МІНІСТЕРСТВО ОСВІТИ І НАУКИ КРАЇНИ
Західноукраїнський національний університет
Фаультет комп'ютерних інформаційних технологій
Кафедра комп'ютерної інженерії

ДЗІВАК Олександр Андрійович

АЛГОРИТМ ЗАХИЩЕНИХ РЕЖИМІВ IP-ТЕЛЕФОНІЇ / ALGORITHM OF IP-TELEPHONY SECURE MODES

спеціальність; 123 – Комп'ютерна інженерія
освітньо-професійна програма - Комп'ютерна інженерія

Кваліфікаційна робота

Виконав студент групи Кім-21
О.А.Дзівак
_____

Науковий керівник:
к.т.н., доцент Л.О,Дубчак
_____

Кваліфікаційну роботу
допущено до захисту
«___» _____2021 р.

Завідувач кафедри КІ
О.М.Березький
_____

Тернопіль - 2021

ВСТУП

Актуальність роботи. Сьогодні можна вже казати про те, що IP-телефонія стала певним стандартом у телефонних комунікаціях [1-3]. Це пояснюється її зручністю, відносною надійністю та відносно невисокою вартістю у порівнянні із аналоговим зв'язком [4-6]. Можна також стверджувати, що IP-телефонія підвищує ефективність ведення бізнесу та дозволяє здійснювати недоступні раніше операції, зокрема, інтеграцію із різними бізнес-додатками [7-9].

Якщо говорити про недоліки та слабкі місця IP-телефонії, та спершу слід відзначити ті самі «хвороби», які властиві іншим службам, що використовують протокол IP [10-11]. Це є схильність до атак із боку черв'яків та вірусів, DoS-атак, а також несанкціонованого віддаленого доступу тощо [12-14]. Хоча при побудові інфраструктури для IP-телефонії зазвичай дану службу відокремлюють від сегментів мережі, де «ходять» неголосові дані, це не є ще гарантією безпеки [15-17]. Зараз велика кількість компаній IP-телефонію інтегрують із іншими додатками, наприклад із послугамии електронної пошти. Таким чином з одного боку з'являються додаткові зручності, а з іншого - нові вразливості [18]. Крім того, при функціонуванні мережі в IP-телефонії потрібна велика кількість складових, таких, як комутатори, сервери підтримки, IP-телефони, маршрутизатори, міжмережеві екрани тощо [19-21].

Серед головних загроз, яким піддається мережа IP-телефонії, можна виділити [22-24]:

- реєстрація чужого терміналу, що дає можливість за чужий рахунок робити дзвінки;
- підміна абонента;
- внесення змін до голосового чи сигнального трафіка;
- зниження якості голосового трафіку;
- перенаправлення голосового чи сигнального трафіку;
- перехоплення голосового чи сигнального трафіку;

- підробка голосових повідомлень;

- завершення сеансу зв'язку;

- відмова у обслуговуванні;

- несанкціонований віддалений доступ до компонентів інфраструктури в IP-телефонії;

- несанкціоноване оновлення на IP-телефоні ПЗ (наприклад, з метою впровадження троянської чи шпигунської програми);

- злом біллінгової системи.

Це є далеко не весь перелік з можливих проблем, які пов'язані із використанням IP-телефонії. Альянс із безпеки VoIP (VOIPSA) розробив документ, який описує широкий спектр загроз IP-телефонії, що, крім технічних загроз, включає також вимагання через IP-телефонію, спам тощо.

Але основне уразливе місце IP-телефонії - це є людський фактор [25-26]. Проблема захищеності при розгортанні телефонної IP-мережі дуже часто відсувається на задній план і проходить вибір рішення без участі фахівців із безпеки. До того ж ці фахівці не завжди налаштовують рішення належним чином, навіть якщо у ньому присутні належні захисні механізми чи купуються засоби захисту, що не призначені для ефективної обробки голосового трафіку (наприклад, міжмережеві екрани можуть не розуміти фірмовий протокол сигналізації, що використовується у рішенні IP-телефонії) [27-28]. Зрештою, організація витрачати змушена додаткові фінансові і людські ресурси для захисту розгорнутого рішення чи миритися із його незахищеністю [29-30].

Випускна кваліфікаційна робота оформлена згідно вимог [31, 32] і присвячена розробці алгоритмів захищених режимів IP-телефонії.

Мета роботи. Метою даної роботи є розробка та реалізація алгоритмів для захищених режимів IP-телефонії.

Досягнення поставленої мети включало розв’язання таких взаємопов’язаних завдань:

- аналіз методів побудови мережі IP-елефонії;
- огляд та аналіз різних підходів до архітектури IP-телефонії;

– класифікація типів загроз в мережах IP-телефонії;

– розробка алгоритмів захищених режимів IP-телефонії;

– розробка режиму використання шлюзів для IP-телефонії;

– розробка програмного засобу для захисту IP-телефонії;

– моделювання передачі даних по IP-телефонії.

Об'єктом дослідження є процес захисту режимів IP-телефонії.

Предметом дослідження є режими роботи IP-телефонії.

Методи дослідження. В основу наукових досліджень покладено методи на основі роботи IP-телефонії, програмування, моделювання та опрацювання і дослідження отриманих результатів.

Наукова новизна одержаних результатів визначається наступним:

– на основі аналітичного огляду різних підходів до побудови мереж IP-телефонії встановлено основні вимоги, які пред'являються до архітектури мереж IP-телефонії та рівня її захищеності;

– на основі порівняння найбільш поширених підходів до побудови мережі IP-телефонії розроблено алгоритми захищених режимів роботи IP-телефонії, що дозволило збільшити рівень захисту мереж IP-телефонії;

– на основі вимог до захищених режимів роботи IP-телефонії розроблено алгоритмічне забезпечення, структурну та функціональну схеми програми, що дозволило визначити компоненти програмної системи, які необхідно спроектувати.

Практична цінність одержаних результатів полягає в тому, що:

– на основі аналітичного огляду обґрунтовано вибір та розробку середовища програмування, що дозволило розробити компоненти програми та здійснити їх інтеграцію у єдиний програмний продукт;

– на основі дослідження роботи програми, імітаційного моделювання та опрацювання отриманих результатів встановлено, що розроблена програмна система відповідає поставленим вимогам і дозволяє використовувати IP-телефонію для захищеної передачі даних.

Публікації та апробація ВКР. За результатами наукових досліджень, проведених у роботі, підготовлено тези доповіді «Модель забезпечення безпеки в IP-телефонії на прикладі site-to-site VPN» обсягом 1 сторінка на IV науково-практичній конференції молодих вчених і студентів «Інтелектуальні комп'ютерні системи та мережі» (м. Тернопіль, червень, 2021 р.) [33] та тези доповіді «Порівняльний аналіз протоколів для побудови мереж IP-телефонії» обсягом 1 сторінка на V науково-практичній конференції молодих вчених і студентів «Інтелектуальні комп'ютерні системи та мережі» (м. Тернопіль, грудень, 2021 р.) [34] (Додаток А).

Випускна кваліфікаційна робота складається із трьох розділів, висновків, списку використаних джерел та додатків.

У першому розділі розглянуто методи та підходи до побудови мереж IP-телефонії, розглянуто різні рівні архітектури IP-телефонії, а також здійснено постановку задачі.

В другому розділі розроблено алгоритми захищених режимів роботи IP-телефонії та розглянуто режим використання шлюзів для IP-телефонії.

У третьому розділі здійснено програмну реалізацію розроблених алгоритмів захищених режимів IP-телефонії та моделювання їх роботи. Проведено експериментальне дослідження розроблених алгоритмів.

1 ПОБУДОВА МЕРЕЖІ IP-ТЕЛЕФОНІЇ

1.1 Транспортні технології для пакетної комутації

Більшість виробників, що для пакетної телефонії мають широкий асортимент продукції, займають положення «технологічно нейтральне» і надають можливість покупцеві самому вибрати ту технологію, що найкраще відповідає для його інтеграційної стратегії [35-36].

Основні технології при пакетній передачі мови – ATM (рисунок 1.1), Frame Relay (рисунок 1.2) та маршрутизація пакетів IP (рисунок 1.3) - відрізняються ефективністю при використанні каналів зв'язку, ступенем охоплення різних ділянок у мережі, керованістю, надійністю, захистом інформації і доступу, а також вартістю [37-38].

Рисунок 1.1 - Мова по ATM

Рисунок 1.2 - Мова по Frame Relay

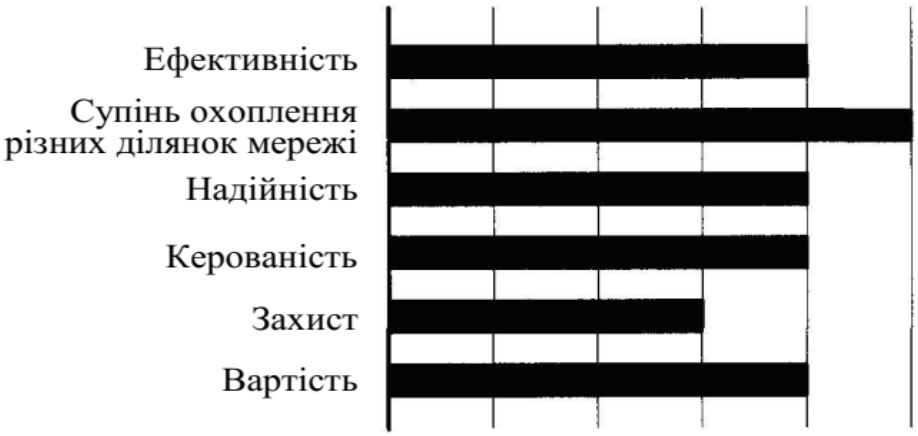

Рисунок 1.3 - Мова по IP

Транспортна технологія ATM уже декілька років використовується успішно в магістральних мережах для загального користування і в корпоративних мережах, а її зараз активно починають використовувати також для високошвидкісного доступу каналами xDSL (для невеличких офісів) та SDH/Sonet (для крупних підприємств) [39-40]. Головні переваги у цій технології – це є її надійність, зрілість і наявність розвинених засобів при експлуатаційному управлінні мережею. В ній є механізми з управління якістю обслуговування та контролю при використанні мережевих ресурсів, за своєю ефективністю неперевершені. Але обмежена поширеність та висока вартість їх обладнання не дають можливості вважати ATM найкращим вибором для організації телефонних з'єднань від одного вузла до іншого.

Технологія Frame Relay відіграє в пакетній телефонії таку саму роль, що й квазіелектронним АТС у телефонії із комутацією каналів: вони показують приклад програмно керованої ефективної техніки, однак мають обмежені можливості з подальшого розвитку [41-42]. Користувачі недорогих послуг у Frame Relay, які забезпечують передбачувану цілком продуктивність, є багато корпоративних мереж, більшість із них своїм вибором задоволені цілком. У короткостроковій перспективі технологія для передачі мови Frame Relay буде ефективна цілком для організації мультисервісного доступу та каналів телекомунікації. Однак мережі Frame Relay незначно поширені: як правило,

використовуються на практиці некомутовані з'єднання в режимі точка-точка [43-44].

Технологія для передачі мовної інформації [45-46] по мережах із маршрутизацією IP-пакетів до себе привертає увагу, в першу чергу, універсальністю - мова перетворена може бути у потік пакетів в будь-якій точці у мережевій інфраструктурі: магістралі в мережі оператора, на кордоні розподіленої мережі, в корпоративній мережі та навіть безпосередньо в терміналі у кінцевого користувача [47-48]. Нарешті, вона може стане найпоширенішою технологією для пакетної телефонії, так як вона здатна охопити усі сегменти ринку, при цьому будучи адаптованою добре до нових умов при застосуванні. Впровадження IP-телефонії, незважаючи на значну універсальність протоколу IP, стримується ще через те, що багато операторів їх вважають погано керованими, недостатньо надійними і тому не дуже ефективними. Однак мережева інфраструктура, спроектована грамотно, із ефективними механізмами при забезпеченні якості обслуговування ці недоліки робить малоістотними. В розрахунку на один порт вартість системи IP-телефонії є на рівні (чи трохи нижча) від вартості системи Frame Relay, але нижча вартості для обладнання у ATM. Причому видно вже зараз, що ціни на товари IP-телефонії швидше знижуються, чим на інші вироби, і тому на цьому ринку відбувається загострення конкуренції.

1.2 Рівні архітектури у IP-телефонії

Архітектура технології для Voice over IP [49] може бути представлена спрощено як дві площини. Нижня площина - це є базова мережа із маршрутизацією IP-пакетів, а верхня - це є відкрита архітектура з управління обслуговуванням викликів (чи запитів для зв'язку).

Нижня площина, спрощено кажучи, собою являє комбінацію з відомих протоколів Інтернет: RTP (Real Time Transport Protocol), який функціонує зверху протоколу UDP (User Datagram Protocol), який розташований, в свою чергу, в стеку з протоколів TCP/IP понад протоколом IP. Отже, свого роду ієрархія RTP/UDP/IP є транспортним механізмом мовного трафіку. Тут же потрібно відзначити, що для передачі даних у мережах із маршрутизацією IP-пакетів передбачаються завжди механізми для повторної їх передачі, коли вони втрачаються. Використання цих механізмів при передачі інформації у реальному часі погіршить тільки ситуацію, і тому для передачі інформації, що чутлива до затримок, однак менш чутлива до втрат, зокрема, мови та відеоінформації, використовується механізм з негарантованої доставки цієї інформації RTP/UDPD/IP. В Рекомендаціях ITU-T допускаються в одному напрямку затримки до 150 мс. Якщо приймаюча станція повторну передачу IP-пакета запрошує, то при цьому затримки занадто будуть великі.

Стосовно верхньої площини для управління зобслуговуванням запитів зв'язку, то для виклику передбачається прийняття рішення, куди має бути направлений виклик і як встановлено має бути між абонентами з'єднання. Інструменти для цього – це телефонні системи, починаючи із тих, що підтримуються декадно-кроковими АТС та передбачають відповідне об'єднання функцій для маршрутизації та функцій для створення комутованого розмовного каналу у одних і тих самих декадно-крокових шукачах. Потім еволюціонували принципи сигналізації до систем сигналізації на сигнальних виділених каналах або багаточастотної сигналізації, протоколів із загальноканальної сигналізації та передачі функцій по маршрутизації в відповідні вузли для обробки послуг в інтелектуальній мережі.

В мережах із комутацією пакетів складніша ситуація. Мережа із маршрутизацією IP-пакетів підтримує принципово цілий ряд різноманітних протоколів для маршрутизації одночасно [50].

На сьогодні такими протоколами є: IGRP (англ. Interior Gateway Routing Protocol), RIP – (англ. Routing Information Protocol), IS-IS – (англ. Intermediate

System-to-intermediate System), EIGRP – (англ. Enhanced Interior Gateway Routing Protocol), BGP – (англ. Border Gateway Protocol), OSPF – (англ. Open Shortest Path First) тощо. Так же само і для IP-телефонії ряд протоколів розроблений.

Найпоширенішим є протокол, що специфікований в рекомендації H.323 ITU-T [51], зокрема, тому, що став він застосовуватися раніше від інших протоколів, яких не існувало взагалі до впровадження H.323.

Інший протокол у площині для управління з обслуговування виклику є SIP - орієнтованим на те, щоби кінцеві пристрої і шлюзи зробити більш інтелектуальними та для користувачів підтримувати додаткові послуги.

Розроблявся протокол SGCP, починаючи із 1998 року, для того, щоби зменшити вартість шлюзів через реалізацію функцій для автоматизованої обробки виклику централізованого устаткування. Протокол IPDC схожий на SGCP, однак має набагато більше, чим SGCP, механізмів з експлуатаційного управління (OAM & P). Потім робоча група з комітету IETF у MEGACO розробила протокол MGCP, що базується на протоколі SGCP, однак із деякими доповненнями.

Ця робоча група не зупинялася на досягнутому і продовжувала вдосконалювати цей протокол для управління шлюзами та розробила функціональніший, чим MGCP, протокол MEGACO.

1.3 Різні підходи до побудови мережі IP-телефонії

Щоби зрозуміти, чим конкретно один від одного відрізняються протоколи, треба розглянути коротко архітектуру мереж, які побудовані на базі цих протоколів, а також процедури встановлення і завершення з їх використанням з'єднання.

Перший підхід в історії на стандартизованій основі до побудови структури мережі IP-телефонії запропонований у рекомендації H.323 Міжнародним

союзом електрозв'язку (ITU). Мережі на основі протоколів H.323 орієнтуються на інтеграцію із телефонними мережами та розглядатися можуть як мережі ISDN, що накладені на мережі для передачі інформації. Так, процедура для встановлення з'єднання з такими мережами для IP-телефонії грунтується на рекомендаціях Q.931 та аналогічна для процедури, що використовується в ISDN.

Рекомендації H.323 передбачають складний досить набір для протоколів, що не просто призначений для передачі в IP-мережах мовної інформації із комутацією пакетів. Мета його - забезпечити роботу у мультимедійних додатках у мережах із негарантованою якістю в обслуговуванні. Мовний трафік - це є тільки один із додатків H.323 разом із відео та даними.

Підхід для побудови мережі у IP-телефонії, що представлений Міжнародним союзом електрозв'язку у рекомендаціях H.323, підходить добре тим операторам з телефонних мереж, що зацікавлені в використанні мережі із комутацією IP-пакетів (чи IP-мережі) для надання міжміського та міжнародного зв'язку. Наприклад, протокол RAS, який входить до сімейства протоколів H.323, має забезпечити контроль при використанні мережевих ресурсів, виконувати аутентифікацію користувачів та забезпечувати нарахування оплати за певні послуги.

На рисунку 1.4 представлена архітектура IP-мережі на основі рекомендації H.323. Основні її пристрої є: шлюз (Gateway), термінал (Terminal), воротар (Gatekeeper) та пристрій для управління конференціями (MCU, Multipoint Control Unit).

Термінал H.323 – це є термінал для користувача IP-мережі, який забезпечує двосторонній мультимедійний (чи мовний) зв'язок із іншим пристроїм H.323, шлюзом чи терміналом для управління конференціями [2].

Шлюз в IP-телефонії реалізує передачу по мережах мовного трафіку із маршрутизацією IP-пакетів по протоколу H.323. Основне його призначення – це перетворення мовної інформації, що надходить від телефонної лінії загального користування, у вигляд, що придатний для передачі по мережі із маршрутизацією IP-пакетів. Крім того, шлюз перетворює сигнальні

повідомлення у системах сигналізації DSS1 та ОКС7 у сигнальні повідомлення H.323 та виробляє певне зворотне перетворення згідно з рекомендаціями ITU H.246.

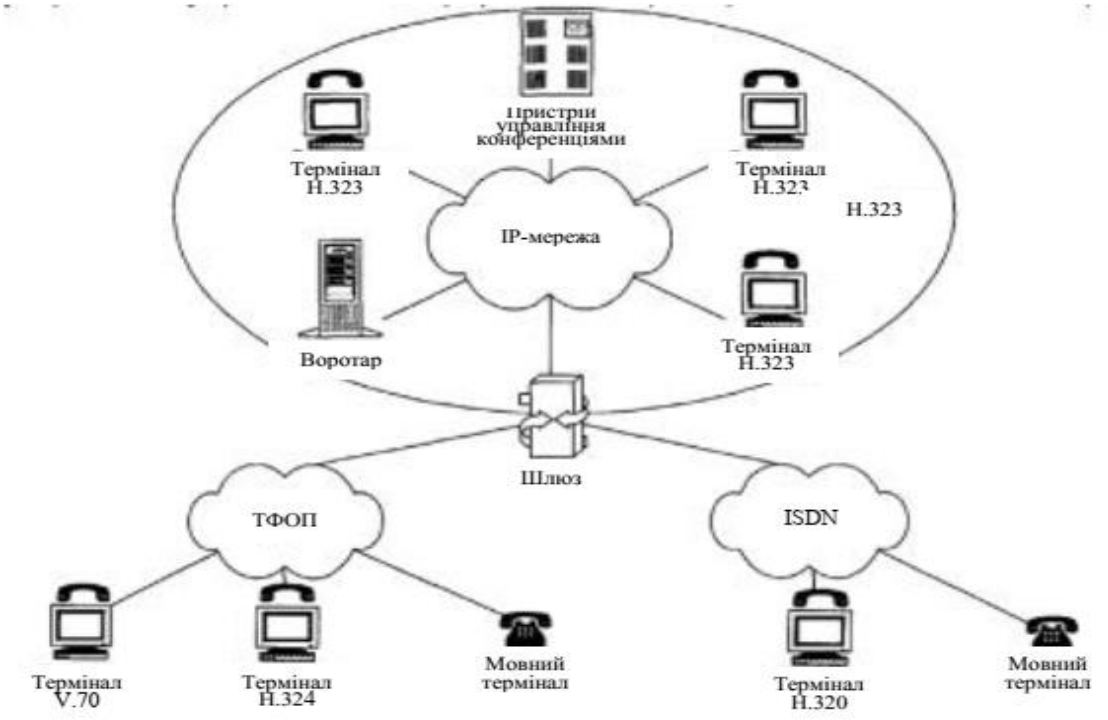

Рисунок 1.4 - Архітектура мережі H.323

В воротарі зосереджена вся інтелектуальна частина для IP-мережі при телефонії.

Мережа, що побудована згідно з рекомендаціями H.323, володіє зонною архітектурою (рисунок 1.5). Воротар має функції з управління однією зоною IP-мережі, куди входять: шлюзи, термінали, пристрої для керування конференціями, що зареєстровані у вибраного воротаря. Окремі частини зони у мережі H.323 можуть бути рознесені територіально і з'єднані один із одним через маршрутизатори.

Найважливіші функції воротаря:

- реєстрація кінцевих, а також інших пристроїв;

- контроль під час доступу користувачів у системі до послуг IP-телефонії на основі сигналізації протоколу RAS;

- перетворення викликаного користувача (оголошення телефонного номера, імені абонента, адреси електронної пошти тощо) у транспортну адресу мереж із маршрутизацією IP-пакетів (IP-адреса + номер порту TCP);

- управління, контроль та резервування пропускної здатності IP-мережі;

- передача сигнальних повідомлень протоколу H.323 між різними терміналами.

