**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ**
**КАФЕДРА КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ**

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
_____ С.В. Казмірчук

«_____»_____2020 р.

На правах рукопису
УДК

# КВАЛІФІКАЦІЙНА РОБОТА

## ЗДОБУВАЧА ВИЩОЇ ОСВІТИ ОСВІТНЬОГО СТУПЕНЯ «МАГІСТР»

**Тема**: Система забезпечення інформаційної безпеки IP-телефонії з використанням ймовірнісно-часових характеристристик протоколу розподілу ключів

**Виконавець:** С.М. Горький

**Науковий керівник:** к.т.н., доц. С.В. Єгоров

**Нормоконтролер:** к.т.н., доц. С.В. Єгоров

**Київ 2020**

# ВСТУП

**Актуальність.** Сучасному періоду розвитку телекомунікацій відповідають зростаючі обсяги трафіку в корпоративних мережах, зокрема, в мережах Інтернет провайдерів.

IP-телефонією називають технологію передачі мови по мережах з пакетною комутацією на базі протоколу IP [1]. Як правило, під цим визначенням також мають на увазі набір протоколів, методів і технологій, що забезпечують голосове спілкування через мережу з комутацією пакетів. Причинами поширення IP-телефонії послужили низька вартість в порівнянні з аналоговою телефонією, викликана застосуванням недорогих мереж з комутацією пакетів, а також універсальність і мобільність, що дозволяє перетворити мова в потік даних в будь-якій точці мережевої інфраструктури.

Розвиток нових протоколів, а також передача голосових пакетів у відкритому вигляді через публічні мережі привели до появи і стандартизації протоколів забезпечення безпеки IP-телефонії. Протоколи були розділені на три групи в залежності від розв'язуваних завдань: забезпечення безпеки сигналізації, захист медіа трафіку і розподіл ключів для медіа трафіку.

Стандартизація протоколів, а також поширене використання персональних комп'ютерів в якості терміналів користувача для послуг IP-телефонії привели до розробки великого числа програм для IP-телефонії, в тому числі програмного забезпечення (ПО) з відкритим вихідним кодом, що дозволяє розширювати можливості і використовувати додаткові алгоритми в програмах.

**Метою дипломної роботи** є підвищення рівня захищеності інформації в сеансах безпечної IP-телефонії та скорочення часу встановлення захищеного з'єднання. Для досягнення поставленої мети вирішені наступні завдання:

- дослідження існуючих протоколів безпеки IP-телефонії, їх параметрів, характеристик і особливостей, а також впливу протоколів на показники якості;

- розробка моделі порушника для оцінки захищеності системи IP-телефонії;
- розробка методу оцінки ймовірнісно-часових характеристик протоколів розподілу ключів захищеної IP-телефонії та розробка пропозицій щодо модифікації протоколу розподілу ключів для поліпшення ймовірносно-часових характеристик протоколу; розробка методу виявлення порушника протоколів розподілу ключів, заснованих на алгоритмі Діффі-Хелмана;

**Об'єкт дослідження:** процес оцінки ефективності протоколів розподілу ключів під час захищеного з'єднання в IP-телефонії.

**Предмет дослідження:** методи і протоколи забезпечення інформаційної безпеки IP-телефонії, а також ймовірносно-часові характеристики цих протоколів.

**Галузь застосування:** Модель порушника може бути використана при розробці методик контролю захищених мереж зв'язку, а також в навчальному процесі з дисципліни "Безпека IP-телефонії".

**Практична цінність:** Метод може бути використаним для оцінки ефективності протоколів розподілу ключів, а саме щодо часу виконання і ймовірності успішного завершення.

Метод оцінки ймовірнісно-часових характеристик може застосовуватися в розрахунках при проектуванні рішень із захищеної IP- телефонії, що використовують в своєму складі протоколи розподілу ключів.

**Наукова новизна:** За рахунок поліпшення ймовірносно-часових характеристик протоколу розподілу ключів було запропоновано систему IP-телефонії з підвищеним рівнем захищеності інформації в сеансах безпечної IP-телефонії та скороченим часом встановлення захищеного з'єднання.

**Методи дослідження** базуються на основі математичного апарату ймовірнісних графів ( для розробки математичної моделі порушника та оцінки ймовірності успішного завершення атаки) та криптографічних даних ( для розробки пропозицій щодо покращення ЙЧХ протоколу).

# Розділ 1. СУЧАСНИЙ СТАН ЗАХИЩЕНОЇ IP-ТЕЛЕФОНІЇ

## 1.1. Принципи передачі голосової інформації в мережах з пакетною комутацією

### 1.1.1. Класифікація протоколів IP-телефонії

Протоколи IP-телефонії поділяються на дві великі групи, а саме протоколи передачі медіа інформації по пакетним мережам, а також протоколи управління встановленням з'єднання.

В першу групу входить протокол RTP (Real-time Transport Protocol) [3], що працює поверх протоколу UDP (User Datagram Protocol). Сукупність протоколів RTP / UDP / IP забезпечує транспортний механізм для мовного трафіку.

Протоколи другої групи забезпечують управління при обслуговуванні виклику між абонентами. До цієї групи належать протоколи SIP (Session Initiation Protocol) [4], H.323, MGCP (Media Gateway Control Protocol) [5]. Протоколи встановлення з'єднання можуть працювати як поверх UDP транспорту, так і по TCP (Transmission Control Protocol). Таким чином, сукупність протоколів (SIP / H.323 / MGCP) / (UDP / TCP) / IP формують сигнальний механізм для передачі мовного і медіа трафіку.

Історично першим протоколом для IP-телефонії, який отримав широке поширення, став H.323, представлений Міжнародним союзом електрозв'язку в рекомендації H.323. Документ описує кілька протоколів, які спільно забезпечують роботу мультимедійних протоколів в мережах з негарантованою якістю обслуговування. Однак, H.323 має досить складну структуру, так як протокол спочатку розроблявся для інтеграції телефонної мережі загального користування (ТМЗК) з мережами передачі даних.

Управління викликами може бути реалізовано за рахунок використання протоколу MGCP, архітектура якого складається з декількох елементів:

1) Шлюз - Media Gateway, що виконує функції перетворення мовної інформації з ТМЗК в мережу з комутацією пакетів;

2) Контролер шлюзів - Call Agent, керуючий шлюзами;

3) Шлюз сигналізації - Signaling Gateway (SG), що забезпечує передачу сигналізації, що надходить з ТМЗК, до контролера шлюзів і в зворотному напрямку.

Особливостями MGCP є зосередження всього інтелекту розподіленого шлюзу в контролері і можливість розділення функцій контролера між декількома обчислювальними платформами.

Третім протоколом, що дозволяє здійснювати управління викликами, є SIP [6]. SIP базується на протоколі HTTPS, має більш просту структуру в порівнянні з H.323 і MGCP. Завдання протоколу - зробити абонентські пристрої і шлюзи більш інтелектуальними, а також забезпечити розширюваність протоколу для підтримки додаткових послуг для користувачів. Підхід до побудови мереж IP-телефонії на базі протоколу SIP набагато простіше, ніж реалізація на H.323 і MGCP. З цієї причини - SIP протокол набув широкого поширення.

Крім наведеної вище класифікації протоколів IP-телефонії, можна додатково виділити кілька підсистем, що функціонують для надання послуг VoIP [1]: • Підсистема забезпечення якості;

• Підсистема забезпечення безпеки IP-телефонії;

• Підсистема білінгу і менеджменту IP- телефонії;

• Підсистема додаткових послуг;

• Підсистема забезпечення управлінням викликами і адресацією.

Підсистема забезпечення якості відповідає за підтримку якості телефонного зв'язку і включає в себе сукупність протоколів, алгоритмів і механізмів, що працюють для досягнення цієї мети.

Підсистема безпеки IP-телефонії відповідає за конфіденційність телефонних переговорів кореспондентів, а так же переданої інформації. Дана система включає в себе сукупність протоколів, механізмів і алгоритмів для забезпечення безпеки в мережі IP-телефонії.

Підсистема білінгу і менеджменту застосовується для обліку викликів користувачів, тарифікації дзвінків і виконання взаєморозрахунків між користувачами (абонентами) і оператором, що надає послугу.

Підсистема додаткових послуг відповідає за надання додаткових сервісів абонентам мережі IP-телефонії. До них відносяться: забезпечення роумінгу і мобільності, надання додаткових сервісів, таких як відео виклики, інформаційні сервіси і т.д. Підсистема складається з протоколів, що застосовуються для надання додаткових послуг.

Підсистема управління викликами і адресації відповідає за виконання базових послуг VoIP, а саме:

• організація викликів і маршрутизацію викликів;

• передача голосового трафіку.

### 1.1.2. Сценарії встановлення з'єднання в IP-телефонії

При описі системи IP-телефонії слід окремо виділити можливі сценарії взаємодії кореспондентів. У загальному випадку сценарієм називається сукупність елементів, взаємодіючих при обробці дзвінка. У більш широкому сенсі, сценарієм може бути названа сукупність застосовуваних при обробці дзвінка протоколів, алгоритмів, механізмів, а також процедур їх взаємодії між собою для досягнення кінцевої мети.

При складанні прикладу сценарію введено допущення, що в якості протоколу сигналізації на мережі IP-телефонії застосовується протокол SIP. При складанні схеми взаємодії враховано, що згідно із законом про зв'язок, заборонено приєднання операторів один до одного за допомогою VoIP. З'єднання різних VoIP операторів дозволяється виконувати тільки через мережу ТМЗК [7].

На рис. 1.1 представлена "Принципова схема підключення оператора VoIP". На її прикладі розглянуті можливі варіанти сценаріїв обробки викликів елементами мережі IP-телефонії: користувачами (абонентами), IP-телефонними станціями (IP АТС, SoftSwitch), прикордонними шлюзами E1.

Для прикладу - наведено два постачальника послуг IP-телефонії, а також оператор традиційної телефонії.

Оператор 1 надає VoIP сервіси абонентам, підключеним на мережі 1. Оператор 1 може використовувати кілька IP АТС, позначених SSx на малюнку, де x - порядковий номер IP АТС. Як правило, ймовірність виклику від абонента А1 іншому абоненту мережі того ж самого оператора (Б1 або В1) вкрай мала для невеликих і середніх компаній. Найбільш поширені дзвінки абонентам, підключеним до інших операторів.

Можливі такі сценарії з'єднання:

- А1-SS1-GW1-ТМЗК-GW2-SS2-В2 (VoIP абонент однієї компанії через ТМЗК дзвонить VoIP абоненту іншого оператора)
- А1-SS1-GW1-ТМЗК-Г (VoIP абонент однієї компанії через ТМЗК дзвонить абоненту мережі ТМЗК іншого оператора).
- А1-SS1-SS2-В1 (VoIP абонент одного оператора дзвонить іншому абоненту цього ж оператора, підключеному до додаткової IP АТС оператора)
- А1-SS1-Б1 (VoIP абонент одного оператора дзвонить іншому абоненту цього ж оператора, при цьому абоненти підключені до однієї IP АТС)

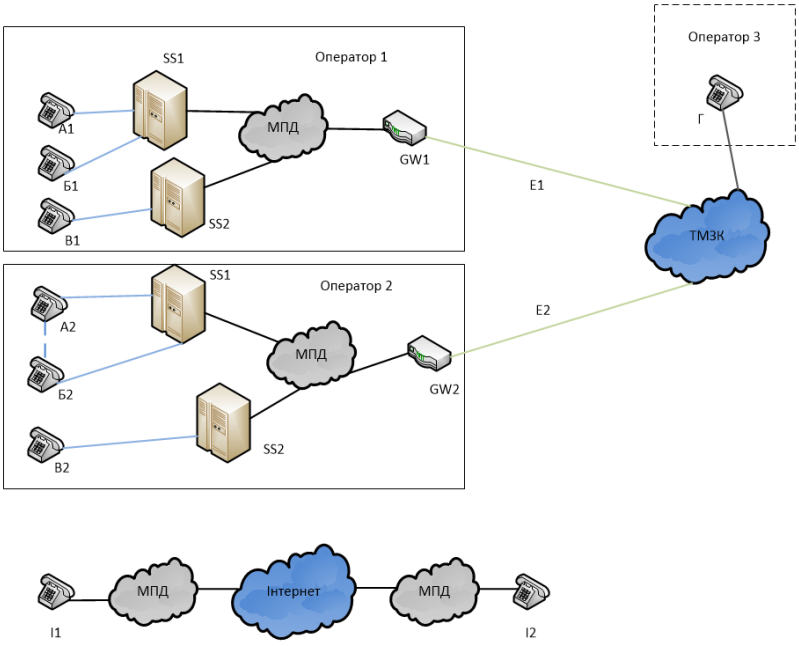


Рис. 1.1. Принципова схема підключення оператора VoIP

- А2-Б2 (VoIP абонент одного оператора дзвонить іншому абоненту,

при цьому виклик здійснюється безпосередньо між кореспондентами, минаючи IP АТС). Такий спосіб найчастіше використовується, коли необхідно організувати передачу абонентської лінії традиційної телефонії по мережах IP. Спосіб з'єднатися без АТС може застосовуватися в корпоративних мережах для організації внутрішнього службового зв'язку, а також між окремими кореспондентами глобальної мережі, що не мають підключення до однієї АТС, але мають потребу проведення сеансів телефонного зв'язку в захищеному режимі.

Описані сценарії наведені також на Рис. 1.2

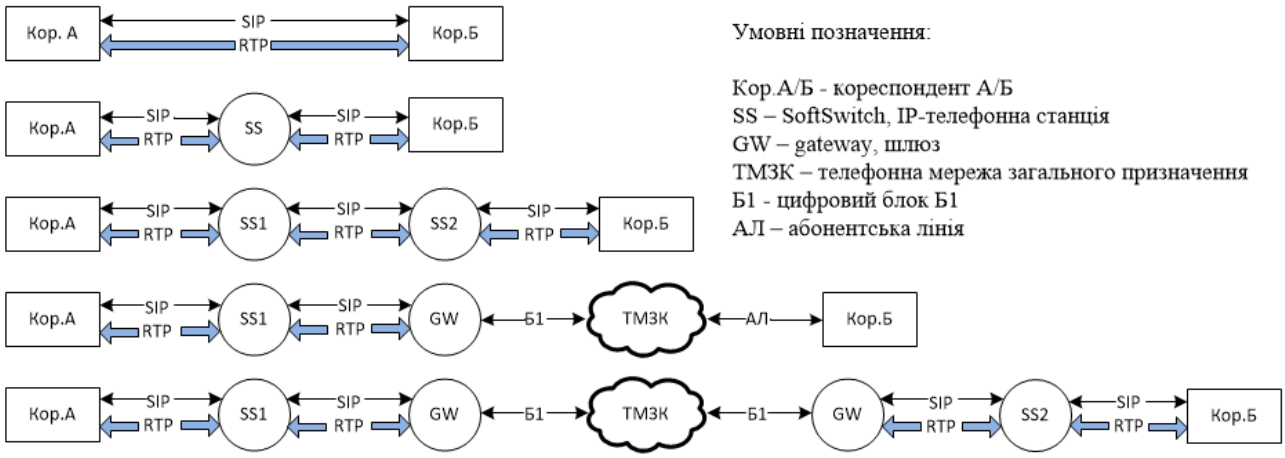


Рис. 1.2 - Можливі сценарії встановлення з'єднання кореспондента VoIP

У всіх вищенаведених сценаріях при обробці викликів повинні виконуватися норми, визначені для телефонного зв'язку. Однак, в сценаріях можуть застосовуватися різні протоколи, алгоритми забезпечення безпеки. Можливе використання різних механізмів підтримки якості обслуговування при встановленні з'єднання між абонентами різних операторів. З цих причин, підсистема забезпечення якості та підсистема забезпечення безпеки IP-телефонії вимагають більш детального вивчення.

## 1.2. Забезпечення якості в IP-телефонії

### 1.2.1. Показники якості IP-телефонії

Міжнародний союз електрозв'язку (МСЕ) визначає якість послуг, що надаються як "сумарний ефект показників якості послуги, який визначає ступінь задоволеності користувача послуги" [8].

Найбільш популярним з показників якості IP-телефонії є оцінка MOS (Mean Opinion Schore), яка визначається як середнє значення оцінок якості за п'ятибальною шкалою, отриманих великою групою слухачів-експертів [9].

Якість IP-телефонії визначається такими двома складовими -якістю мови і якістю сигналізації [1]. Якість мови включає в себе:

- діалог - можливість користувача зв'язуватися і розмовляти в реальному часі в повнодуплексному режимі з іншим користувачем;
- розбірливість - чистота і тональність мови;
- відлуння - чутність власної мови;
- рівень - гучність мови.

Якість сигналізації включає:

- затримки при встановленні виклику - швидкість успішного доступу і час встановлення з'єднання;
- завершення виклику - час відбою і швидкість роз'єднання;
- DTMF - визначення і фіксація сигналів многочастотного набору номера.

При використанні захищеної IP-телефонії додатково з'являються показники:

- час виконання з'єднання, тобто час встановлення захищеного голосового каналу між кореспондентами, які використовують протоколи розподілу ключів;
- ймовірність успішної атаки порушника на IP-телефонію, що працює в захищеному режимі;
- час і ймовірність успішного завершення протоколів забезпечення безпеки.

IP-телефонія стає масовим явищем в наш час, тому на неї так само можуть поширюватися норми, що пред'являються до традиційної телефонії.

Для контроля показників якості IP-телефонії необхідно враховувати дві сукупності норм: норми, що поширюються на пакетні канали зв'язку, а також норми, що поширюються на телефонію.

Для мережі передачі даних виділяють наступні показники:

Втрати - відношення коректно прийнятих пакетів до загальної кількості переданих пакетів.

Затримки - час, який потрібен для передачі пакета від точки відправлення до точки отримання.

Пропускна здатність - доступна для передачі між кореспондентами смуга пропускання.

Коливання затримки - різниця між затримками, що виникли при передачі різних пакетів.

Для мережі передачі даних для різних класів трафіку в рекомендації МСЕ-Т Y.1541 [10] вводяться норми на середню затримку, варіацію затримки, коефіцієнт втрачених пакетів, коефіцієнт помилок в прийнятому пакеті. Норми представлені в табл. 1.1.

*Таблиця 1.1*

Норми за рекомендацією МСЕ-Т Y.1541

| Характеристики мережі | Класи якості обслуговування (QoS) | | | | | |
|---|---|---|---|---|---|---|
| | 0 | 1 | 2 | 3 | 4 | 5 |
| Затримка доставки пакета IP, IPTD (мс) | 100 | 400 | 100 | 400 | 1000 | -- |
| Варіація затримки пакета IP, IPDV (джиттер)(мс) | 50 | 50 | -- | -- | -- | -- |
| Коефіцієнт втрати пакетів IP, IPLR | $10^{-3}$ | $10^{-3}$ | $10^{-3}$ | $10^{-3}$ | $10^{-3}$ | -- |
| Коефіцієнт помилок пакетів IP, IPER | $10^{-4}$ | $10^{-4}$ | $10^{-4}$ | $10^{-4}$ | $10^{-4}$ | -- |

В рекомендації G.114 [11] для телефонної мережі сформовані нормативи на односторонню затримку. Параметр не повинен перевищувати 400 мс при мережевому плануванні. У документі наведено деякі значення затримок, які

рекомендується використовувати в розрахунках при використанні різних середовищ передачі і гібридних каналів передачі даних.

### 1.2.2. Методи забезпечення якості в VoIP

В рекомендації ITU-T Y.1291 [12] виділяється кілька основних конструктивних блоків, розподілених по трьох площинах (Рис. 1.3).

• Площина управління, що містить механізми управління трактами, через які проходить трафік користувача. До складу цих механізмів входить управління допуском, маршрутизація для QoS і резервування ресурсів.

• Площина даних містить механізми, що працюють безпосередньо з трафіком користувача. До складу цих механізмів входить управління буферами, запобігання перевантаження, маркування пакетів, організація черг і диспетчеризація, класифікація трафіку, правила його обробки та моделювання.

• Площина адміністративного управління, що містить механізми, які стосуються експлуатації, адміністрування і адміністративного управління мережею. До складу цих механізмів входять: угода про рівень обслуговування (SLA), відновлення трафіку, вимір і реєстрація, а також задані правила доставки інформації

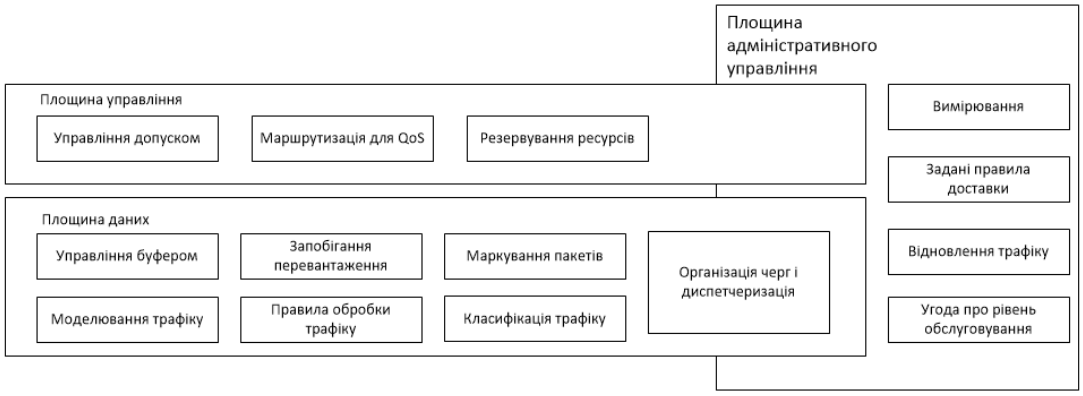


Рис. 1.3 - Архітектурна модель для підтримки QoS за рекомендацією ITU-T Y.1291

Далі будуть розглянуті протоколи і методи забезпечення якості, які застосовуються в різних площинах архітектурної моделі для підтримки QoS. У площині даних виконуються класифікація та маркування пакетів,

застосовуються планування до пакетів, а також використовуються додаткові алгоритми обробки пакетів.

Класифікація може виконуватися в залежності від CoS, MPLS-EXP, номера порту підключення кореспондента до мережевого обладнання або MAC адреси відправника або отримувача, Ethertype відправляємого пакета та інших ознак. Основним завданням класифікації є поділ пакетів на групи з метою їх подальшого маркування з призначенням параметрів пакету:

• MPLS-EXP - три біта в MPLS для маркування QoS;

• біти CoS 802.1p;

• IP Precedence байт (ToS) або DSCP.

Інструмент планування застосовується для визначення який кадр або пакет буде першим виходити з інтерфейсу мережевого вузла. Завдання вирішується за рахунок застосування алгоритмів управління чергою, а також механізмів запобігання переповнення черги. Виділяють алгоритми управління чергою: SP, WRR, WFQ, CBWFQ, MDRR, LLQ (PQ + CBWFQ), WRED.Детальний розгляд кожного з алгоритмів виходить за рамки дослідження. Опис алгоритмів приведено в [13]. Найбільш поширеним є застосування пріоритетності голосового трафіку в низькошвидкісних бездротових каналах зв'язку (КЗ) [14].

Для забезпечення якості VoIP можуть застосовуватися механізми обмеження швидкості - policing або shaping. Policing - обмеження швидкості передачі даних без буферу. Shaping - обмеження швидкості передачі даних з проміжним буфером.

Додатково може застосовуватися управління потоком Ethernet -механізм, що дозволяє попередити відправника про необхідність зупинити передачу даних на зазначеному інтервалі часу з причини, що приймаючий порт не може виконати обробку.

Для низькошвидкісних каналів додатково можуть бути застосовані механізми:

• Фрагментація і чергування пакетів;

• Механізми компресії (Compressed RTP - cRTP).Так cRTP дозволяє стискати заголовок голосового пакету IP / UDP / RTP з 40 до 2-5 байт. Однак - даний механізм використовується тільки в межах одного фізичного каналу зв'язку.

До механізмів площини управління архітектурної моделі для підтримки QoS відносяться застосування RSVP (резервування ресурсів) на мережі, а також використання алгоритмів маршрутизації з урахуванням QoS. В якості вхідних даних алгоритми можуть використовувати значення полів в промаркованих пакетах і таблицю маршрутизації, що враховує різні параметри QoS для інтерфейсів обладнання і для різних маршрутів. Частина такого функціоналу підтримується, наприклад, протоколом маршрутизації OSPF. Механізми маршрутизації з урахуванням вимог QoS і додаткових можливостей протоколу OSPF описані в RFC 2676 [15].

До площини адміністративного управління відносяться механізми зміни параметрів для VoIP трафіку, які застосовуються на призначених для користувача терміналах, IP-телефонних станціях, а також на додаткових елементах мережі VoIP, таких, як RTP-проксі-сервери і прикордонні контролери сесій (SBC, Session Border Controller).

### 1.2.3. Методи оцінки якості VoIP

У світі ведуться активні дискусії про те, які моделі використовувати для оцінки якості наданих сервісів, а також як оцінити ефективність обробки пакетів в мережі, які методики використовувати для оцінки якості послуг, що надаються.

Ведуться активні розробки в напрямку оцінки QoS і QoE VoIP трафіку. QoS (Quality of Service - Якість Обслуговування) за визначенням ITU - це колективний ефект роботи сервісів, який визначає ступінь задоволення користувача обслуговуванням.

QoE (Quality Of Experience - Якість сприйняття) суб'єктивна міра оцінки роботи системи. QoE покладається на людську точку зору і відрізняється від якості обслуговування QoS, яка може бути точно виміряна. Наприклад, реакція

людини при прослуховуванні музики через навушники базується не тільки на частотній характеристиці системи і спікерів, а й на комфорті одиниці, чутливості слуху людини.

Для IP-телефонії МСЕ стандартизував математичну модель в рекомендації G.107 [16] для оцінки QoE виходячи з параметрів якості терміналу і мережі. Ця модель отримала назву E-model і служить для розрахунку R-фактора.

Модель була широко використана для оцінки QoE в мережах IP-телефонії в Японії. В результаті в лабораторії NTT був розроблений набір параметрів для оцінки сприйняття якості відеотелефонії, які згодом використовувалися в новій моделі МСЕ для відеотелефонії.

Використовуючи Е-модель, а також параметри каналу передачі даних і параметри застосовуваної системи IP-телефонії, можна оцінити MoS (Mean Opinion Score) - суб'єктивний рівень якості, що сприймається користувачем послуги IP-телефонії. В рекомендації [16] наводиться відповідність R-фактора, описуваного і обчислюваного з використанням Е-моделі, і параметра MoS (Табл. 1.2).На підставі Табл. 1.3 обрана нижня межа MOS 3.6, якій відповідає R = 70. Необхідно визначити можливі параметри канала зв'язку- затримку в каналі зв'язку (d) і % втрати пакетів (p.l.) - при яких буде досягатися значення R≥70.

*Таблиця 1.2*

Зв'язок R-фактор і MOS за рекомендацією G.107

| R-фактор | MoS (нижній поріг) | Задоволеність користувачів |
|---|---|---|
| 90 | 4,34 | Висока задоволеність |
| 80 | 4,03 | Задоволеність |
| 70 | 3,60 | Деякі користувачі не задоволені |
| 60 | 3,10 | Багато користувачів не задоволені |
| 50 | 2,58 | Майже всі користувачі не задоволені |

В [17] розглядається вплив параметрів каналу зв'язку на надану якість послуг VoIP для різних кодеків: G.711, G.723 і G.729. Для цього виконується

розрахунок MOS з використанням E-моделі для різних затримок каналу зв'язку в інтервалі затримок 0-1200 мс, а також для втрати пакетів 0-12%. На рисунках 1.4-1.6 видно, як змінюється R в залежності від *p.l.* і від *d*. Додатково на графіках відзначені умови, при яких забезпечується значення R ≥ 70.

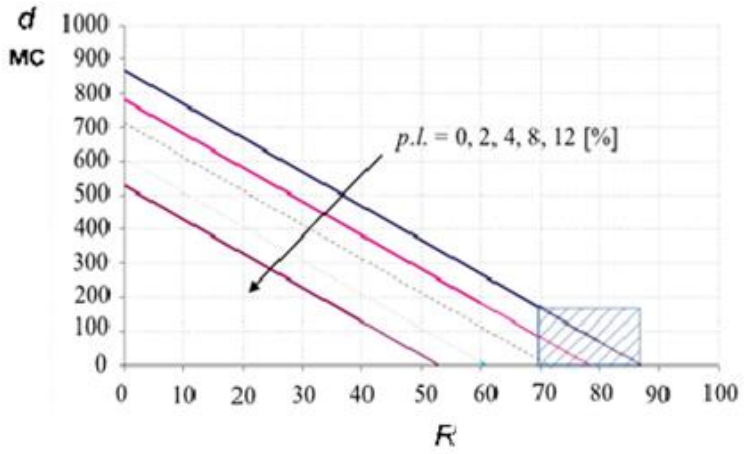


Рис. 1.4 - Залежність R-фактора від втрати пакетів і затримки в каналі зв'язку для G.723 кодека

З рис. 1.4-1.6 видно, що кодек G.711 забезпечує найбільше значення MOS при найгірших умовах в каналі зв'язку: максимальної затримки і втрати пакетів. При *p.l. = 0* умова *R> = 70* виконується для *d <= 300* мс, при *p.l. = 12, R> = 70* виконується для *d <= 100* мс.

