ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ТЕХНІЧНИХ СИСТЕМ КІБЕРЗАХИСТУ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Система захисту інформації в інформаційно-комунікаційних мережах подвійного призначення»

на здобуття освітнього ступеня магістра
зі спеціальності __125__Кібербезпека та захист інформації»
(код, найменування спеціальності)
освітньо-професійної програми Технічні системи інформаційного та кібернетичного захисту

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Владислав САВЧЕНКО

Виконав: здобувач вищої освіти групи СЗДМ 62
Владислав САВЧЕНКО

Керівник: ТУРОВСЬКИЙ Олександр
д.т.н., професор *(ПРІЗВИЩЕ, Ім'я)*

Рецензент: _____
. *(ПРІЗВИЩЕ, Ім'я)*

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Технічних систем кіберзахисту
Ступінь вищої освіти магістр
Спеціальність Кібербезпека та захист інформації
Освітньо-професійна програма Технічні системи інформаційного та кібернетичного захисту

ЗАТВЕРДЖУЮ
Завідувач кафедри ТСКБ
Олександр ТУРОВСЬКИЙ

«____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Савченку Владиславу Миколайовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи:
«Система захисту інформації в інформаційно-комунікаційних мережах подвійного призначення»
керівник кваліфікаційної роботи Олександр ТУРОВСЬКИЙ д.т.н., професор
(ПРІЗВИШЕ Ім'я. науковий ступінь. вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «30» жовтня 2025 р. № 467

2. Строк подання кваліфікаційної роботи 15.12.2025 р.

3. Вихідні дані до кваліфікаційної роботи: об'єкт інформаційної діяльності, технічні канал витоку інформації, вимоги до захисту інформації з обмеженим доступом, сучасні засоби системи контролю та управління доступом, технічні засоби захисту та технічної системи охорони

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
4.1 Здійснити аналіз актуальності процесів захисту інформації в інформаційних мережах.
4.2 Провести класіфікацію та надати опис інформаційних системи.
4.3 Дослідити сучасні методи захисту інформації та запропонувати рішення щодо захисту інформації в телекомунікаційних системах подвійного призначення

5. Перелік графічного матеріалу: Презентаційний матеріал на слайдах

6. Дата видачі завдання 15.10.2025

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури		
2	Написання першого розділу роботи		
3	Написання другого розділу роботи		
4	Написання третього розділу роботи		
5	Написання висновків по роботі		
6	Підготовка демонстраційних матеріалів		
7	Підготовка доповіді		

Здобувач вищої освіти _____ Владислав САВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник роботи _____ Олександр ТУРОВСЬКИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи складається зі вступу, чотирьох розділів, загальних висновків, списку використаних джерел, загальний обсяг роботи складає 87 сторінок. Список використаних джерел містить 36 найменувань і займає 3 сторінки.

Метою кваліфікаційної роботи є підвищення ефективності захисту інформації в інформаційно-комунікаційних мережах подвійного призначення.

У процесі підготовки кваліфікаційної роботи були вирішені наступні задачі:

1) Проведено аналіз актуальності захисту інформації в інформаційно-комунікаційних мережах.

2) Класифіковано інформаційно-комунікаційнісистеми.

3) Досліджено сучасні методи захисту інформації в інформаційно-комунікаційних системах.

4) Проведено аналіз та запропонувано можливі рішення щодо захисту інформації в інформаційно-комунікаційних системах подвійного призначення.

Апробація:

О.В. Матвійчук, В.М. Савченко. Побудова та принципи функціонування системи захищеного допуску користувачів до роботи з інформацією з обмеженим доступом. *Всеукраїнської науково- практичної конференція: Актуальні проблеми безпеки інформаційно-комунікаційних систем*. м. Київ, 05-06 листопада 025 року, Київ: РВЦ ДУІКТ. – 2025. С.31-32. h https://duikt.edu.ua/uploads/p_2779_72486260.pdf

Ключові слова: ІНФОРМАЦІЙНА МЕРЕЖА, ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНІЙ МЕРЕЖІ, КЛАСИФІКАЦІЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМИ, ІНФОРМАЦІЙНА МЕРЕЖА ПОДВІЙНОГО ПРИЗНАЧЕННЯ.

ABSTRACT

The text part of the qualification work consists of an introduction, four sections, general conclusions, a list of sources used, the total volume of the work is 87 pages. The list of sources used contains 36 items and takes up 3 pages.

The purpose of the qualification work is to increase the effectiveness of information protection in dual-purpose information and communication networks.

In the process of preparing the qualification work, the following tasks were solved:

1) An analysis of the relevance of information protection in information and communication networks was conducted.

2) Information and communication systems were classified.

3) Modern methods of information protection in information and communication systems were studied.

4) An analysis was conducted and possible solutions for information protection in dual-purpose information and communication systems were proposed.

Approbation:

O.V. Matviychuk, V.M. Savchenko. Construction and principles of operation of a system of protected user access to work with information with limited access. All-Ukrainian Scientific and Practical Conference: Current Problems of Security of Information and Communication Systems. Kyiv, November 5-6, 2025, Kyiv: DUIKT Research and Development Center. – 2025. P.31-32. h https://duikt.edu.ua/uploads/p_2779_72486260.pdf

Keywords: INFORMATION NETWORK, INFORMATION PROTECTION IN THE INFORMATION NETWORK, CLASSIFICATION OF INFORMATION AND COMMUNICATION SYSTEMS, DUAL-PURPOSE INFORMATION NETWORK.

ЗМІСТ

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ОДВ	–	Орган державної влади
КЗІ	–	Криптографічний захист інформації
КСЗІ	–	Комплексна система захисту інформації
ОМС	–	Орган місцевого самоврядування
ТЗІ	–	Технічний захист інформації
ТМ	–	Транспортна мережа
VPN	–	Virtual Private Network
ASIC	–	Application-specific Integrated Circuit
CAM	–	Content-addressable memory
МТК	–	Мобільний телекомунікаційний комплект
НСКЗ	–	Національна система конфіденційного зв'язку
IDS/IPS	–	Intrusion Detection System

ВСТУП

Застосування інформаційних технологій стало головним пріоритетом для приватних підприємств. Їхня діяльність не лише споживає значну частину їхніх бюджетів та впливає на політику, але й стимулює розвиток у всіх сферах суспільного життя, таких як надання простих послуг або ведення великомасштабного технологічного виробництва. Це не лише збільшує можливості працевлаштування в будь-якій країні, але й сприяє науковому та технологічному прогресу.

Завдяки суспільному розвитку та інформаційним та іншим технологіям, що використовуються людьми, цінність будь-яких конфіденційних даних, пов'язаних з окремими особами, технологіями або певною приватною інформацією, значно зросла. Це, у свою чергу, створює численні ризики та підживлює спроби викрадення конфіденційної інформації, яка може бути використана для недобросовісної конкуренції, порушуючи економічну безпеку пересічних громадян, підприємств і навіть держав.

У сучасну епоху багато країн та приватних установ зі значними економічними та політичними інтересами не лише намагаються захистити власну інформаційну безпеку, але й використовують шпигунство для атаки на конкурентів.

На відміну від державних установ та великих корпорацій, окремі особи не надають пріоритет захисту інформації у всіх сферах своєї роботи, визнаючи його важливість лише тоді, коли відбуваються серйозні інциденти (вторгнення, шахрайство або саботаж, витік конфіденційної інформації).

Одним з головних завдань держав у сфері захисту інформації є вдосконалення методів та надання послуг підприємствам для захисту їхньої економічної та технологічної інформації.

Метою сертифікаційної роботи є підвищення рівня безпеки та захисту інформації комерційних організацій у телекомунікаційних системах подвійного призначення.

Надання допомоги або консультацій щодо захисту інформації сприятиме розвитку ц

1) Технологічний розвиток у цій галузі.

Постійний попит з боку приватного сектору на захист інформації в телекомунікаційних системах надасть можливість для розвитку в цій галузі. Через появу різних існуючих та нових методів кібератак, потреба в нових концепціях захисту інформації продовжуватиме зростати. Подальший розвиток у цій галузі допоможе оптимізувати та знизити витрати з часом.

2) Створення робочих місць.

Телекомунікаційні системи вимагають великої кількості персоналу для захисту інформації приватного сектору. Через високий попит у сфері захисту інформації багато галузей зможуть наймати працівників для розширення виробництва, а різні компанії також можуть розробляти власні рішення щодо захисту інформації, що, у свою чергу, створить попит на інженерів.

3) Додатковий дохід.

Створення робочих місць та надання послуг із захисту інформації генеруватимуть додаткові надходження до бюджету. Однак, послуги, що надаються ключовим секторам, повинні бути безкоштовними.

4) Вирішення питань безпеки.

Здатність захищати приватний сектор дозволить вирішити численні проблеми, які можуть виникнути після втрати інформації, тим самим сприяючи зміцненню економічної, політичної та військової оборони країни.

Під час підготовки до процесу перевірки кваліфікації були поставлені такі завдання:

5) Аналіз актуальності захисту інформації в інформаційних мережах.

6) Класифікація інформаційних систем.

7) Дослідження сучасних методів захисту інформації в телекомунікаційних системах.

8) Аналіз та пропонування можливих рішень для захисту інформації в телекомунікаційних системах подвійного використання.

9) Об'єкт дослідження: Інформаційно-комунікаційні системи подвійного використання.

10) Тема дослідження: Захист інформації в інформаційно-комунікаційних системах подвійного використання.

11) Практична цінність: Результати дослідження можуть бути використані для розуміння важливості захисту інформації приватного сектору та допоможуть вирішити проблему захисту критичної інформації комерційних структур в інформаційно-комунікаційних системах подвійного використання.

Розділ 1
ІНФОРМАЦІЙНІ СИСТЕМИ ТА МЕРЕЖІ

1.1 Аналіз актуальності захисту інформації в інформаційних мережах

Сьогоднішній стрімкий розвиток суспільства вимагає використання інформаційних технологій у різних сферах життя. Це призводить до збільшення обсягу важливої інформації, такої як конфіденційна особиста інформація, інформація про виробництво чи технології тощо. Здатність негайно обмінюватися інформацією між людьми та державою має вирішальне значення як для людського життя, так і для бізнесу. Інформаційні системи та комунікаційні мережі повинні бути найефективнішим та найбезпечнішим способом використання мобільного зв'язку, комп'ютерів та глобальної мережі, включаючи телефонні лінії. Інформаційні системи характеризуються здатністю обслуговувати кількох людей або надавати численні послуги для текстових, зображень, відео, аудіо та інформаційних систем, які передаються або накопичуються. Система дозволяє передавати особисту інформацію. Завдяки цим технологічним можливостям збору інформації людство має швидкий прогрес у соціальному розвитку. Кожна країна на планеті та будь-яка сфера бізнесу завжди намагається використовувати різні інформаційні технології для підвищення якості своїх послуг, просування свого бізнесу чи підприємства. Це сприяє швидкому наданню необхідних нам послуг. Уряд може використовувати інформацію для захисту держави та її конфіденційної інформації. Обслуговування клієнтів та забезпечення задоволення їхніх потреб. Крім того, держава зазвичай володіє значним обсягом інформації та збирає статистику, яка може швидко надати інформацію органам влади про стан різних суспільних потреб. Крім того, використання інформаційних технологій сприяє збільшенню обсягу державного управління. Часто країни використовують різні інформаційні технології для захисту та досягнення цілей у міжнародній сфері [1, 2].

Неможливо описати глибокий вплив бізнесу на життя окремих людей, народів та економіки. Саме приватний сектор бізнесу в нашу епоху збільшує відсоток прибутку, що резервується до державного бюджету, надає високоякісні послуги людям та державі. Також неможливо ігнорувати той факт, що приватні компанії намагаються проводити наукові дослідження, щоб створювати нові ідеї, продукти та інші компоненти, необхідні для покращення життя людей, держави чи суспільства в цілому. [1, 2].

Втрата секретної інформації приватним сектором компанії може призвести до втрати різних технологій, що є частиною військової чи економічної галузей, а також втрата особистої інформації, яка є конфіденційною, може призвести до соціальних проблем, які можуть негативно вплинути на суспільство.

1.2 Телекомунікаційні мережі та їх класифікація

Комплекс технологічних засобів та структур, що використовують радіо-, оптичні або електронні системи для передачі письмового тексту, різних мультимедійних даних, сигналів або використовуються для спрямування трафіку, називається телекомунікаційною мережею.

Телекомунікаційна мережа, призначена для обслуговування як місцевих органів влади, так і державних службовців, називається мережею подвійного призначення. Одна частина ресурсу може бути виділена для надання послуг окремим споживачам.

Найпоширеніша категоризація телекомунікаційних мереж базується на таких критеріях: [2, 3].

За призначенням продукту.

2) За відомчою приналежністю.

3) За типом абонентських пристроїв.

4) Скільки підтримуваних комунікаційних послуг може бути використано?

5) За засобами передачі.

6) За кількістю протоколів та технологій, що використовуються в мережі.

7) За різними типами переходу.

8) За географічним регіоном.

9) За характером топології.

За цільовою функцією

Мережа, призначена для транспорту, або ядро мережі (магістраль або базова мережа), – це універсальна мережа, яка виконує транспортні функції та взаємодіє з іншими мережами через високошвидкісні канали. Транспортна мережа може включати [2, 3]:

1) Вузли, що виконують транзитні та комутаційні функції.

2) Кінцеві вузли, що надають абонентам дозвіл на доступ до транспорту мережі.

3) Індикаторні сервери, що обробляють сигнальну інформацію, з'єднують та керують викликами.

4) Шлюзи, що сприяють об'єднанню різнорідних, тобто апаратних та програмних засобів, нездатних взаємодіяти один з одним.

Сигнальні сервери можуть бути розміщені в окремих пристроях, що обслуговують кілька точок комутації. Використання спільних серверів дозволяє розглядати їх як єдину систему, розподілену по мережі. Це не тільки зменшує складність створення з'єднання, але й є найбільш практичним для постачальників послуг зв'язку, оскільки дозволяє замінити дорогі високопродуктивні комутатори невеликими, універсальними та бюджетними системами. [2,3]

Метою використання серверів, які можна розгорнути на окремих пристроях, є обслуговування кількох точок комутації. Використання спільних серверів дозволяє аналізувати їх як єдину мережеву комутаційну систему. Це спрощує як послідовність дій, необхідних для встановлення з'єднання, так і економічний характер самої системи зв'язку, що дозволяє замінити дорогі системи зв'язку на системи великої ємності, менші, доступніші та універсальні.

За асоціацією за відділом

Телекомунікаційні мережі класифікуються за відділом таким чином, щоб це сприяло ефективності та зниженню витрат.

Мережі зв'язку загального користування.

2) Спеціалізовані системи зв'язку.

3) Технічні мережі зв'язку.

4) Мережі спеціального призначення.

Мережа зв'язку загального користування (ПК) призначена для обслуговування будь-яких телекомунікаційних послуг будь-якому користувачеві. Мережа ПК для зв'язку - це комплекс, що включає кілька мереж зв'язку, які взаємодіють одна з одною, ці мережі призначені для розповсюдження телевізійних та радіопрограм.

Спеціалізовані технологічні, а також мережі зв'язку спеціального призначення є частиною групи обмеженого використання (LPN). Спеціалізовані мережі зв'язку - це мережі, що обслуговують певну аудиторію. Ці мережі можуть взаємодіяти одна з одною, але вони не підключені до загальнодоступного Інтернету.

Технічні комунікаційні мережі призначені для сприяння діяльності організації щодо технологічних процесів.

Спеціалізовані комунікаційні мережі використовуються для задоволення потреб державних органів, оборони, безпеки та правопорядку в країні.

За типом абонентських кінцевих користувачів

За типом абонентських пристроїв, що використовуються в ТКС, комунікаційні мережі поділяються на дві групи: [2, 3, 4].

1) Мережі постійного зв'язку, що з'єднують стаціонарних абонентів через постійні канали зв'язку.

2) Мережі мобільного зв'язку, що дозволяють з'єднання між мобільними (або транспортованими) абонентами.

Традиційно комунікаційні мережі для телекомунікацій поділяються на первинні та вторинні. Первинна мережа - це сукупність каналів і шляхів, що

утворюються обладнанням вузлів та лініями (або фізичними ланцюгами), що з'єднують ці вузли. Призначення первинної мережі полягає в передачі каналів (фізичних шляхів) до вторинної мережі, яка формуватиме комунікаційні шляхи. Вторинна мережа – це набір каналів зв'язку, що виводяться з первинної мережі шляхом комутації (маршрутизації) у вузлах, що складають вторинну мережу, та організації зв'язку між пристроями, що підписані на первинну мережу.

За кількістю підтримуваних протоколів зв'язку

За кількістю підтримуваних протоколів зв'язку мережі бувають [2,3,4]:

1) Односервісні, спочатку призначені для надання однієї послуги зв'язку (наприклад, радіомовлення, кабельне телебачення, громадський телефонний зв'язок, та передача даних загального користування).

2) Мультисервісна, яка призначена для забезпечення двох або більше комунікаційних послуг (наприклад, телефон, факс та різноманітні мультимедійні послуги).

Через середовище передачі

За способом передачі мережі можна додатково розділити:

1) Дротові (аналоговий та цифровий зв'язок; кабельний та волоконно-оптичний зв'язок).

2) Бездротові або радіомережі (стільникові, транкінгові та супутникові).

3) Комбіновані.

За кількістю протоколів та технологій, що використовуються в мережі.

За кількістю протоколів та технологій, що використовуються в мережі, TCS класифікуються як однорідні або гетерогенні, які також відомі як гетерогенні (багатопротокольні). Однорідні мережі зазвичай використовують одну комунікаційну технологію (IP, ATM, MPLS). Багатопротокольна мережа — комунікаційна платформа, яка забезпечує передачу різних типів інформації за допомогою різних технологій та типів протоколів. Для мереж, що включають кілька різних підмереж, часто використовується термін міжмережева мережа.

За типом переходу

За способом поділу мережі її класифікують на дві групи:

1) Незмінні.

2) Передані – канали, повідомлення, пакети передавались комутованим способом.

Коли відправник і одержувач обмінюються повідомленнями, фізичне з'єднання не формується, натомість вузли мережі служать буфером для повідомлень і надсилають їх у пріоритетному порядку певним шляхом.

За допомогою комутації пакетів повідомлення від користувачів розділяються на менші пакети-фрагменти, які потім передаються мережею. Кожен фрагмент орієнтований на обслуговування та містить інформацію про мережу та поле даних. У комутації пакетів використовуються два основні режими передачі даних.

1) Режим віртуального з'єднання, в якому між вузлами створюється та підтримується логічне з'єднання.

2) Режим дейтаграми (служба дейтаграм), в якому кожне повідомлення передається між компонентами мережі незалежно від іншого.

За секторною специфікою

За способом організації мережі вона поділяється на дві категорії: [2,3].

1) Національна магістральна мережа, яка зв'язується з телекомунікаційними вузлами країни в цілому та передає повідомлення через національні кордони.

