МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
Факультет кібербезпеки, комп'ютерної та програмної інженерії
Кафедра комп'ютерних інформаційних технологій

ДОПУСТИТИ ДО ЗАХИСТУ

Завідувач кафедри

Аліна САВЧЕНКО

"__" _____ 2022 р.

ДИПЛОМНИЙ ПРОЕКТ
(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ

"БАКАЛАВРА"

ЗА СПЕЦІАЛЬНІСТЮ 122 «КОМП'ЮТЕРНІ НАУКИ»

Тема: "Багатошарова система інформаційної безпеки корпоративного середовища"

Виконавець: Зоря Олексій В'ячеславович

Керівник: к.т.н., доцент Савченко Аліна Станіславівна

Нормоконтролер: Олександр ШЕВЧЕНКО .
(підпис)

Київ 2022

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки, комп'ютерної та програмної інженерії

Кафедра комп'ютерних інформаційних технологій

Освітній ступінь: "Бакалавр"

Галузь знань, спеціальність, освітньо-професійна програма:

12 "Інформаційні технології, 122 "Комп'ютерні науки", "Інформаційні управляючі системи та технології" .

ЗАТВЕРДЖУЮ

Завідувач кафедри

Аліна САВЧЕНКО

"____" _____ 2022 р.

ЗАВДАННЯ

на виконання дипломного проекту студента

Зорі Олексія В'ячеславовича

(прізвище, ім'я, по батькові)

1. **Тема роботи:** «Багатошарова система безпеки корпоративного середовища» затверджена наказом ректора №454/ст. від 29.04.2022.
2. **Термін виконання роботи:** 09.05.2022 – 10.06.2022.
3. **Вихідні дані до роботи:** організація процесу захисту корпоративного середовища, технології, стандарти та специфікації комп'ютерних мереж.
4. **Зміст пояснювальної записки (перелік питань, що підлягають розробці):** аналіз існуючих методів та засобів для організації інформаційної безпеки в обчислювальних мережах, огляд концепції політики інформаційної безпеки, вибір апаратно-технічного забезпечення, проектування захищеної комп'ютерної мережі.
5. **Перелік обов'язкового графічного матеріалу:** слайди презентації MS PowerPoint.

6. Календарний план-графік

№ з/п	*Завдання*	*Термін виконання*	*Підпис керівника*
1.	Ознайомлення з предметною областю та постановкою задачі дипломного проектування	09.05.2022р. – 13.05.2022р.	
2	Вивчення спеціальної літератури та відповідної технічної документації	14.05.2022р. – 18.05.2022р.	
3	Огляд засобів та методів побудови локальних комп'ютерних мереж	19.05.2022р. – 20.05.2022р.	
4	Аналіз сучасних тенденцій та практик в галузі інформаційної безпеки	21.05.2022р. – 23.05.2022р.	
5	Розробка проекту захищеної мережі підприємства, опис створеної системи	24.05.2022р. – 29.05.2022р.	
6	Оформлення пояснювальної записки	30.05.2022р. – 04.06.2022р.	
7	Підготовка графічного демонстраційного матеріалу	05.06.2022р. – 14.06.2022р.	

Дата видачі завдання: 09.05.2022 р

Керівник дипломного проекту _____ Аліна САВЧЕНКО
(підпис керівника)

Завдання прийняв до виконання _____ Олексій ЗОРЯ
(підпис випускника)

РЕФЕРАТ

Пояснювальна записка до дипломного проекту «Багатошарова система безпеки корпоративного середовища» представлена на 60 сторінках, містить 18 рисунків, 15 наукових джерел.

Мета дипломного проекту: проектування багатошарової системи інформаційної безпеки корпоративного середовища з використанням фізичних пристроїв захисту (*Cisco ASA*).

Об'єкт дослідження: процес передачі даних в корпоративному середовищі.

Предмет дослідження: методи забезпечення інформаційної безпеки обчислювальної мережі за допомогою програмних та апаратних засобів.

Метод дослідження: аналітичний огляд існуючих методів інформаційного захисту корпоративного середовища, порівняльний аналіз програмних та апаратних засобів, технологій для побудови захищеного корпоративного середовища.

Результат проекту: Спроектована інформаційна система може бути використана в якості універсальної основи забезпечення інформаційної безпеки в локальній мережі. Налаштування дозволяють використовувати широкий комплекс програмно-технічних засобів, що можуть працювати безпосередньо з фізичними пристроями захисту (*Cisco ASA*), так і працювати окремо забезпечуючи інші потреби. Загалом розроблена система здатна забезпечувати достатній рівень захисту від більшості існуючих загроз.

ІНФОРМАЦІЙНА БЕЗПЕКА, ІНФОРМАЦІЙНА СИСТЕМА, КОМП’ЮТЕРНА МЕРЕЖА, ПРОТОКОЛ, ЗАГРОЗА

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ІзОД – інформація з обмеженим доступом.

КК – комп’ютерний комплекс.

ІБ – інформаційна безпека.

ЛОМ – локальна обчислювальна мережа.

ПК – персональний комп’ютер.

LAN – local area network.

WAN – wide area network.

IP – internet protocol.

MAC – media access control.

VLAN *– Virtual Local Area Network.*

ВСТУП

В сучасному світі комп'ютерна мережа є одним з основних компонентів будь-якого підприємства. Комп'ютерна мережа являє собою комплексну систему, що складається з апаратних та програмних засобів, які забезпечують обмін даними між обчислювальними пристроями (персональні комп'ютери, сервери, комутатори, маршрутизатори, сховища, тощо). Мережі є основним фактором сучасної глобалізації, оскільки передача інформації являє собою не лише зручним способом зв'язку, а й одним з головних елементів комфорту в розумінні людини 21-го століття.

Завдяки широкому спектру функцій та можливостей, комп'ютерні мережі справедливо отримали широке застосування в державних та комерційних організаціях. Об'єднання основних функціональних вузлів, ресурсів та інших пристроїв в одну систему дає змогу в значній мірі оптимізувати та прискорити виконання багатьох процесів і водночас централізувати адміністрування та керування.

В той же час, із збільшенням ролі та поширенням використання мережевих технологій, постало питання забезпечення безпеки інформаційних систем. Водночас з розвитком комп'ютерних мереж, введенням новітніх рішень та процесом загальної модернізації, зловмисники розроблювали нові способи отримання несанкціонованого доступу до ресурсів систем, пошуку нових вразливостей в програмному та апаратному забезпечені, створенню спеціальних програм для тої чи іншої неправомірної дії.

Необхідність та актуальність захисту інформаційних систем в Україні зросла в багато разів на фоні початку збройної агресії російської федерації в 2014-му році, а після повномасштабного вторгнення 2022-го року стала загальною необхідністю, оскільки на відміну від мережевих атак спричинених окремими особами або групами осіб, інформаційні атаки країни-агресора характеризуються більшою потужністю та небезпекою. Саме тому створення ретельно спланованої та якісної комплексної системи захисту інформації є не просто важливим аспектом роботи підприємства, а необхідністю.

Забезпечення працездатності системи, а також збереженості всіх її окремих компонентів, особливо ресурсів, що стосуються інформації з обмеженим доступом, є

надзвичайно важливим та актуальним питанням сьогодення. Враховуючи вищезазначене проектування багатошарової системи інформаційної безпеки корпоративного середовища є актуальним.

РОЗДІЛ 1
ЗАГАЛЬНА ХАРАКТЕРИСТИКА БЕЗПЕКИ ІНФОРМАЦІЇ В ЛОКАЛЬНИХ ОБЧИСЛЮВАЛЬНИХ МЕРЕЖАХ

1.1. Актуальність та передумови створення систем захисту комп'ютерних мереж

Основним завданням створення багатошарової системи захисту локальних обчислювальних мереж є захист інформаційного середовища від навмисного або випадкового втручання, спроб руйнування його компонентів, отримання несанкціонованого доступу та гарантування роботи системи при виникненні непередбачуваних обставин.

В сучасному світі інформаційні системи займають одне з ключових місць у функціонуванні організацій та підприємств. Призначення інформаційних систем полягає у забезпеченні потреб користувачів в процесі виконання ними їх робочих обов'язків. За допомогою комп'ютерних мереж співробітники підприємства мають змогу проводити швидкий та ефективний обмін інформацією, віддалено зберігати та створювати файли, проводити листування поштою, отримувати доступ до всесвітньої мережі, її ресурсів та безпосередньо взаємодіяти з процесами виробництва, тобто функціонал включає основні аспекти життєдіяльності кожного підприємства. Потенціал та ефективність використання мереж є без перебільшення незамінним у сучасних реаліях.

Найбільшого розповсюдження серед сучасних підприємств набула практика введення єдиної корпоративної інформаційної системи, що дозволяє централізувати адміністрування і в той же час об’єднати всі пристрої в єдине середовище для ефективного функціонування та взаємодії підрозділів.

Зі зростанням ролі інформаційних систем у сфері роботи підприємств одночасно посилилися загрози неправомірного впливу, атак та інших методів для отримання несанкціонованого доступу, спотворення чи руйнування інформації всередині систем. Масштаби шкідливого впливу можуть варіюватися від перебоїв в роботі системи або нанесення фінансових збитків комерційному підприємству до нанесення суттєвої шкоди інтересам України, наприклад розголошення державної таємниці. Тому інформаційній безпеці завжди відводять особливо важливе місце у проектуванні будь-якого підприємства.

Загалом інформаційну безпеку можна охарактеризувати, як стан захищеності систем обробки та зберігання даних, при якому забезпечено відповідність до основних критеріїв оцінки інформаційної безпеки. Самі критерії являють собою сукупність методів для визначення вимог захисту системи, створення захисних компонентів та оцінки ступенів захищеності. [1]

Система передбачає наступні характеристики інформаційної безпеки:

1. Конфіденційність – властивість інформації, яка полягає в тому, що певна інформація може бути отримана лише санкціонованим користувачем.
2. Цілісність – властивість інформації, яка полягає в тому, що інформація може бути змінена, модифікована лише санкціонованим користувачем.
3. Доступність – властивість інформації, яка полягає в тому, що виключно санкціонований користувач, може використовувати ресурс відповідно до правил, встановлених політикою безпеки не очікуючи довше заданого інтервалу часу.

1.2. Види загроз та мережевих атак на інформаційні системи

Основною функцією існуючих комплексів захисту інформації є попередження та/чи ліквідація наслідків загроз інформаційному середовищу. Для кращого розуміння проблематики необхідно ознайомитись із загальними поняттями та різновидами існуючих загроз. [3]

Загроза – це обставини чи події, які можуть спричинити порушення інформаційної безпеки та/або нанесення збитку корпоративному середовищу. Тобто загроза представляє будь-який потенційно можливий несприятливий вплив на існуючу систему.

Загалом до загроз можна віднести:

- навмисні дії порушників ІБ;
- помилки різного характеру персоналу під час експлуатації ресурсів;
- наслідки помилок проектування автоматизованих систем;
- стихійні лиха та непередбачувані аварійні ситуації.

За час експлуатації інформаційних систем найбільшого розповсюдження серед зловмисників набули віддалені мережеві атаки, що являють собою руйнівний вплив на систему, що здійснюється по каналах зв'язку. За характером впливу мережеві атаки класифікують на активні та пасивні. Активний вплив являє собою вплив, що здійснює пряме втручання в роботу системи і призводить до порушень працездатності системи чи її окремих вузлів, взаємодія з компонентами системи, зміна конфігурації, тощо. Пасивний вплив характеризується тим, що такий вплив прямо не відображається на роботу системи. Такі види атак важче виявити. [2] Серед найрозповсюдженіших мережевих атак можна виділити наступні:

1. Атака на мережу методом переповнення буфера – це вид мережевої атаки завдання якої полягає в тому, щоб переповнити буфер запису даних програми більшим обсягом, ніж було закладено творцями програми. Наслідком подібної атаки може бути виконання інструкцій записаних зловмисником.

2. *DNS* спуфінг – це вид мережевої атаки результатом якої є внесення хибної відповідності між *IP*-адресою і доменним іменем в кеш файл *DNS* сервера.

Результатом успішного проведення такої атаки є підміна даних на сервері *DNS*, внаслідок чого користувачі сервера отримають неправдиву інформацію про доменні імена і *IP*-адреси.

3. Сніфінг – це прослуховування каналу даних в межах однієї локальної мережі. Атака полягає у перехопленні пакетів даних, що адресовані іншим санкціонованим пристроям в мережі. Використовується для ефективного аналізу захисту системи, отримання інформації щодо наявного програмного та апаратного обладнання. При використанні сніфера в пасивному режимі, зловмисник може отримати трафік сесій протоколів *SSL, TLS, TCP, UDP*, адреси *IP*, номера портів, що використовуються на різних пристроях і при цьому бути непоміченим програмними засобами захисту.

