Вінницький національний технічний університет
(повне найменування вищого навчального закладу)

Факультет інформаційних технологій та комп'ютерної інженерії
(повне найменування інституту)

Кафедра обчислювальної техніки
(повна назва кафедри)

Пояснювальна записка

до магістерської кваліфікаційної роботи
магістр
(освітньо-кваліфікаційний рівень)

на тему: Методи та засоби безпечного передавання даних в корпоративних мережах

Виконав: студент 2 курсу, групи 2КІ – 18м
спеціальності:
123 «Комп'ютерна інженерія»
(шифр і назва напряму підготовки)

Куцак Ю.В.
(прізвище та ініціали)

Керівник: к.т.н., доц.Войцеховська О.В.
(прізвище та ініціали)

Рецензент: к.т.н, доц. Карпінець В.В.
(прізвище та ініціали)

Вінницький національний технічний університет
(повненайменування вищого навчального закладу)

Факультетінформаційних технологій та комп'ютерної інженерії

Кафедра: Обчислювальної техніки

Освітньо – кваліфікаційний рівень: магістр

Спеціальність: 123 «Комп'ютерна інженерія»

(шифр і назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри_____
д.т.н., проф. Мартинюк Т.Б._____
__ “2” вересня 2019 року

З А В Д А Н Н Я

НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУРОБОТУ СТУДЕНТУ

Куцак Юлії Віталіївні
(прізвище, ім’я, по-батькові)

1. Тема роботи: Методи та засоби безпечного передавання даних в корпоративних мережах
Керівник роботи: Войцеховська Олена Валеріївна, к. т. н., доцент кафедри ОТ
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом вищого навчального закладу від “ 02” жовтня 2019 року № 254
2. Строк подання студентом роботи « 10 » грудня 2019 року
3. Вихідні дані до роботи: список технічної літератури, основні вимоги до проектування захищеної корпоративної мережі, вимоги до активного мережевого обладнання, технічне завдання на магістерську роботу
4. Зміст пояснювальної записки: сучасний стан питання галузі розвитку та захисту корпоративних мереж, комплексний метод захисту мережі на базі обладнання CISCO, проектування захищеної корпоративної мережі.
5. Перелік графічного матеріалу (з точним зазначенням обов’язкових креслень):
узагальнена схема функціональних компонентів корпоративної мережі, узагальнена схема багаторівневого інтегрованого захисту, схема аутентифікації в спрощеному вигляді, схема мережі центрального офісу, схема мережі віддаленого офісу, схема мережі центра обробки даних, адресна схема мережі компанії «ITSosed», загальна схема мережі «ITSosed».

АНОТАЦІЯ

Дана магістерська кваліфікаційна робота присвячена методам та засобам безпечного передавання даних в корпоративних мережах використовуючи обладнання CISCO. В роботі проаналізовано класифікацію видів корпоративних мереж, існуючих сучасних методів та засобів захисту мереж різного типу, здійснено порівняльну характеристику мережевого обладнання CISCO з іншими конкуруючими компаніями.

Розглянуто методи захисту локальної мережі, мережі кордонів та безпечної передачі даних в корпоративних мережах. Вдосконалено комплексний метод захисту мережі, що являє собою багаторівневий інтегрований захист.

Спроектовано захищену корпоративну мережу для підприємства в який використано комплексний метод.

ANNOTATION

This master's qualification is dedicated to methods and means of secure data transmission in corporate networks using CISCO equipment. The classification of types of corporate networks, existing modern methods and means of protection of networks of different types is analyzed in the work, comparative characteristic of CISCO network equipment with other competing companies is made.

The methods of protection of local area network, border network and secure data transmission in corporate networks are considered. An integrated method of network security, which is a multi-level integrated security, has been improved.

A secure corporate network has been designed for the enterprise using the integrated method.

ВСТУП

Актуальність теми дослідження – в сучасному світі високих технологій великої популярності продовжують набувати різні типи комп'ютерних мереж, а саме: локальні, глобальні та корпоративні. Передача даних по комп'ютерній мережі піднімає питання захисту інформації, що є невід'ємною частиною будь-якої системи, яка працює з комерційно цінною інформацією. Світовим лідером захисту та надійності корпоративних мереж під час використання Internet, з'єднання частин компаній і організацій, обмеження доступу зовнішніх користувачів до внутрішніх мереж є виробник мережевого обладнання CISCO. Методів захисту, які використовуються в наш, час велика кількість, але для того, щоб уникнути несанкціонованого доступу до конфіденційної інформації або мінімізувати ризик успішних атак, необхідно знайти найефективніший варіант поєднання цих методів.

Чільним напрямком у захисті корпоративних мереж, що перешкоджає порушенням безпеки системи обробки даних є відсутність регламентування правил використання, обробки і передачі інформації обмеженого доступу, що знижує ефективність комплексних систем захисту комп'ютерних мереж.

Проте, вибір методів захисту для мереж різного призначення та з різними вимогами щодо захисту інформації залишаються незмінними, а це говорить про те, що аналіз методів та технологій захисту на різних рівнях моделі OSI, є актуальною прикладною задачею.

Незважаючи на значну кількість розроблених та впроваджених методів захисту корпоративних мереж, невирішеними досі залишаються задачі ефективної протидії зовнішнім порушенням інформаційної безпеки.

Таким чином, в умовах постійного розширення кола користувачів, що мають безпосередній доступ до обчислювальних ресурсів і масивів даних актуальним є завдання розроблення комплексного підходу для створення захищеного середовища обробки інформації в корпоративних системах.

Дієвим засобом захисту мереж є комплексний підхід, який протистояв би різним видам інформаційних загроз, враховував би програмно-апаратні та організаційні методи захисту мереж, зокрема й інформаційні технології та засоби захисту мереж на базі обладнання Cisco System.

Метою роботи є підвищення рівня захисту корпоративної мережі шляхом вдосконалення методу захисту мережі за рахунок використання комбінацій кількох технологій на базі обладння Cisco System.

Для досягнення поставленої мети потрібно виконати такі **задачі**:

- виконати аналіз та дослідження найсучасніших методів та засобів захисту інформації в корпоративних мережах;
- проаналізувати архітектуру сучасних комп'ютерних мереж, засоби захисту мереж на основі обладнання Cisco та здійснити порівняння з іншими конкуруючими компаніями;
- дослідити раціональність використання методів захисту зовнішніх загроз та від загроз з середитини мережі в різних умовах їх виникнення;
- удосконалити комплексний метод захисту мережі за рахунок комбінацій кількох технологій захист як від зовнішніх так і від внутрішніх загроз;
- розробити захищену корпоративну мережу на прикладі компанії «ITSosed»

Отже, задача створення захищеної мережі підприємства має вагомий прикладний характер. Її розв'язання передбачає врахування великої кількості параметрів та варіацій.

Тема магістерської кваліфікаційної роботи є актуальною, оскільки завжди є потреба у проектування та підтримці захищених мереж на підприємствах. Даний метод буде корисним в будь-яких установах, як державних так і приватних, головним чином якщо їх діяльність пов'язана із IT-індустрією, що передбачає використання глобальних мереж.

Об'єкт дослідження – процеси передачі даних у захищених корпоративних мережах.

Предмет дослідження – методи і засоби захисту корпоративних мереж.

Методи дослідження – для досягнення поставленої в роботі мети використовуються такі методи: теорія обчислювальних систем та мереж, методи системного аналізу для дослідження функціонування програмно-апаратних засобів захищеної корпоративної мережі; методи натурного моделювання, для верифікації моделі захищщеної компютерної мережі.

Наукова новизна одержаних результатів:

- проведено аналітичний огляд методів та засобів захисту корпоративної мережі на базі обладнання Cisco System, що дає можливість подати підсумки досліджень в

оптимальному вигляді для вибору користувачем необхідного засобу захисту корпоративної;

- вдосконалено метод захисту корпоративної мережі, шляхом поєдання таких технологій захисту як, аутентифікація, створення безпечного периметру та утворення захищеного каналу передачі даних, що дало можливість забезпечити захист мережі одночасно як від внутрішніх так і від зовнішніх загроз.

Практичне значення одержаних результатів:

- запропоновано структурну схему багаторіневого інтегрованого захисту та комплексний метод захисту, що дозволяють планувати ефективні системи захисту конфіденційної інформації для різних корпоративних мереж, що підтверджено проведеними дослідженням та практичним застосування на конкретному підприємстві;
- розроблено рекомендації по вибору необхідних засобів захисту корпоративної мережі як від зовнішніх так і від внутрішниій загроз.

Апробація результатів дисертації – основні положеня магістерської кваліфікаційної роботи доповідалися та обговорювалися на таких конференціях: XIV міжнародна науково-практична інтернет-конференція «Інноваційні підходи до розвитку сучасної науки» назва публікації «Безпечна передача даних у корпоративній комп'ютерній мережі»; XLVIII Науково-технічна конференція факультету інформаційних технологій та комп'ютерної інженерії (2019 назва публікації «Методи та засоби захисту корпоративних мережах»); Всеукраїнська науково-практична Інтернет-конференція студентів, аспірантів та молодих науковців «Молодь в науці: дослідження, проблеми, перспективи-2019» назва публікації «Методи та засоби безпечної передачі даних в корпоративних мережах».

Результати виконаного магістерського дослідження впроваджені на підприємстві «ITSosed», про що свідчить акт впровадження. **1 СУЧАСНИЙ СТАН ПИТАННЯ ГАЛУЗІ РОЗВИТКУ ТА ЗАХИСТУ КОРПОРАТИВНИХ МЕРЕЖ**

Даний розділ диплому присвячений аналізу стану питання галузі розвитку та захисту корпоративних мереж. Детально розглянуто визначення та особливості корпоративних мереж їх класифікація та класифікаційні ознаки. Визначено основні організаційні, програмно-апаратні засоби захисту корпоративних мереж. Досліджено засоби захисту мереж на основі обладнання Cisco та здійснено порівняння з іншими конкуруючими компаніями.

ЗМІСТ

1.1 Загальні положення поняття та класифікація корпоративної мережі

Корпоративна мережа – система, яка забезпечує передачу інформації між різними додатками, використовуваними в системі корпорації. Корпоративною мережею вважається будь-яка мережа, що працює по протоколу TCP/IP і використовує комунікаційні стандарти Інтернету, а також сервісні додатки, що забезпечують доставку даних користувачам мережі [1].

Корпоративна мережа в загальному випадку утворює такі функціональні елементи:

1. Робочі місця (абоненти) корпорації, які можуть бути:
   – зосередженими, або розташовуватися в рамках будівлі;
   – розподіленими, або розосередженими на деякій, в загальному випадку, необмежено великій території.
2. Сервери, що зберігають інформацію корпорації, призначені для зберігання і обробки інформаційних масивів (баз даних) різного функціонального призначення. Вони також можуть бути зосередженими або розподіленими на великій території корпорації.

Засоби телекомунікації, які забезпечують взаємодію між собою робочих станцій та їх взаємодія з інформаційним серверами. Засоби телекомунікації в рамках корпорації можуть бути:

– виділеними (або орендованими), які є приналежністю корпорації;
– загального призначення (існуючі поза корпорацією мережі зв’язку).

У рамках компанії може бути реалізований інформаційний вплив у перших лініях (телефонія, телетекст, телетекст, факс); або кілька послуг (інтеграція послуг), щоб забезпечити відповідність кінцевих точок телекомунікацій та абонентів [3].

3. Система управління продуктивністю мережі підприємства. Залежно від наданих послуг корпоративна мережа повинна використовувати власні інструменти управління мережею. По можливості управління корпоративної мережі можна виділити такі елементи:
   - функціональні елементи, якими керує корпорація підприємства (це захищена або додатково запроваджена в корпоративних мережах функція підприємства);
   - функціональні елементи, такі як маршрутизатори та комутатори, якими не керує корпоративний корпус і є аксесуарами для універсальних абонентів компанії.
4. Система управління мережевою безпекою підприємства. Корпоративна мережа повинна впроваджувати необхідні сервіси мережевої безпеки та використовувати відповідні інструменти безпеки.
5. Система мережевої безпеки підприємства. Необхідно забезпечити засоби для забезпечення продуктивності всієї сітки або її фрагментів під час відповіді елементів групи.
6. Діагностична та контрольна система. Мережеві рамки підприємства повинні включати засоби для контролю продуктивності окремих функціональних елементів, систему збору інформації про помилки та збої та систему забезпечення життєздатності. Управління продуктивністю; Управління безпеки. Для підприємств мережі повинні бути розроблені засоби діагностики мережі, які реалізуються як в процесі роботи мережі, так і профілактично [4].
7. Операційна система. У перелічених функціональних елементах комунікаційні мережі підприємств повинні мати план процесу розвитку, який значною мірою визначає функції, які вони містять, особливо на рівні протоколів.

Узагальнюючи представлені ознаки корпоративних мереж, отримаємо можливу їх класифікацію:

- за набором функціональних елементів (рис. 1.1);

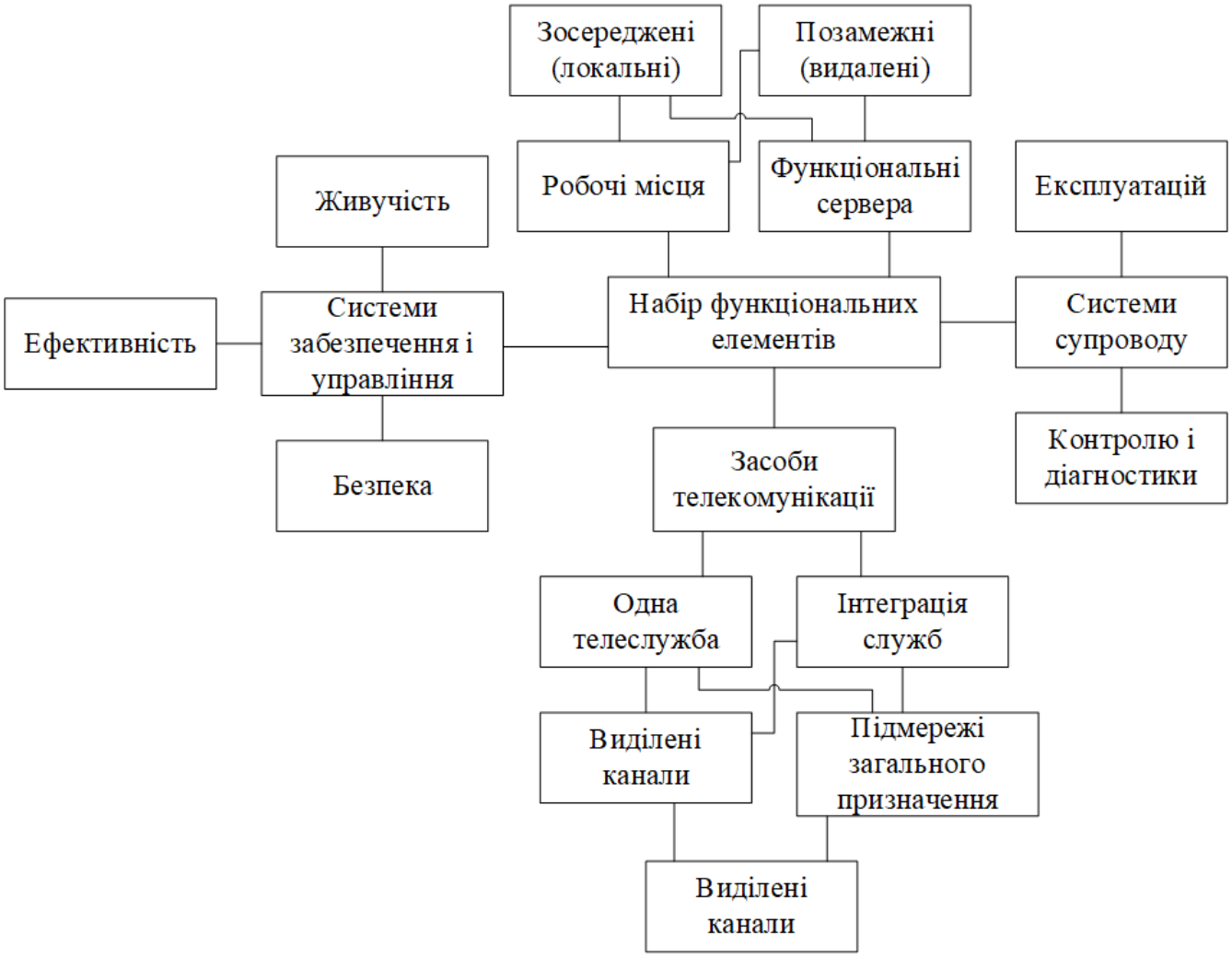


Рисунок 1.1 – Функціональні компоненти корпоративних мереж

– за ієрархією управління (рис. 1.2); у цьому випадку локальна підсистема означає функціональну підсистему, класифікація якої для системи управління безпекою показана на рисунку 1.3 і в якій сама функціональна підсистема показана на рисунку 1.4;
– за набори (за типом та кількістю) поєднуються в підмережах корпоративної мережі загальнодоступних підмереж;

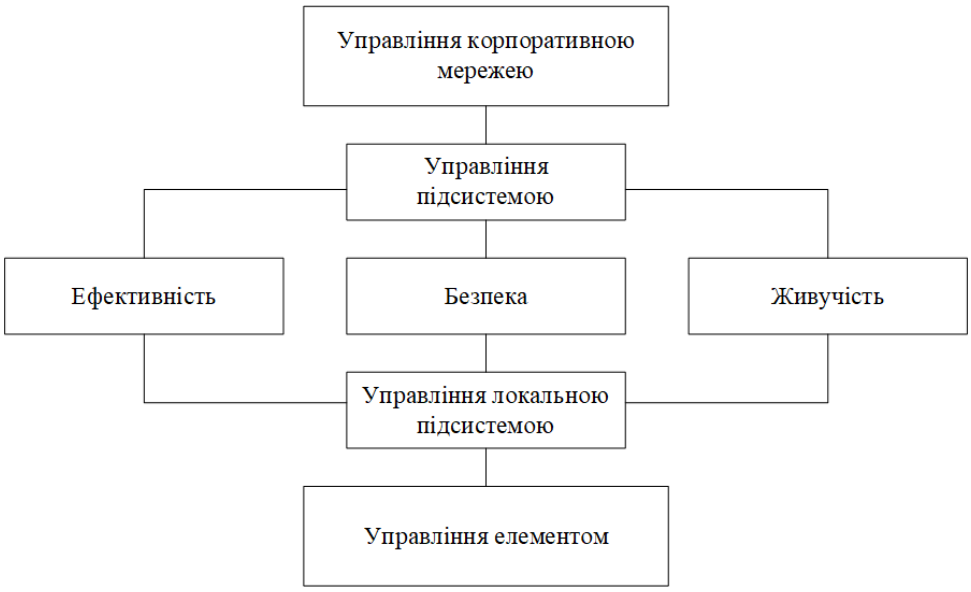


Рисунок 1.2 – Класифікація за ієрархією управління

Рисунок 1.3– Класифікація функціональних підсистем управління безпекою

Залежно від розміру підприємства та складності та різноманітності завдань, що вирішуються, розрізняють відомчі мережі, мережі кампусів та корпоративні мережі (тобто велика мережа підприємств).

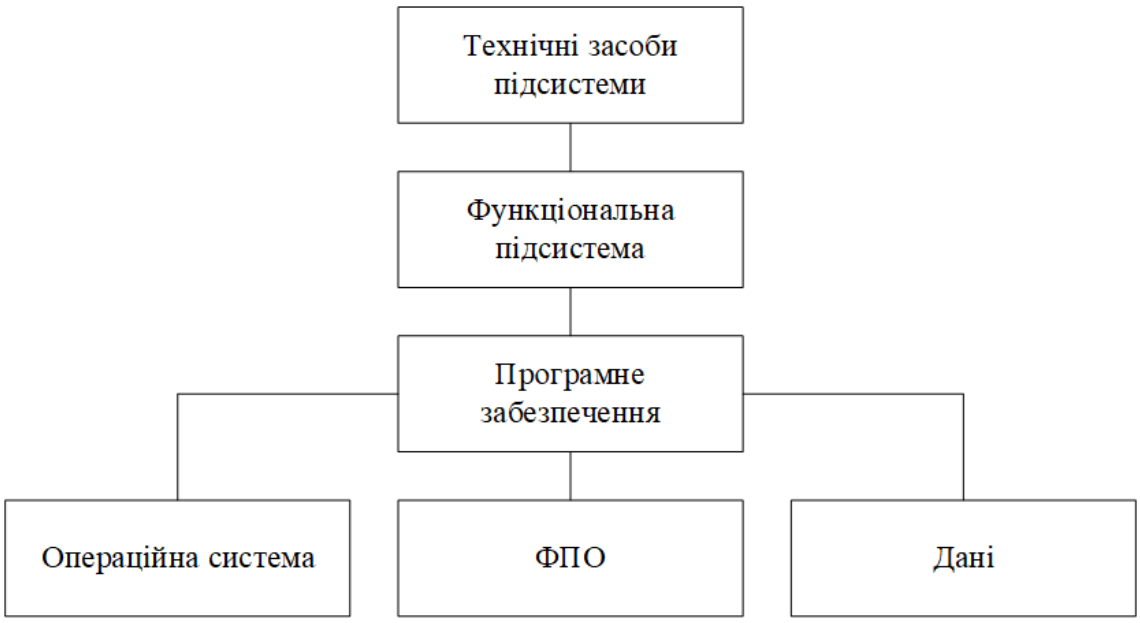


Рисунок 1.4 – Елементи функціональної підсистеми

Доменні мережі – це мережі, якими користується відносно невелика група працівників, які працюють в одному відділі компанії.

Основна мета локальної мережі – це обмін локальними ресурсами, такими як додатки, дані, лазерні принтери та гаджети. Зазвичай у відомчих мережах є один або два файлові сервери та не більше тридцяти користувачів (рис. 1.5). У цих мережах більша частина корпоративного трафіку локалізована. Департаментські мережі, як правило, будуються на основі будь-якої технології мережі Ethernet. Цей тип мережі характеризується одним або двома типами операційних систем.Частіше за все це мережа з виділеним сервером, хоч невелика кількість користувачів робить можливою використання однорангових мережевих ОС, таких, наприклад, як Windows [1].

Завдання адміністрування мережевого рівня відносно прості: залучайте нових користувачів, усувайте прості відповіді, встановлюйте нові вузли та встановлюйте нові версії програмного забезпечення. Такою мережею може керувати лише працівник, який приділяє лише частину свого часу адміністративним завданням.

У більшості випадків адміністратор мережі відділу не має спеціальної підготовки, але він є людиною у відділі, яка найкраще володіє комп’ютером та наполегливо працює над управлінням мережею.

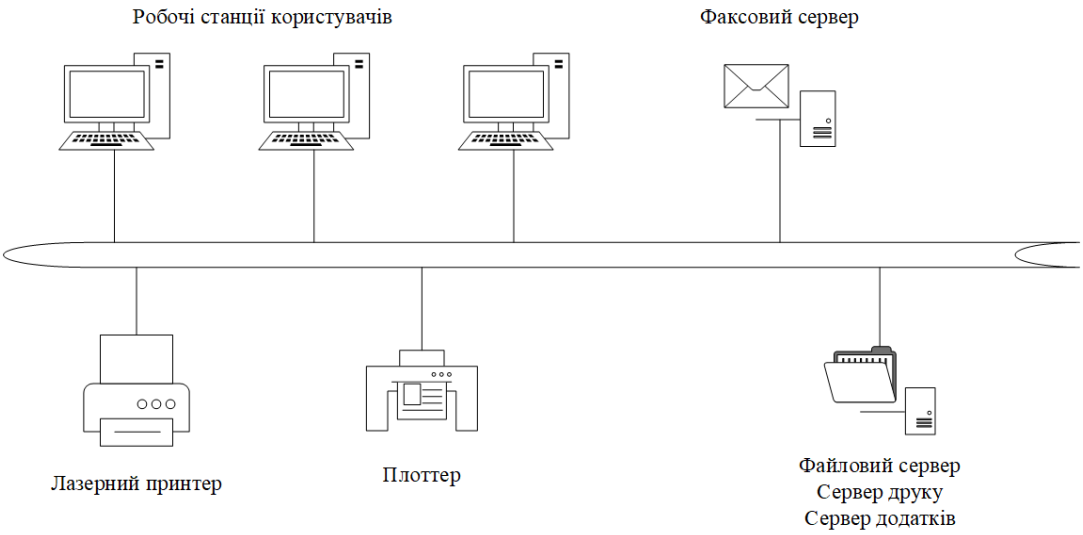


Рисунок 1.5 – Мережа масштабу відділу

Існує ще один тип сітки, який розташований поблизу відділів сітки: робочі групи користувачів. Ці мережі включають дуже малі мережі, які вміщають до 10-20 комп'ютерів. Характеристики мереж робочих груп практично не відрізняються від описаних вище характеристик відомчих робочих груп. Такі властивості, як простота решітки та однорідність, можна знайти у найбільшому концерті, тоді як відомчі решітки можуть у деяких випадках приблизно відповідати найближчій шкалі [5].

Мережа кампусу походить від англійського слова Campus Student Campus. Часто на території кампусу створюється потреба в об'єднанні декількох малих сіток в одну велику сітку. В даний час ця назва не пов'язана зі студентським містечком, але використовується для позначення ланцюгів компанії чи організації.

Основними ознаками вугільної мережі є наступні (рис. 1.6). Мережі цього типу поєднують кілька гереїв різних секцій однієї компанії в живоплотах однієї будівлі або в живоплотах тієї ж площі на площі в кілька квадратних кілометрів. Однак глобальні зв'язки не використовуються у вугільних мережах. Ці мережеві послуги включають взаємодію відомчої мережі, доступ до спільних баз даних підприємств, доступ до спільних факс-серверів, високошвидкісних пристроїв та швидкісних принтерів. Як результат, працівники кожного відділу компанії забороняють доступ до деяких файлів та ресурсів мереж інших

відділів. Важливою послугою мережі кампусів є доступ до корпоративних баз даних незалежно від типу комп’ютера, на якому вони базуються.

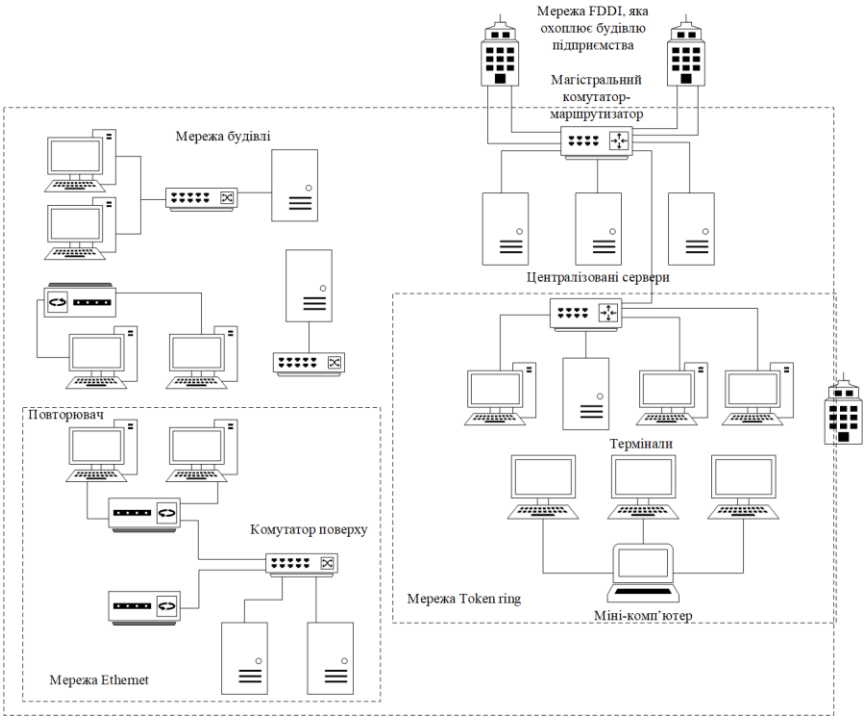


Рисунок 1.6 – Мережа кампуса

На рівні мережі кампусу виникають проблеми інтеграції різнорідного апаратного та програмного забезпечення. Типи комп’ютерів, мережевих операційних систем та мережевого обладнання можуть відрізнятися в різних відділах. Це означає складність управління мережею камусів. У цьому випадку адміністратори повинні пройти навчання та ресурси управління мережею повинні бути складними.

Підприємницькі мережі також відомі як мережі корпоративного масштабу. Це відповідає дослівному перекладу терміна "мережі, що використовується для всіх підприємств", який використовується в англійській літературі для цього типу мереж. Enterprise Scale Networks об’єднує велику кількість комп’ютерів у всіх сферах одного підприємства. Вони можуть бути тісно пов’язані між собою та охопити місто, регіон чи навіть континент. Кількість користувачів та комп’ютерів може сягати тисяч і сотень серверів. Відстані між мережами окремих областей можуть виявитись необхідними для використання глобальної комунікації (рис. 1.7). Для підключення віддалених локальних мереж та окремих комп’ютерів у корпоративній мережі

використовуються декілька засобів зв’язку, включаючи телефон, радіо та супутник. Корпоративні мережі можуть бути представлені як "острови локальної мережі", що плавають у телекомунікаційному середовищі.

Унікальною особливістю такої складної та масштабної мережі є висока неоднорідність мережі – неможливо задовольнити потреби тисяч користувачів з однаковим програмним та апаратним забезпеченням. Корпоративна Web неминуче використовує різні типи комп’ютерів, від кадру посилення до персональних, різних типів операційних систем та безлічі різних додатків. Неоднорідні частини корпоративної мережі повинні працювати як єдине ціле та забезпечувати користувачеві прозорий доступ до всіх необхідних ресурсів [6].

Виникнення корпоративних мереж – хороший приклад відомого філософського постулату про перехід від кількості до якості. При злитті окремих мереж великого підприємства з офісами в різних містах і навіть країнах багато кількісних ознак об’єднаної мережі перевищують певний поріг, з якого починається нова якість. У цих районах існуючі гетто та підходи до традиційних сіток для мереж виявилися непридатними для підприємств підприємств. Основна увага приділялася тим проблемам і проблемам, які мали незначне значення в мережах робочих груп, департаментів. Прикладом може слугувати найпростіша задача (для невеликих мереж) управління обліковими даними користувачів для мережі.