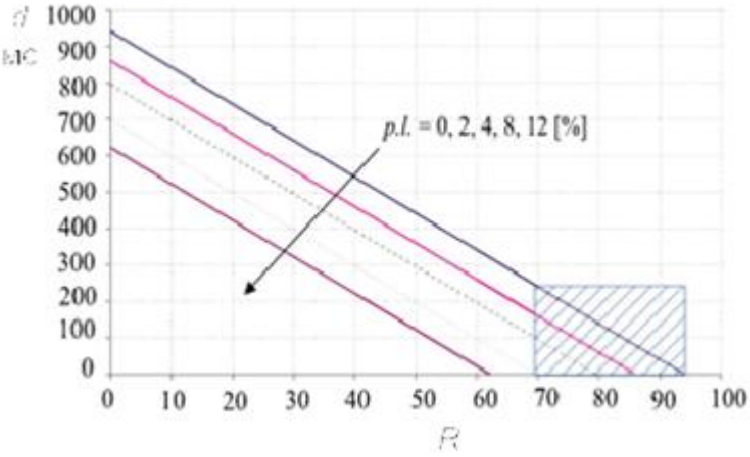


Рис. 1.5 - Залежність R-фактора від втрати пакетів і затримки в каналі зв'язку для G.729 кодека

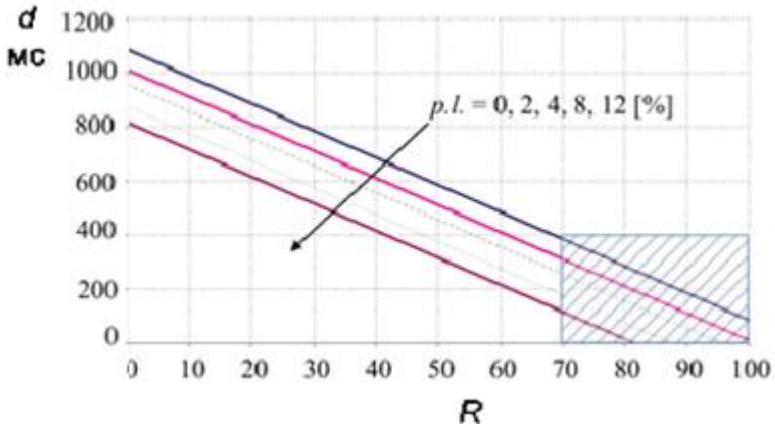


Рис. 1.6 - Залежність R-фактора від втрати пакетів і затримки в каналі зв'язку для G.711 кодека

Подальший аналіз протоколів забезпечення безпеки доцільно проводити для каналу зв'язку з параметрами *d <= 300* і *p.l. <= 12* при використанні G.711 кодека. У наступних обчисленнях також перевага віддається кодеку G.711, як самому стійкому при роботі по каналах зв'язку з помилками.

В якості вхідного параметра при розрахунках замість параметра *p.l.* зручно використовувати похідний параметр - ймовірність бітової помилки в каналі зв'язку p0. Для цього необхідно визначити значення p0, еквівалентне *p.l. = 12* для кодека G.711.

$$p.l.=1-(1-p_0)^{ps} \quad , \tag{1.1}$$

де *ps* - розмір пакета, біт.

Для кодека G.711 допускаються розміри корисного навантаження 80,160,240 байт. При цьому розмір пакета з урахуванням заголовків становитиме відповідно 138,218,296 байт. *p0* визначається за формулою:

$$p_0 = 1 - 10^{\frac{\lg(1-p.l.)}{ps}} \tag{1.2}$$

Розраховані значення наведені в Табл. 1.3 З таблиці видно, що максимальне значення ймовірності бітової помилки *ppl* = 12% відповідає *p0* = $1{,}16 \cdot 10^{-4}$. Відповідно, розрахунки необхідно виконувати для значень *p0*≤$1{,}16 \cdot 10^{-4}$.

*Таблиця 1.3*

Залежність *p0* від *p.l.* для кодека G.711

| імовірність втрати пакету, *p.l.* | Розмір пакету, *ps* , бит | Імовірність бітової помилки, $p_0$ |
|---|---|---|
| 0,12 | 138 | $1{,}16 \cdot 10^{-4}$ |
| 0,12 | 218 | $7{,}33 \cdot 10^{-5}$ |
| 0,12 | 298 | $5{,}36 \cdot 10^{-5}$ |

## 1.3. Забезпечення інформаційної безпеки IP-телефонії

В силу загальнодоступності використовуваних каналів передачі голосової інформації в IP мережах особливої актуальності набуває забезпечення конфіденційності VoIP-сервісів. Для вирішення цього завдання можуть бути використані різні підходи:

• забезпечення прямого захищеного каналу між кореспондентами (наприклад, VPN-тунель);

• застосування спеціальних протоколів забезпечення безпеки для IP-сервісів.

Перший спосіб набув широкого поширення при побудові віртуальних корпоративних мереж, але для його реалізації кореспонденти повинні підтримувати VPN-протокол. Однак, багато VoIP-пристрої не підтримують VPN.

Тому, для забезпечення безпеки досить часто застосовуються спеціальні протоколи забезпечення безпеки IP-телефонії.

### 1.3.1. Протоколи забезпечення безпеки IP-телефонії

До спеціальних протоколів забезпечення безпеки IP-телефонії відносяться протоколи Secured SIP, SRTP, MIKEY, SDES, ZRTP, DTLS, S-MIME. Ці протоколи можна розділити на 3 категорії [2, 16]:

- Протоколи захисту сигналізації (Secured SIP);
- Протокол захисту медіаінформації (SRTP);
- Протоколи генерації і розподілу ключів для протоколів захисту медіаінформації (MIKEY, SDES, ZRTP, DTLS).

Необхідно розглянути докладніше ці категорії.

Протоколи захисту сигналізації призначені для забезпечення безпеки інформації про телефонні номери викликаючого і викликаємого абонента, підтримувані кодеки. Для вирішення цього завдання використовується Secured SIP (SSIP, SIP / TLS) [3]. Цей протокол працює за аналогією з протоколом HTTPS, організовуючи між кореспондентом і сервером SSL тунель з використанням сертифікатів і відкритого ключа. Всі SIP-повідомлення (сигналізація) передаються по цьому тунелю. Недоліком протоколу є необхідність застосування інфраструктури відкритих ключів, що використовується для організації TLS.

Для забезпечення конфіденційності при передачі мови широко використовується захищений протокол реального часу - Secure Real-time Transport Protocol (SRTP) [17], який реалізує функції криптографічного захисту - шифрування і аутентифікації мовних повідомлень на основі алгоритму шифрування AES.

Криптографічний захист пакетів голосової інформації виконується протоколом SRTP в режимі реального часу і не вносить змін в ймовірносно-часові характеристики протоколу RTP. Але для його роботи необхідно попереднє формування криптографічних ключів. Це завдання вирішує протокол розподілу ключів (ПРК).Рекомендація RFC 3711 описує дві складові - власне протокол SRTP для перенесення і криптозахисту медіа даних, а також протокол SRTCP (Secure Real-time Transport Control Protocol) для управління медіа сесією.

Основними завданнями протоколу SRTP є виконання таких функцій:

- шифрування переданих голосових даних;
- аутентифікація переданих повідомлень;
- захист від передачі повторних пакетів;
- збереження смуги пропускання, стиснення RTP заголовків.

Основними завданнями протоколу SRTCP є виконання таких функцій:

- шифрування переданих даних;
- аутентифікація переданих повідомлень.

Аутентифікація і шифрування можуть працювати незалежно один від одного. Таким чином, можливий варіант, коли шифрування вимкнено і SRTP здійснюється виключно з метою аутентифікації. Обмеженням протоколу є те, що аутентифікація повідомлення обов'язкова в SRTP і не може бути відключена.

### 1.3.2. Протоколи генерації і розподілу ключів для захисту медіаінформації

Протоколи третьої групи, за аналогією з родинними протоколами розподілу ключів в бездротових мережах [18], призначені для генерації і розподілу між кореспондентами ключів шифрування медіаінформації. Для вирішення цього завдання можуть використовуватися протоколи MIKEY, SDES, ZRTP, DTLS.

Протокол обміну ключами MIKEY описаний в рекомендаціях RFC3830 [19] і RFC6309 [20]. MIKEY має кілька режимів роботи, що визначають спосіб формування секретного ключа сесії SRTP: режим попередньо встановленого ключа, режим відкритого ключа та режим Діффі-Хелмана. Причому другий і третій режими не захищають від атаки вторгнення в середину (MiTM, Man In the Middle) і вимагають реалізації механізму аутентифікації повідомлень. Транспортом для переносу повідомлень протоколу може виступати як SIP / SDP, так і протокол RTSP (Real Time Streaming Protocol).

SDES (Session Description Protocol Security) [21] описується в RFC4568. Суть протоколу полягає в тому, що один з кореспондентів передає ключ в SIP повідомленні по сигнальному каналу. Кореспондент отримує його і використовує для шифрування. Однак при цьому обмін сигнальними повідомленнями повинен бути захищений від зловмисника. З цієї причини -

SDES може використовуватися тільки при наявності SIP / TLS захищеного з'єднання з цифровим сертифікатом сервера. Також даний спосіб не забезпечує безпеки з кінця в кінець. Це означає, що якщо з'єднання буде виконуватися через IP АТС, SDES буде виконувати розподіл ключів між кореспондентом А і IP PBX, між кореспондентом Б і IP-телефонною станцією, але не між кореспондентами А і Б безпосередньо.

Протокол DTLS [22] для SRTP описується в RFC 5764. Протокол описує формування медіа-сесій точка-точка з двома учасниками з жорстким фіксуванням портів UDP кореспондента і респондента. Повідомлення протоколу передаються спільно з RTP пакетами. Кожна сесія містить одну DTLS асоціацію і два SRTP контексту (для SRTP і SRTCP). Для організації сесії (DTLS-асоціації) кореспонденти виконують обмін повідомленнями, званий DTLS handshake (Рис. 1.7). Так як в основі протоколу лежить TLS, що використовує інфраструктуру відкритих ключів (Public Key Infrastructure, PKI), то застосування TLS можливо теж тільки при наявності PKI.

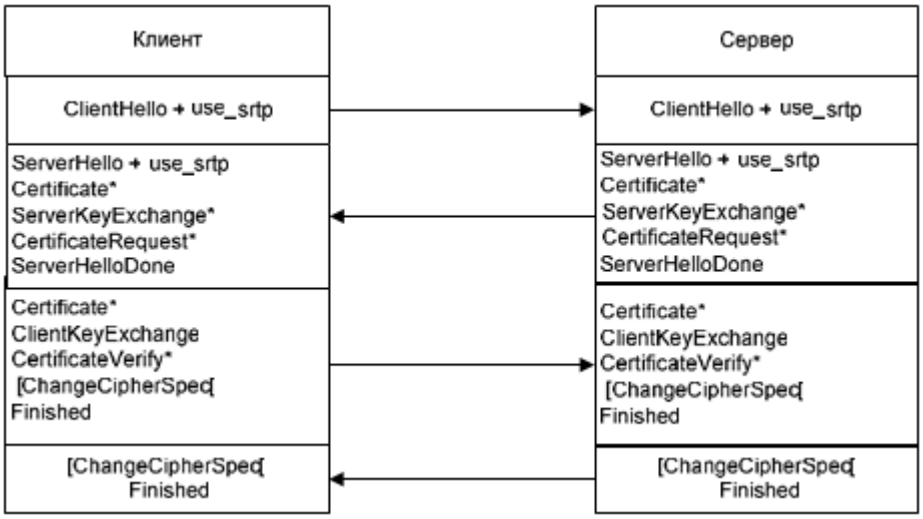


Рис. 1.7 - Обмін повідомленнями DTLS

Одним з найбільш перспективних протоколів генерації ключів є ZRTP [23, 24]. Протокол застосовується в додатку для Android CsipSimple, програмних телефонах Jitsi, Phoner, програмних АТС FreeSwitch і Asterisk, апаратних VoIP шлюзах компанії UM-Labs. Відмінною особливістю ZRTP

протоколу є можливість забезпечення безпеки з кінця в кінець, від одного кореспондента до іншого. Завданнями протоколу ZRTP є:

• генерація ключових параметрів SRTP сесії;

• забезпечення конфіденційності повідомлень протоколу;

• забезпечення аутентифікації кореспондентів;

• захист від атаки вторгнення посередині, як з використанням, так і без використання інфраструктури відкритих ключів.

Протокол передбачає роботу кореспондентів по топології точка-точка, при цьому окремо виділяється можливість застосування протоколу при багатопотоковому режимі, коли необхідно організувати кілька захищених медіа потоків. Крім того, передбачений режим роботи з легітимним посередником, яким може бути, наприклад, корпоративна телефонна станція. Кожен з кореспондентів-учасників протоколу повинен мати встановлений ідентифікатор (ZID), який повинен бути унікальний.

В основі протоколу - обмін ключами по алгоритму Діффі-Хелмана. Особливістю протоколу є передача параметрів всередині RTP пакетів, залишаючи пакети сумісними з RTP / AVP профілем. В цьому випадку, ZRTP-несумісним пристроєм ZRTP-пакети просто відхиляються і не впливають на встановлене з'єднання.

Для аутентифікації кореспондентів, а також виключення атаки вторгнення в середину (MiTM, Man in The Middle), протокол ZRTP передбачає використання короткого аутентифікаційного рядка (SAS, Short Authentication String), а також частини ключового матеріалу від попередніх сесій між кореспондентами. Для контролю цілісності переданих повідомлень кожне повідомлення ZRTP включає в себе код CRC, а також код аутентифікації повідомлення MAC (Message Authentication Code). MAC обчислюється, як ключова хеш-функція, яка узгоджується на першій фазі протоколу.

Виявлення помилки тільки в хеш-повідомленні, як правило, означає виявлення атаки MiTM, оскільки спотворення за рахунок канальних помилок виявляються і при перевірці CRC ZRTP пакета.

Протокол виконується послідовно в чотири фази:

1. Виявлення;

2. Підтвердження;

3. Обчислення ключів;

4. Завершення.

У загальному випадку, ZRTP працює на самому початку розмови кореспондентів, відразу після завершення роботи протоколу SIP, як починає працювати в сторони протокол RTP (Рис. 1.8).

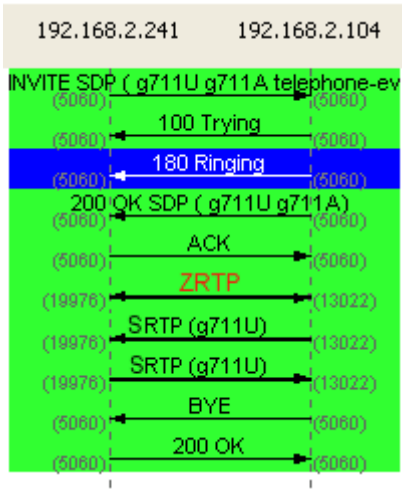


Рис. 1.8 - Схема обміну повідомленнями між кореспондентами з використанням SIP / SRTP / ZRTP

### 1.3.3. Вимоги до протоколів розподілу ключів

Для подальшого дослідження також необхідно сформулювати вимоги, яким повинні відповідати ПРК:

1. Протокол повинен підтримувати роботу як в топології клієнт-сервер, так і в топології клієнт-клієнт.

2. Протокол повинен бути самодостатнім і виконувати функцію розподілу ключового матеріалу без застосування додаткових протоколів між кореспондентами.

3. Протокол повинен підтримувати механізм розподілу ключів в топології клієнт-клієнт без передачі ключа в явному вигляді по каналу зв'язку.

4. Протокол повинен мати механізм виявлення MITM без заздалегідь розподіленого ключового матеріалу між кореспондентами.

5. Протокол повинен використовувати TCP / UDP порти, що застосовуються для IP- телефонії, або TCP / UDP порти, використання яких узгоджено в результаті встановлення з'єднання.

Перша вимога обгрунтована необхідністю забезпечення безпеки в топології клієнт-клієнт, так як в топології клієнт-сервер кореспонденти вже мають перед розподілений загальний секрет, який використовується для захисту повідомлень протоколу розподілу ключів для SRTP.

Друга вимога обґрунтована вимогами по простоті інтеграції в існуючі системи зв'язку, програмні термінали. У разі одночасної роботи кількох протоколів, кожен з яких передає свої повідомлення по каналу зв'язку, це ускладнить інтеграцію протоколу в програмний VoIP термінал користувача.

Третя вимога обгрунтована принципом забезпечення безпеки, обмовлюючим, що ключ шифрування ніколи не повинен передаватися по каналу зв'язку в явному вигляді.

Четверта вимога викликана можливістю використання протоколу розподілу ключів між рівноправними кореспондентами, які не мають попередньо розподіленого ключового матеріалу і загальних сертифікатів, а також загального довіреного центру сертифікації.

П'ята вимога викликана спрощенням інтеграції протоколу безпеки в існуючі мережі з метою перешкоджання блокування повідомлень протоколу

розподілу міжмережевими екранами при використанні TCP або UDP портів, не передбачених протоколами SIP / RTP.

### 1.4. Висновки

У першому розділі розглянуті актуальні проблеми та існуючі підходи їх вирішення в області захищеної IP-телефонії. Зокрема, розглянуто основні компоненти і протоколи IP-телефонії, а також можливі сценарії встановлення з'єднань. Описано механізми і алгоритми, що застосовуються для забезпечення нормованого показника MOS, а також значень інших нормованих показників. Показано значення параметрів каналу зв'язку, при яких має сенс виконувати аналіз роботи протоколів IP-телефонії.

Наведено набір протоколів забезпечення безпеки IP-телефонії, а також класифікація протоколів і їх скорочений опис. Показано вплив протоколів безпеки на параметри функціонування мережі телефонії, виражене у виникненні затримки при встановленні захищеного з'єднання між кореспондентами.

# Розділ 2. МАТЕМАТИЧНА МОДЕЛЬ АКТИВНОГО ПОРУШНИКА ДЛЯ ЗАХИЩЕНОЇ IP-ТЕЛЕФОНІЇ

## 2.1. Загрози інформаційної безпеки в IP-телефонії

Загроза безпеки інформації в IP-телефонії виникає в внаслідок утворення каналу між джерелом загрози і носієм (джерелом) інформації, що створює умови для порушення безпеки інформації.

Актуальність загрози безпеки інформації буде визначатися, в тому числі, видом джерела загрози безпеки інформації, наявністю вразливості джерела інформації і середовищем поширення інформаційного сигналу.

По виду джерела загрози впливів на інформацію можна виділити:

- загрози, пов'язані з діяльністю організацій, що володіють високим потенціалом, оснащеністю і мотивацією, зумовленою політичними, економічними, військовими та іншими цілями іноземних держав;
- загрози, пов'язані з діяльністю організацій, що володіють мотивацією, зумовленою їх економічними, інформаційними та іншими цілями;
- загрози, пов'язані з діяльністю окремих фізичних осіб (злочинних елементів).

Способи впливу на інформацію визначаються можливостями джерела загроз. Джерело загроз, що застосовує дії або здійснює підготовку до дій щодо несанкціонованого впливу на інформацію є порушником інформаційної безпеки.

Далі в якості порушника розглядається фізична особа, що випадково або навмисно скоює дії в своїх інтересах або в інтересах організацій, наслідком яких є порушення безпеки інформації при її обробці технічними засобами в інформаційних системах.

Доцільно розглядати порушників з точки зору наявності права постійного або разового доступу в контрольовану зону (КЗ) [27]. Виділяються два типи порушників:

- порушники, які не мають права доступу в КЗ - зовнішні порушники;

- порушники, які мають право доступу в КЗ - внутрішні порушники.

Зовнішніми порушниками можуть бути:

- представники розвідувальних служб іноземних держав;
- представники терористичних і кримінальних структур;
- сторонні особи.

Внутрішніми порушниками можуть бути:

- працівники оператора;
- працівники сторонніх організацій - розробників або постачальників програмного забезпечення і технічних засобів, що забезпечують супровід цих засобів на захищаємому об'єкті.

Забезпечення безпеки передачі мови в IP-телефонії здійснюється із застосуванням криптографічних протоколів: захищеного протоколу реального часу - SRTP, що реалізує функції криптографічної інкапсуляції даних, а також протоколів, що виконують функцію автоматичного розподілу ключів для сесій SRTP, і протоколів захисту сигналізації.

З огляду на те, що передача даних IP-телефонії здійснюється в мережах загального доступу, а VoIP термінали доступні будь-якій фізичній особі, як і легальний доступ до мереж - можна зробити висновок про актуальність загроз віддаленого доступу і можливості їх реалізації як зовнішніми порушниками, так і окремими категоріями внутрішніх порушників.

### 2.2. Узагальнена модель порушника

Під моделлю порушника розуміється опис сукупності практичних і теоретичних можливостей, знань, часу, місця дії, а також інших характеристик, властивих порушнику.

Під ймовірнісною моделлю [stochastic, probabilistic model] - розуміють модель, яка на відміну від детермінованої моделі містить випадкові елементи [28]. При заданні на вході моделі деякої сукупності значень, на її виході можуть отримуватися різні між собою результати в залежності від дії випадкового фактора.

Під математичною моделлю порушника розуміється модель, яка містить випадкові елементи у вигляді ймовірностей успішного виконання окремих атак, які формують одну загальну атаку, і визначає ймовірність досягнення кінцевої цілі цієї атаки порушником.

Щоб модель порушника була максимально корисною - вона повинна орієнтуватися на конкретний об'єкт захисту. Тому модель не може бути універсальною і синтезується виходячи з аналізу структури системи, ресурсів і способів їх використання.

Існуючі моделі порушника не враховують особливостей роботи безпечної IP-телефонії, що складаються в застосуванні декількох протоколів для забезпечення безпеки, а також не описують атаки безпосередньо на ці протоколи.

Отже, доцільно розробити модель порушника, що враховує ці особливості. Для цього необхідно розглянути схему взаємодії кореспондентів захищеної IP-телефонії для прямого з'єднання клієнт - клієнт, при відсутності попередньо розподіленого ключового матеріалу, і можливі варіанти дії порушника в схемі (Рис. 2.1).

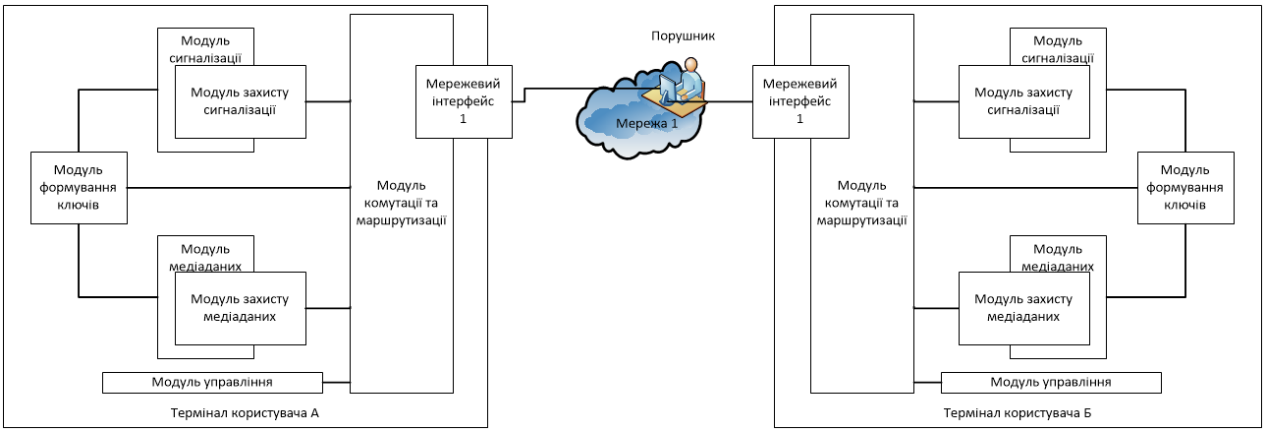


Рис. 2.1 - Структурна схема з'єднання в сценарії клієнт-клієнт

Порушник може використовувати такі стратегії:

- Пасивну, використовуючи тільки перехоплення переданих даних.
- Активну, використовуючи штатні засоби системи захисту і її недоліки для проведення атаки або додаткові кошти для впливу на систему с метою виконання атаки.

Надалі розглядається порушник, який використовує активну стратегію атаки, яка експлуатує уразливість протоколу Діффі-Хелмана, що лежить в основі більшості протоколів розподілу ключів (ПРК) IP- телефонії. Цей протокол захищає від атаки пасивного порушника. Однак, він нестійкий до атаки Man In The Middle (MITM) активного порушника [5, 29].

При здійсненні протиправних дій порушник може:

- перебувати в одній підмережі з об'єктом атаки, в тому числі мати права доступу будь-якого рівня до мережі або до обладнання, на яке виконується атака;
- не перебувати в одній підмережі з об'єктом атаки або не мати прав доступу будь-якого рівня до мережі або до обладнання, на яке виконується атака.

VoIP терміналом користувача, як правило, є IP-телефон, шлюз IP-телефонії, або інший обчислювальний пристрій (стаціонарний комп'ютер або мобільний термінал: ноутбук, планшетний комп'ютер, смартфон і т.д.) з встановленим спеціалізованим програмним забезпеченням IP-телефонії. Цей пристрій дозволяє користувачеві отримувати послуги IP-телефонії і виконувати аудіо або відео виклики інших користувачів.

При розгляді атак на термінал користувача введено допущення, що в одній підмережі з жертвою може перебувати тільки внутрішній порушник. Відповідно, деякі типи атак будуть доступні тільки для цієї категорії порушників.

Для досягнення цілей НСД порушник при проведенні атаки може використовувати такі існуючі загрози безпеці:

1. Навмисний несанкціонований доступ на обладнання оператора або користувача, отриманий за рахунок атаки перебору пароля або іншої атаки на механізми забезпечення безпеки інформаційної системи (ІС), з боку внутрішніх або зовнішніх порушників, що володіють правами і повноваженнями на доступ до обладнання нижчого рівня, або які не мають доступу до нього ,.

2. Навмисний вплив на таблицю маршрутизації з боку зовнішніх або внутрішніх порушників, а також використання штатних засобів обладнання для часткового перенаправлення трафіку користувачами, що володіють правами і повноваженнями на доступ до інформації в інформаційній системі.

3. Навмисний спеціалізований вплив на обмін повідомленнями ПРК, а також на інші дані кореспондентів, що передаються, спрямований на порушення конфіденційності і цілісності переданих даних, з боку внутрішніх і зовнішніх порушників, що володіють правами і повноваженнями на доступ до інформації в ІС.

4. Спеціальний вплив у вигляді атаки на шифр на перехоплену інформацію, передану між кореспондентами, з боку внутрішніх і зовнішніх порушників, що володіють правами і повноваженнями на доступ або перехоплення зашифрованої інформації в інформаційній системі, з метою порушення конфіденційності і дешифрування даних.

5. Умисна несанкціонована спеціальна взаємодія на програмне забезпечення одного або декількох кореспондентів з боку внутрішніх або зовнішніх порушників, що володіють правами і повноваженнями на доступ до обладнання та використовуваного програмного забезпечення користувача.

6. Навмисне несанкціоноване встановлення додаткового обладнання на вузлі оператора для цілей спеціального впливу на передану від користувачів інформацію з боку внутрішніх порушників, що володіють правами і повноваженнями доступу на вузол оператора.

7. Навмисний несанкціонований вплив на конфігураційні файли терміналу з боку внутрішніх і зовнішніх порушників, що володіють правами і повноваженнями доступу до терміналу користувача, з метою зміни налаштувань безпеки.

8. Навмисне несанкціоноване перехоплення авторизаційних даних для управління обладнанням користувача з боку внутрішніх порушників, що володіють правами і повноваженнями на доступ до даних, що передаються між комп'ютером користувача і терміналом користувача.

