адресу 30.0.1.1 з маскою 255.255.255.0.

Налаштуємо можливість проходу всього трафіку через BorderRT в ISP, використовуючи адресу 40.0.1.1 встановлену на ISP в інтерфейсі Gi0/0. Команда "`IP route 0.0.0.0 0.0.0.0 40.0.1.1`" дозволяє трафіку з будь-якого джерела внутрішньої мережі безперешкодно проходити на ISP.

Тепер налаштуємо маршрутизацію для ISP. Спочатку налаштуємо для взаємодії з філією, у філії використовується адресний простір 10.10.10.200, а для виходу на ISP 172.168.112.2. Використовуючи команду “`ip route 10.10.10.0 255.255.255.0 172.168.112.2`” встановимо маршрутизацію між ISP та BranchRT. За аналогією використовуючи команду “`30.0.1.0 255.255.255.0 40.0.1.2`”, де 40.0.1.2 адресу BorderRT, а 30.0.1.0 адресний простір що виходить на ASA, це дозволить встановити маршрутизацію трафіку, що виходить з внутрішньої .

Після налаштування маршрутизації прикордонного роутера BorderRT та ISP перейдемо до налаштування маршрутизації пакетів, проходять через філію. Команда “`ip route0.0.0.0 0.0.0.0 172.168.112.1`” ми встановлюємо прохід пакетів та ISP з інтерфейсу Gi0/1. Командою "`ip route 40.0.1.0 255.255.255.0 172.168.112`" встановлюємо маршрутизацію пакетів від BranchRT через ISP на BorderRT. Командою "`ip route 30.0.1.0 255.255.255.0 40.0.1.2`" встановлюємо прохід пакетів через роутер BorderRT у внутрішню мережу головного відділення компанії.

3.3. Встановлення VLAN в головному офісі

Після побудови взаємодії філії з мережею головного офісу перейдемо до облаштування мережного простору внутрішньої мережі офісу. Розберемо структуру мережі внутрішнього офісу. Внутрішня мережа головного офісу складатиметься з: світчів (BorderSw, Per_Sw, DMZ_Sw), Cisco ASA (ASA v Primary, ASA v Secondary) та DMZ.

У головному офісі для безпеки буде встановлено дві Cisco Asa, якщо одна з них вийде з ладу, друга відразу отримає сигнал від першої і приступить до роботи [21]. Розглянемо основні можливості Cisco ASA:

- статична і динамічна маршрутизація;
- усі види NAT;
- динамічне міжмережне екранування;

- Modular Policy Framework (конструкція для сортування пакетів за класами та застосування до них різних дій);
- аналіз складних протоколів (FTP, SIP, TFTP, IPSec);
- IPSec Site-to-site, Easy VPN Server;
- SSLVPN;
- віртуальні міжмережеві екрани;
- Failover (Active/Standby і Active/Active);
- прозоре екранування (Transparent Firewall).

DMZ - використовується в компанії для підвищення безпеки локальної мережі, він створює розмежування між зовнішніми сервісами, які може використовувати будь-яка людина в мережі від внутрішніх доступу до яких може мати співробітник компанії.

Перейдемо до самої настройки Cisco ASA, будемо налаштовувати ASA v Primary. Налаштовувати в Cisco ASA ми буде VLAN. VLAN (Virtual Local Area Network) – технологія що дозволяє створювати одному фізичному інтерфейсі кілька віртуальних локальних мереж. Використовується технологія VLAN для розмежування або об'єднання груп пристроїв, до яких можна буде застосувати політики безпеки.

Переходимо до самого настроювання, заходимо на потрібний нам інтерфейс "`int Gi0/0`" , створюємо на ньому vlan 80, який дивитиметься на прикордонний роутер BorderRT. Встановлюємо сек'юріті левелів (рівень довіри) 0, що означає відсутність довіри тому, що проходить трафіку та даємо адресу 30.0.1.10 з маскою 255.255.255.0 для нашого VLAN. Цей вілан буде служити для виходу на BorderSW.

```
ciscoasa(config)#
ciscoasa(config)# int g0/0
ciscoasa(config-if)# no sh
ciscoasa(config-if)# int g0/0.80
ciscoasa(config-subif)# vlan 80
ciscoasa(config-subif)# nameif out
INFO: Security level for "out" set to 0 by default.
ciscoasa(config-subif)# ip address 30.0.1.10 255.255.255.0
ciscoasa(config-subif)# no sh
ciscoasa(config-subif)#
```

Рис. 3.5. Налаштування ASAvPrimary

Піднімемо ще один VLAN на ASA v Primary, що дивиться на DMZ. Заходимо на інтерфейс Gi0/1, прив'язуємо до нього 40 vlan. Даємо йому ім'я DMZ та адресу 192.168.40.1 з маскою 255.255.255.0. За стандартом всім створюваним VLAN присвоюється 0 security-level (відсутність довіри), змінюємо security-level на 60, що означає середній рівень довіри до трафіку, що проходить через цей vlan.

Далі піднімемо ще один VLAN для взаємодії з підключеними пристроями внутрішньої мережі Per_Sw. Заходимо на інтерфейс Gi0/2 та створюємо 50 vlan. Привласнюємо йому 100 security-level (повна довіра до трафіку, що проходить) і даємо адресу 192.168.50.1 з маскою 255.255.255.0.

Перейдемо до налаштування транк портів на світчі DMZ_Sw. Trunk port - це комутаційний порт, за допомогою якого може передаватися тегований трафік від одного або кількох VLAN.

Заходимо на інтерфейс Gi0/0, створюємо статичний trunk командою "`switchport mode trunk`", після створення автоматично будуть дозволені всі VLAN. Командою "`switchport trunk allowed vlan 40,50`" дозволимо лише 40 і 50 vlan. Оскільки ми використовуємо кілька на одному порту, кілька VLAN нам необхідно налаштувати інкапсуляцію. Інкапсуляція це "загортання" одного кадру в інший. На одному кінці VLAN інкапсулюються, а на іншому "разінкапсулюються" назад, ми будемо використовувати більше укорочену версію інкапсуляції dot1q. Виконаємо команду "`switchport encapsulation dot1q`".

Проводимо аналогічні налаштування на інтерфейсі Gi0/1. Ми робимо транк для двох VLAN, тому що 40 vlan потрібен для DMZ, а 50 для пристроїв, підключених до per_sw.

```
dmz_SW(config-if)#switchport mode trunk
Command rejected: An interface whose trunk encapsulation is "Auto" can not be c
nfigured to "trunk" mode.
dmz_SW(config-if)#sw
dmz_SW(config-if)#switchport tr
dmz_SW(config-if)#switchport trunk a
dmz_SW(config-if)#switchport trunk allowed vl
dmz_SW(config-if)#switchport trunk allowed vlan 40,50
dmz_SW(config-if)#sw
dmz_SW(config-if)#switchport tr
dmz_SW(config-if)#switchport trunk e
dmz_SW(config-if)#switchport trunk encapsulation d
dmz_SW(config-if)#switchport trunk encapsulation dot1q
dmz_SW(config-if)#
```

Рис. 3.6. Налаштування trunk port на dmz_sw

Далі використовуватимемо access port, це порт, який належить до одного VLAN і може передавати нетегований інформаційний трафік. Трафік проходить через 40 vlan буде виходити через інтерфейс Gi1/0 на DMZ та через Gi1/2 на per_sw. Заходимо на інтерфейси і командою switchport mode access переходимо в access режим, а командою switchport access vlan 40 дозволяємо vlan 40 на даних інтерфейсах.

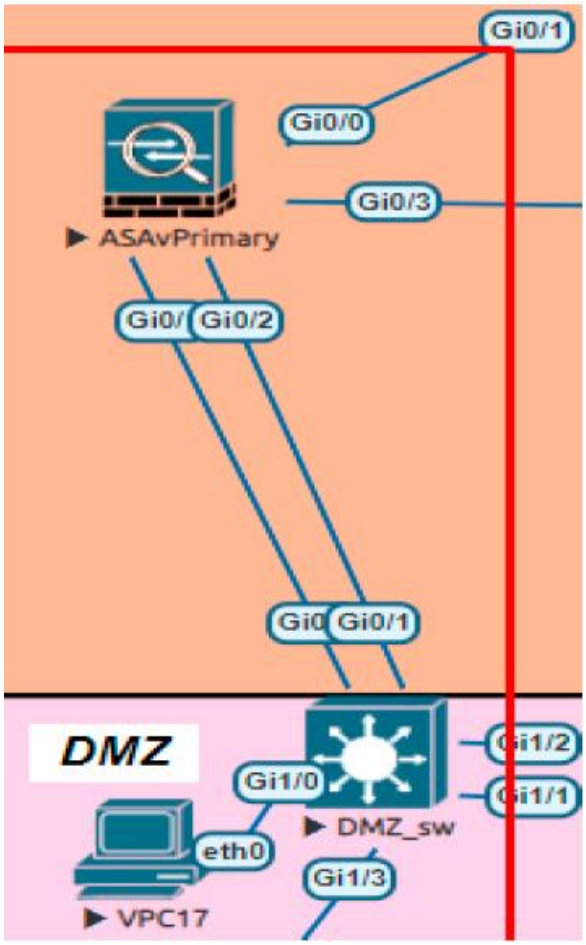

Рис. 3.7. Схема з'єднання

Налаштовуємо світч per_SW. Цей свитч дає нам вихід на підключені пристрої співробітників компанії. Заходимо на інтерфейси, що дивляться на світч dmz_sw і створюємо trunk port для vlan 40,50, що дозволить їх трафіку проходити спокійно.

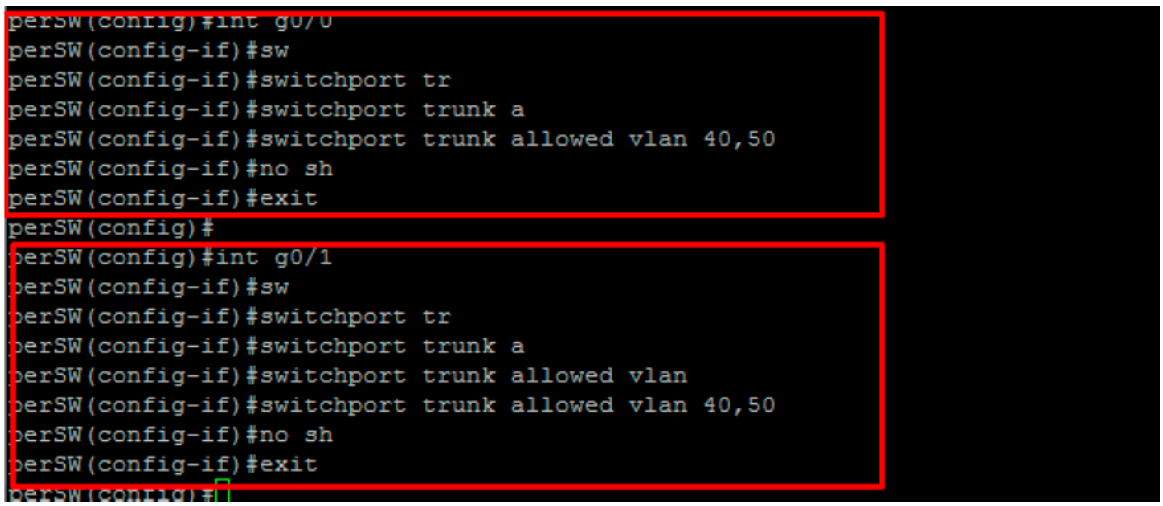

Рис. 3.8. Налаштування trunk port на per_SW

3.4. Налаштування відмовостійкості і живучості Cisco ASA

У головному офісі компанії буде встановлено дві Cisco Asa. Одна буде основною і виконуватиме всі функції, друга буде як резервна. Якщо основна Cisco Asa вийде з ладу, буде переданий сигнал на запасну. Після отримання сигналу, запасна Cisco Asa вивантажить необхідні дані та стане основною.

Налаштуємо основну Cisco Asa що називається ASA v Primary. Заходимо на інтерфейс Gi0/3, що з'єднує ASA v Primary і ASA v Secondary між собою і піднімаємо інтерфейс.

