Міністерство освіти і науки України
Сумський державний університет
Кафедра електроніки і комп'ютерної техніки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проєкту
на тему:
«Захист VoIP-телефонії в телекомунікаційних системах»

Завідуючий кафедри А. С. Опанасюк

Керівник проєкту Ю. О. Зубань

Студент групи ТК - 71 А. О. Лізунов

Суми 2021

Сумський державний університет

Факультет денний **Кафедра** електроніки і комп'ютерної техніки

Спеціальність телекомунікації та радіотехніка

ЗАТВЕРДЖУЮ**:**

Зав. кафедри ЕКТ

Опанасюк А. С.

«___» _____ 2021 р.

Завдання

на дипломний проєкт студенту

Лізунову Андрію Олеговичу

(прізвище,ім'я,по батькові)

1. Тема проєкту: «Захист VoIP-телефонії в телекомунікаційних системах»
затверджено наказом університету від «05» травня 2021 р. № 0154-VI

2. Термін здачі студентом закінченого проєкту 30 травня 2021 р.

3. Вихідні дані до проєкту: розроблена система повинна суттєво підвищити рівень захищеності будь-якої VoIP-системи; впровадити технологічні та профілактичні методи захисту до системи; застосувати протоколи шифрування

4. Зміст розрахунково-пояснювальної записки (перелік питань, які підлягають розробці)

розробка структурної схеми захищеної VoIP-системи

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень) схема передачі повідомлення з використанням симетричного шифрування; схема передачі повідомлення з використанням асиметричного шифрування; структурна схема захищеної VoIP-мережі

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів дипломного проєкту	Термін виконання етапів проєкту	Примітка
1.	Огляд літератури за вибраним напрямком роботи	15.04.21	
2.	Аналіз вразливостей VoIP-систем	22.04.21	
3.	Огляд існуючих атак на VoIP-системи	29.04.21	
4.	Вибір методів підвищення рівня захисту VoIP-систем	06.05.21	
5.	Проектування захищеної VoIP-мережі	16.05.21	
6.	Розробка схеми захищеної VoIP-системи	20.05.21	
7.	Оформлення пояснювальної записки	30.05.21	
8.	Рецензування роботи та підготовка до захисту	07.06.21	

Студент-дипломник _____
(підпис)

Керівник проєкту _____
(підпис)

РЕФЕРАТ

Робота містить 57 сторінок, 11 рисунків, 2 таблиці та структурну схему. У даній кваліфікаційній роботі зроблено вибір тематики та виконано розробку структурної схеми для захищеної VoIP-системи, описано актуальність проєктування, розглянуто найпоширеніші типи атак на VoIP та можливі рішення, направлені на захист від них, розглянуто методи шифрування, деякі протоколи, що застосовуються в IP-телефонії, впроваджено дані протоколи, методи шифрування, а також методи захисту від атак до проектованої мережі. Зроблено висновки щодо спроектованої схеми мережі.

Ключові слова: атака, захист, мережа, протокол, сервер, телефонія, шифрування.

Keywords: attack, defense, network, protocol, server, telephony, encryption.

ЗМІСТ

ВСТУП

З приходом VoIP, цифрові засоби зв’язку все більше почали витісняти традиційну телефонію. Voice Over IP (скорочено – VoIP) – це технологія, яка дозволяє здійснювати дзвінки через інтернет за допомогою IP-телефонів. Дана технологія, на відміну від класичної аналогової телефонії, потребує менших витрат, має високий рівень доступності, високі можливості для масштабування, більш чіткий звук при передачі та підвищений рівень захисту.

Однак, на сьогоднішній день проблеми інформаційної безпеки в світі набувають все більшої актуальності [2]. Кожного дня по всьому світові зловмисниками проводяться атаки на мережі підприємств. Результатом цих атак стає витік важливих або навіть критичних даних, а також розповсюдження різноманітних вірусів. Таким чином, метою даної кваліфікаційної роботи є розробка захищеної VoIP-системи з метою її подальшого впровадження на підприємствах.

Дана система повинна використовувати як технологічні, так і профілактичні методи підвищення рівня захисту. Технологічними методами у даному випадку можуть бути такі методи, як шифрування даних при передачі по каналу зв’язку, налаштування віртуальної приватної мережі для віддалених працівників підприємства, налаштування маршрутизаторів на пріоритезацію голосового трафіку, профілактичними – використання надійних паролів та проведення правил з кібербезпеки для працівників фірми.

1. ПЕРЕДАЧА ГОЛОСУ ЧЕРЕЗ ІНТЕРНЕТ

1.1 Що таке VoIP і для чого він потрібен

IP-телефонія або VoIP – дві назви, які використовуються для позначення ряду служб, які забезпечують передачу голосу шляхом використання IP-мережі. Абревіатуру VoIP можна розшифрувати, як «Voice over IP» (IP – Internet Protocol). Дані терміни також можна замінити терміном «інтернет-телефонія». Термін «Інтернет-телефонія» є більш широким, адже має відношення до передачі голосу через глобальну мережу Інтернет, у той час, як VoIP може бути застосований в межах локальної мережі.

1.2 Поняття PSTN

Абревіатуру PSTN можна розшифрувати, як «Public Switched Telephone Network», що перекладається з англійської, як «Телефонна мережа загального користування» або ТМЗК. Даний термін позначає комутовану телефонну мережу, яка обслуговується національними, регіональними , а також локальними операторами зв’язку. Дані у такій мережі передаються по телефонних, підводних лініях, через супутники, а також по волоконно-оптичних кабелях. У момент здійснення виклику виділенням таких ліній зв’язку для двох абонентів займаються комутаційні центри.

1.3 PSTN І VOIP

Не зважаючи на те, що PSTN та VoIP призначені для однієї цілі – передавання голосу на відстані, ці дві технології суттєво відрізняються. Перша використовує комутацію каналів, друга – комутацію пакетів. VoIP використовує інтернет-з’єднання для передачі даних, у той час, як PSTN використовує спеціальні виділені лінії для цієї мети. Із попередньо сказаного випливає, що інформація у VoIP-мережах передається по різним шляхам, у телефонній мережі – через один канал. Для якісної передачі голосу по IP

пропускна здатність ліній повинна дорівнювати щонайменше 100 кб/с, для телефонних ліній цей показник дорівнює 64 кб/с. Масштабування у ТМЗК потребує введення до складу мережі нового обладнання, у VoIP-і для цього

потрібно лише збільшення пропускної здатності обладнання.

1.4 Переваги VoIP над PSTN

Розгортання телефонної мережі за допомогою технології VoIP є набагато вигіднішим, ніж у випадку використання звичайної ТМЗК. Нижче перелічимо кілька суттєвих факторів, аби підтвердити сказане.

По перше, VoIP є менш затратним, порівнюючи з PSTN. Дзвінки, котрі здійснюються через інтернет-лінії в межах офісу підприємства, є безкоштовними (не враховуючи витрати на електроенергію). Така мережа є простішою у обслуговуванні, на відміну від телефонної. Як показує практика, обслуговування ТМЗК займає багато часу. При переході на VoIP працівники компанії, які працювали з телефонною мережею, звільняються від значного об’єму роботи. Таким чином, вони можуть бути задіяні в іншій сфері, більш важливій для бізнесу.

У більшості випадків підприємство має потребу не тільки в телефонній мережі. Для ведення ефективного бізнесу компанія потребує підключення до Інтернету. Якщо телефонна мережа буде існувати окремо від інтернет-мережі, це призведе до необхідності обслуговування двох мереж. У результаті цього з’являється потреба у збільшенні числа працівників, і, як результат – витрати компанії зростають.

Розширення VoIP-мережі, на відміну від звичайної ТМЗК, не потребує суттєвих затрат.

1.5 Софтфони та хардфони

У даному підрозділі ми розглянемо, що являють собою софтфони та хардфони, а також їх переваги та недоліки.

1.5.1 Хардфони

Хардфонами або IP-телефонами називають апаратні пристрої для проведення розмов між віддаленими абонентами через Інтернет або локальні мережі. IP-телефон виглядає, як звичайний телефонний апарат: він має трубку, клавіатуру для набору номера, а також дисплей. Суттєвою відмінністю від звичайного телефону є те, що хардфон має інтерфейс для підключення до IP-мережі.

Такий пристрій може мати такі додаткові функції, як переадресація та утримання виклику, здійснення дзвінків між декількома абонентами одночасно (конференції) та інші.

Хардфон працює на основі протоколу SIP або H.323 (дані протоколи розглядаються в розділі 5).

1.5.2 Переваги та недоліки IP-телефонів

IP-телефони, на відміну від софтфонів, про які ми поговоримо пізніше, є апаратно реалізованим пристроєм. Такий пристрій призначений тільки для однієї функції – здійснення дзвінків, при достатній смузі пропускання для голосового трафіку, існує мінімальна кількість факторів, що можуть вплинути на продуктивність його роботи. Однією з помітних переваг хардфона є те, що він може прийняти виклик у будь-який момент часу, софтфон же цього зробити не може (у наступних підрозділах розглянемо, чому). Ця особливість є особливо важливою для бізнесу, адже пропуск телефонного дзвінка, наприклад, від потенційного партнера, може призвести до чималих збитків.

Апаратний IP-телефон є менш вразливим до хакерських атак, ніж софтфон, так як для вторгнення та перехоплення даних зловмисник повинен мати більше ресурсів та навичок.

1.5.3 Софтфони

Софтфоном (від «software telephone») називають програмний продукт, котрий дозволяє здійснювати Інтернет-дзвінки. Софтфон може бути інстальований на персональному комп'ютері або смартфоні. Для здійснення дзвінків за допомогою даного програмного рішення комп'ютер (телефон) повинен мати підключення до Інтернету, мікрофон та веб-камеру (у випадку відео-дзвінків).

Як і хардфони, софтфони розроблені на основі протоколів зв'язку SIP та H.323. До софтфонів відносять такі програми, як ZoiPer, 3CX, Bria тощо. Крім того, відносно нещодавно у різних месенджерах, а також соцмережах, таких як Telegram, Viber, Instagram, почали з'являтися функції голосових та відео-викликів.

1.5.4 Переваги та недоліки софтфонів

Основним недоліком цього програмного рішення перед хардфонами є те, що воно використовується не в спеціалізованому середовищі. Іншими словами, софтфон зазвичай встановлюється на пристрої з великою кількістю інших програм. Із цього випливає, що при інтенсивному навантаженні на систему (при одночасному використанні багатьох програм), пристрій може зависнути, в результаті чого, абонент може пропустити важливий дзвінок. Також може виникнути ситуація, коли система потребує оновлень через Інтернет.)До того ж, при використанні софтфону абонент може прийняти виклик лише у випадку, коли комп'ютер увімкнений та програму-софтфон запущено.

Ще одним недоліком програмної реалізації IP-телефонів є те, що паролі від акаунтів користувачів знаходяться на серверах компаній-розробників програм-софтфонів. Захищеність цих даних лежить на плечах цих компаній. В історії не один раз бували випадки, коли конфіденційні дані потрапляли до рук хакерів.

Основними перевагами софтфону над апаратним IP-телефоном є можливість здійснення відео-викликів, надсилання текстових повідомлень, функція онлайн-статусу, багатофункціональний інтерфейс та велика телефонна книга.

1.6 Компоненти VoIP-мережі

1.6.1 User agent

User agent або клієнт – це назва для кінцевих пристроїв, котрі підтримують протокол SIP (даний протокол розглядається у розділі), а також інші протоколи, які є необхідними для проведення голосового або відео-виклику через VoIP. User agent може бути софтфоном або хардфоном, а також Proxy-сервером (розглядається у наступних підрозділах).

1.6.2 Registrar server

Registrar або сервер реєстрації – спеціальний сервер, який обробляє запити про реєстрацію абонента та зберігає, наприклад, таку інформацію, як місцезнаходження абонента, до бази даних. Це потрібно для того, щоб, наприклад, у випадку, коли робітник фірми тимчасово буде переведеним до іншого офісу, дзвінки, які надходять на старе місцезнаходження телефону цього працівника, були переспрямовані до нового офісу.

