Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістра

студента *Ярощука Олексія Романовича*

академічної групи *125м-20-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Забезпечення конфіденційності зв'язку за технологією VoIP*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	к.т.н., доц. Герасіна О.В.			
розділів:				
спеціальний	ас. Мілінчук Ю.А			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2022

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту *Ярощуку Олексію Романовичу* **академічної групи** *125м-20-2*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему *Забезпечення конфіденційності зв'язку за технологією VoIP*

затверджену наказом ректора НТУ «Дніпровська політехніка» від 10.12.2021 № 1036-с

Розділ	Зміст	Термін виконання
Розділ 1	Дослідження технології VoIP, аналіз її проблем та загроз. Аналіз підходів щодо забезпечення захищеності VoIP.	18.11.2021
Розділ 2	Забезпечення безпеки спілкування через Skype, та інших VoIP клієнтів.	07.12.2021
Розділ 3	Розрахунок економічної доцільності запровадження запропонованого способу забезпечення безпеки VoIP у компанію.	04.01.2022

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)

Дата видачі:

Дата подання до екзаменаційної комісії: 26.01.2022

Прийнято до виконання _____ _____
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 98 с., 31 рис., 7 табл., 6 додатків, 18 джерел.

Об'єктом дослідження є результати аналізу проблем та загроз VoIP.

Мета роботи - дослідження результатів аналізу проблем та загроз VoIP, аналіз підходів щодо забезпечення захищеності VoIP та розробка засобів, спрямованих на досягнення безпечної передачі голосу за допомогою VoIP.

Методом роботи було забезпечення безпечної взаємодії в рамках Skype, а саме використання кінцевого шифрування під час передачі голосу та повідомлень. Розроблено програмний засіб, що реалізує зазначений підхід, та підтримує весь необхідний для безпечної взаємодії функціонал, а саме: встановлення сеансового ключа за класичним протоколом Діффі-Хеллмана із заданим абонентом; надсилання та прийом зашифрованих повідомлень заданому абоненту, та їх розшифрування; встановлення сеансового ключа під час здійснення виклику; зашифрування вихідного аудіосигналу; розшифрування вхідного аудіосигналу.

Також створено засіб, що забезпечує безпечне спілкування не лише за допомогою Skype, а й будь-якого іншого VoIP-клієнта. Для його створення було використано віртуальний аудіопристрій та реалізовані наступні функції: обмін звуковими потоками між вхідним та вихідним інтерфейсами, тобто між динаміком та мікрофоном; зашифрування або розшифрування сигналу під час обміну потоками між вхідним та вихідним інтерфейсами аудіопристрою.

Практичне застосування результатів даної роботи може бути використано для безпечної взаємодії за допомогою VoIP, а саме за допомогою віртуального аудіопристрою, що реалізує кінцеве шифрування переданого голосового трафіку, для використання якого достатньо вибрати його як вхідний або вихідний аудіоінтерфейс.

VoIP, АНАЛІЗ ПРОБЛЕМ І ЗАГРОЗ, ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ, ШИФРУВАННЯ, ІНФОРМАЦІЯ, ПОВІДОМЛЕННЯ.

РЕФЕРАТ

Пояснительная записка: 98 стр., 31 рис., 7 табл., 6 приложений, 18 источников.

Объектом исследования являются результаты анализа проблем и угроз VoIP.

Цель работы – исследование результатов анализа проблем и угроз VoIP, анализ подходов по обеспечению защищенности VoIP и разработка средств, направленных на достижение безопасной передачи голоса посредством VoIP.

Методом работы было обеспечение безопасного взаимодействия в рамках Skype, а именно использование оконечного шифрования при передаче голоса и сообщений. Разработано программное средство, реализующее указанный подход, и, поддерживающее весь необходимый для безопасного взаимодействия функционал, а именно: установка сеансового ключа по классическому протоколу Диффи-Хеллмана с заданным абонентом; отправка и прием зашифрованных сообщений заданному абоненту, и их расшифрование; установка сеансового ключа в момент совершения вызова; зашифрование исходящего аудиосигнала; расшифрование входящего аудиосигнала.

Также создано средство, обеспечивающее безопасное общение не только посредством Skype, но и любого другого VoIP-клиента. Для его создания было использовано виртуальное аудиоустройство и реализованы следующие функции: обмен звуковыми потоками между входящим и исходящим интерфейсами, т.е. между динамиком и микрофоном; зашифрование или расшифрование сигнала во время обмена потоками между входным и выходным интерфейсами аудиоустройства.

Практическое применение результатов данной работы может быть использовано для безопасного взаимодействия посредством VoIP с помощью виртуального аудиоустройства, реализующего оконечное шифрование передаваемого голосового трафика, для использование которого достаточно выбрать его в качестве входного или выходного аудиоинтерфейса.

VoIP, АНАЛИЗ ПРОБЛЕМ И УГРОЗ, ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ, ШИФРОВАНИЕ, ИНФОРМАЦИЯ, СООБЩЕНИЯ.

ABSTRACT

Explanatory note: 98 p., 31 fig., 7 tab., 6 additions, 18 sources.

The object of the research is the results of the analysis of VoIP problems and threats.

The purpose of work is to study the results of the analysis of VoIP problems and threats, analyze approaches to ensuring the security of VoIP and develop tools aimed at achieving secure voice transmission over VoIP.

The method of work was to ensure secure communication within Skype, specifically the use of end-to-end encryption in the transmission of voice and messages. A software tool has been developed that implements this approach and supports all the functionality necessary for safe interaction, specifically: installation of a session key according to the classical Diffie-Hellman protocol with a given subscriber; sending and receiving encrypted messages to a given subscriber, and their decryption; setting the session key at the time of the call; encryption of outgoing audio signal; decryption of the incoming audio signal.

The possibility of creating a tool that provides secure communication not only via Skype, but also any other VoIP client. To create it, a virtual audio device was used and the following functions were implemented: exchange of audio streams between incoming and outgoing interfaces, that is between speaker and microphone; encryption or decryption of the signal during the exchange of streams between the input and output interfaces of the audio device.

The practical application of the results of this thesis can be used for secure interaction via VoIP using a virtual audio device that implements end-to-end encryption of transmitted voice traffic, for which it is enough to select it as an input or output audio interface.

VoIP, PROBLEM AND THREAT ANALYSIS, PRIVACY PROVISION, ENCRYPTION, INFORMATION, MESSAGES, VOICE.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ACL - Access Control List - Перелік контролю доступу;

AES – Advanced Encryption Standard – Розширений стандарт шифрування;

API – Application programming interface – Інтерфейс програмування програм;

CPU – Central processing unit – Центральний процесор;

DDoS – Distributed Denial Of Service – розподілена відмова в обслуговуванні;

DES – Data encryption standard – Стандарт шифрування даних;

DHCP – Dynamic Host Configuration Protocol – Протокол динамічного налаштування вузла;

DLP – Data Leak Prevention – Запобігання витоку інформації;

DoS – Denial of Service – Відмова в обслуговуванні;

IP – Internet Protocol – Мережевий протокол;

IPSec – IP Security – Безпека мережного протоколу;

MAC – Media Access Control – Управління доступом до середовища;

P2P – Peer-to-peer – З'єднання рівний до рівного;

PRISM – Program for Robotics, Intelligents Sensing and Mechatronics – Програма робототехніки та технічної розвідувальної діяльності;

SIP – Session Initiation Protocol – Протокол встановлення сеансу;

SMS – Short Message Service – Служба коротких повідомлень;

SPIT – Spam over IP telephony – Спам з IP-телефонії;

SSH – Secure Shell – Безпечна оболонка;

SSL – Secure sockets layer – Рівень захищених сокетів;

SYN – Synchronize sequence numbers – Синхронізація номерів послідовності;

TCP – Transmission Control Protocol – Протокол управління передачею;

TFTP – Trivial File Transfer Protocol – Простий протокол передачі файлів;

Vishing – VoIP-phishing – Фішинг з VoIP;

VLAN – Virtual Local Area Network – Віртуальна локальна комп'ютерна мережа;

VoIP – Voice over IP - Голос по мережному протоколу;

VOIPSA – VoIP Security Alliance – Безпекове об'єднання VoIP;

VoWLAN – Voice over WLAN – Голос по бездротовій локальній мережі;

WDK – Windows Driver Kit – Засоби розробки драйверів Windows;

ВКЗ - Відеоконференцзв'язок;

ВОДВ - Виконавчі органи державної влади;

ДСТУ – Державний стандарт України;

ЄМТМ - Єдина мультисервісна телекомунікаційна мережа;

КД - Керівний документ;

МЕ – Міжмережевий екран;

ММ – Міська мережа;

ОЗП - Оперативне запам'ятовуючий пристрій;

ОС – операційна система;

ПЗ – Програмне забезпечення;

ТФзК – Телефонна мережа загального користування;

ЗМІСТ

с.

ВСТУП

Інформаційні технології є невід'ємною частиною сучасного життя і використовуються для вирішення багатьох завдань, наприклад забезпечення віддаленого спілкування абонентів.

Йдеться спілкування з допомогою IP-телефонії (VoIP).

На початкових етапах ця технологія використовувалася в основному для спілкування звичайних абонентів по всьому світу і на сьогоднішній день спілкування користувачів за допомогою VoIP обчислюється сотнями мільярдів хвилин.

Згодом всі переваги використання IP-телефонії оцінили й інші учасники ринку.

В наш час програмні клієнти, що забезпечують спілкування за допомогою IP-телефонії, використовуються не тільки на побутовому, але й на корпоративному рівні. VoIP є повноцінним інструментом ведення бізнесу нарівні зі стільниковим зв'язком, електронною поштою тощо.

Це можна пояснити багатьма факторами:

1. Висока якість передачі голосу.

2. Можливість передачі не лише голосу, а й відео в режимі реального часу.

3. Можливість обміну миттєвими текстовими повідомленнями.

4. Можливість організації відеоконференцій.

З цих причин VoIP сьогодні також використовується на державному рівні.

Забезпечення взаємодії органів державної влади за допомогою відеоконференцзв'язку є одним із пріоритетних та стратегічних завдань з інформатизації міста та країни.

Однак таке широке поширення VoIP спричинило низку проблем, найзначніші з яких пов'язані з інформаційною безпекою.

У зв'язку з тим, що часто за допомогою IP-телефонії передаються важливі дані корпоративного та державного характеру, забезпечення їх конфіденційності, цілісності та доступності має бути на найвищому рівні.

Це зобов'язує фахівців з інформаційної безпеки в Україні та світі щільно займатися такими питаннями:

1. Аналіз загроз VoIP.

2. Аналіз безпеки взаємодії за допомогою VoIP.

3. Вироблення методик та засобів, спрямованих на забезпечення безпечного спілкування з VoIP.

Ця робота є відображенням потреби сучасного суспільства в безпечному спілкуванні за допомогою IP-телефонії та відповідає викликам сьогодення з боку вороже настроєних країн та організацій.

Об'єктом дослідження дипломної роботи є програмне забезпечення “Skype” та VoIP загалом.

Предметом дослідження є конфіденційність спілкування. Метою дипломної роботи є:

- аналіз проблем та загроз VoIP;

- аналіз підходів щодо забезпечення захищеності VoIP;

- розробка засобів, спрямованих на досягнення безпечної передачі голосу за допомогою VoIP.

У дипломній роботі для досягнення поставлених цілей використовувалися такі методи, як:

- моделювання;

- аналізу літератури;

- вивчення і узагальнення вітчизняної і зарубіжної практики;

- індукція і дедукція;

- абстрагування;

- конкретизація і ідеалізація;

- аналогія;

- класифікація;

- узагальнення;

- теоретичний аналіз і синтез;

- порівняння.

Введення розкриває актуальність, визначає ступінь наукової розробки теми, об'єкт, предмет, мета, завдання та методи дослідження.

У першому розділі надаються основні відомості про проблеми та загрози VoIP, проблеми безпеки протоколу Skype, класифікація загроз, аналіз підходів щодо забезпечення захищеності та постановка задачі.

Другий розділ присвячено забезпеченню захищеності VoIP, забезпеченню безпечної передачі даних у Skype та забезпеченню захищеності голосового трафіку у VoIP і висновкам.

У третьому розділі йдеться мова про економічну складову дипломної роботи.

У висновку підводяться підсумки дослідження, формуються остаточні висновки по даній темі.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Технологія передавання голосової інформації з використанням протоколу IP – Voice over IP (VoIP)

Voice over Internet Protocol - це метод для прийому аналогових аудіо сигналів, подібно до того, що ви чуєте під час розмови по телефону, і перетворення їх у цифрові, які передаються через Інтернет.

Чим це корисно? VoIP перетворює звичайне інтернет-з'єднання на спосіб розміщення безкоштовних телефонних дзвінків. В результаті, завдяки використанню деякого безкоштовного програмного забезпечення VoIP, яке доступне для телефонних дзвінків в Інтернеті, ви повністю позбавляєтеся витрат на дзвінки через телефонну мережу.

VoIP – це революційна технологія, яка може повністю переробити телефонні системи у світі. Постачальники обладнання VoIP, такі як GrandStream, вже давно існують і постійно зростають. Великі оператори вже створюють тарифні плани на ринках по всій території США, Європи, Азії та FCC серйозно розглядає потенційні наслідки обслуговування VoIP.

В даний час існує три різні особливості VoIP-сервісу:

- ATA (аналоговий телефонний адаптер) або шлюз - це найпростіший і найпоширеніший спосіб. ATA дозволяє підключати стандартний телефон до комп'ютера або інтернет-з'єднання для використання з VoIP. Адаптер є аналого-цифровим перетворювачем. Він приймає аналоговий сигнал від вашого традиційного телефону і перетворює його на цифрові дані для передачі через Інтернет. Більшість провайдерів пов'язують ATA із своїм сервісом. Тому для підключення ви просто дістаєте адаптер із коробки, підключаєте кабель від телефону, який зазвичай входить комплект, і ви готові здійснювати VoIP-дзвінки. Деякі телефонні адаптери можуть мати додаткове програмне забезпечення, яке завантажується на комп'ютер для його налаштування.

- IP-телефони – це спеціалізовані телефони, які використовують технології передачі голосу по IP для розміщення та передачі телефонних дзвінків через

Інтернет. На вигляд вони такі самі, як і звичайні телефони: мають телефонну трубку та кнопки. Але замість стандартних телефонних роз'ємів RJ-11 IP-телефони мають роз'єм RJ-45. IP-телефони підключаються безпосередньо до вашого маршрутизатора та мають все необхідне обладнання та програмне забезпечення для роботи з IP-дзвінком. WiFi-телефони дозволяють абонентам VoIP здійснювати дзвінки з будь-якої точки, де доступний Wi-Fi.

- Комп'ютер-комп'ютер – це, безумовно, найпростіший спосіб використання VoIP. Вам навіть не потрібно платити за міжміські дзвінки. Існує кілька компаній, які пропонують безкоштовне або дуже дешеве програмне забезпечення, яке можна використовувати для VoIP цього типу. Вам потрібні тільки VoIP програмне забезпечення та комп'ютер з мікрофоном, динаміками, звуковою картою та підключенням до Інтернету. За винятком звичайного щомісячного внеску ISP, зазвичай немає плати за виклики комп'ютер-комп'ютер, незалежно від відстані.

- АТС-системи уніфікують комунікації у різних місцях підприємства, підтримують IP-телефони, аналогові пристрої та різні інтерфейси з'єднувальних ліній. АТС управляють IP-телефонами та аналоговими лініями, а також сполучними лініями PSTN, E1 та ITSP.

1.1.1 Як саме використовується VoIP

Телефонні компанії використовують VoIP для оптимізації власних мереж. Шляхом маршрутизації тисяч телефонних дзвінків через комутатор в шлюз IP можуть серйозно зменшити пропускну здатність, яка використовується для довгого шляху. Після отримання виклику з іншого боку, він розпаковується, повторно збирається та перенаправляється на комутатор локальної мережі. Навіть якщо це займе деякий час, ви можете бути впевнені, що врешті-решт всі існуючі мережі з комутацією каналів будуть замінені технологією пакетної комутації. IP-телефонія має сенс, як з погляду економіки, і з погляду інфраструктури. Дедалі більше компаній встановлюють проектні рішення VoIP, і технологія продовжуватиме зростати. Мабуть, найбільша привабливість VoIP для домашніх користувачів, які перемикаються – це ціна та гнучкість.

За допомогою VoIP можна здійснювати дзвінки з будь-якого місця, де є широкосмугове підключення. Оскільки IP-телефони або ATA транслюють інформацію через Інтернет, вони можуть керуватися провайдером скрізь, де є з'єднання. Таким чином, ділові мандрівники можуть взяти з собою свої телефони або ATA у поїздки та завжди мати доступ до свого домашнього телефону.

Іншою альтернативою є софтфон (програмний телефон) – це клієнтське програмне забезпечення, яке завантажує службу VoIP на ваш робочий стіл або ноутбук. Якщо у вас є навушники та мікрофон, ви можете здійснювати дзвінки з вашого ноутбука у будь-якому місці світу, де є широкосмугове підключення.

Більшість VoIP-компаній пропонують функції, за які звичайні телефонні компанії стягують додаткову плату.

VoIP включає:

- Caller ID;
- Очікування виклику;
- Перенаправлення виклику;
- Повторний набір;
- Зворотній виклик;
- Тристоронній виклик;

Існують також розширені опції фільтрації дзвінків, доступні від деяких операторів. Ці функції використовують інформацію ідентифікатора абонента, щоб ви могли вибрати спосіб поводження з певним номером. Ви можете:

- Переадресувати виклик на певний номер;
- Надіслати дзвінок безпосередньо на голосову пошту;
- Дати абоненту сигнал зайнятості;
- Відтворити повідомлення "не в обслуговуванні";
- Надіслати абонента на гарячу лінію відмови;

З багатьма послугами VoIP ви також можете перевіряти голосову пошту через Інтернет або прикріплювати повідомлення до електронного листа, який надсилається на ваш комп'ютер.

Тепер, коли ми розглянули VoIP у загальному сенсі, давайте подивимося уважніше на компоненти, які змушують систему працювати. Щоб зрозуміти, як працює VoIP, і чому це краще, ніж традиційна телефонна система, необхідно зрозуміти, як працює звичайна телефонна система.

1.1.2 VoIP: комутація каналів

Існуючі телефонні системи управляються дуже надійним, але дещо неефективним методом для підключення дзвінків, званим комутацією каналів. Комутація каналів – це дуже проста концепція, яка використовується у мережах телефонного зв'язку понад 100 років. Коли дзвінок здійснюється між двома сторонами, з'єднання підтримується під час дзвінка. Оскільки ви поєднуєте дві точки в обох напрямках, з'єднання називається схемою. Це є основою комутованої телефонної мережі загального користування (Public Switched Telephone Network (PSTN)).

Рисунок 1.1 - Public Switched Telephone Network

Ось як працює звичайний телефонний дзвінок:

1. Ви піднімаєте слухавку та слухаєте гудок. Це дозволяє дізнатися, що ви маєте з'єднання з місцевим офісом телефонного зв'язку.

2. Ви набираєте номер учасника, з яким бажаєте поговорити.

3. Виклик надсилається через комутатор вашого місцевого оператора на бік, який ви викликаєте.

4. З'єднання між телефоном та лінією іншої сторони здійснюється за допомогою кількох взаємопов'язаних перемикачів.

5. Телефон на іншому кінці дзвонить, і хтось відповідає на дзвінок.

6. З'єднання відкриває коло.

7. Ви говорите протягом деякого часу, а потім вішаєте трубку.

8. Коли ви повісите трубку, ланцюг закривається, звільняючи лінію і всі лінії між ними.

Телефонні розмови по сьогоднішній традиційній телефонній мережі дещо ефективніші, і вони коштують набагато дешевше. Ваш голос оцифровується, і разом із тисячами інших може бути об'єднаний на одному оптоволоконному кабелі. Ці виклики передаються з фіксованою швидкістю 64 Кбіт/с у кожному напрямку, за загальної швидкості передачі 128 Кбіт/с. Оскільки в кілобайті є 8 кілобіт, це переводить на відкриту передачу по 16 КБ кожну секунду та 960 КБ кожну хвилину. У 10-хвилинній розмові загальна передача становить 9600 КБ, що приблизно дорівнює 10 мегабайтам. Якщо ви подивитеся на типову телефонну розмову, більшість цих переданих даних буде витрачено марно.

1.1.3 VoIP: комутація пакетів

Телефонна мережа з комутацією пакетів є альтернативою комутації каналів. Він працює таким чином: поки ви кажете, інша сторона слухає, а це означає, що у будь-який момент часу використовується лише половина з'єднання. Виходячи з цього, ми можемо припустити, що ми могли б скоротити файл удвічі, аж до 4,7 МБ, підвищення ефективності. Крім того, значна частина часу в більшості розмов - мертве повітря - протягом декількох секунд, жодна зі сторін не розмовляє. Якби ми могли видалити ці тихі інтервали, файл буде ще меншим.