Найпростіший спосіб зробити це – перемістити облікові дані кожного користувача до локальних облікових даних кожного комп’ютера, до яких користувачеві потрібно отримати доступ. При спробі отримати доступ до цих даних вони будуть витягнуті з локальної бази обліку, а доступ буде надано чи заборонено.

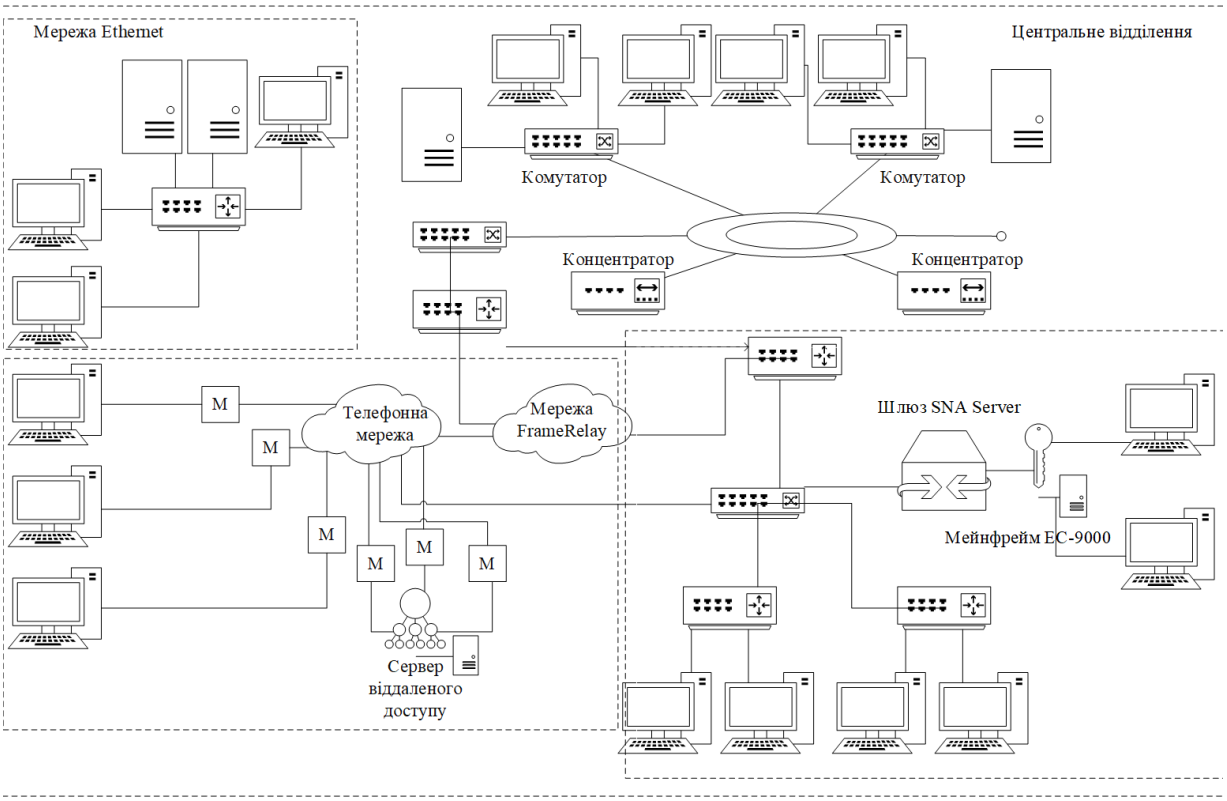


Рисунок 1.7 – Корпоративна мережа

Найпростіший спосіб зробити це – перемістити облікові дані кожного користувача до локальних облікових даних кожного комп'ютера, до яких користувачеві потрібно отримати доступ. При спробі отримати доступ до цих даних вони будуть витягнуті з локальної бази обліку, а доступ буде надано чи заборонено. Для невеликої мережі від 5 до 10 комп'ютерів і приблизно стільки ж користувачів цей метод працює дуже добре. Однак, якщо в Інтернеті є кілька тисяч користувачів, кожному потрібен доступ до декількох десятків серверів, це рішення, очевидно, занадто неефективно. Адміністратор повинен повторити облікові дані користувачів кілька разів. Користувачі також змушені повторювати процес логічного входу щоразу, коли їм потрібен доступ до ресурсів нового сервера. Хорошим рішенням цієї проблеми є те, що велика мережа використовує централізовану службу довідки, яка зберігає всі облікові записи користувачів мережі. Адміністратор здійснює одноразове введення даних користувачів у цю базу даних, а користувач виконує процес одноразового логічного входу не на окремому сервері, а по всій мережі [1].

Оскільки перехід від більш простого типу ланцюга до більш складного – від відомчої мережі до корпоративної мережі, мережа повинна бути більш

надійною та стійкою. Це також значно збільшує переваги для продуктивності. Чим більше передача, тим більше масштаби екрану та їх функції. Все більше і більше даних циркулює в мережі, і сітка повинна забезпечувати її безпеку та доступність. З'єднання для втручання повинні бути більш прозорими. Щоразу, коли ви досягаєте наступного рівня складності, апаратне забезпечення комп'ютера в Інтернеті стає все більш різноманітним, а географічні відстані збільшуються, роблячи цілі складнішими. Більш проблематичним і затратним є управління таким зв'язком.Для корпоративної мережі (мережі підприємств) характерні:

- масштабність – тисячі користувальницьких комп'ютерів, сотні серверів, величезна кількість даних, які зберігаються та передаються по лінії, безліч різних додатків;
- високий ступінь гетерогенності (неоднорідності) – типи комп'ютерів, пристроїв зв'язку, операційних систем та додатків різні;
- використання глобальних зв'язків – філії пов'язані телекомунікаційними засобами, включаючи телефонні канали, радіоканали та супутниковий зв'язок.

Отже, використання корпоративних мереж дає підприємству наступні можливості:

- поділ дорогих ресурсів;
- вдосконалення комутацій;
- поліпшення доступу до інформації;
- швидке і якісне прийняття рішень;
- свобода в територіальному розміщенні комп'ютерів.

1.2 Організаційні заходи захисту корпоративних мереж

В даний час термін "соціальна інженерія" відноситься до методів і засобів несанкціонованого доступу до інформаційних ресурсів, заснованих на характеристиках людської психології. Основна мета соціальних інженерів – заборонити доступ до захищених систем із різноманітним розкраданням інформації, паролями користувачів, інформацією про кредитні картки тощо.

Основна відмінність від стандартної кібератаки полягає в тому, що в цьому випадку комп'ютер та його оператор не вибираються у випадку об'єкта атаки.

Використання соціальної інженерії – це особлива область інформаційного протистояння, яка передбачає низку гетто та методів проведення підготовчих та фундаментальних заходів щодо несанкціонованого отримання патентованої інформації.

Існує багато методів соціальної інженерії, щоб впливати на людину певним чином, але, очевидно, немає універсальних засобів, тому що морально-психологічні, задумане ставлення, життєва позиція та ставлення індивідів до виконання обов'язків є унікальними.

Щоб проаналізувати ефективність боротьби з соціальною інженерією як одним із проявів кіберзлочинності, необхідно ознайомитись з основним способом її використання на практиці. Так, вони можуть містити наступне:

1) фішинг – при такому типі шахрайства лист надсилається так, ніби банк або інша установа, яка переходить на посилання, на яке ви повинні ввести пароль або іншу конфіденційну інформацію, яку вимагає обман Причини надсилання такої інформації можуть бути різними, наприклад, Наприклад, відновлення бази даних після випадкової втрати;
2) вішинг – назва цього виду інтернет-шахрайства пішла від попереднього та полягає у імітування дзвінків на мобільний телефон, ніби як від банківської установи (із попередньо записаним голосом) та отриманні запиту про комунікацію із банком для підтвердження тієї чи іншої інформації. При цьому жертва отримує вимогу сказати свій пароль або іншу конфіденційну інформацію, яка необхідна для доступу до банківських рахунків;
3) фармінг – процедура полягає в перенаправленні потерпілого на недійсну IP-адресу. Шахраї встановлюють на свої комп'ютери зловмисне програмне забезпечення, яке при запуску на комп'ютері гарантує, що жертва перенаправляє сторінку пошуку жертви на підроблені сторінки;

4) попередження про вірус на комп’ютері – в цьому випадку розробник зловмисного програмного забезпечення попереджає жертву зараження їх комп’ютерним вірусом та заявляє, що вам потрібно перейти до посилань та встановити необхідне програмне забезпечення для очищення операційної системи. Ця програма сама по собі шкідлива і забезпечує доступ до необхідної інформації;
5) quid pro quo – вказаний вид інтернет-шахрайства базується на вмінні особи у телефонній розмові або електронною поштою увійти в довіру до жертви (зазвичай офісного працівника) та, представившись співпробітником служби технічної підтримки, запропонувати йому вирішення проблеми, в ході чого він і отримає всю необхідну конфіденційну інформацію;
6) «дорожне яблуко» – метод шахрайства заснований на використанні фізичних засобів масової інформації. Так, шахрай може залишити флешку у публічних засобах масової інформації, компакт-диск із зображенням, який може зацікавити потерпілого, і змусити його переглянути його на своєму комп’ютері;
7) зворотна соціальна інженерія – реалізація цього методу можлива лише в тому випадку, якщо шахрай вже знає і довіряє жертві. У цьому випадку жертва саги звертається до шахрая (наприклад, системного адміністратора), щоб допомогти йому відновити загублений файл (який заховав шахрай). Їй кажуть, що таку дію можна здійснити лише якнайшвидше, увійшовши у свій обліковий запис. При такому вчинку потерпілий на власний розсуд повідомляє всю інформацію про шахрая;
8) претекстинг – напад, при якому шахрайство представляється іншою особою, а потерпілий позбавляється всієї необхідної інформації. Однак такий вид інтернет-шахрайства вимагає дуже якісної підготовки та збору всієї необхідної попередньої інформації про особу.

Вказані види інтернет-шахрайства є найбільш популярними проявами застосування інтернет інженерії. Далі буде розглянуто заходи запобігання інтернет злочинності, які застосовуються в Україні [7]:

1) створити політику безпеки організації та контролювати її виконання; директива, зокрема, повинна включати:
   - стратегію захисту IT-інфраструктури організації;
   - набір правил, згідно з якими інформація створюється, обробляється і зберігається в компанії;
   - правила своєчасного оновлення ПЗ та відповідальність працівників;
   - резервне копіювання та відновлення даних – потрібно регулярно створювати резервні копії вашої бізнес-системи та важливих даних. Резервні копії повинні зберігатися в окремих томах, які фізично відокремлені від цільових систем. Цілісність та повнота резервного копіювання слід регулярно перевіряти на предмет їх регулярного відновлення;
   - план дій з локалізації, блокування розподілу та відновлення після атак;
2) запровадження правила користування обліковими записами в організації, включаючи:
   - персоналізований адміністративний доступ; заборона на використання спільних адміністративних рахунків;
   - використовуйте різні облікові записи для виконання різних адміністративних завдань, таких як: наприклад, для управління доменом, сервером, користувацьким ПК або власним ПК;
   - заборона виконувати регулярні завдання, пов’язані з використанням облікових записів адміністратора, щоб адміністратори на своїх ПК повинні працювати за типовими обліковими записами з належним дозволом звичайного користувача; Управління інформаційною системою повинно здійснюватися з виділеного сервера управління, а не безпосередньо з персонального ПК. Використання адміністратора для конкретних

операцій кожного облікового запису слід ретельно контролювати. Забороніть використання облікових записів адміністратора домену для завдань, які не пов’язані з керуванням контролерами домену;

- гранулярна деталізація прав доступу сервісних облікових записів – облікові записи для функціонування різноманітних служб та ПЗ повинні мати мінімально необхідний рівень прав, достатній для роботи конкретного сервісу;

3) регулярне навчання всіх користувачів організації основ захисту інформації, включаючи:
   - інструктаж щодо правил роботи критичної системи організації та інформації із зовнішніх, неперевірених джерел;
   - регулярний обмін знаннями для контролю над отриманням інформації;
4) регулярне навчання та підвищення кваліфікації ІТ-фахівців та адміністраторів у галузі сучасних загроз та методів безпеки для систем та рішень, що застосовуються в організації;
5) проведення тестових атак, включаючи використання методів «соціальної інженерії» й для перевірки обізнаності користувачів щодо правил безпеки організації та рівня безпеки інформаційних систем;

Розглянуті способи відхилення інформації через вплив на персонал організацій та методи контрзаходів є більш актуальними. Ступінь інформаційної загрози в цілому не може бути оцінена адекватно та всебічно, залежно від тяжкості заподіяної шкоди. Мислення людини не завжди може бути логічно проаналізовано, саме тому неможливо сформулювати чіткий алгоритм його роботи. Ви можете лише визначити перелік цілей і попросити, щоб працівник суворо їх дотримувався.

Ведення діяльності персоналу організації за затвердженими інструкціями та правилами роботи є одним із головних завдань керівника організації. Якщо лідер організації робить це, гетто соціального інжинірингу не становить значної загрози.

1.3 Програмно-апаратні заходи захисту корпоративних мереж

Фізична безпека – це засоби, необхідні для зовнішнього захисту комп'ютерної техніки, територій та об'єктів. Вони реалізовані на основі комп'ютерів, розроблених спеціально для забезпечення фізичних бар'єрів для основних шляхів входу та несанкціонованого доступу до компонентів власницьких інформаційних систем.
Обладнання – це різноманітні електронні, електронні, механічні та інші пристрої, інтегровані до послідовних підрозділів електронної системи обробки та передачі даних для внутрішнього захисту комп'ютерів: термінали, пристрої введення та виведення, процесори, лінії зв'язку тощо.
Функції програмного забезпечення, інтегровані із системним програмним забезпеченням, необхідні для виконання логічних та інтелектуальних функцій захисту [8].
Апаратно-програмні засоби захисту – це засоби, які основані на синтезі програмних та апаратних засобів.
Організація мережевої безпеки організації пов'язана з визначенням сфери мережі, внутрішньої безпеки мережі та політики безпеки системи.
Периметр – це посилена границя мережі, яка може включати до свого складу:

- маршрутизатори (routers);
- брандмауери (firewalls);
- систему виявлення вторгнень (СВВ, IDS);
- пристрої віртуальної приватної мережі (ПВПМ, VPN);
- програмне забезпечення мережі;
- демілітаризовану зону (ДМЗ, DMZ) і екрановані підмережі.

Маршрутизатори контролюють вхідний та вихідний трафік, а також середній смуги руху.
Крайовий маршрутизатор – це останній маршрутизатор перед входом в незахищену мережу і виступає першою і останньою межею захисту мережі.
Брандмауер аналізує трафік за допомогою набору правил, які визначають, чи можна передавати трафік в мережу чи ні. Область брандмауера починається там, де закінчується область прикордонного маршрутизатора.
За допомогою системи виявлення вторгнень ви можете виявити та повідомити про вторгнення в мережу та потенційно небезпечні події. Система може складатися з серії детекторів різного типу, розташованих у найважливіших точках мережі. СВР-детектори шукають конкретні підписи критичних подій або проводять статистичний аналіз мережевих операцій та виявляють аномальні події. У разі критичної події детектор СВ повідомляє про це адміністратору та / або реєструє подію.
Віртуальна приватна мережа – це захищений сеанс, який використовує захищені канали зв'язку. Під ПВПМ мається на увазі перигейтерний технічний комплекс, який забезпечує шифрування сеансу. За допомогою ПВПМ віддалені партнери можуть встановити захищене з'єднання з внутрішньою захищеною мережею з незахищеного середовища [8].
Програмне забезпечення – це програма, яка працює в Інтернеті. Архітектура програмного забезпечення є важливою, оскільки захист даних з точки зору програм та служб є головним завданням веб-області.
Дегілітаризована зона – це підмережа, яка споживає загальнодоступні ресурси та підключається до брандмауера або іншого фільтруючого пристрою, що захищає його від зовнішніх перешкод.
Екранована підмережа – це область, яка виходить за межі екрану коньяку. Захищена підмережа використовується для ізоляції серверів, до яких має бути доступ незахищеною мережею та використовуються користувачами та внутрішніми захищеними підмережами.
Внутрішня мережа – це мережа, яка захищена периметром. Тут розміщені всі сервери, робочі станції та інформаційна інфраструктура. Для захисту внутрішньої мережі використовуються такі пристрої Perigeter: маршрутизатори для фільтрації вхідного та

вихідного трафіку підмережі; внутрішні міжмережеві екрани для розподілу ресурсів; Брандмауери проксі з метою безпеки; SWR-детектор для контролю внутрішнього руху. Внутрішня сітка також використовує: персональні брандмауери для підвищення безпеки хоста; антивірусне програмне забезпечення; поліпшена безпека операційної системи; адміністрація конфігурації системи; аудит.

Захист хоста – це процес зміни конфігурації операційної системи і додатків хоста з метою перекриття потенційних вразливостей системи. Посилення захисту хоста є останнім рубежем оборони системи.

Управління конфігурацією – процес встановлення і підтримки визначеної конфігурації для систем і пристроїв, що входять до мережі. Управління конфігурацією – це найкращий захід організації захищеної стандартної (базової) конфігурації, який призведе до зниження наслідків інцидентів до мінімуму. Управління конфігурацією дозволяє також контролювати неавторизоване встановлення програмного забезпечення [9].

Аудит – процес, який дозволяє контролювати стан безпеки мережі та своєчасно здійснювати з'єднання з архітектурою технічної безпеки.

Концепція мережевої безпеки підприємства передбачає створення ефективної інфраструктури безпеки та визначає рівні та ключові механізми захисту інформаційних ресурсів мережі.Додаткові заходи захисту корпоративної мережі:

1) **наявність впровадженого рішення 802.1x та Network Access Control (NAC)** для запобігання несанкціонованому підключенню сторонніх пристроїв до корпоративної мережі та надайте лише необхідний доступ до мережі, залежно від функціональних обов'язків користувача та стану пристрою. Розчин повинен доставити:
   - контроль пристроїв, підключених до корпоративної мережі; блокуйте сторонні пристрої;
   - гранульований доступ у мережу за результатами авторизації (політика доступу в залежності від користувача, часу, способу, місця підключення і типу пристрою);
   - важливість перевірки пристроїв на відповідність перед підключенням до корпоративної мережі (NAC): наявність встановленого антивірусу та інших продуктів, а також останні оновлення;
   - автоматичне автоматичне заповнення карантину за допомогою індикаторів спільного проектування; У разі спільної проекції хоста у корпоративній мережі для пошуку та запобігання поширенню епідемії вірусу, переконайтеся, що сайт автоматично закривається або на карантин блокується від усіх мережевих з'єднань;

2) **наявність спеціального інструменту «пісочниця» для статичного (аналізу коду) та динамічного (у тестовому середовищі) аналізу невідомих файлів для виявлення їх шкідливого впливу. Для підвищення ефективності антивірусного захисту від атак з нульовими днями рішення пісочниці повинні бути інтегровані в максимальну кількість систем безпеки: веб-екрани та поштові шлюзи, захист кінцевої точки. Системи цього класу можуть також використовуватися адміністраторами як додатковий інструмент для дослідження загроз.Використання системи контролю дій привілейованих користувачів – Privilege Access Management (PAM).** Надання доступу до критичних систем тільки за допомогою рішення, забезпечуючи:
   - збір, запис та аналіз активності привілейованих користувачів;
   - детектування ризикованих дій до того, як це призведе до шкідливих наслідків;
   - можливість взаємодії з користувачем, який виконує ризиковані операції, та блокування його сесії;
3) **наявність системи моніторингу та профілювання мережевих потоків (Network Behavior Analysis, NBA)** для визначення штатного профілю трафіку організації та виявлення відхилень від “нормальної” поведінки. Налаштування збору інформації про трафік з усіх ключових мережевих пристроїв організації для повноти видимості та аналізу потоків даних [10];
4) **наявність спеціального рішення з оцінки вразливості (VA) для періодичного сканування всіх елементів інфраструктури підприємства для виявлення відомих вразливих версій в операційних системах та програмному забезпеченні. Надання можливості швидко ідентифікувати виявлені загрози та інтегруватися із мережевою системою безпеки та аналізу, щоб ізолювати чи фільтрувати доступ до критичних вузлів вразливості;**

5) **використання центральної системи виявлення, аналізу та кореляції аварій безпеки (SIEM) для всебічного, всебічного аналізу стану здоров'я розгорнутої інфраструктури підприємства**:
   - збір інформації журналу та подій з усіх систем підприємства; негативні події з першого погляду (нормалізація) та агрегація даних;
   - створення екранів та звітів для зображення стану IT-інфраструктури;
   - створення правила кореляції для виявлення пов'язаних подій, які вказують на напади та спроби втручання в IT-інфраструктуру компанії;
   - створення правила кореляції на основі ризику для виявлення та висвітлення небезпечних дій та подій на критичних системах;
   - аналіз історичних даних для створення нових правил кореляції;
   - встановлення правил для автоматичної реагування на виявлені події з метою блокувати та припинити поширення загроз.

1.4 Захист корпоративної мережі на базі обладнання компанії Cisco

Найбільш поширеним мережевим обладнанням для побудови мереж є обладнання компанії Cisco [11]. Для безпеки на всіх рівнях корпоративної мережі використовуються такі продукти:

- кінцеві точки – програма-агент Cisco Security Agent захищає комп'ютери і сервери від атак черв'яків;
- захист від мережевих вторгнень – датчики IPS 4200 Series sensors, модулі служб IDS Catalyst 6500 (IDSM-2) або IOS IPS ідентифікують, аналізують і блокують зловмисний небажаний трафік;
- виявлення та усунення атак DDoS – детектор аномалій трафіку Cisco Traffic Anomaly Detector XT і Guard XT забезпечують нормальну роботу в разі атак, що переривають роботу служби; модулі служб детектора аномалій трафіку Cisco і Cisco Guard створюють стійкий захист від атак DdoS в комутаторах серії Catalyst 6500 і маршрутизаторах серії 7600;
- безпека контенту – модуль пристрою Access Router Content Engine module захищає бізнес-додатки, що працюють через інтернет;

- інтелектуальні служби адміністрування мережі і систем безпеки: в маршрутизаторах і комутаторах Cisco знаходять і блокують небажаний трафік і додатки.

Для менеджменту і моніторингу використовуються такі продукти:

- CiscoWorks VPN / Security Management Solution (VMS);
- CiscoWorksSecurity Information Management System (SIMS) – система управління інформацією про стан безпеки.

Вбудовані менеджери пристроїв: менеджер маршрутизаторів і пристроїв безпеки Cisco (SDM), менеджер пристроїв адаптивної безпеки (ASDM) швидко і ефективно здійснюють відстеження, ведуть моніторинг служб безпеки і активності мережі.
Технологія Network Admission Control (NAC) від Cisco.
Контроль доступу в мережу (Network Admission Control, NAC) – це набір технологій і рішень, фундаментом яких є загальногалузева ініціатива, реалізована під патронажем Cisco Systems [12].
NAC використовує мережеву інфраструктуру для контролю за дотриманням безпеки на всіх пристроях, які хочуть отримати доступ до ресурсів мережі. Це зменшує ризик серйозної шкоди мережі від загроз безпеці.
Безпечний віддалений доступ до корпоративної VPN співробітникам і партнерам багатофункціональні пристрої захисту забезпечують за допомогою протоколів SSL і IPsec VPN, вбудованих блокувальних сервісів для попередження та запобігання IPS вторгнень.
Self-Defending Network – стратегія самозахистом мережі від Cisco.
Self-Defending Network є розвивається стратегією майбутнього від Cisco. Технологія дозволяє захистити бізнес-процеси підприємства шляхом виявлення та запобігання атак, адаптації до внутрішніх і зовнішніх загроз мережі.
Підприємства можуть використовувати інтелектуальні ресурси мережевих ресурсів, упорядкувати бізнес-процеси та зменшити витрати.
Пакет управління Cisco Security Management – це набір продуктів і технологій, що розширюють та застосовують політику безпеки для найбільш захищеної мережі Cisco.
Інтегрований продукт Cisco дозволяє автоматизувати завдання управління безпекою за допомогою ключових компонентів: менеджера управління і Cisco Security MARS – системи моніторингу, аналізу та реагування.
Cisco Security Manager має простий інтерфейс для налаштування брандмауерів, VPN та систем захисту від втручання (IPS) на пристроях безпеки, брандмауерах, маршрутизаторах та комутаторах Cisco.

1.5 Порівняльна характеристика засобів захисту корпоративних мереж

Для отримання функціонального мережевого рішення важливо звертати увагу на різних постачальників обладнання. Незаперечним є те, що для побудови мережі логічніше використовувати обладнання одного виробника. В даний час, при побудові такої мережі досягається гармонійна, надійна і відмовостійка IT-інфаструктура.
В даному підрозділі наведено порівняння пристроїв безпеки, маршрутизаторів, комутаторів, бездротових точок доступу і контролерів бездротових точок доступу від виробників Cisco, Huawei, Juniper і HP.
Пристрої безпеки дозволяють захистити доступ в Інтернет, контролювати доступ до зовнішніх ресурсів, переглядати білінг зовнішнього трафіку, виділяти і захищати DMZ, виконувати функції системи виявлення/запобігання вторгнення, створювати захищені тунелі між філіями компанії з розподіленою інфраструктурою, забезпечувати захищений доступ мобільним користувачам. У таблиці 1.1 наведено порівняння лінійок пристроїв безпеки Cisco ASA, Juniper і Huawei [13].

Таблиця 1.1 – Порівняння лінійок пристроїв безпеки Cisco, Juniper і Huawei

Cisco	Juniper	Huawei

SA520/520W	SSG5/20	USG2110-F/F-W/A-W
SA540	SSG140	USG2110-F/F-W/A-W
ASA5505	SSG140	USG2160/2160W
ASA5510	SSG140	USG2160/2160W
ASA5515-X	SSG520M/SRX240	USG2230
ASA5520	SSG520M/SSG250M	USG2230
ASA5540	SSG550M	USG2260
ASA5555-X with SSP10	SRX650	USG5530
ASA5555-X with SSP60	SRX3600	USG5560

Таблиця 1.2 – Перелік моделей пристроїв безпеки Cisco ASA

	ASA 5545-X	ASA 5550	ASA 5555-X	ASA 5585-X with SSP10	ASA 5585-X with SSP10
Пропускна спроможність з перевіркою стану, Мб/с	3000	1200	4000	4000	40000
Пропускна спроможність з використанням IPS, Мб/с	900		1300	2000 з IPS SSP-10	10000 з IPS SSP-60
Підключень в секунду	30000	33000	50000	50000	350000
Пропускна спроможність VPN трафіка 3DES/AES, Мб/с	400	425	700	1000	5000

Таблиця 1.3 – Перелік моделей пристроїв безпеки Juniper SRX

	SRX100	SRX210	SRX1400	SRX3600	SRX5800
Пропускна спроможність з перевіркою стану, Мб/с	700	850	10000	55000	200000
Пропускна спроможність, IPS, Мб/с		85	3000	50000	100000
Підключень в секунду			45000	400000	400000

Пропускна спроможність VPN трафіка 3DES/AES, Мб/с	65	85	4000	15000	

Порівняння провідних виробників мережевого і комунікаційного устаткування за кількома показниками: зростання частки на ринку, фінансові показники, надійність, інновації, сервіс і підтримка.

З точки зору практики, інтеграція стороннього обладнання в інфраструктурі одного виробника, в більшості випадків зменшує витрати на експлуатацію мережі на 15-25%. Вартість обладнання популярних виробників не може компенсувати експлуатаційні витрати. Загальні витрати на експлуатацію та підтримку інфраструктури з обладнанням одного вендора, виявляються вищими.

На противагу домінуючого положення на українському ринку (60% телекомунікаційних мереж, 70-80% держсекторів) корпоративного і комунікаційного устаткування, можна поставити порівняно високі розцінки на обладнання, удосконалення для розширення можливостей, і послуги з технічної підтримки в перебігу всієї роботи обладнання [12].

Зменшити складність мережі при інтегруванні обладнання стороннього виробника видається не логічним, але, таке суміщення призводить до стандартизації мережевий архітектури, і зменшення кількості операційних систем.

Перевага віддається компаніям, що допомагає оптимізувати масштаб мережі та готовим задовольнити особливі вимоги замовника. Оптимізація мережевої інфраструктури, збільшення її простоти, проходження прикладів з практики проектування і управління дасть можливість знизити витрати на експлуатацію. Необхідно, щоб ПО і інструменти управління підходили до вживаного обладнання.

Деякі виробники пропонують власні системи управління (наприклад, hp imc – intelligent management center), з підтримкою як власного мережевого обладнання, так і обладнання інших компаній. Подібні системи управління набагато спрощують і здешевлюють впровадження і експлуатацію мультивендорних рішень.

Таблиця 1.4 – Порівняння основних характеристик компанії Cisco Juniper і Huawei

	Cisco ASR 9922	Juniper MX2020	Huawei NE5000E
System capacity	до 11 Тбіт/с	до 80 Тбіт/с	до 6,4 Тбіт/с
Кількість слотів	20	20	16
Slot capacity	550 Гбіт/с	2 Тбіт/с	400 Гбіт/с
Процесор	2,27 Ггц	1,8 Ггц	1,5 Ггц
Об’єм оперативної пам’яті	до 12 Гб	16 Гб	до 16 Гб
Операційна система	Cisco IOS	JunOS	VRP
Розміри, см	191x45x73	200x44x92	124x44x80
Маса, кг	471	680	300

1.6 Аналізатори та колектори для моніторингу мережевого трафіку

Системи виявлення комп'ютерних атак є одним з найважливіших елементів системи захисту інформації сучасного підприємства, враховуючи те, як кількість проблем з комп'ютерною безпекою зросла за останні роки.

Було встановлено, що інформація про мережевий трафік має статистичний характер і представляє часовий ряд. Методи статистичного аналізу мережевого трафіку широко застосовуються в якості інструментів для прогнозування перевантаженості, простоїв, якості обслуговування тощо. З точки зору безпеки мережі, аналіз мережевого трафіку з метою виявлення ненормальних поведінок (збої, негативні зовнішні впливи, ненавмисні порушення) системи має вирішальне значення як для вирішення проблем в управлінні мережею, так і для функцій.

Існує багато різних програмних та апаратних рішень для збору даних та аналізу трафіку. Найбільш відомими серед яких є:

- розширення Netflow від компанії Cisco Sytems, що застосовується у галузі IT- технологій;
- SNMP(протокол прикладного рівня);
- програмний модуль SFlow.

