**Львівський національний університет імені Івана Франка**

**Факультет електроніки та комп’ютерних технологій**

*Кафедра радіоелектронних і комп’ютерних систем*

**Звіт**

про виконання лабораторної роботи №5

*«Безпека у Skype»*

**Виконав:**

студентки групи ФеІ-31

Зьола О.П.

Викладач:  
Сінькевич О.О.

Львів

2020

**Мета роботи:** ознайомитися із основними відомостями шифрування програми Skype.

**Завдання:** розглянути можливості шифрування програми Skype.

**Порядок виконання роботи:**

1. Дослідила основні відомості про заходи безпеки у ПЗ «Skype» та зробила наступні висновки:

**Skype** – програмне забезпечення, що підтримує шифрований голосовий зв'язок через Інтернет між комп'ютерами (VoIP), а також платні послуги для дзвінків на мобільні і стаціонарні телефони.

У січні 2018-го Skype, слідом за мессенджерами WhatsApp, Google Allo і Facebook Messenger, почав використовувати «Signal Protocol» .

### *Цифрове посвідчення та шифрування у Skype*

Одна з основних цілей Skype — захищати вас від зловмисників, які підслуховують вас і підглядають за вами. Крім того, ми хочемо завадити шахраям видавати себе за інших, що вони часто роблять за допомогою електронної пошти, щоб отримати цінні особисті відомості користувачів. Для цього Skype видає кожному своєму користувачеві "цифровий сертифікат", який дає змогу перевірити особи всіх учасників чату або сеансу телефонного зв'язку в Skype.

Цифровий сертифікат— це електронне посвідчення, яке дає змогу встановити особу користувача Skype, де б він не перебував. Щоб його можна було використовувати для ідентифікації, цифровий сертифікат, як і звичайне посвідчення особи, таке як водійські права, має відповідати певним вимогам, зокрема, він має:

* містити назву відповідного облікового запису;
* бути виданим органом, який може будь-коли відкликати сертифікат;
* мати захист від підробки;
* містити підпис органа-видавця, у нашому випадку — Skype.

***Шифрування***

Зловмисники та хакери можуть перехоплювати дані в мережах зв'язку, таких як Інтернет, багатьма способами. Це одна з причин, з яких вважається, що електронна пошта та багато інших програм обміну текстовими повідомленнями в Інтернеті ненадійно захищають дані. Іншими словами, оскільки існує безліч способів, якими сторонні особи можуть відстежувати спілкування інших, потрібно активно захищатися від такого втручання.

Шифрування— це кодування повідомлення із застосуванням математичних алгоритмів, щоб його міг прочитати лише адресат. Протягом століть було розроблено багато методів шифрування, але всі вони схожі та діють за принципом сейфа та ключа: якщо помістити таємне повідомлення в сейф і закрити його на ключ, це повідомлення зможе прочитати лише власник такого самого ключа. Ключем може бути відома інформація або навіть реальний об'єкт, такий як циліндр певної довжини та товщини. У Skype ключ — це ім'я Skype і пароль, тому надзвичайно важливо захистити їх.

Для захисту повідомлень користувачів Skype від хакерів і зловмисників у Skype використовуються відомі стандартизовані алгоритми шифрування. Таким чином Skype забезпечує конфіденційність користувачів, а також автентичність даних, які передаються між користувачами.

Також для кожного дзвінка Skype створює сесійний 256-бітовий ключ. Сесія існує, поки зв'язок не буде перерваний і протягом певного проміжку часу після. В ході створення підключення Skype передає сесійний ключ. Протягом сесії ключ використовується для шифрування повідомлень в обох напрямках.

Всі дії протягом сесії захищені за допомогою режиму шифрування AES і режиму лічильника CTR. Skype здійснює шифрування поточного лічильника і солі з використанням 256-бітного AES ключа. Після цього повертає ключовий потік, з яким після цього виконується логічна операція додавання по модулю 2 з вмістом повідомлення. В результаті чого виходить зашифрований текст, який передається одержувачу. Сесія містить кілька потоків. Лічильник ICM відповідає номеру потоку і положенню в цьому потоці.

Skype використовує випадкові числа для різних криптографічних операцій. Вони використовуються при створенні ключів RSA, створюються AES-половинки ключів, які відповідають за шифрування. Безпека p2p з'єднання залежить від якості випадкових чисел, створених на початку і кінці сесії. Також генерація випадкових чисел залежить від операційної системи.

Skype використовує такі примітиви шифрування для забезпечення безпеки користувачів: блоковий шифр AES, криптографічні стандарти відкритого ключа RSA, систему підпису ISO 9796-2, систему хешування SHA-1 і потоковий шифр RC4.

**Висновок:** Виконуючи цю лабораторну роботу, я ознайомилася із загальними відомостями шифрування програми Skype.