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

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри

_____ Одарченко Р.С.
“_____”_____2021 р.

ДИПЛОМНА РОБОТА
(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВР

Тема: «Корпоративна мережа VoIP»

Виконавець: _____ Мазуренко І.О.
(підпис)

Керівник: _____ Мачалін І. О.
(підпис)

Нормоконтролер: _____ Бахтіяров Д. І.
(підпис)

Київ 2021

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

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

ЗАТВЕРДЖУЮ
Завідувач кафедри

Одарченко Р.С.
“_____”_____2021 р.

ЗАВДАННЯ
на виконання дипломної роботи

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

1. Тема дипломної роботи (проекту): «Корпоративна мережа VoIP»
затверджена наказом ректора від «06» квітня 2021 р. №559 / ст
2. Термін виконання роботи: з 17.05.2021 р. по 20.06.2021 р.
3. Вихідні дані до роботи: Загальні характеристики та переваги IP-телефонії; Принципи передачі голосового трафіку; Архітектура мережі на базі протоколу SIP.
4. Зміст пояснювальної записки: вихідні дані для проектування; технічне рішення щодо проектування мережі провайдера IP-телефонії; проектування захищеної мережі voip провайдера
5. Перелік обов'язкового графічного (ілюстративного) матеріалу: Схема застосування міжмережевих екранів; Схема застосування шифрованих VPN тунелів; Захищена мережа VoIP провайдера; Приклад мережі на базі протоколу SIP; Шифрування IP-телефонії

6. Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1	Розробити деталізований зміст розділів диплому	17.05.2021-20.05.2021	Виконано
2	Вступ	21.05.2021-22.05.2021	Виконано
3	Назва першого розділу	23.05.2021-27.05.2021	Виконано
4	Назва другого розділу	28.05.2021-03.06.2021	Виконано
5	Назва третього розділу	04.06.2021-09.06.2021	Виконано
6	Усунення недоліків дипломної роботи	10.06.2021-14.06.2021	Виконано

7. Дата видачі завдання: “26" квітня 2021 р.

Керівник дипломної роботи _____ Мачалін І. О.
(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ Мазуренко І.О.
(підпис випускника) (П.І.Б.)

РЕФЕРАТ

Дипломна робота «Корпоративна мережа VoIP» містить 54 сторінки, 11 рисунків, 2 таблиці, 22 використаних джерела.

VOIP ПРОВАЙДЕР, IP-ТЕЛЕФОНІЯ, МЕРЕЖА IP, ЗАХИСТ ІНФОРМАЦІЇ, КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ, ІНФОРМАЦІЙНА БЕЗПЕКА, АТАКА IP МЕРЕЖІ, ОБЛАДНАННЯ IP-ТЕЛЕФОНІЇ.

Об’єктом дипломної роботи є мережа VoIP провайдера призначена для передачі мовного трафіку.

Метою дипломної роботи є застосувати технічні рішення для забезпечення захисту мережі та надання високого рівню інформаційної безпеки IP-телефонії. Захистити інфраструктуру, яка передає трафік, дані голосового трафіку і самі протоколи на базі яких реалізована ця технологія.

Мережа провайдера, що передає трафік IP-телефонії опирається на протокол SIP. Для організації IP-телефонії використовується обладнання вендора JERASOFT, розробником і інтегратором програмного забезпечення маршрутизації та білінгу IP-телефонії. Для організації безпечної і ефективної взаємодії з партнерами використовується провідний розробник рішень MERA. Контроль і фільтрацію мережевих пакетів в мережі відповідно до заданих правил виконує обладнання Cisco ASA.

Матеріали дипломної роботи рекомендується використовувати при проектуванні мереж IP, в яких буде використовуватися голосова телефонія.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ

IP – Internet Protocol - інтернет протокол

VoIP – Voice over IP – технологія передачі голосу по Інтернет-протоколу

ТМЗК – Телефонна мережа загального користування

ISDN – Integrated Services Digital Network – цифрова мережа з інтегрованими послугами

FXS – Foreign Exchange Station or Subscriber

FXO – Foreign eXchange Office

NAT – *Network Address Translation* – Перетворення мережевих адрес

QoS – Quality of service – Якість обслуговування

RTP – Real-time Transport Protocol – Протокол передачі трафіку реального часу

РОС – Розподілена обчислювальна система

ОС – Обчислювальна система

SIP - Session Initiation Protocol - протокол прикладного рівня

DDoS - Distributed Denial-of-service attack — вид нападу на комп'ютерну систему

ЕЦП - Електронний цифровий підпис

VPN - Virtual Private Network – Віртуальна приватна мережа

TLS - Transport Layer Security - криптографічний протокол

Secure Real-time Transport Protocol — Безпечний протокол передачі даних в реальному часі

VLAN - Virtual Local Area Network — віртуальна локальна комп'ютерна мережа

CDR - Call Detail Record - Інформація про дзвінок

ВСТУП

Актуальність теми. Практична можливість повної інтеграції голосу і даних поверх загальної інфраструктури обчислювальних мереж привела до появи так званої «пакетної телефонії» - технології передачі аналогових телефонних сигналів по мережах передачі даних. Для позначення технології передачі мови по IP-мереж використовуються два основні терміни: IP-телефонія (IP Telephony) або голос по IP-мереж (Voice over IP - VoIP) [14].

Під IP-телефонією розуміється технологія, що дозволяє використовувати будь-яку мережу з пакетною комутацією на базі протоколу IP як засіб організації і ведення міжнародних, міжміських і місцевих телефонних розмов і передачі факсів в режимі реального часу [14].

На сучасному рівні розвитку IP-телефонія вже має низку переваг у порівнянні з традиційною:

• послуги IP-телефонії дешевше традиційної міжміського та міжнародного телефонного зв'язку;

• в порівнянні з традиційною телефонією обладнання каналів зв'язку простіше, нижче експлуатаційні витрати;

• мережі з комутацією пакетів більш відмовостійкі, ніж мережі з комутацією каналів, в них ефективніше використовується продуктивність каналів зв'язку;

• кінцевий користувач отримує новий набір пристроїв доступу від традиційних телефонів і факсів до комп'ютерів;

• можливість користувачам мати доступ до одного і того ж набору послуг незалежно від того, де і як вони підключаються до мережі;

• надається можливість настройки набору послуг [9].

IP-Телефонія продовжує прогресувати і бесперечно темпи її зростання залишаться такими стрімкими. За цією технологію вже передається більш ніж 7 від-

сотки міжнародного світового трафіку. У світі обсяг трафіку в IP-мережах та інших мережах з передачі даних вже сьогодні перевищує обсяг голосового трафіку в ТМЗК.

Звичайно, у сфері IP-телефонії все ще існує безліч різних проблем, таких як облік використання технологічних ресурсів, маршрутизації трафіку, білінгу, розрахунку вартості транспортних затримок і т.п.

Дані голосового трафіку є одним з найцінніших ресурсів, тому їх захист - важливе завдання. Чималу роль в роботі організації будь-якого рівня грають телефонні переговори. В силу зростаючої популярності IP-телефонії, все гостріше постає питання забезпечення її безпеки в загальному і конфіденційності розмов зокрема [18].

Знання основних джерел небезпеки для мереж IP-телефонії, а також розуміння методів усунення цих загроз допоможе зберегти репутацію і фінансові ресурси компанії. Дана проблематика актуальна для будь-яких платформ IP-телефонії. Той, хто передає чи приймає дані по мережі IP в незахищеному вигляді, стає привабливою метою для хакерів, в тому числі, коли мова йде про голосових даних. Відповідно, інфраструктур VoIP загрожують ті ж небезпеки, що і для мереж передачі даних. Однак результати успішної атаки на мережу передачі голосових даних більш серйозні: затримане на кілька хвилин електронне лист або повільно працює браузер рідко призводять до тяжких наслідків, на відміну від переривання телефонної розмови або повного виходу з ладу системи комунікацій [21].

Детальним дослідженням рівня захисту інформації в існуючих системах IP-телефонії є саме аналіз структури протоколів передачі даних, що в них застосовуються, на предмет встановлення їх відповідності потребам збереження конфіденційності телефонних переговорів та формування вимог щодо комплексного захищеного протоколу обміну голосовими повідомленнями абонентів високої стійкості.

Захист інформації полягає в підтримці інформаційної безпеки, тобто стану захищеності інформаційного середовища, яке досягається шляхом дотримання

конфіденційності, цілісності та доступності інформації. Згідно з, дотримання вказаних вимог у випадку IP-телефонії можливо лише при умові використання криптографічних перетворень інформації, тобто шифрування [11].

Мета – побудова корпоративної мережі VoIP з елементами захисту мовного трафіку.

Для досягнення поставленої мети вирішуються такі наукові завдання.

1. Аналіз загальних підходів до побудови VoIP мереж.
2. Проектування захищених систем зв'язку в розподілених обчислювальних системах.
3. Проектування корпоративної мережі VoIP з елементами захисту мовного трафіку.

Об'єктом дослідження – передавання мовної інформації через IP мережу.

Предметом дослідження – захист VoIP трафіку.

Практичне значення отриманих результатів.

Результати та напрацювання даної дипломної роботи можуть бути використані інженерами електрозв'язку при проектуванні захищених корпоративних мереж з передаванням мовної інформації за допомогою протоколу IP.

Апробація отриманих результатів. Основні положення роботи доповідалися та обговорювалися на таких конференціях:

- Науково-практична конференція «Проблеми експлуатації та захисту інформаційно-комунікаційних систем», м. Київ, 2021 р.

РОЗДІЛ 1
ВИХІДНІ ДАНІ ДЛЯ ПРОЕКТУВАННЯ

1.1. Організація IP-телефонії

Загальні характеристики та переваги IP-телефонії. IP-телефонія - телефонний зв'язок по протоколу IP. Під IP-телефонією розуміється набір комунікаційних протоколів, технологій і методів, що забезпечують традиційні для телефонії набір номера, дозвон і двостороннє голосове спілкування, а також відеоспілкування через мережу Інтернет або будь-яким іншим IP-мереж. Сигнал по каналу зв'язку передається в цифровому вигляді і, як правило, перед передачею перетворюється (стискується) з тим, щоб видалити надлишок інформації та знизити навантаження на мережу передачі даних [4].

Голосовий та відеозв'язок за допомогою комп'ютерних мереж став популярний у всьому світі з початку XXI століття і в даний час широко використовується як приватними користувачами, так і в корпоративному секторі. Застосування систем IP-телефонії дозволяє компаніям-операторам зв'язку значно знизити вартість дзвінків (особливо міжнародних) і інтегрувати телефонію з сервісами Інтернету, надавати інтелектуальні послуги [4].

IP-телефонія реалізує завдання і рішення, які за допомогою технології телефонної мережі загального користування реалізувати буде важче, або дорожче. Приклади:

- Можливість передавати більше одного телефонного дзвінка в рамках високошвидкісного телефонного підключення. Тому IP-телефонія використовується в якості простого способу для додавання додаткової телефонної лінії вдома або в офісі.

Властивості, такі як

- конференція,
- переадресація дзвінка,
- автоматичне повторення номера,
- визначення номера абонента [7].

Надаються безкоштовно, тоді як в традиційних телекомунікаційних компаніях зазвичай виставляються в рахунок.

- Безпечні дзвінки, зі стандартизованим протоколом. Більшість труднощів для включення безпечних телефонних з'єднань за традиційними телефонними лініями, такі як оцифровка сигналу, передача цифрового сигналу, вже вирішені в рамках IP-телефонії. Необхідно лише зробити шифрування сигналу і його ідентифікацію для існуючого потоку даних.

- Незалежність від місця розташування. Потрібно тільки інтернет-з'єднання для підключення до провайдера IP-телефонії. Наприклад, оператори центру дзвінків за допомогою IP-телефонів можуть працювати з будь-якого офісу, де є в наявності ефективне швидке і стабільне інтернет-підключення.

- Доступна інтеграція з іншими сервісами через інтернет, включаючи відеодзвінок, обмін повідомленнями і даними під час розмови, аудіоконференції, управління адресною книгою і отримання інформації про те, чи доступні для дзвінка інші абоненти.

- Додаткові телефонні властивості - такі як маршрутизація дзвінка, спливаючі вікна, альтернативний GSM-роумінг та впровадження IVR - легше і дешевше впровадити і інтегрувати. Той факт, що телефонний дзвінок знаходиться в тій же самій мережі передачі даних, що і персональний комп'ютер користувача, відкриває шлях до творення нових можливостей [2].

Додатково: можливість підключення прямих номерів у будь-якій країні світу (DID).

Принципи передачі голосового трафіку. «Класичні» телефонні мережі засновані на технології комутації каналів яка для кожної телефонної розмови вимагає виділеного фізичного з'єднання. Отже, одна телефонна розмова є одна фізична з'єднання телефонних каналів. В цьому випадку аналоговий сигнал шириною 3,1 кГц передається на найближчу АТС, де він мультиплексується за технологією тимчасового поділу з сигналами, які надходять від інших абонентів, підключених до цієї АТС. Далі груповий сигнал передається по мережі міжстанційних каналів. Досягнувши АТС

призначення, сигнал демультиплексується і доходить до адресата. Основним недоліком телефонних мереж з комутацією каналів є неефективне використання смуги каналу - під час пауз в мові канал не несе ніякої корисної навантаження [2].