Netflow – представлено в маршрутизаторах Cisco, як розширення, які дають можливість збирати IP-адреси мережевого трафіку, якщо це вказано в інтерфейсі. Таке розширення надає можливість збирати та надалі аналізувати послідуючі дані:

- IP-адреси відправника та отримувача;
- порти джерела та призначення для UDP і TCP;
- код та тип повідомлення для ICMP;
- номер протоколу IP.

На рисунку 1.8 показано інфраструктура Netflow. Вона застосовується на основі колектора, сенсора та аналізатора:

1) сенсор збирає статистику трафіку, що поступає крізь нього. Сенсор потрібгно розміщувати в «вузлових точках» мережі, наприклад, на граничних маршрутизаторах сегментів мережі;

2) колектор виконує збір інформації від сенсорів. Отримані дані формуються в файл для подальшої обробки (різні колектори зберігають дані в різних форматах);

3) аналізатор, або система обробки, зчитує ці файли і генерує звіти у формі, яка є більш зручною для людини. Ця система повинна бути сумісна з форматом даних, що надаються колектором. У сучасних системах колектор і аналізатор часто об’єднані в одну систему [14].

Netflow надає можливість аналізу мережевого трафіку на рівні сеансів, роблячи запис про кожної транзакції TCP/IP. Аналізуючи дані, які надаються Netflow.

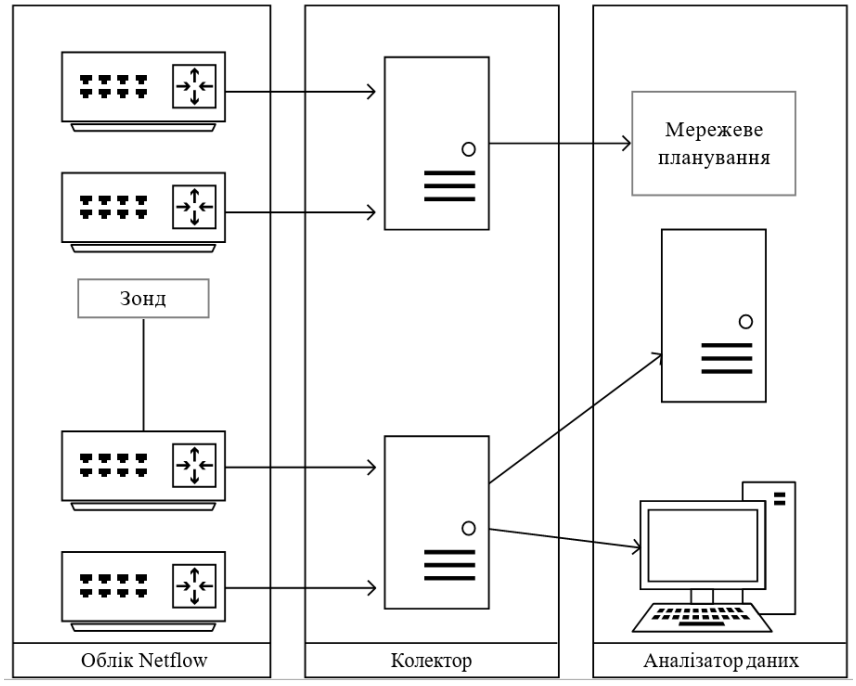


Рисунок 1.8 – Інфраструктура Netflow

Недоліком даного розширення є те, що він може генерувати величезні обсяги зайвих даних. Іноді дуже складно виявити у величезній кількості повідомлень причину виниклої проблеми або, в профілактичних цілях,

відшукати джерела потенційних проблем чи «дірки» в системі безпеки. Також, у даного розширення відсутня можливість ідентифікації сайтів.

SNMP – протокол прикладного рівня, який є частиною протоколу TCP/IP. Він дозволяє адміністраторам керувати продуктивністю мережі, знаходити й усувати проблеми, планувати зростання мережі. Даний протокол збирає статистику по трафіку до кінцевого хоста через пасивні датчики, які реалізуються разом з маршрутизатором. [2]

Для протоколу SNMP притаманні три ключові компоненти:

- керовані пристрої (Managed Devices);
- агенти (Agents);
- системи управління мережею (Network Management Systems).

Хоча даний протокол може бути корисним інструментом в роботі адміністратора безпеки, він має ряд недоліків:

- недостатня кількість точок аналізу;
- відсутність автентифікації;
- відсутність ідентифікації web-сайтів;
- немає інформації про роботу додатків і користувачів – помилкове уявлення про роботу мережі;
- точність обмежується періодом опитування агентів (можуть бути розриви).

SFlow – програмний модуль, що здійснює облік та тарифікацію послуг доступу в мережу Internet (IP послуг), що надаються абонентам по виділеному каналу, засобами апаратури, що підтримує експорт статистичних даних за протоколом SFlow.

Безсумнівним недоліком є те, що програмний модуль підтримується не дуже широким колом виробників, серед яких основним є Hewlett Packard, який здійснює підтримку SFlow другої версії у верхній лінійці комутаторів третього рівня HP ProCurve 53xx і HP ProCurve 93xx.

Аналіз мережевого трафіку є складним завданням, що залежить від безлічі параметрів, яка насилу з важкістю піддається декомпозиції і моделюванню. Однією з причин цього є постійне ускладнення структури глобальної мережі,

яка характеризується взаємодією великої кількості пристроїв самих різних типів, що не мають єдиного центру управління [15].

Висновки за розділом. У результаті проведення аналізу сучасного стану питання галузі захисту мереж було отримано такі результати:

- охарактеризовано особливості захищених мережі, що дає можливість зрозуміти що з себе представляє захищена мережа.
- розглянуто види інформаційних загроз, які несуть небезпеку функціонування захищеної мережі.
- розглянуто комплекс програмних, апаратних та організаційних методів забезпечення захисту мережі.
- розглянуті технології та методи захисту мереж на базі обладнання CISCO, а також проведено порівняння їх з аналогами інших компаній.

2 КОМПЛЕКСНИЙ МЕТОД ЗАХИСТУ МЕРЕЖІ ПІДПРИЄМСТВА НА БАЗІ ОБЛАДНАННЯ CISCO

В даному розділі магістерської роботи описана розробка вдосконаленого комплексного методу захисту мережі підприємства, а саме алгоритм його роботи. Алгоритм застосовано та на його базі розроблено реальну мережу підприємства, що описано у третьому розділі.

2.1 Захист локальної мережі

2.1.1 Автентифікація по стандарту 802.1X

802.1x – це стандарт, який використовується для автентифікації та авторизації користувачів і робочих станцій в мережі передачі даних. Завдяки стандарту 802.1x можна надати користувачам права доступу до корпоративної мережі та її сервісів в залежності від групи або займаної посади, якій належить той чи інший користувач. Так, підключившись до бездротової мережі або через Ethernet в будь-якому місці корпоративної мережі, користувач буде автоматично поміщений в той VLAN, який зумовлений політиками групи, до якої прив'язана обліковий запис користувача або його робочої станції в AD. До даного VLAN буде прив'язаний відповідний список доступу ACL (статичний, або динамічний, в залежності від прав користувача) для контролю доступу до корпоративних сервісів, окрім списків доступу [3].

Для того, щоб реалізувати модель функціонування IEEE 802.1x в мережі передачі даних, побудованої на обладнанні Cisco Systems, необхідно мінімальний набір таких компонентів:

- комутатор, який буде виступати в ролі автентифікатора;
- сервер автентифікації (RADIUS сервер);
- DHCP сервер;
- супплікант (клієнт) 802.1x на робочій станції користувача;

Для розширеного функціоналу не зайвими виявляться:

- сервер зберігання облікових даних користувачів (AD, Samba та ін.);
- сервери сертифікатів.

Для демонстрації роботи стандарту IEEE 802.1x, далі на рисунку 2.1 наведено діаграму процесу авторизації в спрощеному вигляді, де цифрами зазначений номер кроку:

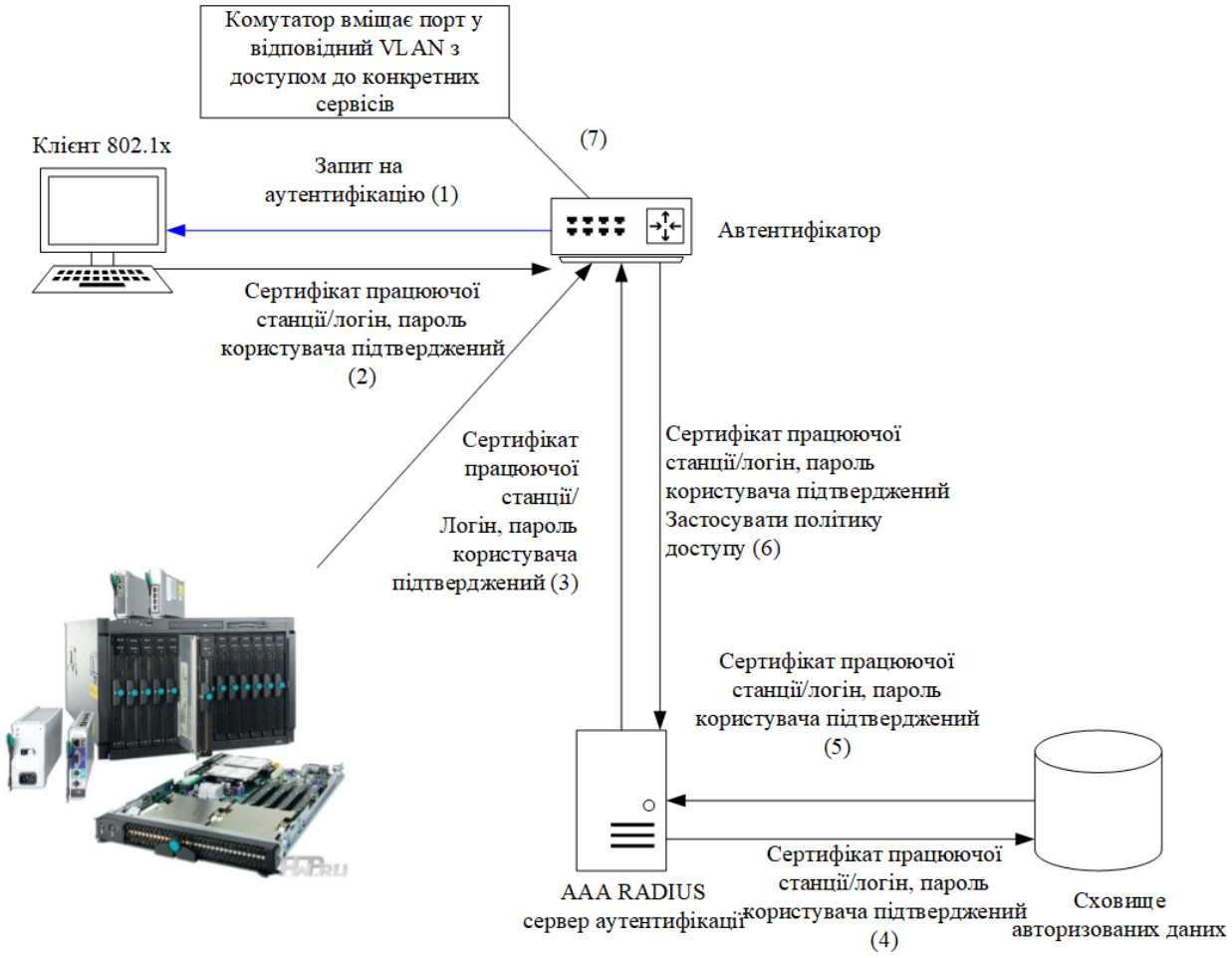


Рисунок 2.1 – Діаграма процесу авторизації в спрощеному вигляді

В наш час важко уявити компанію, інформаційна інфраструктура якої не була б керованою. Під керованої інфраструктурою вважається доменна мережа. При використанні стандарту 802.1x в доменному середовищі необхідно враховувати один нюанс – не можна проводити авторизацію в мережі передачі даних тільки по облікового запису користувача. Вся справа в тому, що при завантаженні, перш ніж вивести вікно авторизації користувача, робоча станція повинна пройти кілька етапів:

- отримати IP адресу;
- визначити сайт і контролер домена;
- встановити безпечний тунель до AD, використовуючи протоколи LDAP, SMB;
- авторизуватися в домені, використовуючи обліковий запис робочої станції по протоколу Kerberos;
- завантажити GPO;
- запустити скрипти, запропоновані GPO на робочу станцію.

Всього цього не трапитися, якщо проводити авторизацію тільки по облікового запису користувача. Причина проста, неавторизована робоча станція при завантаженні не буде допущена до мережі передачі даних, всі протоколи крім EAPoL, які зазвичай використовуються для нормального функціонування, будуть заблоковані до моменту авторизації. Отже, якщо до моменту авторизації користувача, станція була авторизована в мережі, групові політики до неї застосовуватимуться. Якщо необхідно працювати в доменному середовищі, обов'язково потрібно в першу чергу авторизувати в мережі робочу станцію, щоб вона пройшла через всі перераховані вище етапи.

Самим безпрограшним та безпечним варіантом буде авторизація робочої станції в мережі за сертифікатом без авторизації користувача. Звичайно, це не означає, що потрібно назавжди відмовитися від авторизації користувача. Просто для цього необхідно підійти до процесу авторизації кілька з іншого боку якщо до цього ми говорили про процедуру зміни VLAN (динамічний VLAN) в якості основного роздільник прав користувачів, то в даному випадку нам допоможе динамічний список доступу. В результаті, замість зміни VLAN і IP адреси, зміняться правила ACL конкретного VLAN відповідно до прав доступу конкретного користувача. На жаль, така функція доступна не скрізь, проте, вона є на сервері контролю доступу ACS версії 5.2.
Далі буде розглянуто логічні елементи взаємозв'язку між сервером контролю доступу ACS, він же Cisco Access Control Server, він же RADIUS сервер, та сховищем облікових даних, наприклад, Active Directory. На сервері ACS встановлюються взаємини з AD по типу:
Група об'єктів ACS = Група об'єктів AD
Права доступу для об'єктів конкретної групи встановлюються на ACS. Логіка роботи виходить наступна:

1) приходить запит на перевірку авторизаційних даних;
2) ACS звертається до сервера AD з питанням хто це такий і в якій групі AD він знаходиться;
3) AD повідомляє що це за об'єкт та в якій групі він знаходиться;
4) ACS зіставляє ім'я групи AD і локально-створену групу з політиками доступу на ACS, якій вона відповідає;
5) Якщо відповідність знайдено, ACS повідомляє комутатора, які правила доступу застосувати на порт згідно із заданими критеріями безпеки на ACS для цієї групи;
6) Якщо відповідність, не знайдено або сервер AD повідомив, що авторизовані дані недійсні, комутатор поміщає порт в гостьовій VLAN.

Далі розглянуто нештатні ситуації, які відбуваються при авторизації користувача:

1) Клієнт 802.1x виключений У тому випадку, коли клієнт не активний, робоча станція не може ідентифікувати себе, вона автоматично поміщається в гостьовій VLAN з обмеженим доступом до мережі передачі даних. Процес виконання даної функції представлений на рисунку 2.2:

Клієнт 802.1x включений, але налаштований невірно. У тому випадку, коли клієнт не може коректно ідентифікувати себе, робоча станція автоматично поміщається в гостьовій VLAN з обмеженим доступом. Процес виконання даної функції представлений на рисунку 2.3.

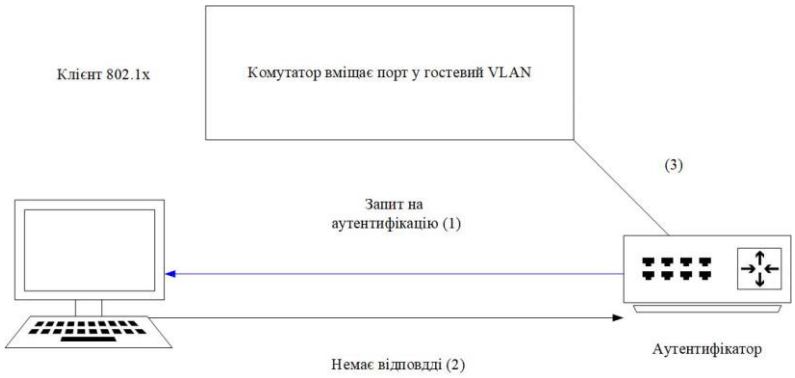


Рисунок 2.2 – Процес виконання функції, якщо клієнт вимкнений

2) RADIUS сервер недоступний. Для підвищення відмовостійкості в разі виходу з ладу сервера аутентифікації, робоча станція поміщається в Failover VLAN з мінімально необхідними для виконання роботи правами доступу до мережі передачі даних [16]:

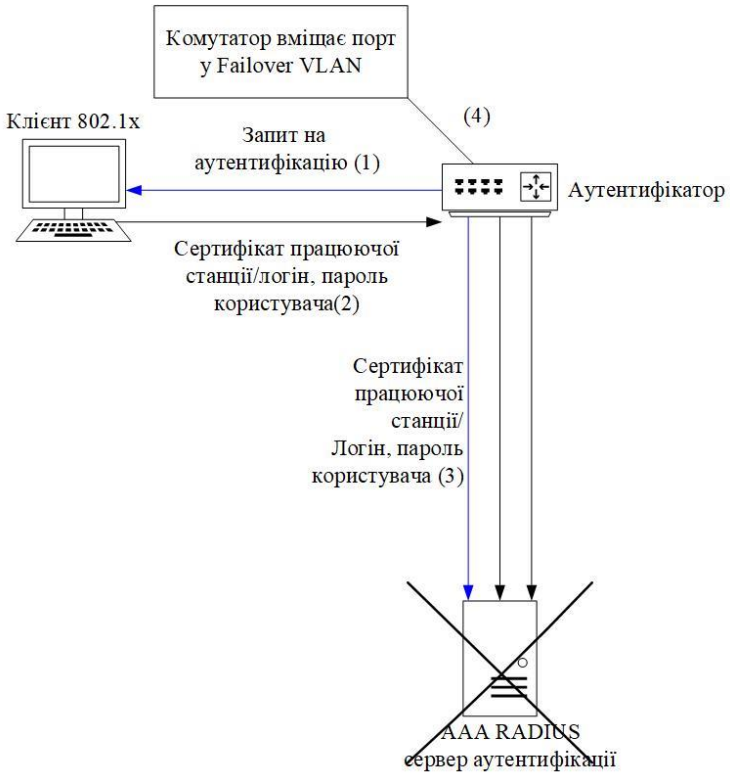


Рисунок 2.3 – Процес виконання функції, якщо клієнт невірно налаштовано

Тут же відзначимо, що з визначенням недоступності сервера RADIUS компанія Cisco Systems здійснила прорив, а саме, після закінчення deadtime таймера, комутатор вважає мертвий сервер RADIUS живим і, якщо він налаштований, то запускає процес переавторизації усіх користувачів, підключених до нього.

2.1.2 Контроль мережевого доступу

Контроль мережевого доступу (NAC) – це комплекс технічних заходів і засобів, який реалізує політики і правила доступу в мережу, який також

забезпечує захист всіх кінцевих пристроїв, що мають до неї доступ, від присутніх всередині загроз безпеки.

Для виконання вимог політик інформаційної безпеки на підприємствах відповідальні співробітники повинні контролювати облікові дані підключилися до сервісів користувачів, інформацію про пристрій, з якого було вироблено підключення, і якими саме програмами співробітник може скористатися в рамках встановленої сесії. Системи NAC дозволяють виконувати це завдання і забезпечити централізоване управління і адміністрування політик доступу співробітників в інформаційне середовище організації.

Дії NAC-системи полягають в тому, щоб з'ясувати, чи безпечно пристрій, робляться спроби підключення до мережі, і чи відповідає його конфігурація певними правилами доступу. Після процедури ідентифікації система приймає рішення про те, який рівень доступу до системних ресурсів необхідно надати.

Паралельно зі збільшенням кількості скоєних зовнішніх атак за допомогою вірусів, хробаків, а також шпигунських програм, рішення NAC продовжують набирати свою популярність. Особливу увагу цього класу продуктів приділяють розробники антивірусних засобів, так як в першу чергу варто розглядати працюють віддалено користувачів як потенційних, навіть якщо і не зумисне, порушників.

Найчастіше компанії, які планують використовувати NAC як засіб захисту від зовнішніх загроз, приходять до висновку, що для забезпечення всіх внутрішніх вимог до такої системи і відповідності внутрішнім політикам інформаційної безпеки необхідно налаштовувати два рішення паралельно. Це залежить в першу чергу від кількості і особливостей вже наявних систем інформаційних технологій всередині корпоративної мережі [15].

2.1.3. Функція відстеження DHCP Snooping

Функція відстеження DHCP (DHCP Snooping) – функція комутатора, яка призначена для захисту від атак з використанням протоколу DHCP (наприклад, підміна або додавання несанкціонованого DHCP-сервера в мережі або атака DHCP starvation, яка змушує DHCP-сервер видати усі існуючі на сервері адреси зловмисникові). Функція DHCP Snooping передбачає наступні дії [11]:

- визначення DHCP-повідомлень від ненадійних (несанкціонованих) джерел (DHCP-серверів) і відфільтровування таких повідомлень,
- розмежування DHCP-повідомлень від надійних та ненадійних джерел з подальшим відкиданням повідомлень або перенаправленням їх на відповідні порти,

- побудова та підтримка бази даних прив’язок, яка містить інформацію про ненадійні вузли з орендованими IP-адресами (вузли, які отримали IP-адреси від несанкціонованих DHCP серверів),
- використання бази даних прив’язок для визначення та фільтрації кадрів від ненадійних вузлів.

2.1.4 Техгологія Dynamic ARP Inspection

Dynamic ARP Inspection – функція комутатора, призначена для захисту від атак з використанням протоколу ARP. Наприклад, атаки ARP-spoofing, що дозволяє перехоплювати трафік між вузлами, які розташовані в межах одного широкомовного домену. Dynamic ARP Inspection регулює тільки повідомлення протоколу ARP і не може вплинути безпосередньо на трафік користувачів або інші протоколи. Для правильної роботи Dynamic ARP Inspection, необхідно вказати які порти комутатора будуть довіреними (trusted), а які – ні (untrusted):

- ненадійні (Untrusted) – порти, до яких підключені клієнти. Для ненадійних портів виконується ряд перевірок повідомлень ARP;
- довірені (Trusted) – порти комутатора, до яких підключений інший комутатор. Повідомлення протоколу ARP отримані з довірених порту не відкидаються.

Якщо порт ненадійний, комутатор перехоплює всі ARP-запити і ARP-відповіді на ненадійних портах перш ніж перенаправляти їх. Комутатор перевіряє відповідність MAC-адреси IP-адресі на ненадійних портах. Перевірка відповідності MAC-адреси IP-адресі може виконуватись на підставі статичних записів або бази даних прив’язки DHCP. Приклад реалізації функції: Використання DAI для CatOS

set security acl arp-inspection dynamic

enable 183 set port arp-inspection 1/3 trust

enable set security acl feature ratelimit 500

Перша команда пов’язує певну VLAN з механізмом DAI, друга – визначає порти, яким «довіряємо», а третя – обмежує смугу пропускання для захисту від DoS-атак. Використання DAI для IOS ip arp inspection vlan 4,104 ip arp inspection trust ip arp inspection limit rate 15 [16].

2.2 Захист кордонів мережі

Міжмережевий екран (МЕ) називається локальним або функціонально розподіленим програмним забезпеченням (програмним забезпеченням), що реалізує управління інформацією, яка надходить в автоматизовану систему та / або виходить з автоматизованої системи. Також зустрічаються загальні назви для брандмауерів та брандмауерів. У зоні будівництва Брендінг (Вогонь, Стіна) називається протипожежною стіною, яка відокремлює окремі блоки багатоквартирного будинку та запобігає поширенню пожежі. МЕ виконує аналогічну функцію для комп'ютерних мереж. За визначенням, МЕ служить контрольною точкою на межі двох ланцюгів. У більшості випадків цей шар лежить між внутрішньою мережею організації та зовнішньою мережею, як правило, Інтернетом (рис. 2.4). Однак, загалом, МП можуть використовуватися для зміни внутрішніх посилань підмережі корпоративної мережі організації.

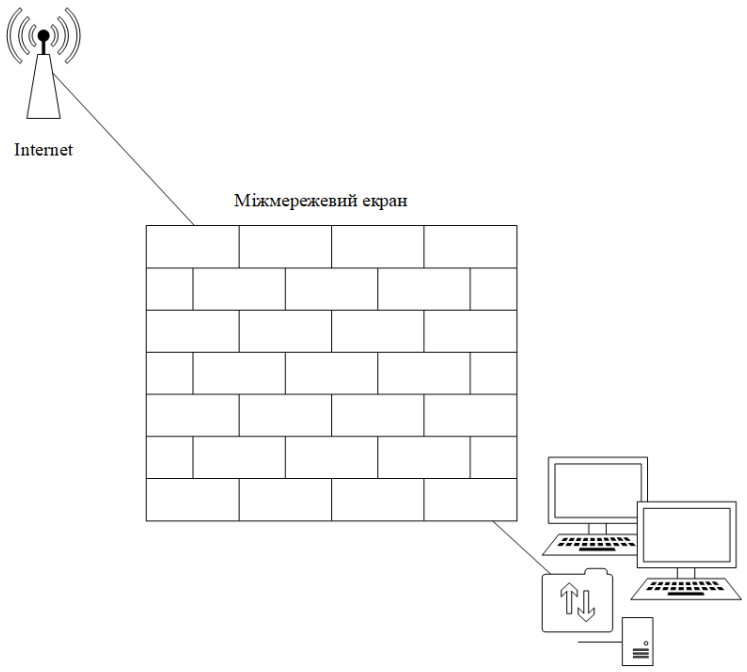


Рисунок 2.4 – Організація мережі

Завданнями МЕ, як контрольного пункту, є:

- контроль всього трафіку, що входять у внутрішню корпоративну мережу;
- контроль всього трафіку, що виходить з внутрішньої корпоративної мережі.

Контроль інформаційних потоків складається з їх фільтрації та перетворення в набір правил. Оскільки сучасна фільтрація МЕ може використовуватися на різних рівнях еталонної моделі взаємодії відкритих систем (EMVOS, OSI), доцільно представити МЕ у формі фільтрувальної системи. Кожен фільтр на основі аналізу проходить через нього, вирішує стрибати далі, прокручувати екран, блокувати або конвертувати дані (рис. 2.5). Ключова функція МЕ є протоколювання інформаційного обміну. Ведення журналів реєстрації дозволяє адміністратору виявити підозрілі дії, помилки в конфігурації МЕ і прийняти рішення про зміну правил МЕ.

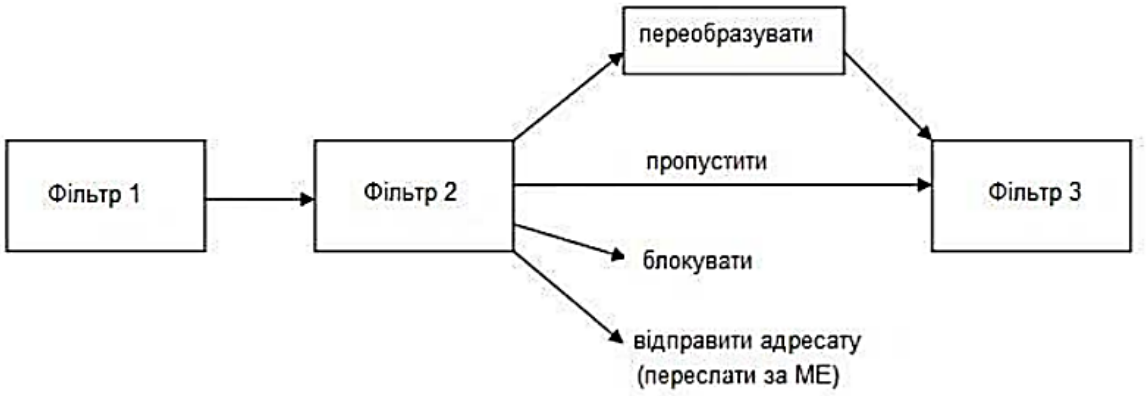


Рисунок 2.5 – Організація мережі

Виділяють таку класифікацію МЕ, у відповідність з функціонуванням на різних рівнях МВОС (OSI):

- мостові екрани (2 рівень OSI);
- фільтруючі маршрутизатори (3 і 4 рівні OSI);
- шлюзи сеансового рівня (5 рівень OSI);
- шлюзи прикладного рівня (7 рівень OSI);
- комплексні екрани (3-7 рівні OSI)

Мостові МЕ. Даний клас МЕ, що працює на 2-му рівні моделі OSI, відомий також як прозорий (stealth), прихований, тіньовий МЕ. Мостові МЕ з’явилися порівняно недавно і представляють перспективний напрям розвитку технологій міжмережевого екранування. Фільтрація трафіку ними здійснюється на канальномурівні, тобто МЕ працюють з фреймами (frame, кадр). До переваг подібних МЕ можна віднести:

– немає необхідності в зміні налаштувань корпоративної мережі, не потрібно додаткового конфігурування мережевих інтерфейсів МЕ;
– висока продуктивність. Оскільки це простіпристрою, вони не вимагають великих витрат ресурсів. Ресурси потрібні або для підвищення можливостей машин, або для більш глибокого аналізу даних;
– прозорість. Ключовим для цього пристрою є його функціонування на 2 рівні моделі OSI. Це означає, що мережевий інтерфейс не має IP – адреси. Ця особливість більш важлива, ніж легкість в налаштуванні. Без IP-адреси цей пристрій не доступно в мережі і є невидимим для навколишнього світу [17].

Схема фільтрації трафіку МЕ забражена на рисунку 2.6.