4. *DoS* атака – це напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними санкціонованим користувачам. Одним із найпоширеніших методів нападу є насичення атакованого комп'ютера або мережевого устаткування великою кількістю зовнішніх запитів, які в процесі атаки можуть значно уповільнити або повністю вивести з ладу пристрій або сервіс. Ефект *DoS* атаки стає в значній мірі більш ефективним, якщо атака відбувається одночасно з великої кількості *IP*-адрес. В результаті така атака називається *DDoS*, тобто розподілена атака на відмову в обслуговуванні.

1.3. Методи виявлення атак

Для попередження та активній протидії зловмисникам використовують системи виявлення вторгнень (*IDS*), що являють собою програмні або апаратні засоби, призначені для виявлення випадків несанкціонованого доступу, певних аномалій та інших незвичайних ситуацій в інформаційній системі. Деякі системи виявлення вторгнень можуть виявити початок атаки на мережу (*IPS*). Аналіз інформації всередині системи є основоположною складовою будь-якої сучасної системи виявлення та запобігання вторгнень. *IDS* системи можна класифікувати відповідно до методів виявлення загроз на основі сигнатур та виявлення аномалій. [2]

Метод виявлення аномалій заснований на профілюванні роботи та процесів у

системі, тобто циркулююча в системі інформація та події сприймаються, як нормальна модель роботи, з якою потім порівнюється нова поведінка. Такий метод виявлення є доволі інноваційним, оскільки використовує окремі аспекти машинного навчання і дозволяє виявляти невідомі види атак, але в той же час має низку недоліків до яких часто відносять велику кількість хибних спрацювань системи. Особливо сильно даний недолік проявляється при використанні специфічного програмного забезпечення, що може залишати особливу сигнатуру в інформаційній системі.

Метод виявлення сигнатур заснований на простому порівнянні послідовності даних зі зразком. Вхідний набір проглядається, аналізується та послідовно порівнюється з сигнатурою – характерним рядком програми, що збігається з характеристикою шкідливого трафіку. Сама сигнатура може бути логічною фразою, командою, або окремим фрагментом коду. При знаходженні відповідності, спрацьовує тригер, що заздалегідь налаштований адміністратором системи. На відміну від методу виявлення аномалій, сигнатурний підхід здатен виявляти лише ті загрози, що присутні в базі сигнатур, і тому такий метод є абсолютно неефективним у виявлені нових невідомих атак. [2]

Використання систем виявлення вторгнень є основою для забезпечення безпеки всередині мережі, а також діагностики. Ретельний аналіз журналів та записів(логів) системи, дозволяє фахівцям в області ІБ проводити ефективні процедури укріплення захисту системи та її подальшого розвитку.

1.4. Використання брандмауера для захисту інформаційної системи

Міжмережевий екран, брандмауер або фаєрвол – апаратний або програмний засіб, що проводить контроль інформації, що надходить чи виходить з інформаційної системи. В залежності від налаштувань, брандмауер може дозволяти чи забороняти трафік, шифрувати дані, виступати інтерпретатором мережевих адрес (*NAT*).

Розрізняють два типи брандмауерів: апаратний та програмний:

- апаратний міжмережевий екран являє собою спеціальний пристрій, що фізично підключається до обчислювальної мережі. Для налаштування такого виду

брандмауера використовують консольний порт на самому пристрої або за допомогою спеціального інтерфейсу командного рядка(*CLI*) з віддаленого ПК через протокол *Telnet* або *SSH*. Прикладами таких пристроїв виступають: *Cisco PIX, Cisco ASA, Firewall ZL1, Watchguard Firebox* та інші;

- програмний міжмережевий являє собою програмний застосунок, що функціонує на окремих кінцевих пристроях: ПК, серверах, а також маршрутизаторах.

Робота брандмауера полягає в аналізі вмісту пакетів інформації, що надходять із зовнішньої мережі і згідно з актуальною конфігурацією проводити відповідні дії. Виступає в якості захисного бар'єру між внутрішньою мережею підприємства та зовнішньою обчислювальною мережею(*WAN*). [6]

Загалом існує три покоління брандмауерів із різними видами фільтрування трафіку. Міжмережеві екрани першого покоління працюють як пакетний фільтр, порівнюючи основну інформацію, таку як оригінальне джерело, призначення пакета, порт чи протокол, з визначеним переліком правил. Брандмауери другого покоління містять додатковий параметр налаштування фільтра – стан з'єднання. Використовуючи цю інформацію технологія може відслідковувати дані про поточні з'єднання, їх початок та кінець. Брандмауери третього покоління побудовані для фільтрування інформації за допомогою всіх рівнів моделі *OSI*, зокрема і прикладного рівня. На основі цієї інформації брандмауер може виявляти атаки, які намагаються обійти його через дозволений порт або несанкціоноване використання протоколу.

1.5. Концепція політики інформаційної безпеки

Політика інформаційної безпеки – це набір правил, рекомендацій, вимог та обмежень, які характеризують та регламентують порядок ІБ на підприємстві. Важливо зазначити, що політика безпеки інформації є частиною загальної політики безпеки організації і повинна успадковувати основні її принципи. [6] Головним завданням створення такого документу є визначення основних правил використання ресурсів підприємства, регламентування програмних засобів, що використовуються на підприємстві, сегментація доступу до ресурсів, порядок та правила протидії порушень.

Проводячи аналіз теми введення політики інформаційної безпеки підприємства можна сформулювати її основні завдання:

- захист КК від втручання в процес його функціонування сторонніх осіб, тобто можливість використання КК і доступ до його ресурсів повинні мати лише зареєстровані користувачі;
- розмежування доступу зареєстрованих користувачів до інформаційних ресурсів КК, тобто можливість доступу лише до тих ресурсів та виконання лише тих операцій, які необхідні конкретним користувачам КК для виконання ними їх службових завдань;
- забезпечення захисту користувачів та інформаційних ресурсів КК при доступі до/з зовнішніх мереж, наприклад, інтернет;
- захист збережених даних по каналах зв'язку даних, у тому числі інформації з обмеженим доступом від несанкціонованої модифікації (спотворення), розголошення (витоку), фальсифікації;
- захист від несанкціонованої модифікації (підміни або знищення) та контроль цілісності використовуваних в КК програмних засобів, а також контроль КК від впровадження несанкціонованого або нелегального програмного забезпечення, включаючи віруси та шкідливе програмне забезпечення;
- контроль цілісності операційного середовища виконання прикладних програм і його відновлення в разі порушення;
- ведення єдиного реєстру ПЗ, що використовується на підприємстві.

Основною метою політики ІБ є захист інформації на підприємстві, що обробляється в автоматизованих системах, створення та підтримка у належному та дієздатному стані системи організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї.

1.6. Постановка задачі та висновки до розділу

В ході огляду предметної області були сформовані основні завдання та підстави створення багатошарової системи захисту інформації підприємства.

У результаті проведеного аналізу було розглянуто:

- види загроз та атак на інформаційну систему, їх небезпека, різновиди, види їх впливу на інформаційну систему;

- методи виявлення мережевих атак;

- принцип роботи та різновиди систем виявлення/попередження вторгнень;

- особливості роботи апаратних та програмних міжмережевих екранів, їх види та ефективність застосування;

- дослідження концепції політики інформаційної безпеки, сформульовані її завдання та переваги.

Проаналізувавши передумови та підстави забезпечення інформаційної безпеки корпоративної мережі підприємства, можна зазначити, що надійність та ефективність проектованої системи безпеки інформації залежить від комплексу програмно-технічних та апаратних засобів, а також їх підкріплення організаційними та правовими заходами зазначеними в політиці інформаційної безпеки.

Враховуючи вищезазначене проектування системи інформаційної безпеки корпоративного середовища є актуальним. Отже метою дипломного проекту є створення багатошарової системи інформаційної безпеки корпоративного середовища з використанням фізичних пристроїв захисту (*Cisco ASA*).

Відповідно до поставленої мети необхідно вирішити такі завдання:

1. Проаналізувати методи та засоби реалізації інформаційної безпеки корпоративного середовища.
2. Спроектувати мережу департаменту підприємства, в тому числі визначити технологію, необхідне апаратне забезпечення, структуровану кабельну систему, конфігурацію обладнання тощо.
3. Визначити методи захисту інформації та конфігурацію обладнання для захисту корпоративного середовища.

РОЗДІЛ 2
АПАРАТНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ЛОКАЛЬНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ПІДПРИЄМСТВА

В розділі будуть розглянуті теоретичні та апаратно-технічні рішення для побудови захищеної мережі підприємства. Загалом будуть розглянуть такі теми: основні терміни в галузі локальних комп'ютерних мереж, технології побудови мереж, класифікація мереж, апаратне забезпечення, окремі мережеві протоколи.

2.1. Основні терміни

Кінцевий пристрій, хост – це будь-який фізичний пристрій в мережі, який може надсилати, отримувати та/або передавати інформацію. Персональний комп'ютер є найбільш розповсюдженим вузлом і тому його часто називають комп'ютерний вузол або інтернет вузол.

Клієнт-сервер – це мережева архітектура, в якій загальні завдання та навантаження розподілені між поставниками послуг(серверами), і замовниками послуг(клієнтами).

Клієнт – це кінцевий пристрій, що використовує ресурси локальної обчислювальної мережі. В той же час клієнт не надає свої ресурси іншим пристроям.

Сервер – це кінцевий пристрій, зазвичай це комп'ютер з високою обчислювальною здатністю, що використовується для надання послуг клієнтам.

Мережевий ресурс – це ресурс, що може бути використаним іншими пристроями в мережі.

Локальний ресурс – це ресурс доступний для використання лише пристроєм, на якому він зберігається.

Протокол - це чіткий набір правил, що визначає пристрої в мережі. Протокол також задає загальні правила взаємодії різних програм, мережевих вузлів чи систем і створює таким чином єдиний простір передачі. Різні протоколи найчастіше описують лише окремі сторони одного типу зв'язку й, узяті разом, утворюють стек протоколів.

Стек протоколів – це ієрархічно організований набір мережевих протоколів, що використовується для взаємодії вузлів в мережі. Найбільш розповсюдженими стеками є модель *OSI* та *TCP/IP*.

Активне мережеве обладнання – це пристрої, що використовуються для побудови локальних обчислювальних мереж і мають набір інтелектуальних функцій для оброки, розподілення і передачі сигналу. У число активного мережевого обладнання входять такі пристрої, як: комутатори, сервери, маршрутизатори, бездротові точки доступу та інші. [6]

Комутація – процес з'єднання абонентів комунікаційної мережі через транзитні вузли. Комунікаційні мережі забезпечують зв'язок своїх абонентів між собою.

Маршрутизація – процес визначення маршруту доставки інформації в мережах зв'язку.

2.2. Концепція побудови та роботи мережі

Головна мета комп’ютерної мережі полягає у об’єднанні пристроїв для подальшого швидкого та ефективного обміну інформацією. Найпростіша мережа може складатися навіть з двох пристроїв. Найпоширенішим прикладом мережі, що складається з двох пристроїв є звичайна домашня локальна мережа для використання ресурсів мережі інтернет. Така система складається з персонального комп’ютера та домашнього маршрутизатора, який також може виконувати роль комутатора, *DHCP*-сервера,

міжмережевого екрану, тощо. Підключення кінцевих пристроїв та активного мережевого обладнання відбувається за допомогою адаптерів. Адаптери можуть бути як дротовими, використовуючи коаксіальний кабель чи більш новітній кабель типу «вита пара», так і бути бездротовими, використовуючи технологію *Wi-Fi*.

2.3. Топологія комп'ютерних мереж

Топологія комп'ютерної мережі являє собою компонування та конфігурацію фізичного розташування кінцевих пристроїв по відношенню один до одного та спосіб їх з'єднання між собою. Топологія відображає структуру зв'язків між її основними функціональними елементами і в залежності від компонентів, прийнято розрізняти логічну та фізичну структуру. Логічна структура визначає логічну взаємодію між кінцевими пристроями, а фізична в свою чергу їх безпосереднє фізичне з'єднання між собою. Варто зазначити, що фізична топологія чітко залежить від технологій та стандартів, що використовуються. [6]

Загалом виділяють 3 базових топології та певну кількість похідних. Нижче будуть описані три основні топології, що використовуються.

«Шина» – це вид мережевої топології, що реалізується за допомогою одного спільного кабелю, до якого підключаються кінцеві пристрої. Кабель у такій топології називається шина або магістраль. [4] На кінцях такого кабелю для запобігання відбиття сигналу використовують поглиначі сигналу, що називаються термінаторами.

Такий вид мережевої топології передбачає використання одного кабелю, до якого підключаються всі комп'ютери мережі. Повідомлення, що надсилається з будь-якої робочої станції, поширюється на всі комп'ютери мережі. Кожний пристрій перевіряє до кого адресоване повідомлення, якщо повідомлення адресоване йому, то обробляє його. Дана топологія вважається застарілою і майже не має практичного використання в наш час. Реалізація такої топології показана на рисунку 2.1.