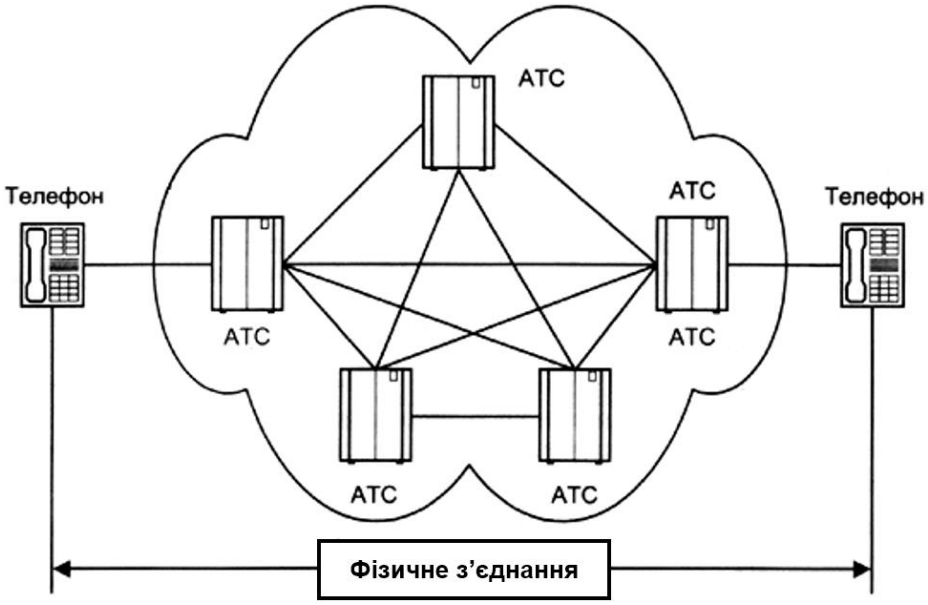

Рис. 1.1. З'єднання в «класичній» телефонній мережі

Перехід від аналогових до цифрових технологій став важливим кроком для виникнення сучасних цифрових телекомунікаційних мереж. Одним з таких кроків в розвитку цифрової телефонії став перехід до пакетної комутації. У мережах пакетної комутації по каналах зв'язку передаються одиниці інформації, що не залежать від фізичного носія. Такими одиницями можуть бути пакети, кадри або осередки (залежно від протоколу), але в будь-якому випадку вони передаються по розділяється мережі, більш того - по окремим віртуальним каналам, які залежать від фізичного середовища. Кожен пакет ідентифікується заголовком, який може містити інформацію про який він використовує каналі, його походження (тобто про джерело або відправника) і пункті призначення (про одержувача або приймачі).

У мережах на основі протоколу IP всі дані - голос, текст, відео, комп'ютерні програми або інформація в будь-якій іншій формі - передаються у вигляді пакетів. Будь-який комп'ютер і термінал такої мережі має свою унікальну IP-адресу, і передавані пакети маршрутизируются до одержувача відповідно до цієї адреси, яка вказана в заголовку [6].

Дані можуть передаватися одночасно між багатьма користувачами і процесами по одній і тій же лінії. При виникненні проблем IP-мережі можуть змінювати маршрут для обходу несправних ділянок. При цьому протокол IP не вимагає виділеного каналу для сигналізації.

Процес передачі голосу по IP-мережі складається з кількох етапів.

На першому етапі здійснюється оцифровка голосу. Потім оцифровані дані аналізуються і обробляються з метою зменшення фізичного обсягу даних, переданих одержувачу. Як правило, на цьому етапі відбувається придушення непотрібних пауз і фонового шуму, а також компресія.

На наступному етапі отримана послідовність даних розбивається на пакети і до неї додається протокольна інформація - адреса одержувача, порядковий номер пакету на випадок, якщо вони будуть доставлені не послідовно, і додаткові дані для корекції помилок. При цьому відбувається тимчасове накопичення необхідної кількості даних для утворення пакету до його безпосередньої відправки в мережу [11].

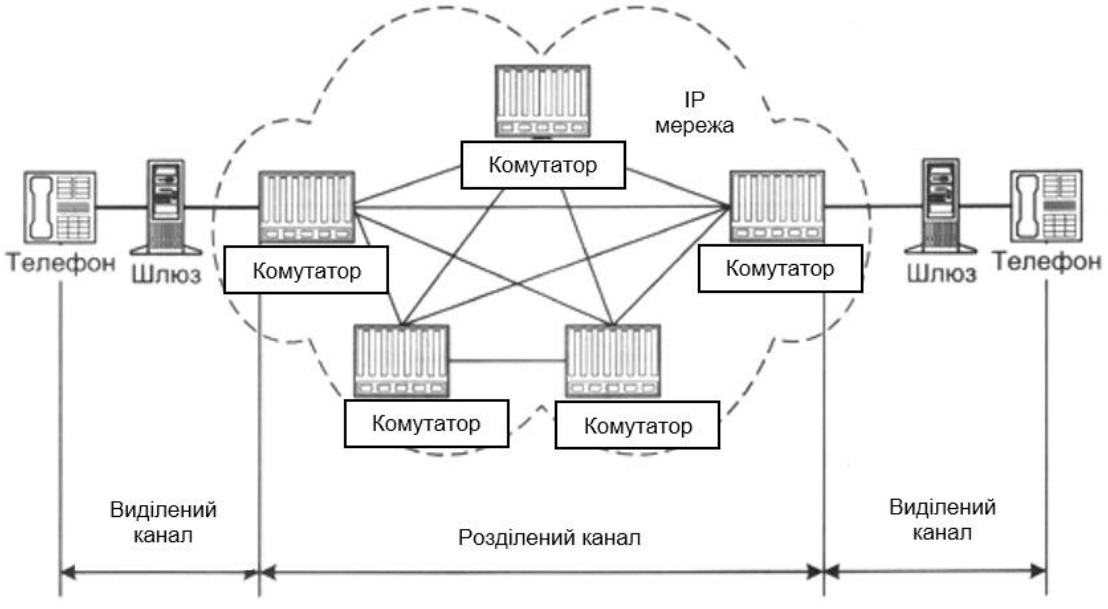

Рис. 1.2. З'єднання в мережі з комутацією пакетів

Витяг переданої голосової інформації з отриманих пакетів також відбувається в кілька етапів. Коли голосові пакети приходять на термінал одержувача, то

спочатку перевіряється їх порядкова послідовність. Оскільки IP-мережі не гарантують час доставки, то пакети зі старшими порядковими номерами можуть прийти раніше, більш того, інтервал часу отримання також може коливатися. Для відновлення початкової послідовності і синхронізації відбувається тимчасове накопичення пакетів. Однак деякі пакети можуть бути взагалі втрачені при доставці, або затримка їх доставки перевищує допустимий розкид. У звичайних умовах приймальний термінал запитує повторну передачу помилкових або втрачених даних. Але передача голосу дуже критична до часу доставки, тому в цьому випадку або включається алгоритм апроксимації, що дозволяє на основі отриманих пакетів приблизно відновити втрачені, або ці втрати просто ігноруються, а пропуски заповнюються даними випадковим чином [12].

Отримана таким чином послідовність даних декомпресується і перетвориться безпосередньо в аудіо-сигнал, що несе голосову інформацію одержувачу.

Таким чином, з великим ступенем ймовірності, отримана інформація не відповідає вихідної (перекручена) і затримана (обробка на передавальної і приймальні сторонах вимагає проміжного накопичення). Однак в деяких межах надмірність голосової інформації дозволяє миритися з такими втратами.

Оператори мереж з пакетною комутацією одержують переваги, властиві розділяється інфраструктурі електрозв'язку по самій її природі. Простіше кажучи, вони можуть продати більше, ніж в дійсності мають, ґрунтуючись на статистичному аналізі роботи мережі. Оскільки передбачається, що абоненти не будуть цілодобово і щодня задіяти всю сплачену полісу, можна обслужити більше абонентів, що не розширюючи магістральну інфраструктуру. Оборот і прибуток при цьому збільшуються [22].

Іншими словами, абонент, який оплатив смугу 64 кбіт / с, використовує канал в середньому лише на 25%. Отже, оператор здатний продати наявний у нього ресурс в чотири рази більшому числу користувачів, не перевантажуючи свою мережу. Такий сценарій вигідний обом сторонам - і клієнту, і продавцю, - оскільки оператор збільшує свої доходи і зменшує абонентну плату за рахунок зниження

витрат. Це виграшне рішення вже визнано в світі передачі даних, а тепер починає використовуватися і на ринку телефонії.

У цій час в IP-телефонії існує два основних способи передачі голосових пакетів по IP-мережі:

- через глобальну мережу Інтернет (Інтернет-телефонія);

- використовуючи мережі передачі даних на базі виділених каналів (IP-телефонія) [11].

У першому випадку смуга пропускання напряму залежить від завантаженості мережі інтернет пакетами, що містять дані, голос, графіку і т.д., а значить, затримки при проходженні пакетів можуть бути самими різними. При використанні виділених каналів виключно для голосових пакетів можна гарантувати фіксовану (або майже фіксовану) швидкість передачі. З огляду на поширення мережі Інтернет особливий інтерес викликає реалізація системи Інтернет-телефонії, хоча слід визнати, що в цьому випадку якість телефонного зв'язку оператором не гарантовано.

Для того, щоб здійснити міжміський (міжнародну) зв'язок за допомогою телефонних серверів, організація або оператор послуги повинні мати по серверу в тих місцях, куди і звідки плануються дзвінки. Вартість такого зв'язку на порядок менше вартості телефонного дзвінка по звичайних телефонних лініях. Особливо велика ця різниця для міжнародних переговорів.

Загальний принцип дії телефонних серверів інтернет-телефонії такий: з одного боку, сервер пов'язаний з телефонними лініями і може з'єднатися з будь-яким телефоном світу. З іншого боку, сервер пов'язаний з інтернетом і може зв'язатися з будь-яким комп'ютером в світі. Сервер приймає стандартний телефонний сигнал, оцифровує його (якщо він початково не цифровий), значно стискає, розбиває на пакети і відправляє через Інтернет за призначенням з використанням протоколу IP. Для пакетів, що приходять з мережі на телефонний сервер і що йдуть в телефонну лінію, операція відбувається в зворотному порядку. Обидві операції (вхід сигналу в телефонну мережу і його вихід з телефонної мережі) відбуваються практично одночасно, що дозволяє забезпечити повнодуплексну розмову. На основі цих базових операцій можна побудувати багато різних конфігурацій. Наприклад, дзвінок «телефон-комп'ютер» або

«комп'ютер-телефон» може забезпечувати один телефонний сервер. Для організації зв'язку телефон (факс) -телефон (факс) потрібно два сервери [8].

Основним стримуючим фактором на шляху масштабного впровадження IP-телефонії є відсутність в протоколі IP механізмів забезпечення гарантованої якості послуг, що робить його поки не найнадійнішим транспортом для передачі голосового трафіку. Сам протокол IP не гарантує доставку пакетів, а також час їх доставки, що викликає такі проблеми, як «рваний голос» і просто провали в розмові. Сьогодні ці проблеми вирішуються: організації зі стандартизації розробляють нові протоколи, виробники випускають нове обладнання, але на цьому рівні справи з сумісністю і стандартизацією йдуть вже не так добре, як з «упаковкою» мови в пакети. Зауважимо, що якщо в рамках приватної корпоративної мережі деяка втрата якості голосового зв'язку при сильній завантаженості ресурсів цілком терпима за умови, що середній показник буде цілком задовільним, то в разі мережі загального користування все набагато серйозніше.

Оскільки провайдер надає деякий сервіс і бере за нього гроші, він зобов'язаний гарантувати його якість. Навіть якщо клієнт згоден (хоча в умовах жорсткої конкуренції на ринку телекомунікацій це малоймовірно) час від часу миритися з не дуже високим рівнем якості, він може пред'явити претензії у разі серйозних або тривалих проблем. Як би там не було, оператор змушений стежити за якістю послуг, що надаються, для чого в разі їх масштабного надання йому потрібна відповідна апаратура і програмне забезпечення, яке досить дорого і є не у всіх точках мережі [22].

З точки зору масштабованості (якщо відволіктися від проблем з неконтрольованим погіршенням якості при зростанні навантаження на мережу) IP-телефонія видається цілком закінченим рішенням. По-перше, оскільки з'єднання на базі протоколу IP може починатися (і закінчуватися) в будь-якій точці мережі від абонента до магістралі. Відповідно, IP-телефонію в мережі можна вводити ділянку за ділянкою, що, до речі, на руку і з точки зору міграції, так як її можна проводити «зверху вниз», «знизу вгору» або з якоїсь іншої схемою. Для рішень IP-телефонії характерна певна модульна: кількість і потужність різних вузлів - шлюзів, gatekeeper («воротарів» - так в

термінології VoIP іменуються сервери обробки номерних планів) - можна нарощувати практично незалежно, відповідно до поточних потреб. Природно, проблеми нарощування ресурсів власне мережевої інфраструктури ми зараз не враховуємо, оскільки вузли самої мережі можуть бути незалежні від системи IP-телефонії, а можуть і поєднувати в собі їх функції.

