НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

ФАКУЛЬТЕТ ЕЛЕКТРОНІКИ
(повна назва інституту/факультету)

КОНСТРУЮВАННЯ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНОЇ АПАРАТУРИ
(повна назва кафедри)

«На правах рукопису»
УДК: 003.26;
004.056.55

«До захисту допущено»

Завідувач кафедри КЕОА

_____ О.М.Лисенко
(підпис) (ініціали, прізвище)

“ 17 ” грудня 2021 р.

Магістерська дисертація

зі спеціальності (спеціалізації) 172 – Телекомунікації та радіотехніка
(код і назва спеціальності)

на тему: Анонімні аудіо-конференції на основі протоколу WebRTC

Виконав: студент_2_курсу, групи ДК-01мп
(шифргрупи)

Сергієнко Артур Володимирович _____
(прізвище, ім’я, по батькові) (підпис)

Науковий керівник к.т.н., доц. Бондаренко В.М. _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Рецензент_Заст. директора ТОВ «Укрспецком», к.т.н. Соловйов О.В. _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.

Студент_____
(підпис)

Київ – 2021 року

Національний технічний університет України
«Київський політехнічний інститут
імені Ігоря Сікорського»

Інститут/факультет електроніки
(повна назва)

Кафедра конструювання електронно-обчислювальної апаратури
(повна назва)

Рівень вищої освіти – другий (магістерський) за освітньо-професійною

програмою Інформаційно-обчислювальні засоби радіоелектронних систем

Спеціальність (спеціалізація) 172 – Телекомунікації та радіотехніка
(код і назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ Лисенко О.М.
(підпис) (ініціали, прізвище)

«04» лютого 2021 р.

ЗАВДАННЯ

на магістерську дисертацію

студенту Сергієнку Артуру Володимировичу
(прізвище, ім'я, по батькові)

1. Тема дисертації Анонімні аудіо-конференції на основі протоколу WebRTC
науковий керівник дисертації Бондаренко Віктор Миколайович, к.т.н., доцент.,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «03» листопада 2021р. № 3666-с

2. Строк подання студентом дисертації 17.12.2021р.

3. Об'єкт дослідження технологія WebRTC

4. Предмет дослідження проблема анонімності в технології WebRTC

5. Перелік завдань, які потрібно розробити 1.Аналіз наявних методів передачі аудіо потоку у VoIP мережах 2. Проблеми безпеки, приватності та групових конференцій в технології WebRTC 3. Розробка системи групових дзвінків та алгоритму дій анонімізації в WebRTC. 4. Розроблення стартап-проекту

6. Перелік графічного (ілюстративного) матеріалу
Презентація у форматі PowerPoint

7. Орієнтовний перелік публікацій 1 публікація

8. Консультанти розділів дисертації

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

9. Дата видачі завдання 04.02.2021р.

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Строк виконання етапів магістерської дисертації	Примітка
1	Аналіз наявних методів передачі аудіо потоку у VoIP мережах	04.02.21—15.03.21	Виконано
2	Огляд проблем безпеки, приватності та групових конференцій в технології WebRTC	16.03.21—29.05.21	Виконано
3	Розробка системи групових дзвінків та алгоритму дій анонімізації в WebRTC	01.06.21—15.08.21	Виконано
5	Розробка стартап-проекту	21.08.21—30.10.21	Виконано
6	Оформлення дисертації	01.11.21—03.12.21	Виконано

Студент _____ Сергієнко А.В.
(підпис) (ініціали, прізвище)

Науковий керівник дисертації _____ Бондаренко В.М.
(підпис) **(ініціали, прізвище)**

РЕФЕРАТ

Магістерська дисертація складається з сторінок 75, в яких міститься 31 рисунки, 22 таблиці, використано 22 джерела.

Актуальність. Технологія передачі голосу VoIP є актуальною на сьогодні, оскільки все більше і більше людей користуються перевагами швидкого інтернету. Комунікація з колегами, друзями, рідними відбувається методом створення аудіо та відео конференцій у відомих застосунках: Google Meets, Zoom, Discord, Telegram тощо. Для проведення конференцій не потрібне додаткове обладнання, лише гаджет (персональний комп`ютер, смартфон) зі стабільним підключенням до інтернету.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційне дослідження проводилися відповідно до тематики наукових досліджень кафедри КЕОА ФЕЛ в рамках пошукової НДР 0116U008452 ("ФЕЛ-4/12") на тему «Дослідження впливу факторів якості та вартості зв'язку на маршрутизацію вихідних викликів у VoIP-мережах» та пріоритетного напряму розвитку науки і техніки України «Інформаційні та комунікаційні технології».

Метою роботи є розробка підходів до анонімізації абонента у групових конференціях на основі технології WebRTC, шляхом використання VPN сервісів або віртуалізації системи.

Для досягнення мети, в роботі вирішувались наступні **задачі**:

– проведено аналіз наявних методів передачі аудіо потоку у VoIP-мережах, обрано технологію та обгрунтовано необхідність її покращення в області безпеки, приватності та можливості створення групових конференцій;

– розглянуто проблеми безпеки, приватності та групових конференцій в технології WebRTC;

– розроблено систему групових дзвінків та алгоритм дій для анонімізації в технології WebRTC;

– виконано проектування та розробка стартап-проекту

Об'єктом дослідження є технологія WebRTC.

Предметом дослідження є проблема анонімності в технології WebRTC.

Методи дослідження. При розв'язанні поставлених у роботі задач для вирішення проблеми анонімності використано методи порівняльної і описової характеристик, теоретичний аналіз та синтез, логічні індукція та дедукція, методи теорії комп'ютерних мереж та програмування.

Наукова новизна отриманих результатів, полягає в наступному:

розроблено систему та алгоритм дій для анонімізації користувачів у аудіо конференціях на основі технології WebRTC з перспективою подальшого розвитку системи.

Практичне значення отриманих результатів визначається запропонованим алгоритмом анонімізації, практично підтвердженою, за допомогою наведених комп'ютерних програм, працездатністю розробленого алгоритму дій та системи групових дзвінків на основі WebRTC.

Апробація результатів дисертації. Результати дисертаційних досліджень апробовано на VI Міжнародної науково-практичної конференції "Перспективи розвитку сучасної науки", м. Київ, жовтень, 2021р.

Публікації. За матеріалами дисертації опубліковано 1 друковану працю в збірнику матеріалів конференції (див. Додаток А): Сергієнко Артур. Технології голосового та відео зв'язку в IP-мережах // «Сучасні перспективи розвитку науки», м. Київ, 2021р. – с.49-51

Ключові слова: WebRTC, VPN, анонімність в IP-мережах

ABSTRACT

The master's dissertation consists of 75 pages, which contain 31 figures, 22 tables, 22 sources.

The relevance. VoIP voice technology is relevant today as more and more people enjoy the benefits of high speed Internet. Communication with colleagues, friends, family is done by creating audio and video conferencing in well-known applications: Google Meets, Zoom, Discord, Telegram, etc. No additional equipment is required for conferences, only a gadget (personal computer, smartphone) with a stable Internet connection.

Connection of work with scientific programs, plans, topics. The dissertation research was conducted in accordance with the research topics of the Department of KEOA FEL in the search research 0116U008452 ("FEL-4/12") on "Study of the impact of quality and cost factors on the routing of outgoing calls in VoIP-networks" and priority areas of development of Science and Technology of Ukraine "Information and Communication Technologies".

The aim of the work is to develop approaches to subscriber anonymization in group conferences based on WebRTC technology, through the use of VPN services or system virtualization.

To achieve this goal, the following **tasks** were solved:

– the analysis of available methods of audio stream transmission in VoIP-networks is carried out, the technology is chosen and the necessity of its improvement in the field of security, privacy and possibility of creation of group conferences is substantiated;

– issues of security, privacy and group conferences in WebRTC technology are considered;

– a system of group calls and an algorithm for anonymization in WebRTC technology are developed;

– design and development of a startup project was performed

The object of research is WebRTC technology.

The subject of the study is the problem of anonymity in WebRTC technology.

Research methods. Methods of comparative and descriptive characteristics, theoretical analysis and synthesis, logical induction and deduction, methods of computer network theory and programming were used to solve the problems set in the work to solve the problem of anonymity.

The scientific novelty of the results is as follows:

a system and algorithm for anonymizing users in audio conferences based on WebRTC technology with the prospect of further development of the system were developed.

The practical value of the obtained results is determined by the proposed anonymization algorithm, which is practically confirmed by the computer programs of the developed algorithm of actions and the system of group calls based on WebRTC.

Approbation of dissertation results. The results of dissertation research were tested at the VI International Scientific and Practical Conference "Prospects for the Development of Modern Science", Kyiv, October, 2021.

Publications. Based on the materials of the dissertation, 1 work was published in the collection of conference materials (see Appendix A): Serhiienko Artur. Technologies of voice and video communication in IP-networks // "Modern perspectives of science development", Kyiv, 2021. - p.49-51

Keywords: WebRTC, VPN, anonymity in IP networks

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

IP – Internet Protocol

P2P – Peer-to-peer

VoIP – Voice Over Internet Protocol

HTML – HyperText Markup Language

HTTPS – Hypertext Transfer Protocol Secure

NAT – Network Address Translation

JS – JavaScript

ICE – Interactive Connectivity Establishment

ОС – Операційна Система

VPN – Virtual Private Network

ТМЗК - телефонна мережа загального користування

SIP - Session Initiation Protocol

UDP - User Datagram Protocol

OSI - Open Systems Interconnection

MGCP - Media Gateway Control Protocol

SCTP - Stream Control Transmission Protocol

SGCP - Simple Gateway Control Protocol

SRTP - Secure Real-time Transport Protocol

API - Application Programming Interface

LAN – Local Access Network

ВСТУП

Актуальність. Технологія передачі голосу VoIP є актуальною на сьогодні, оскільки все більше і більше людей користується перевагами швидкого інтернету. Комунікація з колегами, друзями, рідними відбувається методом створення аудіо та відео конференцій у відомих застосунках: Google Meets, Zoom, Discord, Telegram тощо. Для проведення конференцій не потрібне додаткове обладнання, лише гаджет (персональний комп`ютер, смартфон) зі стабільним підключенням до інтернету.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційне дослідження проводилися відповідно до тематики наукових досліджень кафедри КЕОА ФЕЛ в рамках пошукової НДР 0116U008452 ("ФЕЛ-4/12") на тему «Дослідження впливу факторів якості та вартості зв'язку на маршрутизацію вихідних викликів у VoIP-мережах» та пріоритетного напряму розвитку науки і техніки України «Інформаційні та комунікаційні технології».

Метою роботи є розробка підходів до анонімізації абонента у групових конференціях на основі технології WebRTC, шляхом використання VPN сервісів або віртуалізації системи.

Для досягнення мети в роботі вирішувались наступні **задачі**:

– проведено аналіз наявних методів передачі аудіо потоку у VoIP-мережах, обрано технологію та обгрунтовано необхідність її покращення в області безпеки, приватності та можливості створення групових конференцій;

– розглянуто проблеми безпеки, приватності та групових конференцій в технології WebRTC;

– розроблено систему групових дзвінків та алгоритм дій для анонімізації в технології WebRTC;

– виконано проектування та розробка стартап-проекту

Об'єктом дослідження є технологія WebRTC.

Предметом дослідження є проблема анонімності в технології WebRTC.

Методи дослідження. При розв'язанні поставлених у роботі задач для вирішення проблеми анонімності використано методи порівняльної і описової характеристик, теоретичний аналіз та синтез, логічні індукція та дедукція, методи теорії комп'ютерних мереж та програмування.

Наукова новизна отриманих результатів, полягає в наступному:

розроблено систему та алгоритм дій для анонімізації користувачів у аудіо конференціях на основі технології WebRTC з перспективою подальшого розвитку системи.

Практичне значення отриманих результатів визначається запропонованим алгоритмом анонімізації, практично підтвердженою, за допомогою наведених комп'ютерних програм, працездатністю розробленого алгоритму дій та системи групових дзвінків на основі WebRTC.

Апробація результатів дисертації. Результати дисертаційних досліджень апробовано на VI Міжнародної науково-практичної конференції "Перспективи розвитку сучасної науки", м. Київ, жовтень, 2021р.

Публікації. За матеріалами дисертації опубліковано 1 друковану працю в збірнику матеріалів конференції (див. Додаток А): Сергієнко Артур. Технології голосового та відео зв'язку в IP-мережах // «Сучасні перспективи розвитку науки», м. Київ, 2021р. – с.49-51

Ключові слова: WebRTC, VPN, анонімність в IP-мережах

РОЗДІЛ 1 АНАЛІЗ НАЯВНИХ МЕТОДІВ ПЕРЕДАЧІ АУДІО ПОТОКУ У VOIP МЕРЕЖАХ

1.1 Аналіз сучасного стану VoIP мереж

На сьогодні IP-телефонія є досить перспективною складовою телекомунікацій, оскільки надає вигідну альтернативу класичній телефонії.

IP-телефонія є частиною технології VoIP – Voice over Internet Protocol [1], яка поєднує в собі останні досягнення в областях цифрової обробки сигналів (DSP), аудіокодування, мережних технологій для можливості передачі голосу через інформаційні мережі з мінімальними спотвореннями та втратами. В зв'язку з цим, для голосового трафіку висуваються найвищі пріоритети передачі та обслуговування.

Архітектуру VoIP мереж можна умовно поділити на дві частини у площині моделі OSI. Нижня частина (транспортний, мережевий, канальний, фізичний рівні) – основна мережа з маршрутизацією пакетів IP, верхня площина (прикладний, сеансовий рівні) – це відкрита архітектура управління обслуговуванням викликів.

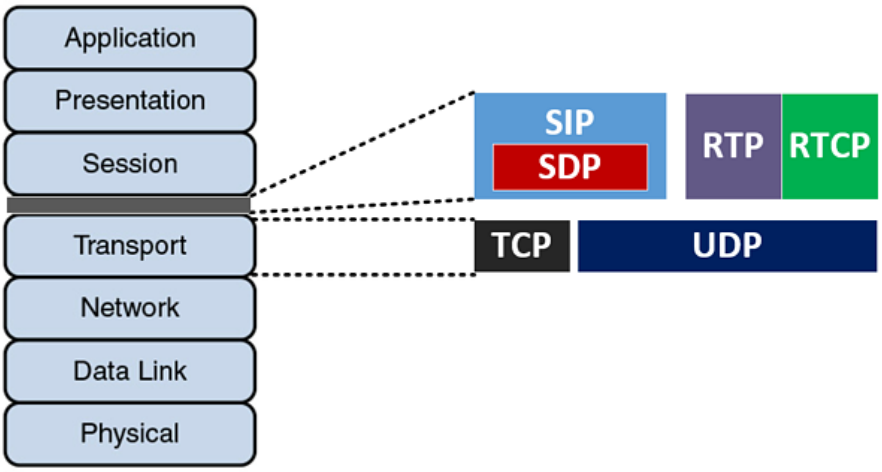

Рисунок 1.1 – модель OSI та протоколи що знаходяться на рівнях

На сьогоднішній день VoIP набуло широкого розповсюдження, можна виділити три основні напрямки використання IP-телефонії:

– гаджет – гаджет;

– гаджет – софтфон або навпаки;

– софтфон – софтфон.

Напрямок «гаджет - гаджет».

Забезпечує безкоштовну Інтернет-телефонію за допомогою програмного забезпечення, такого як Skype, Discord, WhatsUp, Viber, Telegram тощо. Абоненти можуть здійснювати дзвінки, використовуючи різні платформи: смартфони, персональні комп'ютери, планшети, тощо. Користувач може не мати можливості зателефонувати ні на міський, ні на мобільний телефон, без додаткових витрат.

Напрямок «гаджет – софтфон». Програмне забезпечення софтфону використовується для перенаправлення дзвінка в Інтернет та передає його до звичайної телефонної мережі. Щоб користуватися послугою, потрібно мати підписку та внести кошти за зниженими тарифами. Приклади включають Skype, MSN та Google Talk. Потрібні додаткові витрати на модем та аналоговий термінальний адаптер, що конвертує сигнал з цифрового в аналоговий.

Напрямок «софтфон – софтфон». Це апаратне рішення, яке дозволяє абонентам здійснювати дзвінки один одному за допомогою мережі Інтернет. Багато телефонних компаній використовують даний напрямок для обробки міжміських дзвінків. VoIP перетворює цифровий звук в пакети даних і передає ці пакети через Інтернет. Це дозволяє робити невідкладні виклики та не потребує ТМЗК для ініціації та припинення дзвінків.

У зв'язку зі стрімким розвитком програмно-апаратного забезпечення голосові та відео дзвінки стали дуже доступними. У комерційних підприємствах використовують суто програмні рішення для проведення зборів, обговорень, або як говорять: мітингів (від англ. meeting). Найпоширеніші програмні рішення які набули підтримки користувачів: Skype, Zoom, Discord, Google Meets. Для голосового зв'язку не потрібне спеціальне апаратне забезпечення як у випадку з напрямком софтфон-софтфон, або гаджет-софтфон, лише стабільний інтернет та гаджет що має мікрофон та динаміки.

Тому є сенс проводити дослідження в напрямку передачі голосових повідомлень якомога зручним для користувача способом: без додаткових апаратних

рішень, лише програмне забезпечення та розповсюджені програмно-апаратні комплекси: комп’ютери, мобільні телефони, тощо.

1.2 Аналіз існуючих архітектур VoIP-мереж

Системи IP-телефонії базуються на протоколах, вони забезпечують реєстрацію IP – пристрою (шлюз, термінал або IP-телефон) на гейткіпері провайдера, виклик або переадресацію виклику, встановлення голосового з’єднання. Наразі відомі і використовуються наступні протоколи VoIP:

– SIP — забезпечує передачу голосу, для сигналізації, зазвичай використовує порт 5060 UDP;

– H.323— протокол, більш прив'язаний до систем традиційної телефонії, ніж SIP, сигналізація — через порт 1720 TCP;

– IAX2 — через 4569 UDP-порт передаються і сигналізація, і медіа;

– MGCP;

– SIGTRAN;

– SCTP;

– SGCP;

– Skinny/SCCP;

– Unistim — закритий протокол передачі сигнального трафіку в продуктах компанії Nortel.

Мережі, що будуються на базі протоколів H.323, орієнтовані на інтеграцію з телефонними мережами і розглядаються як надбудова над мережами ISDN. Процедура встановлення з’єднання в таких мережах базується на ITU Q.931.

Даний варіант мережі, більше використовується операторами телефонного зв’язку, що надають послуги міжміського та міжнародного зв’язку.

У такому випадку, IP-телефонія буде використовуватись як основна послуга. Використовуючи протокол RAS, який входить у стек протоколів H.323, можливо надавати високий рівень контролю за використанням інтернет-трафіку, аутентифікації користувачів і нарахування оплати за послуги.