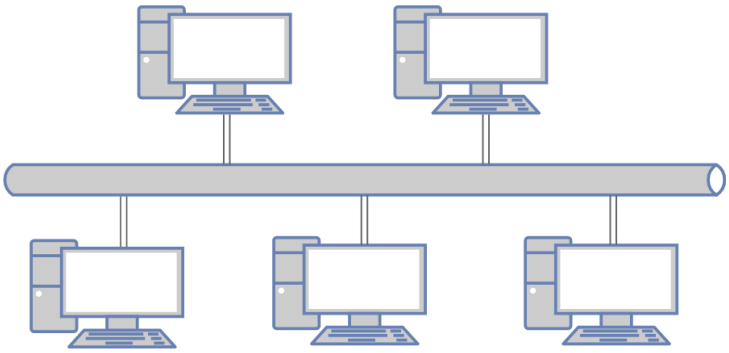

Рис. 2.1. Фізична топологія шина

«Кільце» – це мережева топологія, згідно з якою кінцеві пристрої підключаються до кабелю, замкнутого в коло. Цей варіант топології вирішує проблему топології шина і не потребує встановлення спеціальних термінаторів сигналу на кінцях кабелю. Сигнали передаються по кільцю в одному напрямі і проходять послідовно через кожний пристрій в мережі і останній одночасно виступає в ролі посилювача сигналу.

Один зі способів передачі потоку даних по кільцевій мережі називається передачею маркера. Такий спосіб передачі називається *Token-ring* і передбачає використання спеціальних концентраторів. Фізично мережа утворює зірково-кільцеву топологію, але в дійсності пристрої поєднуються в кільце. Концепція такого способу передачі даних полягає у тому, що спеціальний концентратор переміщує вздовж мережі невеликий блок даних, званий маркером. Володіння цим маркером гарантує право передачі. Маркер передається послідовно по колу. Така архітектура не отримала широкого застосування в силу обмеженості у швидкості(до 16 Мбіт/с) та низки проблем пов’язаних зі складністю фізичної реалізації. Топологія «кільце» продемонстрована на рисунку 2.2.

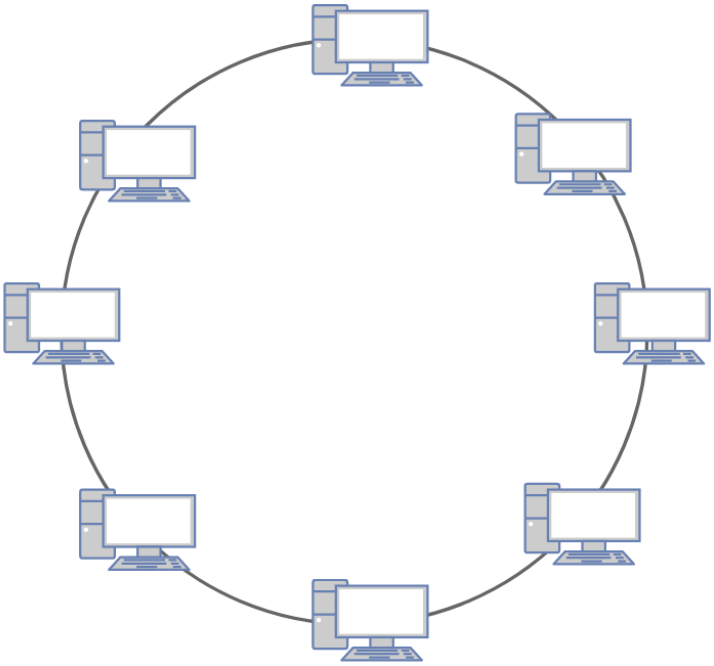

Рис. 2.2. Фізична топологія кільце

«Зірка» – це мережева топологія, що характеризується виділеним центром, до якого підключаються інші пристрої. Обмін інформацією реалізується через центральний пристрій в мережі.

Суттєвою перевагою використання такої топології полягає у стійкості до відмов або інших аварійних ситуацій пов’язаних з кінцевими пристроями, оскільки при виході з ладу одного робочого пристрою, інші можуть продовжувати роботу в звичайному режимі без зниження показників швидкості. З цієї переваги випливає і недолік, що проявляється в тому, що при виході з ладу центрального пристрою, що здійснює передачу даних, передача інформації стає неможливою, тому використовують запобіжні заходи для мінімізації таких випадків. Використання такої топології дозволяє легко контролювати роботу мережі, локалізувати несправності шляхом простого відключення від центра тих або інших абонентів. На цей час, «зірка» є найпоширенішим рішенням серед інших у плануваннях локальних комп’ютерних мереж всіх видів і спрямувань. Реалізація такої топології продемонстрована на рисунку 2.3.

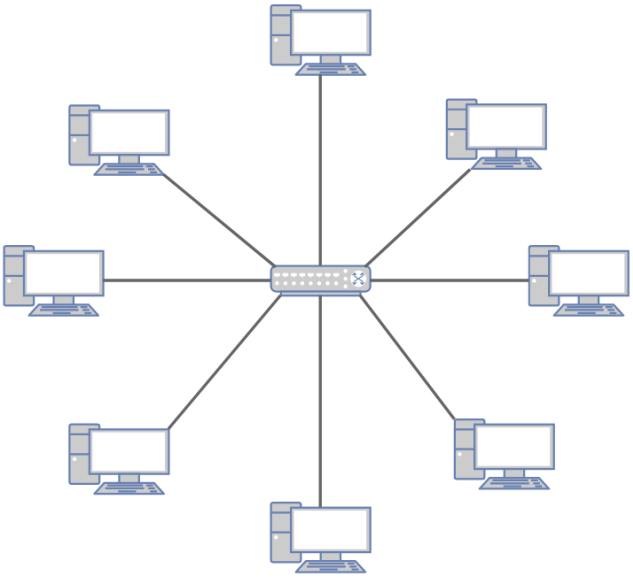

Рис. 2.3. Фізична топологія зірка

Проаналізувавши матеріал можна відзначити, що використання топології «зірка» є оптимальним. Водночас варто взяти до уваги переваги та недоліки такого виду фізичної реалізації та провести комплекс заходів для запобігання затримок пов'язаних з потенційними аварійними ситуаціями, наприклад, використання з'єднання активного мережевого обладнання, що відповідає за передачу даних між пристроями методом *stack*.

2.4. Технології побудови обчислювальних мереж

Мережева технологія – це погоджений набір стандартних протоколів та програмно-апаратних засобів, які їх реалізовують, достатній для побудови локальної обчислювальної мережі.

В локальних мережах, як правило, використовується середовище передачі даних, що розділяється, і основна роль відводиться протоколам фізичного і канального рівнів, оскільки ці рівні найбільшою мірою відображають специфіку локальних мереж. У сучасних локальних обчислювальних мережах широкого поширення набули такі технології або мережева архітектура, як: *Ethernet, Token-ring, Arcnet, FDDI*. Найбільшу популярність і поширеність здобув *Ethernet*, тому проаналізуємо цю технологію.

2.4.1. Технологія *Ethernet*

В даний час ця мережна технологія найпопулярніша у світі. Популярність забезпечується простими, надійними і недорогими технологіями. *Ethernet* було розроблено в 1973 році співробітником компанії *Xerox* Робертом Меткалфом. Згодом технологія *Ethernet* стала широко використовуватись у світі і була описана стандартом *IEEE 802.3*. Популярність можна обґрунтувати простими, надійними та недорогими технологіями. У класичній локальній мережі *Ethernet* застосовується стандартний коаксіальний кабель двох видів (товстий і тонкий). Проте найбільшого поширення набула версія *Ethernet*, яка використовує як середовище передачі виті пари, оскільки монтаж і обслуговування їх набагато простіший. У локальних мережах *Ethernet* мають реалізації топології типу «шина» і «зірка». Для мереж побудованих за топологією «шина» використовується технологія *CSMA/CD* для запобігання колізій. На таблиці 2.1 показані специфікації технології *Ethernet*. [9]

Таблиця 2.1.

Специфікації технології *Ethernet*

Бітова швидкість передачі даних	10 Мбіт/с
Максимальна довжина сегмента	500 м
Загальна максимальна довжина	2500 м
Максимальна кількість сегментів	5
Кількість вузлів в мережі	1024
Кількість вузлів в сегменті	100
Модифікації	10*Base*-5 – «товстий» коаксіальний кабель; 10*Base*-2 – «тонкий» коаксіальний кабель; 10*Base-T* – кабель неекранованої витої пари (*UTP*); 10*Base-F* – оптоволоконний кабель, існує два варіанта цієї специфікації: 10*Base-FL*, 10*Base-FB*.

2.4.2. Технологія *Fast Ethernet*

З плином часу технологія *Ethernet* розвивалася і в 1992 році такі виробники мережевого обладнання, як *3Com* та *SynOptics* об'єднали напрацювання різних компаній та створили нову технологію – *Fast Ethernet*, що являє собою покращену версію *Ethernet* зі збереженням окремих особливостей попередньої технології. В свою чергу нова версія зберегла:

- метод випадкового доступу *CSMA/CD*;
- формату кадру, що був специфікований в стандарті *IEEE 802.3*;
- топологію мережі «зірка»;
- традиційні середовища передачі – витої пари та оптоволоконного кабелю

Стандарт *Fast Ethernet* отримав значне збільшення робочої номінальної швидкості в 100 Мбіт/с, що в 10 разів швидше за початкову для *Ethernet* швидкість у 10 Мбіт/с. В технологію були імплементовані нові сучасні рішення та напрацювання, зокрема використання багатомодових волоконно-оптичних кабелів, витої пари п'ятої та третьої категорії, що використовують чотири та 2 пари відповідно. Технологія була описана в стандарті *IEEE 802.3u*.

Для нового стандарту були встановлені такі специфікації середовища передачі:

- *100Base-T4* – кабель неекранованої витої пари *UTP* 3-ої, 4-ої та 5-ої категорії з максимальною швидкістю передачі 75 Мбіт/с та максимальний віддаленням кінцевого пристрою від комутатора 100 м;
- *100Base-TX* – кабель неекранованої витої пари *UTP* 5-ої категорії з максимальною швидкістю передачі 125 Мбіт/с та максимальним віддаленням кінцевого пристрою від комутатора 100 м;

100Base-FX – кабель багатомодового оптоволоконного кабелю з максимальною швидкістю передачі 125 Мбіт/с та максимальним віддаленням кінцевого пристрою від комутатора 2000 м;

2.4.3. Технологія *Gigabit Ethernet*

Згодом у 1998 році *Інститут інженерів з електротехніки та електроніки (IEEE)* випустив першу редакцію нового стандарту *IEEE 802.3z*. Технологія *Gigabit Ethernet* є наступним логічним кроком розвитку *Fast Ethernet* та, як зазначено в стандарті *IEEE 802.3z*, передбачає використання 1000Base-SX для передачі сигналу багатомодовим волокном, 1000Base-LX - для одномодового волокна, і майже застарілих 1000Base-CX для передачі збалансованим мідним кабелем. На відміну від попереднього стандарту *Gigabit Ethernet* передбачає швидкість передачі в 1000 Мбіт/с, що більше за попередній стандарт в 10 разів. Подальшим розвиток цієї технології є 10 *Gigabit Ethernet* зі швидкістю передачі до 10 Гбіт/с та 100 *Gigabit Ethernet* з швидкістю від 40 до 100 Гбіт/с відповідно.

Для нового стандарту були встановлені такі специфікації середовища передачі:

- *1000BASE-SX* – багатомодовий оптоволоконний кабель з довжиною хвилі світлового сигналу 850 нм з максимальною швидкістю 1 Гбіт/с та функціональною довжиною кабеля від 220 до 550 м;
- *1000BASE-LX* – багатомодовий оптоволоконний кабель з довжиною хвилі світлового сигналу 1300 нм з максимальною швидкістю 1 Гбіт/с та функціональною довжиною кабеля від 550 до 5000 м
- *1000BASE-CX* – екранована вита пара *(STP)* категорії 5E або 6-ої з максимальною швидкістю 1,25 Гбіт/с та макимальною довжиною кабеля до 25 м

1000BASE-T - некранована вита пара *(UTP)* категорії 5E або 6-ої з максимальною швидкістю 1 Гбіт/с та макимальною довжиною кабеля до 100 м.

2.5. Апаратне забезпечення обчислювальної мережі

Апаратне забезпечення мереж складається з комплексу пристроїв, що виконують функцію транспортування інформації по системі. Об’єднання комп’ютерів у мережу здійснюється з використанням каналів передавання даних, а саме середовища

передавання даних та обладнання, що забезпечують передавання даних цими каналами. Канали передачі даних мають певні властивості і значення цих властивостей впливають на якість передачі даних через мережу. До цих властивостей відносять:

- швидкість передачі даних;
- вид середовища передачі даних;
- максимальна відстань передачі(без підсилення сигналу).

Для об'єднання пристроїв в мережі та передачі даних використовують низку пристроїв таких як: комутатори, концентратори, повторювачі, маршрутизатори та інші.