Мережі передачі не використовують комутацію каналів. Ваше інтернет-з'єднання було б набагато повільніше, якби воно підтримувало постійне з'єднання з веб-сторінкою, яку ви переглядали в будь-який момент часу. Натомість мережі передачі даних просто відправляють і витягують дані в міру необхідності. І замість того, щоб маршрутизувати дані виділеною лінією, пакети даних проходять через хаотичну мережу по тисячах можливих шляхів. Це називається комутацією пакетів.

У той час як комутація каналів зберігає з'єднання відкритим та постійним, пакетна комутація відкриває коротке з'єднання - досить довго, щоб відправити невеликий фрагмент даних, званий пакетом, з однієї системи до іншої. Він працює наступним чином:

- Передавальний комп'ютер відкидає дані на невеликі пакети, причому адреса кожного з них вказує мережним пристроям, куди їх надсилати;

- Усередині кожного пакета є корисне навантаження. Корисне навантаження – це частина електронної пошти, музичний файл або будь-який інший тип файлу, який передається всередині пакета;

- Комп'ютер відправляє пакет найближчому маршрутизатору і забуває про це. Найближчий маршрутизатор надсилає пакет іншому маршрутизатору, який знаходиться ближче до комп'ютера-одержувача. Цей маршрутизатор відправляє пакет іншому, ще ближчому маршрутизатору і так далі;

- Коли приймаючий комп'ютер остаточно отримує пакети, він використовує інструкції, що містяться в пакетах, для збору даних у вихідний стан.

Перемикання пакетів дуже ефективне. Воно дозволяє мережі маршрутизувати пакети найменш перевантаженим і найдешевшим лініям. Він також звільняє два комп'ютери, що взаємодіють один з одним, щоб вони могли приймати інформацію з інших комп'ютерів.

1.1.4 Переваги використання VoIP

Технологія VoIP використовує можливості комутації пакетів Інтернету для забезпечення телефонного обслуговування. VoIP має кілька переваг перед перемиканням каналів. Наприклад, комутація пакетів дозволяє декільком

телефонним дзвінкам займати простір, який займає лише один у мережі з комутацією каналів. Використовуючи PSTN, ця 10-хвилинна телефонна розмова про яку ми говорили споживав 10 повних хвилин часу передачі за ціною 128 Кбіт/с. З VoIP цей же виклик міг займати всього 3,5 хвилини часу передачі за ціною 64 Кбіт/с, залишивши ще 64 Кбіт/с вільними ці 3,5 хвилини і плюс додаткові 128 Кбіт/с протягом 6,5 хвилин, що залишилися. На основі цієї простої оцінки ще три або чотири виклики можуть легко вписатися в простір, який використовується одним викликом у звичайній системі. І цей приклад навіть не впливає на використання стиснення даних, що ще більше зменшує розмір кожного дзвінка.

Припустимо, що ви та ваш друг обидва обслуговуєтеся через VoIP-провайдера. У вас обох є аналогові телефони, підключені до АТА, що надається сервісом. Давайте ще раз розглянемо типовий телефонний дзвінок, але цього разу за допомогою VoIP через мережу з комутацією пакетів:

1. Ви піднімаєте приймач, який надсилає сигнал АТА.

2. АТА приймає сигнал та відправляє тональний сигнал відповіді станції. Це дозволяє дізнатися, що у вас є підключення до Інтернету.

3. Ви набираєте номер телефону, з яким хочете поговорити. Аналоговий телефонний адаптер перетворює тони на цифрові дані та тимчасово їх збереже.

4. Дані телефонних номерів надсилаються у формі запиту на процесор викликів вашої VoIP-компанії. Процесор виклику перевіряє його, щоб переконатися, що він у допустимому форматі.

5. Обробник дзвінків визначає, кому можна порівняти номер телефону. При порівнянні номер телефону перетворюється на IP-адресу. Програмний комутатор з'єднує два пристрої з обох кінців виклику. З іншого боку, сигнал відправляється в АТА вашого друга, щоб зв'язаний телефон дзвонив.

6. Як тільки ваш друг бере трубку, сеанс встановлюється між вашим комп'ютером та комп'ютером вашого друга. Це означає, що кожній системі відомо, що пакети даних надходитимуть з іншої системи. Всередині звичайна інфраструктура Інтернету обробляє виклик, якби це була електронна пошта або веб-сторінка. Кожна система повинна використовувати той самий протокол для

зв'язку. В рамках сеансу системи реалізують два канали, по одному для кожного напряму.

7. Ви кажете якийсь час. Під час розмови ваша система та система вашого друга передають пакети туди та назад, коли є дані для відправки. ATA на кожному кінці транслюють ці пакети в міру їхнього прийому і перетворюють їх на аналоговий аудіосигнал, який ви чуєте. Ваш ATA також тримає ланцюг відкритим між собою та вашим аналоговим телефоном, поки він пересилає пакети на та з IP-хоста на іншому кінці.

8. Ви закінчите розмову та повісили трубку.

9. Коли ви повісите трубку, ланцюг закривається між телефоном і ATA.

10. ATA посилає сигнал на м'який комутатор, що з'єднує дзвінок, завершуючи сеанс.

Ймовірно, однією з переконливих переваг пакетної комутації є те, що мережі передачі даних вже розуміють технологію. Переходячи до цієї технології, телефонні мережі відразу отримують можливість повідомляти, як це роблять комп'ютери.

1.1.5 Недоліки використання VoIP

Поточна комутована телефонна мережа загального користування є надійною і досить куленепробивною системою для доставки телефонних дзвінків. Телефони просто працюють, і всі ми залежимо від цього. З іншого боку, комп'ютери, електронна пошта та інші пов'язані з ними пристрої, як і раніше, виглядають нерівними. Подивимося правді в очі – мало хто справді панікує, коли їхня електронна пошта падає на 30 хвилин. Іноді це очікується. З іншого боку, півгодини без тонального сигналу набору можуть легко відправити людей в паніку. Так що PSTN може відчувати брак ефективності, це більш ніж компенсує надійність. Але мережа, яка становить Інтернет, набагато складніша і, отже, функціонує зі значно більшою похибкою. Відповідно одним з основних недоліків VoIP є надійність.

- Насамперед, VoIP залежить від потужності мережі. Ваш поточний телефон працює на фантомному живленні, яке надається по лінії від

центрального офісу. Навіть якщо ваша потужність гасне, ваш телефон все ще працює. За допомогою VoIP немає живлення, немає телефону. Для VoIP необхідно створити стабільне джерело живлення.

- Інший розгляд полягає в тому, що багато інших систем у вашому будинку можуть бути інтегровані в телефонну лінію. Цифрові відеомагнітофони, цифрові абонентські телевізійні послуги та системи домашньої безпеки використовують стандартну телефонну лінію для виконання своїх завдань. В даний час немає способу інтегрувати ці продукти з VoIP.
- Надзвичайні виклики також стають проблемою VoIP. Як зазначалося раніше, VoIP використовує IP-адресні номери телефонів, а не номери NANP. Неможливо зв'язати географічне розташування з IP-адресою. Тому, якщо абонент не може повідомити оператора, де він знаходиться, тоді немає способу дізнатися, який центр обробки викликів направить екстрений виклик і який EMS повинен відповісти. Щоб виправити це, можливо, географічна інформація може бути інтегрована в пакети.
- Оскільки VoIP використовує інтернет-з'єднання, він сприйнятливий до всього, що зазвичай пов'язане з домашніми широкосмуговими послугами. Всі ці фактори впливають на якість зв'язку: латентність, тремтіння та втрату пакетів. Телефонні розмови можуть бути перекручені або втрачені через помилки передачі. Певна стабільність передачі даних в Інтернеті повинна бути гарантована до того, як VoIP дійсно зможе замінити традиційні телефони.
- VoIP вразливий для вірусів та зломів, хоча це дуже рідко, і розробники VoIP працюють над VoIP-шифруванням, щоб протистояти цьому.

Ще одна проблема, пов'язана з VoIP, полягає в тому, що телефонна система залежить від окремих ПК з різними характеристиками та потужністю. На дзвінок може вплинути пошкодження процесора. Припустимо, що ви розмовляєте на своєму програмному телефоні, і ви вирішили відкрити програму, яка знищує ваш процесор. Втрата якості одразу стане очевидною. У найгіршому випадку ваша

система може зазнати краху в середині важливого виклику. У VoIP всі телефонні дзвінки залежать від звичайних проблем із комп'ютером.

Однією з перешкод, які були подолані деякий час тому, було перетворення аналогового аудіосигналу, який телефон отримує в пакети даних. Як аналоговий звук перетворюється на пакети передачі VoIP? Відповідь – це кодеки.

1.2 Аналіз проблем и загроз VoIP

1.2.1 Проблеми безпеки протоколу Skype

На відміну від багатьох інших протоколів IP-телефонії для передачі даних Skype спочатку використовував децентралізовану P2P-архітектуру.

Єдиним центральним елементом Skype є сервер ідентифікації, на якому зберігаються облікові записи користувачів і резервні копії їх списків контактів. Центральний сервер потрібен лише для встановлення зв'язку. Після того, як зв'язок встановлений, комп'ютери пересилають голосові дані безпосередньо один одному (якщо між ними є прямий зв'язок) або через Skype-посередник – супервузол. Раніше як супервузл міг виступати будь-який комп'ютер, у якого є зовнішня IP-адреса і відкритий TCP-порт для Skype, проте потім всі супервузли були перенесені на сервера Microsoft.

1.2.1.1 Неконтрольоване використання

З точки зору безпеки, Skype є одним з потенційних каналів витоку корпоративних та персональних даних, причому стоїть окремо через захищеність від перехоплення.

Існує поширена помилка, що моніторинг інформації, що передається по Skype, так само як і вибірковий контроль використання самої служби окремими користувачами, неможливий або надмірно витратний у зв'язку з високим ступенем захищеності цього каналу комунікацій від прослуховування та перехоплення. Дійсно, якщо перехоплювати трафік Skype на рівні корпоративних серверів і мережевих шлюзів, то його перехоплення та подальше розшифрування будуть

дуже непростою справою. Можна глобально заборонити використання Skype у корпоративній мережі, але це не завжди буде поєднуватися із запитами співробітників, для яких Skype є одним із інструментів бізнесу.

Вирішенням цієї проблеми є використання DLP (Data Leak Prevention) систем.

Так, наприклад, DLP-система SearchInform містить у своїй архітектурі модуль SkypeSniffer, що дозволяє перехоплювати голосові та текстові повідомлення, а також файли та SMS, що передаються через Skype.

Однак вирішення однієї проблеми породило іншу, а саме можливість доступу до особистої інформації користувачів третіх осіб.

1.2.1.2 Неправомірний доступ до особистої інформації

Відповідно до пункту 3 політики конфіденційності Skype, сервіс та його партнери можуть надавати особисті дані, вміст розмов та/або трафік даних користувачів у відповідь на законний запит органів судової влади чи правоохоронної системи. Крім того, миттєві повідомлення, передані користувачем, зберігатимуться протягом 30 днів, якщо інший термін не буде витребуваний представниками держорганів.

А після того, як у травні 2011 р. компанія Microsoft придбала Skype, стала з'являтися інформація не лише про доступ до інформації без судового запиту, а й про можливість спецслужб деяких країн прослуховувати розмови у Skype.

Так, у червні 2013 року Едвард Сноуден розкрив інформацію про американську систему стеження PRISM, яка дозволяла стежити за користувачами Skype та прослуховувати їхнє листування та дзвінки у програмі.

Проте ще задовго до цього у 2006 році був зафіксований випадок, коли місцезнаходження одного зі злочинців, зав'язаного з махінаціями над цінними паперами, виявили за єдиним хвилинним дзвінком дочки, зробленим за допомогою Skype. Як це було здійснено незрозуміло.

У 2008 році на WikiLeaks з'явилися документи, в яких Міністерство юстиції, прокуратура та поліція федеральної землі Баварія обговорюють між собою те, кому

платити за недешеві послуги з встановлення на комп'ютери підозрюваних троянців для доступу до розмов через Skype. У цьому випадку подібну послугу "людина посередині" баварській владі на комерційній основі надавала німецька фірма Digitask. Установка перехоплення Skype оцінена у 3500 євро, перехоплення SSL-сеансів – 2500 євро.

1.2.1.3 Закритість протоколу Skype

У зв'язку із закритістю вихідного коду протоколу Skype та відсутністю будь-якої документації, що відображає методи забезпечення безпеки, існує загроза безпеці, пов'язана з тим, що у користувачів програмного засобу відсутня впевненість у тому, що використовуються ефективні методи забезпечення безпеки мережевої взаємодії.

1.2.1.4 Дзвінки на ТФзК

При здійсненні дзвінка зі Skype на мобільні та стаціонарні телефони частина сигналу, що проходить по ТФзК, не шифрується. Наприклад, у випадку групових викликів за участю двох користувачів по Skype-до-Skype та одного користувача за ТФзК, то частина ТФзК не шифрується, але частина Skype-до-Skype шифрується.

1.2.2 Класифікація загроз VoIP

Розглянемо різні види загроз інформаційним системам, які використовують VoIP.

Складемо класифікацію загроз VoIP на базі таксономії, випущеної організацією VOIPSA (VoIP Security Alliance) у 2005 р. Ця таксономія класифікує та описує більшість відомих на даний момент загроз, не пов'язаних безпосередньо з протоколами прикладного рівня.

Класифікація основних загроз VoIP представлена рисунку 1.15.

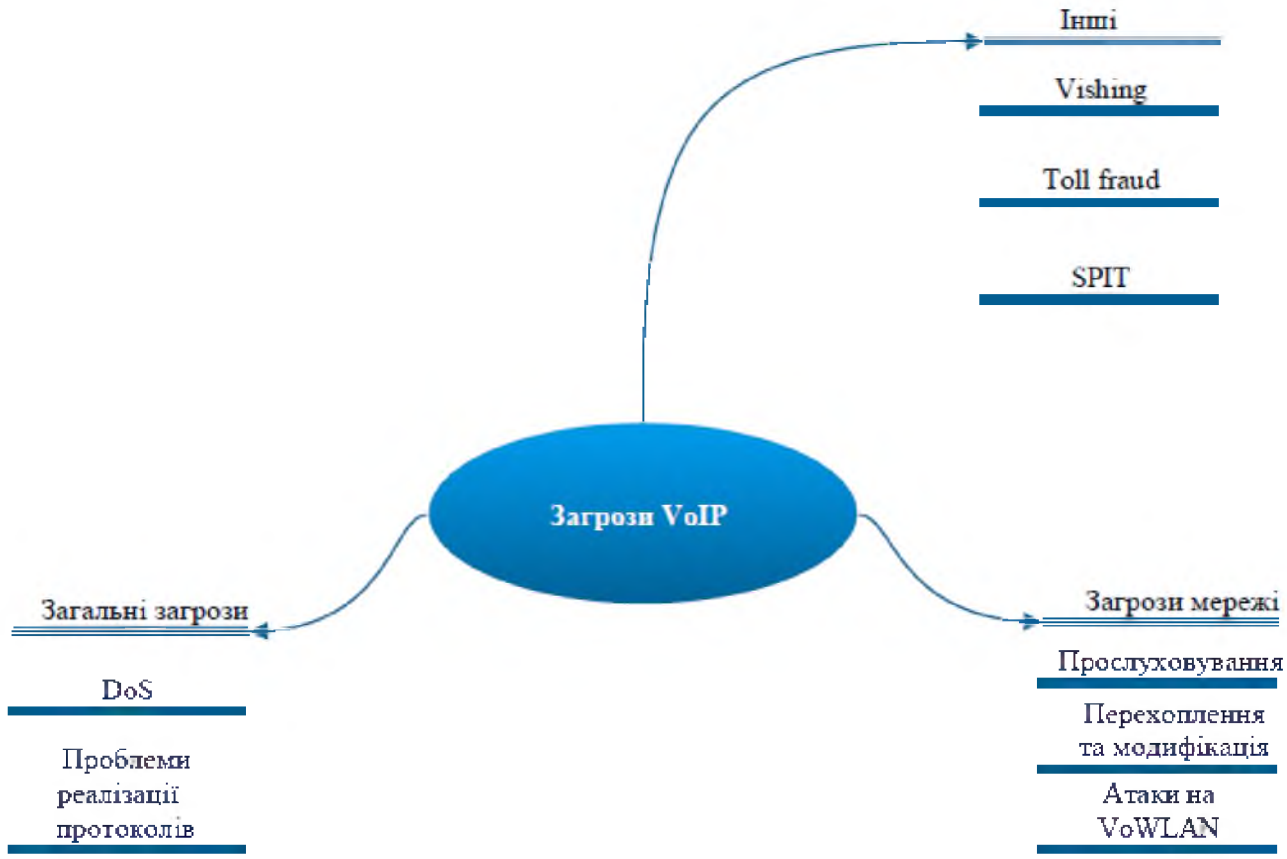

Рисунок 1.2 — Класифікація загроз

Під загальними загрозами розуміються загрози, властиві більшості інформаційних систем.

Під загрозами мережі розумітимемо загрози, пов'язані безпосередньо з передачею даних каналами.

Розглянемо докладніше всі ці небезпеки.

Таблиця 1.1 – Загрози VoIP

Загроза	Опис
Vishing (VoIP-phishing)	Такі загрози є обходом або порушення роботи механізму аутентифікації зловмисником з метою підміни особистості, даних. Іноді зловмисник користується довірою користувачів і йому не потрібно обходити механізм автентифікації. В результаті, іноді з використанням методу соціальної інженерії, зловмисник отримує від користувача необхідні дані. Іноді для Vishing використовуються автоматизовані системи (автовідповідачі та ін. пристрої).
Toll fraud	Зловмисник, отримуючи доступ до мережі, здійснює неавторизовані дзвінки, здійснює видалення або зміну даних рахунків або інші дії, спрямовані на зловмисне користування послугами VoIP. Такі дії можуть довго залишатися непоміченими у великій організації.
Spam over IP telephony (SPIT)	Спам у мережах VoIP найчастіше є записані повідомлення, які надходять на IP-телефони у вигляді вхідних дзвінків. Крім настирливості, SPIT також може викликати навантаження мережі і навіть відмову в обслуговуванні.
Прослуховування	За відсутності шифрування у VoIP, зловмисник може неправомірно підключитися до мережі та зробити запис, аналіз трафіку. Зловмисник може прослуховувати конкретні розмови, так і збирати в автоматичному режимі різні дані, такі як номери телефонів, номери кредитних карт, різні адреси та ін.
Перехоплення та модифікація	На відміну від прослуховування, зловмисник чинить активні дії по відношенню до трафіку мережі. До цієї категорії можна віднести: - Скидання викликів (Call blackholing);

Продовження таблиці 1.1

	- Перенаправлення дзвінків (Call sinkholing); - Підміна факсів; - Підміна викликів; - Зміна вмісту факсів; - Зміна даних дзвінка.
Атаки на VoWLAN	Зловмисник може отримати дані за недостатнього забезпечення безпеки бездротових мереж, що використовуються для передачі голосу.
Відмова в обслуговуванні (DoS)	Можна виділити такі категорії загроз для відмови в обслуговуванні **Характерні для VoIP** Різноманітність протоколів, що використовуються VoIP, надає зловмиснику великий вибір методів здійснення атаки DoS. До таких методів можна віднести: - Флудинг різних запитів (встановлення з'єднання, управління з'єднанням); - формування некоректних запитів; - використання помилкових повідомлень завершення виклику або повідомлень «лінія зайнята»; - Порушення процесу реєстрації користувачів у мережі; - Підміна VoIP-сервера та ін. **Характерні для IP-мереж** Різні відомі методи DoS та DDoS для IP-мереж (SYN attack, Smurf Attack та ін) або для попутно використовуваних сервісів (DHCP, TFTP та ін).
Проблеми реалізації протоколів	Уразливості, що виникають через помилки у реалізації будь-якого протоколу.

1.3 Аналіз підходів за забезпеченням захищеності VoIP

Для протистояння описаним загрозам потрібен комплексний підхід до забезпечення інформаційної безпеки. Розіб'ємо можливі методи безпеки VoIP на групи (рисунок 1.16) і розглянемо кожен метод.

Рисунок 1.3 — Методи забезпечення безпеки VoIP

Таблиця 1.2 – Методи захисту VoIP

Метод захисту	Опис
Навчання персоналу	Насамперед слід подбати про поінформованість персоналу у питаннях забезпечення інформаційної безпеки. Необхідно, щоб персонал знав про існування загроз Vishing та спаму, і при першій їх появі повідомляв про них.
Фізичний контроль доступу	Обмеження фізичного доступу до пристроїв, що забезпечують VoIP інфраструктуру, дозволить захиститися не тільки від відмови в обслуговуванні, але й забезпечити конфіденційність інформації, що передається.
Виділення голосового трафіку в окремі VLAN	Використання окремої VLAN дозволяє уникнути деякої підмножини атак типу Toll Fraud, оскільки забезпечує розмежування прав доступу для різних VLAN. Також використання VLAN дозволяє захиститися від деяких DDoS атак, що стосуються лише мережі передачі даних. Зловмиснику буде складніше здійснити прослуховування трафіку, виділеного в окрему VLAN.
Використання списків контролю доступу	Разом з VLAN можна використовувати списки контролю доступу, що дозволяють обмежити доступ як до послуг VoIP в цілому, так і регулювати повноваження різних груп користувачів щодо різних типів дзвінків, що призведе до ускладнення проведення атаки типу Toll Fraud. Також використання ACL разом з VLAN обмежить кількість точок проходження трафіку, що ускладнить його прослуховування.

