Міністерство освіти і науки України

«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
завідувач кафедри кібербезпеки
та захисту інформації
_____ Н.В. Лукова-Чуйко
« » червня 2021р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

дипломної роботи
бакалавра
(назва освітнього рівня)

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітня програма Кібербезпека
(назва освітньої програми)

на тему: «Розробка захищеної розподіленої корпоративної мережі»

Виконавець: студентка IV курсу, групи КБ-41

_____ **Сарока Світлана Олександрівна**
(підпис) (прізвище ім'я по-батькові)

	Прізвище, ініціали	**Підпис**
Керівник	Зюбіна Р. В.	

Нормоконтроль	Даков С. Ю.	

Київ 2021

Міністерство освіти і науки України

«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувач кафедри кібербезпеки
та захисту інформації
_____ Н.В. Лукова-Чуйко
«10» жовтня 2020 р.

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студентці **КБ-41** **Сароці Світлані Олександрівні**
(група) (прізвище ім'я по-батькові)

Тема дипломної роботи Розробка захищеної розподіленої корпоративної мережі

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема дипломної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №2 від 08.10.2020 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Методи і технології розробки корпоративних мереж

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Необхідно ознайомитися з теорією розробки корпоративних мереж, їх типовими розгортаннями, вразливостями з боку безпеки даних.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Результат даної роботи можна застосувати на підприємстві і таким чином підвищити захищеність мережі і інформації в цілому.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання:12 жовтня 2020 року

Завдання видав _____ (підпис) Р. В. Зюбіна (ініціали, прізвище)

Завдання прийняла до виконання _____ (підпис) С. О. Сарока (ініціали, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	25.01.2021 – 30.01.2021	виконано
2	Аналіз літератури	01.02.2021 – 20.02.2021	виконано
3	Обґрунтування вибору рішення	12.02.2021 – 15.02.2021	виконано
4	Аналіз вимог до розробки корпоративної мережі	16.02.2021 – 20.02.2021	виконано
5	Розробка бізнес-моделі підприємства	22.02.2021 – 21.03.2021	виконано
6	Розробка фізичної моделі корпоративної мережі	22.03.2021 – 30.04.2021	виконано
7	Розробка технічної моделі корпоративної мережі	31.04.2021 – 10.05.2021	виконано
8	Оформлення пояснювальної записки	18.05.2021 – 08.06.2021	виконано
9	Підготовка до захисту дипломної роботи	09.05.2021 – 21.06.2021	виконано

Завдання видав _____ (підпис) Р. В. Зюбіна (ініціали, прізвище)

Завдання прийняв до виконання _____ (підпис) С. О. Сарока (ініціали, прізвище)

Термін подання дипломної роботи до ЕК 08 червня 2021 року

РЕФЕРАТ

Дипломна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатків, має 47 сторінок основного тексту, 2 таблиці та 3 рисунки. Список використаних джерел містить 28 найменування і займає 3 сторінки.

Метою даної роботи є проектування та побудова захищеної розподіленої корпоративної мережі.

У роботі проаналізована існуюча література з теорії розробки корпоративних мереж, виконаний аналіз документів, розроблено захищену розподілену корпоративну мережу.

Ключові слова: корпоративна мережа, VPN, міжмережевий екран, інформаційна безпека, проблеми безпеки, розробка моделі, система захисту ІБ, віртуальна приватна мережа, віддалений доступ, комп’ютерна система, автоматизована система, розподілена мережа, локальна КМ, місцева КМ, глобальна КМ.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

КМ	–	Корпоративна мережа
КС	–	Комп’ютерна система
LAN	–	Локальна комп’ютерна мережа
MAN	–	Місцева комп’ютерна мережа
WAN	–	Глобальна комп’ютерна мережа
VPN	–	Віртуальна приватна мережа
МЕ	–	Міжмережевий екран
АС	–	Автоматизована система
ІБ	–	Інформаційна безпека
СЗІБ	–	Система захисту інформаційної безпеки
СКД	–	Система контролю доступу
IDS	–	Система виявлення вторгнень
SSO	–	Технологія єдиного входу
PKI	–	Інфраструктура відкритих ключів

ЗМІСТ

ВСТУП

Актуальність даної роботи обумовлена тим, що основою інфраструктури сучасних підприємств являються корпоративні мережі, основним завданням яких є запобігання викраденню, викривленню та знищенню конфіденційної інформації.

В наш час велику популярність набули глобальні мережі особливо Internet. І в зв'язку з цим виникли проблеми із захистом інформації. Питання захисту інформації стало невід'ємною частиною будь-якої системи яка працює з комерційною інформацією. При використанні Internet в комерційних межах а також для з'єднання частин компаній і організацій виникають проблеми захищеності інформації яка проходить через мережу і обмеження доступу зовнішніх користувачів до внутрішніх мереж. Захист інформації стоїть на першому місці по актуальності і поставлених задач..

Тому метою роботи є проектування та побудова захищеної розподіленої корпоративної мережі.

Для досягнення поставленої мети необхідно вирішити такі завдання:

- Проаналізувати існуючі методи побудови корпоративних мереж
- Визначити найоптимальніше рішення для побудови корпоративної мережі
- Розробити модель захищеної розподіленої мережі
- Спроектувати та реалізувати корпоративну мережу

*Об'єктом дослідженн*я в даній роботі є процес побудови захищеної розподіленої корпоративної мережі.

Предметом дослідження в даній роботі є методи і засоби захисту корпоративної мережі.

РОЗДІЛ 1
АНАЛІЗ ОСНОВНИХ ТЕХНОЛОГІЙ СТРУКТУРИ КОРПОРАТИВНОЇ МЕРЕЖІ ТА ПИТАННЯ БЕЗПЕКИ

1.1 Загальне поняття мережі та корпоративної мережі

Мережі часто поділяють на три основні категорії: глобальні мережі (WAN), міські мережі (MAN) та локальні мережі (LAN) [1]. Глобальні мережі дозволяють взаємодіяти з абонентами на великих відстанях. Ці мережі працюють на низьких швидкостях і можуть спричинити значні затримки у розповсюдженні інформації. Протяжність глобальних мереж може становити тисячі кілометрів. Зазвичай, вони інтегровані в національні мережі.

Міські мережі (MAN) дозволяють взаємодіяти на менших формах місцевості та працювати на середніх та великих відстанях. Вони не так уповільнюють передачу даних, як глобальні, але все одно не можуть забезпечити взаємодії на великій відстані. Протяжність міських мереж коливається від десятків до сотень кілометрів.

Локальні мережі (LAN) забезпечують найвищу швидкість обміну інформацією між комп’ютерами. Стандартна локальна мережа розміщується в одній будівлі. Протяжність локальних мереж становить близько одного кілометра. Їх головна мета - об’єднати клієнтів для спільної роботи. Такі мережі організовані всередині будинку, поверху чи кімнати.

Методи передачі даних широко варіюються між локальними та глобальними мережами. WAN базуються на зв’язку - між абонентами встановлюється зв'язок перед передачею даних. Локальні мережі використовують методи, які не вимагають попередньої установки з'єднання - пакет даних надсилається без визначення готовності одержувача до обміну.

Окрім різниці в швидкості передачі даних, між сегментами цих мереж є й інші відмінності. У локальних мережах кожен комп'ютер має мережевий адаптер, який підключає його до середовища передачі. Міські мережі мають активні комутуючі

пристрої, а WAN зазвичай складаються з груп потужних маршрутизаторів пакетів, з'єднаних каналами зв'язку. Крім того, мережі можуть бути приватними або загальнодоступними.

Корпоративна мережа - сукупність взаємопов'язаних мереж, служб передачі даних та телеслужб, призначених для забезпечення єдиного захищеного мережевого простору, обмеженого корпоративним колом користувачів.

Ключовими особливостями корпоративних мереж є [2]:

- Використання того ж інструментарію під час роботи із загальнодоступною мережею передачі даних.

- Інформація може бути доступна лише обмеженій групі клієнтів у внутрішній мережі організації. Внутрішня мережа являє собою локальну мережу, відокремлену від глобальних мереж брандмауерами (МЕ).

- Обіг трьох типів інформації: офіційна (розповсюдження якої офіційно дозволено на рівні організації), проектна або організаційна (призначена для використання певною групою працівників, як правило, під захистом) та неофіційна (особиста папка або каталог на сервері, призначений для зберігання статей, нотаток та ідей).

- Наявність централізованої системи управління корпоративною мережею.

Система управління продуктивністю корпоративної мережі. В залежності від набору послуг, які реалізовані в корпоративній мережі, вони повинні використовувати свої інструменти управління мережею, включаючи інструменти маршруту та зміни; засоби адміністрування, реалізовані для ефективного використання мережевих ресурсів. За можливістю управління елементами корпоративної мережі модна виділити:

- функціональні елементи, якими можна управляти в рамках корпорації (власні кошти або додаткові активи, що вводяться в корпоративну мережу);

- функціональні елементи, якими не можна управляти (особливо маршрутизатори та комутатори), які належать до підмереж загального призначення, що використовуються організацією.

Система управління безпекою функціонування корпоративної мережі. Корпоративна мережа повинна містити в собі усі необхідні мережеві служби безпеки.

Система забезпечення надійності корпоративної мережі. Повинні бути передбачені методи, що забезпечують працездатність усієї мережі або фрагментів у разі виходу з ладу її елементів.

Система діагностики та контролю. У межах корпоративної мережі слід передбачати засоби для моніторингу роботи окремих функціональних елементів, системи збору інформації про розлади та збої. Для корпоративної мережі повинні бути розроблені засоби для діагностики, які будуть реалізовані в процесі функціонування мережі, а також профілактично.

Експлуатаційна система. Окрім перерахованих функціональних елементів, КМ повинні містити в собі план (гіпотезу) процесу розвитку, яка визначається функціями, які закладаються у неї на рівні протоколів.

Вимоги до адміністрування КМ [2].

Система управління корпоративною мережею повинна базуватися на таких принципах [3]:

- поєднання адміністрування окремих функціональних підсистем;

- централізоване / розподілене адміністрування, яке передбачає, що основні функції адміністрування повинні вирішуватися у центрі;

- функції автоматизованої системи управління повинні бути реалізовані в системі управління, для підвищення ефективності реагування системи управління на критичні події система повинна впроваджувати автоматизовану обробку певних значущих впливів;

- система безпеки має містити в собі адаптивне управління безпекою, яке змінюється відповідно до подій;

- для підвищення ефективності та надійності системи управління необхідно передбачити систему експертів, тобто систему «рекомендацій» для поліпшення контролюючого впливу на різні події.

1.2 Проблеми безпеки сучасних корпоративних мереж

Нові інформаційні технології активно застосовуються у всіх галузях економіки. З появою локальних та глобальних мереж передачі даних користувачі комп'ютерів знайшли нові можливості для швидкого надання інформації. Донедавна такі мережі створювались лише для конкретних і вузьких цілей (академічні мережі, мережі військових кафедр тощо), а розвиток інтернету та подібних систем призвів до появи глобальних мереж передачі даних, що використовуються майже всіма в межах повсякденного життя.

Оскільки розвиток та складність засобів автоматизованої обробки інформації, методів та форм збільшується залежність суспільства від стандартів безпеки інформаційних технологій, які вони використовують.