1.2. Мережа IP-телефонії на базі протоколу SIP

Основні характеристики протоколу. SIP - протокол передачі даних, що описує спосіб встановлення і завершення користувацького інтернет-сеансу, що включає обмін мультимедійним вмістом (IP-телефонія, відео-та аудіоконференції, миттєві повідомлення, онлайн-ігри) [2].

Протокол описує, яким чином клієнтську програму (наприклад, софтфон) може запросити початок з'єднання в іншого, можливо, фізично віддаленого клієнта, що знаходиться в тій же мережі, використовуючи його унікальне ім'я. Протокол визначає спосіб узгодження між клієнтами про відкриття каналів обміну на основі інших протоколів, які можуть використовуватися для безпосередньої передачі інформації [2]. Допускається додавання або видалення таких каналів протягом встановленого сеансу, а також підключення та відключення додаткових клієнтів (тобто допускається участь в обміні більше двох сторін - конференц-зв'язок). Протокол також визначає порядок завершення сеансу.

У певному сенсі прабатьком протоколу SIP є протокол перенесення гіпертексту - HTTP (Hypertext Transfer Protocol, RFC 2068). Протокол SIP успадкував від нього синтаксис і архітектуру «Клієнт-сервер», яку ілюструє рисунок [2].

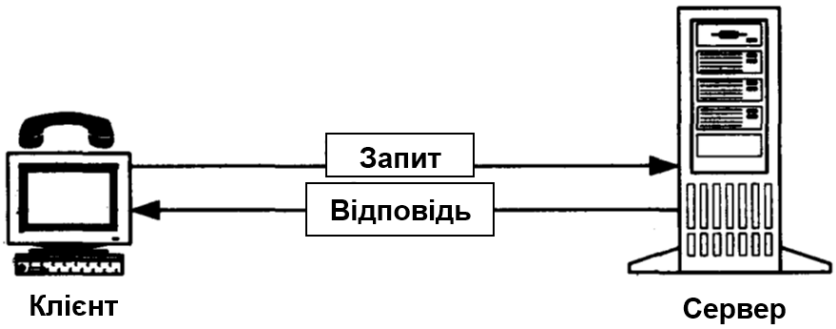

Рис. 1.3. Архітектура "клієнт-сервер"

Клієнт видає запити, в яких вказує, що він бажає отримати від сервера. Сервер приймає запит, обробляє його і видає відповідь, який може містити повідомлення про успішне виконанні запиту, повідомлення про помилку або інформацію, затребувану клієнтом.

Управління процесом обслуговування виклику розподілено між різними елементами мережі SIP. основним функціональним елементом, що реалізує функції управління з'єднанням, є термінал. Інші елементи мережі відповідають за маршрутизацію викликів, а в деяких випадках надають додаткові послуги [2].

Архітектура мережі на базі протоколу SIP. Підхід SIP до побудови мереж IP-телефонії набагато простіше в реалізації, ніж H.323, але менше підходить для організації взаємодії з телефонними мережами. В основному це пов'язано з тим, що протокол сигналізації SIP, який базується на протоколі HTTP, погано узгоджується з системами сигналізації, що використовуються в ТМЗК. Тому протокол SIP більш підходить провайдерам послуг інтернет для надання послуги IP-телефонії, причому ця послуга буде всього лише частиною пакета послуг [2].

Проте, протокол SIP підтримує послуги інтелектуальної мережі (IN), такі як перетворення (меппінг) імен, переадресація і маршрутизація , що істотно для використання SIP як протокол сигналізації в мережі загального користування, де пріоритетним завданням оператора є надання широкого спектру телефонних послуг. Іншою важливою особливістю протоколу SIP є підтримка мобільності користувача, тобто його здатності отримувати доступ до замовлених послуг в будь-якому місці і з будь-якого терміналу, а також здатності мережі ідентифікувати і аутентифікувати користувача

при його переміщенні з одного місця в інше. Це властивість SIP не є унікальною, наприклад, протокол H.323 теж в значній мірі підтримує таку можливість. Зараз настав момент, коли ця можливість стане головною привабливою рисою мереж IP-телефонії нового покоління. Даний режим роботи потребують дистанційної реєстрації користувачів на сервері ідентифікації і аутентифікації [14].

Перейдемо безпосередньо до архітектури мереж, що базуються на протоколі SIP.

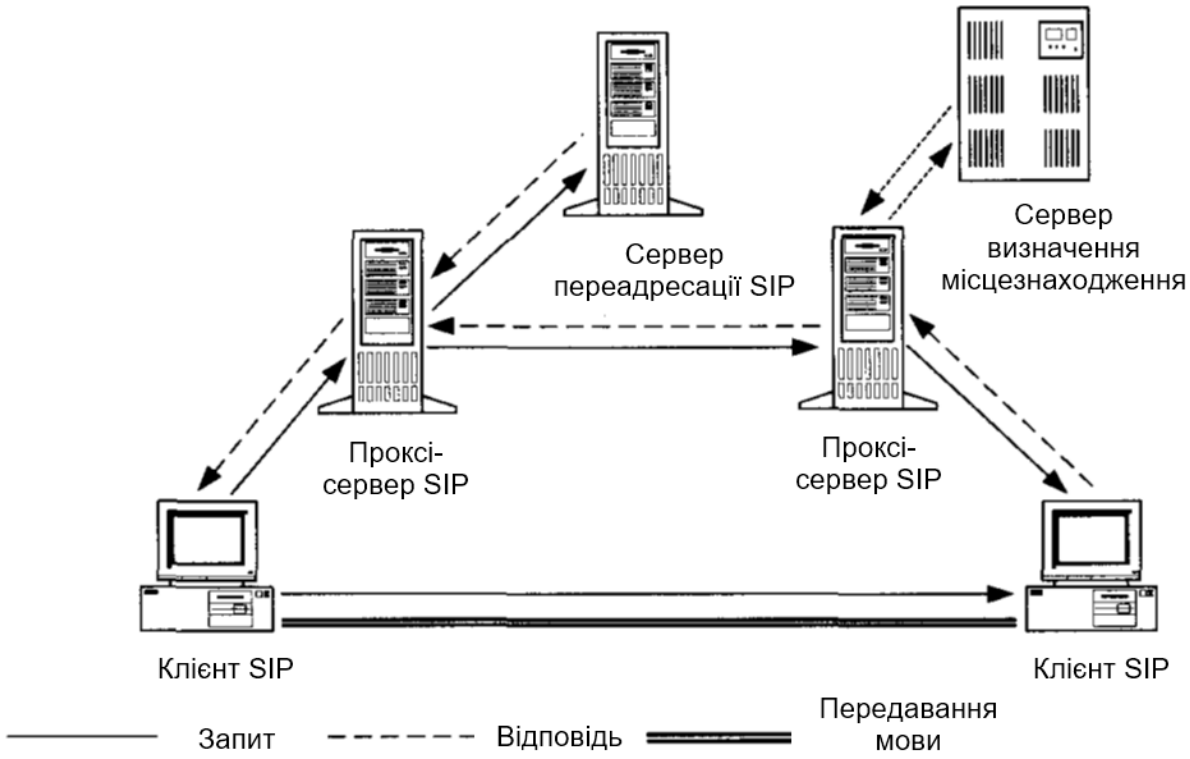

Рис. 1.4. Приклад мережі на базі протоколу SIP

Мережа SIP містить основні елементи трьох видів: агенти користувача, проксі-сервери і сервери переадресації.

Агенти користувача (User Agent або SIP client) є додатками термінального обладнання і включають в себе дві складові: агент користувача - клієнт (User Agent Client - UAC) і агент користувача - сервер (User Agent Server - UAS), інакше відомі як клієнт і сервер відповідно. Клієнт UAC ініціює SIP-запити, тобто виступає в якості викликає боку. Сервер UAS приймає запити і повертає відповіді, тобто виступає в якості викликається сторони [14].

Крім того, існує два типи мережевих серверів SIP: проксі сервери (сервери-посередники) і сервери переадресації. Сервери SIP можуть працювати як в режимі зі збереженням станів поточних з'єднань (statefull), так і в режимі без збереження станів поточних з'єднань (stateless). Сервер SIP, що функціонує в режимі stateless, може обслужити як завгодно велику кількість користувачів, на відміну від H.323, який може одночасно працювати з обмеженою кількістю користувачів [6].

Проксі-сервер (Proxy-server) діє «від імені інших клієнтів» і містить функції клієнта (UAC) і сервера (UAS). Цей сервер інтерпретує і може перезаписувати заголовки запитів перед відправкою їх до інших серверів. Відповідні повідомлення слідують тим самим шляхом назад до проксі-сервера, а не до клієнту.

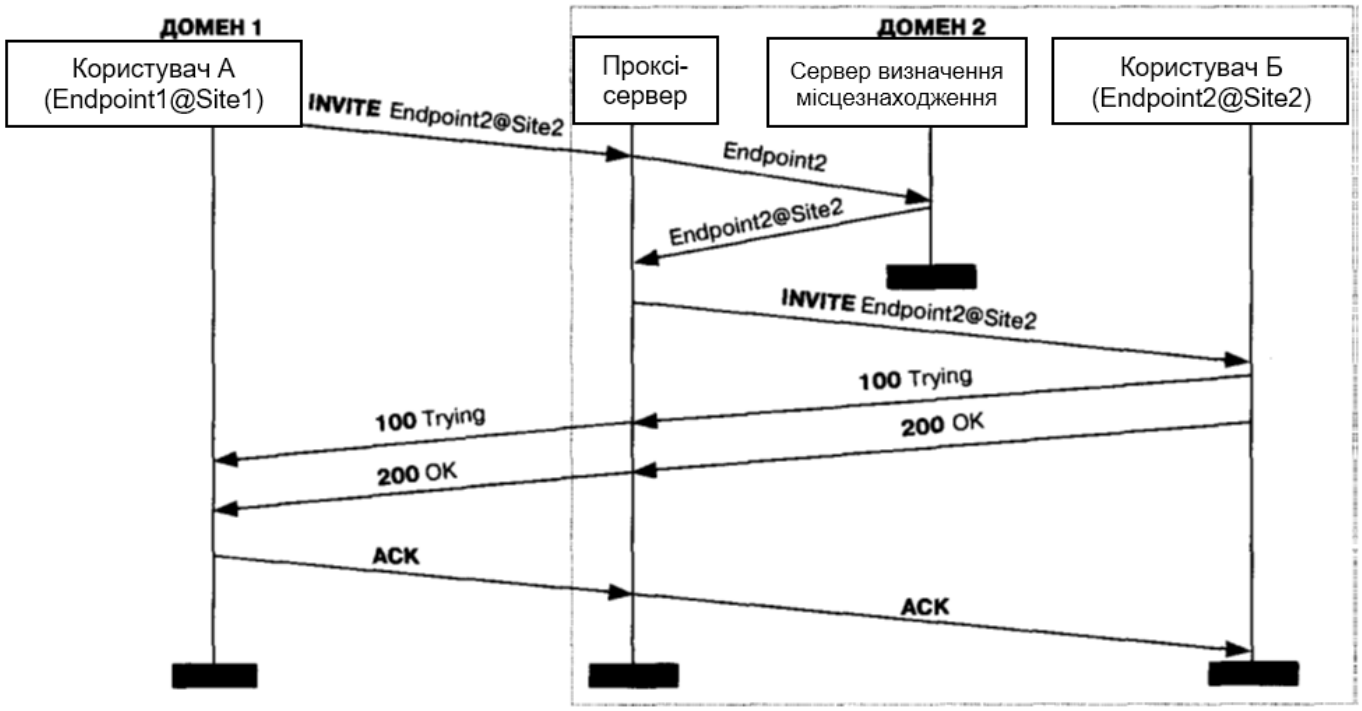

Рис. 1.5. Мережа SIP з проксі-сервером

Нижче представлений алгоритм встановлення з'єднання з допомогою протоколу SIP за участю проксі-сервера [18]:

1. Проксі-сервер приймає запит з'єднання INVITE від обладнання викликає користувача.

2. Проксі-сервер встановлює місцезнаходження клієнта з допомогою сервера позиціонування (location server).

3. Проксі-сервер передає запит INVITE викликається користувачеві.

4. Обладнання викликається користувача повідомляє останнього про вхідний дзвінок і повертає проксі-сервера повідомлення про те, що запит INVITE обробляється (код 100). Проксі-сервер, в свою чергу, направляє цю інформацію обладнанню викликає користувача.

5. Коли абонент приймає виклик, його обладнання сповіщає про це проксі-сервер (код 200), який переправляє інформацію про те, що виклик прийнятий, до обладнання викликає користувача.