2.5.1. Мережеві комутатори

Мережевий комутатор або *switch* – це пристрій, що з'єднує вузли комп'ютерної мережі в межах однієї області. Комутатор дозволяє збільшити ефективність, продуктивність та захищеність за допомогою інтелектуальних елементів, що закладені в пристрій. На відміну від мережевого концентратора(хабу), комутатор передає дані лише тому вузлу до якого адресується інформація. Це дозволяє радикально зменшити навантаження на сегмент та пристрої, що належать до цього сегменту.

Як було сказано раніше, головний завданням комутатора є ефективна передача даних всередині вузла. При передачі інформації та отримані даних, комутатор зберігає в пам'яті відповідність *MAC*-адрес пристроїв до певного порту. У випадку надходження до комутатора фрейму з невідомою для нього адресою, пристрій відправить на всі невідомі підключення широкомовний запит. Після відповіді хоста з необхідною *MAC*-адресою, комутатор запише нове значення в таблицю комутації та передасть фрейми до заданого хосту. У випадку коли на порт комутатора надійде певний фрейм, який був призначений для вузла, *MAC*-адреса якого вже є в таблиці комутації, то цей фрейм буде розподілений тільки через цей порт. В результаті роботи пристрою формується спеціальна таблиця комутації. [15]

Комутатори поділяються на керовані та некеровані, а окремі модулі мають можливість працювати на третьому рівні моделі *OSI*. Такі моделі комутаторів носять

відповідну назву – *L3 Switch*, або комутатор третього рівня. Такі пристрої в свою чергу запозичують окремі функції третього рівня і можуть виконувати певні задачі маршрутизатора.

Керування та налаштування мережевим комутатором здійснюється за допомогою спеціального інтерфейсу командного рядка(*CLI*) через протокол простий протокол керування мережею *SNMP*, чи використовуючи веб-інтерфейс і протокол *HTTP*. Всі сучасні комутатори підтримують такі технології як: *VLAN*, *QoS*.

2.5.2. Маршрутизатори

Маршрутизатор або роутер(*router*) – це спеціальний пристрій, що керує процесом маршрутизації та використовується для поєднання двох або більше мереж. Тобто маршрутизатор на підставі даних про топологію мережі та набору правил приймає рішення про пересилання пакетів між різними сегментами мережі. На відміну від комутатора, роутер це пристрій, що працює на третьому рівні абстрактної мережевої моделі *OSI*. Найчастіше маршрутизатори використовуються для з'єднання локальної мережі організацій, підприємств чи домашніх мереж із зовнішньою обчислювальною мережею(*WAN*). [12]

Для надсилання пакетів в потрібному напрямку, роутер використовує таблицю маршрутизації, що являє собою електрону таблицю, яка описує відповідність між адресами призначення і інтерфейсами/сабінтерфейсами, через які слід відправити пакет даних до наступного маршрутизатора. Для визначення маршруту використовуються статичні маршрути, які адміністратор задає власноруч або використовуються протоколи динамічної маршрутизації – *RIP*, *OSPF*, *BGP*, *EIGRP*, тощо. Наприклад, у випадку використання протоколу маршрутизації *RIP*, основним показником вибору найефективнішого шляху є мінімальна кількість мережевих пристроїв між мережевими вузлами. Маршрутизатор може використовуватись, наприклад, в ЛКМ з технологією *Ethernet* для керування передачею даних за великої кількості мережевих сегментів або для з'єднання мережі з технологією *Ethernet* з мережою іншої технології, наприклад *Token Ring*. Пристрій також може здійснювати трансляцію адреси відправника й

одержувача(*NAT*), здійснювати фільтрацію транзитного потоку, шифрувати та дешифрувати дані.

Підтримка технології *Voice over IP* дозволяє використовувати маршрутизатор як шлюз *IP*-телефонії, тобто для передачі голосу по IP-мережі. Використання *IP*-телефонії дозволяє істотно знизити витрати на міжміську і міжнародну телефонію. За наявності спеціального вбудованого адаптера, маршрутизатор має порти для підключення звичайних аналогових телефонних апаратів або Міні-*АТС*. Для підключення до таких портів зазвичай використовується конектор стандарту *RJ-11*.

2.5.3. Мережеві адаптери

Мережевий адаптер – це периферійний пристрій, що дозволяє комп’ютерам взаємодіяти та передавати інформацію іншим пристроям в мережі. Адаптер відноситься до спеціальних периферійних плат комп’ютерів, за допомогою якого кінцевий пристрій може взаємодіяти з середовищем передачі даних, яке напряму чи за допомогою комунікаційного обладнання пов’язує його з іншими пристроями в мережі.

Функціонування мережевих адаптерів обумовлене використанням безпосередньо апаратною частиною, тобто платою та програмного забезпечення – драйвера. Для функціонування мережевого адаптера необхідне попереднє встановлення драйвера. Мережеві адаптери перетворюють паралельні коди, що використовуються всередині комп'ютера та представлені малопотужними сигналами, в послідовний потік потужних сигналів для передачі даних по зовнішній мережі.

За точки зору кабельної системи адаптери класифікуються на:

- мережеві карти для підключень через коаксіальний кабель;
- мережеві карти для підключення через кабель типу вита пара;
- мережеві карти з бездротовим інтерфейсом.

2.6. *MAC*-адреса

MAC-адреса – це унікальний ідентифікатор пристрою в мережі. Адреси в кожному з просторів теоретично мають бути глобально унікальними, тому на відміну від IP-адреси, яку налаштовує користувач власноруч, *MAC*-адреса визначається виробником пристрою.

Адреса складаються з 48 біт та у своїй структурі мають: індикатор маршруту (перший біт), спосіб призначення адреси (другий біт), унікальний ідентифікатор організації (три перших октета), та три останні октета за унікальність яких відповідає сам виробник. Більшість мережевих протоколів канального рівня (другий рівень моделі *OSI*) використовують *MAC*. Більшість мережевих протоколів використовують один з трьох варіантів *MAC*-адрес: *MAC*-48, *EUI*-48 і *EUI*-64. Найпоширенішими вважаються адреси *MAC*-48.

2.7. *IP*-адреса

IP-адреса – це унікальний ідентифікатор мережевого рівня, що використовується для адресації комп'ютерів та інших пристроїв у мережі, які побудовані з використанням стеку протоколів *TCP/IP*. Найбільш використовуваною версією протоколу є *IPv4*, у якій *IP*-адреса має довжину 4 байти або 32 біти. У *IPv6* використовується 128-бітна адреса. [15]

Адреси *IP* можуть бути статичними, тобто налаштовуватися власноруч, чи бути динамічними. Динамічні *IP*-адреси надається пристрою автоматично при підключенні пристрою до мережі і використовується протягом певного часу, зазначеного в налаштуваннях серверу *DHCP*. Динамічні адреси також можуть бути віртуальними і обслуговуватись протоколом *NAT*, що являє собою протокол перетворення мережевих адрес. За допомогою сервісу *NAT* маршрутизатор, сервер чи брандмауер може перетворювати внутрішню адресу на зовнішню провівши їх безпосередню відповідність. Протокол *NAT* є одним з найголовніших чинників роботи інтернету, оскільки діапазон *IPv4* адрес на даному етапі розвитку мереж і поширеності пристроїв не може забезпечити необхідну кількість адрес.

IP-адреса в своїй структурі містить дві складові: ідентифікатор мережі та хосту. Для логічного розбиття адреси на вищезазначені складові використовується маска підмережі або бітова маска. Маску підмережі можна визначити як кількість біт в адресі, які є номером мережі (кількість біт зі значенням "1"). Наприклад, "8-бітної маскою" називають маску, в якій 8 біт - одиниці, а решта 24 біта – нульові, тобто 255.0.0.0.

2.8. Віртуальна локальна мережа(*VLAN*)

Віртуальна локальна мережа або *VLAN* – це технологія створення віртуальних локальних мереж всередині однієї мережі. Дана функціональна можливість дозволяє логічно розділити мережу на окремі сегменти і за допомогою налаштувань контролювати доступ між цими сегментами. [13]

Зазвичай інженерами в сфері комп'ютерних мереж для однієї підмережі відводиться одна віртуальна мережа. Використання технології *VLAN* дозволяє в значній мірі полегшити адміністрування мережі та водночас підвищити загальний рівень безпеки.

До переваг використання технологій віртуальних локальних мереж можна віднести:

- логічне сегментування мережі на підрозділи, що особливо зручно при проектуванні мереж підприємств та компаній;
- ізоляція пристроїв в окремі групи для полегшення адміністрування;
- зменшення загальної кількості пристроїв в мережі, методом використання меншої кількості комутаторів;

забезпечення високого рівня безпеки та зменшення необхідності використання широкомовного трафіку.

2.9. Висновки до розділу

В розділі був проведений комплексний аналіз та дослідження основних принципів побудови локальних обчислювальних мереж в умовах підприємства. Були зазначені основні терміни та формулювання предметної області, досліджені концепції і технології побудови мереж, досліджені фізичні топології та проаналізоване апаратно-технічне забезпечення функціонування мережі, а також основні протоколи та функції. Проаналізований матеріал буде використаний для практичної реалізації проекту захищеної комп'ютерної мережі підприємства, і виступати в якості основи для реалізації основних тенденцій комплексних заходів із забезпечення безпеки інформаційної системи.

РОЗДІЛ 3
МОДЕЛЮВАННЯ ЗАХИЩЕНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

3.1. Проектування мережі департаменту

Для створення багатошарового захисту корпоративного середовища необхідне ретельне проектування та планування загальної архітектури мережі з врахуванням специфіки виділених для неї приміщень, Також важливим аспектом є правильний підбір апаратного та програмного забезпечення. На рисунку 3.1. зображена план-схема приміщень умовного департаменту на підприємстві з вказаними назвами пристроїв та їх *IP*-адресами.

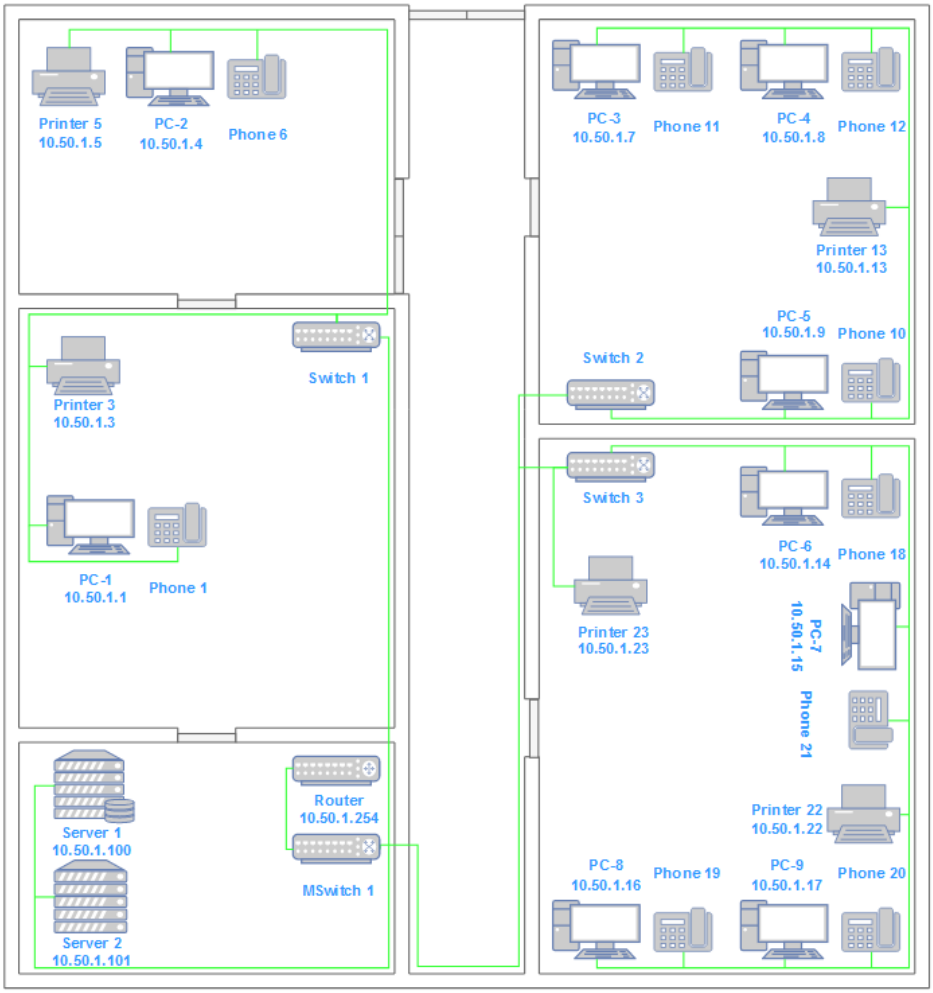

Рис. 3.1. – План-схема приміщень департаменту з обладнанням

Як видно з рисунку наведеного вище, відділ підприємства складається з двох робочих кімнат працівників, кабінету начальника, кабінету секретаря та окреме приміщення з серверами. Загалом відділ налічує 9 персональних комп'ютерів, 5 мережевих принтерів, 9 *IP* телефонів, 4 комутатори, 2 сервери відділу та маршрутизатор.