Доцільність та важливість проблем забезпечення ІБ виникають наступним чином [4]:

- сучасні рівні і темпи розвитку ІБ значно нижче рівнів і темпів розвитку інформаційних технологій;
- високі темпи зростання парку персональних комп'ютерів, що використовується у багатьох сферах людської діяльності;
- швидке розширення спектру користувачів за рахунок прямого доступу до комп'ютерних пристроїв та наборів даних;
- значне збільшення обсягу даних, що збираються, зберігаються та обробляються комп'ютерами та іншими пристроями автоматизації;
- підвищена вразливість програмного забезпечення та мережевих платформ;
- швидкий розвиток глобальної мережі інтернет практично запобігає порушенням безпеки систем обробки інформації у всьому світі;
- сучасні методи збору, обробки та розповсюдження інформації збільшили ризик втрати, викривлення та розкриття даних, що надсилаються або належать кінцевим споживачам.

Загроза безпеці означає потенційний ризик (потенційний або фактичний) будь-якої частини (дії чи бездіяльності), орієнтованої на об'єкт, що охороняється

(джерела інформації), який завдає шкоди власнику або фізичній особі - використання, який піддається ризику спотворення, розголошення або втрати інформації. Майбутня загроза називається атакою.

Наступних цілей можна досягти, реалізуючи загрозу безпеці наступним чином [3]:

- порушенням конфіденційності інформації (інформація, яка зберігається та обробляється в КМ, може бути надзвичайно корисною для її власника, вживання іншими обличчями може серйозно зашкодити інтересам власника);

- порушення цілісності інформації (втрата цілісності інформації (повна або часткова, компрометація, дезінформація) - майже ризик до її розголошення, цінна інформація може бути втрачена внаслідок її несанкціонованого вилучення або зміни;

- відмова у наданні інформації (порушення доступності) не означає підтвердження того, що одна зі сторін взаємодії передає або отримує повідомлення.

Корпоративна інформаційна система (мережа) - інформаційна система, де учасниками може бути обмежена кількість людей, перевірена її власником або за згодою учасників цієї інформаційної системи (за законом про електронні цифрові підписи).

Корпоративні мережі (КМ) - це розподілені комп'ютерні системи, що автоматизують обробку інформації [4]. В основі таких комп'ютерних систем лежить перш за все проблема інформаційної безпеки.

Розглянемо поточну проблему ІБ в організації.

Дослідницька фірма Gartner Group виділяє 4 рівні безпеки компанії з точки зору інформаційної безпеки (ІБ) [5]:

- рівень 0: ніхто не бере участь в ІБ компанії, керівництво компанії не усвідомлює важливості проблем інтелектуальної власності; повна відсутність фінансування; ІБ реалізується за допомогою стандартних операційних систем, баз даних та програм (захист паролем, обмеження доступу до ресурсів та послуг). Найпоширеніший приклад - компанія з невеликою кількістю співробітників, яка,

займається купівлею / продажем товарів. Адміністратор мережі, який часто є студентом, відповідає за всі технічні питання. Тут головне, щоб все працювало.

- рівень 1: Керівництво вважає ІБ суто «технічною» проблемою, не існує єдиної програми (концепції, політики) для поліпшення системи забезпечення ІБ (СЗІБ); фінансування здійснюється в межах загального бюджету; ІБ реалізується за допомогою резервного копіювання нульового рівня, антивірусних інструментів, брандмауерів, пристроїв VPN (традиційні засоби безпеки).

- рівні 2 і 3: керівництво розглядає ряд організаційних та технічних заходів управління, є розуміння важливості інтелектуальної власності для виробничих процесів, програма розвитку СЗІБ узгоджена з регуляторами; фінансування здійснюється в межах встановленого бюджету; ІБ реалізується з використанням вдосконалених засобів автентифікації, інструментів моніторингу електронної пошти та веб-вмісту, IDS (система виявлення вторгнень), інструментів аналізу безпеки, SSO (одноразові інструменти автентифікації), PKI (інфраструктура відкритих ключів) та організаційні заходи (зовнішній аудит, аналіз ризиків, політика інформаційної безпеки).

- рівень 3 дещо відрізняється від рівня : ІБ є частиною корпоративної культури, яка покладається на CISA (головний директор з підтримки ІБ); фінансування здійснюється в рамках конкретного бюджету, який, за даними аналітичної фірми Datamonitor, не перевищує 5% бюджету; ІБ реалізується за допомогою системи управління другого рівня + системи управління ІБ, CSIRT (група реагування на інциденти), SLA (угода про рівень обслуговування).

Як результат, можна побачити, що серйозний підхід до забезпечення ІБ компанії з’являється тільки на 2ому та 3ому рівнях. Такий підхід можна назвати комплексним. Він базується на складному рішенні комплексу різних задач в межах однієї програми.

На даний час цей підхід є важливим для створення безпечного середовища обробки інформації в корпоративних системах, що поєднують різні заходи управління загрозами. До них належать правові, моральні, етичні, організаційні, програмні та технічні методи захисту інформації Уніфікований підхід дозволив

інтегрувати низку автономних систем шляхом їх інтеграції в уніфіковані системи безпеки.

Аналізуючи вище написане, можна зробити висновок, що шляхи вирішення проблем безпеки тісно пов’язані з рівнем науково-технічного розвитку, особливо з рівнем технологічного забезпечення. І типовою схемою розвитку сучасних технологій є процес повної інтеграції. Ця тенденція охоплює мікроелектроніку та комунікаційні технології, сигнали та канали, системи та мережі. Прикладами є дуже великі інтегральні схеми, інтегровані мережі передачі даних, багатофункціональні засоби зв'язку тощо. Подальший розвиток єдиного підходу або його базового формату - це уніфікований підхід, заснований на інтеграції різних підсистем безпеки, підсистем зв'язку в єдину систему із загальним обладнанням, каналами зв'язку, програмним забезпеченням та базами даних. Уніфікований підхід спрямований на досягнення спільної безпеки. Основне поняття інтегральної безпеки полягає у тому, що треба забезпечити такий стан умов функціонування безпеки, в якому він надійно захищений від усіх видів загроз, які можуть виникнути під час поточного виробничого процесу. Концепція інтегральної безпеки бачить обов’язкову безперервність процесу безпеки як у часі, так і в просторі (протягом повного технологічного циклу діяльності) з обов’язковим врахуванням усіх можливих видів загроз (дозвіл на необмежений доступ, знищення інформації, тероризм, пожежа, стихійні лиха тощо).)

У будь-якому форматі, що використовує комплексний або уніфікований підхід, він завжди фокусується на ряді приватних проблем, вирішених у тісному зв'язку із використанням загальних технічних засобів, каналів зв'язку, програмного забезпечення тощо. . Наприклад, з точки зору інформаційної безпеки, найбільш очевидними є дії, що обмежують доступ до інформації, технічно та криптографічно приватну інформацію, обмежують рівень паразитного випромінювання технічних пристроїв, безпеки та попередження. Однак рішення потрібні і для інших, менш важливих завдань. Наприклад, керівники підприємств, члени сім'ї або ключові працівники не повинні виключати існування компанії. Цього можуть зменшити стихійні лиха, аварії, тероризм тощо. Отже, лише інтегровані системи безпеки, які

не здатні на такі загрози безпеці і забезпечують необхідний захист на постійній основі, як у часі, так і в просторі, можуть обробляти, транслювати та зберігати інформацію в процесі підготовки, що забезпечує повну безпеку даних.

Заходи щодо захисту даних

Ключові способи забезпечення ІБ [6]:

- юридичні (правові);
- морально-етичні;
- організаційні (адміністративні);
- технічні;
- програмні.

Правовий захист регулюється законодавством штату, що регулює використання, обробку та розповсюдження інформації з обмеженим доступом та встановлення відповідальності за порушення законодавства. Звичайно, більшість не займаються незаконною діяльністю не тому, що це технічно складно, а тому, що їх критикує та карає суспільство.

Морально-етичні практики включають поведінку, яка традиційно еволюціонувала або розвивалася з розширенням мережі та інформаційних технологій. Ці правила, як правило, не є обов'язковими до виконання, як законодавчі заходи, але їх недотримання зазвичай призводить до втрати довіри та репутації. Ці правила можуть бути створені за допомогою низки норм і правил.

Організаційні (адміністративні) заходи безпеки - це організаційні, технічні та організаційно-правові заходи, що реалізуються шляхом створення та обробки телекомунікаційного обладнання для забезпечення захисту даних. Організаційні стандарти охоплюють усі конструктивні елементи обладнання на всіх етапах їх життєвого циклу.

Організаційні заходи включають [7]:

- обмеження доступу до приміщень, де обробляється конфіденційна інформація;

- допуск до вирішення комп'ютерних завдань, пов'язаних з обробкою конфіденційних даних уповноважених працівників, що пояснює порядок виконання завдань на комп'ютері;

- зберігання магнітних носіїв у закритих жорстких шафах;

- призначення одного або кількох комп’ютерів для обробки цінної інформації та робота лише за цими комп’ютерами;

- налаштування екрану, клавіатури та принтеру таким чином, щоб до них не було доступу стороннім особам з метою перегляду конфіденційних даних;

- заборона дискусій щодо безпосереднього змісту конфіденційної інформації для тих, хто бере участь у їх процесі.

▪ Організаційно-технічні стандарти включають:

- запобігання внутрішньому доступу до комп’ютера, встановлюючи механічний замок;

- видалення всієї інформації з жорсткого диску комп'ютера, коли він надсилається на ремонт за допомогою інструменту низькорівневого форматування;

- організація комп'ютерного живлення від окремого джерела живлення або від загальної (побутової) мережі електроживлення через постійну напругу (мережу) або генератора двигуна;

- встановлення екранів, системних блоків, клавіатур та принтерів на відстані не менше ніж 2,5-3,0 метра від освітлення, кондиціонування, зв'язку (телефонів), металевих труб, телевізійного та радіообладнання, а також інших комп'ютерів, які не використовуються для обробки конфіденційної інформації;

- відключення власного комп’ютера від локальної мережі або мережі віддаленого доступу під час обробки конфіденційної інформації, якщо тільки дані не передаються через мережу;

- під час обробки цінної інформації на комп’ютері рекомендується вмикати пристрої, що генерують додатковий фоновий звук (літаки, вентилятори), а також обробляти іншу інформацію на сусідніх комп’ютерах, ці пристрої повинні встановлюватися на відстані не менше 2,5-3,0 метра;

- знищення інформації відразу після її використання.

Технічні засоби, що використовуються у вигляді механічних, електричних, електромеханічних та електронних пристроїв, призначені для запобігання входу та виходу захисного пристрою, який може там знаходитися. Повний спектр технік поділяється на апаратні та фізичні вироби. Апаратне забезпечення означає пристрої, які вбудовані безпосередньо в телекомунікаційне обладнання, або пристрої, які підключаються до такого обладнання через стандартний інтерфейс. Наприклад, система безпеки робочої станції Secret Net надає додаткову апаратну підтримку для ідентифікації користувачів за допомогою унікального електронного ключа.

Фізичні засоби використовуються у вигляді автоматизованих інструментів та систем. Наприклад, дверні замки, де встановлені побутові прилади, віконні решітки, електромеханічне обладнання для захисту від крадіжки.