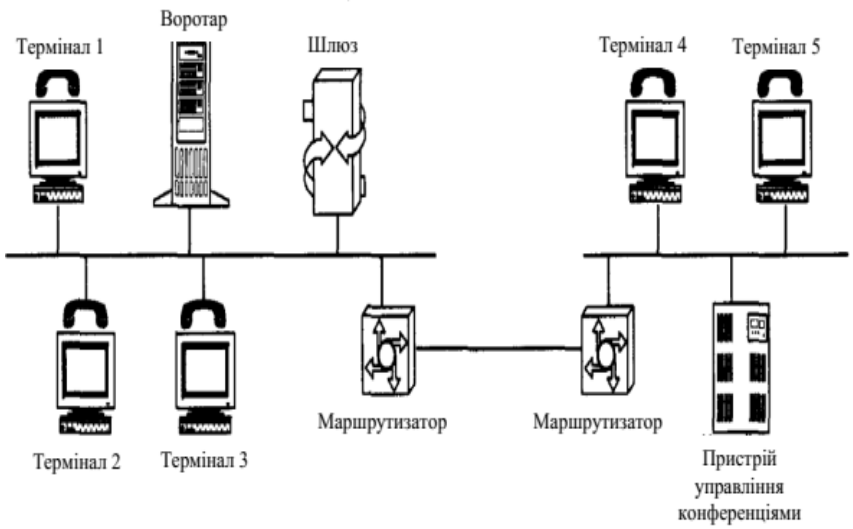

Рисунок 1.5 - Зона мережі H.323

У одній IP-мережі, яка відповідає рекомендаціям ITU H.323, перебувати може декілька воротарів, які взаємодіють один із одним за протоколом RAS.

Поряд з основними функціями, які визначені рекомендаціями H.323, відповідати воротар може за аутентифікацію користувачів та нарахування оплати (або білінг) за телефонні з'єднання. Пристрої для управління конференціями забезпечують можливість для організації зв'язку між трьома або більше учасниками [4].

Рекомендації H.323 три типи конференцій передбачають (рисунок 1.6): централізована (або керована MCU, із яким кожен учасник у конференції під'єднується в режимі точка-точка), децентралізована (кожний учасник у конференції з'єднується із іншими у режимі точка-група точок) та змішана.

Перевага централізованої конференції – це є порівняно просте обладнання терміналів, а недолік – це велика вартість пристроїв для управління у конференціях.

У децентралізованій конференції треба складніше обладнання терміналів та бажано, щоби у IP-мережі підтримувалась передача IP-пакетів у режимі під LGPL (англ., IP multicasting). Коли не підтримується цей режим в мережі, тоді повинен термінал передавати мовну інформацію для кожного із решти учасників в режимі точка-точка.

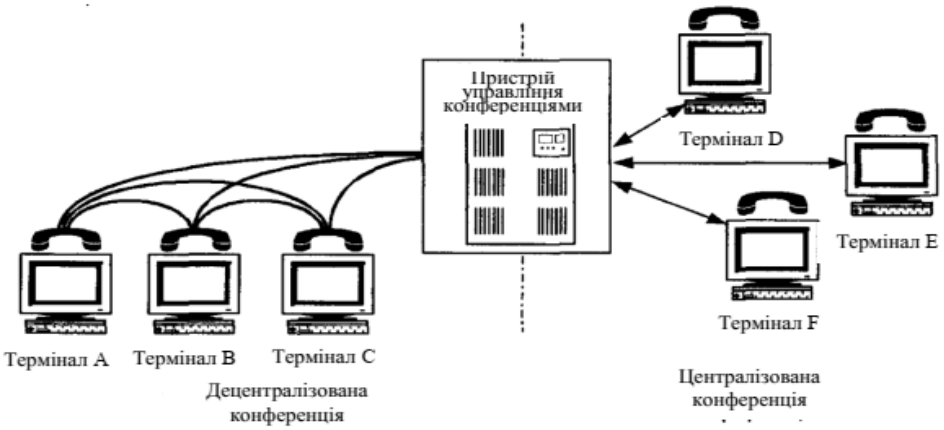

Рисунок 1.6 - Типи конференції в мережах H.323

Пристрій для управління на конференціях складається із обов'язкового одного елемента – це контролер конференцій (Multipoint Controller - MC), і може, крім того, включати в себе один чи більше процесорів для обробки інформації користувача (англ., Multipoint Processor - MP). Може бути контролер суміщений фізично із воротарем, шлюзом чи пристроєм для управління на конференціях, який, в свою чергу, поєднаний може бути з шлюзом чи воротарем.

Контролер у конференціях використовується для організації будь-якої конференції. Організовує він обмін даними між учасниками про режими, що підтримуються їх терміналами, та вказує, в якому режимі учасники передавати можуть інформацію, причому під час конференції режим цей може змінюватися. Наприклад, при підключенні нового учасника.

Оскільки контролерів в мережі кілька може бути, то кожній новостворюваній конференції проведена має бути спеціальна процедура для

виявлення контролера, що керуватиме конференцією. Для організації централізованої конференції, окрім контролера MC, використовуватися повинен процесор MP, який обробляє інформацію від користувача. Він відповідає за перемикання чи змішування всіх мовних потоків, даних і відеоінформації. У децентралізованій конференції не потрібен процесор.

Ще одним важливим елементом мережі H.323 є проксі-сервер H.323 чи сервер-посередник. Функціонує цей сервер на прикладному рівні та може перевірити пакети із інформацією, якою два додатки обмінюються. Проксі-сервер визначати може, із яким додатком (H.323 чи іншим) асоціюється виклик, та здійснювати відповідне з'єднання. Виконує проксі-сервер такі функції:

- підключення засобами комутованого доступу чи локальних мереж терміналів, які не можуть підтримувати протокол для резервування певних ресурсів (RSVP). Два проксі-сервера таких можуть утворювати у IP-мережах тунельні з'єднання із вказаною якістю обслуговування;

- маршрутизація окремо від звичайного трафіку H.323;

- забезпечення сумісності із перетворювачем мережевих адрес, так як допускається розмістити обладнання H.323 в приватних мереж;

- захист доступу – це тільки доступ для трафіку H.323.

Протокол RAS (англ., Registration Admission Status) забезпечує взаємодію кінцевих, а також інших пристроїв із воротарем. Основні функції протоколу: реєстрація у системі пристрою, контроль доступу його до ресурсів мережі, зміна в смузі пропускання, опитування і індикація пристрою в поточному стані. Як транспортний використовується протокол UDP із негарантованою доставкою даних.

Протокол H.225.0 (Q.931) підтримує процедури з встановлення, підтримки і руйнування з'єднання. Як транспортний використовується протокол TCP із установленням з'єднання і гарантованою доставкою даних.

Відбувається за протоколом H.245 обмін інформацією межи учасниками з'єднання, яка необхідна, щоб створити логічні канали. Через такі канали мовна інформація передається, що міститься в пакетах RTP/UDP/IP.

Дотримання процедур, які передбачені протоколом RAS, це початкова фаза встановлення з'єднання при використанні сигналізації H.323. Далі йдуть фаза для сигналізації H.225.0 (Q.931) і обмін повідомленнями керування H.245. Закриття з'єднання відбувається в зворотньому порядку: спочатку керуючий канал H.245 закривається та сигнальний канал H.225.0, сповіщається далі воротар по каналу RAS про звільнення раніше зайнятої смуги пропускання.

Складність протоколу H.323 демонструється на рисунку 1.7, де спрощений сценарій представлений із встановлення між двома користувачами з'єднання. Передбачається в даному сценарії, що кінцеві користувачі знають вже один одного IP-адреси. В звичайному випадку буває більше етапів, так як при встановленні з'єднання участь беруть воротарі та шлюзи.

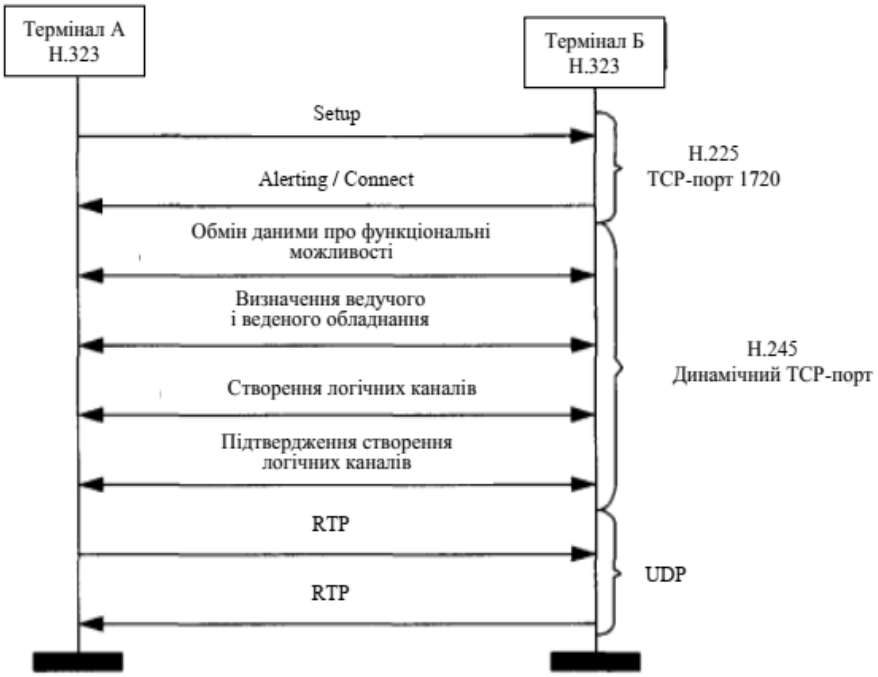

Рисунок 1.7 - Спрощений сценарій для встановлення з’єднання у мережі H.323

Крок за кроком розглянемо спрощений цей процес:

1) кінцевий пристрій посилає від користувача А запит для з'єднання – SETUP-повідомлення - на кінцевий пристрій у користувача В на TCP-порт 1720;

2) кінцевий пристрій у викликаного користувача В повідомленням ALERTING відповідає на повідомлення SETUP, що означає, що пристрій є вільний, а викликаному користувачу про вхідний дзвінок подається сигнал;

3) після того, коли користувач В прийме виклик, тоді передається до викликаючої сторони А повідомлення CONNECT із номером порту TCP у керуючому каналі H.245;

4) кінцеві пристрої по каналі H.245 обмінюються інформацією про типи мовних кодеків (G.723.1, G.729 тощо), а також і інші функціональні можливості обладнання, та один одного сповіщають про номери RTP-портів, куди передавати слід інформацію;

5) відкриваються логічні канали при передачі мовних даних;

6) мовні дані передаються на обидві сторони у повідомленнях RTP-протоколу; ведеться, крім того, контроль при передачі даних за допомогою RTCP-протоколу.

Наведений алгоритм для обслуговування виклику грунтується на версії 1протоколу H.323. Версія 2 цього протоколу дозволяє передавати дані, які необхідні для створення логічних каналів, безпосередньо у SETUP-повідомленні протоколу H.225.0 без використання H.245. Процедура така називається Fast Start («швидким стартом») і вона дозволяє кількість циклів обміну даними скоротити при встановленні з'єднання. Окрім організації для базового з'єднання, передбачено надання додаткових послуг в мережах H.323 відповідно до рекомендації ITU H.450.X.

Треба зазначити ще одну проблему – це якість обслуговування в мережах H.323 [52]. Термінал, який запитує в воротаря дозволу на доступ, може, використавши в повідомленні ARQ протоколу RAS поле transportQoS, повідомити про здатність для резервування мережевих ресурсів. Рекомендації H.323 визначають протокол для резервування ресурсів (англ., RSVP) засобом для забезпечення гарантованої якості при обслуговуванні, яка до терміналів пред'являє вимогу підтримки RSVP протоколу. На жаль, RSVP протокол використовується не повсюдно, і це залишає мережу H.323 без основних механізмів забезпечення гарантованої якості при обслуговуванні. Це є загальна проблема IP-телефонії, яка характерна не тільки для H.323.

Інший підхід до побудови IP-мережі, який розроблений робочою групою MMUSIC від комітету IETF в документі RFC 2543, грунтується на використанні протоколу SIP (англ., Session Initiation Protocol).

SIP - це текстоорієнтований протокол, який є частиною у глобальній архітектурі мультимедіа, яка розроблена комітетом IETF (Internet Engineering Task Force). Включає ця архітектура також в себе протоколи для резервування ресурсів (RSVP, RFC 2205, Resource Reservation Protocol), протокол транспортний у реальному часі (RTP, RFC 1889, Real-Time Transport Protocol), протокол для передачі потоків в реальному часі (RTSP, RFC 2326, Real-Time Streaming Protocol,), протокол для опису параметрів зв'язку (SDP, RFC 2327, Session Description Protocol,), протокол повідомлень про зв'язок (SAP, Session Announcement Protocol,). Однак функції SIP-протоколу не залежать від будь-якого із них.

Відразу треба зазначити, що хоч на сьогодні і отримав найбільше поширення протокол H.323, та все одно більша частина виробників намагається передбачити в нових своїх продуктах підтримку SIP-протоколу. Поки що це є поодинокі явища, тому вони не можуть скласти. серйозної конкуренції для протоколу H.323. Однак, із огляду на темпи при зростанні популярності SIP-протоколу, досить ймовірно, що рішення на його базі у найближчому майбутньому значну нішу займуть на ринку IP-мереж.

Підхід SIP-протоколу до побудови IP-мережі є набагато простіший в реалізації, чим H.323, однак підходить менше для взаємодії із телефонними мережами. Пов'язано це в основному із тим, що SIP-протокол сигналізації, який базується на HTTP-протоколі, узгоджується погано із системами сигналізації, які використовуються у телефонних лініях загального призначення. Тому протокол SIP підходить більше для постачальників послуг Інтернету для надання послуг IP-телефонії. При цьому послуга така всього лише буде частиною пакета послуг.

Протокол SIP проте послуги підтримує з інтелектуальної мережі (IN), зокрема, перетворення (або меппінг) імен, переадресація чи маршрутизація, що

є істотним для використання SIP-протоколу сигналізації в мережах загального користування, у яких основним завданням оператора є надання ряду телефонних послуг. Важливою особливістю SIP-протоколу є підтримка мобільності користувача, який буде здатний до замовлених послуг отримувати доступ в будь-якому місці та із будь-якого терміналу. Також мережа буде здатна ідентифікувати чи аутентифікувати користувача при переміщенні його із одного місця до іншого. Така властивість SIP не є унікальною. Наприклад, протокол H.323 підтримує теж у значній мірі таку Ж можливість. Однак настав зараз момент, коли ця можливість буде головною привабливою властивістю мережі для нового покоління IP-телефонії. Такий режим при роботі потребує на сервері ідентифікації та аутентифікації дистанційної реєстрації користувачів. На рисунку 1.8 представлено архітектуру мережі, яка базується на протоколі SIP.

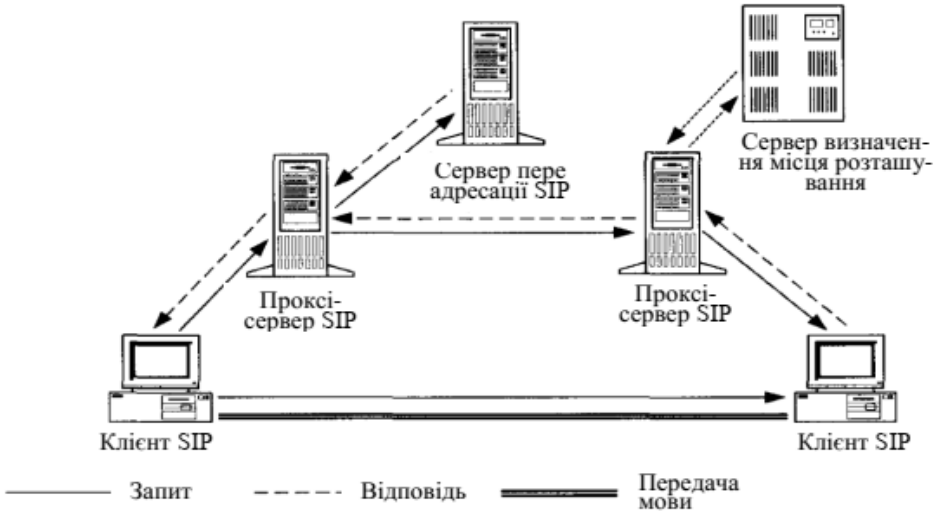

Рисунок 1.8 - Приклад мережі на базі протокола SIP

Містить мережа SIP три види основних елементів: проксі-сервери, агенти користувача та сервери для пере адресації даних. Агенти користувача (англ., User Agent чи SIP-client) є додатки у термінальному обладнанні та дві складові у себе включають: агент користувача - клієнт (англ., User Agent Client, UAC) і агент користувача - сервер (англ., User Agent Server, UAS), відомі інакше як відповідно клієнт та сервер. Клієнт від UAC ініціює SIP-запити, виступає в

якості викликаючої сторони. Далі сервер UAS ці запити приймає та повертає відповіді, отже, виступає в ролі сторони, яка викликається.

Також існує, крім того, два типи мережевих SIP-серверів: проксі-сервери (або сервери-посередники) та сервери переадресації. SIP-сервери можуть працювати і у режимі із збереженням станів для поточних з'єднань (statefull), і в режимі без їх збереження (stateless). SIP-сервер, який функціонує у режимі stateless, обслужити може значну кількість користувачів, тоді як воротар H.323 може працювати одночасно із обмеженою їх кількістю.

Проксі-сервер (англ., Proxy-server) діє «від імені інших клієнтів» та має функції клієнта (UAC) та сервера (UAS). Останній інтерпретує та може заголовки запитів перезаписувати перед їх відправленням до інших серверів (рисунок 1.9). Відповідні повідомлення тим же шляхом слідують до проксі-сервера назад, а не до клієнта. На рисунку 1.9 представлено схему алгоритму для встановлення з’єднання з допомогою протокола SIP при участі проксі-сервера.

Сервер переадресації (англ., Redirect server) визначає поточне розміщення викликаного абонента та повідомляє користувачу, що його викликав (рисунок 1.10). Щоб визначити поточне розміщення викликаного абонента звертається сервер переадресації до сервера для визначення розміщення, принципи роботи якого не специфіковані в документі RFC 2543.

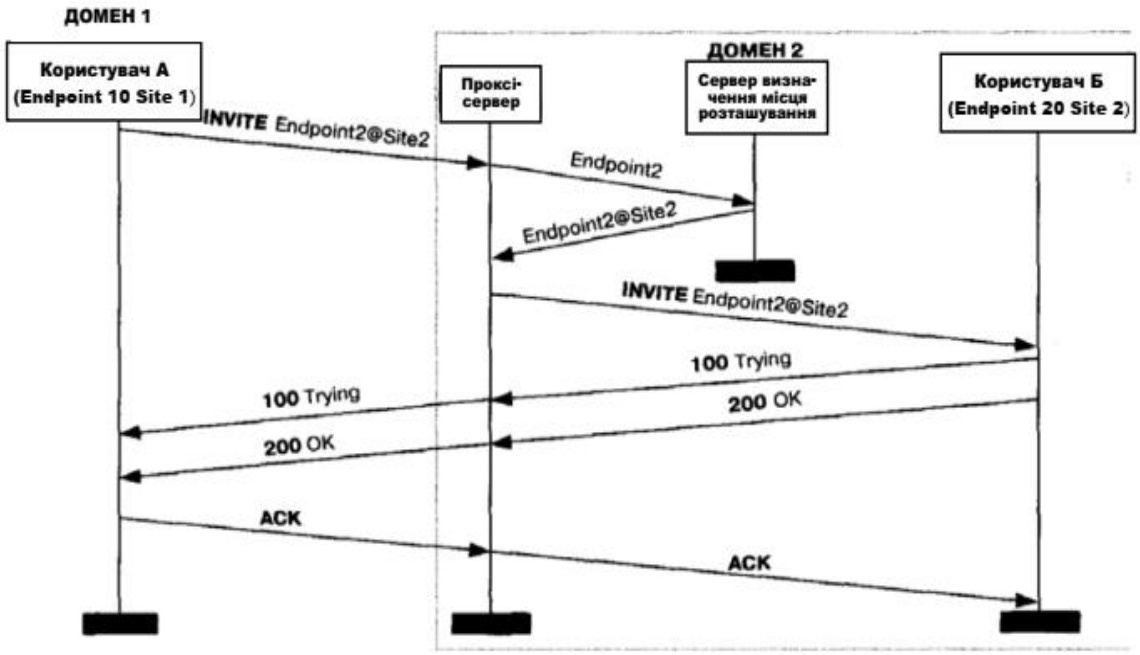

Рисунок 1.9 – SIP-мережа із проксі-сервером

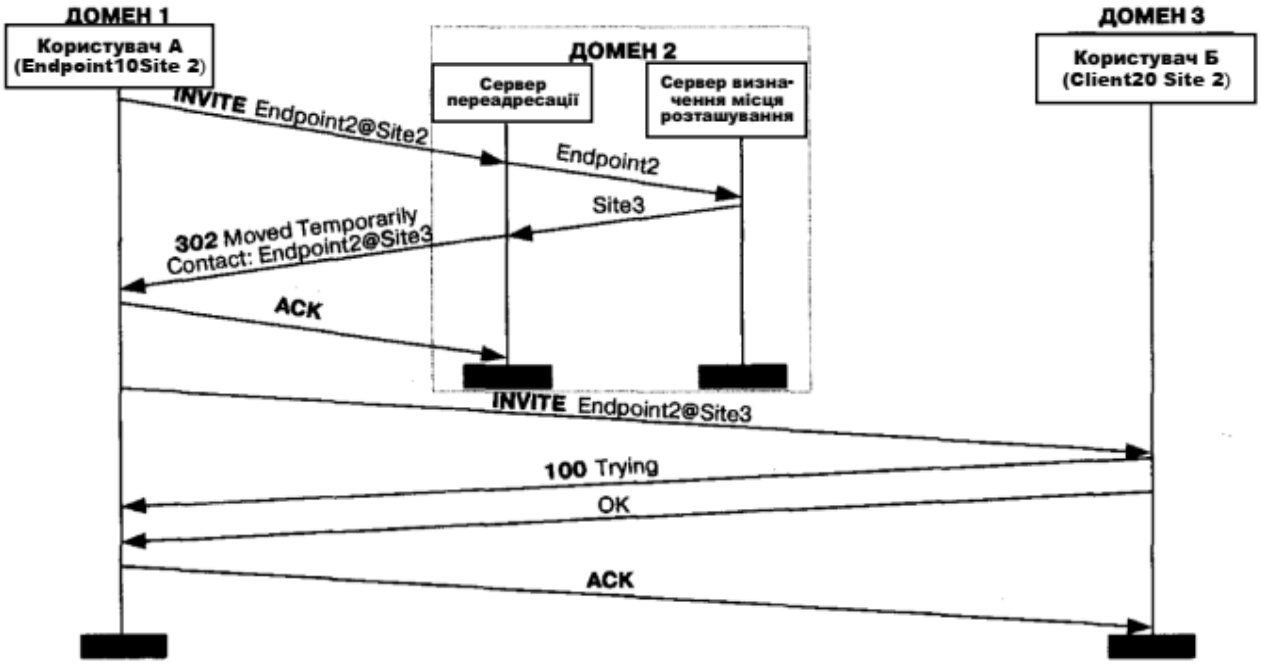

Рисунок 1.10 – SIP-мережа із сервером переадресації

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

SIP-протокол передбачає 5 запитів та відповідей. SIP-сигналізація дозволяє агентам та мережевим серверам, призначеним для користувача,

визначити місця для розташування, запити видавати та керувати з'єднаннями. Можливі такі запити:

- INVITE - запит зарошує користувача чи послугу на участь в сеансі зв'язку та містить опис параметрів зв'язку із ним. Користувач з допомогою цього запиту визначити може функціональні можливості у терміналі свого партнера та почати сеанс, використовуючи обмежену кількість повідомлень та підтверджень прийому їх;

- АСК – підтверджує цей запит прийом відповіді від сторони, що викликає, на команду INVITE та транзакцію завершує;

- OPTIONS - дозволяє цей запит інформацію отримати про функціональні можливості в користувацьких агентах та мережевих сервераї. Але не використовується цей запит для організації сеансів зв'язку;

- BYE – використовується цей запит обома сторонами для закінчення з'єднання. Перед розривом з'єднання агенти, призначені до користувача, відправляють до сервера цей запит, повідомляючи про наміри сеанс зв'язку припинити;

- CANCEL – дозволяє цей запит агентам та мережевим серверам, призначеним для користувача, будь-який переданий раніше запит скасувати, коли на нього відповідь не було ще отримано.