Рис. 3.9. Активація інтерфейсу

Далі нам необхідно показати свитчу BorderSw наші CiscoASA. Заходимо на інтерфейс Gi0/0 до якого прикріплений 80 vlan і дивлячись на BorderSW. Командою "`ip address 30.0.1.100 255.255.255.0 standby 30.0.1.101`" кажемо, що адреса основної ASAvPrimary 30.0.1.100, а ASAvSecondary буде мати логічну адресу 30.0.1.10

Налаштуємо додаткову адресу для DMZ. У разі відмови основної CiscoASA, щоб не скомпрометувати свою DMZ. Заходимо на інтерфейс Gi0/1 з 40 vlan дивлячись на dmz. Командою "`ip address 192.168.40.1 255.255.255.0 standby 192.168.40.101`" встановлюємо додаткову адресу 192.168.40.101.

Встановимо канал зв'язку між CiscoAsa, для цього заходимо на ASAvPrimary, вибираємо необхідний інтерфейс. Використовуючи команду "`link failover g0/3`", вибираємо інтерфейс для каналу зв'язку. Командою "`failover interface ip failover 20.0.1.1 255.255.255.252`" вказуємо адресу, що використовується. Виконуючи команду "`lan unit primary`" кажемо, що ASA в Primary буде основною (першою).

Відкриваємо запасну Cisco ASA. Необхідно налаштувати, щоб вона була запасною (другою). Заходимо на потрібний інтерфейс. Використовуємо аналогічні команди, як із налаштування основний. Різниця лише у команді "`failover unit secondary`", яка робить ASAvSecondary запасним (другим).

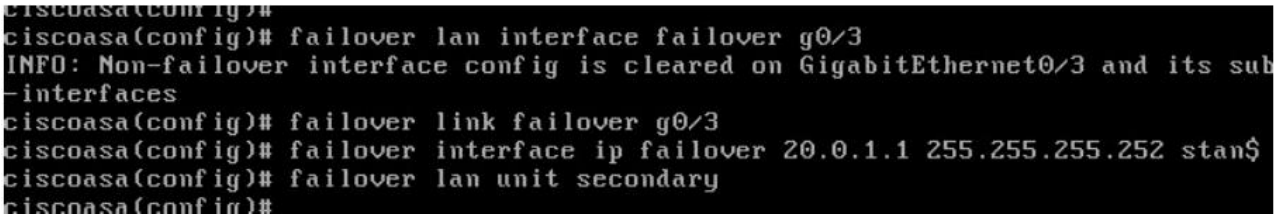

Рис. 3.10. Налаштування

Після налаштування CiscoASA здійснимо тестування роботи. Для тестування здійснимо відправку даних через канал передачі з ASAvPrimary на ASAvSecondary. Використовуючи команду "`failover`" основна CiscoASA, почне передавати дані, а запасна створювати та приймати CA сертифікат. Сертифікат буде використовуватися для підпису даних, що передаються.

Використовуючи команду show, подивимося на конфігураційні дані ASAvPrimary та ASAvSecondary. Виділені рядки говорять нам про стан обладнання на даний момент часу. ASAvPrimary перебуває у стані "`Active`", тобто зараз із мережею компанії працює вона. ASAvSecondary знаходиться в стані "`Standby Ready`", всі її процеси стоять на місці, але вона готова будь-якої миті включитися в роботу.

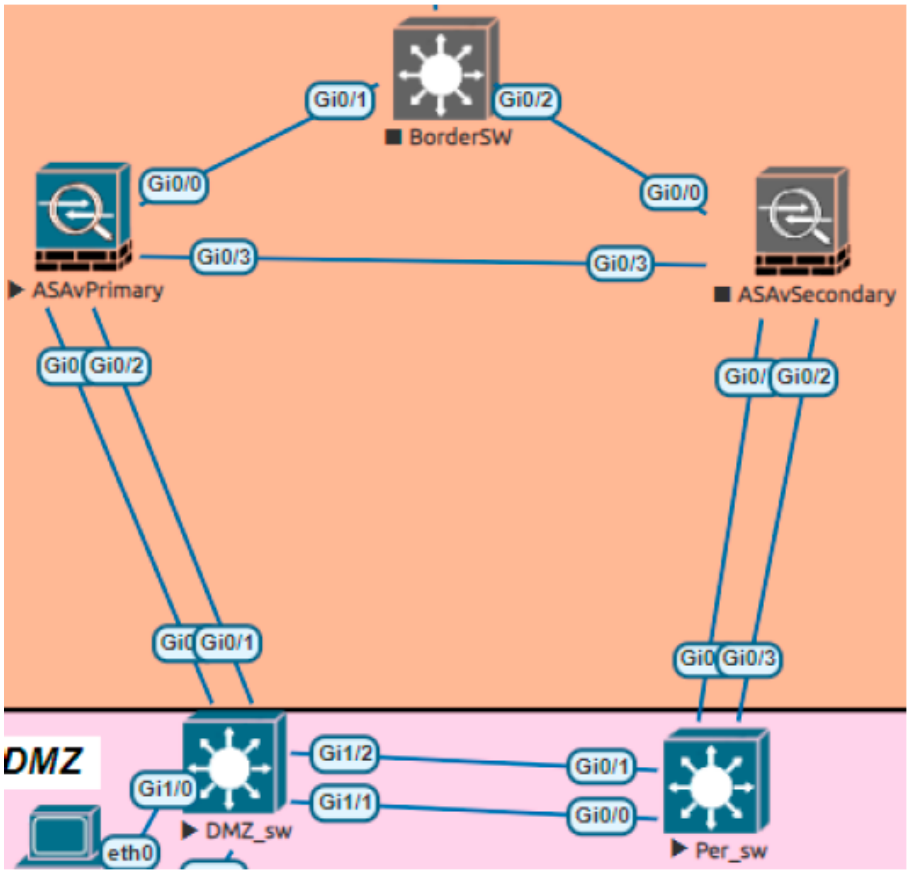

Рис. 3.11. Схема взаємодії

3.5. Конфігурування ACL листів

Далі займемося створенням ACL листів на ASAvPrimary. ACL листи — це текстові команди, що несуть у собі умови [22]. ACl листи працюють з трафіком, що проходять через задані місця і здатні фільтрувати не тільки цілі пакети, але й дивитися їх вміст. Часто їх встановлюють на прикордонних об'єктах, що стоять на межі внутрішньої та зовнішньої мережі для контролю трафіку. Для початку зайдемо на комп'ютер, що знаходиться в dmz і зададимо йому адресу. Команда "`ip 192.168.333.33`" задає адресу.

Створюватимемо ACl листи для проходження трафіку з мережі від пристрою, що знаходиться в dmz зоні у внутрішню мережу компанії. Ми створюватимемо об'єкти, вони дозволяють звертатися через його ім'я, а не адресу. Командою "`object network we_server`" створюємо об'єкт. Далі командою "`jost 192.168.33.33`" вказуємо адресу хоста. Після командою “`nat (DMZ, out) static`

`10.10.10.33`” вказуємо адресу нашого пристрою, яким до нього звертатимуся поза локальною мережею. Створюємо ACL лист командою “`access-list outside_dmz extended permit tcp any host 192.168.33.33`”, який каже нам дозволяти взаємодію хоста з усіма, використовуючи TCP протокол. Після команди “`access-group outside_dmz in interface out`” ми додаємо наш список до групи і прив'язуємо до інтерфейсу.

Дозволимо прохід icmp запитів через ASAvPrimary. Робиться це для можливості здійснення зв'язку ASAvPrimary через icmp запити з іншими пристроями. Робиться це командою "`access-list internet-icmp permit icmp any any echo-reply`".

```
ciscoasa(config)# access-list internet-icmp permit icmp any any echo-reply
ciscoasa(config)# _
```

Рис. 3.12. Створіння ACl листів

Далі прив'язуємо створений вище ACL до інтерфейсу. Виконується це командою "`access-group internet-icmp in interface out`". Пристрій комунікують через встановлений і налаштований на ньому інтерфейс, тому access-group необхідно прив'язувати до конкретно обраного інтерфейсу, щоб він міг контролювати саме його.

```
ciscoasa(config)# acces
ciscoasa(config)# access-gr
ciscoasa(config)# access-group  internet-icmp in in
ciscoasa(config)# access-group  internet-icmp in interface out
ciscoasa(config)# _
```

Рис. 3.13. Прив'язка до інтерфейсу

Створюємо Acl, що дозволяє відправляти http запити, використовуючи tcp протокол. Дозволяється лише пристроям, які мають порт більше 1024. Виконується командою “`access-list internet-http permit tcp any gt 1024 any eq www`”.

Рис. 3.14. Інформація про Acl листа

Перевіримо існування наших acl листів на ASAvPrimary. Команда “`sh access-list`” виведе нам усі acl листи.

3.6. Встановлення парольною захисту

Налаштуємо парольний захист роутерів. Створюється зменшення загрози несанкціонованого доступу. Парольний захист буває різним та захищає різні точки. Спочатку встановлюємо пароль на консоль. За промовчанням пароль на консоль відсутній. Командою "`conf t`" заходимо в режим глобальної конфігурації. Командою “`line console 0`“ режим консольного налаштування. Значення 0 є порядковим номером консолі, за стандартом консольний порт один і має номер 0. Потім командою “`login`” дозволяється вхід із використанням заданого пароля.

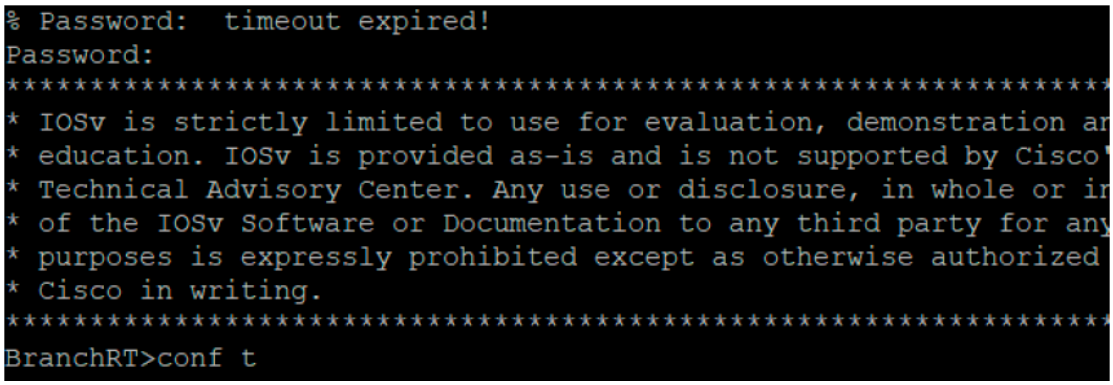

Рис. 3.15. Перевірка пароля

Встановимо паролі для доступу через telnet і ssh. За стандартом ці паролі не встановлені. Відмінність від інших типів паролі, що доки пароля для цього з'єднання не буде встановлено, по ssh і telnet не вийде зайти на пристрій. Буде сказано, що поки пароль не встановлено, віддалений вхід буде заборонено.

Командою "`line vty 0 4`" заходимо в режим налаштування віртуальних терміналів, де 0 4 означає перейти в режим конфігурування всіх віртуальних терміналів з нульового до четвертого.

```
BranchRT#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
BranchRT(config)#line vty 0 4
BranchRT(config-line)#password max
BranchRT(config-line)#login
BranchRT(config-line)#exit
BranchRT(config)#enable password max
BranchRT(config)#exit
BranchRT#
```

Рис. 3.16. Налаштування паролів для telnet та ssh

Встановлюємо пароль на привілейований режим. Підключаючись по консолі, ми спочатку потрапляє в режим користувача, а командою "`enable`" ми переходимо в привілейований. Командою "`enable password max`" ми встановлюємо пароль.

Зайдемо в привілейований режим. З нас відразу вимагає пароль.

Усі встановлені паролі за стандартом зберігаються у незашифрованому вигляді. Командою "`service password-encryption`" ми включаємо сервіс із шифрування паролів.

Зайдемо у файл із конфігураціями та перевіримо встановлені паролі та в якому вигляді вони зберігаються.

```
line con 0
 password 7 03095A13
 login
line aux 0
line vty 0 4
 password 7 082C4D56
 login
 transport input none
!
```

Рис. 3.17. Перевірка паролів на BranchRT

Зробимо аналогічні дії на роутері BorderRT.