До компонентів, що складають новітні оборонні основи ряду оборонних продуктів, належать [8]:

- система механічного захисту;

- фактична фізична перешкода, що характеризується тривалістю захисту та спрацювання датчика тривоги;

- система сповіщень: збільшення ймовірності виявлення злочинців через інформаційну систему вимагає збільшення кількості помилкових спрацьовувань, тому розробка системи сповіщень є вирішальною для пошуку розумного компромісу щодо цих сигналів; подальший розвиток систем сигналізації повинен, перш за все, збільшити ймовірність виявлення та зменшити інтенсивності помилкових спрацювань, використовуючи кілька систем попередження з різними принципами роботи в одному місці;

- системи ідентифікації: однією з умов надійної роботи є аналіз вхідних повідомлень управління для визначення правильного типу. Найпоширенішим методом є телевізійні системи дистанційного моніторингу. Вся територія під контролем сигналізації поділена на секції, де встановлена камера, коли активовані датчики тривоги, зображення, яке передане телевізійною камерою, відображається на екрані монітора в центральній колонці. Справжні причини функціонування системи доведено в умовах високої ефективності змінної роботи. Телевізійні

системи також можуть використовуватися для контролю за діяльністю персоналу у закладах.

- захисні системи - це, як правило, освітлювальні та звукові системи, що використовуються для запобігання вторгнення на територію, яка охороняється;

- ключовий поштовий та охоронний персонал: робота кожного технічного центру завжди знаходиться під керівництвом та контролем ключових служб безпеки, централізовані системи охоронних систем підпорядковуються певним вимогам.

На даний час найдосконалішими системами безпеки є системи контролю доступу (СКД), які забезпечують безпеку персоналу та відвідувачів, зберігають цінність матеріалів та інформації та контролюють ситуацію.

Механічні замки все ще є більш прийнятними для малого бізнесу, незважаючи на появу останнього СКД [10]. Існує безліч замків з високим рівнем захисту як зсередини, так і зовні, які можна використовувати для встановлення в приміщеннях, які потребують особливого захисту. Виробники продовжують розглядати механічні замки з високим захистом як гнучкий, ефективний та недорогий спосіб задовольнити потреби у захисті будівель та підвищити продуктивність. Тому наявність механічного ключа є найпростішою ідентифікаційною особливістю в контролі доступу.

Друга група методів ідентифікації - це свідоцтво із зображенням власника та печаткою. Персоналу будуть вручені вірчі грамоти, а відвідувачі будуть нагороджені - жетонами компанії. Ідентифікаційні картки та жетони можна використовувати разом із засобами управління доступом до картки, перетворюючи їх на допуски. Для підвищення безпеки зображення можна покращити за допомогою зчитувача та набору персональних кодів.

Вважається, що картки жетонів слід використовувати для в'їзду в райони, контрольовані великими компаніями [9].

Існує широкий спектр електронних СКД, серед яких більшу частину місця займає апаратура з використанням мікропроцесорів і комп’ютерів. Однією з переваг цього виду захисту є можливість аналізу ситуації та ведення обліку.

Електронна система контролю доступу включає системи з цифровою клавіатурою (клавішею), електронними картками та клавішами. Клавіатура була додана разом із електричним замком до більших систем безпеки із системою зчитування карток.

У системах контролю доступу до карток ключем є картка з унікальним кодом, яка виконує функцію посвідчення особи працівника.

Програмне забезпечення спеціально розроблене для виконання функцій захисту інформації.

Програмне забезпечення було основою безпеки на ранніх стадіях розвитку технологій комунікаційної безпеки в телекомунікаційних каналах. Програмне забезпечення вважалося основним засобом захисту. Спочатку методи захисту програм, як правило, вбудовувались у системи управління комп'ютером або системи управління базами даних. Практика показала, що надійність цих захисних пристроїв недостатня. Захист паролем був дуже слабким зв'язком. Як наслідок, засоби безпеки стали більш досконалими в майбутньому із введенням інших заходів безпеки.

До цього класу засобів захисту належать: антивірус, криптографічні інструменти, системи контролю доступу, брандмауери, системи виявлення вторгнень тощо.

Основні принципи забезпечення ІБ

Побудова системи безпеки повинна базуватися на таких основних принципах [11]:

- системний підхід;
- комплексні рішення;
- розумна достатність засобів захисту;
- розумна надмірність засобів захисту;
- гнучкість управління та застосування;
- відкритість алгоритмів та методів захисту;
- простота застосування захисту, засобів і методів;
- уніфікація засобів захисту.

Систематичний підхід

Захист інформації повинен враховувати взаємопов’язані та змінні елементи, умови та особливості часу, необхідного для виявлення та вирішення проблем ІБ.

Створюючи систему безпеки, необхідно враховувати слабкі місця та вразливості системи обробки інформації, а також характер можливих елементів порушень та атак на систему з боку зловмисників, методи несанкціонованого доступу до інформації.

Оборонну систему слід будувати з урахуванням не тільки добре відомих каналів управління, а й потенціалу нових і відносно нових способів реалізації загроз безпеці.

Систематичний підхід також визначає діапазон гарантій, які будуть запроваджені. Існують такі типи систем:

Просторова системність Може використовуватися як зв'язка питань для безпосереднього захисту інформації.

Тимчасова систематизація (принцип безперервності оборонної системи) [11]:

- захист даних - це не одноразовий захист, а постійний процес, що означає, що на всіх рівнях циклу вживаються відповідні кроки. Розробка оборонної системи повинна починатися з моменту, коли ви проектуєте оборонну систему, і повинна змінюватися та вдосконалюватися протягом усієї роботи системи;

- більшості інструментів безпеки потрібна підтримка (адміністрування) для виконання своїх завдань, включаючи призначення та зміну паролів, призначення секретних ключів, несанкціонований доступ до доступу тощо.

Організаційна системність. Означає організаційну єдність усієї роботи з ЗІ та управління задля їх здійснення. Систематична систематизація означає створення цілісної державної системи організацій з професійною спрямованістю на ЗІ.

Складність заходів та методів захисту

Експерти інформаційних систем мають широкий спектр заходів, методів та засобів захисту. Уніфіковане використання або інтеграція передбачає узгоджене використання різних заходів безпеки для забезпечення інформаційної безпеки. Цей принцип враховує весь спектр потенційних ризиків.

Принцип розумної достатності

Неможливо створити абсолютно неминучу систему захисту. Отже, коли ви розробляєте систему безпеки, має сенс поговорити про відповідний рівень. У той же час слід розуміти, що високоефективна система захисту є дорогою і може суттєво знизити захищену продуктивність та створити великі незручності для користувача. Важливо правильно вибрати рівень захисту, де враховуються витрати, ризик крадіжки та потенційний рівень шкоди.

Принцип розумної надмірності

Унікальність функціонування системи захисту полягає в тому, що рівень захисту постійно знижується внаслідок роботи системи. Це пояснюється тим, що кожен напад на систему, як успішний, так і невдалий, інформує зловмисника. Збір інформації призводить до успішної атаки. Це суперечить принципу розумної достатності. Виходом тут є компроміс - на етапі розвитку системи захисту її потрібно вбудувати деяку надмірність, що подовжить її життєвий цикл.

Принцип гнучкості управління та застосування (принцип адаптивності)

Система захисту, як правило, розвивається в ситуаціях крайньої невизначеності. Оскільки вбудовані заходи захисту можуть забезпечити захист на відповідному рівні. Тому слід застосовувати принципи регуляторної гнучкості, дозволяючи встановлювати пристрої під час роботи системи. Отже, введення будь-якого нового вузла у фізичну мережу або зміна існуючих умов не повинно знижувати рівень безпеки, що забезпечується фізичною мережею в цілому.

Принцип відкритості алгоритмів та методів захисту

Принцип відкритості алгоритмів і методів захисту не повинен забезпечувати захист виключно через шкоду конфіденційності, структурній безпеці та експлуатаційним алгоритмам своїх підсистем. Знання алгоритмів оборонної системи не повинно давати можливості подолати її. Простий принцип захисту означає, що захисні пристрої повинні бути інтуїтивно зрозумілими та простими у використанні. Він повинен мати інтуїтивно зрозумілий інтерфейс та автоматизовані налаштування. Система безпеки повинна сповільнювати діяльність користувача, виходячи з цього вона повинна працювати у "фоновому режимі".

Принцип інтеграції сучасних методів

Сучасні оборонні системи характеризуються високим ступенем складності, що вимагає високого рівня трудових ресурсів.

Для спрощення управління системами безпеки рекомендується інтегрувати їх, принаймні внутрішньо.

Структура управління мережевою безпекою. Основні вимоги

Система захисту інформації повинна мати багаторівневу структуру та такі етапи [11]:

- рівень автоматизованого захисту робочого місця;
- рівень захисту локальних мереж та інформаційних серверів;
- рівень захисту корпоративної АС.

На автоматизованому рівні захисту робочого місця слід ідентифікувати та перевірити користувача операційної системи. Режим контролю доступу: дозволяє елементи теми відповідно до матриці доступу, продуктивності реєстрації та відображення всіх функцій теми доступу в таблицях.

Рівень захисту локальних мереж та серверів вимагає [12]:

- ідентифікацію та перевірку доступу користувачів до системи, її компонентів;
- захист даних для автентифікації;
- автентифікацію при доступі до серверів;
- передачу засвідчених даних з однієї частини в іншу.

Рівень захисту корпоративної АС повинен гарантувати [12]:

- цілісність передачі інформації від джерела до одержувача;
- безвідмовність у наданні послуг;
- захист від несанкціонованого розголошення інформації.

1.3 Сучасні технології захисту корпоративних мереж

МЕ називається локальним або активним циркулюючим програмним забезпеченням (апаратним забезпеченням), яке контролює інформацію, яка надходить в автоматизовану систему та / або автоматично виходить із системи - мобільна.

За визначенням, МЕ служить контрольно-пропускним пунктом на межі двох мереж. У більшості випадків це межа між внутрішньою мережею організації та зовнішньою мережею, як правило, Інтернетом. Однак у загальному випадку МЕ можна використовувати для визначення підмереж у корпоративній мережі організації.

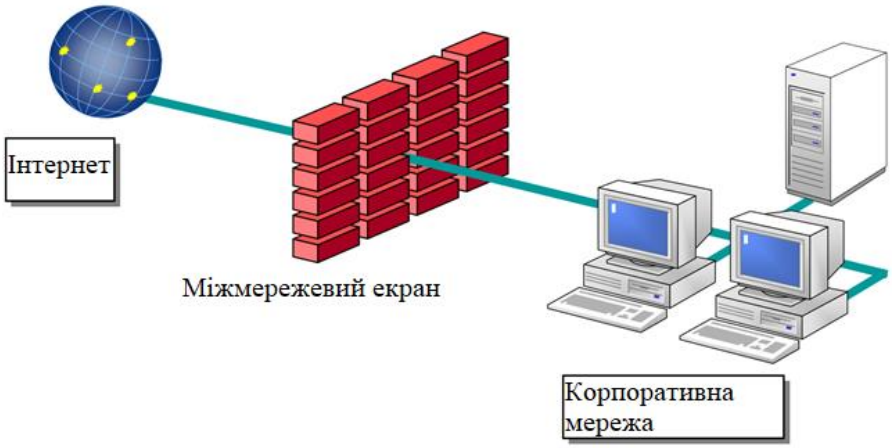

Рисунок. 1. Типове розміщення МЕ у корпоративній мережі

Функціями МЕ, як контрольного пункту, є:

- Повний контроль трафіку до внутрішньої фізичної мережі
- Повний контроль трафіку з внутрішньої фізичної мережі

Контроль інформаційних потоків, включаючи фільтрування та перетворення відповідно до набору правил [13]. Оскільки сьогоднішня фільтрація IU може виконуватися на різних етапах еталонної моделі взаємодії відкритих систем (EMVOS, OSI), IE належним чином представлений у вигляді систем фільтрації. Кожен фільтр на основі аналізу даних, що проходять через нього, вирішує - пройти далі, перекинути його через екран, заблокувати або увімкнути.