Регіональні (або зональні) мережі, що будуються на території одного або кількох регіонів (груп регіонів) країни.

3) Регіональні мережі, що формуються на території адміністративної або іншої визначеної території та не пов'язані з жодною іншою мережею для зв'язку. Локальні мережі поділяються на міські та сільські.

4) Міжнародна мережа - загальнодоступна мережа, що підключена до комунікаційних мереж інших країн.

За характером топографії мережі

За характером топології мережі поділяються на дві категорії:

1) Повністю інтегровані, тобто мережі, в яких кожен вузол підключений до кожного іншого.

2) Повністю роз'єднані.

З великою кількістю вузлів повністю зв'язана мережа має велику кількість каналів зв'язку та її важко реалізувати через технічні проблеми та високі витрати. Як результат, більшість мереж не є повністю пов'язаними. Незважаючи на те, що при певній кількості вузлів у неповній мережі існує велика кількість можливих конфігурацій мережевих вузлів, на практиці зазвичай використовується кілька основних підходів до підключення мережевих вузлів (топологій)..

Класифікація за географічним розташуванням

Глобальні комунікації

Глобальні мережі характеризуються охопленням великих територій. Прикладом такого типу мережі є мережа, яка має кілька, сотні або навіть мільйони комп'ютерів, розподілених по великій площі. Ця функція використовується для з'єднання великих міст, регіонів або цілих штатів. Ці мережі мають численні переваги та недоліки порівняно з локальними мережами.

Швидкість обміну даними є однією з основних відмінностей між глобальними та локальними мережами. Ця різниця в глобальній мережі пояснюється наявністю швидких каналів обміну даними. Вони пропонують швидкість, порівнянну зі швидкістю комп'ютерних дисків або внутрішніх шин даних.

Глобальні мережі в основному використовуються для таких послуг, як отримання або надсилання електронної пошти, а також для надання послуг обміну файлами з обмеженою кількістю обмежень, пов'язаних з передачею файлів з віддалених серверів. Локальні мережі можуть надавати широкий спектр послуг, таких як друк, факс, електронна пошта тощо.

Швидкість глобальної мережі нижча через те, що проходження пакета може тривати кілька секунд, тоді як проходження локальної мережі триває лише мілісекунди.

Канали зв'язку в локальних мережах спільно використовуються кількома мережевими компонентами одночасно, проте глобальні мережі складаються з окремих компонентів, які працюють самостійно.

Одним із найсуттєвіших недоліків глобальної мережі порівняно з локальними є нерівномірний розподіл навантаження. У локальних мережах пакети передаються через Інтернет швидше, ніж у глобальних мережах, це пов'язано з тим, що локальні мережі менші за масштабом. Ефективність комутації пакетів демонструється здатністю передавати великі обсяги даних протягом певного періоду часу. Цей підхід також застосовний до глобальних комунікацій. Однак, поряд з ним у рівній мірі використовуються комутація каналів та нетрадиційні технології [5,6].

Значною перевагою глобальної мережі є її хороша масштабованість, яка розроблена для роботи з будь-якими топологіями, які можна визначити, тоді як локальні мережі мають узгодженість базових топологій, які можуть визначати довжину ліній та спосіб підключення станцій.

Міський зв'язок

Цей тип мережі призначений для обслуговування великого міста або мегаполіса. Ця мережа часто складається з волоконно-оптичних та цифрових ліній зв'язку, ці лінії забезпечують високу швидкість передачі даних.

Локальна спільнота

Локальна мережа характеризується складною структурою через кількість комп'ютерів, які можна підключити, та кількість людей, яких можна використовувати в обмеженому просторі. Її технології забезпечують передачу даних зі швидкістю від 10 Мбіт/с до кількох Гбіт/с. Створення локальної мережі, виділеної для комп'ютерів, пропонує користувачам значні переваги. Розробка протоколів для взаємодії з мережами та дослідження середовищ передачі даних позитивно вплинули на поширення цього типу мережі по

всьому світу. Можливість спільного доступу до периферійних пристроїв, інформації та комп'ютерів, сховищ даних та програмного забезпечення зробила цю мережу популярною в бізнесі, освіті та інших сферах. Локальні мережі мають розподіл даних. Дані в мережі розташовані на основному ПК та можуть бути доступні іншим комп'ютерам, які мають зв'язок з цією конкретною областю мережі. Розподіл ресурсів є однією з найбільш визнаних переваг. Це полегшує використання периферійних пристроїв, таких як факс або лазерний принтер, з мережею.

Кожен має можливість використовувати програми, встановлені на головному комп'ютері, але інтернет-версія цих програм повинна бути ефективною.

Наявність електронної пошти в локальних мережах полегшує отримання або передачу повідомлень для користувачів.

Основні обов'язки локальних мереж полягають у розподілі ресурсів. Це дозволяє користувачеві отримувати доступ до різних мережевих ресурсів та програмного забезпечення, а також використовувати їх незалежно від їхнього місцезнаходження.

Підвищення надійності мережі є однією з найпоширеніших причин існування мережі. Висока стабільність та надійність системи. Вихід з ладу одного комп'ютера не обов'язково призводить до значних проблем через можливість отримання інформації з інших комп'ютерів, пов'язаних з мережею.

Економія коштів є одним із компонентів створення мережі. Бажання витрачати менше грошей є однією з основних цілей створення мережі, тому використання менших комп'ютерів, які є економічно ефективними та мають більший діапазон можливостей, є більш доцільним. Економічна доцільність ідеї полягає в тому, що надання користувачам потужних персональних комп'ютерів або станцій, а також використання серверів для розміщення комп'ютерів, є значною економією коштів. Оскільки ідея реалізується у більшому масштабі, вартість на одного користувача знижується.

Здатність мережі забезпечувати потужну комунікаційну платформу, яка використовується учасниками мережі, є її найбільшим активом. Це полегшує діяльність певних груп працівників, члени яких можуть знаходитися будь-де, але вони мають можливість співпрацювати над одними й тими ж даними. Це полегшує негайну передачу змін користувачів іншим членам групи. Потенційне використання електронної пошти, електронних дощок для інформації та перекладу адрес під час телеконференцій. Це полегшує комунікацію між учасниками, незалежно від відстані між ними. Концентрація трафіку в цих невеликих регіонах є економічно вигідною, що є важливим компонентом створення цієї мережі. Комп'ютерна мережа відповідає за виконання завдань, що передбачають складні обчислення на інших віддалених потужних комп'ютерах, та отримання результату в графічному форматі на вашому комп'ютері або робочій станції.

Віртуальна мережа

Віртуальна приватна мережа — це загальний термін для віртуальних мереж, які створюються поверх інших мереж з нижчим ступенем довіри. VPN-тунель між двома вузлами дозволяє підключеному клієнту брати участь у віддаленій мережі та використовувати її ресурси — внутрішні сайти, комп'ютери, принтери та доступ до Інтернету. Безпека передачі інформації через загальнодоступні мережі досягається за допомогою шифрування, цей механізм створює канал для передачі інформації, ізольований від інших джерел. Технологія VPN дозволяє об'єднати кілька географічно розрізнених мереж (або окремих клієнтів) в єдину мережу, використовуючи незаплановані канали для зв'язку між ними. Багато постачальників пропонують як послуги підприємствам, які хочуть використовувати VPN, так і окремим особам, які хочуть отримати доступ до Інтернету. VPN — це клієнтська технологія, призначена для забезпечення безпечного зв'язку між серверами та клієнтами. Категоризація віртуальної мережі проілюстрована на рис. 1.1 [5,7].

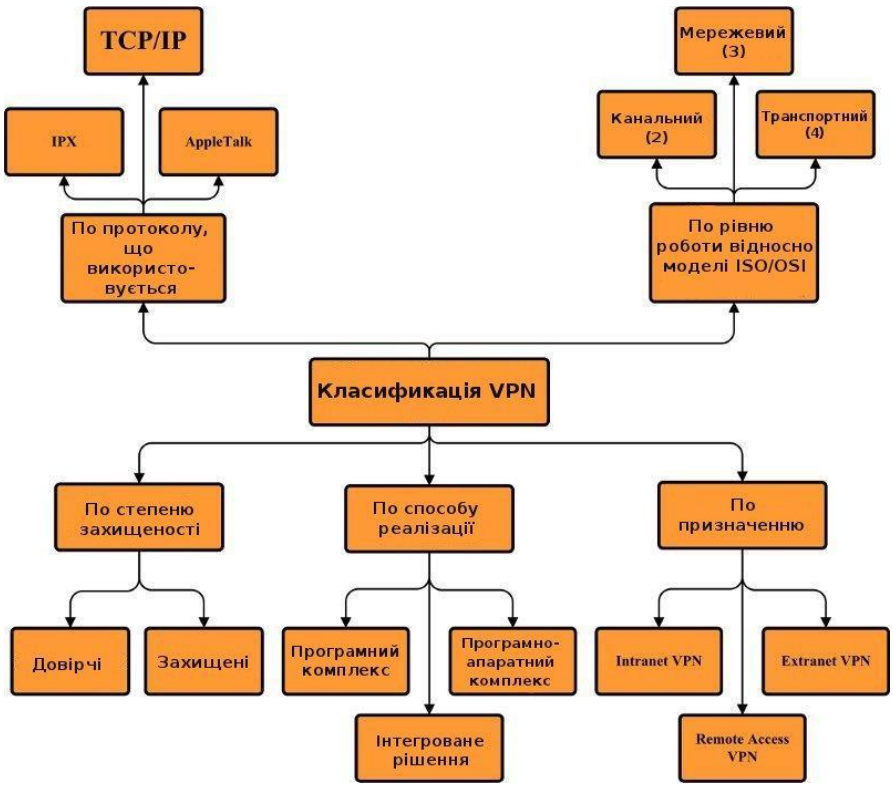


Рис. 1.1 Класифікація VPN [5]

Класифікація за топологією

Абонент

Підмножина мереж, що мають кілька компонентів: лінії передачі та комутаційні пристрої. Лінії передачі використовуються для передачі інформації між абонентами, тоді як комутаційні компоненти призначені для з'єднання кількох ліній передачі та є спеціалізованими комп'ютерами. Замість терміна, що комутує елементи, також використовується термін пакетний комутатор або комутаційний вузол. Ця підмережа може бути двох різних типів: або абонент-абонент, або широкомовні канали.

У цій мережі, яка комутується між абонентами, лінії передачі виділені одна одній, тому повідомлення або пакет передається від одного компонента до іншого через один або кілька проміжних вузлів. Цей пакет запам'ятовується, і коли потрібна лінія доступна, вона ретранслює пакет. Як результат, ці підмережі називаються буферними або пакетно-комутованими підмережами. Це поширено для багатьох глобальних мереж.

У менших мережах цього типу використання комутації каналів може поєднуватися з нею. Це поширено для глобальних мереж, які використовують телефонну мережу для передачі інформації. Фізичний зв'язок між джерелом повідомлення та його пунктом призначення створюється під час початку сеансу. У цьому випадку максимальна швидкість передачі даних не може перевищувати пропускну здатність встановленого каналу зв'язку.

Конфлікт між вимогами передачі даних та передачі голосу по телефонній мережі полягає в тому, що сеанс у телефонній мережі завжди створюється для однакової швидкості передачі даних через широкий характер голосового спектру в телефонії, проте необхідні швидкості передачі даних можуть значно відрізнятися. Результатом цього є використання інформаційної ємності каналу дуже неефективним чином [3,7].

Кільце

У цій конфігурації кожен вузол має лише два канали зв'язку з іншими вузлами. Сигнали в цій конфігурації передаються по колу та лише в одному напрямку, і кожен вузол їх отримує. На відміну від пасивної "канальної" конструкції, кожен вузол у цій конструкції функціонує як ретранслятор, який підсилює сигнали, а потім передає їх наступному вузлу. В результаті, якщо один з вузлів втрачається, вся мережа стає неактивною. Простий приклад проілюстровано на рис. 1.2.[5,6]

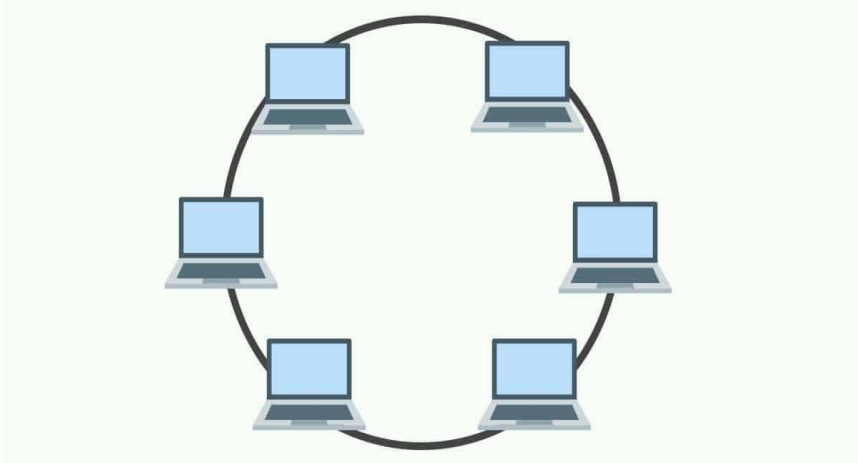


Рис. 1.2.1 Формат кільця

Дворівнева структура кільця

Подвійна кільцева топологія — це кільцева топологія, призначена для роботи в обох напрямках, тобто двонаправлена. Ця подвійна топологія дозволяє кожному доступному вузлу мати два зв'язки, кожне з яких знаходиться в іншому напрямку. Ця інформація може вказувати, чи можуть дані в цій топології рухатися за годинниковою стрілкою чи проти годинникової стрілки [6, 7].

Оскільки протокол базується на токенах, існує невелика ймовірність зіткнення пакетів, оскільки одночасно може передавати лише одна станція. Дані накопичуються з часом, що є корисним для конструкції кільця. Однак складність полягає в тому, що дані передаються з високою швидкістю через вузли, яку можна збільшити лише за рахунок додаткових вузлів.

Топології з подвійним кільцем можуть збільшити лінію захисту, роблячи їх більш стійкими до збоїв. Прикладом цього є те, що коли кільце біля основи вузла втрачається, інше кільце може функціонувати як підсилювач і генерувати додаткове джерело. Однією з переваг цієї топології є низька вартість встановлення. Приклад такої конфігурації показано на рис. 1.3.[5,7].

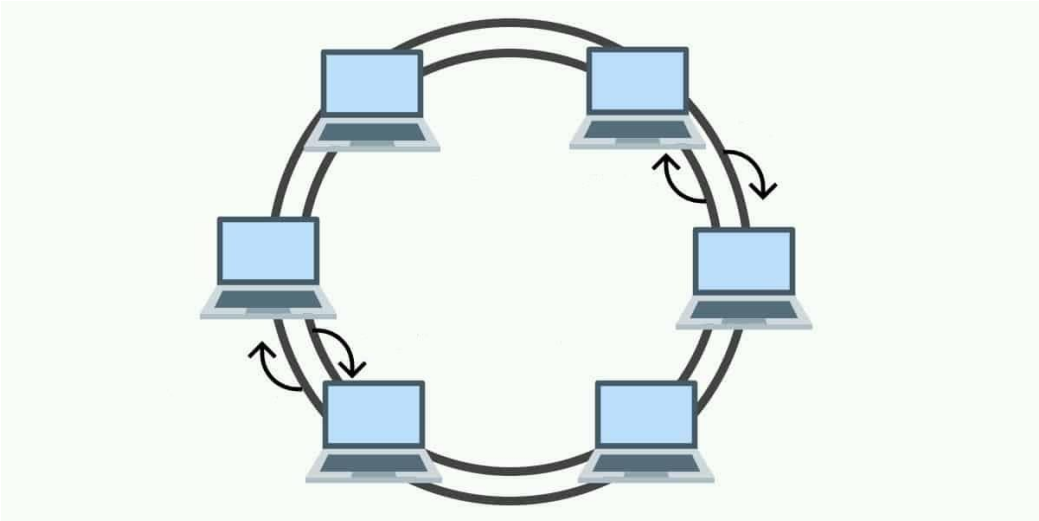


Рис. 1.3 Топологія «Подвійна кільцева топологія» [4]

С сітка

Компоненти цієї мережі індивідуально пов'язані з більшістю інших компонентів. Також немає центрального контролера чи комп'ютера, який міг би служити вузлом для зв'язку між абонентами для передачі даних.

Окрім цього, вона в основному складається з [7]:

повністю інтегрованої сітчастої структури

частково зв'язаних сітчастих топологій

У повністю зв'язаному графі всі вузли сітки одночасно підключені до кожного іншого вузла, тоді як у частково зв'язаному графі їх немає.

Така конструкція має кілька переваг:

Кожне посилання може здійснювати власну передачу даних

● Підвищує безпеку та секретність

Висока надійність

Топологічні недоліки:

Усі вищезазначені варіанти необхідно враховувати при масовому з'єднанні.

З більшою кількістю з'єднань зростає складність встановлення та налаштування.

У частково зв'язаній сітчастій мережі не всі вузли, які можна з'єднати один з одним, доступні. Схематичне зображення цієї топології показано на рис. 1.4.[5,7]

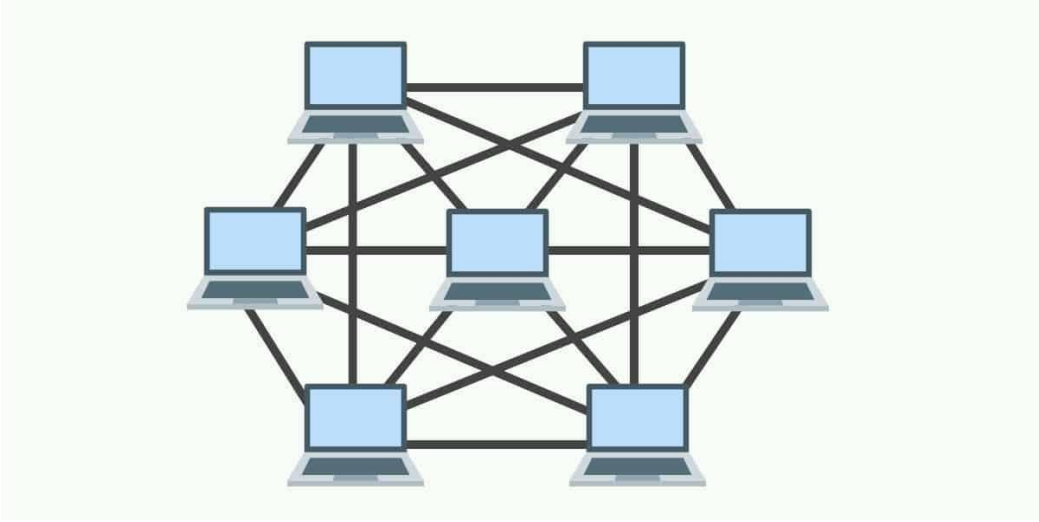


Рис. 1.4 Топологія «Сітка»[4]

Зірка

Зіркова топологія – це мережева конструкція, в якій кожен мережевий компонент підключено до одного центрального хаба. Кожен пристрій у мережі безпосередньо підключений до комутатора та опосередковано до всіх інших пристроїв. Зв'язок між цими компонентами полягає в тому, що центральним мережевим компонентом є сервер, а інші компоненти вважаються клієнтами. Центральна частина мережі відповідає за керування передачею даних і функціонує як ретранслятор. У зіркових конфігураціях комп'ютери підключені за допомогою коаксіального кабелю, крученої пари або волоконно-оптичного кабелю.