1.6.3 Redirect server

Redirect server або сервер переспрямування – сервер, який здійснює переспрямування викликів. Після отримання запитів, даний сервер надсилає відповідь, яка має певний код та містить IP-адресу абонента. Якщо місцезнаходження клієнта, до якого намагається додзвонитися інший клієнт, змінилося, сервер переспрямування повинен повідомити клієнта про це. Після отримання інформації про нове місцезнаходження, один із клієнтів виконає повторне ініціювання виклику, використовуючи ці нові дані. Часто у якості сервера переспрямування виступає клієнтський софтфон або хардфон, на якому є налаштованою функція переадресації.

1.6.4 Proxy server

Proxy-сервер є компонентом VoIP-мережі, котрий може виступати в ролі як клієнта, так і сервера та здійснювати запити від імені клієнтів. Proxy-сервер виконує маршрутизацію пакетів. Запити клієнта, які він не може відправити напряму до іншого клієнта, маршрутизуються через proxy. Крім того, proxy-сервер здійснює контроль доступу абонентів до сервісів. Наприклад, він може отримувати інформацію про те, чи вистачає є «доступним» абонент тощо. Основна робота proxy-сервера – доставка SIP-запитів та SIP-відповідей клієнта. Він може вносити зміни до SIP-повідомлень та переправляти модифіковані повідомлення до інших елементів мережі, які знаходяться на шляху маршрутизації цих повідомлень.

1.6.5 Back-to-Back user agent

Back-to-Back user agent або скорочено – B2BUA – це компонент VoIP-мережі, який здійснює підтримку SIP-діалогу між двома абонентами. Даний елемент умовно поділяє канал зв’язку на дві гілки (або ще їх іноді називають ногами). Даний елемент виконує наступні функції:

- керування викликами (завершення дзвінка, білінг (облік даних про кошти на рахунках користувачів тощо));
- приховування топології мережі та приватних IP-адрес;
- мережеву взаємодію.

Під розподілом лінії зв'язку на дві гілки мається те, що B2BUA обробляє виклик таким чином, щоб для двох абонентів «здавалося», ніби вони з'єднані між собою напряму. Таким чином, за допомогою B2BUA, кінцевий користувач «не бачить» шлях проходження даних по мережі.

2. ЗАХИЩЕНІСТЬ VOIP-СИСТЕМ

2.1 Вразливість VoIP-систем

Не завжди дані, які передаються по мережі, можуть бути захищені. Так як при передаванні від одного користувача до іншого вони прямують по мережі Інтернет, вони можуть бути перехоплені.

При використанні телефонних IP-мереж у межах офісу без наявних каналів зв'язку до глобальної мережі, VoIP, так само, як і звичайна телефонна мережа, є захищеним. У цьому випадку дані є відносно захищені. Відносність пояснюється тим, що конфіденційна інформація, яка передається у межах локальної мережі підприємства, може бути використана у будь-яких цілях зловмисником, який потрапив до офісу.

При здійсненні дзвінків за межі офісу дані, що передаються, є вразливими до зовнішніх атак. У процесі виконання виклику бере участь ряд протоколів. До цих протоколів відносять SIP (Session Initiation Protocol), RTP (Real-Time Transport Protocol), SDP (Session Description Protocol), MGCP (Media Gateway Control Protocol) та ін. Структуру та призначення даних протоколів ми розглянемо у наступних розділах. Згадані протоколи є засобами зв'язку між внутрішньою мережею підприємства та Інтернетом. Таким чином, за допомогою вразливостей цих протоколів зловмисник може отримати доступ до мережевої інфраструктури компанії. Щоб запобігти цьому існує ряд

методів, які направлені на підвищення рівня захищеності телефонних IP-мереж (ці методи розглядаються у розділі 4).

2.2 Способи атак на VoIP-мережу

Зловмисники зазвичай шукають найбільш вразливі місця VoIP-систем та намагаються їх атакувати. Існує набір атак, якими вони найчастіше користуються. Ці атаки можна розділити на певні класи, до яких відносять: прослуховування, спуфінг, DoS-атаки (DoS – Denial of Service), Toll-Fraud, а також спам. Задля того, щоб захистити мережу підприємства від потенційних атак, вона має бути правильно налаштована до того, як буде під'єднана до Інтернету.

2.3 Прослуховування

Прослуховування або снiфінг – вид атаки, при якій зловмисник використовує програмні або апаратні засоби з метою перехоплення мережевого трафіку для збору загальної інформації про мережу. Ця інформація може бути використана ним для підготування подальших атак. Якщо даний вид атаки направлений на VoIP-мережу, атакуюча сторона може отримати інформацію сигнальних протоколів або медіа-дані, які передаються між абонентами.

2.3.1 Можливі рішення, направлені на захист від прослуховування

До засобів та методів, направлених на запобігання снiфінгу відносять наступні:

- обмеження списку MAC-адрес, котрі мають доступ до певних портів мережевого обладнання;
- профілактика мережі за допомогою сканування мережі з метою виявлення пристроїв, які працюють у нерозбірливому режимі (коли всі пакети мережі потрапляють на мережевий інтерфейс);

- обмеження фізичного доступу до шаф з електрообладнанням, за виключенням кількох довірених осіб;

2.4 Спуфінг-атаки

Даний тип атаки полягає у тому, що атакуюча сторона намагається ідентифікувати себе у якості авторизованої особи для виконання кібер-атак. Отримавши доступ до мережі підприємства, зловмисник може дістатись до конфіденційної інформації або навіть викликати збої у роботі VoIP-системи. Дуже часто зустрічається випадок, коли злочинці намагаються отримати доступ до мережі жертви за допомогою фішингових атак. Фішингова атака – це вид атаки, при якій зловмисник відправляє жертві електронні листи від імені уповноважених сторін з метою отримання персональної інформації, такої, як паролі і т. п.

2.4.1 Можливі рішення, направлені на захист від спуфінг-атак

До методів та порад, направлених на запобігання спуфінгу відносять наступні:

- двофакторна аутентифікація та шифрування;
- використання надійних паролів;
- вихід з акаунтів після завершення сесії;
- періодична зміна паролів;
- не відкривайте електронні листи від невідомих осіб.

2.5 DoS-атаки

«Deny of Service» або «Відмова у обслуговуванні» - вид атаки, направлений на зниження працездатності або виведення мережі та мережевого обладнання із ладу за допомогою фіктивних запитів. До атак цього типу відносять наступні:

- затоплення SYN-пакетами;

- затоплення ICMP-пакетами;
- атака пропускної здатності та ін.

У випадку VoIP-обладнання, даний вид атаки може привести до виведення із ладу IP-телефонів підприємства. Уявіть ситуацію, коли важливі переговори між представниками різних компаній будуть зірвані внаслідок DoS-атаки на одну із них. Така атака може проводитися протягом значного відрізку часу, за який компанія може зазнати серйозних фінансових втрат. Тому дуже важливим є захист мережевої інфраструктури від потенційних DoS-атак.

2.5.1 Можливі рішення, направлені на захист від DoS-атак

До методів та засобів, направлених на запобігання DoS-атакам у VoIP-системах, відносять наступні:
- використання фаєрволів (міжмережевих екранів);
- моніторинг та фільтрація з метою виявлення підозрілих користувачів та подальшого обмеження їх можливостей на ініціювання нових сесій;

- автентифікація користувачів перед відправленням даних у мережу;

2.6 Toll-Fraud

Toll Fraud (у перекладі з англ. – шахрайство за допомогою телефонного зв'язку) – це тип атаки, при якій атакуюча сторона генерує дуже великі об'єми трафіку через інтернаціональні або дорогі маршрути за рахунок жертви. За даними CFCA (Communications Fraud Control Association) у 2018 році втрати телефонних систем компаній, які стали жертвами атаки даного типу, становлять 28 мільярдів доларів США.

Постає питання, як саме шахраї заробляють на здійсненні дзвінків за рахунок компаній. Дійсно, яка, здавалося б, користь зловмиснику від того, що фірма втрачає гроші? Справа у тому, що існують певні провайдери телеком-

зв’язку, які співпрацюють з шахраями. Після отримання доступу до мережевого обладнання певного підприємства, злочинець зможе здійснювати дорогі дзвінки за рахунок жертви. Таким чином, оператори зв’язку ділять дохід, отриманий з цих дзвінків, зі зловмисниками.

Для будь-якого підприємства дуже важливо захистити себе від даного типу атак, адже toll-fraud може з великою імовірністю може призвести до падіння бізнесу.

2.6.1 Можливі рішення, направлені на захист від Toll-Fraud-атак

До методів та засобів, направлених на запобігання Toll-Fraud-атакам, відносять наступні:

- налаштування фаєрволів на приймання викликів тільки з довірених підмереж;
- проведення сканування маршрутизаторів мережі з метою виявлення відкритих портів (результат сканування не повинен виявити відкритих SIP, SCCP або H.323-портів);
- обмеження кількості та тривалості дзвінків, які можуть бути виконані за один день.

2.7 Спам-атаки

Даний вид атаки також називають «Spam over Internet Telephony» (SPIT), що у перекладі з англійської означає «Спам через Інтернет-телефонію». Для нього існує наступне визначення: «SPIT – набір небажаних спроб ініціації голосового, відео-зв’язку, а також інших типів комунікації». При успішній ініціалізації виклику, спамер починає поширювати інформацію, яка не має практичної користі для приймальної сторони. Ця атака є досить серйозною, адже потребує засобів захисту у реальному часі. Уявіть, наприклад, наступну ситуацію: у фірми А є 20 VoIP-телефонів, і до офісу через певні проміжки часу дзвонить десять спамерів. Абонент на приймальній стороні не має жодної уяви

про те, хто саме здійснює виклик. Піднявши слухавку, він чує голосові повідомлення рекламного характеру. На те, щоб отримати інформацію, з ким він веде розмову, робітник витрать певний час. На обслуговування виклику витрачається електроенергія, а також цінний час, у який працівник міг би прийняти інший виклик. Слід взяти до уваги, що такі дзвінки можуть, до речі, виснажувати персонал. Уявіть, наскільки виснажливим буде прийняття десяти таких викликів. Даний вид атаки також несе певні втрати для бізнесу, тому потрібні певні механізми захисту для запобігання SPIT.

2.7.1 Можливі рішення, направлені на захист від SPIT

До методів та засобів, які можна направити на захист від SPIT, відносять наступні:

- ведення чорних списків для ряду IP-адрес (наприклад, за допомогою міжмережевих екранів). Даний метод полягає у можливості блокування операції ініціювання виклику для певних IP-адрес. Він є робочим то тих пір, поки спамер не змінить свою IP-адресу. У ситуації, що описана у попередньому розділі, даний метод міг би стати у нагоді. Додавши IP-адреси зловмисників до чорного списку, вони більше не змогли б організувати спам-атаку на офіс компанії. Навіть у випадку зміни Інтернет-адрес зловмисниками, нові адреси можуть бути додані до чорного списку. Плюсом даної ситуації є

те, що кількість доступних глобальних IP-адрес, якими можуть скористатися спамери, є обмеженою, а отримання нових є затратною процедурою, що не є вигідним для зловмисника.

- Проведення інструктажу з безпеки під час телефонних дзвінків. Бувають ситуації, коли зловмисник намагається здобути конфіденційну інформацію (наприклад, логіни, паролі та ін.) за допомогою соціальної інженерії, тому персонал повинен знати, яку інформацію можна повідомляти під час виклику, а яку – ні.

3. СПОСОБИ ПІДВИЩЕННЯ РІВНЯ ЗАХИСТУ VOIP-СИСТЕМ

3.1 VPN

Одним із дієвих способів захисту VoIP-мережі від зовнішніх атак є впровадження VPN на підприємстві. VPN (Virtual Private Network) у перекладі з англійської – «віртуальна приватна мережа». Даним терміном позначають сукупність певних мереж, об'єднаних у єдину ізольовану (приватну) мережу.

Ця технологія прийшла на зміну виділеним каналам, так як на її розгортання потребується менше грошових ресурсів, що дуже вигідно для будь-якого бізнесу, де конфіденційність даних є критичною. Також однією з суттєвих переваг VPN над класичними виділеними лініями є те, що дана технологія використовує канали не з комутацією каналів, а пакетів (наприклад, IP або Ethernet). Це дозволяє економити на купівлі додаткових каналів зв'язку, що не можна сказати про випадок з комутацією каналів.

Виділяють два типи VPN, у залежності від того, ким реалізовується технологія – клієнтом або провайдером: «віртуальна мережа, що підтримується провайдером» (Provider Provisioned Virtual Private Network, PPVPN) та «віртуальна мережа, що підтримується клієнтом» (Customer Provided Virtual Private Network, CPVPN).