Третій підхід при побудові IP-мереж, що грунтується на використанні MGCP-протоколу, запропонований також комітетом IETF та робочою групою із MEGACO.

Робоча група із MEGACO при розробці даного протоколу спиралась на мережеву архітектуру, яка містить функціональні основні блоки трьох видів (рисунок 1.11):

- шлюз – (англ., Media Gateway MG), який виконує перетворення мовної інформації, що надходить від телефонних мереж для загального користування із постійною швидкістю при передачі, у вигляд, що придатний для передачі по мережах із маршрутизацією IP-пакетів (кодування та упаковку мовної інформації в пакети RTP / UDP / IP, та зворотне перетворення);

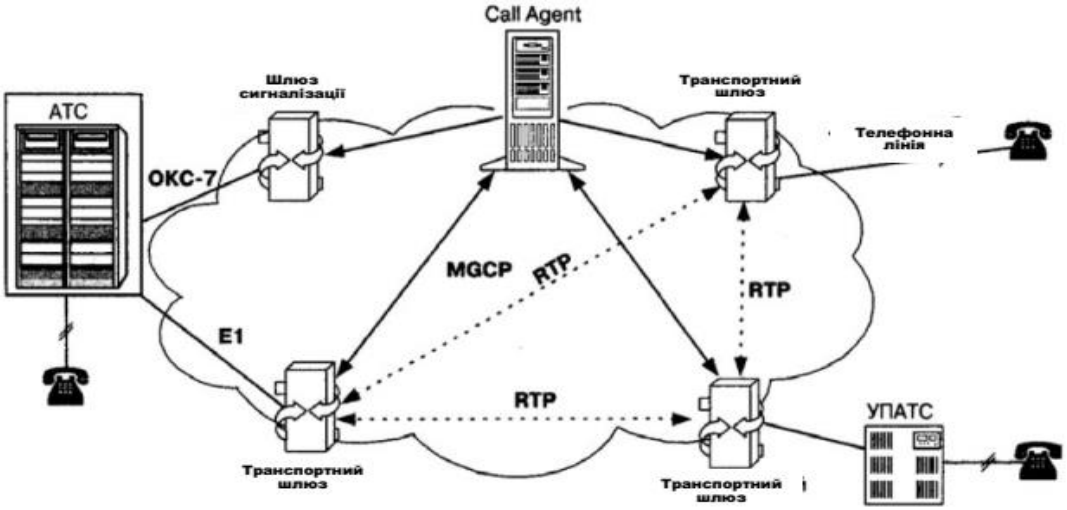

Рисунок 1.11 - Архітектура мережі на базі протоколу MGCP

- контролер шлюзів – (англ., Call Agent), який виконує управління шлюзами;

- шлюз сигналізації – (англ., Signaling Gateway, SG), який забезпечує доставку сигнальної інформації, що надходить від ТМЗК до контролера шлюзів та її перенесення в зворотному напрямку.

Отже, все управління функціонально розподіленого шлюзу зосереджене в контролері. Його функції розподілені можуть бути між декількома комп'ютерними платформами [7].

Шлюз для сигналізації виконує STP-функції - транзитний пункт мережі дл сигналізації ОКС7. Шлюзи ж тільки виконують функції для перетворення мовної інформації. Одночасно один контролер управляє декількома шлюзами. В мережі присутні можуть бути декілька контролерів. Вважається, що вони між собою синхронізовані та управляють злагоджено шлюзами, які участь беруть у з'єднанні. Разом із тим, MEGACO-протокол для синхронізації роботи контролерів не визначає. У ряді робіт, що присвячені дослідженню можливостей MGCP-протоколу, пропонується для цієї мети використовувати протоколи SIP, H.323 чи ISUP/IP. Повідомлення MGCP-протоколу протоколом переносяться без гарантованої доставки UDP-повідомлень. Робоча група SIGTRAN з комітету IETF розробляє у даний час механізми взаємодії контролера для шлюзів та шлюзів для сигналізації.

Шлюзи сигналізації приймати повинні пакети з нижніх трьох рівнів від системи для сигналізації ОКС7 (рівнів підсистеми для перенесення MTP-повідомлень) та передавати сигнальні повідомлення з верхнього, користувацького рівня до контролера для шлюзів. Шлюз для сигналізації має також вміти передати сигнальні повідомлення Q.931 по IP-мережі.

Найбільша увага приділяється робочою групою SIGTRAN питанням для розробки найефективнішого механізму при передачі по IP-мереж сигнальної інформації. Треба зазначити, що декілька причин існує, через які довелося відмовитися від використання для цієї мети TCP-протоколу. Робоча група з SIGTRAN для передачі сигнальної інформації пропонує використовувати протокол SCTP (англ., Stream Control Transport Protocol), який має переваги перед TCP-протоколом. Головна із них - це значне зниження часу для доставки сигнальної інформації і, відповідно, часу для встановлення з'єднання. Це для якості обслуговування є одни із найважливіших параметрів. Коли використовується в ТМЗК сигналізація по виділених сигнальних каналах (ТСК), то спочатку сигнали надходять разом із користувальницькою інформацією до транспортного шлюзу і передаються потім без посередництва шлюзу сигналізації в контролер шлюзів [8].

Зазначимо, що MGCP-протокол є внутрішнім для обміну даними між функціональними блоками у розподіленому шлюзі, що видається ззовні одним шлюзом. MGCP-протокол є master/slave-протоколом. Це значить, що контролер для шлюзів є ведучим, а шлюз - веденим пристроєм, який повинен виконувати усі команди, які надходять від контролера Call Agent.

Таке рішення масштабованість мережі забезпечує та простоту управління нею через контролери шлюзів. Шлюзи не мають бути інтелектуальними пристроями, вони вимагають процесорів меншої продуктивності і стають дешевшими. Крім того, швидко дуже вводяться нові протоколи для сигналізації чи додаткових послуг, так як зміни ці лише контролер шлюзів зачіпають, а не самі шлюзи.

Третій метод, що пропонується організацією IETF (робоча група із MEGACO), підходить добре для розгортання глобальних IP-мереж, які на зміну приходять традиційним телефонним мережам.

Розглянем алгоритми для встановлення та руйнування з'єднання при використанні MGCP-протоколу. Приклад перший охоплює взаємодію MGCP-протоколу із протоколом ОКС7 (рисунок 1.12).

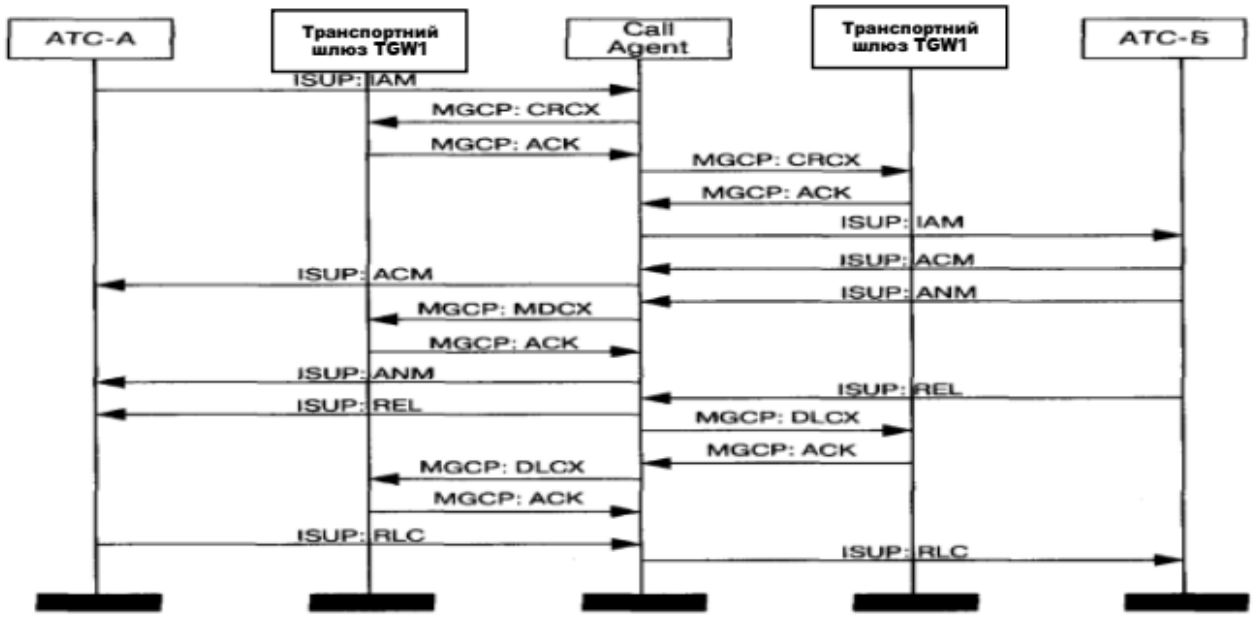

Рисунок 1.12 - Встановлення та закінчення з'єднання із використанням MGCP-протоколу (Приклад 1)

Від телефонної станції АТС-А по загальному каналу до шлюзу для сигналізації SG1 запит з'єднання надходить в вигляді IAM-повідомлення ISUP-протоколу. На рисунку 1.12 шлюз для сигналізації SG1 та SG2 суміщені відповідно із транспортними шлюзами TGW1 та TGW2. Передає шлюз SG1 IAM-повідомлення до контролера шлюзів, що обробляє запит та визначає, який виклик направлений повинен бути до АТС-Б за допомогою шлюзу TGW2.

Резервує контролер порт для шлюзу TGW1 (розмовний канал). З такою метою він до шлюзу передає команду CreateConnection. Порт шлюзу TGW1 тільки може інформацію приймати (режим «recvonly»), оскільки він не обізнаний ще про те, за якою адресою та яким чином слід йому інформацію

передавати. Шлюз TGW1 у відповіді на таку команду повертає опис параметрів в сеансі зв'язку. Контролер, що прийняв відповідь шлюзу TGW1, передає команду CRCX від другого шлюзу TGW2 із метою зарезервувати в цьому шлюзі порт. Вибирає шлюз TGW2 порт, який братиме участь в з'єднанні, і підтверджувати прийом команди CRCX. Створюється з допомогою двох команд CRCX розмовний односпрямований канал для передачі акустичних сигналів чи мовних підказок та повідомлень абонентові. Одночасно порт для шлюзу TGW2 може вже не тільки приймати, але і передавати інформацію, оскільки отримав він від зустрічного шлюзу опис параметрів зв'язку.

Потім передає контролер шлюзів IAM-повідомлення до АТС-Б. На IAM-повідомлення станція АТС-Б відповідає ACM-підтвердженням, що пересилається негайно до станції АТС-А. Тоді, як прийме абонент виклик, АТС-Б передасть ANM-повідомлення до контролера шлюзів.

Потім замінює контролер режим «recvonly» у шлюзі TGW1 на повнодуплексний режим з допомогою команди MDCX. Виконує шлюз TGW1 та зміну режиму підтверджує. Контролер передає ANM-повідомлення до АТС-А, а далі починається розмовна фаза при з'єднанні.

Відбувається завершення розмовної фази таким чином. Викликаючий абонент Б першим дає відбій. Через шлюз сигналізації АТС-Б передає REL-повідомлення до контролера шлюзів. Прийнявши REL-повідомлення, контролер шлюзів із викликаним абонентом завершує з'єднання. Шлюз підтверджує це завершення і передає до контролера статистичні дані, що зібралися за час з'єднання.

Контролер шлюзів передає RLC-повідомлення до АТС-Б із метою підтвердження розз'єднання. Контролер паралельно завершує з'єднання з викликаючою стороною. ШлюзTGW1 завершення з'єднання підтверджує та до контролера передає статистичні дані, зібрані за час з'єднання. АТС-А передачею RLC-повідомлення підтверджує завершення з'єднання, після чого вважається з'єднання закінченим.

2 АЛГОРИТМИ ЗАХИЩЕНИХ РЕЖИМІВ IP-ТЕЛЕФОНІЇ

2.1 Порівняння підходів до побудови мережі IP-телефонії

В даний час при побудові у IP-телефонії добре функціонуючих та сумісних із телефонними мережами для загального користування підходять протоколи H.323 та MGCP. Протокол SIP взаємодіє дещо гірше із системами сигналізації, які використовуються в ТфОП.

Підхід, що заснований на використанні MGCP-протоколу, має важливу досить перевагу перед підходом, що запропонований ITU в рекомендаціях H.323: підтримка для сигналізації ОКС7 шлюзів контролером та інших видів сигналізації, а також прозора трансляція мережею IP-телефонії сигнальної інформації. В мережі, що побудована на основі рекомендацій H.323, сигналізація ОКС7, як будь-яка інша, конвертується в сигнальні повідомлення H.225.0 (Q.931) шлюзом.

Основний недолік третього із наведених вище підходів - це незакінченість стандартів.

Функціональні складові для розподілених шлюзів, які розробляються різними фірмами, що виробляють телекомунікаційне обладнання, є практично несумісними. Функції контролера для шлюзів не є точно визначеними. Не стандартизовані також механізми для перенесення до контролера від шлюзу сигналізації сигнальної інформації і у зворотному напрямку. До недоліків також можна відносити відсутність стандартизації протоколу для взаємодії між різними контролерами. Крім того, MGCP-протокол є протоколом для управління шлюзами, але він не призначається для управління з'єднаннями при участі термінального обладнання у користувачів (наприклад, IP-телефонів). Це значить, що у мережі, яка побудована на базі MGCP-протоколу, для управління термінальним обладнанням має бути присутній воротар чи сервер SIP.

Варто відзначити також, що для існуючих програмах з IP-телефонії, зокрема, надання послуг міжнародного і міжміського зв'язку, використовувати

MGCP-протокол (SIP-як протокол) є недоцільно у зв'язку із тим, що переважна кількість IP-мереж побудовані сьогодні на базі протоколу H.323. Тоді оператору доводиться будувати для IP-телефонії окрему мережу на основі MGCP-протоколу (чи SIP), що є пов'язано із великими капіталовкладеннями. В той же час, оператори зв'язку, що мають обладнання із стандарту H.323, можуть приєднуватися до існуючих мереж у IP-телефонії.

У останньому з згаданих підходів (у проекті четвертої версії рекомендацій H.323) ITU-T ввів принципи декомпозиції шлюзів, який у третьому підході використовується. Для розподіленого шлюзу управління функціональними блоками здійснюватися буде контролером цього шлюзу - MGC (англ., Media Gateway Controller) з допомогою протоколу MEGACO/H.248. У проекті четвертої версії рекомендацій H.323 передбачена можливість також для прозорої передачі сигналізації ОКС7 або інших видів сигналізації по IP-мережах і обробка сигналізацій всіх видів воротарем без перетворення на сигнальні повідомлення H.225.0.

2.2 Типи загроз в мережах IP-телефонії

Конфіденційність і безпека - це обов'язкові вимоги для будь-якої телефонної мережі. З часом забезпечити вдалося певний, хоча і далекий від досконалості, рівень безпеки у традиційних мережах. Поширення IP-телефонії і її претензії на те, щоб стати основною технологією передачі голосу в недалекому майбутньому, породжують ряд проблем, традиційна телефонія з якими чи ніколи не стикалася, чи давно про них забула, чи вже навчилася справлятися.

В корпоративних колах існують сьогодні як противники, так і прихильники з впровадження IP-телефонії (IPT) в якості альтернативної технології для передачі голосу. І коли перші, так би мовити, можуть не

турбуватися, то другі повинні усвідомлювати, що нові конвергентні мережі і голосові сервіси приносять також нові уразливості для мереж.

Питання безпечного зв'язку завжди було одним із важливих у мережах телекомунікацій. На даний час в зв'язку із бурхливим розвитком глобальних комп'ютерних мереж, у тому числі мереж Інтернет-телефонії, забезпечення безпеки при передачі інформації стає актуальним ще більше. Розробка заходів у області безпеки має проводитися на основі аналізу ризиків, визначення критично важливих ресурсів системи та можливих загроз. Існує декілька основних типів загроз, що становлять найбільшу небезпеку для мереж IP-телефонії:

- підміна даних про користувача значить, що один з користувачів мережі себе видає за іншого. При цьому виникає вірогідність несанкціонованого доступу до важливих функцій системи. Використання механізмів аутентифікації та авторизації у мережі підвищує впевненість у тому, що користувач, із яким встановлюється зв'язок, є не підставною особою і йому можна надавати санкціонований доступ;

- підслуховування. При передачі даних про користувача (призначених для користувачів ідентифікаторів та паролів) чи приватних конфіденційних даних по незахищених каналах можна підслухати ці дані і ними згодом зловживати. Методи для шифрування даних знижують ймовірність такої загрози;

- маніпулювання даними. Дані, що передаються в каналах зв'язку, можна змінити. В багатьох методах шифрування використовується технологія захисту цілісності даних, яка запобігає несанкціонованим їх змінам;

- відмова в обслуговуванні (Denial of Service - DoS) - це різновид хакерської атаки, у результаті якої стають недоступними важливі системи. Це досягається шляхом переповнення системи непотрібним трафіком, на обробку якого йдуть усі ресурси системної пам'яті та процесора. Система зв'язку має мати засоби для розпізнавання подібних атак та обмеження їх впливу на мережу;

- найбільш розвиненою формою шахрайства у Інтернет є, без сумніву, фішинг. Типовими інструментами фішингу є mail (поштові повідомлення, які

використовують методи соціальної інженерії) і спеціально розроблені web-сайти.

Число фішинг-атак зросла удвічі за шість перших місяців 2021 року, повідомляє Reuters із посиланням на "Звіт по загрозах інтернет-безпеки", що підготовлений Symantec.

В першому півріччі 2021 року фішери відправили 157 тисяч унікальних листів, що є на 81 відсоток більшим у порівнянні із другим півріччям 2020 року (рисунок 2.1). За словами авторів дослідження, такий кожен лист відправлений може бути сотням тисяч інтернет-користувачів.

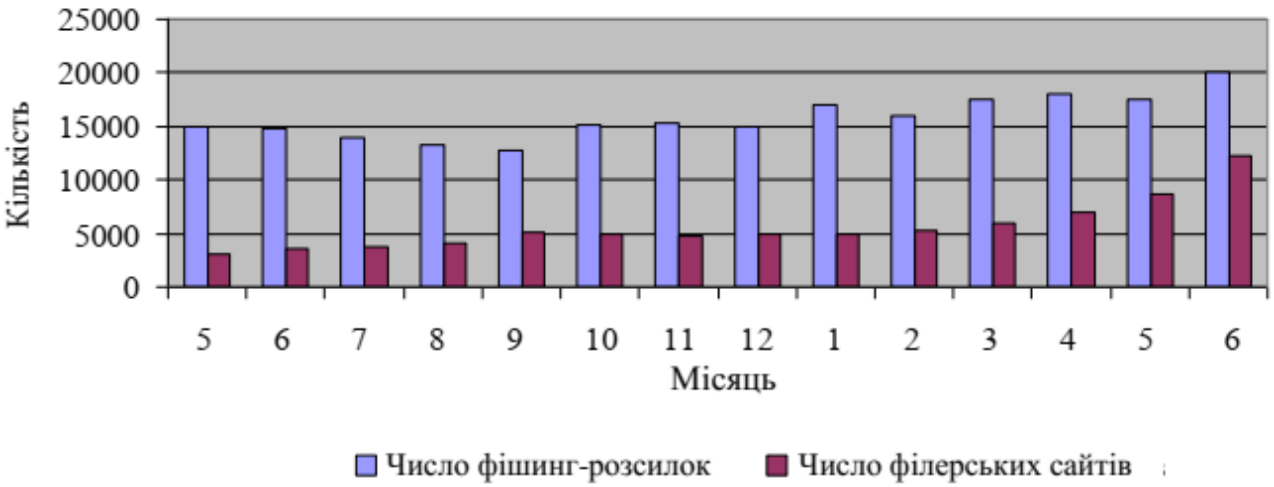

Рисунок 2.1 - Число фішинг розсилок і фішерських сайтів в світі з травня 2020 по червень 2021 року

Базовими елементами у області безпеки є аутентифікація, цілісність та активна перевірка. Аутентифікація покликана запобігати загрозі знеособлення та несанкціонованого доступу до ресурсів та даних. Хоч не завжди авторизація включає аутентифікацію до свого складу, але частіш за все обов'язково одне має на увазі інше. Цілісність забезпечує захист від підслуховування та маніпулювання даними, підтримуючи конфіденційність та незмінність переданої інформації. І, нарешті, активна перевірка означає перевірку правильності при реалізації елементів технології безпеки та допомагає виявляти несанкціоноване проникнення у мережу та атаки типу DoS.

Основа будь-якого захищеного зв'язку - це криптографія. Криптографією називається технологія складання і розшифровки зашифрованих повідомлень. Крім того, криптографія є важливою складовою для механізмів аутентифікації, цілісності і конфіденційності. Аутентифікація є засобом підтвердження особи відправника чи одержувача інформації. Цілісність означає, що дані не були змінені, а конфіденційність створює ситуацію, при якій дані не може зрозуміти ніхто, крім їх відправника та одержувача. Зазвичай криптографічні механізми існують у вигляді алгоритму (математичної функції) і секретної величини (ключа). Алгоритми широко відомі, в секреті необхідно тримати тільки криптографічні ключі. Причому чим більше бітів в такому ключі, тим менше він вразливий.