6. Первинна сторона підтверджує встановлення з'єднання передачею запиту АСК, яке проксі-сервер переправляє викликається стороні. встановлення з'єднання закінчено, абоненти можуть обмінюватися мовною інформацією.

Сервер переадресації (Redirect server) визначає поточне місце розташування абонента і повідомляє його первинному користувачеві. Для визначення поточного місцеположення абонента сервер пере адресації звертається до сервера визначення місця розташування, принципи роботи якого в документі RFC 2543 не специфіковані [16].

Алгоритм встановлення з'єднання з використанням протоколу SIP за участю сервера переадресації виглядає наступним чином [2]:

1. Сервер переадресації приймає від викликаючої сторони запит з'єднання INVITE і зв'язується з сервером визначення місцезнаходження, який видає поточну адресу викликається клієнта.

2. Сервер переадресації передає цю адресу викликаючій стороні. На відміну від проксі-сервера, запит INVITE до устаткування викликається користувача сервер переадресації його не передає.

3. Обладнання викликає користувача підтверджує завершення транзакції з сервером переадресації запитом АСК.

4. Далі обладнання викликає користувача передає запит INVITE на адресу, отриманий від сервера переадресації.

5. Обладнання викликає користувача повідомляє останнього про вхідний дзвінок і повертає викликаючому обладнанню повідомлення про те, що запит INVITE обробляється (Код 100).

6. Коли абонент приймає виклик, про це сповіщається обладнання викликає користувача (код 200). Встановлення з'єднання закінчене, абоненти можуть обмінюватися мовною інформацією.

Існує також і безсерверний варіант з'єднання, коли один термінал може передати запит іншому терміналу безпосередньо.

Дамо коротку характеристику самого протоколу SIP. Слід помітити, що повідомлення SIP можуть переноситися як протоколом TCP, так і протоколом UDP.

Протокол SIP передбачає 6 запитів і відповідей на них. Сигналізація SIP дає можливість призначеним для користувача агентам і мережевих серверів визначати місце розташування, видавати запити і керувати з'єднаннями.

INVITE - запит залучає користувача або послугу до участі в сеансі зв'язку і містить опис параметрів зв'язку з цим. За допомогою цього запиту користувач може визначити функціональні можливості терміналу свого партнера по зв'язку і розпочати сеанс зв'язку, використовуючи обмежену кількість повідомлень і підтверджень їх прийому.

АСК - запит підтверджує прийом від викликається сторони відповіді на команду INVITE і завершує транзакцію.

OPTIONS - запит дозволяє отримати інформацію про функціональні можливості користувацьких агентів і мережевих серверів. Однак цей запит не використовується для організації сеансів зв'язку.

BYE - запит використовується викликає і викликається сторонами для руйнування з'єднання. Перед тим як зруйнувати з'єднання, призначені для користувача агенти відправляють цей запит до сервера, повідомляючи про намір припинити сеанс зв'язку.

CANCEL- запит дозволяє призначеним для користувача агентам і мережевих серверів скасувати будь раніше переданий запит, якщо відповідь на неї ще не було отримано [10].

1.3. Якість обслуговування мережі провайдера IP-телефонії

Характер інформації, переданої по мережах з маршрутизацією пакетів IP, сьогодні драматично змінюється. Крім передачі даних, IP-мережі використовуються для прослуховування музичних програм, для відтворення відео, обміну мовною інформацією, проведення мультимедійних конференцій, оперативного контролю / управління, мережевих ігор та інших програм реального часу.

Протокол IP, докладно спочатку не призначався для обміну інформацією в реальному часі. Адже пакети одного і того ж потоку даних маршрутизируются по мережі незалежно один від одного, а час обробки пакетів у вузлах може змінюватися в широких межах, в силу чого такі параметри передачі як затримка і варіація затримки пакетів також можуть змінюватися. А параметри якості мережевих послуг, що забезпечують передачу інформації в реальному часі, як відомо, сильно залежать від характеристик затримок пакетів, в яких ця інформація переноситься.

Транспортні протоколи стека TCP / IP, що реалізуються в обладнанні користувачів і функціонують поверх протоколу IP, також не забезпечують високої якості обслуговування трафіку, чутливого до затримок. Протокол TCP, хоч і гарантує достовірну доставку інформації, але переносить її з непередбачуваними затримками. Протокол UDP, який, як правило, використовується для перенесення інформації в реальному часі, забезпечує меншу, в порівнянні з протоколом TCP, час затримки, але, як і протокол IP, не містить жодних механізмів забезпечення якості обслуговування [2].

Крім того, в самій мережі Інтернет немає ніяких механізмів, підтримують на належному рівні якість передачі інформації у реальному часі. Іншими словами, ні в вузлах IP-мереж, ні в обладнанні користувачів в даний час немає коштів, забезпечують гарантовану якість обслуговування.

Разом з тим, в наявності необхідність отримання від мережі гарантій, що в періоди перевантаження пакети з інформацією, чутливої до затримок, що не будуть простоювати в чергах або, принаймні, отримають більш високий пріоритет, ніж пакети з

інформацією, не чутливої до затримок. Інакше кажучи, необхідно гарантувати доставку такої інформації, як мова, відео та мультимедіа, в реальному часі з мінімально можливою затримкою. Для цієї мети в мережі повинні бути реалізовані механізми, що гарантують потрібну якість обслуговування (Quality of Service - QoS). Аналізу таких механізмів і присвячена ця глава.

Ідеальною була б наступна ситуація. Додаток «домовляється» з мережею про те, що пакети такого-то потоку даних із середньою швидкістю передачі X Кбіт / с будуть доставлятися від одного кінця з'єднання до іншого з затримкою не більше Y мс, і що мережу протягом всього з'єднання буде стежити за виконанням цього договору. Крім зазначеної характеристики, мережа повинна підтримувати узгоджені значення таких параметрів передачі як мінімально доступна смуга частот, максимальна зміна затримки (джиттер), максимальні втрати пакетів.

В кінцевому рахунку, якість обслуговування залежить не тільки від мережі, але і від обладнання користувача. Слабкі системні ресурси обладнання користувача - малий обсяг оперативної пам'яті, невисока продуктивність центрального процесора і інше, можуть зробити показники якості обслуговування неприйнятними для користувача незалежно від того, як дотримується «домовленість» мережі. Хороша якість обслуговування досягається лише тоді, коли користувач задовільно оцінює роботу системи в цілому [9].

Слід зазначити, що висока якість обслуговування представляє інтерес не тільки для кінцевого користувача, а й для самого провайдера IP-телефонії. Наприклад, дослідження, проведені в мережах мобільного зв'язку, показали, що з поліпшенням якості передачі мови абоненти частіше і довше користуються послугами таких мереж, що означає збільшення річних доходів операторів.

Щоб домогтися гарантій якості обслуговування від мереж, спочатку на це не орієнтованих, необхідно «накласти» на мережу так звану QoS-архітектуру, яка включає в себе підтримку якості на всіх рівнях стека протоколів TCP / IP і під всіх мережевих елементах. Але і при цьому забезпечення гарантованої якості обслуговування все одно залишається самим слабким місцем процесу передачі інформації від джерела до приймача [9].

Оскільки все більше додатків стають розподіленими, все більше зростає потреба в підтримці якості обслуговування на нижніх мережевих рівнях. Це може викликати певні труднощі, так як навіть стандартні операційні системи робочих станцій не підтримують доставку інформації в реальному часі.

Крім того, якість обслуговування - це відносне поняття, його сенс залежить від програми, з якою працює користувач. Як вже зазначалося раніше, різні додатки вимагають різних рівнів або типів якості. Наприклад, швидше за все, користувача не засмутить той факт, що його текстовий файл буде передаватися на секунду довше, або що за першу половину часу передачі буде передано 80% файлу, а за другу - 20%. Водночас, при передачі мовної інформації такого роду явища дуже небажані або навіть неприпустимі.

РОЗДІЛ 2
ТЕХНІЧНЕ РІШЕННЯ ЩОДО ПРОЕКТУВАННЯ МЕРЕЖІ ПРОВАЙДЕРА IP-ТЕЛЕФОНІЇ

2.1. Проектування захищених систем зв'язку в розподілених обчислювальних системах

Виділений канал зв'язку між об'єктами розподіленої обчислювальної системи. Найкраще з точки зору безпеки взаємодію об'єктів в розподіленої ОС можливо тільки по фізично виділеному каналу [3].

Всі об'єкти розподіленої обчислювальної системи взаємодіють між собою по каналах зв'язку. Причина успіху, що складається в використанні в РОС для зв'язку між об'єктами широкомовної середовища передачі яке означає, що всі об'єкти розподіленої обчислювальної системи підключаються до однієї загальної шині. Це призводить до того, що повідомлення, призначене (адресоване) тільки одному об'єкту системи, буде отримано усіма її об'єктами. Однак тільки об'єкт, адреса якого вказана в заголовку повідомлення як адреса призначення, буде вважатися тим об'єктом, кому це повідомлення безпосередньо прямувало. Очевидно, що в РОС з топологією "загальна шина" необхідно використовувати спеціальні методи ідентифікації, так як ідентифікація на канальному рівні можлива тільки в разі використання мережевих криптокарт [5].

Також очевидно, що ідеальною з точки зору безпеки буде взаємодія об'єктів розподіленої обчислювальної системи по виділених каналах. Існують два можливі способи організації топології розподіленої ОС з виділеними каналами. У першому випадку кожен об'єкт пов'язується фізичними лініями зв'язку з усіма об'єктами системи. У другому випадку в системі може використовуватися мережевий концентратор, через який здійснюється зв'язок між об'єктами (топологія "зірка") [21].

Плюси розподіленої ОС з виділеними каналами зв'язку між об'єктами полягають у наступному [19]:

- передача повідомлень здійснюється безпосередньо між джерелом і приймачем, минаючи інші об'єкти системи. У такій системі в разі відсутності доступу до об'єктів, через які здійснюється передача повідомлення, не існує програмної можливості для аналізу мережевого трафіку;

- є можливість ідентифікувати об'єкти розподіленої системи на канальному рівні за їхніми адресами без використання спеціальних криптоалгоритмів шифрування трафіку. Це виявляється, оскільки система побудована так, що з даного виділеному каналу здійсненна зв'язок тільки з одним певним об'єктом. Поява в такий розподіленої системі помилкового об'єкта неможливо без апаратного втручання (підключення додаткового пристрою до каналу зв'язку);

- система з виділеними каналами зв'язку - це система, в якій відсутня невизначеність з інформацією про її об'єктах. Кожен об'єкт в такій системі спочатку однозначно ідентифікується і володіє повною інформацією про інші об'єкти системи.

До мінусів РОС з виділеними каналами відносяться:

- складність реалізації і високі витрати на створення системи;

- обмежене число об'єктів системи (залежить від числа входів у концентратора);

- складність внесення в систему нового об'єкта.

Аналізуючи всі плюси і мінуси використання виділених каналів для побудови захищених систем зв'язку між об'єктами РОС, можна зробити висновок, що створення розподілених систем тільки з використанням широкомовної середовища передачі або тільки з виділеними каналами неефективно. Тому видається правильним при побудові розподілених обчислювальних систем з розгалуженою топологією і великим числом об'єктів використовувати комбіновані варіанти з'єднань об'єктів. Для забезпечення зв'язку між об'єктами великій мірі значущості можна використовувати виділений канал. Зв'язок менш значущих об'єктів системи може здійснюватися з використанням комбінації загальна шина-виділений канал.

У варіанти мережевих топологій з виділеними каналами зв'язку розглянуті тільки фізичні канали зв'язку і запропоновані більш-менш безпечні способи взає-

модії об'єктів системи по цих каналах. Однак вибір безпечної топології РОС є необхідним, але аж ніяк не достатньою умовою для створення захищених систем зв'язку між об'єктами розподілених ОС.

Віртуальний канал як засіб забезпечення додаткової ідентифікації / аутентифікації об'єктів в розподіленої ОС. При створенні ВК можуть використовуватись криптоалгоритми з відкритим ключем (наприклад, в Internet прийнято подібний стандарт захисту ВК, званий Secure Socket Layer - SSL). Дані криптоалгоритми засновані на результатах досліджень, отриманих в 70-х роках У. Діффі. Він ввів поняття односторонньої функції з потайним входом. Це не просто обчислюється в одну сторону функція, обіг якої неможливо, вона містить потайний вхід (trapdoor), який дозволяє обчислювати зворотну функцію особі, яка знає секретний ключ [10]. Сутність криптографії з відкритим ключем (або двохключового криптографії) в тому, що ключі, наявні в криптосистеме, входять в неї парами і кожна пара задовольняє наступним двом властивостям [15]:

- текст, зашифрований на одному ключі, може бути дешифрований на іншому;
- знання одного ключа не дозволяє обчислити інший.

Тому один з ключів може бути опублікований. При опублікованому (відкритому) ключі шифрування і секретному ключі дешифрування виходить система шифрування з відкритим ключем. Кожен користувач мережі зв'язку може зашифрувати повідомлення за допомогою відкритого ключа, а розшифрувати його зможе тільки власник секретного ключа. При опублікуванні ключа дешифрування виходить система цифрового підпису. Тут тільки власник секретного ключа створення підпису може правильно зашифрувати текст (тобто підписати його), а після перевірки підпису (дешифрувати текст) може будь-хто на підставі опублікованого ключа перевірки підпису.