У першому випадку обов'язки по обслуговуванню та налаштуванню мережі накладаються на провайдера послуги, у випадку другої – на клієнта, тобто робітників компанії. При використанні CPVPN від провайдера потребується тільки надання доступу до Інтернету. PPVPN має більше переваг над CPVPN, адже провайдер має фізичний доступ до усіх свої ліній зв'язку та може сконструювати їх так, аби відокремити мережі різних клієнтів одне від одного. Клієнт же цього самостійно зробити не може. CPVPN більш вигідний у тому випадку, коли компанія має декілька офісів, близько розташованих географічно. У такому випадку шлях проходження пакетів буде невеликим, а з цього випливає що, кількість вразливих місць у мережі буде меншою.

Обслуговування такої мережі буде набагато легшим, ніж, наприклад, у випадку, коли офіси компанії розкидані по всьому світу. Мережі VPN, які обслуговуються клієнтом, зазвичай використовують шифрування та тунелювання трафіку.

У залежності від того, який рівень використовується при впровадженні даної технології, VPN поділяють:

- на VPN другого рівня (канального);
- на VPN третього рівня (мережевого).

Ми ж будемо розглядати тільки VPN третього рівня, так як він застосовується частіше.

3.1.1 VPN третього рівня

У випадку VPN третього рівня мережі клієнтів об’єднуються на основі інформації третього рівня мережевої моделі OSI, або, іншими словами, IP-адрес. Простими словами, при впровадженні даного типу VPN клієнт бачить мережу провайдера у вигляді маршрутизатора, що має декілька інтерфейсів. У місці стиків мереж клієнта (клієнтських інтерфейсів) з інтерфейсами цього так званого маршрутизатора, клієнт сам призначає IP-адреси на своїх маршрутизаторах. Для інтерфейсу, що «дивиться» у локальну мережу клієнта, призначається приватна IP-адреса, а для інтерфейсу, котрий «дивиться» у сторону мережі провайдера – публічна. Для того, щоб реалізувати описане рішення використовується MPLS у зв’язці з протоколом GRE та IPSec.

MPLS або «Multi Protocol Label Switching», що у перекладі з англійської мови означає «багатопротокольна комутація за позначками» – технологія передачі даних, яка використовує спеціальні «транспортні» позначки для визначення шляху проходження даних по мережі та використовує для цього будь-який протокол. Під час проходження даних по мережі позначки за необхідності можуть або додаватися, або видалятися, при чому вміст пакетів не змінюється та не аналізується.

Терміном IPSec або «IP Security» називають набір протоколів захисту даних, які передаються за допомогою IP (сюди відноситься шифрування, перевірка цілісності даних та підтвердження автентичності даних).

GRE або «Generic Routing Encapsulation» – протокол тунелювання та пакування даних (пакетів), за допомогою якого встановлюється захищене з'єднання між двома точками з використанням інкапсуляції протоколів на мережевому рівні. До того ж, захищене з'єднання встановлюється за допомогою логічного зв'язку.

При розгортанні віртуальних мереж MPLS третього рівня всю роботу по підтримці VPN виконують спеціальні суміжні маршрутизатори PE (PE – від Provider Edge), а для передачі MPLS пакетів використовуються внутрішні маршрутизатори провайдера P.

3.1.2 Маршрутизація пакетів у VPN

Усю роботу по маршрутизації пакетів виконують прикордонні маршрутизатори провайдера PE і P. На рис 3.1 зображена спрощена топологія, яка показує, як саме розміщується мережеве обладнання провайдера та клієнта, яке виконує операції маршрутизації трафіку при розгортанні VPN.

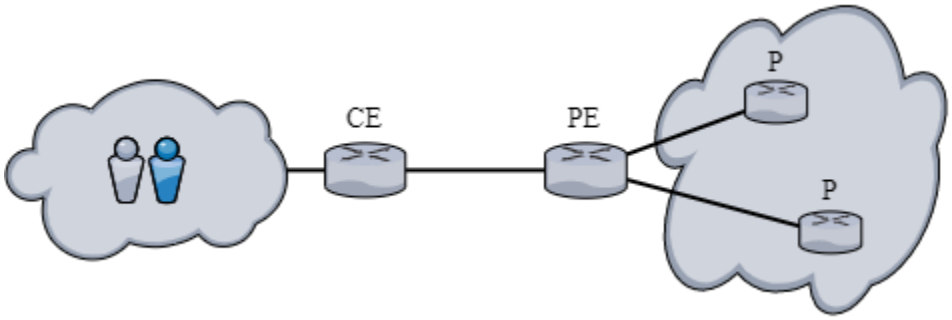

Рисунок 3.1 – спрощена топологія обладнання, яке виконує маршрутизацію у VPN-мережі.

До мереж клієнтів не повинна потрапляти маршрутна інформація про мережі провайдера, вона повинна триматися у секреті. Водночас з цим, для коректної роботи VPN, маршрутна інформація про мережі клієнта повинна бути відома тільки в межах його VPN-мережі та мережі провайдера.

Прикордонний маршрутизатор PE виконує функцію обміну маршрутною інформацією з клієнтськими маршрутизаторами CE, інтерфейси яких з'єднані з інтерфейсами першим. Обмін інформацією між CE та PE про маршрути клієнта здійснюється за допомогою одного з протоколів маршрутизації класу IGP.

IGP або «Interior Gateway Protocol» (у перекладі з англійської – «протокол внутрішнього шлюзу») – це тип протоколу, що застосовується для автоматичного обміну маршрутною інформацією між шлюзами, яка може бути використана для маршрутизації протоколів мережевого рівня (наприклад, IP). До даного типу відносять протоколи RIP (Routing Information Protocol), OSPF (Open Shortest Path First), EIGRP (Enhanced Interior Gateway Routing Protocol), а також IS-IS (Intermediate System to Intermediate System).

Перелічені протоколи дозволяють маршрутизатору PE отримувати інформацію про доступність мереж клієнта. До функцій роутера PE також входить збір маршрутної інформації від інших прикордонних маршрутизаторів провайдера та маршрутизаторів P із внутрішньої мережі провайдера.

Для того, щоб реалізувати основну функцію мережі VPN, протоколи маршрутизації на PE повинні бути налаштовані на прийом та передачу маршрутної інформації у залежності від інтерфейсу та відправника повідомлень. Іншими словами, PE повинен знати, від кого та з якого інтерфейсу йому слід приймати повідомлення з інформацією про маршрути, а також на які інтерфейси та кому їх переправляти.

На прикордонному маршрутизаторі PE може бути встановлено декілька екземплярів протоколів класу IGP, кожен з яких буде приймати та обробляти маршрутну інформацію від різних джерел. Наприклад, один екземпляр протоколу може обробляти маршрутну інформацію, котра надходить від клієнтського обладнання, а інший – від обладнання провайдера, тобто внутрішніх маршрутизаторів провайдера P.

Прикордонний маршрутизатор, на основі отриманої від різних сторін інформації, формує таблиці маршрутизації двох типів: одна називається глобальною таблицею маршрутизації, інша – VRF (VPN Routing and Forwarding).

Глобальною таблицею маршрутизації називається таблиця, що формується на PE на основі даних, отриманих із магістральної мережі провайдера (через P). До цієї таблиці входить інформації про маршрути в межах мережі провайдера, клієнтське обладнання не має до неї доступу.

Іншим типом таблиці є таблиця «VPN Routing and Forwarding», що у перекладі з англійської означає «VPN-маршрутизація та переправлення». VRF-таблиця на PE – це таблиця маршрутизації, яка формується на основі маршрутної інформації, отриманої від мереж клієнта, та містить дані про топологію його мережі. До того ж, кожна така таблиця містить не тільки маршрути, інформація про які надходить через напряму під'єднані до PE клієнтські мережі, а й маршрути з інших мереж клієнта, що не є безпосередньо під'єднаними до того самого PE. Це досягається шляхом використання багатопротокольного розширення для BGP (MP-BGP). Цей протокол дозволяє прикордонним маршрутизаторам PE обмінюватися маршрутною інформацією зі своїх VRF-таблиць. Передача цієї інформації відбувається на основі вказаних у конфігураційних параметрах сусідів. Це означає, що дані про маршрути, що містяться у VRF, будуть передаватися не всім суміжним маршрутизаторам PE, а тільки тим, що вказані у конфігурації у якості сусідів.

Маршрутизатори P, на відміну від PE, приймає та обробляє маршрутну інформацію протоколів тільки від обладнання провайдера. Таблиці маршрутизації на них містять інформацію про мережі провайдера.

3.1.3 Особливості призначення адрес у VPN-мережах

У мережах VPN адресний простір є незалежним, тобто, простіше кажучи, одна й та сама IP-адреса у різних приватних віртуальних мережах

клієнта може бути використана декілька разів. Варто взяти до уваги, що адреси не можуть повторюватись у межах однієї конкретної VPN-мережі, у протилежному випадку підмережі клієнта не зможуть взаємодіяти одна з одною.

Ситуація з використанням дубльованого адресного простору у різних мережах VPN є проблемною для прикордонних маршрутизаторів PE. Протокол BGP, за допомогою якого поширюється маршрутна інформація, ідентифікує вузли мережі на основі унікальності IPv4-адреси, тобто він передбачає, що адреси, з якими він працює, є глобально унікальними. BGP працює таким чином, що, отримавши маршрути з різних мереж VPN, котрі мають однакові IPv4-адреси, він буде вважати, що ці маршрути ведуть до одного й того самого вузла. Це означає, що у таблицю VRF буде додано тільки один маршрут.

Дану проблему було вирішено за допомогою впровадження так званого визначника маршрутів (Route Distinguisher, далі RD). RD є складовою частиною адресів нового типу, а саме VPN-IPv4. Даний визначник додається до IPv4-адрес із адресного простору певної мережі VPN у якості префіксу, у результаті чого ми отримуємо VPN-IPv4-маршрут. У якості RD записується або публічна адреса одного з інтерфейсів маршрутизатора PE, або номер автономної системи.

При переправленні маршрутних повідомлень, які містять IP-адреси, відмінні від IPv4, у нагоді розширений протокол MP-BGP, котрий окрім IPv4 здатний обробляти адреси IPX, IPv6 та VPN-IPv4.

Префікс RD додається до IPv4-адреси призначення, яка вказана у маршруті, цим самим робить з нього маршрут VPN-IPv4. Адреси VPN-IPv4 використовуються тільки у межах окремих приватних віртуальних мереж певних клієнтів, які користуються послугами провайдера. Ці адреси передаються по протоколу BGP між сусідніми маршрутизаторами PE як складові частини певних маршрутів.

Коли маршрутизатор PE отримує пакети з маршрутною інформацією, він додає до адреси призначення маршруту префікс RD, враховуючи при цьому до якого сайту (підмережі) клієнта прямує даний маршрут. Різним сайтам призначається різний префікс, навіть якщо маршрути мають однакові IPv4-адреси. IPv4-адреса у парі з префіксом RD може мати вигляд, наприклад, 15.144.82.10:2. Адреси з префіксами передаються між сусідніми PE, що дозволяє протоколу BGP коректно розпізнавати маршрути, навіть якщо IPv4-адреси, котрі відносяться до різних VPN-мереж, співпадають. Після отримання маршруту до мережі VPN-IPv4, прикордонний маршрутизатор PE відкидає RD-префікс та додає отриманий маршрут до таблиці VRF. Після цих операцій інформація про маршрут передається суміжному з PE маршрутизатору клієнта CE, котрий входить до тієї ж VPN-мережі.

3.2 Налаштування маршрутизаторів на підвищення пріоритету голосового трафіка

Тема захищеності VoIP-системи корелює з темою призначення пріоритету голосовому трафіку, що проходить по мережі. Трафіку, що проходить через транзитне обладнання, може бути заданий пріоритет. Завдяки цьому можна, наприклад, налаштувати маршрутизатор таким чином, щоб відсоток голосового трафіку, що проходить через нього, дорівнював 60 відсоткам. Таким чином, у будь-який момент часу, відсоток іншого трафіку, що проходить через маршрутизатор, не буде більшим, ніж 40 відсотків. Це означає, що при проведенні атаки зловмисником на мережу підприємства, він не зможе вивести, наприклад, вивести з ладу мережу підприємства за допомогою DoS-атаки.