2.3 Формат передачі цифрового сигналу

Для передачі голосу в системах IP-телефонії початковий аналоговий сигнал перетворюється в цифровий формат – послідовність цифрових відліків, які можуть бути передані в IPпакетах. Процедура перетворення складається з трьох етапів: дискретизація; кодування; компресія динамічного діапазону.

Якщо для кодування відліків використовувати лінійну функцію, тобто таку, за якої співвідношення рівнів відліків буде точно відповідати співвідношенню кодів, якими вони представлені, сітка можливих значень кодів буде використовуватися неефективно. Рівень типового сигналу знаходиться здебільшого в середньому діапазоні, в той час як епізодичні сплески несуть в собі меншу частину інформації про сигнал (рисунок 2.2). Використання рівномірної сітки значень кодів у разі лінійної функції кодування призведе до того, що для кодування сплесків буде використовуватися невиправдано велика кількість значень.

Рисунок 2.2 - Діаграма сигналу вимовленого слова «технологія» (для запису використано програму Audacity)

Більшу ефективність кодування надає використання нелінійної функції, за якої для кодування рівнів сигналу в середньому діапазоні використовується щільніша сітка значень, ніж для кодування сплесків (рисунок 2.3).

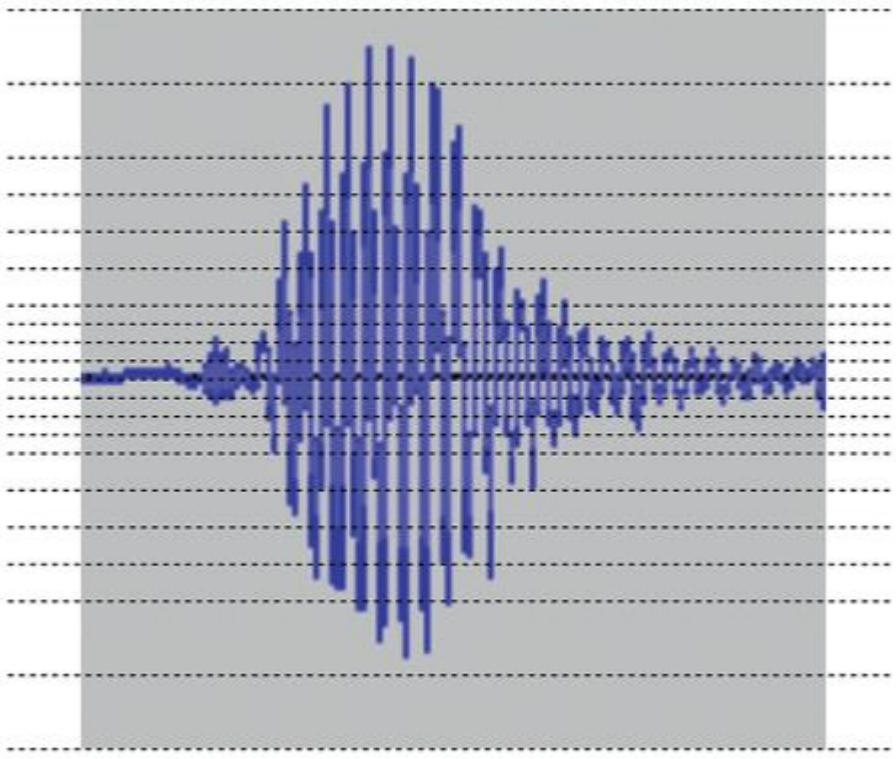

Рисунок 2.3 – Використання нелінійної функції кодування

Співвідношення між максимальним та мінімальним рівнями сигналу відомо як динамічний діапазон. У разі використання нелінійної функції кодування різниця між кодами сигналу в середньому діапазоні та сплеском є меншою ніж різниця між фактичними рівнями початкового сигналу, тому використання нелінійної функції кодування відомо як компресія (стискання)

динамічного діапазону сигналу. На сьогодні використовуються дві стандартні нелінійні функції кодування відліків, відомі під назвами α-law, яка поширена в Європі, та μ-law, яка поширена в США та Японії.

Описана процедура аналогово-цифрового перетворення відома під назвою «імпульсно-кодова модуляція» (англ.: Pulse Code Modulation або PCM). PCM формат використовує представлення початкового аналогового сигналу у вигляді 8-бітових цифрових кодів, які слідують з частотою 8000 за секунду. Для відтворення голосу співрозмовника з отриманої послідовності кодів виконується зворотна процедура цифро-аналогово го перетворення, до якої входять етапи:

- відновлення (декомпресія) динамічного діапазону;
- формування рівнів сигналу відповідно до цифрових кодів;
- згладжування для отримання аналогового сигналу з дискетних відліків.

Цифровий формат даних для передачі голосового сигналу у вигляді 8-бітових відліків, які передаються в темпі 8000 відліків за секунду, визначає потребу в пропускній здатності телефонної мережі на рівні 8х8 = 64 Кбіт/с для кожної телефонної розмови. В мережах традиційної телефонії на базі TDM для передачі кожної розмови в усіх проміжних каналах резервується ресурс – часовий слот. Наявність заздалегідь зарезервованого ресурсу згідно базового принципу мереж з комутацією каналів робить непотрібними будь-які заходи зі скорочення загального обсягу даних, що передаються.

В IP-телефонії ситуація відрізняється, адже замість резервування ресурсів під кожну розмову IP-пакети, кожен з яких містить відліки певної телефонної розмови, передаються через спільні канали. В цьому разі зменшення загального обсягу даних, що передаються, здатне знизити навантаження на канал або передати через нього більше одночасних розмов.

Для зниження обсягу – стиснення, голосових даних використовуються спеціальні функції – кодеки. З боку відправника початкові цифрові відліки голосу, для передачі яких потрібна пропускна здатність 64Кбіт/с, піддаються кодуванню, внаслідок якого обсяг даних знижується і відповідно для їх передачі

потрібна менша пропускна здатність. На боці отримувача здійснюється зворотня процедура – зі стиснутих даних відновлюються початкові відліки, які вже використовуються для відтворення голосового сигналу. Слово «кодек» утворене з початкових літер слов «кодування» та «декодування» і означає набір з двох функцій, які за сумісного використання на різних кінцях тракту передачі голосових даних забезпечують зменшення обсягу цих даних, що передається.

На перший погляд може здатися, що кодеки є подібними до відомих программ архівування файлів на кшталт zip або rar. Насправді це не так, оновними відмінностями кодеків від програм для архівування є такі:

- програми для архівування опрацьовують файл у цілому, тоді як кодеки обробляють лише потокові дані, тобто вони надходять постійно;

- час роботи програм для архівування не регламентується, тобто суттєве збільшення часу на стискання файлу некритичне, тоді як тривалість при обробці кодеком голосових даних додається до загальної затримки при передачі голосу до співрозмовника і перевищувати прийнятної межі не може;

- програми для архівування забезпечують 100 % зберігання інформації, файл до архівації і файл, що був відновлений із архіву, повністю є ідентичні, тоді як кодеки природу голосового сигналу враховують і з метою економії даних можуть привносити незначне погіршення якості.

Існує багато типів кодеків, що розрізняються такими параметрами, як рівень стиснення даних, ступінь погіршення якості, складність обробки, оптимальні умови використання. Деякі кодеки мають статус стандартних, описані документами Міжнародного Телекомунікаційного Союзу (International Telecommunication Union або ITU) та позначаються кодами виду G.7xx (наприклад, G.711, G.726, G.729 та ін.). Існують також фірмові кодеки, для їх використання необхідне використання на обох кінцях тракту передачі голосових даних обладнання певного виробника. В таблиці 2.1 наведено показники розповсюджених кодеків.

Таблиця 2.1 – Характеристики кодексів

Кодек	Потрібна пропускна здатність, Кбіт/с	Якість передачі голосу за 5-тибальною шкалою	Типове використання
G.711	64,0	4,3	Передача розмов
G.726r32	32,0	3,8	Передача розмов
G.736r24	24,0	3,75	Передача розмов
G.726r16	16,0	3,7	Передача розмов
G.728	16,0	3,75	Передача розмов
iLBC	13,3 або 15, 2	4,14	Використання в мережах з нестабільною якістю передачі пакетів
GSM Full Rate	13,0	3,5	Голосові меню, голосова пошта
G.729a	8,0	3,7	Передача розмов
G.723r63	6,3	3,7	Передача голосу та мультимедіа
G.723r53	5,3	3,65	Передача голосу та мультимедіа
G.722	64,0	4,5	Передача сигналу ширшого спектру до 7 кГц та кращої якості кодування 14 біт на відлік
G.722.1	32,0 або 24,0	4,09	Передача сигналу ширшого спектру до 7 кГц та кращої якості кодування 14 біт на відлік
G.722.2	16,0	3,98	Система сумісної передачі голосу і файлів зі змінними умовами щодо швидкості передачі даних

Стосовно передачі голосу через мережі IP-телефонії важливо пам'ятати про те, що до даних, які передаються, відносяться не лише цифрові відліки, але службова інформація, зокрема заголовки IP-пакетів і фреймів канального рівня.

Для визначення потрібної пропускної здатності мережі недостатньо використовувати значення, вказані в таблиці 2.1, натомість до них треба додати пропускну здатність під час накладних витрат – передачі службової інформації.

Як приклад можна навести розрахунки потрібної пропускної спроможності Ethernet-мережі для передачі однієї голосової розмови із використанням кодеку G.711.

Вихідні данні:

- тривалість фрагменту розмови, що передається одним IP-пакетом (визначає затримку при передачі голосу) – 20 мс;

- розмір заголовку контейнера у протоколі транспортування голосу (Real-time Transport Protocol чи RTP) – 12 байт;

- розмір заголовку у датаграмі транспортного протоколу UDP – 8 байт;

- розмір заголовку для пакета протоколу IP – 20 байт;

- розмір заголовку і контрольної інформації фрейму Ethernet – 18 байт.

Фрагмент розмови тривалістю 20 мс потребує 0,02x8000=160 відліків, тобто 160 байтів голосових даних. Після додання накладних витрат протоколів RTP, UDP, IP та фреймів Ethernet отримуємо загальний розмір фрейму 218 байт.

Передача фрагментів по 20 мс вимагає їх відправку в темпі 1/0,02=50 фреймів за секунду. Передача 50 фреймів розміром 218 байт за секунду потребує пропускної здатності мережі 10900 байт/с або 87,2 Кбіт/с.

Як бачимо, реальна потрібна пропускна здатність (87,2 Кбіт/с) на 36 % перевищує швидкість, потрібну для передачі лише голосових даних (64 Кбіт/с). Долю накладних витрат можна було б зменшити за рахунок подовження тривалості фрагменту, який передається в одному пакеті, але це призведе до збільшення затримки голосу і негативного впливу на якість послуги.

Слід зазначити що паралельно з кожною сесією взаємодії між абонентами по протоколу RTP для передачі голосу між ними також передаються пакети зі службовою інформацією по протоколу RTP Control Protocol (RTCP), але їх внесок в загальну потрібну пропускну здатність мережі незначний.

У разі використання кодеків з високим рівнем економії голосових даних, наприклад кодеку G.729a, який забезпечує передачу голосових даних зі швидкістю 8 Кбіт/с, доля накладних витрат ще більш зростає – для тривалості фрагменту в одному пакеті 20 мс потрібна пропускна здатність становитиме 31,2 Кбіт/с, тобто накладні витрати становитимуть 290%, а якщо збільшити тривалість фрагменту в пакеті до 30 мс – 23,5 Кбіт/с і 193% відповідно!Втім, порівняно з кодеком G.711 економія все одно істотна – 23,5 Кбіт/с проти 87,2 Кбіт/с для кожної телефонної розмови.

На завершення про кодеки доцільно зазначити, що вкрай бажано, щоби кінцеві пристрої абонентів, які проводять розмову, підтримували однаковий набір кодеків. Якщо умова відповідності кодеків не виконується, на шляху передачі голосових даних необхідним є перетворення між кодеками. Ця процедура потребує продуктивних сигнальних процесорів, збільшує затримку сигналу та погіршує його якість (адже будь-яка обробка погіршує початковий сигнал). Зазвичай в телефонній мережі, підконтрольній одній технічно-адміністративній групі, визначається єдиний базовий кодек, з використанням якого відбуваються всі розмови. У разі спілкування абонентів різних телефонних мереж з різними кодеками необхідною є підтримка кодеків обох мереж кінцевими пристроями абонентів (з яких під час розмови буде обрано той, що забезпечує вищу якість), або здійснення перетворення між кодеками на стику телефонних мереж.

2.4 Розробка алгоритмів захищених режимів IP-телефонії

Серед усієї різноманітності способів несанкціонованого перехоплення інформації особливе місце займає аналіз трафіку в мережі доступу, оскільки

мережа доступу - найперше і найзручніше джерело зв'язку між абонентами в реальному масштабі часу і при цьому найбільш незахищене.

Мережа доступу має ще один недолік з точки зору безпеки - можливість перехоплення мовної інформації з приміщень, по яких проходить телефонна лінія, і де підключений телефонний апарат (далі кінцеве обладнання (КО)), навіть тоді, коли не ведуться телефонні переговори. Для такого перехоплення існує спеціальне обладнання, яке підключається до телефонної лінії всередині контрольованого приміщення або навіть за його межами.

Для зручності аналізу проведено класифікацію каналу зв'язку за ступенем захищеності (захисту) переданої інформації. Зокрема, структурна схема алгоритму передачі даних у відкритому каналі показана на рисунку 2.4, а в напіввідкритому – на рисунку 2.5.

Рисунок 2.4 – Схема алгоритму передачі даних у відкритому каналі даних

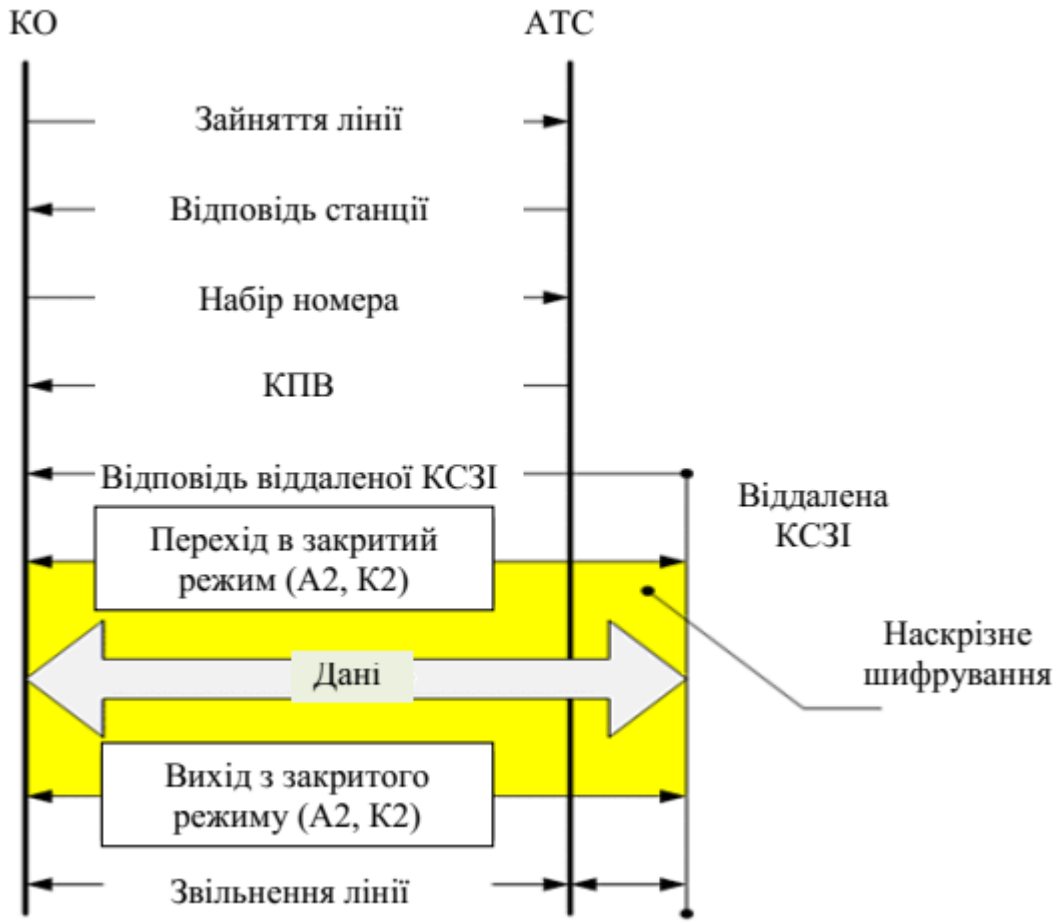

Рисунок 2.5 – Схема алгоритму передачі даних у напіввідкритому каналі даних

Основна проблема, із якою стикаються користувачі мереж, в яких застосовується наскрізне шифрування, пов'язана із тим, що службова інформація, що використовується для встановлення з'єднання, передається по мережі у незашифрованому вигляді. Досвідчений криптоаналітик може для себе отримати масу корисної інформації, знаючи хто із ким, як довго і о котрій годині спілкується через мережу доступу. Йому для цього не потрібно навіть бути у курсі предмета спілкування.

В порівнянні із канальним, шифрування наскрізне характеризується більш складною роботою із ключами, так як кожна пара користувачів має бути забезпечена однаковими ключами перед тим, як вони можуть зв'язатися один із одним. Оскільки криптографічні алгоритми реалізовані на верхніх рівнях моделі OSI, то доводиться стикатися також із багатьма суттєвими відмінностями у комунікаційних протоколах та інтерфейсах мережі доступу (наприклад:

відправник - канал ТЧ, одержувач - 2В + D). Це все ускладнює практичне застосування наскрізного шифрування.

Наведені вище методи захисту інформації вже не задовольняють сучасних вимог. При використанні цих методів зловмисник може перехоплювати адресну інформацію, вести моніторинг переданих даних, несанкціоновано підключатися до лінії, спотворювати інформацію, що передається.

Єдиним можливим методом, що задовольняє всім сучасні вимогам, є використання комбінації канального і наскрізного шифрування. При цьому може закривається вся передана по каналу зв'язку інформація.

Комбінація канального та наскрізного шифрування даних в мережі доступу обходиться значно дорожче, ніж кожне із них окремо. Однак саме такий підхід дозволяє найкращим чином захистити дані, що передаються по мережі. Шифрування у кожному каналі зв'язку не дозволяє зловмисникові аналізувати службову інформацію, що використовується для маршрутизації. Наскрізне шифрування зменшує ймовірність доступу до незашифрованих даних у вузлах мережі.

При цьому зловмисник може проводити аналіз тільки відкрито переданих даних, але не може нелегально використовувати лінію зв'язку.

Структурна схема передачі даних в закритому каналі показана на рисунку 2.6.

При зайнятій лінії (отриманні сигналу виклику від АТС) відбувається автоматичний перехід в закритий режим зв'язку (А1, К1). Після переходу в закритий режим, абонентський комплект (АК) або криптографічний модуль перед АК АТС аутентифікує КСЗІ. Даний крок необхідний для усунення можливості несанкціонованого використання лінії. Після проведення аутентифікації можливий вихід із закритого режиму.

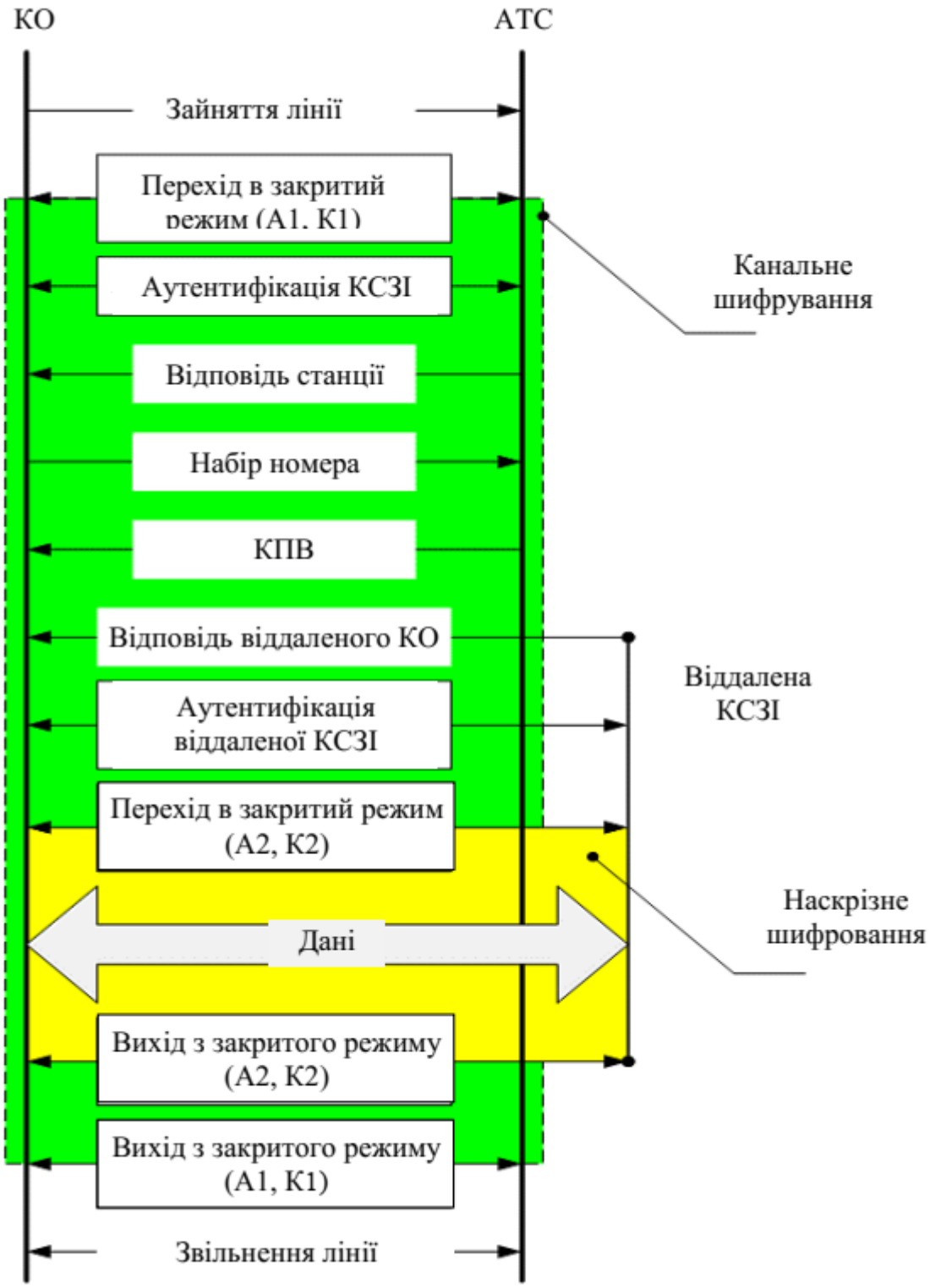

Рисунок 2.6 - Передача даних в закритому каналі

При виклику з боку абонента АТС приймає адресну інформацію і встановлює з'єднання. При відповіді віддаленої КСЗІ можливі два варіанти: аутентифікації віддаленої КСЗІ і перехід в закритий режим (А2, К2) або перехід в закритий режим (А2, К2) і аутентифікація віддаленої КСЗІ.