3.7. Вихід в мережу

Налаштуємо вихід у мережу на роутері. У вкладці Network створимо об'єкт Cloud і призначимо параметр 5.

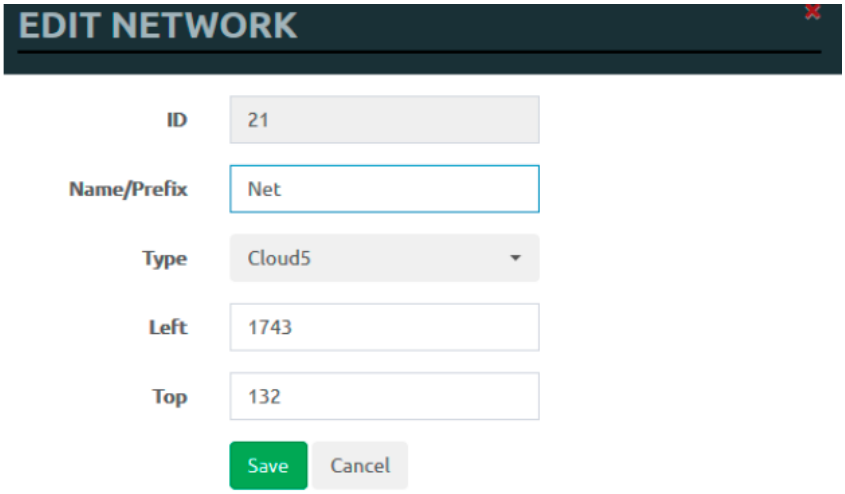

Рис. 3.18. створіння об'єкта Cloud

Створимо зв'язок між Cloud5 та роутером. Пакети надходитимуть з роутера на Cloud5, який передаватиме їх на сервер віртуальної машини eve-ng. Cloud5 буде прив'язаний до pnet5 на сервер. Зайдемо на сервер і командою "`ip address add 172.16.0.10/24 dev pnet5`" прив'яжемо адресу pnet5.

Потрібно дати можливість проходити трафіку через сервер eve-ng. За стандартом значення файлу ip_forward 0, щоб була можливість проходу трафіку, нам потрібно змінити це значення на 1. Використовуючи команду "`nano`" і шлях до файлу змінимо значення на 1.

Після попереднього налаштування eve-ng, призначимо адреси та маршрутизацію на роутері. Встановлюємо на вибраному інтерфейсі адресу 172.16.0.100 з маскою 255.255.255.0 та піднімаємо її. Командою "`do sh ip int br`" виводимо всі встановлені адреси та стану інтерфейсів. Пінгуємо адресу pnet5 172.16.0.10. Налаштуємо маршрутизацію командою "`ip route 0.0.0.0 0.0.0.0 172.16.0.10`" що дозволяє всім пакетам з роутера йти на pnet5.

Виконані налаштування не дають нам можливості виходу в Інтернет. У нас є лише одна адреса, що має вихід у мережу, і вона прив'язана до pnet0. Заходимо на сервер і вводимо команду "`iptables -t nat -A POSTROUTING -o pnet0 -s 172.16.0.0/24 -j MASQUERADE`". Команда звертається до списку адрес та дає прохід трафіку з мережі 172.16.0.0. через pnet0.

Повернімося до роутера та перевіримо вихід у мережу командою "`ping 8.8.8.8`" звернення до серверів google.

Внесені зміни повинні залишитися збереженими на сервері, щоб працювати з ними далі. Якщо ми просто вийдемо із сесії сервера eve-ng і перезавантажимо його, то все злетить.

Перейдемо до директорії /etc/network/if-pre-up.d/ і створимо там файл iptables-load. Відкриємо його та напишемо невеликий скрипт. Другим рядком ми створюємо адресу із зазначенням маски та pnet до якої ми хочемо її прив'язати. Третій рядок ми вказуємо звідки завантажувати налаштування nat. Четвертим рядком ми даємо дозвіл пропуску пакетів через віртуальну машину із зазначенням файлу, значення якого треба змінити. Код п'ятого рядка даватиме можливість скрипту завершитися.

Після створення скрипту перевіримо його наявність у директорії. Потрібно зробити цей файл виконуваним. Командою "`chmod +x iptables-load`" дамо право на виконання файлу. Після цього можна спокійно перезавантажувати.

```
root@eve-ng:~# cd /etc/network/if.pre.up.d/
-bash: cd: /etc/network/if.pre.up.d/: No such file or directory
root@eve-ng:~# cd /etc/network/if-pre-up.d/
root@eve-ng:/etc/network/if-pre-up.d# ls -all
total 20
drwxr-xr-x 2 root root 4096 May  1 18:32 .
drwxr-xr-x 7 root root 4096 May  1 18:28 ..
lrwxrwxrwx 1 root root   29 Aug 20  2015 bridge -> /lib/bridge-utils/ifupdown.sh
-rwxr-xr-x 1 root root  344 Mar 14  2016 ethtool
-rw-r--r-- 1 root root  145 May  1 18:32 iptables-load
lrwxrwxrwx 1 root root   42 Oct  4  2018 openvswitch -> /usr/share/openvswitch/scripts/ifupdown.sh
-rwxr-xr-x 1 root root  241 Nov 17  2014 uml-utilities
root@eve-ng:/etc/network/if-pre-up.d# chmod +x iptables-load
root@eve-ng:/etc/network/if-pre-up.d# ls -all
total 20
drwxr-xr-x 2 root root 4096 May  1 18:32 .
drwxr-xr-x 7 root root 4096 May  1 18:28 ..
lrwxrwxrwx 1 root root   29 Aug 20  2015 bridge -> /lib/bridge-utils/ifupdown.sh
-rwxr-xr-x 1 root root  344 Mar 14  2016 ethtool
-rwxr-xr-x 1 root root  145 May  1 18:32 iptables-load
lrwxrwxrwx 1 root root   42 Oct  4  2018 openvswitch -> /usr/share/openvswitch/scripts/ifupdown.sh
-rwxr-xr-x 1 root root  241 Nov 17  2014 uml-utilities
root@eve-ng:/etc/network/if-pre-up.d# _
```

Рис. 3.19. Призначення прав файлу iptables- load

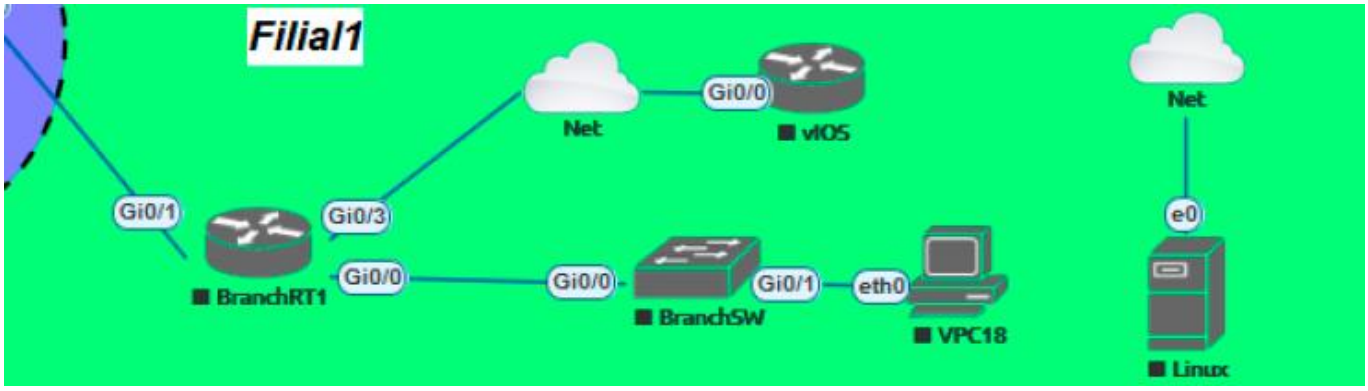

Рис. 3.20. Схема мережі першого філії

3.8. Налаштування компонентів мережі другої філії

Перейдемо до налаштування мережі другої філії. У другій філії буде використовуватися роутер BranchRT2, що з'єднує філію з основним офісом та з другою філією. Використовуватиметься Cisco ASA для безпеки та маршрутизації трафіку. У філії 2 налаштуємо vlan 70 і 10 для безпечної роботи співробітників. Зайдемо на інтерфейси та поставимо адреси 195.221.31.2/30 на вихід у мережу та 31.0.1.1/24 на вихід у внутрішню мережу філії.

Створення GRE тунелю. Generic Routing Encapsulation (GRE) – це один із можливих тунельних механізмів передачі пакетів. Створений тунель дозволять транспортувати пакет одного протоколу пакет іншого протоколу. Пакет, який транспортується називається пакет "пасажир". Пакет, який переносить "пасажира", називається транспортним протоколом. Тунель працює point to point, що означає, що пакет передається від відправника точно до одержувача. Налаштування GRE вимагає створення логічного інтерфейсу кінцевих точках тунелю[22].

Будемо створювати тунелі між головним офісом та філією. Почнемо налаштування GRE тунелю між філіями. Створюємо логічний інтерфейс Tunnel1. Адреса 172.16.1.3 255.255.255.0 використовуватиметься тунелем на стороні BranchRT2. GRE є інкапсульованим протоколом (модульним), тому нам необхідно задати maximum

transfer unit (mtu) та maximum segment size (mss). Командою "`ip mtu 1400`" встановимо mtu, а командою “`ip tcp adjust-mss 1360`” mss, заданих значень вистачить, щоб пакети не фрагментувалися. Після чого потрібно задати адресу хоста, використовується адреса BranchRT2 та адреса одержувача, яким є BranchRT. Далі, використовуючи команду “`do s hip int br`”, виведемо параметри всіх інтерфейсів пристрою.

Перейдемо на BranchRT1, який є роутером першої філії і налаштуємо GRE тут. Адреса тунелю на стороні BranchRT1 буде 172.16.1.4 з маскою 255.255.255.0, адреса джерело сама BranchRT1, а одержувач роутер BranchRT2. Після налаштування зробимо Icmp echos і переконаємось у роботі тунелю.

Далі налаштуємо GRE тунель між роутером головного офісу BorderRT та роутером першого філії BranchRT1. Адреса тунелю на стороні BranchRT1 буде 40.16.1.1, адреса джерела інтерфейс BranchRT1 дивиться на BorderRT, адреса одержувача буде BorderRT.

Після налаштування GRE на BorderRT. Адреса тунелю на боці BorderRT буде 40.16.1.2. Джерелом буде адреса самого BorderRT, а одержувачем адреса BranchRT1.

Перевіримо працездатність GRE тунелю між BorderRT та BranchRT1, відправивши Icmp echos на адреси входів у тунелі.

Останнім будемо налаштовувати тунель між роутером головного офісу BorderRt та роутером другого офісу BranchRT2. Адреса тунелю на стороні BranchRT2 буде 172.50.1.9. Джерелом буде адреса самого BranchRT2, одержувачем буде BorderRT.

Налаштуємо GRE на боці BorderRT. Адреса тунелю буде 172.50.1.10. Джерелом буде адреса самого роутера, одержувач буде роутером BranchRT2. Значення mtu та mss залишаться незмінними.

Перевіримо працездатність каналу, відправивши Icmp echos на адресу тунелю.

Налаштування IPsec шифрування. Сам собою GRE тунель не підтримує шифрування і передає трафік у відкритому вигляді від джерела до одержувача і без вимоги аутентифікації. Можна встановити поверх GRE тунелю IPSEC шифрування. Налаштування IPSEC шифрування складається із двох етапів. У першому визначаємо

політику безпеки (ISAKAMP IKE) для створення тунелю. У другому етапі налаштовуємо параметри тунелю (IPSec) передачі даних [22].

Організуємо IPSec шифрування між роутером головного офісу BorderRT та роутером другої філії BranchRT2. Командою “`crypto isakmp policy1`” перейдемо до настроювання політик безпеки. Команда “`encryption aes`” визначає метод шифрування AES. Далі створюємо метод аутентифікації pre-share командою “`authentication pre-share`”. Group 2 є методом обміну секретними ключами, а саме методом Діффі-Хеллмана. Встановимо час життя сесії 10000с. Визначаємо адресу кінцевої точки тунелю, а саме адресу BrnchRT2, а також їхній загальний ключ pre-share для аутентифікації. Командою “`crypto ipsec transform-set GRE-IPSEC esp-3des esp-sha-hmac`” налаштовуємо параметри тунелю IPSec.