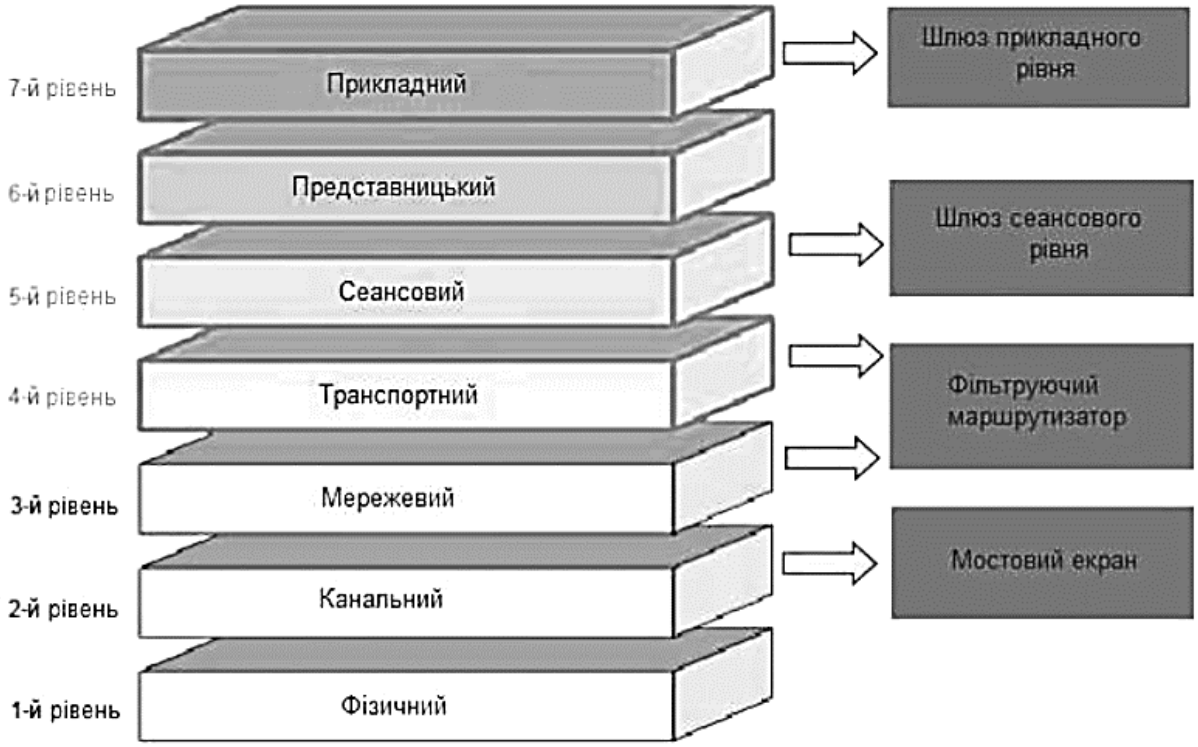


Рисунок 2.6 – Фільтрація трафіку МЕ на різних рівнях MBOS

Фільтруючі маршрутизатори. Packet-filtering firewall (Брандмауер з фільтрацією пакетів) – міжмережевий екран, який є маршрутизатором або комп’ютером, на якому працює програмне забезпечення, сконфігуроване таким чином, щоб фільтрувати певні види вхідних і вихідних пакетів. Фільтрація

пакетів здійснюється на основі інформації, що міститься в TCP- і IP- заголовках пакетів (адреси відправника і одержувача, їх номери портів та ін.) Особливості:

- працюють на 3 рівні;
- також відомі, як ME на основі порту;
- кожен пакет порівнюється зі списками правил (адреса джерела/одержувача, порт джерела/одержувача);
- недорогий, швидкий (продуктивний в силу простоту), але найменш безпечний;
- технологія 20-річної давності;

Приклад: список контролю доступу (ACL, access control lists) маршрутизатора.

Шлюз на рівні сеансу. Шлюз рівня управління – брандмауер, який запобігає прямій взаємодії між авторизованим клієнтом та зовнішнім хостом. По-перше, він приймає запит довіреного клієнта щодо конкретних послуг та підключається до зовнішнього хоста після перевірки законності запитуваного сеансу. Потім шлюз просто копіює пакети в обох напрямках, не фільтруючи їх. На цьому рівні ви можете скористатися функцією перекладу мережевих адрес (NAT). Внутрішні адреси транслюються стосовно всіх пакетів, які виходять із внутрішньої мережі. Ці пакети автоматично перетворюють IP-адреси домашнього комп'ютера в одну IP-адресу, пов'язану із захистом вводу-виводу. В результаті всі пакети, що надходять із внутрішньої мережі, надсилаються до ІУ, виключаючи прямий контакт між внутрішньою та зовнішньою мережею. IP-шлюз рівня сесії стає єдиною активною IP-адресою, що надсилається до зовнішньої мережі. Особливості:

- працює на 4 рівні;
- передає TCP підключення, грунтуючись на порту;
- недорогий, але більш безпечний, ніж фільтр пакетів;
- взагалі потребує роботи користувача або програми конфігурації для повноцінної роботи;
- приклад: SOCKS файрвол.

Шлюз прикладного рівня. Шлюз прикладної рівень – міжмережевья екрана, Який віключає прий взаємодого міжа авторізованім клієнтом і зовнішнім хостом, фільтруючі всі вхідні і вихідні пакети на Прикладні Рівні моделі OSI. Доступні програми, які програмують, користувачі переносять через інтерактивну передачу, що генерує конкретні сервіси TCP / IP [13]. Можливості:

- ідентифікація та аутентифікація користувачів при спробі встановлення з'єднання через МЕ;
- фільтрація потоку повідомлень, наприклад, динамічний пошук вірусів і прозоре шифрування інформації;
- реєстрація подій та реагування на події;
- кешування даних, запитуваних із зовнішньої мережі. На цьому рівні з'являється можливість використання функцій посередництва (Proxy). Для кожного обсуговуваного протоколу прикладного рівня можна вводити програмних посередників
- HTTP-посередник , FTP-посередник і т.д.

Посередник кожної послуги TCP/IP фокусується на обробці повідомлень та виконанні функцій захисту для цієї послуги. Як і шлюз рівня сеансу, шлюз додатків перехоплює вхідні та вихідні пакети, використовуючи відповідні захисні агенти, копіює та спрямовує інформацію через шлюз, і діє як проксі-сервер, уникаючи прямих зв'язків між внутрішніми та зовнішніми посиланнями. Однак шлюзи, що використовуються шлюзом додатків, сильно відрізняються від агентів шлюзу каналу. По-перше, посередники шлюзу додатків призначаються конкретним серверним програмам, а по-друге, вони можуть фільтрувати потік повідомлень на рівні MBOS рівня програми.

Особливості:

- працює на 7 рівні;
- специфічний для додатків;
- помірно дорогий і повільний, але більш безпечний і допускає реєстрацію діяльності користувачів;
- вимагає роботи користувача або програми конфігурації для повноцінної роботи;

Приклад: Web (http) proxy.

МЕ експертного рівня. Stateful inspection firewall – міжмережевий екран експертного рівня, який перевіряє вміст прийнятих пакетів на трьох рівнях моделі OSI: мережевому, сеансовому і прикладному. При виконанні цього завдання використовуються спеціальні алгоритми фільтрації пакетів, з допомогою яких кожен пакет порівнюється з відомим шаблоном авторизованих пакетів. Особливості:

- фільтрація 3 рівня;
- перевірка правильності на 4 рівні;
- огляд 5 рівня;
- високі рівні вартості, захисту і складності;

Приклад: CheckPoint Firewall [16].

Деякі сучасні МЕ використовують комбінацію перерахованих вище методів і забезпечують додаткові способи захисту, як мереж, так і систем. «Персональні» МЕ. Цей клас МЕ дозволяє далі розширювати захист, допускаючи управління по тому, які типи системних функцій або процесів мають доступ до ресурсів мережі. Ці МЕ можуть використовувати різні типи сигнатур і умов, для того, щоб дозволяти або відкидати трафік. Ось деякі із загальних функцій персональних МЕ:

- блокування на рівні додатків;
- дозволяти лише деяким додаткам або бібліотекам виконувати мережеві дії або приймати вхідні підключення;
- блокування на основі сигнатури – постійно контролювати мережевий трафік і блокувати всі відомі атаки.

Додатковий контроль збільшує складність управління безпекою за допомогою потенційно великої кількості систем, які можуть бути захищені особистими брандмауерами. Це також збільшує ризик пошкодження та вразливості через неякісне обладнання.

Динамічні МЕ. Динамічні МЕ об’єднують в собі стандартні МЕ (перераховані вище) та методи виявлення вторгнень, перелічені вище, щоб блокувати мережеві з’єднання, що відповідають певній сигнатурі, і дозволяти

з’єднанням з інших джерел до того ж порту. Наприклад, ви можете заблокувати активність мережевих черв’яків, не заважаючи нормальному трафіку.

Найпростішим рішенням є те, що мережевий брандмауер просто захищає сітку від глобальної. Сервер WWW, FTP-сервер, поштовий сервер та інші сервери також захищені брандмауерами. Особливо обережно слід забезпечити неможливість доступу до захищених локальних мереж через легкодоступні сервери WWW. Схема єдиного захисту локальної мережі показана на малюнку 2.7.

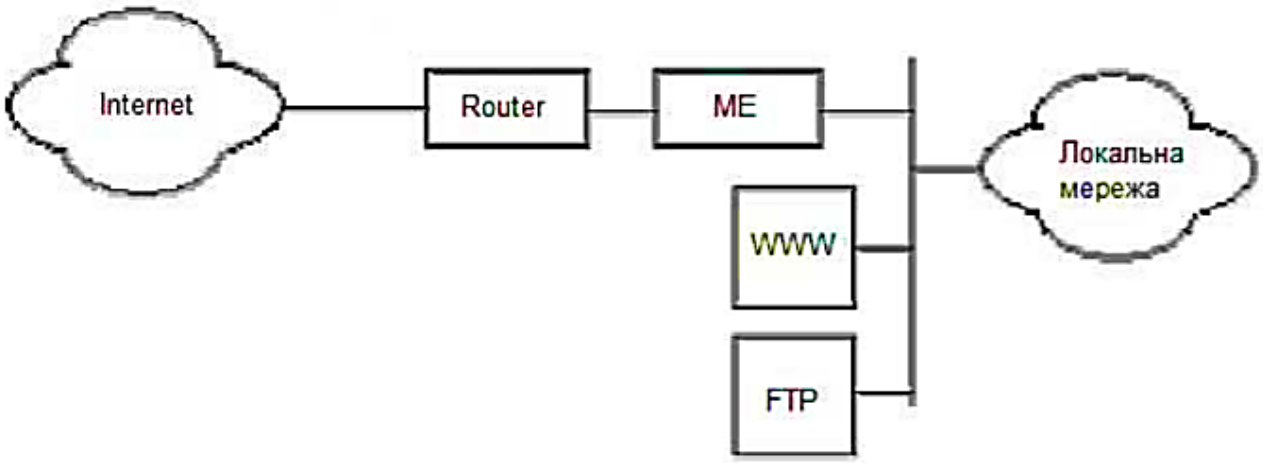


Рисунок. 2.7 – Схема єдиного захисту локальної мережі

Схема захищена закритою і не захищена відкритою підмережами. Для запобігання доступу в локальну мережу, використовуючи ресурси WWW-сервера, рекомендується загально доступні сервери підключати перед міжмережевим екраном. Даний спосіб має більш високу захищеність локальної мережі, але низьким рівнем захищеності WWW FTP-серверів [18]. Схема захищена закритою і не захищена відкритою підмережами зображено на рисунку 2.8.

Окрема схема безпеки для закритих і відкритих підмереж. Ця схема електромонтажу має найвищий рівень безпеки в порівнянні з вищевказаним. Схема заснована на застосуванні двох ME, які захищають окрему закриту і відкриту підмережу (рис 2.9). Ділянка мережі між ME також називається екранованої підмережею або демілітаризованою зоною (DMZ, demilitarized zone).

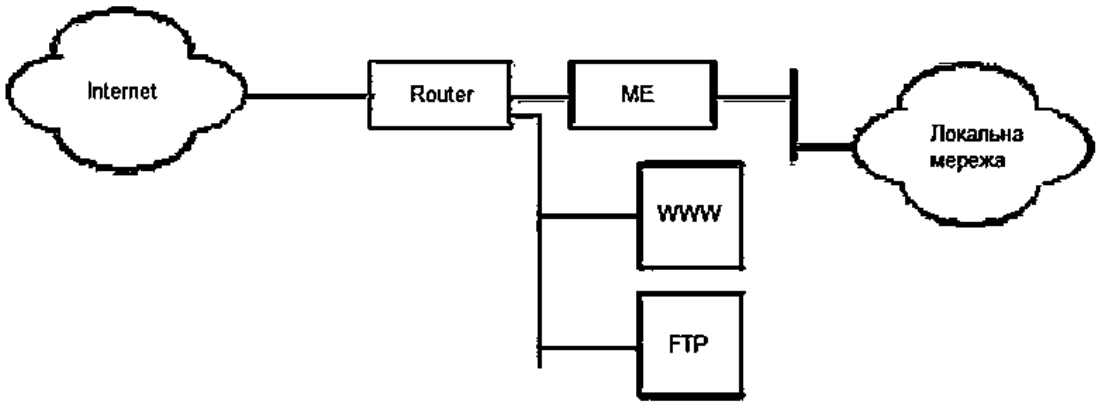


Рисунок 2.8 – Схема захищена закритою і не захищена відкритою підмережами

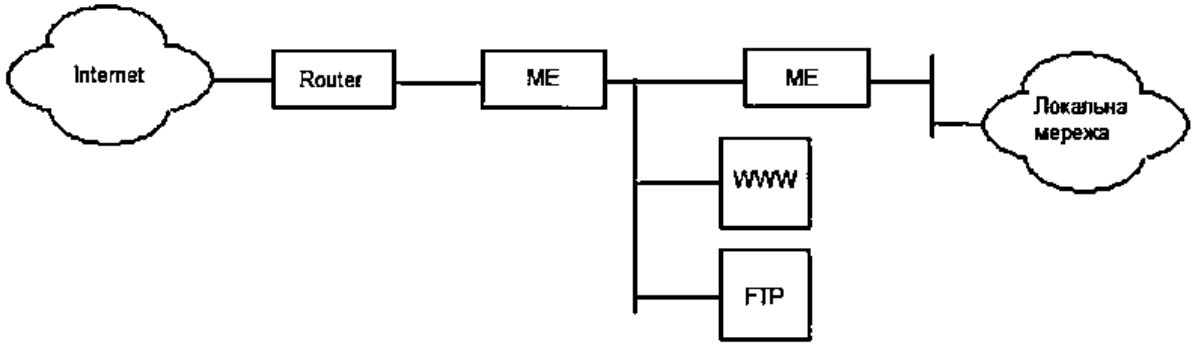


Рисунок 2.9 – Схема з роздільним захистом закритою і відкритою підмережею

2.3 Віртуальна приватна мережа VPN

Віртуальна приватна мережа VPN (Virtual Private Network) являє собою технологію, використовувану для створення приватної мережі через відкриту мережа. Це дозволяє надати доступ за допомогою захищених тунелів, як одиничним віддаленим співробітникам, так і віддаленим локальних мереж до внутрішньої мережі підприємства з будь-якого місця через небезпечну мережу загального користування. Технологія VPN створює віртуальну мережу за допомогою протоколу тунелювання, для досягнення конфіденційності, протоколу, забезпечує туннелювання, передаються дані оброблені протоколом шифрування.

Глобальне мережеве об’єднання засобами VPN має велику цінність для підприємства. Це забезпечує економію витрат, масштабованість і підвищує безпеку і надійність зв’язку.

Гроші є найважливішим активом всіх компаній. VPN економить велика кількість грошей, при створенні локальної мережі. VPN став популярним, тому що його служба віддаленого доступу забезпечує автентифікацію віддаленого користувача. Службу віддаленого доступу було дорого і складно масштабувати за допомогою модемних пулів. Тоді VPN прибутку і підтримує велику кількість можливостей віддаленого доступу під час раннього віку широкосмугового доступу в Інтернет. VPN придбав популярність, пропонуючи більш високу продуктивність, низьку вартість, а також високошвидкісний доступ в Інтернет. VPN може використовуватися як канал глобальної мережі, що економить гроші і допомагає покрити основні витрати WAN.

Масштабованість VPN в порівнянні з іншими технологіями, просто

унікальна. Як збільшувати або зменшувати VPN, необхідно просто надати хосту або шлюзу локальної мережі доступ до глобальної мережі Internet і додати нові аутентифікаційні дані сервера VPN.
Віддалений користувач може підключитися до корпоративної мережі в будь-який час за допомогою VPN. VPN сервер може забезпечити рівну якість з'єднання для кожного користувача.
VPN може бути реалізований в мережі за допомогою апаратних засобів або програмного забезпечення.

2.3.1 Апаратна реалізація VPN

Існує міф про те, що апаратне забезпечення VPN може забезпечити більш високий рівень безпеки, ніж програмне забезпечення. Проте, VPN-пристрій підтримує більш високу продуктивність, і це позначається на швидкості мережі.
Є два типи VPN-пристроїв: окреме апаратний пристрій VPN з спеціалізованої ОС реального часу, що має 2 або більше мережевих інтерфейсу і апаратну криптографічний підтримку, і багатофункціональні пристрої, тобто пристрою іншого призначення (світч, комутатор та ін.), в який вбудовані засоби VPN. Окремі пристрої VPN мають більш високу швидкість передачі даних, ніж багатофункціональні пристрої. Крім того, окремі пристрої мають кілька протоколів аутентифікації (RADIUS, LDAP і Active Directory), в той час як багатофункціональні пристрої підтримують більш обмежений список. Окремі VPN пристрою є більш дорогими, особливо якщо враховувати їх вузьку спеціалізацію, ніж багатофункціональні комбайни.
VPN-пристрої різних виробників можуть працювати як на своїй власній операційній системі, так і на сторонніх ОС (Windows і Linux). Різні типи VPN пристроїв, доступні на ринку від безлічі виробників. Розглянемо кілька відомих мережевих компаній і їх апаратні пристрої VPN.
Juniper Network Secure Access. Він заснований на платформі реального часу і використовує захищений протокол сокетов. пристрої Juniper Network Secure Access 700 і 2000 використовуються для малих і середніх підприємств.
SonicWALL має два бізнес-типу VPN пристроїв. SSL-VPN 2000 на підприємств з кількістю віддалених підключень до 1000 і SSL-VPN 200 для малих компаній приймають до 50 підключень одночасно.
Cisco IOS VPN забезпечує гнучкість в VPN інтермережі, він підтримує різноманітні мережеві середовища, надійність доставки чутливого до затримок трафіка. Також Cisco System випустила окреме обладнання для VPN, яке так і називається Cisco 1720 VPN Access Router (маршрутизатор доступу до VPN). Призначено цей пристрій для встановлення в компаніях малого і середнього розміру.
Рішення ViPNet Custom призначене для об'єднання в єдину захищену віртуальну мережу довільного числа робочих станцій, мобільних користувачів і локальних мереж [8].

2.3.2 VPN програмного рішення

Програмне забезпечення надає основу VPN, дешевше, і порівняно з функціональності з апаратними пристроями. Функції ідентичні в обох VPN системах.
Існує безліч різного як платного, так і безкоштовного, частіше всього з відкритим кодом, програмного забезпечення для створення VPN тунелів.
Openswan є повноцінною реалізацією IPSec для ядер ОС сімейства Linux.
Microsoft розробила і впровадила сервіси VPN в операційні системи сімейства Windows.
OpenVPN є популярним програмним забезпеченням з відкритим вихідним кодом. OpenVPN є кроссплатформенної програмою і прекрасно запускається і функціонує як на Linux машинах, так і на Windows.
З огляду на дорожнечу VPN-пристроїв, а також великої кількості необхідних до підключення в мережу VPN одиночних хостів і необхідності реалізувати нааштування доступу та підтримку її після за допомогою штатних засобів ОС на клієнті, вибір реалізації упав на програмний метод.

2.3.3 Вибір протоколу VPN

Існують різні протоколи для реалізації VPN тунелів і шифрування. З огляду на необхідність використання вбудованого сервісу організації VPN тунелю в ОС Microsoft Windows розглянемо дві основні зв'язки протоколів, що забезпечують захищене тунелювання [8].

Таблиця 2.1 – Порівняльна характеристика протоколів для реалізації VPN

	PPTP	L2TP/IPSec
Походження	Специфікація PPTP не містить опису шифрування та авторизації та покладається на PPP протокол.	Безпечний протокол, формально стандартизований зараз як заміна для PPTP, в разі необхідності підвищеної безпеки.
Шифрування даних	Передані дані, через PPP, шифруються з використанням MPPE (Microsoft's Point-to-Point Encryption protocol). MPPE включає RSA RC4 алгоритми шифрування з ключем довжиною до 128 біт.	Корисні дані, що передаються через мереженезалежні L2TP, шифруються з використанням протоколом з IPSec. RFC 4835 вказує, що для конфіденційності необхідно використовувати алгоритми шифрування AES або 3DES.
Налаштування/ конфігурація	Всі мережеві версії Windows і більшість інших операційних систем, включаючи платформи для мобільних пристроїв, мають вбудовану підтримку PPTP. PPTP вимагає тільки введення логіна з паролем, а також адреси VPN сервера.	Всі версії Windows, починаючи з 2000 / XP і Mac OSX починаючи мати вбудовану підтримку L2TP/IPSec. Основна частина сучасних мобільних платформ, також мають мають вбудовану підтримку цієї технології.
Швидкість	При довжині ключа в 128 біт протокол PPTP може бути по швидкості більш швидким, ніж аналоги, проте різниця в швидкості, швидше за все, не буде значною.	L2T/ IPSEC інкапсулює дані двічі, що трохи сповільнює його роботу щодо інших систем тунелювання.
Порти	PPTP використовує TCP +1723 порт і протокол (ID 47) GRE (General Routing Encapsulation). PPTP може бути легко заблокований провайдером за допомогою обмеження GRE протоколу.	L2TP для установки з'єднання та управління їм потрібні TCP 1701 / UDP 1701, UDP 4500 для NAT операцій. IPSec при динамічної зміні ключів протоколом IEK необхідний UDP 500.
Стабільність / сумісність	Існують деякі проблеми з GRE протоколом, як в деяких мережах провайдерів, так і на деяких приватних роутерах. Так само труднощі представляє кидок GRE через NAT (з локальної мережі назовні)	Велика комплексність L2TP / IPSec призводить до деякої складності в його конфигурировании для надійної роботи між пристроями за NAT

		роутерами. Однак надійність і стабільність цієї зв'язки затверджується його широким застосуванням і практикою використання
Проблеми безпеки	Прекрасно зламується методом man-in-the-middle. MSCHAP-v2 вразливий до АТТАК через брутфорс (підбір ключа через спеціальні словники), а RC4 алгоритм може бути об'єктом bit-flipping атак.	IPSec набагато складніший для злому, однак можливість для аткі man-inthe-middle і досягнення успіху всетаки присутня.
Сумісність клієнтів	Windows, Mac OSX, Linux Apple iOS, Android, DD-WRT	Windows,Mac OSX, Linux iOS,Android

Виходячи з перерахованих особливостей двох наведених типів побудови VPN тунелів, для забезпечення більшої захищеності корпоративних даних слід вибрати зв'язку протоколів L2TP/IPSec.

2.3.4 Структура IPsec

IPsec – це набір протоколів, націлених на забезпечення безпеки IP передачі даних. Його ядро складають три ключові протоколу які виконують ролі механізму обміну, алгоритмів шифрування і обміну ключами.

Так само ключовим поняттям IPSec є SA (Security Association) представляє собою набір параметрів, що характеризують з'єднання (використовувані алгоритми шифрування, хеш-функції, секретні ключі та ін.).

Так як IPSec здатний встановлювати не єдине підключення для зберігання параметрів SA кожного з'єднання використовується SAD (Security Associations Database).

Всі записи SA зберігаються в базі даних SAD IPsec-модуля. кожне SA має унікальний маркер, що складається з трьох елементів:

- індекс параметрів безпеки SPI;
- IP-адреса призначення;
- ідентифікатор протоколу безпеки (ESP або AH).

IPsec-модуль, використовуючи дані параметри, може відшукати в SAD запис про конкретному SA. Крім бази даних SAD, IPsec підтримують таку базу даних, як SPD (Security Policy Database). SPD призначена для співвіднесення приходять IP-пакетів з правилами їх обробки. Записи в SPD складаються з двох полів. В першому зберігаються характерні ознаки пакетів, які дозволяють виділити той чи інший потік інформації. Ці поля називаються селекторами. Друге поле в SPD містить політику захисту, зіставлення даного потоку пакетів.

Селектори використовуються для фільтрації вихідних пакетів з метою зіставлення кожного пакета з певним SA. При надходженні пакета, порівнюються значення відповідних полів в пакеті (селекторні поля) з записаними в SPD. При знаходженні збіги читається поле політики захисту, в якому міститься інформація про те, що робити з даними пакетом: передати без змін, відкинути або обробити.

У разі рішення обробки в цьому ж полі присутнє посилання на відповідний запис SAD. Потім визначається SA для пакета і зв'язаний з нею індекс параметрів безпеки (SPI), після чого виконуються операції IPsec (операції протоколу AH або ESP).

При вхідному пакеті в ньому відразу міститься SPI.

2.3.5 Режими роботи IPsec

IPsec працює в двох режимах: тунельний режим і режим транспорту. У тунельному режимі, захищений з'єднання (тунель) встановлюється між двома маршрутизаторами або шлюзами. Шлюз відповідає за доставку даних на хост. При використанні тунельного режиму, IPsec здатний повністю шифрувати оригінальний IP-пакет. Таким чином тунельний режим роботи IPSec захищає як дані передаються по тунелю, так і інформацію про локальні

мережі, пов’язаних цим тунелем У режимі транспорту IPSec встановлює захищене з’єднання між двома кінцевими вузлами, видимими одне для одного, тобто що знаходяться в межах оной мережі (будь то локальна мережа або мережа Internet). Відповідно IPsec може шифрувати тільки дані IP пакета.

2.3.6 Протоколи IPSec

AH (Authentication Header) – забезпечує цілісність даних шляхом перевірки того, що жоден біт в захищається частини пакета не був змінений у час передачі і аутентифікацію віртуального з’єднання, підтверджуючи, що ми зв’язуємося саме з тим, з ким припускаємо. Однак слід зазначити, що використання AH може викликати труднощі, наприклад, пов’язані з проходженням пакета через NAT, адже NAT необхідно змінити IP адреси пакета для доступу в Internet с закритого локального адреси. Оскільки пакет в такому випадку зміниться, то контрольна сума, вирахувана приймаючою стороною, не співпаде з контрольною сумою AH пакету. AH протокол розроблявся тільки для забезпечення цілісності і не гарантує конфіденційності пакета [10].

ESP (Encapsulating Security Protocol) – інкапсулює протокол безпеки, що забезпечує як цілісність, так і конфіденційність. В режимі транспорту ESP заголовок знаходиться між оригінальним IP заголовком і заголовком TCP (або UDP). У режимі ж тунелю заголовок ESP розміщується між новим IP заголовком і зашифрованим оригінальним IP пакетом. ESP протокол використовує алгоритми шифрування DES, 3DES і AES.

IKE (Internet Key Exchange protocol) – протокол, що зв’язує роботу компонентів IPSEC. IKE здійснює початковий аутентифікацію сторін, обмін загальними секретними ключами.

2.3.7 Атаки на AH, ESP і IKE

Всі види атак на компоненти IPSec можна розділити на наступні групи: атаки, які експлуатують кінцеві ресурси системи (Denial-of-service), атаки, що використовують помилки конкретних реалізації IPSec і, нарешті, атаки, засновані на слабкостях самих протоколів, що входять до складу IPSec (AH, ESP, IKE). Криптографічні атаки можна не розглядати, тому що обидва протоколи визначають поняття Pseudo-Hadamard transform (PHT), куди приховують криптографію. Якщо використовуваний криптоалгоритм стійок, а визначений з ним PHT не вносить додаткових слабкостей, то з цього боку все нормально.

Replay Attack – нівелюється за рахунок використання SA в заголовку поля Sequence Number (правда це не працює при використанні ESP без аутентифікації і без AH).

Denial-Of-Service атака. Як відомо, від цієї атаки не існує повної захисту. Проте, швидка відбраковування поганих пакетів і відсутність якої-небудь зовнішньої реакції на них (згідно RFC) дозволяють більш-менш добре справлятися з такою спробою.

Взагалі, більшості або навіть всім відомим мережевим атакам (sniffing, spoofing, hijacking та ін.) протоколи AH і ESP, при правильному їх застосуванні, успішно протистоять. З IKE трохи складніше. Протокол дуже складний і важкий для аналізу. В силу помилок при його написанні і деяких не надто вдалих рішень (той же HASH_R і HASH_I) він містить деякий кількість потенційних «дірок» (наприклад, в першій фазі не всі Payload в повідомленні автентифіковані). Втім, вони не ведуть до компрометації інформації, а максимум до відмови у встановленні з’єднання.

Від таких атак як replay, spoofing, sniffing, hijacking IKE успішно захищений. З криптографією дещо складніше, так як вона не винесена (як в AH і ESP) окремо, а реалізована всередині самого протоколу. І все ж при використанні стійких алгоритмів і примітивів (PRF), проблем виникати не має.

Слабким місцем IPSec можна було б вважати те, що в якості єдиного обов’язкового до реалізації криптографічного алгоритму в нинішніх специфікаціях вказується DES (як для ESP, так і для IKE), проте 56 біт ключа в наш час вже ніяк не можна вважати достатньо стійким [11].

Однак це формальна слабкість, так як самі специфікації є алгоритм незалежними. До того ж все давно реалізували 3DES і AES.

Таким чином, при правильній реалізації, найбільш реальною для виконання атакою залишається простий Denial-Of-Service.

2.4 Структурна схема багатрівневого інтегрованого захисту

Розробка і впровадження комп'ютерної мережі на підприємстві дозволяє підвищити ефективність його роботи, зокрема підвищити прибуток, покращити якість роботи співробітників, досягти результативної взаємодії усіх відділів підприємства як всередині окремо взятого офісу, так і між віддаленими філіями [3].

При проектуванні корпоративної мережі конкретного підприємства часто не враховують усі можливі загрози і, як наслідок, використовують захист мережі або тільки від зовнішніх загроз або тільки від загроз із середини мережі. Однак, на сьогодні, із збільшенням доступності різних електронних пристроїв і збільшенням їх кількості у користувачів, зростає відсоток загроз саме з боку легальних користувачів мережею [3]. І описаний вище підхід вже не буде забезпечувати повноцінного захисту мережі та інформації, що в ній передається. Тому було запропоновано застосувати багаторівневий інтегрований захист мережі, узагальнену структурну схему якого подано на рисунку 2.10.