У поєднанні з захистом VoIP-мережі, пріоритезація голосового над іншими видами трафіку також гарантує передачу високоякісного сигналу. Під пріоритезацією голосового трафіку мається на увазі надання вищого пріоритету для даних, що пов’язані з сигналізацією та передаванням аудіо.

Із вище сказаного можна зробити висновок, що захист та якість VoIP тісно пов’язані між собою. Для підвищення якості зв’язку, VoIP-трафік повинен мати належну смугу пропускання, компенсацію затримки та джиттеру (jitter).

Джиттером називають різницю між затримками трафіку в різні проміжки часу. Даний показник вважають припустимим, якщо зміни затримки становлять менше, ніж 100 мс. Для того, щоб компенсувати jitter, використовуються спеціальні jitter-буфери.

QoS забезпечує краще обслуговування мережевих сервісів, надаючи наступні привілегії:

- регулювання характеристик втрат;
- підтримка сталої пропускної здатності;
- запобігання виникнення перевантажень мережі та реагування на них;
- призначення пріоритетів для трафіку в мережі.

3.2.1 Роль IP Precedence у пріоритезації VoIP-трафіку

«IP Precedence» у перекладі з англійської означає «Пріоритет IP». IP-пакети мають набір певних полів у своїх заголовках (рис. 3.2). Одним з таких полів є поле «ToS», що розшифровується, як «Тип сервісу» (Type of Service). Головним завданням цього поля є позначення пріоритету трафіку, здійснення запитів маршруту з більшою пропускною здатністю, зменшення затримки сигналів та забезпечення надійності сервісу в цілому. Дане поле також називають ToS-байтом. Для зручності надалі будемо його називати так само.

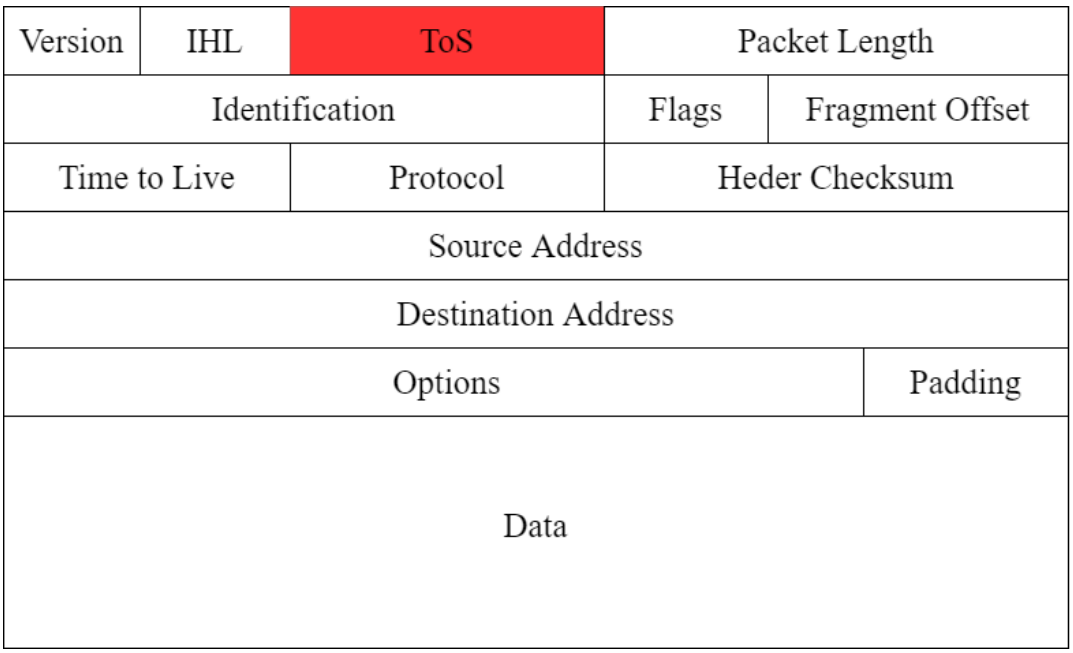

Рисунок 3.2 – структура заголовка IP-пакету.

ToS-байт, як видно з його назви, складається з восьми бітів. Структура цього поля наведена на рис. 3.3. Перші три біти ToS-байту позначають пріоритет пакету. Більше значення відповідає більшому пріоритетові. Пріоритет пакета вступає у дію при виникненні перевантаження мережі: пакети з меншим пріоритетом будуть відкидатися першими. Біти з третього по шостий призначені для вказання типу сервісу. Останній біт розшифровується, як «Must Be Zero» («Повинен бути нульом»), котрий є експериментальним.

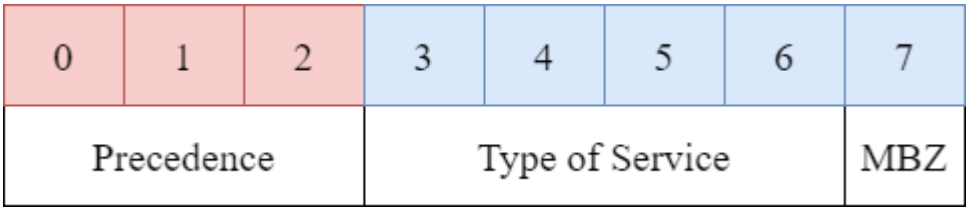

Рисунок 3.3 – стуктура ToS-байту.

Біти, котрі позначають пріоритет, можуть приймати такі значення:

- 000 – Routine;
- 001 – Priority;
- 010 – Immediate;

- 011 – Flash;
- 100 – Flash Override;
- 101 – Critic/Critical;
- 110 – Internetwork Control;
- 111 – Network Control.

Біти, що позначають тип сервісу, можуть приймати наступні значення:

- 1000 – minimize delay;
- 0100 – maximize throughput;
- 0010 – maximize riliablility;
- 0001 – minimize monetary cost;
- 0000 – normal service.

3.2.2 Команди для надання пріоритету VoIP-трафіку

Для того, щоб голосовий трафік передавався по мережі без жодних проблем у реальному часі, повинна бути надана належна смуга пропускання. Наприклад, для VoIP-дзвінка (80 кб/с), який виконується за допомогою кодека G.711, канал зв'язку зі смугою пропускання 64 кб/с буде поганим, адже щонайменше 16 кб пакетів буде відкинуто, що становить близько 20 відсотків.

Для того, щоб задати пріоритет VoIP-трафіку на маршрутизаторі Cisco, який під час виникнення у мережі перевантажень буде дорівнювати 64 кб/с (при цьому веб-трафіку також надається стала смуга пропускання 64 кб/с), потрібно виконати наступні команди у режимі глобальної конфігурації:

- *class-map voip;*
- *match ip precedence 5;*
- *exit;*
- *class-map webtraffic;*
- *match ip precedence 3;*
- *policy-map llq;*
- *class voip;*

- *priority 64;*
- *class webtraffic;*
- *bandwidth 64;*
- *class class-default;*
- *fair-queue.*

Перші п’ять команд створюють клас «voip» для голосового трафіку, пріоритет операцій якого дорівнює 5 (IP precedence 5), та клас «webtraffic» для веб-трафіку з пріоритетом операцій, що дорівнює 3. Усі подальші команди призначені для надання пріоритету голосовому та веб-трафіку і видачі решти смуги пропускання для інших типів трафіку. Виконання перелічених команд на прикладі середовища «Cisco Packet Tracer» показано на рис. 3.4.

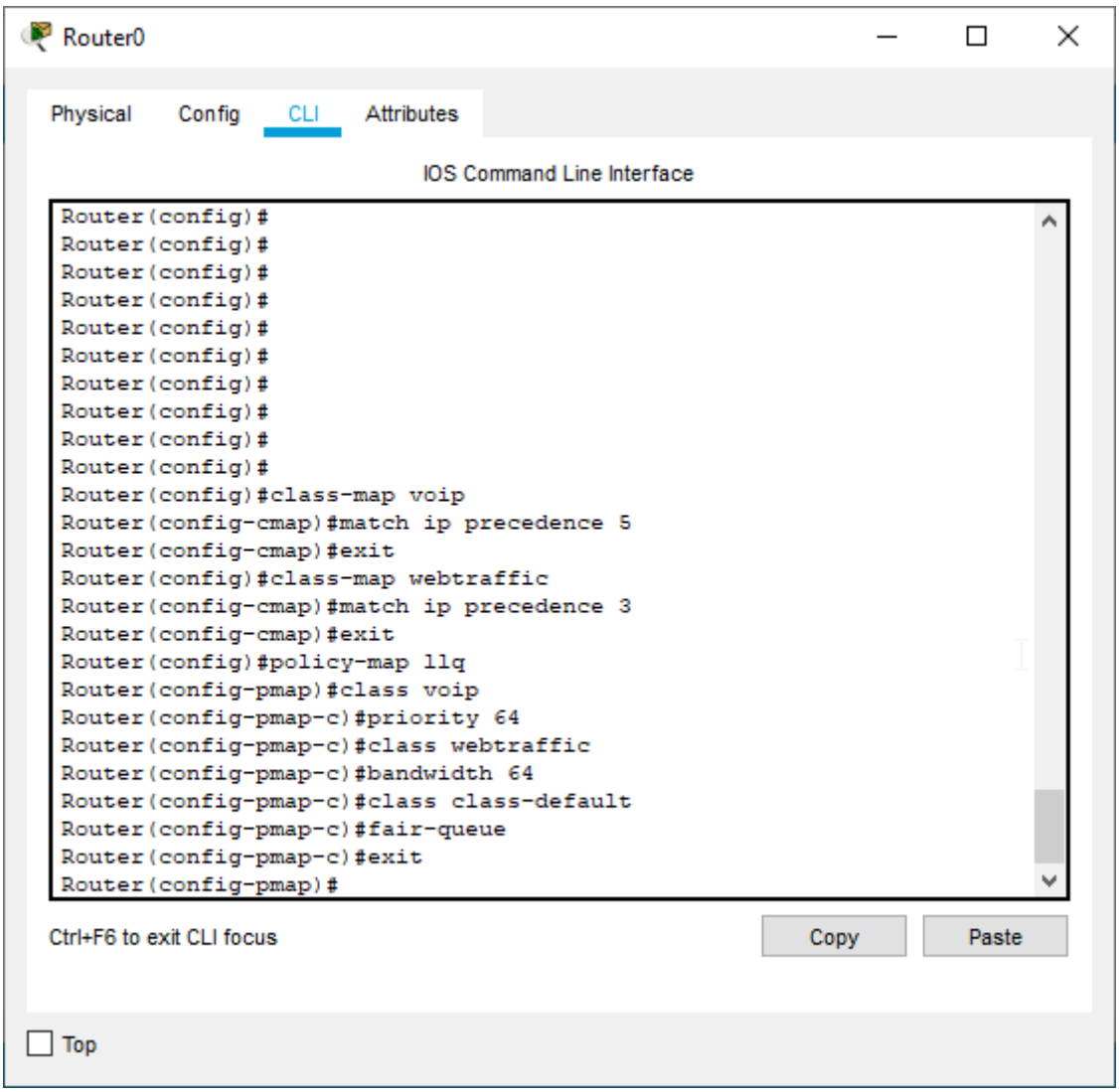

Рисунок 3.4 – команди пріоритезації голосового трафіку на прикладі середовища «Cisco Packet Tracer».

На Linux-роутері, пріоритезацію VoIP-трафіку можна налаштувати за допомогою служби iptables та bwadd. Правила iptables та команди bwadd для цього виглядають наступним чином:

bwadd --dev I-Name --classid 10 --minimum 256Kbit --maximum 1Mbit --priority 1;

-A POSTROUTING -t mangle -o I-Name -d Destination-Network -j CLASSIFY --set-class 1:10;

-A POSTROUTING -t mangle -o I-Name -s Source-Network -j CLASSIFY --set-class 1:10.

Замість «I-Name» вказується ім’я інтерфейсу, а замість «Destination-Network» та «Source-Network» – мережа до якої надсилаються дані та мережа, з якої надходять дані, відповідно.

3.3 Проведення тренінгів з правил кібербезпеки для працівників компанії

Ще одним із методів підвищення рівня захисту VoIP-системи підприємства є проведення спеціальних тренінгів для персоналу фірми. Здавалося б, що такого особливого у звичайних інструктажах? Однак існують ситуації, коли знання простих правил кібербезпеки є необхідною базою для підтримання безпеки більшості інформаційних систем.