Продовження таблиці 1.2

Використання міжмережевих екранів	VoIP використовує безліч різних протоколів, а, отже, портів, і це робить інформаційну систему вразливішою до загроз ззовні, таким як DoS, а також внутрішнім загрозам, таким як Toll Fraud. Отже, необхідно використати МЕ.
Використання механізмів шифрування	Часто використання шифрування на кінцевих пристроях неможливо, з огляду на їх низьку продуктивність і виникнення неприйнятних затримок. У такому випадку можна використовувати шифрування на шлюзах чи маршрутизаторах. Варто зазначити, що сучасні IP-телефони підтримують апаратне шифрування AES з достатньою для нормальної передачі трафіку швидкістю.
Використання механізмів автентифікації	Необхідне використання механізмів автентифікації, які можуть бути реалізовані як у протоколах вищих рівнів (SIP), так і на рівні мережевого обладнання (наприклад, подібне реалізовано у продукції Cisco).
Використання тунелювання	Використання тунелів дозволяє не тільки забезпечити конфіденційність інформації, що передається, але і уникнути атак типу Toll Fraud, так як шифрується не тільки корисне навантаження, але і заголовки, які містять дані, які можуть бути використані зловмисником, такі як MAC і IP адреси терміналів.

Продовження таблиці 1.2

Забезпечення безпеки пристроїв	Розглянемо базові принципи безпеки пристроїв. **Уникати конфігурації «за замовчуванням»** Слід проводити налаштування всіх нових пристроїв в інфраструктурі, щоб уникнути ситуацій, коли зловмисник може отримати доступ до конфігурації пристрою за допомогою логіну/паролю за замовчуванням. **Безпека програмних VoIP-клієнтів** Особливу увагу слід приділити програмним VoIP-клієнтам, оскільки вони схильні до загроз, пов'язаних з ОС та використовуваними сервісами. **Контроль оновлення ПЗ** Не оновлюйте ПЗ пристроїв за допомогою небезпечних протоколів, таких як TFTP. **Забезпечення своєчасного оновлення ПЗ** Для захисту від різних уразливостей у реалізації тих чи інших протоколів чи драйверів апаратного забезпечення пристроїв необхідно регулярно оновлювати програмне забезпечення. **Забезпечення безперебійного живлення** Для захисту від відмови в обслуговуванні необхідно забезпечити ключові пристрої VoIP-мережі механізмами забезпечення безперебійного живлення на випадок відключення електропостачання. **Захист механізмів віддаленого доступу** Для віддаленого доступу до пристроїв слід використовувати лише захищені протоколи, такі як IPSec або SSH.

1.4 Висновок

VoIP - це значне поліпшення порівняно з існуючою телефонною системою ефективності, вартості та гнучкості. Як і будь-яка нова технологія, VoIP має деякі проблеми для подолання, але ясно, що розробники продовжуватимуть удосконалювати цю технологію, поки вона в кінцевому підсумку не замінить поточну телефонну систему.

Технологія Voice over Internet Protocol (VoIP) може підвищити загальну продуктивність організації, дозволяючи своїм співробітникам виконувати багатозадачність без перерв. Вона також дозволяє організації виділяти кошти, зазвичай витрачені традиційні телефонні рахунки, інші аспекти бізнесу. VoIP дає можливість користувачам прикладати документи, проводити віртуальні зустрічі та обмінюватися даними за допомогою відеоконференцій. На даний момент виробники інтенсивно працюють над усуненням основної проблеми VoIP – покращення чіткості голосу, щоб зробити її невідмінною від традиційної телефонії. Раніше версії VoIP виробляли спотворені телефонні дзвінки, відставання в передачі та відкидаються дзвінки, але зміни у технології VoIP зробило її більш привабливою для бізнесу та корпорацій, враховуючи, що йде постійна робота над попередніми помилками.

Результатом першого розділу є детальне дослідження VoIP та IP-телефонії як засобів зв'язку, аналіз та види загроз у ній, та методи захисту VoIP, які будуть детально розібрані у другому розділі.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Забезпечення безпеки VoIP

Для забезпечення захищеності інформації, що передається через VoIP, будемо використовувати її шифрування.

Більшість VoIP-клієнтів, наприклад Skype, використовують шифрування даних при передачі. Однак у випадку використання Skype, який є найпоширенішим VoIP-клієнтом (станом на кінець 2010 року зареєстровано 663 мільйони користувачів, а в 2013 році користувачами було здійснено дзвінків тривалістю 214 мільярдів хвилин), використовувані засоби забезпечення інформаційної безпеки не можна вважати надійними . Як було розглянуто вище, на сьогоднішній день всі функції безпеки Skype реалізуються серверами компанії Microsoft, що є неприйнятним при передачі конфіденційних даних. По-перше, тому, що до інформації має доступ третя сторона (Microsoft). По-друге, тому що засоби забезпечення безпеки не є документованими, тобто немає впевненості у їх стійкості.

Тому в даній роботі мова вестимемося про використання кінцевого шифрування, при якому можливість зашифрування і розшифрування мають лише сторони, які спілкуются.

2.1.1 Кінцеве шифрування в Skype

Для забезпечення кінцевого шифрування в Skype необхідно виконати такі етапи:

1. Забезпечити можливість формування сеансового ключа для симетричного шифрування.

2. Забезпечити можливість зашифрування та розшифрування аудіопотоку.

При цьому у зв'язку з тим, що Skype є можливість обміну текстовими миттєвими повідомленнями, необхідно також реалізувати зашифрований обмін повідомленнями.

Для виконання цих етапів необхідно мати можливість програмно ініціювати

надсилання повідомлень з метою:

- встановлення сеансового ключа;
- надсилання зашифрованих повідомлень.

Для цього використовуватимемо програмний інтерфейс (API), що надається Skype.

2.1.1.1 Skype API

При використанні програмного інтерфейсу Skype можна програмно виконувати основні функції, що надаються Skype.

Для початку роботи з клієнтом Skype необхідно створити об'єкт Skype і ініціювати з'єднання з програмним клієнтом:

```
Skype skype;
skype = new Skype();
```

Далі можна виконувати різні стандартні функції залежно від потреб.

Так, наприклад, надсилання повідомлень здійснюється наступним чином:

```
skype.SendMessage("ім'я_абонента", "повідомлення");
```

Організація групового чату виглядає так:

```
UserCollection members;
User user;
IChat ichat;
user = new SKYPE4COMLib.User();
user.Handle ="абонент_1";
user.Handle ="абонент_2";
members.Add(user);
```

```
ichat = MicInterceptor.skype.CreateChatMultiple(members);
ichat.SendMessage("повідомлення");
```

Виклик абонента:

```
Call call;
call = skype.PlaceCall("імя_абонента");
```

2.1.2 Шифрування звуку

Для зашифрування та розшифрування звукового потоку в режимі реального часу до алгоритму шифрування висуваються такі вимоги:

- висока швидкодія;
- висока криптостійкість.

Наведеним вище вимогам відповідає стандарт симетричного шифрування ДСТУ ГОСТ 28147:2009.

При цьому необхідно, щоб довжина зашифрованого сигналу не була більшою за довжину початкової довжини сигналу. Ця вимога обумовлена тим, що передача більшого за розміром потоку займає відповідно більшу кількість часу, що спричинить неприйнятну розсинхронізацію з відео.

Тому використовуватимемо шифрування ДСТУ ГОСТ 28147:2009 в режимі простої заміни.

2.1.3 Сеансовий ключ

Для зашифрування та розшифрування даних за алгоритмом ДСТУ ГОСТ 28147:2009 необхідно, щоб сторони домовилися про використання сеансового ключа довжиною 256 біт.

Встановлення сеансового ключа за класичним протоколом Діффі-Хеллмана дозволяє сторонам встановити сеансовий ключ незахищеним каналом зв'язку.

Даний протокол вразливий до атаки "людина посередині" у зв'язку з тим, що

сторони, які спілкуються, не можуть достовірно визначити з ким вони спілкуються. Однак використання цього протоколу при забезпеченні безпечного спілкування через IP-телефонію різко знижує ймовірність реалізації цієї загрози. Це можна пояснити тим, що сторони мають можливість бачити і чути один одного після встановлення зашифрованого з'єднання, а при перехопленні зашифрованих пакетів третьою стороною з подальшою передачею співрозмовнику спричинить неприйнятні затримки при передачі. Така затримка свідчить про можливу атаку «людина посередині».

2.2 Забезпечення безпечної передачі даних у Skype

Як уже було сказано, оптимальним засобом досягнення безпечної передачі даних є можливість шифрування інформацією, що надходить у програмний клієнт Skype, та інформацією, що виходить із нього.

Для цього мовою програмування C# було розроблено програмний засіб з наступним функціоналом:

1. Встановлення сеансового ключа за класичним протоколом Діффі-Хеллмана із заданим абонентом.
2. Надсилання повідомлень, зашифрованих за алгоритмом симетричного шифрування ДСТУ ГОСТ 28147:2009 заданому абоненту.
3. Прийом зашифрованих повідомлень та їх розшифрування.
4. Встановлення сеансового ключа під час здійснення виклику.
5. Зашифрування вихідного аудіосигналу.
6. Розшифрування вхідного аудіосигналу.
7. Збереження згенерованого сеансового ключа.
8. Відкриття раніше згенерованого сеансового ключа.

На рисунку 2.1 зображено інтерфейс розробленого програмного засобу.

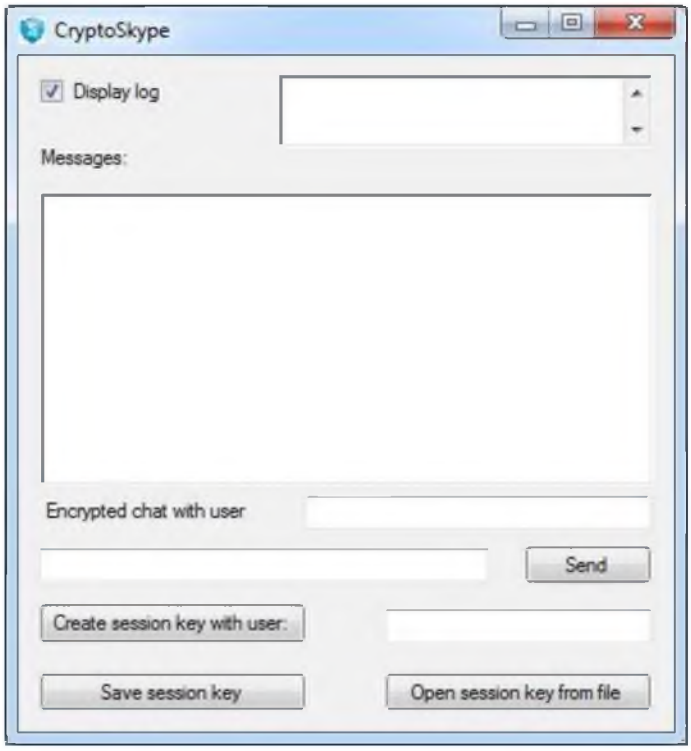

Рисунок 2.1 – Інтерфейс програмного засобу

Далі опишемо розроблений функціонал.

2.2.1 Встановлення сеансового ключа

Згідно з класичним протоколом Діффі-Хеллмана сторони обмінюються параметрами p і g. У розробленій програмі (додаток Д) дані параметри генерує сторона, яка ініціювала встановлення сеансового ключа. Це відбувається так.

```
p = BigInteger.GenPseudoPrime(512, 30, _strongRng);
g = (BigInteger)2;
skype.SendMessage("имя_абонента", "!#skey_init#!p" +p.ToString(36));
skype.SendMessage("имя_абонента", "!#skey_init#!g" +g.ToString(36));
```

Далі сторони генерують великі випадкові числа та обмінюються результатом операції зведення в ступінь за модулем:

$$g^e (mod\ p)$$

b = BigInteger.GenPseudoPrime(512, 30, _strongRng);

skype.SendMessage(“имя_абонента”, "!#skey_init#!e" + g.ModPow(b, p).ToString(36));

$$g^{ab}(mod\ p)$$

recv = new BigInteger(mesg, 36); //полученной сообщение

key = new byte[recv.ModPow(a, p).GetBytes().Length];

key = recv.ModPow(a, p).GetBytes(); //сеансовый ключ

На рисунку 2.2 показано результат встановлення сеансового ключа абонентами.

Рисунок 2.2 – Процес встановлення сеансового ключа

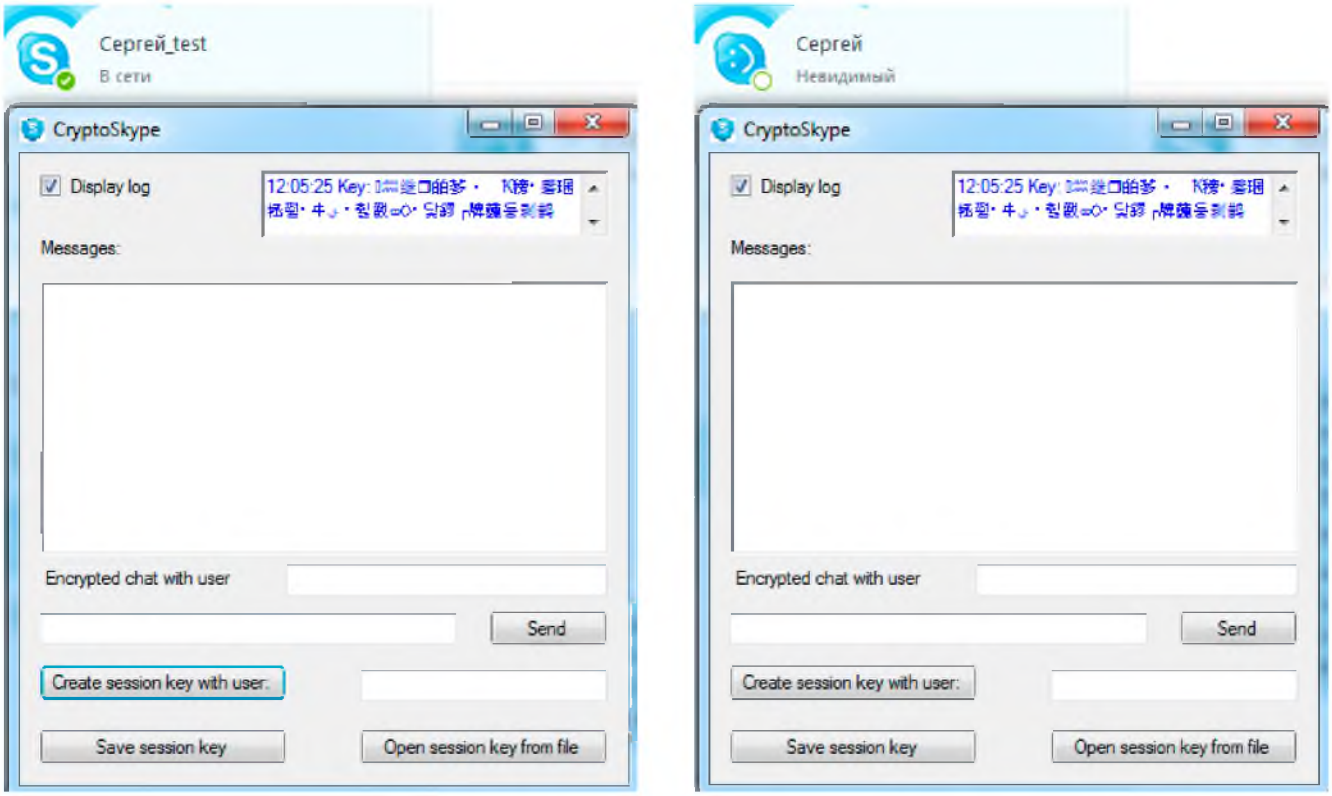

Рисунок 2.3 – Встановлений сеансовий ключ

Для встановлення сеансового ключа між трьома та більше абонентами необхідно перерахувати їх через точку з комою у полі введення (рисунок 2.4).

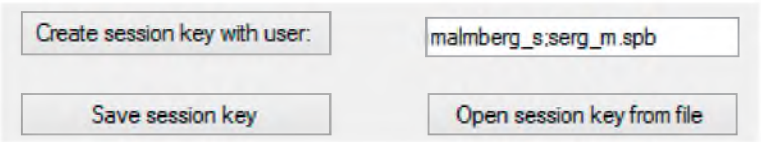

Рисунок 2.4 — Встановлення сеансового ключа між трьома абонентами

Встановлення сеансового ключа для трьох абонентів відбувається так, як показано на рисунку 2.5.

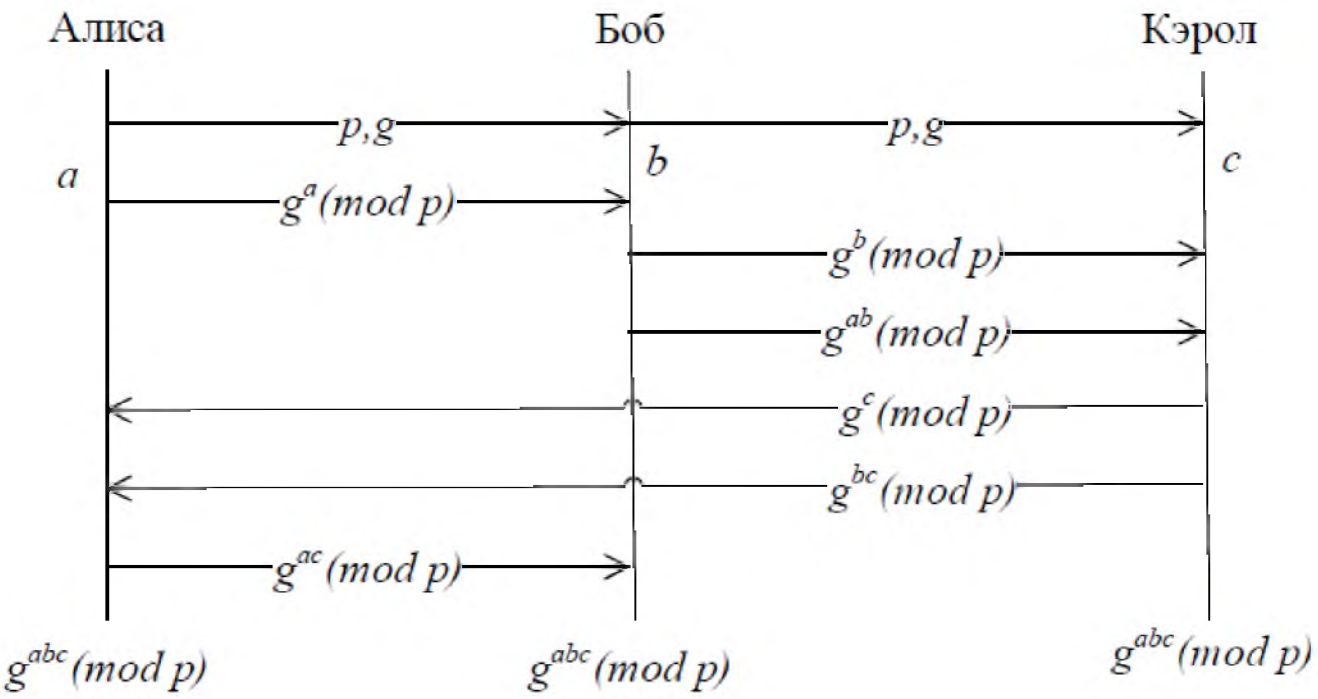

Рисунок 2.5 — Встановлення сеансового ключа між трьома абонентами за класичним протоколом Діффі-Хеллмана

2.2.2 Шифрування голосу

Здійснюючи дзвінок з боку абонента, який ініціював виклик, надсилаються повідомлення з метою встановлення сеансового ключа за класичним протоколом Діффі-Хеллмана.

```
if (status == TCallStatus.clsRouting) //если совершается вызов
{
this.call = call;
nick = call.PartnerHandle;
DHkey(); //установка сеансового ключа
}
```

Якщо установка сеансового ключа пройшла успішно, то на згенерованому ключі здійснюється зашифрування даних, що надійшли на мікрофон, та розшифрування сигналу, що надійшов мережею (рисунок 2.6).