Після встановлення всіх параметрів тунелю необхідно налаштувати профіль підключення. Командою “`crypto ipsec GRE`” встановлюємо назву профілю GRE. Далі встановлюємо час життя сесії. Насамкінець нам необхідно прив'язати наш профіль до тунельного інтерфейсу Tunnel3, для цього використовуємо команду “`tunnel protection ipsec profile GRE`”.

Зробимо аналогічні налаштування на роутері другої філії BranchRT2. Різниця буде адресою кінцевої точки тунелю, а саме адресою BorderRT.

У результаті після настроювання IPSec шифрування тунелю відобразимо статус сесії шифрування тунелю. Використовуємо команду "`sh crypto session`". У конфізі, що відображається, ми бачимо, що відображені кінцеві і початкові точки входу трфіка для шифрування, для підняття сесії залишається відправити Icmp echos.

3.9. Ідентифікація активів і заходів захисту

Один із етапів аналізу ризиків полягає в ідентифікації всіх об'єктів, які потребують захисту. Деякі активи (наприклад, апаратура) ідентифікуються очевидним чином. Про інші (наприклад, людей, які використовують інформаційні системи) нерідко забувають. Необхідно зважити на все, що може постраждати від порушень режиму безпеки.

Може бути використана наступна класифікація активів:

- апаратура: процесори, модулі, клавіатури, термінали, робочі станції, персональні комп'ютери, принтери, дисководи, комунікаційні лінії, термінальні сервери, мости, маршрутизатори;
- програмне забезпечення: вихідні тексти, об'єктні модулі, утиліти, діагностичні програми, операційні системи, комунікаційні програми;
- дані: оброблювані, безпосередньо доступні, архівовані, збережені у вигляді резервної копії, реєстраційні журнали, бази даних, дані, що передаються комунікаційними лініями;
- люди: користувачі, обслуговуючий персонал;
- документація: за програмами, апаратурою, системною, адміністративними процедурами, безпекою;
- витратні матеріали: папір, форми, бланки, барвник, магнітні носії.

Після того, як виявлено активи, що потребують захисту, необхідно ідентифікувати загрози цим активам та розміри можливої шкоди. Ця робота має бути спрямована на те, щоб зрозуміти, яких загроз слід побоюватися найбільше.

Несанкціонований доступ до комп'ютерних ресурсів – загроза, типова для більшості організацій. Несанкціонований доступ може набувати різних форм. Іноді це нелегальне використання рахунку іншого користувача для доступу до системи. В інших випадках ресурсами користуються без попереднього дозволу.

Ступінь важливості проблеми несанкціонованого доступу до різних організацій різна. Іноді передача прав доступу до неавторизованого користувача може призвести до руйнування магнітних носіїв. Найчастіше несанкціонований доступ полегшує виконання інших загроз. Різна і реальність нападу: деякі організації (відомі університети, урядові та військові установи) притягують до себе зловмисників. Отже, ризик несанкціонованого доступу змінюється від підприємства до підприємства.

Нелегальне ознайомлення з інформацією – інша поширена загроза. Визначте ступінь конфіденційності інформації, яка зберігається на ваших комп'ютерах.

Комп'ютери та мережі надають своїм користувачам безліч цінних послуг, від яких залежить ефективна робота багатьох людей. Коли послуги раптом стають недоступними, виникають втрати -прямі та непрямі.

Відмова в обслуговування виникає по різним причин і проявляється по-різному. Мережа може прийти в непрацездатний стан від підробленого пакету, навантаження або через відмову компонента. Вірус здатний уповільнити чи паралізувати роботу комп'ютерної системи. Кожна організація повинна визначити собі набір необхідних сервісів і кожного з них проаналізувати наслідки його недоступності.

Активи, розглянуті в даній роботі:

- DMZ (поштовий, веб-сервер);
- сервер (Dhcp, Dns, AD, Me);
- маршрутизатор;
- комутатор;
- Cisco ASA;
- PC.

Таблиця 3.1

Інформаційні активи

№	Код активу	Найменування	До л-во	Відповідальний	Цінність	Пріорітет
1	DM	DMZ (поштовий, веб-сервер)	1	Мережевий адміністратор	6	3
2	SR	Сервер (DHCP, DNS, M E, AD)	1	Інженер ІБ	5	4
3	RO	Маршрутизатор	4	Мережевий адміністратор	3	4
4	SW	Комутатор	5	Мережевий адміністратор	3	5
5	AS	Cisco ASA	2	Інженер ІБ	5	2
6	PC	PC (персональний комп'ютер)	20	Мережевий адіністартор	3	2

Розглянемо заходи захисту, які використовуються для створення захищеної мережі:

- міжмережеві екрани нового покоління Cisco ASA серії 5500-X допомагають замовникам знайти баланс між ефективністю забезпечення безпеки та продуктивністю. Це рішення, що є поєднанням найпопулярнішого в галузі міжмережевого екрану з контролем стану з'єднань і повного асортименту сервісів мережевої безпеки нового покоління;
- ACL (Access Control List) - це строго кажучи, механізм для вибору з усього потоку трафіку якоїсь частини за заданими критеріями. ACL-і бувають двох видів: стандартні та розширені. Стандартні дозволяють відфільтровувати трафік лише за одним критерієм: адреса відправника, в CCNA розглядається лише IP адресу відправника. Розширений ACL дозволяє фільтрувати трафік по великій кількості параметрів: адреса відправника, адреса одержувача, TCP/UDP порт відправника, TCP/UDP порт одержувача, протоколу, загорнутому в IP (відфільтрувати тільки TCP, тільки UDP, тільки ICMP, тільки GRE тощо), типу трафіку для даного протоколу (наприклад, для ICMP відфільтрувати лише ICMP-Reply);
- VLAN (Virtual Local Area Network, віртуальна локальна мережа) - це функція в роутерах та комутаторах, що дозволяє на одному фізичному мережевому інтерфейсі (Ethernet, Wi-Fi інтерфейсі) створити кілька віртуальних локальних мереж. VLAN використовують для створення логічної топології мережі, яка ніяк не залежить від фізичної топології;
- тунелювання надає механізм транспортування пакету одного протоколу всередині іншого. Протокол, який транспортується, називається протоколом пасажиром. Протокол, який "несе" протокол, називається транспортним протоколом. Generic Routing Encapsulation (GRE) — це один із можливих тунельних механізмів, який використовує IP як транспортний протокол та може бути використаний для перенесення багатьох інших протоколів пасажирів. Тунелі є Point-to-Point з'єднаннями, що визначаються Tunnel Source і Tunnel Destination адресами обох кінцях;

- IPsec (скорочення від IP Security) - набір протоколів для забезпечення захисту даних, переданих по міжмережевому протоколу IP. Дозволяє здійснювати підтвердження автентичності (аутентифікацію), перевірку цілісності та/або шифрування IP-пакетів. IPsec також включає протоколи для захищеного обміну ключами в мережі Інтернет . В основному застосовується для організації VPN -з'єднань;
- для захисту пристроїв Cisco від несанкціонованого доступу використовується кілька видів паролів. У курсі CCNA розглядається налаштування паролів на консоль, паролів на підключення по Telnet та SSH, а також пароль для доступу до привілейованого режиму роботи пристрою. Паролі налаштовуються однаково для маршрутизаторів і комутаторів.

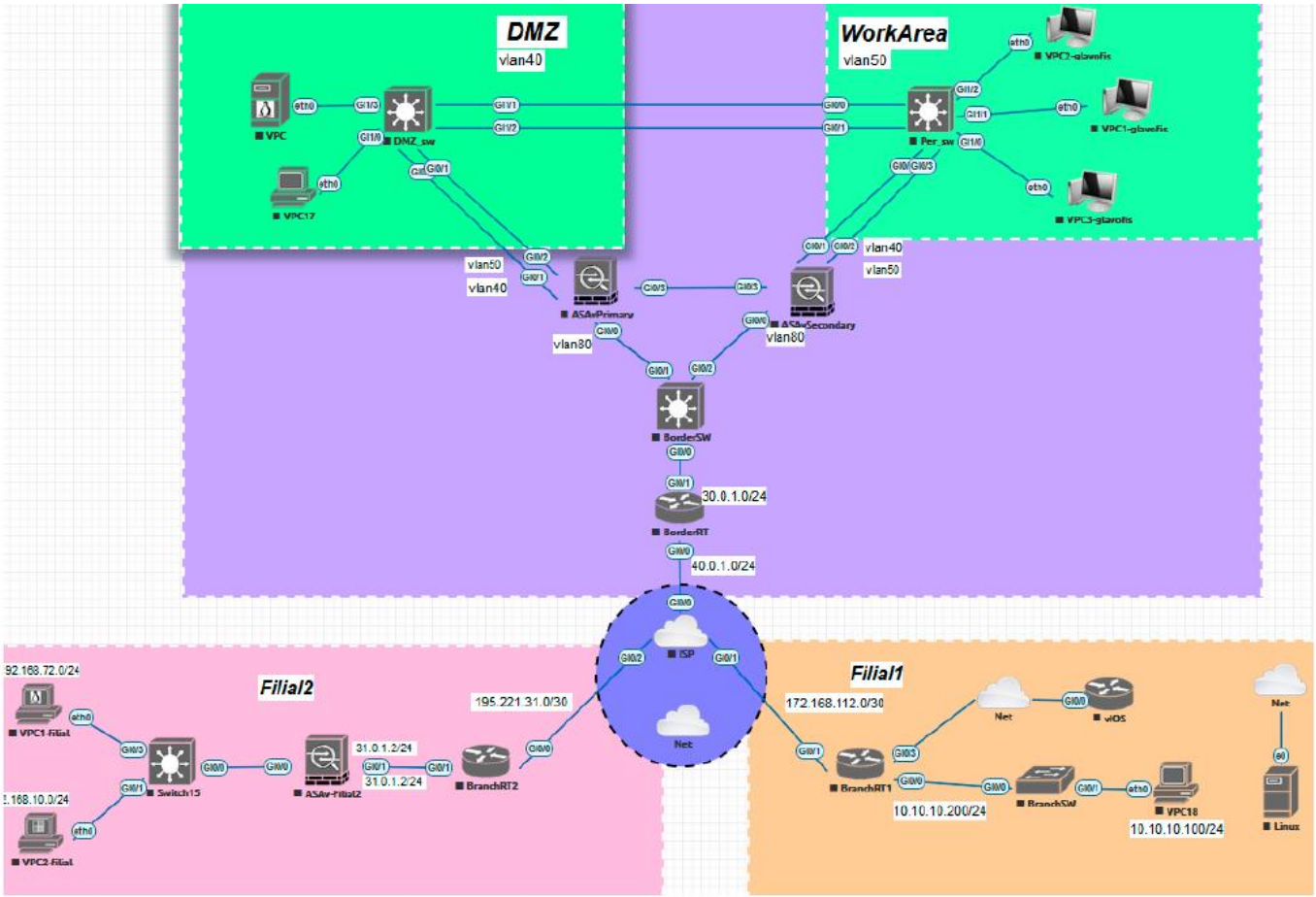

Рис. 3.21. Схема організації інформаційної безпеки в корпоративній мережі

РОЗДІЛ 4
ОХОРОНА ПРАЦІ

4.1. Аналіз небезпечних і шкідливих факторів, що впливають на інженера

Відділ проектування знаходиться на другому поверсі п’ятиповерхового будинку. Приміщення має розміри: довжина 8 м, ширина 4 м, висота 4. Загальна площа - 32 м^2, загальний об’єм – 128 м^3. У відділі знаходиться 5 робочих місць інженерів-проектувальників, оснащені комп’ютерами.

Робоча площа одного співробітника становить:

$$S_{\text{роб}} = \frac{S_{\text{заг.пл}}}{N} = \frac{32}{5} = 6{,}4 \text{ м}^2$$

Робочий об’єм одного співробітника:

$$V_{\text{роб}} = \frac{V_{\text{заг.об}}}{N} = \frac{128}{5} = 25{,}6 \text{ м}^3$$

N- кількість співробітників у відділі

$S_{\text{заг.пл}}$ – загальна площа;

$V_{\text{заг.об}}$ – загальний об’єм.