Перевага цієї топології полягає в тому, що до всієї мережі можна отримати доступ з одного місця: центрального контролера. Таким чином, якщо периферійний вузол, який не є центральним, буде втрачено, мережа все ще зможе функціонувати. Це пропонує зірковим топологіям засіб захисту від збоїв, який не завжди присутній в інших топологіях. Аналогічно, ви можете додавати нові комп'ютери до мережі, не відхиляючись від кільцевого формату. Це називається ad hoc мережею.

З точки зору фізичного дизайну, зіркові конфігурації мають менш суворі вимоги до дизайну кабелів, ніж інші конфігурації. Це полегшує їх встановлення та управління в довгостроковій перспективі. Загальна конструкція проста, що полегшує усунення неполадок.

Недоліком цієї конструкції є необхідність надання адміністратору контролю за стабільністю центральної платформи. Ефективність мережі також залежить від конфігурацій та продуктивності основного вузла. Зіркові топології прості в адмініструванні здебільшого, але вони далеко не економічно ефективні у створенні та використанні ресурсів.

Схематичне зображення цієї топології показано на рисунку 1.5.

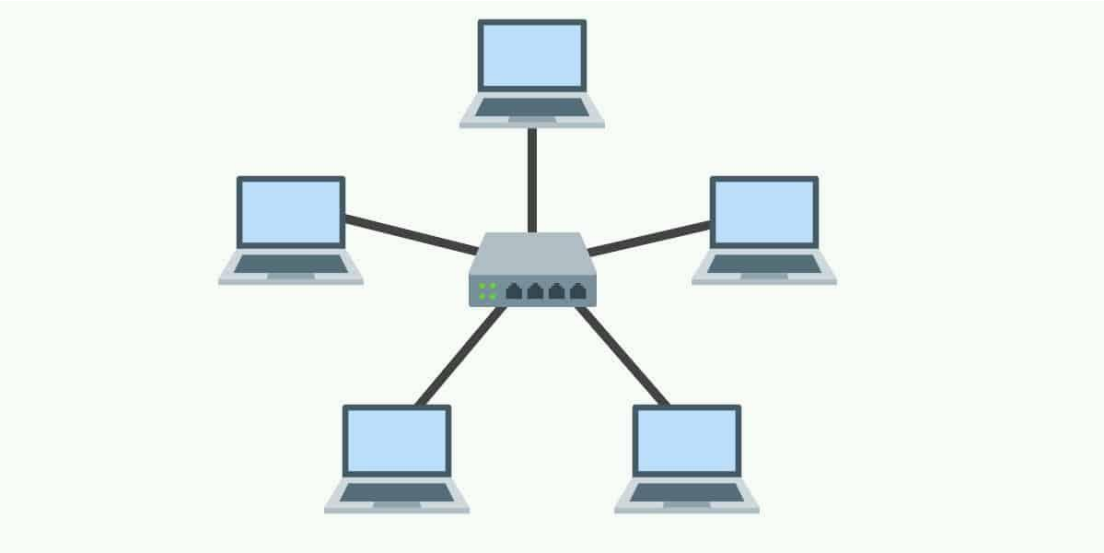


Рис. 1.5 Топологія «Зірка» [4]

Шина

У цій конфігурації кожен пристрій підключено до одного кабелю, який розгалужується від одного кінця мережі до іншого. Цей стиль топології часто називають лінійним. Цей транспортний засіб має один напрямок передачі даних.

У невеликих мережах цього типу для підключення пристроїв використовується коаксіальний кабель або кабель RJ45. Незважаючи на просту конструкцію та відсутність складного управління конфігурацією, ця топологія все ще є вигідною для використання, оскільки для запуску мережі потрібен один кабель, що сьогодні не використовується. Вихід з ладу кабелю є репрезентативним для всієї мережі, це займе багато часу та коштуватиме багато грошей. Іншим негативним аспектом є те, що швидкість передачі даних зростає зі збільшенням кількості з'єднань.

Зображення цієї топографії показано на рисунку 1.6 [8,9].

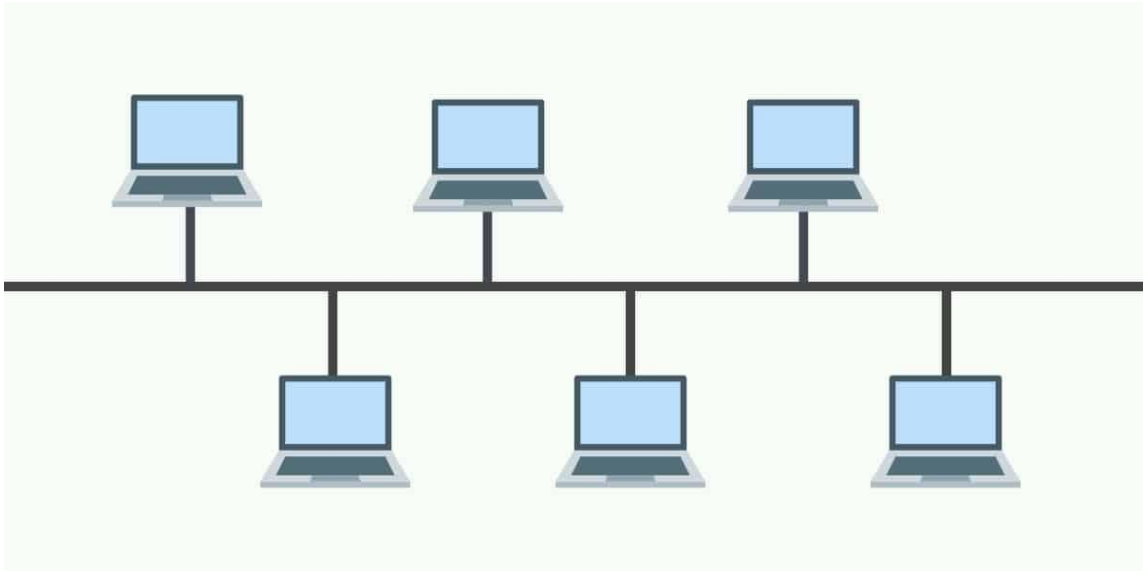


Рис. 1.6 Топологія «Шина» [4]

Топологія дерев

Цей дизайн є прикладом структури мережі. Він схожий на дерево з гілками, з топографією, що нагадує гору. Топології дерев мають один кореневий вузол, який з'єднаний з другим набором вузлів. Зв'язок у цій конфігурації можна описати як батьківський і дочірній об'єкти, які мають лише одне спільне з'єднання між собою. Визнано, що ця топологія повинна мати три рівні ієрархії, тому цей стиль використовується в глобальних мережах, які мають велику кількість пристроїв для підтримки.

Цей дизайн можна використовувати для розширення як зіркоподібної, так і шинної топології. Цей ієрархічний формат є корисним, оскільки він дозволяє додавати нові вузли, виявляти помилки та усувати несправності зі збільшенням розміру організації.

Одним з негативних аспектів є вихід з ладу кореневого вузла, якщо це станеться, підвузли стануть роз'єднаними. Незважаючи на це, в середині мережі буде частковий зв'язок, і чим більше вузлів, тим менш керованою буде мережа. Ще одним негативним аспектом топографії дерева є велика кількість необхідного кабелю. Для підключення кожного пристрою до найвищого рівня необхідно використовувати кабелі, що збільшує складність конструкції порівняно з простішою топологією. Зображення цієї топографії показано на

рисунку 1.7.

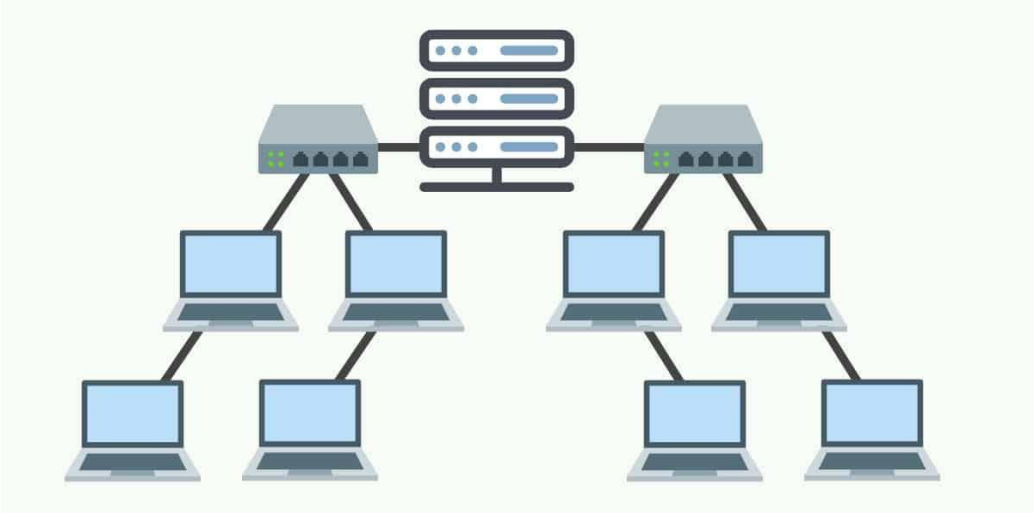


Рис. 1.7 Топологія «Дерев» [4]

Гібридна топологія

Якщо мережа має кілька різних топологій, вона називається гібридною мережею. Гібриди зазвичай зустрічаються у великих організаціях, які мають окремі відділи з мережевими топологіями, що відрізняються від інших відділів організації. Поєднання цих двох топологій створить гібридну топологію. Таким чином, можливості та вразливості залежать від типів топологій, пов'язаних одна з одною [4,9].

Об'єднуючи кілька топологій в одну гібридну конфігурацію, гібридні топології масштабуються, що, у свою чергу, робить їх придатними для великих мереж.

Існує багато причин, чому використовуються гібриди, але всі вони мають одну спільну властивість: гнучкість. У структурі існує кілька обмежень, які гібридна топологія не може врахувати, кілька топологій можна об'єднати в одну гібридну конфігурацію. Таким чином, гібридні мережі є дуже гнучкими. Масштабованість гібридних конфігурацій є вигідною для великих мереж.

Одним із негативних аспектів є складність управління мережею через необхідність підтримувати унікальні характеристики кожної мережі. Зображення цієї топографії показано на рисунку 1.8.[9]

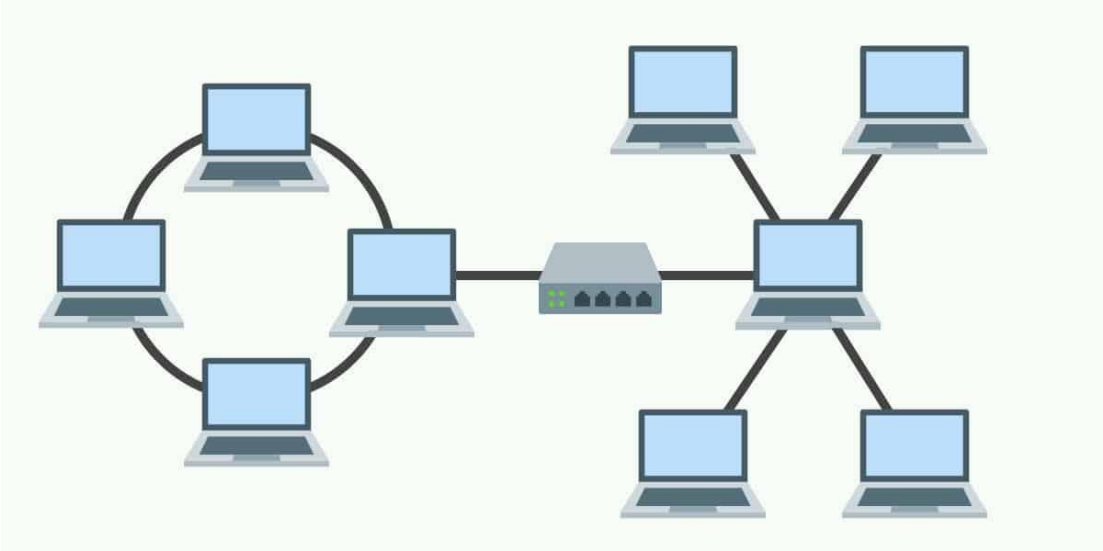


Рис. 1.8 Гібридна топологія [4]

1.3 Функції комунікаційних мереж.

Було визначено різні аспекти телекомунікаційних мереж, і ці аспекти певною мірою є актуальними [7,10].

Основна та найбільша роль телекомунікаційних мереж полягає в передачі інформації з одного місця в інше або на велику відстань та створенні інтерфейсу між відправником та одержувачем, все це може бути досягнуто за допомогою різноманітних середовищ. Оскільки станції та вузли можуть бути підключені до мережі.

2) Випадковим чином ця система вибирає найефективніші способи надсилання повідомлень цільовому одержувачу з мінімальним часом.

3) Передача інформації відбувається миттєво та найкоротшим шляхом за мінімальний час.

4) Ці системи також гарантують, що лише цільовий користувач отримує цільове повідомлення, а під час передачі також контролюються помилки.

5) Як загальновідомо, мережі використовують різне програмне та апаратне забезпечення для передачі інформації по каналах, які відрізняються в

різних середовищах, що призводить до того, що телекомунікації відповідають за перетворення та контроль швидкості передачі на платформу.

6) Він також може конвертувати повідомлення з одного формату в інший, оскільки інформація представлена по-різному на різних платформах.

7) Контролювати потік інформації, який залежить від методів зв'язку та інших факторів. В результаті ця система регулює їх обидва одночасно.

1.4 Приклади телекомунікаційних мереж

Прикладами комунікаційних мереж є телефони, доступ до Інтернету або підписка на кабельне телебачення.

1) Комунікаційні пристрої в телефонах, мікрохвильових печах, оптоволоконних пристроях, телеграфах, радіо, супутниках, а найбільш поширеним прикладом є Інтернет.

2) Багато людей вважають, що телекомунікації пов'язані з сучасними технологіями, проте вони також використовувалися як форма сигналу, що спричиняла появу диму.

3) Інші мобільні телефони, які мають можливість конференц-дзвінків, також вважаються телекомунікаційними пристроями.

4) Телекомунікаційні технології на Місяці полегшили зв'язок між людьми на Землі.

5) Для телекомунікацій використовуються супутники зв'язку. Різні супутникові телефони мають різні розміри, але всі вони потребують мережі супутників.

6) Для телекомунікацій можуть використовуватися клітинні вежі.

7) Телефон GSM - це стільниковий телефон.

8) Телекомунікаційні мережі сприяють дистанційному керуванню військовими підрозділами за допомогою комп'ютеризованих систем.

9) Геліограф — це оптичний комунікаційний пристрій, який використовує відбивну поверхню, що відбиває світло, що імітує запалювання лампочки.

1.5 Використання телекомунікаційних мереж

Нижче наведено перелік способів щоденного використання телекомунікаційних мереж (7, 10, 11).

1) Відстань зв'язку: Практика надсилання листів відійшла в минуле. Сьогодні спілкування з людьми з усіх куточків світу стало доступнішим, ніж будь-коли раніше. Люди можуть спілкуватися за допомогою телефонів, дзвінків, текстових повідомлень, електронних листів або соціальних мереж. Засоби зв'язку просто полегшили можливість підтримувати зв'язок з близькими на більш зручному, ефективному та економічно ефективному рівні.

2) Відпочинок: Розвиток телекомунікаційних технологій докорінно змінив ландшафт відпочинку. Сьогодні люди мають доступ до багатьох телевізійних станцій для перегляду новин, фільмів та музики. Соціальні мережі зазвичай використовуються для відпочинку, а також для обміну відео, зображеннями та короткими оповіданнями.

3) Соціалізація: Зі збільшенням кількості людей, які працюють та мають кар'єру, їм стає важко знайти час для спілкування. Однак збільшення кількості платформ соціальних мереж наразі заповнило цю прогалину для сучасного покоління. Сьогодні кожен може спілкуватися з новими людьми та заводити нових друзів через Facebook, Instagram та Twitter під час роботи. Інші

використовують Skype, Whatsapp, Google Hangouts та інші додатки для спілкування з іншими в режимі реального часу за допомогою відеодзвінків.

Використання телекомунікаційних мереж у банківській галузі задокументовано в цій дослідницькій роботі.

Сьогодні банки зв'язуються з кожним зі своїх клієнтів за допомогою телефонів або комп'ютерів. Клієнти можуть бажати перевірити баланс свого рахунку, обговорити з ними банківські продукти чи послуги або надати інформацію про свої рахунки чи транзакції. Через службу підтримки клієнтів банки можуть взаємодіяти з клієнтами та легко вирішувати їхні проблеми. Зараз також випускаються банківські додатки, які дозволяють клієнтам перевіряти свою фінансову історію, транзакції та баланси.

2) Мобільні банківські транзакції: Технології розвиваються щодня. Сьогодні люди можуть отримувати доступ до своїх банківських рахунків, знімати готівку, вносити кошти та перевіряти баланс за допомогою своїх мобільних телефонів. Інтеграція мобільних банківських додатків полегшила управління особистими рахунками та транзакціями.

3) Комбінований голосовий відповідач та менеджер повернення коштів: Комбінований голосовий відповідач (IVR) та менеджер повернення коштів – це дві важливі технології, що використовуються фінансовими установами. Практика інтегрованого голосового відповіді особливо корисна для банків, які хочуть забезпечити першокласну підтримку клієнтів. Впровадження управління зворотними дзвінками також може суттєво вплинути на підвищення ефективності банківської справи.

Використання телекомунікаційних мереж у бізнесі зростає [7,10,11].

Сьогодні компанії мають багато часу, який потрібно витрачати на комунікаційну логістику: раніше вони подорожували, щоб зустрітися з клієнтами, співробітниками чи партнерами. Тепер, завдяки телекомунікаційним технологіям, їм не потрібно нікуди їздити. Вони мають можливість проводити відеоконференції, розмовляти, керувати розмовами, а також брати участь в онлайн-зустрічах на комп'ютерах, телефонах чи інших пристроях.

2) Ділові розмови: З розвитком технологій компанії можуть взаємодіяти зі своїми виборцями за допомогою телефонних дзвінків, відеодзвінків або інтернет-зв'язку. Використання відеоконференцій полегшило проведення корпоративних зустрічей, таких як зустрічі масштабу компанії, зустрічі Google та хмарні зустрічі.

3) Міжнародні клієнти: Інтернет має значний вплив на зростання електронної комерції. Тепер компанії можуть рекламувати свої продукти та послуги через Інтернет, соціальні мережі, а також телебачення. Фізичні кордони між споживачами та бізнесом були скасовані, і компанії отримують більше доходів.