Аутентифікація віддаленої КСЗІ необхідна для протидії атаці, при якій віддалена КСЗІ зловмисника за допомогою перекомутації видає себе за КСЗІ легального користувача.

Після вдалої аутентифікації віддаленої КСЗІ можливий вихід із захищеного режиму (відмова від входження в захищений режим).

Також під час передачі даних необхідно проводити т.зв. перевірку зворотного коду. Вона являє собою процедуру захисту, яка здійснюється в процесі передачі даних і полягає в тому, що у віддаленій КСЗІ періодично запитується ідентифікуюча інформація, яка і називається зворотним кодом. Ця інформація порівнюється з еталонною, збереженою при аутентифікації на початку сеансу зв'язку. При розбіжності кодів передача блокується. Перевіркою зворотного коду можна виявити факт зміни (перекомутації) напрямків видачі даних або злочинного використання приймального пристрою зареєстрованого (законного) респондента.

2.5 Режим використання шлюзів для IP-телефонії

У загальному випадку IP-телефонія базується на двох основних операціях:

- перетворення аналогової двобічної мови у цифрову форму всередині кодую чого чи декодуючого пристрою (тобто кодека);

- упаковку у пакети для передачі по IP-мережі.

Такі функції виконують найчастіше автономні шлюзи, що кілька різновидів мають. Це можуть бути чи виділені пристрої, чи поєднані маршрутизатори або комутатори із вбудованим апаратним та програмним забезпеченням у шлюзі. Інший тип - це коли шлюз об'єднаний із обладнанням для віддаленого доступу та пулом модемів.

Незалежно від способу при апаратній реалізації шлюзи у IP-телефонії мають володіти необхідними властивостями:

- сумісність з стандартом H.323. Базовим для роботи IP-обладнання прийнято було протокол H.323v2, що стандартизує мультимедійний зв'язок у мережах із комутацією пакетів. Абоненти можуть підключатися до цієї системи шлюзів. Виклики можуть бути при цьому спрямовані на підтримуючі H.323 шлюзи від інших виробників. У результаті дана система буде забезпечувати інтеграцію мови, відео та даних у реальному масштабі часу (наприклад, система Microsoft NetMeeting);

- наявність механізмів для резервування ресурсів. Підтримка деякої схеми пріоритетності (протокол резервування RSVP чи байт диференціації послуг - DS) для її здійснення при можливості вибору пріоритету між переданою промовою чи даними є важлива характеристика шлюзу. Протокол RSVP при цьому маршрутизаторам дозволяє резервувати частину смуги для пропускання при організації голосового трафіку;

- підтримка основних телефонних інтерфейсів та типів сигналізацій. Важливим критерієм для оцінки характеристик шлюзів є найбільш можлива різноманітність у телефонних інтерфейсах, що підтримуються IP-шлюзом (E1, BRI, PRI), зокрема, аналоговий. А також підтримка таких основних типів телефонної сигналізації: DTMF, CAS, PRI і ОКС № 7. При цьому відіграє істотну роль підтримка обладнанням механізмів для безпеки відповідно до рекомендацією H.235;

- транспортні архітектури. Діапазон транспортних архітектур, з якими сучасні шлюзи працюють, є досить широкий: ISDN, виділені лінії, Frame Relay, Ethernet, ATM;

- масштабованість, що забезпечується модульною побудовою в обладнанні. При першому етапі у розгортанні мережі для IP-телефонії можливе використання деякого неповного ресурсу усіх наявних портів при поступовому збільшенні числа задіяних голосових портів. Тоді число портів відповідає кількості з одночасних викликів, що може зробити шлюз, оскільки кожен з його портів оснащений власним сигнальним цифровим процесором (DSP - Digital Signal Processor) для оцифрування голосових сигналів;

- забезпечення факс-зв'язком. Це на два стандарти спирається. У стандарті T.37 передача факсів зводиться до доставки із проміжним зберіганням, оскільки зображення у факсах передаються як вкладення електронної пошти. Завдяки стандарту T.37 факс-апарати та факс-сервери взаємодіяти можуть один із одним злагоджено, як і факси традиційні. Стандарт T.38 описує передачу факсів у реальному масштабі часу чи з допомогою імітації з'єднання із факс-апаратом, чи з допомогою методу для модуляції під назвою FaxRelay. T.38 використовуватися може і для реалізації функціональності, яка схожа із факсимільним традиційним зв'язком;

- управління шлюзом. Шлюзи відрізнятися можуть передбаченими засобами для управління. Дані засоби для управління своєю функцією мають маршрутизацію викликів між шлюзами та перекодування з телефонних номерів у IP-адреси. Вони можуть конструктивно бути інтегровані із шлюзом чи собою являти окремий «мультимедійний менеджер конференцій» чи «багатоголосовий менеджер доступу». Одним із рішень є використання єдиного пакета, який включає у себе засоби для білінгу, маршрутизації викликів та мережевого адміністрування;

- можливість встановлення різних алгоритмів для кодування мови. На якість переданого голосу в IP-мережі впливає істотно схема кодування, що використовується у шлюзі IP-телефонії для стиснення голосової інформації. Найпоширенішою є схема, яка забезпечить найбільший ступінь для стиснення інформації і відповідна специфікації G.723.1 (до 5.3 кбіт / с). Застосовуються інші схеми - G.711, G.729a, G.728, G.726.

В останній час з'явилися такі види обладнання для IP-телефонії при усіх сценаріях:

- автономні шлюзи для IP-телефонії, які підключаються до АТС через цифрові та аналогові інтерфейси та здійснюють попередню обробку мовних сигналів, їх компресію, упаковку у IP-пакети та передачу їх у мережу;

- мовні магістральні плати із інтерфейсом 10 / 100BaseT (ЛВС Ethernet) для підключення існуючих засобів до корпоративної IP-мережі. Після установки у

АТС такої плати мовний трафік в вигляді IP-пакетів направлений може бути по локальній чи глобальній пакетній мережі подібно, як він передається по телефонній мережі від АТС;

- телефонні апарати, що упаковують мовну інформацію у IPпакети (IP-телефони) та підключаються не у телефонну мережу, а в ЛВС Ethernet. Вимагають такі апарати мінімальних налаштувань мережевого адміністратора, використовуючи при цьому протокол динамічної конфігурації DHCP;

- спеціалізовані комутатори для мовних пакетів, які призначені для виконання функцій традиційної АТС на основі протоколу IP (IP-АТС). Апаратура для IP-телефонії випускається у суміщеній чи автономній конструкції. Виконує поєднаний сервер функції шлюзу, воротаря та адміністратора (manager), здійснює маршрутизацію та збір білінгової інформації (IP-адреса, час початку та кінця розмови тощо), придушення ехосигналів та детектування пауз у розмові, заповнення пауз при прийомі комфортним рівнем шуму (comfort noise) та буферизацію прийнятих пакетів для зменшення джитера, інтерполяцію втрачених мовних пакетів та контроль стану у розмовному каналі (джитер, середній час для затримки, відсоток втрат у пакетах). У автономній конструкції функції ці виконуються окремими пристроями.

В ранніх моделях уся цифрова обробка сигналів проводилася програмними засобами. Потім програмна обробка змінилася апаратною, почали виконувати основну роль плати DSP (Digital Signal Processing), що розвантажило основний процесор та оперативну пам'ять, а також збільшило число портів для обладнання і зменшило час для затримки мовної інформації.

Найвідоміші плати DSP фірм Texas Instrument, Dialogic (DM3 IP Link) та Natural Microsystems (Quad E1). На рисунку 2.7 представлена структурна схема шлюзу, яка реалізована на базі спеціалізованих процесорів DSP, інші функції виконує ПЗ, яке використовує універсальний процесор.

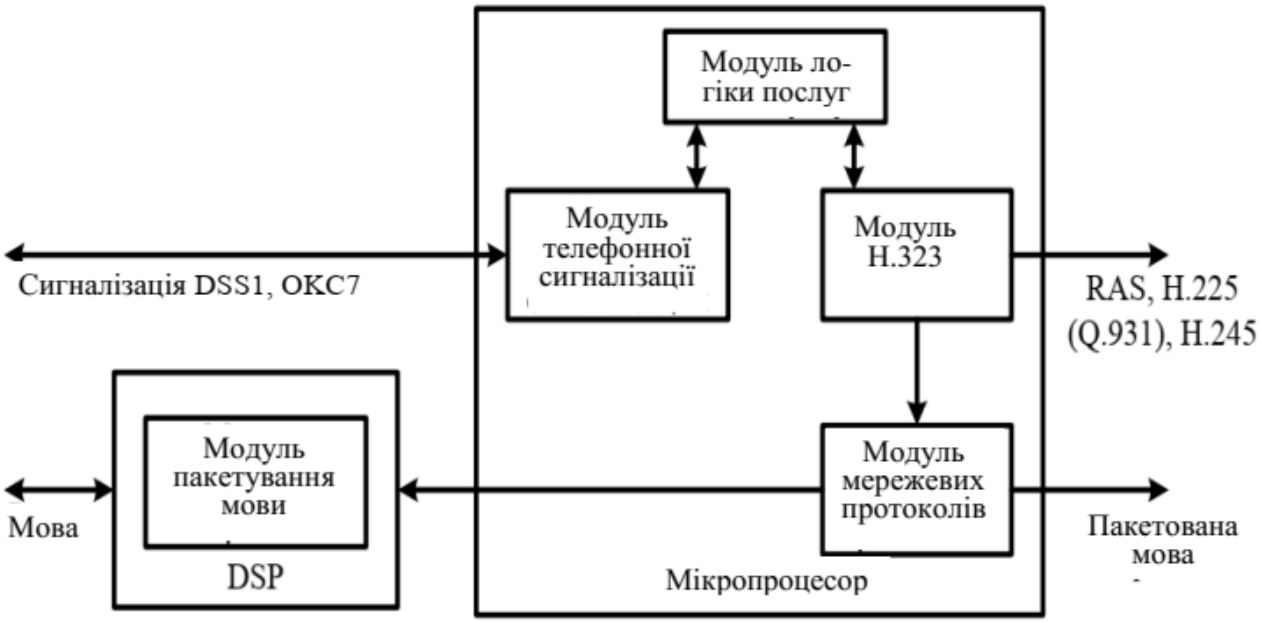

Рисунок 2.7 - Структурна схема для шлюзу

Модуль для обробки телефонної сигналізації взаємодіє із телефонним обладнанням і перетворює сигнали систем DSS1 та ОКС7 у внутрішньосистемні примітиви, які відображають стан процесу при обслуговуванні виклику (встановлення з'єднань, відбій тощо) і використовуються у модулі логіки для послуг шлюзу при встановленні з'єднань. Модуль сигналізації H.323 має обробляти сигнальну інформацію з протоколів RAS, H.225.0 (Q.931) та H.245. Інформація про стани процесу при обслуговуванні виклику у IP-мережі передається у модуль логіки для послуг шлюзу.

Модуль логіки для послуг шлюзу у IP-телефонії відповідає за маршрутизацію виклику, який надійшов у IP-мережу. Виробляються операції контролю доступу та аналізу телефонного номера абонента, який викликається, із подальшим визначенням та наданням необхідної послуги. Модуль пакетування мови виконує функції для підготовки мовного сигналу, який надходить із постійною швидкістю, для подальшої передачі його по мережі із маршрутизацією пакетів IP.

Основні функції модуля: перетворення мовного сигналу на основі ІКМ, кодування для мовного сигналу, ехокомпенсація, виявлення активних періодів та пауз у мові, а також адаптація відтворення. Крім того, відповідає модуль за

детектування та генерацію сигналів DTMF, за обробку факсимільних та модемних сигналів. На рисунку 2.8 представлена структура для модуля пакетування мови.

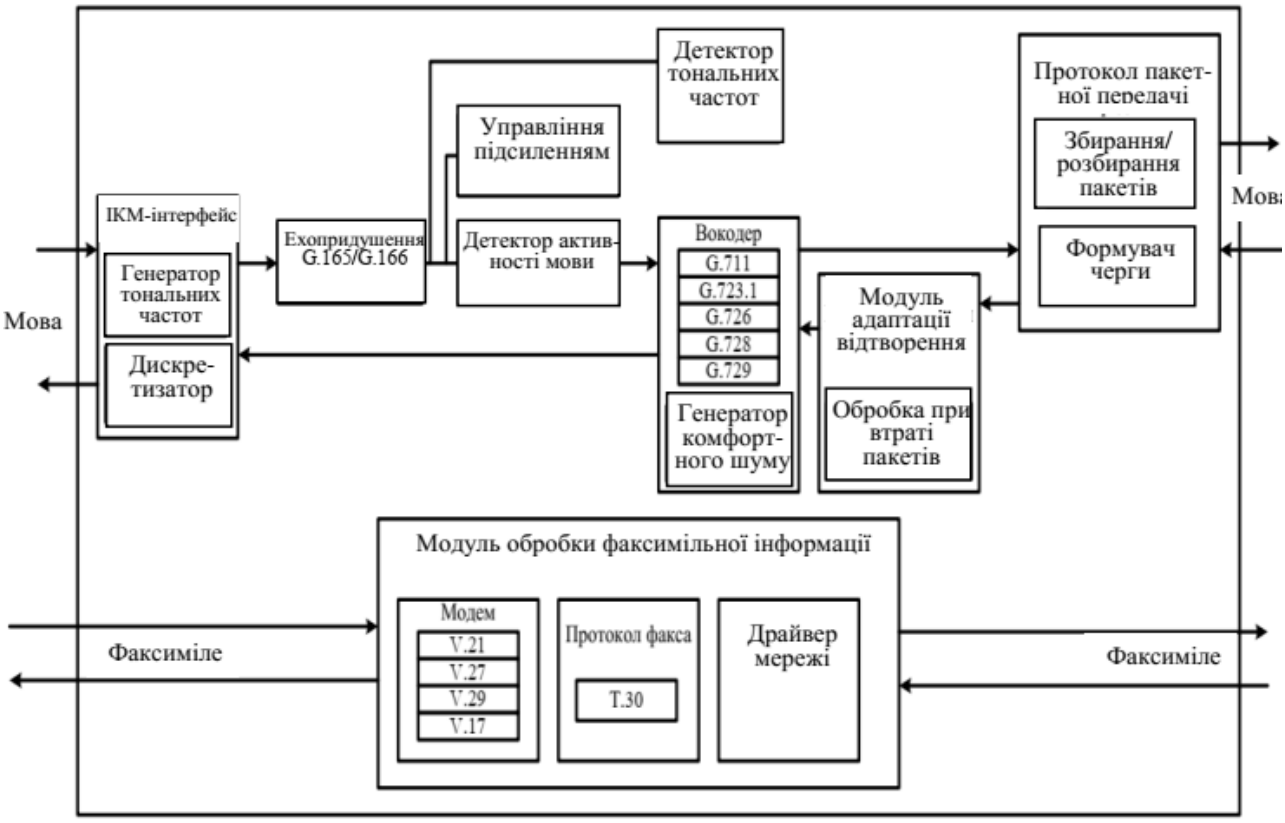

Рисунок 2.8 - Модуль пакетування мови

Механізм для виявлення активних періодів мовної інформації перевіряє одержуваний сигнал на наявність у ньому мовної інформації. Коли протягом певного часу мовної інформації не знайдено, тоді передача мовних IP-пакетів у IP-мережу припиняється. Використання такого механізму підвищує істотно ефективність використання у смузі пропускання. Економія для смуги доходити може до 60%.

3 РЕАЛІЗАЦІЯ ТА ДОСЛІДЖЕННЯ РОЗРОБЛЕНИХ АЛГОРИТМІВ

3.1 Побудова Site-to-site VPN на Cisco ASA

VPN (Virtual Private Network) - приватна віртуальна мережа. Технологія VPN передбачає підключення віддалених користувачів через загальнодоступні мережі до локальних мереж по захищених каналах зв'язку (рисунок 3.1).

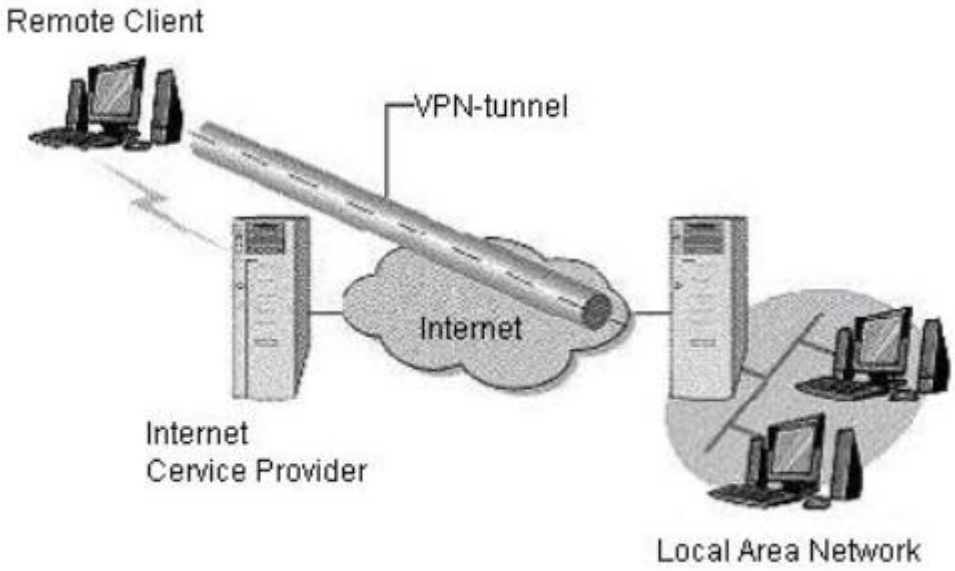

Рисунок 3.1 - Структурна схема VPN для віддалених користувачів

В якості віддалених користувачів виступають:

-працівники, які працюють в підприємствах з розділеною інфраструктурою, тобто компанії, у яких може бути кілька точок, магазинів, офісів; які розташовані в різних районах міста або області;

-працівники, у яких робота безпосередньо пов'язана з відрядженнями, але їм необхідно мати доступ до локальної мережі компанії.

Технологія VPN забезпечує безпеку передачі даних по загальнодоступних мережах за допомогою їх шифрування.

Для організації мережі VPN потрібно:

- канал доступу для центрального офісу, кожного підрозділу або користувача. Це може бути як виділена, так і комутована лінія;

- обладнання вузла доступу в центральному офісі (VPN-сервер), обладнання доступу для кожного підрозділу або користувача (VPNкліент).

Основною функцією VPN є захист трафіку. Таке завдання дуже складне на криптографічному рівні захисту. Для цього, по-перше, необхідно мати надійну криптографію, яка б гарантувала захист від прослуховування, володіти надійною системою захисту управління ключами, захист від атак, а також перевірка працездатності користувача на даний момент. По-друге, потрібно забезпечити масштабованість конкретної VPN. Найбільш успішно для цього застосовуються VPN-агенти, які здійснюють захист трафіку на всіх видах обладнання - робочих станціях, серверах або шлюзах.

У VPN є відмінна риса, вона зазвичай може розрізняти окремі комп'ютери, але не самих користувачів. Але іноді необхідно, щоб вона могла відрізнити окремі застосування і користувачів. Користувач зобов'язаний сприйняти однакову сукупність налаштувань програми незалежно від того, за яким комп'ютером він сидить. Необхідні для цього всі дані містяться в призначеному для користувача електронному пристрої, дискеті, на флешці тощо. Якщо підприємство застосовує спеціальні сервери доступу, то VPN повинна вміти працювати спільно з такою системою, і вона не повинна підключати до системи користувачів, які не пройшли авторизацію.

VPN утворює непроникні канали зверху відкритих мереж. В звичайному житті підприємствам необхідно, щоб працівники мали доступ з VPN у відкриту мережу і Інтернет. Міжмережевий екран (МЕ) здійснює контроль в критичних точках контакту з відкритою мережею. Формулювання: мережею VPN забезпечуються функції МЕ в кожній області, де присутній її агент. МЕ, який контролюється з центру безпеки, і VPN вважаються взаємодоповнюючими системами, вони вирішують дві пов'язані задачі:

- використовує відкриті мережі в якості каналу дешевого зв'язку (VPN);

- забезпечує захист від атак, які при роботі з відкритою інформацією містяться у відкритих мережах (МЕ).

VPN гарантує захист інформації, яка передається, але не може здійснити її захист на відправному кінцевому комп'ютері. Таке завдання вирішується спеціальними засобами:

- система криптозахисту даних;
- система захисту від несанкціонованого доступу до обладнання;
- антивірусні системи тощо.

Тунелювання (tunneling) або інкапсуляція (encapsulation) – метод передачі корисних даних за допомогою проміжної мережі. В якості інформації можуть бути пакети іншого протоколу. При способі інкапсуляції кадр відправляється не у вигляді згенерованого вузлом відправника, а йому присвоюється додатковий заголовок, в якому міститься інформація про маршрут, адресу термінатора тунелю і ініціатора тунелю, які дозволяють проходити через Інтернет інкапсульованим пакетам. Передача пакетів здійснюється термінатором тунелю на кінці шляху після деінкапсуляції. Даний процес, який включає в себе інкапсуляцію і подальшу передачу пакетів, називається тунлюванням. Тунелем називається шлях пересування переданих інкапсульованих пакетів.

Робота VPN заснована на протоколі Point-to-Point Protocol (PPP). Цей протокол створений для передачі даних через телефонні мережі і виділеним сполученням «точка-точка» - xDSL, він також може працювати з багатоканальними з’єднаннями - ISDN, X.25 і Frame Relay. Розширення пропускної здатності в PPP досягається за допомогою підключення декількох паралельних каналів MultiLink Protocol (MP). Протокол PPP проводить інкапсуляцію пакетів IP, IPX і NetBIOS в кадри PPP і здійснює їх передачу по виділених каналах «точка-точка». Використовується даний протокол маршрутизаторами, які з'єднані за допомогою виділених каналів, або клієнтом, з’єднаним віддаленим підключенням.

Одним з методів захисту даних в мережах IP-телефонії є застосування шифрованих тунелів VPN. Організація з'єднання у VPN відбувається по каналу типу точка-точка, яка по-іншому називається тунелем (рисунок 3.2). Тунель зазвичай створюється в загальнодоступній мережі Інтернет, де мережа

незахищена. Зв'язок типу точка-точка говорить про те, що з'єднання встановлюється між двома комп'ютерами, які називаються peers.