Відповідно до [31] площа на одне робоче місце має становити не менше ніж 6 м^2, а об'єм не менше ніж 20 м^3. Робоче місце інженера-проектувальника відповідає вимогам.

В проектному відділі інженера-проектувальника знаходяться: комп’ютери, принтер. У даному приміщенні температура повітря у теплий період року становить 30℃, використовується природне та штучне освітлення. Штучне освітлення виконано у вигляді переривчастих ліній світлодіодних світильників. Рівень шуму в приміщенні становить 54 дБ, а згідно з Державними санітарними нормами [32] не повинен перевищувати 50 дБ.

Робоче місце розташоване так, щоб природне світло падало з лівої сторони, при цьому відстань зі світлом до робочого місця - 1 м. Висота робочої поверхні столу над підлогою 750 мм, глибина столу – 800 мм, ширина столу 1300мм. Робочий стіл має простір для ніг висотою 650 мм та шириною 600 мм.

Перелік шкідливих та небезпечних виробничих чинників.

Створення сприятливих умов праці, в роботі інженера-проектувальника, має велике значення як для полегшення , так і для підвищення продуктивності праці. Відповідно до [33] шкідливими виробничими факторами є:

1. Підвищена температура робочого приміщення
2. Недостатня освітленість робочої поверхні
3. Виробничий шум
4. Електромагнітні випромінювання радіочастотного діапазону
5. Іонізуючі випромінювання

Відповідно до [34] робота інженера-проектувальника у приміщенні з енерговитратами 90-120 ккал/год. відносяться до категорії легких фізичних робіт Іа (роботи, що виконуються сидячи і не потребують фізичного напруження).

Таблиця 4.1

Оптимальні величини температури

Період року	Категорія робіт	Температура повітря,°С
Холодний період року	Легка Іа	22-24
Теплий період року		23-25

Допустимі величини температури на постійних робочих місцях:

Період року	Категорія робіт	Температура повітря,°С	
		Верхня межа	Нижня межа
Холодний період року	Легка Іа	25	21
Теплий період року		28	22

У проектному відділі температура повітря становить 30℃ в теплий період року,що перевищує допустиму на 2 ℃. Забезпечили температуру приміщення 23 ℃,за допомогою механічної вентиляції з вентилятором VORTICE VARIO, повітрообмін якого становить 680 $м^3$ /год.

Недостатня освітленість. В приміщенні встановлені персональні комп’ютери, присутнє природне та штучне освітлення . За вимогами [35], величина коефіцієнта природної освітленості повинна бути не менше 1.5%. В проектному відділі порушенні

вимоги, освітленість робочої поверхні складає 370 лк , а коефіцієнт освітленості складає 1.2%. Природне світло проникає у приміщення через бічні світло прорізи. Вікна мають жалюзі. Штучне освітлення виконано у вигляді переривчастих ліній світлодіодних світильників, розташованих паралельно лінії зору інженера-проектувальника. Для місцевого освітлення використовувати галогенні лампи розжарювання

Виробничий шум. Шум на робочому місці створюється: комп'ютером та периферійним пристроєм. Допустимі рівні звукового тиску на робочому місці повинні відповідати вимогам [36]:

Таблиця 4.2

Санітарні норми виробничого шуму, ультразвуку та інфразвуку

Вид трудової діяльності, робоче місце	Рівні шуму та еквівалентні рівні шуму, ДБА, дБАекв
Конструювання та проектування.	50

Реальний рівень шуму в проектному відділі становить 54 дБ, що перевищує допустимий рівень.

Для зменшення рівня шуму рекомендується використовувати місцеву та загальну звукоізоляцію, шумопоглинаючі екрани, поглинаючі фільтри.

4.2. Організаційні та конструктивно-технологічні заходи для зниження впливу шкідливих виробничих факторів

Нормалізація повітря робочої зони. Для створення й автоматичної підтримки в ІТ відділі незалежно від зовнішніх умов оптимальних значень температури, вологості, чистоти і швидкості руху повітря, у холодний час року використовується водяне опалення, у теплий час року застосовується кондиціонування повітря [37].

Виробниче освітлення. Під час аналізу освітлення на робочому місті програміста було встановлено, що воно не відповідає встановленим нормам, тому для покращення умов праці рекомендуємо збільшити рівень загальної освітленості приміщення

шляхом встановлення 5 додаткових світильників, щоб загальна кількість лам відповідала розрахованому вище значенню, а саме 36 світлодіодних ламп. Також для підтримки запроектованого освітлення у чистому виді необхідно скласти графік, де передбачити очищення віконних блоків і світильників не менше 2 разів на рік [38].

Електробезпека. Електробезпечність у приміщенні ІТ відділу пропоную забезпечити наступними технічними способами і засобами захисту:

– для зменшення накопичення статичної електрики застосовувати зволожувачі і нейтралізатори, антистатичне покриття підлоги;

– забезпечити приєднання металевих корпусів устаткування до жили, що заземлює. Заземлення корпуса ПК забезпечити підведенням жили, що заземлює, до розеток. Опір заземлення 4 Ом, згідно (ПУЭ) для електроустановок з напругою до 1000 В. А також організаційними заходами:

– своєчасне проведення інструктажів з техніки безпеки [39].

Ергономіка та організація робочого місця. Після проведення аналізу робочого місця програміста в ІТ Відділі було з'ясовано, що воно відповідає встановленим вимогам.

Виходячи з результатів аналізу важкості та напруженості праці пропоную скоротити час роботи за комп'ютером, робити перерви сумарний час яких повинен складати 50 хвилин при 8-ми годинному робочому дні [40].

4.2.1. Розрахунок повітрообміну за надлишком тепла у проектному відділі

Приміщення має розміри 4×8×4, яке розміщується на другому поверсі п’ятиповерхового будинку з південного боку. Площа вікон F = 2,88 м^2. На вікнах розміщенні жалюзі. У приміщенні 5 інженерів-проектувальників, розташовано $N_{пк} = 5$ персональних комп’ютерів та принтер. Для штучного освітлення використовується 4 офісних світлодіодних світильника потужністю 125 Вт.

1. Розраховуємо загальну кількість тепла:

$$Q_{над} = Q_{осв} + Q_{облад} + Q_{ін\text{-}пр.} + Q_{рад,}\ \text{Вт} \qquad (4.1)$$

$Q_{над}$ – загальна кількість тепла

$Q_{осв}$ - кількість тепла від джерел штучного освітлення

$Q_{облад}$ - кількість тепла від обладнання

$Q_{ін\text{-}пр.}$- кількість тепла від інженерів-проектувальників

$Q_{рад,}$- кількість тепла від сонячної радіації

2. Розраховуємо кількість тепла від джерел штучного освітлення:

$$Q_{осв} = N \cdot \eta \,, \tag{4.2}$$

де N - сумарна потужність джерел освітлення, Вт; η - коефіцієнт теплових витрат (η = 0,55 – для світлодіодних ламп).

$$Q_{осв.} = 125 \cdot 4 \cdot 0{,}55 = 275 \text{ Вт}$$

2. Розраховуємо кількість тепла при роботі обладнання: 5 комп'ютерів і принтера (в режимі друку):

$$Q_{облад} = n \cdot P_{комп.} + P_{пр.}, \tag{4.3}$$

де n – кількість комп'ютерів (обладнання);

$P_{комп}$ – встановлена потужність комп'ютерів, $P_{комп} = 400$ Вт

$P_{пр.}$ – потужність принтера в режимі друку, $P_{пр} = 465$ Вт

$$Q_{облад} = 5 \cdot 400 + 465 = 2.5 \text{ кВт}$$

3. Розраховуємо кількість тепла від інженерів-проектувальників:

$$Q_{ін\text{-}пр.} = n \cdot q \text{ , Вт} \tag{4.4}$$

n – кількість інженерів-проектувальників

q – кількість тепла, що виділяється одним інженером-проектувальником

Кількість тепла, що виділяється одним інженером-проектувальником, який виконує легку фізичну роботу дорівнює 99 Вт.

$$Q_{ін\text{-}пр} = 5 \cdot 99 = 495 \text{ Вт}$$

4. Розраховуємо кількість тепла від сонячної радіації:

$$Q_{рад} = m \cdot S \cdot k \cdot q_{скл} \tag{4.5}$$

де m – число вікон; $S_{вікна}$ – площа одного вікна, $S_{вікна}$ =2,88 $м^2$;

k – коефіцієнт, віконного переплетення: k = 0,6 матові;

$q_{скл.}$ – надходження тепла через 1 $м^2$ вікна при різній орієнтації вікон: $q_{скл.}$ = 150 – південь;

$$Q_{рад} = 1 \cdot 2{,}88 \cdot 0{,}6 \cdot 150 = 259{,}2 \text{ Вт}$$

5. Загальна кількість тепла в проектному відділі:

$Q_{над}= Q_{осв}+ Q_{облад}+ Q_{ін\text{-}пр.} + Q_{рад}=275+2500+495+259{,}2 = 3{,}529$ кВт

6. Потрібний повітрообмін за надлишком тепла:

$$L = \frac{Q}{c \cdot \rho \cdot (t_{\text{вид}} - t_{\text{зовн}})}, \text{м}^3/\text{год} \quad (4.6)$$

Q - кількість тепла, яке виділяється в приміщення за годину, Дж:

$$Q=3600 \cdot Q_{надл}=3600 \cdot 3529=12704 \text{ Вт} = 5328 \text{ кДж};$$

c – теплоємність повітря, Дж/кг (в інтервалі температур від 0ºС до 100ºС приймається рівною $1{,}01 \cdot 10^3$Дж/кг);

ρ – густина повітря, кг/м^3(дорівнює $\rho_{внт}$=1,2 кг/м^3);

$t_{вид}$– температура повітря, що видаляється, $t_{вид}=30$℃

$t_{зовн.}$- температура повітря, що подається до робочої зони, $t_{зовн.}$=23℃

$$L = \frac{5328}{1{,}01 \cdot 10^3 \cdot 1{,}2 \cdot (30 - 23)} = 628 \text{ м}^3/\text{год}$$

Оскільки, в проектному відділі підвищена температура повітря на 2 ℃ від допустимого значення 28℃, встановили механічну вентиляцію з вентилятором VORTICE VARIO , яка забезпечила надходження до приміщення температури повітря 23 ℃, дане значення є оптимальним.

4.3. Пожежна безпека

Відповідно до [39-40] дане приміщення відноситься до категорії В по вибухово-пожежній та пожежній небезпеці із-за використання у ньому твердих горючих матеріалів з температурою спалаху понад 61℃.

Проектний відділ оснащено:

- Двома безпровідними датчиками детектування диму SD-02 (оповіщає при задимленні приміщення; площа обслуговування: до 20 м^2);
- двома порошковими вогнегасниками ВП-5 (для приміщення категорії В за відсутності горючих газів і рідин, площею до 50 м^2 і масою вогнегасної речовини – 5 кг, мінімальна кількість порошкових вогнегасників 2).

- LifeSOS LS-30LR бездротова пожежно-охоронна система (при детектуванні вторгнення, датчики передають на центральний блок сигнал тривоги по радіоканалу без проводів. Централь приймає сигнал від датчиків, включає сирену, відправляє інформацію на пульт централізованого нагляду, дзвонить на зазначені телефонні номери та відправляє SMS повідомлення з повідомленнями про тривогу.)

Для попередження виникнення пожеж проводяться організаційно-технічні заходи пожежної безпеки, які включають:

- включення питань пожежної безпеки у всі інструкції по техніці безпеки;
- виконання встановленого режиму експлуатації електричних мереж та обладнання;
- заборона куріння в недозволеному місці;
- видання необхідних інструктажів, планів евакуації

План евакуації складається з графічної і текстової частин. Графічна частина являє собою схематичний план поверху (рис. 5.1), в якому зеленими суцільними стрілками вказують шляхи евакуації, що ведуть до основних евакуаційних виходів, а пунктирними зеленими стрілками - до аварійних виходів. Двері на шляху евакуації відчиняються назовні у напрямку виходу з будівлі. На плані евакуації умовними знаками показано розміщення вогнегасників, пожежних гідрантів, телефонів, аптечок медичної допомоги, електрощитів, датчиків диму, системи охоронно-пожежної сигналізації.