1.6 Переваги та недоліки телекомунікаційних мереж

1.6.1 Переваги телекомунікаційних систем

Переваги телекомунікаційних технологій перелічені в [7,10,11]:

1) Зниження витрат: Телекомунікації мають потенціал для зменшення витрат на ведення бізнесу. Безпаперові офіси, які використовують електронну пошту як основний засіб зв'язку, зменшують витрати на папір, друк, утилізацію та переробку. Надсилати електронні листи кільком клієнтам дорожче, ніж надсилати один електронний лист з однаковою інформацією кільком клієнтам. Як результат, телекомунікації допомагають заощаджувати гроші.

2) Скорочення часу: Сьогодні телекомунікаційні пристрої, такі як комп'ютери, мобільні телефони та факси, є поширеними, ці пристрої ефективніше надсилають повідомлення. Порівняно зі старим методом комунікації, який передбачав рукописне написання листів, інформація передавалася швидше за коротший проміжок часу.

3) Міжнародний клієнт: підключені до Інтернету інструменти, такі як Інтернет, дозволяють здійснювати електронну комерцію по всьому світу. Це

означає, що компанії можуть спілкуватися з більшою кількістю клієнтів за коротший проміжок часу в усьому світі. Крім того, телекомунікації можуть допомогти компанії збільшити дохід, обходячи географічні обмеження компаній та споживачів.

4) Покращена комунікаційна логістика: Компанії витрачають багато грошей і часу на спілкування з клієнтами. Завдяки телекомунікаційним методам, таким як телеконференції, зменшуються витрати та обмеження, пов'язані з логістикою. Телеконференції – це використання Інтернету та телефонної лінії для спілкування з людьми, які знаходяться далеко.

5) Підвищення швидкості прийняття рішень: Завдяки своїм телекомунікаційним характеристикам, телеконференції можуть бути швидшими, особливо для компаній, які мають міжнародні партнерства, оскільки клієнти можуть спілкуватися безпосередньо з партнерами, не маючи потреби подорожувати далеко або довго чекати на відповіді від іншої сторони.

6) Реклама: Маркетингові та рекламні кампанії мають вирішальне значення для багатьох компаній. Телемаркетингова реклама та методи маркетингу включають маркетинг у соціальних мережах, телефонний маркетинг та онлайн-рекламу. Ці кампанії поширюють інформацію про продукти серед ширшої аудиторії. Це може призвести до збільшення доходів та розширення клієнтської бази.

1.6.2 Недоліки телекомунікаційних систем

Переваги дистанційної роботи включають [7,10,11]:

1) Подовжений робочий час: Визнано, що дистанційні працівники мають вибір щодо того, скільки годин працювати протягом дня, але цей вибір призводить до того, що їм доводиться працювати постійно. Це спричинено відсутністю у дистанційних працівників можливості знайти хороший баланс між роботою та особистим життям, що призводить до необхідності обмежувати

позакласну діяльність, щоб вчасно завершити проект. Час, витрачений на планування дня, витрачається даремно і не може бути повернутий.

2) Зворотній зв'язок: Офісним працівникам пощастило отримувати негайний зворотний зв'язок протягом робочого дня, що дозволяє їм покращити свої зусилля. Легше регулювати важливі для вас речі, коли ви розумієте, як саме ваші плани сприймають інші, включаючи вашого роботодавця, ваших колег та клієнтів. Це включає негайні відповіді, які вони вам дають.

3) Логістика: Дистанційні працівники не зобов'язані планувати поїздку, але вони повинні зустрічатися з іншими в інших місцях, ніж в офісі. Ще однією складністю, пов’язаною з роботою з дому, є внутрішньоофісна електронна пошта, яку в цьому випадку вам не доставляє спеціальний співробітник, а натомість потрібно забрати з дому.

4) Емоційні зв’язки. Найбільшим недоліком дистанційної роботи є те, що співробітники в офісах часто користуються безкоштовними подарунками протягом дня, особливо з особливих нагод. Завдяки дистанційній роботі вони повинні знайти нове розуміння своєї корпорації.

1.7 Національна система конфіденційного зв'язку

Національна система конфіденційного зв'язку (України) – це спеціальна телекомунікаційна система (мережа) подвійного призначення, яка використовує криптографічні методи, а також технічні засоби для забезпечення передачі конфіденційної інформації в інтересах державних органів та органів місцевого самоврядування, що дозволяє цим органам взаємодіяти з системою як у звичайний час, так і у разі надзвичайного або воєнного стану.

Експлуатація системи в Державній службі спеціального зв'язку та захисту інформації делегована [7,10,11]:

1) Департаменту стратегії розвитку спеціальних інформаційно-телекомунікаційних систем.

2) Департаменту спеціальної інформації та телекомунікацій.

3) Державному підприємству "Українські спеціальні системи".

4) Створення та розвиток НСЗ має потенціал для вирішення наступних стратегічних питань:

5) Забезпечення захисту службової інформації відповідно до норм законодавства.

6) Створення умов для інтеграції розподілених інформаційних ресурсів та інформаційних систем для аналізу стану на різних рівнях управління з поширенням службової інформації.

7) Забезпечити можливість взаємодії інформації з аналітичними системами державних органів різних рівнів управління.

8) Забезпечити надійну передачу офіційної інформації між абонентами системи.

1.8 Висновки до першого розділу

У першій частині кваліфікаційного завдання було проведено дослідження важливості захисту інформації в бізнес-структурах. Було проведено категоризацію телекомунікаційних мереж. Було задокументовано можливості, а також переваги та недоліки телекомунікаційних систем. Це сприяло виявленню проблем, які могли виникнути, та забезпечило засоби для вибору найефективнішого рішення для вибору найкращого проекту мережі. Було задокументовано Національну систему конфіденційного зв'язку, її цільові функції та завдання.

РОЗДІЛ 2
ПРИНЦИПИ ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

2.1 Принципи, технології та обладнання комутації

2.1.1 Принципи побудови комутації

Комутація має вирішальне значення для зв'язку між вузлами, це дозволяє зменшити кількість необхідних ліній зв'язку, водночас збільшуючи обсяг каналів зв'язку. Надзвичайно важко виділити кожній парі вузлів виділену лінію зв'язку, тому мережі зазвичай використовують один із двох методів переходу абонентів, який використовує існуючі лінії зв'язку для передачі даних до різних вузлів. Для локальних мереж використовується комутація пакетів (всі дані, які передає користувач, розділяються на невеликі пакети – кадри). Кожен пакет супроводжується заголовком, який, щонайменше, ідентифікує адресу отримання вузла та номер пакета. Пакети передаються по мережі без урахування інших пакетів. Комутатори в цьому типі мережі мають внутрішній буфер, який зберігає пакети протягом короткого періоду часу, що забезпечує плавний потік інформації по лініях зв'язку між комутаторами. Комутатор локальної мережі підтримує таблицю, яка визначає, як трафік має пересилатися через комутатор. Ця таблиця підтримується у зв'язку з картою, що забезпечує швидкий пошук на високій швидкості. Як результат, таблиця MAC-адрес також відома як таблиця CAM. Комутатор переміщує трафік на основі номера вхідного порту та MAC-адреси призначення кадру. Комутатор складається з інтегральних схем та пов'язаного з ними програмного забезпечення, яке спрямовує потік даних через комутатор. Щоб комутатор розпізнав, який інтерфейс активувати для передачі кадру, він повинен спочатку дізнатися, які пристрої підключені до кожного інтерфейсу. Коли комутатор отримує кожен кадр Ethernet, використовується наступна двоетапна процедура [12].

Коли кожен кадр підтверджено, комутатор оновлює інформацію в ньому. Для цього він перевіряє MAC-адресу джерела кадру та номер інтерфейсу, через який він надійшов до комутатора. Якщо MAC-адреси джерела немає в таблиці MAC-адрес, адреса та пов'язаний номер вхідного каналу додаються до таблиці, або якщо адреса вже існує, комутатор оновлює таймер для цього запису. За замовчуванням більшість комутаторів зберігають запис у таблиці протягом п'яти хвилин. Якщо MAC-адреса джерела присутня в таблиці, але на іншому інтерфейсі, комутатор інтерпретує це як новий запис.

Якщо MAC-адреса призначення є одноадресною, комутатор зіставить місце призначення кадру з адресою в таблиці MAC-адрес, яка вже використовується.

Якщо MAC-адреса призначення вказана в таблиці, комутатор передасть кадр через призначений інтерфейс.

Якщо MAC-адреса призначення не вказана в таблиці, комутатор передасть кадр через усі інші інтерфейси, крім вхідного інтерфейсу.

Це називається невідомою одноадресною розсилкою. Якщо MAC-адреса призначення є широкомовною або багатоадресною адресою, кадр також передається через усі інтерфейси, крім вхідного інтерфейсу. У регіонах Ethernet на основі концентраторів пристрої в мережі намагаються використовувати спільне середовище. Сегменти мережі, які дозволяють пристроям використовувати спільну пропускну здатність, називаються доменами колізій. Якщо два або більше пристроїв в одній зоні колізій намагаються одночасно надсилати дані, відбудеться колізія: передача двох або більше кадрів від станцій, які намагаються передати кадр, буде об'єднана. У комутаторах на основі Ethernet ймовірність колізій визначається режимом роботи інтерфейсів комутатора. Коли інтерфейси комутатора працюють у повнодуплексному режимі, зони колізій відсутні. Коли комутатор використовує протокол Ethernet у напівдуплексному режимі, кожен сегмент знаходиться у власній області колізій. За замовчуванням комутатори Ethernet, що працюють у повнодуплексному режимі, мають пропускну здатність, що перевищує найвищу

доступну пропускну здатність для обох пристроїв. Якщо інтерфейс комутатора підключено до пристрою, такого як традиційний концентратор, який працює в напівдуплексному режимі, інтерфейс також працюватиме в напівдуплексному режимі. У цьому випадку інтерфейс комутатора буде частиною області колізій. Набір підключених комутаторів складається з одного домену широкомовлення, який включає всі пристрої в локальній мережі, що отримують широкомовні кадри від певного вузла. Коли комутатор отримує широкомовний кадр, він надсилає кадр з усіх своїх інтерфейсів, крім вхідного інтерфейсу. Вхідний інтерфейс - це інтерфейс, який отримав широкомовний кадр. Кожен пристрій, пов'язаний з комутатором, отримує копію широкомовного кадру та обробляє її. Тільки пристрій на мережевому рівні, такий як маршрутизатор, може розділити область широкомовлення на два рівні.[12,14]

2.1.2 Протоколи та технології комутації

Комутатори дуже швидко реагують на рішення протоколу 2-го рівня. Це зумовлено програмним забезпеченням, що працює на спеціалізованих інтегральних схемах. ASIC зменшують час, необхідний для обробки кадру на пристрої, і дозволяють пристрою мати більшу кількість кадрів без негативного впливу на продуктивність.

Метод збереження та пересилання – цей метод використовується, коли отримано повний кадр, і якщо він перевіряється на наявність помилок за допомогою математичного механізму, використовується циклічний код надмірності (CRC). Комутація з збереженням та пересиланням є основним методом комутації локальних мереж у продуктах Cisco.

Метод наскрізної комутації – у цьому методі процес пересилання починається після розпізнавання MAC-адреси пункту призначення вхідного кадру та вихідного інтерфейсу.

На відміну від наскрізного комутатора, збереження та пересилання має дві основні властивості:

1) Виявлення помилок – після отримання всього кадру комутатор перевіряє значення поля Послідовність перевірки кадру (FCS) в останньому полі на відповідність власним розрахункам. FCS – це процедура, яка виявляє фізичні помилки та помилки каналу в кадрі. Якщо проблем не виявлено, комутатор переміщує кадр вперед; в іншому випадку кадр відкидається.

2) Автоматична буферизація – процес буферизації інформації на вхідній стороні, який використовується комутаторами з переадресацією та збереженням, дозволяє підтримувати будь-яку швидкість Ethernet.

Наприклад, обробка вхідного кадру, що передається через Ethernet-канал зі швидкістю 100 Мбіт/с і призначений для надсилання на канал зі швидкістю 1 Гбіт/с, потребує комутатора з переадресацією та збереженням. Будь-яка невідповідність швидкості між вхідним та вихідним інтерфейсами призводить до того, що комутатор зберігає весь кадр у буфері, перевіряє FCS, а потім надсилає його до буфера вихідного інтерфейсу.

Метод переадресації та збереження перемикається через кадри, які не можуть пройти перевірку FCS. Як результат, він не поширює неправильні (помилкові) кадри. І навпаки, при наскрізній комутації існує можливість наявності невідповідних кадрів, оскільки перевірка FCS не виконується. У разі високого рівня помилок (недійсний кадр) у мережі, наскрізна комутація може негативно вплинути на пропускну здатність, спричиняючи надлишок пошкоджених та неефективних кадрів [12,14].

При наскрізній комутації комутатор може прийняти рішення про пересилання кадру, щойно він визначить адресу призначення кадру в таблиці MAC-адрес. Комутатору не потрібно чекати, поки решта компонентів кадру надходять до вхідного інтерфейсу, щоб прийняти рішення про пересилання чи ні. Як результат, наскрізна комутація здатна виконувати швидку ротацію кадрів. Завдяки низькій затримці, наскрізна комутація є більш ефективною для програм, які потребують багато ресурсів, ці процеси повинні мати затримку не

більше 10 мікросекунд.

2.1.3 Структуризація мереж

У локальних мережах з обмеженою кількістю комп'ютерів (10-30) найчастіше використовуються технології та структури, що забезпечують властивість однорідності, всі комп'ютери в мережі мають однаковий доступ до інших комп'ютерів. Така однорідність структури зменшує труднощі збільшення кількості комп'ютерів, полегшує обслуговування мережі та забезпечує безпеку.

Однак, під час створення великих мереж однорідний склад з'єднань стає шкідливим, а не корисним. У таких мережах використання типових структур має різні обмеження, найбільш суттєвими з яких є [14,15]:

1) Максимальна довжина з'єднання між вузлами обмежена.

2) Максимальна кількість вузлів у мережі обмежена.

3) Максимальна інтенсивність трафіку на кожному вузлі мережі обмежена.

Наприклад, технологія Ethernet на тонкому коаксіальному кабелі дозволяє використовувати кабель довжиною не більше 185 метрів, до якого можна підключити не більше 30 комп'ютерів. Однак, якщо комп'ютери інтенсивно обмінюються інформацією, іноді необхідно зменшити кількість комп'ютерів, підключених до кабелю, до 20 або навіть до 10, щоб кожен комп'ютер отримував відповідну частину загальної пропускної здатності мережі.

Щоб обійти ці обмеження, використовуються унікальні методи структурування мережі та спеціальне обладнання для створення структури – ретранслятори, концентратори, мости, комутатори та маршрутизатори. Це обладнання також називають комунікаційним, що означає, що окремі сегменти мережі взаємодіють один з одним через нього.

2.2. Адресування в телекомунікаційних та інформаційних мережах

Щоб розпізнати абонентів та визначити їхнє положення в мережі, кожному з них надається певна адреса. Адреса — це звичайна адреса, відома відправнику. Цієї інформації достатньо для передачі повідомлення цільовому одержувачу. Метод розподілу адрес, який враховує розташування та структуру мережі, називається методом адресації. Поточний стек мереж на основі протоколів використовує три різні адреси:

1) Регіональні (так звані апаратні фізичні адреси).

2) Мережеві (IP-адреси).

3) Символічні (доменні імена). Фізична локальна адреса — це адреса, призначена для надсилання інформації в межах локальної мережі (підмереж), яка складається з елементів складної мережі. Фізична локальна адреса — це MAC-адреса (Media Access Control), яка призначена для мережевих адаптерів та інтерфейсів маршрутизаторів, ПК та всіх інших мережевих компонентів. MAC-адреса заздалегідь визначена виробником обладнання та не є унікальною, оскільки вона централізована. Усі відомі технології локальних мереж (LAN) мають 48-бітну MAC-адресу (6 октетів), наприклад: 11-A0-17-3D-BC-01 [14,15].

MAC-адреса складається з двох окремих частин. Перша частина – це унікальна назва виробника обладнання (Organizationally Unique Name, OUN). Цей унікальний атрибут позначено IEEE як унікальний ідентифікатор виробника.

Останні 24 біти MAC-адреси визначені виробником обладнання. Перший байт MAC-адреси (I/G) вказує, чи є адреса індивідуальною чи колективною (14, 15):

1) 0 (персональна) – адреса, пов’язана з певним мережевим компонентом.

2) 1 (групова) – адреса, пов’язана з кількома або всіма вузлами певної мережі.

2.3. Принципи керування мережами

2.3.1 Задачі систем управління телекомунікаційних та інформаційних мереж

Система управління мережею виконує завдання надання адміністратору інформації про склад мережі з усіма з'єднаннями, інформацію про стан керованих об'єктів (кінцевих точок, ліній зв'язку та інтерфейсів комунікаційних пристроїв). Для вирішення цієї проблеми існують спеціалізовані пакети програмного забезпечення для управління, які зазвичай використовуються з обладнанням певного виробника.

Це приклади типів продуктів, що виробляються 3Com, Bay Networks та Heckle-Packard, а також обладнанням Spectrum та Nways Manager від IBM. Крім того, LanDesk - це продукт від Intel, який керує робочими станціями. Часто обов'язки з управління обмежуються комунікаційним обладнанням, і не все воно охоплюється. Зменшення обсягу зазвичай спричинене високою вартістю інструментів управління.

Завдання управління мережами [14,15]:

1) Вимірювання параметрів, що визначають пропускну здатність, час відгуку, кількість ліній тощо. Система контролює значення параметрів, обчислює їх середні (нормальні) значення, і коли будь-який з параметрів досягає критичного порогу, генерує попередження або автоматично виконує дії. Окрім моніторингу мережі, ця область управління також може активно змінювати мережу за допомогою генераторів трафіку (симуляторів трафіку). Це сприятиме оцінці поведінки мережі при збільшенні навантаження (наприклад, під час планування її розширення) та ініціюватиме необхідні дії для забезпечення компетентної роботи.

2) Відстежувати інформацію щодо апаратних та програмних компонентів складових елементів мережі, включаючи тип та версію продуктів, їх налаштування тощо. Це також передбачає взяття під контроль загальної функції пристроїв та налаштування їх інтерфейсу.

3) Облік трафіку на кожному окремому вузлі та їх сукупності безпосередньо впливає як на розподіл мережевих ресурсів, так і на визначення оплати за надані послуги.

4) Виявлення та документування збоїв, призначених для повідомлення адміністратору та відновлення функціональності. З появою симптомів збою система повинна ізолювати зону проблеми, використовувати додаткові компоненти, реєструвати події та відновлювати початкову конфігурацію після виправлення збоїв.

5) Контроль доступу до мережевих ресурсів: авторизація користувачів, захист від несанкціонованого доступу, запобігання блокуванню мережі (навмисному чи ненавмисному).