Об'єкти А і В домовилися про вибір в якості загальної початкової інформації великого простого числа р і примітивного кореня ступеня р - 1 з 1 в поле відрахувань по модулю р. Тоді ці користувачі діють відповідно до протоколу:

- А виробляє випадкове число x, обчислює число a^x (mod p) і посилає його B;
- B виробляє випадкове число y, обчислює число a^y (mod p) і посилає його A;
- потім A і B зводять отримане число в ступінь зі своїм показником і отримують число a^{xy} (mod p).

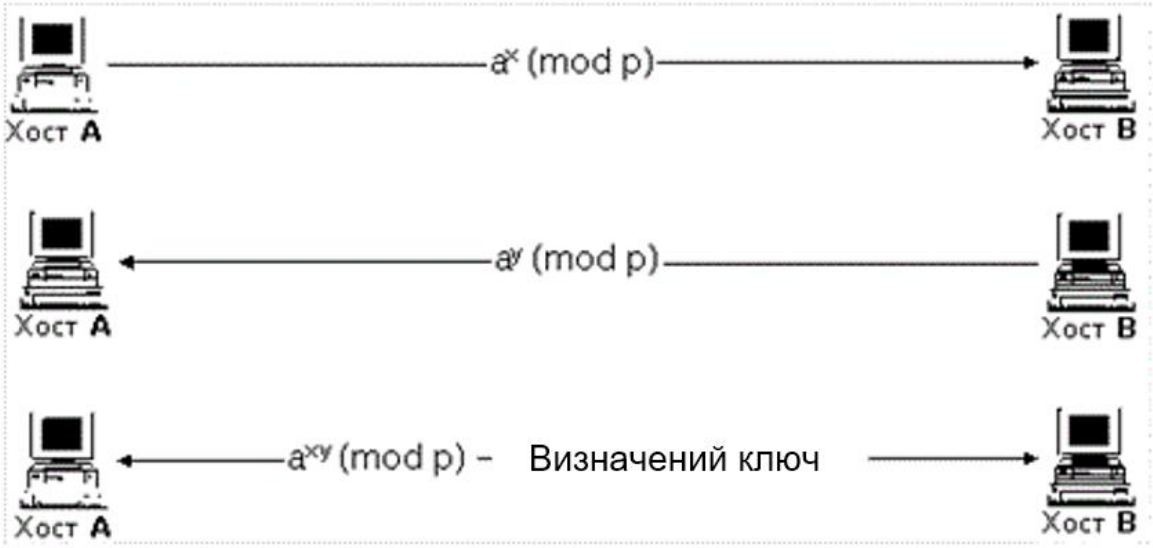

Рис. 2.1. Безпечний зв'язок з використанням шифрування

Це число і є сеансовим ключем для одноключевого алгоритму, наприклад, AES. Для розкриття цього ключа криптоаналітику необхідно по відомим a^x (mod p), a^y (mod p) знайти a^{xy} (mod p), тобто знайти x або y. Знаходження числа x по його експоненті a^x (mod p) називається завданням дискретного логарифмування в простому полі. Це завдання є тяжким для вирішення, і тому отриманий ключ, в принципі, може бути стійким.

Особливість даного криптоалгоритму полягає в тому, що перехоплення по каналу зв'язку пересилаються в процесі створення віртуального каналу повідомлень a^x (mod p) і a^y (mod p) не дозволить атакуючому отримати кінцевий ключ шифрування axy (mod p). Цей ключ далі повинен використовуватися, по-перше, для

цифрового підпису повідомлень і, по-друге, для їх криптозахисту. Цифровий підпис повідомлень дозволяє надійно ідентифікувати об'єкт розподіленої ОС і віртуальний канал [15].

Контроль за маршрутом повідомлення в розподіленій ОС. Кожен об'єкт розподіленої ОС повинен володіти адресою, унікально його ідентифікує. Для того, щоб повідомлення від одного об'єкта було передано на інший об'єкт системи, воно повинно пройти через ланцюг маршрутизаторів, завдання яких - проаналізувавши адреса призначення, зазначений в повідомленні, вибрати оптимальний маршрут і, виходячи з нього, переправити пакет або на наступний маршрутизатор або безпосередньо абоненту, якщо він безпосередньо підключений до даного вузла. Таким чином, маршрут до об'єкта визначається ланцюжком вузлів, пройдених повідомленням. Як було показано раніше, маршрут повідомлення може бути інформацією, аутентифицирующей з точністю до підмережі справжність адреси суб'єкта, відіславши повідомлення. Очевидно, що перед будь-якою системою зв'язку об'єктів в РОС встає стандартна проблема перевірки автентичності адреси повідомлення, що прийшов на об'єкт. Це завдання, з одного боку, можна вирішити, запровадивши додаткову ідентифікацію повідомлень на іншому, більш високому рівні OSI. Так, адресація здійснюється на мережевому рівні, а додаткова ідентифікація, наприклад, на транспортному. Однак подібне рішення не дозволить уникнути проблеми контролю за створенням з'єднань, так як додаткова ідентифікація абонентів буде можлива тільки після створення з'єднання. Тому розробникам розподіленої ОС можна запропонувати наступні шляхи вирішення проблеми.

Функцію перевірки автентичності адреси відправника можна покласти на маршрутизатор. Це нескладно зробити, так як маршрутизатор може відстежити, звідки до нього прийшов пакет (від іншого маршрутизатора або від підключеного до нього хоста з підмереж, безпосередньо підключених до даного маршрутизатора). Маршрутизатор може перевіряти відповідність адреси відправника з адресою відповідної підмережі, звідки прийшло повідомлення. У разі збігу повідомлення пересилається далі, а в іншому випадку - фільтрується. Цей спосіб дозволить на початковій стадії відкинути пакети з невірними адресами відправника [8].

Інший варіант рішення може полягати в створенні в заголовку пакета спеціальних полів, куди кожен маршрутизатор, через який проходить пакет, заносить маршрутну інформацію (частина своєї адреси, наприклад). При цьому перший маршрутизатор, на який надійшов пакет, заносить також інформацію про клас мережі (A, B, C), звідки прийшов пакет. Проте, внесення в пакет адрес всіх пройдених по шляху маршрутизаторів буде неоптимальним рішенням, так як в цьому випадку складно заздалегідь визначити максимальний розмір заголовка пакету.

Коли повідомлення дійде до кінцевого адресата, в його заголовку буде повністю відзначений пройдений маршрут. За цим маршрутом, незалежно від зазначеного в пакеті мережевого адреси відправника, можна, по-перше, з точністю до підмережі ідентифікувати справжність адреси і, по-друге, визначити з точністю до підмережі істинний адресу відправника. Отже, отримавши таке повідомлення з вказаним маршрутом, мережева операційна система аналізує маршрут і перевіряє справжність адреси відправника. У разі його недостовірності пакет відкидається.

2.2. Методи криптографічного захисту голосового трафіку

Криптографія є важливою складовою для механізмів аутентифікації, цілісності і конфіденційності. Аутентифікація є засобом підтвердження особи відправника або одержувача інформації. Цілісність означає, що дані не були змінені, а конфіденційність створює ситуацію, при якій дані не може зрозуміти ніхто, крім їх відправника і одержувача. Зазвичай криптографічні механізми існують у вигляді алгоритму (математичної функції) і секретної величини (ключа). Алгорітми широко відомі, в секреті необхідно тримати тільки криптографічні ключі. Причому чим більше бітів в такому ключі, тим менше він вразливий [11].

У системах забезпечення безпеки використовуються три основних криптографічних методу:

- Симетричне шифрування;
- Асиметричне шифрування;
- Односторонні хеш-функції.

Всі існуючі технології аутентифікації, цілісності і конфіденційності створені на основі саме цих трьох методів. Наприклад, цифрові підписи можна представити у вигляді поєднання асиметричного шифрування з алгоритмом односторонньої хеш-функції для підтримки аутентифікації і цілісності даних.

Симетричне шифрування, за допомогою секретних ключів, в основному використовується для забезпечення конфіденційності даних. При цьому два користувача повинні спільно вибрати єдиний математичний алгоритм, який буде використовуватися для шифрування і розшифровки даних. Крім того, їм потрібно вибрати загальний ключ (секретний ключ), який буде використовуватися з прийнятим ними алгоритмом шифрування / розшифрування.

Використовуються алгоритми секретних ключів типу Data Encryption Standard (DES), 3DES (або «потрійний DES») і International Data Encryption Algorithm (IDEA). Ці алгоритми шифрують повідомлення блоками по 64 біта. Якщо обсяг повідомлення перевищує 64 біта (як це зазвичай і буває), необхідно розбити його на блоки по 64 біта в кожному, а потім якимось чином звести їх воєдино. Таке об'єднання, як правило, відбувається одним з наступних чотирьох методів: електронної кодової книги (ЄСВ), ланцюжки зашифрованих блоків (CBC), x-бітової зашифрованою зворотного зв'язку (CFB-x) або вихідний зворотного зв'язку (OFB) [3].

Шифрування за допомогою секретного ключа найчастіше використовується для підтримки конфіденційності даних і дуже ефективно реалізується за допомогою незмінних «вшитих» програм (firmware). Цей метод можна використовувати для аутентифікації і підтримки цілісності даних, але метод цифрового підпису є більш ефективним.

Метод секретних ключів має такі недоліки [3]:

- Необхідно часто міняти секретні ключі, оскільки завжди існує ризик їх випадкового розкриття;

- Важко забезпечити безпечне генерування і поширення секретних ключів.

Асиметричне шифрування часто називають шифруванням за допомогою загального ключа, при якому використовуються різні, але взаємно доповнюють одна одну ключі і алгоритми шифрування і розшифровки. Цей механізм покладається на два

взаємопов'язаних ключа: загального ключа і приватного ключа. Найбільш типові приклади використання алгоритмів загальних ключів:

- Забезпечення конфіденційності даних;
- Аутентифікація відправника;
- Безпечне отримання загальних ключів для спільного використання.

Важливим аспектом асиметричного шифрування є те, що приватний ключ повинен зберігатися в таємниці. Якщо приватний ключ буде розкрита, то людина, яка знає цей ключ, зможе виступати від вашого імені, отримувати ваші повідомлення і відправляти повідомлення так, ніби це зробили ви.

Механізми генерування пар загальних / приватних ключів є досить складними, але в результаті виходять пари дуже великих випадкових чисел, одне з яких стає загальним ключем, а інше - приватним. Генерування таких чисел вимагає великих процесорних потужностей, оскільки ці числа, а також їхні твори повинні відповідати суворим математичним критеріям. Однак цей процес генерування абсолютно необхідний для забезпечення унікальності кожної пари загальних / приватних ключів. Алгоритми шифрування з допомогою загальних ключів рідко використовуються для підтримки конфіденційності даних через обмеження продуктивності. Замість цього їх часто використовують в додатках, де аутентифікація проводиться за допомогою цифрового підпису та управління ключами.

Серед найбільш відомих алгоритмів загальних ключів можна назвати RSA і ElGamal.

Безпечної хеш-функцією називається функція, яку легко розрахувати, але зворотне відновлення якої вимагає непропорційно великих зусиль. Вхідне повідомлення пропускається через математичну функцію (хеш-функцію), і в результаті на виході отримують якусь послідовність бітів. Ця послідовність називається «хеш» (або «результат обробки повідомлення»). Цей процес неможливо відновити.

Хеш-функція приймає повідомлення будь-якої довжини і видає на виході хеш фіксованої довжини. Звичайні хеш-функції включають:

- Алгоритм Message Digest 4 (MD4);
- Алгоритм Message Digest 5 (MD5);

- Алгоритм безпечного хеша (Secure Hash Algorithm - SHA) [3].

Технологія шифрування часто використовується в додатках, пов'язаних з управлінням ключами й аутентифікації. Наприклад, алгоритм Діффі-Хеллмана дозволяє двом сторонам створити загальний для них секретний ключ, відомий тільки їм двом, незважаючи на те, що зв'язок між ними здійснюється по незахищеному каналу. Потім цей секретний ключ використовується для шифрування даних за допомогою алгоритму секретного ключа. Важливо відзначити, що на сьогодні поки що не створено коштів для визначення автора такого ключа, тому обмін повідомленнями, зашифрованими цим способом, може піддаватися атакам хакерів. Алгоритм Діффі-Хеллмана використовується для підтримки конфіденційності даних, але не використовується для аутентифікації. Аутентифікація в даному випадку досягається за допомогою цифрового підпису.

Цифровий підпис є зашифрований хеш, який додається до документа. Вона може використовуватися для аутентифікації відправника та цілісності документа. Цифрові підписи можна створювати за допомогою поєднання хеш-функцій і криптографії загальних ключів [16].