Рисунок. 2. Схема фільтрації МЕ

Основна роль МЕ - фіксувати обмін інформацією. Протоколювання дозволяє адміністратору виявляти підозрілі дії, помилки конфігурації IU та вирішувати змінити правила МЕ.

Системи виявлення нападів

На додаток до звичайного захисту, без якого нормальне функціонування АС неймовірне (наприклад, IU, резервні системи та антивірусні засоби), слід використовувати SOA (IDS, системи виявлення або виявлення атак), які є основними засобами для боротися з мережевими атаками.

В даний час SOA починає все частіше використовуватися в практиках корпоративної безпеки мережі. Однак існує низка проблем, які неминучі для організацій при впровадженні системи виявлення атак. Ці проблеми значно посилюють, а іноді перешкоджають впровадженню IDS. Ось деякі з них [14]:

- висока вартість комерційного SOA;

- низька ефективність сьогоднішнього SOA, характеризується великою кількістю неправильних предметів і збій (помилково позитивний та хибно помилковий)

- вимоги до ресурсів і часом незадовільні Продуктивність SOA в мережах зі швидкістю 100 Мбіт / с;

- ігнорування небезпеки мережевих атак;

- відсутність аналізу та управління ризиками в організації, що дозволяє провести відповідну оцінку рівня ризику та обґрунтувати витрати на порушення нормативних норм;

- Висококваліфіковані експерти з виявлення нападів, необхідні для впровадження та застосування SOA.

Типова архітектура системи виявлення атак зазвичай складається з наступних компонентів [15]:

- Датчик (метод збору інформації);
- Аналізатор (інструмент аналізу інформації);
- Інструменти реагування;
- Інструменти управління.

Звичайно, всі ці частини можуть працювати на одному комп'ютері і навіть у межах однієї програми, але вони, як правило, розподіляються географічно та функціонально. Компоненти SOA, такі як аналізатори та елементи керування, небезпечні для розміщення ME у зовнішній мережі, оскільки, якщо вони скомпрометовані, зловмисник може отримати доступ до інформації про структуру внутрішньої мережі, яка порушена. Захист шляхом аналізу правил за допомогою SOA

Концепція побудови безпечних VPN

Концепція побудови безпечних VPN базується на дуже простій ідеї: якщо глобальна мережа має два вузли, які хочуть обмінюватися інформацією, то для забезпечення конфіденційності та цілісності інформації через відкриті мережі необхідно між ними побудувати значний тунель . надзвичайно складно для всіх активних та пасивних глядачів на відкритому повітрі [15]. Термін "віртуальний" означає, що зв'язок між двома мережевими вузлами не є постійним (жорстким) і існує лише тоді, коли трафік проходить через мережу.

Вигоди для компанії від створення таких значних тунелів - це, перш за все, значна економія.

Висновки за розділом 1

1) Локальні мережі (LAN) забезпечують найвищу швидкість обміну інформацією між комп'ютерами. Стандартна локальна мережа розміщується в одній

будівлі. Протяжність локальних мереж становить близько одного кілометра. Їх головна мета - об’єднати клієнтів для спільної роботи.

2) Корпоративна інформаційна система (мережа) - інформаційна система, де учасниками може бути обмежена кількість людей, перевірена її власником або за згодою учасників цієї інформаційної системи (за законом про електронні цифрові підписи).

3) Шляхи вирішення проблем безпеки тісно пов’язані з рівнем науково-технічного розвитку, особливо з рівнем технологічного забезпечення. І типовою схемою розвитку сучасних технологій є процес повної інтеграції. Ця тенденція охоплює мікроелектроніку та комунікаційні технології, сигнали та канали, системи та мережі. Прикладами є дуже великі інтегральні схеми, інтегровані мережі передачі даних, багатофункціональні засоби зв'язку тощо. Подальший розвиток єдиного підходу або його базового формату - це уніфікований підхід, заснований на інтеграції різних підсистем безпеки, підсистем зв'язку в єдину систему із загальним обладнанням, каналами зв'язку, програмним забезпеченням та базами даних.

4) Система захисту, як правило, розвивається в ситуаціях крайньої невизначеності. Оскільки вбудовані заходи захисту можуть забезпечити захист на відповідному рівні. Тому слід застосовувати принципи регуляторної гнучкості, дозволяючи встановлювати пристрої під час роботи системи. Отже, введення будь-якого нового вузла у фізичну мережу або зміна існуючих умов не повинно знижувати рівень безпеки, що забезпечується фізичною мережею в цілому.

РОЗДІЛ 2
ТЕХНОЛОГІЇ, ЩО ЗАСТОСОВУЮТЬСЯ ДЛЯ ПОБУДОВИ КОРПОРАТИВНОЇ ЗАХИЩЕНОЇ МЕРЕЖІ

2.1 Категорії мереж

Мережі часто поділяють на три основні категорії: широкосмугові мережі (WAN), мережі мегаполісів (MAN) та локальні мережі (LAN) [16]. У нашій країні локальні мережі набагато частіше, ніж міські чи глобальні. Традиційним скороченням для локальних мереж є локальна мережа (локальна мережа). Глобальні мережі дозволяють взаємодіяти з абонентами на великі відстані. Ці мережі працюють на дуже низьких швидкостях і можуть спричинити значні затримки у розповсюдженні інформації. Протяжність глобальних мереж може становити тисячі кілометрів. Як такі, вони інтегровані в національні мережі.

Міські мережі забезпечують взаємодію менших форм рельєфу та працюють на середніх та великих відстанях. Вони уповільнюють передачу даних менше загальних даних, але не можуть забезпечити взаємодії на великі відстані. Протяжність міських мереж коливається від десятків до сотень кілометрів.

Локальні мережі забезпечують найшвидшу швидкість обміну інформацією між комп’ютерами. Стандартна локальна мережа розміщується в одній будівлі. Протяжність локальних мереж становить близько одного кілометра. Їх головна мета - об’єднати клієнтів для спільної роботи. Такі мережі організовані всередині будинку, поверху чи кімнати.

Методи передачі даних широко варіюються в локальних та глобальних мережах. VAN базуються на посиланнях - між абонентами встановлюється зв'язок перед передачею даних. Локальні мережі використовують методи, які не вимагають попередньої установки з'єднання - пакет даних надсилається без визначення готовності одержувача до обміну.

Таблиця 2.1. Технології та мережі

Технологія	Масштаб мережі
X.25	LAN
Ethernet	LAN
Frame Relay	MAN
FDDI	MAN
DQOB	MAN
SMDS	MAN
ATM	WAN
B-ISDN	WAN

Окрім відмінностей у швидкості передачі даних, існують і інші відмінності між цими категоріями мереж. У локальних мережах кожен комп'ютер має мережевий адаптер, який підключає його до знімних носіїв. Міські мережі мають активні машини під ключ, і VAN, як правило, складаються з груп потужних пакувальників, з'єднаних каналами зв'язку. Крім того, мережі можуть бути приватними або загальнодоступними.

Основною функцією корпоративної мережі є забезпечення передачі інформації між різними програмами, що використовуються в організації. Програмне забезпечення - це програмне забезпечення, яке безпосередньо потрібно користувачеві, наприклад, бази даних, електронна пошта тощо [17]. Корпоративна мережа дозволяє взаємодіяти з програмами, які часто розташовані в географічно різноманітних районах, і дозволяє отримати до них доступ віддаленими користувачами. На рис. 1.1 показано загальну функціональну схему мережі.

Успішна діяльність багатьох організацій та компаній сьогодні залежить від способу спілкування. Інтернет та мультимедіа почали відігравати важливу роль у діловому житті. Тільки сучасне програмне та апаратне забезпечення дозволяють успішно використовувати сучасні інформаційні технології. Важливо зробити

правильний стратегічний вибір для розвитку мережі вашої компанії. Для цього потрібно мати усі знання про сучасні мережеві технології, знати їх можливості та вміти оцінювати витрати. Що стосується стратегії розвитку, технологія банкомату є однією з найбільш перспективних. Це, безумовно, зможе задовольнити потреби більшості користувачів у майбутньому. Оскільки банкомат не стоїть на місці, а постійно змінюється, межі цього майбутнього рухаються все далі і далі. Тільки багатий потенціал цієї технології дозволяє в повній мірі скористатися наявною мережевою інфраструктурою. У цьому випадку термін інфраструктура означає внутрішні канали зв'язку, велику кількість локальних мереж та мережевого обладнання.

Можливості сучасних корпоративних мереж

Вибір концепції побудови конкретної корпоративної мережі визначається цілою низкою чинників: затребувані інформаційні послуги, обсяги переданого трафіку, існуюча інфраструктура і т. д. Але існують і загальні вимоги до корпоративних мереж. Мережі підприємств повинні бути побудовані на основі перевірених технологій, що володіють такими якостями, як масштабованість, гнучкість, мультисервісність, і найголовніше - надійність.

Мережа сучасного підприємства, як правило, повинна підтримувати ряд найбільш затребуваних для бізнесу додатків і керованих сервісів. В першу чергу це [18]:

- можливість високошвидкісного доступу до мережі Інтернет.
- створення віртуальних приватних мереж (VPN).
- передача голосу поверх IP.
- проведення відеоконференцій.
- захист інформації та зберігання даних.

2.2. Віртуальна приватна мережа VPN

У зв'язку з широким розповсюдженням internet, intranet, extranet при розробці та застосуванні розподілених інформаційних мереж і систем одним з найактуальніших завдань є вирішення проблем інформаційної безпеки [4].

Захищеною віртуальною мережею VPN називають об'єднання локальних мереж і окремих комп'ютерів через відкриту зовнішню середу передачі інформації в єдину віртуальну корпоративну мережу, що забезпечує безпеку циркулюючих даних.

VPN легко масштабується і є оптимальним варіантом для підприємств, що володіють певною кількістю відділень, а також для фірм, чиї співробітники часто бувають у відрядженнях або працюють з дому. Підключення нового офісу або нового віддаленого співробітника здійснюється без додаткових витрат на комунікації.

При підключенні корпоративної локальної мережі до відкритої мережі виникають загрози безпеки двох основних типів [19]:

- несанкціонований доступ до корпоративних даних в процесі їх передачі по відкритій мережі;

- несанкціонований доступ до внутрішніх ресурсів корпоративної локальної мережі, одержуваний зловмисником внаслідок несанкціонованого входу в цю мережу.

Захист інформації в процесі передачі по відкритих каналах зв'язку заснована на виконанні таких основних функцій:

- аутентифікації взаємодіючих сторін;

- криптографічному закритті (шифруванні) переданих даних;

- перевірці справжності та цілісності доставленої інформації.

Ці дії характеризуються взаємозв’язками. Їх застосування засноване на використанні криптографічних методів для захисту інформації.