Під час проведення тренінгів з кібербезпеки, інструктор повинен донести до працівників фірми ряд основних правил поводження з обладнанням або програмним продуктом. До таких правил можна віднести наступні:

- не під’єднувати зовнішні носії інформації (флешки, диски тощо) до комп’ютерів, якщо їх безпечність є під сумнівом; ні в якому разі працівник фірми не повинен вставляти носій інформації, знайдений, наприклад, на вулиці біля офісу, якщо він не знає, кому цей носій належить та що на ньому зберігається; існує імовірність того, що вірус, який буде на цій флешці (диску тощо) запуститься до того, як буде просканований антивірусом;
- регулярно змінювати паролі та не зберігати дані для входу у систему в легкодоступних місцях; найкраще було б, звичайно, запам’ятовувати всі паролі, але паролі повинні бути складними, з чого випливає, що тримати їх у себе в голові буде важко, тому паролі слід тримати, наприклад, в директоріях та файлах з обмеженими правами доступу;
- паролі не повинні містити дат народження, номерів телефонів, номерів автомобілів тощо, повинні бути унікальними (такими, що не використовуються для входу до інших систем);

- після завершення роботи з програмами та сервісами, працівники фірми повинні виходити зі своїх акаунтів;
- не переходити за посиланнями невідомого походження (наприклад, за посиланнями в електронних листах від невідомих відправників);
- не відкривати та не завантажувати файли невідомого походження, які мають потенційно небезпечне розширення (.py, .js, .sh, .exe, .dll, .cs тощо);

Також існують інші правила кібербезпеки, які не відносяться до інструктажів, але також є не менш важливими для підтримання безпеки інформаційної системи будь-якого підприємства. До них відносять наступне:
- використання антивірусного програмного забезпечення (бажано ліцензійного, так як платні версії зазвичай мають набагато більший функціонал, ніж безкоштовні);
- використання фаєрволів на шляху проходження даних по мережі (наприклад, між глобальною мережею та шлюзом, що сполучає з нею офіс);
- резервне копіювання даних;
- підготовка засобів відновлення системи;
- використання ліцензійного та довіреного програмного забезпечення; програми зі сторонніх сайтів можуть містити віруси;
- ведення списків довірених IP-адрес для підключення за допомогою віддаленого доступу;
- обмеження кількості неправильно введених паролів.

3.4 Шифрування голосового трафіку

3.4.1 Основні поняття

Шифрування – це процес перетворення інформації в інший вигляд, при якому дані не можуть бути розпізнані людиною або машиною без додаткових засобів.

Шифрування є двостороннім процесом. Це означає, що кожне зашифроване повідомлення після певних процедур повинне повертатися до

початкового стану. Процес повернення зашифрованого повідомлення у вихідний стан називають дешифруванням.

Зв’язка цих двох методів утворює нове поняття, яке називають криптосистемою. У будь-якій криптосистемі існують спеціальні правила, за допомогою яких шифрують та дешифрують дані. За цими правилами зазвичай стоїть певна сутність, яку називають ключем. Наприклад, правилом шифрування може бути заміна кожної алфавіту, що використовується, на літеру, зміщену на декілька позицій вперед або назад.

Даний метод шифрування відомий як шифр Цезаря. Він був названий у честь римського полководця Гая Юлія Цезаря, котрий використовував цей метод для військового листування.

Число позицій, на яке зміщається літера вихідного алфавіту, у даному випадку виступає ключем. Наприклад, літера «а», зашифрована шифром Цезаря з ключем «3», мала б вигляд літери «г».

Ключ буває секретним та навпаки, або, іншими словами – закритим та публічним. З цього випливає, що існують методи шифрування, які використовують різні типи ключів. У залежності від того, які ключі використовуються при шифрування, існує два класи криптосистем – симетричні та асиметричні.

Симетричною системою шифрування називають систему, в якій відкритий за закритий ключі шифрування співпадають, тобто є одним елементом. Це означає, що повідомлення, зашифроване одним ключем, може бути ним же розшифроване. Прикладом симетричного шифрування є шифр Цезаря, де літера вихідного алфавіту, зашифрована, наприклад, ключем «3» (зміщена на три позиції), може бути розшифрована зміщенням на три позиції вперед (назад).

Асиметричною системою шифрування називають систему, в якій для операцій шифрування та дешифрування використовуються різні ключі. Це досягається за допомогою спеціальних математичних методів.

3.4.2 Процес передачі повідомлення за допомогою методів симетричного шифрування

На рис. 3.5 наведена схема передачі повідомлення від Боба до Аліси (ці імена зазвичай використовуються у прикладах ситуацій, пов’язаних з темою криптографії). Боб та Аліса заздалегідь домовляються про те, як вони обміняються ключем, який, до того ж, є тільки одним. Для шифрування та дешифрування вони використовують один ключ.

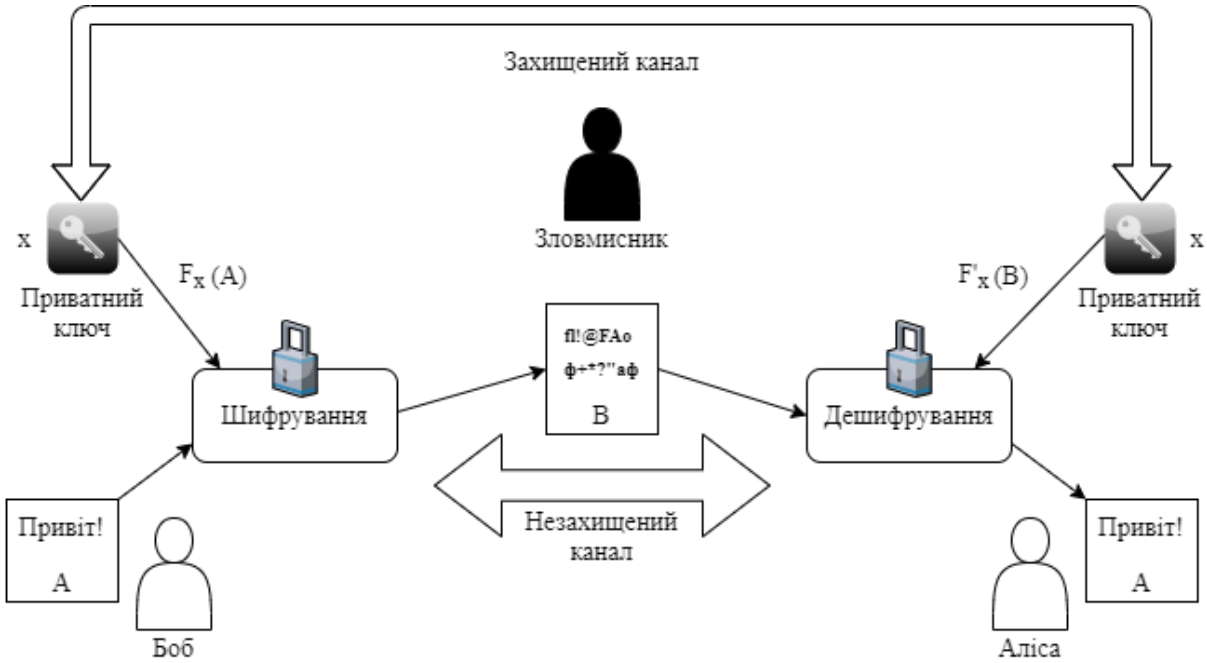

Рисунок 3.5 – схема передачі повідомлення з використанням симетричного шифрування.

У цій ситуації, окрім Боба та Аліси, є ще третя сторона, якою виступає зловмисник. Уявімо, що зловмисник у цій ситуації потенційно може отримати доступ до ліній, через які будуть передаватись повідомлення. Боб та Аліса знають, що лінії зв’язку є вразливими до атак, тому вони вирішують, як саме їм обмінятися ключем. Ключ може бути переданий трьома способами: через незахищену лінію зв’язку, іншу захищену та особисто при зустрічі. Третій спосіб є найкращим, якщо відправник та отримувач повідомлень знаходяться

близько один до одного (живуть в одному місті, на одній вулиці, і т.п.), але не є раціональним, коли дві географічно далеко рознесені (наприклад, знаходяться в різних країнах), перший також не є раціональним, тому залишається тільки другий – передати ключ через захищену лінію зв'язку. Захищеною буде лінія зв'язку, до якої потенційні зловмисники не матимуть фізичного доступу.

Уявимо, що Аліса та Боб вже обмінялися ключем. Боб є відправником повідомлення, Аліса – одержувачем. Нехай Боб передає вихідний незашифрований текст A, який він шифрує за допомогою функції F з ключем x та передає зашифроване повідомлення B через відкритий канал. Аліса, отримавши повідомлення, передає його на вхід функції дешифрування F'. За допомогою цієї функції здійснюється операціє приведення тексту до початкового стану. Функція F' виконує дії функції F у зворотному порядку, при чому ця операція є здійсненною при наявності в Аліси однакового з Бобом закритого ключа. Якщо Аліса захоче відправити повідомлення Бобові, вона має виконати ті ж самі операції, що виконав він для шифрування повідомлення.

3.4.3 Процес передачі повідомлення за допомогою методів асиметричного шифрування

Успішність передачі повідомлення описаним вище способом залежить від надійності захищеного каналу, по якому передається ключ, а також від складності алгоритму шифрування та розміру ключа. Не завжди знайдеться канал зв'язку, по якому можна було б безпечно передати ключ, тому постає проблема, як саме його передати. Тут на допомогу приходять асиметричні методи шифрування.

При асиметричному шифруванні використовується два ключі – один для шифрування, а другий – дешифрування. Перший пересилається по мережі

абонентові Y (для прикладу назвемо отримувача повідомлень абонентом X, відправника – абонентом Y) власником обох ключів, тобто абонентом X. Маючи публічний ключ, абонент Y може зашифрувати повідомлення, при цьому, розшифрувати його можна лише приватним ключем, який є тільки у абонента X. Навіть, якщо публічний ключ потрапить до рук зловмисника, він не зможе розшифрувати повідомлення, зашифровані цим ключем.

На рис. 3.6 наведена схема передачі повідомлення від Боба до Аліси з використанням асиметричного шифрування.

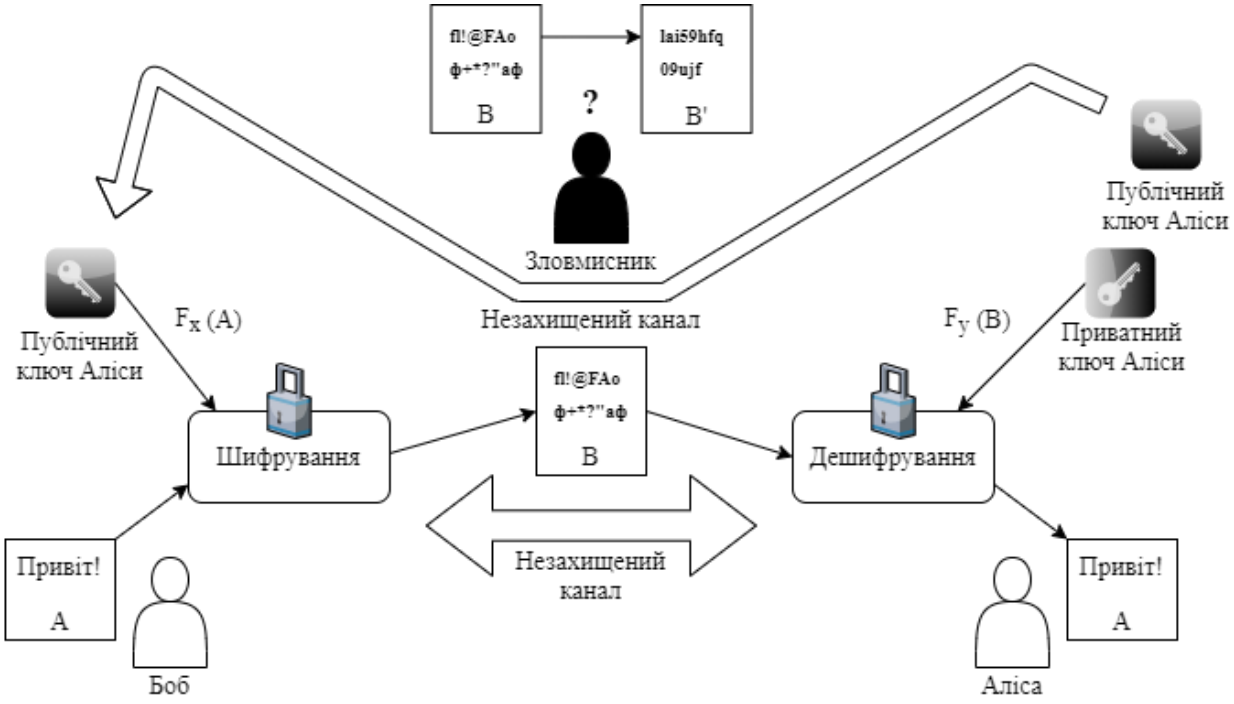

Рисунок 3.6 – схема передачі повідомлення з використанням асиметричного шифрування.