Повідомлення, яке відправляється по каналу зв'язку, складається з документа і цифрового підпису. На іншому кінці каналу зв'язку повідомлення ділиться на оригінальний документ і цифровий підпис. Так як цифровий підпис була зашифрована приватним ключем, то на приймальному кінці можна провести її розшифровку за допомогою загального ключа. Таким чином, на приймальному кінці виходить розшифрований хеш. Далі подається текст документа на вхід тієї ж функції, яку використовувала передає сторона. Якщо на виході вийде той же хеш, який був отриманий в повідомленні, цілісність документа і особу відправника можна вважати доведеними.

Цифровим сертифікатом називається повідомлення з цифровим підписом, яке в даний час зазвичай використовується для підтвердження дійсності загального ключа. Цифровий сертифікат в стандартному форматі X.509 включає наступні елементи:

- Номер версії;
- Серійний номер сертифіката;
- Емітент інформації про алгоритм;

- Емітент сертифікату;

- Дати початку і закінчення дії сертифіката;

- Інформація про алгоритм загального ключа суб'єкта сертифіката;

- Підпис емітує організації.

На практиці часто використовують спільно шифрування і цифрові сертифікати. Наприклад, маршрутизатор і міжмережевий екран мають по одній парі загальних / приватних ключів. Припустимо, що організації (CA) вдалося отримати сертифікати X.509 для маршрутизатора і міжмережевого екрану по захищених каналах. Далі припустимо, що маршрутизатор і міжмережевий екран теж отримали копії загального ключа CA по захищених каналах [2]. Тепер, якщо на маршрутизаторі є трафік, призначений для брандмауера, і якщо маршрутизатор хоче забезпечити аутентифікацію і конфіденційність даних, необхідно зробити наступні кроки.

1. Маршрутизатор відправляє в організацію CA запит на отримання загального ключа брандмауера.

2. CA відправляє йому сертифікат брандмауера, зашифрований приватним ключем CA.

3. Маршрутизатор розшифровує сертифікат загальним ключем CA і отримує загальний ключ брандмауера.

4. Брандмауер направляє CA запит на отримання загального ключа маршрутизатора.

5. CA відправляє йому сертифікат маршрутизатора, зашифрований приватним ключем CA.

6. Брандмауер розшифровує сертифікат загальним ключем CA і отримує загальний ключ маршрутизатора.

7. Маршрутизатор і міжмережевий екран використовують алгоритм Діффі-Хеллмана і шифрування за допомогою загальних ключів для аутентифікації.

8. За допомогою секретного ключа, отриманого в результаті використання алгоритму Діффі-Хеллмана, маршрутизатор і міжмережевий екран проводять обмін конфіденційними даними.

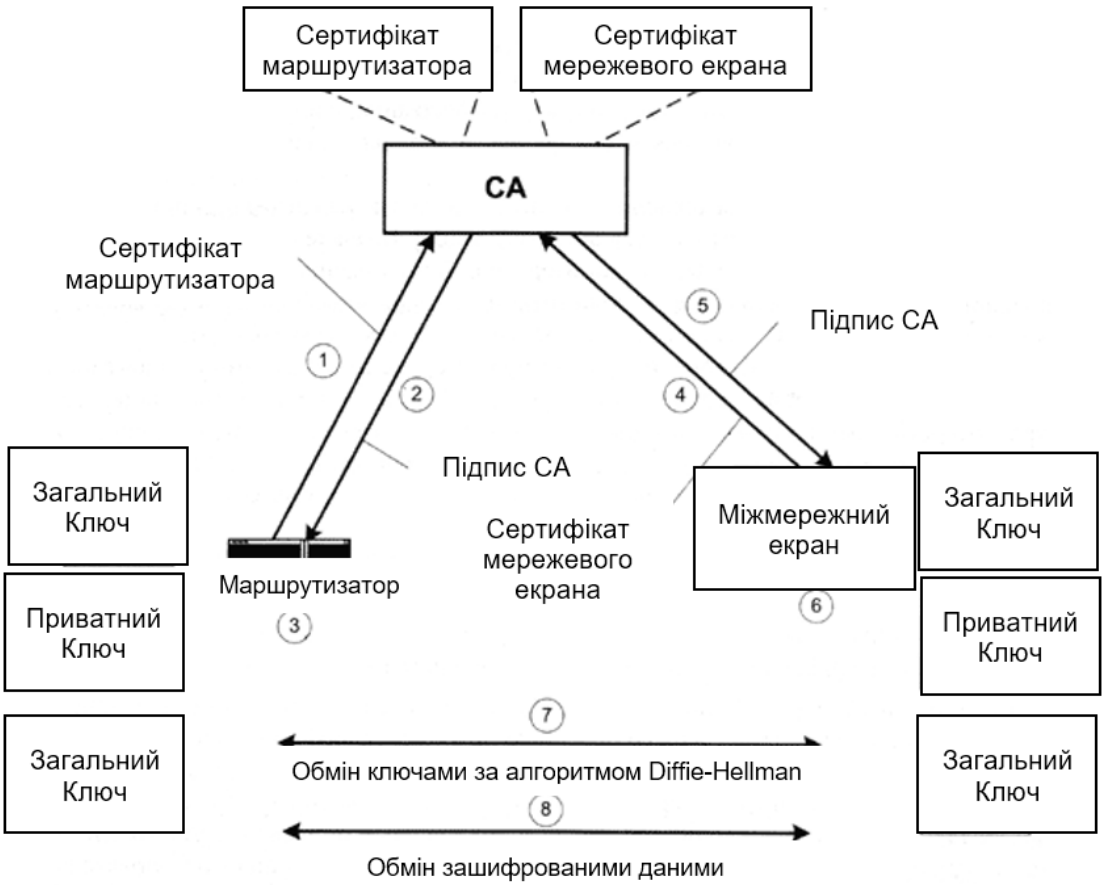

Рис. 2.2. Безпечний зв'язок з використанням шифрування

Для захисту конфіденційних переговорів і мінімізації можливості потрапляння конфіденційної або комерційної інформації в руки зловмисника необхідно захистити передані по відкритих каналах зв'язку дані від перехоплення і прослуховування.

Оскільки для здійснення дзвінка клієнт і сервер попередньо обмінюються службовими даними для встановлення з'єднання, дану проблему можна розділити на дві складові - захист службових даних IP-телефонії та захист голосового трафіку. Як засіб захисту можуть бути використані протокол TLS (Transport Layer Security) для захисту SIP сигналів і протокол SRTP (Secure Real Time Protocol) для захисту голосового трафіку.

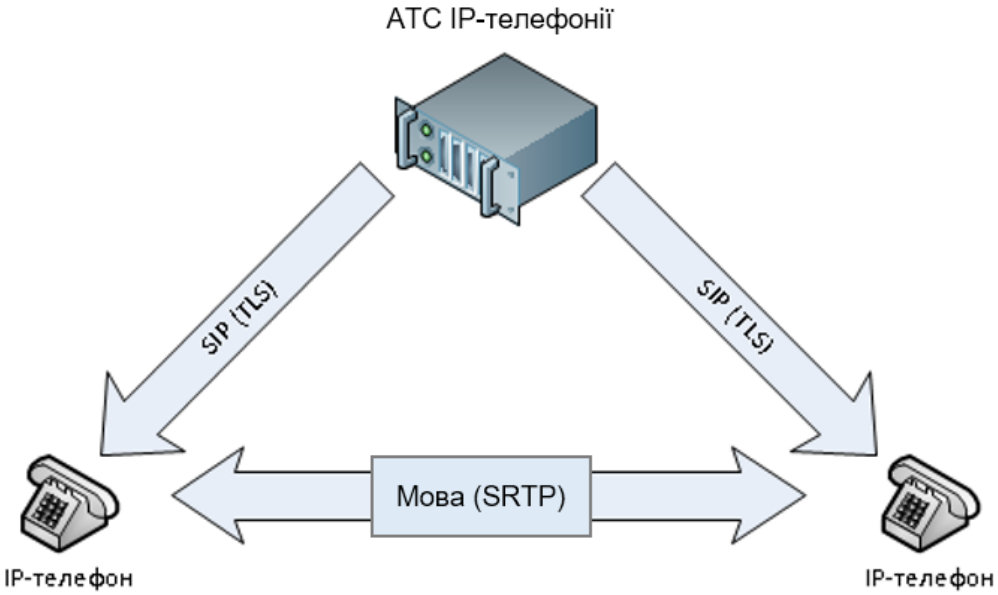

Рис. 2.3. Шифрування IP-телефонії [8]

TLS - криптографічний протокол, що забезпечує захищену передачу даних між вузлами в мережі, є стандартним методом для шифрування SIP-протоколу. TLS забезпечує конфіденційність і цілісність інформації, що передається, здійснює аутентифікацію.

Після встановлення захищеного з'єднання починається передача голосових даних, убезпечити які дозволяє застосування протоколу SRTP.

Протокол SRTP вважається одним з кращих способів захисту IP телефонії на базі IP-АТС. Основна перевага цього протоколу - відсутність будь-якого впливу на якість зв'язку. Схема роботи протоколу SRTP виглядає так: кожному здійснюваного вами дзвінку присвоюється унікальний код, який робить підслуховування розмов неавторизованих в системі користувачами практично неможливим. Завдяки цьому протокол SRTP вибирають як для звичайних, так і для конфіденційних дзвінків.

Не слід забувати про необхідність захисту підключення сервера телефонії до зовнішніх каналів зв'язку (мобільний зв'язок, телефонні мережі загального користування).

2.3. Технології аутентифікації

Аутентифікацією відбувається визначення користувача або кінцевого пристрою (клієнта, сервера, комутатора, маршрутизатора, брандмауера і т.д.) і його розташування в мережі з подальшою авторизацією користувачів і кінцевих пристроїв. Найбільш простим способом аутентифікації є використання паролів, але для підтримки високого рівня безпеки паролі доводиться часто міняти. Методи використання одноразових паролів застосовуються як і раніше широко. Серед них можна відзначити методи аутентифікації по протоколу S / Key або за допомогою спеціальних апаратних засобів (token password authentication). Механізм аутентифікації по протоколу Point-to-Point Protocol (PPP) часто застосовується в середовищі модемного доступу і включає використання протоколів Password Authentication Protocol (PAP), Challenge Handshake Protocol (CHAP) і Extensible Authentication Protocol (EAP). Розробка протоколу EAP все ще триває, але вже зараз він дає можливість більш гнучкого використання існуючих і тільки з'являються технологій аутентифікації в каналах PPP. TACACS + і Remote Access Dial-In User Service (RADIUS) - це протоколи, які підтримують масштабовані рішення в області аутентифікації. Протокол Kerberos (Цербер) використовується в обмежених областях для підтримки єдиної точки входу в мережу [2].

Система одноразових паролів S / Key, певна в RFC 1760, являє собою систему генерування одноразових паролів на основі стандартів MD4 і MD5. Вона призначена для боротьби «повторними атаками», коли хакер підслуховує канал, виділяє з трафіку ідентифікатор користувача і його пароль і надалі використовує їх для несанкціонованого доступу.

Система S / Key заснована на технології клієнт-сервер, де клієнтом зазвичай є персональний комп'ютер, а сервером - сервер аутентифікації. Спочатку і клієнта, і сервер потрібно налаштувати на єдину парольний фразу і рахунок ітерації. Клієнт починає обмін S / Key, відправляючи серверу пакет ініціалізації, а сервер у відповідь відправляє порядковий номер і випадкове число, так зване «зерно» (seed). Після цього клієнт генерує одноразовий пароль.

Після створення одноразового пароля його потрібно перевірити. Для цього клієнт передає одноразовий пароль на сервер, де він і перевіряється. Для перевірки аутентифікації система одноразово пропускає отриманий одноразовий пароль через захищену хеш-функцію. Якщо результат цієї операції збігається з попереднім паролем, що зберігаються у файлі, результат аутентифікації вважається позитивним, а новий пароль зберігається для подальшого використання.

Аутентифікація за допомогою апаратних засобів працює по одній з двох альтернативних схем:

- за схемою запит-відповідь;
- за схемою аутентифікації з синхронізацією за часом.

У схемі запит-відповідь користувач підключається до сервера аутентифікації, який, в свою чергу, пропонує ввести персональний ідентифікаційний номер (PIN) або призначений для користувача ідентифікатор (user ID). Користувач передає PIN або user ID на сервер, який потім робить «запит» (передає випадкове число, яке з'являється на екрані користувача). Користувач вводить це число в спеціальне апаратний пристрій, схоже на кредитну картку, де число запиту шифрується за допомогою призначеного для користувача шифрувального ключа. Результат шифрування відображається на екрані. Користувач відправляє цей результат на сервер аутентифікації. У той час як користувач підраховує цей результат, сервер аутентифікації розраховує цей же результат самостійно, використовуючи для цього базу даних, де зберігаються всі призначені для користувача ключі. Отримавши відповідь від користувача, сервер порівнює його з результатом власних обчислень. Якщо обидва результату збігаються, - користувач отримує доступ до мережі. Якщо результати виявляються різними, доступ до мережі не надається.