Для побудови математичної моделі порушника виконано аналіз загроз і їх джерел. Використовуючи уразливості, активний порушник може виконувати комбінацію атак, яка може привести до досягнення несанкціонованого доступу.

В якості основних можливих атак активного порушника [26] виділені:

- Перебір пароля для доступу до управління обладнанням оператора або користувача;
- Організація проксінгу або перенаправлення всього або частини трафіку будь-яким доступним способом;
- Виконання атаки MITM на ПРК і інші протоколи безпечної IP-телефонії;
- Атака на шифр - перебір ключа до перехопленого медіа трафіку;
- Установка закладки, модифікація програмного забезпечення (ПО)термінала користувача;
- Встановлення додаткового обладнання на вузлі оператора зв'язку;
- Зміна налаштувань термінала користувача для часткового відключення безпеки;
- Перехоплення авторизаційних даних для управління терміналом користувача за рахунок прослуховування трафіку управління шлюзом.

Атака перебір пароля до обладнання [30] дозволяє отримати нелегітимному користувачеві контроль над обладнанням, що атакується для подальшої організації атаки несанкціонованого доступу. Складність атаки залежить від протоколу управління, на який виконується атака (telnet, ssh, snmp, web і т.д.), від довжини використовуваних паролів, обчислювальних ресурсів порушника, і додаткових обмежень і захисних механізмів обладнання що атакується, а також від ширини каналу зв'язку між порушником і жертвою. Атака виконується з використанням спеціалізованого програмного забезпечення при наявності каналу зв'язку для віддаленого доступу до інтерфейсу управління обладнанням.

Атака "організація проксінгу або перенаправлення трафіку" дозволяє порушнику частково або повністю пропускати через своє обладнання трафік легітимного кореспондента. Це може бути досягнуто за рахунок використання функції віддзеркалення портів на обладнанні оператора, за рахунок використання маршрутизації на основі політик (policy based routing), а також за рахунок інших механізмів, доступних на обладнанні оператора зв'язку з комутацією пакетів.

Атака на ПРК полягає в організації MITM і вироблення ключів по черзі з кожним з кореспондентів [31]. Вона дозволяє порушнику ставати проміжним елементом між кореспондентами і прослуховувати або модифікувати передану інформацію. При цьому небезпека і поширеність даної атаки найбільш активно відзначається в різних джерелах масової інформації [32 - 35].

Атака на шифр полягає в отриманні ключа шифрування при наявності зашифрованого повідомлення. Атака може виконуватися за допомогою спеціалізованого програмного забезпечення, що здійснює перебір пароля на підставі часткової інформації про передані данні.

Установка закладки, модифікація програмного забезпечення термінала користувача дозволяє порушнику отримувати контроль над обладнанням користувача та будь-якою інформацією, що проходить через термінал, а також виконувати відведення інформації на свій сервер з метою виконання атаки несанкціонованого доступу.

Встановлення додаткового обладнання на вузлі оператора зв'язку, дозволяє порушнику виконувати модифікацію даних, переданих між кореспондентами, без необхідності зміни маршрутизації на мережевому обладнанні оператора. Атака виконується за рахунок включення між обладнанням оператора і кореспондента обладнання порушника, або підключення цього обладнання в мережу передачі даних оператора.

Атака "зміна налаштувань терміналу користувача для зниження рівня безпеки" може виконуватися за рахунок зміни таблиці маршрутизації на терміналі користувача, часткового відключення механізмів безпеки, наприклад,

зміна режиму роботи протоколу SRTP на аутентифікацію повідомлень без шифрування, модифікації даних телефонної книжки і т.д.

Атака "перехоплення авторизаційних даних користувача, що застосовуються для управління VoIP-терміналом", може бути виконана внутрішнім порушником, що знаходиться в одній підмережі з легітимним користувачем, і досягається шляхом перехоплення трафіку в момент авторизації користувача на VoIP терміналі за рахунок атаки на MAC-таблицю обладнання, або перенастроювання мережевого обладнання.

### 2.3. Окремі моделі порушників

При розробці моделі порушника введено допущення, що якщо суб'єкт атаки знаходиться в одній мережі з об'єктом атаки, то такий порушник є внутрішнім. В іншому випадку він є зовнішнім. Тоді проміжними цілями порушників з точки зору отримання несанкціонованого доступу є [41]:

- $Ц_А$) захоплення обладнання оператора зовнішнім порушником;
- $Ц_Б$) захоплення терміналу користувача зовнішнім порушником;
- $Ц_В$) захоплення обладнання оператора внутрішнім порушником;
- $Ц_Г$) захоплення терміналу користувача внутрішнім порушником.

Кінцевою метою кожної атаки є НСД.

#### 2.3.1. Внутрішній порушник

Розробка моделі починається з аналізу алгоритмів дій порушника по кожній з перерахованих цілей.

##### 2.3.1.1. Захоплення обладнання оператора зовнішнім порушником

Розглянуто модель для зовнішнього порушника, завданням якого є досягнення НСД, а вирішується завдання через захоплення обладнання оператора. Алгоритм дій порушника наведено на Рис. 2.2.

Для початку атаки порушник повинен визначити, на який ресурс або який пристрій оператора почати виконувати атаку. Однією з можливостей отримати цю інформацію є використання команди tracert для визначення проміжних вузлів між порушником і жертвою. Відповідно - з великою ймовірністю ці вузли можуть брати участь в обміні пакетами між двома кореспондентами.

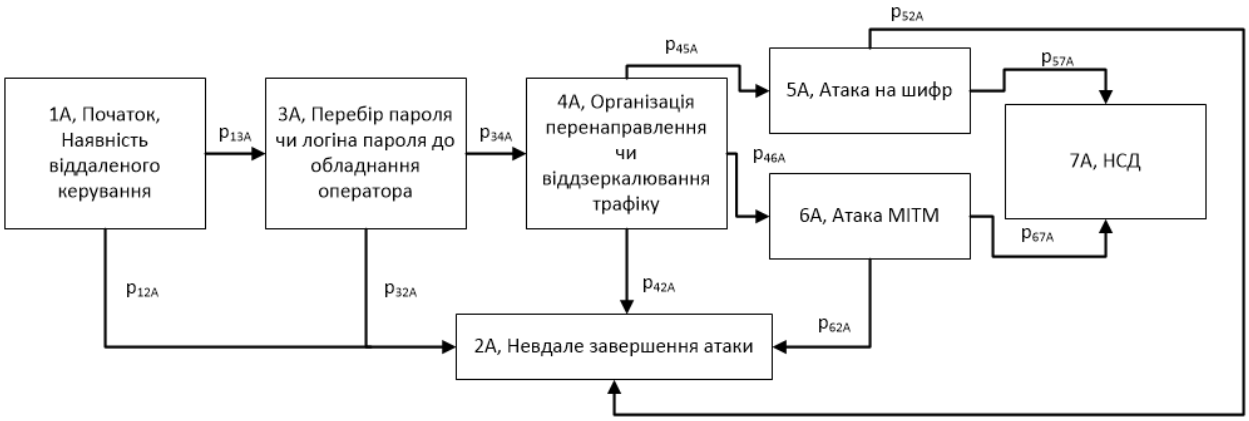


Рис. 2.2 - Можливий алгоритм дій при виконанні захоплення обладнання оператора зовнішнім порушником

Після вибору вузла порушник може спробувати захопити управління цим вузлом, виконуючи, наприклад, атаку перебір пароля. Однак - технічно віддалене управління може бути заборонено для порушника з використанням списків доступу ACL (Access Control List).

Імовірність $p_{12}$ відображає подію, що віддалене управління з боку порушника відключено або у оператора встановлені ACL.

Імовірність $p_{13}$ відображає подію, зворотню $p_{12}$, що існує можливість віддаленого підключення до пристрою оператора.

Порушник вибирає доступний протокол (telnet, SNMP, ssh, http / https або ін.) віддаленого управління, на який буде виконувати атаку перебором пароля. Імовірність успішного перебору пароля за обмежений час визначається, як

$$p_{34A}=F(l, D, T, C), \quad (2.1)$$

де $l$ - довжина логіна / пароля;

$T$ - час, протягом якого потрібно виконати перебір;

$D$ - додаткові обмеження протоколу, що ускладнюють виконання перебору пароля, а також технічні можливості порушника;

$c$ - швидкість каналу зв'язку, по якому виконується перебір.

Імовірність $p_{34A}$ відображає подію, що перебір пароля виконано успішно і порушник отримав доступ на обладнання оператора. Імовірність $p_{32}$ відображає подію, що перебір пароля за обмежений час закінчився неуспішно.

У разі успішного захоплення віддаленого управління, порушник може досягти НСД двома шляхами: виконати перебір пароля до медіа трафіку, що передається, і прослуховувати дані, або виконати атаку на механізм розподілу ключів і дешифрувати трафік з використанням отриманого ключового матеріалу. Однак - успішне виконання цих двох атак може не привести до позитивного результату щодо досягнення НСД, якщо не існує можливості виконати атаку MITM на медіа трафік, створивши правила на обладнанні оператора, які дозволять порушнику пропускати трафік користувача через своє обладнання. З цієї причини - подія "атака на медіа трафік" в моделі порушника перенесено раніше, ніж "перебір ключа медіа трафіку", або "атака на механізм розподілу ключів".

Імовірність успішної атаки на медіа трафік (MITM, організація проксінгу) можна визначити за формулою:

$$1 - p_{42A} \begin{cases} 1, \text{якщо існує технічна можливість на обладнанні оператора} \\ \text{створити правило для перенаправлення трафіку користувача} \\ \text{в сторону порушника для виконання цілей "проксінгу" MITM} \\ 0, \text{якщо не існує такої технічної можливості} \end{cases} \quad (2.2)$$

Під атакою розуміється зміна маршруту передачі пакетів мультимедійних файлів, щоб вони проходили через обладнання порушника. У разі успішного проведення атаки порушник намагається виконати одну з двох можливих атак.

- перебір ключа медіа трафіку;
- атака на механізм розподілу ключів.

При цьому ймовірності відображають:

$p_{45A}$ - ймовірність, що порушник почав виконувати перебір пароля до медіа трафіку.

$p_{46A}$ - ймовірність, що порушник почав атаку на механізм розподілу ключів VoIP.

Імовірність $p_{57}$ означає успішну атаку по перебору пароля. В цьому випадку - порушнику стає доступним прослуховування медіа трафіку однієї конкретної розмови, а також модифікації даних при наявності проксінгу і швидкого дешифрування ключа.

Імовірність $p_{52}$ відображає неуспішне закінчення атаки по перебору пароля за обмежений час. Перехоплені дані можуть зберігатися у порушника скільки завгодно довго, проте актуальність перехоплених даних може застарівати згодом. Так розшифровані через 100 років переговори можуть не принести ніякої користі порушнику, так як за цей час дані втратять актуальності. $T_{NAR\_AKT}$ - час, протягом якого дані є актуальними - залежить від характеру даних. $T_{NAR\_SRTP}$ - час, необхідний на перебір пароля, залежить від технічних потужностей порушника - $Nar_{TH}$, що застосовуються для захисту мультимедійних файлів криптографічних примітивів і криптоалгоритмів - $Nar_K$, довжини ключа - $Nar_L$, а також від ускладнюючих елементів (застосування ініціалізуючого вектора, додаткових лічильників і т.д. ) - $Nar_D$.

$$p_{57A} = f(T_{NAR\ ACT}, T_{NAR\ SRTP}) = f(T_{NAR\ ACT}, Nar_{TH}, Nar_k, Nar_L, Nar_D) \quad (2.3)$$

$$p_{52A} = 1 - p_{57A} \quad (2.4)$$

Імовірність $p_{67}$ визначає успішну атаку на механізм розподілу ключів. Під атакою розуміється вторгнення порушника в середину каналу зв'язку в момент обміну ключами між кореспондентами. Це дозволяє порушнику виробити два ключа - один для роботи з першим кореспондентом і другий для роботи з другим кореспондентом. Тим самим, під час розмови двох кореспондентів порушник виконує шифрування і дешифрування мультимедійних файлів з використанням власних джерел. Імовірність атаки залежить від наявності у порушника технічних і програмних засобів для проведення MITM на протокол розподілу ключів.

Слід зазначити, що для проведення даної атаки потрібна розробка спеціалізованого програмного забезпечення, але не потрібні великі обчислювальні потужності.

Імовірність $p_{62}$ відображає неуспішне виконання атаки і може бути визначена, як:

$$p_{62A} = 1 - p_{67A} \quad (2.5)$$

Для аналізу алгоритму використовується математичний апарат імовірнісних графів [36], який дозволяє отримати для досліджуваного алгоритму оцінки середнього часу виконання і ймовірність успішного завершення.

На Рис. 2.3 представлений імовірнісний граф, що відповідає наведеному раніше алгоритму. Імовірнісний граф використовується для отримання твірної функції, що відповіднає переходу системи з початкового стану в кінцевий.

Кожній гілки графа відповідає виробляє функція виду:

$$H_{zy} = p_{zy} x^{T_{zy}} \quad (2.6)$$

де $p_{zy}$ - ймовірність переходу в стан y з стану z,

$T_{zy}$ - час, необхідний для переходу зі стану z в стан y.

Використовуючи можливий алгоритм дій порушника, складено імовірнісний граф, представлений на Рис. 2.3.

По графу виділена гілка, що відповідає успішному виконанню атаки НСД і складена твірна функція *H (x)* цієї гілки.

Для графа відповідно до методики, наведеної в [36], представлені $P_{\text{НСД}} = H(x = 1)$:

$$P_{\text{нсдЦА}} = p_{13A} p_{34A} (p_{45A} p_{57A} + p_{46A} p_{67A}), \quad (2.7)$$

де $p_{ijA}$ - ймовірність переходу з вершини *i* графа в вершину *j*.

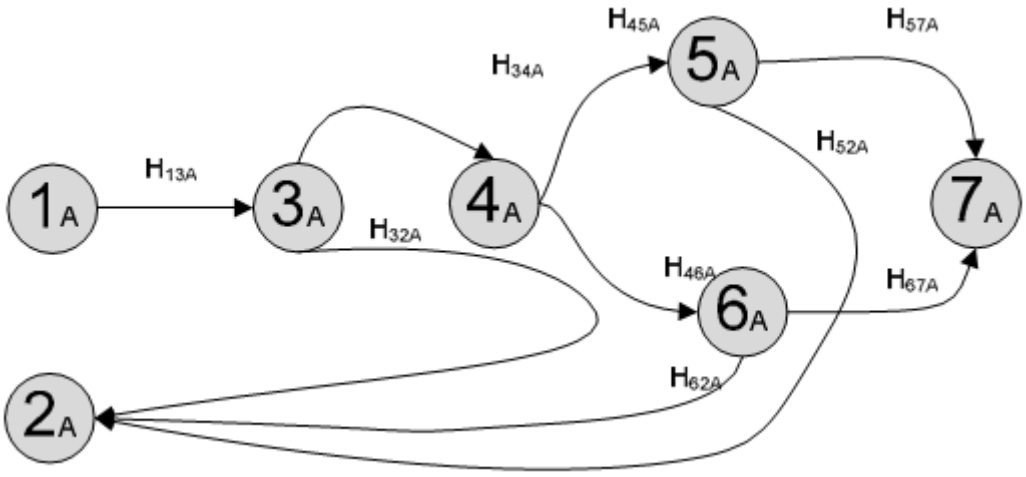


Рис. 2.3 - Імовірнісний граф - захоплення обладнання оператора зовнішнім порушником

**2.3.1.2. Захоплення термінала користувача зовнішнім порушником**

Розглянуто модель для зовнішнього порушника, завданням якого є досягнення НСД, а вирішується завдання через захоплення термінала користувача. Алгоритм дій порушника наведено на Рис. 2.4.

Розглянуто детальніше атаки, які може здійснити порушник, в залежності від використання у одного з кореспондентів шлюзу або персонального комп'ютера зі спеціалізованим програмним забезпеченням.

При використанні шлюзу найбільш вірогідною є атака з проксуванням всього трафіку через обладнання порушника. Атака виконується за схемою, зазначеною на Рис. 2.5, де IP1, IP2 - шлюзи користувачів, а Sн - сервер порушника зі спеціалізованим програмним забезпеченням.

Для проведення цієї атаки порушнику потрібно в першу чергу захопити управління VoIP терміналом користувача і виконати його перенастроювання. Наприклад - якщо у кореспондента в режимі точка-точка в телефонній книжці шлюзу введені поєднання номер - IP-адреса, то порушник може підмінити IP - адреса кореспондента Б в записнику кореспондента А на свій, тим самим дзвінки з телефону кореспондента А будуть приходити на Sн . Далі - сервер порушника виконує протоколи безпеки між собою і кореспондентом Б від імені

кореспондента А. Протоколи безпеки теж виконуються між кореспондентами Б і сервером порушника. В результаті - порушник отримує доступ до всієї інформації, що передається від кореспондента А до кореспондента Б, у відкритому вигляді і при необхідності може не тільки прослуховувати, але і змінювати дані, що передаються між кореспондентами. Перенаправлення трафіку від кореспондента А на Sн можна здійснювати не тільки за рахунок підміни запису в адресній книжці, а й за рахунок зміни налаштувань на шлюзі кореспондента А, встановивши адресу свого Sн в якості проксі-сервера або основного сервера IP-телефонії.

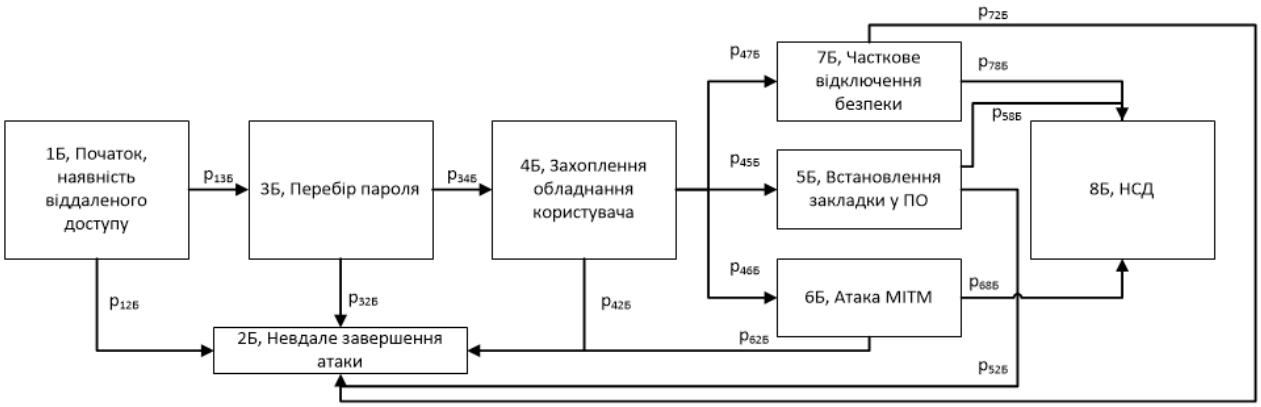


Рис. 2.4 - Можливий алгоритм дій при захопленні терміналу користувача зовнішнім порушником

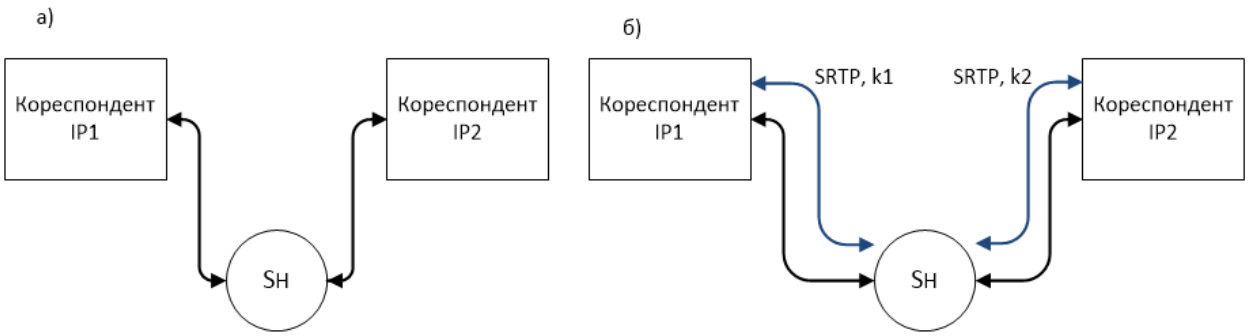


Рис. 2.5 - Атака з проксуванням а) виконання ПРК, б) встановлений захищений мовний канал

При використанні комп'ютера з встановленим програмним шлюзом IP-телефонії найбільш реалізованими є атаки:

- атака з проксуванням всього медіарафіка кореспондентів через Sн;
- впровадження програми-шпигуна на комп'ютер.

Перший вид атаки був описаний раніше. Атака з впровадженням програми-шпигуна полягає в установці на термінал користувача програмного забезпечення, яке відправляє голосові дані у відкритому вигляді з терміналу або передає всі вихідні і вхідні пакети з мережевого інтерфейсу термінала користувача на Sн для подальшої обробки. Тоді для доступу до інформації, що передається порушнику може знадобитися вимкнути застосовані на терміналі користувача А протоколи безпеки IP-телефонії, або, як мінімум, змінити режим роботи SRTP, вимкнувши шифрування переданих мультимедійних файлів.

Як правило, IP-телефони і шлюзи мають можливість віддаленого управління, яка використовується самими користувачами для їх налаштування. Обчислювальні пристрої також можуть мати дистанційне керування, організоване внутрішніми засобами застосовуваної операційної системи, або з використанням додаткового програмного забезпечення. Однак, віддалене управління може бути також відключено користувачем, або можливості віддаленого управління можуть бути обмежені за рахунок застосування списків доступу.

Для успішного виконання атаки порушник повинен захопити віддалене управління користувацьким терміналом. В першу чергу успіх атаки залежить від багатьох факторів. Імовірність успішного проведення цього етапу атаки розглядається, як

$$p_{\text{З4Б}} = \begin{cases} 1, \text{якщо у користувацького терміналу включено віддалене управління} \\ \text{і немає налаштованих списків доступу на всі віддалені протоколи} \\ 0, \text{якщо у користувацького терміналу включено віддалене управління} \\ \text{і є налаштовані списки доступу на всі видалені протоколи} \\ 0, \text{якщо у користувацького термінала вимкнено віддалене управління} \end{cases} \quad (2.8)$$

При наявності віддаленого управління, порушнику для проведення атаки потрібно підібрати пароль або пару логін-пароль для авторизації на терміналі користувача [37]. Передбачається, що IP адреса жертви відома порушнику заздалегідь. Підбір паролю або логіна-паролю залежить від протоколу віддаленого управління, на який виконується атака. Імовірність успішного

перебору пароля має сенс оцінювати за кінцевий інтервал часу T, тому що ймовірність успішного перебору пароля за нескінченний час буде дорівнює 1.

Імовірність успішного перебору пароля можна визначити як:

$$p_{45Б} = F(l, D, T, C), \quad (2.9)$$

де $l$ - довжина логіна-паролю;

$T$ - час, протягом якого потрібно завершити перебір;

$D$ - додаткові обмеження протоколу, що ускладнюють виконання перебору пароля, а також технічні можливості порушника;

$C$ - швидкість каналу зв'язку, по якому виконується перебір.

Після успішного перебору пароля і отримання доступу до термінала користувача, порушник з певною ймовірністю може вибрати один з двох можливих шляхів:

- встановлення закладки, модифікація ПО терміналу;
- зміна налаштувань терміналу користувача;
- MITM для всіх протоколів IP-телефонії.

Можливість вибору однієї з двох атак визначається технічною оснащеністю порушника, а також наявністю у нього спеціалізованих інструментів і засобів.

Сенс першої атаки полягає в захопленні голосової інформації в обхід протоколів IP-телефонії, або в виключенні протоколів безпеки IP- телефонії, або в зміні режимів роботи протоколів безпеки IP-телефонії, щоб можна було виконувати прослуховування.

Сенс другої і третьої атаки полягає в зміні налаштувань користувача терміналу для реалізації атаки MITM, при якій всі дані протоколів безпеки проходять через порушника, що дозволяє йому контролювати передані голосові пакети, а також при необхідності виконувати модифікацію переданих даних. Фактично, при даній атаці порушник виконує з'єднання по черзі з кожним з кореспондентів, використовуючи протоколи забезпечення безпеки IP-телефонії, реалізуючи схему, представлену на Рис. 2.6.

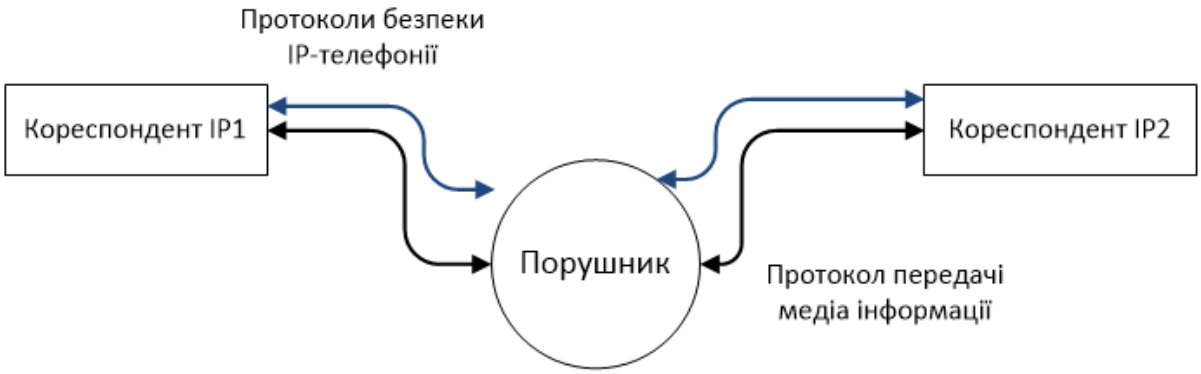


Рис. 2.6 - Реалізація атаки MITM для всіх протоколів забезпечення безпеки VoIP

Вибравши одну з атак, порушник спробує здійснити її для отримання несанкціонованого доступу до інформації, що передається. Однак існує ймовірність неуспішного виконання обраної атаки, яка відображається ймовірностями p72 і p62 відповідно. Наприклад - атака "зміна налаштувань терміналу користувача" може скінчитися неуспішно, якщо користувач помітить змінені налаштування і відновить свої налаштування, змінивши паролі доступу до термінала або відключивши віддалене керування.

Використовуючи можливі алгоритми дій порушника, складено ймовірнісний граф, представлений на Рис. 2.7.

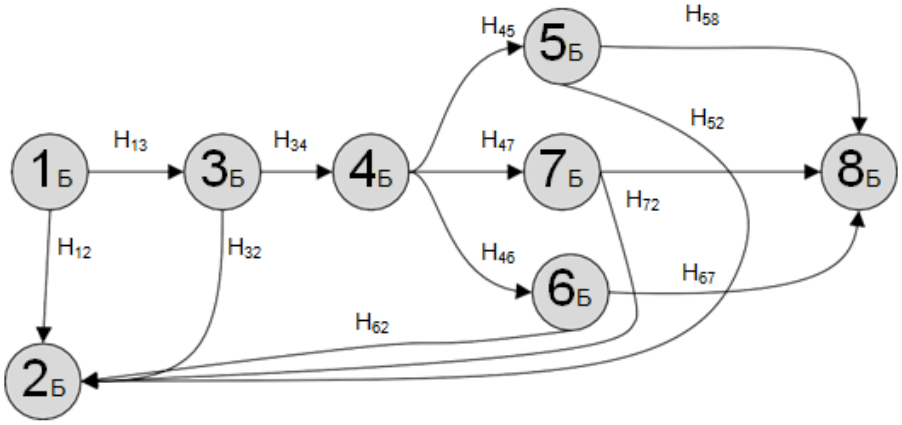


Рис. 2.7 - Ймовірнісний граф захоплення термінала користувача зовнішнім порушником

З графа виділена гілка, що відповіднає успішному виконанню атаки НСД, і складена твірна функція H(x) цієї гілки.

Для графа відповідно до методики, наведеної в [36], представлені

$P_{\text{НСД}} = H(x = 1)$:

$$P_{\text{нсдЦБ}} = p_{13\text{Б}}p_{34\text{Б}}(p_{45\text{Б}}p_{58\text{Б}} + p_{46\text{Б}}p_{68\text{Б}} + p_{47\text{Б}}p_{78\text{Б}}), \quad (2.10)$$

де $p_{ijБ}$ - ймовірність переходу з *i*-й в *j*-ту вершину графа.

### 2.3.2. Внутрішній порушник

#### 2.3.2.1. Захоплення обладнання оператора внутрішнім порушником

Розглянуто модель внутрішнього порушника, завданням якого є досягнення НСД, а вирішується завдання через захоплення обладнання оператора.