При проектуванні корпоративної мережі реального підприємства для забезпечення захисту мережі від внутрішніх загроз використано технологію аутентифікації 802.1x та AAA-сервіс компанії Cisco Systems [3]. Створення безпечного периметру реалізовано шляхом побудови міжмережевих екранів (firewalls), які не пропускають у внутрішню мережу небажаний трафік, що надходить з небезпечних мереж. Реалізація захищеної передачі даних відбувається з допомогою віртуальних приватних мереж VPN та застосуванням протоколу IPsec.

Багаторівневий захист забезпечується шляхом поєднання методів захисту локальної мережі (захист від внутрішніх загроз), створення безпечного периметру та утворення захищеного каналу передачі даних (захист від зовнішніх загроз)[4].

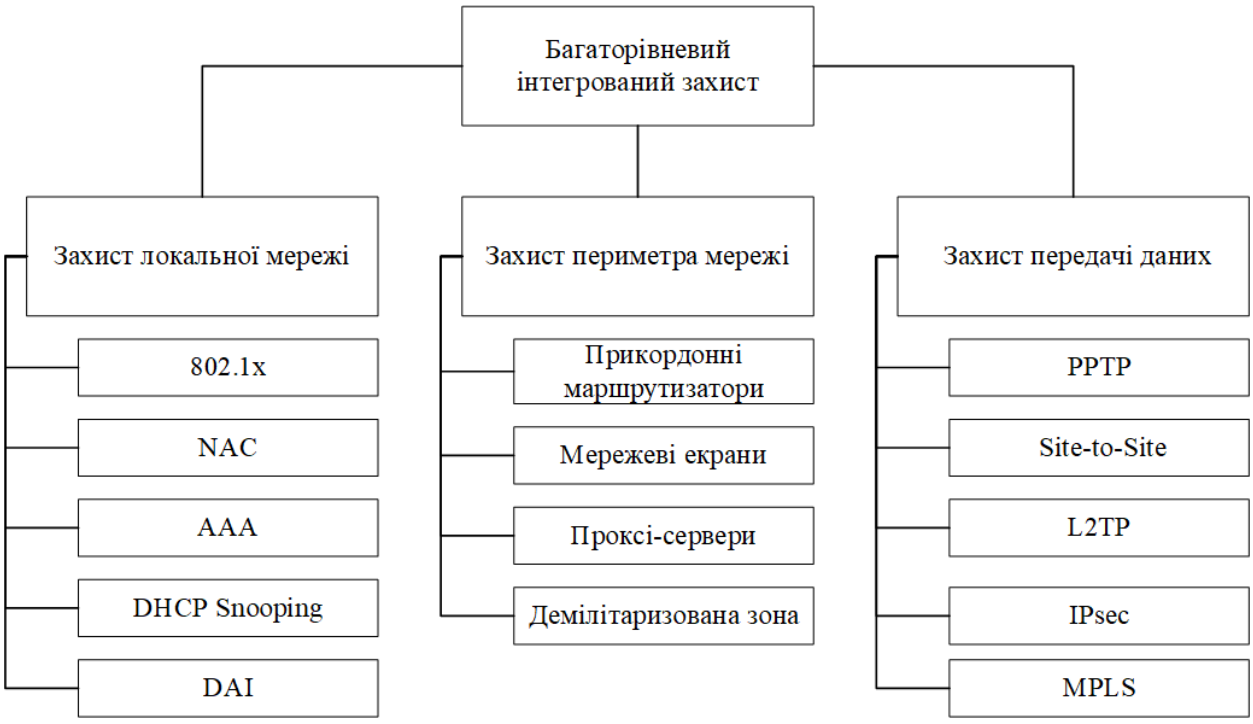


Рисунок 2.10 – Узагальнена схема багаторівневого інтегрованого захисту

Висновки за розілом. Розглянуто системний комплексний підхід, що забезпечує раціональне об'єднання технологій і засобів інформаційного захисту; технологію виявлення вторгнень та активного дослідження безпеки інформаційних ресурсів; захищені віртуальні мережі VPN для захисту інформації, переданої по відкритих каналах зв'язку; застосування розподіленого програмно-апаратного комплексу для захисту корпоративної мережі від зовнішніх загроз при підключенні до загальнодоступних мереж зв'язку; управління

доступом на рівні користувачів та захист від несанкціонованого доступу до інформації; ідентифікацію користувачів шляхом застосування засобів аутентифікації, тощо.

3 ПРОЕКТУВАННЯ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ

За час свого існування підприємство «ITSosed» не одноразово потрапляло під атаки. На далі, для забезпечення свого захисту, компанія вирішила створити надійну захищену мережу на базі обладнання Cisco. Необхідно реалізувати захист для трьох сегментів, а саме для територіальної мережі, віддаленого доступу та доступу до мережі Internet. Також необхідно забезпечити реалізацію механізму захисту даних на серверах, контролю вихідного трафіку, ввести систему авторизації, автентифікації та практику мережевого аудиту.

Мережа підприємства складається з:

- мережі центрального офісу;
- мережі віддаленого офісу;
- дата-центру;

Також в наявності є декілька віддалених клієнтів, яким теж необхідно забезпечити можливість доступу до мережі. Схема мережі компанії подана на рисунку 3.1.

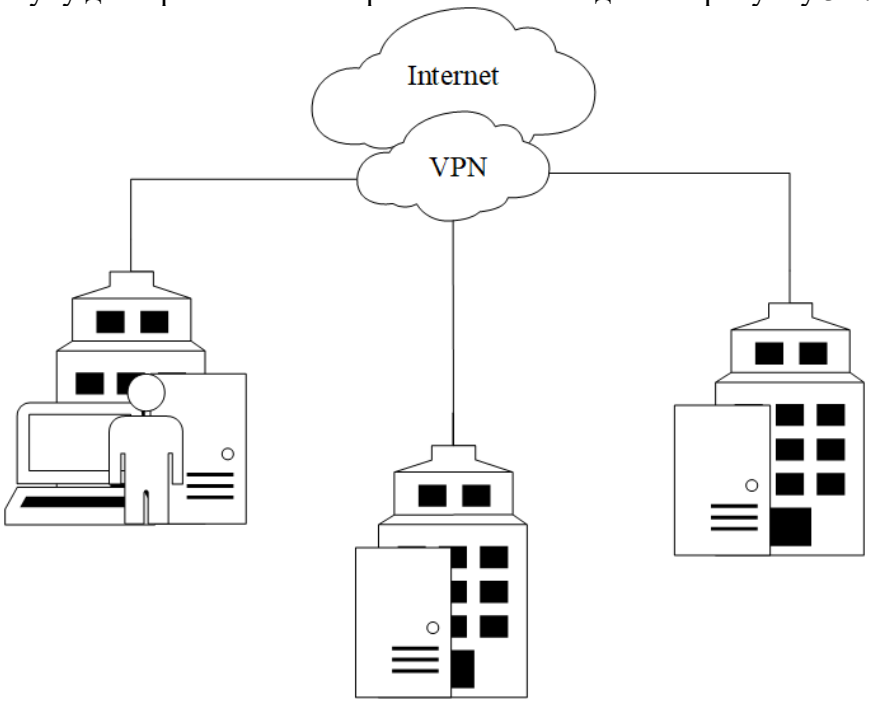


Рисунок 3.1 – Схема мережі підприємства

Метою розробки методу являється забезпечення захисту мережевого середовища даного підприємства.

Підприємство розділено на 3 мережі. Кожна з яких розбита на відділи та розрахований на різну кількість робочих місць. Кожне робоче місце має персональний комп’ютер, підключений до мережі підприємства.

При проектуванні мереж слід використати технологію, яка б надавала співробітникам обмежений доступ до даних, які знаходяться на комп’ютерах розташованих по офісу [17]. Конструкція мережі повинна враховувати

можливість підключення мобільних елементів (ноутбуків), які можуть працювати автономно або можуть підключатися до різних вузлів у мережі.

Проектовані мережі офісів повинні забезпечити:

- можливість накопичування даних;
- працювати з файлами, що зберігаються на будь-якому комп'ютері;
- налагодити для всіх комп'ютерів мережі загальний доступ підключення до Інтернету;
- використовувати один комп'ютер для забезпечення безпеки всієї мережі захисту підключення до Інтернету;
- розсилання повідомлень електронною поштою.

В процесі побудови мереж слід передбачити можливий значний розвиток в майбутньому.

3.1 Реалізація адресної схеми мережі

Виділення адрес один з найбільш трудомістких процесів проектування мережі, вибравши спочатку невірний спосіб розподілу мережевих адрес призведе в майбутньому до таких проблем, як збої в роботі мережі при додавання нових вузлів або мереж. Так як стабільність маршрутизації безпосередньо залежить від числа існуючих в мережі маршрутів і обсягу обчислень, які повинні бути виконані при зміні топології мережі.

Існує кілька типів стратегій адресації:

- «перший прийшов – перший оброблений», адреси для вузлів та мереж виділяються в міру надходження від них заявок; отримана схема адресації при великій мережі викличе проблеми, пов'язані зі стабільністю функціонування;
- структурний принцип розподілу адрес, однакові структурні підрозділи підприємства (відділи) об'єднуються в загальний адресний простір;
- географічний принцип розподілу адрес, кожна філія і центральний офіс мають власний простір для виділення адрес;
- топологічний принцип розподілу адрес, залежить від точки підключення до мережі; даний спосіб гарантує можливість підсумовування маршрутів, необхідний для масштабування мережі.

Для розподілу адрес ПК по філіях використано географічний метод. Усередині філії кожному відділу виділяється своя IP мережа, це необхідно для виконання вимоги безпеки мереж і розмежування різнотипного трафіку.

В таблицях 3.1, 3.2 та 3.3 розміщено інформацію про IP-адреси та маску мережі, яке використовується у захищеній корпоративній мережі підприємства «ITSosed»

Таблиця 3.1 – Розподіл IP-адрес центрального офісу ITSosed

Обладнання	IP-адреса	Маска мережі	Номер VLAN
PC0	172.16.30.103	255.255.255.0	30
PC1	172.16.30.101	255.255.255.0	30
PC2	172.16.30.102	255.255.255.0	30
LaptopAdmin1	172.16.30.90	255.255.255.0	30
PC3	172.16.40.100	255.255.255.0	40
PC4	172.16.40.103	255.255.255.0	40
PC7	172.16.40.102	255.255.255.0	40
PC5	172.16.40.104	255.255.255.0	40

Продовження таблиці 3.1

PC6	172.16.40.101	255.255.255.0	40
LaptopAdmin2	172.16.40.90	255.255.255.0	40
PC8	172.16.30.100	255.255.255.0	30
PC9	172.16.30.104	255.255.255.0	30

Таблиця 3.2 – Розподіл IP-адрес віддаленого офісу ITSosed

Обладнання	IP-адреса	Маска мережі	Номер VLAN
PC11	172.17.35.102	255.255.255.0	35
PC12	172.17.35.101	255.255.255.0	35
PC10	172.17.35.103	255.255.255.0	35
LaptopAdmi3	172.17.35.90	255.255.255.0	35
PC13	172.17.45.103	255.255.255.0	45
PC14	172.17.45.100	255.255.255.0	45
PC15	172.17.45.101	255.255.255.0	45
PC16	172.17.45.104	255.255.255.0	45
PC17	172.17.45.102	255.255.255.0	45
LaptopAdmin4	172.17.45.90	255.255.255.0	45
PC18	172.17.35.104	255.255.255.0	35
PC19	172.17.35.108	255.255.255.0	35

Серверному блоку привласнено статичні адреси, які присвоєні серверу у ручну. Він прописується адміністратором мережі в налаштуваннях протоколу TCP/IP на кожному сервері мережі і жорстко закріплюється за сервером.

Перевага: постійна відповідність IP-адресів певним серверам.

У привласненні статичних адрес є певні недоліки:

- адміністратор мережі повинен вести облік всіх використовуваних адрес, щоб виключити повтори;
- при великій кількості комп'ютерів в локальній мережі установка і налаштування IP-адресів віднімають багато часу.

Таблиця 3.3 – Розподіл IP-адрес центра обробки даних ITSosed

Обладнання	IP-адреса	Маска мережі	Номер VLAN
PC20	172.18.3.151	255.255.255.0	3
PC21	172.18.3.150	255.255.255.0	3
Web Server	172.18.3.1	255.255.255.0	3
TFTP Server	172.18.3.2	255.255.255.0	3

Для комп'ютерів центрального та віддаленого офісу, а також центра обробки даних привласнено динамічні IP-адреса, тобто адреса призначається автоматично службою DHCP у діапазоні. При кожному підключенні комп'ютера до локальної мережі адреса може мінятися, але завжди залишатися в межах заданого діапазону. Функція автоматичного призначення IP-адреса гарантує унікальність видаваної IP-адреса. У мережах, керованих сервером, динамічна IP-адрес призначається спеціальною серверною службою DHCP. Сервер, на якому працює ця служба, називається DHCP-сервер. Комп'ютер, який отримує IP-адрес з мережі, називається DHCP-клієнт.

Таблиця 3.4 – Розподіл IP-адрес серверного блоку ITSosed

Обладнання	IP-адреса	Маска мережі	Номер VLAN
NTP Server	172.18.3.3	255.255.255.0	3
DNS Server INT	4.2.2.1	255.255.255.0	2
Mail Server INT	4.2.2.2	255.255.255.0	2
Web Server INT	4.2.2.3	255.255.255.0	2
Radius Server	4.2.2.3	255.255.255.0	2

3.2 Впровадження сучасних мережевих технологій в структуру компанії ITSosed

3.2.1 Налаштування VPN з використанням IPsec

Всі філіали ITSosed налаштовано через VPN з використанням IPsec для трафіку, що проходить між відповідними мережами. IPsec забезпечує передачу конфіденційної інформації в захищеному режимі по незахищеним мереж, таким як Інтернет. IPsec діє як протокол мережного рівня, забезпечуючи захист і

аутентифікацію IP пакетів між що беруть участь в зв'язку пристроями IPsec (рівноправними вузлами), такими як маршрутизатори Cisco(рис. 3.2).

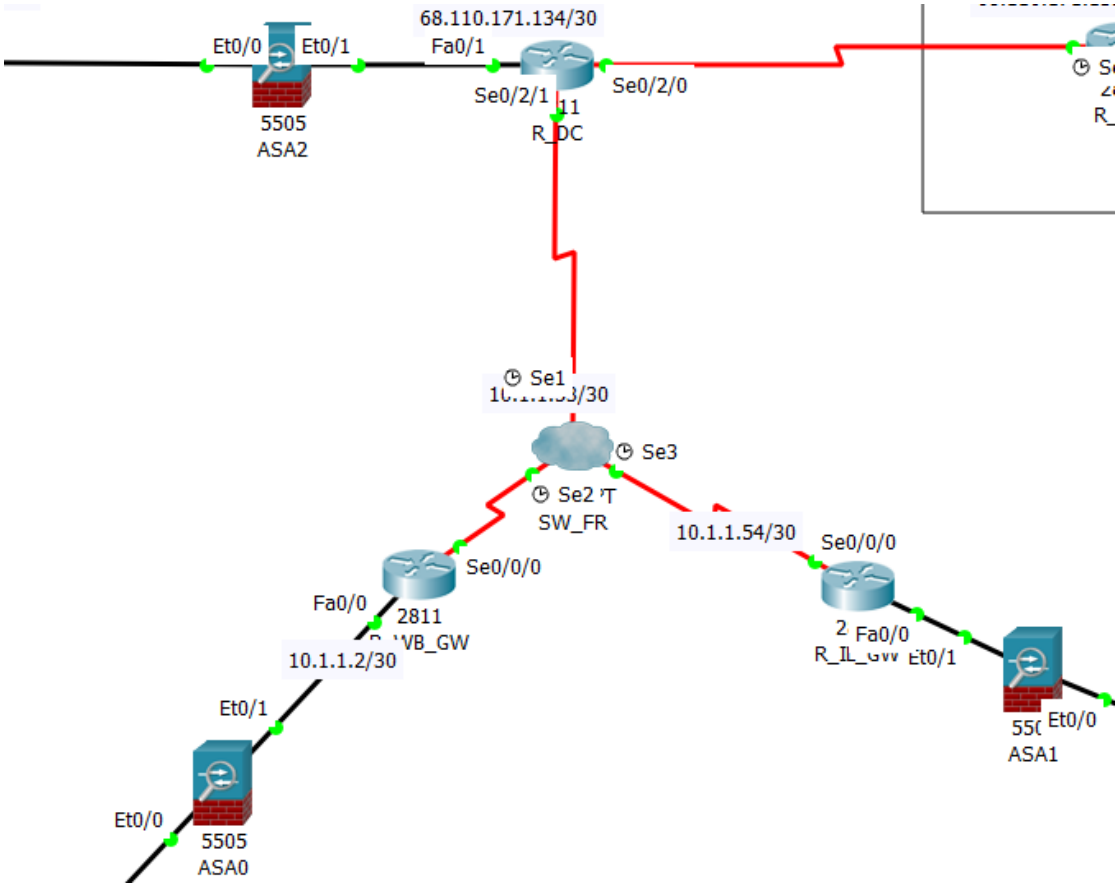


Рисунок 3.2 – Схема з'єднання філіалів ITSosed на основі технології VPN

Конфігурація для налаштування VPN тунелю складається з таких етапів:

- створення інтерфейсу використовуючи команду interface tunnel 0;
- призначення IP-address;
- ідентифікація інтерфейсу відправника за допомогою команду tunel source
- ідентифікація інтерфейсу отримувача використовуючи команду tunnel destination
- налаштування протоколу інкапсуляції командою tunnel mode gre

Приклад налаштування на одному з роутерів зображено на рисунку 3.3.

```
R_WB_GW(config)#interface tunnel 0
R_WB_GW(config-if)#ip address 10.1.1.53 255.255.255.252
R_WB_GW(config-if)#tunnel source serial 0/0/0
R_WB_GW(config-if)#tunnel destination 68.110.171.134
R_WB_GW(config-if)#tunnel mode gre ip
R_WB_GW(config-if)#
```

Рисунок 3.3 – Приклад налаштування GRE Tunnel на роутері R_WB_GW

Функція Port Security дозволяє налаштувати будь-який порт комутатора так, щоб доступ до мережі через нього міг здійснюватися тільки певними 162 пристроями. Пристрої, яким дозволено підключатися до порту, визначаються за MAC-адресами. MAC-адреси можуть бути призначені динамічно або вручну налагоджені адміністратором мережі.Також, функція Port Security дає можливість обмежувати кількість MAC-адрес, що вивчаються портом, тим самим обмежуючи кількість вузлів, що підключаються до нього.

Налаштування комутатора здійснюється таким чином:

– активізувати функцію Port Security на відповідних портах і заборонити вивчення MAC-адрес (параметр maxlearningaddr встановити рівним 0).

config port_security ports 1-24 admin_state enabled max_learning_addr 0

– створити записи в статичній таблиці MAC-адрес (ім’я VLAN в прикладі «default»).

create fdb default 05-50-BA-00-00-01 port 2

create fdb default 05-50-BA-00-00-02 port 2

create fdb default 05-50-BA-00-00-03 port 2

create fdb default 05-50-BA-00-00-04 port 2

create fdb default 05-50-BA-00-00-05 port 8

3.2.2 Налаштування аутентифікації 802.1x

Стандарт IEEE 802.1X використовується для підтримки аутентифікації за допомогою сервера аутентифікації і визначає процес інкапсуляції даних EAP, що передаються між клієнтами і серверами аутентифікації. Стандарт IEEE 802.1X здійснює контроль доступу і не дозволяє неавторизованим пристроям підключатися до локальної мережі через порти комутатора

Для налаштування аутентифікації користувачів за стандартом IEEE 802.1X необхідно визначити наступні три ролі (рис. 3.4):

- клієнт (client/supplicant);
- аутентифікатор (authenticator);
- сервер аутентифікації (authentication server).

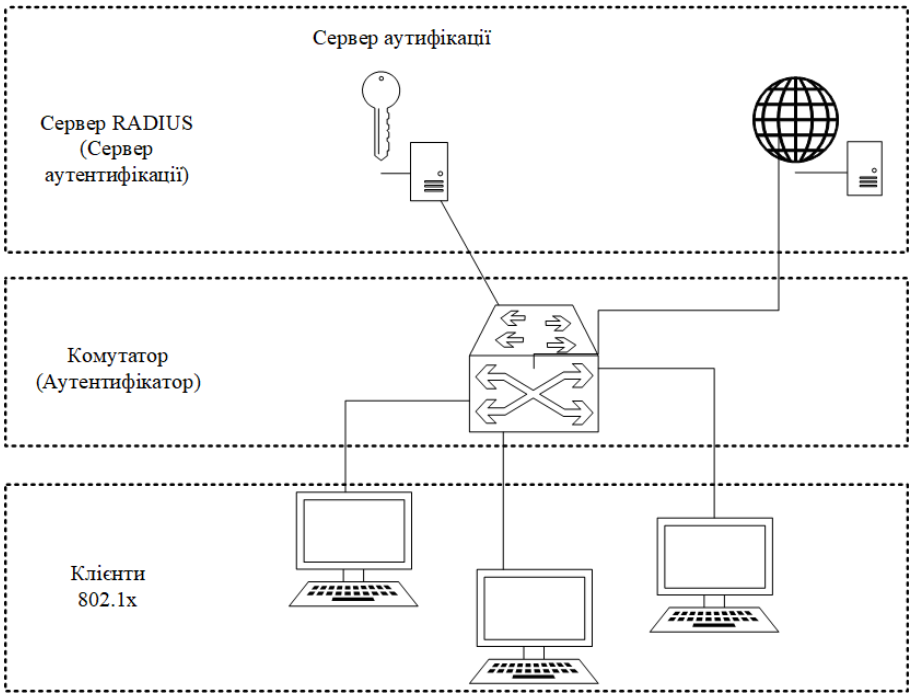


Рисунок 3.4 – Мережа з аутентифікацією 802.1x

Для налаштування зв’язку з RADIUS сервером необхідні наступні команди в режимі глобальної конфігурації:

aaa new-model

aaa authentication dot1x default group radius

aaa authorization network default group radius

radius-server dead-criteria time 5 tries 4

radius-server deadtime 30

radius-server host 4.2.2.3 key SecretKey12568

dot1x system-auth-control

Для налаштування окремого порта слід використати такі команди:

interface GigabitEthernet1/0/1

switchport mode access

authentication port-control auto

authentication violation protect

dot1x pae authenticator

dot1x timeout quiet-period 5

dot1x timeout server-timeout 10

dot1x timeout tx-period 5

spanning-tree portfast

3.2.3 Налаштування VLAN

Технологія VLAN дозволяє розділяти мережу на логічні сегменти. Кожен такий логічний сегмент має свій широкомовний домен. VLAN часто використовується для поділу IP сегментів мережі, з подальшою маршрутизацією і фільтрацією трафіку між різними VLAN на маршрутизаторі або на L3 комутаторі. Перед налаштуванням VLAN на комутаторі, необхідно визначитися чи буде в мережі використовуватися протокол VTP (VLAN Trunking Protocol) чи ні.

Налаштування VLAN на комутаторі можна виділити в три етапи: створення VLAN, налаштування портів, перевірка [18].

Для створення VLAN потрібно увійти в привілейований режим та при необхідності ввести пароль (команда «enable»), переключитися в режим глобального конфігурування (команда «configure terminal»), створити VLAN командою « vlan id», де id – номер VLAN (після створення, консоль виявиться в режимі конфігурації VLAN, де можна задати перераховані вище параметри для VLAN)(рис. 3.5). Далі потрібно поставити необхідні параметри, для створеного VLAN (наприклад ім’я).

```
SW_NY_2#en
SW_NY_2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW_NY_2(config)#vlan 1
SW_NY_2(config-vlan)#vlan 10
SW_NY_2(config-vlan)#vlan 30
SW_NY_2(config-vlan)#vlan 40
SW_NY_2(config-vlan)#
```

Рисунок 3.5 – Створення VLAN

Щоб налаштувати портів свіча необхідно виконати такі дії:

- увійти в привілейований режим (команда: «enable»);
- увійти в режим глобального конфігурування (команда: «configure terminal»);
- увійти в режим конфігурації мережевого інтерфейсу (команда: «interface interface-id», де interface-id – ім’я та номер інтерфейсу, наприклад «interface FastEthernet0/1»);

– задати динамічний режим порту / інтерфейсу (команда: «switchport mode dynamic auto »);
– задати VLAN, який буде на інтерфейсі, якщо порт перейде з режиму trunk в режим access, за замовчуванням VLAN 1 (команда: «switchport access vlan vlan-id», де vlan-id – номер VLAN)(рис. 3.6);

```
SW_NY_2(config)#int fa 0/5
SW_NY_2(config-if)#sw m acc
SW_NY_2(config-if)#sw acc vl 40
```

Рисунок 3.6 – Приклад налаштування порта свіча в режимі Access

– задати Native VLAN, для IEEE 802.1q транка, за замовчуванням Native VLAN 1 (команда: «switchport trunk native vlan vlan-id», де vlan-id – номер Native VLAN)(рис. 3.7);

```
SW_NY_2(config-if)#int fa0/24
SW_NY_2(config-if)#sw m tr
SW_NY_2(config-if)#sw tr na vl 99
```

Рисунок 3.7 – Приклад налаштування порта свіча в режимі Access

– включити порт / інтерфейс (команда: « no shutdown») ;
– вийти з режиму конфігурації інтерфейсу (команда: «exit» або «end»).

Для перевірки налаштування VLAN на комутаторі використовуємо команду «show vlan»(рис.3.8).

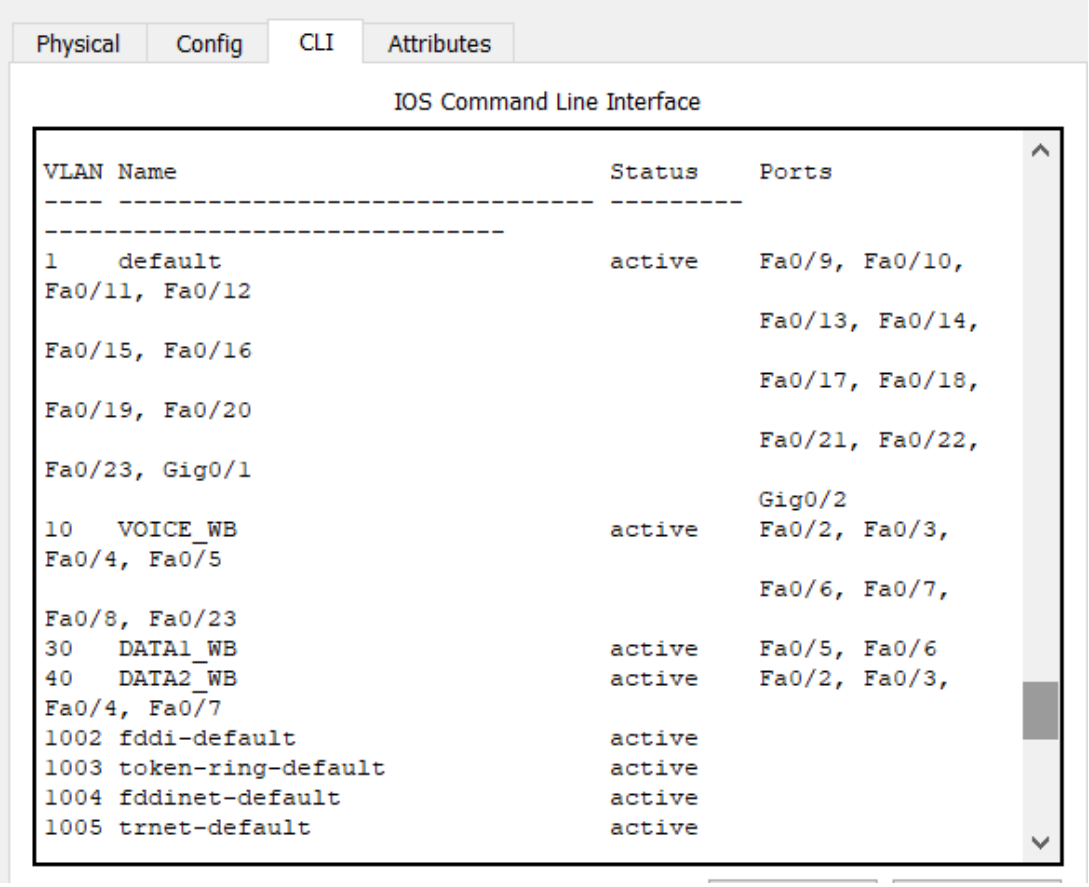


Рисунок 3.8 – Результат налаштування VLAN

VTP – VLAN Trunking Protocol, дозволяє полегшити адміністрування комутаторів, а саме управління VLAN-ами на комутаторах Cisco. За допомогою VTP можна створювати, змінювати або видаляти VLAN-и на VTP сервері всі ці зміни автоматично перенесяться на комутатори в одному домені VTP. Існує три режими роботи VTP (VTP mode):

1) VTP Server – серверний режим. В цьому режимі можна створювати, видаляти і змінювати VLAN-и, а так само задавати різні параметри, такі як версію протоколу (vtp version), vtp фільтрацію (vtp pruning) для всього VTP домену. VTP сервер сповіщає про свою конфігурацію VLAN-ів інших комутаторів, що знаходяться в тому ж VTP домені, і синхронізує їх конфігурацію VLAN. Так само VTP сервер може синхронізувати свою конфігурацію з конфігурацією VTP клієнта, якщо у клієнта вище рівень редакції конфігурації. Обмін VTP інформацією відбувається через транкові порти [14].

2) VTP Client – режим клієнта. На комутаторі з режимом VTP Client можна створювати, видаляти або змінювати VLAN-и. Все налаштування VLAN-ів комутатор бере від VTP сервера.

3) VTP Transparent – прозорий режим. В цьому режимі комутатор не застосовує собі конфігурацію VLAN від VTP сервера і не сповіщає про свою конфігурацію іншім комутаторам, але дозволяє пропускати через свої транкові порти VTP сповіщення від інших комутаторів.