Для досягнення цих цілей система керування системою функціонує наступним чином:

1) Контроль конфігурації.

2) Управління якістю.

3) Усунення несправностей керування.

4) Математичне керування.

5) Контроль безпеки.

Контроль конфігурації пов'язаний з:

1) Отриманням, збереженням та відображенням інформації про мережеві компоненти (їх типи, розташування, унікальні ідентифікатори тощо).

2) Включенням компонентів в роботу та їх випуском.

3) Створенням та зміною логічних зв'язків між компонентами.

Управління продуктивністю пов'язане з підтримкою необхідної якості основних властивостей мережі. Управління несправностями включає такі кроки: 1) Локалізація та розпізнавання несправностей у мережі.

2) Виявлення помилок та надання відповідної інформації обслуговуючому персоналу.

3) Надання рекомендацій щодо усунення несправностей.

4) Управління виставленням рахунків:

5) Спостереження за ступенем використання мережевих ресурсів.

6) Сприяння функції нарахування плати за цю мету.

2.3.2 Реалізація задач маршрутизації в телекомунікаційних мережах

Процедура вибору шляху (маршруту) для переміщення об'єктів (пакетів) від джерела до місця призначення називається маршрутизацією. Своєчасна та надійна доставка повідомлень (пакетів), а також навантаження на центральні офіси (маршрутизатори) в першу чергу залежить від ефективності використовуваних алгоритмів маршрутизації. У мережах, що перемикаються між каналами, алгоритм, що визначає шляхи (маршрути), впливає лише на етап формування з'єднання. У мережах, що перемикають пакети, алгоритм маршрутизації визначає шлях (маршрут) для кожного повідомлення (пакета) окремо або для серії повідомлень (пакетів). Принцип руху (передачі) використовується для розрізнення спрямованих та ненаправлених методів маршрутизації. Направлена маршрутизація - послідовно вибирає найбільш підходящий маршрут на основі прийнятих критеріїв. Для цього використовуються таблиці маршрутизації, які формуються відповідними протоколами маршрутизації (динамічні маршрути), а замість статичних маршрутів створюються адміністратором мережі. У свою чергу, за способом формування таблиць маршрутизації, методи спрямованої маршрутизації поділяються на детерміновані (фіксовані) та адаптивні. Детерміністичний метод припускає, що центри мають фіксовану (статичну) таблицю шляхів і що вони забезпечують один шлях передачі для кожного напрямку зв'язку. Вони також не використовують інші наразі використовувані шляхи передачі. Цей підхід підходить для мереж з низьким обсягом трафіку. Адаптивний метод дозволяє

слідувати різними шляхами в кожному центрі обертання (ровері) на основі його навантаження та стану його з'єднань.

Дані, необхідні для вибору шляху передачі (маршруту) в певний момент часу, знаходяться в [14, 15]:

1) У попередньому списку маршрутів, який був складений у комутаційному центрі (маршрутизаторі).

2) Технічні характеристики вихідних каналів.

Довжина черг, що очікують передачі на кожному каналі.

Маршрут з найбільшою ефективністю вибирається за допомогою обчислень, які задовольняють вимоги передачі за певним критерієм.

Адаптивний метод складається з таких кроків:

1) Локальна адаптивна маршрутизація, яка базується на інформації, доступній у його місці розташування, для вибору шляху (маршруту) в кожному центрі, що комутується.

2) Розподілена адаптивна маршрутизація, за якої інформація про маршрут розподіляється та реалізується пристроєм, що має атрибути централізованої маршрутизації.

Спрямована маршрутизація – не існує універсального алгоритму, який визначає, як надсилати (пакетувати) повідомлення через мережу. Цей метод маршрутизації доцільний за відсутності інформації щодо структури комунікаційної мережі. У цьому випадку немає протоколів для комутації маршрутів у центрах, які перемикають маршрути. Метод генерації маршрутів передбачає створення маршрутів, які є непередбаченими або випадковими.

У лавинному методі інформація з центрів, що перемикають (маршрутизаторів), ретранслюється у всіх напрямках, пов'язаних з ними, крім каналу, через який ця інформація надійшла до центру.

За допомогою випадкового перемикання каналів повідомлення може бути надіслано на будь-який з вихідних інтерфейсів (каналів). За допомогою методів, які не вимагають напрямку, не потрібно знати топографію мережі. Цей тип маршрутизації вигідний для використання в мережах з низьким навантаженням

і потребують стабільності, поки інші компоненти виходять з ладу.

2.4 Висновки до другого розділу

У другій частині кваліфікаційного завдання вивчалися принципи експлуатації телекомунікаційних та інформаційних мереж. Розглядалися фундаментальні принципи передачі інформації та управління мережами. Адресація та організація телекомунікаційних мереж.

Розділ 3

СУЧАСНІ ВИДИ ТА МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

3.1 Види захисту ІТС

Брандмауер — це програмна або апаратна система, яка запобігає доступу хакерів або шкідливих програм до комп'ютера через Інтернет або мережу. Для цього брандмауер контролює дані з Інтернету або мережі та визначає, чи слід їх передавати на комп'ютер. Це більш чітко показано на рис. 3.1[11,14].

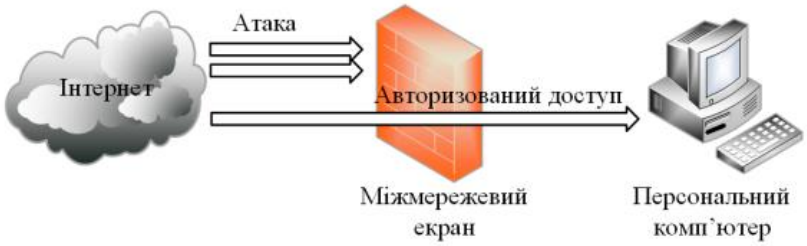


Рис. 1. Схема роботи міжмережевого екрану[11]

VPN-з'єднання між мережами (логічні з'єднання) дозволяють організаціям створювати маршрути, що з'єднують окремі офіси або інші організації із загальнодоступною мережею, забезпечуючи при цьому безпеку зв'язку. Це показано на рис. 3.1[11,14].

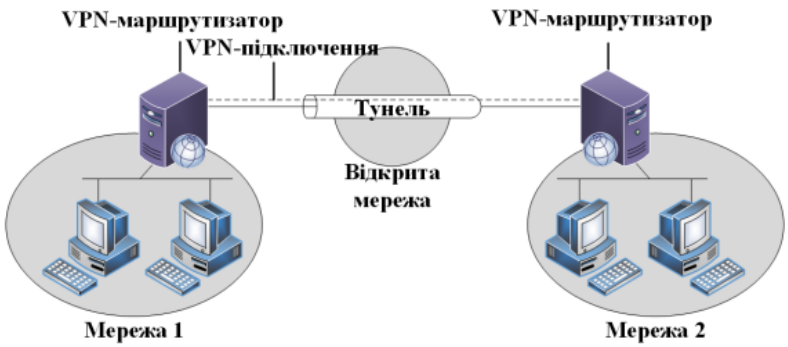


Рис. 2. Організація VPN-з’єднання двох віддалених вузлів[11]

SVV є software або hardware device that is used to recognize the presence of

unuthorized access to computer system (interaction) or the control of this system by someone other that the authorized user. SZV є надійною системою для програмного забезпечення або hardware, що помилки, які використовуються, є, якщо він є визнаним.

3.2 Криптографічні засоби захисту

3.2.1 Визначення криптографічного захисту

Криптографія – це дисципліна, яка використовує найновіші досягнення фундаментальної науки, і в першу чергу стосується математики. І навпаки, всі конкретні аспекти криптографії залежать від ступеня розвитку технологій та інженерії, використовуваних засобів зв'язку та способу передачі інформації.

Криптографія займається методами перекладу інформації, які не дозволяють зловмиснику відокремити її від повідомлень, що контролюються. У цьому випадку захищається не сама інформація, а результат її перетворення за допомогою шифру, який зловмисник повинен розпізнати.

Тобто, криптографія повинна гарантувати, що ця інформація захищена таким чином, що навіть якщо вона була зламана або оброблена комп'ютерами та новітніми науковими досягненнями, вона не буде розшифрована протягом понад десяти років.

Шифрування – це процедура зміни інформації таким чином, щоб її вміст більше не був зрозумілим для людей, які не мають права на це.

Дешифрування – це процедура отримання інформації із зашифрованого тексту.

3.2.2 методи шифрування

Криптографія є важливою для надання щонайменше трьох послуг безпеки:

1) Шифрування.

2) Контроль цілісності.

3) Автентифікація.

Шифрування є найефективнішим методом забезпечення секретності. Воно розташоване в центрі багатьох програмних та технічних правил безпеки, є основою для реалізації багатьох з них, і водночас є останньою (а іноді й єдиною) лінією захисту. Для портативних комп'ютерів лише шифрування забезпечує конфіденційність даних незалежно від крадіжки.

На практиці для захисту інформації використовуються як симетричні, так і асиметричні методи шифрування.

Метод симетричного шифрування використовує один секретний ключ, який використовується як для шифрування, так і для дешифрування даних.

Були створені ефективні (швидкі та надійні) симетричні криптосистеми. Також існують національні рекомендації щодо перетворення криптографічних алгоритмів. Рисунок, що ілюструє процедуру використання методу симетричного шифрування, зображено на рис. 3.1 [14,15].

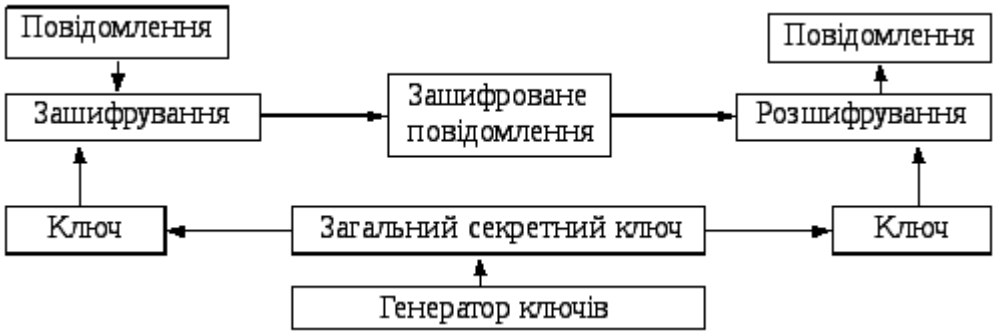


Рис. 3.1 Схема використання методу симетричного шифрування

Фактично, асиметрична криптографія використовує підклас односторонніх функцій – тих, що мають додаткові кроки, ці функції називаються односторонніми функціями з обходами. Однак, обернену функцію можна визначити просто як пряму функцію, якщо відома спеціальна інформація про обходи. Ця унікальна інформація функціонує як секретний ключ [9,15].

Асиметричні криптосистеми використовують два різні ключі. Один з них є незахищеним (його можна опублікувати разом з іншою загальнодоступною

інформацією про користувача), він використовується для шифрування інформації, інший є секретним (відомим лише одержувачу), він використовується для дешифрування інформації. Схема використання асиметричного криптографічного методу проілюстрована на рис. 3.2. [14,15].

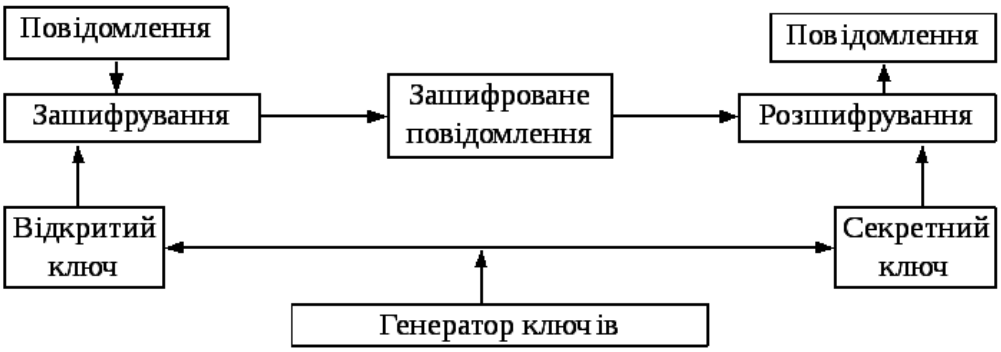


Рис. 3.2 Схема використання методу асиметричного шифрування

Найбільш відомими асиметричними криптографічними системами є криптосистеми RSA (Рівеста, Шаміра, Адлемана), Діффе-Хеллмана, Ель-Гамаля та еліптичних кривих (9, 15).

Найпоширеніші способи використання асиметричних криптосистем такі:

1) Передача конфіденційного ключа симетричного шифрування через відкриту мережу (відправник шифрує цей ключ за допомогою відкритого ключа одержувача, який може розшифрувати отримане повідомлення лише за допомогою свого секретного ключа).

2) Електронні цифрові підписи, захищені секретним ключем автора (автор документа засвідчує легітимність документа за допомогою свого особистого ключа, після чого будь-який інший власник секретного ключа може перевірити справжність документа).

Асиметричний криптоаналіз також сприяв вирішенню важливого завдання створення спільних секретів (це критично важливо, якщо сторони не довіряють одна одній). Це важливо для того, щоб сеанс взаємодії розпочався без необхідності обміну секретами.

Однак, сучасні асиметричні криптосистеми не можуть бути повністю замінені симетричними криптосистемами з таких причин:

Тривала тривалість процесів шифрування та дешифрування (понад у 1000 разів довша, ніж при симетричному шифруванні).

2) Необхідність використання значно довшого ключа шифрування для забезпечення того ж рівня криптографічної стійкості шифру (наприклад, симетричний ключ 56 бітів еквівалентний асиметричному ключу 384 біти, а симетричний ключ 112 бітів еквівалентний асиметричному ключу 1792 біти) [14,15].

3.3 Сучасні комплекси технічного захисту інформації

В Україні численні компанії мають дозвіл на створення комплексу інформаційних засобів, проте найпопулярнішими є «Криптон» та «Трітел».

Криптографічний захист – це форма захисту, яка передбачає перетворення інформації на спеціальні дані (ключові дані) з метою приховування (або відновлення) змісту інформації, перевірки її автентичності, цілісності, авторства тощо.[1,14]. Розглянемо товари, що виробляються компанією «Трітел».

Avalanche

Система криптографічного захисту інформації компанії "Trytel"

Цей комплекс складається з таких компонентів [1,14]:

● Шифрувальник О371

Пристрій генерації ключових даних О372.

Централізована система керування (ЦСК)

Шифрувальник призначений для захисту конфіденційності трафіку у високопродуктивних IP-мережах, а також використовується для забезпечення безпеки дротового, супутникового, радіо та стільникового (3G, 4G) зв'язку.

Основний пристрій, що генерує дані, призначений для зберігання, розподілу та генерації важливої інформації. [1,14]

Централізована система керування (ЦСК) призначена для дистанційного керування зашифрованим мережевим зв'язком. [1,14]

Зображення показано на рис. 3.3.

Рис. 3.3 Зовнішній вигляд КЗІ «Лавина»

Цей комплекс має такі можливості: [1, 14]

1) Кодування IP-мережевого трафіку, що проходить.

Шифрування трафіку використовується на зовнішній стороні периметра локальної мережі. Обробка криптографічної інформації в онлайн-режимі називається «прозорою», це досягається за допомогою програм обробки даних, IP-телефонії та відеоконференцій.

2) Віртуальні канали для зашифрованого зв'язку.

Під час передачі зашифрованої інформації формуються віртуальні канали зв'язку за схемою, запропонованою адміністратором комплексу.

3) Фіксація каналу.

Для кожного напрямку зв'язку можна встановити кілька віртуальних каналів з різними шляхами, що забезпечує узгодженість каналів зв'язку.

4) Система ключів.

Основна система відповідає за підготовку та поширення важливої інформації. Коли пристрій О372 генерує важливі дані, використовуються фізичні датчики, що відповідають стандарту FIPS 140-2. Розповсюдження програмного забезпечення здійснюється двома способами: через зашифровану мережу зв'язку та/або за даними, що мають ключі.

5) Апаратна реалізація криптографічного модуля.

Функції перетворення, що є криптографічними, виконуються спеціалізованими мікроелектронними схемами, які були продубльовані, що збільшує обсяг даних, що оброблюються, та забезпечує їх шифрування.

Балансування навантаження каналів.

Віртуальні канали можна об'єднувати в кластери для вирівнювання навантаження на вузли мережі та збільшення швидкості потоку через мережу.

7) Наявність кількох однакових або подібних пристроїв.

Обладнання може бути повторене з метою "гарячого" резервного копіювання та агрегації пропускної здатності.

8) Відстеження та керування.

Моніторинг та керування обладнанням здійснюється як локально, так і віддалено, з використанням централізованої системи CSC. Програмне забезпечення CSC встановлюється на комп'ютер під керуванням ОС Windows і дозволяє керувати режимом роботи обладнання, змінювати конфігурацію параметрів, переглядати статистичну інформацію, реєструвати та обробляти повідомлення щодо подій у мережі зашифрованого зв'язку. Безпека обладнання підвищується завдяки двофакторній автентифікації [1,14].

Схема процедури продемонстрована на рис. 3.4.

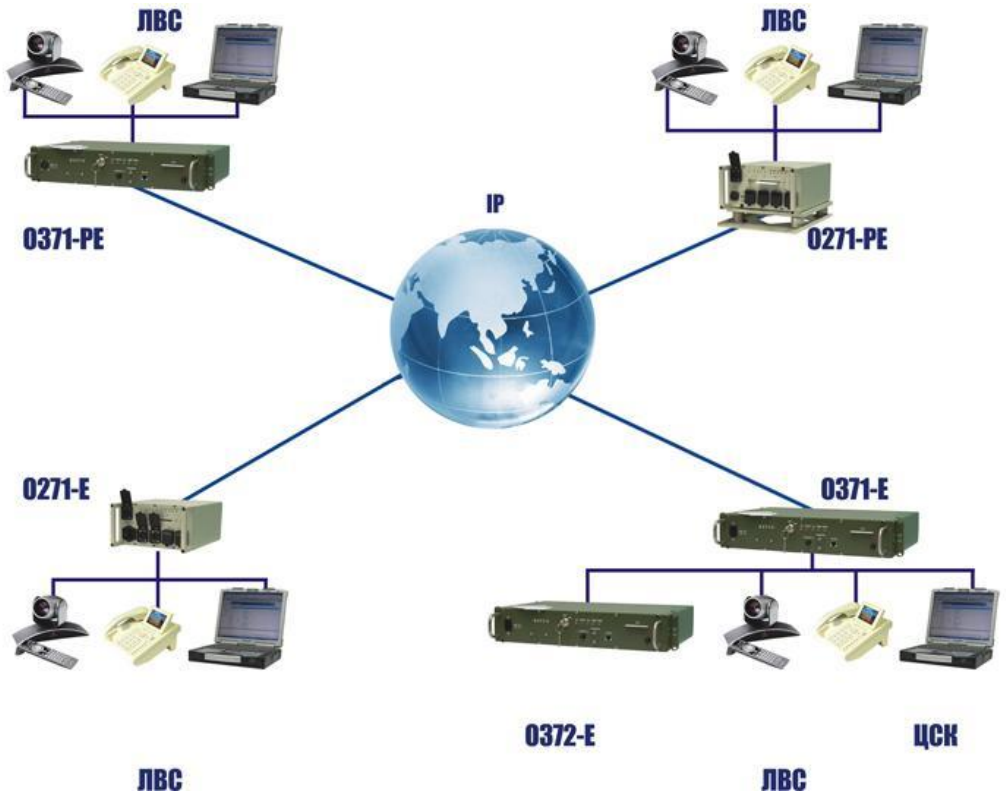


Рис. 3.4 Схема застосування «Лавина»

Triton

Криптор, який перемикається між різними режимами за допомогою інтегрованого модуля на базі Tritel.