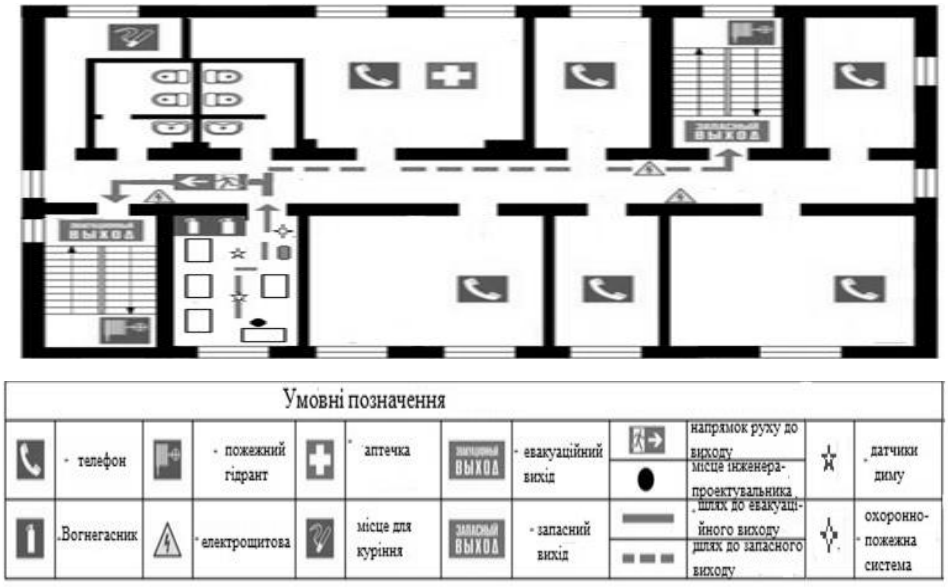

Рис 5.1. План евакуації 2 поверх

4.4. Інструкція з охорони праці при роботі з персональним комп'ютером

Вимоги безпеки перед початком роботи.

- Перед початком роботи працівник повинен зовнішнім оглядом перевірити цілісність корпусів системного блоку, відео монітора, принтера, клавіатури.
- Перевірити цілісність кабелів живлення, місць їх підключення (розеток електромережі, продовжувачів електромережі, розгалужувальних коробок, штепсельних вилок).
- Підготувати своє робоче місце, прибравши речі, які можуть заважати при виконанні роботи.
- Ввімкнути живлення ПК.
- У випадку, якщо після ввімкнення ПК не проходить загрузка або комп'ютер не виходить на робочий режим, працівник повинен повідомити керівника чи спеціаліста відділу інформаційних технологій.
- При виявленні ушкодження або яких-небудь інших недоліків повідомити безпосереднього керівника. Не приступати до роботи без його вказівки.

Вимоги безпеки під час роботи

- Необхідно стійко розташувати всі складові пристрої на столі, в тому числі і клавіатуру. Разом з тим повинна бути передбачена можливість переміщення клавіатури. ЇЇ розташування і кут нахилу повинні відповідати побажанням користувача ПК. Якщо в конструкції клавіатури не передбачений простір для опору долонь, то її слід розташовувати на відстані не менше 100 мм від краю столу в оптимальній зоні моніторного поля. При роботі на клавіатурі слід сидіти прямо, не напружуватись.
- Для зменшення несприятливого впливу на користувача пристроїв типу "миша" (вимушена поза, необхідність постійного контролю за якістю дій) слід забезпечити вільною більшу площу поверхні столу для переміщення "миші" і зручного упору ліктьового суглоба.
- Не припустимі сторонні розмови, роздратовуючи шуми тощо.

- Періодично при вимкнутому ПК слід видаляти злегка зволоженою мильним розчином хлопко-паперовою салфеткою пил з поверхонь апаратури. Екран і захисний екран протирають ватою, зволоженою спиртом.
- Не дозволяється використовувати рідинні або аерозольні засоби чистки поверхонь ПК.

Забороняється:

- самостійно ремонтувати апаратуру, в яких кінескоп та інші елементи можуть знаходитись під високою напругою (до 25 кВ0.)
- класти будь-які речі на апаратуру ПК, бутерброди та напої на клавіатуру або поруч з нею. Це може вивести її з ладу;
- затуляти вентиляційні отвори в апаратурі, це може призвести до її перегріву і виходу з ладу.

- Для зменшення негативного впливу на стан здоров'я працівників різних факторів ризику, пов'язаних з роботою на ПК, передбачаються додаткові регламентовані перерви для відпочинку користувачів ПК:

- через кожний час безперервної роботи – 10 хвилин;
- через кожні 2 години – 15 хвилин.

- При можливості слід чергувати зміну діяльності з іншою, не пов'язаною з роботою на ПК.
- З метою зменшення негативного впливу монотонності доцільно застосовувати чергування операцій введення тексту і введення даних (зміна змісту і темпу роботи) і т.п.
- При роботі на лазерних принтерах:
- Розташовувати принтер необхідно поряд з системним блоком так, щоб з'єднувальні шнури не були натягнуті. Забороняється ставити принтер на системний блок.
- Перш, ніж програмувати роботу принтера, впевніться, що він знаходиться в режимі зв'язку з системним блоком.
- Для досягнення високоякісного, чистого, з високою роздільною здатністю зображення щоб не зіпсувати апарат, потрібно використовувати папір, марка якого вказана в інструкції до принтера (найчастіше папір вагою 60-135 г/м^2, типу Canon або Xerox 4024).

- Обрізання країв паперу повинно бути виконаним гострим лезом ножа, без зазусенців – це зменшить вірогідність загинання паперу.
- При виконанні роботи (більше 20 хвилин), коли втручання користувача в роботу програми не потрібне, бажано вимикати живлення відео монітора.
- Для підтримки загального тонусу м'язів, профілактики кістково-м'язових порушень, зорового дискомфорту та інших несприятливих суб'єктивних почуттів під час регламентованих перерв необхідно виконувати комплекси рекомендованих вправ для очей, для хребта, для рук.
- Кількість мікро пауз до 1-2 хвилин слід визначити індивідуально. Форма та зміст перерв можуть бути різними виконання допоміжних робіт, не пов'язаних з роботою ПК , приймання їжі, виконання рекомендованих вправ.
- Виконання фізичних вправ протягом дня рекомендується індивідуально, залежно від почуття втоми. Гімнастика повинна біти на корекцію вимушеної пози покращення кровообігу, часткову компенсацію, дефіциту рухової активності.
- Про виявлені несправності (іскріння, пробоїв, запаху гару, ознак горіння тощо) негайно припинити роботу, відключити все обладнання від електромережі і терміново повідомити безпосереднього керівника або спеціаліста по ремонту ПК.

Вимоги безпеки при закінчення роботи на ПК.

- Закінчити і зберегти в пам'яті ПК файли, які знаходились у роботі. Виконати всі дії для коректного завершення роботи в оперативній системі.
- Вимкнути принтер та інші периферійні пристрої, вимкнути системний блок. При наявності пристрою безперебійного живлення (ПБЖ) вимкнути його живлення.
- Вимкнути ПК кнопкою «POWER" (ЖИВЛЕННЯ) та вийняти штепсельну вилку кабелю живлення з розетки
- Накрити клавіатуру кришкою для попередження попадання в неї пилу.
- Навести порядок на робочому місці.

Вимоги безпеки в аварійних ситуаціях.

- Якщо після ввімкнення ПК відчувається запах горілого або при доторканні до металевих частин ПК відчувається дія електричного струму, потрібно негайно відключити ПК від електромережі та повідомити про це своєму керівникові.
- У випадку виникнення пожежі негайно розпочати гасіння наявними засобами пожежогасіння і повідомити за телефоном 101 (міська пожежна охорона) та начальнику ДПД підприємства. Пам`ятайте, що загашувати електроустановки слід вуглекислотними вогнегасниками, сухим піском, щоб уникнути ураження електричним струмом.

У разі виникнення інших аварійних ситуацій слід припинити роботу і повідомити про це керівника робіт.

ВИСНОВОК ДО РОЗДІЛУ 4

На підставі виконаного розрахунку повітрообміну за надлишком тепла, значення якого 628 $м^3$/год, встановили механічну вентиляцію з вентилятором VORTICE VARIO, оскільки використання природної вентиляції є малоефективним. Механічна вентиляція здатна забезпечити виведення з проектного відділу температури 30℃ і підтримувати температуру повітря допустимого та навіть оптимального значення.

РОЗДІЛ 5
ОХОРОНА НАВКОЛИШНЬОГО СЕРЕДОВИЩА

На сьогоднішній день радіотехнічне та електронне виробництво є досить розвинутим і без нього суспільство не уявляє свого життя. Електронна і радіотехнічна промисловість грає провідну роль в науково-технічній революції. Впровадження електронних приладів в різні сфери людської діяльності значною мірою сприяє успішній розробці складних науково-технічних проблем, підвищенню продуктивності фізичної і розумової праці, поліпшенню економічних показників виробництва.

В кваліфікаційній роботі розроблена система захисту з використанням серверного обладнання, що може здійснювати негативний вплив на навколишнє середовище.

5.1. Аналіз впливу техногенних чинників

Широке використання електричного та електронного обладнання дозволило не тільки підвищити якість життя людей, але й призвело до негативних наслідків для навколишнього середовища та здоров’я людини. Можна виділити основні шкідливі та небезпечні чинники, які впливають на навколишнє середовище [42]:

- шумове забруднення;
- вібраційне забруднення;
- електромагнітне забруднення
- теплове забруднення
- радіаційне забруднення

Шумове забруднення. У сучасному світі в умовах науково-технічного прогресу шум став однією з форм фізичного (хвильового) забруднення природного середовища. Шумом прийнято вважати усі неприємні та небажані звуки або їх сукупність, які заважають нормально працювати, сприймати потрібну звукову інформацію та відпочивати.

Адаптація до нього практично неможлива. Фоновий рівень шуму навколишнього середовища становить 30-60 децибел. До цього природного фону за сучасних умов додаються виробничі й транспортні шуми, рівень яких нерідко перевищує 100 децибел. Джерелами шуму є: промислові об'єкти, транспорт, гучномовні пристрої, телевізори, радіоприймачі, музичні інструменти, юрби людей тощо. Шум у виробничих умовах негативно впливає на працівника: послаблює увагу, посилює розвиток втоми, сповільнює реакцію на небезпеку. Внаслідок цього знижується працездатність та підвищується ймовірність нещасних випадків. Допустимі рівні звукового тиску в октавних смугах частот на робочих місцях у виробничих приміщеннях наведені в таблиці 5.1 [42]:

Таблиця 5.1

Допустимі рівні звукового тиску в октавних смугах частот

Рівні звукового тиску в дБ, в октавних смугах частот, Гц								
31,5	63	125	250	500	1000	2000	4000	8000
107	95	87	82	78	75	73	71	69

Встановлено, що рослини під впливом шуму знижують енергію до зростання, у них спостерігається надмірне (навіть повне, що призводить до загибелі) виділення вологи через листя, можливі порушення у клітинах. Гинуть листя і квіти рослин, які розташовані близько до джерела інтенсивного шуму (звуку). Відсутність шуму особливо необхідний для тварин, які обмінюються звуковою інформацією, а також аналізуючи звуки навколишнього середовища з метою покращання отримання інформації, в тому числі сигналів тривоги. Аналогічно діє шум на тварин. Від шуму реактивного літака гинуть личинки бджіл, самі

вони втрачають здатність орієнтуватися, у пташиних гніздах дає тріщини шкаралупа яєць. Від коливань повітря, які утворюються звуками переносної радіоапаратури, не можуть піднятися у повітря жуки, джмелі та інші комахи.

Вібраційне забруднення. Вібрація – це механічні коливання твердого тіла. Вібрацію поділяють на природну та штучну. Джерелами природної вібрації є землетруси, що викликаються природними чинниками. Джерелами штучної вібрації є промисло-

вість, транспорт. Тривалі вібрації завдають великої шкоди здоров'ю людини – від сильної втоми до змін багатьох функцій організму: порушення серцевої діяльності, нервової системи, спазмів судин, деформації м'язів, струсу головного мозку тощо. Особливо небезпечна вібрація з частотою, яка є резонансною з частотою коливання окремих органів чи частин тіла людини, що може призвести до їх пошкодження. Тривала дія вібрації може спричинити професійне захворювання – вібраційну хворобу [42].