Перед налаштуванням VTP потрібно знати:

- всі комутатори в мережі повинні мати однакове ім’я домену VTP (VTP domain);
- всі комутатори в одному VTP домені повинні використовувати одну й ту ж саму версію протоколу VTP (VTP version);
- всі комутатори в одному VTP домені повинні використовувати один і той же VTP пароль, якщо він встановлений (VTP password);
- всі VTP сервера, повинні мати однаковий рівень редакції конфігурації, і цей номер повинен бути найбільшим в VTP домені (VTP revision number);
- У версії протоколу 1 і 2 анонсуються VLAN-и тільки з основного (VLAN 1-1005) діапазону, якщо потрібен розширений діапазон (VLAN 1006-4094), то слід використовувати версію VTP 3.

Для отримання інформації про конфігурування VTP можна використовувати команду «show vtp status» – вона відображає загальну інформацію про VTP(в якому режимі працює комутатор, яке ім’я VTP домена, яка версія протоколу та інше)(рис. 3.9).

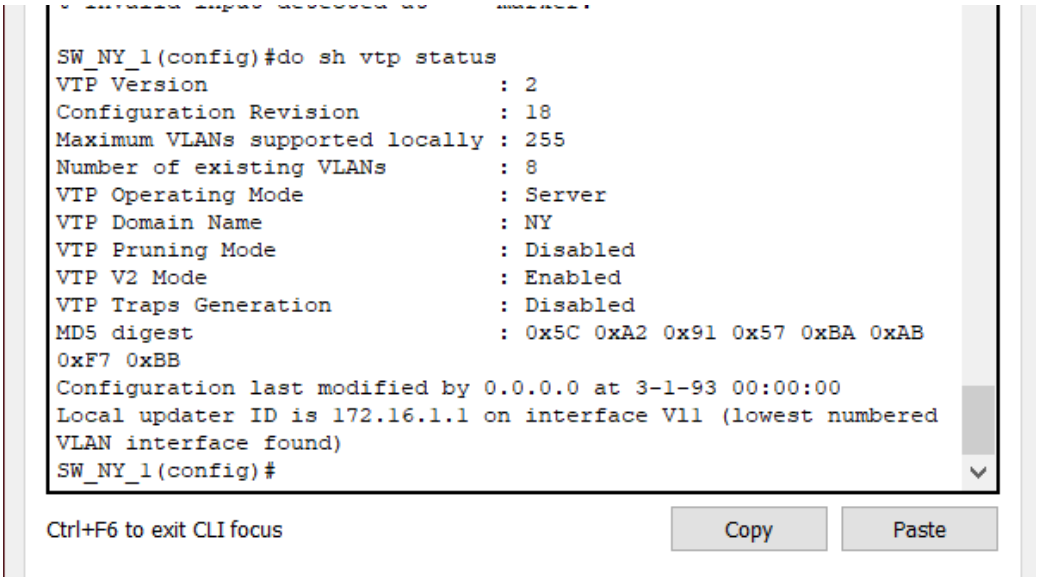


Рисунок 3.9 – Результат конфігурування Cisco VTP

На шлюзовому маршрутизаторі налаштовано порт FastEthernet у підмережі VLAN 40, порт на комутаторі VLAN та DHCP-пули для мереж VLAN 30 та 40.
Мережевий інтерфейс FastEthernet0/0 розбито на три vlan`а. На інтерфейсі FastEthernet0/0.10 налаштовано 172.16.10.0, FastEthernet0/0.30 – 172.16.30.0 та FastEthernet0/0.40 – 172.16.40.0. Далі представлено налаштування DHCP-пулів.
ip dhcp pool FORVLAN40
мережа 172.16.40.0 255.255.255.0
default-router 172.16.40.254
dns-сервер 4.2.2.2
ip dhcp pool FORVLAN30
мережа 172.16.30.0 255.255.255.0
default-router 172.16.30.254
dns-сервер 4.2.2.2
ip dhcp pool FORVLAN10_VOICE
мережа 172.16.10.0 255.255.255.0
default-router 172.16.10.254
option 150 ip 172.16.10.254
На рисунку 3.10 зображено поточну працюючу конфігурацію шлюзового роутера.

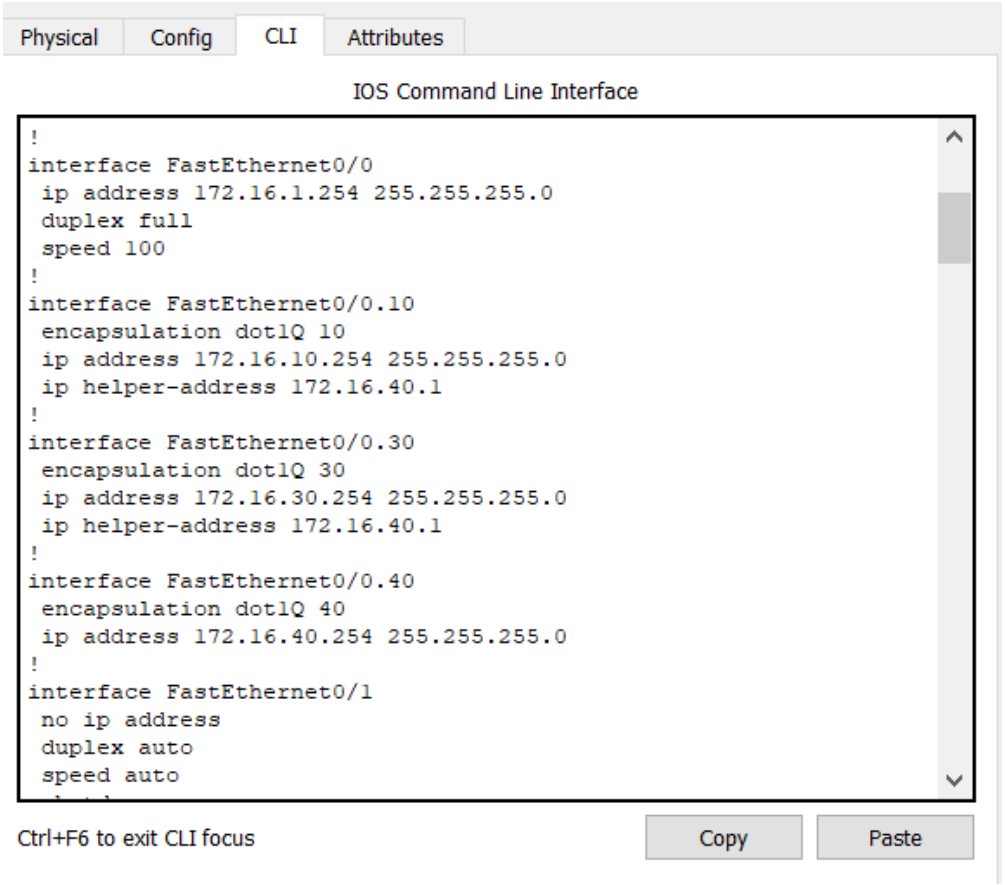


Рисунок 3.10 – Конфігурування шлюзового маршрутизатора

DHCP-сервер надає адміністратору ряд переваг. Головне – економія часу, що виникає внаслідок відмови від ручного налаштування кожної машини. Нові комп'ютери частіше постачаються з попередньо встановленою ОС, тому якщо такий комп'ютер вже сконфігуровано як DHCP-клієнт, можна підключити його до мережі, і у нього відразу ж буде автоматично присвоєна IP-адреса.
Первинне присвоєння IP-адреси – не єдине, на що економиться час. DHCP спрощує і інші адміністративні завдання. А зокрема, легко можна перемістити комп'ютер з однієї підмережі в іншу.
У DHCP є переваги і для користувачів. Користувачі ноутбуків, наприклад, не зможуть підключитися до мережі, якщо адреси виділяються вручну. Однак клієнти, що підтримують DHCP, за підключенням відразу отримують нові дійсні IP-адреси.
Крім того, DHCP дозволяє здійснювати спільне використання IP-адрес. Кожного разу під час підключення до мережі співробітник отримує IP-адресу. Після вимкнення система відновлює адресу, щоб видати його наступному користувачеві [19].

3.3 Маршрутизація в захищеній корпоративній мережі

У мережі присутні маршрутизатори двох типів: маршрутизатори ядра і маршрутизатори рівня доступу.

Основне призначення маршрутизаторів ядра – швидке пересилання пакетів. В ядрі не рекомендується застосовувати списки доступу, політики маршрутизації та інші технології, що зменшують швидкість обробки пакетів.

На маршрутизаторі ядра потрібно вказати параметри, загальні для всіх пристроїв, налаштувати мережеві інтерфейси і протокол маршрутизації [19].

Налаштування протоколу маршрутизації полягає в наступному:

- встановлюється протокол маршрутизації;
- вказуються обслуговуючі мережі;
- настройка додаткових параметрів (для усунення зациклення, тимчасові, управління оновленнями).

Маршрутизатор рівня доступу обробляють меншу кількість пакетів. Разом з тим, їх часто використовують для виконання додаткових функцій.

Маршрутизатор доступу до Інтернет крім аналогічної фільтрації пакетів повинен виконувати трансляцію внутрішніх і зовнішніх адрес.

Після налаштування параметрів, спільних для всіх пристроїв, необхідно виконати настройку мережевих інтерфейсів в режимі конфігурації.

Як протоколу внутрішньої маршрутизації виберемо фірмовий протокол фірми Cisco EIGRP. Він був розроблений компанією Cisco Systems, а отже, часто використовується на обладнанні цієї компанії.

Даний протокол має наступні якості:

- більш швидка збіжність в порівнянні з іншими протоколами на базі вектора відстаней, яка досягається завдяки алгоритму DUAL (Diffusing Update Algorithm); алгоритм становить таблицю топологій, в якій зазначено два кращих шляху до мережі призначення (основний і резервний); на обох цих маршрутах не виникають петлі;
- зниження споживання смуги пропускання досягається за рахунок того, що при будь-яких змінах у мережі, алгоритм DUAL відправляє тільки нові оновлення, а не всю таблицю маршрутизації;
- підтримка декількох протоколів мережевого рівня (IP, IPX, AplleTalk);
- безкласовий протокол маршрутизації;

Принцип роботи протоколу EIGRP:

1) Протокол EIGRP спочатку повинен виявити своїх сусідів, для цього він використовує протокол Hello, який в свою чергу розсилає hello-пакети

(за замовчуванням кожні 5 секунд). Для відправки пакетів використовується багатоадресна розсилка.

2) Після того, як сусіди встановлені, відбувається обмін інформацією про топологію мережі. Спочатку пересилається інформація про повну топологію мережі між маршрутизаторами. А далі, при зміні на мережі, маршрутизатори обмінюються наступними пакетами:
   - пакет оновлень маршрутів (Update) – у цих пакетах зберігається інформація про зміну маршрутів; пакети можуть пересилатися по багатоадресній або одноадресній розсилці;
   - пакет запитів (Query) – необхідний, коли маршрутизатор немає резервного маршруту і перераховує будь-який; маршрутизатор відправляє запит сусідам, якщо у сусідів є маршрут, то вони відповідають шляхом посилки пакета відповіді на запит (Reply), якщо маршруту немає, то вони відправляють запит уже своїм сусідам;
   - крім цього, при отриманні вище зазначених пакетів (update, query, reply), у відповідь надсилається пакети підтвердження (Acknowledgment).

Для гарантованої доставки відправлених пакетів протокол EIGRP використовує надійний транспортний протокол (Reliable Transport Protocol – RTP). Протокол повторно пересилає маршрутну інформацію, якщо повідомлення було втрачено. За рахунок використання протоколу RTP зменшується ймовірність виникнення петель.

3) Далі відбувається вибір найкращого шляху. Маршрутизатор аналізує топологічну таблицю і вибирає з неї шлях з найменшою метрикою.

Таким чином, маршрутизатори, що працюють на основі протоколу EIGRP, підтримують три таблиці:

- таблиця сусідів, в якій вказані всі сусіди;
- таблиця топології, в якій записуються маршрутів до кожного місця призначення, відомі маршрутизатора;
- таблиця маршрутизації, куди заносяться кращі маршрути з таблиці топології.

Для налаштування протоколу динамічної маршрутизації EIGRP на роутері R_WB_GW необхідно активувати EIGRP, використовуючи Process ID 1:

R_WB_GW(config) # router eigrp 1

Використавши команду network, сконфігуровано маршрутизатор для анонсування мережі 172.16.0.0:

R_WB_GW (config-router) #network 172.16.0.0

Налаштовано анонсування мережі 10.1.1.1/24:

R_WB_GW (config-router) # network 10.1.1.1 0.0.0.255

Аналогічно налаштовано й інші маршрутизатори. Застосувавши команду «show ip eigrp neighbors» виведено таблицю сусідніх EIGRP-маршрутизаторів(рисунок 3.11).

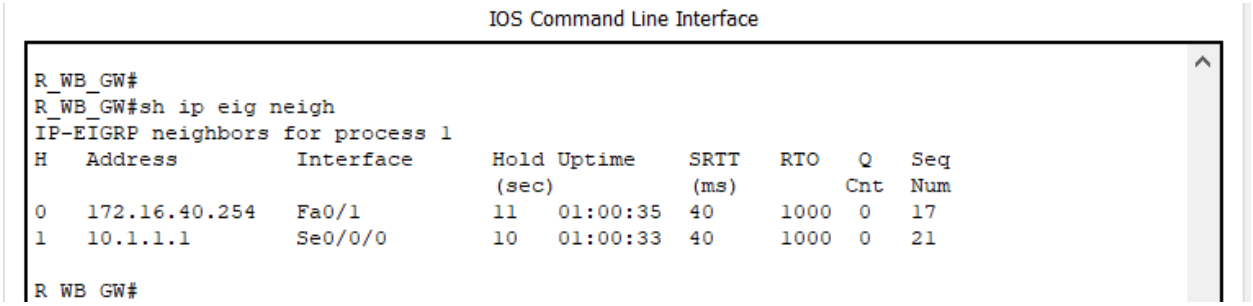


Рисунок 3.11 – Таблиця сусідніх EIGRP-маршрутизаторів

Детальну інформацію по виконаному протоколу динамічної маршрутизації виведено за допомогою команди «show ip protocols»(рис. 3.12).

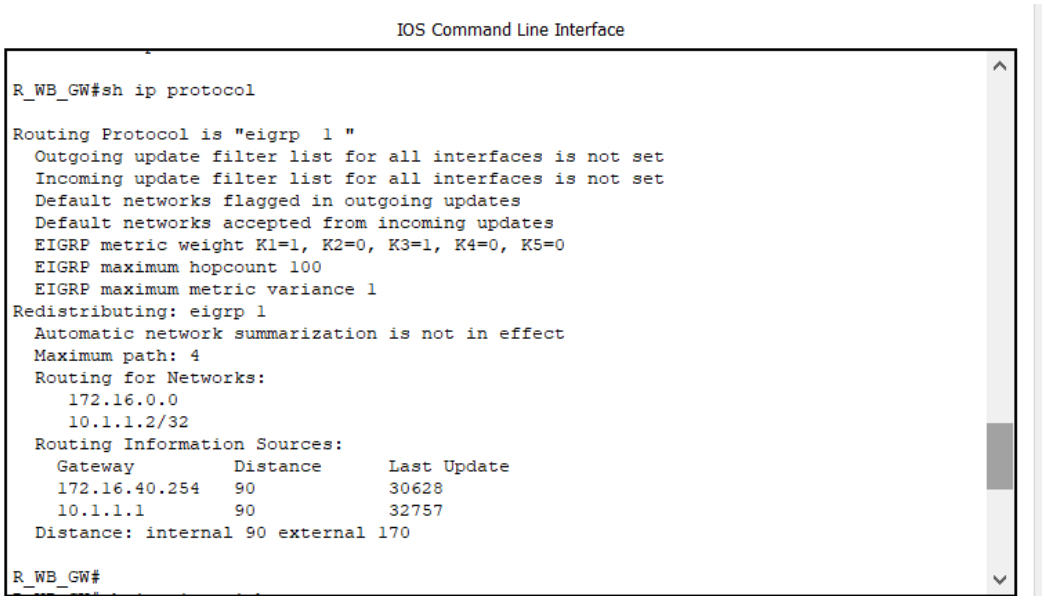


Рисунок 3.12 – Таблиця сусідніх EIGRP-маршрутизаторів

Перегляд таблиці маршрутизації здійснюється за допомогою команди «show ip route»(рис. 3.13).

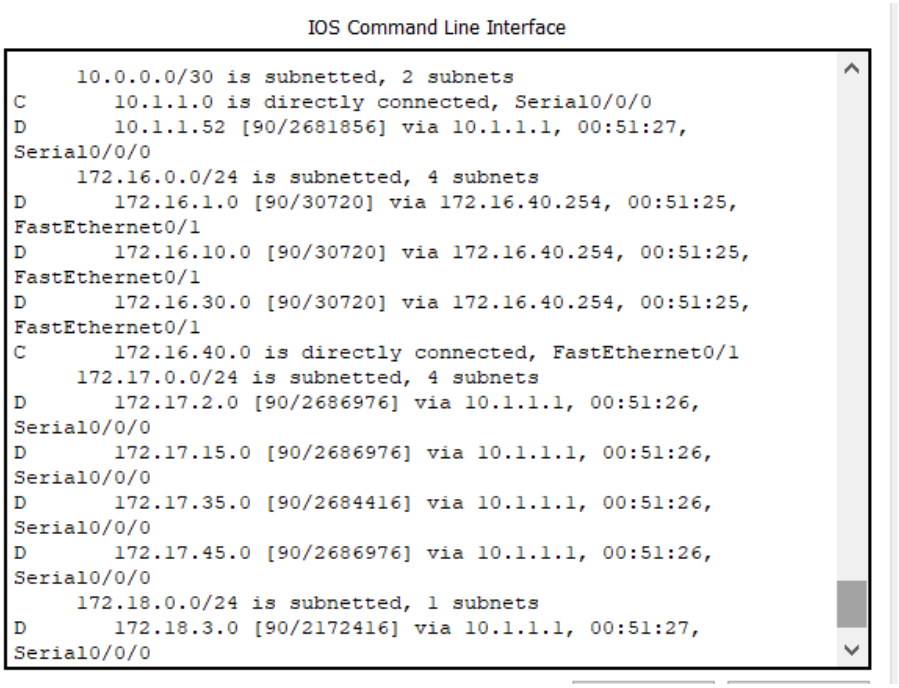


Рисунок 3.13 – Таблиця маршрутизації на маршрутизаторі R_WB_GW

До переваг протоколу EIGRP відноситься:

- швидка збіжність у великих мережах;
- значно менша завантаження каналів і CPU при роботі протоколу;
- можливість балансування трафіку по нееквівалентним каналах.

Недоліком протоколу EIGRP, є те що він обмежений кількістю вузлів рівне 100 і є закриті, тобто може бути реалізований на обладнанні компанії Cisco Systems.

3.4 Захист периметра мережі

Основа захисту інформації в корпоративних мережах полягає в тому, щоб закрити трафік корпоративної мережі засобами захисту інформації мережевого рівня (побудувати віртуальну корпоративну мережу) і організувати фільтрацію інформації в точках з’єднання з відкритими мережами. Як основний засіб фільтрації інформації на інтерфейсах традиційно застосовується міжмережевий екран (firewall). Для підвищення надійності організації захисту на мережі підприємства встановлено зону контрольованого доступу (так звану "демілітаризовану зону" – demilitarized zone (DMZ)).

Демілітаризована зона є, як правило, сегментом мережі, який характеризується тим, що в ньому представляються інформаційні ресурси для доступу з відкритої мережі. При цьому сервери, що надають ці ресурси для відкритого доступу, конфігуруються спеціальним чином для того, щоб на них не могли використовуватися так звані "небезпечні" сервіси (додатки), які можуть дати потенційному порушникові можливість реконфігурувати систему, компрометувати її, і, спираючись на скомпрометовані ресурси, атакувати корпоративну мережу. У демілітаризованій зоні можуть розташовуватися деякі сервери службового обміну між корпоративною і відкритою мережею. Крім того, в середовищі демілітаризованої зони (як і в середовищі корпоративної мережі) часто використовуються засоби виявлення порушника (intrusion detection). Призначення цих засобів полягає в тому, щоб за непрямими ознаками (таким, наприклад, як аномалії мережевої активності) забезпечити виявлення компрометації мережі, яке може бути вироблене в наслідок, наприклад, неправильної конфігурації міжмережевого екрану або внаслідок помилки програмного забезпечення [16].

В межах зони контрольованого доступу будуть розміщені сервери. Важливим механізмом захисту буде політика роботи міжмережних фільтрів, який буде залежати в першу чергу від напряму приходу трафіку. Для трафіку від користувачів центрального офісу та філіалів буде забезпечено необмежений доступ до серверів. Для трафіку із зовнішньої мережі буде повністю заборонений прямий доступ у напрямі ресурсів корпоративної мережі центрального офісу, та буде здійснено фільтрацію трафіку у напрямі серверів.

Міжмережний екран приймає рішення про доступ кожного пакету на основі набору правил фільтрації, інформації, що міститься в пакеті. Головними критеріями такої інформації будуть ip-адреса відправника та тип використовуваного транспортного протоколу, що вказуватиме на тип мережного сервісу.

Для захисту периметра корпоративної мережі використано мережевий екран Cisco ASA. Для зручного адміністрування необхідно вказати hostname, за допомогою команди hostname FW-MainOffice. Далі виконано налаштування зовнішнього та внутрішнього інтерфейсів:

```
FW-MainOfficce(config)#interface Ethernet0/1
FW-MainOfficce(config-if)#nameif outside
FW-MainOfficce(config-if)#security-level 0
```

FW-MainOfficce(config-if)#ip-address 55.55.55.57 255.255.255.252
FW-MainOfficce(config-if)#no shutdown
FW-MainOfficce(config)#interface Ethernet0/0
FW-MainOfficce(config-if)#nameif inside
FW-MainOfficce(config-if)#security-level 100
FW-MainOfficce(config-if)#ip-address 172.16.16.1 255.255.255.0
FW-MainOfficce(config-if)#no shutdown
Далі створюємо користувача з правами адміністратора та пароль в режимі enable:
FW-MainOfficce(config)#username admin password cisco privilege 15
FW-MainOfficce(config)#enable password ciscoadmin
Налаштування доступу до ASA по протоколу HTTPS(через графічний інтерфейс ASDM):
FW-MainOfficce(config)#http server enable
FW-MainOfficce(config)#http 172.17.35.1 255.255.255.0 insade
FW-MainOfficce(config)#aaa authentication http console LOCAL
Налаштування доступу до ASA по протоколу SSH (командною строкою CLI):
FW-MainOfficce(config)#hostname ASA
FW-MainOfficce(config)#domain-name admin
FW-MainOfficce(config)#crypto key fenerate rsa modulus 2048
FW-MainOfficce(config)#ssh 172.17.35.1 255.255.255.255 inside
FW-MainOfficce(config)# aaa authentication ssh console LOCAL

NAT (Network Address Translation) – трансляція мережевих адрес, технологія, яка дозволяє перетворювати (змінювати) IP адреси і порти в мережевих пакетах.

NAT використовується для здійснення доступу пристроїв з мережі підприємства в Інтернет, або навпаки для доступу з Інтернет на який-небудь ресурс всередині мережі.

NAT застосовують для перетворення приватних адрес в глобальні. Крім можливості доступу в зовнішню мережу (Інтернет), NAT має ще кілька позитивних сторін. Так, наприклад, трансляція мережевих адрес дозволяє приховати внутрішню структуру мережі і обмежити до неї доступ, що підвищує безпеку. А ще ця технологія дозволяє економити Глобальні IP адреси, так як під одною глобальною адресою в Інтернет може виходити безліч хостів [20].

Задано пул зовнішніх адрес, в які транслюються внутрішні адреси. Для завдання пулу, який містить тільки одну адресу – адресу зовнішнього інтерфейсу роутера – необхідно ввести команду:

FW-MainOfficce(config)# ip nat pool natpool 0.0.0.0 68.110.171.133 netmask 0.0.0.0

При задані пулу адрес необхідно вказати перший і останній адреса з вхідної пул послідовності адрес. Якщо в пулі 1 адреса необхідно вказати його 2 рази.

Задано список доступу:

FW-MainOfficce(config)# access-list 9 permit any

Важливо : 9 – число від 1 до 99 позначає № списку доступу і задається адміністратором. Any – ключове слово, означає, що список доступу дозволятиме пакети з будь-якою адресою відправника.

FW-MainOfficce(config)# ip nat inside source list 9 pool natpool overload

Дана команда «говорить» роутеру, що у всіх пакетів, отриманих на внутрішній інтерфейс і дозволених списком доступу номер 9, адреса відправника буде трансльована на адресу з NAT пулу «natpool».

Висновки за розділом. Спроектовано мережу центру обробки даних, центрального та віддаленого офісу. Запропоноване рішення характеризується такими результатами:

Мережа організації ITSosed побудована на базі маршрутизаторів фірми Cisco Systems, тому, відповідно, як протокол динамічної маршрутизації вибрано EIGRP. Протокол EIGRP здатний забезпечити менший час збіжності оптимальних маршрутів, а саме 40 секунд, але настроювати їх складніше. Крім того, для досягнення належної продуктивності ці протоколи, у порівнянні з протоколом RIP, очікуватимуть від маршрутизатора більшого об’єму оперативної пам’яті і більш швидкий процесор. Проте, оскільки задачею дипломного проекту є захист, то саме EIGRP є найкращим протоколом динамічної маршрутизації у даному випадку.

4.1 Оцінювання комерційного потенціалу розробки

Метою проведення технологічного аудиту є оцінювання комерційного потенціалу розробки, створеної в результаті науково-технічної діяльності. В результаті оцінювання робиться висновок щодо напрямів організації подальшого її впровадження з врахуванням встановленого рейтингу.

Результатом магістерської кваліфікаційної роботи «Методи та засоби безпечної передачі даних в корпоративних мережах» є розробка вдосконаленого комплексного методу захисту корпоративних мереж. Для оцінювання комерційного потенціалу розробки було проведено опитування 3х незалежних експертів: керівник магістерської роботи к.т.н., доц. Войцеховська О. В. та провідні викладачі кафедри ОТ – к.т.н., доц. Крупельницький Л. В. та к.т.н., доц. Захарченко С. В.

Проведено оцінювання комерційного потенціалу розробки за 12-ма критеріями, наведеними в таблиці 4.1 [19].

Таблиця 4.1 – Рекомендовані критерії оцінювання комерційного потенціалу розробки та їх можлива бальна оцінка

Критерії оцінювання та бали (за 5-ти бальною шкалою)					
Крит.	0	1	2	3	4
Технічна здійсненність концепції:					
1	Достовірність концепції не підтверджена	Концепція підтверджена експертними висновками	Концепція підтверджена розрахунками	Концепція перевірена на практиці	Перевірено роботоздатність продукту в реальних умовах
Ринкові переваги (недоліки):					
2	Багато аналогів на малому ринку	Мало аналогів на малому ринку	Кілька аналогів на великому ринку	Один аналог на великому ринку	Продукт не має аналогів на великому ринку

Продовження таблиці 4.1

Крит.	0	1	2	3	4
3	Ціна продукту значно вища за ціни аналогів	Ціна продукту дещо вища за ціни аналогів	Ціна продукту приблизно дорівнює ціна аналогів	Ціна продукту приблизно дорівнює ціна аналогів	Ціна продукту значно нижче за ціни аналогів
4	Технічні та споживчі властивості продукту значно гірші, ніж в аналогів	Технічні та споживчі властивості продукту трохи гірші, ніж в аналогів	Технічні та споживчі властивості продукту на рівні аналогів	Технічні та споживчі властивості продукту трохи кращі, ніж в аналогів	Технічні та споживчі властивості продукту значно кращі, ніж в аналогів

5	Експлуатаційні витрати значно вищі, ніж в аналогів	Експлуатаційні витрати дещо вищі, ніж в аналогів	Експлуатаційні витрати на рівні експлуатаційних витрат аналогів	Експлуатаційні витрати трохи нижчі, ніж в аналогів	Експлуатаційні витрати значно нижчі, ніж в аналогів
Ринкові перспективи					
6	Ринок малий і не має позитивної динаміки	Ринок малий, але має позитивну динаміку	Середній ринок з позитивною динамікою	Великий стабільний ринок	Великий ринок з позитивною динамікою
7	Активна конкуренція великих компаній на ринку	Активна конкуренція	Помірна конкуренція	Незначна конкуренція	Конкурентів немає
Практична здійсненність					
8	Відсутні фахівці як з технічної, так і з комерційної реалізації ідеї	Необхідно на наймати фахівців або витрачати значні кошти та час на навчання наявних фахівців	Необхідне незначне навчання фахівців та збільшення їх штату	Необхідне незначне навчання фахівців	Є фахівці з питань як з технічної, так і з комерційної реалізації ідеї
9	Потрібні значні фінансові ресурси, які відсутні. Джерела фінансування ідеї відсутні	Потрібні незначні фінансові ресурси. Джерела фінансування відсутні	Потрібні значні фінансові ресурси. Джерела фінансування є	Потрібні незначні фінансові ресурси. Джерела фінансування є	Не потребує додаткового фінансування
10	Необхідна розробка нових матеріалів	Потрібні матеріали, що використовуються у військово-промисловому	Потрібні дорогі матеріали	Потрібні досяжні та дешеві матеріали	Матеріали для реалізації ідеї відомі та давно використовуються у виробництві

Продовження таблиці 4.1

11	Термін реалізації ідеї більший за 10 років	Термін реалізації ідеї більший за 5 років. Термін окупності інвестицій більше 10-ти років	Термін реалізації ідеї від 3-х до 5-ти років. Термін окупності інвестицій більше 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій від 3-х до 5-ти років	Термін реалізації ідеї менше 3-х років. Термін окупності інвестицій менше 3-х років
12	Необхідна розробка регламентних документів та отримання великої кількості дозвільних документів на виробництво та реалізацію продукту	Необхідно отримання великої кількості дозвільних документів на виробництво та реалізацію продукту, що вимагає значних коштів та часу	Процедура отримання дозвільних документів для виробництва та реалізації продукту вимагає незначних коштів та часу	Необхідно тільки повідомлення відповідним органам про виробництво та реалізацію продукту	Відсутні будь-які регламентні обмеження на виробництво та реалізацію продукту

Результати оцінювання комерційного потенціалу розробки відображено в таблиці 4.2.