У порівнянні із зовнішнім порушником, внутрішній щодо оператора порушник має низку переваг. Він спочатку має певний рівень доступу до обладнання оператора зв'язку, а також може мати можливість встановлення і підключення додаткового обладнання до існуючого обладнання в мережі оператора.

Якщо порушник не має достатнього рівня доступу до обладнання оператора, він може спробувати отримати доступ, виконуючи атаку перебору паролів для отримання більш високого рівня.

Алгоритм дій порушника наведено на Рис. 2.8.

p18B характеризує ймовірність, що у внутрішнього порушника спочатку є доступ достатнього рівня для проведення подальших дій для досягнення несанкціонованого доступу.

Імовірність p18B може бути визначена, як:

$$p_{18\text{B}} = \begin{cases} 1, \text{якщо порушник має достатній рівень доступу} \\ 0, \text{якщо порушник не має достатній рівень доступу} \end{cases} \quad (2.11)$$

p19B відображає ймовірність події, що порушнику вдалося підключити своє додаткове обладнання в мережі оператора на вузол, через який проходить медіа трафік жертви.

$$p_{19\text{B}} = \begin{cases} 1, \text{якщо порушник зміг встановити додаткове} \\ \text{обладнання на вузлі оператора;} \\ 0, \text{якщо порушник не зміг встановити додаткове} \\ \text{обладнання на вузлі оператора;} \end{cases} \quad (2.12)$$

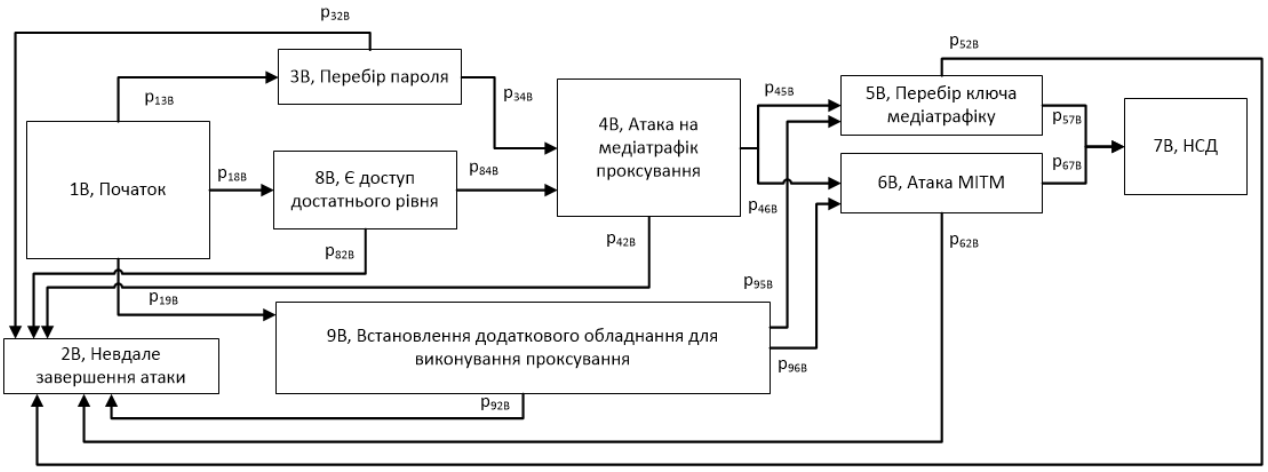


Рис. 2.8 - Можливий алгоритм дій при виконанні захоплення обладнання оператора внутрішнім порушником

Обладнання, що встановлюється спочатку повинно мати функціонал модифікації або віддзеркалення пакетів. З цього кроку порушник може вибирати один з двох шляхів для подальшого проведення атаки. Вибір залежить від технічних можливостей встановленого обладнання. Однак, навіть при установці обладнання порушника є певна ймовірність, що атака може бути проведена неуспішно. Наприклад - це може статися в тому випадку, якщо клієнти почнуть застосовувати додаткові механізми для відстеження вторгнення або додаткові протоколи, використання яких може бути не враховано в обладнанні порушника.

Використовуючи можливі алгоритми дій порушника, складений ймовірнісний граф, представлений на Рис. 2.9.

У графі виділена гілка,що відповідає успішному виконанню атаки НСД і складена твірна функція *H(x)* цієї гілки. Для графа відповідно до методики, наведеної в [36], представлені $P_{НСД}$.

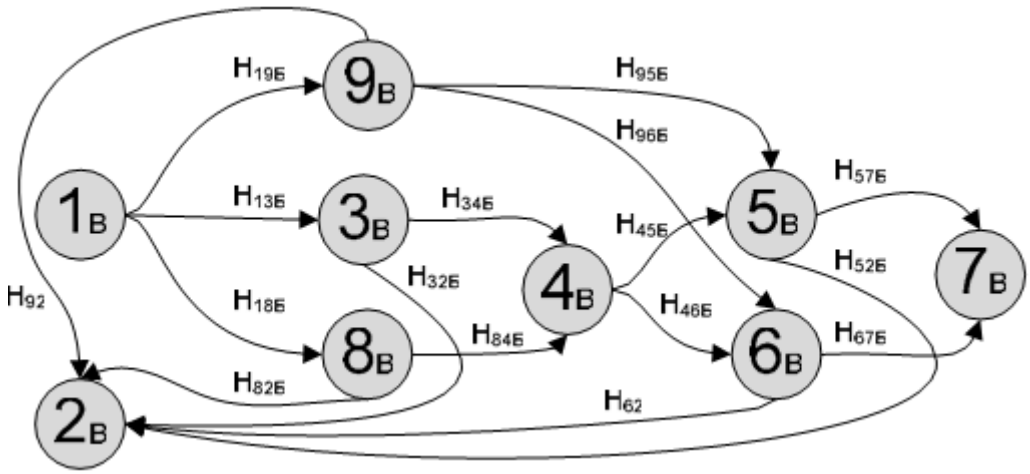


Рис. 2.9 - Ймовірнісний граф - Захоплення обладнання оператора внутрішнім порушником

$$p_{\text{нсдЦВ}} = \big((p_{13\text{В}}p_{34\text{В}} + p_{18\text{В}}p_{84\text{В}})p_{45\text{В}} + p_{19\text{В}}p_{95\text{В}}\big)p_{57\text{В}} + \big((p_{13\text{В}}p_{34\text{В}} + p_{18\text{В}}p_{84\text{В}})p_{46\text{В}} + p_{19\text{В}}p_{96\text{В}}\big)p_{67\text{В}}, \quad (2.13)$$

де $p_{ijX}$ - ймовірність переходу з вершини $i$ в вершину $j$ графа. Тоді ймовірність захисту від атаки НСД матиме вигляд:

$$P_{\text{защ\_нсд\_В}} = 1 - p_{\text{нсдЦВ}} = 1 - \big((p_{13\text{В}}p_{34\text{В}} + p_{18\text{В}}p_{84\text{В}})p_{45\text{В}} + p_{19\text{В}}p_{95\text{В}}\big)p_{57\text{В}} + \big((p_{13\text{В}}p_{34\text{В}} + p_{18\text{В}}p_{84\text{В}})p_{46\text{В}} + p_{19\text{В}}p_{96\text{В}}\big)p_{67\text{В}} \quad (2.14)$$

де $p_{13B}$ - ймовірність вибору атаки перебір пароля для доступу до обладнання оператора;

$p_{18B}$ - ймовірність наявності доступу достатнього рівня до обладнання оператора;

$p_{19B}$ - ймовірність наявності у порушника можливості встановлення додаткового обладнання для здійснення атаки;

$p_{34B}$ - ймовірність успішного завершення атаки перебір пароля для доступу до обладнання оператора;

$p_{45B}$ - ймовірність вибору атаки "злом шифру";

$p_{46B}$ - ймовірність вибору "атака на механізм розподілу ключів"; p57B - ймовірність успішного завершення атаки "злом шифру";

$p_{67B}$ - ймовірність успішного завершення атаки "атака на механізм розподілу ключів";

$p_{95B}$ - ймовірність вибору атаки "злом шифру";

$p_{96B}$ - ймовірність вибору "атака на механізм розподілу ключів".

**2.3.2.2. Захоплення термінала користувача внутрішнім порушником**

Розглянуто модель для внутрішнього порушника, завданням якого є досягнення НСД, а вирішується завдання через захоплення термінала користувача. Алгоритм дій порушника наведено на Рис. 2.10.

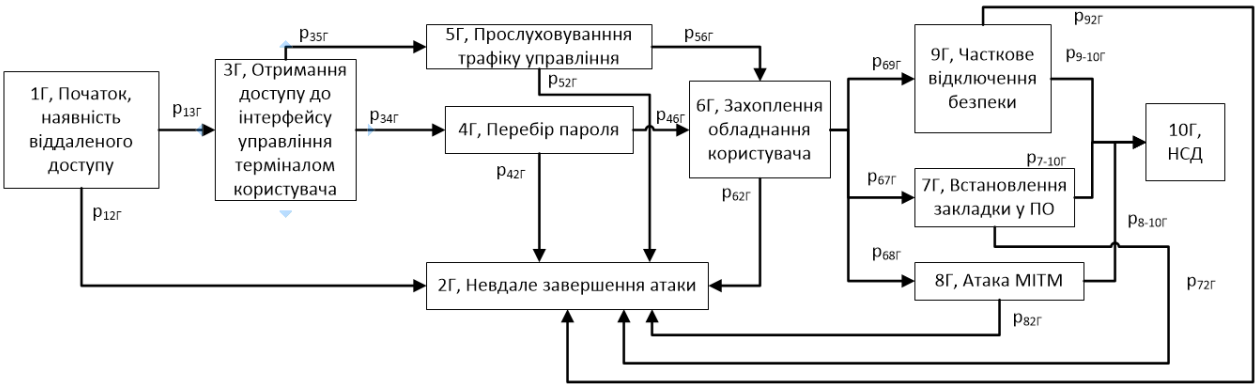


Рис. 2.10 - Можливий алгоритм дій при виконанні захоплення термінала користувача внутрішнім порушником

Використовуючи можливий алгоритм дій порушника, складено ймовірнісний граф, представлений на Рис. 2.11. З графа виділена гілка, що відповідає успішному виконанню атаки НСД, і складена твірна функція H(x) цієї гілки. Для графа відповідно до методики[36] представлена ймовірність успішного завершення атаки НСД - $P_{НСД}$:

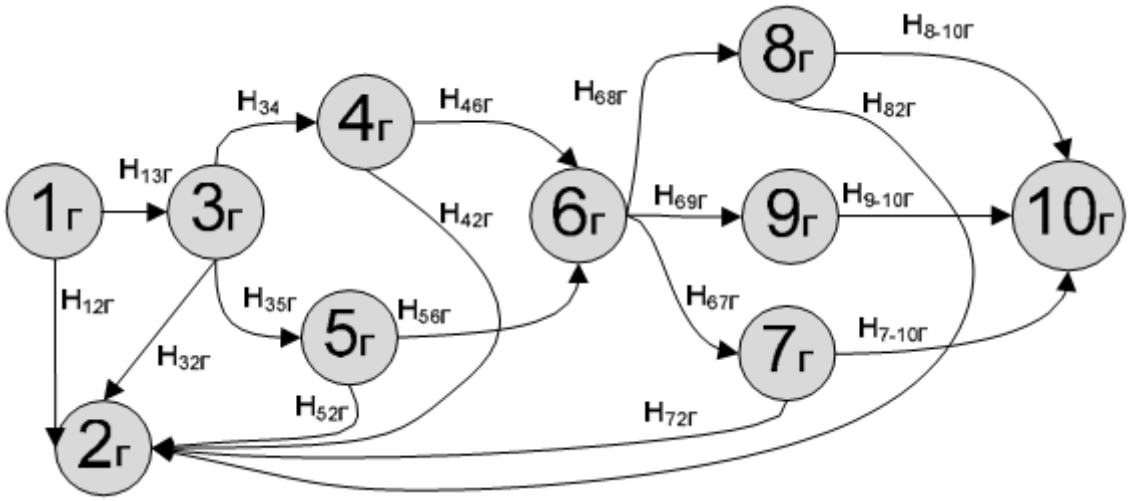

Рис. 2.11 - Ймовірнісний граф - захоплення терміналу користувача внутрішнім порушником

$$P_{\text{нсдЦГ}} = p_{13\text{Г}}(p_{34\text{Г}}p_{46\text{Г}} + p_{35\text{Г}}p_{56\text{Г}})(p_{67\text{Г}}p_{7-10\text{Г}} + p_{68\text{Г}}p_{8-10\text{Г}} + p_{69\text{Г}}p_{9-10\text{Г}}) \quad (2.15)$$

де $p_{ijГ}$ - ймовірність переходу з вершини *i* графа в вершину *j*.

Імовірність захисту від атаки матиме вигляд:

$$P_{\text{зах\_нсд\_Г}} = 1 - P_{\text{нсдЦГ}} = 1 - p_{13\text{Г}}(p_{34\text{Г}}p_{46\text{Г}} + p_{35\text{Г}}p_{56\text{Г}})(p_{67\text{Г}}p_{7-10\text{Г}} + p_{68\text{Г}}p_{8-10\text{Г}} + p_{69\text{Г}}p_{9-10\text{Г}}) \quad (2.16)$$

де $p_{13Г}$ - ймовірність наявності віддаленого підключення;

$p_{34Г}$ - ймовірність вибору атаки "перебору пароля до обладнання користувача";

$p_{46Г}$ - ймовірність успішного перебору пароля до обладнання користувача за обмежений час;

$p_{35Г}$ - ймовірність вибору атаки "отримання пароля до обладнання користувача за рахунок прослуховування трафіку користувача";

$p_{56Г}$ - ймовірність успішного завершення атаки "перехоплення пароля до обладнання користувача за рахунок прослуховування трафіку управління";

$p_{68Г}$ - ймовірність вибору атаки MITM для всіх протоколів VoIP;

$p_{8\text{-}10Г}$ - ймовірність успішного завершення атаки MITM для всіх протоколів VoIP;

$p_{67Г}$ - ймовірність вибору атаки "встановлення закладки на терміналі користувача";

$p_{7\text{-}10Г}$ - ймовірність успішного завершення атаки "встановлення закладки на терміналі користувача або відключення безпеки".

$p_{6\text{-}9Г}$ - ймовірність вибору атаки "повне або часткове відключення безпеки";

$p_{9\text{-}10Г}$ - ймовірність успішного завершення атаки "повне або часткове відключення безпеки".

Значення багатьох ймовірностей, що входять в формулу, вимагають експертної оцінки і не можуть бути обчислені. Також значення цих ймовірностей залежать від порушника, його можливостей, а також додаткових обставин.

### 2.4. Оцінка ймовірності успішного завершення атаки

Для кожного з розглянутих графів відповідно до методики, наведеної в [36], наведені $P_{НСД}$:

$$P_{\text{нсдЦА}} = p_{13\text{А}}p_{34\text{А}}(p_{45\text{А}}p_{57\text{А}} + p_{46\text{А}}p_{67\text{А}}) \quad (2.17)$$

$$P_{\text{нсдЦБ}} = p_{13\text{Б}}p_{34\text{Б}}(p_{45\text{Б}}p_{58\text{Б}} + p_{46\text{Б}}p_{68\text{Б}} + p_{47\text{Б}}p_{78\text{Б}}) \quad (2.18)$$

$$P_{\text{нсдЦВ}} = \big((p_{13\text{В}}p_{34\text{В}} + p_{18\text{В}}p_{84\text{В}})p_{45\text{В}} + p_{19\text{В}}p_{95\text{В}}\big)p_{57\text{В}} + \big((p_{13\text{В}}p_{34\text{В}} + p_{18\text{В}}p_{84\text{В}})p_{46\text{В}} + p_{19\text{В}}p_{96\text{В}}\big)p_{67\text{В}} \quad (2.19)$$

$$P_{\text{нсдЦГ}} = p_{13\text{Г}}(p_{34\text{Г}}p_{46\text{Г}} + p_{35\text{Г}}p_{56\text{Г}})(p_{67\text{Г}}p_{7-10\text{Г}} + p_{68\text{Г}}p_{8-10\text{Г}} + p_{69\text{Г}}p_{9-10\text{Г}}) \quad (2.20)$$

де $p_{ijX}$ - ймовірність переходу з вершини *i* в вершину *j* відповідного графа.

$$P_{\text{нсд}} = \max\{P_{\text{нсдЦА}}, P_{\text{нсдЦБ}}, P_{\text{нсдЦВ}}, P_{\text{нсдЦГ}}\} \quad (2.21)$$

Очевидно, в разі встановлення з'єднання в сценарії кореспондент-кореспондент без сервера і при відсутності попередньо розподіленого ключового матеріалу, сам користувач є найбільш зацікавленою особою для підвищення безпеки і зниження $P_{НСД}$. При цьому користувач може застосовувати VoIP термінал, що підтримує функцію відключення віддаленого управління, що призведе до $p_{13Б} = 0$, $p_{13Г} = 0$, і, як наслідок, $P_{нсдЦБ} = 0$, $P_{нсдЦГ} = 0$.

Однак, користувач не може впливати на ймовірності $p_{ijA}$, $p_{ijB}$. Залежно від проміжних цілей порушника виділяється кілька приватних моделей порушників, представлених в Табл. 2.1.

Слід зауважити, що $p_{57A}$, $p_{57B}$ залежать від застосовуваного алгоритму шифрування. Існуючі рекомендації SRTP передбачають застосування алгоритму AES с ключем 128 або 256 біт. Злом такого алгоритму є вкрай малоймовірним [38]. Тому найбільш вірогідним буде вибір атаки MITM на ПРК з боку порушника. Отже, можна ввести допущення, що ймовірність вибору

атаки на шифр $p_{45A} = 0$, $p_{45B} = 0$, а ймовірність вибору атаки MITM $p_{46A} = 1$, $p_{46B} = 1$.

Тоді ймовірність успішної атаки НСД матиме вигляд:

$$P_{\text{нсд}} = \max\{ P_{\text{нсдЦА}}, P_{\text{нсдЦВ}}\} \quad (2.22)$$

$$P_{\text{нсдЦА}} = p_{13\text{A}} p_{34\text{A}} p_{46\text{A}} p_{67\text{A}} \quad (2.23)$$

$$P_{\text{нсдЦВ}} = \big((p_{13\text{B}} p_{34\text{B}} + p_{18\text{B}} p_{84\text{B}}) p_{46\text{B}} + p_{19\text{B}} p_{96\text{B}}\big) p_{67\text{B}} \quad (2.24)$$

Залежно від проміжних цілей і можливостей також виділяється кілька порушників (В1, В2, В3, А4), представлених в Табл. 2.1.

Підставивши значення $p_{ijX}$ з таблиці в формули 2.23,2.24 отримуємо:

$$P_{\text{нсдВ1}} = p_{34\text{B}} p_{67\text{B}} \quad (2.25)$$

$$P_{\text{нсдВ2}} = p_{84\text{B}} p_{67\text{B}} \quad (2.26)$$

$$P_{\text{нсдВ3}} = p_{67\text{B}} \quad (2.27)$$

$$P_{\text{нсдА4}} = p_{34\text{A}} p_{67\text{A}} \quad (2.28)$$

$$P_{\text{НСД}} = \max\{ P_{\text{нсдВ1}}, P_{\text{нсдВ2}}, P_{\text{нсдВ3}} P_{\text{нсдА4}}\} \quad (2.29)$$

*Таблиця 2.1*

Ймовірності атак в залежності від цілей порушника

| Цільова функція | Модель | Цілі порушників |
|---|---|---|

| | | B1) Атака внутрішнього порушника через захоплення обладнання оператора за рахунок перебору пароля і організація MITM | B2) Атака внутрішнього порушника при наявності у нього доступу до обладнання шляхом організації MITM | B3) Атака внутрішнього порушника через установку додаткового обладнання на вузлі оператора шляхом організації MITM | A4) Атака зовнішнього порушника через захоплення обладнання оператора за рахунок перебору пароля |
|---|---|---|---|---|---|
| p13B - ймовірність вибору атаки "перебір пароля для доступу до обладнання оператора " | 0..1 | 1 | 0 | 0 | - |
| p18B - ймовірність наявності доступу достатнього рівня до обладнання оператора | 0..1-$p_{13B}$ | 0 | 1 | 0 | - |
| p19B - ймовірність наявності у порушника можливості установки додаткового обладнання на вузлі оператора зв'язку для виконання атаки | 0..1 - $p_{18B}$- $p_{13B}$ | 0 | 0 | 1 | - |
| p34A, p34B - ймовірність успішного завершення атаки перебір пароля для управління обладнанням оператора | 0..1 | 0..1 | - | - | 0..1 |
| p84B - ймовірність використання порушником наявного доступу достатнього рівня до обладнання оператора | 0..1 | - | 0..1 | - | - |
| p46A, p46B - ймовірність вибору "атаки MITM на ПРК і інші протоколи безпечної IP- телефонії" | 0..1-$p_{45A}$ 0..1-$p_{45B}$ | 1 | 1 | - | 1 |
| p67A, p67B - ймовірність успішного завершення "Атаки MITM на ПРК і інші протоколи безпечної IP-телефонії" | 0..1 | 0..1 | 0..1 | 0..1 | 0..1 |
| p96B - ймовірність вибору "атаки MITM на ПРК і інші протоколи безпечної IP-телефонії " | 0..1-$p_{95B}$ | - | - | 1 | - |
| p13A - ймовірність наявності можливості віддаленого підключення до обладнання оператора | 0 або 1 | - | - | - | 1 |

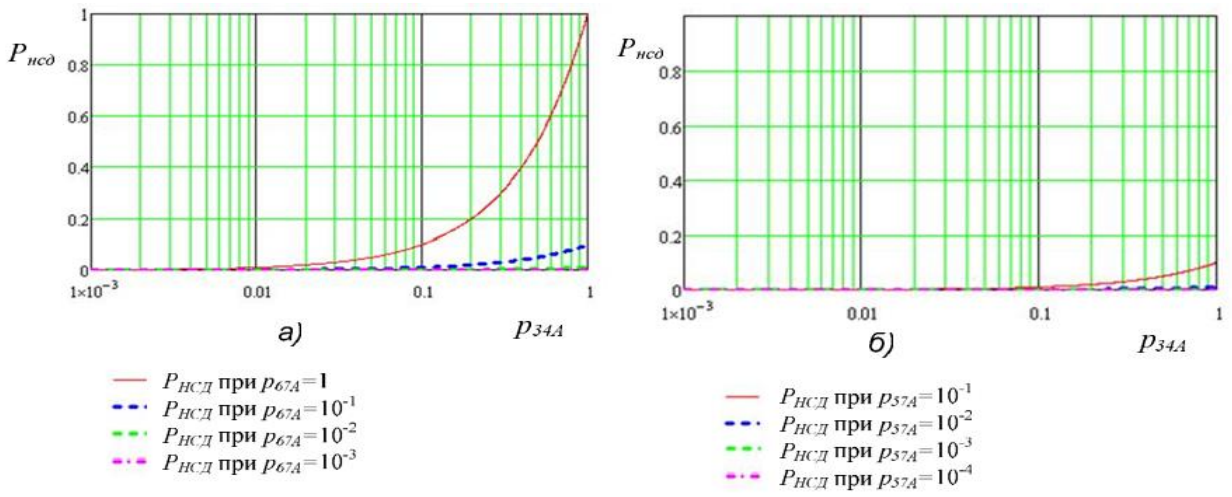


Рис. 2.12 - Залежність $P_{НСД}$ для моделі - захоплення обладнання оператора зовнішнім порушником а) при виборі MITM б) при виборі атаки на шифр

Очевидно, що $P_{нсдВ3}$ більше або дорівнює $P_{нсдВ1}$, $P_{нсдВ2}$, $P_{нсдА4}$. Отже, $P_{НСД}$ буде визначатися величиною $p_{67B}$, яка буде відповідати атаці НСД внутрішнього порушника на вузлі оператора зв'язку за допомогою встановлення додаткового обладнання для організації MITM. Тому, доцільно скоротити $p_{67B}$, забезпечуючи захист від порушника, націленого на MITM. Графік залежності $P_{НСД}$ для моделі захоплення обладнання оператора зовнішнім порушником наведено на Рис. 2.12.

## 2.5. Висновки

Було наведено визначення порушника і опис терміналу користувача. Показана сукупність атак, які може виконувати порушник для досягнення несанкціонованого доступу. Представлено математичну модель активного порушника для захищеної IP-телефонії, що враховує можливості цього порушника реалізувати атаку MITM на ПРК і інші атаки. Модель дозволяє розрахувати ймовірність успішної атаки, націленої на НСД, в залежності від значень ймовірностей проміжних атак. Наведено окремі моделі порушників в залежності від обраних цілей, можливостей і місця розташування порушника.

Для боротьби з порушником, який поставив за мету захопити управління обладнанням користувача, необхідно виконувати всі рекомендації щодо забезпечення безпеки під час налаштування обладнання, а саме, блокувати

віддалене управління з нелегітимних і інших мереж, або відключати віддалене управління.

Наведено оцінку ймовірності вибору кожним з приватних порушників певних проміжних цілей при реалізації атаки. Показані можливі дії користувача для захисту від атак, а також визначена найбільш небезпечна для користувача атака MITM на протокол забезпечення безпеки IP- телефонії, яка також є найкращою для порушника.

Показано, що особливу небезпеку становить зовнішній і внутрішній порушники, які виконують атаку на обладнання оператора. Представлена імовірнісна модель такого порушника. Показано, що найбільш небезпечною є атака MITM на протоколи розподілу ключового матеріалу.

# Розділ 3. РОЗРОБКА ПРОПОЗИЦІЙ ЩОДО ВДОСКОНАЛЕННЯ ПРОТОКОЛІВ РОЗПОДІЛУ КЛЮЧІВ

Для дослідження ймовірносно-часових характеристик необхідно розглянути протоколи розподілу ключів захищеної IP-телефонії, що відповідають вимогам до ПРК, описаних в першому розділі:

$К_1$. Підтримка топологій клієнт-сервер і клієнт-клієнт;

$К_2$. Самодостатність (функціонування без застосування додаткових протоколів між кореспондентами для реалізації функції розподілу ключів);

$К_3$. Робота без передачі ключа у відкритому вигляді по каналу зв'язку;

$К_4$. Наявність механізму виявлення MITM без заздалегідь розподіленого ключового матеріалу між кореспондентами, а також без використання сертифікатів;

$К_5$. Використання TCP / UDP портів, що застосовуються для IP-телефонії (SIP / RTP), або TCP / UDP портів, використання яких узгоджено в результаті встановлення з'єднання;

У разі виконання вимоги, $K_i = 1$. В іншому випадку $K_i = 0$.

Порівняння протоколів приведено в Табл. 3.1.

*Таблиця 3.1*

Оцінка ПРК на відповідність вимогам

| Опис вимоги до ПРК | Протоколи | | | |
|---|---|---|---|---|
| | DTLS | ZRTP | SDES | MIKEY |
| $К_1$ | 1 | 1 | 0 | 1 |
| $К_2$ | 1 | 1 | 0 | 0 |
| $К_3$ | 1 | 1 | 0 | 1 |
| $К_4$ | 0 | 1 | 0 | 0 |
| $К_5$ | 1 | 1 | 1 | 1 |
| $Q_{ПРК}$ | 4 | 5 | 1 | 3 |

Оцінка кожного з протоколів проводиться відповідно до функції $Q_{ПРК}$:

$$Q_{\text{ПРК}} = \sum_{i=5}^{5} K_i \quad (3.1)$$

Протокол DTLS не задовільняє четверту вимогу, представлену в Табл. 3.1, так як розроблявся для роботи в топології клієнт - сервер і використовує

попередньо встановлені сертифікати для захисту від MITM у обох кореспондентів. Тому для DTLS К4 = 0.

На відміну від інших протокол ZRTP має вбудований механізм SAS (Short Authentication String) для захисту від MITM. Тому для ZRTP К4 = 1. Для SDES і MIKEY К4 = 0.

Протокол MIKEY не задовольняє другу вимогу з Табл. 3.1, так як повідомлення протоколу можуть передаватися або в SIP / SDP-повідомлення, або поверх RTSP (Real Time Streaming Protocol), але в останньому випадку кореспонденти повинні додатково підтримувати протокол RTSP. Тому К2 = 0 для MIKEY.

П'ята вимога при роботі поверх RTSP протоколу не виконується, але при цьому виконується друга вимога. При роботі MIKEY поверх в SIP / SDP-повідомлення П'ята вимога виконується, але не виконується друга вимога. Так як при оцінці QПРК використовується К2 = 0, то К1 = 1 для MIKEY.