Електромагнітне забруднення. У процесі еволюції біосфера постійно знаходилася і знаходиться під впливом електромагнітного поля (ЕМП) природного походження (природний фон): електричного й магнітного поля Землі, космічного електромагнітного випромінювання, насамперед того, що генерується Сонцем. У період науково-технічного прогресу людство створювало і дедалі ширше використовувало штучні (антропогенні) джерела ЕМП. У наш час ЕМП антропогенного походження значно перевищують природний фон і є тим несприятливим чинником, вплив якого на людину та довкілля рік за роком зростає. Ступінь впливу ЕМП на організм людини залежить від діапазону частот, інтенсивності та тривалості дії, характеру випромінювання (неперервного чи модульованого), режиму опромінювання, розміру поверхні тіла, що зазнає опромінювання, індивідуальних особливостей організму. Електромагнітні поля можуть викликати біологічні та функціональні порушення у функціонуванні організму. Функціональні ефекти проявляються у передчасній втомлюваності, частих болях голови, погіршенні сну, порушенні функцій серцево-судинної та центральної нервової систем. Тривалий та інтенсивний вплив ЕМП призводить до стійких порушень та захворювань. Біологічні негативні ефекти впливу ЕМП проявляються у тепловій та нетепловій діях. Теплова дія призводить до підвищення температури тіла та місцевого вибіркового нагрівання органів і тканин організму внаслідок переходу електромагнітної енергії в теплову. Таке нагрівання особливо небезпечне для органів із слабкою терморегуляцією (головний мозок, очі, нирки, шлунок тощо). Наприклад, випромінювання сантиметрового діапазону призводить до появи катаракти, тобто до поступової втрати зору [42].

Теплове забруднення. Теплове забруднення – це результат розсіювання в навколишнє середовище теплоти, яка виділяється у багаточисельних теплових процесах,

насамперед пов’язаних зі згоранням палива. Під час згорання палива щорічно витрачається до 23% кисню, що утворюється в процесі фотосинтезу на Землі за рік. За підрахунками під час спалювання вугілля в навколишнє середовище викидається радіоактивних компонентів більше, ніж за той самий час на всіх атомних електростанціях у разі безаварійної роботи. Теплове забруднення гідросфери відбувається переважно внаслідок скидання у водойми підігрітих вод від ТЕС, АЕС та інших енергетичних об’єктів. Тепла вода змінює термічні та біологічні режими водойм і шкідливо впливає на їхніх мешканців [42].

5.2. Вплив приймальних пристроїв на навколишнє середовище

Абонентський приймач – телевізійний приймач (приставка), пристрій, що приймає сигнал цифрового телебачення, декодує його і перетворює в аналоговий сигнал для виведення через роз'єми RCA або SCART або перетворює в цифровий сигнал для виведення через роз'єм HDMI , і передає його далі на телевізор.

Перехід до цифрового телебачення призвів до зростання виробництва цифрових абонентських приймачів, що в свою чергу може негативно впливати на навколишнє середовище. Приймач продукує слабкі електричні і магнітні змінні поля в широкому діапазоні частот. Проте проблема впливу електромагнітних випромінювань, що продукуються заслуговує на особливу увагу. Наукові дослідження показали, що ЕМВ мають у своєму складі чинник, котрий впливає на користувачів при наявності сучасних екранів від ЕМВ. Вчені України ідентифікували цей чинник як торсіонові поля, котрі супроводжують будь-яке електромагнітне випромінювання та являються його інформаційною компонентою [45]. Робоча група Всесвітньої організації охорони здоров’я з гігієнічних аспектів користування моніторами та радіо терміналами виявили порушення стану здоров’я при користуванні пристроями, які мають електромагнітне випромінювання, найсерйозніші з яких:

- погіршення зору;
- порушення імунної системи;
- порушення психоемоційної сфери (стресовий синдром, агресивність)

Для забезпечення безпеки здоров'я користувачів в Україні діють Державні санітарні норми і правила при роботі з джерелами електромагнітних полів «ДСанПіН 3.3.6.096-2002». Значення ГДР напруженості електричної ($Е_{гд}$) і магнітної ($Н_{гд}$) складових залежно від тривалості їх дії наведені в таблиці 5.2.

Таблиця 5.2

Значення ГДР напруженості електричної ($Е_{гд}$) і магнітної ($Н_{гд}$) складових

Час перебування персоналу, год	$Е_{гд}$, В/м					$Н_{гд}$, А/м			
	1-10 кГц	10-60 кГц	0,063 МГц	3-30 МГц	30-300 МГц	1-10 кГц	10-60 кГц	0,06-3 МГц	30-50 МГц
8	120	70	50	30	10	9	7	5	0,3
7	130	75	53	32	11	9,8	7,5	5,3	0,32
6	140	82	58	34	12	10,6	8,1	5,8	0,34
5	155	90	63	37	13	11,6	8,8	6,3	0,38
4	175	110	71	42	14	13	9,9	7,1	0,42
3	200	115	82	48	16	15	11,4	8,2	0,49
2	250	140	100	59	20	18,4	14	10	0,6
1	350	200	141	84	28	26	19,7	14,2	0,85
0,5	500	280	200	118	40	37,6	27,9	20	1,2

У результаті дії на організм людини електромагнітних випромінювань в діапазоні 30 кГц - 300 МГц (НЧ) спостерігається: загальна слабкість, підвищена втома, сонливість, порушення сну, головний біль та біль в ділянці серця. З'являється роздратованість, втрачається увага, сповільнюються рухово-мовні реакції. Виникає ряд симптомів, які свідчать про порушення роботи окремих органів - шлунку, печінки, підшлункової залози.

Для того, щоб зменшити рівень електромагнітного випромінювання потрібно обмежити безперервний час роботи абонентського приймача [43-46].

В Україні норми електромагнітної безпеки регламентуються Державними санітарними нормами і правилами захисту населення від впливу електромагнітного випромінювання, згідно з якими допустимі рівні інтенсивності електромагнітного випромінювання для цивільного населення становлять 2,5 мкВт/см^2.

Абонентський приймач під час роботи створює шум, рівень якого становить 54 дБ. Допустимий рівень звукового тиску повинний відповідати «ДСН 3.3.6.037-99 Санітарні норми виробничого шуму, ультразвуку та інфразвуку», а саме 50 дБ.

Велика кількість звукових сигналів, що поступають до кори головного мозку, викликають переживання, страх, передчасну втому. Дія шуму на людину виражається в широкому діапазоні - від суб'єктивного роздратування до об'єктивних змін в ЦНС, органах слуху, серцево-судинних та ендокринній системах, травному акті та інших органів і систем. Першим показником шкідливої дії шуму є скарги на роздратованість, переживання, порушення сну [45].

5.3. Засоби для захисту від електромагнітного випромінювання та шуму, проблема електронних відходів

Захист від електромагнітного випромінювання. Для зменшення впливу ЕМП на персонал та населення, яке знаходиться у зоні дії радіоелектронних засобів, потрібно вжити ряд захисних заходів. До їх числа можуть входити організаційні, інженерно-технічні та лікарсько-профілактичні.

До заходів щодо зменшення впливу на працівників ЕМП належать: організаційні, інженерно-технічні та лікарсько-профілактичні.

Організаційні заходи здійснюють органи санітарного нагляду. Вони проводять санітарний нагляд за об'єктами, в яких використовуються джерела електромагнітних випромінювань.

Інженерно-технічні заходи передбачають таке розташування джерел ЕМП, яке б зводило до мінімуму їх вплив на працюючих, використання в умовах виробництва дистанційного керування апаратурою, що є джерелом випромінювання, екранування джерел випромінювання, застосування засобів індивідуального захисту (халатів, комбінезонів із металізованої тканини, з виводом на заземлюючий пристрій). Для захисту очей доцільно використовувати захисні окуляри ЗП5-90. Скло окулярів вкрито напівпровідниковим оловом, що послаблює інтенсивність електромагнітної енергії при світлопропусканні не нижче 75%.

Взагалі, засоби індивідуального захисту необхідно використовувати лише тоді, коли інші захисні засоби неможливі чи недостатньо ефективні: при проходженні через зони опромінення підвищеної інтенсивності, при ремонтних і налагоджувальних роботах в аварійних ситуаціях, під час короткочасного контролю та при зміні інтенсивності опромінення. Такі засоби незручні в експлуатації, обмежують можливість виконання трудових операцій, погіршують гігієнічні умови.

У радіочастотному діапазоні засоби індивідуального захисту працюють за принципом екранування людини з використанням відбиття і поглинання ЕМП. Для захисту тіла використовується одяг з металізованих тканин і рідіопоглинаючих матеріалів. Металізовану тканину роблять із бавовняних ниток з розміщеним всередині них тонким проводом, або з бавовняних чи капронових ниток, спірально обвитих металевим дротом. Така тканина, наче металева сітка, при відстані між нитками до 0,5 мм значно послаблює дію випромінювання. При зшиванні деталей захисного одягу треба забезпечити контакт ізольованих проводів. Тому електрогерметизацію швів здійснюють електропровідними масами чи клеями, які забезпечують гальванічний контакт або збільшують ємнісний зв'язок безконтактних проводів.

Лікарсько-профілактичні заходи передбачають проведення систематичних медичних оглядів працівників, які перебувають у зоні дії ЕМП, обмеження в часі перебування людей в зоні підвищеної інтенсивності електромагнітних випромінювань, видачу працюючим безкоштовного лікарсько-профілактичного харчування, перерви санітарно-оздоровчого характеру.

Захист від шуму. Для зменшення і ліквідації шуму застосовується цілий комплекс заходів, що називається шумозахистом. Це застосування звукопоглинаючих матеріалів, раціональне розміщення будівельних об'єктів, створення вздовж вулиць екранів у вигляді земляних валів, стін різних конструкцій, шумовідбиваючих, як правило не житлових будівель - магазинів, складів, гаражів.

Проблема електронних відходів. Згідно Закону України «Про відходи» з метою запобігання або зменшення обсягів утворення відходів потрібно здійснювати системи збирання та утилізації електричного та електронного обладнання [30]. Вирішення проблеми електронних відходів в Україні мав би забезпечити «Технічний регламент з поводження з

відходами електричного та електронного обладнання», розробка якого в Україні здійснюється з 2008 року. Згідно з проектами цих законодавчих актів імпортери і виробники можуть як самостійно утилізувати електровідходи, так і підписувати договори на виконання робіт з організації збирання, заготівлі та утилізації відповідних видів техніки з уповноваженими підприємствами. Розроблено також проект Постанови Кабінету Міністрів України «Про затвердження Технічного регламенту з поводження з відходами електронного та електричного устаткування». Цим регламентом передбачається створення пунктів збору відходів електронного та електричного обладнання, які повинні розташовуватися у місцях, зручних для користувачів, та забезпечувати безоплатність послуг, що надаються цими пунктами для користувачів. Наразі обговорюється ще один варіант вирішення проблеми, а саме проект внесення змін до Податкового Кодексу, в якому передбачає централізоване стягнення коштів з імпортерів та виробників різних споживчих товарів з метою забезпечення за рахунок цих коштів належної організації збирання, заготівлі та утилізації відходів від зазначених товарів.

Однак, загалом проблему електронних відходів в Україні необхідно вирішити як в організаційно-правовому аспекті – створення фондів виробників, підтримка держави підприємств з утилізації відходів, так і в соціально-інформаційному: українців треба переконати в тому, що виносити на звичайний смітник поламаний електронний пристрій – не можна.

ВИСНОВОК ДО РОЗДІЛУ 5

Телекомунікаційні ресурси створюють негативний вплив на навколишнє середовище. Вони є джерелами електромагнітного випромінювання та шумового забруднення. Для мінімізації ризику виникнення захворювань, ефективними є інженерно-технічні заходи, які зменшать дію шкідливих чинників. Також були розглянута проблема електронних відходів, одним зі шляхом вирішення якої є створення пунктів збору відходів електронного та електричного обладнання.