Боб хоче відправляти повідомлення, тому йому потрібен відкритий ключ Аліси x. Аліса має у себе закритий ключ y, який вона не відправляє нікому. Спочатку Аліса відправляє свій відкритий ключ Бобові через незахищений канал, де він, звичайно, потрапляє до рук зловмисника. Отримавши ключ, Боб шифрує повідомлення A цим ключем (функція $F_x(A)$) та відправляє його через незахищений канал. Повідомлення на шляху проходження може потрапити до

рук зловмисника, але, тільки маючи публічний ключ, він не зможе його розшифрувати. Аліса, отримавши зашифроване повідомлення, розшифровує його за допомогою свого приватного ключа у (функція $F_y(A)$), після чого повідомлення набуває початкового вигляду.

Здавалося б у даної криптографічної системи немає недоліків, але вони є. Отримавши публічний ключ, зловмисник може видати себе за Боба та почати надсилати Алісі повідомлення від його імені за допомогою спуфінгу. Якщо виникне така ситуація, Аліса, не усвідомлюючи ситуацію, може повідомити зловмиснику конфіденційну інформацію, скажімо, наприклад, паролі від акаунтів для якого-небудь додатку-софтфона, де дзвінки є платними. Фатальність такої ситуації для бізнесу була б неминучою. Щоб такої ситуації не сталося, існують певні засоби, які розглядаються у наступному підрозділі.

3.4.4 Важливість шифрування для VoIP-систем

Шифрування є невід'ємним елементом будь-якої служби інформаційної безпеки. Скрізь, де однією з вимог до інформації є конфіденційність, потрібне шифрування. VoIP-мережі також не є виключенням.

Отримавши доступ до VoIP-системи підприємства, зловмисник може прослуховувати уві дзвінки, які мають ненадійне шифрування або взагалі його не мають. Щоб запобігти такій ситуації, бажано використовувати протокол TLS (Transport Layer Security, що у перекладі з англ. означає «безпека транспортного рівня»). TLS є криптографічним протоколом.

3.4.5 Встановлення TLS-з'єднання

Для того, щоб клієнт та сервер могли обмінюватися даними за допомогою TLS, вони повинні узгодити версії протоколу, обрати набір шифрів, а також при необхідності завірити сертифікати. Операції, котрі здійснюються під час встановлення TLS-з'єднання, наведені на рис. 3.7. Кожен

з цих кроків потребує надсилання нових пакетів, за рахунок чого до TLS-з’єднань додається додаткова початкова затримка.

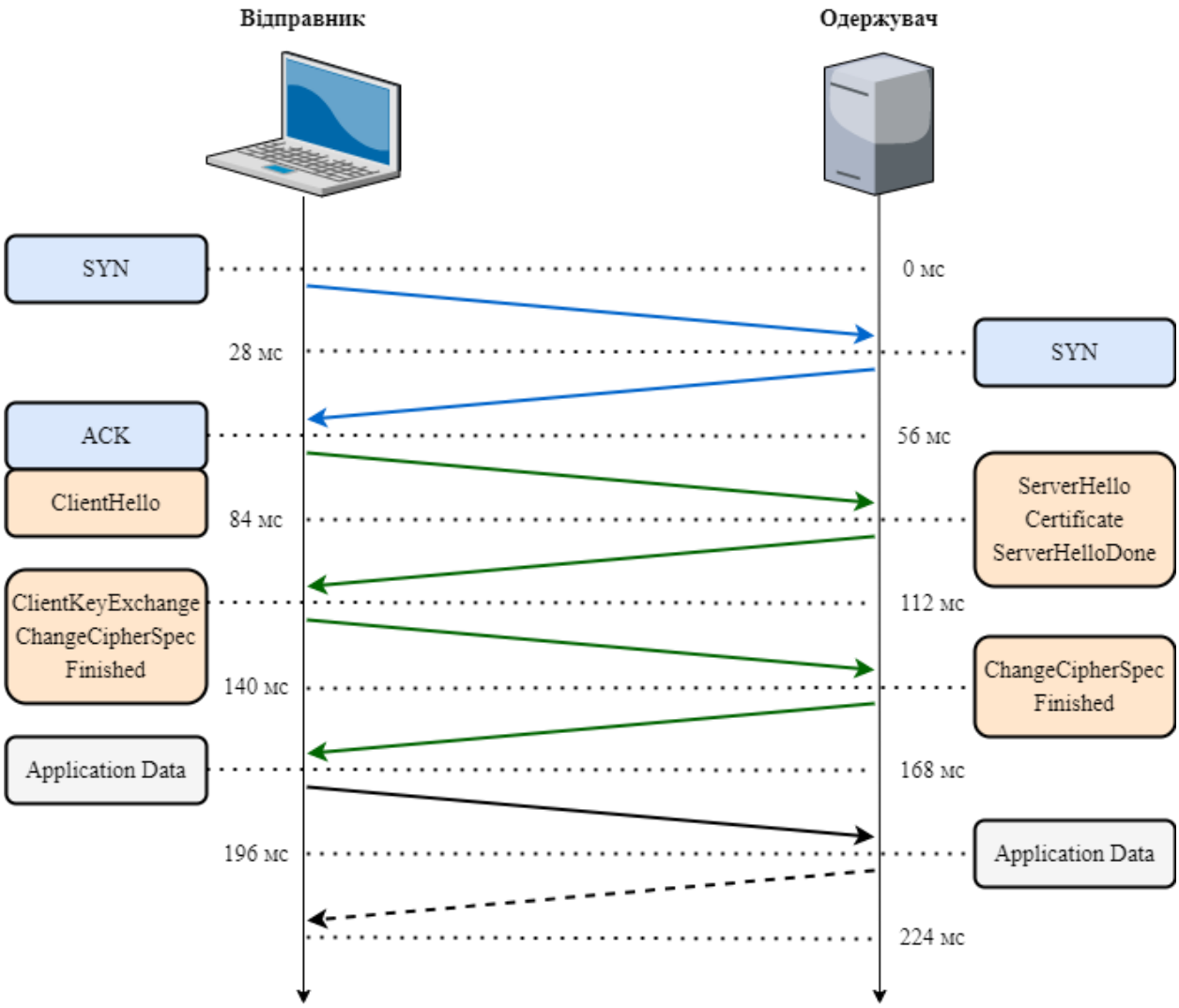

Рисунок 3.7 – етапи встановлення TLS-з’єднання.

Для встановлення з’єднання за допомогою TLS сервер та клієнт виконують наступні операції (дані наведені у вигляді «позначення часу виконання: операції»):

- 0 мс: проведення «трикратного TCP-рукостискання»;
- 56 мс: відправка ряду специфікацій у виді звичайного тексту (сюди відноситься версія протоколу TLS, список підтримуваних шифрів та ін.);

- 84 мс: вибір сервером версії протоколу TLS для подальшого обміну даними, вибір набору шифрів, які надав клієнт, для використання, відправлення сервером сертифікату та відповіді клієнтові, а також запит сертифіката клієнта та інших параметрів при необхідності;

112 мс: ініціювання RSA або обмін ключами Діффі-Хеллмана, котрий використовується для встановлення симетричного ключа для сесії;

140 мс: сервер обробляє параметри обміну ключами, котрі були надіслані клієнтом, перевіряє цілісність повідомлень шляхом перевірки MAC, після чого надсилає зашифровану відповідь «Finished» клієнтові;

168 мс: клієнт розшифровує відповідь сервера за допомогою завіреного симетричного ключа, перевіряє MAC, і, якщо перевірки проходять успішно, встановлюється захищене з'єднання, по котрому можуть бути передані програмні дані.

Перелічені операції називають повним «TLS-рукостисканням» (TLS handshake).

Детально ознайомитись зі структурою повідомлень, які використовуються під час встановлення TLS-з'єднання, можна у документі «RFC 8446» організації IETF (Internet Engineering Task Force).

MAC (Message Authentication Code) або код автентифікації повідомлень – це невеликий фрагмент інформації (величиною до 32 байт), який використовується під час встановлення TLS-з'єднання та використовується для перевірки цілісності та достовірності повідомлень.

3.4.6 Структура заголовка та полів протоколу TLS

Дані, якими обмінюються вузли в рамках сесії TLS, формуються за чітко визначеними правилами. За це відповідає протокол запису TLS (TLS record protocol). Даний протокол виконує обробку різних видів повідомлень, передача яких здійснюється в рамках TLS-сеансу, а також захист та перевірку цілісності кожного повідомлення. TLS-запис (так будемо називати одиницю

даних протоколу TLS record) може бути зашифрованим, стиснутим, доповненим, а також ідентифікований за допомогою MAC. Кожний такий запис обов'язково містить у собі наступні поля: Content Type, Version, Length. Перше вказує на тип вмісту TLS-запису, друге – на версію протоколу TLS, третє – на довжину пакета без урахування полів Content Type, Version та Length.

На рис. 3.8 наведений приклад структури TLS-запису у програмі «Wireshark» під час встановлення з'єднання між клієнтом та веб-сервером Apache. Тип вмісту запису видно з поля Content Type, значення якого записано, як «Handshake (22)».

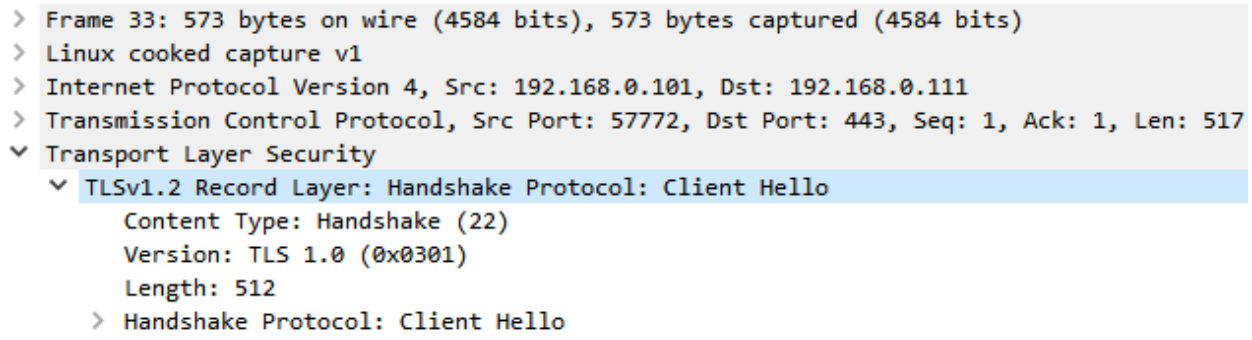

Рисунок 3.8 – приклад структури протоколу запису TLS у програмі «Wireshark».

3.4.7 Відновлення TLS-з'єднання

«TLS-рукостискання» дозволяє програмам використовувати захищене з'єднання, але воно, у свою чергу, призводить до збільшення затримок при передачі даних та додаткових обчислювальних втрат. Все це призводить до того, що ефективність роботи таких програм падає. Затримки у роботі програм на обладнанні підприємства є особливо небажаними. Якщо, наприклад, програма-софтфон зависне, існує імовірність того, що дзвінок від потенційного партнера або клієнта буде пропущено. На щастя, цю проблему було взято до уваги. Протокол TLS використовує спеціальний механізм, який

дозволяє відновити з’єднання за допомогою відомих раніше параметрів, таких як секретний ключ та використані алгоритми шифрування.

Процедура відновлення виклику багато у чому є схожою на звичайне встановлення TLS-з’єднання. Для того, щоб не створювати додаткові обчислювальні витрати на генерування нового сеансового ключа, котрий використовується для операцій шифрування та дешифрування вже після встановлення зв’язку, TLS створює спеціальний ярлик, який використовується для відновлення сеансу. Цей ярлик створюється в кінці операції звичайного встановлення TLS-зв’язку.