Представлена мережа побудована за топологією зірка, що є найпоширенішим рішенням для проектування подібних видів мереж. Вибір такої топології дозволяє раціонально розподілити ресурси та витрати на необхідне обладнання зберігаючи при цьому достатній рівень стійкості до аварійних ситуацій, а також рівномірний розподіл навантаження.

Підрозділ виконує робочі обов'язки використовуючи робочі станції, телефони, принтери та сервери для отримання та зберігання даних. Об'єднання різних кімнат та окремих пристроїв в мережі відбувається за допомогою комутаторів. Маршрутизація

до інших мереж та підмереж підприємства відбувається за допомогою маршрутизатора.

Для виконання робочих обов'язків деяких працівників може виникнути потреба використання ресурсів зовнішньої обчислювальної мережі або інтернет (*WAN*). При використанні ресурсів зовнішньої мережі необхідно забезпечити максимальний рівень захищеності внутрішньої мережі підприємства та її ресурсів. Реалізація такого підключення можлива з використанням демілітаризованої зони або просто *DMZ*, що являє собою сегмент мережі, що містить загальнодоступні сервіси та відокремлює їх від приватних. Зазвичай загальнодоступним сервісом виступає вебсервіс. Такий сервіс фізично розміщений у локальній мережі та повинен відповідати на будь-які запити із зовнішньої мережі, при цьому ізолюючи інші локальні ресурси (робочі станції, файлові сервери відділів і т.д.). Таке рішення надає додатковий рівень безпеки в локальній мережі, який дозволяє мінімізувати збитки в разі атаки на один із загальнодоступних сервісів. Для розділення сегментів та контроль трафіку між ними використовують міжмережевий екран, що здійснює контроль доступу з зовнішньої мережі в ДМЗ та навпаки, а також контроль доступу з внутрішньої мережі в зовнішню. Реалізація такого рішення представлена на рисунку 3.2.

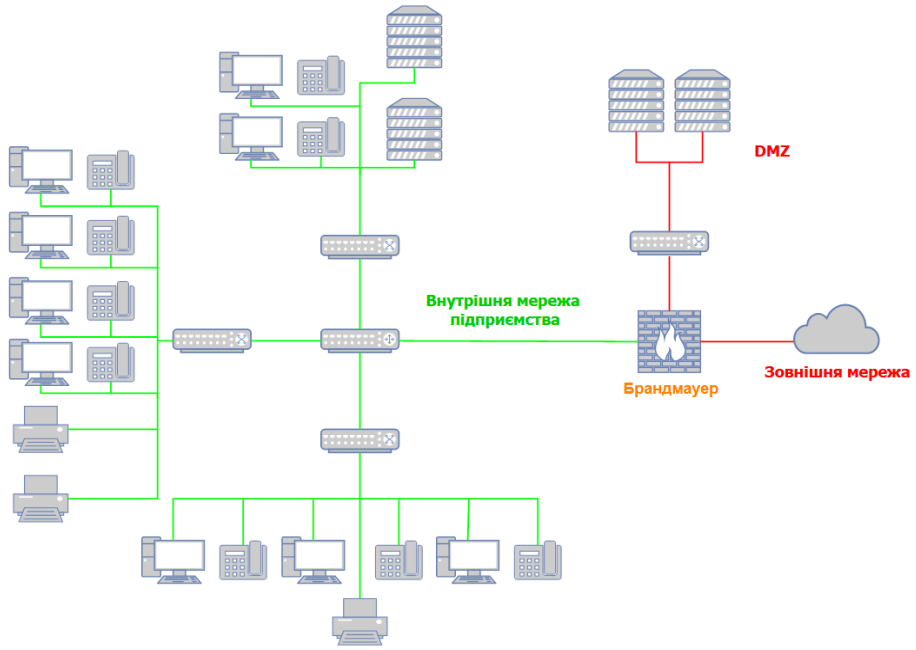

Рис. 3.2. План-схема *DMZ* сегменту та внутрішньої мережі департаменту підприємства

На план-схемі зображене підключення внутрішньої мережі підприємства до зовнішньої мережі інтернет та її з'єднання з сегментом *DMZ*. В якості брандмауера (*firewall*) часто використовують активне мережеве обладнання, наприклад, *Cisco ASA 5505,5506-X*.

3.2. Специфікація та вибір апаратного забезпечення

Для реалізації запропонованої системи використовується широкий спектр апаратного та програмного забезпечення. До активного мережевого обладнання відносяться комутатори, маршрутизатори, міжмережеві екрани та набір різних кінцевих пристроїв. Проведемо перелік необхідного активного мережевого обладнання для створення системи.

Cisco Catalyst 2960 – це лінійка стекових комутаторів фіксованої конфігурації, які призначаються для об'єднання групи пристроїв та подальшої передачі інформації. Вищезазначений пристрій ефективним та відносно недорогим способом вирішення широкого спектру задач. Технічні характеристики пристрою показані в таблиці 3.1.

Таблиця 3.1

Технічні характеристики комутатора *Cisco Catalyst 2960*

Характеристика	Опис характеристики
Загальні характеристики	
Тип	комутатор
Маршрутизація/тип комутації	L2 (другий рівень моделі OSI)
Кількість і тип портів Ethernet	24 x RJ45 10/100 Fast Ethernet 2 x SFP/1000BASE-T комбінований 1 x Консольний порт RJ45 Ethernet
Набір функцій програмного забезпечення Cisco IOS	LAN Base
Протокол віддаленого адміністрування	SNMP 3

Продовження таблиці 3.1

Комутаційна здатність	16 Гбіт/сек
Максимальна кількість активних VLAN	255
Комутаційна смуга пропускання	повнодуплексна ємність
Робоча напруга, струм	від 100 до 240 В змінного струму, 0.4 - 0.2 А
Пам’ять пристрою	
Flash-пам'ять	64 МБ
Динамічний ОЗП	128 МБ
Стандарти, що підтримуються	IEEE 802.1Q VLAN, IEEE 802.1s, IEEE 802.1w, IEEE 802.1X, IEEE 802.1ab (LLDP), IEEE 802.3ad, IEEE 802.3af; Повний дуплекс IEEE 802.3x на портах 10BASE-T, 100BASE-TX і 1000BASE-T, IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX, IEEE 802.3ab 1000BASE-T, IEEE 802.3z 1000BASE-X
Фізичні габарити	
Габарити	4.4 x 45 x 24.2 см
Вага	3.6 кг

Рис. 3.3. Зовнішній вигляд *Cisco Catalyst 2960*

Cisco Catalyst 3650-24 – серія комутаторів третього рівня від компанії Cisco. Є сучасним високотехнологічним пристроєм для офісів та підприємств. Специфікація представлена у таблиці 3.2.

Таблиця 3.2

Технічні характеристики комутатора *Cisco Catalyst 3650-24*

Характеристика	Опис характеристики
Загальні характеристики	
Тип	комутатор
Маршрутизація/тип комутації	L3 (третій рівень моделі OSI)
Кількість і тип портів Ethernet	24 x 10/100/1000 (POE+); 4 x 1G SFP1
Набір функцій програмного забезпечення Cisco IOS	LAN Base
Протокол віддаленого адміністрування	SNMP 3
Комутаційна здатність	160 Гбіт/сек
Максимальна кількість активних VLAN	4,094
Комутаційна смуга пропускання	повнодуплексна ємність
Робоча напруга, струм	від 100 до 240 В змінного струму, 0.4 - 0.2 А
Пам’ять пристрою	
Flash-пам'ять	2 ГБ
Динамічний ОЗП	4 ГБ
Стандарти, що підтримуються	IEEE 802.1D STP, IEEE 802.1p CoS Prioritization, IEEE 802.1Q VLAN, IEEE 802.1s, IEEE 802.1w, IEEE 802.1X, IEEE 802.1X-Rev, IEEE 802.11, IEEE 802.1ab (LLDP), IEEE 802.3ad, IEEE 802.3x повний дуплекс 10BASE-T, 100BASE-TX та 1000BASE-T, IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX, IEEE 802.3ab 1000BASE-T, IEEE 802.3z 1000BASE-X

Продовження таблиці 3.2

Фізичні габарити	
Габарити	44,5 x 44,5 x 4.4 см
Вага	17.49 кг

Рис. 3.4. – Зовнішній вигляд комутатора *Cisco Catalyst 3650-24*

Cisco 2811 – серія маршрутизаторів для підприємств та офісів. Є одним з найпоширеніших комутаторів від компанії *Cisco* та в повній мірі відповідає заявленим потребам. Специфікація та технічні характеристики показані в таблиці 3.3.

Таблиця 3.3

Технічні характеристики маршрутизатора *Cisco 2811*

Характеристика	Опис характеристики
Загальні характеристики	
Тип	маршрутизатор
Призначення роутера	серверний
Інтерфейси	WAN: 2 x 10/100/1000 RJ-45 1 x USB 2.0
Протокол віддаленого адміністрування	SNMP 3
Сукупна пропускна здатність	від 100 Мбіт/с до 300 Мбіт/с
Робоча напруга, струм	від 100 до 240 В змінного струму, 0.4 - 0.2 А
Пам’ять пристрою	
Flash-пам'ять	64 МБ
Динамічний ОЗП	256 МБ / 760 МБ максимум

Продовження таблиці 3.3

Фізичні габарити	
Габарити (висота х ширина х довжина)	4.5 х 43.8 х 41.7 см
Вага	6.4 кг

Рис. 3.5. Зовнішній вигляд *Cisco 2811*

Cisco ASA 5505 – багатофункціональні пристрої з лінійки мережевої безпеки, що представляють собою брандмауер, транслятор мережевих адрес (*NAT*), система запобігань вторгнення у системи (*IPS*). Пристрої також використовується для забезпечення роботу віртуальної приватної мережі (*VPN*). *ASA* – представляє собою уніфікований пристрій керування загрозами, який об'єднує комплекс функцій безпеки мережі в одному приладі. Нижче в таблиці 3.2.6 наведені технічні характеристики *Cisco ASA 5505*.

Таблиця 3.4

Технічні характеристики *Cisco ASA 5505*

Характеристика	Опис характеристики
Загальні характеристики	
Тип	багатофункціональний брандмауер
Інтерфейси	8xGE Base-T Gigabit Ethernet, 1xGE Base-T Gigabit Ethernet Management, 1 RJ-45 або Mini USB консольний порт
Протокол віддаленого адміністрування	SNMP 3
Пакетів в секунду (64 байти)	246,900

Максимальна кількість нових підключень за секунду	5000
Швидкість LAN портів	100 Мбіт/с
Система централізованого налаштування, збору логів, моніторингу	Multidevice Cisco Security Manager and Cisco FireSIGHT Management Center
Пам’ять пристрою	
Flash-пам'ять	4 ГБ
Твердотільний накопичувач	50 GB mSata
Фізичні габарити	
Габарити	4.369 x 19.992 x 23.44 cm
Вага	1.82 кг

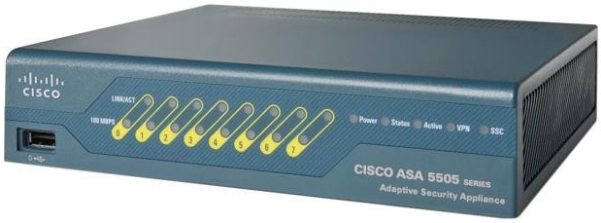

Рис. 3.6. Зовнішній вигляд пристрою *Cisco ASA 5505*

3.3. Визначення матеріальних витрат на виконання проекту

Головною метою проведення подібних видів робіт є здійснення економічних розрахунків, які спрямовані на визначення загальної економічної вартості розробки проекту та прийняття рішення про перспективність його подальшого розвитку.

Кількість та найменування необхідного активного мережевого обладнання продемонстровані в таблиці 3.5. Для об’єктивності розрахунку витрат на обладнання були взяті середні ціни ринку на задані товари. Слід зазначити, що розрахунки не включають персональні робочі станції, пристрої виводу інформації (принтери), телефони та робочі сервери, оскільки в залежності від компанії та конкретної галузі або задачі виробництва, технічні вимоги зазначених пристроїв можуть в значній мірі відрізнятися, тому розрахунки включають обладнання, що безпосередньо забезпечує

транспортування та захист інформації.

Таблиця 3.5

Зведені розрахунки матеріальних витрат

Назва пристрою	Одиниця виміру	Кількість	Ціна за одиницю, грн.	Загальна ціна, грн
Cisco Catalyst 2960	штуки	4	13110,00	52440,00
Cisco Catalyst 3650	штуки	1	55844,00	55844,00
Cisco 2811	штуки	1	37051,00	37051,00
Cisco ASA 5505	штуки	1	12321,00	12321,00
Кабель *UTP cat 5E*	метри	250	20,00	5000,00
Разом				162656,00

Отже, зведені витрати на матеріальні ресурси 162656,00грн.