Таблиця 4.2 – Результати оцінювання комерційного потенціалу розробки

Критерії	Прізвище, ініціали, посада експерта		
	1.Войцеховська О.В.	2.Крупельницький Л. В.	3. Захарченко С. М.
	Бали, виставлені експертами		
1	2	3	4
1	3	4	2
2	4	3	3
3	3	2	3
4	3	3	3
5	4	3	3
6	3	3	3

Продовження таблиці 4.2

1	2	3	4
7	3	2	3
8	3	4	4
9	3	3	3
10	4	3	4
11	3	4	4
12	3	4	4
Сума балів	$СБ_1 = 39$	$СБ_2 = 38$	$СБ_3 = 39$
Середньоарефме-тична сума балів СБ	СБ = 38,7		

Відповідно до результатів аналізу можна зробити висновок, щодо рівня комерційного потенціалу розробки. Порівняємо отриманий результат з рівнями комерційного потенціалу розробки, що представлено в таблиці 4.3.

Таблиця 4.3 – Рівні комерційного потенціалу розробки

Середньоарифметична сума балів $\overline{СБ}$, розрахована на основі Висновків експертів	Рівень комерційного Потенціалу розробки
0 – 10	Низький
11 – 20	Нижчесереднього
21 – 30	Середній
31 – 40	Вищесереднього
41 – 48	Високий

Оскільки середньоарифметична сума балів (СБ) становить 38,7 та знаходиться в межах від 31 до 40, то можна зробити висновок, що рівень комерційного потенціалу розробки є вище середнього.

Проаналізуємо суть технічної проблеми та розглянемо аналоги.

В даний час швидкими темпами розвиваються інформаційні технології, які проникають в усі галузі людської діяльності. Без сумніву, інформаційна безпека, на сьогодні, являє собою важливу складову корпоративної мережі. Кожне підприємство активно працює над забезпеченням інформаційної безпеки, але цього недостатньо. Для реалізації багаторівневого інтегрованого захисту необхідно зв’язуватися з підприємствами, які надають аутсорсингові послуги по захисту мережі.

Створено систему, яка є універсальною, недорогою і не вимагає від користувача надзвичайних навиків. Доцільно вдосконалено метод, який буде враховує максимальну кількість параметрів корпоративної мережі починаючи від кількості хостів, закінчуючи стеками технологій. В результаті застосування даного методу повинна утворється захищена корпоративна мережа, в якій реалізовані всі необхідні заходи захисту, а також дотримано баланс між продуктивністю та захищеністю мережі з врахуванням затрат на реалізацію системи.

Головними конкурентами серед аналогів є методи захисту мережі, які налаштовані за рахунок використання мережевого обладнання різних компаній, зокрема Juniper. Порівняльну характеристику мережевого обладнання представлено в таблиці 4.4.

Таблиця 4.4 – Порівняння основних характеристик компанії Cisco та Juniper

	Cisco ASR	Juniper MX

System capacity	до 90 Тбіт/с	до 80 Тбіт/с
Кількість слотів	20	20
Slot capacity	2,5 Тбіт/с	2 Тбіт/с
Процесор	2,27 Ггц	1,8 Ггц
Об’єм оперативної пам’яті	до 20 Гб	16 Гб

Продовження таблиці 4.4

Операційна система	Cisco IOS	JunOS
Розміри, см	191x45x73	200x44x92
Маса, кг	471	680

Відповідно до таблиці 4.4 можна зробити висновки, що комплексний метод, який реалізовано з використанням мережевого обладнання Cisco, отримує максимальні показники захищеності за рахунок ……

Основна мета магістерської роботи – вдосконалення й розробка комплексного методу захисту корпоративної мережі та забезпечення безпеки інформації, що відповідають інтересам, вимогам і законодавству України.

Дана розробка дозволяє вирішити ряд питань, які є необхідними на кожному підприємстві, а саме: безпека передачі даних як в локальній, так і в глобальній мережі, підтримка захищеності мережі, забезпечення цілісності та безпеки мережевих пристроїв, методи протидії найсучаснішим мережевим атакам.

Комплексний метод формулює науково-технічні принципи побудови систем забезпечення безпеки інформаційних ресурсів в корпоративних мереж з урахуванням сучасних тенденцій розвитку мережевих інформаційних технологій, розвитку видів мережевих протоколів, їх взаємної інкапсуляції та спільного використання.

Технології, які використовуються в даному багаторівневому інтегрованому захисті зменшують забруднення навколишнього середовища, а саме надають можливість створення єдиної, спільної мережі без використання мережевого кабелю.

Даний метод готовий до використання, тому зараз ведуться переговори з керівниками підприємств для подальшої реалізації.

В умовах жорсткої конкуренції реалізація свого продукту без забезпечення рекламної та маркетингової компанії неможливий. Тому виконано цілий комплекс заходів, пов’язаних із представленням даного рішення на ринку, а саме:

- приведення до товарного вигляду продукту;
- підготовка і випуск рекламних, навчальних матеріалів;
- організація реклами на сайтах аутсорсингових компаній;

4.2 Прогнозування витрат на виконання науково-дослідної, дослідно-конструкторської та конструкторсько-технологічної роботи

1-й етап: розрахунок витрат, які безпосередньо стосуються виконавців даного розділу роботи, здійснюється за такими статтями та формулами:

Проведемо розрахунок основної заробітної плати кожного із розробників Зо, які працюють в сфері ІТ розробки за формулою.

$$З_0 = \frac{М}{Т_р} \cdot t \text{ грн.},$$

де М – місячний посадовий оклад конкретного розробника (інженера, дослідника, науковця тощо), грн.
$Т_р$ – число робочих днів в місяці;
t – число робочих днів роботи розробника (дослідника).
Заробітна плата наукового керівника:

$$З_{0с} = \frac{7293}{21} \cdot 3 = 1042 \text{ (грн)}.$$

Заробітна плата науковця:

$$З_{0с} = \frac{10000}{21} \cdot 66 = 31428 \text{ (грн)}.$$

Зроблені розрахунки зведено до таблиці 4.5.

Таблиця 4.5 – Основна заробітна плата розробників

Найменування посади виконавця	Місячний посадовий оклад, грн.	Оплата за робочий день, грн.	Число днів роботи	Витрати на оплату праці, грн.
1. Науковий керівник	7293	347	3	1042
2. Науковець	10000	476	66	31428
Всього				32470

Додаткова заробітна плата $З_д$ всіх розробників, які брали участь у виконанні даного етапу роботи складає 10%...12% від основної:

$$З_д = (0{,}1 \ldots 0{,}12) \cdot З_о \text{ (грн)}.$$

$$З_д = 0{,}12 \cdot 32470 = 3896{,}4 \text{ (грн)}.$$

Нарахування на заробітну плату $Н_{зп}$ розробників, які брали участь у виконанні даного етапу роботи, розраховуються за формулою.

$$Н_{зп} = (З_0 + З_д) \cdot \frac{\beta}{100} \text{(грн)},$$

де: $З_о$ – основна заробітна плата розробників, грн.;
$З_Д$ – додаткова заробітна плата розробників, грн.;
β – ставка єдиного внеску на загальнообов'язкове державне соціальне страхування, %. Ставка єдиного внеску на загальнообов'язкове державне соціальне страхування для працівників бюджетної сфери складає 22%.

$$Н_{зп} = (32470 + 3896) \cdot \frac{22}{100} = 7120 \text{ (грн)}.$$

Амортизація обладнання, комп'ютера та приміщення, що використовувались під час виконання даного етапу роботи. Дані відрахування розраховуються по кожному виду обладнання, приміщенням тощо.
У спрощеному вигляді амортизаційні відрахування А в цілому будуть розраховані за формулою:

$$А = \frac{Ц \cdot Н_а}{100} \cdot \frac{Т}{12} \text{ (грн)},$$

де: Ц – загальна вартість всього обладнання, комп'ютерів, приміщень тощо, що використовувались для виконання даного етапу роботи, грн;
$Н_а$ – річна норма амортизаційних відрахувань. Для нашого випадку можна прийняти, що На = (10...25)%;
Т – термін, використання обладнання, приміщень тощо, місяці.

$$А = \frac{20000 \cdot 10}{100} \cdot \frac{3}{12} = 500$$

Таблиця 4.6 – Амортизаційні відрахування

Найменування обладнання	Балансова вартість, грн.	Норма амортизації, %	Термін використання, міс.	Величина амортизаційних відрахувань, грн
1	2	3	4	5
1. Комп'ютер	20000	10	3	500
2. Принтер	5000	15	3	187,5
Всього:				687,5

Витрати на матеріали заведено в таблиці 4.7.

Таблиця 4.7 – Вартість матеріалів

№	Найменування комплектуючого	Ціна, грн.	Скільки витрачено, шт.	Вартість витрачених комплектуючих, грн.
1	Заправка картриджа	200	1	220
2	Ручка	15	1	10
3	Папір	100	1	126
Всього				356

Витрати на силову електроенергію розраховується за формулою:

$$В_е = В \cdot П \cdot Ф \cdot К_п \text{ (грн)},$$

де В – вартість 1кВт-години електроенергії, В=2 грн/кВт-год;
П – установлена потужність обладнання, кВт, 0,6 кВт;
Ф – фактична кількість годин роботи обладнання, 528 години;
$К_п$ – коефіцієнт використання потужності, 0,7.

$$В_е = 2 \cdot 0{,}6 + 528 \cdot 0{,}7 = 443{,}52 \text{ (грн)}.$$

Інші витрати доцільно приймати як 100%...300% від суми основної заробітної плати розробників, що виконували роботу:

$$В_{ін} = 2 \cdot 31428 = 62856 \text{ (грн)}.$$

Розрахунок загальних витрат на виконання даної роботи.
Загальна вартість всієї наукової роботи визначається за $В_{заг}$ формулою:

$$B_{заг} = \frac{B}{\alpha}$$

де: α – частка витрат, які безпосередньо здійснює виконавець даного етапу роботи, у відносних одиницях.

$$B_{\text{заг}} = \frac{62856}{1} = 62856 \text{ (грн)}.$$

Прогнозування загальних витрат ЗВ на виконання та впровадження результатів виконаної наукової роботи здійснюється за формулою:

$$\text{ЗВ} = \frac{B_{\text{заг}}}{\beta},$$

де: β – коефіцієнт, який характеризує етап виконання даної роботи.

$$\text{ЗВ} = \frac{62856}{0.9} = 69480 \text{ (грн)},$$

4.3 Прогнозування комерційних ефектів від реалізації результатів розробки

Оскільки розробка дає можливість прямо оцінити зростання чистого прибутку підприємства від впровадження результатів, то збільшення прибутку підприємства $\Delta П_i$ для кожного з років, протягом яких очікується отримання позитивних результатів можна розрахувати за формулою:

$$\Delta П_i = (\Delta П_я \cdot N + П_я \Delta N),$$

де: $\Delta П_я$ – покращення основного якісного показника від впровадження результатів розробки у даному році;

N – покращення основного кількісного показника діяльності підприємства від впровадження результатів розробки;

ΔN – покращення основного кількісного показника діяльності підприємства від впровадження результатів розробки;

$П_я$ – основний якісний показник, який визначає діяльність підприємства у даному році після впровадження результатів наукової розробки;

n – кількість років, протягом яких очікується отримання позитивних результатів від впровадження розробки.

Уявимо, що після впровадження наукової новизни підприємство матиме змогу надавати клієнтам новий вид послуг, заробляючи на цьому додаткових 300 грн (що автоматично збільшить чистий прибуток на 300 грн), кількість реалізації такої послуги може скласти до 120 шт. у перший рік, протягом другого року ще 60 шт., протягом третього – ще 30 шт. До впровадження наукової новизни реалізація продукції складала 1 шт., а прибуток становив 800 грн.

Збільшення чистого прибутку підприємства $\Delta П_i$ протягом першого року складе:

$$\Delta П_1 = 1000 \cdot 1 + (1000 + 300) \cdot 120 = 157000 \text{ (грн)}.$$

Збільшення чистого прибутку підприємства $\Delta П_i$ протягом другого року складе:

$$\Delta П_2 = 1000 \cdot 1 + (1000 + 300) \cdot (120 + 60) = 235000 \text{ (грн)}.$$

Збільшення чистого прибутку підприємства $\Delta П_i$ протягом третього року (відносно базового року до провадження результатів наукової розробки) складе:

$$\Delta П_3 = 1000 \cdot 1 + (1000 + 300) \cdot (120 + 60 + 30) = 274000 \text{ (грн)}.$$

4.4 Розрахунок ефективності вкладених інвестицій та періоду їх окупності

Для початку потрібно розрахувати вартість інвестицій PV, що вкладаються у наукову розробку. Такою вартістю можна вважати прогнозовану величину загальних витрат ЗВ на виконання та впровадження результатів НДДКР, тобто можна вважати що ЗВ = PV.
У розділі 4.3 було розраховано очікуване збільшення прибутку, що його отримає підприємство від впровадження результатів наукової розробки, для кожного з років, починаючи з першого року впровадження.
Припустимо, що загальні витрати ЗВ на виконання та впровадження результатів НДДКР (або вартість інвестицій) складає 69840 грн. Результати вкладених у наукову роботу інвестицій почнуть виявлятися з першого року.
Ці результати проявляються у тому, що за перший рік підприємство отримає збільшення чистого прибутку на 157000 грн., відносно, у другому році збільшення чистого прибутку на 235000 грн., у третьому році – збільшення чистого прибутку на 274000 грн.
Тоді рисунок, що характеризує рух платежів (інвестицій та додаткових прибутків) матиме вигляд, наведений на рисунку 4.1.

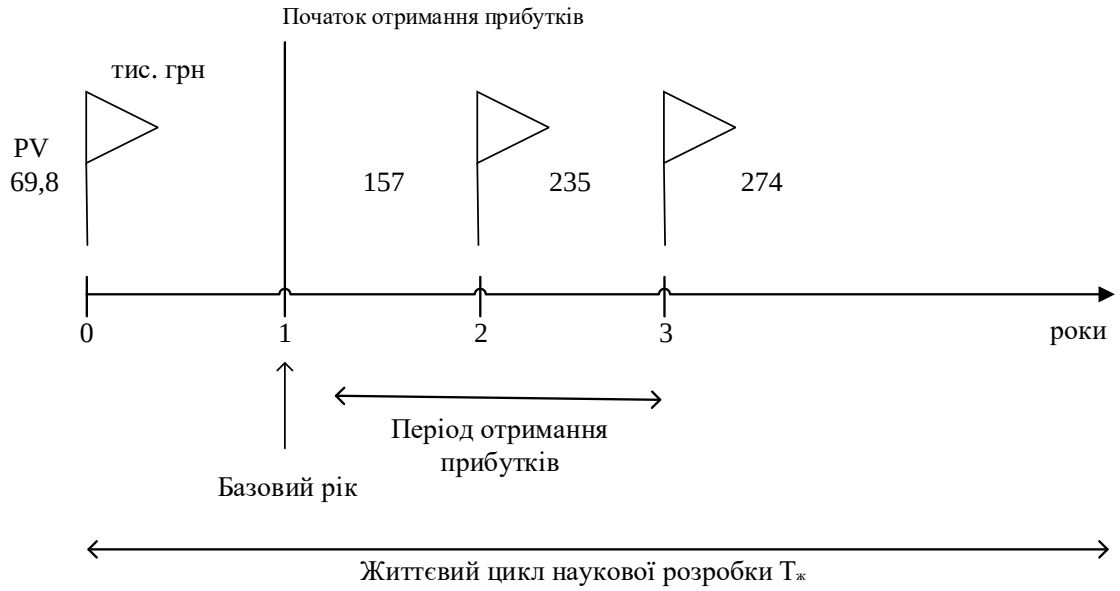


Рисунок 4.1 – Вісь часу з фіксацією платежів, що мають місце під час розробки та впровадження результатів НДДКР

Розрахунок ефективності вкладених інвестицій $E_{абс}$ проводиться за формулою:

$$E_{абс} = (ПП - PV),$$

де: ПП – приведена вартість усіх чистих прибутків, що їх отримає підприємство від реалізації результатів наукової розробки, грн.;
PV – теперішня вартість інвестицій.
У свою чергу, приведена вартість всіх чистих прибутків ПП розраховується за формулою:

$$ПП = \sum_{1}^{T} \frac{\Delta П_i}{(1+\tau)^t},$$

де: $\Delta П_i$ – збільшення чистого прибутку у кожному із років, протягом яких виявляються результати виконаної та впровадженої НДДКР, грн;

T – період часу, протягом якого виявляються результати впровадженої НДДКР, роки;

τ – ставка дисконтування, за яку можна взяти щорічний прогнозований рівень інфляції в країні; для України цей показник знаходиться на рівні 0,1;

t – період часу (в роках) від моменту отримання чистого прибутку до точки «0».

Отже:

$$ПП=\frac{157000}{(1+0,1)^1}+\frac{235000}{(1+0,1)^2}+\frac{274000}{(1+0,1)^3}=142727,2+194214,8+209160,3=543102,3\ (грн).$$

$$Е_{абс} = (543102,3 – 69840) = 473262,3\ (грн).$$

Оскільки $Е_{абс} > 0$, то вкладання коштів на виконання та впровадження результатів НДДКР може бути доцільним.

Розрахунок щорічної відносної ефективності вкладених в наукову розробку інвестицій $Е_в$ проводиться за формулою:

$$E_B = \sqrt[T_ж]{1+\frac{E_{абс}}{PV}} - 1,$$

де: $Т_ж$ – життєвий цикл наукової розробки, роки.

Далі розрахована величина $Е_В$ порівнюється з мінімальною ставкою дисконтування τ_{min}, яка визначає ту мінімальну дохідність, нижче за яку інвестиції вкладатися не будуть. У загальному вигляді мінімальна ставка визначається за формулою:

$$\tau = d + f\ ,$$

де: d – середньозважена ставка за депозитними операціями в комерційних банках; в 2019 році в Україні d = (0,14…0,2);

f – показник, що характеризує ризикованість вкладів; зазвичай f= (0,05…0,1), але може бути і значно більше.

Якщо величина $Е_В > \tau_{min}$, то інвестор може бути зацікавлений у фінансуванні даної наукової розробки, в іншому випадку фінансування наукової розробки не буде.

Спочатку необхідно спрогнозувати величину τ_{min}. Припустимо, що за даних умов τ_{min} = 0,2 + 0,05 = 0,25.

Тоді відносна ефективність вкладених інвестицій в проведення наукових досліджень та впровадження їх результатів складе:

$$Е_в = \sqrt[3]{1+\frac{473262,3}{69840}} - 1 = 1,98 - 1 = \ 0,98 \text{ або } 98\ \%$$

Допустимо що за даних умов ставка дисконтування $\tau_{мін}$ = 0,25 або 25%. Оскільки Ев = 0,98% > $\tau_{мін}$ = 0,25 = 25%, то інвестори будуть зацікавлені вкладати гроші в дану наукову розробку, оскільки вони отримають значні прибутки від реалізації даної розробки.

Термін окупності вкладених у реалізацію наукового проекту інвестицій $Т_{ок}$ визначається за формулою:

$$T_{ок} = \frac{1}{E_B}.$$

Якщо $Т_{ок}$< 3…5-ти років, то фінансування даної наукової розробки в принципі є доцільним. В інших випадках потрібні додаткові розрахунки та обґрунтування.

$$Т_{ок} = \frac{1}{0.98} = 1,02$$

Для нашого випадку термін окупності вкладених у реалізацію проекту інвестицій Ток складає 1,02 року, що є менше 3-5 років, тому фінансування даної наукової розробки є доцільним.

Висновки: отже, після проведення даних розрахунків витрат на виконання науково-дослідної роботи встановлено, що витрати на основну заробітну плату становлять 32470 грн, затрати на матеріали – 310 грн. При цьому амортизаційні витрати на обладнання становлять 687,5 грн. Загальний розмір чистого прибутку може скласти близько 473262,3 грн, а окупність проекту 1,01 року. Тому можна зробити висновок що проект буде цікавим для інвесторів.

ВИСНОВКИ

Дана магістерська кваліфікаційна робота присвячена методам та засобам безпечної передачі даних в корпоративних мережах та складається з чотирьох розділів.
В першому розділі охарактеризовано особливості захищених мереж, розглянуто види інформаційних загроз, які несуть небезпеку функціонування захищеної мережі. Проаналізовано комплекс програмних, апаратних та організаційних методів забезпечення захисту мережі. А також визначено основний аналізатор для моніторингу мережевого трафіку – NetFlow, що дає можливість збирати та аналізувати мережевий трафік на рівні сеансів.

У другому розділі розглянуто методи безпечної передачі даних в корпоративних мережах. Вдосконалено метод захисту корпоративної мережі шляхом поєднання захисту від внутрішніх та зовнішніх загроз з використанням таких технологій захисту як аутентифікація, створення безпечного периметру та утворення захищеного каналу передачі даних. Запропоновано структурну схему багаторіневого інтегрованого захисту, що дозволяє планувати ефективні системи захисту конфіденційної інформації для різних корпоративних мереж.

Для забезпечення високого рівня захисту ресурсів корпоративної інформаційної системи необхідно реалізувати найбільш перспективні та надійні технології інформаційної безпеки. Тому в третьому розділі було спроектовано та об’єднано мережу центру обробки даних, центрального та віддаленого офісу використовуючи захищені віртуальні мережі VPN для захисту інформації, переданої по відкритих каналах зв’язку. Виконано захист локальних мереж за рахунок використання техногології 802.1x, що дозволяє активно протидіяти внутрішнім порушенням інформаційної безпеки. Здійснено управління доступом на рівні користувачів та захист від несанкціонованого доступу до інформації, налаштовано ідентифікацію користувачів шляхом застосування засобів аутентифікації.

В корпоративній мережі організовано зону контрольованого доступу – DMZ, що дозволило забезпечити високий рівень безпеки у мережі та повністю контролювати доступ до інформаційних ресурсів підприємства. Використано мережевий екран, що захищає периметр мережі. Створено та налаштовано DHCP сервер, завдяки якому реалізоване динамічне присвоєння IP адрес всім

хостам мережі та забезпечує економію IP-адрес у розмірі 10% від їх початкової кількості. Реалізовано технологію NAT, яка дає можливість передавати дані з локальних мереж у глобальні методом підміни IP адреси на публічну. Налаштовано протокол динамічної маршрутизації EIGRP, який здатний забезпечити менший час збіжності оптимальних маршрутів, а саме 40 секунд.

Розроблена мережа відповідає всім сучасним мережевим стандартам та задовольняє потреби підприємства у повному обсязі. Використання сучасного обладнання дозволить мережі підприємства виконувати поставлені завдання та стабільно працювати протягом всього строку її експлуатації.

В четвертій частині виконано розрахунки витрат на виконання науково-дослідної роботи та встановлено, що витрати на основну заробітну плату становлять 32470 грн, затрати на матеріали – 310 грн. При цьому амортизаційні витрати на обладнання становлять 687,5 грн. Спрогнозувавши комерційні ефекти від впровадження наукової новизни визначено ймовірне збільшення чистого прибутку впродовж 3-х років після впровадження. Загальний розмір чистого прибутку може скласти близько 473262,3 грн, а окупність проекту 1,01 року. Тому можна зробити висновок що проект буде цікавим для інвесторів.

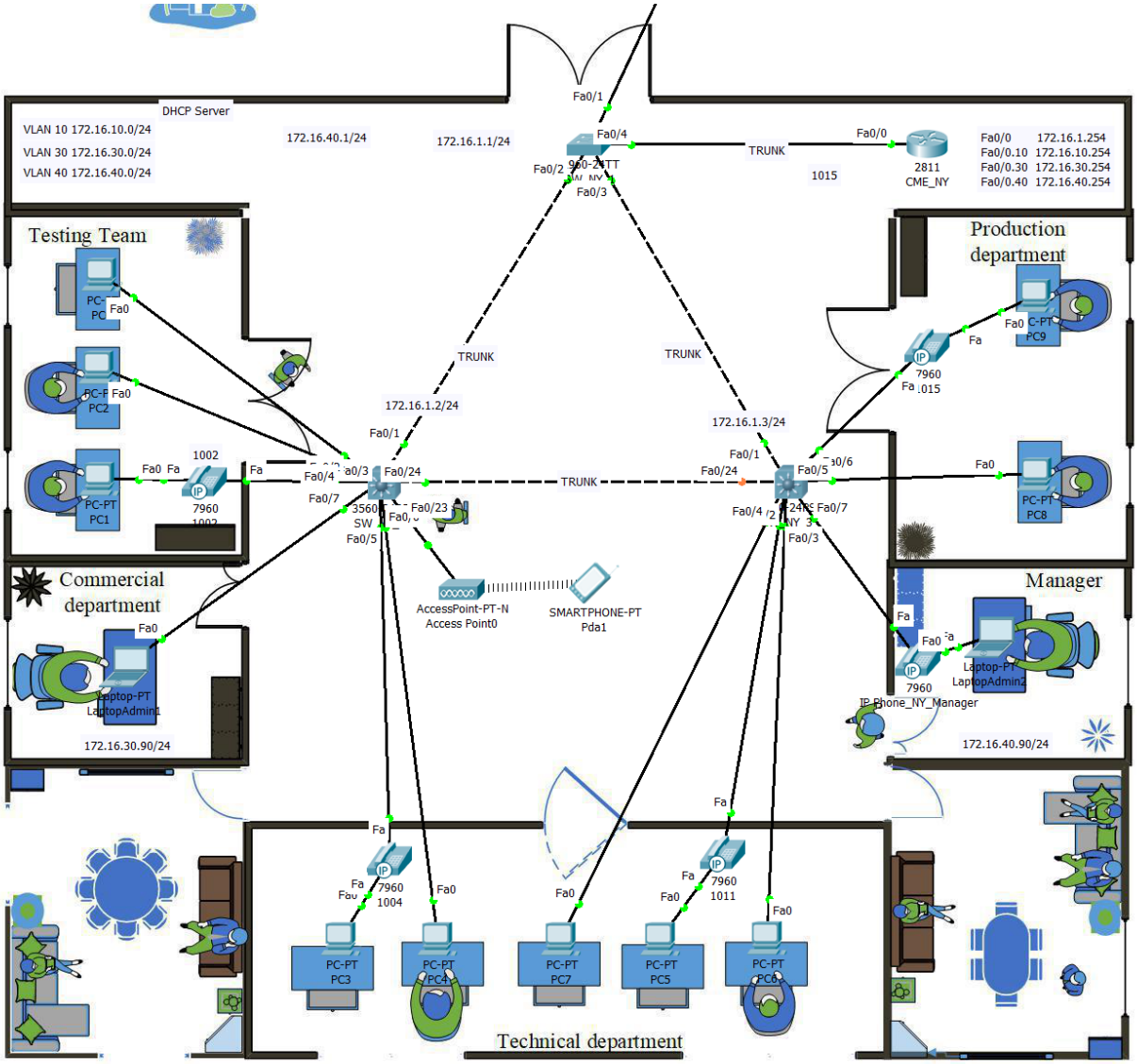
Перелік ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Астахов А. Анализ защищенности корпоративных автоматизированных систем / А. Астахов. – Москва, 2010.
2. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для ВУЗов. 3-е изд.- СПб.: Питер., 2010. – 958 с.
3. Мінухін С.В. Комп’ютерні мережі. Принципи організації роботи глобальних комп’ютерних мереж та основи безпеки в комп’ютерних мережах // С.В. Мінухін, С.В. Кавун, С.В. Знахур – Х.: вид ХНЕУ, 2009, – 312 с.
4. Кульгин М. Технологии корпоративных сетей / Кульгин Михаил. – С-Пт.: Питер. 2016.-704 с.
5. Соколов А. В. Защита информации в распределенных корпоративных сетях и системах / Соколов А. В., Шаньгин. В. Ф. – ДМК Пресс., 2012. – 656с.
6. Захарченко С.М. Метод багаторівневого захисту даних в корпоративних мрежах / Захарченко С.М., Войцеховська О.В., Куцак Ю.В. // Збірник Матеріалів XLV НТК ВНТУ (2019). Режим доступу: https://conferences.vntu.edu.ua/index.php/mn/mn2020/author/submissionReview/8483
7. Захарченко С. М Основи побудови захищених мереж на базі обладнання компанії Cisco. // Захарченко С. М., Трояновська Т. І., Бойко О. В. Навчальний посібник. Вінниця : ВНТУ, 2017. – 133 с.
8. Коробейнікова Т.І Методи та засоби безпечної передачі даних в корпоративних мережах. // Коробейнікова Т.І., Куцак Ю.В. // Збірник Матеріалів XLV НТК ВНТУ (2019). Режим доступу: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2019/paper/view/6606/5491
9. Побудова швидкісних мультисервісних мереж / Трояновська Т. І., Савицька Л. А., Максюта М. О., Поліщук Д. М. // Міжнародна науково-технічна конференція “Smart and Young”. – Київ, 2016. – №8, с. 72–78.