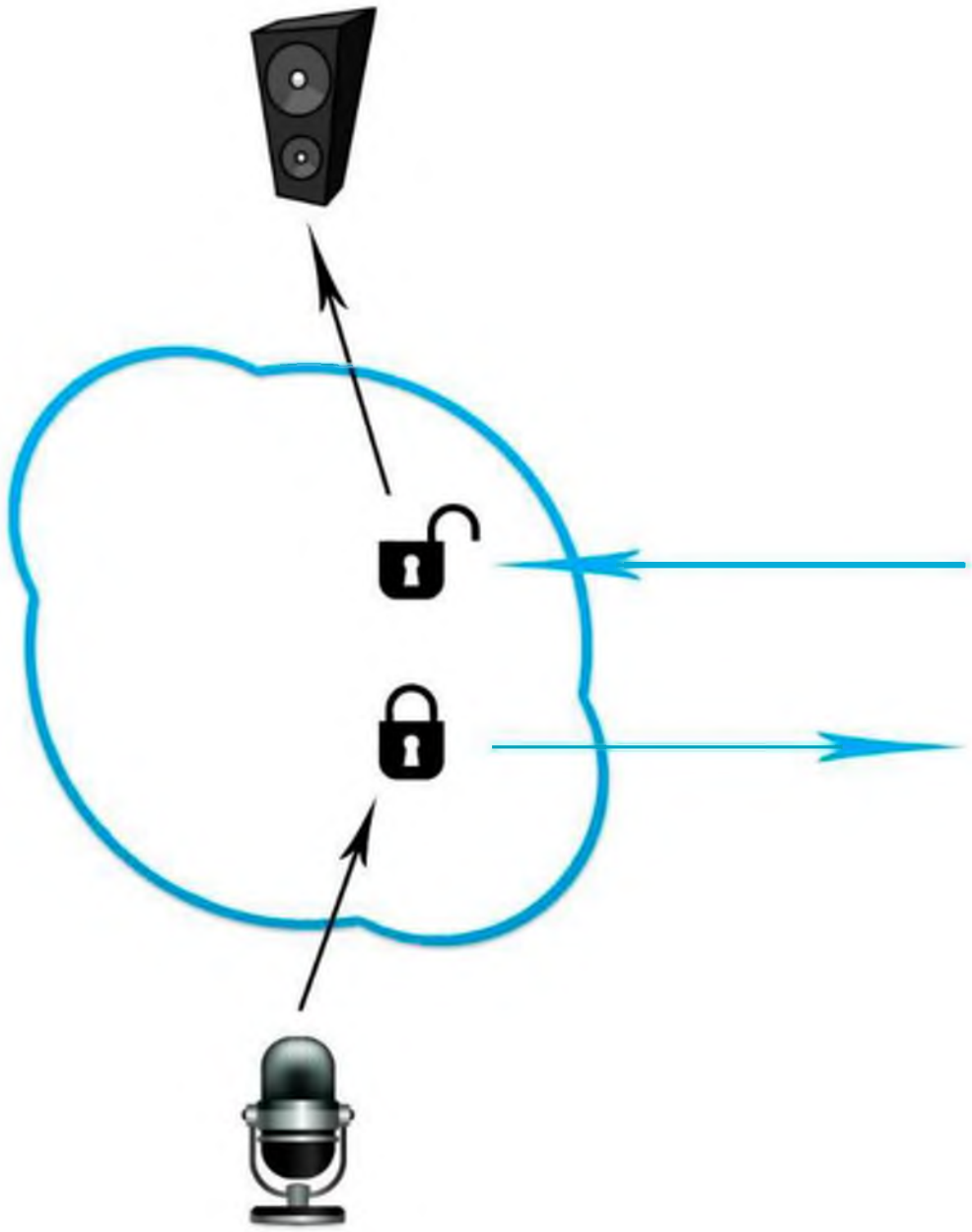

Рисунок 2.6 — Схема шифрованої передачі голосу

У випадку, якщо встановити сеансовий ключ не вдалося (в результаті, наприклад, відсутності запущеного програмного засобу в одного з абонентів), то здійснюється зашифрування голосу на випадково згенерованому ключі.

Здійснення зашифрованого групового виклика можливе після встановлення сеансового ключа (рисунок 2.4) шляхом повторного натискання на кнопку “Create session key with user”.

Опишемо процес зашифрування та розшифрування голосу.

2.2.2.1 Зашифрування голосу

Отримавши доступ до програмного клієнта Skype через програмний інтерфейс, ми контролюємо вхідні та вихідні потоки.

Зашифрування вихідного голосового потоку виглядає так.

```
if (outStream != null)
{
bufferStream.SetLatestInBuffer(args.Buffer);
byte[] encr = new byte[args.Buffer.Length];
Gost28147.Gost28147Ecb(args.Buffer, encr, key);
outStream.Write(encr, 0, encr.Length);
}
```

2.2.2.2 Розшифрування голосу

Для розшифрування використовується доступ до аудіопотоку за допомогою класу NetworkStream простору імен System.Net.Sockets.

```
while (client.Connected)
{
int available = client.Available;
if (available > 0)
{
byte[] buffer = new byte[available];
int read = inStream.Read(buffer, 0, available);
byte[] decr = new byte[buffer.Length];
Gost28147.Gost28147EcbDecrypt(decr, buffer, key);
inStream.Write(decr, 0, decr.Length);
OnDataReceived(decr);
```

```
}
}
```

2.2.3 Зашифрований обмін повідомленнями

Після успішного встановлення сеансового ключа можна здійснити зашифрований обмін повідомленнями.

При введенні повідомлення у відповідне поле розробленого програмного засобу (рисунок 2.7) відбувається зашифрування введеного повідомлення та його подальша передача адресату.

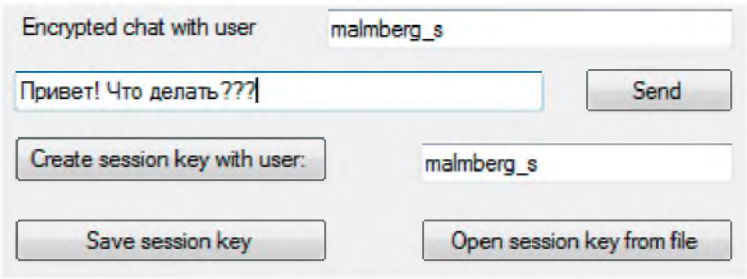

Рисунок 2.7 — Надсилання повідомлення зашифрованим чатом

```
byte[] plain = GetBytes(textBox2.Text);
byte[] encr = new byte[plain.Length];
Gost28147.Gost28147Ecb(plain, encr, key);
msg_log.Info(false, " to {0}\n{1}", textBox3.Text,textBox2.Text);
skype.SendMessage(nick, "!#encr__msg#!" + GetString(encr));
```

На рисунку 2.8 представлено зашифрований обмін повідомленнями.

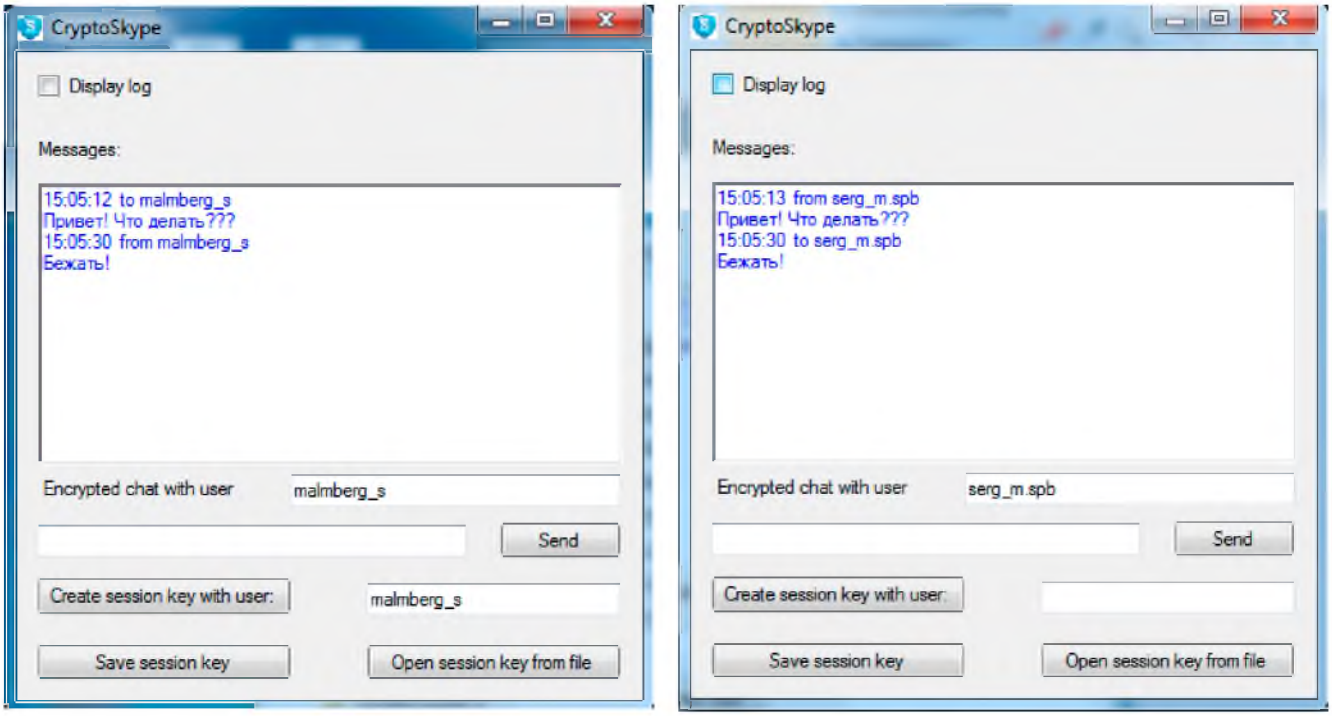

Рисунок 2.8 — Зашифрований чат

При цьому Skype оперує лише зашифрованими повідомленнями (рисунок 2.9).

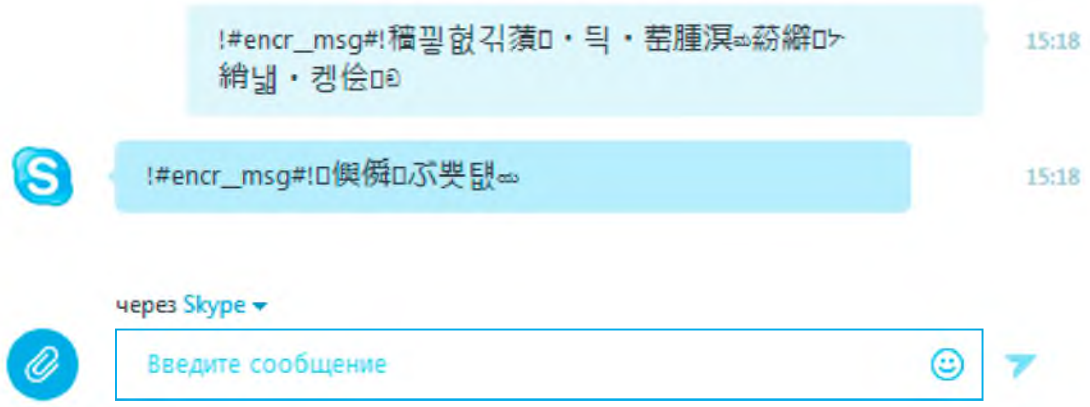

Рисунок 2.9 — Обмін зашифрованими повідомленнями

На рисунку 2.10 представлений зашифрований обмін повідомленнями у груповому чаті.

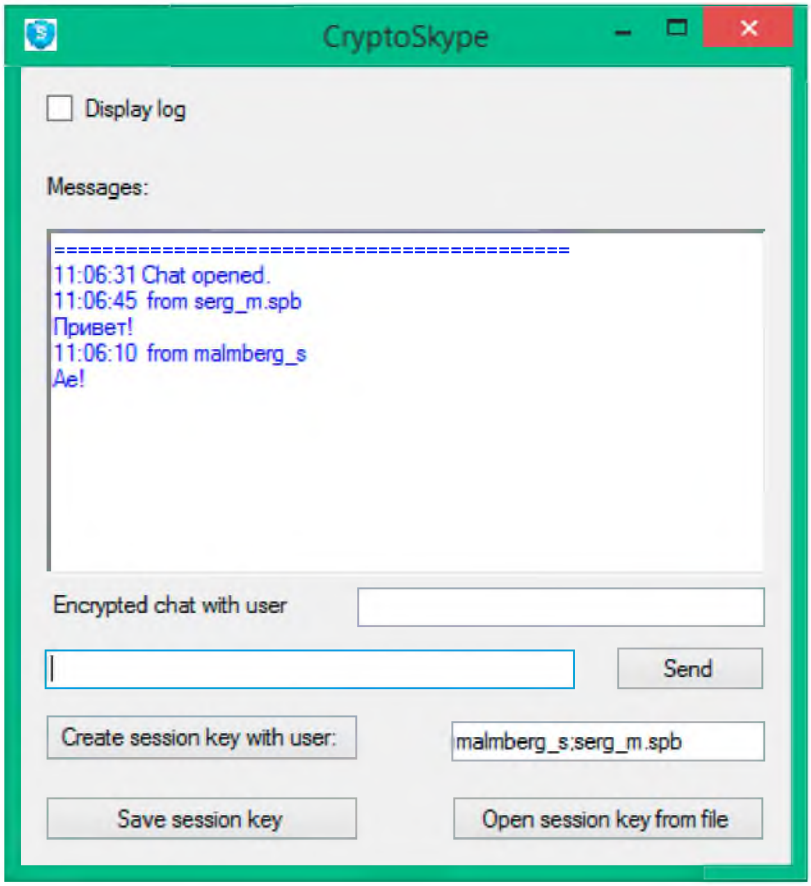

Рисунок 2.10 — Обмін зашифрованими повідомленнями у груповому чаті

2.2.4 Результати

Опишемо підсумкову схему роботи програмного засобу.

При передачі (рисунок 2.11) повідомлення вводяться у вікні розробленої програми, зашифровуються і далі передаються програмний клієнт Skype. Потік даних із мікрофона перехоплюється та зашифровується перед відправкою.

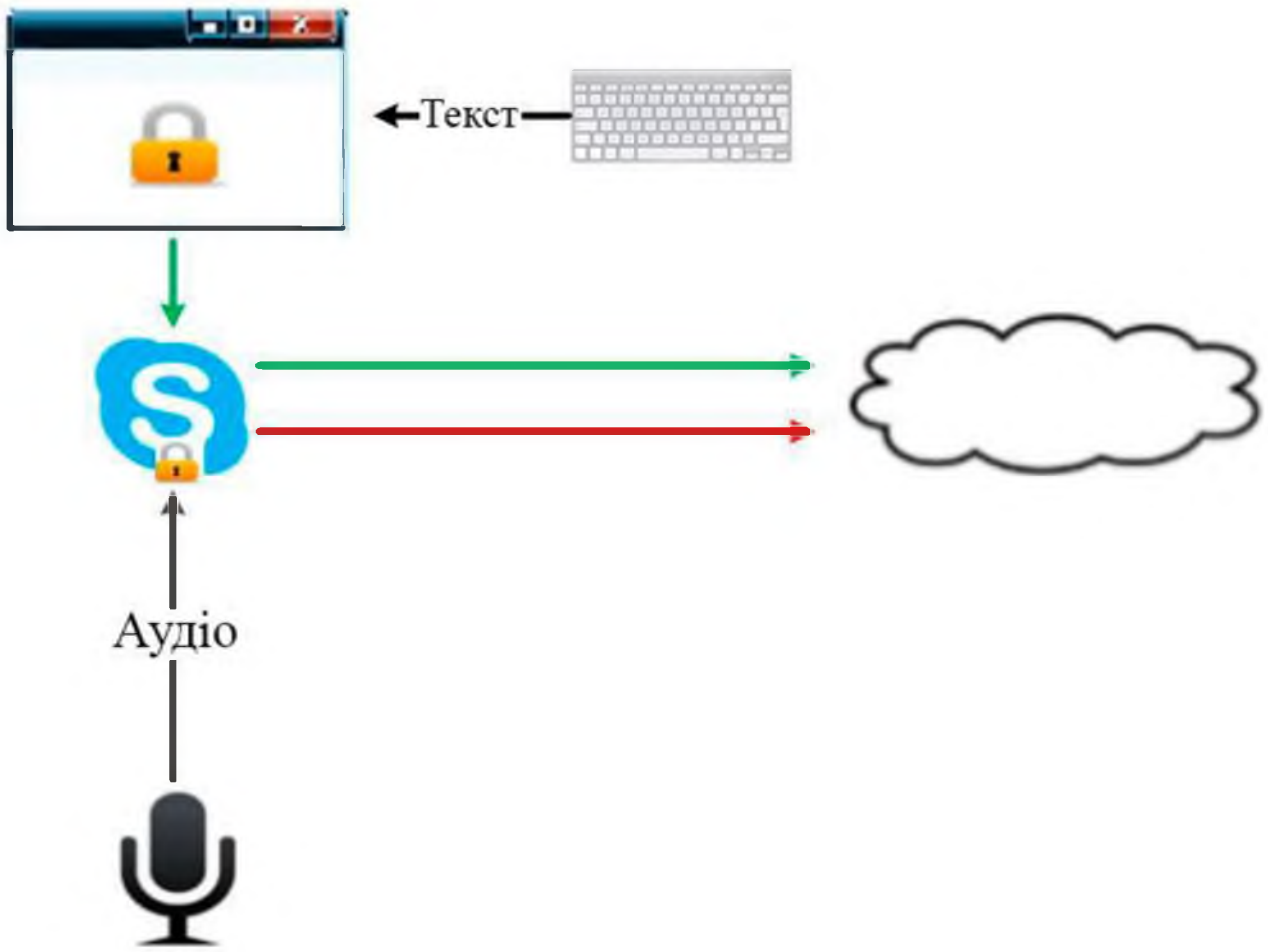

Рисунок 2.11 — Передача зашифрованих даних

На стороні, що приймає (рисунок 2.12), здійснюється розшифрування отриманого по мережі аудіопотоку. Отримані зашифровані повідомлення передаються у програмний засіб, де відображаються у розшифрованому вигляді.

Рисунок 2.12 — Прийом та розшифрування даних

Для роботи програмного засобу необхідно дозволити використовувати Skype. Це можна зробити після запуску програми у головному вікні програмного клієнта Skype (рисунок 2.13)

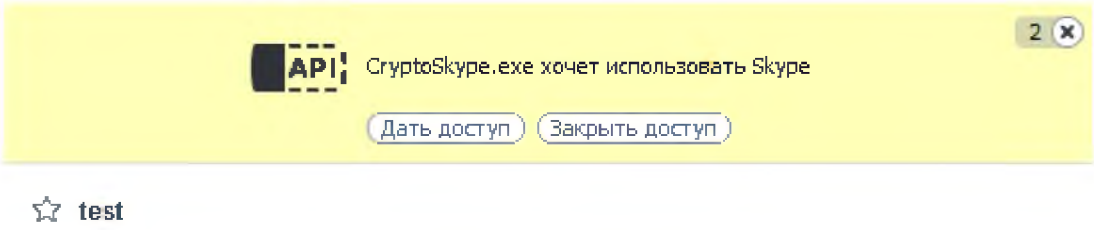

Рисунок 2.13 — Запит на отримання доступу до програмного засобу Skype

2.2.4.1 Оцінка тимчасових затримок

Проведемо оцінку тимчасових затримок під час використання шифрування для різних конфігурацій комп'ютера, а саме:

1. Низька потужність.

ОС: Windows 7 Starter; CPU: Intel Atom 1.5 ГГЦ; ОЗУ: 2 ГБ

2. Середня потужність.

ОС: Windows 7 Professional; CPU: Intel Core i5 3.0 ГГЦ; ОЗУ: 8 ГБ

3. Висока потужність.

ОС: Windows 8.1; CPU: Intel Core i7 3.1 ГГЦ; ОЗУ: 16 ГБ

У таблиці 2.1 представлена середня тимчасова затримка, виражена у відставанні звуку від відео, різних конфігурацій.

Таблиця 2.1 — Оцінка тимчасових затримок

Конфігурація	Тимчасова затримка, с
Низька потужність	0,4
Середня потужність	10^{-1}
Висока потужність	10^{-2}

З наведеної таблиці 2.1 видно, що некомфортне спілкування під час використання шифрування може бути лише за використанням комп'ютера низької потужності. В інших випадках шифрування не завдає незручностей при спілкуванні.

2.2.4.2 Оцінка навантаження

Проведемо оцінку навантаження з використанням шифрування та без нього для конфігурацій із попереднього пункту.

На рисунку 2.14 показано навантаження на комп'ютер низької потужності, яке надає програмний клієнт Skype з використанням шифрування та без нього, а також загальне навантаження на комп'ютер. При цьому навантаження на процесор, яке виробляється програмним засобом, становить 5%.

Рисунок 2.14 — Оцінка навантаження на комп'ютер низької потужності

На рисунку 2.15 показано навантаження на комп'ютер середньої потужності, яке надає програмний клієнт Skype з використанням шифрування та без нього, а також загальне навантаження на комп'ютер. При цьому навантаження на процесор, яке виробляється програмним засобом, становить 3%.