Протокол SDES не задовольняє першу і третью вимоги (К1 = 0 і К3 = 0), так як ключ передається між кореспондентами в явному вигляді в повідомленнях SDP і вимагає їх додаткового захисту. Для захисту як правило використовується додатковий протокол SIPS. Однак, при з'єднанні клієнт-клієнт, коли у кореспондентів немає заздалегідь розподіленого ключового матеріалу, SIPS з'єднання з захистом від MITM організувати неможливо. Протокол SDES не задовольняє другу вимогу, так як для передачі даних протокола SDES використовуються повідомлення SIP / SDP. Відповідно К2 = 0 для SDES.

Виходячи з Табл. 3.1, в більшій мірі наведеним вимогам відповідають протоколи ZRTP і DTLS, що мають найбільше значення QПРК. Оцінка ЙЧХ виконується для цих протоколів.

Результати проведених досліджень показують, що відомі протоколи розподілу ключів необхідно вдосконалювати в двох напрямках:

1) підвищення безпеки;

2) покращення ЙЧХ протоколів.

У розділі 2 показано, що найбільш небезпечною атакою є атака MITM на протокол розподілу ключів.

Одним із шляхів підвищення безпеки протоколу є зниження ймовірності вторгнення порушника до протоколу вироблення ключового матеріалу за рахунок використання декількох незалежних каналів зв'язку. Таким чином, використовувані в протоколі канали зв'язку повинні відповідати вимозі - не мати спільних точок, контролюючи які, порушник може одночасно атакувати використовувані канали.

В даному розділі проводиться дослідження ймовірності успішного вторгнення порушника в канали зв'язку, що використовуються під час виконання протоколу, а також успішного розподілу загального ключа. Зокрема, описується метод підвищення безпеки ZRTP за рахунок автоматичної перевірки аутентифікаційного рядка.

### 3.1. Метод підвищення безпеки ZRTP за рахунок автоматичної перевірки автентифікаційного рядка

Протокол Діффі-Хелмана може бути повністю скомпрометований активним зловмисником. Тому при роботі протоколу необхідно забезпечити справжність вихідних даних [42]. З цієї причини протокол обміну ключами Діффі-Хелмана зазвичай застосовують по захищеному каналу передачі даних [43], в якому неможливо виконати підміну переданих повідомлень, або при використанні сертифікатів [44] або довіреного центра сертифікації, якому довіряють обидва кореспондента для цілей аутентифікації.

У разі необхідності встановити захищене з'єднання між двома кореспондентами, вони, по-перше, можуть не мати спільних сертифікатів (тобто сертифікатів, що мають один і той же кореневий довірений центр), не мати загальний довірений центр сертифікації або розподілу ключів, а також можуть не мати захищений канал зв'язку між собою.

При наявності у кореспондентів сертифікатів, підписаних різними центрами сертифікації, неможливо перевірити справжність сертифікату, так як кожен з кореспондентів може не довіряти центру сертифікації респондента.

Для організації захищеного з'єднання між кореспондентами також потрібно виконати розподіл ключового матеріалу для цього з'єднання. Кореспонденти можуть використовувати симетричне або асиметричне шифрування. При використанні симетричного шифрування - один з кореспондентів повинен передати іншому секретний ключ. Якщо цей ключ стане відомим порушнику - передані в процесі сеансу зв'язку повідомлення будуть розшифровані порушником. При використанні асиметричного шифрування - інформація не буде прочитана порушником навіть в разі перехоплення повідомлень. Однак - при обміні ключами для організації захищеного з'єднання у кореспондентів не буде можливості упевнитися - що відкритий ключ передається між ними без модифікації порушником, як представлено на Рис. 3.1.

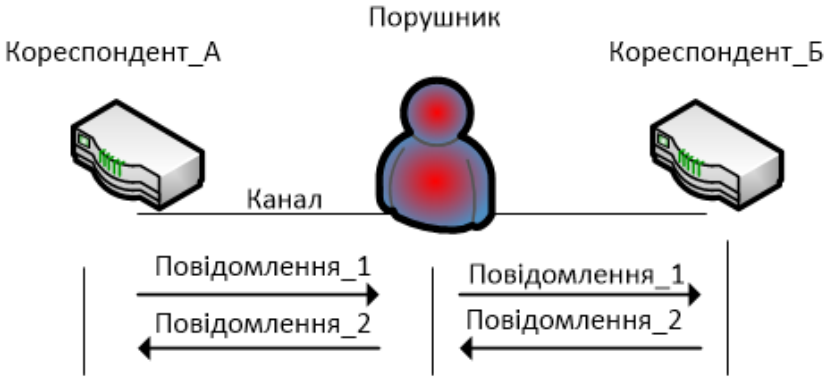


Рис. 3.1 - MITM при використанні асиметричного шифрування

Також варто відзначити, що відкритий і закритий ключі мають велику довжину і їх передача між кореспондентами в словесному або письмовому вигляді ускладнена.

Для підвищення безпеки пропонується використовувати два методи:

- підвищення безпеки за рахунок автоматизації перевірки аутентифікаційного рядка по другому каналу зв'язку;
- використання двох і більше каналів зв'язку для виконання протоколу розподілу ключів.

Захист від порушника в режимі клієнт-клієнт виконується за рахунок перевірки автентифікаційного рядка, який передається по голосовому каналу в

ручному режимі. Голосовий канал в цьому випадку є додатковим каналом зв'язку по відношенню до IP-каналу. Доцільно автоматизувати процес перевірки SAS. Існуючий метод не безпечний, тому що використовується один канал зв'язку, а сучасні засоби аналізу і синтезу мови дозволяють виконувати автоматичне вирізання рядка і заміну на рядок, синтезований порушником.

Проведене практичне дослідження показало, що існує висока ймовірність наявності між кореспондентами незалежних непересічних маршрутів при використанні декількох каналів зв'язку. В основі пропонованих протоколів використана перевага легітимних кореспондентів над нелегітимними, що полягає в тому, що тільки легальні кореспонденти можуть отримувати повідомлення з двох і більше каналів зв'язку одночасно, володіючи знаннями про IP-адреси кореспондентів, при цьому ця інформація не є секретною для порушника. Слід зазначити, що метод модернізації протоколів розподілу ключів розглядається, як підвищення безпеки, але при цьому не забезпечує 100% достовірність.

Розглядаються кілька можливих варіантів модернізації протоколу розподілу ключів при використанні двох або трьох каналів зв'язку. В якості критеріїв оцінки використовуються величини наступних ймовірностей:

- ймовірність успішної атаки MITM PУA;
- ймовірність виявлення атаки MITM POH;
- ймовірність успішної генерації загального секрету РУК.

Протокол ZRTP має механізм захисту від MITM, виражений у вербальній перевірці короткого автентифікаційного рядка SAS по мовному каналу між обома кореспондентами. Це означає, що після виконання протоколу ZRTP і встановлення мовного каналу в топології клієнт-клієнт без сервера кореспонденти отримують значення SAS - обчислений текстовий рядок з комбінації символів.

*SAS = f (hash (Hello респондента || Commit || DHPart1 || DHPart2).*

Один з кореспондентів вимовляє аутентифікаційний рядок по встановленому мовному каналу. Другий кореспондент звіряє SAS на своєму

терміналі зі значенням, отриманим по мовному каналу. Якщо SAS збігаються, значить, не має місце атака MITM, або має місце атака з підробкою SAS по мовному каналу зв'язку. Якщо SAS розрізняються - значить, має місце атака MITM у каналі передачі даних. Таким чином, при з'єднанні двох кореспондентів без участі сервера - автентифікація виконується за рахунок знання кореспондентом голосу другого кореспондента, а також за рахунок неспотвореної передачі інформації по двох каналах - по мовному каналу SRTP і каналу передачі даних.

Сучасні технології досить просто дозволяють виконувати як аналіз голосу кореспондентів, так і синтез мови, в тому числі, синтез мови для цілей підробки голосу. Розглядаються два варіанти:

1. Кореспонденти знають голос один одного.

2. Кореспонденти не знають голос один одного.

У першому випадку, при з'єднанні викликає кореспондент,що викликає, як правило, вимовляє привітання і ім'я викликаємої сторони. Після цього виконується вербальна перевірка SAS. Зібраних голосових даних може бути достатньо для синтезу мови кореспондента для заміни одних слів на інші з метою підміни SAS в голосовому каналі. В цьому випадку - перевірка SAS пройде успішно навіть при наявності атаки MITM (Рис. 3.2).

У другому випадку, коли кореспонденти не знають голос один одного, не потрібно збору даних, так як синтез можна виконувати з використанням будь-якого голосу.

В якості модернізації протоколу ZRTP пропонується додавання автоматизованої перевірки аутентифікаційного рядка SAS. При використанні двох і більше каналів зв'язку, перевірка дозволить виявити порушника.

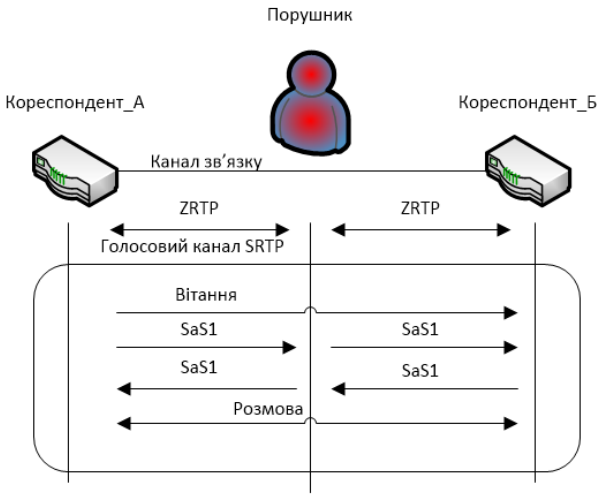


Рис. 3.2 - Порушник, який виконує заміну SAS в голосовому каналі зв'язку

Інформація про IP-адреси може бути передана між кореспондентами по телефону, по електронній пошті, при особистій зустрічі, листом і іншими доступними способами. Відмінною особливістю є те, що інформація про IP-адреси не є секретною інформацією для порушника і може бути передана по відкритих каналах зв'язку, в той час, як пароль для симетричного шифрування є секретним і розголошення призведе до можливості порушника дешифрувати передану інформацію. У порівнянні з довжиною асиметричного ключа, загальна довжина двох IPv4 або IPv6 адрес набагато менше. При перехопленні асиметричного ключа - порушник може відправляти дані легітимному респонденту так само, як і легітимний кореспондент.

При використанні IP-адрес додатковим заходом для підвищення безпеки є перевірка IP-адрес відправника повідомлень респондентом, а також можливість отримання всіх повідомлень, відправлених по двох каналах зв'язку, тільки легітимними респондентами при відсутності атаки MITM одночасно в декількох каналах.

Даний метод підвищення безпеки ZRTP вимагає передачі всього одного повідомлення від кожного з кореспондентів по додатковому каналу зв'язку. В якості другого каналу зв'язку може виступати не обов'язково канал передачі даних, але і SMS, MMS транспорт.

Особливістю підходу також є невисока складність розробки програмної реалізації протоколу за рахунок використання існуючих бібліотек [39, 40]. Значення SAS передається в додаток за результатами виконання протоколу ZRTP. Досить додатково передати цей параметр кореспонденту по другому каналу зв'язку у відкритому або зашифрованому вигляді для реалізації автоматичної перевірки.

Недоліком методу підвищення безпеки у вигляді автоматизації перевірки SAS є виявлення порушника в каналі зв'язку безпосередньо після успішного виконання протоколу, а не під час виконання.

Для оцінки можливості застосування декількох каналів зв'язку для цілей підвищення безпеки необхідно вирішити такі завдання:

- оцінити ймовірність наявності загальної точки в двох і більше каналах зв'язку при використанні різних операторів зв'язку між кореспондентами;
- розробити алгоритм прийняття рішення про наявність порушника і оцінка ймовірності помилки можливих рішень.

Пропонується використовувати наступний алгоритм автоматичної перевірки SAS. Кореспонденти A і B виконують попередній обмін інформацією про IP-адреси $IP_{A1}$, $IP_{A2}$, $IP_{B1}$, $IP_{B2}$, де $IP_{A1}$, $IP_{A2}$ - адреси кореспондента A, $IP_{B1}$, $IP_{B2}$ - адреси кореспондента B, а також налаштовують таблицю маршрутизації. Для встановлення захищеного з'єднання, кореспонденти A і B, виконують протокол ZRTP через канал зв'язку $IP_{A1}$ - $IP_{B1}$, в результаті чого кожен обчислює значення SAS (Рис. 3.3). Кореспондент A відправляє $SAS_A$ по каналу зв'язку $IP_{A2}$ - $IP_{B2}$ кореспонденту B. Кореспондент B отримує $SAS_A'$. Кореспондент B відправляє $SAS_B$ по каналу зв'язку $IP_{A2}$ - $IP_{B2}$ кореспонденту A. Кореспондент A отримує $SAS_B'$.

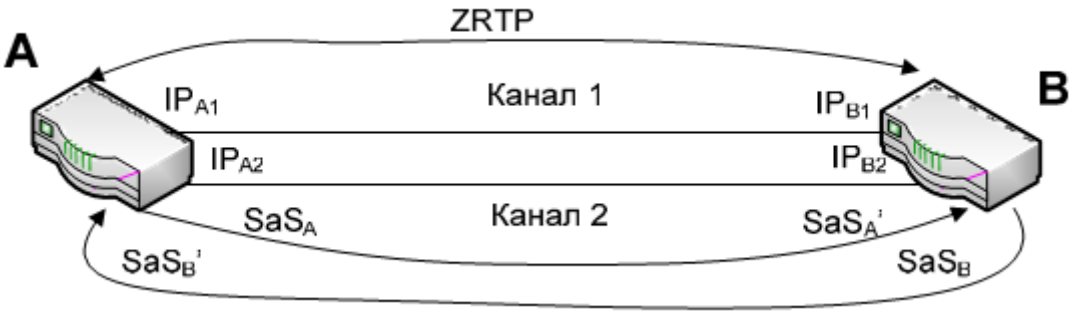


Рис. 3.3 - Механізм автоматичної перевірки SAS

Кореспондент B виконує порівняння $SAS_A'$ і $SAS_B$. Якщо вони збігаються - значить відсутній активний порушник в двох каналах зв'язку, або присутній один і той же активний порушник одночасно в двох каналах зв'язку. Якщо значення SAS не збігаються, кореспондент B отримує повідомлення від терміналу про наявність порушника в каналі зв'язку.

Кореспондент A виконує порівняння $SAS_A$ і $SAS_B'$. Якщо вони збігаються- значить відсутній активний порушник в двох каналах зв'язку, або присутній один і той же активний порушник одночасно в двох каналах зв'язку. Якщо значення SAS не збігаються, кореспондент A отримує повідомлення від терміналу про наявність порушника в каналі зв'язку.

Фактично - протокол дозволяє виявити наявність активного порушника, який працює в одному з двох каналів зв'язку.

Виконується розрахунок ймовірностей подій: $P_{УА}$, $P_{ВП}$, $P_{УК}$.

Під успішною атакою розуміється подія, що порушник успішно реалізував атаку MITM, виконавши обмін ключами з обома кореспондентами при використанні декількох каналів зв'язку, не виявивши себе при проведенні атаки. Це можливо лише в одному випадку, якщо один і той же порушник може контролювати всі використовувані кореспондентами канали зв'язку і виконувати синхронну модифікацію переданих повідомлень в кожному з каналів зв'язку. Імовірність успішної атаки $P_{УА\_SAS}$ для протоколу с автоматичною перевіркою SAS відповідає ймовірності події, що порушник

може прослуховувати і виконувати модифікацію повідомлень в двох каналах зв'язку одночасно.

$$P_{УА2\_SAS} = (P_{З1К})^2 \quad (3.1)$$

Під подією виявлення порушника визначається подія, що порушник виявлений кореспондентами в одному з використовуваних каналів зв'язку. Виявлення порушника дозволяє користувачам визначити, що може бути вироблений компрометований ключ, який дозволить порушнику дешифрувати і прослуховувати передану інформацію, а також виконувати модифікацію переданих повідомлень.

Ймовірність виявлення порушника РВП_SAS для протоколу с автоматичною перевіркою SAS відповідає ймовірності знаходження порушника в одному каналі зв'язку при відсутності порушника в іншому каналі зв'язку.

Нехай сеанс ZRTP виконується по першому каналу зв'язку.

Імовірність наявності порушника в першому каналі зв'язку при відсутності порушника в другому каналі зв'язку матиме вигляд:

$$P_{ПОР1К\_НІ\_ПОР2К} = (1 - P_{З1К})P_{З1К} \quad (3.2)$$

Імовірність наявності порушника в другому каналі зв'язку при відсутності порушника в першому каналі зв'язку буде визначатися по аналогії з 3.2.

$$P_{ВП\_SAS} = 2(1 - P_{З1К})P_{З1К} \quad (3.3)$$

Під подією успішного вироблення ключа розуміється, що порушник не виявлений ні в одному з каналів зв'язку і кореспонденти виробляють ключ для подальшої роботи і шифрування переданих даних. Подія можлива тільки в разі, якщо порушника немає ні в одному з каналів зв'язку.

Імовірність успішного вироблення ключа $Р_{УК\_SAS}$ для протоколу с автоматичною перевіркою SAS відповідає вірогідності відсутності порушника в обох каналах зв'язку. Імовірність відсутності порушника в одному каналі зв'язку $Р_{НЕМ\_ПОР}$ має вигляд:

$$P_{НЕМ\_ПОР} = 1 - P\_З1К \quad (3.4)$$

Тоді:

$$P_{\text{УК\_SAS}} = P_{\text{НЕМ\_ПОР}}{}^{2} = (1 - P_{\text{З1К}})^{2} \quad (3.5)$$

Однак, протокол з автоматичною перевіркою SAS не дозволяє визначити, який саме з каналів зв'язку атакує порушник. Також наявність порушника визначається тільки при повному виконанні протоколу і не може бути детермінована протягом виконання протоколу. З цієї причини - слід розглянути додаткові варіанти модернізації протоколу ZRTP, в тому числі варіанти, позбавлені вище описаних недоліків.

### 3.2. Висновки

Запропоновано метод підвищення безпеки ПРК, що відрізняється від існуючого методу вербальної перевірки SAS автоматизацією процесу виявлення порушника, не потребує участі користувачів.

## Розділ 4. ДОСЛІДЖЕННЯ ЙМОВІРНОСНО-ЧАСОВИХ ХАРАКТЕРИСТИК ПРОТОКОЛІВ IP-ТЕЛЕФОНІЇ

## 1.1. Методика оцінки ймовірнісно-часових характеристик протоколів розподілу ключів захищеної IP-телефонії

Огляд протоколів безпеки VoIP показує, що практично будь-який протокол можна представити у вигляді сукупності повідомлень і сукупності фаз, спрямованих на виконання кінцевої мети протоколу. Виділяються два можливих варіанти завершення протоколу - успішне завершення і неуспішне завершення.

Успішним називається таке завершення протоколу, при якому досягається мета ініціалізації протоколу. Наприклад - для протоколів розподілу ключів IP-телефонії успішним вважається завершення, якщо кореспонденти в результаті виконання протоколу отримали ключовий матеріал для роботи SRTP. Неуспішним називається завершення протоколу, при якому не досягається кінцева мета протоколу. Стосовно до ПРК IP- телефонії - неуспішним вважається завершення, якщо кореспонденти не погодили ключі для роботи SRTP.

Як правило, будь-який протокол можна розділити на логічні частини - фази. Фази різних протоколів можна описати з використанням примітивів. Слід зауважити, що для багатьох протоколів безпеки IP-телефонії передбачена повторна передача повідомлень в тих випадках, коли повідомлення не вдалося доставити до респондента, або не отримано повідомлення, що підтверджує прийом повідомлення. Дану особливість необхідно враховувати при оцінці ймовірносно-часових характеристик.

При аналізі протоколу має сенс оцінювати такі ймовірносно- часові характеристики (ЙЧХ), як середній час виконання протоколу і ймовірність успішного завершення [45, 46]. Дані характеристики оцінюються при заданих початкових умовах, при яких виконується протокол.

Для аналізу ЙЧХ вважається, що повідомлення протоколу передаються в дискретному каналі без пам'яті (ДКБП), параметром якого є швидкість $c$, ймовірність побутової помилки $p_0$, а також затримка $d$. Для кількісної оцінки

ЙЧХ протоколів пропонується використовувати метод ймовірносних графів [46, 47].

Суть методу полягає в тому, що будь-який процес з кінцевим числом станів можна описати імовірнісним графом, гілки якого характеризуються твірними функціями (ТФ), аргументом яких є $p_{ij}$ - імовірність переходу з *i*-ї в *j*-у вершину, а час *t* - параметром, що визначає процес.

Розглядається простий процес передачі повідомлення від одного кореспондента іншому. Нехай *n* - довжина пакета в бітах. Тоді ймовірність успішної передачі пакету $p_{pkt\_success}$, матиме вигляд:

$$p_{pkt\_success} = (1 - p_0)^n \quad (4.1)$$

Ймовірність, що пакет з n біт передано з помилкою, буде мати вигляд:

$$p_{pkt\_loss} = 1 - (1 - p_0)^n \quad (4.2)$$

Наведений вище процес описується ймовірнісним графом, представленим на рисунку 4.1, де f1, f2 - твірні функції гілок.

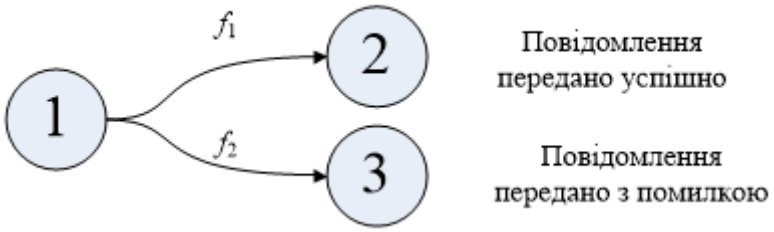


Рис. 4.1 - Граф передачі повідомлення від одного кореспондента до іншого

Нехай t - час передачі пакета по каналу зв'язку. Він визначається формулою 4.3:

$$t = \frac{n}{c} + d, \quad (4.3)$$

де *c* - швидкість каналу зв'язку, біт / с;

*d* - затримка в каналі зв'язку, с.

ТФ для гілки 1-2 матиме вигляд:

$$f_1(x) = (1 - p_0)^n x^{\frac{n}{c}+d} \quad (4.4)$$

ТФ для гілки 1-3:

$$f_2(x) = (1 - (1 - p_0)^n)x^{\frac{n}{c}+d} \quad (4.5)$$

Твірна функція далі застосовується для розрахунку Tcp - середнього часу виконання протоколу:

$$T_{\text{ср}} = \frac{df_1(x)}{dx}(x = 1) \quad (4.6)$$

ТФ також використовується для розрахунку ймовірності успішного завершення, яка визначається, як значення твірної функції в точці x = 1:

$$P = f_1(x = 1) \quad (4.7)$$

## 1.2. Дослідження ВВХ DTLS

### 1.2.1. Аналіз параметрів протоколу DTLS, що визначають ймовірносно- часові характеристики

DTLS - один з протоколів обміну ключовим матеріалом між кореспондентами в IP-телефонії. DTLS [48] є адаптацією іншого протоколу забезпечення безпеки - TLS. На відміну від попередника, DTLS адоптований для роботи по мережі з негарантованою доставкою повідомлень з використанням протоколу UDP. Головним завданням DTLS протоколу є узгодження між кореспондентами головного секретного ключа, що застосовується згодом для SRTP протоколу.

У загальному вигляді - схема обміну повідомленнями протоколу DTLS для генерації ключів SRTP представлена на Рис. 4.2.

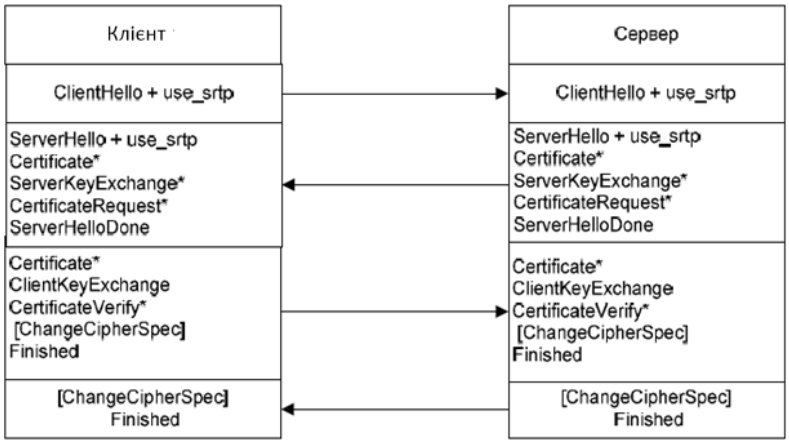


Рис. 4.5 - Обмін повідомленнями по протоколу DTLS

При розрахунках ймовірнісно-часових характеристик протоколу DTLS слід врахувати особливість повторної передачі повідомлень. Згідно [48],

значення таймерів повторної передачі повідомлення вибираються реалізацією протоколу, неузгодженість таймерів може привести до виникнення черг повідомлень. Початкове значення таймера повторної передачі рекомендується встановити в 1 секунду (мінімальне значення, визначене в[49]), і подвоювати значення таймера кожен раз до досягнення значення в 60 секунд. Значення таймера обнуляється кожен раз, коли має місце успішна передача повідомлення.

Після довгого періоду бездіяльності, наприклад, після здійсненої передачі даних, значення таймера може бути скинуто на початкове значення. Протокол DTLS не регламентує обмеження по числу повторів. Відповідно до рекомендації RFC 6298 значення таймера повторної передачі повідомлення повинно змінюватися в діапазоні від однієї секунди до шести десяти секунд. Таймер буде приймати значення: 1 с., 2 с., 4 с., 8 с., 16 с., 32 с., 60с. Значення таймера забезпечують сім повторів. При передачі - декілька повідомлень протоколу, як правило, групуються в комплексні повідомлення.

Відповідно до вищеописаного, при розрахунку ВВХ протоколу вводяться такі припущення:

· Повторні повідомлення відправляє тільки клієнт, який не отримав наступного за сценарієм повідомлення протягом часу, рівного поточному значенню таймера повторної передачі.

· При передачі одного повідомлення максимальне число повторів становить сім, після чого протокол завершує роботу.

Протокол DTLS може працювати в різних режимах, в залежності від яких може змінюватися довжина переданих повідомлень. Розрахунок виконується для режиму Діффі-Хелмана з аутентифікацією, в якому беруть участь всі повідомлення.

### 1.2.2. Оцінка і розрахунок ЙЧХ протоколу DTLS

Для складання ймовірнісного графа враховуються описані раніше особливості цього ПРК і вводяться такі змінні:

*NH* - розмір повідомлень Client Hello + Hello Verify Request, біт;

*NC* - розмір повідомлення Client Hello with COOKIE, біт;

*ND* - розмір повідомлень Server Hello, Certificate, Server Hello Done, біт;

*NF* - розмір повідомлень Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message, біт;

*NK* - розмір повідомлень Change Cipher Spec, Encrypted Handshake Message,біт;

$H_{XX}$ - твірна функція гілки, де xx - позначення відповідної гілки.

Імовірнісний граф всього протоколу DTLS, наведено на рисунку 4.3.