Для захисту локальних мереж та окремих комп’ютерів від несанкціонованих дій із зовнішнього середовища зазвичай використовуються брандмауери, які

підтримують безпеку інформаційних взаємодій, фільтруючи двосторонній потік повідомлень, а також виконуючи функції посередництва в обміні інформацією. Брандмауер розташований на стику локальної та відкритої мережі. Для захисту віддаленого комп'ютера, підключеного до відкритої мережі, на цьому ж комп'ютері встановлено програмне забезпечення для доступу до мережі, тому брандмауер називається персональним екраном.

Тунелювання.

Захист інформації в процесі передачі через відкриті канали заснований на побудові захищених віртуальних каналів зв'язку, відомих як криптографічно-захищені тунелі. Кожен такий тунель - це з'єднання, встановлене через відкриту мережу, де пакети повідомлень криптографічно передаються та передаються.

Створення захищеного тунелю здійснюється частинами віртуальної мережі, які працюють на вузлах, між якими створений тунель [20]. Ці деталі називаються тунельними пускачами та фінішерами. Запуск програми тунелю вставляє (встановлює) пакети в нову папку, яка, крім вихідних даних, містить новий заголовок з інформацією про відправника та одержувача. Хоча всі пакети, що передаються через тунель, є IP-пакетами, пакети захоплення можуть бути приєднані до будь-якого типу протоколу, включаючи нестандартні пакети протоколів, такі як NetBEUI. Шлях між пусковою установкою та тунельним тунелем визначається стандартною IP-мережею, яка може бути неінтернет-мережею. Термінатор тунелю виконує процес розвороту - він видаляє нові кінцеві точки і пересилає кожен пакет до локального стеку протоколу або пункту призначення в локальній мережі.

Циркуляція сама по собі не впливає на безпеку пакетів повідомлень, що надсилаються через тунель. Але завдяки інкапсуляції існує можливість повного криптографічного захисту пакетів захоплення. Конфіденційність пакетів включень забезпечується їх криптографічним закриттям, тобто шифруванням, а цілісністю та автентифікацією - шляхом створення цифрового підпису. Оскільки так багато способів захистити криптографічні дані, дуже важливо, щоб пусковий пристрій і кінець тунелю використовували однакові методи і могли узгоджувати цю інформацію між собою.

Крім того, щоб мати можливість розшифрувати дані та перевірити цифровий підпис при отриманні, ініціатор тунелю та тунель повинні підтримувати ключові функції обміну. Нарешті, для того, щоб створювати тунелі лише між авторизованими користувачами, слід визначити кінцеві точки взаємодії.

Для технологій безпечної передачі даних через загальнодоступну (незахищену) мережу використовується загальна назва - захищений канал. Захищений канал можна побудувати за допомогою системних інструментів, реалізованих на різних етапах еталонної моделі взаємодії відкритих систем (EMBBC, OSI)

Таблиця. 2.2 Рівні протоколів захищеного каналу

Протоколи захищеного доступу	Прикладний	Впливають на додатки
	Представницький	
	Сеансовий	
	Транспортний	
	Мережевий	Невидимі для додатків
	Канальний	
	Фізичний	

Здатність активованої VPN та її сумісність із програмами IP, а також інші методи безпеки сильно залежать від обраного рівня інвалідності. Залежно від рівня роботи модуля OSI виділяються такі групи VPN [21]:

- Вторинний VPN (канал);
- VPN (мережа) третього рівня;
- VPN п’ятого класу (сесія).

VPN побудовані на дуже низьких рівнях модулів OSI. Причиною цього є те, що менша безпека захищеного каналу полегшує ясність програм та протоколів програм. Однак є ще одна проблема - залежність протоколів безпеки від конкретної мережевої технології.

Якщо для захисту даних використовується протокол високого рівня (додаток або представник), цей спосіб захисту не залежить від того, які мережі (IP або IPX, Ethernet або ATM) використовуються для передачі даних, що можна розглядати як безсумнівну перевагу . З іншого боку, така програма буде залежати від конкретного протоколу безпеки, тобто Для програм такий протокол не є очевидним.

Ще одним недоліком захищеного каналу із високим рівнем безпеки є його розгортання. Протокол захищає лише певну мережеву службу - файл, hip-link або пошту. Наприклад, S / MIME захищає лише повідомлення електронної пошти. Тому для кожної служби потрібно розробити відповідну захищену версію протоколу.

На вищих рівнях моделі OSI існує сильний зв’язок між використовуваним стеком протоколів та програмою.

VPN канального рівня

Пристрої VPN, що використовуються на рівні покриття каналу OSI, дозволяють включати різні типи третинного (і вище) трафіку і будувати віртуальні тунелі від точки до точки (від маршрутизатора до маршрутизатора або від персонального комп'ютера до шлюзу локальної мережі).). У цю групу входять продукти VPN, що використовують протоколи L2F (рівень 2) та PPTR (протокол прохідного тунелювання), а також нещодавно затверджений стандарт L2TP (протокол тунелювання рівня 2), розроблений Cisco Systems та Microsoft. .

Протокол PPP із захищеним каналом базується на протоколі PPP та забезпечує прозорість функцій захисту програм та служб на рівні додатків. Протокол PPTR може передавати пакети як в мережах IP, так і в мережах, що використовують протоколи IPKS, DECnet або NetBEUI.

Протокол L2TP використовується для налаштування віддаленого доступу до локальної мережі (оскільки він в основному базується на Windows). У той же час рішення другого рівня навряд чи отримають таке саме значення для взаємодії локальної мережі через недостатню масштабованість, коли потрібні кілька тунелів із загальними кінцевими точками.

VPN мережевого рівня

Результати VPN на мережевому рівні включають IP в IP. Одним з добре відомих протоколів на цьому етапі є SKIP, який поступово замінюється новим протоколом IPSec, призначеним для автентифікації, тунелювання та шифрування IP-пакетів.

Мережа IPSec є компромісом. З одного боку, він прозорий для додатків, а з іншого боку, він може працювати майже у всіх мережах, оскільки заснований на широкому протоколі IP.

Протокол IPSec забезпечує стандартні методи ідентифікації користувачів або комп'ютерів при запуску тунелю, стандартні методи використання тунельного шифрування кінцевої точки та стандартні методи обміну та управління ключами шифрування між кінцевими точками.

IPSec може працювати з L2TP; в результаті обидва ці протоколи забезпечують більш надійну ідентифікацію, стандартне шифрування та цілісність даних. Тунель IPSec між двома локальними мережами може підтримувати безліч окремих каналів даних, що призводить до масштабування таких програм.

Говорячи про IPSec, слід зазначити, що протокол (IKE) дозволяє передавати інформацію про передачу від зовнішніх перешкод. Вирішує проблему безпечного управління та обміну криптографічними ключами між віддаленими пристроями.

VPN сеансового рівня

Деякі VPN використовують інший метод, який називається проксі-ланцюгом. Цей метод працює вище транспортного рівня і перерозподіляє трафік із захищеної мережі в загальнодоступний Інтернет для кожного окремого сокета. (IP не має п’ятого рівня сеансу, але активність сокета називається операцією на рівні сесії.)

Шифрування інформації, що передається між пусковою установкою та термінатором тунелю, часто здійснюється шляхом захисту транспортної оболонки TLS.

Для регулювання тестового коридору через брандмауери консорціум IETF визначив протокол, який називається SOCKS, і SOCKS v.5 в даний час використовується для звичайного використання посередників каналів.

У SOCKS v.5 комп'ютер-месенджер встановлює автентифікований сокет (або сеанс) із проксі-сервером. Цей брокер - єдиний спосіб спілкування через брандмауер. Посередник, у свою чергу, виконує всі дії, які вимагає клієнт. Оскільки постачальник добре знайомий з трафіком на рівні сокета, він може здійснювати пильний контроль, наприклад, блокувати певні споживчі програми, якщо у них немає необхідних авторів.

Архітектура корпоративних мереж: варіанти побудови VPN

Залежно від особливостей роботи фірми і її конкретних завдань, VPN може бути побудована за однією з наступних моделей:

- Remote Access. У цьому випадку створюється захищений канал між офісом і віддаленим користувачем, що підключаються до ресурсів підприємства з домашнього ПК через Інтернет. Подібні системи прості в побудові, але менш безпечні, ніж їх аналоги, вони використовуються підприємствами з великою кількістю віддалених співробітників.

- Intranet. Такий варіант дозволяє об'єднати кілька філій організації. Передача даних здійснюється по відкритих каналах. Intranet може використовуватися для звичайних філій компаній і для мобільних офісів. Але слід мати на увазі, що такий спосіб передбачає установку серверів у всіх підключаються офісах.

- Extranet. Доступ до інформації підприємства надається клієнтам і іншим зовнішнім користувачам. При цьому їх можливості по використанню системи помітно обмежені. Не призначені для абонентів файли надійно захищаються засобами шифрування. Це відповідне рішення для фірм, яким необхідно забезпечити своїм клієнтам доступ до певних відомостей.

- Client / Server. Цей варіант дозволяє обмінюватися даними між декількома вузлами всередині одного сегмента. Він користується найбільшою популярністю у організацій, яким необхідно в рамках однієї фізичної мережі створити кілька логічних (наприклад, окремі структури можуть бути створені для фінансового відділу, кадрової служби та ін.). Для захисту трафіку під час поділу використовується шифрування.

Класифікація VPN за способом технічної реалізації

За способом технічної реалізації розрізняють такі групиVPN [22]:

- VPN на основі мережевої операційної системи;

- VPN на основі міжмережевих екранів;

- VPN на основі маршрутизаторів;

- VPN на основі програмних рішень;

- VPN на основі спеціалізованих апаратних засобів із вбудованими шифропроцесорами.

VPN на основі мережевої ОС

Програму VPN на основі мережевої ОС можна розглянути на прикладі операційної системи Windows NT. Щоб створити VPN, Microsoft пропонує протокол PPTR, підключений до мережевої операційної системи Windows NT. Це рішення виглядає привабливо для організацій, які використовують Windows як корпоративну операційну систему. VPN на базі операційної системи Windows NT використовують базу даних обміну повідомленнями, що зберігається в основному контролері домену (PDC). При підключенні до сервера PPTR користувач отримує дозвіл за протоколами PAP, CHAP або MS CHAP. Шифрування використовує нестандартний протокол шифрування "точка-точка" з 40-бітовим ключем, який отримується при встановленні з'єднання.

Як перевагу цієї схеми слід зазначити, що вартість мережевого рішення на базі ОС набагато нижча, ніж вартість інших рішень.

Неповнота такої системи безпеки є достатньою для протоколу PPTR.

VPN на основі маршрутизаторів

Цей метод побудови VPN передбачає використання маршрутизатора для створення захищених каналів. Оскільки вся інформація, що надходить з локальної мережі, проходить через маршрутизатор, природно також помістити їх у функцію шифрування.

VPN на основі міжмережевих екранів

Більшість брандмауерів виробників мають функції тунелювання та шифрування даних. Модуль шифрування додано до самого брандмауера.

Недоліки цього підходу включають високу вартість рішення для однієї робочої станції та залежність продуктивності від обладнання, на якому працює брандмауер. Використовуючи комп'ютерний брандмауер, майте на увазі, що цей параметр підходить лише для невеликих мереж з обмеженою інформацією.

VPN на основі програмного забезпечення

Програмні рішення також використовуються для побудови VPN. Реалізація цих схем використовує спеціалізоване програмне забезпечення, яке працює на певному комп’ютері і в основному виконує функції проксі-сервера. Комп’ютер з таким програмним забезпеченням можна розмістити за брандмауером.