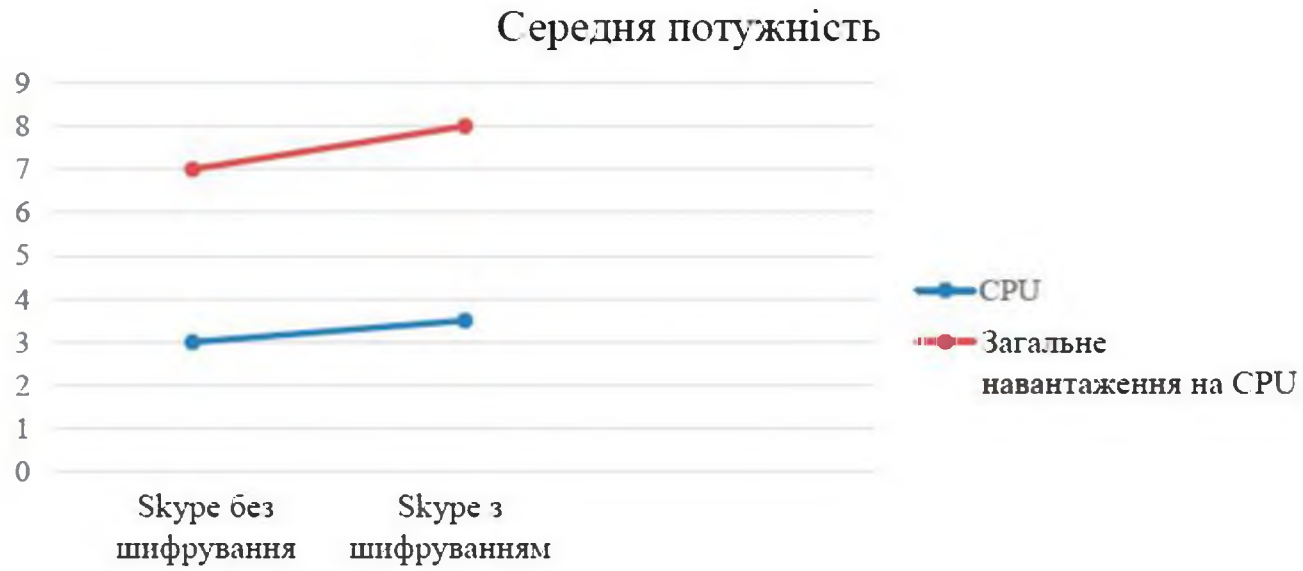

Рисунок 2.15 — Оцінка навантаження на комп'ютер середньої потужності

На рисунку 2.16 показано навантаження на комп'ютер високої потужності, яке надає програмний клієнт Skype з використанням шифрування та без нього, а

також загальне навантаження на комп'ютер. При цьому навантаження на процесор, яке виробляється програмним засобом, становить 1%.

Рисунок 2.16 — Оцінка навантаження на комп'ютер високої потужності

Таким чином, навантаження на комп'ютер не є критичним в жодному випадку, а для конфігурацій середньої та високої потужності вона незначна.

2.3 Забезпечення захищеності голосового трафіку у VOIP

Описаний у попередньому розділі програмний засіб крім зазначеного недоліку має ще один – його можна використовувати тільки з клієнтом Skype.

Тому розглянемо можливість створення засобу, що забезпечує безпечну передачу голосу без використання програмних інтерфейсів, що надаються VoIP-клієнтом, так щоб його можна було використовувати з будь-яким VoIP-клієнтом.

2.3.1 Засіб захисту голосу, що передається будь-яким VoIP-клієнтом

Для того, щоб реалізувати засіб, що забезпечує безпечну передачу голосового трафіку за допомогою будь-якого VoIP-клієнта, необхідно працювати на рівні драйверів.

Новий підхід має передбачати можливість зашифрування та розшифрування

аудіопотоку віртуальним аудіо драйвером.

2.3.2 Віртуальний аудіопристрій

Поставлене завдання можна вирішити при використанні такої архітектури (рисунок 2.17), при якій програмний клієнт VoIP відправляє аудіопотік спочатку на віртуальний аудіопристрій, на якому відбувається розшифрування, а потім розшифрований аудіосигнал надходить на динаміки. Відповідно для зашифрування аудіосигналу він повинен надходити з мікрофона на віртуальний пристрій, що робить зашифрування, а потім VoIP-клієнт.

Таке рішення можна використовувати в будь-якому VoIP-клієнті у зв'язку з тим, що в них існує можливість вибору пристрою запису та пристрою відтворення.

На рисунку 2.17 схематично показано використання такого підходу у різних VoIP-клієнтах, а саме Skype та Cisco Jabber Video for TelePresence (рисунок 2.18).

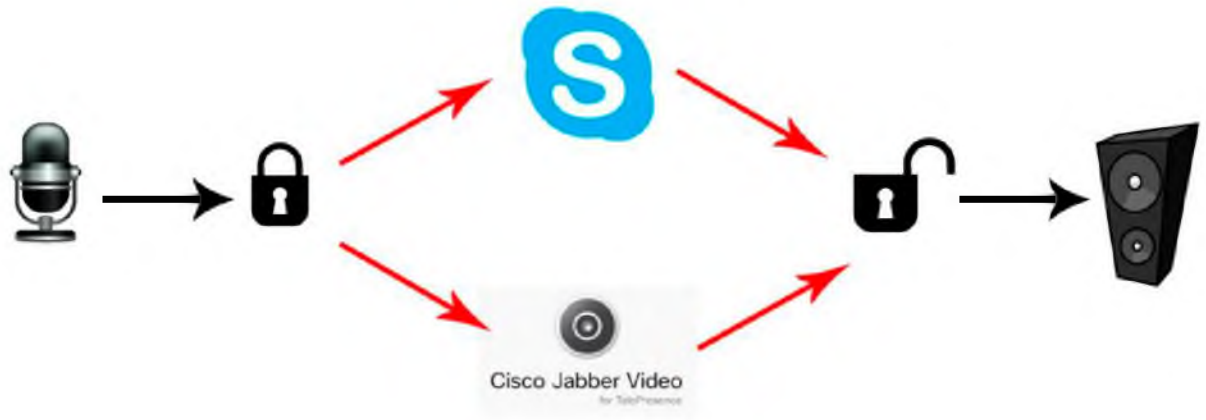

Рисунок 2.17 — Забезпечення захищеної передачі голосу за допомогою віртуального аудіопристрою

Рисунок 2.18 — Інтерфейс програми Cisco Jabber Video for TelePresence

Для реалізації запропонованої архітектури необхідно, щоб віртуальний аудіопристрій мав можливість обміну звуковими потоками між вхідним та вихідним інтерфейсами, тобто. між динаміком та мікрофоном (рисунок 2.19).

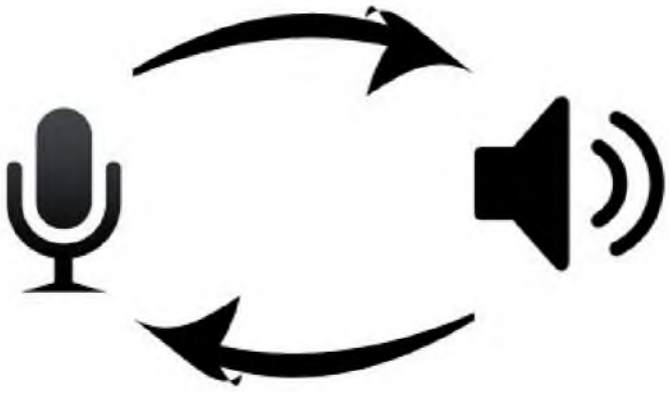

Рисунок 2.19 — Обмін потоками між вхідним та вихідним інтерфейсами

аудіопристрою

Такий підхід дозволяє зашифрувати або розшифрувати сигнал під час обміну потоками між вхідним і вихідним інтерфейсами аудіопристрою (рисунок 2.20).

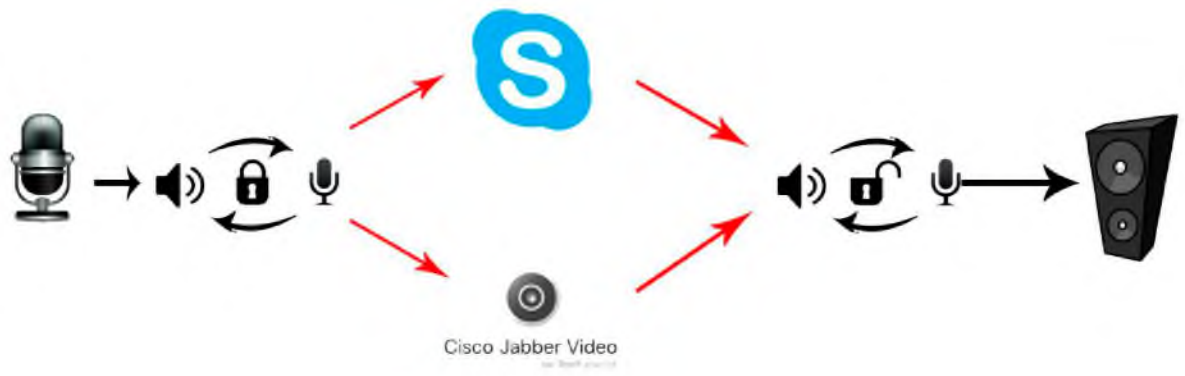

Рисунок 2.20 — Зашифрування та розшифрування голосу віртуальним аудіопристроєм

2.3.3 Розробка драйвера Windows

Програмістам надається ряд засобів для розробки драйверів Windows, наприклад Windows Driver Kit (WDK).

До складу засобів WDK входить, зокрема, ряд прикладів драйверів.

Для вирішення поставленого завдання скористаємося одним із них, а саме Microsoft Virtual Audio Device Driver Sample – simple.

При цьому існує ряд відкритих проектів розробки та модифікації драйверів з відкритим вихідним кодом. Реалізувати віртуальний аудіопристрій для вирішення поставленого завдання будемо на основі одного з них, а саме LoopbackAudioDriver.

Для обміну потоками між інтерфейсами використовуватимемо функції CopyFrom та CopyTo.

```
STDMETHODIMP_(void) CMiniportWaveCyclicStream::CopyFrom(
    IN PVOID Destination,
```

```
        IN ULONG ByteCount
    )
    {
     ULONG i = 0;
     ULONG FrameCount = ByteCount/2;
     if (!m_pMiniport->myBufferLocked)
     {
        while (i < FrameCount)
            {
                ((PWORD)Destination)[i]=((PWORD)m_pMiniport-
                >myBuffer)[m_pMiniport->myBufferReadPos];
                i++;
                m_pMiniport->myBufferReadPos++;
            }
            Encrypt(Destination,key,FrameCount);
        }
    }
```

У функції CopyFrom для віртуального пристрою введення ми отримуємо потік даних із віртуального мікрофона та робимо його зашифрування. Для віртуального пристрою виведення відповідно проводиться розшифрування.

```
STDMETHODIMP_(void) CMiniportWaveCyclicStream::CopyTo(
    IN PVOID Source,
    IN ULONG ByteCount
)
{
    ULONG i = 0;
    ULONG FrameCount = ByteCount/2;
    if (!m_pMiniport->myBufferLocked)
    {
        while (i < FrameCount)
        {
          ((PWORD)m_pMiniport->myBuffer)[m_pMiniport-
    >myBufferWritePos]=((PWORD)Source)[i];
          i++;
          m_pMiniport->myBufferWritePos++;
        }
    }
```

```
}
```

У функції CopyTo потік із віртуального мікрофона передається на віртуальні динаміки.

2.3.4 Ключ шифрування

На цьому етапі роботи окреме рішення для встановлення сеансового ключа не розроблялося.

Для зашифрування та розшифрування голосу тут можна використовувати сеансовий ключ, згенерований сторонніми програмами, наприклад, програмним засобом, розробленим у попередньому розділі.

Файл із ключовою інформацією повинен розташовуватися в папці C:\Windows та називатися audio.

Коли віртуальний динамік починає надходити звук, відбувається зчитування ключа з файла.

```
UNICODE_STRING uniName;
OBJECT_ATTRIBUTES objAttr;
RtlInitUnicodeString(&uniName, L"\\DosDevices\\C:\\WINDOWS\\audio");
InitializeObjectAttributes(&objAttr, &uniName,
                                        OBJ_CASE_INSENSITIVE |
                                OBJ_KERNEL_HANDLE,
                                        NULL, NULL);
LARGE_INTEGER byteOffset;
CHAR buffer[KEY_SIZE];
size_t cb;
HANDLE handle;
NTSTATUS ntstatus;
IO_STATUS_BLOCK ioStatusBlock;
```

```
        ntstatus = ZwCreateFile(&handle,
                                        GENERIC_READ,
                                        &objAttr, &ioStatusBlock,
                                        NULL,
                                        FILE_ATTRIBUTE_NORMAL,
                                        0,
                                        FILE_OPEN,
                                        FILE_SYNCHRONOUS_IO_NONALERT,
                                        NULL, 0);
        if(NT_SUCCESS(ntstatus))
        {
                byteOffset.LowPart = byteOffset.HighPart = 0;
                        ntstatus = ZwReadFile(handle, NULL, NULL, NULL, &ioStatusBlock,
                                        buffer, KEY_SIZE, &byteOffset, NULL);
                        if(NT_SUCCESS(ntstatus))
                        {
                                buffer[KEY_SIZE-1] = '\0';
                                for (int i = 0; i < KEY_SIZE; i++)
                        {
                                        key[i] = (INT)buffer[i];
                        }
                }
        ZwClose(handle);
}
```

2.3.5 Результати

Скомпілювавши віртуальний драйвер за допомогою Windows Build Utility (Build.exe), отримуємо файл cryptoaudio.sys.

Для його встановлення використовуємо cryptoaudio.inf файл (додаток Е) та утиліту DevCon:

```
devcon install cryptoaudio.inf *cryptoInput
devcon install cryptoaudio.inf *cryptoOutput
```

Після встановлення в диспетчері пристроїв з'являються пристрої CRYPTO INPUT і CRYPTO OUTPUT (рисунок 2.21).

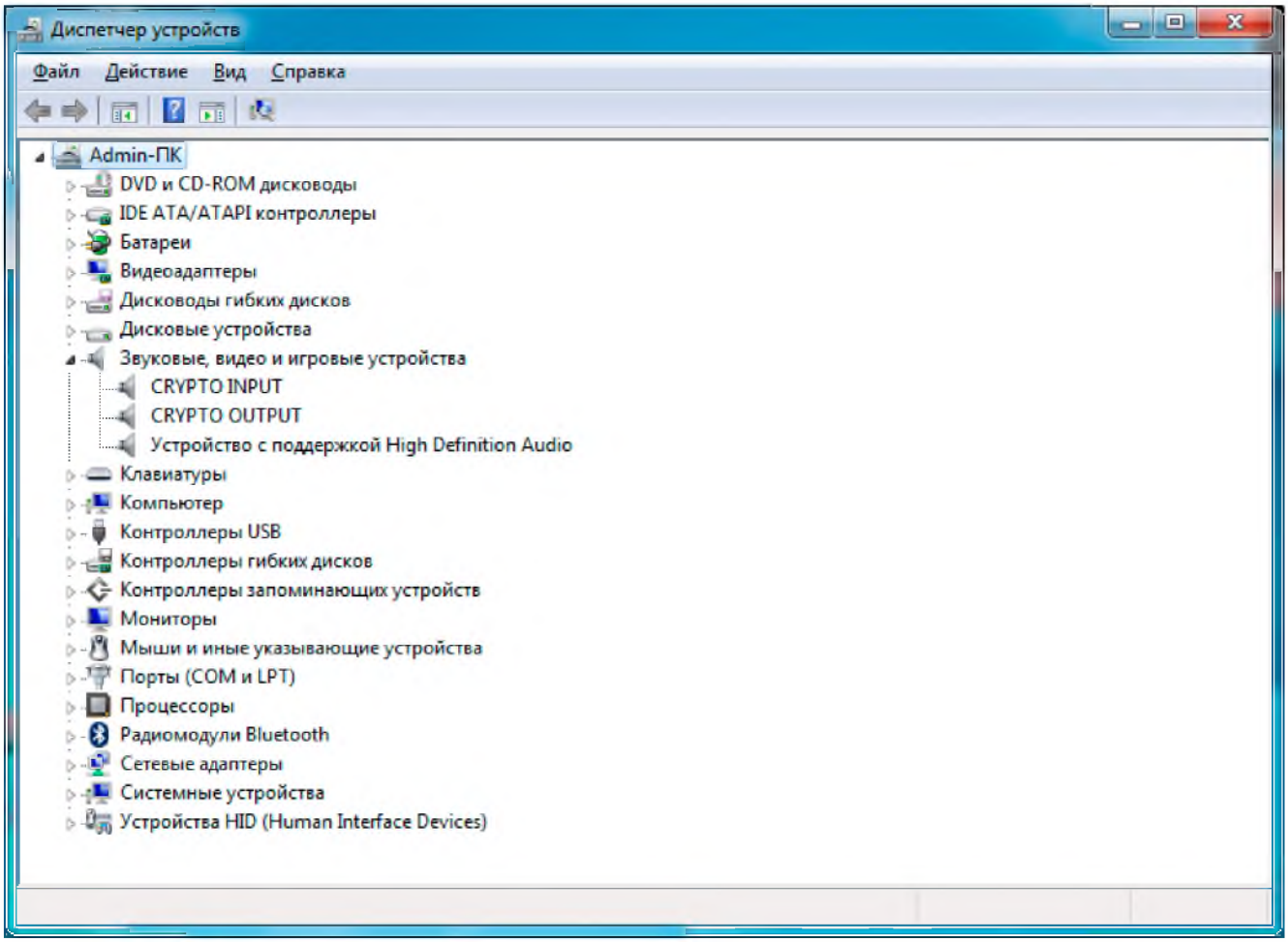

Рисунок 2.21 — Віртуальні аудіопристрої в диспетчері пристроїв Windows

Тепер дані аудіопристрої доступні для вибору у VoIP-клієнті, наприклад, Skype (рисунок 2.22) або Cisco Jabber Video for TelePresence (рисунок 2.23).

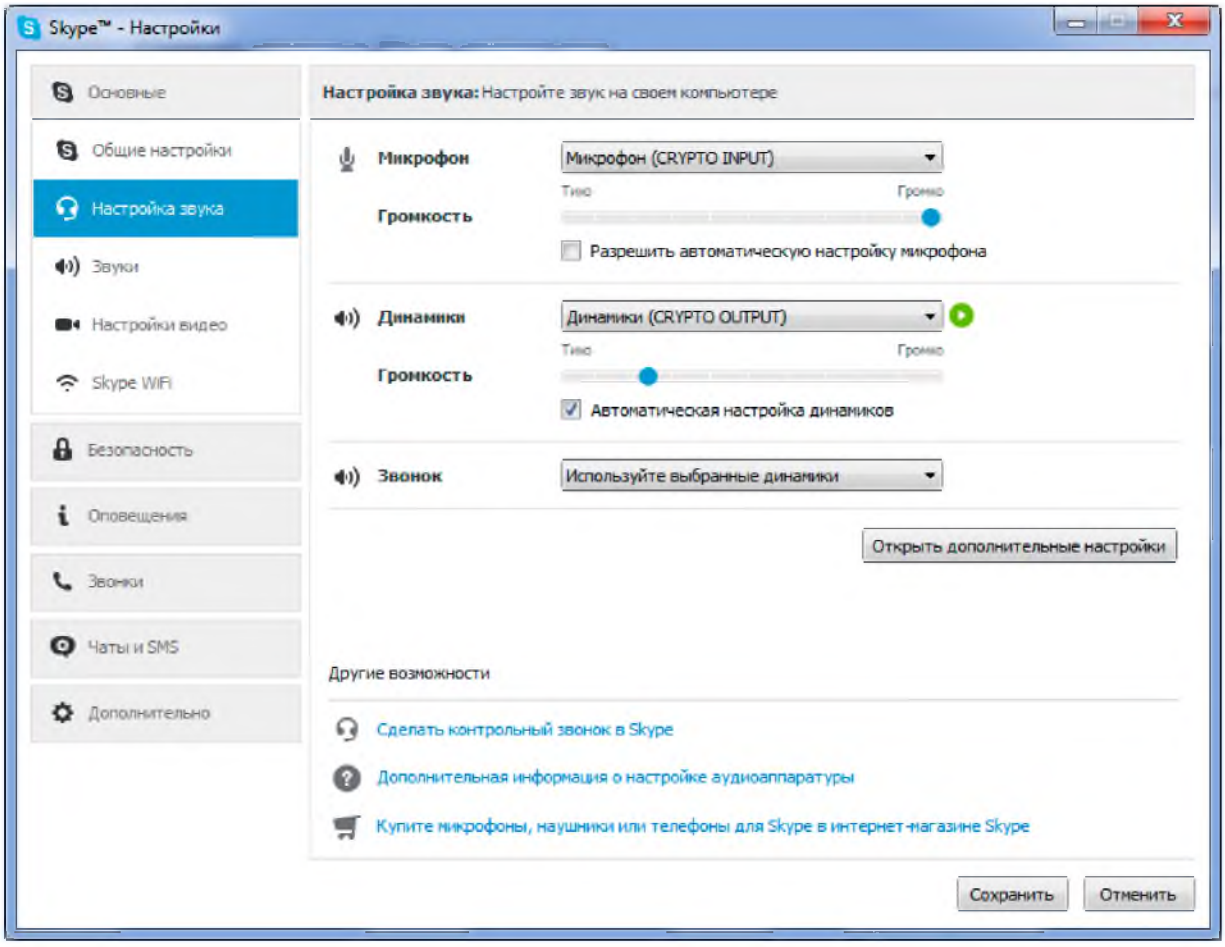

Рисунок 2.22 — Віртуальні аудіопристрої в Skype

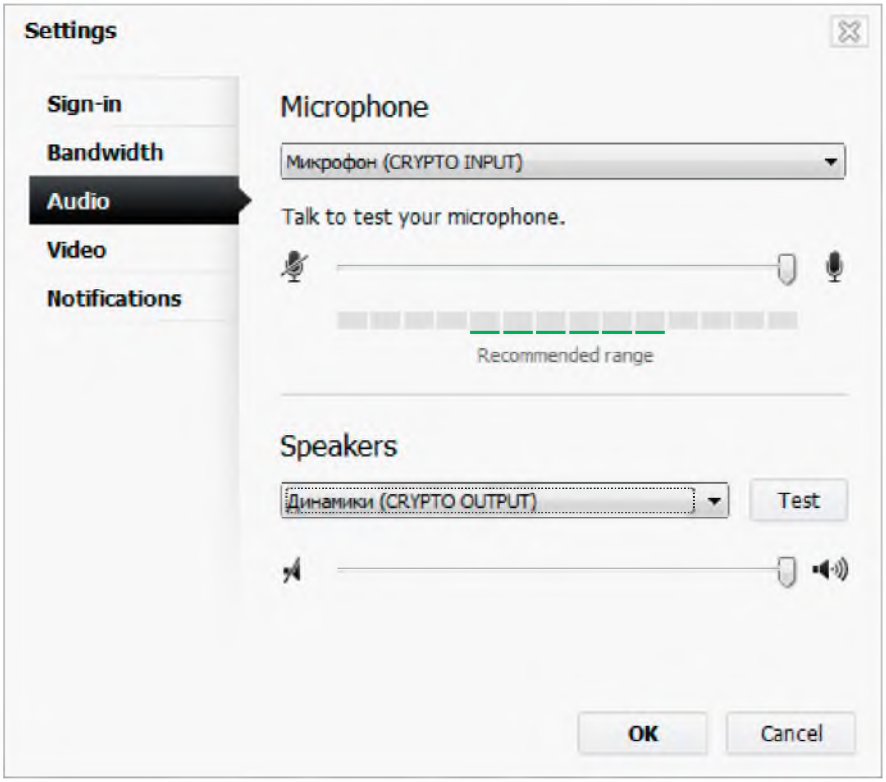

Рисунок 2.23 — Віртуальний аудіопристрій у Cisco Jabber Video for TelePresence

Для того, щоб подати на віртуальний мікрофон потік із реального мікрофона та з віртуальних динаміків на реальні – скористаємося стороннім додатком Audio Repeater 1.51.