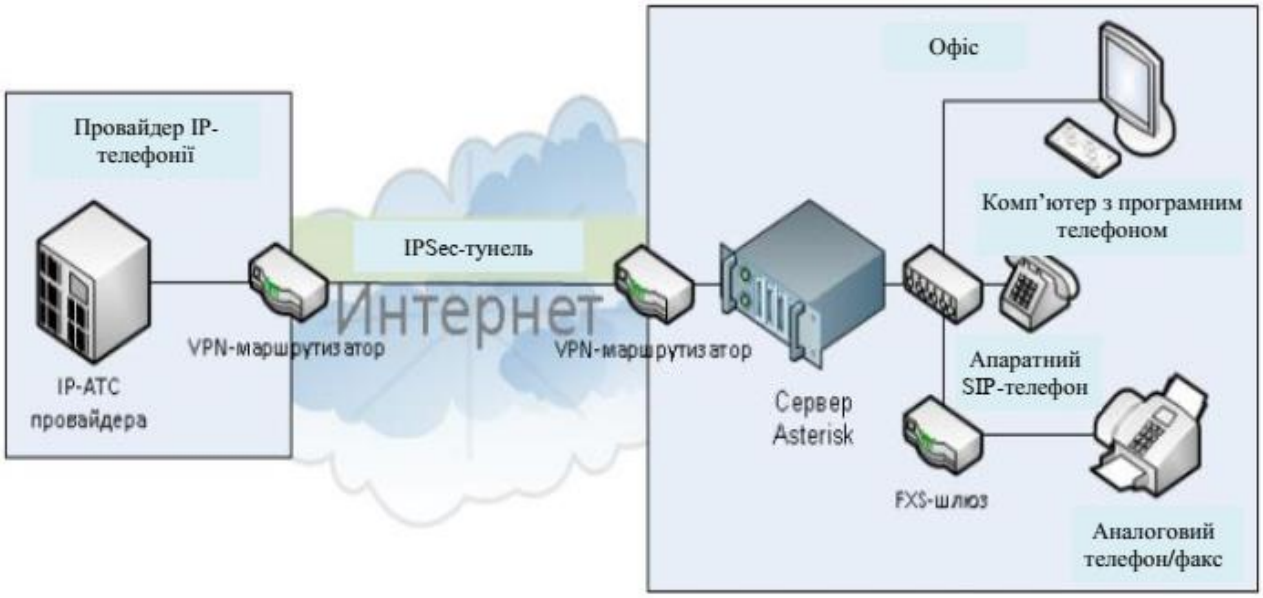

Рисунок 3.2 - Схема роботи IP-телефонії через VPN-тунель

Віртуальна приватна мережа в порівнянні з іншими способами віддаленого доступу має деякі економічні переваги. Потреба в застосуванні модемів виключається, так як у користувача є можливість безкомутованого з'єднання звернутися до корпоративної мережі. Організація віддаленого доступу без виділених ліній теж є однією з переваг.

Приклад побудови мережі між двома офісами - центрального і філії за допомогою логічного з'єднання (тунелю) можна розглянути в багатофункціональній програмі - Cisco Packet Tracer.

Як приклад можна розглянути організацію мережі між двома офісами і необхідно організувати віддалений доступ з локальної мережі центрального офісу на філію. Необхідність здійснити захист трафіку по мережі Інтернет є одним з головних завдань.

Два МЕ доцільно налаштовувати для організації постійного безпечного тунелю VPN із застосуванням набору протоколів IPSecurity (IPSec). Вони

передаються по міжмережевому протоколу IP. Організація VPN типу Site-to-site передбачає об’єднання двох сторін.

Процес побудови мережі можна розділити на дві фази. Перша фаза – дві сторони по протоколу IKE узгоджують параметри технологічного з'єднання; якщо вони автентифіковані, то піднімається захищений ISAKMP Tunnel, за яким обидві сторони домовлятимуться про основні IPSec тунелі. Друга фаза передбачає укладення угоди про параметри IPSec тунелю. Потім піднімається сам тунель, по якому будуть рухатися призначені для користувача дані в зашифрованому вигляді.

3.2 Засіб для захисту IP-телефонії

З точки зору системної інтеграції запропонований засіб складається із двох підсистем: програмної, яка забезпечує інтерфейс із мережевим протоколом, та апаратної, що реалізує представлений алгоритм шифрування інформації на базі нерозкривних шифрів. Загальну схему взаємодії підсистем показано на рисунку 3.3.

Запропонована система для захисту працює у потоковому режимі, тобто зашифровані дані, які передають каналом зв'язку, розшифровуються у прикінцевому пристрої, а обробляються далі іншими застосуваннями чи апаратними пристроями. Тому режим функціонування для системи захисту не припускає збереження даних в зашифрованому вигляді.

Програмна підсистема дає необхідний набір з API-функцій для сторонніх застосувань, та реалізує розроблений функціонал. Для застосувань апаратна підсистема представляється в вигляді набору з функцій, що викликаються при виклику заданих API-функцій з програмної підсистеми. Така реалізація дозволяє модифікувати гнучко різні підпрограми без необхідності повторного перепрограмування всього пристрою.

Рисунок 3.3 - Загальна схема роботи пристрою захисту

Крім цього з'являється можливість додавати у апаратну частину нові реалізації для алгоритмів генерації псевдовипадкових чисел, протоколів узгодження, спеціалізованих функцій обробки різного контенту тощо. Із урахуванням зростаючої необхідності у передачі мультимедійної потокової інформації у комп'ютерних мережах був створений пристрій (рисунок 3.4) на базі спецпроцесора серії TMS320 C5505 цифрової обробки сигналів. Це забезпечило необхідну продуктивність.

Суть розробленого алгоритму шифрування така. В масив пам'яті SD-картки записуються істинно випадкові числа (шум двигунів, шум лісу тощо), з яких створюється спеціальний масив (буде він секретним ключем). Береться байт з мультимедійного файлу, що треба зашифрувати, розшукується в секретному ключі його адреса, яка передається по мережі. На приймаючій стороні є такий же самий масив з істинно випадкових чисел (це є секретний ключ), на якій розшукується відповідно до прийнятої адреси значення байта, що стане байтом у зашифрованій послідовності. Даний алгоритм буде гранично криптостійким. Існує багато варіантів для його реалізації.

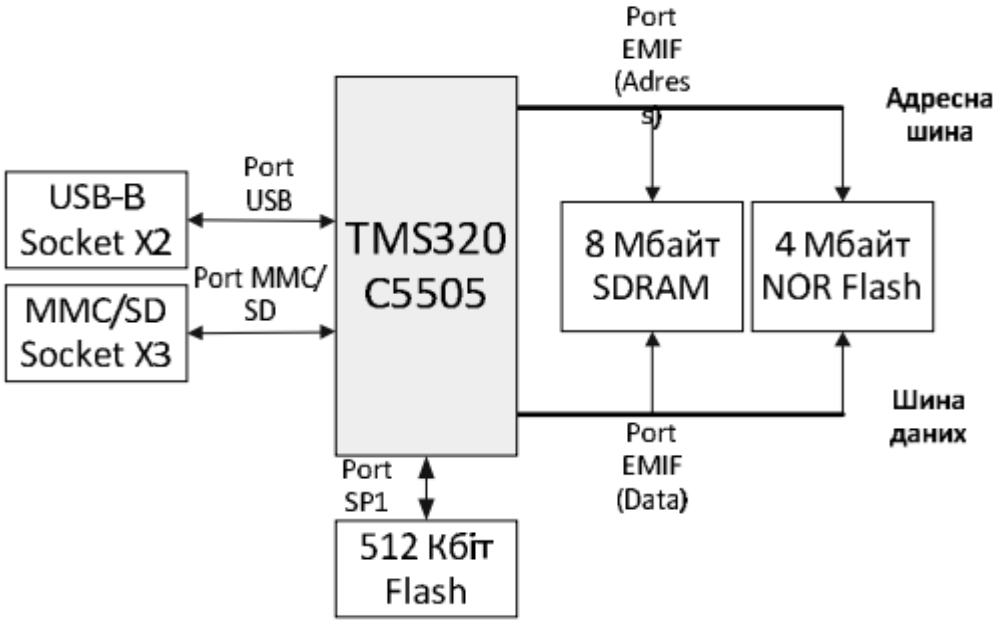

Рисунок 3.4 - Схема пристрою шифрування

Схему спрощеного варіанта пропонованого алгоритму шифрування наведено на рисунку 3.5.

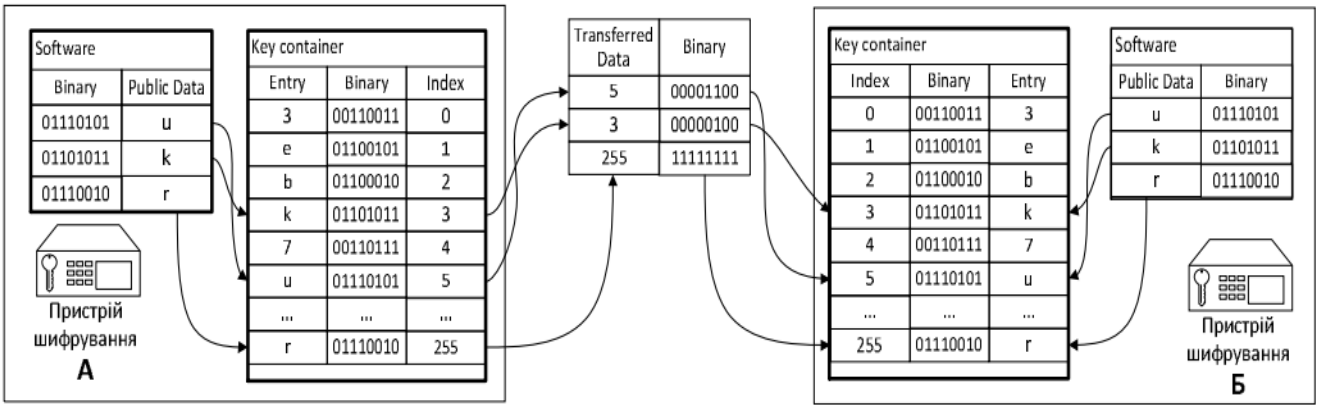

Рисунок 3.5 - Спрощений алгоритм для передавання зашифрованої потокової інформації у реальному часі

Наприклад, вибирається один з кращих алгоритмів генерації псевдовипадкових чисел із певними параметрами («зерно»). Передаюча сторона на основі істинно випадкових чисел (відповідно до вказаного алгоритму) відправляє приймаючій стороні «зерно». Приймаюча сторона, використовуючи всі ці параметри, генерує на льоту відповідні псевдовипадкові числа і них чисел

вибирає байти для переданої мультимедійної інформації. У такому випадку об’єм вихідного масиву чисел значно меншим може бути.

3.3 Модель організації забезпечення безпеки в IP-телефонії на прикладі Site-to-site VPN

Як вже було згадано вище, одним з методів захисту даних в мережах IP-телефонії є використання шифрованих тунелів VPN. Організація з’єднання у віртуальній приватній мережі (VPN) відбувається по каналу типу точка-точка, яка по-іншому називається тунелем. Тунель зазвичай створюється у загальнодоступній мережі Інтернет, де мережа незахищена. Зв'язок типу точка-точка говорить про те, що з’єднання встановлюється між двома комп’ютерами, які називаються peers.

В якості прикладу організації з’єднання у віртуальній приваній мережі розглянуто організацію мережі між двома офісами і необхідно здійснити віддалений доступ з локальної мережі центрального офісу на філіал (рисунок 3.6). Необхідність забезпечення захисту трафіка по мережі Інтернет є однією з головних задач.

Для налаштування двох міжмережевих екранів для організації постійного безпечного тунеля VPN доцільно використовувати набір протоколів IPSecurity (IPSec). Організація VPN типу Site-to-site передбачає об’єднання двох сторін.

Cisco ASA є апаратним міжмережевим екраном з інспектуванням сесій із збереженням стану (stateful inspection). ASA може працювати в двох режимах: routed (режим маршрутизатора за замовчуванням) і transparent (прозорий міжмережевий екран, коли ASA працює як бридж з фільтрацією).

Перед тим, як приступити до роботи, потрібно з допомогою команди show run перевірити настройки конфігурації Cisco ASA 1 (рисунок 3.7). Видно, що fastEthernet 0/0 налаштований на Vlan 2, який є outside інтерфейсом.

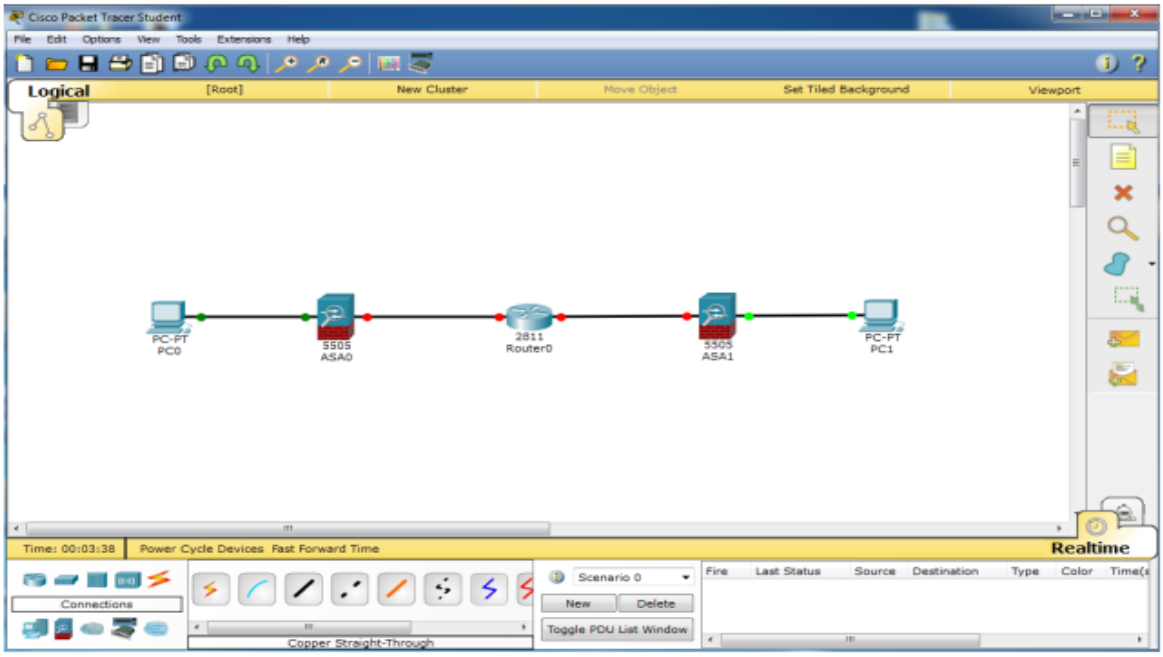

Рисунок 3.6 – Схема Site-to-site VPN на Cisco ASA

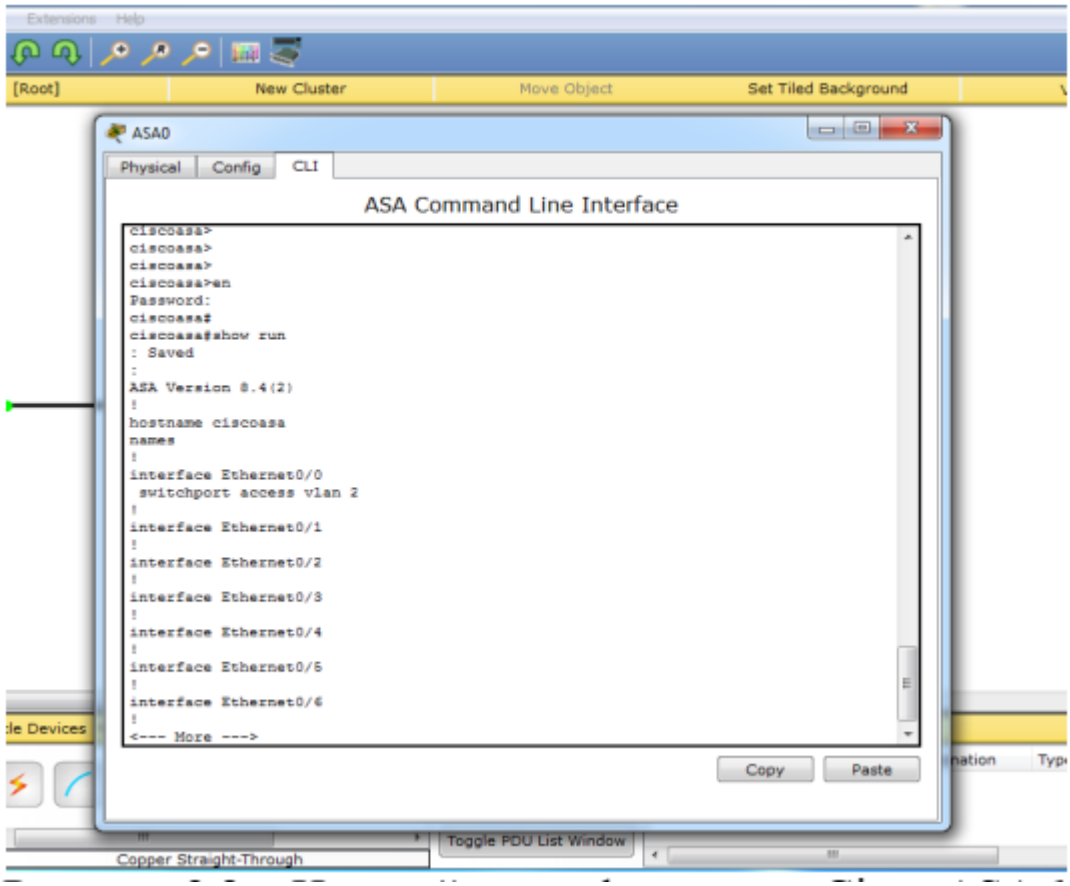

Рисунок 3.7 – Налаштування конфігурації Cisco ASA 1

Проведемо такі операції в налаштуваннях Cisco ASA 1. Задамо IP-адресу 210.210.1.2 на outside інтерфейс з маскою 255.255.255.252. Далі потрібно добавити default маршрут на Cisco ASA 1, через outside інтерфейс з допомогою IP-адреси інтернет-провайдера 210.210.210.1.1. Проведення інспектування трафіка (stateful inspection) є обов'язковим моментом і воно проводиться з визначенням класу map, далі створюється policy map і з вказанням створеного map інспектується icmp-трафік. Таку ж роботу треба проробити на іншому приладі Cisco ASA 2.

Потім налаштовується роутер провайдера (рисунок 3.8). На інтерфейсі fastEthernet 0/0 налаштовується IP-адреса 210.210.1.1 з маскою 255.255.255.252, а на інтерфейсі fastEthernet 0/1 IP-адрес буде 210.210.2.1 з маскою 255.255.255.252.

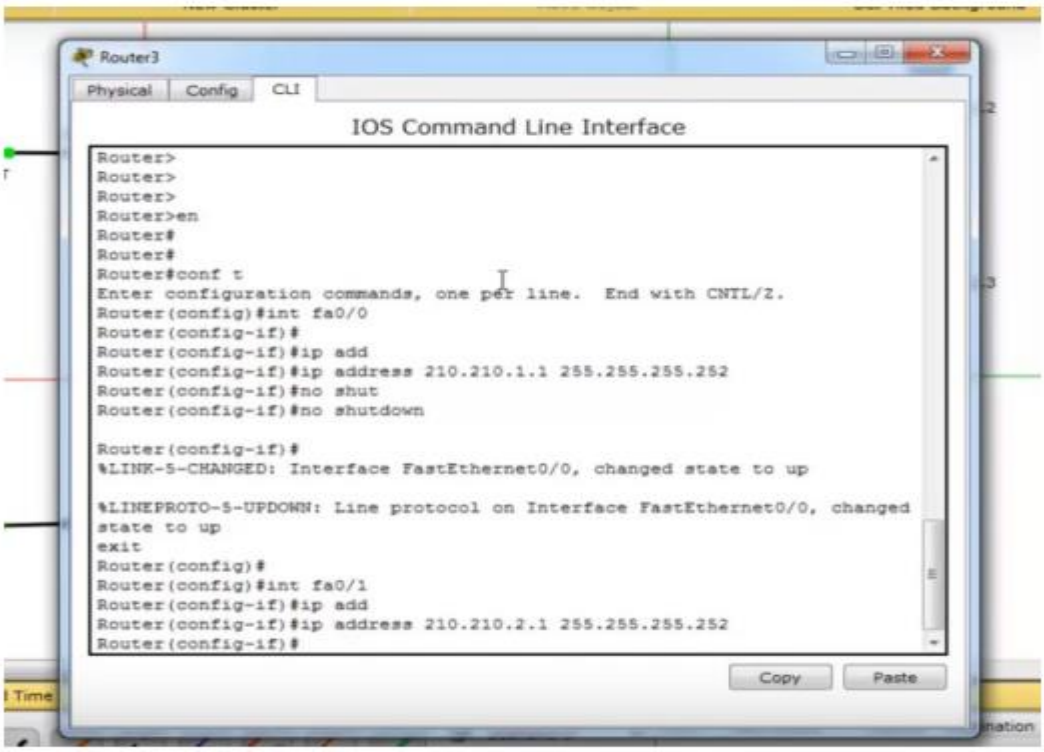

Рисунок 3.8 – Налаштування роутера провайдера

Далі організовується VPN. Даний процес можна розділити на дві фази. Перша фаза – дві сторони по протоколу IKE узгоджують параметри технологічного з'єднання; якщо вони аутентифікуються, то піднімається

захищений ISAKMP Tunnel, по якому обидві сторони будуть домовлятися про основний IPSec тунель. Друга фаза передбачає заключення домовленостей про параметри IPSec тунеля. Потім піднімається сам тунель, по якому будуть рухатися користувацькі дані в зашифрованому вигляді.

Аналогічно до попереднього, спочатку виконуються всі операції на Cisco ASA 1, потім виконується ця ж робота на Cisco ASA 2.

Для налаштування першої фази включається на outside інтерфейсі протокол IKE з допомогою команди crypto ikev1 enable outside. Потім налаштовується політика crypto ikev1 policy 1 і прописуються наступні параметри: encr 3des, hash md5.

Далі проводиться аутентифікація командою authentication pre-share key і визначається алгоритм Діффі-Хеллмана group 2. Після команди exit можна приступати до наступного рівня (рисунок 3.9).