При використанні схеми з синхронізацією за часом на апаратному пристрої користувача і на сервері працює секретний алгоритм, який через певні синхронізовані проміжки часу генерує ідентичні паролі і замінює старі паролі на нові. Користувач може з'єднуватися із сервером аутентифікації, який запитує у користувача введення пароля. Після цього користувач вводить свій PIN в апаратне карткове пристрій, і в результаті на екран

виводиться деяка величина, яка являє собою одноразовий пароль. Цей пароль і відправляється на сервер. Сервер порівнює його з паролем, який був обчислений на самому сервері. Якщо паролі збігаються, користувач отримує доступ до мережі……

РОЗДІЛ 3
ПРОЕКТУВАННЯ ЗАХИЩЕНОЇ МЕРЕЖІ VOIP ПРОВАЙДЕРА

3.1. Проектування комплексних методів та засобів забезпечення захисту VoIP мережі

Основні методи та засоби захисту VoIP мережі. VoIP для передачі голосових даних задіє загальнодоступну мережу IP. Той, хто передає чи приймає дані по мережі IP в незахищеному вигляді, стає привабливою метою для хакерів, в тому числі, коли мова йде про голосових даних. Відповідно, інфраструктур VoIP загрожують ті ж небезпеки, що і для мереж передачі даних. Однак результати успішної атаки на мережу передачі голосових даних більш серйозні: затримане на кілька хвилин електронне лист або повільно працює браузер рідко призводять до тяжких наслідків, на відміну від переривання телефонної розмови або повного виходу з ладу системи комунікацій [14].

При проектуванні мережі застосування наступних заходів підвищує рівень захисту мережі VoIP провайдера [14]:

- З транзитним оператором передачі міжнародного трафіку використання виділений голосовий VLAN локальна комп'ютерна мережа для підключення VoIP-транка до обладнання оператора, замість підключення через мережу Інтернет, що істотно підвищує безпеку.
- Використовуються два мережевих інтерфейси. Використання декількох мережевих інтерфейсів на платформі, де SIP протокол повністю доступний тільки на внутрішньому мережевому адресу. А, наприклад, об'єднання клієнтів здійснюється по SIP протоколу, з явним відкриттям на firewall тільки IP адрес клієнтів і фільтрацією для всіх інших. У такій конфігурації у зловмисника відсутня фізична можливість атакувати обладнання VoIP з використанням вразливостей VoIP протоколів.

- Firewall з можливістю розпізнавання DoS атак. При ризиках атаки типу Denial Of Service (DoS), встановлюється спеціальне обладнання, яке розпізнає такий тип атак і автоматично блокує атакуючого з повідомленням системного адміністратора.При ризиках атаки типу Denial Of Service (DoS), встановлене спеціальне обладнання, яке розпізнає такий тип атак і автоматично блокує атакуючого з повідомленням системного адміністратора.

- Доступ до обладнання VoIP мають тільки відповідальні за нього особи на фізичному рівні.

- Вимкненння будь-яких невживаних сервісів на обладнанні VoIP. snmp, ftp, http або web-сервер. Особливо вразливі програмні IP АТС, що працюють під управлінням різних Linux або Windows дистрибутивів. Операційна система може запускати різні сервіси, про наявність яких адміністратор навіть не здогадується, але вони легко можуть бути використані зловмисниками для злому. Наприклад, список мережевих сервісів і відкритих портів в Linux легко можна дізнатися, скориставшись командою netstat -atnup | grep LISTEN:

- Обмежений доступ до віддаленого управління. За допомогою командного рядка. Використовується протокол SSH (Secure SHell).

Щоб підвищити безпеку доступу по SSH, виконання рекомендацій:

1) Зміна порту за замовчуванням. Порт 22 використовується службою SSH за замовчуванням. Замінений номер порту на нестандартний. Багато атаки на пристрої в мережі починаються зі сканування стандартних портів з метою визначити, прослуховують їхні мережеві сервіси. Якщо такі порти існують - пробувати їх зламати.

2) Явна перерахування користувачів, що мають доступ до системи, в директиві AllowUsers. У тому випадку, якщо все-таки необхідно надати доступ до системи ряду довірених осіб.

3) Використання тільки SSH протокол версії 2. Заборонений прямий доступ до облікового запису користувача root. Це істотно ускладнить і швидше унеможливить атаку на перебір пароля, так як користувачу root буде заборонений доступ в систему, навіть при введенні коректного пароля.

4) Використання тимчасових обмежень по введенню пароля або сертифікатів. Установка мінімально можливого часу для введення пароля, наприклад, 1 секунда, може добре збити з толку зловмисника [2].

Приклад налаштувань:

```
/ etc / ssh / sshd_config для Linux:
/ Etc / ssh / sshd_config
AllowUsers vasya petya borya
Port 23465
Protocol 2
LoginGraceTime 1s
PermitRootLogin no
```

- Через Web-інтерфейс. Слід не забувати змінити пароль за замовчуванням і обмежити доступ до web-інтерфейсу списком конкретних IP адрес. Також рекомендується використовувати SSL шифрування для протоколу http.
- Можливе використання нестандартних портів для сигнальних протоколів. Як слухача порту для SIP, наприклад, порт 5089 замість стандартного 5060. Зазвичай першим етапом при скануванні діапазону IP адрес в Інтернеті з метою виявити пристрою VoIP для подальшого злому є пошук відкритих сигнальних портів SIP, H.323 і т.д
- Прийом дзвінків лише з IP адрес вашого партнера/оператора/клієнта.

Особливо це актуально, якщо між VoIP платформоюі транзитними операторами, налаштований статичний

VoIP-транк. Це дозволить уникнути ймовірності: Здійснення викликів через вашу VoIP платформу, якщо зловмисник знає ваш AOH (CALLER ID) і знає, яким чином набрати номер абонента, що викликається, щоб виклик був відправлений по вихідному каналу. Для Cisco IOS системний адміністратор легко зробить налаштування, використовуючи вбудовані ACL. У нових версіях IOS Cisco в конфігурації за замовчуванням у всіх ACL є рядок deny any. Це означає, що за замовчуванням мережеві підключення закриті для всіх IP адрес і слід відкривати доступ тільки для конкретних мереж і хостів. Наприклад на Linux сервері:

Дозволити вхідні пакети на порт 5060 тільки для зазначених хостів і мереж, всім іншим заборонити:

```
922 tables -A INPUT -s 71.25.103.0/24 -p udp --dport 5060 -j ACCEPT
923 tables -A INPUT -s 71.25.79.150 -p udp --dport 5060 -j ACCEPT
924 tables -A INPUT -s 71.25.66.206 -p udp --dport 5060 -j ACCEPT
925 tables -A INPUT -s 71.25.73.38 -p udp --dport 5060 -j ACCEPT
926 tables -A INPUT -s 71.25.66.106 -p udp --dport 5060 -j ACCEPT
927 tables -A INPUT -s 71.157.120.91 -p udp --dport 5060 -j ACCEPT
928 iptables -A INPUT -p udp --dport 5060 -j DROP.
```

- Обмежена реєстрація користувачів. Клієнти можуть реєструватися на IP АТС провайдера прямо з мережі Інтернет (що рекомендується тільки з використанням захищеного каналу VPN), відхиляти повідомлення про реєстрації REGISTER з будь-якого IP адреси без необхідності. Обмежений список IP адрес, з яких можуть реєструватися клієнти. Настійно рекомендується використовувати для доступу до корпоративної мережі VoIP захищену мережу VPN.
- Логування всіх подій в системі. Використання журналів всіх подій в системі. Бажано, щоб логи (журнали) про події в системі записувалися віддалено. Це пов'язано з тим, що зловмисник, отримавши доступ до пристрою, зокрема до IP АТС, намагається приховати свою присутність і свої дії шляхом видалення всіх подій з файлів журналів. Якщо логи будуть відправлятися на віддалений сервер, це утруднить або зробить неможливим для зловмисника приховати свою присутність.
- Ведення журналів CDR (Call Detail Record). У журналах деталізованої інформації про виклики можуть міститися інформація, яка вкаже, що обладнання незаконно використовується.

Застосування міжмережевих екранів. Мережеві екрани надають захист мережі або окремих її вузлів від несанкціонованого доступу. Також мережеві екрани фільтрують пакети, що не підходять під критерії, визначені в конфігурації.

Можливе здійснення трансляції адрес - динамічну заміну внутрішньомережевих (сірих) адрес або портів на зовнішні, що використовуються за межами локальної мережі, що може забезпечувати додаткову безпеку [21].

Можливості:

- Фільтрація доступу до свідомо незахищеним службам.
- Перешкоджання отриманню закритої інформації з захищеної підмережі, а також впровадження в захищену підмережу помилкових даних за допомогою вразливих служб.
- Контроль доступу до вузлів мережі.
- Може реєструвати всі спроби доступу як ззовні, так і з внутрішньої мережі, що дозволяє вести облік використання доступу в Інтернет окремими вузлами мережі.
- Регламентування порядку доступу до мережі.
- Повідомлення про підозрілу діяльність, спробах зондування або атаки на вузли мережі або сам екран.
- Внаслідок захисних обмежень можуть бути заблоковані деякі необхідні користувачеві служби, такі як Telnet, FTP, SMB, NFS, і так далі. Тому настройка файрволу вимагає участі фахівця з мережевої безпеки. В іншому випадку шкода від неправильного конфігурування може перевищити користь.

Також слід зазначити, що використання брандмауера збільшує час відгуку і знижує пропускну здатність, оскільки фільтрація відбувається не миттєво.

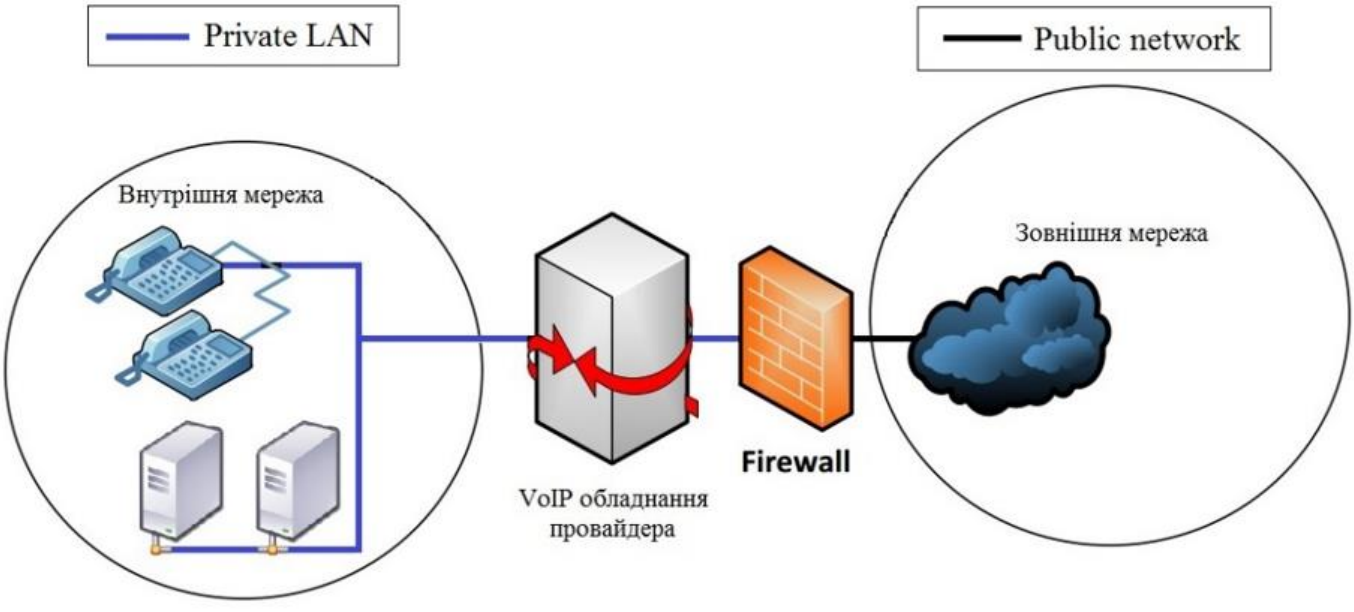

Рис. 3.1. Схема застосування міжмережевих екранів

Міжмережевий екран пропускає вихідний трафік від сервера телефонії до SIP-клієнтів і фільтрує вхідний за певними правилами. Раціональним рішенням є фільтрування IP-адрес на міжмережевому екрані та фільтрування всіх мережевих портів для IP-телефонії, крім необхідних для коректної роботи і адміністрування. Цей же метод захисту доцільно застосовувати на самому сервері телефонії, щоб захистити його від внутрішніх атак. У такій конфігурації у зловмисника відсутня фізична можливість атакувати обладнання VoIP з використанням вразливостей VoIP протоколів.

Застосування шифрованих тунелів VPN. При підключенні послуг телефонії через публічні мережі (Інтернет) використовується VPN підключення до телефонної мережі оператора зв'язку. При такій схемі підключення клієнту видається на відповідальне зберігання Переднастроєні VPN маршрутизатори, забезпечують надійний захист телефонної мережі клієнта і високу стабільність роботи. Весь голосовий трафік і всі VoIP пристрої будуть приховані всередині VPN тунелю, і не будуть доступні з публічних мереж.