З його допомогою перенаправимо потік з мікрофона на віртуальний пристрій CRYPTO INPUT (рисунок 2.24).

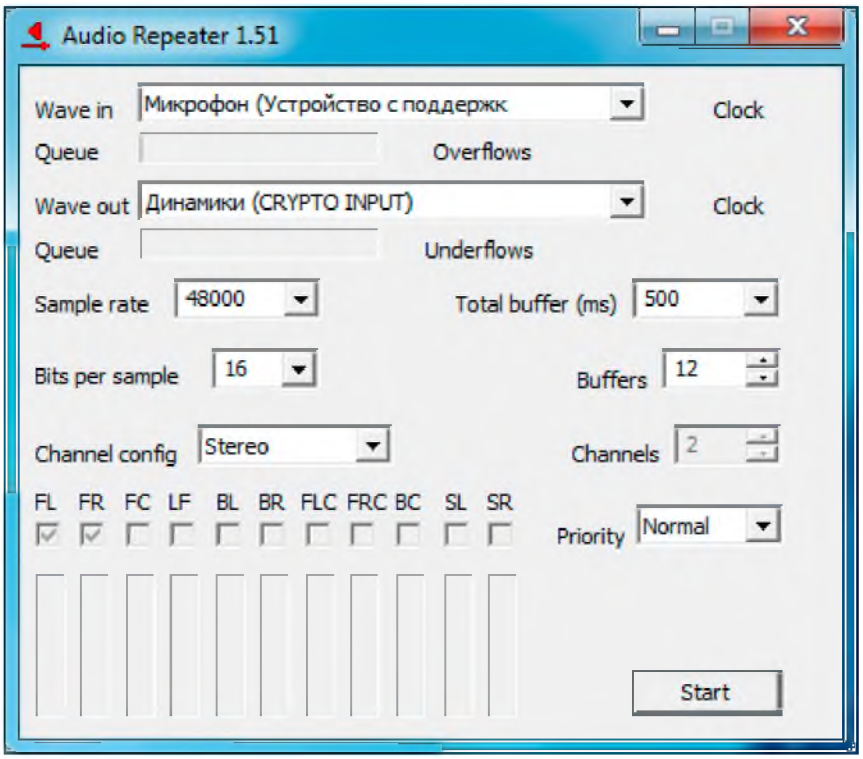

Рисунок 2.24 — Перенаправлення потоку з мікрофона на віртуальний аудіопристрій

Також необхідно перенаправити потік із віртуального пристрою CRYPTO OUTPUT на динаміки (рисунок 2.25).

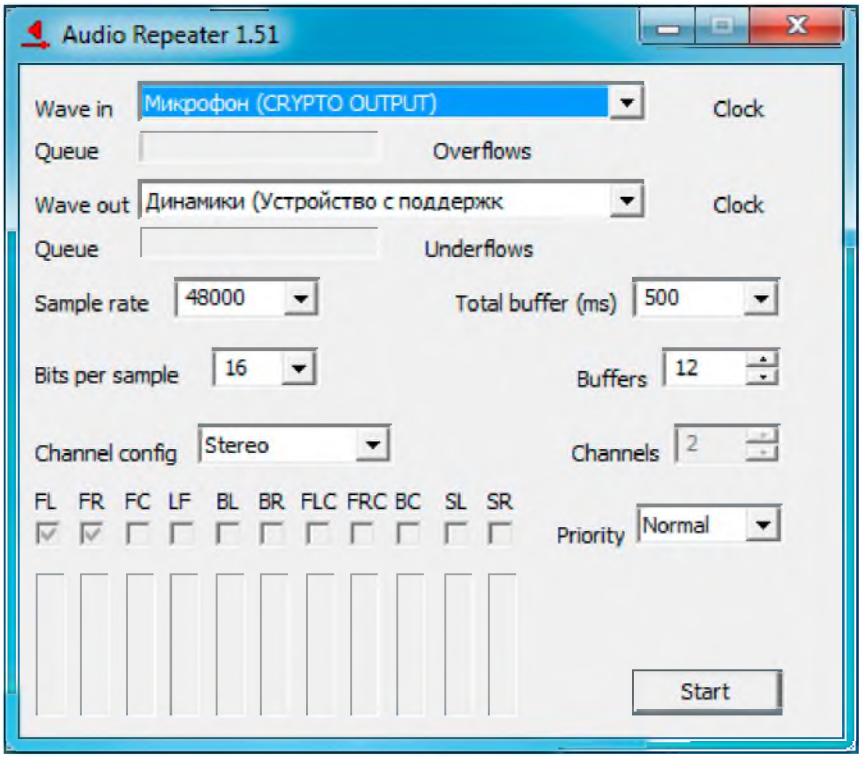

Рисунок 2.25 — Перенаправлення потоку з віртуального аудіопристрою на динаміки

В результаті VoIP-клієнти оперують зашифрованим голосовим трафіком. Це спричинило деякі проблеми.

Справа в тому, що Skype перед шифруванням проводить ряд маніпуляцій з голосовим потоком, спрямованих, швидше за все, на його стиснення, тобто. Практично передається видозмінений початковий сигнал. Це пояснює той факт, що голос при спілкуванні за допомогою Skype завжди дещо відрізняється від оригінального.

Тому при розшифруванні переданого сигналу на стороні, що приймає, виходить сигнал відмінний від переданого, який не можна сприймати комфортно.

У той же час, при спілкуванні за допомогою Cisco Jabber Video for TelePresence голос передається в дуже високій якості, завдяки цьому при використанні запропонованого підходу безпечної передачі голосу досягається комфортне сприйняття розшифрованої інформації.

2.3.5.1 Оцінка тимчасових затримок

Проведемо оцінку тимчасових затримок під час використання шифрування щодо різноманітних конфігурацій комп'ютера, описаних у пункті 2.2.4.1.

У таблиці 2.2 представлена середня тимчасова затримка, виражена у відставанні звуку від відео, різних конфігурацій.

Таблиця 2.2 — Оцінка тимчасових затримок

Конфігурація	Тимчасова затримка, с
Низька потужність	0,8
Середня потужність	0,4
Висока потужність	10^{-1}

З наведеної таблиці 2.2 видно, що некомфортне спілкування під час використання шифрування може бути при використанні комп'ютера низької потужності. Також деякі незручності можуть виникати у разі середньопотужного комп'ютера. При використанні комп'ютера високої потужності затримки зводяться до мінімуму.

2.3.5.2 Оцінка навантаження

Проведемо оцінку навантаження з використанням шифрування та без нього для конфігурацій із пункту 2.2.4.1.

На рисунку 2.26 показано загальне навантаження на комп'ютер низької потужності під час використання шифрування та без нього.

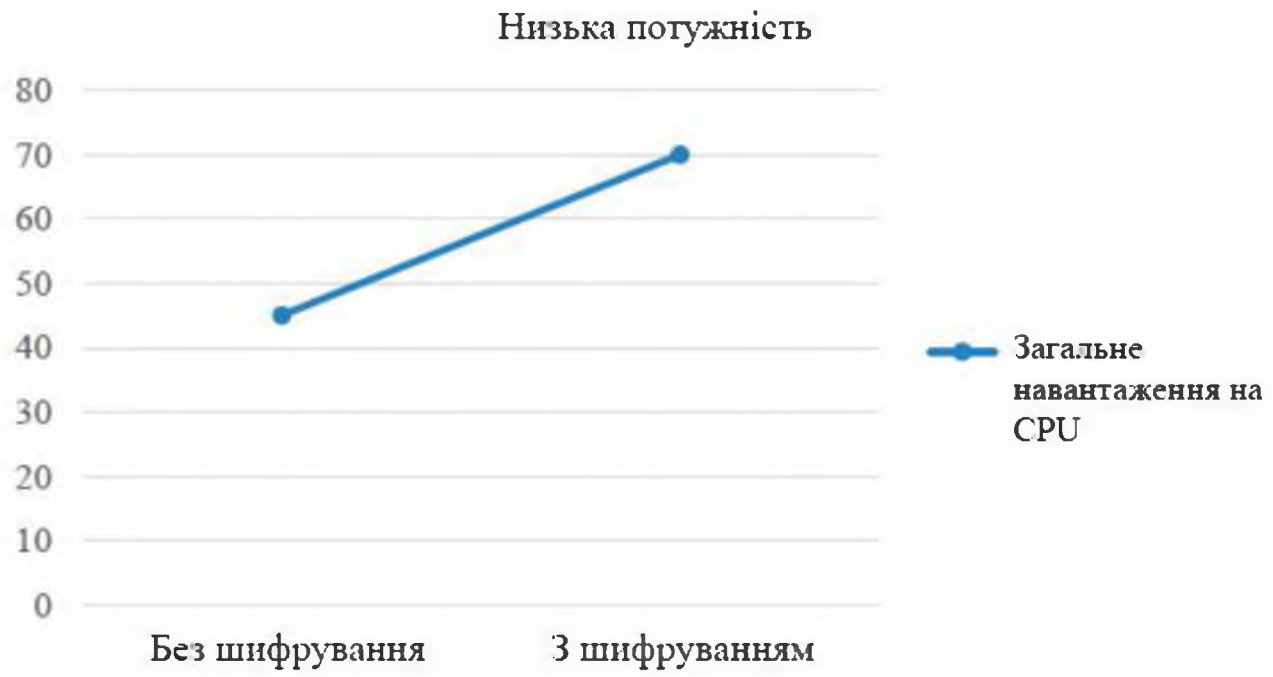

Рисунок 2.26 — Оцінка навантаження на комп'ютер низької потужності

На рисунку 2.27 показано загальне навантаження на комп'ютер середньої потужності при використанні шифрування та без нього.

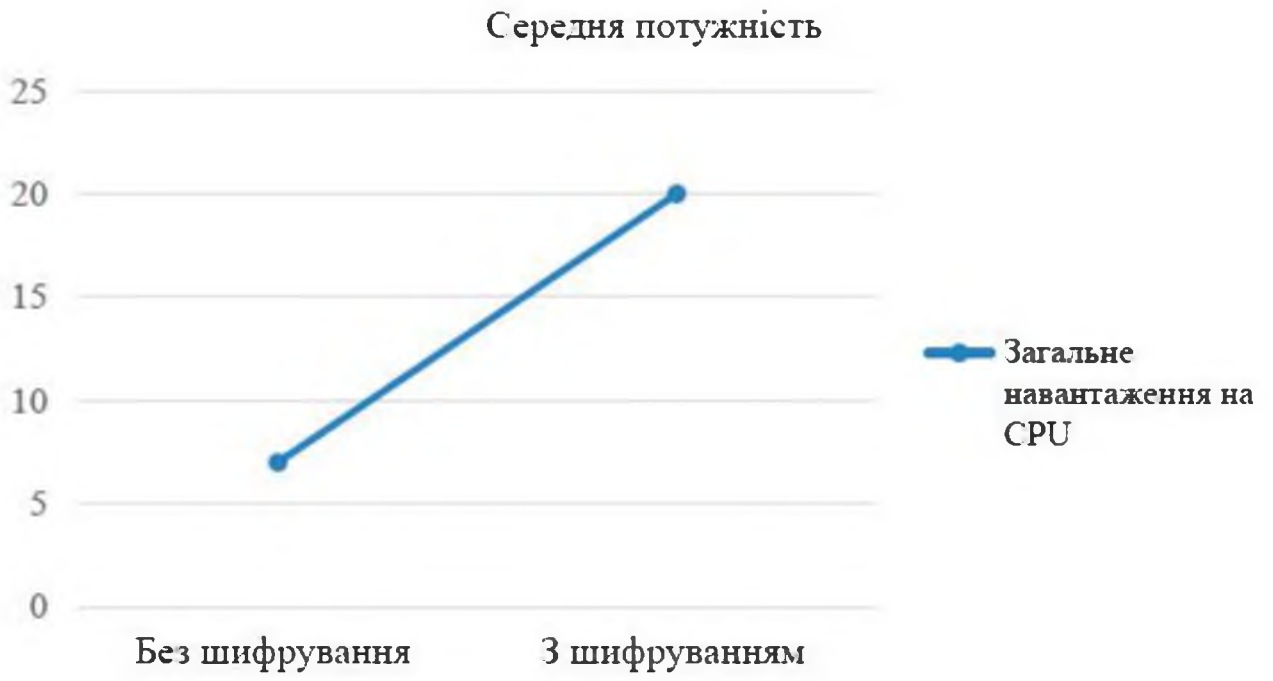

Рисунок 2.27 — Оцінка навантаження на комп'ютер середньої потужності

На рисунку 2.28 показано загальне навантаження на комп'ютер високої потужності під час використання шифрування та без нього.

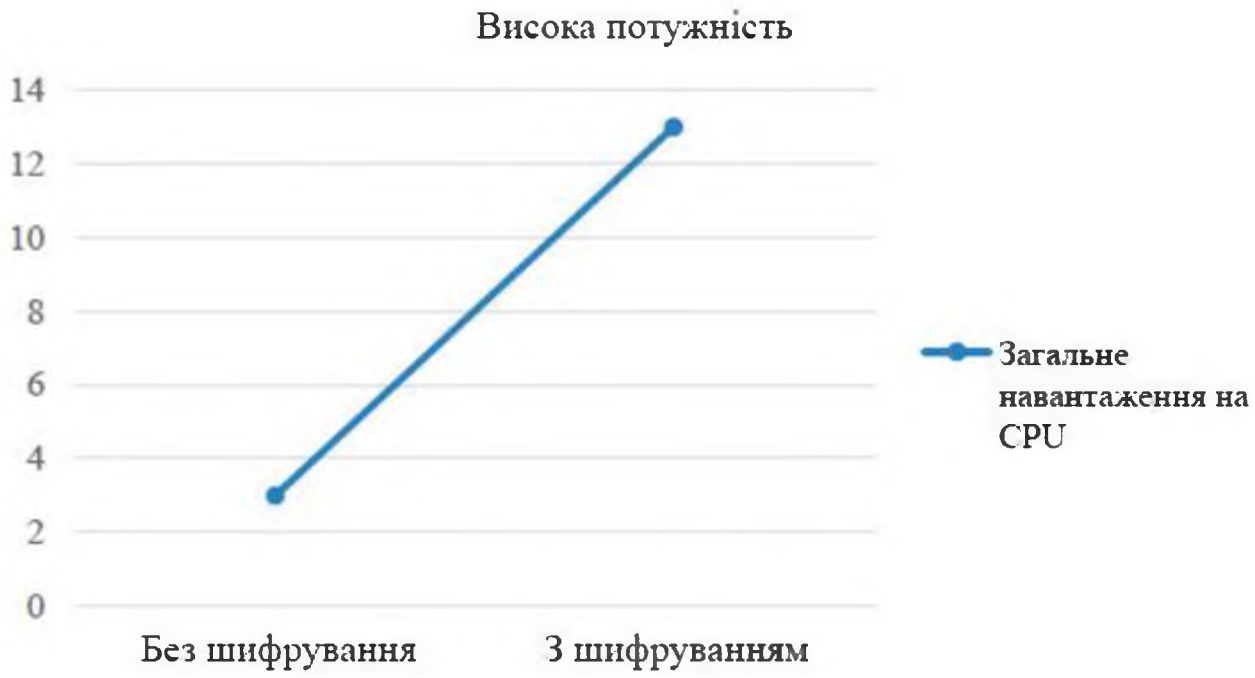

Рисунок 2.28 — Оцінка навантаження на комп'ютер високої потужності

Таким чином, навантаження на комп'ютер можна вважати критичним тільки для комп'ютера низької потужності, а для конфігурацій середньої та високої потужності воно невелике.

2.4 Висновок

Розроблений засіб в розділі 2.2 дозволяє захистити голосові дані, що передаються за допомогою Skype, від прослуховування навіть корпорацією Microsoft у зв'язку з тим, що програмні клієнти Skype оперують вже зашифрованим трафіком. Це робить результат цієї роботи засобом гарантовано безпечної передачі даних у Skype, аналогів якому немає у вільному доступі.

Проте водночас має серйозний недолік.

Справа в тому, що розроблений програмний засіб використовує програмний інтерфейс Skype. Без цього функціонування програми неможливе, що робить

розроблений засіб вкрай залежним від підтримки Skype API.

У випадку, якщо корпорацією Microsoft буде прийнято рішення про обмеження або повне закриття програмного інтерфейсу Skype, можливість гарантованого безпечного спілкування за допомогою Skype буде втрачена.

Тому подальшим напрямком роботи буде забезпечення безпечної передачі голосу без опори на програмний інтерфейс, який надається VoIP-клієнтом.

Розроблений засіб у розділі 2.3 дозволяє захистити голосовий трафік, що надсилається за допомогою IP-телефонії. При цьому відсутня залежність від будь-яких засобів розробки та інших інструментів, що надаються VoIP-клієнтами.

У той же час для використання цього засобу висуваються підвищені вимоги до передачі голосу через мережу. Не допускається сильне стискання потоку під час передачі, перешкоди та інші видозміни сигналу.

Цим вимогам можуть задовольнити лише спеціалізовані, корпоративні засоби VoIP, наприклад програмний клієнт Cisco Jabber Video for TelePresence.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

Метою розділу є обґрунтування економічної доцільності розробки політики забезпечення захищеності інформації, що передається через VoIP, та визначення витрат на проектування та експлуатацію цієї системи.

3.1 Визначення витрат на розробку політики забезпечення захищеності інформації VoIP

3.1.1 Визначення трудомісткості розробки та розрахунок витрат на створення вимог

Трудомісткість створення вимог визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації за умови роботи одного робітника:

$T = t_{тз} + t_в + t_а + t_{вз} + t_{озб} + t_{овр} + t_д = 5 + 1{,}5 + 2 + 2 + 5 + 18 + 2 = 35{,}5$ годин

$t_{тз}$ – тривалість складання технічного завдання на розробку політики забезпечення захищеності інформації;

$t_в$ – тривалість розробки концепції у організації;

$t_а$– тривалість процесу аналізу ризиків;

$t_{вз}$– тривалість визначення вимог до заходів, методів та засобів забезпечення;

$t_{озб}$– тривалість вибору основних рішень з забезпечення;

$t_{овр}$– тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації;

$t_д$ – тривалість документального оформлення політики захищеності;

Витрати на створення вимог $К_{рп}$ складаються з витрат на заробітну плату спеціаліста $З_{зп}$ і вартості витрат машинного часу, що необхідний для опрацювання програми на персональному комп'ютері $З_{мч}$:

$$К_{рп} = З_{зп} + З_{мч} = 3718{,}98 + 1149{,}85 = 4868{,}83 \text{ грн}$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальне потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) и визначається за формулою:

$$З_{зп} = t \cdot З_{іб} = 35{,}5 \cdot 104{,}76 = 3718{,}98 \text{ грн}$$

де t – загальна тривалість створення програмного забезпечення, годин;

Зіб – середньогодинна заробітна плата спеціаліста з інформаційної безпеки в Україні з нарахуваннями, грн/годину.