В результаті розрахунків була отримана остаточна сума основних витрат виконання проекту. До витрат входять оплата самого обладнання, його транспортування, оплата роботи залучених до проекту працівників та витраченої електроенергії. Варто зазначити, що у загальну суму не входять програмні застосунки з ліцензіями, оскільки в залежності від масштабу виробництва, залучених до праці людей та робочих станцій, загальна вартість та різновид програмного забезпечення може змінюватись радикальним чином.

3.4. Налаштування багатошарового захисту мережі

Перед безпосередньою реалізацією проекту розробленої мережі необхідно впевнитися в коректності її роботи. Для створення та перевірки роботи системи та її окремих вузлів був використаний програмний застосунок *Cisco Packet Tracer* 8.1.1, що представляє собою симулятор створення та налаштування комп’ютерних мереж. Програма дозволяє максимально наближено симулювати роботу обчислювальної мережі.

Для початку створимо таблицю (табл. 3.6.) відповідності пристроїв до їх назв, *IP*-адрес та відношення до віртуальних локальних мереж (*VLAN*).

Таблиця 3.6

Детальний список кінцевих пристроїв в мережі

Назва пристрою	Тип пристрою	IP-адреса	VLAN	Порт комут.
PC-1	ПК	10.50.1.1/24	10	Fa 0/5(SW1)
PC-2	ПК	10.50.1.4/24	10	Fa 0/6 (SW1)
PC-3	ПК	10.50.1.30/24	10	Fa 0/2 (SW2)
PC-4	ПК	10.50.1.8/24	10	Fa 0/3(SW2)
PC-5	ПК	10.50.1.9/24	10	Fa 0/4(SW2)
PC-6	ПК	10.50.1.14/24	10	Fa 0/6(SW3)
PC-7	ПК	10.50.1.15/24	10	Fa 0/5(SW3)
PC-8	ПК	10.50.1.16/24	10	Fa 0/7(SW3)
PC-9	ПК	10.50.1.17/24	10	Fa 0/8(SW3)
Phone-1	IP-телефон	автоматично	20	Fa 0/7(SW1)
Phone-6	IP-телефон	автоматично	20	Fa 0/8(SW1)
Phone-10	IP-телефон	автоматично	20	Fa 0/7(SW2)
Phone-11	IP-телефон	автоматично	20	Fa 0/6(SW2)
Phone-12	IP-телефон	автоматично	20	Fa 0/5(SW2)
Phone-18	IP-телефон	автоматично	20	Fa 0/2(SW3)
Phone-19	IP-телефон	автоматично	20	Fa 0/3(SW3)
Phone-20	IP-телефон	автоматично	20	Fa 0/4(SW3)
Phone-21	IP-телефон	автоматично	20	Fa 0/1(SW3)
Printer-3	Принтер	10.50.1.3/24	10	Fa 0/4(SW1)
Printer-5	Принтер	10.50.1.5/24	10	Fa 0/3 (SW1)
Printer-13	Принтер	10.50.1.13/24	10	Fa 0/1(SW2)
Printer-22	Принтер	10.50.1.22/24	10	Fa 0/10(SW3)
Printer-23	Принтер	10.50.1.23/24	10	Fa 0/9(SW3)
Server-1	Сервер	10.50.1.100/24	10	Fa 0/2 (SW1)
Server-2	Сервер	10.50.1.101/24	10	Fa 0/1 (SW1)
Router	Маршрутиза-тор	10.50.1.254/24	-	Gi1/0/5(MSW1)
DMZ-1	Сервер	10.50.10.10/24	3	Fa 0/2(SW4)
DMZ-2	Сервер	10.50.10.11/24	3	Fa 0/1(SW4)

Отже створимо макет запропонованої мережі використовуючи план схему (рис.3.2.) та таблицю пристроїв (табл. 3.6.).

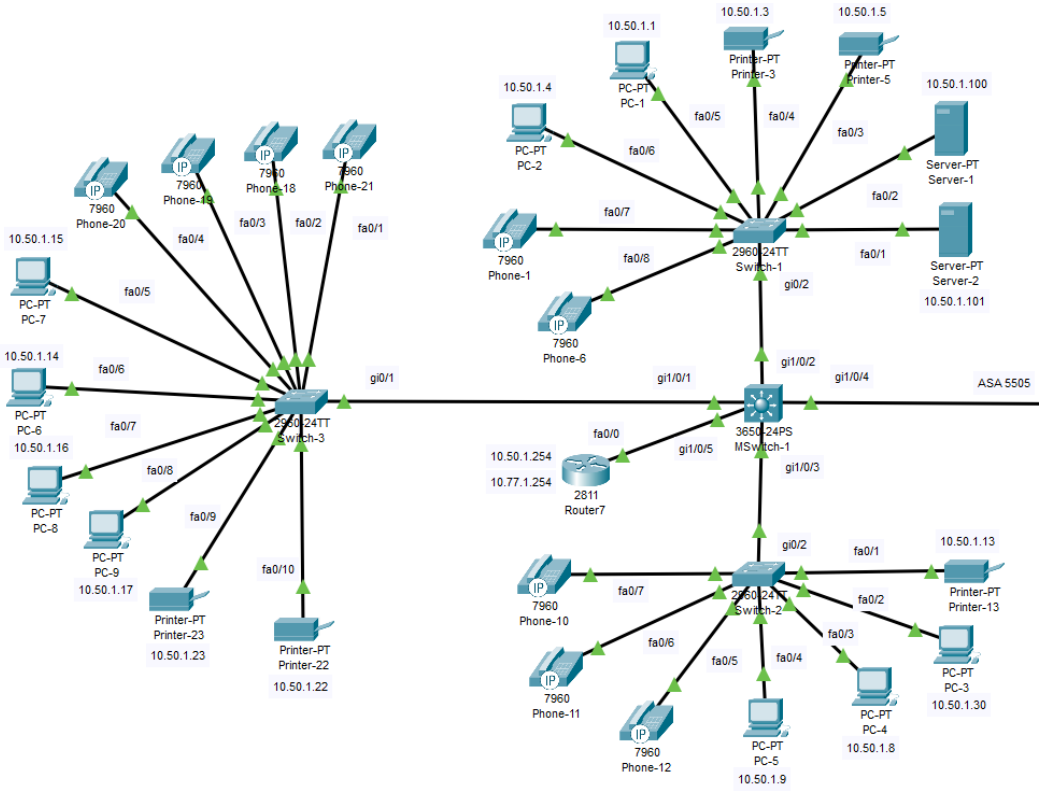

Рис. 3.7. – Внутрішній сегмент мережі

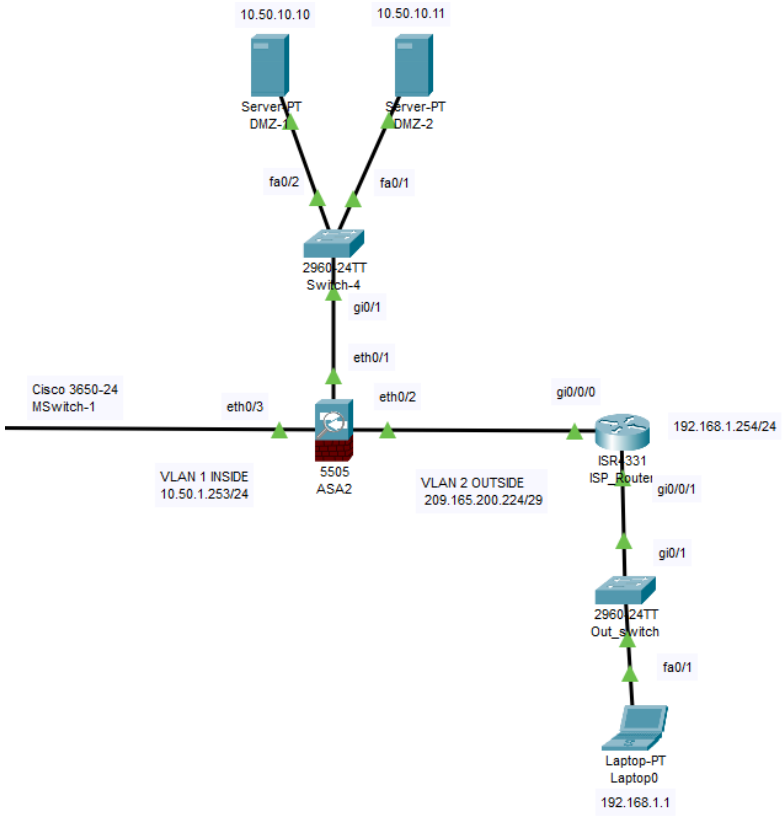

Рис. 3.8. – Зовнішній сегмент мережі

Комп’ютерна мережа представлена на рисунках 3.7. та 3.8. складається з 9 ПК, 9 телефонів, 5 принтерів, 4 серверів, 1 маршрутизатора, 5 комутаторів та 1 мережевого екрану.

В першу чергу необхідно налаштувати *IP*-адреси, маску та шлюз кінцевих пристроїв, а саме ПК, принтерів та серверів.

Для налаштування активного мережевого обладнання використовується спеціально розроблений інтерфейс командного рядка (*CLI*), що є текстовим інтерфейсом користувача, в якому інструкції вводяться за допомогою спеціальних команд із клавіатури.

На лістингу 3.1. представлені налаштування комутатора *Switch-3*.

Лістинг 3.1.

```
Switch(config)#service password-encryption
Switch(config)#vlan 10
Switch(config-vlan)#name data
Switch(config)#vlan 20
Switch(config-vlan)#name phone
Switch(config)#vlan 66
Switch(config-vlan)#name misc
Switch(config)#interface range fastEthernet 0/1-4
Switch(config-if-range)#switchport voice vlan 20
Switch(config-vlan)#exit
Switch(config)#interface range fastEthernet 0/5-10
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-vlan)#exit
Switch(config)#interface gigabitEthernet 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 10,20
Switch(config-if)#exit
Switch(config)#interface range fastEthernet 0/11-24
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 66
Switch(config-if-range)#shutdown
Switch(config-if)#exit
Switch(config)#interface gigabitEthernet 0/2
Switch(config-if)#shutdown
Switch(config)#interface range fastEthernet 0/1-10
Switch(config-if-range)#switchport mode access
```

Продовження лістингу 3.1

```
Switch(config-if-range)#switch port-security
Switch(config-if-range)#switch port-security maximum 1
Switch(config-if-range)#switch port-security violation restrict
Switch(config-if-range)#switch port-security mac-address sticky
Switch(config-if-range)#exit
Switch#copy running-config startup-config
```

Вищезазначеними командами на комутаторі створений *VLAN* 10 (*data*) та назначені до нього порти *FastEthernet* 0/5-10 та *VLAN* 20 (*phone*) з портами *FastEthernet* 0/1-4 в режимі voice відповідно. Порт *GigabitEthernet* 0/1 був сконфігурований як магістральний для передачі даних від комутатора *MSwitch*-1. На портах *FastEthernet* 0/1-10 був налаштований *port-security* таким чином, щоб зв'язок був можливий лише до санкціонованих пристроїв з незмінною *MAC*-адресою. Порти *FastEthernet* 0/11-24 та *GigabitEthernet* 0/2 були вимкнені в ручному режимі для безпеки та перенесені у *VLAN* 66 (*misc*). Конфігурація комутатора *Switch-3* продемонстрована на рисунку 3.8. Налаштування на комутаторах *Switch*-2,1 проводиться таким же чином.

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Gig0/1
10   data                              active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10
20   phone                             active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
66   misc                              active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24, Gig0/2
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Рис.3.8. – Конфігурація комутатора *Switch*-3

Далі необхідно провести налаштування комутатора *MSwitch*-1. Він виконує роль центрального компонента, що з'єднує інші активні мережеві пристрої, тому всі його порти будуть налаштовані у магістральному режимі. У лістингу 3.2. наведені команди налаштування комутатора *MSwitch*-1.

Лістинг 3.2.

```
Switch(config)#service password-encryption
Switch(config)#vlan 10
Switch(config-vlan)#name data
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name phone
Switch(config-vlan)#vlan 66
Switch(config-vlan)#name misc
Switch(config)#exit
Switch(config)#interface range gigabitEthernet 1/0/1-5
Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#switchport trunk allowed vlan 10,20
Switch(config-if)#exit
Switch(config)#interface range gigabitEthernet 1/0/6-24
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 66
Switch(config-if-range)#shutdown
Switch(config-if-range)#exit
Switch(config)#interface range gigabitEthernet 1/1/1-4
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 66
Switch(config-if-range)#shutdown
Switch(config-if-range)#exit
Switch(config)#interface range gigabitEthernet 1/0/1-24
Switch(config-if-range)#switchport port-security maximum 1
Switch(config-if-range)#switchport port-security mac-address sticky
Switch(config-if-range)#switchport port-security violation restrict
Switch(config-if-range)#exit
Switch#copy running-config startup-config
```

Після виконання заданих команд на комутаторі *MSwitch*-1 були створені *VLAN* аналогічні, як на комутаторах *Switch*-1,2,3 порти *GigabitEthernet* 1/0/1-5 були переведені в магістральний режим роботи для передачі інформації між собою. Була налаштована підсистема безпеки портів port-security та примусово виключені порти *GigabitEthernet* 1/0/5-24, а також *GigabitEthernet* 1/1/1-4. Конфігурація комутатора *MSwitch-1* продемонстрована на рисунку 3.9.