Шифратор з інтегрованим модулем комутації, розроблений для захисту найвищого рівня безпеки IP-трафіку, – це О271. Внутрішній керований комутатор дозволяє підключати обладнання, підключене до мережі, безпосередньо до шифратора. Його призначення – захист дротових, супутникових, радіо та стільникових (3G, 4G) каналів зв'язку.

Зображення показано на рис. 3.5.

Рис. 3.5 Зовнішній вигляд шифратора «Тритон»

Цей комплекс має такі можливості: [1, 14]

1) Кодування IP-мережевого трафіку, що проходить.

Шифрування трафіку використовується на зовнішній стороні периметра локальної мережі. Обробка криптографічної інформації в онлайн-режимі називається «прозорою», це досягається за допомогою програм обробки даних, IP-телефонії та відеоконференцій.

2) Віртуальні канали для зашифрованого зв'язку.

Під час передачі зашифрованої інформації формуються віртуальні канали зв'язку за схемою, запропонованою адміністратором комплексу.

3) Фіксація каналу.

Для кожного напрямку зв'язку можна встановити кілька віртуальних каналів з різними шляхами, що забезпечує узгодженість каналів зв'язку.

4) Система ключів.

Основна система відповідає за підготовку та поширення важливої інформації. Коли пристрій О372-Е генерує важливі дані, використовуються фізичні датчики, що відповідають стандарту FIPS 140-2. Розповсюдження програмного забезпечення здійснюється двома способами: через зашифровану мережу зв'язку та/або за даними, що мають ключі.

5) Апаратна реалізація криптографічного модуля.

Функції перетворення, що є криптографічними, виконуються спеціалізованими мікроелектронними схемами, які були продубльовані, що збільшує обсяг даних, що оброблюються, та забезпечує їх шифрування.

Балансування навантаження каналів.

Віртуальні канали можна об'єднувати в кластери для вирівнювання навантаження на вузли мережі та збільшення швидкості потоку через мережу.

7) Наявність кількох однакових або подібних пристроїв.

Обладнання можна повторювати з метою "гарячого" резервного копіювання та агрегації пропускної здатності.

8) Відстеження та керування.

Моніторинг та керування обладнанням здійснюється як локально, так і віддалено, і для цього використовується централізована система CSC.

Схема застосунку проілюстрована на рис. 3.6.

Рис 3.6 Схема застосування «Тритон»[1]

Skat

Шифрувальник, що поєднує модуль перетворення інформації з криптографічним модулем.

Шифрувальник поєднує безпеку криптографічного ключа з перетворенням голосової інформації в цифрову. Це дозволяє захищати голосову інформацію та передавати її через високоякісні IP-мережі. Внутрішній модуль перетворення голосової інформації може використовуватися для підключення телефонної трубки або гарнітури до шифрувальника. Призначений для використання на стаціонарних та портативних об'єктах. Підтримується криптографічними системами О371, О271. Забезпечує можливість використання дротових, супутникових, радіо-, стільникових (3G, 4G) та KH/VHF комунікаційних пристроїв [1,14].

Зображення показано на рис. 3.7.

Рис. 3.7 Зовнішній вигляд шифратора «Скат» [1]

Цей комплекс має такі можливості: [1, 14]

1) Кодування IP-мережевого трафіку, що проходить.

Шифрування трафіку використовується на зовнішній стороні периметра локальної мережі. Обробка криптографічної інформації в онлайн-режимі

називається «прозорою», це досягається за допомогою програм обробки даних, IP-телефонії та відеоконференцій.

2) Віртуальні канали для зашифрованого зв'язку.

Під час передачі зашифрованої інформації формуються віртуальні канали зв'язку за схемою, запропонованою адміністратором комплексу.

3) Фіксація каналу.

Для кожного напрямку зв'язку можна встановити кілька віртуальних каналів з різними шляхами, що забезпечує узгодженість каналів зв'язку.

4) Система ключів.

Основна система відповідає за підготовку та поширення важливої інформації. Коли пристрій О372-Е генерує важливі дані, використовуються фізичні датчики, що відповідають стандарту FIPS 140-2. Розповсюдження програмного забезпечення здійснюється двома способами: через зашифровану мережу зв'язку та/або за даними, що мають ключі.

5) Апаратна реалізація криптографічного модуля.

Функції перетворення, що є криптографічними, виконуються спеціалізованими мікроелектронними схемами, які були продубльовані, що збільшує обсяг даних, що оброблюються, та забезпечує їх шифрування.

Балансування навантаження каналів.

Віртуальні канали можуть бути об'єднані в кластери для вирівнювання навантаження на вузли мережі та збільшення швидкості потоку через мережу.

7) Наявність кількох однакових або подібних пристроїв.

Обладнання може бути повторене з метою "гарячого" резервного копіювання та агрегації пропускної здатності.

8) Відстеження та керування.

Моніторинг та керування обладнанням здійснюється як локально, так і віддалено, з використанням централізованої системи CSC. Програмне забезпечення CSC встановлюється на комп'ютер під керуванням ОС Windows і дозволяє керувати режимом роботи обладнання, змінювати конфігурацію параметрів, переглядати статистичну інформацію, реєструвати та обробляти

повідомлення щодо подій у мережі зашифрованого зв'язку. Безпека обладнання підвищується завдяки двофакторній автентифікації [1,14].

Схема процедури продемонстрована на рис. 3.8.

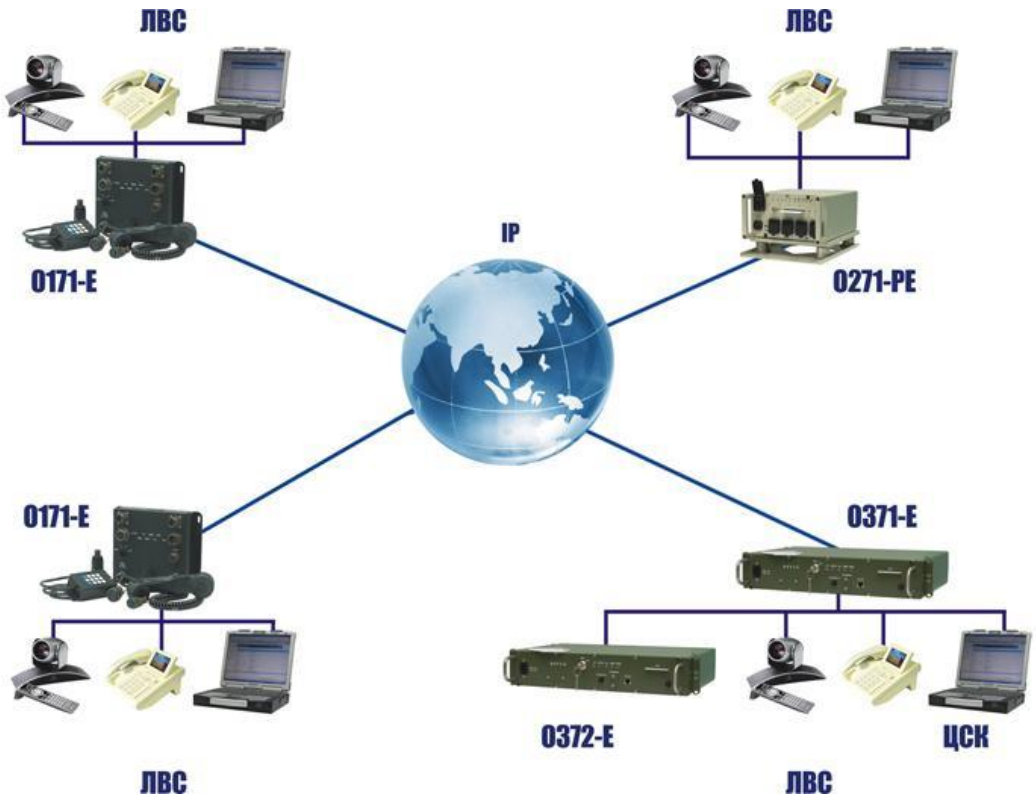


Рис. 3.8 Схема застосування «Скат»

Pelena

Комплекс криптографічного захисту інформації від Tritel.

Склад комплексу такий:

● Шифратор B371

Пристрій, що генерує найважливіші дані, – B364.

Централізована система адміністрування

Шифратор V371-E призначений для захисту цифрового контенту в Інтернеті із середнім та високим ступенем секретності. Його призначення – захист дротових, супутникових, радіо та стільникових (3G, 4G) каналів зв'язку. Він виробляється у варіантах, які можна використовувати у стаціонарних місцях [1,14].

Зображення показано на рис. 3.9.

Рис. 3.9 Зовнішній вигляд КЗІ «Пелена»[1]

Цей комплекс має такі можливості: [1, 14]

1) Кодування IP-мережевого трафіку, що проходить.

Шифрування трафіку використовується на зовнішній стороні периметра локальної мережі. Обробка криптографічної інформації в онлайн-режимі називається «прозорою», що досягається за допомогою програм обробки даних, IP-телефонії та відеоконференцій.

2) Віртуальні канали для зашифрованого зв'язку.

Під час передачі зашифрованої інформації формуються віртуальні канали зв'язку за схемою, запропонованою адміністратором комплексу.

3) Фіксація каналу.

Для кожного напрямку зв'язку можна встановити кілька віртуальних каналів з різними шляхами, що забезпечує узгодженість каналів зв'язку.

4) Система ключів.

Основна система відповідає за підготовку та поширення важливої інформації. Під час генерації важливих даних за допомогою пристрою В364 використовуються фізичні датчики, що відповідають стандарту FIPS 140-2. Розповсюдження програмного забезпечення здійснюється двома способами: через зашифровану мережу зв'язку та/або за даними, що мають ключі.

5) Апаратна реалізація криптографічного модуля.

Функції перетворення, що є криптографічними, виконуються спеціалізованими мікроелектронними схемами, які були продубльовані, що збільшує обсяг оброблюваних даних та забезпечує їх шифрування.

Балансування навантаження каналів.

Віртуальні канали можна об'єднувати в кластери для вирівнювання навантаження на вузли мережі та збільшення швидкості потоку через мережу.

7) Наявність кількох однакових або подібних пристроїв.

Обладнання можна повторювати з метою "гарячого" резервного копіювання та агрегації пропускної здатності.

8) Відстеження та керування.

Моніторинг та керування обладнанням здійснюється як локально, так і віддалено, і забезпечується централізованою системою CSC.

Схема застосунку проілюстрована на рис. 3.10.

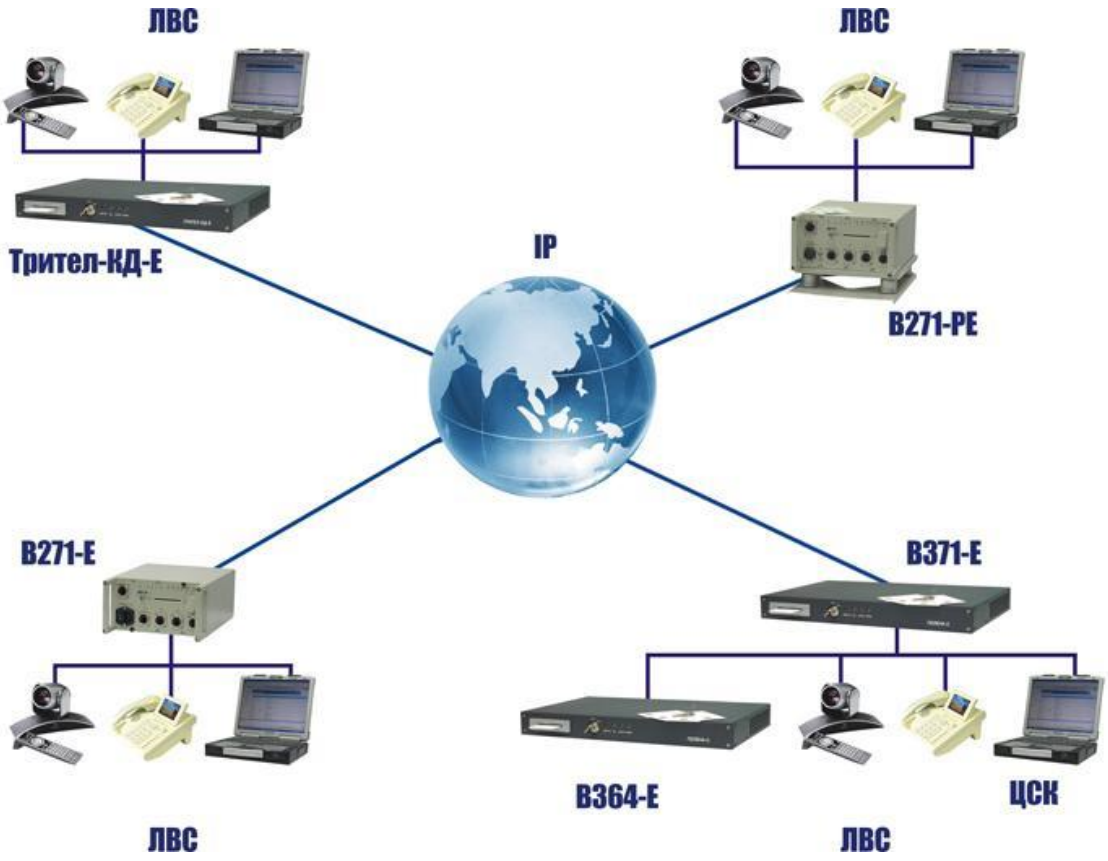


Рис. 3.10 Схема застосування «Пелена»[1]

Gnom

Криптор, що перемикається між різними режимами за допомогою інтегрованого модуля на базі Tritel.

Шифратор Gnom-E призначений для захисту цифрового контенту в Інтернеті із середнім та високим ступенем секретності. Його призначення — захист дротових, супутникових, радіо та стільникових (3G, 4G) каналів зв'язку. Він виготовляється у версіях, призначених для використання на стаціонарних (В371) та мобільних (В371) об'єктах.

Зображення показано на рис. 3.11.

Рис. 3.11 Зовнішній вигляд шифратора «Гном»[1]

Цей комплекс має такі можливості:

1) Кодування IP-мережевого трафіку, що проходить.

Шифрування трафіку використовується на зовнішній стороні периметра локальної мережі. Обробка криптографічної інформації в онлайн-режимі називається «прозорою», що досягається за допомогою програм обробки даних, IP-телефонії та відеоконференцій.

2) Віртуальні канали для зашифрованого зв'язку.

Під час передачі зашифрованої інформації формуються віртуальні канали зв'язку за схемою, запропонованою адміністратором комплексу.

3) Фіксація каналу.

Для кожного напрямку зв'язку можна встановити кілька віртуальних шляхів з різними маршрутами, що забезпечує наявність резервних каналів зв'язку.

4) Система ключів.

Первинна система відповідає за підготовку та поширення важливої інформації. Коли пристрій О372 генерує важливі дані, використовуються фізичні датчики, що відповідають стандарту FIPS 140-2. Розповсюдження програмного забезпечення здійснюється двома способами: через зашифровану мережу зв'язку та/або за даними, що мають ключі.

5) Апаратна реалізація криптографічного модуля.

Функції перетворення, що є криптографічними, виконуються спеціалізованими мікроелектронними схемами, які були продубльовані, що збільшує обсяг даних, що оброблюються, та забезпечує їх шифрування.

Балансування навантаження каналів.

Віртуальні канали можна об'єднувати в кластери для вирівнювання навантаження на вузли мережі та збільшення швидкості потоку через мережу.

7) Наявність кількох однакових або подібних пристроїв.

Обладнання може бути повторено з метою "гарячого" резервного копіювання та агрегації пропускної здатності.

8) Відстеження та керування.

Моніторинг та керування обладнанням здійснюється як локально, так і віддалено, за допомогою централізованої системи CSC. Програмне забезпечення CSC встановлюється на комп'ютер під керуванням ОС Windows і дозволяє керувати режимом роботи обладнання, змінювати конфігурацію параметрів, переглядати статистичну інформацію, реєструвати та обробляти повідомлення щодо подій у мережі зашифрованого зв'язку. Безпека вашого обладнання підвищується завдяки двофакторній автентифікації.

Схема програми проілюстрована на рис. 3.12.

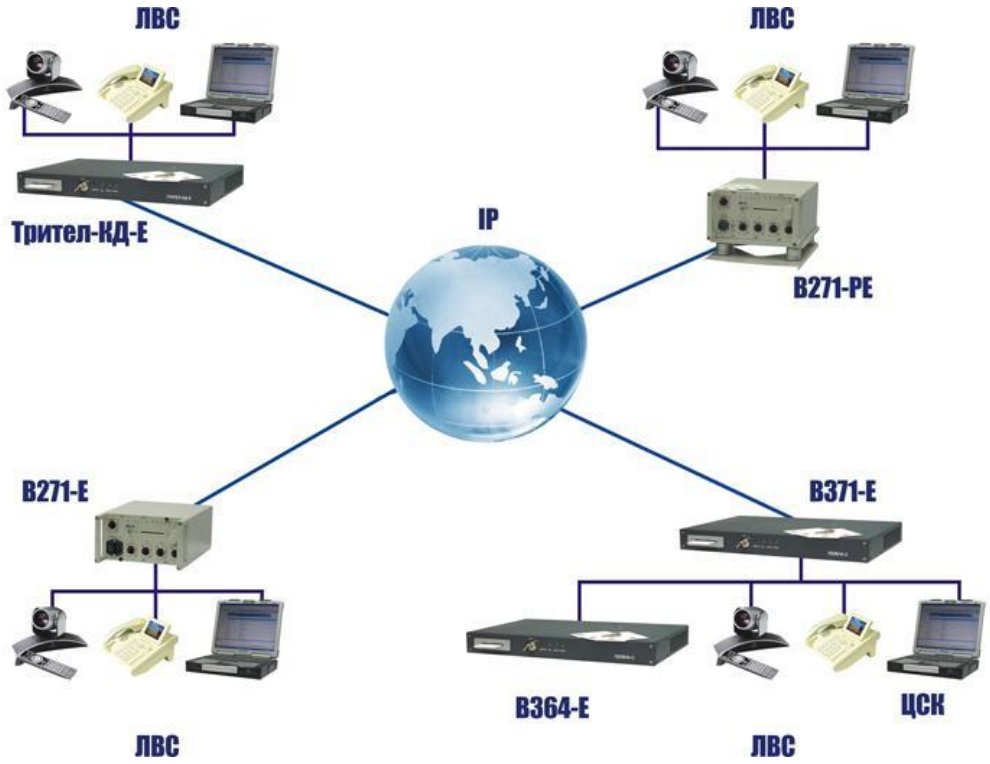


Рис. 3.12 Схема застосування «Гном»[1]

МТК

МТК призначений для забезпечення безпечної передачі різних типів інформації (даних, відео, аудіо) з високим ступенем секретності [1, 14].