Вартість машинного часу для розробки вимог на персональному комп'ютері визначається за формулою:

$$З_{мч} = t \cdot С_{мч} = 35{,}5 \cdot 32{,}39 = 1149{,}85 \text{ грн}$$

де t – трудомісткість розробки вимог з інформаційної безпеки на ПК, годин;

$C_{мч}$ – вартість 1 години машинного часу персональному комп'ютері, грн./година.

Вартість 1 години машинного часу персонального комп'ютера визначається за формулою:

$$C_{мч} = P \cdot t_{нал} \cdot C_e + \frac{Ф_{зал} \cdot H_a}{F_p} + \frac{K_{лпз} \cdot H_{апз}}{F_p} = 0{,}45 \cdot 35{,}5 \cdot 1{,}68 + \frac{17200 \cdot 0{,}6}{2002} + \frac{3360 \cdot 0{,}24}{2002} =$$

$$26{,}84 + 5{,}15 + 0{,}40 = 32{,}39 \text{ грн/год}$$

де P – встановлена потужність персонального комп'ютера, кВт;

C_e – тариф на електричну енергію, грн/кВт·година;

$Ф_{зал}$ – залишкова вартість персонального комп'ютера на кінець року, грн.;

H_a – річна норма амортизації на персональному комп'ютері, частки одиниці;

$H_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$K_{лпз}$ – вартість ліцензійного програмного забезпечення, грн.;

F_p – річний фонд робочого часу (за 40 – годинного робочого тижня F_p = 2021 рік).

Таким чином, капітальні витрати на розробку та впровадження вимог складають 4868,83 грн.

3.1.2 Визначення та розрахунок витрат на придбання та збирання комп'ютера для програмування.

Капітальні витрати - грошові видатки, пов'язані з вкладенням в основний капітал чи в приріст виробничих запасів.

$$К_е = К_{пр} + К_м = 37858 + 600 = 38458 \text{ грн}$$

де $К_е$ – вартість витрат на придбання та встановлення системи відеоспостереження;

$К_{пр}$ – вартість придбання (таблиця 3.1);

$К_м$ – вартість монтажу.

Таблиця 3.1 - Витрати на матеріали і обладнання

Найменування обладнання та матеріалів	Кількість, шт	Вартість, грн	Сума, грн
Комп'ютер Asus ROG Strix G15DK-R5600X0870	1	25860	25860
Монітор Samsung Odyssey G3 F24G35TFW	2	5999	11998
Разом:			37858

Вище наведено таблицю з вартістю обладнання. Вартість збирання комплектуючих комп'ютера становитиме 600 грн.

Виходячи з розрахунків, загальні витрати на придбання та збирання комп'ютера для програмування складе 38458 грн.

3.1.3 Визначення та розрахунок витрат на впровадження антивірусу та систему захисту інформації від несанкціонованого доступу

Витрати на впровадження антивірусу та систему захисту інформації від несанкціонованого доступу визначаються за формулою:

$$К_{пу} = З_{зп} + З_{мч} + К_{пз} = 419,04 + 129,56 + 2510 = 3058,60 \text{ грн}$$

де $К_{пу}$- вартість впровадження технології;

$К_{пз}$ – вартість придбання ліцензійного ПЗ.

Трудомісткість впровадження програмного забезпечення наведена у таблиці 3.2.

Таблиця 3.2 - Трудомісткість впровадження антивірусу та систему захисту інформації від несанкціонованого доступу

Склад витрат	Трудомісткість, год-осіб	Вартість грн/год – осіб з податками	Сума, грн
Встановлення ПЗ	1	104,76	104,76
Налаштування ПЗ	3		314,28
Всього			419,04

Вартість машинного часу впровадження антивірусу та систему захисту інформації від несанкціонованого доступу на персональному комп'ютері визначається за формулою:

$$З_{мч} = t \cdot С_{мч} = 4 \cdot 32{,}39 = 129{,}56 \text{ грн}$$

де t – трудомісткість розробки вимог з інформаційної безпеки на ПК, годин;

$С_{мч}$ – вартість 1 години машинного часу персональному комп'ютері, грн./година.

Вартість 1 години машинного часу персонального комп'ютера розрахована в розділі 3.1.1 та становить 32,39 грн

Таким чином, впровадження антивірусу та систему захисту інформації від несанкціонованого доступу коштуватиме підприємству 3058,60 грн.

Отже, капітальні витрати складають 46385,43 грн.

3.2 Розрахунок поточних (експлуатаційних) витрат

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проектування за визначений період, що виражені у грошовій формі.

За методикою Gartner Group до поточних (експлуатаційних) варто відносити наступні витрати:

1. Вартість Upgrade – відновлення й модернізації системи ($С_в$);

2. Витрати на керування системою в цілому ($С_к$);

3. Витрати, викликані активністю користувачів системи ($С_{ак}$ – "активність користувача").

Під "витратами на керування системою" маються на увазі витрати, пов'язані з керуванням і адмініструванням серверів та інших компонентів системи. До цієї статті витрат можна віднести наступні витрати:

1. Навчання адміністративного персоналу й кінцевих користувачів;

2. Амортизаційні відрахування від вартості обладнання та програмного забезпечення;

3. Заробітна плата обслуговуючого персоналу;

4. Технічне й організаційне адміністрування й сервіс.

5. Щорічні витрати на експлуатацію заходів з підвищення забезпечення захищеності інформації, що передається через VoIP

3.2.1 Розрахунок поточних витрат на вимоги з забезпечення захищеності інформації, що передається через VoIP

У зв’язку зі швидким розвитком інформаційної інфраструктури та технологій необхідно підтримувати актуальність розроблених вимог забезпечення захищеності інформації, що передається через VoIP. Для цього потрібно кожні пів року розглядати документ та якщо необхідно вносити корективи до нього.

Таблиця 3.3 - Трудомісткість розгляду вимог на можливість внесення необхідних коректівів

Склад витрат	Трудомісткість, год-осіб	Вартість грн/год – осіб з податками	Сума, грн
Аналіз тенденцій	1	104,76	104,76
Розгляд існуючого документу	0,5		52,38
Можливе внесення коректівів	1	104,76	104,76
Всього			261,90

Поточні затрати на підтримання актуальності вимог з забезпечення захищеності інформації, що передається через VoIP становлять 261,90 грн.

3.2.2 Розрахунок поточних витрат при експлуатації комп'ютера для програмування

Витрати на поточний ремонт комп'ютера для програмування становить 5% від суми витраченої на обладнання спочатку.

$$C_{рем} = 0,05 * 37858 = 1892,90 \text{ грн.}$$

Витрати на матеріали, які споживаються протягом року, складають 1% від балансової вартості основного устаткування і складають 378,58 грн.

Виходячи з розрахунків наведених вище – поточні витрати при експлуатації комп'ютера для програмування становитимуть 2271,48 грн/рік.

3.2.3 Розрахунок поточних витрат при використанні антивірусу та систему захисту інформації від несанкціонованого доступу

Поточні (експлуатаційні) витрати використання антивірусу та систему захисту інформації від несанкціонованого доступу можна розрахувати за формулою:

$$С_п = С_л + С_о = 1600 + 205,72 = 1805,72 \text{ грн}$$

де $С_п$ – поточні витрати;

$С_л$ – витрати на продовження ліцензії;

$С_о$ – витрати на оновлення ПЗ;

Для розрахування витрат на оновлення ПЗ використовується формула:

$$С_о = З_{зп} + З_{мч} = 157,14 + 48,58 = 205,72 \text{ грн}$$

За умови, що трудомісткість оновлення складає 1,5 години.

Поточні (експлуатаційні) витрати використання антивірусу та систему захисту інформації від несанкціонованого доступу становлять 1805,72 грн.

3.2.4 Розрахунок амортизаційних відрахувань від вартості обладнання та програмного забезпечення

$$C_{воп} = (37858 + 1600) / 5 = 7891,60 \text{ грн}$$

3.2.5 Розрахунок поточних витрат на заробітну плату обслуговуючого персоналу

$$C_{зпо} = 261,90 * 12 * 1 = 3142,80$$

Щорічні витрати на експлуатацію заходів з підвищення захищеності інформації, що передається через VoIP та інформаційної безпеки в цілому розраховуються за формулою:

$$C = \sum С_п = 261,90 + 1892,90 + 1805,72 + 7891,60 + 3142,80 = 14994,92 \text{ грн}$$

3.3 Оцінка можливого збитку від атаки (злому) на вузол або сегмент корпоративної мережі.

Кінцевим результатом впровадження й проведення заходів щодо забезпечення захищеності інформації, що передається через VoIP та інформаційної безпеки в цілому є величина відвернених втрат, що розраховується, виходячи з імовірності виникнення інциденту інформаційної безпеки та можливих економічних втрат. Дана величина відображає частину прибутку, яка могла бути втрачена.

3.3.1 Оцінка величин збитків

Загалом можливо виділити такі види збитку, що можуть вплинути на ефективність комп'ютерної системи інформаційної безпеки (КСІБ):

1. Порушення конфіденційності ресурсів КСЗІ (тобто неможливість доступу до них неавторизованих суб'єктів або несанкціонованого використання каналів зв'язку);

2. Порушення доступності ресурсів КСЗІ (тобто можливість доступу до них авторизованих суб'єктів (завжди, коли їм це потрібно);

3. Порушення цілісності ресурсів КСЗІ (тобто їхня неушкодженість);

4. Порушення автентичності ресурсів КСЗІ (тобто їхньої дійсності, непідробленості).

Можна виділити й деякі універсальні форми нанесення збитку, наприклад, порушення конфіденційності, доступності, цілісності або автентичності ресурсу можна характеризувати як компрометацію ресурсу, тобто втрату довіри до нього користувачів (це може мати прямий збиток, зв'язаний, наприклад, з переустановленням програмного забезпечення або проведенням розслідування).

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки.

Необхідні вихідні дані для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, годин;

$З_о$ – місячна заробітна плата обслуговуючого персоналу (адміністраторів та ін.) з нарахуванням єдиного соціального внеску, грн на місяць;

$З_с$ – місячна заробітна плата співробітника атакованого вузла або сегмента корпоративної мережі з нарахуванням єдиного соціального внеску, грн на місяць;

Заробітна плата не повинна бути нижче мінімальної заробітної плати на 01 січня поточного року. Ставка єдиного соціального внеску 22% и більше згідно класу професійного ризику підприємства, на якому проводиться захист інформації.

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та програмних інженерів), осіб.;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, осіб.;

О – обсяг чистого прибутку/дохід від реалізації/ атакованого вузла або сегмента корпоративної мережі, грн у рік, або оподаткований прибуток атакованого вузла або сегмента корпоративної мережі;

$П_{зч}$ – вартість заміни встаткування або запасних частин, грн;

I – число атакованих вузлів або сегментів корпоративної мережі;

N – середнє число можливих атак на рік.

Упущена вигода від простою атакованого вузла або сегмента корпоративної мережі становить:

$$U = П_п + П_в + V = 6840 + 7852{,}84 + 7129{,}60 = 21822{,}44 \text{ грн}$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$П_п = \frac{\sum З_с \cdot Ч_с}{F} \cdot t_п = \frac{\sum 15\,960 \cdot 18}{168} \cdot 4 = 6840 \text{ грн}$$

де F – місячний фонд робочого часу (при 40 – а годинному робочому тижні становить 160 – 176 ч).

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч} = 1710 + 942{,}84 + 5200 = 7852{,}84 \text{ грн}$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ви} = \frac{\sum З_с \cdot Ч_с}{F} \cdot t_{ви} = \frac{\sum 15\,960 \cdot 18}{168} \cdot 1 = 1710 \text{ грн}$$

Витрати на відновлення вузла або сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньо годинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{пв} = \frac{\sum З_о \cdot Ч_о}{F} \cdot t_в = \frac{\sum 17\,599{,}68 \cdot 3}{168} \cdot 3 = 942{,}84 \text{ грн}$$

Втрати від зниження очікуваного обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із середньо годинного обсягу продажів і сумарного часу простою атакованого вузла або сегмента корпоративної мережі:

$$V = \frac{O}{F_г} \cdot (t_п + t_в + t_{ви}) = \frac{1\,925\,000}{2160} \cdot (4 + 3 + 1) = 7129{,}60 \text{ грн}$$

де $F_г$ – річний фонд часу роботи організації становить близько 2160 ч.

Таким чином, загальний збиток від атаки на вузол або сегмент корпоративної мережі організації складе:

$$B = \sum\sum U \cdot N \cdot I = \sum\sum 21822{,}44 \cdot 3 \cdot 1 = 65467{,}32 \text{ грн}$$

3.4 Загальний ефект від впровадження комплексу заходів

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки становить:

$$E = B \cdot R - C = 65467{,}32 \cdot 0{,}33 - 14994{,}92 = 6609{,}30 \text{ грн}$$

де B – загальний збиток від атаки на вузол або сегмент корпоративної мережі, тис. грн;

R – очікувана імовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці;

C – щорічні витрати на експлуатацію всіх заходів, тис. грн.

3.5 Визначення та аналіз показників економічної ефективності системи захищеності інформації, що передається через VoIP та інформаційної безпеки в цілому

Оцінка економічної ефективності системи захисту інформації та системи захищеності інформації, що передається через VoIP, розглянутої у спеціальній частині дипломного проекту, здійснюється на основі визначення та аналізу наступних показників:

1. Коефіцієнт повернення інвестицій (ROI). У сфері інформаційної безпеки йому відповідає показник ROSI (Return of Investment for Security).
2. Термін окупності капітальних інвестицій T_O.

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки.

Щодо до інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від атаки на сегмент або вузол корпоративної мережі, а отже:

$$\text{ROSI} = \frac{\text{E}}{\text{K}} = \frac{6609{,}30}{46385{,}43} = 0{,}14, \text{ частки одиниці}$$

де Е - загальний ефект від впровадження комплексу заходів (розділ 3.4), тис. грн;

К - капітальні інвестиції за варіантами, що забезпечили цей ефект, тис. грн.

Термін окупності капітальних інвестицій T_O показує, за скільки років

капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи:

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{0,14} = 7,1 \text{ , років}$$

3.6 Висновок

В даному розділі розглянуто техніко-економічний розрахунок модернізації системи забезпечення захищеності інформації, що передається через VoIP та програмного забезпечення на підприємстві ТОВ «Комунальні інформаційні системи», в тому числі визначено розмір необхідних витрат на закупівлю обладнання, розрахунок експлуатаційних витрат, а також проведено аналіз показників ефективності представленого проекту. Виходячи з вищевикладеного можна зробити наступний висновок: модернізація системи забезпечення захищеності інформації, що передається через VoIP та програмного забезпечення для організації ТОВ «Комунальні інформаційні системи» буде ефективна, так як загальний збиток від атаки на вузол або сегмент корпоративної мережі організації за рік може скласти 65467,32 грн. А після впровадження системи відеоспостереження та програмного забезпечення середній збиток за рік буде складати 6609,30 грн. Коефіцієнт повернення інвестицій ROSI дорівнює 0,14 частки одиниці. Капітальні інвестиції за рахунок загального ефекту від впровадження системи інформаційної безпеки окупляться за 7,1 років.

ВИСНОВКИ

У цій роботі було досліджено, проаналізовано та класифіковано загрози VoIP.

Окремо розглянуті проблеми протоколу Skype, найпоширенішого VoIP-клієнта у світі. Показано, що рівень безпеки Skype не є достатнім для безпечної взаємодії для передачі конфіденційних даних.

У зв'язку з викладеним, у цій роботі запропонований спосіб забезпечення безпечної взаємодії в рамках Skype, а саме використання кінцевого шифрування при передачі голосу та повідомлень.

Був розроблений програмний засіб, що реалізує зазначений підхід, та підтримує весь необхідний для безпечної взаємодії функціонал, а саме:

1. Встановлення сеансового ключа за класичним протоколом Діффі-Хеллмана із заданим абонентом.

2. Надсилання повідомлень, зашифрованих за алгоритмом симетричного шифрування ДСТУ ГОСТ 28147:2009 заданому абоненту.

3. Прийом зашифрованих повідомлень та їх розшифрування.

4. Встановлення сеансового ключа під час здійснення виклику.

5. Зашифрування вихідного аудіосигналу.

6. Розшифрування вхідного аудіосигналу.

В результаті було отримано засіб, що забезпечує безпечне спілкування через Skype.

Однак дослідження та розробка, що проводяться в рамках даної дипломної роботи, на цьому не закінчилася.

Була проаналізована можливість створення засобу, що забезпечує безпечне спілкування не лише через Skype, але й будь-якого іншого VoIP-клієнта.

Таку можливість було знайдено.

Для цього був використаний віртуальний аудіопристрій та реалізовані наступні функції:

1. Обмін звуковими потоками між вхідним та вихідним інтерфейсами, тобто між динаміком та мікрофоном.

2. Зашифрування або розшифрування сигналу під час обміну потоками між вхідним та вихідним інтерфейсами аудіопристрою.

В результаті був отриманий віртуальний аудіоприс трій, що реалізує кінцеве шифрування голосового трафіку, що передається. Для безпечної взаємодії за допомогою VoIP достатньо вибрати його як вхідний або вихідний аудіоінтерфейс.

Таким чином, у цій роботі були запропоновані способи досягнення безпечної передачі голосу за допомогою VoIP.

Також на підприємстві пропонується встановити антивірусне ПЗ та систему захисту від несанкціонованого доступу на основі програмного продукту Avast Endpoint Protection та СЗІ від НСД "Аура 1.2.4". Це робиться для комплпексного захисту інформації, що передається за допомогою VoIP.

При виборі технічних засобів особлива увага приділялася їх функціональних характеристик. Розроблений комплекс захисту інформації, що передається через VoIP відповідає поставленим вимогам і готовий до установки на підприємстві. Витрати на реалізацію заходів складають 38458 грн. Капітальні інвестиції за рахунок загального ефекту від впровадження системи інформаційної безпеки окупляться за 7,1 років.

ПЕРЛІК ПОСИЛАНЬ

1. Baset S., Schulzrinne H. An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol. Department of Computer Science Columbia University, New York 2004.

2. Does Skype use encryption? [Електронний ресурс] . ─ 2021 ─ Режим доступу до ресурсу: https://support.Skype.com/en/faq/FA31/does-Skype-use-encryption?q=security.

3. LoopbackAudioDriver. [Електронний ресурс] . – 2021 ─ Режим доступу до ресурсу: https://github.com/02strich/LoopbackAudioDriver.

4. Microsoft Virtual Audio Device Driver Sample. [Електронний ресурс]. – 2021 ─ Режим доступу до ресурсу: https://code.msdn.microsoft.com/windowshardware/virtual-audio-device-3d4e6150.

5. VoIP Security and Privacy Threat Taxonomy. [Електронний ресурс] . – 2021 ─ Режим доступу до ресурсу: http://www.voipsa.org/Activities/VOIPSA_Threat_Taxonomy_0.1.pdf.

6. Microsoft допомагав АНБ та ФБР шпигувати за користувачами Hotmail, Skype та Outlook [Електронний ресурс]. – 2021 – http://habrahabr.ru/post/186460/.

7. Skype with care – Microsoft is reading everything you write [Електронний ресурс]. – 2021 – http://www.h-online.com/security/news/item/Skype-with-care-Microsoft-is-reading-everything-you-write-1862870.html.

8. Skype and the Bavarian trojan in the middle [Електронний ресурс]. – 2021 – http://wikileaks.org/wiki/Skype_and_the_Bavarian_trojan_in_the_middle.

9. Skype захопив 40% міжнародних розмов [Електронний ресурс]. – 2021 – http://www.white-windows.ru/skype-zakhvatil-40-mezhdunarodnykh-razgovorov/.

10. Skype змінює топологію своєї мережі [Електронний ресурс]. – 2021 –

https://minfin.com.ua/amp/2012/05/02/584147/.

11. Skype невразливий? Міф! [Електронний ресурс]. – 2021 – http://discussiya.com/2012/09/17/Skype-securiry/.

12. System.Net.Sockets – простір імен. [Електронний ресурс]. – 2021 – https://docs.microsoft.com/ru-ru/dotnet/api/system.net.sockets?redirectedfrom=MSDN&view=net-6.0.

13. 5 common VoIP security risks that might threaten your business [Електронний ресурс]. – 2021 – https://www.cloudtalk.io/blog/5-common-voip-security-risks-that-might-threaten-your-business.