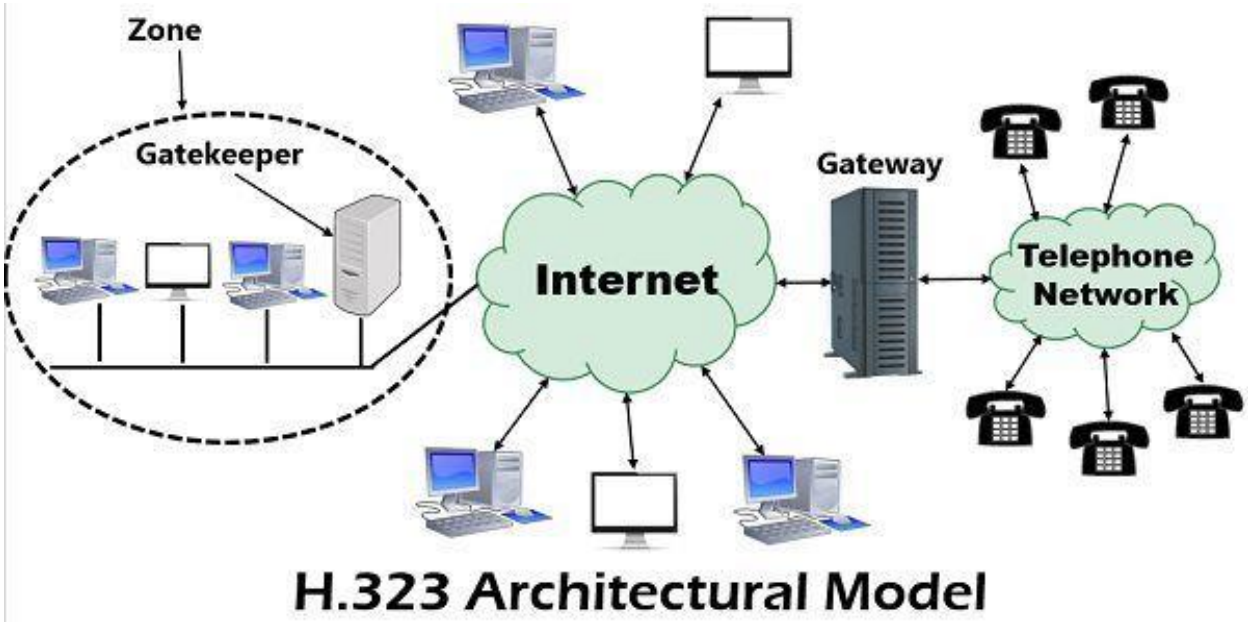

Рисунок 1.2 – Архітектура мережі, що базується на протоколі H.323

Інший протокол, має назву SIP (Session Initiation Protocol), орієнтований на інтеграцію з мережею Internet, з подальшою передачею голосового трафіку по IP-мережі.

Рішення було запропоноване організацією IETF в документі RFC 2543. Даний протокол вважається простішим за H.323, але зазвичай не використовується для організації взаємодії з телефонними мережами. Це пов’язано з тим що архітектура серверу SIP побудована таким чином, що він не зберігає інформацію про поточні з’єднання, в свою чергу вузли ТМЗК зберігають дану інформацію. Також є певні

проблеми в узгодженні протоколу HTTP з системами сигналізації, які використовуються в ТМЗК.

Даний протокол підходить для Інтернет-провайдерів. Вони можуть надавати ще одну послугу – інтернет-телефонію. Причому ця послуга є невеликою частиною тарифного плану, і надається за фіксованими тарифами.

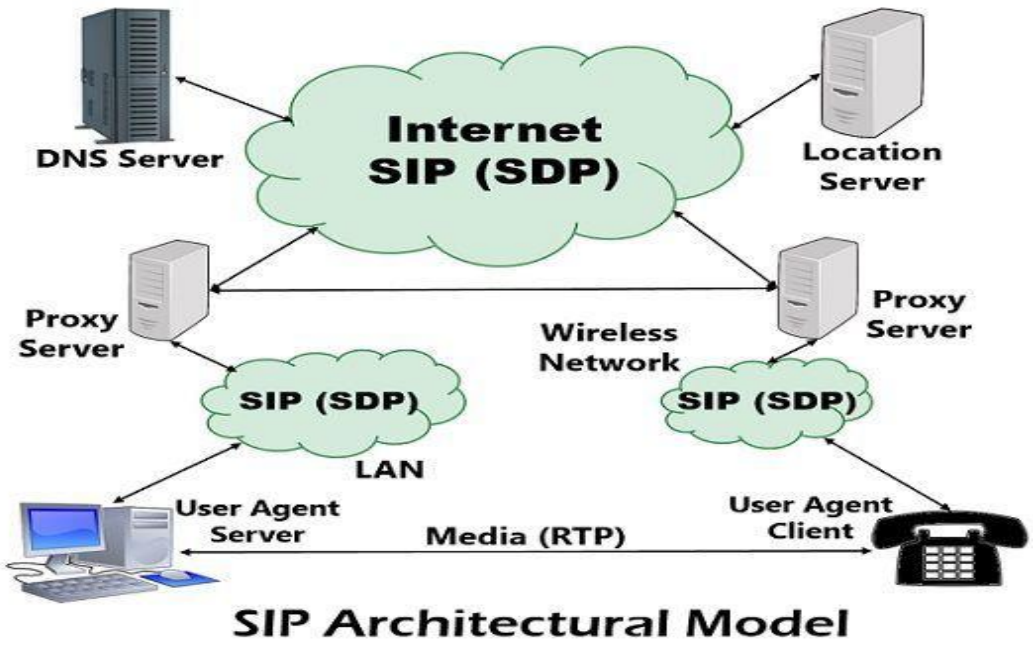

Рисунок 1.3 – Архітектура мережі, що базується на протоколі SIP

Ще один підхід – MGCP, пов’язаний з декомпозицією шлюзів, пропонує розбиття шлюзів на функціональні блоки: шлюз – MG (Media Gateway), пристрій управління шлюзом – CA (Call Agent) і сигнальний шлюз – SG (Signalling Gateway). Шлюзи виконують функцію перетворення голосової інформації з головної телефонної мережі у вигляд, придатний для передачі даних по мережах. Контролер шлюзів CA виконує керування іншими шлюзами одночасно. Сигнальний шлюз виконує функції STP транзитного пункту сигналізації.

Використовуючи даний підхід, забезпечується висока ступінь розширення і експлуатації мережі. Даний протокол, через свою відносну дешевизну добре підходить для розгортання глобальних мереж IP-телефонії.

Одна з основних вимог, що пред’являються до протоколу MGCP, полягає в тому, що пристрої які реалізують даний протокол, не повинні зберігати інформацію про послідовність транзакцій між пристроями управління та шлюзами. Даний протокол є внутрішнім протоколом, що використовує принцип ведучого/веденого, де ведучий – пристрій управління шлюзами, а транспортний шлюз – ведений.

Основним недоліком даного рішення є незакінченість стандартів. Через це, обладнання, розроблене різними фірмами-виробниками, не є сумісним. Також недоліком є відсутність стандартизованого протоколу взаємодії між пристроями управління шлюзом. Переважна кількість систем побудована на протоколі H.323, і оператору, що вибрав даний протокол, доведеться будувати свою систему на базі MGCP, це призведе до чималих фінансових вкладень.

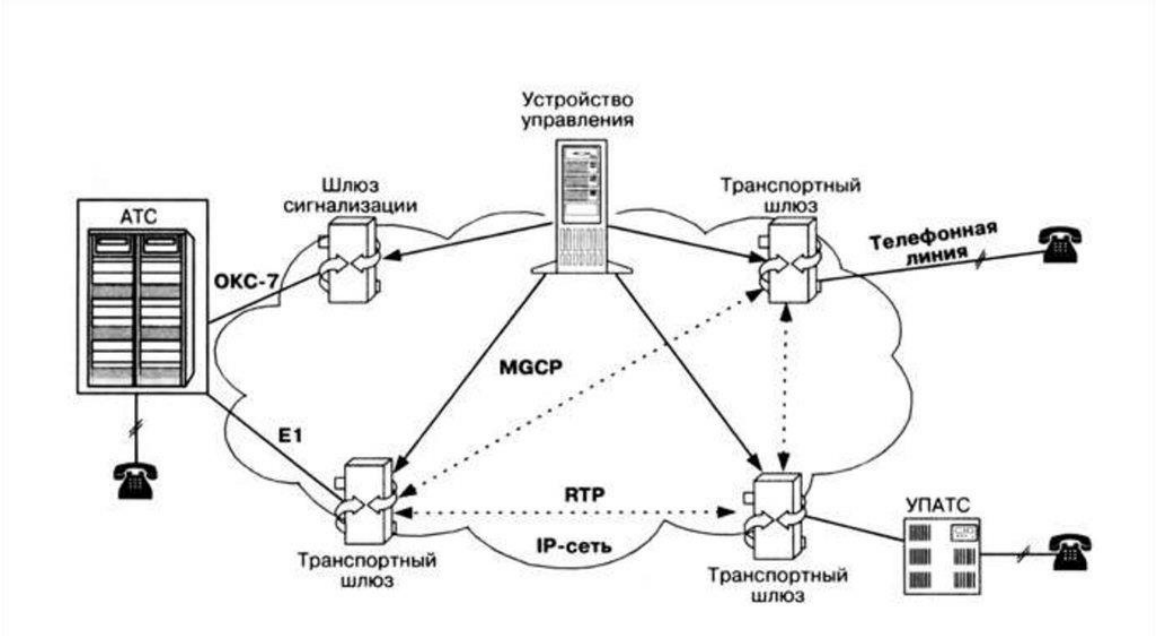

Рис 1.4 – Архітектура мережі, що базується на протоколі MGCP

WebRTC – протокол, що лежить в основі багатьох популярних платформ для передачі аудіо-відео даних. Проекти, побудовані на основі даного протоколу: BigBlueButton, Google Meet, Jitsi Meet, Discord [2][3].

Технологія на базі протоколу WebRTC є проектом з відкритим кодом, яка призначена для організації передачі потокових даних між браузерами, або іншими застосунками, що підтримують з'єднання точка-точка (peer-to-peer).

У якості транспорту IP-пакетів, виступають RTP. STUN/ICE – механізми, що допомагають встановити з'єднання поміж різних типів мереж.

В WebRTC використовуються три аудіокодеки: iSAC, iLBC та Opus, а також відеокодеки VP8 та H.264. Аудіо потік обробляється вбудованими методами придушення шуму та exo: AEC (Acoustic Echo Canceler) та NR (Noise Reduction).

Хоча WebRTC планувалось як рішення для з'єднання точка-точка, наявно декілька готових реалізацій WebRTC серверів, що надають можливість створювати групові конференції. Ці сервери підтримують можливість приєднання SIP та H.323-терміналів. Архітектура протоколу та мережі зображена на рисунках 1.5 та 1.6 відповідно.

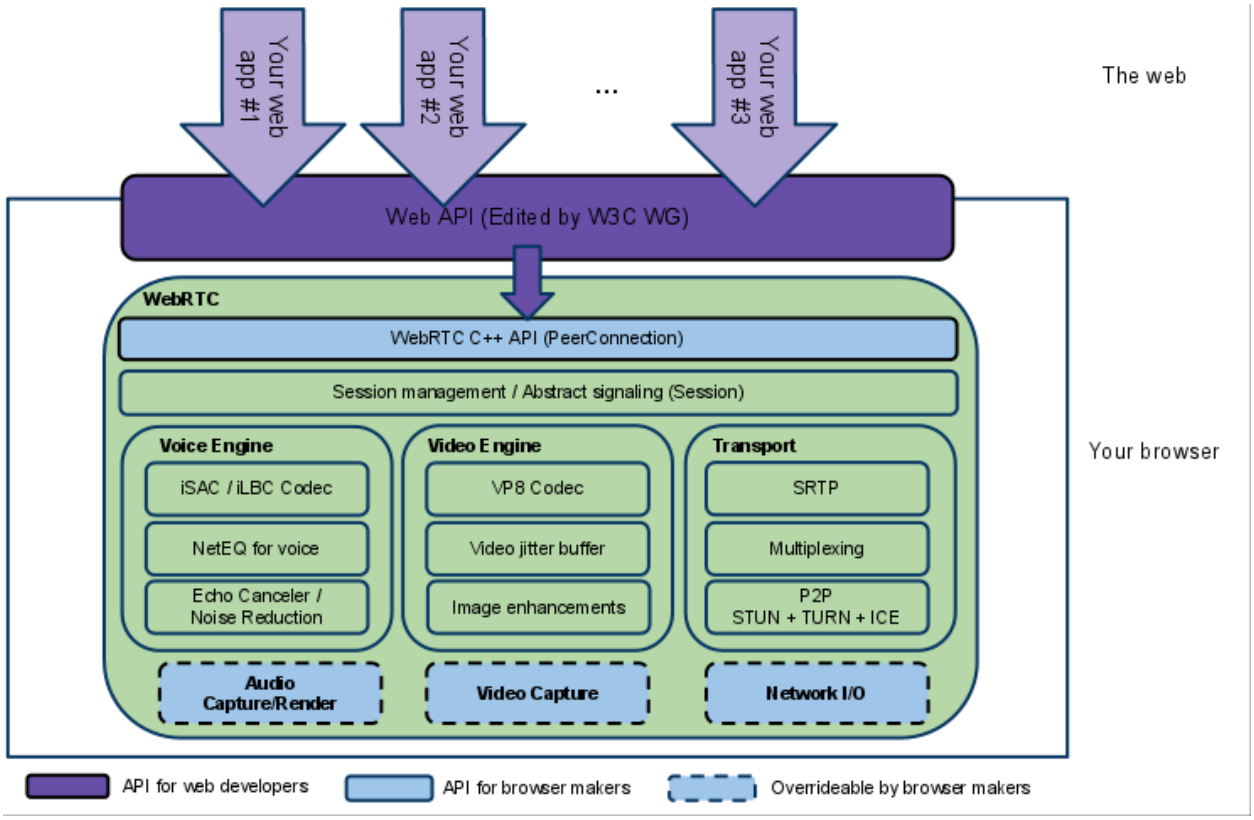

Рисунок 1.5 – Архітектура протоколу WebRTC

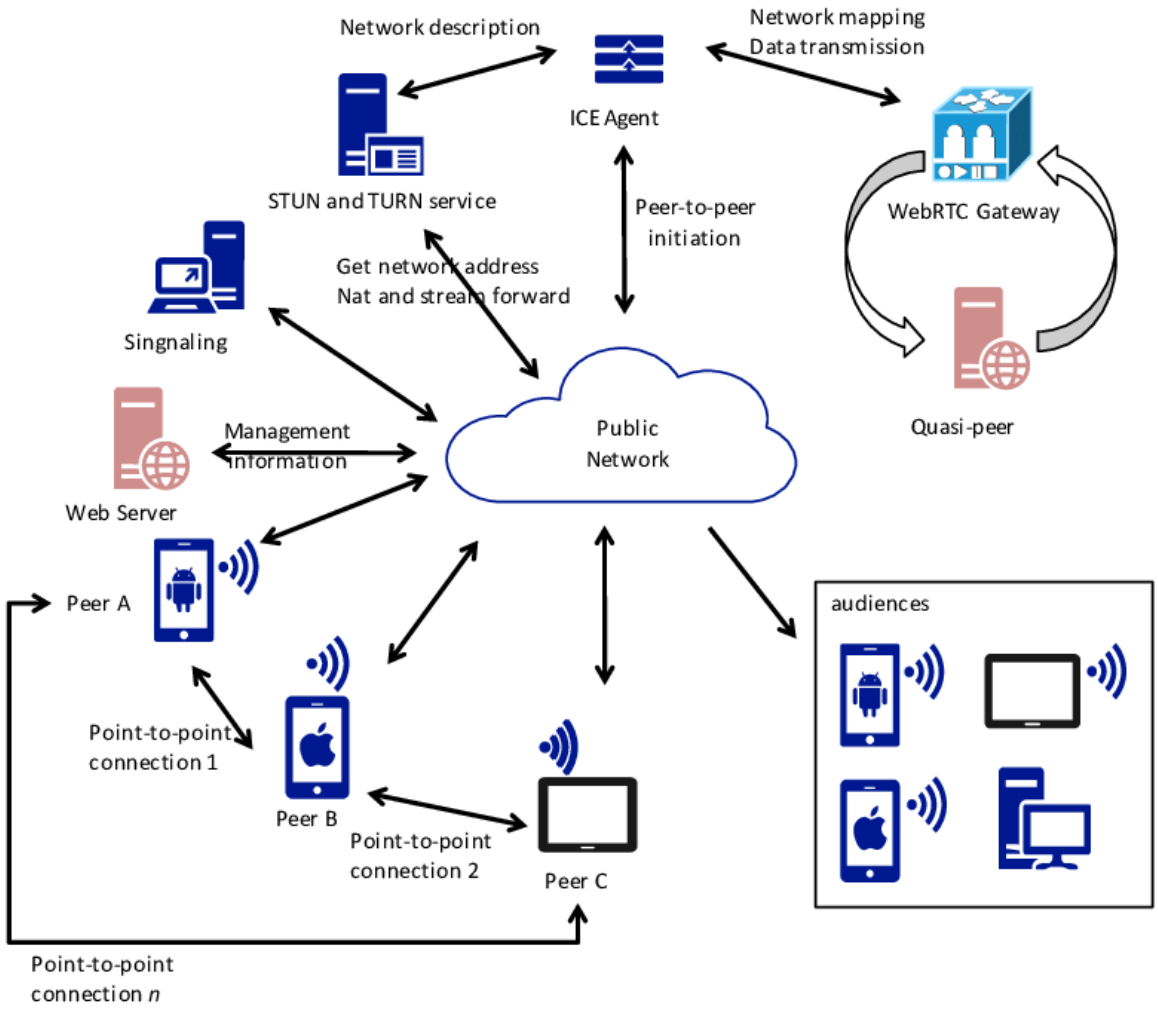

Рисунок 1.6 – Архітектура мережі на основі WebRTC [5]

1.3 Аналіз основних проблем VoIP-мереж

Мережі VoIP неідеальні, часто можна зіткнутись з проблемою передачі голосу, обриву сигналу, затримкою, шумом, тощо. Основними проблемами є [4]

– Пропускна здатність:

Мережу можна поділити на багато менших вузлів, що будуть генерувати велику кількість трафіку окрім VoIP. Це може спричинити перенавантаження пакетами в мережі, та знизити QoS (Quality of Service). З’являється затримка і так званий джиттер (jitter), тому що пакети повинні чекати своєї черги на обробку. Дуже важливо розрахувати пропускну здатність мережі настільки, щоб забезпечити високу

якість VoIP. Зазвичай, модернізація маршрутизаторів та комутаторів з 100 Мбіт / с до 1000 Мбіт / с забезпечує гарний запас пропускної здатності.

– Системи резервного живлення:

Традиційні телефони працюють при напрузі, яка подається по самій телефонні лінії, їм не потрібне зовнішнє живлення і можуть працювати при збої живлення системи. Для VoIP, в такому випадку, потребується резервна система живлення, для корректної роботи у разі відключення живлення.

– Софтфон:

Софтфони краще не встановлювати в системи, де безпека грає не останню роль. На сьогодні світ комп'ютерних вірусів дуже різноманітний, і від них стає все важче і важче захищатись. Навіть відкриття, на перший погляд безпечного веб-сайту, може призвести до зараження та майбутньої атаки. Тому використання софтфонів може знизити шанси на побудову захищеної системи.

– Екстрені дзвінки:

Традиційна телефонна лінія приєднується до фізичного місця розташування, тому екстрена служба допомоги може легко відслідкувати місце дзвінка. У разі екстреного дзвінка з допомогою VoIP, екстрена служба не може визначити місце, звідки надійшов дзвінок, тому що він міг надійти з будь-якого місця.