Для того, щоб відновити обірвану TLS-сесію, клієнт та сервер здійснюють наступні кроки:

- клієнт надсилає серверові «ClientHello», вказавши у повідомленні останню підтримувану версію протоколу TLS, список підтримуваних методів шифрування та стиснення даних, випадкове число, а також ідентифікатор минулої сеансу зв’язку «session id»;
- сервер у відповідь на «ClientHello» надсилає повідомлення «ServerHello», яке містить підтверджену сервером версію протоколу TLS, яка буде надалі використовуватись, випадкове число клієнта, яке було надіслано клієнтом, підтверджені алгоритм шифрування та метод стиснення даних (обираються із запропонованих клієнтом); після того, як сервер отримує «session id», він додає його в «ServerHello»; у випадку відмови у відновленні попереднього сеансу, сервер генерує новий «session id», тим самим інформуючи клієнта про дану неможливість;
- сервер надсилає клієнтові повідомлення «ChangeCipherSpec», яке містить інформацію про алгоритми шифрування, затверджені під час операції встановлення зв’язку;
- далі сервер надсилає зашифроване повідомлення «Finished», до якого входять хеш а також MAC, які генеруються на основі даних про попередній сеанс установлення зв’язку;

- клієнт, отримавши від сервера повідомлення «Finished», намагається розшифрувати його для того, щоб перевірити хеш та MAC; у випадку, коли повідомлення не може бути розшифроване або дані повідомлення не проходять перевірку, з’єднання обривається;
- після успішної перевірки даних повідомлення «Finished» від сервера, клієнт надсилає серверові повідомлення «ChangeCipherSpec», яке інформує про те,

що вся інформація, яка буде пересилатись надалі, буде зашифрована встановленим у процесі підтвердження сеансу методом, використовуючи при цьому спільний сеансовий ключ;
- далі клієнт надсилає повідомлення «Finished» серверові у зашифрованому вигляді, отримавши яке, сервер за схожою схемою перевіряє отримані хеш та MAC;
- сеанс зв’язку встановлено, усі дані, що надалі будуть передаватися, будуть зашифровані.

4. ПРОТОКОЛИ, ЩО БЕРУТЬ УЧАСТЬ У ФУНКЦІОНУВАННІ VOIP-МЕРЕЖІ

4.1 Вступ

Обладнання, що бере участь у функціонуванні VoIP-мережі, виконує дуже широкий набір функцій. Для того, щоб ці функції працювали коректно, існує ряд певних протоколів. До таких протоколів відносять SIP, RTP, RTCP, SRTP, SDP, IAX, XMPP, MGCP, Jingle, RADIUS, а також Diameter. Деякі з них ми розглянемо більш детально в наступних підрозділах.

4.2 Протокол сигналізації SIP

Протокол встановлення з'єднання, або коротко – SIP (від англ. «Session Initiation Protocol»), є протоколом сигналізації. Сигналізацією в телефонії називають набір програмно-апаратних засобів, які виконують відправку спеціальних повідомлень, пов'язаних з управлінням сенсом зв'язку. До таких повідомлень можна віднести запити на встановлення, розрив сесії тощо.

Протокол SIP є текстовим протоколом (інформація передається у відкритому вигляді) прикладного рівня, за замовчанням на транспортному рівні використовує UDP, для більш надійної доставки – TCP, для захищеної передачі – TLS. Даний протокол часто використовується в парі з такими протоколами, як SDP та RTP, про які ми поговоримо у наступних підрозділах. Головними стандартами, які описують даний протокол, є «RFC2543» та «RFC3261». Аналогами цього протоколу у звичайній телефонії є SS7 та H.323.

Протокол SIP виконує наступні завдання:

- установлення сеансу зв'язку;
- управління викликом у реальному часі (зміна параметрів виклику і т. п.);
- виявлення місцезнаходження абонента, до якого здійснюється виклик;
- перевірка готовності одного з абонентів прийняти виклик;
- обмін даними про використовувані абонентами кодеки;

- узгодження медіа-параметрів виклику (використовуваних кодеків і т. п.);
- відправлення повідомлень про статус абонента;
- здійснення голосових та відео-конференцій;

4.2.1 Типи повідомлень-запитів протоколу SIP

Для того, щоб абонентські пристрої та інше обладнання, яке бере участь у здійсненні VoIP-дзвінка, знали, що потрібно робити на конкретній стадії виклику, протокол SIP надсилає певні сигналізаційні повідомлення. В залежності від цілі, яку переслідують SIP-повідомлення, вони поділяються на запити на відповіді.

У даному підрозділі розглядаються SIP-запити, їх також називають методами. На кожний запит може приходити відповідь або не може. Список основних SIP-методів та їх короткий опис наведемо у табл. 4.1.

Таблиця 4.1 – Основні SIP-методи та їх короткий опис.

Назва методу	**Короткий опис**
INVITE	Встановлення сесії
CANCEL	Скасування сесії, яку ще не було встановлено
BYE	Завершення вже встановленої сесії
ACK	Підтвердження отримання фінальної відповіді від певного учасника VoIP-мережі; не потребує відповіді
REGISTER	Запит на реєстрацію користувача на сервері реєстрації
OPTIONS	Обмін інформацією про можливості (використовувані кодеки і т. п.) абонентів, які хочуть встановити між собою з'єднання
INFO	Надсилання проміжної інформації, яка не змінює параметри сесії (наприклад, зображень або даних про залишок на балансі клієнта)
NOTIFY	Надсилання інформації про зміни стану підписок абонента, інформування підписника про нові події
MESSAGE	Надсилання повідомлень
SUBSCRIBE	Підписка на сповіщення про події
REFER	Запит на переспрямування сесії до іншого абонента
UPDATE	Зміна параметрів сесії (списку використовуваних медіа-потоків та їх кодеків), які не впливають на стан діалогу

4.2.2 Типи повідомлень-відповідей протоколу SIP

Як було сказано у попередньому підрозділі, у відповідь на SIP-запити можуть надходити SIP-відповіді. Всі SIP-відповіді можна розділити на певні категорії. Кожна така відповідь має свій код, і, в залежності від значення цього коду, присвоюється до певного класу. У табл. 4.2 наведено інтервали кодів SIP-відповідей у вигляді «цифра-xx», де замість «x» може бути будь-яка цифра

від 0 до 9, класи цих інтервалів, опис даних класів, а також приклади SIP-відповідей з позначенням коду.

Таблиця 4.2 – Класифікація кодів SIP-відповідей.

Інтервал	**Клас**	**Опис класу**	**Приклади**
1xx	Інформаційні відповіді	Вказує на те, що запит було оброблено успішно	100 Trying 180 Ringing 182 Queued
2xx	Відповіді про успіх операцій	Вказує на успішне завершення запиту	200 OK 202 Accepted
3xx	Відповіді про переспрямування	Вказує на те, що для успішної обробки потрібне переспрямування запиту іншій стороні	301 Moved Permanently 302 Moved Temporarily
4xx	Відповіді про невдалі запити клієнта	Вказує на те, що запит має синтаксичну помилку або не може прийнятий сервером; помилки на стороні клієнта	400 Bad Request 401 Unathorized (вказує на те, що запит потребує автентифікації абонента) 403 Forbidden 413 Unsupported Media Type
5xx	Відповіді про збої у роботі сервера	Вказує на те, що сервер не може обробити запит, навіть, якщо він не є помилковим; помилки на стороні сервера	500 Server Internal Error 502 Bad Gateway 503 Service Unavailable
6xx	Відповіді про глобальні помилки	Вказує на глобальні помилки, пов’язані із запитами, які не може обробити жоден сервер	600 Busy Everywhere 603 Decline 607 Unwanted

4.2.3 Структура SIP-повідомлень

Кожне SIP-повідомлення має стандартизований формат, котрий містить чотири основні блоки: початковий рядок, заголовки, пустий рядок та тіло. Приклади SIP-повідомлень можна подивитись в документації «RFC 2543» та «RFC 3261». На рис. 4.1 наведено приклад SIP-повідомлення.

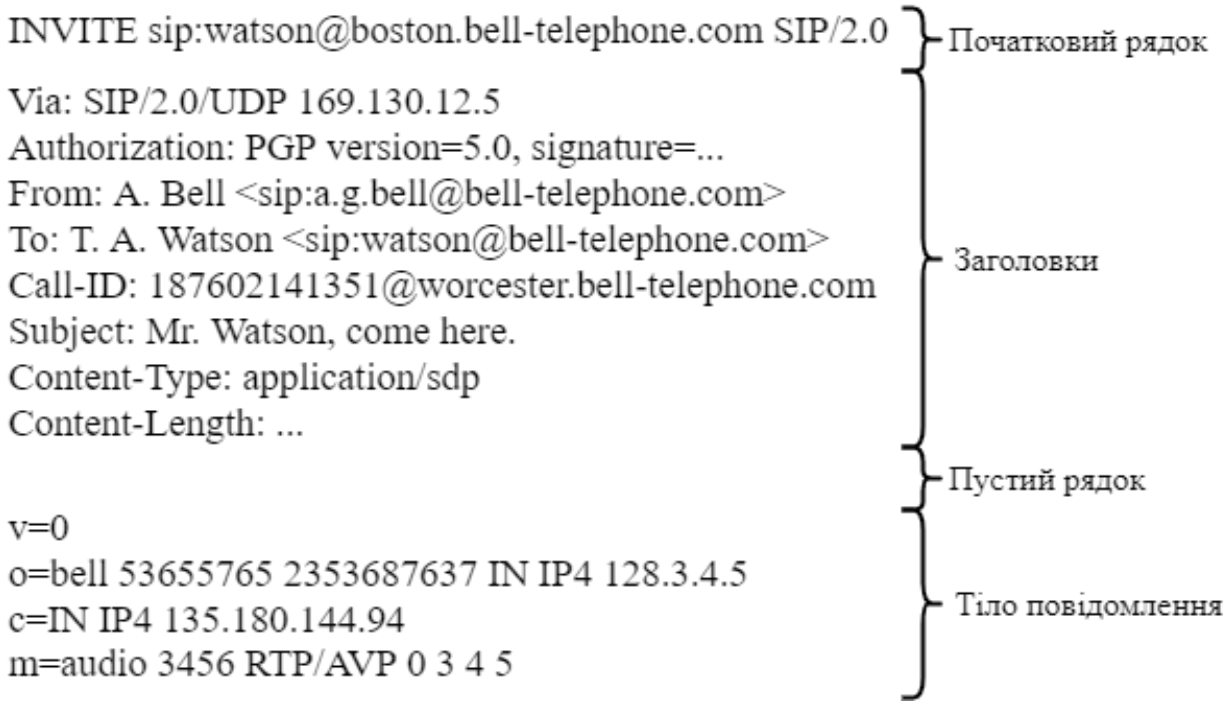

Рисунок 4.1 – структура SIP-повідомлення.

4.3 Протоколи RTP та SRTP

«Real-time Transport Protocol» (англ.) – це протокол, котрий забезпечує функції передачі трафіка у реальному часі, наприклад, голосових даних або відео, як у випадку з VoIP. Даний протокол не забезпечує гарантовану доставку даних. Це завдання виконує протокол RTCP, який використовується у парі з RTP.

Для того щоб, дані у корпоративній мережі передавались безпечно, потрібно використовувати протокол SRTP. Цей протокол є профілем розширення RTP, він додає певну інформацію до RTP, надаючи при цьому

функції автентифікації повідомлень, а також захист від прослуховування. Структура RTP-пакету наведена на рис. 4.2.

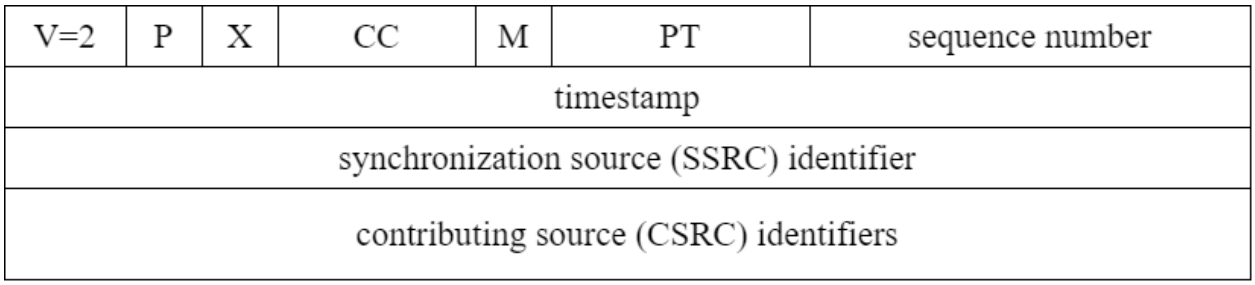

Рисунок 4.2 – структура RTP-пакету.