Виконується спрощення графа. Твірна функція гілки успішного завершення *H _ success* матиме вигляд:

$$H_{success} = H_{AS} \cdot H_{BS} \cdot H_{QS}, \quad (4.8)$$

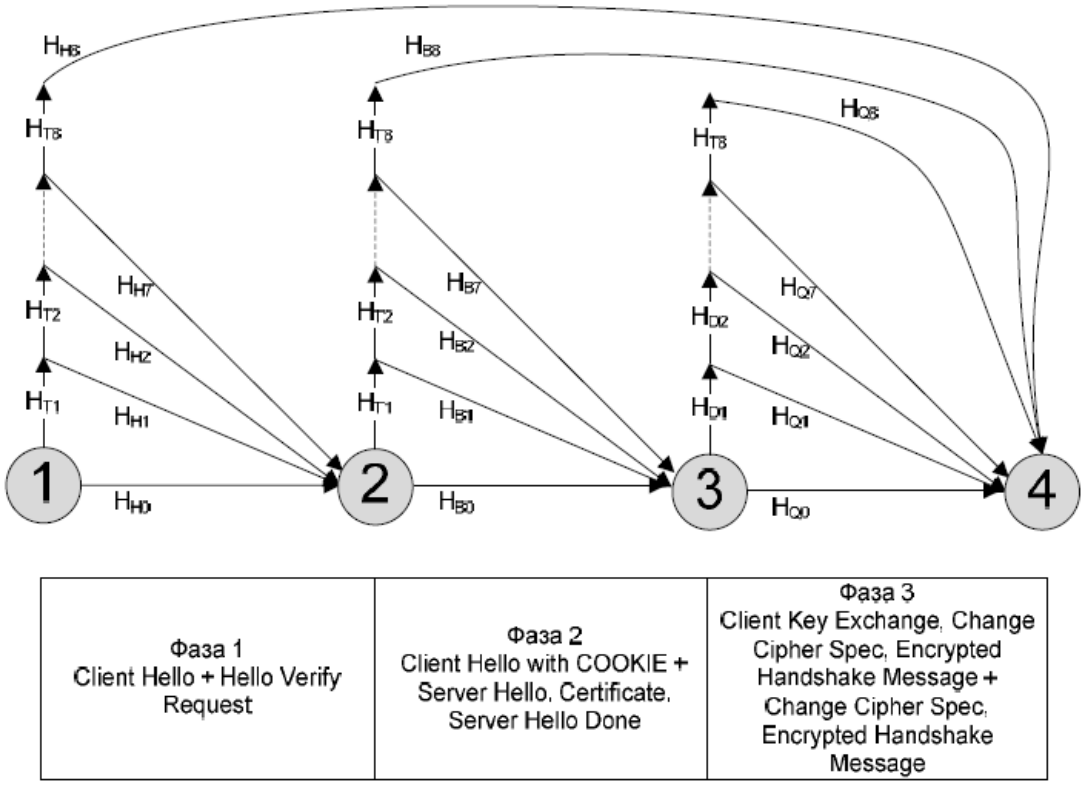


Рис. 4.3 - Ймовірнісний граф протоколу DTLS

Де $H_{AS} = (\sum_{y=0}^{6}(H_A(y) \cdot \prod_{i=1}^{y} H_T(i))) + H_{A\_ост} \prod_{i=0}^{7} H_T$ (4.9)

$$T_{Hi}(i) = \begin{cases} 0, \text{при } i = 0 \\ 1, \text{при } i = 1 \\ 2, \text{при } i = 2 \\ 4, \text{при } i = 3 \\ 8, \text{при } i = 4 \\ 16, \text{при } i = 5 \\ 32, \text{при } i = 6 \\ 60, \text{при } i \geq 7 \end{cases} \quad (4.10)$$

$$H_A(y) = [1 - p_0]^{NH} \cdot x^{\frac{NH}{c}+2d} \cdot ((1 - (1 - p_0)^{NH})x^{T_{Hi}})^y \quad (4.11)$$

$$H_{A\_\text{ост}} = 1 - \sum_{r=0}^{6}((1 - p_0)^{NH}) \cdot (1 - (1 - p_0)^{NH})^r) \quad (4.12)$$

$$H_T(i) = x^{T_{Hi}(i)} \quad (4.13)$$

Твірні функції $H_{BS}$, $H_{QS}$ визначаються за аналогією з твірною функцією $H_{AS}$:

$$H_{BS} = (\sum_{y=0}^{6}(H_B \cdot \prod_{i=1}^{y} H_T)) + H_{B\_\text{ост}} \prod_{i=0}^{7} H_T \quad (4.14)$$

$$H_B = [1 - p_0]^{NC+ND} \cdot x^{\frac{NC+ND}{c}+2d} \cdot ((1 - (1 - p_0)^{NC+ND})x^{T_{Hi}})^y \quad (4.15)$$

$$H_{B\_\text{ост}} = 1 - \sum_{y=0}^{6}((1 - p_0)^{NC+ND}) \cdot (1 - (1 - p_0)^{NC+ND})^y) \quad (4.16)$$

$$H_{QS} = (\sum_{y=0}^{6}(H_Q \cdot \prod_{i=1}^{y} H_T)) + H_{Q\_\text{ост}} \prod_{i=0}^{7} H_T \quad (4.17)$$

$$H_Q = [1 - p_0]^{NF+NK} \cdot x^{\frac{NF+NK}{c}+2d} \cdot ((1 - (1 - p_0)^{NF+NK})x^{T_{Hi}})^y \quad (4.18)$$

$$H_{Q\_\text{ост}} = 1 - \sum_{y=0}^{6}((1 - p_0)^{NF+NK}) \cdot (1 - (1 - p_0)^{NF+NK})^y) \quad (4.19)$$

Середній час завершення протоколу DTLS, а також ймовірність успішного завершення, визначається за методикою, описаною раніше.

$$T_{\text{ср}} = \frac{dH\_success}{dx}(x = 1) \quad (4.20)$$

$$P = H\_success(x = 1) \quad (4.21)$$

Отримані залежності представлені на рисунках 4.4, 4.5.

Зрозуміло, що в каналах високої якості ($p_o<10^{-5}$) час успішного виконання протоколу істотно залежить від величини затримки повідомлень в каналі зв'язку і практично не залежить від імовірності помилки. При цьому в каналах з затримкою понад 150 мс час виконання протоколу DTLS стає порівнянним з величинами, що визначають повний час встановлення з'єднань в мережах телефонного зв'язку загального користування.

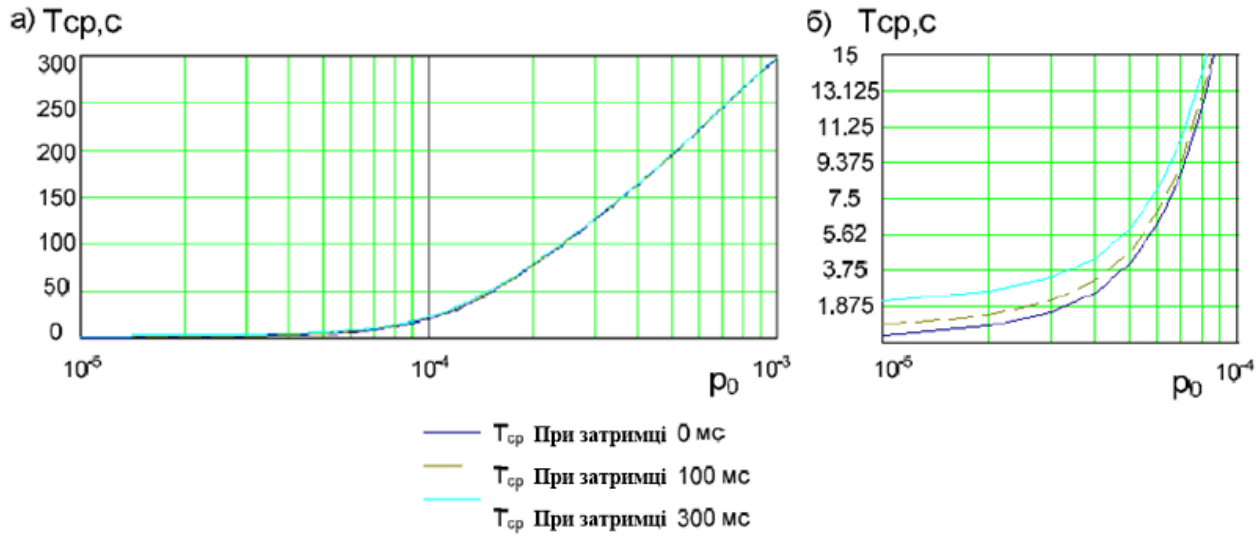


Рис. 4.4 - Середній час успішного завершення протоколу DTLS від p0

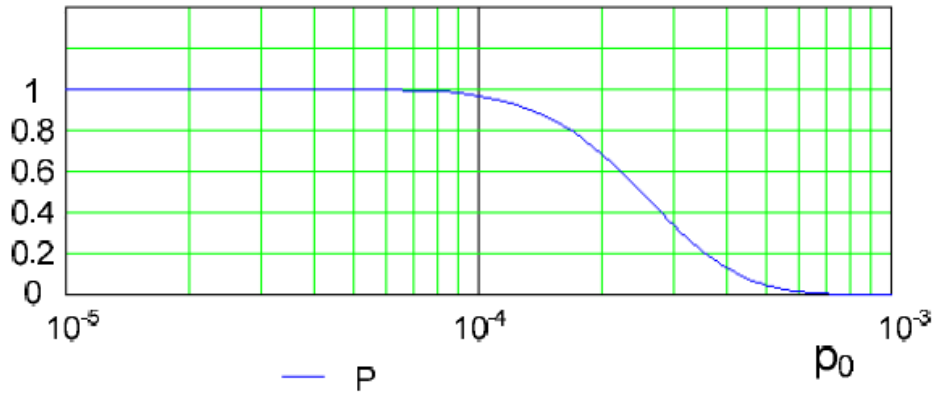


Рис. 4.5 - Залежність ймовірності успішного завершення протоколу DTLS від $p_0$ при $10^{-5} \leq p0 \leq 10^{-3}$

З погіршенням якості каналу при ро ≥ 10-5 середній час виконання протоколу різко зростає, а залежність від затримки пакетів в каналі зв'язку нівелюється.

### 1.3. Дослідження ЙЧХ ZRTP

#### 1.3.1. Аналіз параметрів протоколу ZRTP, що визначають ймовірносно- часові характеристики

В основу протоколу ZRTP покладено алгоритм Діффі-Хелмана [50].

Протокол виконується послідовно в чотири фази: виявлення, підтвердження, обчислення ключів і завершення.

Кореспонденти відправляють один одному повідомлення *Hello* на першій фазі протоколу. Вони містять дані про підтримувані криптографічні набори для

визначення можливості застосування SRTP: алгоритми хешування, алгоритми шифрування, типи аутентифікаційних тегів, протоколи узгодження ключів, типи SAS. Також передається інформація про версії ZRTP, набір прапорів і параметрів для різних операцій. Протоколом визначається повторна відправка повідомлення *Hello* до 20 разів, після чого протокол завершується неуспішно і сесія не встановлюється в захищеному режимі. Повторна передача *Hello* виконується зі змінною затримкою, величина якої має значення: 50, 100, 200 мс. Починаючи з четвертого повтору, затримка має постійне значення 200 мс. Кожне з отриманих повідомлень *Hello* підтверджується відповідним *HelloACK* повідомленням, після прийому якого повторна відправка Hello припиняється.

Для переходу в наступну фазу повідомлення *Hello* повинні отримати обидва кореспонденти, а повідомлення *HelloACK* повинен отримати хоча б один з них.

У другій фазі протоколу кореспонденти узгодять між собою, хто буде ініціатором для виконання алгоритму Діффі-Хелмана. Ініціатор першим відправляє "*Commit*" повідомлення. Якщо обидва кореспонденти вибирають роль ініціатора і відправляють повідомлення "*Commit*" одночасно, порівнюються значення хешу hvi з цих повідомлень. Той, чиє значення hvi виявиться більше - зберігає роль ініціатора.

Протокол передбачає повторну передачу повідомлення "*Commit*" до 10 разів, після чого протокол завершується неуспішно і сесія не встановлюється в захищеному режимі. Повторна передача *Commit* повідомлення виконується зі змінною затримкою, величина якої має значення: 150, 300, 600, 1200 мс. Починаючи з четвертого повтору, затримка має постійне значення 1200 мс. Кожне отримане по каналу зв'язку повідомлення *Commit* підтверджується відповідним повідомленням *DHPart1* третьої фази, після прийому якого повторна передача *Commit* припиняється.

У третій фазі в результаті обміну відкритими повідомленнями *DHPart1* і *DHPart2* проводиться формування секретних ключів для SRTP сесії.

Протокол передбачає повторну передачу *DHPart2* повідомлення до 10 разів, після чого протокол завершується неуспішно і сесія не встановлюється в захищеному режимі. Повторна відправка *DHPart2* повідомлення виконується зі змінною затримкою, величина якої має значення: 150, 300, 600, 1200 мс. Починаючи з четвертого повтору затримка має постійне значення 1 200 мс. Кожне отримане повідомлення *DHPart2* підтверджується відповідним повідомленням *Confirm1* четвертой фази, після прийому якого повторна передача *DHPart2* припиняється.

У четвертій фазі для підтвердження успішного формування загального ключа здійснюється обмін *Confirm2* і *ConfACK* повідомленнями. Послідовність обміну повідомленнями між взаємодіючими кореспондентами в процесі виконання протоколу ZRTP показана на Рис. 4.6. Для *Confirm2* передбачена повторна відправка повідомлень з параметрами, аналогічними повідомленням *DHPart2.*

Протокол вважається завершеним, коли ініціатор отримує повідомлення *ConfACT* або перший SRTP пакет з вірним тегом аутентифікації.

### 1.3.2. Оцінка ЙЧХ протоколу ZRTP

На Рис. 4.6. представлено обмін повідомленнями протоколу ZRTP між взаємодіючими кореспондентами.

Використовуючи описані раніше особливості ПРК, складається повний імовірнісний граф і описуються твірні функції для першої фази протоколу ZRTP, в ДКБП з рівномірним розподілом помилок в повідомленнях. Для цього визначаються наступні параметри:

$T_{HA}$ - час формування та передачі повідомлення *Hello* кореспондентом А, с;

$T_{оч}$ - час очікування при передачі повідомлення *Hello*, яке вичікує кореспондент між повторними передачами повідомлення, с;

*l*- розмір пакета, переданого по каналу зв'язку, біт;

$p_0$ - ймовірність бітової помилки в каналі зв'язку;

*NH* - розмір повідомлення *Hello,* (*Hello_A, Hello_B*), біт;

*NA* - розмір в бітах повідомлення *HelloACK*, біт.

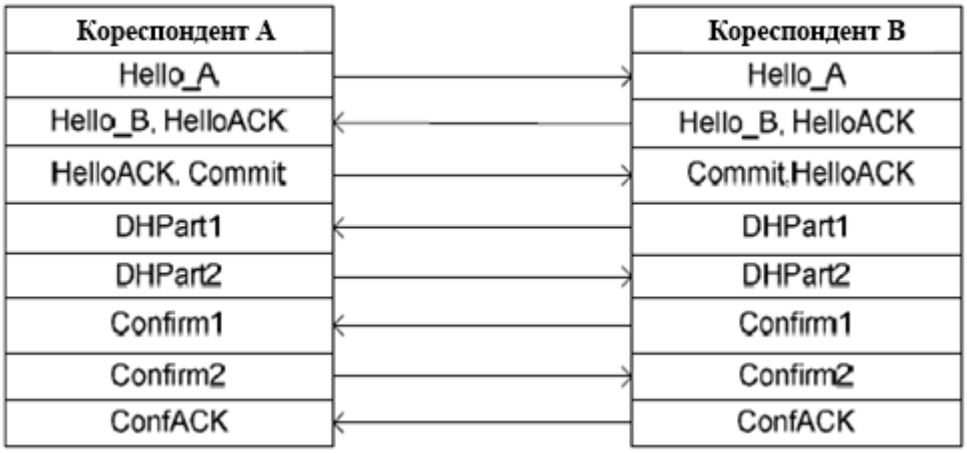


Рис. 4.6 - Обмін повідомленнями по протоколу ZRTP

При визначенні твірної функції елемента для першої фази протоколу, а саме передачі одного повідомлення Hello, необхідно врахувати особливості, що повтор повідомлення Hello проводиться тільки 20 разів, після чого протокол завершує роботу. Для кожного повтору $T_{оч}=T_{Hi}(i)$:

$$T_{Hi}(i) = \begin{cases} 0, \text{при } i = 0 \\ 0.05, \text{при } i = 1 \\ 0.1, \text{при } i = 2 \\ 0.2, \text{при } i \geq 3 \end{cases} \quad (4.22)$$

$H_{Ti}(i) = x^{T_{Hi(i)}}$

При оцінці ВВХ вводитися допущення, що доставка повідомлення Hello не підтверджується повідомленням HelloACK.

У даних умовах, твірна функція першої фази протоколу (Рис. 4.7) при передачі повідомлення Hello матиме такий вигляд:

$$H_{HELLO} = H_0 + H_1 + \cdots + H_{20} + H\_21, \quad (4.23)$$

Де $H_i = H_{H(i)} \prod_{k=1}^{i} H_{T(k)}$

$H_{H0} = (1 - (1 - p_0)^l) x^{T_{HA}}$ - твірна функція, яка визначає гілку безпомилкової передачі повідомлення *Hello* при одиничній передачі повідомлення.

$H_{H1} = (1 - (1 - p_0)^l)^2 x^{T_{HA}}$ - твірна функція, яка визначає гілку безпомилкової передачі повідомлення *Hello* при одній повторній передачі повідомлення.

$H_{H(i)} = (1-(1-p_0)^l)^i x^{T_{HA}}$ - твірна функція, яка визначає гілку безпомилкової передачі повідомлення *Hello* при *i*-й повторній передачі повідомлення, $i$=1..20.

$H_{21}$ - твірна функція, яка визначає гілку недоставки повідомлення за 20 повторних передач повідомлення:

$$H_{21} = P_{\text{зал}} x^{T_{HA}+\sum_{i=1}^{20} T_{Hi}(i)}, \quad (4.24)$$

де *Рзал* - ймовірність, що повідомлення *Hello* не було передано за 20 спроб;

$$T_{HA} = \frac{l}{c}, \quad (4.25)$$

де *c* - швидкість каналу зв'язку, біт / с.

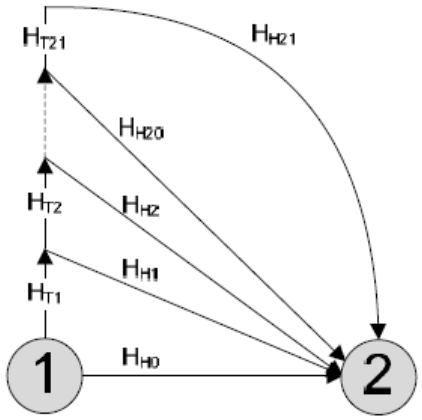


Рис. 4.7 - Ймовірнісний граф передачі повідомлення Hello

Для складання ймовірнісного графа всього протоколу ZRTP необхідно скористатися раніше описаними особливостями ПРК. Введено наступні змінні:

*NC* - розмір повідомлення *Commit*, біт;

*ND* - розмір повідомлення *DHPart1*, біт;

*NP* - розмір повідомлення *DHPart2*, біт;

*NO* - розмір повідомлення *Confirm1*, біт;

*NF* - розмір повідомлення *Confirm2*, біт;

*NK* - розмір повідомлення *ConfACK*, біт;

$H_{XX}$ - твірна функція гілки, де xx - позначення відповідної гілки.

Ймовірнісний граф всього протоколу ZRTP представлений на Рис. 4.8.

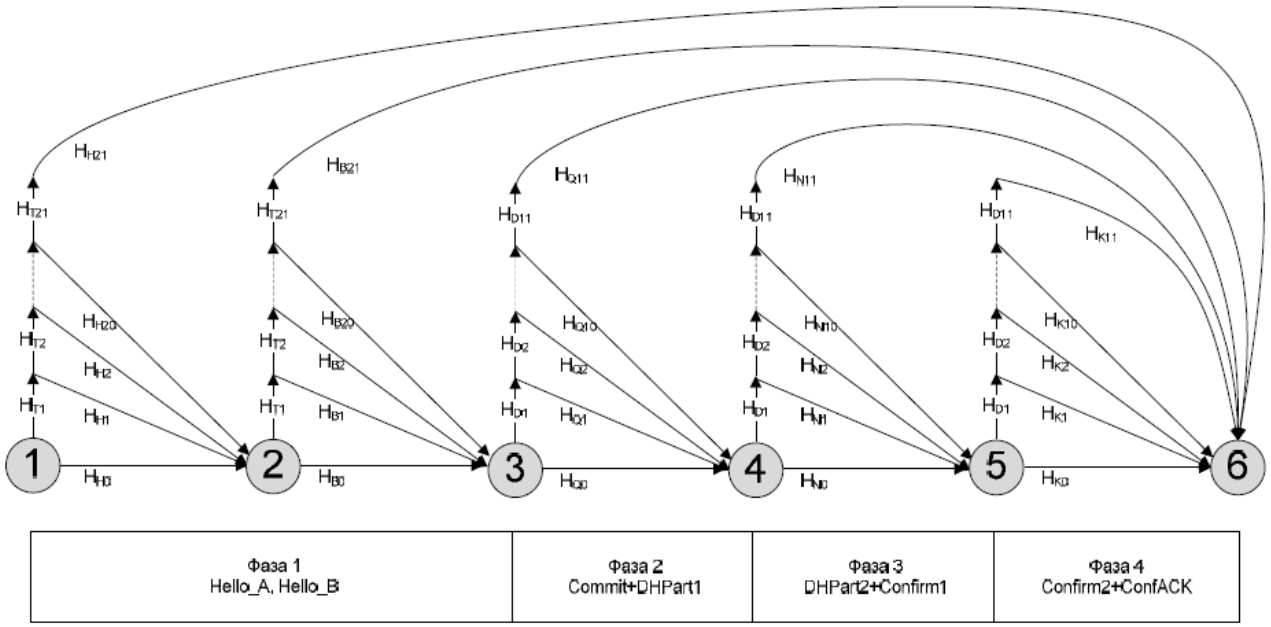


Рис. 4.8 - Ймовірнісний граф протоколу ZRTP

Для розрахунків граф спрощується (Рис. 4.9, 4.10), а також розбивається на гілки, що характеризують успішне і неуспішне виконання протоколу в кожній фазі.

Для розрахунку середнього часу успішного завершення протоколу необхідно визначити твірну функцію успішної гілки виконання протоколу.

Для цього виконується розщеплення гілок графа на успішне і неуспішне завершення протоколу.

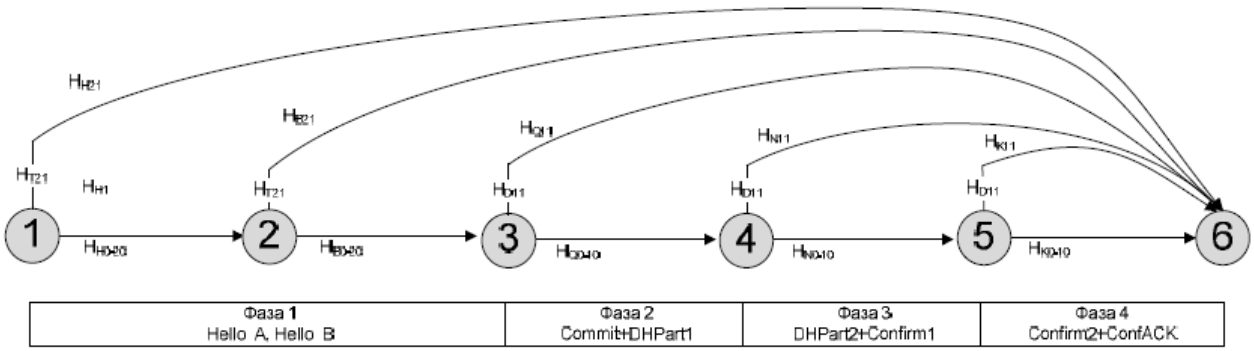


Рис. 4.9 - Спрощений імовірнісний граф протоколу ZRTP

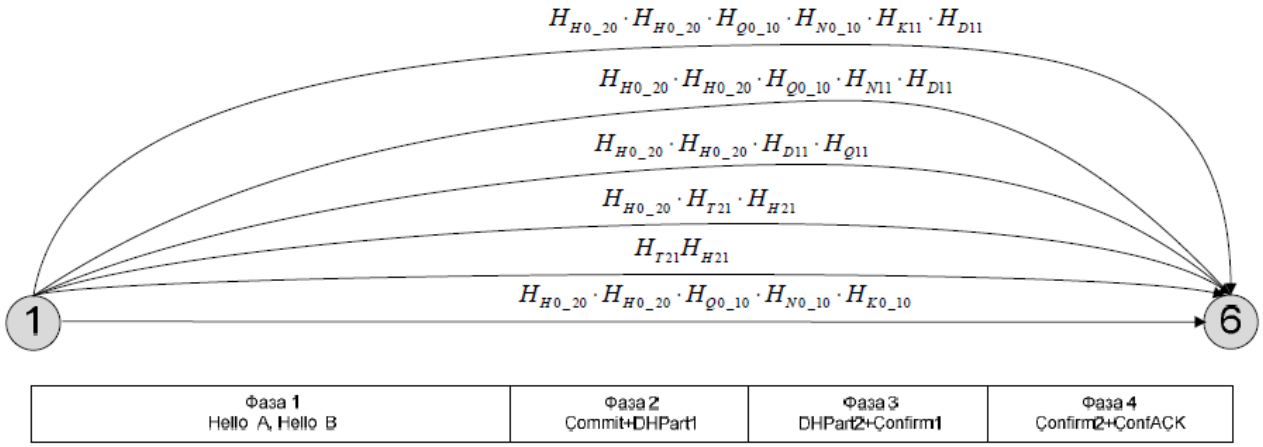


Рис. 4.10 - Спрощений імовірнісний граф протоколу ZRTP

Спрощений граф з розділеними гілками успішного і неуспішного завершення протоколу наведений на Рис. 4.11.

Твірна функція всього графа має вигляд:

$$H_{full} = H_{H0\_20} \cdot H_{H0\_20} \cdot H_{Q0\_10} \cdot H_{N0\_10} \cdot H_{K0\_10} + H_{T21} H_{H21} + H_{H0\_20} \cdot (H_{T21} \cdot H_{H21} + + H_{H0\_20} \cdot H_{D11}[H_{Q11} + H_{Q0\_10} \cdot (H_{N0\_10} \cdot H_{K11} + H_{N11})]) \quad (4.26)$$

Твірна функція гілки неуспішного виконання протокола:

$$H_{fail} = H_{T21} H_{H21} + H_{H0\_20} \cdot (H_{T21} \cdot H_{H21} + H_{H0\_20} \cdot H_{D11}[H_{Q11} + H_{Q0\_10} \cdot H_{K11} + H_{Q11})]) \quad (4.27)$$

Твірна функція гілки успішного виконання протокола:

$$H_{success} = H_{H0\_20} \cdot H_{H0\_20} \cdot H_{H0\_10} \cdot H_{H0\_10} \cdot H_{K0\_10} \quad (4.28)$$

На першому і другому етапі першої фази протоколу ZRTP, при передачі *Hello* від кореспондента А до кореспондента В, а також *Hello* від В до А, повідомлення мають однакову довжину, тому передача повідомлень для обох ітерацій представлена у вигляді однакових твірних функцій НН 0_ 20.