– Фізична безпека:

Найважливішою проблемою мережі VoIP є фізична безпека. Зловмисник може зробити так звану MITM (Man-in-the-middle) атаку та перенаправити весь трафік через себе, цим самим захопивши контроль над всіма голосовими з'єднаннями. Тому важливо налаштувати політику фізичної безпеки та засоби контролю трафіку.

– Бездротова безпека:

Безпека бездротових мереж слабше в порівнянні з дротовими мережами. Алгоритм захисту 802.11 слабкий, тому що його можна обійти, використовуючи доступне в мережі інтернет програмне забезпечення. Для кращого захисту, потрібно використовувати бездротові мережі, що мають більш захищені алгоритми, наприклад WPF або WPA20.

1.4 Аналіз відомих технічних рішень на основі патентного пошуку

Нижче розглядаються технічні рішення застосування VoIP, їх недоліки та переваги.

1. Патент US 20150181027 . Система для анонімних дзвінків. Опубліковано: 25.06.2015

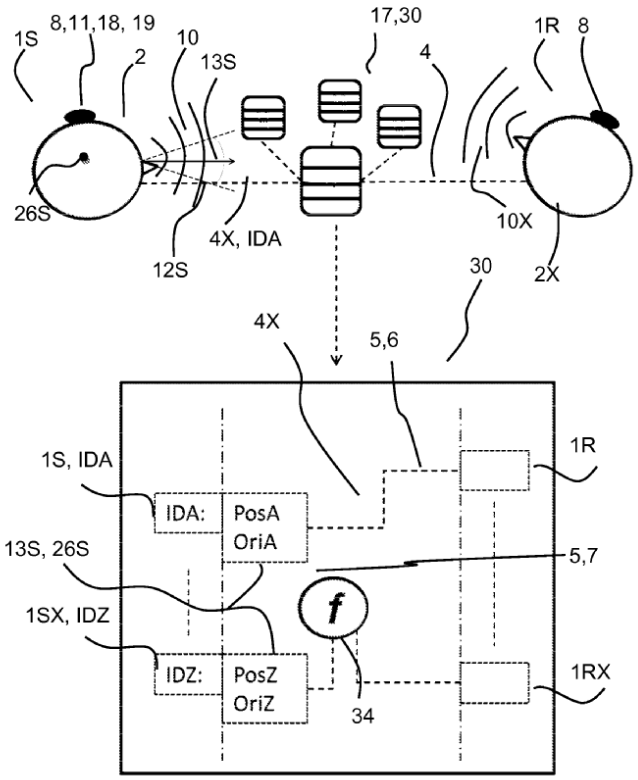

Рисунок 1.7 - Система зв’язку, що здійснює підключення через загальнодоступну мережу

Системи аудіо зв'язку, такі як мобільні телефони, стали дуже поширеними, але вони обмежені доступом для зв'язку за допомогою ідентифікатора виклику, такого як номер телефону, наданий оператором загальнодоступної мережі, або будь-яким іншим ідентифікатором.

Метою цього винаходу є подолання такого обмеження.

Зокрема, мета цього винаходу полягає в тому, щоб зробити ідентифікатор виклику доступним для дзвінка або з'єднання між сторонами, які не знають

телефонний номер, але які можуть мати іншу інформацію, наприклад, місцезнаходження пристрою.

Іншою метою даного винаходу є забезпечення системи в якості абонента і спосіб з'єднання з системою аудіо зв'язку, яка є частиною загальнодоступної мережі, що дозволяє здійснювати дзвінок або з'єднання з абонентом. Зокрема, щоб зробити дзвінок або з’єднання можливим на основі розташування абонента.

Для досягнення мети винаходу, потрібен спільний сервер, що налаштований на передачу/прийом даних. Даний сервер налаштовується для роботи з як мінімум одним із користувачів в залежності від положення абонента на даний момент.

Переваги:

- анонімність дзвінків, через відсутність ідентифікаторів;
- можливість створювати групові дзвінки.

Недоліки:

- складність реалізації.

2. Патент US 20130183949 . Система для хостінгу анонімних дзвінків, SMS та MMS. Опубліковано: 18.07.2013

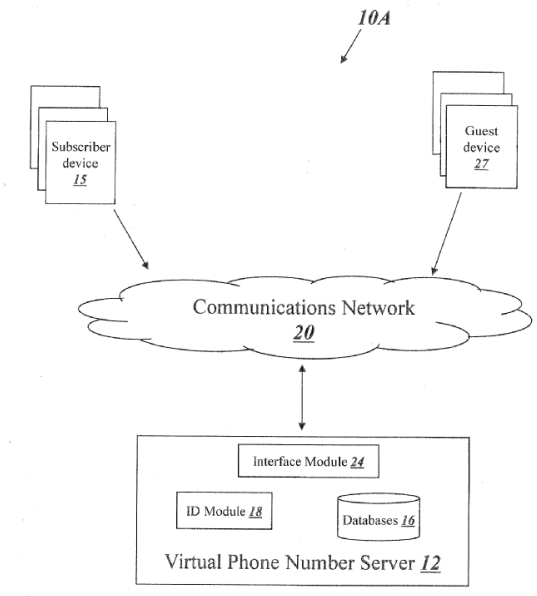

Рисунок 1.8 - Структурна схема системи

Даний винахід забезпечує спосіб встановлення та проведення сеансів через телефонну мережу, з використанням мережевих адрес і віртуальних телефонних номерів у спосіб, який забезпечує взаємну анонімність шляхом маскування фактичної мережевої адреси всіх кінцевих точок від усіх причетних кінцевих користувачів. Принаймні один користувач, який бере участь в анонімному сеансі, повинен попередньо підписатися на послугу віртуальної мережі («абонент»), а інші користувачі-учасники є «гості». У певних варіантах здійснення оператор, який працює вдома або в кол-центрі, може під’єднатись до віртуальної мережі, а клієнти кол-центру можуть брати участь у ролі гостя.

Згідно з варіантом здійснення цього винаходу, реалізований комп'ютером спосіб включає прийом через інтерфейсний модуль виклику на віртуальний номер телефону від гостьового пристрою, що має адресу мережі гостя. За допомогою модуля ідентифікації визначається унікальна ідентифікація та пов’язується з адресою гостьової мережі. За допомогою зв'язку з використанням інтерфейсного модуля визначається, чи доступний абонентський пристрій, пов'язаний з віртуальним номером телефону, для отримання віртуального сеансу.

Унікальна ідентифікація передається через інтерфейсний модуль на пристрій абонента, пов'язаний з віртуальним номером телефону. Віртуальний сеанс розміщується на інтерфейсному модулі між абонентським пристроєм і гостьовим пристроєм.

Переваги:

– анонімізація за рахунок створення віртуальних сесій та заміни номера абонента.

Недоліки:

– потреба в виділеному “центрі дзвінків

1.5 Вибір архітектури та її аналіз

Серед проаналізованих існуючих VoIP архітектур, фаворитом у сучасному світі є архітектура, побудована на базі протоколу WebRTC. На сьогоднішній день, створюється все більше і більше застосунків для гаджетів на основі WebRTC. Даний протокол є доволі новим та технічно прогресивнішим, порівняно з SIP та H.323. Використовуючи технологію на базі протоколу WebRTC, можна створити VoIP-мережу з мінімумом апаратної частини, легку у розгортанні, подальшій розробці та підтримці. Є сенс проводити дослідження саме в напрямку даної технології.

Оглянемо переваги та недоліки даної архітектури, та порівняємо її з іншими.

Переваги технології:

- для конференції потрібен лише оновлений браузер, не потрібно встановлювати додаткові застосунки;
- кодеки, що використовуються, дають гарну якість зв'язку;
- відкритий вихідний код, що розширює горизонти для використання.

У першу чергу, основною перевагою над протоколами SIP та H.323 є відсутність складного додаткового апаратного забезпечення такого як гейткіпери та додаткові проксі-сервери, простота розгортання, відкрите програмне забезпечення. Також неабиякою перевагою є наявність підтримки досить великого ком'юніті розробників на платформі github, постійні оновлення програмного забезпечення, введення нових функцій.

На даний момент все більше і більше компаній переводить своїх співробітників на віддалений режим роботи. Якщо компанія використовувала VoIP-мережу на основі протоколів H.323, SIP, тощо, то їй потрібно підключати кожного віддаленого співробітника до мережі та виділяти фінанси на додаткове апаратне забезпечення. Але в реаліях сьогодення, компанії використовують програмне забезпечення на

основі WebRTC, що дозволяє без додаткових витрат зберегти комунікацію поміж колективом.

Протоколи SIP та H.323 мають місце бути, тому що провайдери даних технологій пропонують дешеві тарифи на дзвінки поміж містом та за місто. Комунальні та державні підприємства не мають такого фінансування, щоб витрачатись на оновлення матеріально-технічної бази, тому ще залишаються у використанні стаціонарні телефони. Очевидно, що певний час дані протоколи ще будуть використовуватись.

Протокол WebRTC підтримує обов'язкове кодування трафіку, що вирішує проблему безпеки. На вибір може бути два стандартизованих протоколи DTLS (Datagram Transport Layer Security на основі SSL) та SRTP (Secure Real-time Transport Protocol).

Область застосування протоколу WebRTC є досить широкою, але в основному це передача голосу, та за потребою відео-потоку. Потенційними користувачами технології на базі даного протоколу є всі гаджети, що мають браузери з підтримкою WebRTC (більше 2-3 млрд.).

Недоліки технології:

– технологія лише визначає загальний стандарт передачі даних, адресація абонентів на різних браузерах виконана по-різному, тому навіть дзвінки між різними браузерами спричиняють складність;
– нереалізована можливість створення групових конференцій;
– ще знаходиться у розробці;
– кросплатформеність технології, але не застосунків на її основі;
– відсутність анонімності при використанні даної технології, тому що вона визначає реальну IP-адресу.

Проаналізувавши недоліки технології, можна сказати що вони не є суттєвими, але для користувачів, що прагнуть анонімності, проблема визначення IP-адреси технологією – є суттєвою, тому що знаючи цю інформацію, можна дізнатись як

мінімум місце знаходження користувача. Це ставить під загрозу прагнення до анонімності користувачів, тому є сенс розробити підходи до анонімізації, що вирішить цю проблему. На основі алгоритму дій, побудується експериментальна програма з підтримкою групових дзвінків та з відсутністю недоліка витоку IP-адреси.

Висновок до розділу 1

1. Проведено аналіз сучасного стану VoIP-мереж. З'ясовано, що напрямок "гаджет-гаджет" є найперспективнішим, оскільки потребує мінімум апаратних рішень.

2. Проведено аналіз поширених архітектур VoIP-мереж на основі протоколів: SIP, H.323, MGCP, WebRTC. Визначено області застосувань кожного з протоколів.

3. Проаналізовано основні проблеми VoIP-мереж, серед яких можна виділити наступні:

– низька пропускна здатність (при використанні застарілого обладнання);

– системи безперебійного живлення;

– софтфони;

– дротові підключення (MITM атака);

– бездротові підключення (застарілі протоколи).

4. Виконано аналіз відомих технічних рішень на основі патентного пошуку. Проведено аналіз двох патентів. Визначено переваги та недоліки кожного патенту, також визначено області застосувань.

5. Обрано архітектуру на базі протоколу WebRTC та проведено її аналіз. Обгрунтовано вибір протоколу, наведено переваги та недоліки технології на базі протоколу WebRTC. Виокремлено недоліки технології, над якими відбудеться подальша робота.

РОЗДІЛ 2 ПРОБЛЕМИ БЕЗПЕКИ, ПРИВАТНОСТІ ТА ГРУПОВИХ КОНФЕРЕНЦІЙ В ТЕХНОЛОГІЇ WEBRTC

2.1 Архітектурні складові WebRTC

Веб-зв'язок у реальному часі (WebRTC). WebRTC — це набір стандартів, протоколів і API JavaScript (JS), які дозволяють обмінюватися аудіо, відео та даними за допомогою однорангового з’єднання (P2P) через браузери. WebRTC вбудований у сучасні браузери, тому він не залежить від жодних додаткових плагінів. Веб-додатки, сумісні з сучасними популярними веб-браузерами, зазвичай можуть керувати всіма необхідними ресурсами (наприклад, мікрофоном і камерою) за допомогою стандартного JavaScript API.

Протокол WebRTC передбачає однорангову мережеву архітектуру, як показано на рисунку 2.1. Для мережевої передачі WebRTC використовує протокол RTP/S, RTP для потокової передачі медіа та Interactive Connection Establishment (ICE) для встановлення підключення. Фреймворк ICE у WebRTC підтримує виділену потокову передачу мережевих медіа, трансляцію мережевих адрес (NAT), утиліти обходу сеансів для NAT(STUN) та обхід із використанням Relay навколо NAT (TURN). Коли не вдається встановити пряме однорангове з’єднання через мережеві обмеження, замість NAT(STUN) застосовуються альтернативи NAT (TURN)[5]. Також, WebRTC використовує протокол SDP для налаштування потоку медіаданих шляхом описання початкових параметрів.

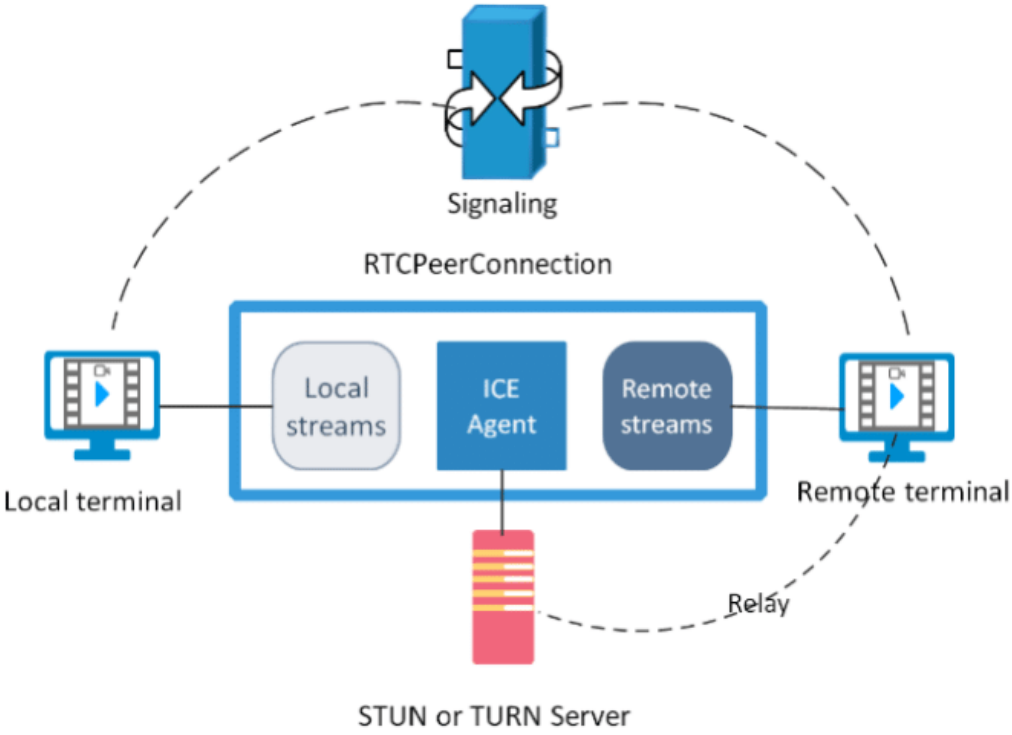

Рисунок 2.1 - Структурна схема складових WebRTC

Розглянемо приклад з'єднання двох WebRTC застосунків. Аліса і Боб обидва користувачі загальної служби дзвінків. Для того, щоб спілкуватися, вони повинні бути одночасно підключені до веб-сервера, який реалізує службу виклику. Коли вони спрямовують свої браузери на веб-сторінку служби викликів, вони завантажують сторінку HTML, що містить JavaScript код, який підключається до сервера через безпечне з'єднання HTTPS або WebSocket. Коли Аліса натискає кнопку веб-сторінки, щоб розпочати дзвінок з Бобом, JavaScript створює об'єкт PeerConnection. Після створення PeerConnection код JavaScript на стороні служби виклику повинен налаштувати медіа за допомогою функції MediaStream. Також необхідно, щоб Аліса надала доступ до своєї камери та мікрофона.

У поточному API W3C після додавання деяких потоків, браузер Аліси, генерує сигнальне повідомлення. Точний формат такого повідомлення ще остаточно не визначений. Відомо, що він повинен містити інформацію про медіа-канал і кандидатів ICE, а також інформацію, яка прив'язує повідомлення до відкритого ключа Аліси. Потім це повідомлення надсилається на сервер сигналізації (наприклад, за допомогою XMLHttpRequest або WebSocket). На рисунку 2.2

зображено типовий потік викликів, пов’язаний із налаштуванням каналу зв’язку між Алісою та Бобом у реальному часі. Сервер сигналізації обробляє повідомлення з браузера Аліси, та визначає, що це виклик Боба, надсилає сигнальне повідомлення браузеру Боба. JavaScript у браузері Боба обробляє вхідне повідомлення та сповіщає Боба. Якщо Боб вирішить відповісти на дзвінок, JavaScript, який працює в його браузері, створить екземпляр PeerConnection, пов’язаний з повідомленням, яке надходить від Аліси. Потім відбуватиметься процес, подібний того що робилось у Аліси. Браузер Боба перевіряє, що служба виклику схвалена, а медіа-потоки створено; після цього сигнальне повідомлення, що містить медіа-інформацію, кандидатів ICE, надсилається назад Алісі через службу сигналізації.