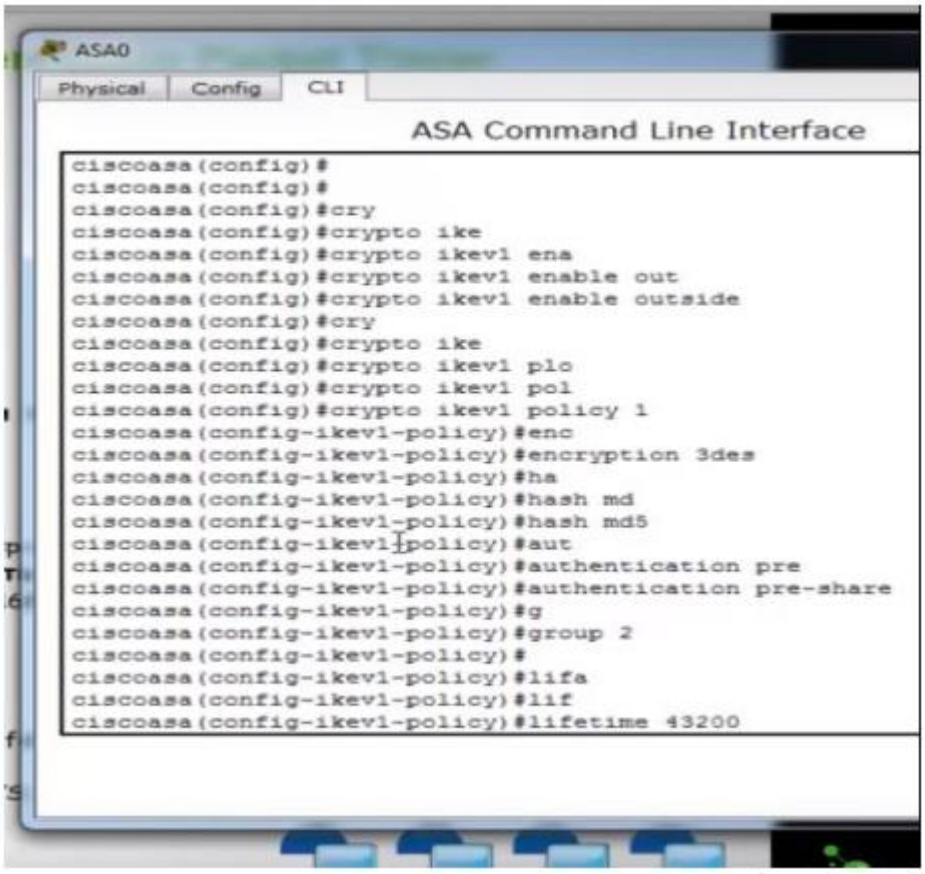

Рисунок 3.9 – Налаштування першої фази

Налаштування ключа аутентифікації здійснюється за допомогою tunnel-group (на ньому пишуться параметри для аутентифікації на першій фазі IPsec) з вказуванням IP-адреси Cisco ASA 2 210.210.2.2, в якості типу аутентифікації використовується type ipsec-l2l. Задаються атрибути IPSec tunnelgroup 210.210.2.2 ipsec-attributes, а саме ikev1 pre-shared-key cisco (рисунок 3.10).

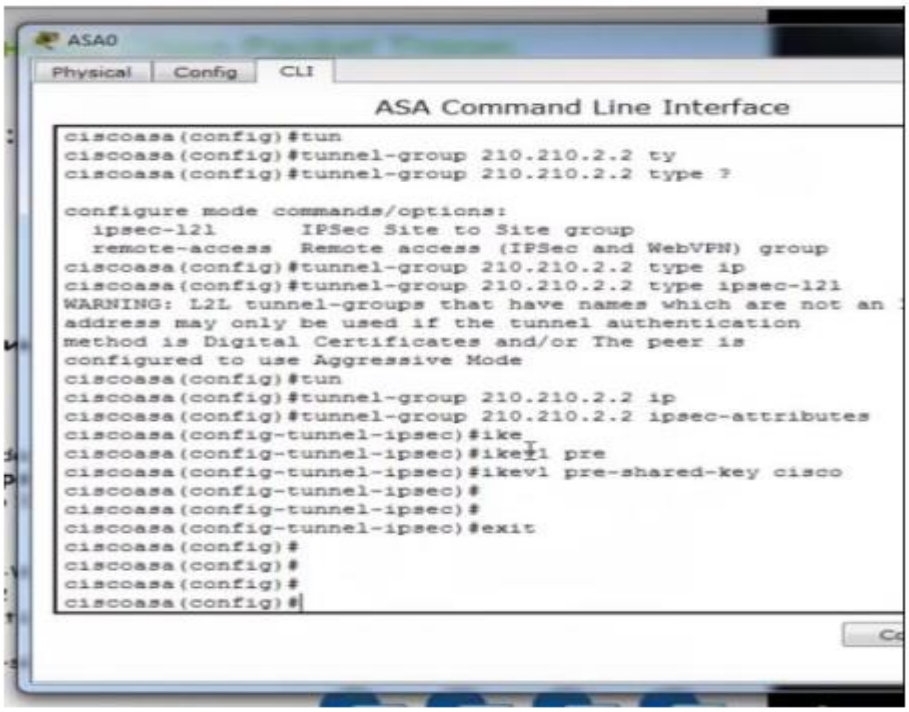

Рисунок 3.10 – Налаштування ключа аутентифікації

У другій фазі задаються параметр crypto ipsec ikev1 transform-set TS (набір перетворень, необхідний для захисту даних) esp-3des (метод шифрування) esp-md5-hmac (алгоритм хешування) (рисунок 3.11).

Далі потрібно визначити, який трафік хочемо пропускати через VPN-тунель. Для цього створюється Access List командою access-list FOR-VPN extended permit icmp 192.168.1.0 255.255.255.0 (source – джерело) 192.168.2.0 255.255.255.0 (destination – місце призначення).

Створення криптокарти (рисунок 3.12) поєднує раніше задані конфігурації ISAKMP та IPSec. Потрібно записати crypto map, задати ім’я To-Site2, дати номер 1 і вказати, що потрібно використати трафік Access List FOR-VPN. Далі

вказується peer 210.210.2.2 – IP-адреса Cisco ASA 2 (філіалу). Потім вказується в секундах lifetime тунеля, за замовчуванням 86400 (час життя ключа).

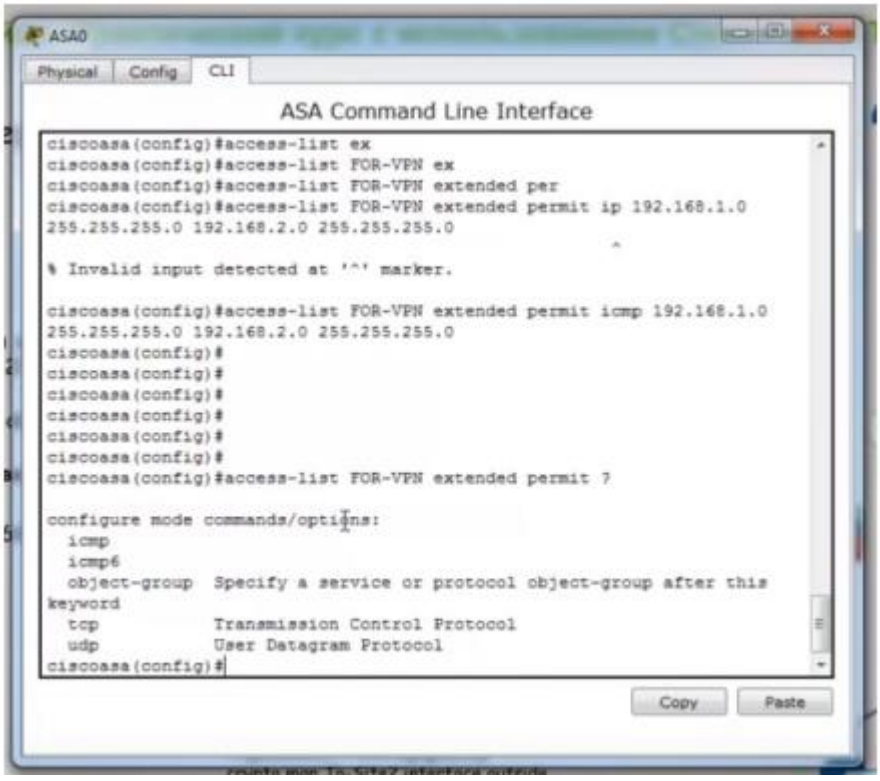

Рисунок 3.11 – Визначення трафіка, необхідного для шифрування

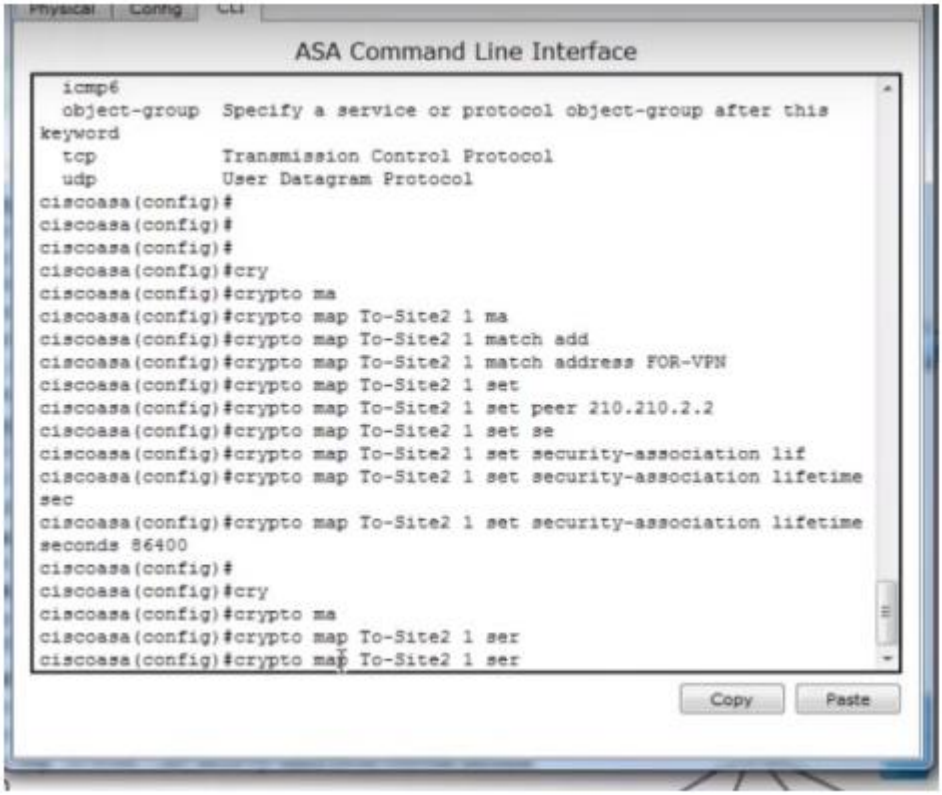

Рисунок 3.12 – Створення криптокарти

Прив’язка криптокарти до outside інтерфейсу здійснюється з допомогою команди crypto map To-Site2 interface outside. Після виконання всіх маніпуляцій виконується перевірка командою ping (рисунок 3.13). Наприклад, IP-адреса комп’ютера 192.168.2.5 знаходиться за другим Cisco ASA.

З рисунка 3.13 видно, що перевірка пройшла успішно і організація зв’язку Site-to-site VPN між двома Cisco ASA позитивна.

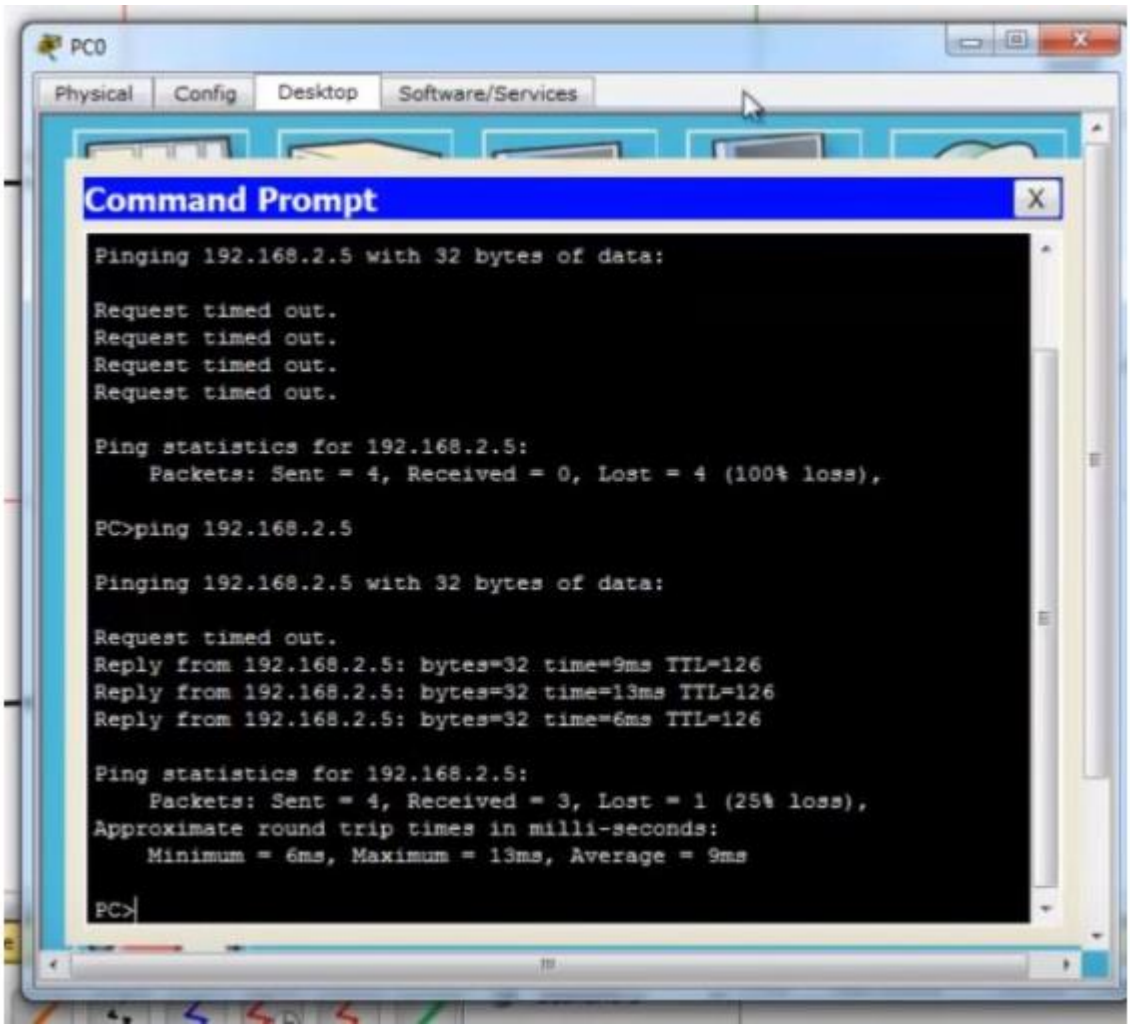

Рисунок 3.13 - Перевірка мережі за допомогою команди ping

Отже, в рамках забезпечення безпеки з точки зору несанкціонованого доступу рекомендується використання протоколу RADIUS, а з точки зору забезпечення конфіденційності та цілісності інформації, яка передається в каналах мережі IP-телефонії, технології IPSec.

3.4 Моделювання передачі даних IP-телефонії

Припустимо, що необхідно зімітувати мережу деякої компанії, штаб-квартира якої з'єднана з офісами філій IP-телефонією. Пропонується використовувати 100 телефонних ліній для зв'язку штаб-квартири компанії з її офісами в філіях. Щоб забезпечити 100 одночасних телефонних розмов з кодеком G.711, необхідний канал шириною 8560 Кбіт / с (85,6 Кбіт / с 100 = 8560 Кбіт / с). Структурна схема моделі представлена на рисунку 3.14.

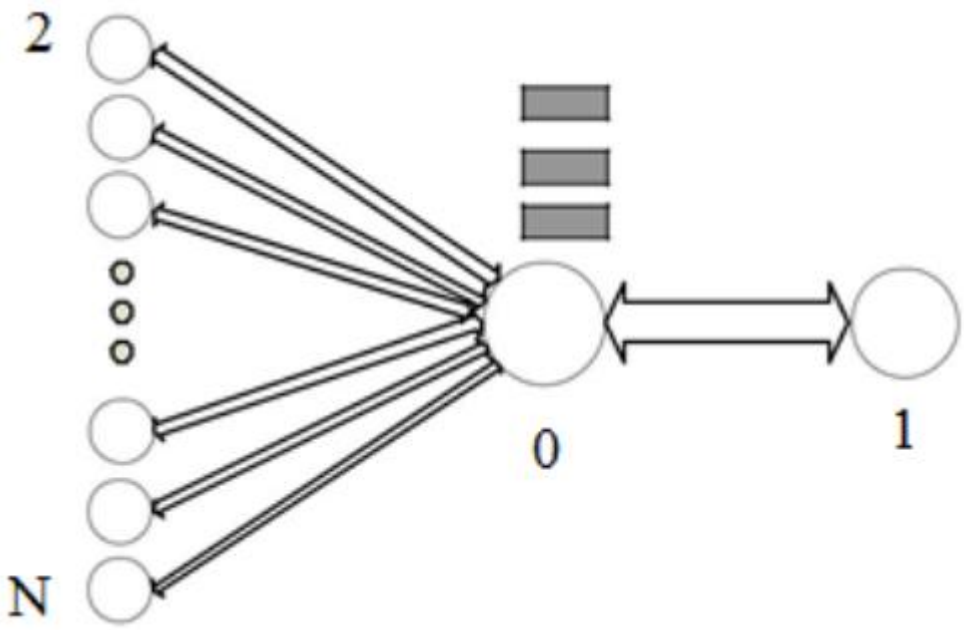

Рисунок 3.14 – Схема моделювання в NS2

Модель призначена для імітування VoIP-мережі, в якій відбувається передача мовних даних (телефонних розмов) в реальному часі. Вузли представляють собою джерела сегментованого мовного потоку. Дані для параметризації джерел (тривалості періодів мови і пауз) отримані за допомогою алгоритму сегментації на основі вейвлет-перетворень.

Моделювання дозволило отримати дані для кожного джерела за кількістю переданої інформації (в байтах і в пакетах), кількістю отриманої адресатом інформації (в пакетах), кількістю втрачених пакетів, відсотком втрат пакетів,

затримки при передачі, джитером і середньоквадратичному відхиленні (СКВ) джитера (рисунок 3.15).

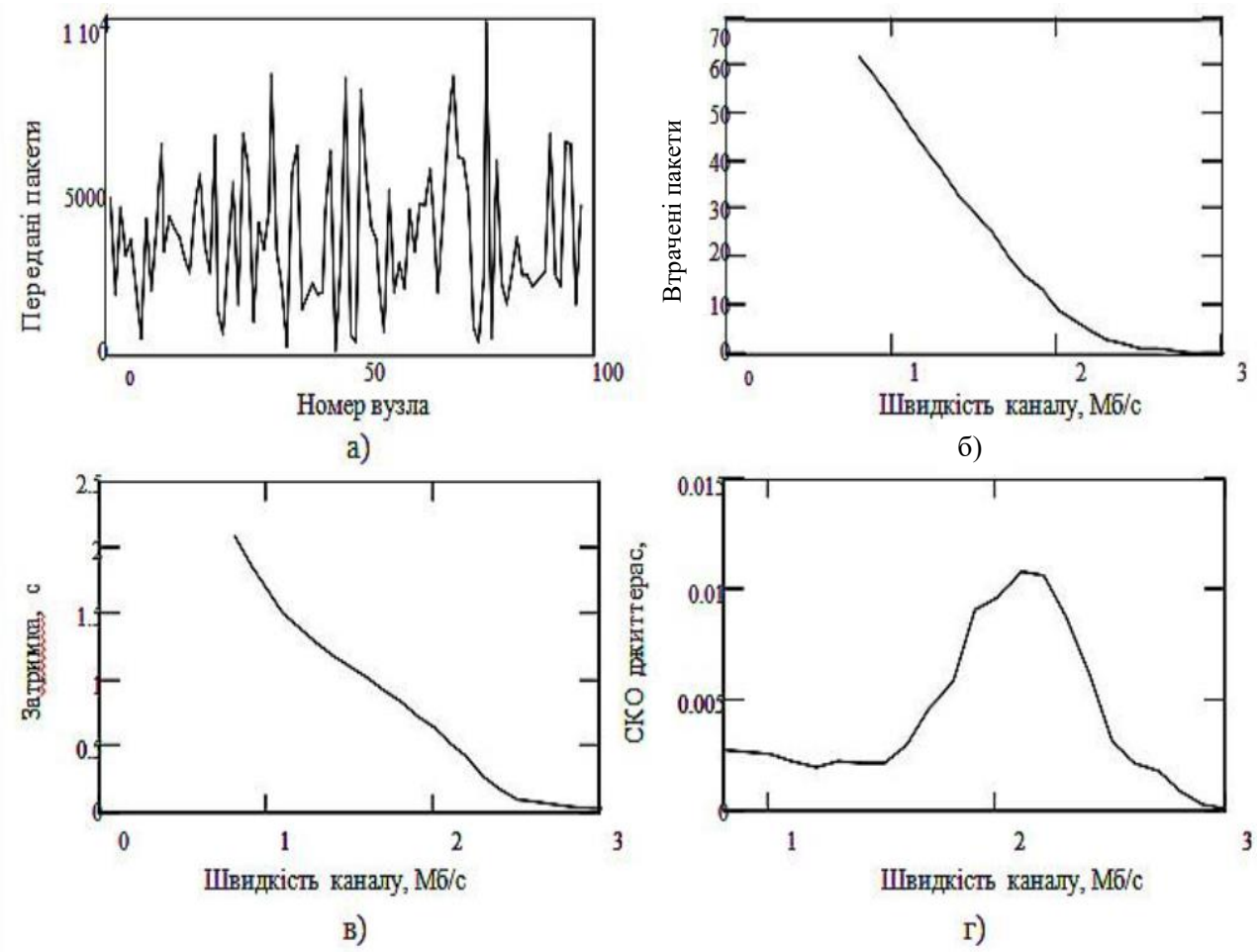

Рисунок 3.15 – Показники якості роботи VoIP-мережі: а - число переданих пакетів для вузлів, які брали участь в моделюванні; б - залежність відсотка втрачених пакетів від пропускної здатності головного каналу; в - залежність середньої затримки на пакет від пропускної здатності головного каналу; г - залежність СКВ джиттера від пропускної здатності головного каналу.