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Gig1/0/4, Gig1/0/5
10   data                              active
20   phone                             active
66   misc                              active    Gig1/0/6, Gig1/0/7, Gig1/0/8, Gig1/0/9
                                                 Gig1/0/10, Gig1/0/11, Gig1/0/12,
Gig1/0/13
                                                 Gig1/0/14, Gig1/0/15, Gig1/0/16,
Gig1/0/17
                                                 Gig1/0/18, Gig1/0/19, Gig1/0/20,
Gig1/0/21
                                                 Gig1/0/22, Gig1/0/23, Gig1/0/24, Gig1/1/1
                                                 Gig1/1/2, Gig1/1/3, Gig1/1/4
```

Рис. 3.9. – Конфігурація комутатора *MSwitch*-1

Використання маршрутизатора в корпоративній мережі обумовлене необхідністю здійснювати маршрутизацію пакетів і тим самим їх передачею в інші мережі на підприємстві. Також маршрутизатор використовується для створення пулу *IP*-адрес для функціонування телефонів та інших завдань в мережі.

Налаштування маршрутизатора також відбувається за допомогою *CLI*, як і у випадку з комутаторами. Нижче наведений лістинг 3.3. з командами для конфігурації роутера.

Лістинг 3.3.

```
Router(config)#service password-encryption
Router(config)#ip ips notify log
Router(config)#interface fastEthernet 0/0.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 10.50.1.254 255.255.255.0
Router(config-subif)#exit
Router(config)#interface fastEthernet 0/0.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 10.77.1.254 255.255.255.0
Router(config-subif)#exit
Router(config)#interface fastEthernet 0/0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#ip dhcp excluded-address 10.77.1.254
Router(config)#ip dhcp pool phone20
Router(dhcp-config)#network 10.77.1.254 255.255.255.0
Router(dhcp-config)#default-router 10.77.1.254
Router(dhcp-config)#option 150 ip 10.77.1.254
Router(dhcp-config)#exit
Router(config)#telephony-service
```

Продовження лістингу 3.3.

```
Router(config-telephony)#max-dn 9
Router(config-telephony)#max-ephones 9
Router(config-telephony)#ip source-address 10.77.1.1 port 2000
Router(config-telephony)#ephone-dn 1-9
Router(config-ephone-dn)#number 101-9
Router(config)#dial-peer voice 1 voip
Router(config-dial-peer)#destination-pattern 10
Router(config-dial-peer)#session target ipv4:10.77.1.254
```

Після налаштування на маршрутизаторі було створено два сегмента на інтерфейсі *FastEthernet* 0/1. Першу 10.77.1.254/16 для телефонії та 10.50.1.254/24 для інших кінцевих пристроїв внутрішньої мережі. Був включений монітор *IPS* для логування, пул *IP*-адрес для телефонів та налаштовані їх номера, а також встановлене максимальне значення телефонів в мережі – 9. На рисунку 3.10. показані налаштування маршрутизатора *Router*-1.

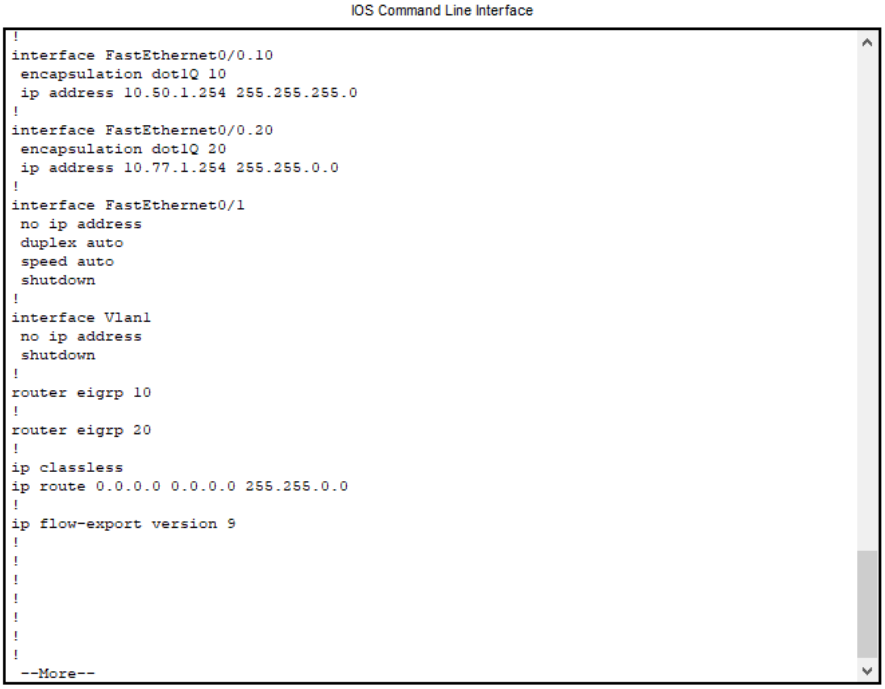

Рис. 3.10. – Конфігурація маршрутизатора

Останнім етапом конфігурації буде налаштування *Cisco ASA 5505*. Конфігурація полягає у тому, щоб логічно відокремити зовнішню мережу провайдера *ISP* (209.165.200.224/29), внутрішню мережу підприємства (10.50.1.0/16) та *DMZ*

(10.66.1.0). В якості представлення зовнішньої мережі виступає маршрутизатор провайдера (*ISP_Router*), комутатор та ноутбук. *Cisco ASA*, як і інші апаратні брандмауери, дозволяє провести широкий спектр налаштувань, а програмний компонент *Cisco Firesight* ще більше розширює можливості. На лістингу 3.4. наведені команди в оболонці *CLI* для його конфігурації.

Лістинг 3.4.

```
ciscoasa>enable
ciscoasa#configure terminal
ciscoasa(config)#hostname ASA
ASA(config)#domain-name department.com
ASA(config)#interface vlan 2
ASA(config-if)#nameif outside
ASA(config-if)#ip address 209.165.200.226 255.255.255.248
ASA(config-if)#security-level 0
ASA(config-if)#exit
ASA(config)#interface vlan 1
ASA(config-if)#nameif inside
ASA(config-if)#ip address 10.50.1.254 255.255.0.0
ASA(config-if)#security-level 100
ASA(config)#interface ethernet 0/3
ASA(config-if)#switchport access vlan 1
ASA(config-if)#exit
ASA(config)#interface ethernet 0/2
ASA(config-if)#switchport access vlan 2
ASA(config-if)#exit
ASA(config)#interface ethernet 0/3
ASA(config)#route outside 0.0.0.0 0.0.0.0 209.165.200.225
ASA(config-if)#exit
ASA(config)#object network inside-net
ASA(config-network-object)#subnet 10.50.1.0 255.255.255.0
ASA(config-network-object)#nat (inside,outside) dynamic interface
ASA(config-network-object)#exit
ASA(config)#class-map inspection_default
ASA(config-cmap)#match default-inspection-traffic
ASA(config-cmap)#end
ASA(config)#policy-map global_policy
ASA(config-pmap)#class inspection_default
ASA(config-pmap-c)#inspect icmp
ASA(config-pmap-c)#inspect dns
ASA(config-pmap-c)#inspect tftp
```

Продовження лістингу 3.4.