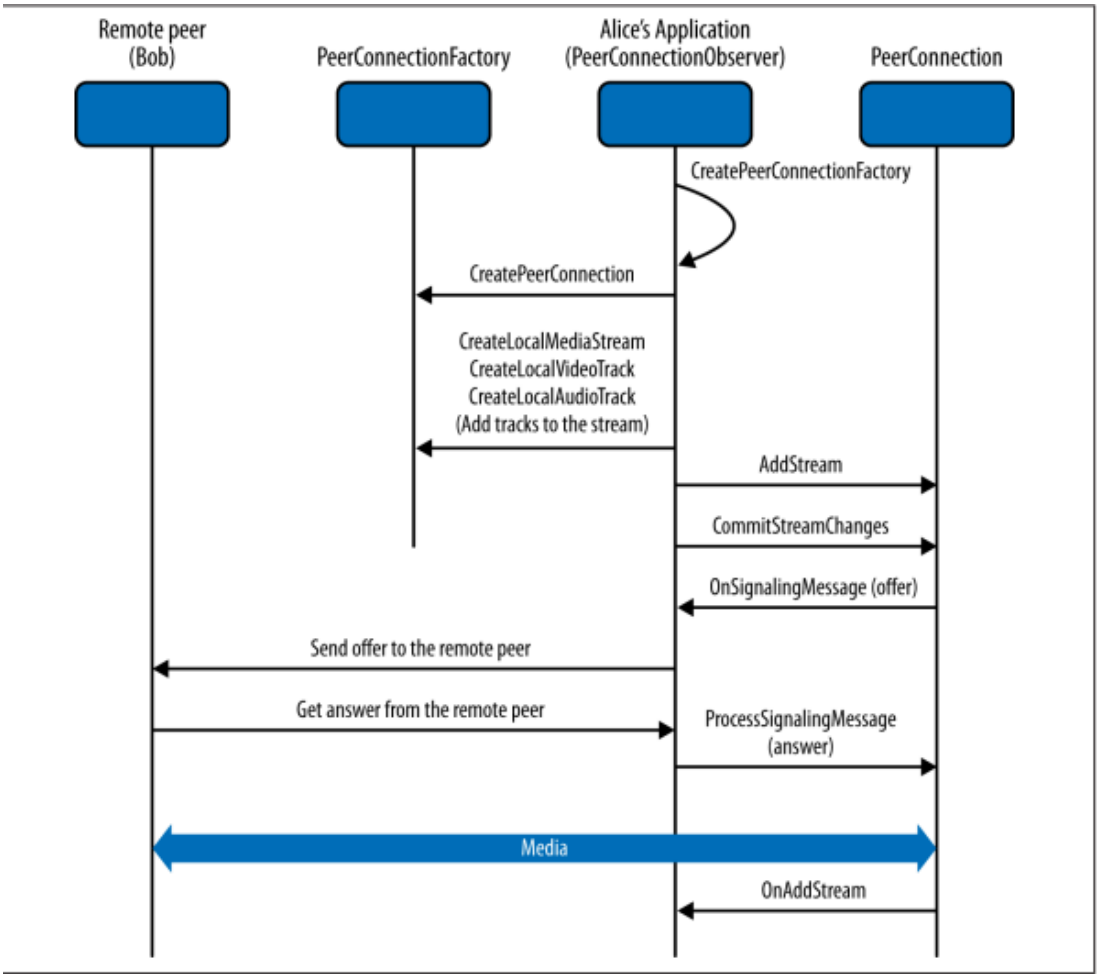

Рисунок 2.2 – Процес ініціалізації з’єднання поміж користувачами

2.1.1 Транспортний рівень WebRTC

«Утиліти проходження сеансів для NAT» (STUN) дозволяють клієнтам дізнатися, яка їх публічна IP-адреса та порт із NAT. Як тільки ці дані буде отримано, можна буде надати правильні дані іншим клієнтам, які хочуть підключитися до вас. Як правило, потрібен сервер STUN. Клієнт STUN може надсилати повідомлення на сервер STUN, щоб отримати інформацію про загальнодоступну IP-адресу і порти. Однак цей протокол не працює для симетричних NAT. Симетричні NAT, які генерують порти, є випадковими для прив'язок. STUN не може підтримати динамічне розподілення портів під час узгодження медіа-шляхів.

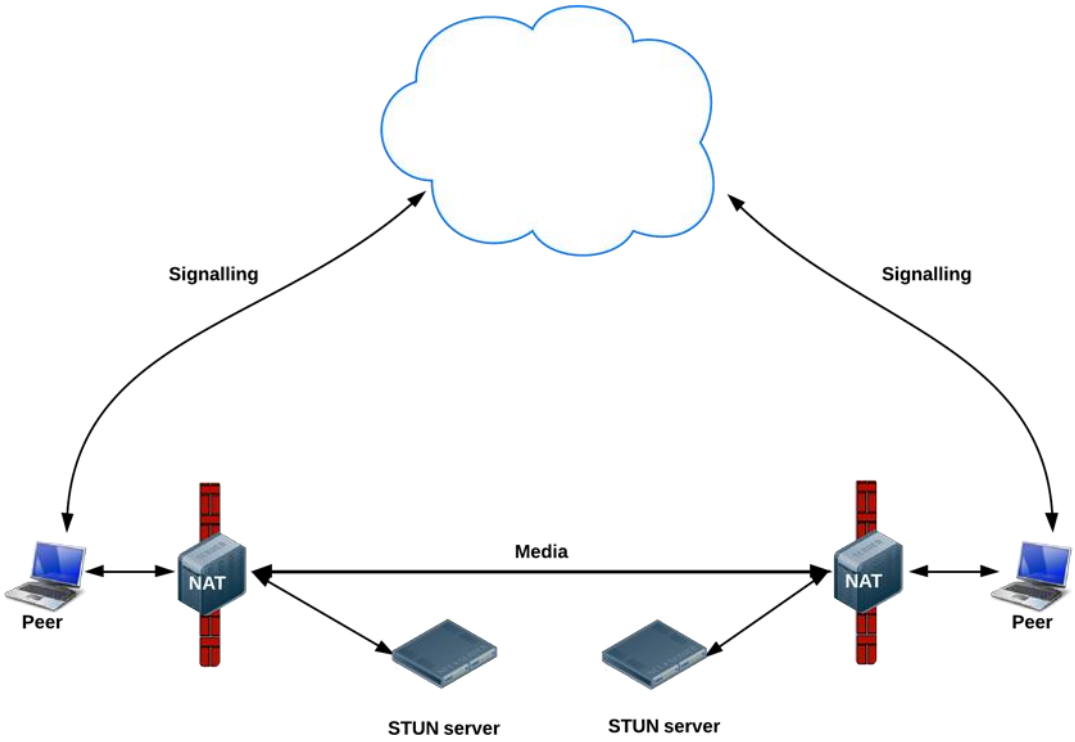

Рисунок 2.3 - Структурна схема використання STUN серверу

«Обхід за допомогою Relay NAT» (TURN) дозволяє клієнтам відправляти та отримувати дані через сервер-посередник. Протокол TURN є розширенням протоколу STUN. Коли клієнти знаходяться за різними типами NAT або коли використовується симетричний NAT, легше надсилати медіа через сервер ретрансляції. Це те, що робить TURN. Клієнти підключаються до сервера TURN, а не намагаються підключитися через NAT [6].

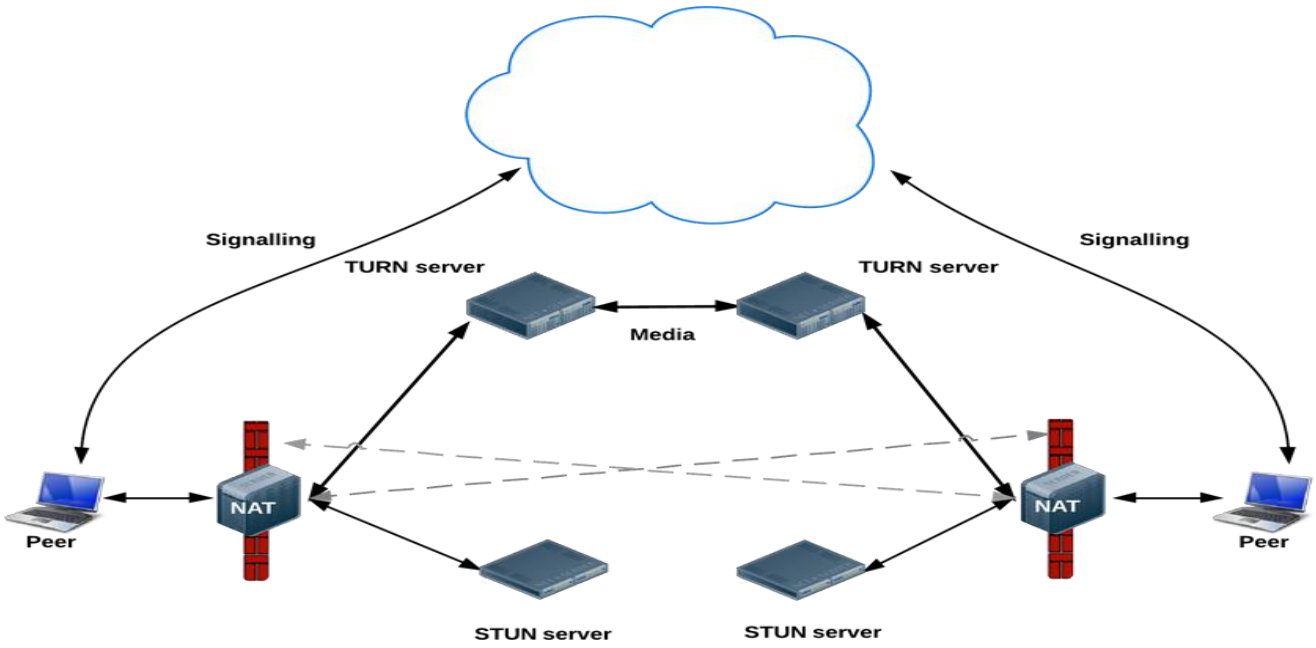

Рисунок 2.4 - Структурна схема використання TURN серверу

2.1.2 Голосовий рушій WebRTC

В основі обробки голосового потоку лежить протокол iSAC (internet Speech Audio Codec), розроблений компанією Global IP Solutions. Закодовані блоки повинні бути інкапсульовані у відповідний протокол транспортного рівня, в нашому випадку – це SRTP.

Протокол iSAC має наступні параметри:

– частота дискретизації 32 kHz;
– змінний бітрейт від 10 кбіт/с до 52 кбіт/с;
– адаптивний розмір пакету від 30 до 60 мс;
– алгоритмічна затримка ~3 мс.

Також, у WebRTC може використовуватись протокол iLBC (internet Low Bitrate Codec). Він призначений для вузькополосних інтернет-каналів, зі швидкістю передачі аудіосигналу – 13.33 кбіт/с при довжині кадру 30 мс та 15.20 кбіт/с при 20 мс.

Протокол iLBC має наступні параметри:

– частота дискретизації 8 кГц/16 біт;
– фіксований бітрейт:

– фіксований розмір кадру (304 біта в кадрі 20 мс, 400 біт в кадрі 30 мс).

Для зменшення джиттеру та втрати пакетів, використовується NetEQ. Його головна мета — забезпечити плавне відтворення вхідних аудіопакетів із мережі з невеликою кількістю аудіо артефактів (зміни оригінального вмісту пакетів) і, в той же час, зберегти якомога меншу затримку.

2.1.3 RTCPeerConnection

PeerConnection [7] дозволяє двом користувачам спілкуватися безпосередньо, браузер з браузером. Це являється віддаленим одноранговим з'єднанням, яке зазвичай і є іншим екземпляром тієї ж програми JavaScript, що працює на іншому кінці. Зв'язок координується через канал сигналізації, наданий кодом JavaScript на сторінці через веб-сервер, наприклад, XMLHttpRequest або WebSocket. Після встановлення однорангового з'єднання мультимедійні потоки (локально пов'язані з об'єктами MediaStream, визначеними для спеціального призначення) можуть спілкуватись безпосередньо з віддаленим браузером.

Механізм PeerConnection використовує протокол ICE разом із серверами STUN та TURN, щоб дозволити медіа-потокам на основі UDP передаватись через NAT та брандмауери. ICE дозволяє браузерам виявляти достатньо інформації про топологію мережі, щоб знайти найкращий шлях зв'язку, який можна використовувати. Використання ICE також забезпечує захід безпеки, оскільки не дозволяє ненадійним веб-сторінкам і додаткам надсилати дані хостам, які не очікують їх отримати. Кожне повідомлення що прийшло, передається в PeerConnection. API надсилають сигнальні повідомлення, які більшість додатків розглядатимуть як чорні ящики, але вони повинні безпечно та ефективно передаватися іншим одноранговим веб-додаткам через веб-сервер.

2.2 Вектори вразливості WebRTC

WebRTC – це перша технологія на основі браузера, яка порушує сувору архітектуру сервер-клієнт у мережі, забезпечуючи прямий зв'язок між браузером без сервера, що виступає посередником та передає дані. Специфікації на протокол

навмисно відкриті, щоб використовувати декілька рішень шляхом розділення сигнальної та медіа-площин без вказівки, який протокол буде використовуватися як сигнальний. Однак, поки в основному це вигідно для всіх сторін, різноманітність серед існуючих рішень в кінцевому підсумку означає, що не існує єдиного безпечного рішення, що працюватиме для кожної реалізації [8]. WebRTC має велику комбінацію утиліт, що робить його цікавою мішенню для атаки. Наприклад, зловмисники можуть:

– зловживати JavaScript API;
– зламати веб-сайт постачальника послуг;
– створити плутанину в ідентифікації;
– створити зв'язки між неправильними користувачами.

Традиційні двосторонні заходи веб-безпеки клієнт-сервер передбачають використання HTTPS, але в більш складній взаємодії, такій як передача файлів або програми VoIP, де використовується WebRTC з існуванням серверу для посередництва між користувачами, протокол HTTPS не є ефективним.

У цих випадках користувачі повинні отримати довіру сервера, щоб він не використовував дані негативним чином, логував, змінював особисту інформацію або не змінював повідомлення.

WebRTC страждає від цих проблем, оскільки проміжний сервер сигналізації — це лише засіб дістатися до користувачів, з якими вони дійсно хочуть спілкуватися. Це фактично означає, що шкідливий сайт на основі WebRTC може підключитися до невірної особи. WebRTC не може функціонувати без серверів сигналізації з багатьох причин, наприклад, підключення може змінитися, і тоді потрібен сервер сигналізації, щоб партнери могли повторно підключитись та обмінюватися запитами/відповідями.

2.3 Проблема підтвердження ідентифікації користувачів

Сервер потенційно може записувати або перенаправляти повідомлення або дзвінки користувачів. Щоб забезпечити наскрізну безпеку без довіри сайту, що викликає, потрібен новий спосіб контролю автентифікації, тому введено постачальник ідентифікації (Identity Assertion Provider idP). Ідентифікатор можна використовувати разом із WebRTC для підтвердження того, що користувач є

авторизованим користувачем, а також може повертати іншу інформацію про відповідного користувача, наприклад, ім’я користувача або електронну адресу. Ця модель ідентифікації на основі повноважень також повинна бути незалежною від сайту, що викликає, для забезпечення безпеки; ілюстрація реалізації idP для WebRTC показана на рисунку 2.5 [9].

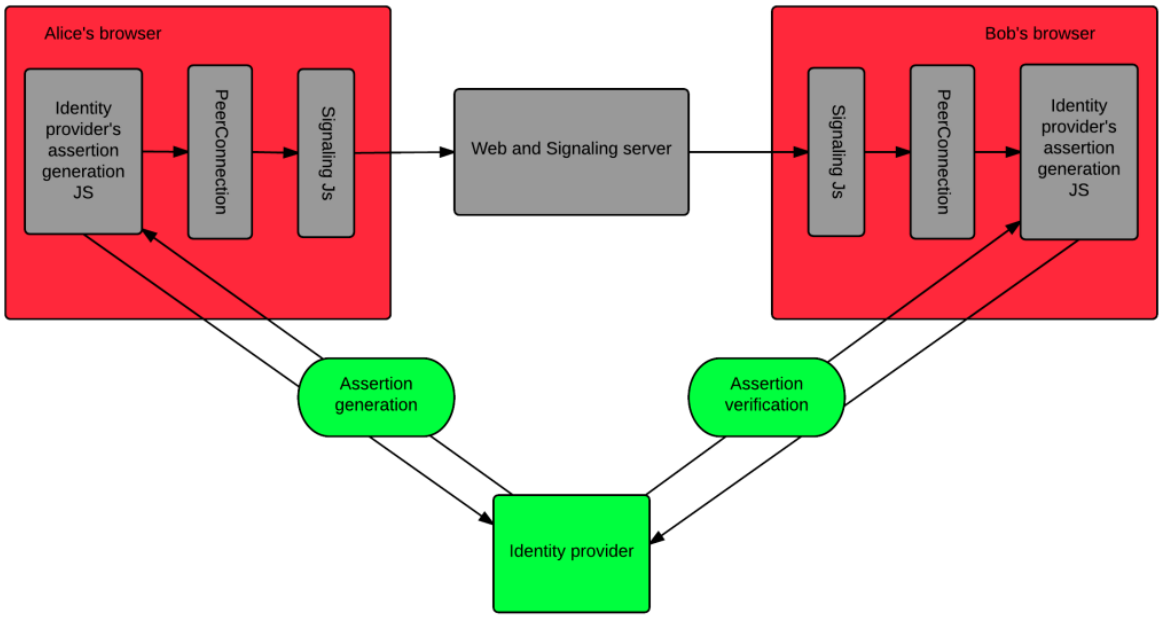

Рисунок 2.5 - Життєвий цикл ідентифікації WebRTC

При реалізації моделі ідентифікації на основі повноважень будь-який веб-сервер може діяти як idP, якщо він здатний надавати JavaScript код для перевірки дійсності. Цей код перевіряє особу користувача та створює підтвердження ідентичності, прив’язуючи ідентифікатор користувача з відкритим ключем, який використовується в сеансі безпеки транспортного рівня дейтаграм – безпечного транспортного протоколу реального часу (DTLS-SRTP) [10]. Коли користувач хоче здійснити виклик, сервер сигналізації додатків WebRTC надсилає підтвердження абоненту. Підтвердження містить доменне ім’я постачальника ідентифікаційних даних. Для того щоб абонент підтвердив ідентичність, браузер абонента завантажує код підтвердження ідентичності постачальників і просить перевірити підтвердження, яке він отримав від сервера сигналізації. Якби WebRTC реалізовував

спосіб легкого використання підтвердження ідентичності, ми були б впевнені, що не відбулась підміна, та користувач є дійсно тим самим користувачем.

2.4 Проблема витікання IP-адрес

Впровадження WebRTC API в сучасні браузери створила нову загрозу конфіденційності користувачів [11]. Дане API використовує діапазони IP-адрес клієнта, які стануть доступними для відвідуваного веб-сайту через JavaScript, навіть якщо використовується VPN. Це потенційно серйозна проблема для користувачів, які використовують послуги VPN для анонімності.

В ідеальному варіанті , коли користувач підключається до Інтернету через віртуальну приватну мережу (VPN), IP-адреси (наприклад, публічна IP-адреса) клієнтського пристрою прихована від відвідуваних веб-сайтів. Якщо користувач використовує VPN з міркувань анонімності, то відкриває одну чи більше своїх IP-адрес відвідуваному веб-сайту або додатку для браузера, який може виконувати JavaScript у браузері клієнта і це ймовірно, спростує ціль використання VPN. Розкриття IP-адрес клієнта може дозволити відстежувати та/або ідентифікувати клієнта. Крім того, за допомогою пошуку геолокації, публічна IP-адреса клієнта може розкрити його країну і місто.

Впровадження WebRTC у сучасні веб-браузери створило новий і простий метод для веб-сайтів виявляти IP-адресу клієнта. WebRTC — це набір API та протоколів зв'язку, які надають браузерам і мобільним додаткам можливості зв'язку в реальному часі (RTC). Ідентифікація клієнтських IP-адрес за допомогою функцій WebRTC вперше була продемонстрована розробником Roesler [12] у 2015 році. У цій статті вказано на розкриття IP-адреси клієнта веб-сайту на основі WebRTC під час використання VPN.

Метод Роеслера можна використовувати для виявлення низки IP-адрес клієнтів за допомогою коду JavaScript, який виконується в браузері, що підтримує WebRTC. Приватні (або внутрішні) IP-адреси (тобто адреси, дійсні лише в локальній підмережі) можна отримати з протоколу SDP, який необхідний для встановлення P2P (peer-to-peer) підключення, тоді як загальнодоступні (або зовнішні) IP-адреси (тобто глобально унікальні адреси) можна отримати шляхом успішного пінгу сервера

STUN. Сервер STUN (Session Traversal of User Datagram Protocol) через Network Address Translators (NATs) server дозволяє клієнту NAT встановлювати зв'язок, наприклад телефонний дзвінок з провайдером VoIP, розміщеним поза локальною мережею. Важливо зазначити, що витоки IP адрес можуть вплинути на конфіденційність клієнта, навіть якщо VPN не використовується. Це пов'язано з тим, що приватна IP-адреса клієнта може витікати, інформація, яка в іншому випадку не була б доступна для веб-сайту, навіть за відсутності VPN. Однак ці адреси не обов'язково дуже чутливі до конфіденційності, оскільки клієнтам зазвичай призначаються приватні адреси IPv4 в діапазоні 192.168.0.x.