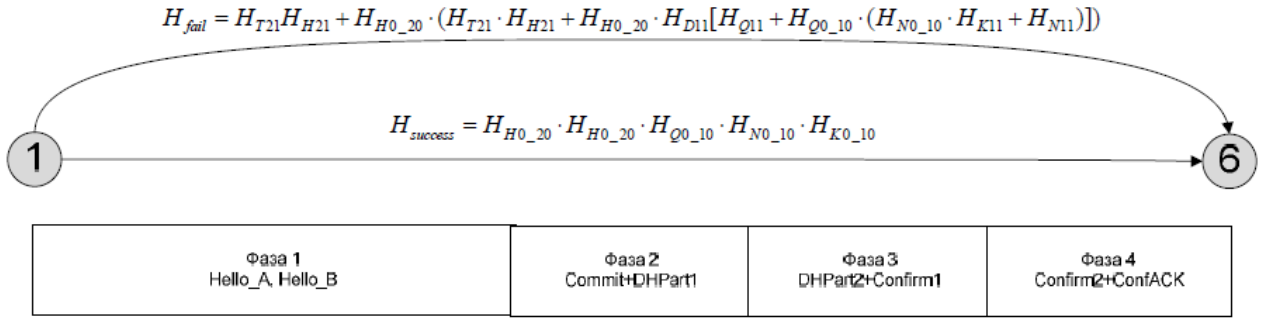


Рис. 4.11 - Спрощений імовірнісний граф протоколу ZRTP

Твірна функція $H_{H0\_20}$ візначається як

$$H_{H0\_20} = \left[\sum_{y=0}^{19}\left[H_A \cdot \left(\prod_{i=1}^{y} H_T\right)\right]\right] + H_{A\_зал} \cdot \prod_{i=0}^{20} H_T, \quad (4.29)$$

Де твірна функція передачі і-го повідомлення:

$$H_A = \left[(1-p_0)^{NH} \cdot x^{\frac{NH}{c}}\right] \cdot \left[\left[[1-(1-P_0)^{NH}] \cdot x^{T_{Hi}(y)}\right]^y\right] \quad (4.30)$$

$$H_{A\_зал} = 1 - \left[\sum_{y=0}^{19}\left[[(1-p_0)]^{NH} \cdot [[1-(1-p_0)^{NH}]^y]\right]\right]. \quad (4.31)$$

Твірна функція гілки очікування перед повторною передачею повідомлення, у разі недоставки на попередній спробі:

$$H_T(i,x) = x^{T_{Hi}(i)} \quad (4.32)$$

$T_{Hi}(i)$ – затримка перед повторною передачею повідомлення Hello, с:

$$T_{Hi}(i) = \begin{cases} 0, \text{при } i = 0 \\ 0.05, \text{при } i = 1 \\ 0.1, \text{при } i = 2 \\ 0.2, \text{ при } i \geq 3 \end{cases} \quad (4.33)$$

$H_Q$ описує передачу повідомлень другої фази протокола, а саме передачу Commit+DHPart1повідомлень.

$$H_{Q0\_10} = \left[\sum_{i=0}^{9}\left[H_Q \cdot \left(\prod_{i=0}^{y} H_D\right)\right]\right] + H_{Q\_зал} \cdot \prod_{i=0}^{10} H_D, \quad (4.34)$$

$$H_Q = \left[1-p_0)^{NC+ND} \cdot x^{\frac{NC+ND}{c}}\right] \cdot \left([1-(1-P_0)^{NC+ND}]x^{T_{Di}(y)}\right)^y \quad (4.35)$$

$$H_{Q\_зал} = 1 - \left[\sum_{y=0}^{9}\left[[(1-p_0)]^{NC+ND} \cdot [[1-(1-p_0)^{NC+ND}]^y]\right]\right]. \quad (4.36)$$

$H_D$ - Твірна функція гілки очікування перед повторною передачею повідомлення, у разі недоставки на попередній спробі:

$$H_D(i) = x^{T_{Hi}(i)} \quad (4.37)$$

$T_{Di}(i)$ – затримка перед повторною передачею повідомлень Commit, DHPart2, Confirm2, с:

$$T_{Di}(i) = \begin{cases} 0, \text{при } i = 0 \\ 0.05, \text{при } i = 1 \\ 0.1, \text{при } i = 2 \\ 0.2, \text{ при } i \geq 3 \end{cases} \quad (4.38)$$

$H_N$ описує передачу повідомлень третьої фази протокола, а саме передачу DHPart2+Confirm1 повідомлень.

$$H_{N0\_10} = \left[\sum_{i=0}^{9}\left[H_N \cdot \left(\prod_{i=0}^{y} H_D\right)\right]\right] + H_{N\_зал} \cdot \prod_{i=0}^{10} H_D, \quad (4.39)$$

$$H_N = \left[1 - p_0)^{NP+NO} \cdot x^{\frac{NP+NO}{c}}\right] \cdot \left([1 - (1 - P_0)^{NP+NO}]x^{T_{Di}(y)}\right)^y \quad (4.40)$$

$$H_{N\_зал} = 1 - \left[\sum_{y=0}^{9}\left[[(1 - p_0)]^{NP+NO} \cdot [[1 - (1 - p_0)^{NP+NO}]^y]\right]\right]. \quad (4.41)$$

На четвертій фазі протокола передаються повідомлення Confirm2 + ConfACK, загальним розміром *N_K* біт

*N_K=NF+NK*, біт

Твірна функція візначається як:

$$H_{K0\_10} = \left[\sum_{i=0}^{9}\left[H_K \cdot \left(\prod_{i=0}^{y} H_D\right)\right]\right] + H_{K\_зал} \cdot \prod_{i=0}^{10} H_D, \quad (4.42)$$

де

$$H_K = \left[(1 - p_0)^{N\_K} \cdot x^{\frac{N\_K}{c}}\right] \cdot \left[\left[[1 - (1 - P_0)^{N\_K}] \cdot x^{T_{Di}(y)}\right]^y\right] \quad (4.43)$$

$$H_{K\_зал} = 1 - \left[\sum_{y=0}^{10}\left[[(1 - p_0)]^{N\_K} \cdot [[1 - (1 - p_0)^{N\_K}]^y]\right]\right]. \quad (4.44)$$

Для розрахунку середнього часу успішного завершення протоколу визначена твірна функція гілки успішного виконання протоколу. Функція середнього часу і ймовірності успішного завершення ПРК матиме вигляд:

$$T_{\text{ср}} = \frac{dH_{success}}{dx}(x = 1) \quad (4.45)$$

$$P_{success} = H_{H0\_20}(x = 1) \cdot H_{H0\_20}(x = 1) \cdot H_{Q0\_10}(x = 1) \cdot H_{N0\_10}(x = 1) \cdot H_{K010}(x = 1) \quad (4.46)$$

### 1.3.3. Розрахунок ЙЧХ ZRTP

Графік середнього часу успішного виконання протоколу ZRTP для різних величин затримки пакетів в каналі зв'язку представлений на Рис. 4.12. Імовірність успішного завершення матиме вигляд, представлений на Рис. 4.13.

Очевидно, що в каналах хорошої якості ($p_o$ <$10^{-4}$) час успішного виконання протоколу істотно залежить від величини затримки повідомлень в каналі зв'язку і практично не залежить від імовірності помилки. При цьому в каналах з затримкою більш 150 мс час виконання протоколу ZRTP стає порівнянним з величинами, що визначають повний час встановлення з'єднань в мережах телефонного зв'язку загального користування.

З погіршенням якості каналу від $p_o = 10^{-4}$ до $p_o = 10^{-3}$ середній час виконання протоколу різко зростає, а залежність від затримки пакетів в каналі зв'язку нівелюється.

Ймовірність успішного виконання протоколу ZRTP в каналах хорошої якості не залежить від затримок в каналі зв'язку і близька до одиниці, і тільки в каналах з імовірністю помилки на символ більше $5 \cdot 10^{-4}$ починає знижуватися до 0,8 при $p_o = 10^{-4}$.

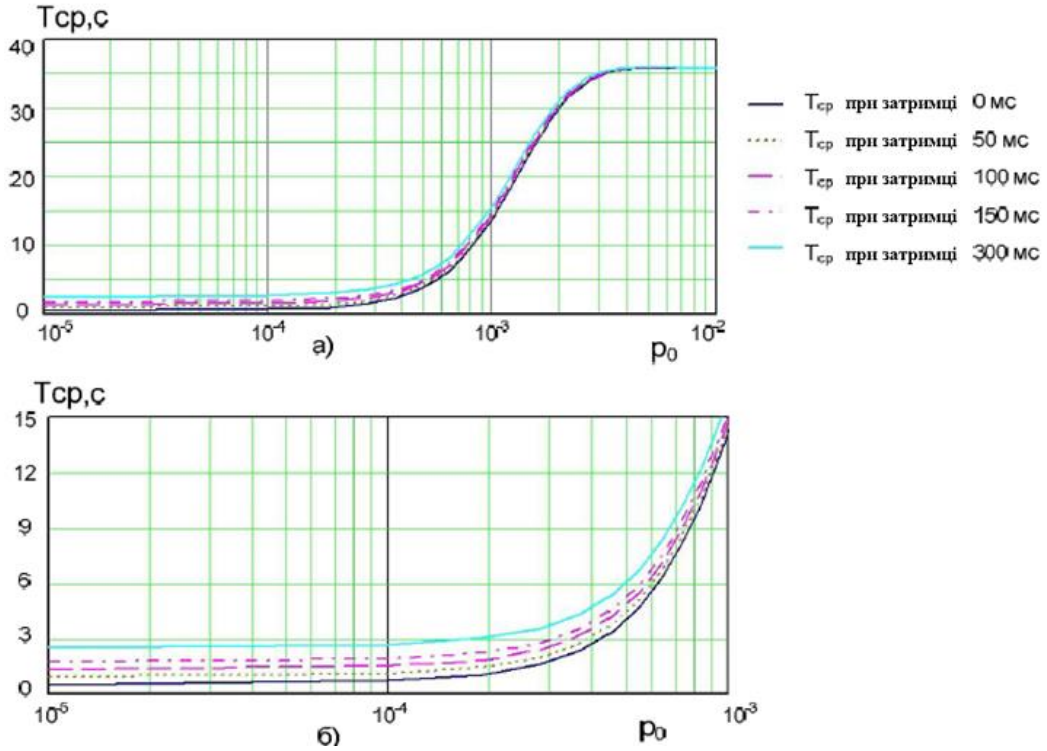


Рис. 4.12 - Залежність TCP ZRTP від ймовірності помилки в каналі із затримками пакетів а) $10^{-5} \le p_0 \le 10^{-2}$ б) $10^{-5} \le p_0 \le 10^{-2}$

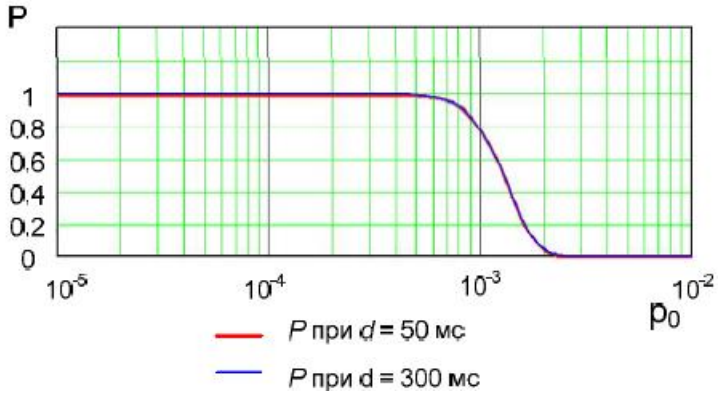


Рис. 4.13 - Залежність ймовірності успішного завершення протоколу від ймовірності помилки

На рисунку 4.14 представлено порівняння середнього часу успішного завершення ZRTP і DTLS. Очевидно, ZRTP забезпечує менше значення TCP в каналах більш поганої якості в порівнянні з DTLS. Тому подальший аналіз буде виконуватися саме для протоколу ZRTP.

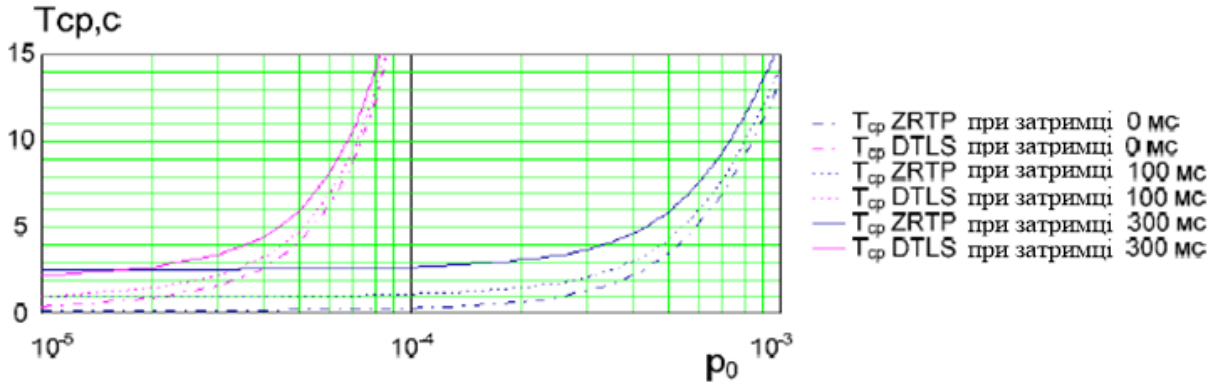


Рис. 4.14 - Залежність середнього часу виконання протоколу ZRTP і DTLS від ймовірності помилки в каналі при різних значеннях d

### 1.4. Розробка пропозицій щодо покращення ймовірносно-часових характеристик протоколу ZRTP

Детально принцип розрахунку ЙЧХ протоколу ZRTP був викладений в розділі 4.1. Відповідно до Наказу Міністерства інформаційних технологій і зв'язку РФ від 27.09.2007 № 113 «Про затвердження Вимог до організаційно-технічного забезпечення стійкого функціонування мережі зв'язку загального користування» час з моменту отримання користувацьким (кінцевим) обладнанням викликаючого абонента інформації про відповідь від користувацького (кінцевого ) обладнання викликаємого абонента до моменту встановлення з'єднання між користувацьким (кінцевим) обладнанням викликаючого і викликаємого абонента (час виконання з'єднання) не повинно перевищувати 1 с в мережі зонового телефонного зв'язку і в мережі міжміського і міжнародного телефонного зв'язку, а також не повинно перевищувати 1,5 с в мережі місцевого телефонного зв'язку [47].

Відповідно до теоретичних розрахунків, а також практичного експерименту при односторонній затримці в лінії понад 100 мс середній час виконання протоколу ZRTP становить близько 0.9 с, а при 150 мс становить 1.2

с, що перевищує встановлену норму. У разі наявності помилок в каналі зв'язку час виконання протоколу також зростає за рахунок необхідності повторної відправки повідомлень.Таким чином, за певних умов час виконання протоколу ZRTP не задовольняє існуючим нормативам. Відповідно - має сенс виконати модернізацію протоколу для покращення параметрів ЙЧХ.

Протокол можна розділити на кілька етапів:

- узгодження початкових параметрів і умов;
- підготовка до обміну повідомленнями;
- обмін і генерація спільного ключа по протоколу Діффі-Хелмана;
- перевірка загального ключа.

На етапі підготовки від одного кореспондента до іншого передається параметр hvi, який розташовується в повідомленні Commit і визначається, як

hvi = hash (DHPart2 || Hello респондента)

Експериментальна оцінка і теоретичні розрахунки показали, що в режимі Діффі-Хелмана протокола ZRTP загальна довжина повідомлень Commit + Hello порівнянна з довжиною повідомлень DHPart1 або DHPart2. Тому в якості модернізації протоколу пропонується об'єднати повідомлення HelloB + Commit. Після отримання повідомлення Hello_A другий кореспондент уже володіє всіма необхідними даними, щоб вибрати криптографічний набір для продовження роботи протоколу.

Недоліком підходу може бути необхідність вже на першій фазі ZRTP виконати обчислення для протоколу Діффі-Хелмана, що вимагає задіяти обчислювальні ресурси на обладнанні обох кореспондентів. Однак, додатково підхід дозволяє виключити з протоколу останнє повідомлення Conf2ACK. Необхідність повідомлення у вихідному протоколі викликана наявністю незавершеної четвертої фази, де на повідомлення ініціатора Confirm2 респондент повинен відповісти повідомленням. При об'єднанні пакетів Hello + Commit повідомлення DHPart2 буде відповідним до DHPart1, повідомлення Confirm2 буде відповідним до повідомлення Confirm1. При такому підході

повідомлення Confirm2 буде відповідним, і не потребуватиме додаткового повідомлення Conf2ACK.

Так в оновленій версії протоколу буде шість повідомлень: два повідомлення Hello і Commit, повідомлення DHPart1 і DHPart2, два повідомлення перевірки виробленого ключа.

Модернізований протокол буде мати сценарій обміну повідомленнями, представлений на Рис. 4.15. Необхідно виконати оцінку ВВХ оновленого протоколу. Граф оновленого протоколу представлений на Рис. 4.16. Виконано спрощення графа за аналогією з повною версією протоколу. Спрощений граф представлений на Рис. 4.17.

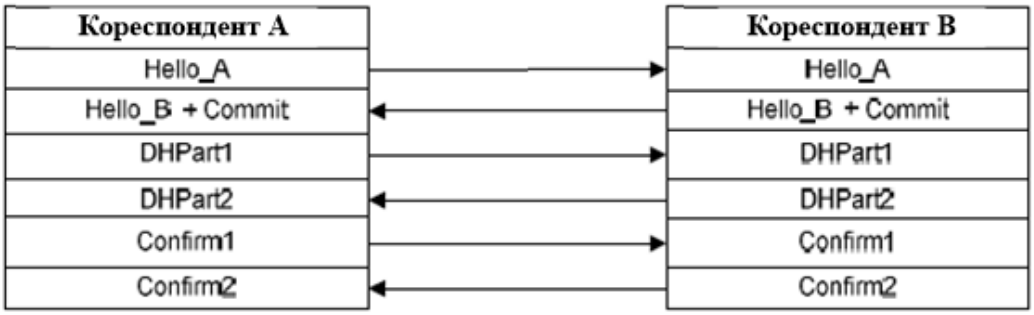


Рис. 4.15 - Сценарій обміну повідомленнями модернізованого протоколу

Твірна функція гілки успішного завершення протоколу буде визначатися, як:

$$H_{SUCCESS} = H_{HA0\_20} \cdot H_{B0\_20} \cdot H_{N0\_10} \cdot H_{N0\_10} \quad (4.47)$$

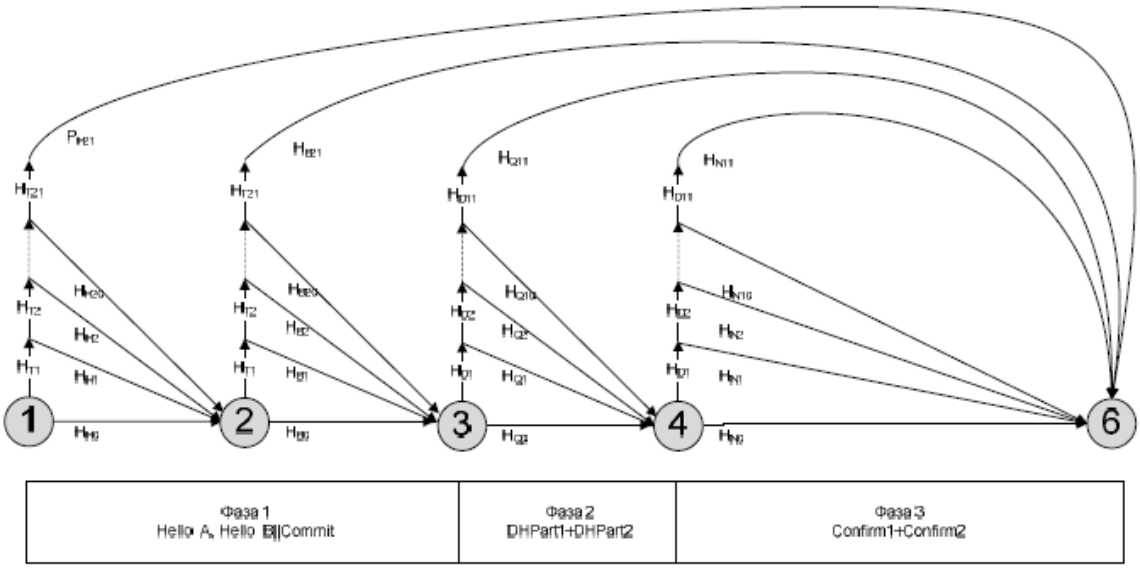


Рис. 4.16 - Граф оновленого протоколу ZRTP

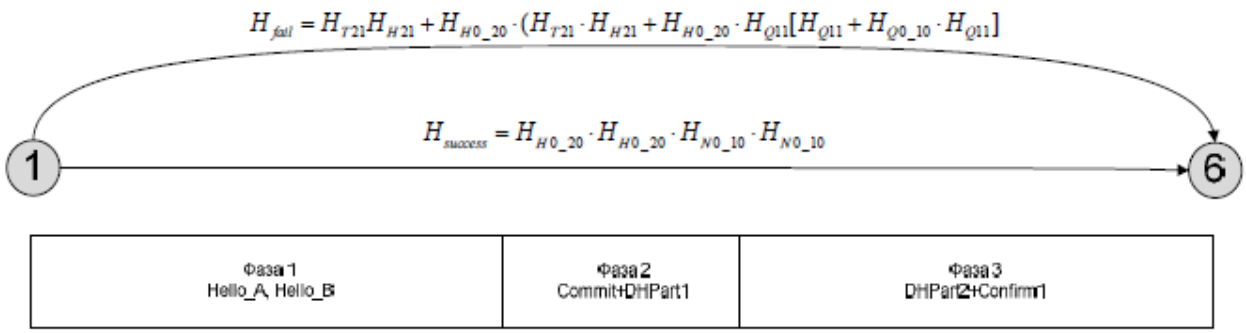


Рис. 4.17 - Спрощений граф оновленого протоколу ZRTP

Залежність середнього часу успішного виконання оновленого протоколу від $p_0$ представлена на рисунках 4.18. Проводиться оцінка виграшу в модифікованому протоколі в порівнянні з вихідним. Для цього визначається час виконання протоколу при роботі по каналах із затримками при наступних параметрах:

- затримка: 50 мс, 150мс, 300мс
- $p_0$: $10^{-5}$, $5*10^{-5}$, $10^{-4}$

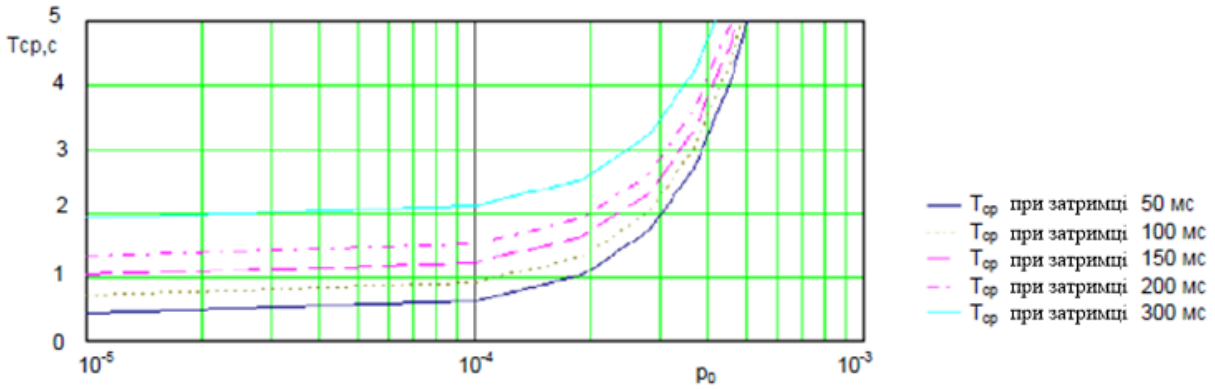


Рис. 4.18 - Середній час успішного завершення оновленого протоколу ZRTP

Виграш оцінюється, як

$$T_{B1} = T_{ZRTP} - T_{\text{мод1}} \quad (4.48)$$

$$B_{B1} = (T_{ZRTP} - T_{\text{мод1}})/T_{ZRTP} \quad (4.49)$$

де $T_{ZRTP}$ - середній час виконання вихідного протоколу, с;

$T_{мод1}$- середній час виконання модифікації протоколу, с;

Результати обчислень представлені в Табл. 4.1.

Виконується додаткове скорочення числа окремих повідомлень в протоколі ZRTP [122, 74]. Для цього об'єднуються повідомлення Hello_B +

Commit + DHPart1, а також повідомлення DHPart2 + Confirm1. Модернізований протокол буде мати сценарій обміну повідомленнями, представлений на Рис. 4.19а.

Об'єднання повідомлень призводить до втрати попередньої передачі параметра hvi, проте дозволяє зберегти концепцію протоколу і виконати між кореспондентами перевірку отриманого ключа. Спрощення графа наведено на Рис. 4.20.

*Таблиця 4.1*

Оцінка виграшу середнього часу успішного завершення протоколу ZRTP першої модифікації

| $d$ | 50мс | | | 150мс | | | 300мс | | | 400мс | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $p_0$ | $10^{-5}$ | $5\cdot10^{-5}$ | $10^{-4}$ | $10^{-5}$ | $5\cdot10^{-5}$ | $10^{-4}$ | $10^{-5}$ | $5\cdot10^{-5}$ | $10^{-4}$ | $10^{-5}$ | $5\cdot10^{-5}$ | $10^{-4}$ |
| $T_{ZRTP}$, с | 0,52 | 0,58 | 0,7 | 1,3 | 1,38 | 1,5 | 2,5 | 2,59 | 2,7 | 3,32 | 3,38 | 3,51 |
| $T_{мод1}$, с | 0,42 | 0,49 | 0,62 | 1,02 | 1,09 | 1,2 | 1,92 | 1,99 | 2,09 | 2,52 | 2,59 | 2,72 |
| $T_{B1}$, с | 0,1 | 0,09 | 0,08 | 0,28 | 0,29 | 0,3 | 0,58 | 0,6 | 0,61 | 0,8 | 0,79 | 0,79 |
| $B_{B1}$, % | 19,2 | 15,5 | 11,4 | 21,5 | 21 | 20 | 23,2 | 23,1 | 22,5 | 24,1 | 23,37 | 22,5 |

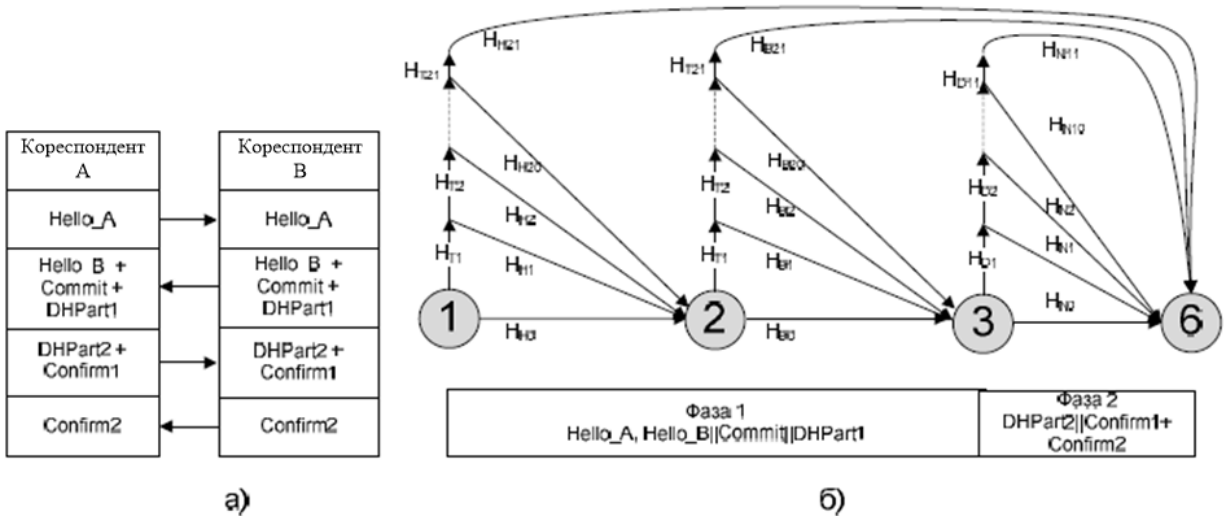


Рис. 4.19 - Друга модифікація протоколу; а) сценарій обміну повідомленнями б) ймовірнісний граф

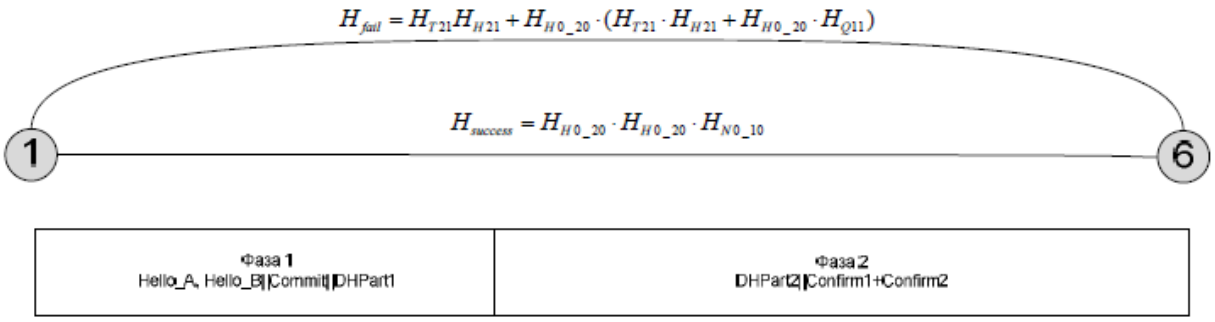


Рис. 4.20 - Спрощений граф модернізованого протоколу ZRTP

За аналогією обчислено $T_{мод2}$ - середній час виконання другої модифікації протоколу в залежності від затримки і втрати пакетів в каналі зв'язку. Графік наведено на Рис. 4.21.