VPN на основі спеціалізованих апаратних засобів із вбудованими шифропроцесором.

Параметр VPN може бути побудований на конкретному обладнанні для використання у високопродуктивних мережах. Недоліком цього рішення є висока вартість.

Технічні та економічні переваги впровадження технологій VPN в корпоративні мережі

Технологія VPN дозволяє ефективно вирішувати проблеми, пов'язані з циркуляцією конфіденційної інформації з каналів зв'язку. Це забезпечує зв'язок між мережами, а також між віддаленим користувачем та фізичною мережею через захищений (тунельний) канал, "Прокладений" у загальнодоступному Інтернеті.

Отже, на сучасному етапі розвитку, в ситуаціях, коли філії однієї компанії знаходяться на великій відстані одна від одної, потреба у швидкому та надійному обміні інформацією загострилася. Використання дорогих широкосмугових каналів не завжди можливо і економічно вигідно. Розвиток комунікацій, особливо найдешевших та доступних (наприклад, Інтернет), призвело до широкого використання практичного використання, особливо в корпораціях. За цих умов ганьба використовувати їх для просування цінної корпоративної інформації, яка може негативно вплинути на діяльність компанії. Тому використання безпечних мереж VPN з урахуванням їх переваг стає все більш важливим і вирішальним. Концепція цих мереж дозволяє обмінюватися життєво-важливою інформацією

всередині компанії та з месенджерами з найкращим поєднанням продуктивності, ефективності, безпеки та витрат. Слід визнати, що такі технології, як VPN, будуть розвиватися, розвиватися і набувати все більшого поширення.

2.3. Аналіз систем моделювання

Моделювання є потужним методом наукового пізнання, при якому предмет, що вивчається, замінюється на більш простий предмет, який називається моделлю. Основними типами процесів моделювання можна вважати два типи - математичне та фізичне моделювання. При фізичному моделюванні досліджувана система замінюється системою інших придатних матеріалів, яка відтворює властивості досліджуваної системи, зберігаючи фізичну природу. Прикладом такого типу моделювання є пілотна мережа, яка досліджує основні можливості побудови мережі на основі спеціалізованих комп'ютерів, комунікаційних пристроїв, операційних систем та додатків.

Можливості фізичного моделювання дуже обмежені. Це дозволяє вирішувати окремі проблеми за допомогою невеликої кількості комбінацій аналізованих параметрів системи. Насправді в повномасштабній моделі комп'ютерної мережі практично неможливо перевірити її функціональність на можливості, використовуючи різні типи комунікаційних пристроїв - маршрутизатори, комутатори та інші пристрої. У тесті десяток різних типів маршрутизаторів пов'язані не лише з великими зусиллями та часом, але й із значними матеріальними витратами.

Але навіть у тих випадках, коли оптимізація мережі не змінює типи пристроїв та операційних систем, а лише їх параметри, тестування в режимі реального часу для великої кількості комбінацій цих параметрів майже неможливе в той час, який доступний для огляду. Навіть проста зміна максимального розміру пакета будь-якого протоколу вимагає зміни конфігурації операційної системи на сотнях мережевих комп'ютерів, що вимагає багато роботи від адміністратора мережі.

Тому математичне моделювання в основному використовується для оптимізації мережі. Математична модель - це сукупність взаємозв'язків (формул, рівнянь, нерівностей, логічних умов), що визначають процес зміни стану системи відповідно до її параметрів, вхідних сигналів, початкових умов та часу.

Імітаційні моделі - це особливий клас математичних моделей. Такі моделі є комп'ютерними програмами, які поступово відтворюють події, що відбуваються в реальній системі. На відміну від комп'ютерних мереж, їх імітаційні моделі копіюють процеси генерації повідомлень із додатків, розбиття повідомлень на пакети та фрейми конкретних протоколів, затримки, пов'язані з обробкою повідомлень, пакетів та паралельні рамки.

Результат імітаційної моделі збирається під час спостереження статистичних даних про найважливіші особливості мережі: час відгуку, коефіцієнти використання каналів і вузлів, ймовірність втрати пакетів.

Специфічні системи, орієнтовані на моделювання програмних систем комп'ютерної мережі, в яких процес створення модуля спрощений. Такі програмні системи самі генерують мережеву модель на основі вихідних даних про її топологію та використовувані протоколи, інтенсивність додатків між мережевими комп'ютерами, довжину ліній зв'язку, типи обладнання та використовувані програми.

Імітаційні програмні системи можуть бути дуже вузькими та надзвичайно гнучкими, що дозволяє моделювати мережі різних типів. Якість результатів моделювання значною мірою залежить від точності вихідних даних мережі, що передаються в систему моделювання.

Далі представлені сучасні системи модулювання [23]:

- Сімейство CANE (компанія ImageNet) - проектування та реінжиніринг обчислювальної системи, оцінка різних варіантів, сценарії "що, якщо". Моделювання на різних рівнях моделі OSI. Розвинена бібліотека пристроїв, яка включає фізичні, електричні, температурні і інші характеристики об'єктів. Можливе створення своїх бібліотек.

- BONeS (фірма Systems and Networks) - графічна система моделювання загального призначення для аналізу архітектури систем, мереж і протоколів. Описує моделі на транспортному рівні і на рівні додатків. Дає можливість аналізу впливу додатків типу клієнт - сервер і нових технологій на роботу мережі.

- . Netmaker (фірма OPNET Technologies) - проектування топології, засобів планування і аналізу мереж широкого класу. Складається з різних модулів для розрахунку, аналізу, проектування, візуалізації, планування і аналізу результатів.

- Optimal Perfomance (фірма Compuware; Optimal Networks) - має можливості швидкого оцінного і точного моделювання, допомагає оптимізувати розподілене програмне забезпечення.

- Prophesy (компанія Abstraction Software) - проста система для моделювання локальних і глобальних мереж. Дозволяє оцінити час реакції комп'ютера на запит, кількість "хітів" на WWW-сервері, кількість робочих станцій для обслуговування активного устаткування, запас продуктивності мережі при поломці певного устаткування.

- Сімейство OPNET (фірма OPNET Technologies) - засіб для проектування і моделювання локальних і глобальних мереж, комп'ютерних систем, додатків і розподілених систем. Можливість імпорту і експорту даних про топологію і мережевий трафік. Аналіз впливу додатків типу клієнт - сервер і нових технологій на роботу мережі. Моделювання ієрархічних мереж, багато протокольних локальних і глобальних мереж; облік алгоритмів маршрутизації. Об'єктно-орієнтований підхід. Вичерпна бібліотека протоколів і об'єктів. Включає наступні продукти: Netbiz (проектування і оптимізація обчислювальної системи), Modeler (моделювання і аналіз продуктивності мереж, комп'ютерних систем, додатків і розподілених систем), ITGuru (оцінка продуктивності комунікаційних мереж і розподілених систем).

- Сімейство COMNET (фірма Compuware; CACI Products Company) - об'єктно-орієнтована система моделювання локальних і глобальних мереж. Дозволяє моделювати рівні: додатків, транспортний, мережевий, канальний. Використовує всі відомі на сьогодні технології і протоколи, а також системи клієнт - сервер. Легко

налаштовується на модель устаткування і технологій. Можливість імпорту і експорту даних про топологію і мережевий трафік. Моделювання ієрархічних мереж, багато протокольних локальних і глобальних мереж; облік алгоритмів маршрутизації.

- Stressmagic (фірма NetMagic Systems) - підтримка стандартних тестів виміру продуктивності; імітація пікового навантаження на файл-сервер і сервер друку. Можливе моделювання взаємодії різних користувачів з файл-сервером. Включає 87 тестів продуктивності.

- Packet Tracer (Cisco) - симулятор мережі передачі даних, що випускається фірмою Cisco Systems. Дозволяє робити працездатні моделі мережі, налаштовувати (командами Cisco IOS) маршрутизатори і комутатори, взаємодіяти між декількома користувачами (через хмару).

Для чого потрібне використання Packet Tracer (Cisco) [24]:

- Створення віртуальних мереж;

- Перевірка нових ідей при побудові інфраструктур, управлінні ними та забезпеченні їх безпеки;

- Візуалізація внутрішніх процесів в режимі реального часу;

- Застосування навичок в рамках лабораторних та інтерактивних занять.

Висновки за розділом 2

1) Глобальна мережа передачі даних (WAN) - це мережа взаємопов’язаних ліній за допомогою спеціалізованого телекомунікаційного обладнання та обладнання для передачі даних абонентів, розташованих на значній території.

2) Локальна мережа передачі даних (LAN) - це мережа взаємопов’язаних комп’ютерів або інших кінцевих пристроїв, розташованих на невеликій території. Локальні мережі дозволяють користувачам отримати доступ до розподілених засобів, розміщених на інших комп’ютерах.

3) Основною метою WAN є надання методів зв'язку багатьом різним користувачам, тобто виконання транспортних завдань при розподілі мережевого трафіку.

4) Захищеною віртуальною мережею VPN називають об'єднання локальних мереж і окремих комп'ютерів через відкриту зовнішню середу передачі інформації в єдину віртуальну корпоративну мережу, що забезпечує безпеку циркулюючих даних.

Розвиток комунікацій, особливо найдешевших та доступних (наприклад, Інтернет), призвело до широкого використання практичного використання, особливо в корпораціях. За цих умов ганьба використовувати їх для просування цінної корпоративної інформації, яка може негативно вплинути на діяльність компанії. Тому використання безпечних мереж VPN з урахуванням їх переваг стає все більш важливим і вирішальним.

5) Було досліджено види моделей побудови VPN: Remote Access, Intranet, Extranet, Client/Server.

РОЗДІЛ 3
РОЗРОБКА МЕРЕЖІ ПІДПРИЄМСТВА

3.1 Аналіз етапів проектування

3.1.1 Аналіз вимог

Аналіз вимог включає визначення проблем компанії та бізнес-цілей, а також розробку дизайнерської діяльності та цілей відповідно. Аналіз вимог до цього допоможе оцінити ділову значимість рішення інформаційних технологій, визначити ключові цілі та вибрати пріоритети для окремих частин комп'ютерної системи, які потребують розробки або розширення. Чітке визначення вимог до мережевих операцій допоможе уникнути використання непотрібних властивостей мережі, що врятує компанію.

Іншими словами, перед проектуванням мережі потрібно зрозуміти, які переваги має отримати компанія від оновлення KKS (наприклад, зменшення виробничого циклу, впорядкування швидшого або більшої продуктивності завдяки взаємодії співробітників, більш ефективною), які завдання вирішує мережа, які основні транспортні потоки будуть. як фізично розгортаються користувачі та ресурси, чи потрібні пріоритетні дії, як вирішуються проблеми із захистом даних у мережі, як мережа підключена до Інтернету, як вирішити проблеми з виставленням рахунків, управління доступом споживачів. Крім того, фаза аналізу заявок вимагає перевірки стану будівель та споруд у місці встановлення мережі, аналіз існуючої інфраструктури. Ця інформація є важливою для вирішення проблем дизайну та для самого дизайну.

3.1.2. Розробка функціональної моделі

Операційна модель (або бізнес-модель) виробництва відображає послідовність операцій і технологічних процесів підприємства, а також кожен з окремих підрозділів, визначаючи набір мережевих завдань, що виконуються в одиниці, виходячи з чого вимогами до проектування та ініціатив в цілому [25].