WebRTC визначає IP-адреси, використовуючи ICE протокол. Дана технологія надає можливість визначити IP-адресу двома шляхами, які описані нижче.

2.4.1 Визначення IP-адрес за допомогою STUN/TURN серверів

STUN/TURN сервери грають важливу роль у протоколі WebRTC, вони надають дозвіл веб-браузерам отримувати інформацію про публічну IP-адресу, також полегшують можливість спілкування поміж двома пристроями, навіть якщо ці пристрої знаходяться за NAT. В цьому і є проблема, STUN/TURN сервери напряму впливають на приватність, тому що видають IP-адресу веб-сайту, щоразу ви відвідуєте його.

2.4.2 Визначення IP-адрес за допомогою виявлення хостинг кандидатів

Більшість пристроїв мають кілька IP-адрес, пов'язаних з їх апаратним забезпеченням. Зазвичай вони приховані від веб-сайтів і серверів STUN/TURN через брандмауери. Проте опис протоколу ICE визначає, що браузери можуть збирати ці IP-адреси, просто зчитуючи їх із вашого пристрою.

IP-адреси, які найчастіше асоціюються з вашим пристроєм, є локальними адресами IPv4, і їх виявлення не вплине на вашу конфіденційність. Однак, якщо у вас є адреси IPv6, ваша конфіденційність може бути під загрозою.

Адреси IPv6 не працюють так само, як адреси IPv4. Як правило, IPv6-адреса є загальнодоступною (що означає, що вона унікальна для вас). Якщо у вас є IPv6-

адреса, пов’язана з вашим пристроєм, і вона виявляється через ICE, ваша конфіденційність під загрозою.

Веб-сайт може використовувати сервери STUN/TURN або метод хостинг кандидатів щоб обманом змусити ваш браузер розкрити IP-адресу, яка може ідентифікувати вас, без вашого відома.

2.4.3 IP-адреси, що під загрозою розкриття за допомогою технології WebRTC

– Публічна IPv6 адреса: це IPv6 адреса системи, що надається провайдером інтернету (ISP);

– публічна тимчасова IPv6 адреса: це адреса, що призначена мережею, до якої приєднана клієнтська платформа;

– унікальна локальна адреса (ULA) надана LAN: це IPv6 адреса, що призначена мережею, до якої приєднана клієнтська платформа, та є протилежністю приватної IPv4 адреси;

– приватна IP адреса, призначена VPN сервером: приватна (IPv4 або IPv6, в залежності від конфігурації VPN) адреса, що призначена VPN сервером;

– приватна IPv4 адреса, призначена LAN: дана адреса призначена локальною мережею до якої приєднаний клієнт.

Розкриття IPv6 адрес є більш серйозним у разі приватності, в порівнянні з IPv4. Також, витік IP-адрес клієнтів, у яких призначення IP-адрес відбувається статично, більш вірогідніший, аніж у клієнтів що мають динамічне призначення IP-адрес.

2.5 Проблеми створення групових конференцій

Виходячи з призначення технології WebRTC, відомо, що вона підтримує лише однорангові з’єднання (тобто peer-to-peer). Тому постає проблема в підключенні більше двох клієнтів до однієї групи. Дана проблема вирішується використанням сітчастих-мереж , приклад яких наведений на рисунку 2.6(mesh).

Сітчаста мережа — топологія комп'ютерної мережі, в якій кожен вузол (називається вузлом меш) передає дані по мережі і виступає в ролі комутатора. Всі вузли співпрацюють у розподілі даних в мережі, тобто кожен вузол бере участь у передачі даних.

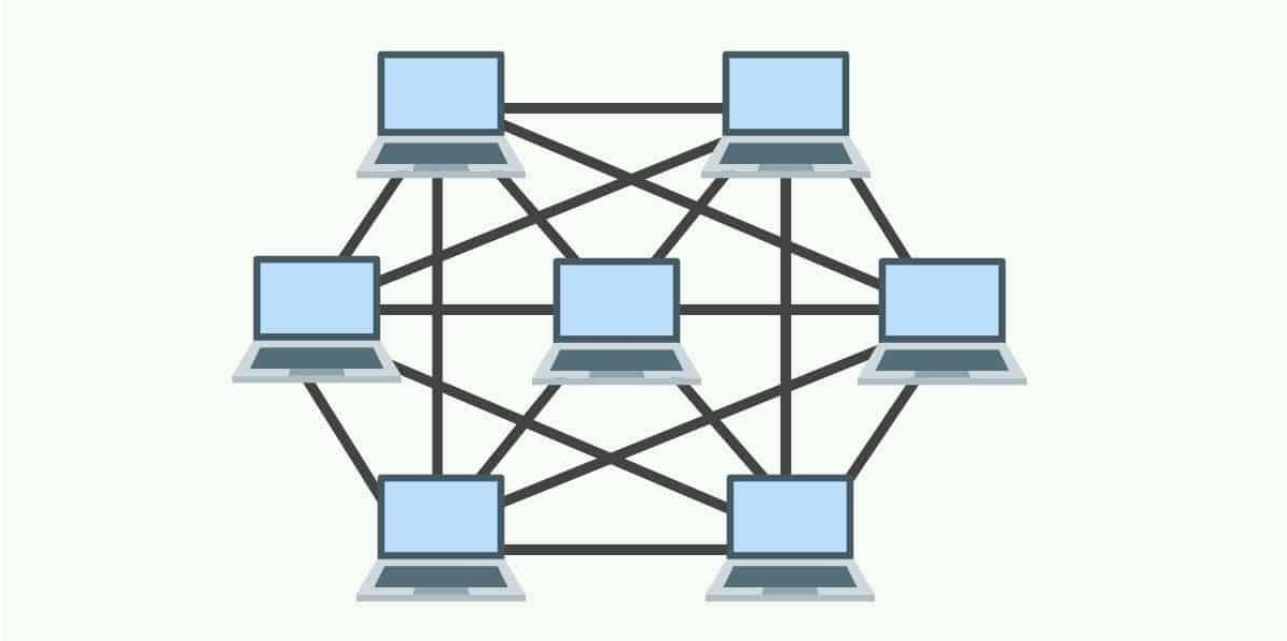

Рисунок 2.6 - Приклад структури сітчастої мережі

Для утворення групового дзвінка, потрібен сигнальний сервер, до якого під’єднуються усі користувачі, для обміну інформацією про їх браузери.

Користувачі підключаються у сітчасту-мережу, формуючи групу, структура наведена на рисунку 2.7, і передаючи одну і ту ж інформацію усім користувачам в мережі в одночас [13].

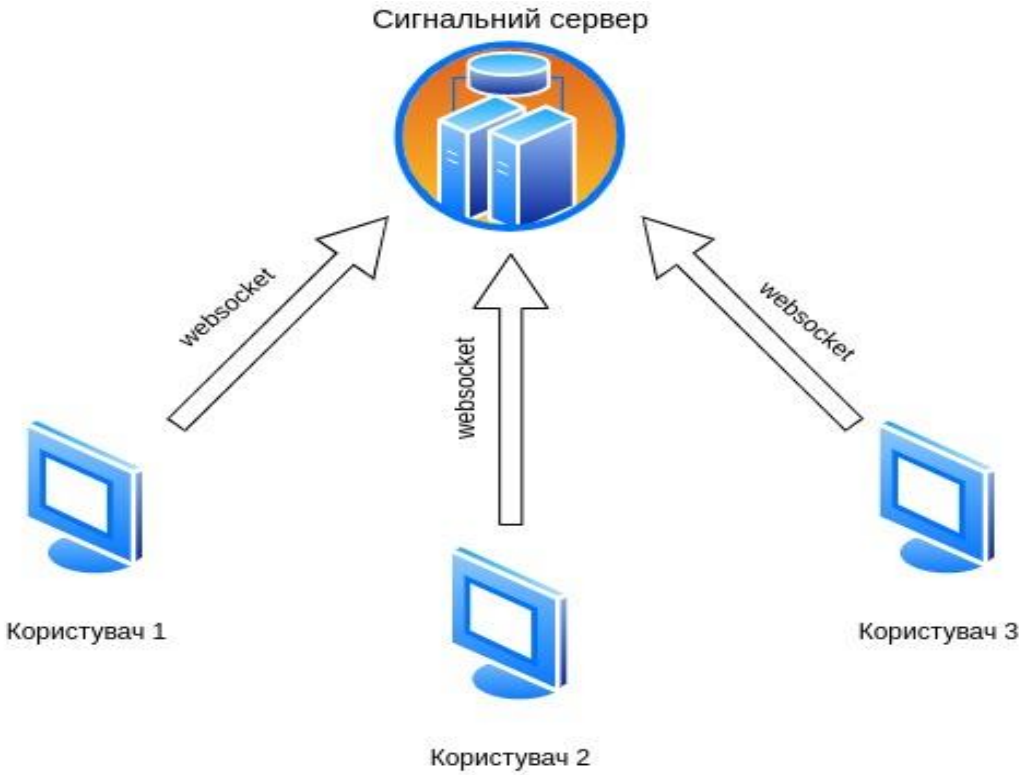

Рисунок 2.7 - Процес формування групового дзвінка

Користувачі підключаються безпосередньо один до одного в сітчастій мережі(рис 2.8) за допомогою webrtc datachannel. Повідомлення чату надсилатимуться безпосередньо між користувачами, не проходячи через сервер сигналів.

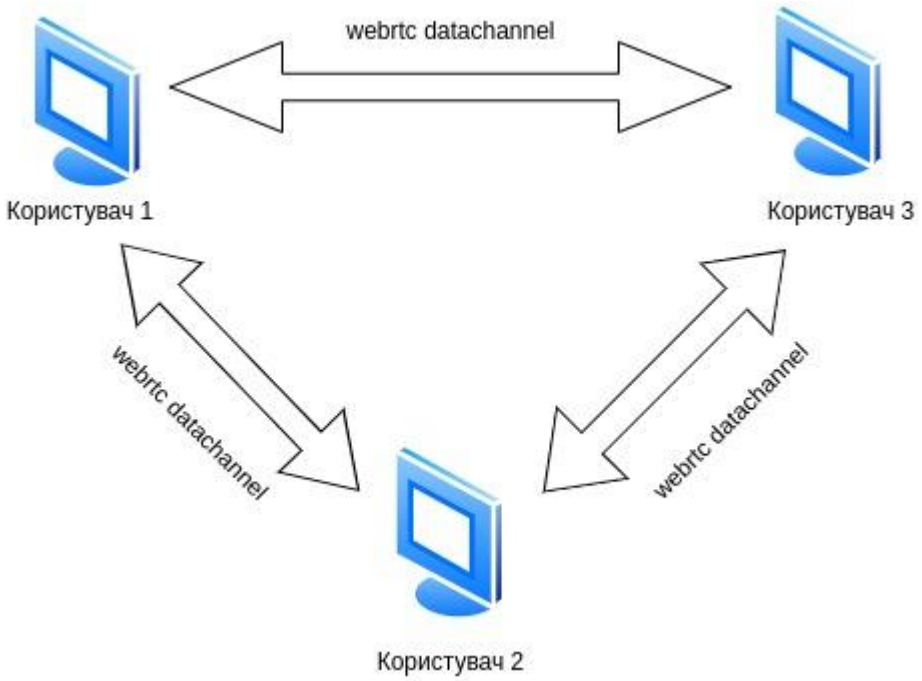

Рисунок 2.8 - Сітчаста мережа

У разі невдачі при обході NAT, обмін повідомленнями може відбуватись через виділений сервер.

2.6 Анонімізація за допомогою VPN або віртуалізації

Через проблему витоку IP-адрес, є проблеми з безпекою користувача, якщо він не бажає, аби його IP-адресу дізнались інші користувачі. Для забезпечення анонімності при використанні технології WebRTC можна використати VPN, що приховає вашу реальну IP-адресу або скористатись віртуальною машиною.

2.6.1 VPN та анонімність

VPN (Virtual Private Network) або віртуальна приватна мережа(рис 2.9) – це захищений тунель між вашим пристроєм і мережею Інтернет. Підключення до мережі VPN захищає інтернет-трафік від прослуховування, стороннього втручання і цензури [14].

Рисунок 2.9 - Структурна схема підключення VPN

Використання VPN змінює вашу IP-адресу, унікальний номер, за яким можна легко ідентифікувати вашу особу та місце, де ви зараз перебуваєте. За допомогою нової IP-адреси ви можете користуватися Інтернетом, так якщо б ви перебували в Великобританії, Німеччині, Канаді, Японії або будь-який іншій країні, в якій у VPN-сервісу є сервери.

Зміна IP-адреси за допомогою VPN приховує вашу особистість від веб-сайтів, додатків і сервісів, які хочуть відстежувати ваші дії. Крім того, хороші VPN приховують все, що ви робите онлайн, від вашого інтернет-провайдера, оператора

мобільного зв’язку і всіх, хто може отримати доступ до трафіку. Це можливо завдяки надійному шифруванню.

2.6.2 Віртуалізація та анонімність у WebRTC

Віртуальна машина [15] – це спеціальне програмне забезпечення, яке емулює роботу фізичної машини. Попри те, що віртуальна машина знаходиться в межах реального фізичного "хазяїна" і використовує його ресурси, вона лишається цілком незалежною, оскільки володіє власними програмними компонентами (процесором, материнською платою, відеоадаптером, мережевим інтерфейсом, пам'яттю, жорсткими дисками), які можуть навіть відрізнятися від тих, які має хост, а також містить свою ОС і додатки.

Операційна система, на якій встановлено віртуальну машину, називається основною або хост-ОС, а операційна система самої віртуальної машини називається гостьовою. Кожна гостьова ОС запускається в окремому вікні на основній ОС, аналогічно до звичайної програми.

Все віртуальне обладнання, яке живить гостьову ОС, керується спеціальним механізмом, який називається гіпервізором. Гіпервізор відомий як менеджер віртуальної машини: він виділяє фізичні ресурси для кожної з систем і гарантує, що вони не перериватимуть роботу одна одної. Як правило, гіпервізори реалізуються на програмному рівні, але існують і такі, що вже вбудовані в прошивку системи.

Існує два способи виходу віртуальної машини в Інтернет [16]:

1. Міст.

Коли гостьова віртуальна машина запускаться, вона безпосередньо використовує мережевий адаптер хоста і виходить в Інтернет. У цьому випадку гостьова віртуальна машина використовуватиме ту саму IP-адресу як і хост. Це не є прийнятним з міркувань безпеки.

2. Трансляція мережевих адрес (NAT).

Це найпоширеніший метод, який використовується і вважається безпечним. Хост-машина буде діяти як шлюз NAT (він же маршрутизатор), переводячи IP-адресу

гостьової віртуальної машини на свою власну для виходу в Інтернет. Весь трафік надходить з хост-машини, оскільки NAT приховує справжній IP гостьової віртуальної машини.

Використовуючи другий метод підключення до інтернету через NAT, ми можемо спробувати приховати нашу реальну IP-адресу, і навіть якщо відбудеться витік IP-адреси віртуальної машини, це не буде нести ніякої важливої інформації.

Висновки до розділу 2

1. Детально оглянуто складові архітектури WebRTC, а саме транспортний рівень та голосовий рушій. Визначено тонкощі підключення користувачів, які знаходяться за різними типами NAT.

2. Розібрано вектори вразливостей технології WebRTC. Через високу кількість архітектурних елементів, WebRTC має велику кількість векторів атак, що ускладнює задачу забезпечення безпеки.

3. Розглянуто спосіб ідентифікації користувачів. Даний спосіб є небезпечний тим, що будь-який сервер може виступати у ролі ідентифікатора користувачів, тому ми не можемо знати, що спілкуємось саме з тим користувачем.

4. Оглянуто проблеми витоку IP-адрес. Це є основною проблемою анонімізації в WebRTC. З’ясовано причини, чому відбувається виток IP-адрес та які саме типи IP-адрес схильні бути розкриті.

5. Виявлено причину проблеми створення групових конференцій. Встановлено, що реалізація сіткової мережі за допомогою проміжного сигнального серверу надасть можливість створення групових дзвінків.

6. Виконано огляд двох варіантів анонімізації користувача при роботі з WebRTC. Використовуючи VPN або віртуалізацію, можливо досягти підміни IP-адреси, що в свою чергу збереже від витоку реальну IP-адресу.

РОЗДІЛ 3 РОЗРОБКА СИСТЕМИ ГРУПОВИХ ДЗВІНКІВ ТА АЛГОРИТМУ ДІЙ АНОНІМІЗАЦІЇ В WEBRTC

3.1 Розробка системи групових аудіо-конференцій

За основу системи взято код з сайту github [17]. Середовищем для тестування та розробки виступав дистрибутив на основі ядра Linux Ubuntu 18.04. Для запуску та перевірки системи використовувався браузер Chromium.

3.1.1 Архітектурні складові системи

Систему можна представити у вигляді двох складових: серверної та клієнтської.

Серверна частина використовує node.js та socket.io для створення сигнального серверу. Даний сервер розподіляє інформацію поміж користувачами та налаштовує сітчасту мережу.

Клієнтська частина використовує JavaScript код, який виконує усі етапи: підключення, створення віртуального чату, передача аудіо-потоку до всіх користувачів, використовуючи WebRTC API.

3.1.2 Підготовка середовища

Для розробки та тестування системи, потрібно встановити додаткове програмне забезпечення, а саме сервер node.js.

Команди, наведені на рисунку 3.1 встановлюють в систему пакети, що потрібні для правильної роботи серверу.

```
sudo apt-get install nodejs-dev node-gyp libssl1.0-dev
sudo apt install npm
npm install
```

Рисунок 3.1 - Команди для встановлення серверу

Конфігурація серверу наведена на рисунку 3.2 нижче.

Рисунок 3.2 - Конфігурація серверу

3.1.3 Розробка серверної частини

Виходячи з конфігураційного файлу для серверу, видно, що при запусканні серверу командою *npm run start* файл **signaling-server.js** підвантажується та починає відповідати на запити від клієнтів.

Користувачі підключаються до сервера сигналізації, після чого вони видають сигнал «join», щоб приєднатися до певного каналу. Код наведений на рисунку 3.3.

```
socket.on('join', function (config) {
    console.log("["+ socket.id + "] join ", config);
    var channel = config.channel;
    var userdata = config.userdata;

    if (channel in socket.channels) {
        console.log("["+ socket.id + "] ERROR: already joined ", channel);
        return;
    }

    if (!(channel in channels)) {
        channels[channel] = {};
    }

    for (id in channels[channel]) {
        channels[channel][id].emit('addPeer', {'peer_id': socket.id, 'should_create_offer': false});
        socket.emit('addPeer', {'peer_id': id, 'should_create_offer': true});
    }

    channels[channel][socket.id] = socket;
    socket.channels[channel] = channel;
});
```

Рисунок 3.3 - Функція обробник join

Сервер сигналізації відстежує всі сокети, які знаходяться в каналі, і під час приєднання надсилатиме події 'addPeer' кожній парі користувачів у каналі. Коли клієнти отримають 'addPeer', вони почнуть налаштовувати RTCPeerConnection один з одним. Під час цього процесу їм потрібно буде передати один одному інформацію ICECandidate, а також інформацію SessionDescription. Код наведений на рисунку 3.4.

```
socket.on('relayICECandidate', function(config) {
    var peer_id = config.peer_id;
    var ice_candidate = config.ice_candidate;
    console.log("["+ socket.id + "] relaying ICE candidate to [" + peer_id + "] ", ice_candidate);

    if (peer_id in sockets) {
        sockets[peer_id].emit('iceCandidate', {'peer_id': socket.id, 'ice_candidate': ice_candidate});
    }
});
```

Рисунок 3.4 - Функція обробник relayICECandidate

Після налаштування вони зможуть завершити однорангове з’єднання і будуть транслювати аудіо між собою.