14. VoIP Security and Privacy Threat Taxonomy. [Електронний ресурс]. – 2021 – http://www.voipsa.org/Activities/VOIPSA_Threat_Taxonomy_0.1.pdf.

15. Voice Security Primer: Protecting the Voice Infrastructure, Call-Management System, Applications, and Endpoints. [Електронний ресурс]. – 2021 – https://info.calltower.com/hubfs/Cisco%20Rated%20Top%20Secure%20voice%20platform.pdf.

16. WDK, debugging tools, and driver samples. [Електронний ресурс]. – 2021 – https://developer.microsoft.com/ru-ru/windows/hardware/.

17. ДСТУ ГОСТ 28147 – 2009. Система обробки інформації. Криптографічний захист інформації. Алгоритм криптографічного перетворення. [Електронний ресурс]. – 2021 – https://usts.kiev.ua/wp-content/uploads/2020/07/dstu-host-28147-2009.pdf.

18. Положення про конфіденційність корпорації Microsoft. [Електронний ресурс]. – 2021 – https://privacy.microsoft.com/ru-ru/privacystatement.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	2	
3	А4	Зміст	2	
4	А4	Вступ	3	
5	А4	1 Розділ	20	
6	А4	2 Розділ	32	
7	А4	3 Розділ	12	
8	А4	Висновки	2	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	
14	А4	Додаток Д	8	
15	А4	Додаток Е	6	

ДОДАТОК Б. Перелік документів на оптичному носії

Пояснювальна записка.docx

Презентація.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

В І Д Г У К
на кваліфікаційну роботу студентки групи 125м-20-2
Ярощука Олексія Романовича
на тему: «Забезпечення конфіденційності зв'язку за технологією VoIP»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на 98 сторінках.

Метою кваліфікаційної роботи є забезпечення конфіденційності зв'язку за технологією VoIP.

Тема кваліфікаційної роботи безпосередньо пов’язана з об’єктом діяльності магістра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: використання кінцевого шифрування під час передачі голосу та повідомлень; створення засобу, що забезпечує безпечне спілкування не лише за допомогою Skype, а й будь-якого іншого VoIP-клієнта.

Практичне значення результатів кваліфікаційної роботи полягає у підвищенні безпеки взаємодії за допомогою VoIP.

Оформлення пояснювальної записки до кваліфікаційної роботи виконано з незначними відхиленнями від стандартів.

Недоліком роботи відсутність достатньо аргументованих висновків в підрозділах та розділах роботи.

В цілому за час дипломування Ярощук О.Р. проявила себе фахівцем, здатним вирішувати поставлені задачі та заслуговує присвоєння кваліфікації магістр за спеціальністю 125 Кібербезпека, освітньо-професійної програми «Кібербезпека».

Рівень запозичень у кваліфікаційній роботі не перевищує вимог “Положення про систему виявлення та запобігання плагіату”.

Кваліфікаційна робота заслуговує оцінки «задовільно»/70б.

Керівник кваліфікаційної роботи к.т.н., доц. Олександра ГЕРАСІНА

Керівник спеціального розділу ас. Юлія МІЛІНЧУК

ДОДАТОК Д. Кінцеве шифрування в Skype

```
namespace CryptoSkype
 {
        class Intercept : IDisposable
         {
                NetworkStream outStream;
                Call call;
                public static ILog log,msg_log;
                public static string nick;
                public static BigInteger p, g, a, b, recv;
                public static BigInteger[] exp = new BigInteger[100];
                public static StrongNumberProvider _strongRng = new
        StrongNumberProvider();
                public static bool role = false;
                public static UserCollection members;
                public static User user;
                public static IChat ichat;
                public static byte[] key = new byte[0];
                public static bool key_status = false;
                public static bool multi = false, multicall = false;
                public static string[] users;
                public static int count;
                public static int index = 0, ii = 0;

                private void skype_MessageStatus(ChatMessage msg,
        TChatMessageStatus status)
                {       // перехоплення вхідних та вихідних повідомлень
                        if (msg.Body.IndexOf(trigger) == 0 &&
                String.Compare(status.ToString(), "cmsReceived") == 0)
                        {
                                string mesg = msg.Body.Remove(0, trigger.Length);
                                string type = mesg.Substring(0, 1);
                                mesg = mesg.Remove(0, 1);
                                switch (type)
                                {// обмін повідомленнями за протоколом Діффі-Хеллмана
                                   case "m"://групповой чат
                                        multi = true;
                                        count = Convert.ToInt32(mesg);
```

```
            users = new string[count];
            exp = new BigInteger[100];
            messages = new string[1000];
            mes_num = 0;
            break;
        case "u":// абоненти групового чату
            users[0] = mesg;
            break;
        case "p":
            p = new BigInteger(mesg, 36);
            index = 0;
            ii = 0;
            key = null;
            key_status = false;
            role = false;
            break; case "g":
            g = new BigInteger(mesg, 36);
            break;
        case "e":
            if (!role) // пасивна роль у встановленні ключа
            {
                if (multi)//групповой чат
                {
                    exp[ii] = new BigInteger(mesg, 36);
                    if (index == 0)
                    {
                        a =
                    BigInteger.GenPseudoPrime(512, 30,
                    MicInterceptor._strongRng);
                        skype.SendMessage(users[0],
                        "!#skey_init#!e" + g.ModPow(a,
                        p).ToString(36));
                    }
                    if (index == count - 1)
                    {
                        key = new byte[exp[ii].ModPow(a,
                    p).GetBytes().Length];
                        key = exp[ii].ModPow(a,
                    p).GetBytes();
```

```
                        key_status = true;
                        msg_log.Info(true,
                    "================================
                    ==============");
                        msg_log.Info(true, "Chat opened.");
                    }
                    else if (index < count - 1)
                    {
                        skype.SendMessage(users[0],
                    "!#skey_init#!e" + exp[ii].ModPow(a,
                    p).ToString(36));
                    }
                    index++;
                    ii++;
                }
                else // чат з одним абонентом
                {
                    recv = new BigInteger(mesg, 36);
                    a = BigInteger.GenPseudoPrime(512, 30,
                MicInterceptor._strongRng);
                    skype.SendMessage(msg.Sender.Handle,
                "!#skey_init#!e" +
                MicInterceptor.g.ModPow(MicInterceptor.a,
                MicInterceptor.p).ToString(36));
                    key = new byte[recv.ModPow(a,
                p).GetBytes().Length];
                        key = recv.ModPow(a,
                    p).GetBytes();
                        key_status = true;
                    }
                }
            else// активна роль у встановленні ключа
            {
                if (multi) //групповой чат
                {
                    exp[ii] = new BigInteger(mesg, 36);
                    if (index == count - 1)
                    {
                        key = new byte[exp[ii].ModPow(b,
```

```
                p).GetBytes().Length];
                    key = exp[ii].ModPow(b, p).GetBytes();
                    key_status = true;
                    for (int i = 0; i < users.Length; i++)
                    {
                        user = new SKYPE4COMLib.User();
                        user.Handle = users[i];
                        members.Add(user);
                    }
                    ichat = skype.CreateChatMultiple(members);
                    msg_log.Info(true,
                "==========================================
                ====");
                    msg_log.Info(false, "Chat opened.");
                    ichat.SendMessage("!#chat_init#!");
                }
                else if (index < count - 1)
                {
                    skype.SendMessage(users[0], "!#skey_init#!e" +
                exp[ii].ModPow(b, p).ToString(36));
                }
                index++;
                ii++;
            }
            else // чат з одним абонентом
            {
                recv = new BigInteger(mesg, 36);
                key = new byte[recv.ModPow(b,
            p).GetBytes().Length];
                key = recv.ModPow(b, p).GetBytes();
                key_status = true;
                role = false;
            }
        }

        break;
            }
        }
        else if (msg.Body.IndexOf(trigger2) == 0 &&
```

```
        String.Compare(status.ToString(), "cmsReceived") == 0)
            {// прийом та розшифрування зашифрованого повідомлення
                string mesg = msg.Body.Remove(0, trigger2.Length);
                byte[] uplain = GetBytes(mesg);
                byte[] decr = new byte[uplain.Length];
                Gost28147.Gost28147EcbDecrypt(decr, uplain, key);
                msg_log.Info(false, " from {0}\n{1} ", msg.FromHandle
            ,GetString(decr));
            }
        }
        void OnSkypeCallStatus(Call call, TCallStatus status)
        {// встановлення сеансового ключа в момент здійснення виклику
            log.Info(false, "SkypeCallStatus: {0}", status);
            if (status == TCallStatus.clsRouting)
            {
                role = true;
                this.call = call;
                nick = call.PartnerHandle;
                key = BigInteger.GenPseudoPrime(512, 30,
            _strongRng).GetBytes();
                DHkey();
            }
        }

        void DHkey()
        {// встановлення та надсилання параметрів для встановлення
сеансового ключа за класичним протоколом Діффі-Хеллмана
            if (role)
            {
                p = BigInteger.GenPseudoPrime(256, 30, _strongRng);
                b = BigInteger.GenPseudoPrime(256, 30, _strongRng);
                g = (BigInteger)2;

                skype.SendMessage(nick, "!#skey_init#!p" + p.ToString(36));
                skype.SendMessage(nick, "!#skey_init#!g" + g.ToString(36));
                skype.SendMessage(nick, "!#skey_init#!e" + g.ModPow(b,
            p).ToString(36));
            }
        }
```

```
            void OnMicServerExecute(object sender, DataReceivedEventArgs args)
            {// Зашифрування вихідного аудіопотоку
            if (outStream != null)
            {
                bufferStream.SetLatestInBuffer(args.Buffer);
                byte[] encr = new byte[args.Buffer.Length];
                Gost28147.Gost28147Ecb(args.Buffer, encr, key);
                outStream.Write(encr, 0, encr.Length);
            }
        }
    }
}


namespace CryptoSkype
{
    [Export(typeof(MainForm))]

    public partial class MainForm : Form
    {
        public MainForm()
        {
            InitializeComponent();
            var log = new RichTextLogger(this.richTextBox1);
            var msg_log = new RichTextLogger(this.richTextBox2);
            audioGraph = new MainFormAudioGraph(log, msg_log);
            audioGraph.ConnectToSkpe();
        }

        private void button1_Click(object sender, EventArgs e)
        {// збереження сеансового ключа у файл
            SaveFileDialog save = new SaveFileDialog();
            save.InitialDirectory =
        Convert.ToString(Environment.SpecialFolder.MyDocuments);
            save.Filter = "Session key file (*.KEY)|*.key|All Files (*.*)|*.*";
            if (save.ShowDialog() == DialogResult.OK)
            {
                using (FileStream fstream = new FileStream(save.FileName,
            FileMode.OpenOrCreate))
```

```
                {
                    fstream.Write(Intercept.key, 0, Intercept.key.Length);
                }
            }
        }
        private void button2_Click(object sender, EventArgs e)
        {// відкриття сеансового ключа із файлу
            OpenFileDialog open = new OpenFileDialog();
            open.InitialDirectory =
        Convert.ToString(Environment.SpecialFolder.MyDocuments);
            open.Filter = "Session key file (*.KEY)|*.key|All Files (*.*)|*.*";
            open.Title = "Select a SessionKey File";
            if (open.ShowDialog() == DialogResult.OK)
            {
                using (FileStream fstream = File.OpenRead(open.FileName))
                {
                    Intercept.key = new byte[fstream.Length];
                    fstream.Read(Intercept.key, 0, Intercept.key.Length);
                    Intercept.log.Info(false, "Session key: {0}",
                Intercept.GetString(Intercept.key));
                }
            }
        }
        private void button3_Click(object sender, EventArgs e)
        {// встановлення сеансового ключа із заданим абонентом
            Intercept.role = true;
            if (textBox1.Text == "")
                MessageBox.Show("Имя пользователя не заполнено");
            else
            {
                Intercept.nick = textBox1.Text;
                DHkey();
                textBox3.Text = textBox1.Text;
            }
        }

        private void button4_Click(object sender, EventArgs e)
        {// зашифрований чат між абонентами
            if (Intercept.key.Count<Byte>() == 0)
```

```
                    MessageBox.Show("Session key is not set");
                else if (textBox2.Text != "" && textBox3.Text != "")
                {
                    Intercept.nick = textBox3.Text;
                    byte[] plain = Intercept.GetBytes(textBox2.Text);
                    byte[] encr = new byte[plain.Length];
                    Gost28147.Gost28147Ecb(plain, encr, Intercept.key);
                    Intercept.msg_log.Info(false, " to {0}\n{1}",
                textBox3.Text,textBox2.Text);
                    Intercept.skype.SendMessage(Intercept.nick, "!#encr__msg#!"
                + Intercept.GetString(encr));
                    textBox2.Clear();
                }
            }
        }
    }
```

ДОДАТОК Е. Інсталятор драйвера (cryptoaudio.inf)

```
[Version]
Signature="$CHICAGO$"
Class=MEDIA
Provider=%MSFT%
ClassGUID={4d36e96c-e325-11ce-bfc1-08002be10318}
DriverVer = 02/22/2007, 6.0.6000.1


[SourceDisksNames]
222="CryptoAudio","",222

[SourceDisksFiles]
cryptoaudio.sys=222
cryptoaudio2.sys=222

[Manufacturer]
%MfgName%=MicrosoftDS,NTAMD64

[MicrosoftDS]
%cryptoInput.DeviceDesc%=cryptoInput,*cryptoInput
%cryptoOutput.DeviceDesc%=cryptoOutput,*cryptoOutput

[MicrosoftDS.NTAMD64]
%cryptoInput.DeviceDesc%=cryptoInput,*cryptoInput
%cryptoOutput.DeviceDesc%=cryptoOutput,*cryptoOutput

[DestinationDirs]
cryptoInput.CopyList=10,system32\drivers
cryptoOutput.CopyList=10,system32\drivers


;=================================================================
; cryptoInput
;=================================================================
[cryptoInput]
AlsoInstall=ks.registration(ks.inf),wdmaudio.registration(wdmaudio.inf)
CopyFiles=cryptoInput.CopyList
```

```
AddReg=cryptoInput.AddReg

[cryptoInput.CopyList]
cryptoaudio.sys

[cryptoInput.Interfaces]
AddInterface=%KSCATEGORY_AUDIO%,%KSNAME_Wave%,cryptoInput.I.Wave
AddInterface=%KSCATEGORY_RENDER%,%KSNAME_Wave%,cryptoInput.I.Wav
e
AddInterface=%KSCATEGORY_CAPTURE%,%KSNAME_Wave%,cryptoInput.I.Wa
ve
AddInterface=%KSCATEGORY_AUDIO%,%KSNAME_Topology%,cryptoInput.I.To
po

[cryptoInput.AddReg]
HKR,,AssociatedFilters,,"wdmaud,swmidi,redbook"
HKR,,Driver,,cryptoaudio.sys

HKR,Drivers,SubClasses,,"wave,midi,mixer"

HKR,Drivers\wave\wdmaud.drv,Driver,,wdmaud.drv
HKR,Drivers\midi\wdmaud.drv,Driver,,wdmaud.drv
HKR,Drivers\mixer\wdmaud.drv,Driver,,wdmaud.drv

HKR,Drivers\wave\wdmaud.drv,Description,,%cryptoInput.DeviceDesc%
HKR,Drivers\midi\wdmaud.drv,Description,,%cryptoInput.DeviceDesc%
HKR,Drivers\mixer\wdmaud.drv,Description,,%cryptoInput.DeviceDesc%

HKLM,%MediaCategories%\%Simple.NameGuid%,Name,,%Simple.Name%

;=================================================================
; cryptoOutput
;=================================================================
[cryptoOutput]
AlsoInstall=ks.registration(ks.inf),wdmaudio.registration(wdmaudio.inf)
CopyFiles=cryptoOutput.CopyList
AddReg=cryptoOutput.AddReg

[cryptoOutput.CopyList]
```

```
cryptoaudio2.sys

[cryptoOutput.Interfaces]
AddInterface=%KSCATEGORY_AUDIO%,%KSNAME_Wave%,cryptoOutput.I.Wav
e
AddInterface=%KSCATEGORY_CAPTURE%,%KSNAME_Wave%,cryptoOutput.I.
Wave
AddInterface=%KSCATEGORY_AUDIO%,%KSNAME_Topology%,cryptoOutput.I.
Topo

[cryptoOutput.AddReg]
HKR,,AssociatedFilters,,"wdmaud,swmidi,redbook"
HKR,,Driver,,cryptoaudio2.sys

HKR,Drivers,SubClasses,,"wave,midi,mixer"

HKR,Drivers\wave\wdmaud.drv,Driver,,wdmaud.drv
HKR,Drivers\midi\wdmaud.drv,Driver,,wdmaud.drv
HKR,Drivers\mixer\wdmaud.drv,Driver,,wdmaud.drv

HKR,Drivers\wave\wdmaud.drv,Description,,%cryptoOutput.DeviceDesc%
HKR,Drivers\midi\wdmaud.drv,Description,,%cryptoOutput.DeviceDesc%
HKR,Drivers\mixer\wdmaud.drv,Description,,%cryptoOutput.DeviceDesc%

;=================================================================
; COMMON
;=================================================================

[MSVAD.I.Wave]

AddReg=cryptoOutput.I.Wave.AddReg

[MSVAD.I.Wave.AddReg]

HKR,,CLSID,,%Proxy.CLSID%

HKR,,FriendlyName,,%cryptoOutput.Wave.szPname%


[MSVAD.I.Topo]

AddReg=cryptoOutput.I.Topo.AddReg
```

```
[MSVAD.I.Topo.AddReg]
HKR,,CLSID,,%Proxy.CLSID%
HKR,,FriendlyName,,%cryptoOutput.Topo.szPname%

;=================================================================
; cryptoInput
;=================================================================
[cryptoInput.NT]
Include=ks.inf,wdmaudio.inf
Needs=KS.Registration, WDMAUDIO.Registration
CopyFiles=cryptoInput.CopyList
AddReg=cryptoInput.AddReg

[cryptoInput.NT.Interfaces]
AddInterface=%KSCATEGORY_AUDIO%,%KSNAME_Wave%,cryptoInput.I.Wave
AddInterface=%KSCATEGORY_RENDER%,%KSNAME_Wave%,cryptoInput.I.Wav
e
AddInterface=%KSCATEGORY_CAPTURE%,%KSNAME_Wave%,cryptoInput.I.Wa
ve
AddInterface=%KSCATEGORY_AUDIO%,%KSNAME_Topology%,cryptoInput.I.To
po

[cryptoInput.NT.Services]
AddService=cryptoInput,0x00000002,cryptoInput_Service_Inst

[cryptoInput_Service_Inst]
DisplayName=%cryptoInput.SvcDesc%
ServiceType=1
StartType=3
ErrorControl=1
```

```
ServiceBinary=%10%\system32\drivers\cryptoaudio.sys

;=================================================================
; cryptoOutput
;=================================================================
[cryptoOutput.NT]
Include=ks.inf,wdmaudio.inf
Needs=KS.Registration, WDMAUDIO.Registration
CopyFiles=cryptoOutput.CopyList
AddReg=cryptoOutput.AddReg

[cryptoOutput.NT.Interfaces]
AddInterface=%KSCATEGORY_AUDIO%,%KSNAME_Wave%,cryptoOutput.I.Wav
e
AddInterface=%KSCATEGORY_CAPTURE%,%KSNAME_Wave%,cryptoOutput.I.
Wave
AddInterface=%KSCATEGORY_AUDIO%,%KSNAME_Topology%,cryptoOutput.I.
Topo

[cryptoOutput.NT.Services]
AddService=cryptoOutput,0x00000002,cryptoOutput_Service_Inst

[cryptoOutput_Service_Inst]
DisplayName=%cryptoOutput.SvcDesc%
ServiceType=1
StartType=3
ErrorControl=1
ServiceBinary=%10%\system32\drivers\cryptoaudio2.sys

;=================================================================
```

```
; COMMON
;=====================================================
[Strings]
MSFT="CryptoAudio"
MfgName="CryptoAudio"
cryptoInput.DeviceDesc="CRYPTO INPUT"
cryptoOutput.DeviceDesc="CRYPTO OUTPUT"


MSVAD.Wave.szPname="Crypto Wave"
MSVAD.Topo.szPname="Crypto Topology"
MSVAD_MIDI="MSVAD -> WDM Midi Device"

Proxy.CLSID="{17CCA71B-ECD7-11D0-B908-00A0C9223196}"
KSCATEGORY_AUDIO="{6994AD04-93EF-11D0-A3CC-00A0C9223196}"
KSCATEGORY_RENDER="{65E8773E-8F56-11D0-A3B9-00A0C9223196}"
KSCATEGORY_CAPTURE="{65E8773D-8F56-11D0-A3B9-00A0C9223196}"

KSNAME_Wave="Wave"
KSNAME_Topology="Topology"

cryptoInput.SvcDesc="CRYPTO INPUT"
cryptoOutput.SvcDesc="CRYPTO OUTPUT"

MediaCategories="SYSTEM\CurrentControlSet\Control\MediaCategories"

Simple.NameGuid="{946A7B1A-EBBC-422a-A81F-F07C8D40D3B4}"
Simple.Name="MSVAD (Simple)"
```