У даній моделі число джерел дорівнює 100. Вузол 0 є передавачем цих розмов адресату - вузлу 1. До вузла 0 від джерел - вузлів 2 ... N ведуть вхідні канали передачі з пропускною здатністю, яка дорівнює 1 Мб, і з затримкою передачі даних 10 мс. Параметри вузлів 2 ... N: 1) розмір пакетів, що генеруються 214 біт (кодек G.711); 2) інтервал для трафіку 0,1 с; 3) швидкість потоку 85600 біт / с (85,6 Кбіт / с); 4) величини періодів мови і періодів пауз задаються згідно

з результатами сегментації. Для визначення якості функціонування системи в різних умовах в процесі моделювання оцінювалися такі параметри головного каналу (канал, що з'єднує вузли 0 і 1):

1) смуга пропускання (змінюється в межах від 1 до 3 Мб);

2) розмір буфера вузла 0 (1000 пакетів);

3) величина затримки передачі даних в каналі (10 мс).

Згідно з інформацією, представленою на рисунку 3.10, відсоток втрат і середня затримка пакетів з ростом пропускної здатності головного каналу різко знижуються і в кінцевому рахунку приймають постійні значення. СКВ джиттера, навпаки, з ростом пропускної здатності головного каналу володіє деяким глобальним максимумом. Допустимими (граничними) значеннями показників якості є: затримка - 0,4с; втрати- 5%; СКВ джитера - 0,01 с. Смуга пропускання шириною 2,2 Мб характеризується наступними величинами: втрати - 4,44%, СКВ джитера - 0,01 с, затримка передачі - 0,425с і має відповідну пропускну спроможність каналу для заданих граничних умов якості.

Для більш детального дослідження показників якості на рисунку 3.16 наводиться відсоток втрачених пакетів і середня затримка на пакет для окремих джерел (вузол 20).

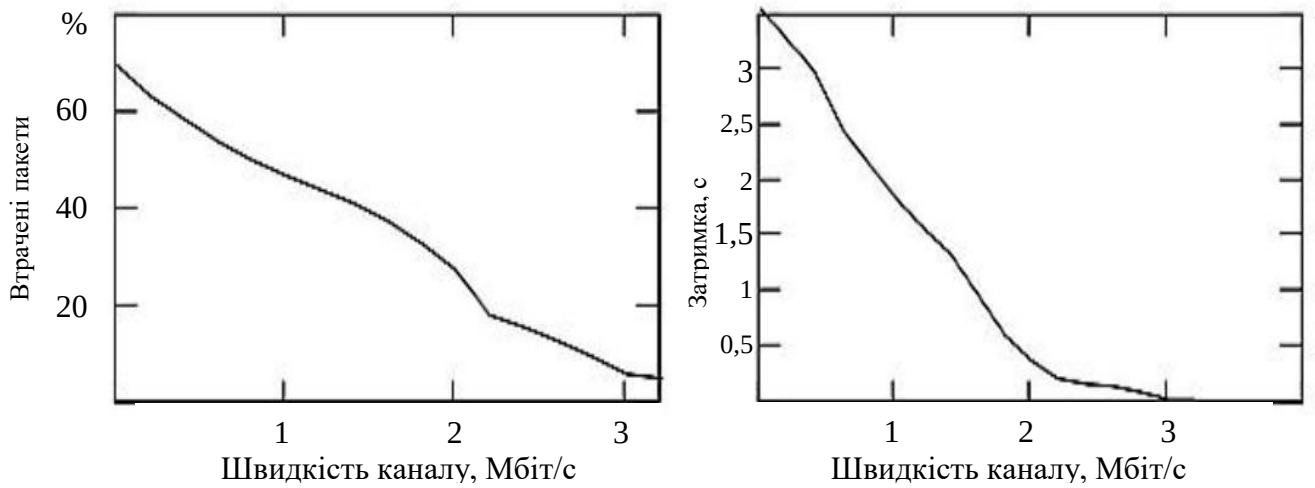

Рисунок 3.16 – Відсотки втрачених пакетів і середні затримки одного пакету для вузла 20

Очевидно, що ці залежності схожі з тими, які отримані для усереднених випадків на рисунку 2.10. На рисунку 3.16 наводяться графіки відсотка втрачених пакетів для всіх вузлів, які брали участь у моделюванні для різних швидкостей головного каналу. Очевидно, що з ростом пропускної здатності мінливість представленої характеристики знижується.

3.5 Якість обслуговування в IP-мережах

IP-телефонія - це одна із областей для передачі даних, у якій важливий порядок поступлення пакетів та важлива динаміка при передачі сигналу, що забезпечується відповідними методами кодування та передачі інформації. Транспортні протоколи у стеку TCP / IP, які функціонують зверху протоколу IP, не забезпечать високу якість обслуговування трафіку, що чутливий до затримки. Протокол TCP, хоча й гарантує доставку інформації, але це буде із непередбачуваними затримками. Протокол UDP, що використовують для перенесення інформації у реальному часі, забезпечить меншу, порівняно із протоколом TCP, тривалість затримки, але не містить жодних механізмів, щоб забезпечити якість обслуговування.

Необхідно разом із тим забезпечити механізми, згідно яких у періодах перевантаження пакети із інформацією, що чутлива до затримок (зокрема, мова), не будуть чекати у чергах чи будуть отримуватиь вищий пріоритет, як пакети із інформацією, що не чутлива до затримки. Для такої мети у мережі мають бути реалізовані механізми, які гарантують відповідну якість при обслуговуванні QoS (Quality of Service).

Показниками якості є такі:

- зміна затримки у мережі;
- пропускна здатність мережі.

Оцінюється час відгуку так:

- проміжок часу від момента передачі пакета до момента його прийому;

- час затримки односпрямованого наскрізного з'єднання, так званий часом запізнювання (latency);

- пропускна здатність.

Готовність та надійність оцінюється так:

- можливість отримати доступ до ресурсів мережі чи коефіцієнта використання;

- результати контролювання рівня обслуговування під час режиму роботи 24 години в добу 7 днів у тиждень.

Заходи для забезпечення QoS, які застосовуються у IP-мережах:

- резервування ресурсів (для часу з'єднання запитуються та резервуються ресурси, що необхідні для виконання програми);

- пріоритизація трафіка (поділ трафіка у мережі на класи із пріоритетним порядком при обслуговуванні деяких із них);

- перемаршрутизація (під час перевантаження у мережі дозволяє перевести трафік на резервний маршрут).

У сучасних IP-мережах перераховані заходи реалізуються з допомогою технологій DiffServ, IntServ та MPLS із використанням протокола RSVP.

Продуктивність мережі (чи швидкість при передачі даних) користувача визначають як ефективну швидкість при передачі, що вимірюється у бітах за секунду. Значення даного параметру не збігається із максимальною пропускною здатністю в мережі. Мінімальне значення для продуктивності гарантується зазвичай провайдером послуг, а він, у свою чергу, має мати від мережевого провайдера відповідні гарантії.

Зазвичай користувачі очікують від систем зв'язку високого рівня надійності. Надійність мережі визначена може бути через ряд параметрів, із яких найчастіше використовується коефіцієнт готовності, що вираховується відношенням часу під час простою об'єкта до сумарного часу спостереження, який включає час простою та час між відмовами. У ідеальному випадку коефіцієнт готовності має бути рівний 1. Це означає стовідсоткову готовність у

мережі. Рекомендація MCE-TY.1540 визначає такі параметри, які характеризують доставку IP-пакетів:

1) затримка доставки пакета IP (IP packet transfer delay, IPTD). Параметр IPTD визначається часом (t_2 - t_1) між двома подіями - введенням пакета до вхідної точки мережі у момент t_1 та виведенням пакету із вихідної точки мережі у момент t_2, причому ($t_2 > t_1$) та (t_2 - t_1) = T_{max}. Взагалі параметр IPTD визначається часом доставки пакета від джерелом до одержувача для усіх пакетів - і успішно переданих, і уражених помилками. Середня затримка при доставці пакета IP – це параметр, який специфікований у Y.1540 і визначається середнім арифметичним усіх затримок пакетів у обраному наборі переданих та прийнятих пакетів. Значення для середньої затримки залежатиме від переданого у мережу трафіку та доступних ресурсів мережі, наприклад, пропускна здатність. Зростання навантаження та зменшення мережевих ресурсів приводять до зростання черг в вузлах мережі та збільшення середніх затримок при доставці пакетів. Мовна та відеоінформація є прикладами трафіку, що чутливий до затримок, а додатки даних у основному менше чутливі до таких затримок. Коли затримка при доставці пакету перевищуватиме певні значення T_{max}, то такі пакети будуть відкидатися. В застосунках реального часу (зокрема, у IP-телефонії) це приводить до погіршення якості мови. Обмеження, що пов'язані із середньою затримкою IP-пакетів, відіграють ключову роль при успішному впровадженні IP-технології, відео-конференцій і інших додатків у реальному часі. Такий параметр багато у чому визначатиме готовність користувачів для прийняття подібних додатків;

2) варіація при затримці IP-пакета (IP-packet delay variation, IPDV). Параметр V_k характеризує варіацію при затримці IPDV. Для IP-пакета із індексом k параметр цей визначається між вхідною та вихідною точками мережі в вигляді різниці між абсолютною величиною самої затримки X_k при доставці пакета із індексом k, та певною еталонною (чи опорною) величиною затримки при доставці IP-пакета $d_{1,2}$ для тих самих мережевих точок: $V_k = X_k - d_{1,2}$. Еталонна затримка при доставці IP-пакета $d_{1,2}$ між джерелом та

одержувачем визначається абсолютним значенням затримки доставки першого IP-пакету між даними точками мережі. Варіація затримки IP-пакету, чи джитер, проявляється у тому, що послідовні пакети до одержувача прибувають у нерегулярні моменти часу. В системах IP-телефонії це веде, наприклад, до спотворень звуку і у результаті до того, що стає мова нерозбірливою;

3) коефіцієнт втрати IP-пакетів (IP packet loss ratio, IPLR). Коефіцієнт IPLR визначається відношенням числа втрачених IP-пакетів до загальної кількості прийнятих у обраному наборі переданих та прийнятих пакетів. Втрати пакетів у IP-мережах виникають у тому випадку, коли при передачі значення затримок перевищує нормоване значення, що визначене як T_{max}. Коли пакети губляться, тоді при передачі даних можлива повторна їх передача за запитом приймаючої сторони. В системах IP пакети, які прийшли до одержувача із затримкою, що перевищує T_{max}, відкидаються. Це веде до провалів у прийнятті мови. Серед причин, які викликають втрати IP-пакетів, необхідно відзначити зростання черг в вузлах IP-мережі, які при перевантаженнях виникають;

4) коефіцієнт помилок IP-пакетів (IP packet error ratio, IPER). Коеффіцієнт IPER визначається сумарною кількістю пакетів, які прийняті із помилками, до суми успішно прийнятих та пакетів, прийнятих із помилками.

Рекомендація Y.1540 визначає значення параметрів, що наведені у таблиці 3.1.

Таблиця 3.1 – Норми характеристик мереж IP-телефонії

Хар-ки	Класи QoS					
	0, мс	1, мс	2, мс	3, мс	4, с	5, с
IPTD	100	400	100	400	1	Не норм.
IPDV	50	50	Не норм.	Не норм.	Не норм.	Не норм.
IPLR	10^{-3}	10^{-3}	10^{-3}	10^{-3}	10^{-3}	Не норм.
IPER	10^{-4}	10^{-4}	10^{-4}	10^{-4}	10^{-4}	Не норм.

Рекомендацією Y.1541 встановлено відповідність між класами QoS та додатками:

- клас 0 – це додатки реального часу, які чутливі до джиттера, що характеризуються високим рівнем інтерактивності (відеоконференції, VoIP);

- клас 1 – це додатки для реального часу, які чутливі до джиттера, інтерактивні (відеоконференції, VoIP);

- клас 2 – це транзакції даних, які характеризуються високим рівнем інтерактивності (сигналізація);

- клас 3 – це транзакції даних, вони інтерактивні;

- клас 4 - додатки, які низький рівень втрат допускають (масиви даних, потокове відео, короткі транзакції);

- клас 5 - традиційні застосування IP-мереж.

Більша частина IP-трафіку складається з потоків інформації, що чутлива до затримок. Найбільша затримка не має перевищувати 250 мс, сюди входить і час на обробку інформації на кінцевій станції. Варіація затримки (джитер) необхідно також до мінімуму звести. Необхідно враховувати також, що інформація при стисненні стає чутливішою до помилок, що виникають при передачі. Їх не можна шляхом перезапиту виправляти через необхідність передачі саме у реальному часі.

Загальна затримка для мовної інформації ділиться на основні дві частини - затримка при кодуванні та декодуванні мови у шлюзах чи термінальному обладнанні користувачів та затримка, що самою мережею вноситься. Зменшити цю загальну затримку двома шляхами можна: по-перше, інфраструктуру мережі спроектувати таким чином, щоби затримка у ній була мінімальна, і, по-друге, час обробки мовної інформації зменшити шлюзом.

Для зменшення затримки у мережі скорочувати потрібно кількість транзитних маршрутизаторів та з'єднувати між собою їх високошвидкісними каналами. Для згладжування варіації затримки використовувати ефективно можна такі методи, як, наприклад, механізм для резервування мережевих ресурсів. Одним з способів уникнути того, щоби мова та інша інформація, яка

вимагає передачі у режимі реального часу, не простоювала б в чергах нарівні з статичною інформацією (звичайні, неголосові дані), є виділення та сортування пакетів, які містять голосову інформацію.

Трафік, який поступив в мережу, класифікується та нормалізується прикордонними маршрутизаторами. Це дозволяє організувати для різнотипного трафіку гнучке обслуговування, враховуючи максимально потреби кожної програми.

ВИСНОВКИ

1. На основі аналітичного огляду різних підходів до побудови мереж IP-телефонії встановлено основні вимоги, які пред'являються до архітектури мереж IP-телефонії та рівня її захищеності.

2. На основі порівняння найбільш поширених підходів до побудови мережі IP-телефонії розроблено алгоритми захищених режимів роботи IP-телефонії, що дозволило збільшити рівень захисту мереж IP-телефонії.

3. На основі вимог до захищених режимів роботи IP-телефонії розроблено алгоритмічне забезпечення, структурну та функціональну схеми програми, що дозволило визначити компоненти програмної системи, які необхідно спроектувати.

4. На основі аналітичного огляду обґрунтовано вибір та розробку середовища програмування, що дозволило розробити компоненти програми та здійснити їх інтеграцію у єдиний програмний продукт.

5. На основі дослідження роботи програми, імітаційного моделювання та опрацювання отриманих результатів встановлено, що розроблена програмна система відповідає поставленим вимогам і дозволяє використовувати IP-телефонію для захищеної передачі даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бакланов И.Г. ISDN и IP-телефония / Вестник связи, 1999, №4.
2. DeMartino K. ISDN and the Internet. - Computer Networks, 1999.
3. Faynberg I., Gabuzda L, Lu Hui-Lan. Converged Networks and Services: Internetworking IP and the PSTN. - John Wiley & Sons, 2000.
4. Goncalves M. Voice Over IP Networks. - McGraw Hill Publishing, 1998.
5. Goralski W., Kolon M. IP Telephony. - McGraw Hill Publishing, 1999.
6. Harte . Voice Over Data Network Internet, Frame Relay, and ATM.- APDG Inc. 2000
7. Котов П. А. Повышение достоверности передачи цифровой информации. М.: Радио и связь, 2006. С.183.
8. Голубицкая Е.А., Жигульская Г.М. Экономика связи. М.: Радио и связь, 2003. 318 с.
9. Воинов Б.С., Бугров В.Н., Воинов Б.Б. Информационные технологии и системы: поиск оптимальных, оригинальных и рациональных решений. М:. Наука, 2007. 730 с.
10. Деднев М.А., Дыльнов Д.В. Защита информации в банковском деле и электронном бизнесе. М.: КУДИЦ ОБРАЗ, 2004. 321 с.
11. Казарин О.В. Безопасность программного обеспечения компьютерных систем. М.: Высшая школа, 2013. 243 с.
12. Барсуков В.С. Современные технологии безопасности: Интегральный подход / В.С. Барсуков. – М.: Нолидж, 2010. – 496 с.
13. Омельянчук А.М. Формирование системы комплексной безопасности. Подготовка техзадания и проектирование. *Системы безопасности*. 2009. №5. С. 114-117.
14. Ковцур М.М., Никитин В.Н., Юркин Д.В. Протоколы обеспечения безопасности VoIPтелефонии. Защита информации. Инсайд, 2012, №3, с.74–81.

15. Нопин С. В., Шахов В. Г. Анализ защищенности абонентских систем IP-телефонии от несанкционированного доступа // Информационные технологии. 2008. № 11. С. 67-74.

16. Стив Мак-Квери, Келли Мак-Грю, Стивен Фой. Передача голосовых данных по сетям Cisco Frame Relay, ATM и IP; Киев, 2007.

17. Houghton T. F, E. C. Schloemer, E. S. Szurkowski, W. P. Weber. A packet telephony gateway for public network operators. - Bell Laboratories, Lucent Technologies - U.S.A., XVI World Telecom Congress Proceeding,

18. Мафтик С. Механизмы защиты в компьютерных сетях. М.: Мир, 2013. 219 с.

19. Curtin P., Whyte B. Tigris - A gateway between circuit-switched and IP networks / Ericson Rewiew, 1999, №2.

20. Ломакин Д. Технические решения IP-телефонии / Мобильные системы, 1999 №8.

21. Hersent 0, Gurle D., Petit Jean-Pierre. IP Telephony: Packet-Based Multimedia Communications Systems.- Addison-Wesley Pub Co, 2000.

22. Волокітін А.В. Інформаційна безпека державних організацій і комерційних фірм / Волокітін А.В., Маношкин А.П., Солдатенков А.В., Савченко С.А., Петров Ю.А. - К.: Юніор, 2012. – 303 с.

23. Иксар В. Современные способы перехвата информации / В. Иксар // Специальная техника. – 2008. - №2. – С. 104-111.

24. Зайцев А.П. Справочник по техническим средствам защиты информации и контроля технических каналов утечки информации / А.П. Зайцев, А.А. Шелупанов. – Томск: Изд. Томского гос. ун-та систем управления и радиоэлектроники, 2014. - 197с.

25. Петров В.П., Петров С.В. Информационная безопасность человека и общества. М.: ЭНАС, 2007. 334 с.

26. Аносов А.М. Персональная спутниковая связь / А.М. Аносов, В.В. Герасимов, А.В. Колосов // Технологии электронных коммуникаций. – 2006. - Т. 64. - №3. – С. 37-47.

27. Аблазов В.И. Преобразование, запись и воспроизведение речевых сигналов / В.И. Аблазов. – К.: Либідь, 2011. – 208 с.

28. Хорев А.А. Технические каналы утечки акустической (речевой) информации / А.А. Хорев // Специальная техника. – 2008. - №1. – С.173-180.

29. Конеев И.Р. Информационная безопасность предприятия / Конеев И.Р. – СПб.: БХВ-Петербург, 2003. – 752 с.

30. Меньшаков Ю.К. Защита объектов и информации от технических средств разведки / Меньшаков Ю.К. - М.: Российск. гос. гуманит. ун-т, 2012. -281 с.

31. Березький О.М. Методичні рекомендації до виконання магістерської роботи з освітнього ступеня “Магістр”. Спеціальність: 123 - Комп’ютерна інженерія. Магістерська програма - Комп’ютерна інженерія" / О.М. Березький, Л.О. Дубчак, Г.М. Мельник /Під ред. О.М. Березького. Тернопіль: ТНЕУ, 2018. 41 с.

32. Методичні вказівки до оформлення курсових проектів, звітів про проходження практики, випускних кваліфікаційних робіт для студентів спеціальності «Комп’ютерна інженерія» / І.В. Гураль, Л.О. Дубчак / Під ред. О.М. Березького. Тернопіль: ТНЕУ, 2019. 33 с.

33. Дзівак О.А. Модель забезпечення безпеки в IP-телефонії на прикладі Site-to-Site VPN. *Інтелектуальні комп’ютерні системи та мережі*: Матеріали IV науково-практичної конференції молодих вчених і студентів. 2 червня 2021 р. Тернопіль. С. 6.

34. Дзівак О.А. Порівняльний аналіз протоколів для побудови мереж IP-телефонії. *Інтелектуальні комп’ютерні системи та мережі*: Матеріали V науково-практичної конференції молодих вчених і студентів. 2 грудня 2021 р. Тернопіль. С. 22.

35. Голдсмит А. Беспроводные коммуникации. М.: Техносфера, 2011. 329 с.

36. Швиденко М.З. Сучасні комп’ютерні технології / М.З.Швиденко. – Л.: ННЦ Інститут аграрної економіки, 2007. – 705 с.

37. Котов П. А. Повышение достоверности передачи цифровой информации. М.: Радио и связь, 2006. С.183.

38. Костров Б.В. Основы цифровой передачи кодированной информации. М.:Тех-Бух, 2007. 193 с.

39. Кульгин М. Технологии корпоративных сетей. Изд. «Питер», 1999.

40. Reid M. Multimedia conferencing over ISDN and IP networks using ITU-T H-series recommendations: architecture, control and coordination / Computer Networks, 1999 - №31

41. Вендров А.М. CASE-технологии. Современные методы и средства проектирования информационных технологий / А.М.Вендров. – СПб.: Питер, 2012. – 324 с.

42. Гайдамакин Н. А. Автоматизированные информационные системы, базы и банки данных. М.: Гелиос АРВ, 2012. 368 с.

43. Гольдштейн Б.С., Ехриель И.М., Рерле Р.Д. Интеллектуальные сети. М.: Радио и связь, 2000.

44. Кааранен Х. Сети UMTS. Архитектура, мобильность, сервисы / Х. Кааранен, А. Ахтиайнен. – СПб.: Питер, 2007. - 281 с.

45. Хорев А.А. Методы защиты речевой информации и оценка их эффективности / А.А. Хорев, Ю.К. Макаров // Защита информации. – 2001. - №4. – С. 22-33.

46. Джонатан Дэвидсон, Джеймс Питерс, Манож Бхатия, Сатиш Калидинди, Судипто М. Основы передачи голосовых данных по сетям IP (IP Voice over IP Fundamentals); Вильямс, 2007.

47. Minoli D., Minoli E. Delivering Voice over IP Networks / John Willey & Sons, Inc., 1998.

48. Armitage Grenville. Quality of Service in IP Networks. - Macmillan Technical Publishing, 2000.

49. Uyless Black. Voice over IP, Prentice Hall PTR, 2000.

50. *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.

51. Брау Д. Грядет год стандарта H.323? / Сети и системы связи, 1999. №14.

52. Яновский Г. Г. Качество обслуживания в сетях IP // Вестник связи, – Алматы, 2008. – № 1. – С1-15.