3.1.4 Розробка клієнтської частини

При приєднанні до серверу, клієнт отримує сторінку з JavaScript кодом яку і починає виконувати. Коли користувач приєднується до групи, сервер сигналізації надсилає подію 'addPeer' кожній парі користувачів у групі. Код наведений на рисунку 3.5.

```
signaling_socket.on('addPeer', function(config) {
    console.log('Signaling server said to add peer:', config);
    var peer_id = config.peer_id;
    if (peer_id in peers) {
        /* This could happen if the user joins multiple channels where the other peer is also in. */
        console.log("Already connected to peer ", peer_id);
        return;
    }
    var peer_connection = new RTCPeerConnection(
        {"iceServers": ICE_SERVERS},
        {"optional": [{"DtlsSrtpKeyAgreement": true}]} /* this will no longer be needed by chrome
                                                        * eventually (supposedly), but is necessary
                                                        * for now to get firefox to talk to chrome */
    );
    peers[peer_id] = peer_connection;
```

Рисунок 3.5 - Функція обробник addPeer

Паралельно відслідковується під’єднання користувачів, при успішному приєднанні викликається функція *ontrack*. Код наведений на рисунку 3.6.

```
peer_connection.ontrack = function(event) {
    console.log("ontrack", event);
    var remote_media = USE_VIDEO ? $("<video>") : $("<audio>");
    remote_media.attr("autoplay", "autoplay");
    if (MUTE_AUDIO_BY_DEFAULT) {
        remote_media.attr("muted", "true");
    }
    remote_media.attr("controls", "");
    peer_media_elements[peer_id] = remote_media;
    PEERS_COUNT++;
    var usr_str = "USER #" + PEERS_COUNT.toString();
    var par = document.createElement("p");
    var text = document.createTextNode(usr_str);
    var x = document.createElement("STYLE");
    var t = document.createTextNode("body {font: 40px verdana;color: white}");
    x.appendChild(t);
    par.appendChild(text);
    par.appendChild(x);
    $('body').append(par);
    $('body').append(remote_media);

    attachMediaStream(remote_media[0], event.streams[0]);
}
```

Рисунок 3.6 - Функція обробник ontrack

Клієнти обмінюються описами сеансів функцією sessionDescription, які містять інформацію про їхні налаштування аудіо характеристик. Спочатку «пропонувач» надсилає опис «відповідачеві» (з типом «offer»), потім відповідач надсилає його назад (з типом «answer»). Код наведений на рисунку 3.7.

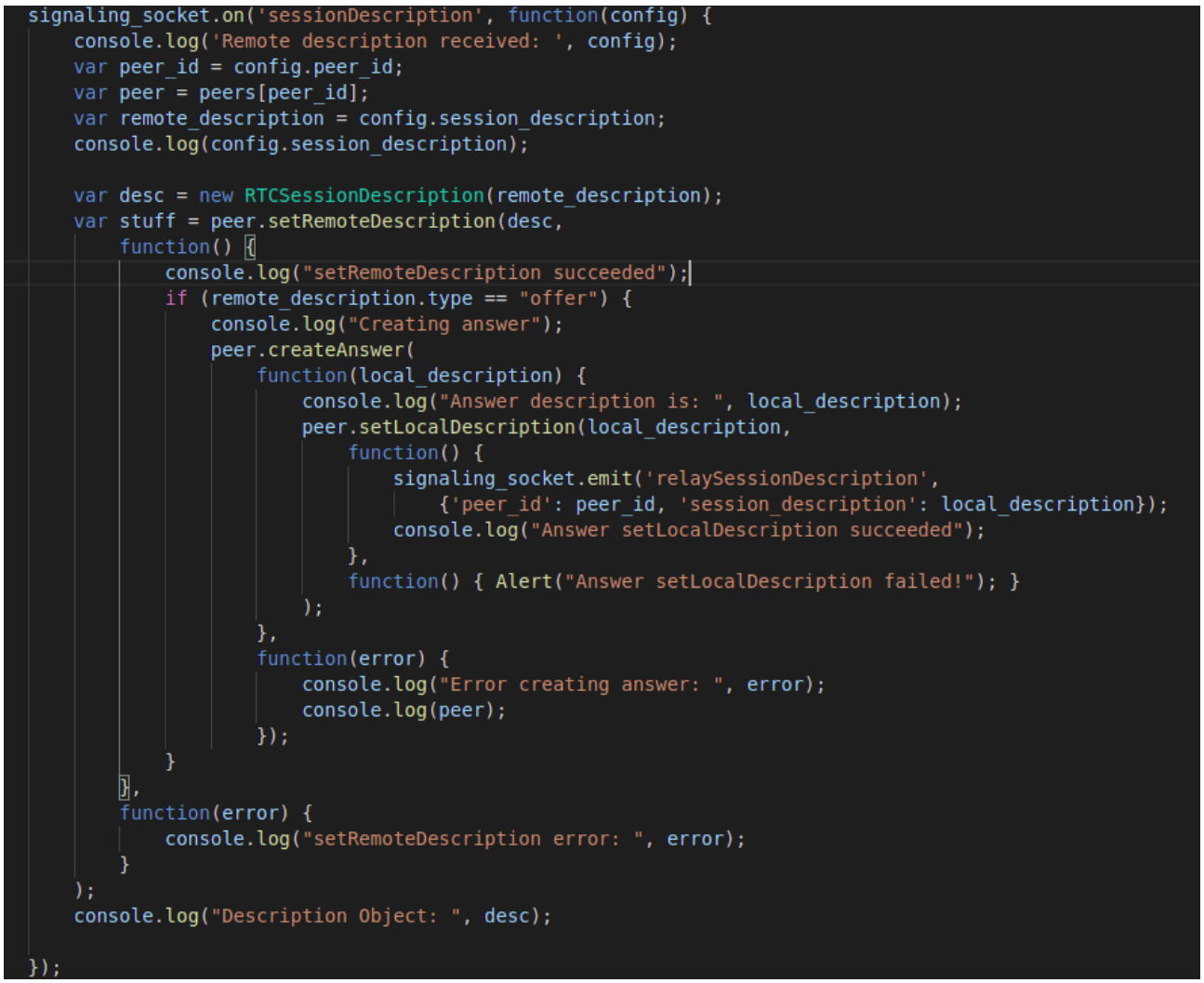

Рисунок 3.7 - Функція обробник sessionDescription

Коли користувач залишає канал (або відключається від сервера сигналізації), кожен користувач отримає повідомлення «removePeer» із вказівкою видалити медіа-канали, які вони відкрили для цього користувача. Якщо саме цей клієнт залишив канал, він також отримає RemovePeers. Якщо цей клієнт був відключений, він не отримуватиме removePeers, запуститься код signaling_socket.on ('disconnect') та зруйнує всі однорангові сеанси. Код наведений на рисунку 3.8.

```
    */
    signaling_socket.on('removePeer', function(config) {
        console.log('Signaling server said to remove peer:', config);
        var peer_id = config.peer_id;
        if (peer_id in peer_media_elements) {
            peer_media_elements[peer_id].remove();
        }
        if (peer_id in peers) {
            peers[peer_id].close();
        }

        delete peers[peer_id];
        delete peer_media_elements[config.peer_id];
    });
}
```

Рисунок 3.8 - Функція обробник removePeer

3.1.5 Запуск та тестування системи

Для запуску серверу, потрібно виконати команду *npm run start*. Для полегшення тестування, сервер запускається на loopback адресі. Створюємо групову конференцію, шляхом відкриття трьох браузерів та під'єднання до серверу. Результат можна побачити на рисунку 3.9.

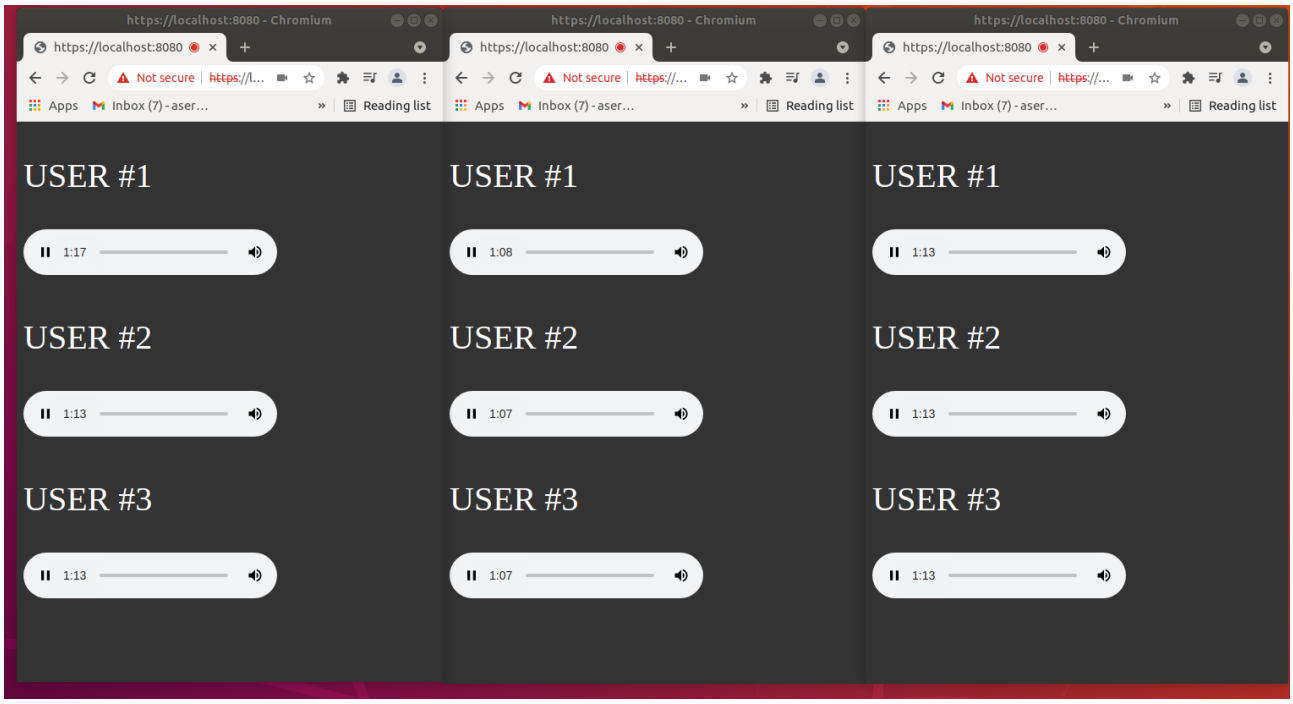

Рисунок 3.9 - Система для групових конференцій

3.2 Анонімізація шляхом використання VPN

На даний момент, сервісів VPN наявно у великій кількості, але не всі можуть подолати проблему витоку IP-адреси WebRTC; нижче наведено перелік VPN провайдерів, що мають цю функцію.

NordVPN [18], ExpressVPN [19], UnlimitedVPN [20]. Всі сервіси є платними для користування протягом тривалого часу, але VPNUnlimited має безкоштовний випробувальний період, яким ми і скористаємось для тестування.

Встановлюємо дану утіліту на ПК та запускаємо. Підключаємось до VPN серверу, та отримуємо іншу адресу. Результат на рисунку 3.10.

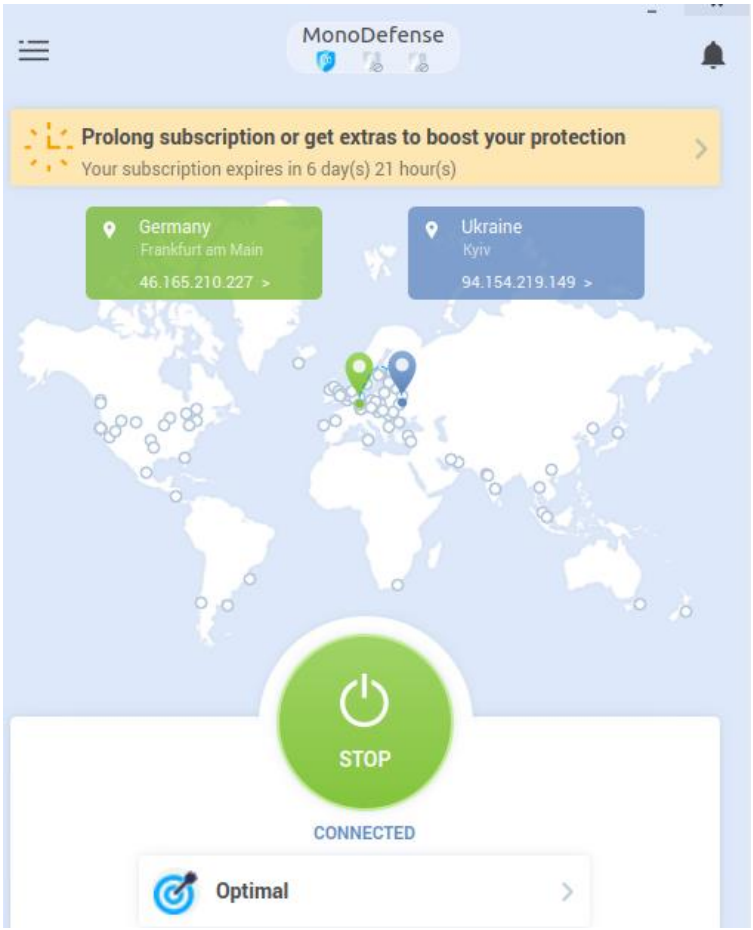

Рисунок 3.10 - Процес підключення до VPN

Для перевірки витоку IP-адреси, скористаємось веб-сайтом [21] для перевірки витоків. Результат наведено на рисунку 3.11.

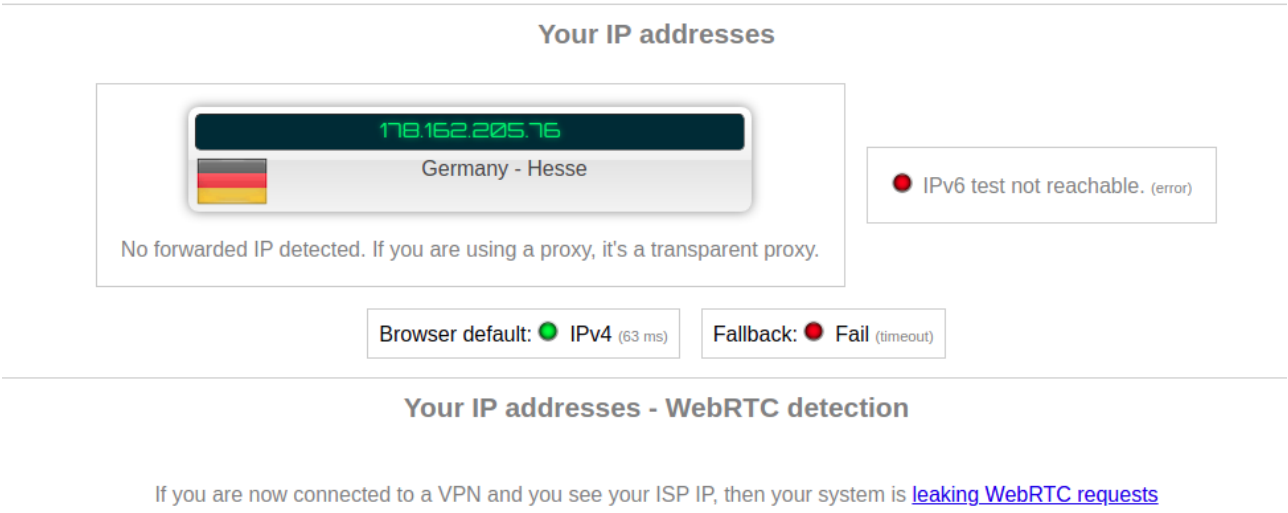

Рисунок 3.11 - Перевірка витоку IP-адреси

Як можемо побачити, наша справжня IP-адреса була прихована. Рахуємо, що даний метод попередження витоку IP-адреси є дієвим.

3.3 Анонімізація шляхом використання віртуальної машини

У якості віртуаілзатору, оберемо VMware [22], тому що дане програмне забезпечення має простий та легкий в розгортуванні інтерфейс.

Завантажимо образ операційної системи Ubuntu 18.04 та налаштуємо показаним на рисунку 3.12 чином.

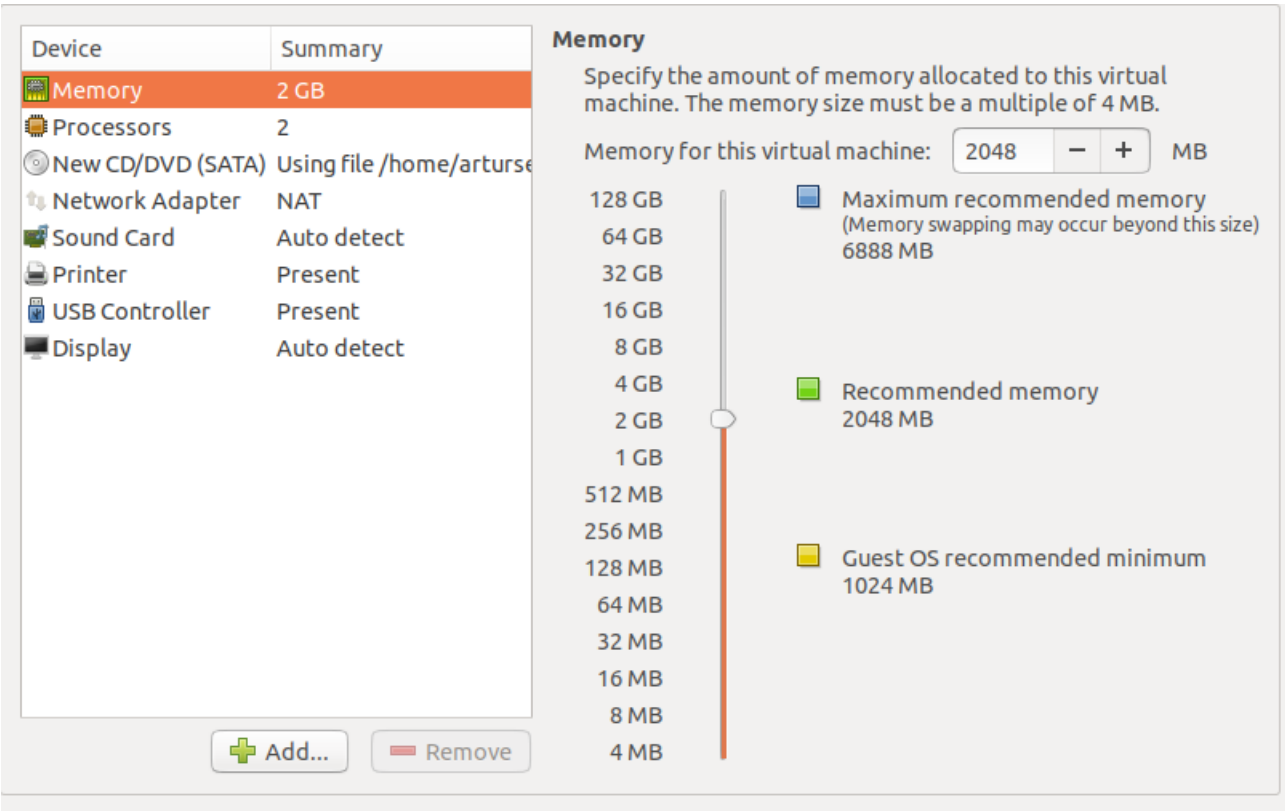

Рисунок 3.12 - Налаштування віртуальної машини

Обираємо тип мережевого адаптеру NAT. Встановлюємо образ та завантажуємось в систему.