Окрім формулювання вимог до корпоративної мережі, вам потрібно отримати огляд того, що відбувається в кожному регіоні. Це те, що описує модель дії. Зазвичай він не стосується комп'ютерної системи, він зосереджений на комерційному використанні та порядку роботи. Спочатку будується модель, яка показує порядок роботи всієї компанії, а потім - модель порядку роботи в кожному відділі. Необхідно також зазначити, як виконується робота, хто буде її виконувати та які стосунки між робочими групами та департаментами.

Щоб розробити модель дій KKS, слід зібрати команду з керівниками підрозділів, ключовими експертами та персоналом у відділі автоматизації та досягти наступного [26]:

- опитувати керівників відділів та кінцевих користувачів корпоративних мереж, щоб визначити їх діяльність та з'ясувати, як комп'ютерні системи допомагають їм у роботі;

- з'ясувати, як робота передається з одного підрозділу в інший і як інформація та діяльність передаються від одного працівника до іншого;

- з'ясувати, які є залежності - хто дозволить будь-який рівень роботи та в якому порядку рівень повинен бути завершений;

- зрозуміти, які пляшки має система - тривалий час відгуку або неефективна обробка даних.

3.1.3. Розробка технічної моделі

Після розробки моделі дії та прийняття рішення про те, які методи потрібно змінити або вдосконалити, необхідно побудувати технічну модель ККС. Технічна

модель, як правило, визначає, яке комп'ютерне обладнання слід використовувати для досягнення описаних раніше цілей. Для побудови технічної моделі необхідно вивчити існуюче обладнання, визначити вимоги до системи, оцінити стан сучасного та завтрашнього дня.

Аналіз існуючого обладнання зводиться до апаратного реєстру та бази програм, що працюють у корпоративній мережі, в результаті чого приймається рішення про використання частини обладнання в новому проекті ССС. Це рішення повинно базуватися на відповідності обладнання вимогам до спроектованої мережі на етапі розробки експлуатаційної моделі, а також на рівні перевірки системних вимог до технічної моделі. Процес перепису можна і потрібно автоматизувати. Є програми, які можуть автоматично сканувати апаратне та програмне забезпечення, яке вже працює в комп'ютерній мережі. Загалом такі програми можуть визначати тип процесора, доступну пам'ять, тип диска та вільний простір на ньому, додаткові доступні контролери - такі як мережеві пристрої, факс-модеми тощо. Для програмного забезпечення ви можете дізнатися назву та версію програм, версії операційної системи, встановлені мережеві драйвери.

Щоб пояснити вимоги системи, необхідно відповісти на такі запитання:

- Що потрібно зав'язати? Чи повинен співробітник будь-якого підрозділу спілкуватися з невеликою (великою) кількістю людей на невеликій території чи повинен спілкуватися з невеликою (великою) кількістю людей на великій території? Широта та розподіл планшета допоможуть визначити критичну потужність комп'ютера, а також типи та швидкість комунікаційного обладнання та послуг.

- Яке обладнання та програмне забезпечення буде використано для нової системи? Які системи повинні жити в покращеній корпоративній мережі? Чи потрібно підключати ці системи до мережі? Чи будуть існуючі системи нормально працювати в новій мережі? Чи існують стандарти компанії, чи є надійні програми? Яке обладнання та додатки потрібно додати для досягнення встановлених виробничих цілей?

- Які обсяги інформації передаються по мережі? Обсяг переданої інформації визначає необхідну пропускну здатність мережі. Обчисліть це, підрахувавши

кількість користувачів мережі, середню кількість транзакцій на одного користувача на день та середній розмір транзакцій. Цей розрахунок допоможе визначити технологію доступу до середовища передачі даних (Ethernet, FDDI, ...) та вимоги до глобальних послуг.

- Який час відгуку мережі підходить? Чи чекатимуть клієнти одну секунду, пів секунди чи дві? Такі вимірювання допоможуть визначити вимоги до відстані до обладнання, додатків та комунікацій.

- Скільки часу займає мережа для роботи компанії? Вам потрібна мережа 24 години на добу та 7 днів на тиждень або лише 8 годин на день та 5 днів на тиждень? Чи потрібно сьогодні збільшувати можливості використання мережі?

- Які вимоги до середнього часу вирішення проблем? Як роботи з технічного обслуговування та ремонту мережі впливають на ефективність бізнесу? Чи втратить компанія 5 мільйонів доларів або 100 000 доларів, якщо мережа вийде з ладу протягом години? Що шкодить простій мережі протягом двох годин?

- Яке заплановане зростання системи? Який зараз рівень використання мережі та як він може змінитися протягом наступних 6 місяців, року, двох років? Навіть якщо ви ретельно розробили мережу, але не замислювались про потенціал для зростання та розвитку, вимоги системи повинні змінюватися та збільшуватися. Зростання мережі слід планувати заздалегідь, а не лише у відповідь на фактичне зростання навантаження.

3.1.4. Розробка фізичної моделі

Після того, як для мережі обрано технічну модель, необхідно оцінити, наскільки вона відповідає вимогам виробництва. Необхідно повернутися до моделі дії та порівняти її вимоги з технічними рішеннями. Наприклад, якщо співробітники компанії часто переходять від відділу до відділу, вимога до моделі дії щодо переведення є високою [27]. Потім технічна модель повинна забезпечувати швидке підключення та відключення робочої станції.

Після оцінки відповідності технічної моделі виробничим вимогам повинна бути побудована фізична модель. Фізична модель визначає деталі технічної моделі і являє собою дуже детальний опис мережі, що показує технічні характеристики пасивного, функціонального та термінаційного обладнання, тоді як технічна модель використовує більш загальні терміни.

На етапі фізичного моделювання проектувальник повинен описати, які деталі потрібні, якою мірою, де вони будуть розташовані і як ці частини будуть взаємопов'язані у фізичній мережі.

Встановлення системи та усунення несправностей. Цей рівень включає координацію закупівель у субпідрядників, управління конфігурацією, встановлення та модифікацію обладнання, навчання персоналу [28].

3.2 Розробка корпоративної мережі

Аналіз вимог до побудови корпоративної мережі

Розподілена корпоративна мережа повинна відповідати наступним вимогам:

- можливість розширення - показує ймовірність легкого додавання окремих елементів мережі (користувачів, комп'ютерів, додатків, послуг), збільшення довжини елементів мережі та заміни існуючого обладнання на більш надійне.

Зрозуміло, що система легко розтягується в певних обмежених межах. Наприклад, локальна мережа Ethernet, заснована на одній ділянці товстого коаксіального кабелю, має чудову масштабованість у тому сенсі, що дозволяє легко підключати нові станції. Однак така мережа обмежена кількістю станцій - їх кількість не повинна перевищувати 30-40. Правда, мережа дозволяє фізичне з'єднання з більшим сегментом і кількістю станцій (до 100), але часто знижує ефективність мережі. Наявність такого обмеження свідчить про погану масштабованість системи з чудовою масштабованістю;

- масштабованість - показує, що мережа може збільшити кількість вузлів і довжину з'єднань на широкій ділянці, не знижуючи при цьому ефективність мережі.

Для забезпечення масштабованості мережі необхідно використовувати додаткове комунікаційне обладнання, а мережа повинна бути структурована певним чином.;

- продуктивність – висока мережева продуктивність необхідна для нормальної роботи більшості програм;

- керованість - він має можливість централізованого моніторингу стану основних елементів мережі, виявлення та вирішення проблем, що виникають під час функціонування мережі, проведення огляду продуктивності та планування розвитку мережі. Тобто наявність ймовірностей взаємодії співробітників з мережею для оцінки роботи мережі та її елементів, встановлення параметрів та внесення змін до мережі;

- надійність - здатність передавати інформацію без спотворень і втрат;

- безпека - здатність системи захистити дані від несанкціонованого доступу.

Бізнес-модель підприємства

В даному випадку при розробці захищеної розподіленої корпоративної мережі було дотримано таку функціональну модель. Організація складається з чотирьох відділів: підтримка, бухгалтерія, розробка, а також відділ з інформаційної безпеки.

Розробка технічної моделі

Обладнання, яке потрібно було при побудові захищеної розподіленої корпоративної мережі:

- 7 робочих місць;

- 3 маршрутезатора;

- 3 комутатори;

- сервер.

Розробка фізичної моделі

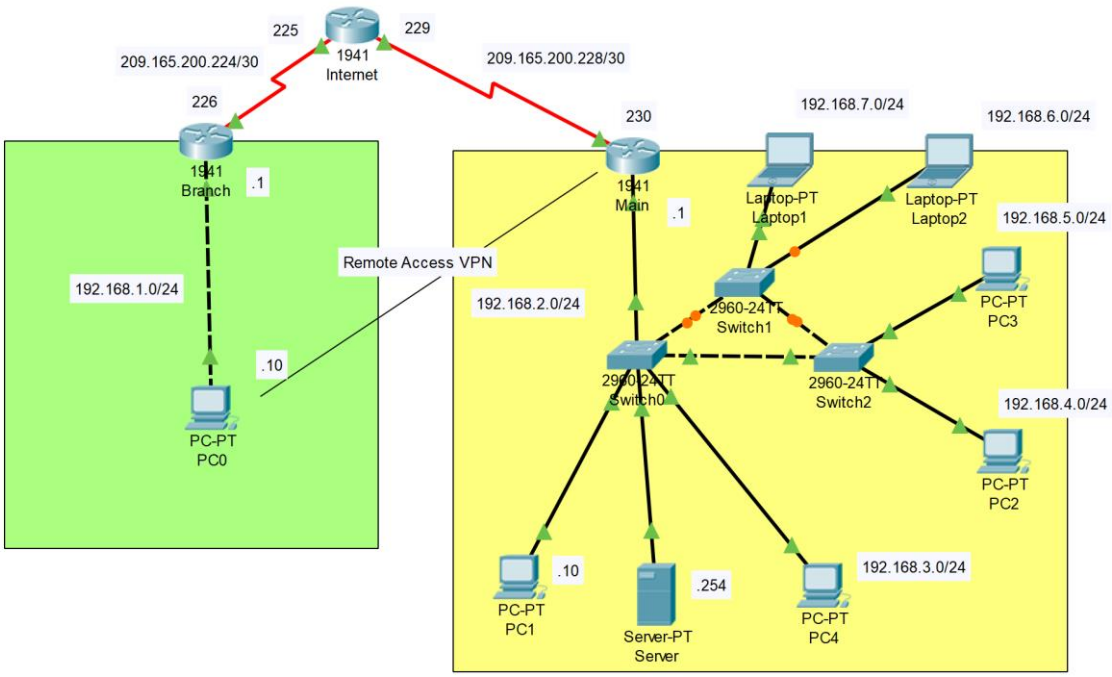

Рисунок 3.1 – Remote Access VPN

Висновки за розділом 3

1) Функціональна виробництва відображає послідовність робіт і технологічних процесів підприємства, а також кожного з підрозділів окремо, визначає набір мережевих завдань, які виконуються в кожному з підрозділів, на підставі яких формулюються вимоги до проектованої мережі, що пред'являються до неї специфікою бізнес процесів кожного з підрозділів окремо і підприємства в цілому.

Одночасно з формулюванням вимог до корпоративної мережі, потрібно отримати загальне уявлення про те, що відбувається в кожному відділі.