```
ASA(config-pmap-c)#inspect http
ASA(config-pmap-c)#exit
ASA(config)#service-policy global_policy global
ASA(config)#interface vlan 3
ASA(config-if)#ip address 10.50.10.0 255.255.255.0
ASA(config-if)#no forward interface vlan 1
ASA(config-if)#security-level 75
ASA(config-if)#nameif dmz
ASA(config-if)#exit
ASA(config)#interface ethernet 0/1
ASA(config-if)#switchport access vlan 3
ASA(config-network-object)#object network dmz
ASA(config-network-object)#host 10.50.10.0
ASA(config-network-object)#nat (dmz, outside) static 209.165.200.225
ASA(config-network-object)#exit
ASA(config)#access-list OUTSIDE-DMZ permit icmp any host 10.50.10.10
ASA(config)#access-list OUTSIDE-DMZ permit tcp any host 10.50.10.10 eq 80
ASA(config)#access-group OUTSIDE-DMZ in interface outside
```

Таким чином *ASA* була налаштована таким чином, щоб пропускати вихідний трафік з внутрішньої мережі до зовнішньої мережі використовуючи *NAT*, змінюючи внутрішню адресу на зовнішню, пропускати у сегмент *DMZ* пакети *ICMP* та *HTTP* для отримання доступу до веб-сервера підприємства (10.50.10.10), а також створена політика, що перевіряє пакети *ICMP*, *DNS*, *TFTP*, *HTTP*, що надходять до *ASA*. У свою чергу порти *Ethernet* 0/1,2,3 були перенесені у відповідні *VLAN* з назвами *dmz*, *outside*, *inside*.

Для перевірки роботи створеної мережі можна скористуватись командою ping для ПК, використати телефони та перейти до тестового веб-сайту підприємства з зовнішньої мережі. Відповідні дії продемонстровані на рисунках 3.11 – 14.

Рис. 3.11. – Перевірка зв’язку між телефонами

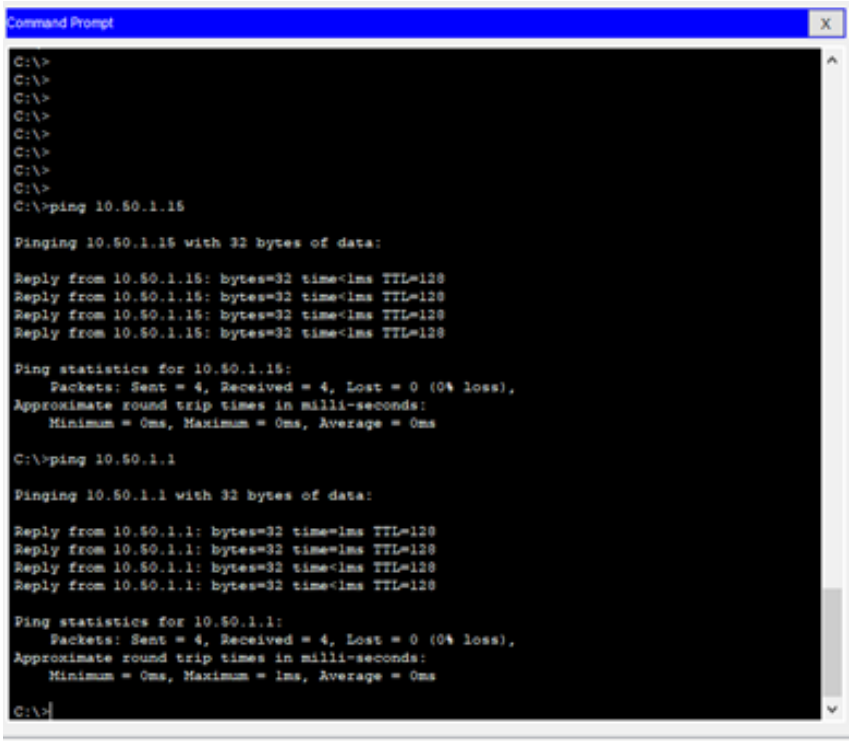

Рис. 3.12. – Перевірка зв’язку комп’ютерів в мережі

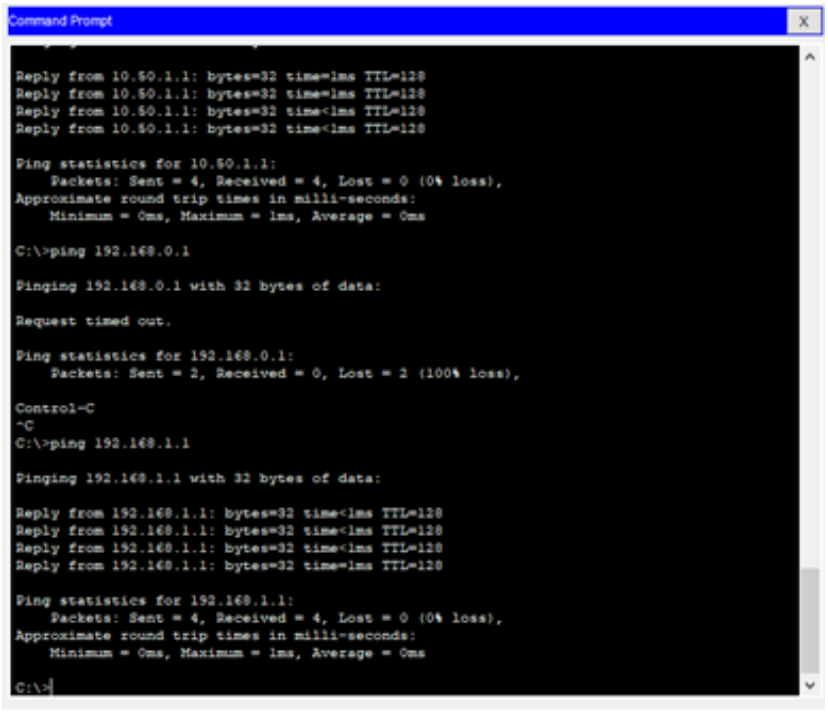

Рис. 3.13. – Перевірка зв’язку між ПК у внутрішній та зовнішній мережі

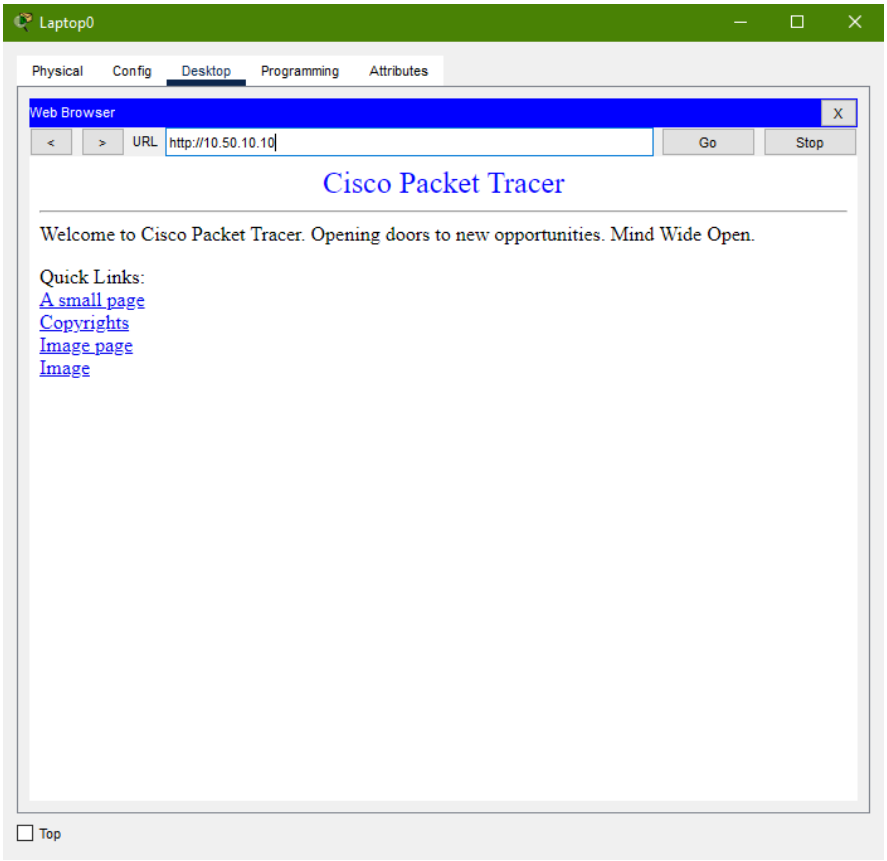

Рис. 3.14. – Використання веб-сайту підприємства з зовнішньої мережі (ноут-бука)

Таким чином була спроектована мережа підприємства, в якій працівники можуть обмінюватись інформацією, а також використовувати основні ресурси департаменту. При необхідності працівники компанії можуть використовувати ресурси зовнішньої мережі. За допомогою апаратного брандмауеру *Cisco ASA* можливо здійснювати гнучкі налаштування безпеки. Був створений окремий сегмент мережі *DMZ*, що дозволяє пристроям в зовнішній мережі використовувати окремі ресурси підприємства, наприклад веб-сайт підприємства. Загалом створена система представляє надійну основу для підтримання інформаційної безпеки на підприємстві, проте для повного захисту системи необхідне активне адміністрування та використання програмно-технічних засобів.

3.5. Програмно-технічні засоби методи захисту інформації

Використання програмних засобів захисту інформації є одним із найголовніших аспектів забезпечення безпеки інформаційного середовища. Серед основних завдань програмних застосунків виділяють ідентифікацію, автентифікацію та перевірку повноважень користувачів системи, захист від несанкціонованих змін, копіювання чи спотворення інформації, контроль пристроїв вводу/виводу, захист системи від шкідливого програмного забезпечення та вірусів, запобігання мережевих атак, виявлення аномалій та загальної профілактики.

Для створення надійного механізму захисту та протидії зловмисникам, використовують комплекс програмно-технічних засобів та відповідних заходів, що повинні у встановленому порядку бути занесені до політики інформаційної безпеки. Таким чином це дозволяє значно зменшити ризики проведення атак та отримання несанкціонованого доступу до системи.

Для забезпечення ІБ був використаний такий комплекс інформаційних засобів:

- *ESET Endpoint Security* – програма-антивірус для детектування всіх типів шкідливих програм за допомогою одної з найбільших баз сигнатур серед існуючих аналогів. Програма використовує технологію *ESET Live Grid*, що до-

зволяє забезпечити додатковий рівень захисту пристроїв в мережі за допомогою перевірки репутації додатків до їх безпосереднього запуску. Програма використовує вбудовану пісочницю на основі технологій машинного навчання, запобігає зараженню погрозами нульового дня. Функціонал застосунку також дозволяє використовувати контроль та логування пристроїв вводу/виводу Для адміністрування та налаштування системи використовується спеціальна консоль адміністратора. Для імплементації застосунку необхідний окремий сервер. Широкий функціонал застосунку та якісна підтримка дозволяє використовувати *ESET Endpoint Security* в якості системи контролю пристроїв вводу/виводу інформації, наприклад компакт-дисків, *USB*-накопичувачів, тощо;

- *Cisco Firesight* використовується в якості програмного брандмауера. Програма дозволяє автоматично агрегувати та співвідносити інформацію, створену *Cisco ASA* і тим самим забезпечує повну видимість активності у мережі: фізичних та віртуальних хостів, операційних системи, програм, служб, протоколів, користувачів, поведінку мережі, а також інформацію про мережеві атаки та шкідливе програмне забезпечення. Використання застосунку *Cisco Firesight* дозволяє значно розширити загальний функціонал апаратного брандмауеру *Cisco ASA*;
- *ESET Mail Security* – програма для захисту поштових серверів від усіх типів шкідливого програмного забезпечення та для фільтрації поштових повідомлень у режимі реального часу. Застосунок дозволяє фільтрувати вкладення за типом файлів та використовувати локальний карантин для керування заблокованими повідомленнями;
- *Splunk Enterprise* – програмний застосунок, що використовує технологію *SIEM*, тобто управління інформаційною безпекою та управління подіями безпеки. Програма забезпечує аналіз в реальному часі подій безпеки, отриманих від мережевих пристроїв і додатків. Дозволяє ефективно об’єднати та централізувати події (логи) вищезазначених систем та тим самим, створити

центр моніторингу подій ІБ. *Splunk* також використовується для журналювання даних і генерації звітів.

Варто зазначити, що використаний комплекс програмно-технічного забезпечення, необхідний набір ПЗ на робочих станціях, процедура отримання облікових записів, правила та обмеження використання окремих ресурсів повинні бути чітко описаний у політиці інформаційної безпеки підприємства.

3.6. Висновки до розділу

В даному розділі були реалізовані та опрацьовані наступні пункти:

- була створена план-схема приміщення департаменту підприємства з вказанням пристроїв та їх розташуванням, зазначені *IP*-адреси основних кінцевих пристроїв;
- розроблена специфікація обладнання, що використовується в локальній обчислювальній мережі з зазначенням основних характеристик;
- обрахована загальна сума витрат на обладнання;
- поетапно налаштовані кінцеві пристрої, створені конфігурації активного мережевого обладнання;
- обрані програмно-технічні засоби та обґрунтована їх необхідність для реалізації плану захисту мережі

Враховуючи вищезазначені пункти можна стверджувати, що етап планування та практичної реалізації були виконані успішно. Створена система була перевірена на правильність і коректність функціонування її компонентів.

ВИСНОВКИ

В результаті виконання дипломної роботи був створений проект багатошарової захищеної мережі підприємства, який включає основні сучасні підходи та тенденції для створення комплексної системи безпеки корпоративного середовища.

В першому розділі роботи були оглянуті загальні поняття та основні концепції безпеки інформаційних системи, проаналізовані принципи роботи сучасних програмних комплексів для запобігання вторгнень та попереджень мережевих атак, був оглянутий спектр існуючих мережевих атак та способи протидії загрозам. Також в ході роботи була проаналізована важливість політики інформаційної безпеки підприємства.

В другому розділі проводився огляд концепції комп'ютерних мереж, технологій, що використовуються, мережевого обладнання та окремих протоколів зі стеку *TCP/IP*. Були порівняні найпоширеніші топології мереж та принципи їх побудови.

Третій розділ є безпосередньою реалізацією проекту та використання аналітичного матеріалу, що був опрацьований раніше. Загалом була спроектована мережа умовного відділу підприємства, створені план-схеми приміщень, був проведений розрахунок вартості необхідного для виконання поставленого завдання обладнання із зазначенням технічних специфікацій та обґрунтування вибору. В результаті пристрої були підключені та налаштовані. У кінці був сформований список необхідного програмного забезпечення для адміністрування та забезпечення програмного захисту ресурсів мережі.

Розроблена інформаційна система може бути використана в якості універсальної основи забезпечення ІБ в локальній мережі. Налаштування дозволяють використовувати широкий комплекс програмно-технічних засобів, що можуть працювати безпосередньо з фізичними пристроями захисту(*Cisco ASA*), так і працювати окремо забезпечуючи інші потреби. Загалом розроблена система здатна забезпечувати достатній рівень захисту від більшості існуючих загроз, однак світ інформаційних техно-

логій безупинно розвивається і саме тому якісне адміністрування, своєчасна профілактика, діагностика та модернізація є основною необхідністю будь-якої інформаційної системи.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Смирнов И.Г. Структурированные кабельные системы - проектирование, монтаж и сертификация./ И.Г. Смирнов – СПб.: Экон-Информ, 2005.- 131 с.;
2. Хорошко В. Методы и средства защиты информации/ Хорошко В. А., Чекатков А. А. – К.: Издательство Юниор, 2003. – 504 с.;
3. Домарев В. В. Безопасность информационных технологий. Системный подход: - К.: ООО «ТИД ДС», 2004. – 992с.;
4. В. Г. Олифер. Компьютерные сети. Принципы, технологии, протоколы/ В. Г. Олифер, Н. А. Олифер. СПб.: Питер, 2001. – 672 с.;
5. Домарев В. В. Защита и безопасность компютерных ссистем/ В. В. Домарев. – К.: Издательство «Диа-Софт», 1999. – 480 с.;
6. Виткев О. Основы сетей Cisco, том 1. / Виткев О. М.: Издательский дом "Вильяме", 2005. – 231 с
7. ESET [Електронний ресурс] – Режим доступу: https://www.eset.com/ua/ (дата звернення 20.05.2022р.) – Назва з екрану;
8. Телекомунікаційні системи та мережі [Електронний ресурс] – Режим доступу: *https://www.znanius.com/3533.html* (дата звернення 22.05.2022р.) – Назва з екрану;
9. Комп'ютерні мережі [Електронний ресурс] – Режим доступу: https://sites.google.com/site/komputernimerezi440/4 (дата звернення 22.05.2022р.) - Назва з екрану;
10. Cisco Community Networking [Електронний ресурс] – Режим доступу: https://community.cisco.com/t5/networking/ct-p/4461-network-infrastructure (дата звернення 22.05.2022р.) - Назва з екрану;
11. ДСТУ 3396-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт. – К.: Держстандарт України, 1995. – 6 с.;
12. Маршрутизатор [Електронний ресурс] – Режим доступу: *https://westelecom.ua/ua/blog/222_cto-takoe-marsrutizator-i-kak-on-rabotaet.html* (дата звернення 22.05.2021р.) – Назва з екрану;

13. Cisco VLANs [Електронний ресурс] – Режим доступу: https://community.cisco.com/t5/networking-documents/vlans/ta-p/3114286 (дата звернення 23.05.2022р.) – Назва з екрану;
14. Using the Cisco IOS Command-Line Interface [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/configuration/15 (дата звернення 24.05.2022р.) – Назва з екрану;
15. IP Networking Basics [Електронний ресурс] – Режим доступу: https://www.cisco.com/en/US/docs/security/vpn5000/manager/reference/guide/appA.html (дата звернення 24.05.2022р.) – Назва з екрану.