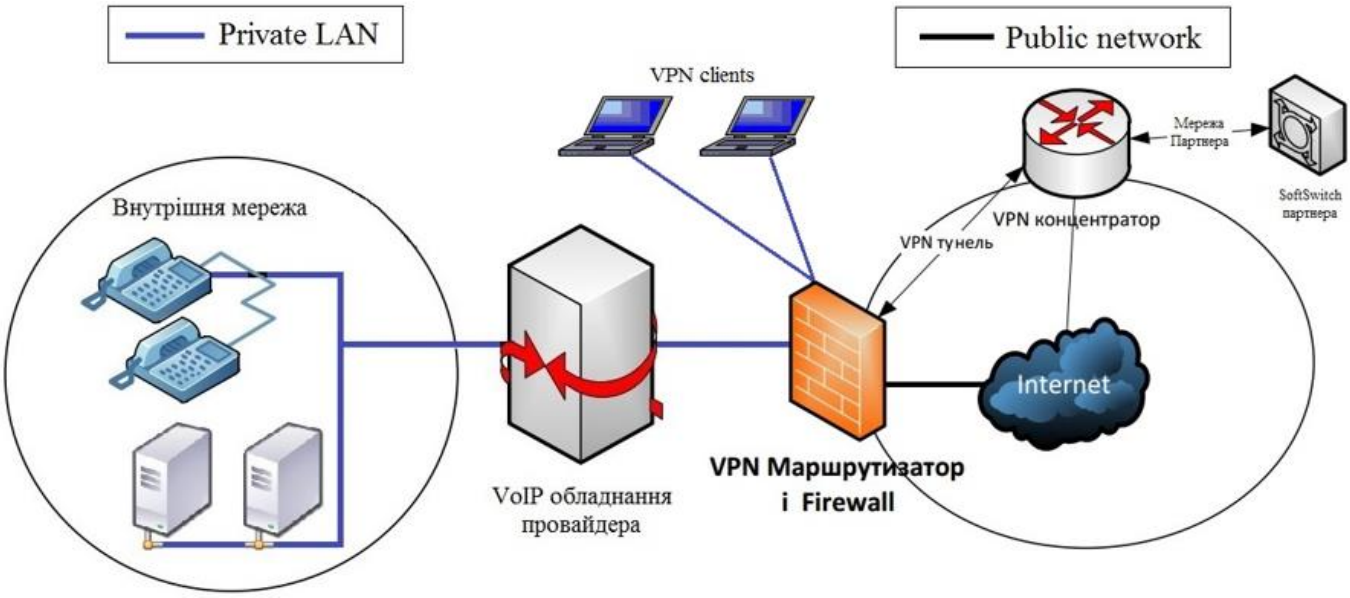

Рис. 3.2. Схема застосування шифрованих VPN тунелів

Однак технологія VPN має ряд недоліків, що обмежують її застосування:

- зниження якості зв'язку через затримки, що створюються шифруванням;

- підвищене навантаження на канали зв'язку й устаткування, викликана необхідністю шифрування;

- ускладнення мережевої структури.

Шифрування телефонних розмов. При неможливості реалізації VPN тунелю для захисту конфіденційних переговорів і мінімізації можливості потрапляння конфіденційної або комерційної інформації в руки зловмисника необхідно захистити передані по відкритих каналах зв'язку дані від перехоплення і прослуховування.

Оскільки для здійснення дзвінка клієнт і сервер попередньо обмінюються службовими даними для встановлення з'єднання, дану проблему можна розділити на дві складові - захист службових даних IP-телефонії та захист голосового трафіку. Як засіб захисту можуть бути використані протокол TLS (Transport Layer Security) для захисту SIP сигналів і протокол SRTP (Secure Real Time Protocol) для захисту голосового трафіку [2].

TLS - криптографічний протокол, що забезпечує захищену передачу даних між вузлами в мережі, є стандартним методом для шифрування SIP-протоколу. TLS забезпечує конфіденційність і цілісність інформації, що передається, здійснює аутентифікацію.

Після встановлення захищеного з'єднання починається передача голосових даних, убезпечити які дозволяє застосування протоколу SRTP.

Протокол SRTP вважається одним з кращих способів захисту IP телефонії на базі IP-АТС Asterisk. Основна перевага цього протоколу - відсутність будь-якого впливу на якість зв'язку. Схема роботи протоколу SRTP виглядає так: кожному здійснюваного вами дзвінку присвоюється унікальний код, який робить підслуховування розмов неавторизованих в системі користувачами практично неможливим. Завдяки цьому протокол SRTP вибирають як для звичайних, так і для конфіденційних дзвінків.

3.2. Проектування захищеної мережі VoIP провайдера

В даній мережі застосований комплексних систем захисту інформації для забезпечення безпеки мережі VoIP провайдера. VoIP обладнання надається вендором

JERASOFT з внутрішньою політикою безпеки. Для взаємодії телефонії використовується VoIP switch MERA, свіч дає можливість фільтрування IP-адрес та портів. Шлюзом мережі є маршрутизатор з функціями фаєрволу та VPN серверу - Cisco ASA. З клієнтами/партнерами/транзитними операторами IP-телефонії встановлюється VPN-тунель для захисту передачі даних. В мережі здійснюється локальне адміністрування. Всі мережеві пристрої контролюються адміністратором мережі. Для забезпечення віддаленого доступу до мережі та її адміністрування, можливе підключення VPN-клієнтів за допомогою ПЗ Cisco VPN client

Рис. 4.4. Захищена мережа VoIP провайдера

JeraSoft є провідним розробником і інтегратором високої якості програмного забезпечення Telecom Billing. Інженерна компанія, яка надає можливості адмініструванні рішень VoIP високопродуктивних і програмного забезпечення білінгу для малих, середніх і великих телекомунікаційних компаній. Орієнтована на забезпечення стабільних та економічно ефективних білінгових і управлінських рішень.

Використовується обладнання:

JeraSoft VCS 40 / VCS Retail 25k з параметрами

CPU: 2 x Intel® Xeon® E5-2630 v3

RAM: 64 GB

HDD: Hardware RAID 1+0 with at least 8 x 300 GB 15K RPM SAS

Платформа надає внутрішню Полі́тику інформаці́йної безпеки, набір вимог, правил, обмежень, рекомендацій, які регламентують порядок інформаційної діяльності в мережі і спрямовані на досягнення і підтримку стану інформаційної безпеки VoIP провайдера.

MERA VoIP Transit Softswitch (MVTS) - контролер з'єднань, що виконує функції центрального вузла управління трафіком в мережі провайдера IP-телефонії. MVTS - це принципове спрощення організації та підвищення безпеки VoIP-мереж, контроль якості сервісу і сполучення різнорідного обладнання.

ALOE Systems (MERA Systems) розробляє передові програмні комутатори и контролери сесій, які дозволяють операторам и постачальникам послуг ефективного управляти VoIP. Рішення компаниї представляються собою потужного комбінацію масштабованості и широкі функціональні можливості. На сьогоднішній день, ALOE Systems є ключовими постачальником високонадійніх и економічних VoIP послуг на основі комутації и VAS платформ.

Основними перевагами MVTS є:

- Єдина точка входу VoIP-трафіку в ядро мережі (централізована авторизація та білінг, подолання NAT, підтримка COPM).

- Сумісність різнорідного обладнання.

- Безпека мережі.

- Зручність и простота управління мережі.

- Інтелектуальний роутинг.

- IP-Пряме з'єднання операторських и клієнтських мереж.

- Управління якістю обслуговування (QoS).

Машрутизатором з функціями між мережевого екрану є маршрутизатор Cisco ASA 5580-40.

Можливостями є:

- Міжмережеве екранування з урахуванням стану з'єднань;
- Глибокий аналіз протоколів прикладного рівня;
- Трансляція мережевих адрес;
- IPsec VPN;
- SSL VPN (підключення до мережі через веб-інтерфейс);
- Протоколи динамічної маршрутизації (RIP, EIGRP, OSPF).

Таблиця 4.1

Апаратне забезпечення

Модель	Рік випуску	Процесор	Тактова частота	Обсяг ОЗУ за замовчуванням	Пристрій зберігання	Обсяг пристрою зберігання
5580-40	2018	AMD Opteron (4 процессора, 8 ядер)	3.6 GHz	16 GB	ATA CompactFlash	128 GB SSD

Мінімальна підтримувана версія	Максимальне число віртуальних інтерфейсів	Карти розширення	Число з'єднань	Підтримка резервування
8.1.1	250	6 інтерфейсних карт	2 за замовчуванням, максимум 10000	Active/Standby, Active/Active

Таблиця 4.2

Продуктивність Cisco ASA 5580-40.

Модель	Нешифрований-ввід-вивід	Введення-виведення AES / Triple DES, Мбіт / с	Число одночасних з'єднань	Максимальне число IPSec-з'єднань	Максимальне число з'єднань SSL VPN
5580-40	10 000	1000	2000000	10000	10000

ВИСНОВКИ

У даній дипломній роботі мною був розроблений проект захищеної мережі VoIP провайдера.

Розглянувши основні схеми побудови криптосистем, види алгоритмів, специфікації та протоколи IP- телефонії, можна зробити висновок, що існуючі системи IP-телефонії реалізують недостатньо високий рівень захисту інформації та використовують відносно нестійкі криптографічні алгоритми. Таким чином, захист інформації в VoIP потребує проведення подальших досліджень, у тому числі удосконалення вже існуючих систем шляхом використання додаткових засобів захисту, які б дозволили підвищити надійність існуючих методів шифрування, або розроблення нових методів та схем захисту з урахуванням потреб сьогодення.

Також слід врахувати що абсолютну гарантію безпеки, на жаль, не зможе дати жоден комплекс заходів. Розглянуті аспекти лише частково вирішують задачу побудови захищеної комунікаційної системи. На практиці слід розглядати всю інфраструктуру мережі, проводити глибокий аналіз необхідного рівня захисту. Необхідно враховувати не тільки необхідність забезпечення безпеки IP-телефонії, а й виходів на зовнішні канали зв'язку. Тільки такий підхід, разом з постійним вдосконаленням систем інформаційної безпеки, дозволить створити надійну і захищену систему.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гольдштейн Б.С. Сигнализация в сетях связи. Том 1. М.: Радио и связь, 1998.
2. Гольдштейн Б.С. Протоколы сети доступа. Том 2. М.: Радио и связь, 1999.
3. Гольдштейн Б.С., Ехриель И.М., Рерле Р.Д. Интеллектуальные сети. М.: Радио и связь, 2010.
4. Кузнецов А.Е., Пинчук А. В., Суховицкий А.Л. Построение сетей IP-телефонии / Компьютерная телефония, 2010.
5. Кульгин М. Технологии корпоративных сетей. Изд. «Питер», 2019.
6. Ломакин Д. Технические решения IP-телефонии / Мобильные системы, 2019 №8.
7. Мюнх Б., Скворцова С. Сигнализация в сетях IP-телефонии. - Часть I, II/Сети и системы связи, 2019.
8. Шнепс-Шнеппе М.А. Интеллектуальные услуги - это ДВО / Информ - курьер-связь, 2010 - №9.
9. Armitage Grenville. Quality of Service in IP Networks. - Macmillan Technical Publishing, 2010.
10. Anquetil L-P., Bouwen J., Conte A., Van Doorselaer. B. Media Gateway Control Protocol and Voice over IP Gateway. - Alcatel Telecommunications Review, 2nd Quarter 1999.
11. Caputo R. Cisco Packetized Voice and Data Integration. - McGrawHill Cisco Technical Expert, 2016
12. Curtin P., Whyte B. Tigris - A gateway between circuit-switched and IP networks / Ericson Rewiew, 2013, №2.
13. DeMartino K. ISDN and the Internet. - Computer Networks, 2012.
14. Douskalis B. IP Telephony. The Integration of Robust VolP Services. -Prentice Hall, 2015.

15. Durham D., Yavatkar R.. Inside the Internet's Resource Reservation Protocol: Foundations for Quality of Service, 2010

16. Faynberg I., Gabuzda L, Lu Hui-Lan. Converged Networks and Services: Internetworking IP and the PSTN. - John Wiley & Sons, 2017.

17. Goncalves M. Voice Over IP Networks. - McGraw Hill Publishing, 2018.

18. GoralskiW., Kolon M. IP Telephony. - McGraw Hill Publishing, 2014.

19. Harte . Voice Over Data Network Internet, Frame Relay, and ATM.- APDG Inc. 2010

20. Hersent 0, Gurle D., Petit Jean-Pierre. IP Telephony: Packet-Based Multimedia Communications Systems.- Addison-Wesley Pub Co, 2011.

21. Horak R. Communications systems & networks / Second Edition, MEt T Books and IDG Books Worldwide, Inc., 2016.

22. Houghton T. F, E. C. Schloemer, E. S. Szurkowski, W. P. Weber. A packet telephony gateway for public network operators. - Bell, 2015.