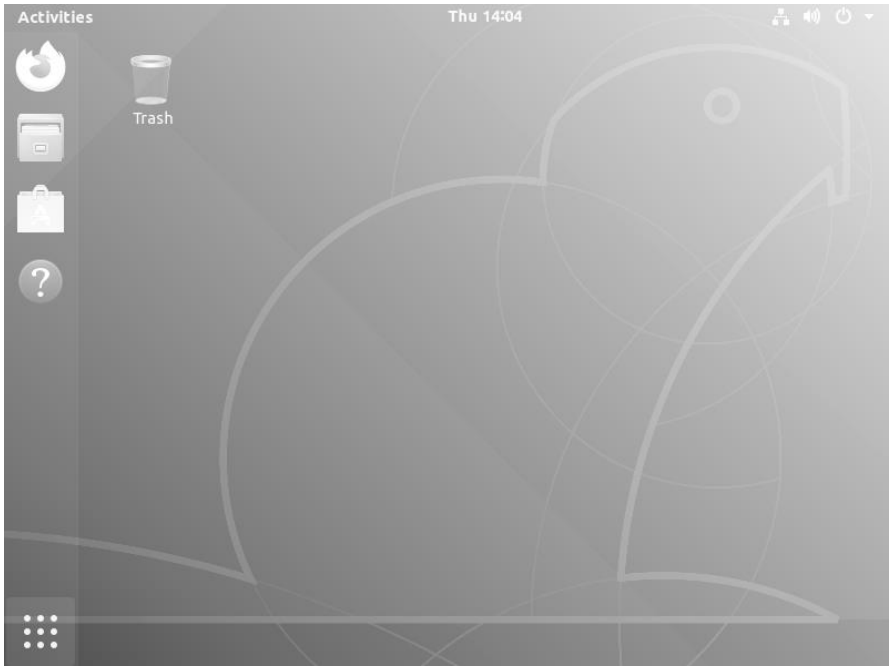

Рисунок 3.13 - Початковий екран віртуалізованої системи

Перевіряємо IP-адресу командою *ip a*. Результат команди можемо побачити на рисунку 3.14.

```
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 00:0c:29:62:4f:3b brd ff:ff:ff:ff:ff:ff
    inet 172.16.170.128/24 brd 172.16.170.255 scope global dynamic noprefixrout
e ens33
       valid_lft 1510sec preferred_lft 1510sec
    inet6 fe80::46c9:b9b:912c:d391/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Рисунок 3.14 - IP-адреса в операційній системі, що запускається під віртуальною машиною

Перевіримо, як відображається IP-адреса. Як можемо побачити з рисунку 3.15, IP-адресу не вдалось приховати, використовуючи віртуалізацію.

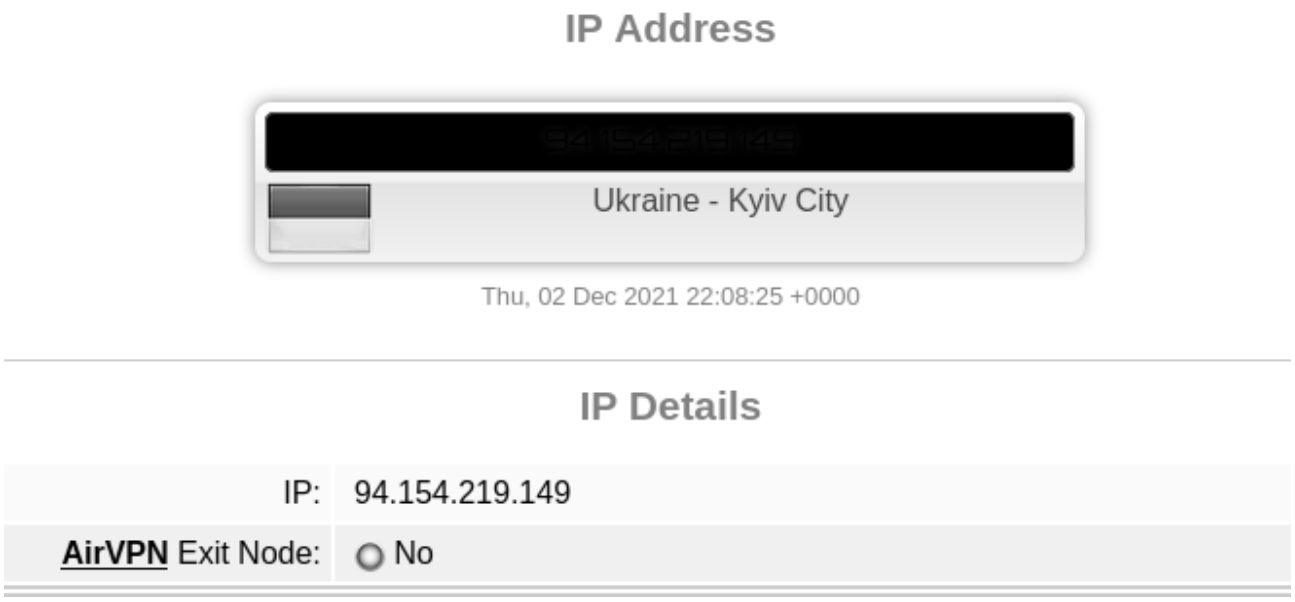

Рисунок 3.15 - Перевірка витоку IP-адреси через віртуальну машину.

3.4 Рекомендації та перспективи в розробці

Отримані результати можна використовувати для подальшої розробки системи анонімних групових конференцій. VPN сервіси показали себе дієвими для приховання IP-адреси, єдиним недоліком VPN є – ціна. Можливо розвивати цю задумку та інтегрувати VPN сервіс в систему групових конференцій, що зменшить кількість окремих елементів та створить монолітну систему. Також однією з проблем VPN є обмеження в швидкості підключення, але сучасні VPN провайдери надають прийнятний по швидкості трафік, тому можна вважати цю проблему несуттєвою.

Систему анонімних групових дзвінків також можна покращувати, наприклад введенням маскування голосу, що підвищить шанс залишитись не розкритим. Також графічна оболонка системи може змінюватись в кращу сторону.

Висновки до розділу 3

1. Розроблено та протестовано систему групових дзвінків на основі WebRTC. Оглянуто архітектурні складові системи. Описано серверну та клієнтську частину.

2. Надано послідовність дій для захисту від витоку IP-адрес за допомогою використання VPN сервісів. З’ясовано, що реальна IP-адреса не витікає при використанні VPN.

3. Перевірено метод віртуалізації для захисту від витоку IP-адреси. Цей метод не дав позитивних результатів, тому що мережеві пакети все одно проходять через хост систему, а хост система використовує напряму IP-адресу провайдера.

4. Надано рекомендації для подальшого розвитку системи. Оглянуто проблеми VPN.

РОЗДІЛ 4 РОЗРОБКА СТАРТАП ПРОЕКТУ

4.1. Опис ідеї проекту

Запропоновано використання системи, що має можливість підтримувати анонімність користувача у аудіо конференціях.

Далі послідовно проаналізовано та подано у вигляді таблиць: зміст ідеї; можливі напрямки застосування; основні переваги, які може отримати користувач товару та чим відрізняється від існуючих аналогів та замінників.

Таблиця 4.1 - Опис ідеї стартап-проекту

Зміст ідеї	*Напрямки застосування*	*Переваги для користувача*
	1. Збереження конфіденційності в аудіо конференціях.	Забезпечення конфіденційності користувача

Висновки: в табл. 4.1 наведено основні напрямки використання запропонованого рішення. Споживачами даної продукції можуть бути як компанії для застосування в телекомунікаційних системах, так і державні установи для побудови захищених систем.

Таблиця 4.2 - Визначення сильних, слабких та нейтральних характеристик

№ п/п	*Техніко-економічні характеристики ідеї*	*(потенційні) товари/концепції конкурентів*				*W*	*N*	*S*
		Мій проект	Конку-рент1	Конку-рент2	Конку-рент3			
1.	Собівартість	20	30	30	40			+

2.	Продуктивність	23250000	20000000	22000000	23000000			+
3.	Розмір	-	-	-	-	-		
4.	Інтерфейс зв’язку	Ethernet/Wi-Fi	Ethernet/Wi-Fi	Ethernet/Wi-Fi	Ethernet/Wi-Fi		+	
5.	Масштабованість	є	є	є	є		+	
6.	Споживання	1	1	1	0,8	-		

В табл. 4.2 W – слабка сторона, N – нейтральна сторона, S – сильна сторона. Під масштабованістю розуміється можливість зменшення розмірів системи в майбутньому.

Висновки: у порівнянні з конкурентами товар має перевагу у кращому відношенні ціна/продуктивність. Масштабованість притаманна усім системам. Система споживає стільки ж енергії, скільки і інші типові представники.

4.2. Технологічний аудит ідеї проекту

Таблиця 4.3 - Технологічна здійсненність ідеї проекту

№ п/п	*Ідея проекту*	*Технології її реалізації*	*Наявність технологій*	*Доступність технологій*
1.	Додавання можливості відео конференцій	Розширення системи шляхом написання додаткових функцій користування	Наявна	Доступна

		API WebRTC		
2.	Додавання зміни голосу для підвищення анонімності	Моделювання та написання драйверу маскування голосу	Наявна	Доступна
Обрана технологія реалізації ідеї проекту: за основу можна поєднати два пункти, і їх використання дозволить продукту більше виділятись на ринку відносно конкурентів.				

4.3. Аналіз ринкових можливостей запуску стартап-проекту

Таблиця 4.4 - Попередня характеристика потенційного ринку стартап-проекту

№ п/п	*Показники стану ринку (найменування)*	*Характеристика*
1.	Кількість головних гравців, од	10
2.	Загальний обсяг продаж, грн/ум.од	300
3.	Динаміка ринку (якісна оцінка)	зростає
4.	Наявність обмежень для входу (вказати характер обмежень)	немає
5.	Специфічні вимоги до стандартизації та сертифікації	відсутні

6.	Середня норма рентабельності в галузі (або по ринку), %	65%

Висновки: проаналізувавши табл. 4.4, можна зазначити, що вихід на ринок є рентабельним, через низьку варість, що дає змогу швидко покрити витрачені кошти на розробку системи.

Таблиця 4.5 - Характеристика потенційних клієнтів стартап-проекту

№ п/п	*Потреба, що формує ринок*	*Цільова аудиторія (цільові сегменти ринку)*	*Відмінності у поведінці різних потенційних цільових груп клієнтів*	*Вимоги споживачів до товару*
1.	Збільшення продуктивності та надійності сучасних телекомунікаційних мереж	Державний сектор, приватний сектор	Інтеграція з існуючими системами	Продуктивність, анонімність, висока надійність

Висновки: формування ринку визначається потребою збільшення продуктивності та надійності телекомунікаційних мереж. Основними споживачами продукту є усі сфери, які прагнуть збільшити автоматизацію процесів, що використовуються. Тому головними вимогами до товару є продуктивність та надійність роботи.

Таблиця 4.6 - Фактори загрози

№ п/п	*Фактор*	*Зміст загрози*	*Можлива реакція компанії*
1.	Економічний	Економічний стан країни-розробника	Зміна країни-розробника
2.	Конкуренція	Ім’я конкурентів є більше відомим на ринку	Проведення потужної рекламної кампанії
3.	Політичний	Політична ситуація країни-розробника	Зміна країни розробника

Висновки: основними факторами загрози є конкуренція та економічно-політичний стан країни виробника. Існуючі товари вже мають певне ім’я та репутацію. Також економічна та політична ситуація країни-розробника може зіграти значну роль у втраті прибутку.

Таблиця 4.7 - Фактори можливостей

№ п/п	*Фактор*	*Зміст можливості*	*Можлива реакція компанії*
1.	Збільшення попиту	Різке збільшення зацікавленості до продукту	Підвищення розробки нових функцій
2.	Новітні технології	Можливість покращити функції анонімності	Співпраця з іншими компаніями в даній сфері
3.	Розширення кругозору компанії	Можливість додавання нових систем до існуючої для пришвидшення розвитку	Відкриття нових спеціалізованих підрозділів компанії
4.	Індивідуальне замовлення	Можливість додавати індивідуальні потреби для клієнтів	Проведення аналізу раціональності замовлення та можливість укладання нового контракту із заданими потребами
5.	Кооперація із лідерами ринку	Конкуренти запропонували об’єднання компаній	Оцінка можливих переваг та ризиків об’єднання

Висновки: сфера ринку програмного забезпечення у галузі зв’язку наразі є досить популярною. Голосовий зв’язок потрібен усюди, що спричиняє зростання клієнтів на ринку, які в свою чергу збільшують попит на запропоновану систему в тому числі. Це приведе до збільшення кількості користувачів та заключення великої

кількості контрактів, що в свою чергу створює вигідні економічні можливості для дослідження нових технологій та покращення існуючої системи.

Таблиця 4.8 - Ступеневий аналіз конкуренції на ринку

Особливості конкурентного середовища	*В чому проявляється дана характеристика*	*Вплив на діяльність підприємства (можливі дії компанії, щоб бути конкурентоспроможною)*
Вказати тип конкуренції - чиста	Мала кількість постачальників даного товару	Розвивати систему збільшуючи її продуктивність та надійність
За рівнем конкурентної боротьби - міжнародний	Наявність замовників та виробників із інших держав	Вихід на міжнародний ринок
3. За галузевою ознакою - міжгалузева	Використання у різних галузях	Проведення потужної рекламної кампанії
4. Конкуренція за видами товарів – товарно-видова	Запропонований товар є одного виду	Орієнтація стратегії компанії на клієнта та адаптація до змін ринкових умов
5. За характеристиками конкурентних переваг - нецінова	Основним є якість та надійність товару	Проведення робіт щодо постійного покращення продукту
6. За інтенсивністю - марочна	Бренд грає велику роль в постачанні продукту	Проведення рекламної кампанії та доведення якості продукту

Висновки: ринок є конкурентним, проте вид конкуренції є чистим, так як окремі гравці мало впливають на ціну товару. Конкурентний ринок є міжнародним та міжгалузевим. Конкуренція за видами товарів – видова.

Таблиця 4.9 - Аналіз конкуренції в галузі за М. Портером

Складові аналізу	*Прямі конкуренти в галузі*	*Потенційні конкуренти*	*Постачальники*	*Клієнти*	*Товари-замінники*
	Google Metaverse Discord Jitsi BBB	Zoom	Аутсорсові компанії	Держ. та приватний сектори	-
Висновки:	Конкуренція є високою	Вихід на ринок є відносно простим. Наявні потенційні конкуренти	Постачальники не мають диктувати ціни на ринку	Клієнти можуть диктувати умови через присутність компаній з хорошою репутацією	Існують обмеження по використанню

Таблиця 4.10 - Обґрунтування факторів конкурентоспроможності

№ п/п	*Фактор конкурентоспроможності*	*Обґрунтування (наведення чинників, що роблять фактор для порівняння)*
1.	Собівартість	Низька собівартість – більша доступність кінцевого продукту

2.	Продуктивність	Вища продуктивність в порівнянні з конкурентами
3.	Анонімність	Наявні процеси для анонімізації користувачів

Висновки: Анонімізація є доволі сильною стороною системи. Також низька собівартість робить продукт більш конкурентоспроможною.

Таблиця 4.11 - Порівняльний аналіз сильних та слабких сторін проекту

№ п/п	*Фактор конкурентоспроможності*	*Бали 1-20*	*Рейтинг товарів-конкурентів у порівнянні з Google*						
			-3	*-2*	*-1*	*0*	*1*	*2*	*3*
1.	Собівартість	15							+3
2.	Продуктивність	20		-2					
3.	Надійність	19			-1				

Висновки: аналізуючи табл. 4.11 можна зробити висновок, що запропонована система має більший рейтинг відносно головного конкурента. Дана таблиця демонструє основні особливості продукту, які відрізняють його від основного конкурента.

Таблиця 4.12 - SWOT-аналіз стартап-проекту

Сильні сторона: Низька собівартість Анонімність	Слабкі сторони: Малий функціонал
Можливості: Вихід на міжнародний ринок Збільшення попиту	Загрози: Конкуренція Економічна нестабільність

	Політична нестабільність

Таблиця 4.13 - Альтернативи ринкового впровадження стартап-проекту

№ п/п	*Альтернатива (орієнтований комплекс заходів) ринкової поведінки*	*Ймовірність отримання ресурсів*	*Строки реалізації*
1.	Максимізація власного виграшу (індивідуалізм)	Середня	15 місяців
2.	Максимізація спільного виграшу (кооперація)	Середня	18 місяців
3.	Суперництво	Високі	24 місяці

Висновки: було обрано кооперацію як альтернативну ринкову поведінку, так як за відносно не високий термін існує велика ймовірність отримання ресурсів.

4.4. Розроблення ринкової стратегії проекту

Таблиця 4.14 - Вибір цільових груп потенційних споживачів

№ п/п	*Опис профілю цільової групи потенційних клієнтів*	*Готовність споживачів сприйняти продукт*	*Орієнтовний попит в межах цільової групи (сегменту)*	*Інтенсивність конкуренції в сегменті*	*Простота входу у сегмент*
1.	Державний сектор	-	+	висока	-
2.	Приватний сектор	+	+	висока	+
Які цільові групи обрано: основною характеристикою вибору цільової групи є готовність прийняти продукт. В даній області приватний сектор є					

більш готовим, адже державний сектор потребує більше дозволів та роз'яснень для введення нового продукту в системи.

Таблиця 4.15 - Визначення базової стратегії розвитку

№ п/п	*Обрана альтернатива розвитку проекту*	*Стратегія охоплення ринку*	*Ключові конкурентоспроможні позиції до обраної альтернативи*	*Базова стратегія розвитку*
1.	Індивідуалізм	Стратегія недиференційованого маркетингу	Адаптація до вимог ринку Використання новацій	Стратегія спеціалізації

Висновки: через існування на ринку більш сильних та розкручених гравців було обрано стратегію розвитку спеціалізація.

Таблиця 4.16 — Стартові умови проекту

№ п/п	*Чи є проект «першопрохідцем» на ринку?*	*Чи буде компанія шукати нових споживачів, або забирати існуючих у конкурентів?*	*Чи буде компанія копіювати основні характеристики товару конкурента, і які?*	*Стратегія конкурентної поведінки*
1.	Не є	Буде як шукати	Компанія не	Стратегія

	першопрохідцем на ринку	нових споживачів, так і забирати вже існуючих	буде копіювати основні характеристики конкурента	виклику лідера

Висновки: оскільки на ринку вже є проекти-конкуренти, компанія може обрати стратегію виклику лідера, так як проект має переваги. Також можлива колаборація з конкурентами для досягнення кращого успіху, адже система є новою та ще тільки вивчається та досліджується. Можливість об’єднати зусилля дає змогу в майбутньому краще засвоїти це направлення та створювати кращі системи.

Таблиця 4.17 - Визначення стратегії позиціонування

№ п/п	*Вимоги до товару цільової аудиторії*	*Базова стратегія розвитку*	*Ключові конкурентоспроможні позиції власного стартап-проекту*	*Вибір асоціацій, які мають сформувати комплексну позицію власного проекту (три ключових)*
1.	Продуктивність	Стратегія спеціалізації	Продуктивна	Висока швидкодія роботи
2.	Надійність	Стратегія спеціалізації	Якість	Висока надійність роботи

Висновки: як зазначалось раніше, збільшення продуктивності збільшує і надійність системи, що повинно викликати довіру до продукту у споживачів.

4.5. Розроблення маркетингової програми стартап-проекту

Таблиця 4.18 - Визначення ключових переваг концепції потенційного товару

№ п/п	*Потреба*	*Вигода, яку пропонує товар*	*Ключові переваги перед конкурентами (існуючі або такі, що потрібно створити)*
1.	Введення анонімізації в системах голосового зв’язку	Висока продуктивність та надійність	Ціна, продуктивність, надійність

Висновки: визначившись з основними перевагами концепції товару, можливе створення відповідної рекламної кампанії для кінцевих клієнтів.

Таблиця 4.19 - Опис трьох рівнів моделі товару

<table>
<tr><td>Рівні товару</td><td colspan="3">Сутність та складові</td></tr>
<tr><td>I. Товар за задумом</td><td colspan="3">Продукт дає змогу голосового зв’язку без втрати анонімності</td></tr>
<tr><td rowspan="4">II. Товар у реальному виконанні</td><td>Властивості/характеристики
Безпека

Вартість</td><td>М/Нм
100
10
</td><td>Вр/Тх /Тл/Е/Ор
Тх

Тх</td></tr>
<tr><td colspan="3">Якість: програмне забезпечення з усіма рівнями тестів</td></tr>
<tr><td colspan="3">Пакування: відсутнє</td></tr>
<tr><td colspan="3">Марка: назва організації-розробника – RT4K Development, назва товару – AnonAudio (AA)</td></tr>
<tr><td rowspan="2">III. Товар із підкріпленням</td><td colspan="3">До продажу – допомога в налаштуванні.</td></tr>
<tr><td colspan="3">Після продажу – технічна підтримка.</td></tr>
<tr><td colspan="4">Шифрування зібраного вихідного коду</td></tr>
</table>

Висновки: шляхом шифрування вихідного коду створюється захист від його копіювання. Також закладені характеристики на другому рівні товару роблять його досить унікальним та конкурентоспроможним.

Таблиця 4.20 - Визначення меж встановлення ціни