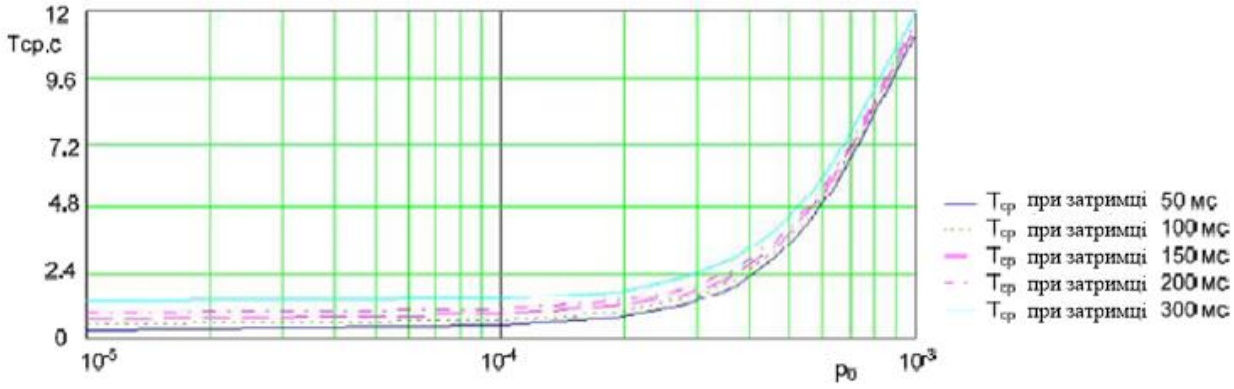


Рис. 4.21 - Середній час виконання модернізованого протоколу ZRTP другої модифікації

Додатково проведено оцінку виграшу в модифікованому протоколі в порівнянні з вихідним. Для цього визначено час виконання протоколу при роботі по каналах із затримками при наступних параметрах:

- затримка 50 мс, 150мс, 300мс;

- $p_0 = 10^{-5}, 5*10^{-5}, 10^{-4}$.

Виграш у часі $T_{B2}$, що характеризує заощаджений час за рахунок застосування модифікованого протоколу в порівнянні з вихідним, і відносний виграш $B_{B2}$, що відображає відношення зекономленого часу до $T_{прот}$, визначені за формулами:

$$T_{B2} = T_{ZRTP} - T_{\text{мод2}} \quad (4.50)$$

$$B_{B2} = (T_{ZRTP} - T_{\text{мод2}})/T_{ZRTP} \quad (4.51)$$

$T_{мод2}$- середній час виконання другої модифікації протоколу, с;

Результати обчислень представлені в Табл. 4.2. Виграш модифікованого протоколу з шести повідомлень перед стандартним протоколом складає від 11% до 24%.Виграш перед стандартним протоколом модифікованого протоколу, скороченого до чотирьох повідомлень, склав від 35% до 48% відповідно до Табл. 4.2.

Таким чином, модифікований протокол ZRTP дозволяє працювати по каналах зв'язку з більшою затримкою в порівнянні зі стандартним протоколом ZRTP, при цьому вкладаючись в нормативи для параметрів ТМЗК.

*Таблиця 4.2*

Оцінка виграшу середнього часу успішного завершення протоколу ZRTP другої модифікації

| *d* | 50мс | | | 150мс | | | 300мс | | | 400мс | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $p_0$ | $10^{-5}$ | $5\cdot10^{-5}$ | $10^{-4}$ | $10^{-5}$ | $5\cdot10^{-5}$ | $10^{-4}$ | $10^{-5}$ | $5\cdot10^{-5}$ | $10^{-4}$ | $10^{-5}$ | $5\cdot10^{-5}$ | $10^{-4}$ |
| $T_{ZRTP}$, с | 0,52 | 0,58 | 0,7 | 1,3 | 1,38 | 1,5 | 2,5 | 2,59 | 2,7 | 3,32 | 3,38 | 3,51 |
| $T_{мод2}$, с | 0,31 | 0,36 | 0,45 | 0,71 | 0,76 | 0,85 | 1,31 | 1,36 | 1,45 | 1,71 | 1,76 | 1,85 |
| $T_{B2}$, с | 0,20 | 0,22 | 0,24 | 0,58 | 0,62 | 0,64 | 1,18 | 1,23 | 1,24 | 1,60 | 1,62 | 1,65 |
| $B_2$, % | 39,4 | 37,9 | 35,5 | 45,0 | 44,9 | 43,2 | 47,4 | 47,4 | 46,2 | 48,3 | 47,93 | 47,2 |

Для підвищення безпеки модифікованого протоколу пропонується використовувати розроблений в третьому розділі метод виявлення порушника.

Виконано імітаційне моделювання для протоколу ZRTP і другої модифікації протоколу, для чого було розроблено додаток на мові програмування PHP. Вихідний код програми наведено в додатку. Результати імітаційного моделювання для вихідного протоколу ZRTP представлені на Рис. 4.22.

Результати імітаційного моделювання для другої модифікації протоколу ZRTP представлені на Рис. 4.23. Отримані результати підтверджують теоретично отриману залежність.

Порівняння залежностей $T_{мод2}$, $T_{мод2}$, $T_{ZRTP}$ наведено на Рис. 4.24.

Наскільки видно з Табл. 4.2, при $p_0 \leq 10\text{-}4$ і $d \leq 300$ мс $T_{мод2} \leq 1{,}45$ с. Таким чином, завдання про виконання норм [25] при роботі по каналах зв'язку $d \leq 300$ мс вирішена.

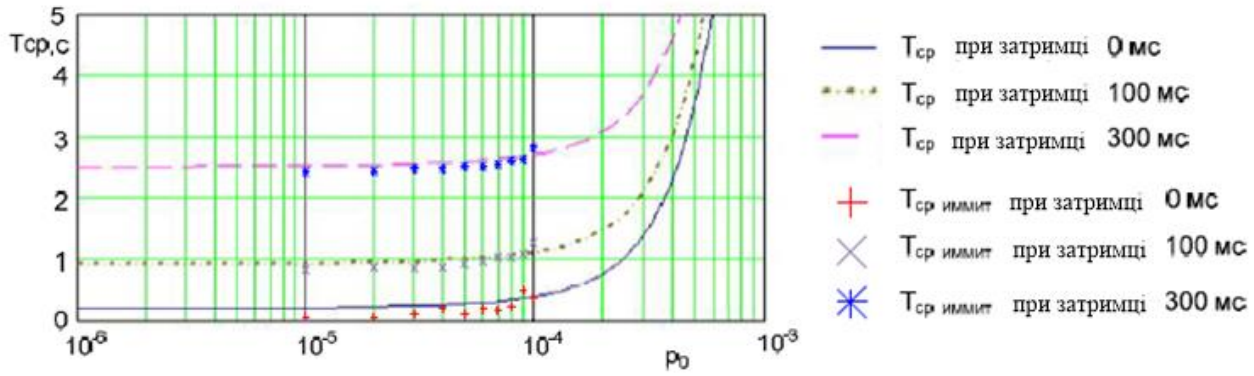


Рис. 4.22 - Результати імітаційного моделювання $T_{ср}$ для вихідного протоколу ZRTP

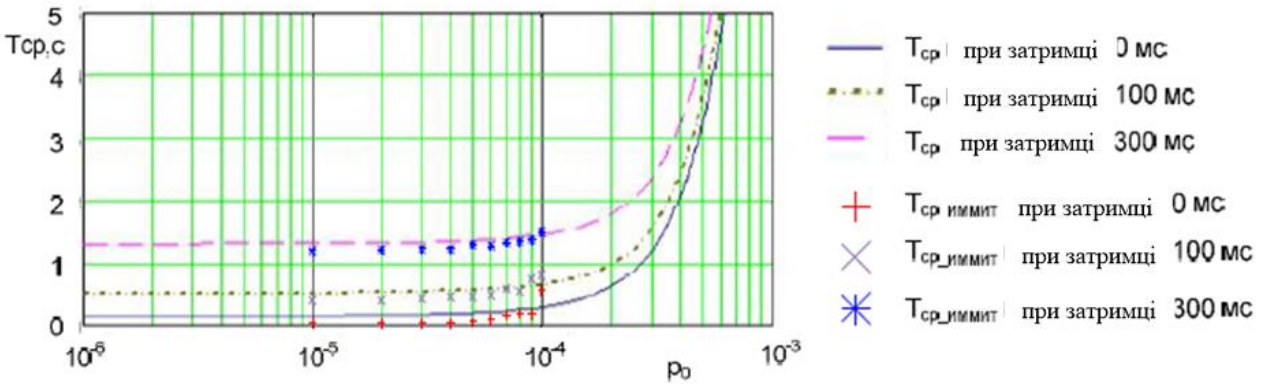


Рис. 4.23 - Результати імітаційного моделювання $T_{ср}$ для другої модифікації протоколу ZRTP

### 1.5. Висновки

Представлена методика оцінки ймовірнісно-часових характеристик протоколів розподілу ключів захищеної IP-телефонії, що дозволяє визначити ефективність роботи протоколів по каналах з затримками і помилками, оцінюючи середній час, а також ймовірність успішного завершення протоколу. Методика враховує особливості ПРК, пов'язані з обмеженим числом повторів, а також з варіацією затримки в кожному з повторів.

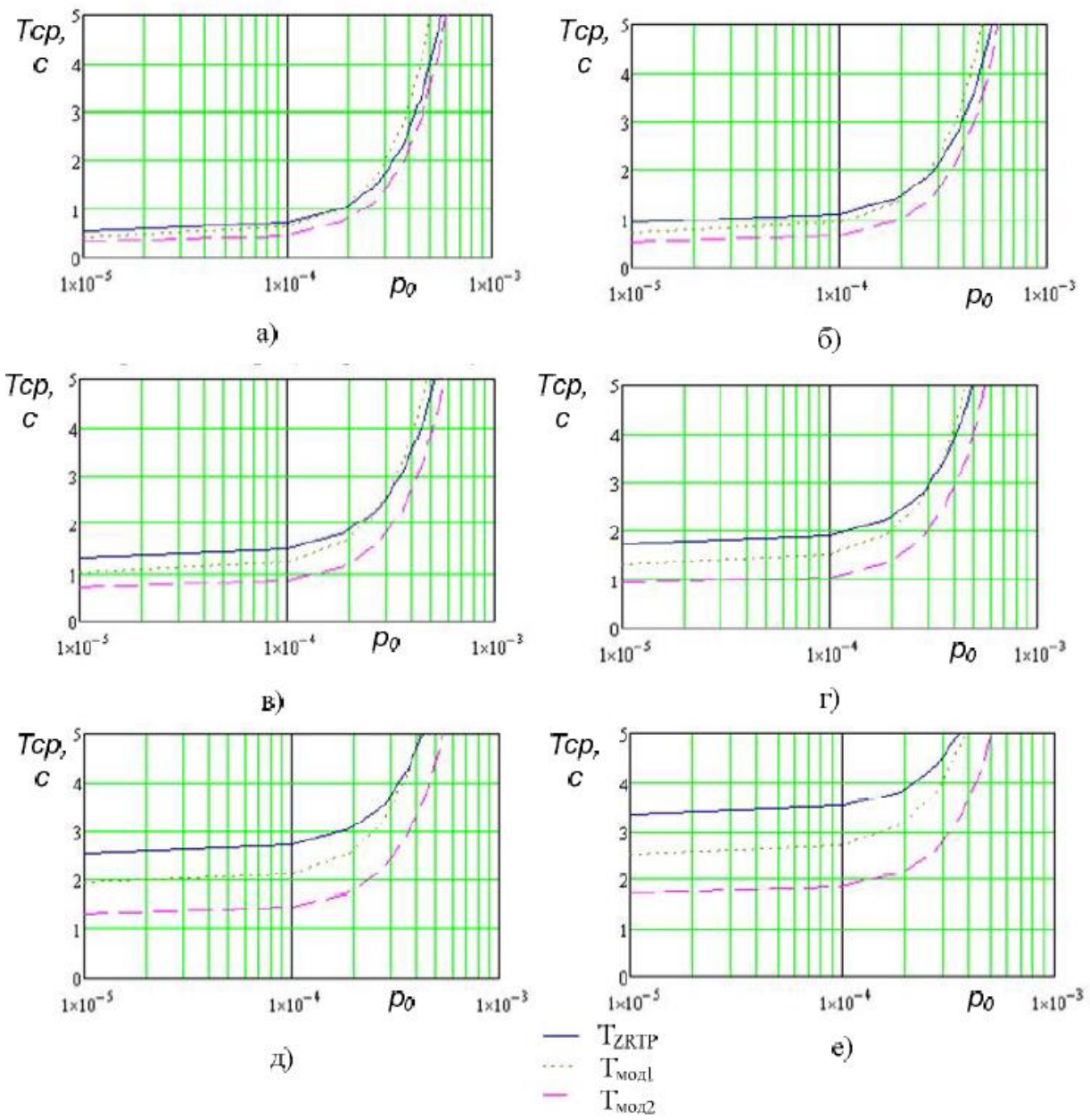


Рис. 4.24 - Порівняння середнього часу успішного завершення оригінального ZRTP, першої та другої модифікацій ZRTP а) d = 50 мс; б) d = 100 мс; в) d = 150 мс; г) d = 200 мс; д) d = 300 мс; е) d = 400 мс

Проведено дослідження ВВХ протоколів DTLS і ZRTP, відповідно до запропонованої методики обчислені середній час успішного завершення і ймовірність успішного завершення.

Для протоколу ZRTP виконана експериментальна оцінка середнього часу успішного завершення, а також виконано порівняння отриманої оцінки з розрахованим за методикою значенням. На підставі порівняння зроблено висновок про збіг теоретичних і практичних результатів.

Показано, що в каналах з високою затримкою протоколу ZRTP потрібен досить великий час на встановлення захищеного з'єднання, що негативно позначається на дотриманні норм на час встановлення голосового каналу між кореспондентами.

Виходячи з вищенаведеного, модернізація протоколу розподілу ключів є актуальним завданням, що дозволяє зберегти переваги протоколу ZRTP, при цьому прискоривши виконання протоколу при роботі по каналах з великими затримками.

Розроблено метод поліпшення часових характеристик криптографічного протоколу ZRTP, що складається у виключенні механізму розподілу ролей ініціатора і респондента, а також в об'єднанні інформаційного блоку даних про підтримувані кореспондентами криптографічнінабори з блоком даних протоколу Діффі-Хелмана.

Виграш В2 в порівнянні з вихідним ZRTP склав від 39,42% до 48,3%, дозволивши при затримці до 300 мс скоротити час успішного виконання протоколу до 1,45, що менше встановленої норми 1.5 с, що дозволяє виконувати цю норму. Застосування модифікованого протоколу спільно з запропонованим методом виявлення порушника в режимі ОН дозволяє знизити ймовірність успішної атаки MITM на 3 порядки, тим самим підвищуючи інформаційну безпеку.

# ВИСНОВКИ

У дипломній роботі вирішена актуальна науково-технічна задача підвищення рівня захищеності інформації в сеансах безпечної IP- телефонії та скорочення часу встановлення захищеного з'єднання за рахунок поліпшення ймовірносно-часових характеристик протоколів, в тому числі отримані наступні основні результати:

1. Запропоновано математичну модель активного порушника для захищеної IP-телефонії, що враховує можливість цього порушника реалізувати атаку людина посередині на протокол розподілу ключів, яка дозволяє розрахувати ймовірність успішної атаки, націленої на несанкціонований доступ до інформації (НСД), в залежності від значень ймовірностей проміжних атак.

2. Запропоновано методику оцінки ймовірнісно-часових характеристик протоколів розподілу ключів захищеної IP-телефонії, що враховує особливості протоколів, виражені в наявності обмеження числа повторних передач повідомлень і змінного таймера повторної передачі.

3. Представлена модифікація протоколу розподілу ключів ZRTP, яка дозволяє виконувати протокол за менший час у порівнянні з вихідною реалізацією. Виграш досягається за рахунок поліпшення тимчасових характеристик протоколу розподілу ключів ZRTP, що складається у виключенні алгоритму розподілу ролей ініціатора і респондента, а також в об'єднанні інформаційних даних про підтримувані криптографічні набори і блоки протоколу Діффі - Хелмана. Розроблено метод виявлення порушника протоколів розподілу ключів, який застосовується при роботі за сценарієм клієнт-клієнт для кореспондентів, які не мають заздалегідь розподіленого ключового матеріалу. Метод дозволяє з більш високою ймовірністю встановити захищене з'єднання між двома кореспондентами в порівнянні з існуючими методами, а також виявити наявність активного порушника в каналі зв'язку. Запропоновано модифікації протоколу ZRTP, що реалізують розроблений

метод виявлення порушника. Модифікації в порівнянні з вихідним протоколом дозволяють виявити активного порушника, що реалізує атаку людина посередині на протокол розподілу ключів.

Перспективними завданнями дослідження є розробка програмної реалізації модифікованого протоколу розподілу ключів із застосуванням загальнодоступних бібліотек, розробка програмного клієнта IP-телефонії, що реалізує протокол, а також доопрацювання рішення за рахунок впровадження елементів стеганографії в запропоновані методи підвищення безпеки.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Росляков А.В. IP-телефония / А.В. Росляков., М.Ю. Самсонов, И.В.Шибаева.– М.:Эко-трендз,2003. – 256 с.
2. Нопин, С.В. Разработка защищенных от несанкционированного доступа систем IP-телефонии на основе операционной системы Windows / С.В. Нопин, В.Г. Шахов // Омский научный вестник. 2006. – №9(46). – С.137-142.
3. Нопин, С.В. Передача мультимедийных данных по цифровым каналам в режиме, защищенном от несанкционированого доступа: дис. канд. техн. наук. – Новосибирск: Омский государственный технический университет, 2008. - 233 с.
4. Нопин, С.В. Разработка защищенной от несанкционированного доступа системы IP-телефонии, функционирующей в операционной системе Windows / С.В. Нопин // Научная сессия ТУСУР-2007: Материалы докладов всероссийской научно-технической конференции студентов, аспирантов и молодых ученых, Томск, 3-7 мая, 2007 г. Томск: В-Спектр, 2007. Ч.2. с. 177- 179.
5. Говор Т. А. Обеспечение безопасности современных VOIP-сетей / Т. А. Говор // Радиопромышленность. – 2011.– № 4.– с. 37–43.
6. Докучаев В.А. Защита информации на корпоративных сетях VoIP / В.А. Докучаев, А.В. Шведов // Электросвязь. –2012. –№ 4.– с. 5–8.
7. Макарова О. С. Методика формирования требований по обеспечению информационной безопасности сети IP-телефонии от угроз среднестатистического «хакера» / О. С. Макарова // Докл. Томского государственного университета систем управления и радиоэлектроники. – 2012.–№ 1. с. 51–67.
8. Крюков, Ю. С. Безопасность VolP-контента. Текущая ситуация, анализ угроз и тенденции рынка / Ю. С. Крюков // Защита информации. INSIDE. – 2008. - №.3.– с. 83-99
9. Onica E. Securing the Media Stream Inside VoIP SIP Based Sessions Technical Report. /Onica E.// Technical report TR 09-01, October 2009. Режим доступу: http://thor.info.uaic.ro/~tr/tr09-01.pdf (Дата звернення: 25.09.2020).
10. Bresciani R. ProVerif Analysis of the ZRTP Protocol/ Bresciani R. Butterfield A.// International Journal for Infonomics. – 2010. – V.3. – №3. – P.306–313
11. Атрощенко В.А. К вопросу оценки достоверности информации для предотвращения MITM-атаки при передаче закрытой информации по открытым каналам связи / Атрощенко В.А., Руденко М.В., Дьяченко Р.А., Багдасарян Р.Х. //Современные проблемы науки и образования. –2013– №. 3. – с. 82-88.
12. Canteaut A. Sieve-in-the-middle: improved mitm attacks /Canteaut A., Naya- Plasencia M., Vayssière B.// Lecture Notes in Computer Science. 2013.

T. 8042 LNCS. № PART 1. С. 222-240. Режим доступу: http://eprint.iacr.org/2013/324.pdf (Дата звернення: 22.09.2020)

13. Sun H. Survey of authentication in mobile IPv6 network /Sun H., Song J., Chen Z. // 2010 7th IEEE Consumer Communications and Networking Conference, CCNC 2010 Las Vegas, NV, 2010. С. 1-4.

14. Радивилова, Т.А., Анализ основных атак на dns-сервер и методы использования DNSSec при защите DNS-сервера / Т.А. Радивилова, В.С. Бушманов // Технологический аудит и резервы производства. –2013– Т. 2. № 1 (10).– С. 16-19.

15. Карпухин, Е.О., Метод формирования сетевых пакетов для защиты от информационных атак «человек посередине» в телекоммуникационных сетях / Е.О. Карпухин, В.Ю. Михайлов // Вопросы радиоэлектроники. – 2013– Т. 3. № 2. – С. 83-93.

16. Сухов, А. М. Научные основы анализа качества интернет трафика: диссертация на соискание ученой степени доктора технических наук по специальности 05.13.13/ Сухов Андрей Михайлович– Самара.:2007– 232 с.

17. Мошак, Н.Н. Модель сигнального трафика в защищенной мультисервисной сети / Н.Н. Мошак, С.Р. Рудинская// XVIII международная научно-техническая конфереция «Современные средства связи». Минск, 15-16 октября 2013 г.: Материалы конференции / Высший государственный колледж связи. – г. Минск, 2013. – С. 45-47

18. Федосеева, О.С. "Исследование особенностей обеспечения характеристик качества обслуживания различных типов трафика в NGN-мультисервисных сетях" [Електронний ресурс] / О. С. Федосеева – Режим доступу: http://masters.donntu.edu.ua/2007/kita/fedoseeva/diss/diss.htm (Дата звернення: 22.09.2020)

19. E. Gelenbe Cognitive Packet Networks: QoS and Performance / E. Gelenbe, R. Lent, A. Montuori , Z. Xu // School of Electrical Engineering and Computer Science, University of Central Florida, Orlando, FL 32816 [Електронний ресурс] – Режим доступу:http://pdf.aminer.org/000/339/717/cognitive_routing_in_packet_networks.pdf (Дата звернення: 22.09.2020)

20. Lijing Ding Performance Study of Objective Voice Quality Measures in VoIP/ Lijing Ding, Radwan, A., El-Hennawey, M.S., Goubran, R.A.//ISCC 2007: P. 197-202 Режим доступу: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=4381543&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D4381543 (Дата звернення: 22.09.2020)

21. Nikitin V., Yurkin D., Chilamkurti N. The influence of the cryptographic protocols on the quality of the radio transmission . // Proc. of International Conference on Ultra Modern Telecommunications. – ICUMT-2009, St.-Petersburg, Russia. P. 1–5.

22. Никитин, В. Н. Улучшение способов аутентификации для

каналов связи с ошибками / В. Н. Никитин, Д. В. Юркин // Информационно-управляющие системы. – №6. – 2010. –С .42–46.

23. Никитин, В.Н. Анализ протоколов шифрования / В.Н. Никитин, Д.В. Юркин // Журнал радиоэлектроники. – 2009. – № 4. – С. 7.

24. Нсангу М. М. Разработка вероятностных моделей для анализа показателей эффективности установления сессий в мультисервисной сети : диссертация на соискание ученой степени кандидата физико-математических наук по специальности 05.13.17 / Нсангу Мушили Мама – М.:2012 – 105 с.

25. Об утверждении Требований к организационно-техническому обеспечению устойчивого функционирования сети связи общего пользования/ приказ Министерства информационных технологий и связи Российской Федерации от 27.09.2007 № 113. Минюст РФ 22 октября 2007 г. N 10380. [Електронний ресурс] – Режим доступу справ.- правовая система «КонсультантПлюс».

26. Ковцур М.М. Методы повышения информационной безопасности IP-телефонии с учётом вероятностно-временных характеристик протоколов распределения ключей. – 2016 –С. 12-141.

27. ГОСТ Р ИСО/МЭК 15408-2-2013 - Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности– 2013 – М.: Изд. Стандартинформ России, 2014.

28. Лопатников Л. И. Экономико-математический словарь: Словарь современной экономической науки./ Л. И. Лопатников — 5-е изд., перераб. и доп. — М.: Дело, 2003. — 520 с.

29. Красов, А.В. Методика построения системы обнаружения вторжений для voip-трафика/А.В. Красов, Д.И. Кириллов //63-я научно-техническая конференция профессорско-преподавательского состава, научных сотрудников и аспирантов СПбГУТ. – СПб.: СПбГУТ, 2011, т1. – С.248-249.//Фундаментальные исследования. – 2014 – № 8(часть 6). – С. 1300-1308.

30. Статистика уязвимостей корпоративных информационных систем (2013 год)[Електронний ресурс]. — Режим доступу: http://www.ptsecurity.ru/download/PT_Corporate_vulnerability_2014_rus.pdf (Дата звернення: 20.09.20).

31. PGPfone Pretty Good Privacy Phone Owner’s Manual ,Version 1.0 beta 7 -8 July 1996 Philip R. Zimmermann [Електронний ресурс]. — Режим доступу: ftp://ftp.pgpi.org/pub/pgp/pgpfone/manual/pgpfone10b7.pdf (Дата звернення: 29.10.2020).

32. АНБ занимается экономическим шпионажем [Електронний ресурс]. — Режим доступу: http://www.securitylab.ru/news/444645.php/ (Дата звернення: 01.10.20).

33. Facebook не может защитить пользователей от MITM-атак

[Електронний ресурс]. — Режим доступу: http://www.securitylab.ru/news/450391.php / (Дата звернення: 01.10.20).

34. Wi-Fi spies - 34% use no protection at Wi-Fi hot spots [Електронний ресурс]. - Режим доступу: http://www.kaspersky.com/about/news/press/2013/Wi-Fi_spies_-_34_percent_use_no_protection_at_Wi-Fi_hot_spots /(Дата звернення: 01.10.20).

35. Таргетированные MiTM-атаки с перенаправлением интернет-трафика по BGP [Электронный ресурс]. — Режим доступа: http://www.xakep.ru/post/61620/default.asp (дата обращения: 01.09.2020).

36. Шварцман, В.О. Теория передачи дискретной информации: учебник для вузов связи/ В.О. Шварцман, Г.А. Емельянов. – М.: Связь, 1979. – 424 с.

37. Радько, Н.М Сравнительная оценка вероятностно-временных характеристик преодоления парольной защиты/ Н.М.Радько, В.М. Аксютин, Д.Н. Курдяев, А.С. Суховерхов // Информация и безопасность. – 2007. –Т. 10. № 3.– С. 439-444.

38. Advanced Encryption Standard [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org/wiki/Advanced_Encryption_Standard (Дата обращения 02.09.2020)

39. C++ Implementation of ZRTP protocol - GNU ZRTP C++ [Електронний ресурс]. – Режим доступу: https://github.com/wernerd/ZRTPCPP (Дата звернення 12.10.2020)

40. ZRTP Protocol Library [Електронний ресурс]. – Режим доступу: http://freecode.com/projects/libzrtpcpp (Дата звернення 10.10.2020)

41. Перфильев, Ю.Ю. Российское интернет-пространство: развитие и структура / Ю.Ю. Перфильев. – М.:Гардарики, 2003. – 272 с.

42. Коржик, В. И. Основы криптографии/ В. И. Коржик, В. П. Просихин – СПб.: Линк, 2008. – 256 с.

43. Пат. 2183348 Российская Федерация, G06F12/14, H04L9/32. Способ аутентификации объектов/ Молдовян А. А., Молдовян Н. А., Никитин В. Н., Фокин А. О. – № 2000119274/09; заявл. 19.07.2000; опубл. 10.06.2002, Бюл. № 6. – 9 с.: ил.

44. Кирюшкин, С.А. Трансграничный юридически-значимый документооборот: нюансы решений актуального вопроса / С.А. Кирюшкин // Connect! Мир связи – 2011. – № 4. – С. 120-123.

45. Юркин, Д.В. Сравнение стойкости реализаций протокола при выборе различных криптографических систем / Юркин Д.В., Никитин В.Н.// Защита информации. Инсайд. – 2008. №6.–С. 17–21.

46. Eppinger, S. D. Generalized Models of Design Iteration Using Signal Flow Graphs / S. D. Eppinger, M. V. Nukala, D. E. Whitney // Research in Engineering Design. – 1997.– V. 9, – No. 2 – C. 112-123.

47. Никитин, В. Н. Улучшение способов аутентификации для каналов связи с ошибками / В. Н. Никитин, Д. В. Юркин // Информационно-управляющие системы. – 2010 – №6.– С. 42–46.

48. RFC6347 (01/2012) Datagram Transport Layer Security Version 1.2 [Електронний ресурс]. – Режим доступу: http://tools.ietf.org/html/rfc6347 (Дата звернення 02.09.2020)

49. RFC 6298 - Computing TCP\x27s Retransmission Timer RFC6298 [Електронний ресурс]. – Режим доступу: https://tools.ietf.org/html/rfc6298 (Дата звернення 02.09.2020)

50. Menezes, A. J. Handbook of Applied Cryptography / A. J. Menezes, P. C. van Oorschot, S. A. Vanstone. – CRC Press LLC, 1996. – 780 p.