Поля, зображені на рис. 4.2, мають наступні значення:

- version (V): 2 біти

Дане поле вказує на версію протоколу. «V=2» означає, що використовується друга версія RTP.

- padding (P): 1 біт

Якщо даний біт встановлено, до пакету додається один або декілька додаткових октети, які грають роль відступів для протоколів шифрування або декількох пакетів RTP, котрі передаються в одному пакеті нижніх рівнів. Останній октет даного поля вказує на те, скільки таких октетів виступають у ролі відступів.

- extension (X): 1 біт

Визначає розширення заголовку [5].

- CSRC count (CC): 4 біти

Лічильник CSRC позначає число CSRC-ідентифікаторів [5], котрі йдуть після фіксованого заголовка.

- marker (M): 1 біт

Маркер, котрий визначається профілем [5]. Позначає важливі події, наприклад, границі кадра в загальному потоці.

- payload type (P): 7 біт

Дане поле позначає тип корисного навантаження та його формат, а також

його інтерпретацію програмою.

- sequence number: 16 біт

Вказує на порядковий номер RTP-пакету, може бути використано отримувачем для виявлення втрат пакетів.

- timestamp: 32 біти

Часова позначка [5].

- SSRC: 32 біти

Це поле вказує на джерело синхронізації [5].

- CSRC list: від 0 до 15 елементів, 32 біти кожен

CSRC-список вказує на допоміжні джерела [5] для корисного навантаження пакету.

Заголовок SRTP у цілому схожий на заголовок протоколу RTP, але має два додаткові поля – «MKI» та «Authentication tag».

Довжина поля MKI (Master Key Identifier) не є фіксованою, дане поле є необов’язковим. MKI вказує на головний ключ, з якого було отримано сесійний ключ (ключі), який здійснює автентифікації та (або) шифрування окремого пакету.

Довжину тегу автентифікації (поля «Authentication tag», коротко - AT) можна налаштувати, є рекомендованим полем, на відміну від MKI. Дане поле використовується для передачі автентифікаційних даних повідомлень. Дані SRTP, що проходять автентифікацію, складаються із заголовка RTP, доповненого зашифрованою частиною SRTP. AT забезпечує автентифікацію для заголовка та корисного навантаження протоколу RTP, а також захист від дублювання пакетів через автентифікацію порядкового номера пакету (поля sequence number).

4.4 TLS і SRTP

Для того, щоб дзвінки між абонентами були максимально захищені, потрібно використовувати TLS у парі з SRTP.

TLS шифрує службову інформацію, яка передається під час виклику. Інакше кажучи, даний протокол захищає SIP-повідомлення від зміни їх зловмисником. SRTP здійснює шифрування медіа-даних та автентифікацію повідомлень, які передаються під час виклику. Таким чином, для захищеного дзвінка, обидва абоненти, які ведуть між собою телефонну розмову, повинні використовувати на своїй стороні SRTP та TLS.

5. ПРОЕКТУВАННЯ ЗАХИЩЕНОЇ VOIP-МЕРЕЖІ

Головною метою даної роботи є проектування захищеної VoIP-мережі для підприємств. У наш час з'являються все нові й нові способи проведення атак на мережі. Методи, які використовуються у такій мережі, суттєво підвищують захист від таких атак, як спуфінг, прослуховування, DoS, Toll-Fraud, а також SPIT.

Структурна схема захищеної VoIP-мережі наведена на рис. 5.1. Дана схема містить чотири мережі, між якими можуть здійснюватися дзвінки за допомогою технології VoIP, мережу провайдера, та VPN-мережу. Першою мережею є локальна мережа підприємства, другою та третьою – приватні мережі віддалених працівників фірми, четвертою – приватна мережа клієнта. Для простоти сприйняття, кількість локальних мереж клієнтів та підприємства, а також кількість пристроїв у цих підмережах зведено до мінімуму.

Спочатку детально розглянемо локальну мережу підприємства. До складу даної підмережі входять декілька IP-телефонів та софтфони. Усі ці пристрої під'єднані до спільного маршрутизатора через комутатор або Wi-Fi. Цей маршрутизатор базується на системі Linux і використовує пріоритезацію VoIP-трафіка, а також виступає у якості фаєрволу. Дані функції реалізовано за допомогою служби iptables.

Зв'язок між мережею підприємства та віддаленими працівниками реалізовано за допомогою VPN-каналу. На маршрутизаторах цих працівників також налаштовано пріоритезацію VoIP-трафіку.

Шифрування сигналізаційного та медіа-трафіку здійснюється за допомогою протоколів TLS та SRTP відповідно.

У мережі клієнта є софтфон та IP-телефон. За налаштування та захист даної мережі цілком відповідає клієнт.

Обладнання, що знаходиться у мережі провайдера, використовується для здійснення дзвінків за межі офісу (до клієнтів). До складу мережевого

обладнання провайдера, яке обслуговує VoIP-дзвінки, зазвичай входить proxy-сервер, сервер реєстрації, redirect-сервер, B2BUA.

Також варто взяти до уваги те, що для максимального захисту даних, у даній системі передбачається застосування не тільки технологічних методів, а також профілактичних. Цими профілактичними методами підвищення рівня захисту даної VoIP-системи є проведення тренінгів з кібербезпеки для працівників фірми, а також використання надійних паролів.

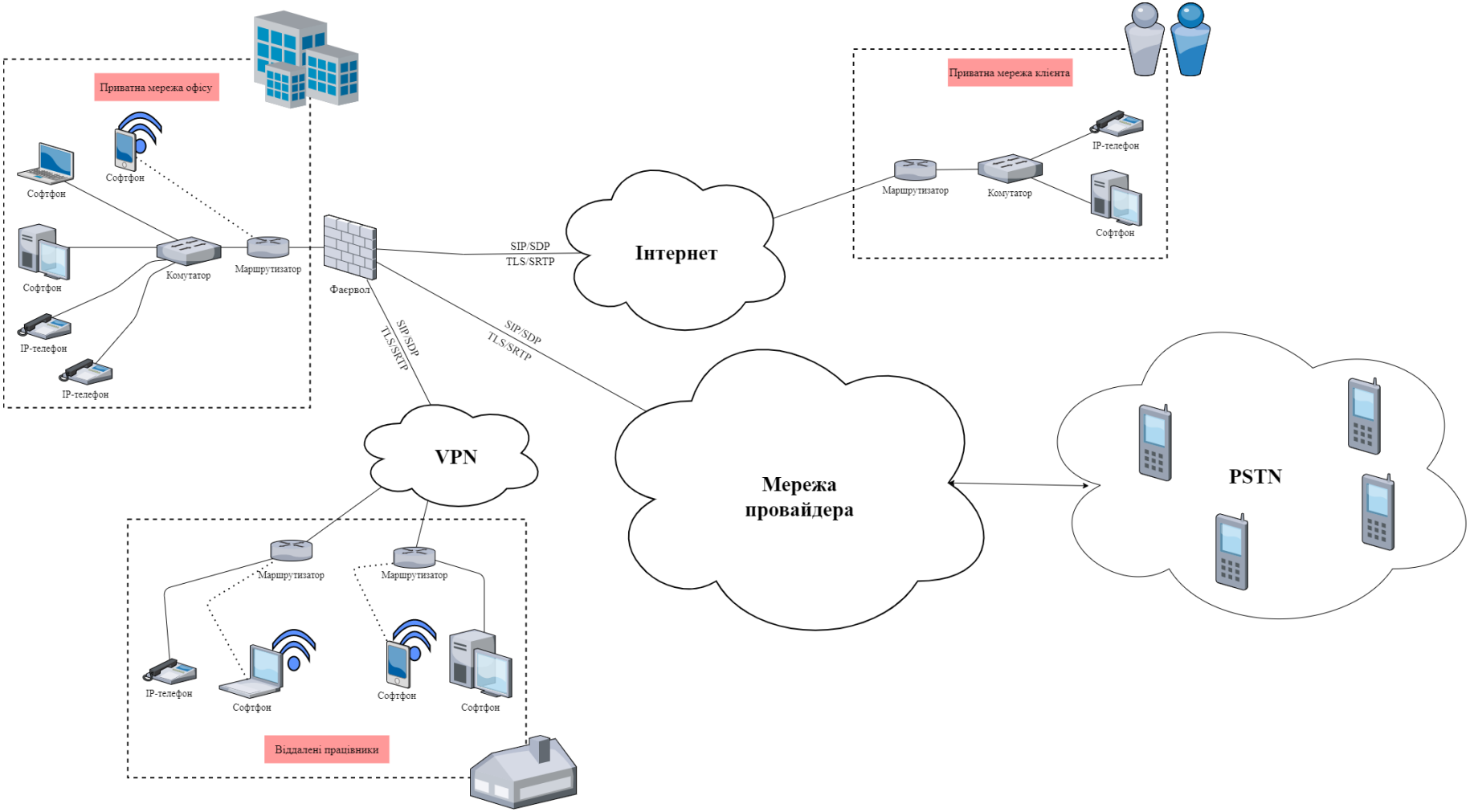

Рисунок 5.1 - структурна схема захищеної VoIP-мережі.

ВИСНОВКИ

У даній роботі було розглянуто актуальні проблеми, пов’язані із захистом IP-телефонії, а також можливі рішення, направлені на вирішення цих проблем. На основі цих даних було розроблено схему захищеної VoIP-системи, яка складається з окремих мереж. Дана система є придатною до впровадження на підприємствах. У системі було застосовано профілактичні та технологічні методи захисту. Було обрано ряд протоколів та технологій, які суттєво підвищують рівень захисту VoIP-систем. Зроблено висновки про доцільність використання протоколів TLS та RTP у парі.

СПИСОК ЛІТЕРАТУРИ

1. Б. С. Гольдштейн, Н. А. Соколов, Г. Г. Яновский. Сети связи: Учебник для ВУЗов. СПб.: БХВ-Санкт-Петербург, 2010. – 400 с., илл.

2. Лізунов А. О. Захист VoIP-телефонії в телекомунікаційних системах / А. О. Лізунов, О. В. Д'яченко, // ФЕЕ–2021 : матеріали та програма міжнародної науково-технічної конференції студентів та молодих вчених, Суми, 19–23 квітня 2021. – С. 100.

3. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 5-е изд. – СПб.: Питер, 2016. – 992 с.: илл.

4. E. Rescorla. Rfc 8446 – The Transport Layer Security (TLS) Protocol Version 1.3. Technical report, IETF, 2018

5. H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson. RFC 3550 – RTP: A Transport Protocol for Real-Time Applications. Technical report, IETF, 2003.

6. Ilya Grigorik. High-Performance Browser Networking. O'Reilly Media, 2013.

7. J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler. RFC 3261 – SIP: Session Initiation Protocol. Technical report, IETF, 2002.

8. J. Rosenberg, H. Schulzrinne, M. Handley, and E. Schooler. RFC 2543 – SIP: Session initiation protocol. Technical report, IETF, 1999.

9. S. Donovan. RFC 2976 – The SIP INFO Method. Technical report, IETF, 2000.

10. J. Rosenberg. RFC 3311 – The Session Initiation Protocol (SIP) UPDATE Method. Technical report, IETF, 2002.

11. M. Baugher, D. McGrew, M. Naslund, E. Carrara, K. Norrman. RFC 3711 – The Secure Real-time Transport Protocol (SRTP). Technical report, IETF, 2004.

12. Phithakkitnukoon, Santi; Dantu, Ram and Baatarjava, Enkh-Amgalan. VoIP security – attacks and solutions. Information Security Journal: A Global Perspective, 17(3) pp. 114-123.

13. Quality of Service for Voice over IP – Cisco. URL: https://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/qos_solutions/QoSVoIP/QoSVoIP.html (дата зверн. 25.05.2021).
14. T. Dierks, E. Rescorla. RFC 5246 – The Transport Layer Security (TLS) Protocol Version 1.2. Technical report, IETF, 2008.