Залежно від конфігурації, МТК може складатися з: мережевого обладнання, засобів криптографічного захисту (шифрувальників), систем живлення тощо.[1].

МТК використовується як на стаціонарних, так і на мобільних об'єктах.

Як обладнання для підписки, підключене до МТК, можна використовувати екрановані комп'ютери, IP-телефони, пристрої відеоконференцзв'язку, аналогові телефони.

Зовнішній вигляд зображений на рис. 3.13.

Рис. 3.13 Зовнішній вигляд МТК[1]

Цей комплекс має такі можливості[1]:

1. Мультисервісність.

Обмін інформацією будь-якого типу здійснюється через IP-протокол, який має високий ступінь гнучкості, масштабованості та легкості взаємодії з іншими комп'ютерами та системами зв'язку.

2. Модульність.

Модульна конструкція дозволяє створювати спеціалізовані комунікаційні компоненти для різних цілей, а також використовувати різні методи транспортування.

3. Канали зв'язку.

Для зв'язку між ізольованими МТК, що територіально розділені, використовуються канали: дротові, супутникові, радіо та стільникові (3G, 4G).

Схема застосування проілюстрована на рис. 3.14.

Рис. 3.14 Схема застосування МТК[1]

ZPMK-26

Інтелектуальний маршрутизаційний комутатор ZPMK-26 призначений для маршрутизації та комутації високозахищеного IP-трафіку.

ZPMK-26 забезпечує високу доступність та підтримує функції управління послугами найвищої якості. Як обладнання для підписки, підключене до ZPMK-26, він може використовувати захищені комп'ютери, IP-телефони та пристрої для відеоконференцій.

ZPMK-26 – це комутатор Cisco Catalist 3750, встановлений у 19-дюймовому корпусі, який є одночасно захищеним та вентильованим.

ZPMK-26 використовується на стаціонарних (ZPMK-26) та мобільних (ZPMK-26-R) об'єктах. Дисплей показано на рис. 3.15..

Рис. 3.15 Зовнішній вигляд ЗПМК [1]

Цей комплекс має такі можливості:

1) Обмеження пропускної здатності.

Пропускна здатність обмежується IP-адресою, MAC-адресою, інформацією 4-го рівня (TCP/UDP) або механізмами політик, залежно від контексту. Асинхронні потоки даних від кінцевих точок мережі можна спрямовувати, створюючи вихідні та вхідні черги для пакетів. Можливість створювати до 64 загальних та персоналізованих обмежень пропускної здатності для кожного порту комутатора.

2) Підтримка Plug-and-Play.

Функціональний стек комутаторів є автономним та має окрему конфігурацію. При зміні кількості комутаторів або їх видаленні головний комутатор автоматично змінює спосіб маршрутизації та комутації стеку.

3) Функції захисту.

Комутатори мають комплексний набір функцій безпеки для підключень та контролю доступу до ресурсів, включаючи списки доступу, авторизацію та автентифікацію, а також функції безпеки окремих портів, використання протоколу 802.1x та його розширень, і зазвичай використовуються разом із брандмауерами.

Схема програми проілюстрована на рис. 3.16.

Рис. 3.16 Схема застосування ЗПМК [1]

Каштан

Продукт Каштан призначений для полегшення передачі криптографічно захищених файлів віддаленим абонентам з центральною точкою спеціального зв'язку, а також між собою. Цей продукт був розроблений корпорацією Crypton.

Продукт Каштан сприяє організації наступних криптографічних мереж зв'язку [2, 14]:

● Циркулярний зв'язок - призначений для надсилання циклічних повідомлень через одну мережу з використанням однакових ключових даних.

● Парно-селективний зв'язок - призначений для обміну інформацією між будь-якими абонентами однієї мережі, що використовують два різні продукти Каштан.

Зображення показано на рис. 3.17.

.

Рис. 3.17 Зовнішній вигляд «Каштан»[2]

Основні технічні властивості [2,14]:

● кодування та шифрування інформації зі швидкістю не менше 400 кбіт/с

● час безперервної роботи не менше 6 годин;

Процес реалізації криптографічного алгоритму стандартний у режимі зворотного зв'язку;

● система ключів - "симетричного" типу;

Максимальна кількість абонентів у мережі - 100.

D300

Продукт D-300EM призначений для криптографічного захисту інформації, що передається по первинних цифрових каналах типу E1. Цей продукт є похідним від бренду Triton [2,14].

Конструкція структури кодера дозволяє 100% апаратне відтворення функцій шифрування та керування. Крім того, кодер і декодер повторюються двічі, щоб реалізувати перемикання ключів, яке відбувається "на ходу", коли перша спроба кодування з новим ключем не вдається і не втрачає передану інформацію.

Для захисту одного напрямку, два комплекти D-300EM повинні бути встановлені в проміжку між станцією та комунікаційним обладнанням щодо каналізації. Завдяки щоденній автоматичній зміні ключів, комплекти можуть працювати рік без технічного обслуговування.

Після ввімкнення живлення D-300EM проводить серію тестів, що включають тестування протоколу FIPS 140-2. Під час роботи виконується тестування методів шифрування або дешифрування, а також постійна перевірка якості каналу зв'язку.

Зображення показано на рис. 3.18. .

Рис. 3.18 Зовнішній вигляд «Д300» [2]

Основні технічні властивості [2,14]:

Процес глушіння передбачає реалізацію криптографічного алгоритму, який є стандартним у режимі глушіння.

Максимальний рівень захищеної інформації – «Для службового користування».

Довжина довгострокової ключової складової становить 512 біт;

● довжина сеансового ключа – 256 біт;

● система ключів – це «симетричний» тип ключа.

● конструктивні характеристики – висота 1U, достатня для встановлення у стандартну 19-дюймову шафу (443x226x44 мм).

3.6 Висновок до третього розділу

Третя частина кваліфікаційного завдання стосувалася сучасних технологій захисту інформації. Перелічені тут атрибути дозволяють вибрати найбільш підходящий інструмент, але питання вартості захисту все ще залишається невирішеним. Найефективніші інструменти, що використовуються державними установами, можуть бути непрактичними та дорогими в обслуговуванні. Було проведено дослідження різних типів та пристроїв, що використовуються для захисту інформації.

Розділ 4
ЗАХИСТ ІНФОРМАЦІЇ КОМЕРЦІЙНИХ СТРУКТУР

4.1 Концепція багаторівневого захисту

Різні методи захисту інформації в комерційних структурах та запобігання витоку інформації постійно розвиваються. Різні компанії спеціалізуються на різних послугах інформаційної безпеки. Однак, єдиного найкращого рішення не існує, але є кілька важливих аспектів, які необхідно врахувати, найважливішим та найкориснішим аспектом є використання концепції багаторівневого захисту.

Концепція багаторівневого захисту полягає в тому, що інформацію можна захистити за допомогою кількох рівнів захисту. Це підвищить безпеку об'єкта та мінімізує збитки, пов'язані з розкриттям інформації.

4.2 Завдання системи захисту інформації

Основні обов'язки [3,4,5]:

• телекомунікаційна допомога для функціонування спеціальних систем зв'язку, призначених для вирішення функціональних питань.

• забезпечення можливості інформаційної взаємодії між інформаційними системами та аналітичними системами в суб'єктах господарювання;

• створення передумов для інтеграції розподілених інформаційних ресурсів та інформаційних систем суб'єктів господарювання в рамках системи, при цьому інформаційний потік розподіляється між державою, фізичними та юридичними особами.

• запобігання втраті інформації конференцій відповідно до норм законодавства.

4.2 Принципи створення системи захисту

Ці принципи перелічені як основа для розробки системи інформаційної безпеки.

Ідея системи організації. Суть цього принципу полягає в тому, що під час процесу створення ми використовуємо концепцію системного підходу, і таким чином можемо розглядати систему як складну. Це сприяє поділу цієї складної системи на менші підсистеми. Як результат, за допомогою одного спеціального завдання ми маємо можливість окремо створювати та впроваджувати зміни.

Принцип розширення є основою зростання компанії. Фундаментальна ідея цього принципу полягає в розширенні системи та додаванні послуг для більшої кількості користувачів, а також збільшенні кількості резервних послуг. Збільшення розміру не вплине негативно на продуктивність або не призведе до погіршення експлуатаційних характеристик.

Концепція відкритості. Цей принцип може надати деякі рекомендації щодо модульного або блочного проектування системи та її компонентів. Перераховано деякі поширені протоколи або проектні рішення, що використовуються.

Концепція еволюції з спрямованим шляхом. Важливість цього принципу демонструється процесами проектування, які потенційно можуть змінити сучасну структуру системи або її компонент. Це дає компанії можливість реагувати на сучасні вимоги користувачів.

Концепція комплексної безпеки. Фундаментальна концепція полягає в зусиллях численних пов'язаних рішень, спрямованих на захист самої системи від різних небезпек. Негативні явища природного або навмисного характеру можуть значно порушити роботу системи, що є особливо важливим.

Ці принципи визначають майбутнє значення та обґрунтованість важливих рішень, які будуть використані для створення системи. Також, забезпечуючи засоби для модернізації, вдосконалення та розвитку системи, це дозволить вибрати широкий спектр телекомунікаційних технологій.

Для забезпечення безпечної передачі інформації та комерційних структур між спеціальними мережами, що надають послуги, важливо спиратися на мережу Національної системи конфіденційної інформації (NSCI).

Приклад того, як мережа NSCI працює з різними мережами, що надають системні послуги, та деякими, що взаємодіють з нею, зображено на рис. 4.1.[3,4,5]

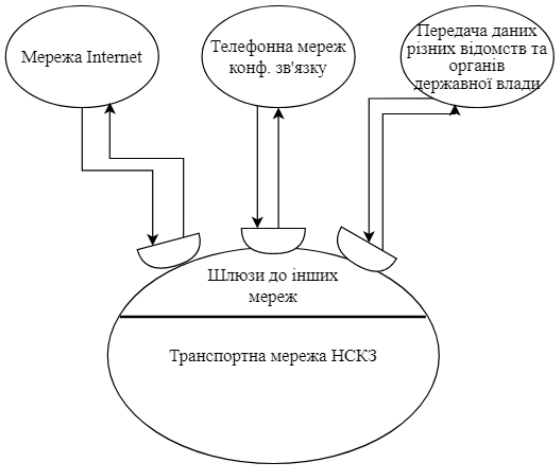


Рис. 4.1 Взаємодія транспортної мережі з мережами надання послуг

4.3 Система виявлення вторгнень

С Все частіше системи виявлення вторгнень інтегруються в інфраструктуру мережевої безпеки. IDS функціонують як засіб виявлення та спостереження за шкідливою активністю. Вони розпізнають порушників, які обійшли брандмауер, і повідомляють про це адміністратору, який, у свою чергу, вживає додаткових заходів для запобігання атаці. Технології виявлення вторгнень не є повністю ефективними. Як правило, IDS мають такий склад[11,14]:

1) Підсистема датчиків - ця підсистема відповідає за збір інформації щодо мережевої безпеки.

2) Інформація, зібрана з датчиків та аналізатора, зберігається.

3) Аналізатор: він виявляє аномальний трафік та атаки на основі даних датчиків.

4) Консоль керування, доступна через Інтернет, дозволяє налаштувати SVM.

Склад можна побачити на рис. 4.2.[13,14]

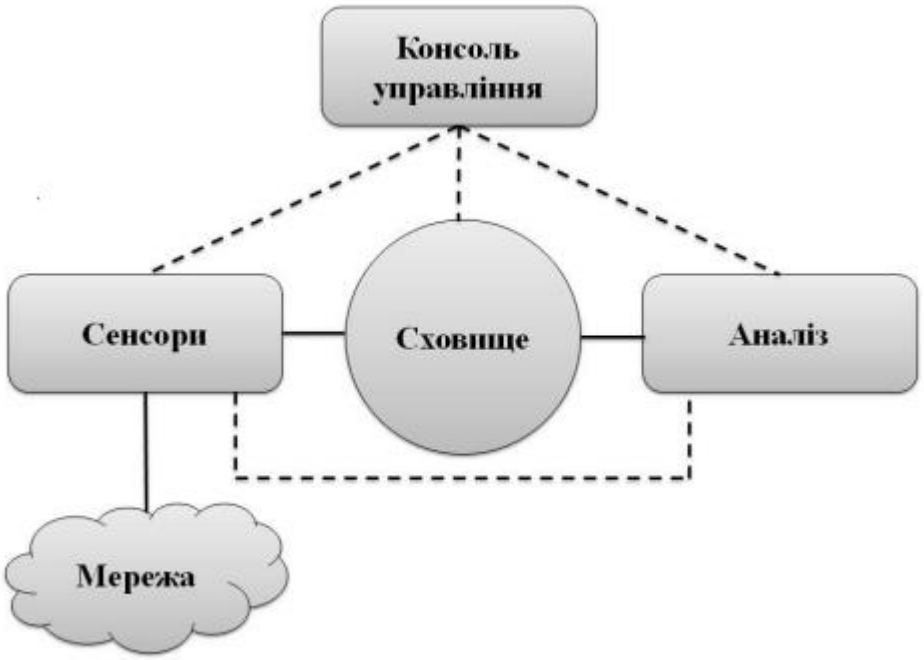


Рис. 4.2 Загальна структура СВВ

Доступно багато сучасних систем виявлення вторгнень. Однак найпоширенішими та найпопулярнішими варіантами є:

1) Brat.

Цей SVN-репозиторій та журнал відстежує та аналізує трафік. Забезпечує видимість пакетів та має механізм для подій та сценаріїв. Він здатний спостерігати за SNMP-трафіком. Можна спостерігати за поведінкою FTP, DNS та HTTP.

2) OSSEC.

Безкоштовно надає можливість використовувати інструменти безпеки з відкритим кодом. Можна розпізнавати зміни в реєстрі у Windows та контролювати будь-які спроби входу до облікового запису root у Mac-OS.

3) Hrop.

Сніфер пакетів, реєстратор пакетів, розвідка загроз, блокування сигнатур, оновлення сигнатур безпеки в режимі реального часу, детальна звітність, здатність розпізнавати різноманітні атаки, включаючи відбитки пальців ОС, SMB-зонди, CGI-атаки, переповнення буфера та приховане сканування портів.[11,13].

4) Meerkat.

Дані збираються на рівні програми, що дозволяє моніторити протоколи нижчого рівня, такі як TCP, IP, UDP, ICMP та TLS, а також трасувати мережеві програми в режимі реального часу, такі як SMB, HTTP та FTP. Ці функції поєднуються зі сторонніми інструментами, такими як Anaval, Squil, BASE та Snorby. Крім того, використовується інтелектуальна архітектура обробки.[11,13].

5) Застава.

Повноцінний дистрибутив Linux, який зосереджений на управлінні журналами, моніторингу безпеки та виявленні вторгнень, усі ці функції є частиною конфігурації за замовчуванням в Ubuntu, вони походять від кількох інструментів аналізу та фронтенду, включаючи NetworkMiner, Snorby, Xplico, Sguil, ELSA та Kibana. Також включені функції HIDS, а для аналізу мережі використовується сніффер пакетів, графіки та діаграми включені до конфігурації за замовчуванням.

4.4.1 Аналіз сигнатур та протоколів

Першим підходом, який використовувався для розпізнавання вторгнень, був аналіз сигнатур. Цей підхід простий і базується на концепції пов'язування послідовності зі шаблоном. Кожен байт вхідного пакета оцінюється побайтово та порівнюється з сигнатурою, що дозволяє визначити природу шкідливого трафіку. Ця сигнатура зазвичай складається з низки ключових слів або фраз, пов'язаних з атакою. Якщо виявлено збіг, спрацьовує тривога.

Інший підхід полягає у спостереженні за трафіком даних, які суворо відформатовані. Для супроводу кожного повідомлення використовуються різні протоколи. Крім того, кожен протокол зазвичай має кілька параметрів із певними значеннями, які є призначеними або типовими. Якщо в одному з полів протоколу зустрічаються неочікувані значення, вважається, що сталося порушення протоколу, і спрацьовує тривога.

4.5 Програмне забезпечення для криптографічного перетворення

Програмне забезпечення для криптографічної трансформації – це програмне забезпечення, яке в першу чергу призначене для шифрування та дешифрування даних у вигляді файлів (або сегментів), жорстких дисків та знімних носіїв (дискети, компакт-диски, USB-флеш-накопичувачі), електронних листів або пакетів, що передаються через комп'ютерні мережі.

Найпопулярнішим криптографічним програмним забезпеченням цього року є [10, 11]:

1) AxCrypt.

AxCrypt був розроблений спеціально для малих та середніх організацій. Продукт надійний та потужний. Він надає вам всю необхідну інформацію та ресурси для збереження ваших файлів у безпеці.

Файли захищені 128-бітним або 256-бітним AES-шифруванням, яке має бути простим для захисту від будь-якого вторгнення. Вони також сприяють зберіганню даних у хмарі як частині свого сервісу.

Це програмне забезпечення автоматично захищатиме файли, що зберігаються в таких сервісах, як Google Диск та Dropbox. Це корисний бонус, оскільки файли, яких немає на вашому персональному комп'ютері, також захищені AxCrypt.

Нею вже розмовляють понад 11 різними мовами, і нові мови будуть додаватися.

Також є функція керування паспортами, а також потужний додаток, який можна використовувати для керування всіма вашими документами. Існує безкоштовна версія програмного забезпечення AxCrypt, призначена для шифрування, але вона все ще досить обмежена.

2) VeraCrypt.

Якщо ви шукаєте найефективніше безкоштовне програмне забезпечення для шифрування, то VeraCrypt — це те, що вам обов’язково варто розглянути. Вони пропонують чудовий безкоштовний сервіс криптоаналізу для всіх. Вони мають один із найпопулярніших інструментів безпеки, цей інструмент забезпечує шифрування корпоративного рівня для вашої важливої інформації.

VeraCrypt має базову версію, яка є повністю безкоштовною та дуже надійною. Вона проста у використанні та розумінні. Все, що вона насправді робить, це додає зашифрований пароль до вашої інформації та роздільників.

Опишіть функціональність програмного забезпечення щодо ваших даних, наприклад, розмір і розташування тому, і залиште його робити інші речі.

Він повністю сліпий, тому вам не потрібно турбуватися про те, що хакери зламають ваші паролі чи інші конфіденційні персональні дані. Якщо у вас є бюджет, ознайомтеся з ним.