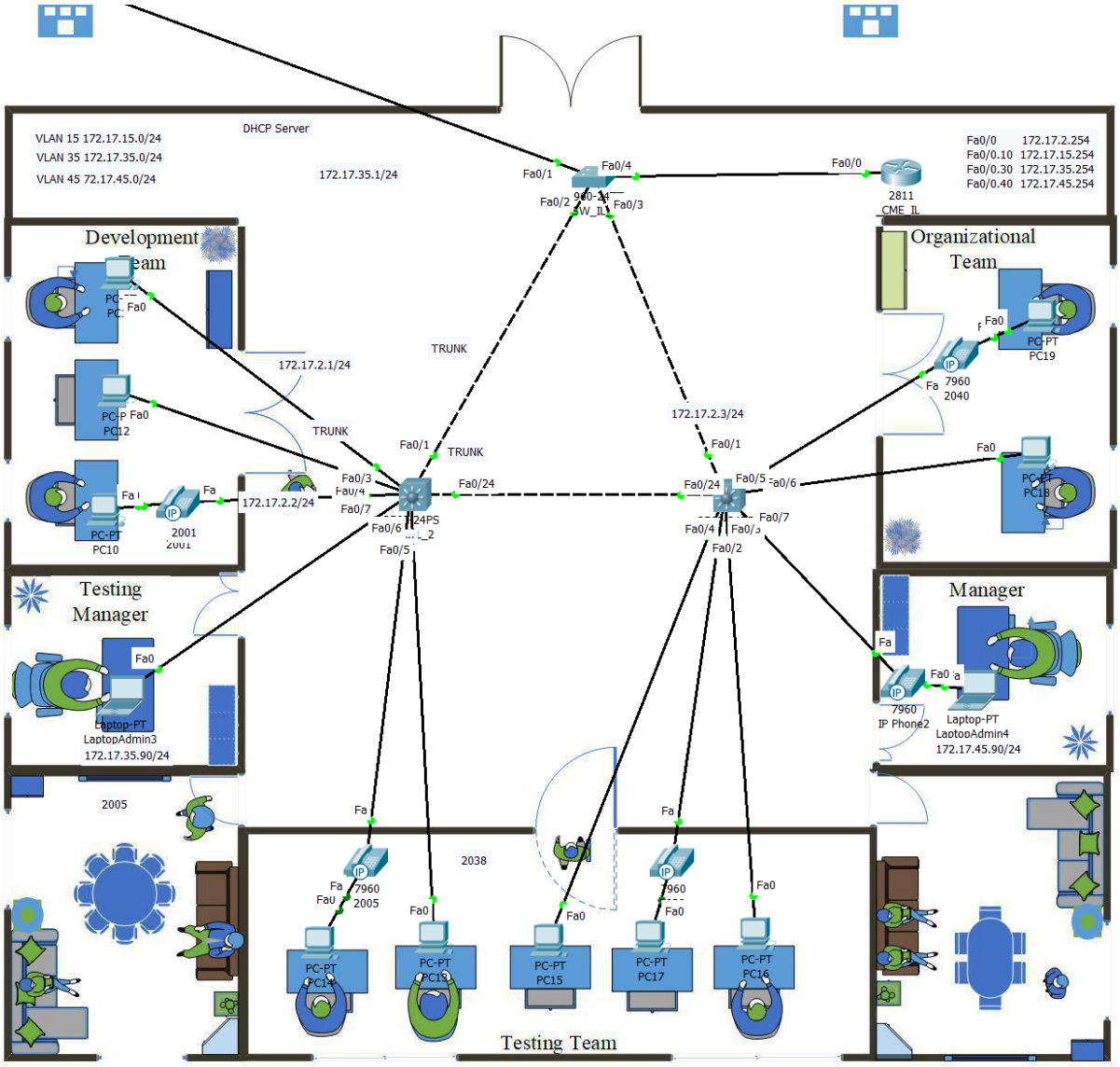
10. Аспекти побудови корпоративних мереж підприємства / Трояновська Т. І., Максюта М. О. // Збірник Матеріалів XLV НТК ВНТУ (2016). Режим доступу: http://conferences.vntu.edu.ua/public/conferences/9/schedConfs/6/program-uk_UA.pdf
11. Case J.D., Davin J.R., Fedor M.S., Schoffstall M.L. Internet network management using the simple network management protocol [Electronic resourse] / J.D.Case, J.R.Davin, M.S.Fedor, M.L.Schoffstall
12. Полный справочник по Cisco 3-е изд. //Пер. С англ. – К.Птицын. :2009. – 1088с.
13. Руководство Cisco по технологиям объединенных сетей, 4-е изд.// Cisco Systems// Пер. с англ. — М. :Издательский дом "Вильяме", 2005. − 1040 с. : ил — Парал. тит. Англ.
14. Компьютерные сети. 5-е изд./Таненбаум Э., Уэзеролл Д. //Т18 – СПб.: Питер, 2012. – 960 с.: ил.
15. VLAN в Cisco [Електронний ресурс] / Н. Самойленко. – Режим доступу : http://xgu.ru/wiki/VLAN_%D0%B2_Cisco.
16. Бэрри Нанс. Компьютерные сети пер. с англ. /Бэрри Нанс. –М.: БИНОМ, 2013. – 320 с.
17. Колесников О. Создание виртуальных частных сетей (VPN) / Колесников Олег. Хетч Барт. – М.: КУДИЦ-ОБРАЗ, 2015. – 464 с.
18. CCNA Discovery 4.0 Проектирование и поддержка компютерных сетей [Електронний ресурс]: Cisco System Inc., 2008. – Режим доступу:http://www.cisco.com/web/RU/learning/netacad/course_catalog/ ccna.html.
19. Методичні вказівки до виконання студентами-магістрантами економічної частини магістерських кваліфікаційних робіт / Уклад. В. О. Козловський – Вінниця: ВНТУ, 2012. – 22 с

ДОДАТКИ

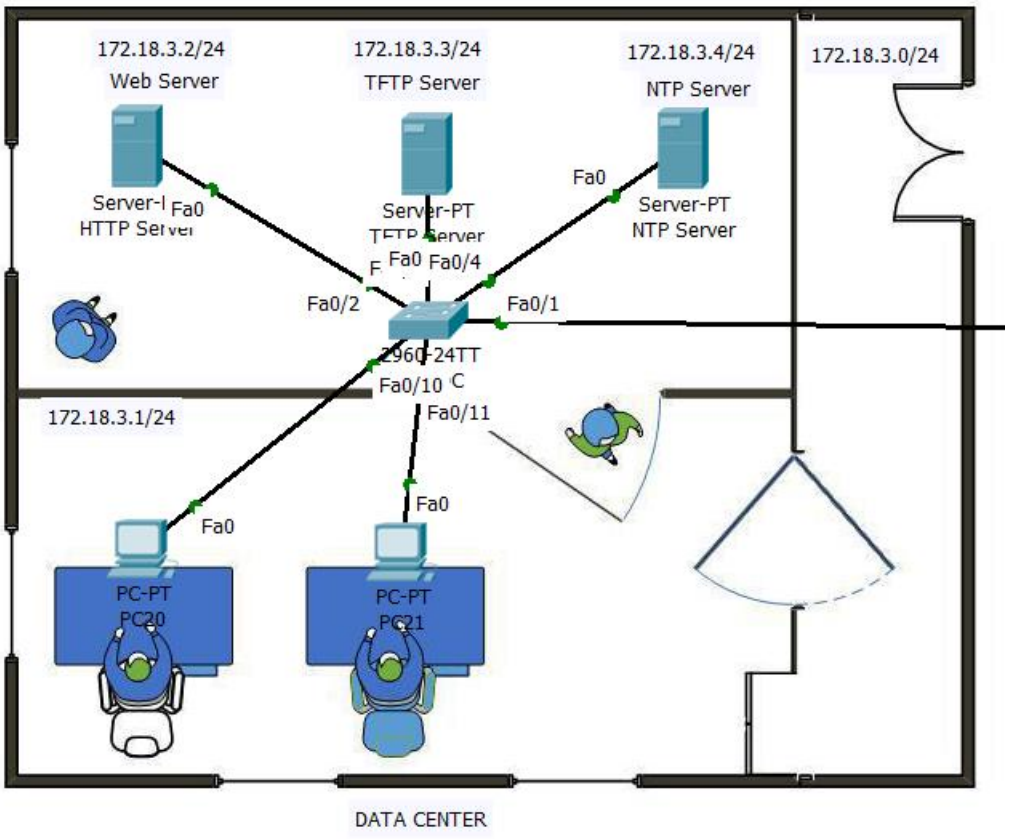
Д – Схема мережі центрального офісу



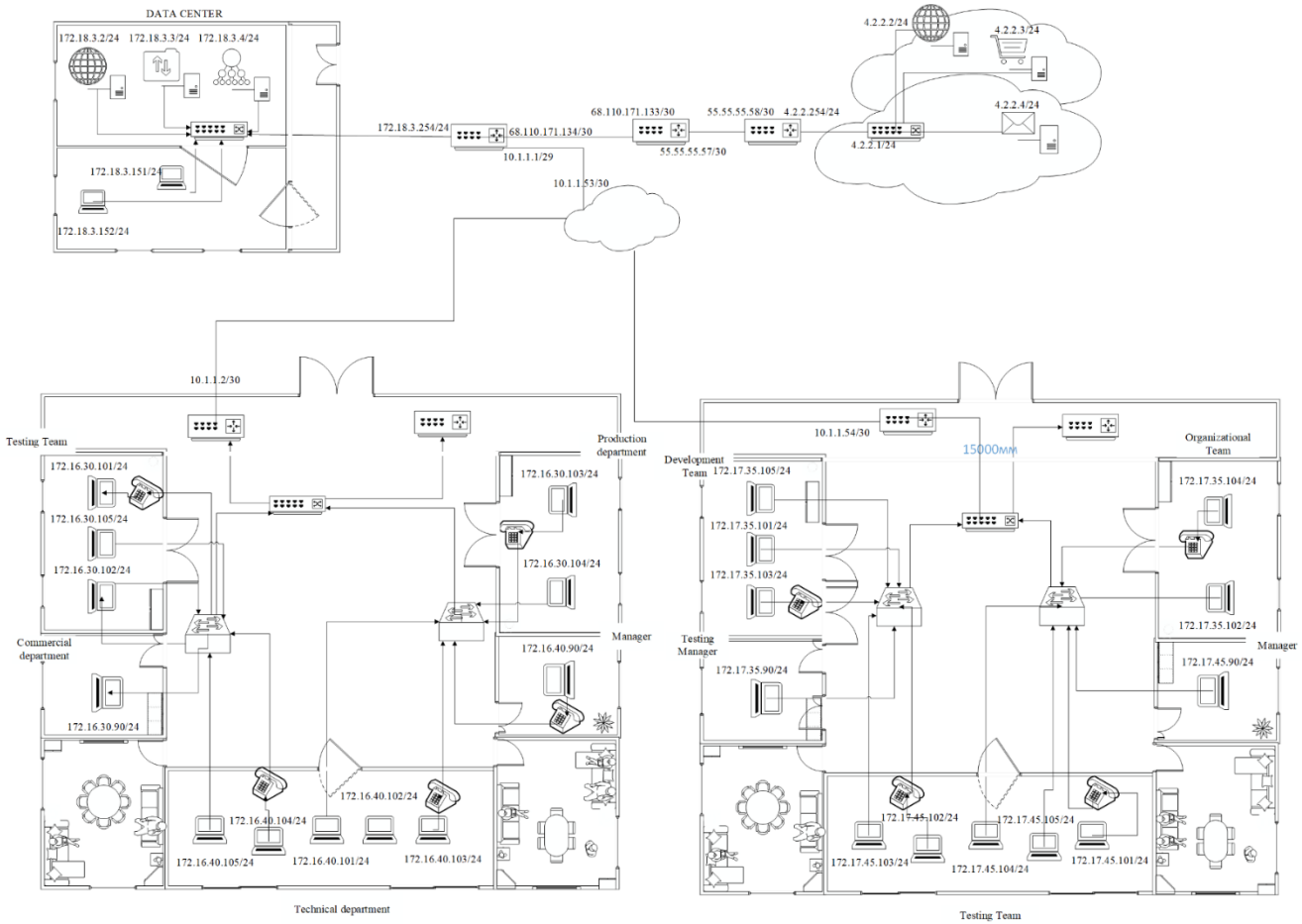
Додаток Ж – Схема мережі віддаленого офісу



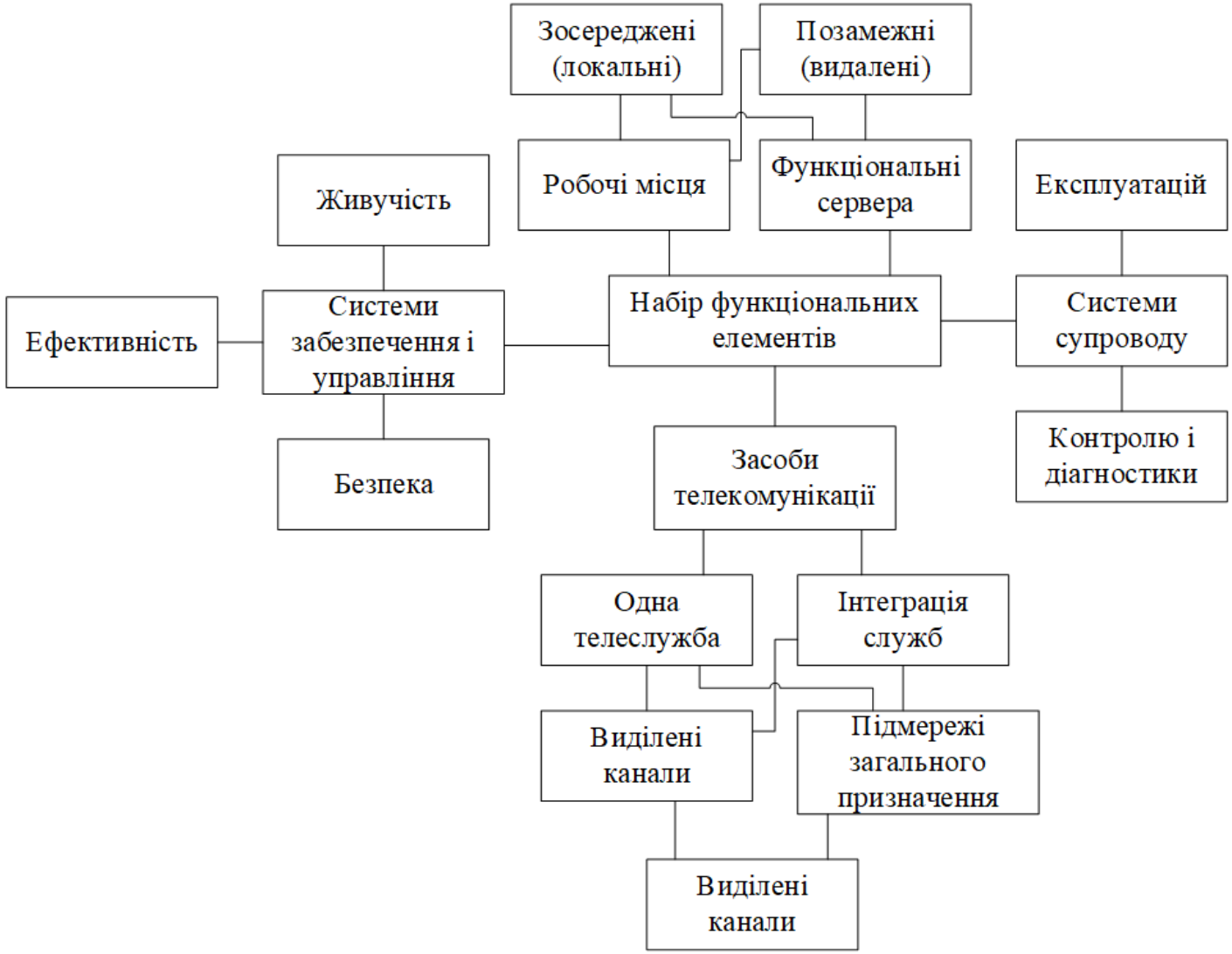
Додаток К – Схема мережі центра обробки даних



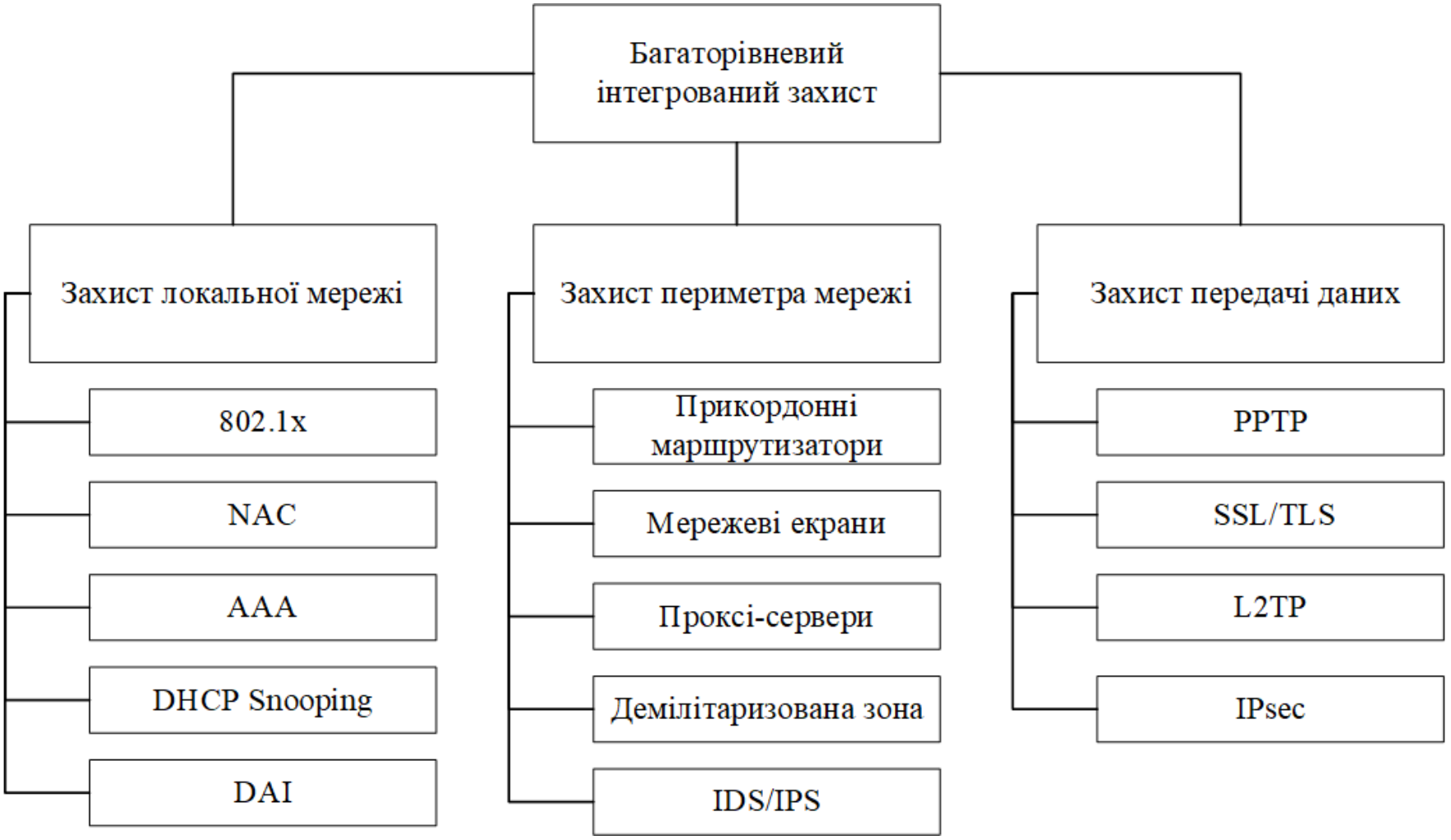
Додаток Л – Адресна схема мережі компанії «ITSosed»


DATA CENTER
172.18.3.2/24
172.18.3.3/24
172.18.3.4/24
172.18.3.151/24
172.18.3.152/24
172.18.3.254/24
68.110.171.134/30
68.110.171.133/30
55.55.55.57/30
55.55.55.58/30
4.2.2.254/24
4.2.2.2/24
4.2.2.3/24
4.2.2.4/24
4.2.2.1/24
10.1.1.1/29
10.1.1.53/30
10.1.1.2/30
10.1.1.54/30
15000мм
Testing Team
Production department
Development Team
Organizational Team
Commercial department
Manager
Testing Manager
172.16.30.101/24
172.16.30.105/24
172.16.30.102/24
172.16.30.90/24
172.16.30.103/24
172.16.30.104/24
172.16.40.90/24
172.16.40.102/24
172.16.40.104/24
172.16.40.105/24
172.16.40.101/24
172.16.40.103/24
172.17.35.105/24
172.17.35.101/24
172.17.35.103/24
172.17.35.90/24
172.17.35.104/24
172.17.35.102/24
172.17.45.90/24
172.17.45.102/24
172.17.45.105/24
172.17.45.103/24
172.17.45.104/24
172.17.45.101/24
Technical department
Testing Team

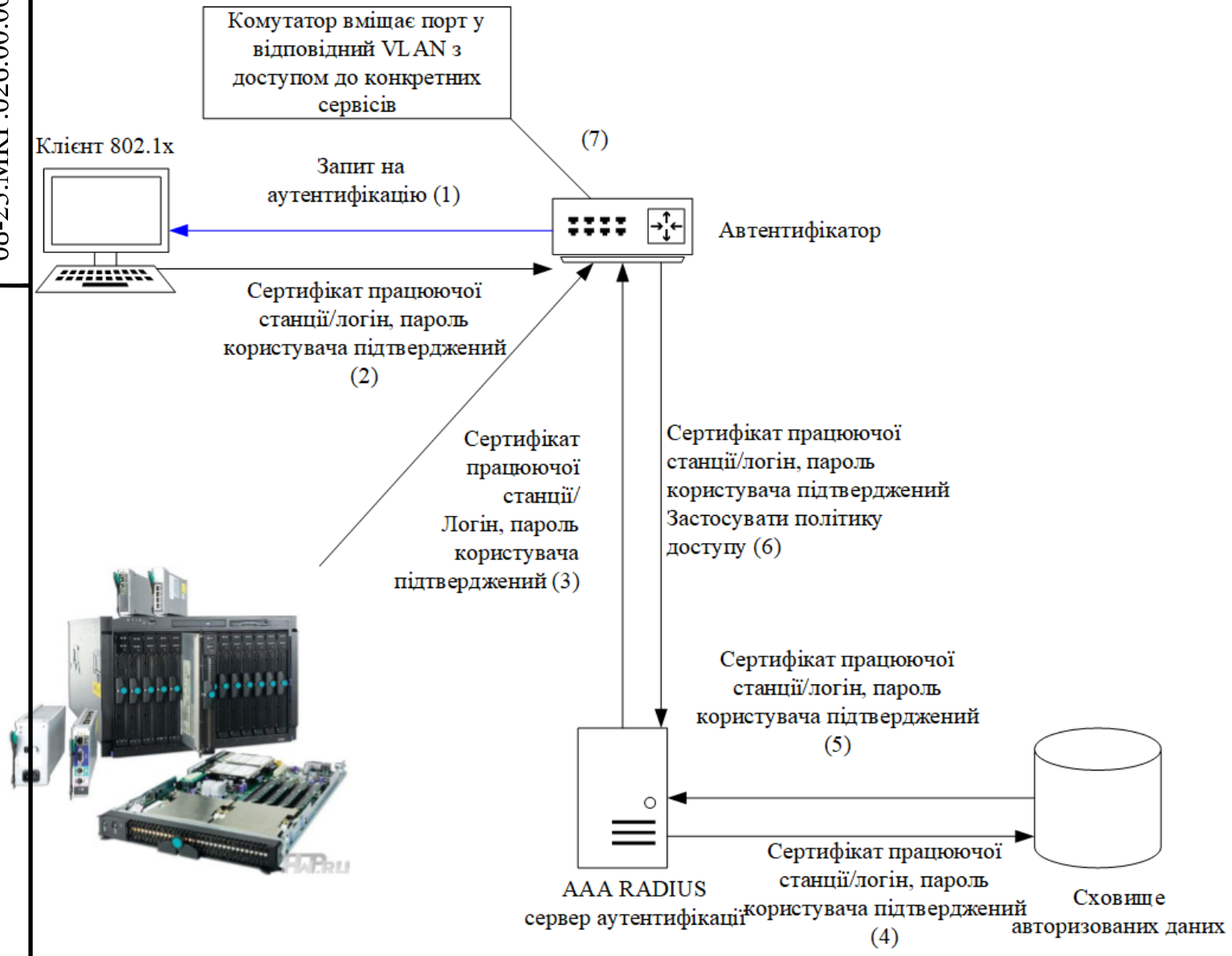
Додаток Б – Узагальнена схема функціональних компонентів корпоративних мере



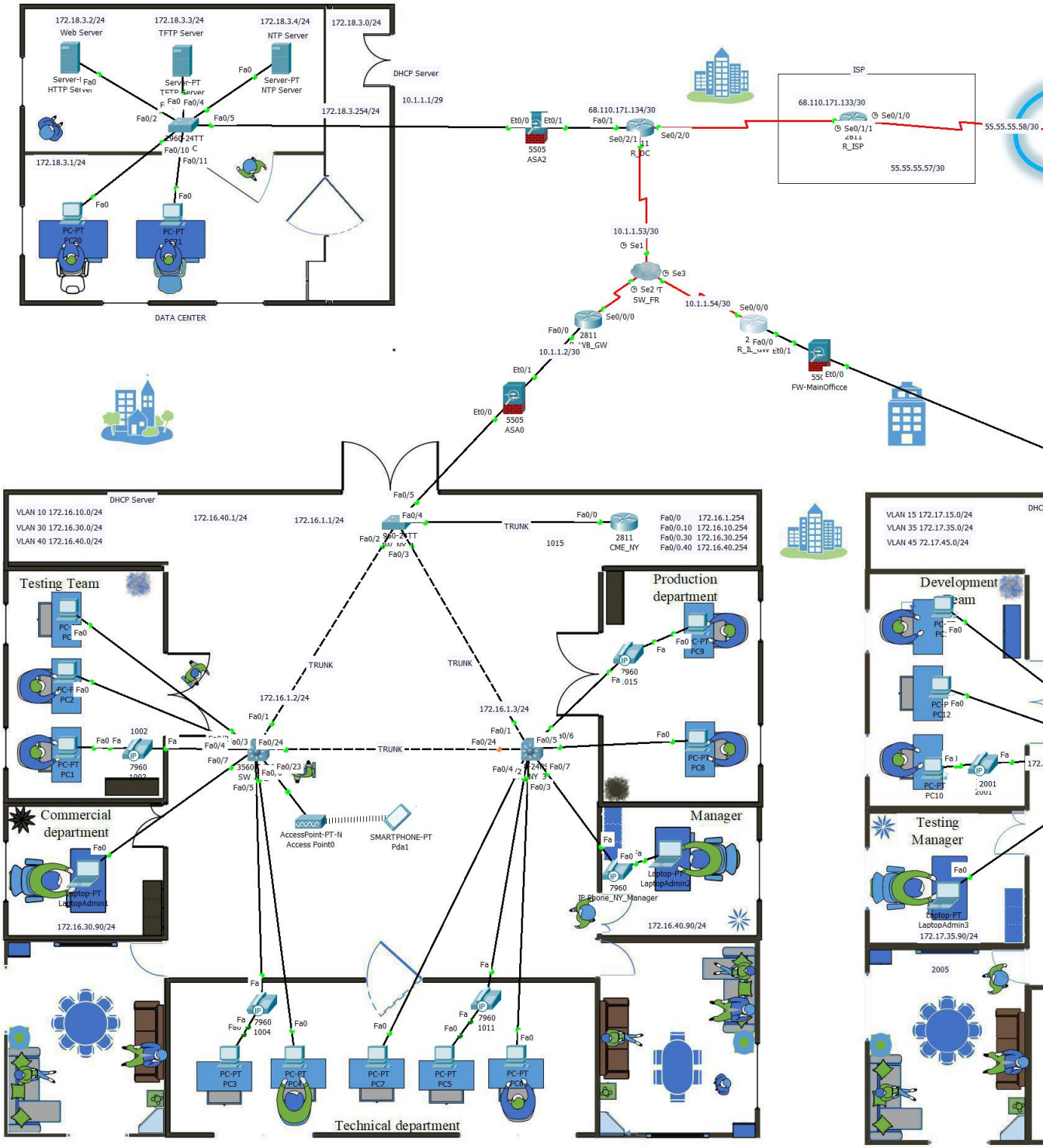
Додаток В – Узагальнена схема багаторівневого інтегрованого захисту



Додаток Г – Схема процесу аутентифікації в спрощеному вигляді



Додаток М – (обов'язковий)



Додаток А

Міністерство освіти і науки України

Вінницький національний технічний університет

Факультет інформаційних технологій та комп’ютерної інженерії

Кафедра обчислювальної техніки

ЗАТВЕРДЖУЮ

Завідувач кафедри ОТ

д.т.н., проф. Мартинюк Т.Б.

_____

(підпис)

“04” жовтня 2019 р.

ТЕХНІЧНЕ ЗАВДАННЯ

на виконання магістерської кваліфікаційної роботи

Методи та засоби безпечного передавання даних в корпоративних мережах

08-023.МКР.026.00.000.ТЗ

Науковий керівник: Войцеховська О.В.

_____

(підпис)

студент групи 2КІ-18м

_____ Куцак Ю.В.

(підпис)

Вінниця 2019 р.

1. Підстава для виконання магістерської кваліфікаційної роботи (МКР)

а) актуальність досліджень;

б) наказ по ВНТУ № 254 від 2 жовтня 2019 р. про затвердження теми магістерської кваліфікаційної роботи.

2. Мета і призначення МКР

а) мета – розробка методів та засобів візуалізації даних;

б) призначення розробки – застосування розроблених методів для розробки мобільного додатку.

3. Вихідні дані для виконання МКР

- сучасні методи та засоби захисту корпоративних мереж;
- типові об’єкти обслуговування;
- середовище розробки Cisco Packet Traser)

4. Вимоги до виконання МКР

- розробити методи та засоби безпечного передавання даних ;
- продемонструвати роботу методів на прикладі розробленої схеми.

5. Етапи МКР та очікувані результати

Етап	Зміст	Початок	Кінець	Результат
1	Інформаційний пошук та огляд літературних джерел.	02.10.19	25.10.19	Чернетки.
2	Аналіз зібраної інформації	26.11.19	18.11.19	Розділи 1-2
3	Розробка комплексного методу захисту мереж	9.11.19	20.12.19	Розділ 3
4	Виконання економічних обчислень	21.12.19	28.12.19	Розділ 4
5	Підготовка матеріалів пояснювальної записки.	29.12.19	9.12.19	Пояснювальна записка.

6. Матеріали, що подаються до захисту МКР

Пояснювальна записка МКР, графічні і ілюстративні матеріали, протокол попереднього захисту МКР на кафедрі, відзив наукового керівника, відзив опонента, протоколи складання державних екзаменів, анотації до МКР українською та іноземною мовами, нормоконтроль про відповідність оформлення ДР діючим вимогам.

7. Порядок контролю виконання та захисту МКР

Виконання етапів графічної та розрахункової документації ДР контролюється науковим керівником згідно зі встановленими термінами. Захист МКР відбувається на засіданні Державної екзаменаційної комісії, затвердженою наказом ректора.

8. Вимоги до оформлення МКР

Вимоги викладені в МЕТОДИЧНИХ ВКАЗІВКАХ до дипломного проектування, ДСТУ_ 3008-95, ДСТУ 3974-2000 «Правила виконання дослідно-конструкторських робіт. Загальні положення» та діючого ГОСТ 2.114-95 ЕСКД.

9. Вимоги щодо технічного захисту інформації в ДР з обмеженим доступом

Відсутні.

м.Вінниця - 2019 рік