№ п/п	*Рівень цін на товари замінники*	*Рівень цін на товари-аналоги*	*Рівень доходів цільової групи споживачів*	*Верхня та нижня межі встановлення ціни на товар/послугу*
1.	4-10 у.о	20-30 у.о	500-5000 у.о.	3-20 у.о.

Висновки: обрано низьку категорію цін, адже занадто велика ціна відлякує споживачів.

Таблиця 4.21 - Формування системи збуту

№ п/п	*Специфіка закупівельної поведінки цільових клієнтів*	*Функції збуту, які має виконувати постачальник товару*	*Глибина каналу збуту*	*Оптимальна система збуту*
1.	Продаж	Повний супровід товару до замовника	Нульового рівня	Безпосередній (прямий)

Висновки: основним каналом збуту є продаж продукту. На старті компанії очікуються відносно невеликі об’єми виробництва, тому на даному етапі можливо обійтись без посередників і продавати товар напряму клієнтам. Саме тому було обрано нульовий рівень глибини каналу збуту та пряму систему збуту.

Таблиця 4.22 - Концепція маркетингових комунікацій

№ п/п	*Специфіка поведінки цільових клієнтів*	*Канали комуні-кацій, якими користуються цільові клієнти*	*Ключові позиції, обрані для позиціону-вання*	*Завдання рекламного повідомлення*	*Концепція рекламного звернення*
1.	Розвиток технологій спонукає споживача до оновлення власних використо-вуваних систем	Реклама SMM Відео-інструкції по використанню товару на ресурсі tiktok, telegram	Висока продукти-вність та надійність Легкість у встановленні та використанні	Донести реальність продукту та ефективність продукту.	Демон-страція можли-востей даної системи та принцип її викори-стання

Висновки: маркетингова кампанія відбувається за рахунок соціальних мереж та цільових рекламних кампаніях. Метою даних оголошень є донести усі перспективи та можливості даної системи для користувача.

4.6. Можливі області застосування та очікуваний ефект

Даний проект буде застосовуватись на базі приватного підприємства, та довіреного кола осіб, що виконують розробку та підтримку.

Позитивний економічний ефект досягається за рахунок меншої собівартості системи в порівнянні з конкурентами.

Висновки до розділу 4

1. Розроблено перший етап створення стартап-проекту. Оскільки кожна наукова робота повинна знаходити своє місце в застосуванні у реальному житті, тому стартап-проект може бути практичним відображенням наукової праці.

2. Висвітлено зміст ідеї проекту шляхом розгляду потенційних зацікавлених осіб, які в майбутньому можуть стати клієнтами запропонованої продукції. Також розглянуто ризики реалізації продукції, а проведений аналіз сильних та слабких сторін надав можливість визначити аспекти, на які слід зробити ставку.

3. Проведено технічний аудит проекту та визначено технології, які використовуватимуться. Запропоновані технології вже існують, проте їх використання не дає можливість переваги над конкурентом.

4. Проведено аналіз усіх аспектів ринку, який показав, що імплементація проекту можлива в реальних умовах, проте слід враховувати, що на ринку уже існують гравці з досить високою репутацією, що може зіграти негативну роль у впровадженні проекту. Для уникнення провалу проекту необхідно провести потужну рекламну кампанію, в якій донести до споживача усі переваги даного проекту та необхідність обрати саме запропонований продукт.

ВИСНОВКИ

В дисертаційній роботі вирішено актуальну науково-прикладну задачу анонімізації користувачів в групових аудіо конференціях шляхом використання методів порівняльної і описової характеристик, теоретичного аналізу та синтезу, методів теорії комп'ютерних мереж та програмування.

Під час дослідження отримано наступні науково-практичні результати:

1. Проведено аналіз сучасного стану VoIP-мереж: напрямок "гаджет-гаджет" є найперспективнішим. Проаналізовано найпоширеніші архітектури VoIP-мереж, визначено області застосування протоколів. Визначено основні проблеми VoIP-мереж, виділено найбільш суттєві. Проведено патентний пошук, визначено переваги та недоліки патентних виробів. Обгрунтовано вибір архітектури WebRTC, сконцентровано дослідження на найбільш суттєвих проблемах технології.

2. Описано складові архітектури WebRTC, визначено вектори вразливостей технології, з'ясовано, що проблеми безпеки є суттєвими через велику кількість векторів атак. Розглянуто спосіб ідентифікації користувачів, проблему підміни користувача через сервер ідентифікації. Проаналізовано проблеми витоку IP-адрес, з'ясовано причини та які IP-адреси під загрозою розкриття. Розібрано проблему створення групових конференцій, встановлено методи вирішення проблеми. Виконано огляд двох методів анонімізації користувачів: VPN та віртуалізація.

3. Розроблено та протестовано систему групових дзвінків. Описано серверну та клієнтську частини. Надано послідовність дій для захисту від витоку IP-адрес. Виявлено неефективність методу віртуалізації для захисту від витоку IP-адреси. Неефективність обумовлена тим, що мережеві пакети в кінцевому випадку проходять через хост систему. Надано рекомендації для подальшого розвитку системи. Розглянуто проблеми VPN.

4. Розроблено перший етап створення стартап проекту. Висвітлено зміст ідеї проекту, шляхом розгляду потенційних зацікавлених осіб, які в майбутньому можуть стати клієнтами запропонованої продукції. Проведено технічний аудит проекту і

визначено технології, що будуть використовуватись. Проведено аналіз усіх аспектів ринку, який показав, що імплементація проекту можлива в реальних умовах, проте слід враховувати, що на ринку уже існують гравці з досить високою репутацією, що може зіграти негативну роль у впровадженні проекту.

Таким чином, можна стверджувати, що основні завдання роботи виконані, а мета магістерської дисертації досягнута.

Отримані результати можна використовувати при подальшому розробленні програмного забезпечення групових конференцій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Voice over Internet Protocol (VoIP) Technology / [Електронний ресурс] – Режим доступу до ресурсу: https://ukdiss.com/examples/voice-over-internet-protocol.php
2. What is WebRTC and how does it work ? / [Електронний ресурс] - Режим доступу до ресурсу: https://bit.ly/3yWnKuL
3. WebRTC-based architecture with a quasi-peer / [Електронний ресурс] – Режим доступу до ресурсу : https://www.researchgate.net/figure/WebRTC-based-architecture-with-a-quasi-peer_fig3_3404199216
4. Voice over Internet Protocol (VOIP): Overview, Direction And Challenges ISSN 2224-5782 (print) ISSN 2225-0506 (online) Vol.3, No.4, 2013
5. Audio and Video Mixing Method to Enhance WebRTC. / [Електронний ресурс] - Режим доступу до ресурсу: https://www.researchgate.net/publication 340419921_Audio_and_Video_Mixing_Method_to_Enhance_WebRTC
6. ICE and WebRTC: What Is This Sorcery? We Explain / [Електронний ресурс] – Режим доступу до ресурсу: https://temasys.io/ice-and-webrtc-what-is-this-sorcery-we-explain/
7. Real-Time Communication with WebRTC / [Електронний ресурс] – Режим доступу до ресурсу: http://subnets.ru/books/real-time-communication-with-webrtc-peer-to-peer-in-the-browser.pdf
8. L. Desmet and M. Johns, “Real-time communications security on the web,” Internet Computing, IEEE, vol. 18, no. 6, pp. 8–10, 2014
9. V. Beltran, E. Bertin, and N. Crespi, “User identity for WebRTC services: A matter of trust,” IEEE Internet Computing, no. 6, pp. 18–25, 2014.
10. R. Barnes and M. Thomson, “Browser-to-browser security assurances for WebRTC,” 2014.

11. Peer-to-peer communication in web browsers using WebRTC / [Електронний ресурс] - Режим доступу : http://www8.cs.umu.se/education/examina/Rapporter/ChristerJakobsson.pdf
12. One Leak Will Sink A Ship: WebRTC IP Address Leaks / [Електронний ресурс] - Режим доступу: https://arxiv.org/pdf/1709.05395.pdf
13. Building a Peer to Peer Group Chat using Deno and Webrtc. / [Електронний ресурс] - Режим доступу: https://nighthour.sg/articles/2020/building-a-peer-to-peer-groupchat-using-deno-and-webrtc.html
14. Що таке VPN-підключення і як працює VPN? / [Електронний ресурс] - Режим доступу: https://samoosvita.in.ua/scho-take-vpn-pidklyuchennya-i-yak-pratsyue-vpn/
15. Основи віртуальних машин та їх потенційні проблеми з втратою даних / [Електронний ресурс] - Режим доступу: https://www.ufsexplorer.com/uk/articles/storage-technologies/virtual-machines-data-organization.php
16. Two ways a VM can break out to the internet. / [Електронний ресурс] - Режим доступу: https://www.quora.com/Does-the-virtual-machine-use-the-port-of-the-host-machine-to-connect-to-the-internet-directly-or-would-it-connect-to-somewhere-on-the-host-machine-first-i-e-indirectly-and-then-go-to-the-port-of-host-machine-and
17. WebRTC group chat example. / [Електронний ресурс] - Режим доступу : https://github.com/anoek/webrtc-group-chat-example
18. NordVPN. / [Електронний ресурс] Режим доступу : https://nordvpn.com/
19. ExpressVPN. / [Електронний ресурс] Режим доступу : https://www.expressvpn.com/webrtc-leak-test
20. VPNUnlimited. / [Електронний ресурс] Режим доступу: https://www.vpnunlimited.com/
21. IP leak test. / [Електронний ресурс] Режим доступу: https://ipleak.net/
22. VMWare . / [Електронний ресурс] Режим доступу : https://www.vmware.com/products/workstation-player.html

ДОДАТОК А

Сергієнко А.В.,
студент,
Бондаренко В.М.,
к.т.н., доцент,

Національний технічний університет України
"Київський політехнічний інститут ім. Ігоря Сікорського"

ТЕХНОЛОГІЇ ГОЛОСОВОГО ТА ВІДЕО ЗВ'ЯЗКУ В IP-МЕРЕЖАХ

Актуальність. На сьогодні IP-телефонія є досить перспективною складовою телекомунікацій, оскільки надає вигідну альтернативу класичній телефонії.

IP-телефонія є частиною технології VoIP – Voice over Internet Protocol [1], яка поєднує в собі останні досягнення в областях цифрової обробки сигналів (DSP), аудіокодування,

мережних технологій для передачі голосу через інформаційні мережі з мінімальними спотвореннями та втратами. В зв'язку з цим, для голосового трафіку висуваються найвищі пріоритети передачі та обслуговування.

Тема VoIP є актуальною на сьогодні. Все більше і більше людей користується перевагами швидкого інтернету. Комунікація з колегами, друзями, рідними відбувається методом створення аудіо та відео конференцій у відомих застосунках: Google Meets, Zoom, Discord, Telegram тощо. Для проведення конференцій не потрібне додаткове обладнання, лише гаджет (персональний комп`ютер, смартфон) зі стабільним підключенням до інтернету.

Метою дослідження є вибір технології, що не потребує додаткового апаратного забезпечення для проведення групових конференцій.

Порівняльний аналіз. Системи IP-телефонії базуються на протоколах, які забезпечують реєстрацію IP-пристрою (шлюз, термінал або IP-телефон) на гейткіпері провайдера, виклик або переадресацію виклику, встановлення голосового з'єднання. На сьогодні найпоширеніші протоколи VoIP наступні:

- SIP – забезпечує передачу голосу; для сигналізації зазвичай використовує порт 5060 UDP;
- H.323 – протокол, більш прив'язаний до систем традиційної телефонії, ніж SIP; сигналізація – через порт 1720 TCP;
- MGCP;

складного додаткового апаратного забезпечення, такого як гейткіпери та додаткові проксі-сервери, простота розгортання, відкрите програмне забезпечення. Також неабиякою перевагою є наявність підтримки досить великого ком'юніті розробників на платформі github, постійні оновлення програмного забезпечення, додавання нових функцій.

На даний момент все більше і більше компаній переводить своїх співробітників на віддалений режим роботи. Якщо компанія використовувала VoIP мережу на основі протоколів H.323, MGCP, SIP тощо, то їй потрібно підключати кожного віддаленого співробітника до мережі та виділяти фінанси на додаткове апаратне забезпечення. Але в реаліях сьогодення, компанії використовують програмне забезпечення на основі WebRTC, що дозволяє без додаткових витрат зберегти комунікацію поміж колективом.

Недоліки технології WebRTC:

- технологія лише визначає загальний стандарт передачі даних, адресація абонентів на різних браузерах виконана по-різному, тому навіть дзвінки між різними браузерами спричиняють складність;
- не реалізована можливість створення групових конференцій;
- ще знаходиться у розробці;
- кросплатформеність технології, але не застосунків на її основі;
- відсутність анонімності при використанні даної технології, оскільки вона визначає реальну IP-адресу.

Зважаючи на вищезазначену основну перевагу технології WebRTC, варто зосередитись на дослідженні можливості створення групових конференцій з забезпеченням анонімності при використанні технології (WebRTC Leak) [3].

Висновок. Проведено аналіз сучасних технологій голосового та відео зв'язку. З'ясовано, що в реаліях сьогодення технології, що потребують додаткового апаратного забезпечення, відійшли на другий план. Для голосового та відео зв'язку потрібен лише стабільний інтернет та відповідний гаджет. Застосунки, що використовують WebRTC, задовольняють потреби користувачів, але їх практичне впровадження потребує додаткових досліджень.

Література:

1. Voice over Internet Protocol (VOIP): Overview, Direction And Challenges ISSN 2224-5782 (print) ISSN 2225-0506 (online) Vol.3, No.4, 2013
2. What is WebRTC and how does it work ? URL: https://bit.ly/3yWnKuL
3. WebRTC Leak. URL : https://ieeexplore.ieee.org/abstract/document/8167801

- WebRTC.

Мережі, що будуються на базі протоколів H.323, орієнтовані на інтеграцію з телефонними мережами і розглядаються як надбудова над мережами ISDN. Процедура встановлення з'єднання в таких мережах базується на ITU Q.931. Даний варіант мережі традиційно використовується операторами телефонного зв'язку, що надають послуги міжміського та міжнародного зв'язку.

SIP (Session Initiation Protocol), орієнтований на інтеграцію з мережею Internet, з подальшою передачею голосового трафіку по IP-мережі. Даний протокол вважається простішим за H.323, але зазвичай не використовується для організації взаємодії з телефонними мережами. Це пов'язано з тим, що архітектура серверу SIP побудована таким чином, що він не зберігає інформацію про поточні з'єднання, в свою чергу вузли ТМЗК зберігають дану інформацію.

MGCP, пов'язаний з декомпозицією шлюзів, пропонує розбиття шлюзів на функціональні блоки: шлюз – MG (Media Gateway), пристрій управління шлюзом – CA (Call Agent) і сигнальний шлюз – SG (Signalling Gateway). Шлюзи виконують функцію перетворення голосової інформації з головної телефонної мережі у вигляд придатний для передачі даних по мережах. Контролер шлюзів CA виконує керування іншими шлюзами одночасно. Сигнальний шлюз виконує функції STP транзитного пункту сигналізації.

WebRTC – протокол, що лежить в основі багатьох популярних платформ для передачі аудіо-відео даних. Проекти, що побудовані на основі даного протоколу: BigBlueButton, Google Meet, Jitsi Meet, Discord [2].

Технологія WebRTC є проектом з відкритим кодом, що призначена для організації передачі потокових даних між браузерами, або іншими застосунками, що підтримують з'єднання точка-точка (peer-to-peer).

У якості транспорту IP-пакетів, виступає RTP. STUN/ICE – механізми, що допомагають встановити з'єднання поміж різних типів мереж.

Серед наведених існуючих VoIP архітектур, фаворитом у сучасному світі є архітектура побудована на протоколі WebRTC. На сьогоднішній день створюється все більше і більше застосунків для гаджетів на основі WebRTC. Даний протокол є доволі новим та технічно прогресивнішим, порівняно з SIP та H.323.

У першу чергу, основною перевагою над протоколами SIP, MGCP та H.323 є відсутність

ДОДАТОК Б

Міжнародний Центр Науки і Досліджень

International Center for Science and Research

Международный Центр Науки и Исследований

СЕРТИФІКАТ

Даний сертифікат підтверджує, що

Сергієнко А.В. та Бондаренко В.М.

брали участь у роботі

VI Міжнародній науково-практичній конференції "Перспективи розвитку сучасної науки"

Оргкомітет конференції
30-31 жовтня 2021 року