2) Після розробки функціональної моделі і визначення того, які процедури вимагають зміни чи поліпшення, необхідно побудувати технічну модель ККС. Технічна модель описує в досить загальних термінах, яке комп'ютерне обладнання треба використовувати, щоб досягти цілей, визначених раніше. Щоб побудувати технічну модель, потрібно проаналізувати існуюче обладнання, визначити системні вимоги, оцінити сьогоднішній і завтрашній стан техніки.

3) Були проаналізовані вимоги до побудови захищеної корпоративної мережі а також була розроблена фізична модель корпоративної мережі.

ВИСНОВКИ

У дипломній роботі вирішено актуальну науково-технічну задачу розробки захищеної корпоративної мережі на основі методів побудови корпоративних мереж за допомогою технології VPN.

VPN легко масштабується і є оптимальним варіантом для підприємств, що володіють певною кількістю відділень, а також для фірм, чиї співробітники часто бувають у відрядженнях або працюють з дому. Підключення нового офісу або нового віддаленого співробітника здійснюється без додаткових витрат на комунікації.

Основні результати дипломної роботи:

1) Були проаналізовані існуючі методи побудови корпоративних мереж. В даній роботі використовувались методи…

2) Було визначене найоптимальніше рішення для побудови корпоративної мережі. Це використання технології віддаленого доступу з поєднанням технології VPN. Дане рішення дозволить забезпечити найвищу захищеність корпоративної мережі.

3) Була розроблена модель захищеної розподіленої мережі за допомогою програмного забезпечення Cisco Packet Tracer (див. рис.3.1). В даному випадку при розробці захищеної розподіленої корпоративної мережі було дотримано таку функціональну модель. Організація складається з чотирьох відділів: підтримка, бухгалтерія, розробка, а також відділ з інформаційної безпеки.

4) Була спроектувати та реалізована корпоративна мережа.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Arif Mohamed. A history of cloud computing [Електронний ресурс]. – Режим доступу: http://www.computerweekly.com/feature/A-history-of-cloud-computing

2. Peter M. Mell, Timothy Grance The NIST Definition of Cloud Computing [Електронний ресурс]. – Режим доступу: https://www.nist.gov/node/568586

3. SoCC 10: Proceedings of the 1st ACM symposium on Cloud computing, Hellerstein, Joseph M. - N. Y.: ACM, 2010. - ISBN 978-1-4503-0036-0.

4. Gillam, Lee. Cloud Computing: Principles, Systems and Applications / Nick Antonopoulos, Lee Gillam. — L.: Springer, 2010. — p. 379.

5. Баранов А.П. Чи можна захистити в «хмарі» конфіденційну інформацію? А. Баранов // Системи високої доступності. — 2012. — Т. 8. — № 2. — С. 12-15.

6. Бабаш А.В., Гольєв Ю.І., Ларін Д.А., Шанкін Г.П. Про розвиток криптографії в XIX столітті // Захист інформації. Конфидент. — 2003. — №5 — с. 90-96.

7. Безпека життєдіяльності. Безпека технологічних процесів і виробництв (Охорона праці): Навч. посібник для вузів // П.П. Кукін, Е.А. Підгорний та ін. - М .: Висш.шк., 1999. — с. 318.

8. А. Астахов. IDS как средство управления рисками / А. Астахов : [Електронный ресурс]. – Режим доступу : URL : http://www.globaltrust.ru/security/Pubs/Pub2_part5. - Назва з екрану.

9. А. В. Соколов. Защита информации в распределенных корпоративных сетях и системах / А. В. Соколов, В. Ф. Шаньгин. - ДМК Пресс., 2012. – 656с.

10. Hacker Dictionary [Electronic Resource]. – Mode of access : URL : http://www.robergraham.com/hacker-dictionary. - Назва з екрану.

11. Deborah Russell. Computer Security Basics, O'Reilly & Associates / Deborah Russell, G. T. Gangemi. – CA, 2011.

12. Крысин В.А. Безопасность предпринимательской деятельности / Крысин В.А. - М:Финансы и статистика, 2010.

13. Аджиев В. Мифы о безопасности программного обеспечения / Аджиев В. – К: Уроки знаменитых катастроф, 2005. – (Открытые системы).

14. Структура руководства по обеспечению информационной безопасности [Електронный ресурс]. – Режим доступу : URL : http://www.globaltrust.ru/security/knowbase/Policies/Guide_Struct. - Назва з екрану.

15. Как обосновать затраты на информационную безопасность? [Електронный ресурс]. – Режим доступу : URL : http://www.iitrust.ru/articles/zat_ibezop. - Назва з екрану.

16. Демин В.С. Автоматизированные банковские системы / Демин В.С. - М: Менатеп-Информ, 2003.

17. Whalen, Sean. An Introduction to ARP Spoofing / Whalen, Sean. – 2001.

18. RFC 1734 POP3 Authentication command [Electronic Resource]. – Mode of access : URL : http://www.faqs.org/rfcs/rfc1734. - Назва з екрану.

19. RFC 959 File Transfer Protocol [Electronic Resource]. – Mode of access : URL : http://www.faqs.org/rfcs/rfc959. - Назва з екрану.

20. Cracking NTLMv2 Authentication [Electronic Resource]. – Mode of access : URL : http://www.securityfriday.com. - Назва з екрану.

21. Kimmo Kasslin Antti Tikkanen Attacks on Kerberos V in a Windows 2000 Environment [Electronic Resource]. – Mode of access : URL : www.hut.fi/~autikkan/kerberos/docs/phase1/pdf/LATEST_final_report. - Назва з екрану.

22. Frank O'Dwyer Feasibility of attacking Windows 2000 Kerberos Passwords [Electronic Resource]. – Mode of access : URL : http://www.brd.ie. - Назва з екрану.

23. [Electronic Resource]. – Mode of access : URL : http://lasecwww.epfl.ch/php_code/publications/search.php?ref=Oech03. - Назва з екрану.

24. [Electronic Resource]. – Mode of access : URL : http://www.antsight.com/zsl/rainbowcrack. - Назва з екрану.

25. Цифры на стороне Microsoft [Електронный ресурс]. – Mode of access : URL : Internet URL http://www.izone.kiev.ua . - Назва з екрану.

26. [Electronic Resource]. – Mode of access : URL : http://www.microsoft.com/technet/security/bulletin/ms03-026.mspx. - Назва з екрану.

27. Daiji Sanai Detection of Promiscuous Nodes Using ARP Packets [Electronic Resource]. – Mode of access : URL : http://securityfriday.com. - Назва з екрану.

28. SANS Bulletin Why your switched network isn't secure [Electronic Resource]. – Mode of access : URL : http://www.sans.org. - Назва з екрану.

ДОДАТОК А

Апробація

1. Зюбіна Р. В., Сарока С. О. Побудова захищеної розподіленої корпоративної мережі // IV Міжнародна науково-практична конференція 15-16 квітня 2021 року “Проблеми кібербезпеки інформаційно-телекомунікаційних систем” (PCSITS), ст. 92-93.

ДОДАТОК Б

Налаштування віддаленого доступу по VPN

Internet:

```
Press RETURN to get started!

System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC disabled

Readonly ROMMON initialized

program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340

IOS Image Load Test
_____
Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x2bb1c58
Self decompressing the image :
################################################################################ [OK]
Smart Init is enabled
smart init is sizing iomem
TYPE MEMORY_REQ
HWIC Slot 0 0x00200000 Onboard devices &
buffer pools 0x01E8F000
-----------------------------------------------
TOTAL: 0x0268F000
Rounded IOMEM up to: 40Mb.
Using 6 percent iomem. [40Mb/512Mb]

Restricted Rights Legend
Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706
```

```
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thurs 5-Jan-12 15:41 by pt_team
Image text-base: 0x2100F918, data-base: 0x24729040

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)
--- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]: no
Press RETURN to get started!
Router>en
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Internet
Internet(config)#int s0/0/0
Internet(config-if)#ip address 209.165.200.225 255.255.255.252
Internet(config-if)#clock rate 4000000
Internet(config-if)#no shutdown
Internet(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
Internet(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
Internet(config-if)#int s0/0/1
Internet(config-if)#ip address 209.165.200.229 255.255.255.252
Internet(config-if)#clock rate 4000000
Internet(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
Internet(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
```

```
Internet con0 is now available
Press RETURN to get started.
Internet>en
Internet#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Internet(config)#
Internet con0 is now available
Press RETURN to get started.
%LINK-3-UPDOWN: Interface Serial0/0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to down
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
```

Main:

```
Main>en
Main#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Main(config)#
Main(config)#ip local pool PoolVPN 192.168.2.100 192.168.2.115
Main(config)#aaa new-model
Main(config)#aaa authentication login UserVPN local
Main(config)#aa authorization network GroupVPN local
Main(config)#username uservpn secret ciscovpn
Main(config)#crypto isakmp policy 100
Main(config-isakmp)#encryption aes 256
Main(config-isakmp)#hash sha
Main(config-isakmp)#authentification pre-share
^
% Invalid input detected at '^' marker.
Main(config-isakmp)#authentication pre-share
Main(config-isakmp)#group 5
Main(config-isakmp)#lifetime 3600
Main(config-isakmp)#exit
Main(config)#crypto isakmp client configuration
% Incomplete command.
Main(config)#crypto isakmp client configuration group GroupVPN
Main(config-isakmp-group)#key ciscogroupvpn
Main(config-isakmp-group)#pool PoolVPN
Main(config-isakmp-group)#exit
Main(config)#crypto ipsec transform-set SetVPN esp-aes esp-sha-hmac
Main(config)#crypto dynamic-map DynamicVPN 100
Main(config-crypto-map)#set transform-set SetVPN
Main(config-crypto-map)#reverse-route
Main(config-crypto-map)#exit
Main(config)#crypto map StaticMap client configuration address respond
Main(config)#crypto map StaticMap client authetication list UserVPN
^
% Invalid input detected at '^' marker.
```

```
Main(config)#crypto map StaticMap client authentication list UserVPN
Main(config)#crypto map StaticMap isakmp authorization list GroupVPN
Main(config)#crypto map StaticMap 20 ipsec-isakmp dynamic DynamicVPN
Main(config)#int s0/0/1
Main(config-if)#crypto map StaticMap
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Main(config-if)#
Main con0 is now available
Press RETURN to get started.
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
```

Branch:

```
Router>enable
Router#cong term
^
% Invalid input detected at '^' marker.
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname Branch
Branch(config)#int g0/0
Branch(config-if)#ip address 192.168.1.1 255.255.255.0
Branch(config-if)#no shutdown
Branch(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
Branch(config-if)#int s0/0/0
Branch(config-if)#ip address 209.165.200.226 255.255.255.252
Branch(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
Branch(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
Branch con0 is now available
Press RETURN to get started.
Branch>en
Branch#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Branch(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
%Default route without gateway, if not a point-to-point interface, may impact performance
Branch(config)#ip access-list standard ACL_NAT
Branch(config-std-nacl)#permit 192.168.1.0 0.0.0.255
Branch(config-std-nacl)#exit
Branch(config)#ip nat inside source list ACL_NAT interface s0/0/0
Branch(config)#int s0/0/0
Branch(config-if)#ip nat outside
Branch(config-if)#int g0/0
Branch(config-if)#ip nat inside
Branch(config-if)#
Branch con0 is now available
Press RETURN to get started.
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
```

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up