ВИСНОВКИ

У цій кваліфікаційній роботі проводилося проєктування та оптимізація захищеної інтрамережі за допомогою Eve-NG на платформі Windows 11 Professinal. У першій частині проводився теоретичний огляд підходу побудови захищеної мережі.

У ході огляду були розглянуті теми: топології мережі, основні положення у проєктуванні мережі, життєвий цикл системи, аксіоми безпеки, захист мережевої інфраструктури. При проєктуванні мережі були розглянуті найкращі практики, описані в другому розділі. У другій частині проведено розгортання віртуальної лабораторії eve-ng на Windows 11 Professinal. У ході розробки основними компонентами були маршрутизатори, комутатори, CISCOASA. Як захисні заходи використовувалися: VLAN, ACL-листи, парольний захист, GRE-тунель, IPSEC шифрування. Для підвищення стійкості до відмов мережного модуля на CISCOASA був налаштований FAILOVER. Для можливості у випадку виникнення надзвичайної ситуації надсилання даних на резервну CISCOASA готову до роботи. Передостання частина роботи була присвячена безпеці життєдіяльності. Спочатку було проведено аналіз умов праці співробітників офісу. До якого входили норми щодо створення мікроклімату офісних приміщень та допустимого рівня шуму Фінальні значення отримані у розрахунках повністю задовольняють встановлені норми безпеки. Також проведено аналіз та оцінку ризиків. Оцінка ризиків відбувається за двома параметрами. Активами є: маршрутизатор, комутатор, DMZ, Server, PC, CISCOASA. Спочатку ми з'ясували, що можливі ризики для цих активів є неприйнятними. Після цього ми ввели захисні заходи і здійснили розрахунки повторно. Введення захисних заходів дозволило знизити ризики та перевести ризики до категорії прийнятних. На завершення кваліфікаційної роботи ми маємо розроблений модуль захищеної мережі, розрахований на впровадження у компанії середнього та малого бізнесу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. J. M. Rabaey, "Human-centric computing", IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 28, no. 1, pp. 3-11, Dec. 2019.
2. S. Sen, S. Maity and D. Das, "The body is the network: To safeguard sensitive data turn flesh and tissue into a secure wireless channel", IEEE Spectr., vol. 57, no. 12, pp. 44-49, Dec. 2020.
3. F. Solt et al., "Energy efficient heartbeat-based MAC protocol for WBAN employing body coupled communication", IEEE Access, vol. 8, pp. 182966-182983, 2020.
4. X. Chen et al., " Analysis and design of an ultra-low-power Bluetooth low-energy transmitter with ring oscillator-based ADPLL and frequency edge combiner ", IEEE J. Solid-State Circuits, vol. 54, no. 5, pp. 1339-1350, Feb. 2019.
5. G. de Streel et al., "SleepTalker: A ULV 802.15.4a IR-UWB transmitter SoC in 28-nm FDSOI achieving 14 pJ/b at 27 Mb/s with channel selection based on adaptive FBB and digitally programmable pulse shaping", IEEE J. Solid-State Circuits, vol. 52, no. 4, pp. 1163-1177, Apr. 2017.
6. Y.-J. Lin, S.-Y. Park, X. Chen, D. Wentzloff and E. Yoon, "4.32-pJ/b overlap-free feedforward edge-combiner-based ultra-wideband transmitter for high-channel-count neural recording", IEEE Microw. Wireless Compon. Lett., vol. 28, no. 1, pp. 52-54, Jan. 2017.
7. Y. Park and D. D. Wentzloff, "An all-digital 12 pJ/pulse IR-UWB transmitter synthesized from a standard cell library", IEEE J. Solid-State Circuits, vol. 46, no. 5, pp. 1147-1157, May 2021.
8. P. P. Mercier, D. C. Daly and A. P. Chandrakasan, "An energy-efficient all-digital UWB transmitter employing dual capacitively-coupled pulse-shaping drivers", IEEE J. Solid-State Circuits, vol. 44, no. 6, pp. 1679-1688, Jun. 2019.
9. T. Bos, W. Dehaene and M. Verhelst, "Ultrasound in-body communication with OFDM through multipath realistic channels", Proc. IEEE Biomed. Circuits Syst. Conf. (BioCAS), pp. 1-4, Oct. 2019.

10. J. Yoo, "Body coupled communication: Towards energy-efficient body area network applications", Proc. IEEE Int. Symp. Radio-Frequency Integr. Technol. (RFIT), pp. 244-246, Aug. 2017.

11. J. Park and P. P. Mercier, "Magnetic human body communication", Proc. 37th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. (EMBC), pp. 1841-1844, Aug. 2017.

12. J. Park and P. P. Mercier, "A Sub-10-pJ/bit 5-Mb/s magnetic human body communication transceiver", IEEE J. Solid-State Circuits, vol. 54, no. 11, pp. 3031-3042, Nov. 2019.

13. M. A. Callejon, D. Naranjo-Hernandez, J. Reina-Tosina and L. M. Roa, "Distributed circuit modeling of galvanic and capacitive coupling for intrabody communication", IEEE Trans. Biomed. Eng., vol. 59, no. 11, pp. 3263-3269, Nov. 2019.

14. J. Bae, H. Cho, K. Song, H. Lee and H.-J. Yoo, "The signal transmission mechanism on the surface of human body for body channel communication", IEEE Trans. Microw. Theory Techn., vol. 60, no. 3, pp. 582-593, Mar. 2019.

15. A. Thielens et al., "A comparative study of on-body radio-frequency links in the 420 MHz–2.4 GHz range", Sensors, vol. 18, no. 12, pp. 4165, Nov. 2018.

16. R. Benarrouch, A. Thielens, A. Cathelin, A. Frappé, A. Kaiser and J. Rabaey, "Capacitive body-coupled communication in the 400–500 MHz frequency band", Proc. EAI Int. Conf. Body Area Netw., pp. 218-235, 2019.

17. S. Maity, B. Chatterjee, G. Chang and S. Sen, "BodyWire: A 6.3-pJ/b 30-Mb/s −30-dB SIR-tolerant broadband interference-robust human body communication transceiver using time domain interference rejection", IEEE J. Solid-State Circuits, vol. 54, no. 10, pp. 2892-2906, Oct. 2019.

18. W. Saadeh, M. A. B. Altaf, H. Alsuradi and J. Yoo, "A 1.1-mW ground effect-resilient body-coupled communication transceiver with pseudo OFDM for head and body area network", IEEE J. Solid-State, vol. 52, no. 10, pp. 2690-2702, Oct. 2017.

19. J. Jang et al., "4-camera VGA-resolution capsule endoscope with 80 Mb/s body-channel communication transceiver and sub-cm range capsule localization", IEEE ISSCC Dig. Tech. Papers, pp. 282-284, Feb. 2018.

20. B. Chatterjee, A. Srivastava, D.-H. Seo, D. Yang and S. Sen, "A context-aware reconfigurable transmitter with 2.24 pJ/bit 802.15.6 NB-HBC and 4.93 pJ/bit 400.9 MHz MedRadio modes with 33.6% transmit efficiency", Proc. IEEE Radio Freq. Integr. Circuits Symp. (RFIC), pp. 75-78, Aug. 2020.

21. B. Zhao, Y. Lian, A. M. Niknejad and C. H. Heng, "A low-power compact IEEE 802.15. 6 compatible human body communication transceiver with digital sigma–delta IIR mask shaping", IEEE J. Solid-State Circuits, vol. 54, no. 2, pp. 346-357, Nov. 2018.

22. IEEE Standard for Local and Metropolitan Area Networks—Part 15.6: Wireless Body Area Networks, pp. 1-271, 2012.

23. D. Marchaland, M. Villegas, G. Baudoin, C. Tinella and D. Belot, "System concepts dedicated to UWB transmitter", Proc. Eur. Conf. Wireless Technol., pp. 141-144, Oct. 2005.

24. S. Clerc, T. Di Gilio and A. Cathelin, The Fourth Terminal: Benefits of Body-Biasing Techniques for FDSOI Circuits and Systems, Cham, Switzerland:Springer, 2020.

25. M. Blagojevic, M. Cochet, B. Keller, P. Flatresse, A. Vladimirescu and B. Nikolic, "A fast flexible positive and negative adaptive body-bias generator in 28 nm FDSOI", Proc. IEEE Symp. VLSI Circuits (VLSI-Circuits), pp. 1-2, Jun. 2016.

26. D. Gaidioz, M. De Matos, A. Cathelin and Y. Deval, "Ring VCO phase noise optimization by pseudo-differential architecture in 28nm FD-SOI CMOS", Proc. IEEE Int. Symp. Circuits Syst. (ISCAS), pp. 1-4, Oct. 2020.

27. J. A. McNeill, "Jitter in ring oscillators", IEEE J. Solid-State Circuits, vol. 32, no. 6, pp. 870-879, Jun. 2017.

28. G. Tochou, A. Cathelin, A. Frappe, A. Kaiser and J. Rabaey, "Impact of forward body-biasing on ultra-low voltage switched-capacitor RF power amplifier in 28 nm FD-SOI", IEEE Trans. Circuits Syst. II Exp. Briefs, vol. 69, no. 1, pp. 50-54, Jan. 2022.

29. G. Tochou, RFIC Industry Showcase—IMS 2021, Jun. 2021, [online] Available: https://ieeetv.ieee.org/channels/mtts/guillaume-tochou-rfic-industry-showcase-ims-2021.

30. J. M. Rabaey, A. C. Arias and R. Muller, "Architecting the human intranet", Proc. IEEE 47th Eur. Solid State Circuits Conf. (ESSCIRC), pp. 15-20, Sep. 2021.

31. НПАОП 0.00-1.28-10 Правила охорони праці під час експлуатації електронно-обчислювальних машин.

32. ДСН 3.3.6.037-99 «Санітарні норми виробничого шуму, ультразвуку та інфразвуку».

33. Державні санітарні норми та правила «Гігієнічна класифікація праці за показниками шкідливості та небезпечності факторів виробничого середовища, важкості та напруженості трудового процесу».

34. «ДСН 3.3.6.042-99 Санітарних норми мікроклімату виробничих приміщень».

35. ДБН 13.2.5-28-2006 «Природне і штучне освітлення».

36. ДСН 3.3.6.037-99 «Санітарні норми виробничого шуму, ультразвуку та інфразвуку».

37. ДСТУ 12.1.005-88 «ССБП. Загальні санітарно-гігієнічні вимоги до повітря робочої зони».

38. ДБН В.2.5-28-2006 «Інженерне обладнання будинків і споруд. Природне і штучне освітлення».

39. ДСТУ Б В.2.5-82:2016 «Електробезпека в будівлях і спорудах. Вимоги до захисних заходів від ураження електричним струмом».

40. ДСТУ 8604:2015 «Дизайн і ергономіка. Робоче місце для виконання робіт у положенні сидячи. Загальні ергономічні вимоги».

41. НАПБ Б.03.002-2007 «Норми визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпекою».

42. Прогнозування екологічних ризиків з використанням аналізу ієрархів та теорії нечітких множин: міжнародна науково-практична конференція «І-й всеукраїнський з'їзд екологів»: Тези доповідей. Україна, м. Вінниця, 4-7 жовтня 2016. – 2016. – С.25.

43. Клап Я. А., Яремкевич О. С., Червецова В. Г., Заярнюк Н. Л., Новіков В. П., Дослідження впливу електромагнітних, постійних магнітних та акустичних полів

на організм людини // Вісник Нац. ун-ту “Львівська політехніка”. – 2016 – № 812. – С. 365–372.

44. Сучасний стан досліджень впливу електромагнітних випромінювань на організм людини [Електронний ресурс]/[А. П. Чорний, В. В. Никифоров, Д. І. Родькін, В. Ю. Ноженко] // Інженерні та освітні технології в електротехнічних та комп'ютерних системах: щоквартальний науково-практичний журнал. – Кременчук: КрНУ, 2013.

45. Екологія та охорона навколишнього природного середовища: навч. посібник для вузів / В. С. Джигирей. - 6-те вид., випр. і доп. - К. : Знання, 2017. - 422 с.

46. Боротьба з шумом на виробництві: Довідник / Під ред. О. Я. Юдіна. – М: Машинобудування, 2015. – 297 с.