3) Boxcryptor.

Boxcryptor – ще один популярний вибір програмного забезпечення для шифрування сьогодні. Він забезпечує повну безпеку для хмари. Якщо ви

самотня людина або маєте малий бізнес, який переважно використовує хмарне сховище замість локальних сервісів, то Boxcryptor має бути сервісом, який ви давно хотіли використовувати.

Що Boxcryptor робить, на відміну від іншого програмного забезпечення для шифрування, орієнтованого на хмару, не робить, так це надає програмне забезпечення, специфічне для 30 найпопулярніших хмарних сервісів. Ці сервіси включають Dropbox, Google Drive та Microsoft OneDrive.

Вони досягають цього, поєднуючи 256-бітну криптосистему AES та криптосистему RSA. Основна концепція Boxcryptor полягає в тому, що вони прагнуть забезпечити максимально просте шифрування для кількох сервісів та пристроїв.

Зацікавлені таємницею того, як функціонують паролі, файлові ключі та ключі доступу? Усі вони одночасно зберігаються на пристроях користувачів. Ключі бізнес-користувачів, групові ключі та ключі компанії зашифровані та зберігаються на сервері Boxcryptor.

Boxcryptor також пропонує обмежену безкоштовну версію, сумісну з двома різними пристроями. Якщо ви хочете дізнатися більше про служби безпеки для хмар, це чудове місце для початку.

4) NordLocker.

NordLocker – це програмне забезпечення, яке охоплює шифрування файлів в операційних системах MacOS та Windows. Воно використовує два найпотужніші методи шифрування, доступні на даний момент: AES-256 та 4096-бітний RSA. Продукт простий у використанні та має дуже інтуїтивно зрозумілий інтерфейс.

Додаток ефективний на багатьох платформах та захищає інформацію, яка зберігається на вашому пристрої або в будь-якому іншому хмарному сервісі.

5) CryptoForge.

CryptoForge пропонує простий, контекстно-відповідний підхід до шифрування та безпечного видалення. Вони також мають можливість

розшифровувати звичайний текст. Вони є надійним варіантом для захисту ваших файлів.

Продукт простий в установці та має простий інтерфейс, який просто відображає діалогове вікно з налаштуваннями. Доступ до функцій здійснюється через контекстне меню, що викликається клацанням правою кнопкою миші.

ВИСНОВКИ

Результатом кваліфікаційного процесу є вдосконалення методів захисту інформації комерційних структур у телекомунікаційних системах подвійного призначення. У процесі виконання завдання було зроблено такі висновки:

1) Інформаційні системи та зв'язок.

2) Принципи експлуатації комунікаційних та інформаційних мереж.

3) Сучасні різновиди та методи захисту інформації.

4) Захист комерційної інформації в телекомунікаційних системах подвійного призначення.

У першій частині кваліфікаційного завдання було розглянуто важливість захисту інформації в телекомунікаційних мережах. Було задокументовано категоризацію та функції телекомунікаційних систем, їх переваги та недоліки. Було проведено дослідження NSCI.

Все це продемонструвало, що захист інформації більше не є частиною повсякденного життя жодної частини нашого суспільства. Підвищення ефективності телекомунікаційних систем та безпеки конфіденційної особистої інформації є одними з найважливіших завдань технологічних інновацій сьогодення.

У другому розділі було оцінено фундаментальні принципи побудови та поширення інформації. Підвищення швидкості, безпеки та простоти використання мають підвищити популярність телекомунікаційних процесів.

Процедура створення телекомунікаційних технологій має бути однією з провідних сфер зростання для країни. Значення та поширення настільки великі, що створення нових методів атак проводиться постійно, як наслідок, методи та технології, що використовуються для захисту, також повинні розвиватися.

У третьому розділі розглянуто сучасні методи та різні способи захисту інформації. Незважаючи на те, що методи захисту використовуються повсюдно, не встановлено фундаментальної концепції захисту інформації. Різні комерційні структури мають різні методи захисту, специфічні для їхніх структур, що ускладнює розуміння основних вимог до захисту. Різні комерційні

підприємства з різними фінансовими активами мають різні вимоги до захисту, як наслідок, вони використовують різні методи захисту. Якщо великі організації можуть дозволити собі використовувати криптографічні методи інформаційної безпеки, то менші організації не мають такої можливості. Це виключає створення конкретної національної оборони загалом.

У четвертому розділі було оцінено IPTV та різні криптографічні програми. Невеликі організації, що мають комерційний характер, можуть мати великий обсяг даних, які потребують захисту, але через свою потенційно малу капіталізацію вони не можуть цього зробити. Незважаючи на це, найефективнішим способом побудови захисту інформації є використання концепції кількох рівнів захисту. Цей принцип передбачає створення різних рівнів захисту інформації в телекомунікаційних системах. Як наслідок, першим і найважливішим кроком є підключення комерційних організацій до NSPC. Крім того, через обмежене фінансування рекомендується використовувати кілька програм та систем виявлення ризиків. На відміну від інших криптографічних методів, вони є менш витратними, доступнішими та простішими в обслуговуванні.

Практичне застосування створення комерційних систем дозволить:

1) Підвищити ефективність системи, створивши умови для її ефективного функціонування та управління, ці умови повинні забезпечити передачу конфіденційної інформації та її захист відповідно до вимог чинного законодавства.

2) Зберегти кошти для комерційних структур, надавши можливість використовувати технічні ресурси, які доступні по всій державі.

3) Надати поштовх та необхідність розвитку сектору захисту інформації, а саме розробки дешевших та більш технологічних методів для цивільного сектору.

Впровадження послуг з використанням NSPC збільшить доходи країни та сприятиме розвитку національної мережі, що дозволить країні зберегти не лише таємниці держави, а й таємниці народу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средства защиты информации. В 2-х томах. Том I. Несанкционированное получение информации – К.: Арий, 2008. - 464 с.

2. Конахович Г.Ф., Климчук В.П., Паук С.М., Потапов В.Г Защита информации в телекоммуникационных системах.. — К.: МК-Пресс, 2005. — 288 с, ил.

3. Грибунин В.Г., Чудовский В.В. Комплексная система защиты информации на предприятии Учебное пособие. – М.: Академия, 2009. – 416 с.

4. Кашкаров А.П. Системы видеонаблюдения. Практикум. Ростов-на-Дону: Феникс, 2014. — 120 с.: ил. — ISBN: 978-5-222-22579-0.

5. 15. Ворона В.А., Тихонов В.А. Системы контроля и управления доступом. –М.: Горячая линия – Телеком, 2013. – 272 с.

6. 16. Гришина Н.В. Организация комплексной системы защиты информации. М.: Гелиос АРВ, 2007. — 256 с, ил.

7. 17. Хорев А.А. Технические каналы утечки акустической (речевой) информации – М.: Специальная Техника, №№4, 5, 6 - 2004 год. 37 с.

8. 18. Андрончик А.Н., Богданов В.В. Домуховский Н.А. и др. Защита информации в компьютерных сетях. Практический курс/ А.Н. Андрончик, В.В. Богданов, Н.А. Домуховский, А.С. Коллеров, Н.И. Синадский, Д.А. Хорьков, М. Ю. Щербаков. – Екатеринбург: УГТУ-УПИ, 2008. – 248 с. — ISBN: 978-5-321-01219-2

9. 19. Мохор В. В. Наставления по кибербезопасности (ISO/IEC 27032:2013) / В. В. Мохор, А. М. Богданов, А. С. Килевой. К.: ООО «Три-К», 2013. — 129 с.

10. 20. Домарєв В.В. Організація захисту інформації на об’єктах державної та підприємницької діяльності /Домарєв В.В., Скворцов С.О./ Навч. Посібник. – К.: Вид-во Європейського університету, 2006. – 102с.

11. ISO/IEC 27001:2022 — https://www.iso.org/standard/27001

12. ISO/IEC 27002:2022 — https://www.iso.org/standard/75652.html

13. ДСТУ ISO/IEC 27001:2023 — https://zakon.isu.net.ua/sites/default/files/normdocs/dstu_iso_iec_27001_2023.pdf

14. ISO/IEC 27006:2015 — https://www.iso.org/standard/62313.html

15. NIST CSF 2.0 (NIST CSWP 29) — https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

16. NIST SP 800-53 Rev. 5 — https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

17. NIST SP 800-207 (Zero Trust Architecture) — https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf

18. ISO/IEC 27033-1:2015 — https://www.iso.org/standard/63461.html

19. ISO/IEC 27032:2023 — https://www.iso.org/standard/76070.html

20. ITU-T X.805 — https://www.itu.int/rec/dologin_pub.asp?id=T-REC-X.805-200310-I%21%21PDF-E&lang=e&type=items

21. ITU-T X.509 — https://www.itu.int/rec/t-rec-x.509

22. ETSI EN 303 645 V3.1.3 — https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf

23. ETSI TS 133 501 / 3GPP TS 33.501 — https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/16.03.00_60/ts_133501v160300p.pdf

24. ENISA 5G Security Controls Matrix — https://www.enisa.europa.eu/sites/default/files/all_files/ENISA%205G%20Security%20Controls%20Matrix%20paper.pdf

25. Directive (EU) 2022/2555 (NIS2) — https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

26. Regulation (EU) 2022/2554 (DORA) — https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

27. Закон України № 80/94-ВР — https://zakon.rada.gov.ua/go/80/94-%D0%B2%D1%80

28. Закон України № 2163-VIII — https://zakon.rada.gov.ua/go/2163-19

29. Закон України № 1882-IX — https://zakon.rada.gov.ua/go/1882-20

30. NIST SP 800-82 Rev. 3 — https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf

31. IEC 62443-3-3:2013 — https://webstore.iec.ch/en/publication/7033

32. FIPS 140-3 — https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf

33. ISO/IEC 15408-1:2022 — https://www.iso.org/standard/72891.html

34. ISO/IEC 18045:2022 — https://www.iso.org/standard/72889.html

35. ISO 22301:2019 — https://www.iso.org/standard/75106.html

36. ISO/IEC 27035-1:2023 — https://www.iso.org/standard/78973.html

Кваліфікаційна робота

Презентаційні матеріали до захисту

Система захисту інформації

в інформаційно-комунікаційних мережах подвійного призначення

Владислав Савченко, СЗДМ-62

Київ, 2026

Актуальність теми

- Інформаційно-комунікаційні мережі стали базовою інфраструктурою для державних, комерційних та спеціалізованих сервісів.
- Зростання цінності конфіденційних даних посилює ризики витоку, шпигунства, несанкціонованого доступу та саботажу.
- Мережі подвійного призначення потребують комплексного підходу до захисту інформації з урахуванням цивільних і спеціальних функцій.
- Захист має охоплювати організаційні, криптографічні, технічні та програмні механізми.

Мета, об’єкт і предмет дослідження

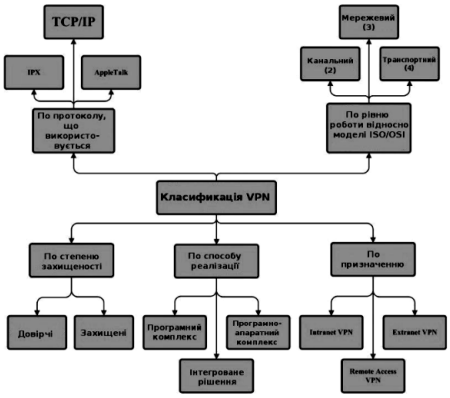
- Мета: підвищення ефективності захисту інформації в інформаційно-комунікаційних мережах подвійного призначення.
- Об’єкт дослідження: інформаційно-комунікаційні системи подвійного використання.
- Предмет дослідження: засоби та методи захисту інформації в таких системах.
- Практичне значення: формування підходів до захисту критичної інформації комерційних структур і спеціальних мереж.

Завдання магістерської роботи

- Провести аналіз актуальності захисту інформації в інформаційних мережах.
- Класифікувати інформаційно-комунікаційні системи та мережі за основними ознаками.
- Дослідити сучасні методи захисту інформації в інформаційно-комунікаційних системах.
- Запропонувати рішення щодо захисту інформації в телекомунікаційних системах подвійного призначення.

Класифікація телекомунікаційних мереж

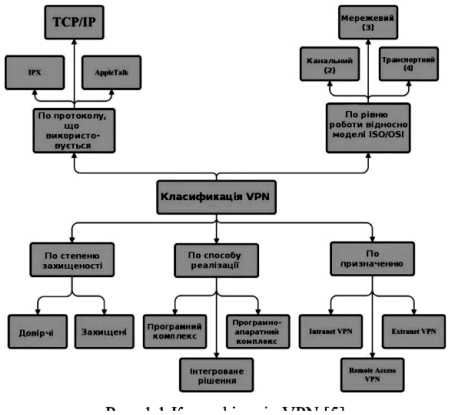
- За призначенням: транспортні, спеціалізовані, технологічні та спеціального призначення.
- За середовищем передавання: дротові, бездротові та комбіновані.
- За кількістю сервісів: односервісні та мультисервісні.
- За топологією: кільце, подвійне кільце, сітка, повнозв’язні та неповнозв’язні структури.



Мережі подвійного призначення

- Призначені для забезпечення потреб органів влади, спеціальних служб, оборони, безпеки та окремих цивільних споживачів.
- Поєднують вимоги високої доступності, конфіденційності, контрольованості та стійкості до збоїв.
- Потребують розмежування ресурсів, сегментації трафіку та контролю доступу до інформаційних сервісів.
- Ключова вимога - захист службової та конфіденційної інформації на всіх рівнях мережевої взаємодії.

VPN як інструмент захищеної взаємодії



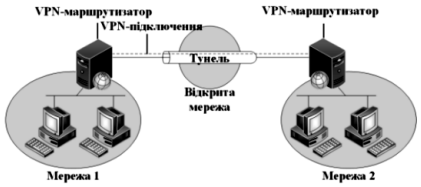


Рис. 2. Організація VPN-з'єднання двох віддалених вуз

- VPN створює логічно ізольований канал поверх мережі нижчого рівня довіри.
- Захищений тунель дозволяє об'єднувати віддалені сегменти та користувачів у єдину мережеву інфраструктуру.

Топологічна стійкість мереж

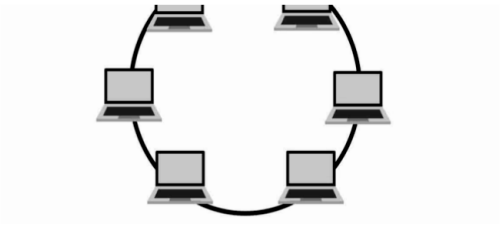
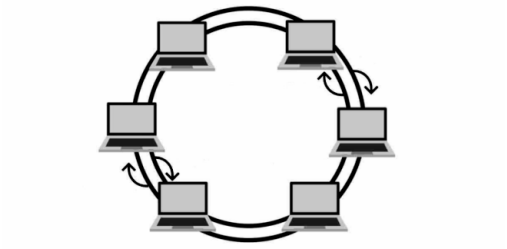


Рис. 1.2.1 Формат кільця

додаткове джерело. Однією з переваг цієї топології є низька встановлення. Приклад такої конфігурації показано на рис. 1.3.[5,7].



- Кільцева структура забезпечує послідовну передачу сигналу між вузлами, але є чутливою до відмов окремих елементів.
- Подвійне кільце підвищує стійкість, оскільки може забезпечити альтернативний напрям передавання даних.

Принципи функціонування ІКМ

- Комутація забезпечує встановлення маршрутів і передавання повідомлень, пакетів або каналів.
- Адресування визначає ідентифікацію вузлів, маршрутизацію та взаємодію мережевих сервісів.
- Керування мережею охоплює маршрутизацію, контроль працездатності, моніторинг стану вузлів та управління навантаженням.
- Для мереж подвійного призначення важливе централізоване адміністрування політик безпеки.

Основні загрози інформаційній безпеці

- Несанкціонований доступ до ресурсів і служб мережі.
- Перехоплення, модифікація або блокування інформаційного трафіку.
- Використання шкідливого програмного забезпечення, мережевих атак та експлуатація помилок конфігурації.
- Компрометація облікових даних, слабкий контроль доступу та порушення регламентів експлуатації.

Сучасні види та методи захисту інформації

- Організаційний захист: регламенти, ролі, політики доступу та відповідальність персоналу.
- Програмний захист: антивірусні засоби, міжмережеві екрани, IDS/IPS, контроль подій безпеки.
- Криптографічний захист: шифрування, електронний підпис, контроль цілісності та автентифікація.
- Технічний захист: захист каналів, обладнання, периметра та вузлів інфраструктури.

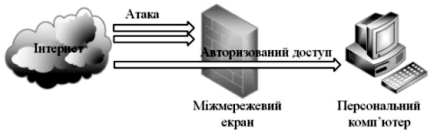


Рис. 1. Схема роботи міжмережевого екрану[11]

Криптографічний захист інформації

- КЗІ забезпечує конфіденційність, цілісність, автентичність та неможливість безконтрольної зміни даних.
- Симетричні алгоритми ефективні для швидкого шифрування великих обсягів даних.
- Асиметричні алгоритми використовуються для обміну ключами, електронного підпису та ідентифікації сторін.
- Комбіноване застосування КЗІ та VPN підвищує захищеність віддалених сегментів мережі.

Комплексний технічний захист

- Комплексна система захисту інформації поєднує криптографічні, програмні, технічні та організаційні механізми.
- Ключовими елементами є сегментація мережі, контроль доступу, журналювання, моніторинг і резервування.
- Захист має будуватися за принципом мінімальних привілеїв та багаторівневої оборони.
- Ефективність визначається здатністю системи зменшувати ризики витоку, порушення цілісності та недоступності даних.

IDS/IPS та виявлення вторгнень

- IDS виявляє ознаки атак, а IPS додатково блокує або обмежує небезпечну активність.
- Аналіз може виконуватись за сигнатурами, поведінковими моделями та протокольними аномаліями.
- Для мереж подвійного призначення важливе поєднання мережевого та вузлового моніторингу.
- Система виявлення вторгнень має бути інтегрована з журналюванням, реагуванням та політиками доступу.

Запропонований підхід до захисту

- Сформувати багаторівневу модель захисту інформації: периметр - мережевий сегмент - вузол - застосунок - дані.
- Розмежувати цивільні та спеціальні сервіси за допомогою сегментації, VPN, контролю доступу та політик маршрутизації.
- Використати криптографічний захист для передавання та зберігання критичної інформації.
- Забезпечити постійний моніторинг подій безпеки, аналіз інцидентів і регулярне оновлення конфігурацій.

Висновки

- Проведено аналіз інформаційно-комунікаційних мереж та їх класифікації.
- Визначено специфіку захисту мереж подвійного призначення з урахуванням вимог конфіденційності, доступності та стійкості.
- Досліджено сучасні методи захисту: VPN, КЗІ, міжмережеві екрани, IDS/IPS, технічні та організаційні заходи.
- Запропоновано комплексний підхід до підвищення ефективності захисту інформації в мережах подвійного призначення.