Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет ННЦЗФН
(повна назва)

Кафедра Інформаційно-мережної інженерії
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (магістерський)

Дослідження захищеності месенджерів
(тема)

Виконала:
студентка 2 курсу, групи ІМІзм-22-1
Маслакова Н.Ю.
(прізвище, ініціали)

Спеціальність 172 Телекомунікації та радіотехніка
(код і повна назва спеціальності)
Тип програми освітньо-професійна
Освітня програма Інформаційно-мережна інженерія
(повна назва освітньої програми)

Керівник Золотарьов В.А.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Безрук В.М.
(підпис) (прізвище, ініціали)

2024 р.

Не містить відомостей заборонених до відкритого публікування

Студентка _____ / Маслакова Н.Ю./

Керівник _____ / Золотарьов В.А./

Харківський національний університет радіоелектроніки

Факультет ННЦЗФН

Кафедра Інформаційно-мережної інженерії

Рівень вищої освіти другий (магістерський)

Спеціальність 172 Телекомунікації та радіотехніка

Тип програми освітньо-професійна
(код і повна назва)

Освітня програма Інформаційно-мережна інженерія
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«24» жовтня 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентці Маслаковій Наталії Юріївні
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження захищеності месенджерів

затверджена наказом університету від 23 жовтня 2023 р. № 238 Стз

2. Термін подання студентом роботи до екзаменаційної комісії 25 січня 2024 р.

3. Вихідні дані до роботи: *Керуючись статистичними даними обрати найпопулярніші месенджери в Україні та докладно порівняти їх за наступними критеріями: наявність наскрізного шифрування, можливість збору даних і метаданних, наявність відкритого коду додатків; можливість передавання даних третім особам, наявність шифрування у хмарах, підтримку однорангового з'єднання, інформацію при реєстрації. Порівняти наявні захисні функції методом аналізу ієрархій.*

4. Перелік питань, що потрібно опрацювати в роботі: *Вступ*
1 МЕСЕНДЖЕРИ. ВИКОРИСТАННЯ ТА АНАЛІЗ СИСТЕМ МИТТЄВИХ ПОВІДОМЛЕНЬ
2 БЕЗПЕКА МЕСЕНДЖЕРІВ
3 ПОРІВНЯЛЬНИЙ АНАЛІЗ ФУНКЦІЙ БЕЗПЕКИ ТА ПРИВАТНОСТІ МЕСЕНДЖЕРІВ
4 ПОРІВНЯННЯ ТА РОЗРАХУНОК ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ МЕСЕНДЖЕРІВ МЕТОДОМ АНАЛІЗУ ІЄРАРХІЇ
Висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання з рішенням випускової кафедри) _____
Слайди у форматі Power Point – Титульний аркуш. Мета роботи. Вступ.
МЕСЕНДЖЕРИ. ВИКОРИСТАННЯ ТА АНАЛІЗ СИСТЕМ МИТТЄВИХ ПОВІДОМЛЕНЬ

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Ознайомлення із завданням. Уточнення ТЗ.	23.10.2023	вик.
2	Підбір літератури за темою роботи	01.11.2023	вик.
3	Виконання розділу 1	07.11.2023	вик.
4	Виконання розділу 2	18.11.2023	вик.
5	Виконання розділу 3	29.11.2023	вик.
6	Виконання розділу 4	15.01.2024	вик.
7	Оформлення презентаційного матеріалу	19.11.2024	вик.

Дата видачі завдання 24 жовтня 2023 р.

Студентка _____
(підпис)

Керівник роботи _____ доц. Золотарьов В.А.
(підпис)

РЕФЕРАТ

Пояснювальна записка: 80 с., 51 рис., 6 табл., 21 джерело, 5 додатків.

Об'єктом дослідження є захищеність месенджерів.

Мета роботи – дослідження захищеності безпеки найпопулярніших в Україні з месенджерів за різними критеріями.

В процесі дослідження проведено порівняльний аналіз функцій безпеки та приватності месенджерів за різними критеріями.

Проведене дослідження за різними критеріями показало, що найбільш захищеним месенджером станом на січень 2024 року є Wickr Me, який має найкращу функціональність: власні сервери, анонімну реєстрацію та додавання контактів без сервера каталогів.

МЕСЕНДЖЕРИ; БЕЗПЕКА МЕСЕНДЖЕРІВ; СИСТЕМА МИТТЕВИХ ПОВІДОМЛЕНЬ; АНАЛІЗ ФУНКЦІЙ БЕЗПЕКИ; ПОРІВНЯННЯ МЕСЕНДЖЕРІВ.

THE ABSTRACT

Explanatory note: 80 p., 51 figs., 6 tables, 21 sources, 5 appendix.

The object of study is the security of messengers.

Purpose - to study the security of the most popular messengers in Ukraine according to various criteria.

During the study, a comparative analysis of the security and privacy functions of messengers was conducted according to various criteria.

The study by various criteria showed that the most secure messenger as of January 2024 is Threema, which has the best functionality: its own servers, anonymous registration and adding contacts without a directory server.

MESSENGERS; MESSENGER SECURITY; INSTANT MESSAGING SYSTEM; ANALYSIS OF SECURITY FEATURES; COMPARISON OF MESSENGERS.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

AD – ідентифікаційне повідомлення.

AES-256 (Advanced Encryption Standard) – симетричний алгоритм блочного шифрування.

AKE (Authenticated Key Exchange) – обмін автентифікованими ключами

API (Application Programming Interface) – інтерфейс програмування програми.

C++ – мова програмування.

CBC (Cipher Block Chaining) – ланцюжок блоків шифрування.

CK (Chaining Key) – ланцюговий ключ.

DH – протокол Діффі-Хеллмана.

E2E (end-to-end) – наскрізне тестування.

GNU (GNU’s Not UNIX) – вільна Unix-подібна операційна система, що розробляється проектом GNU.

GDPR (General Data Protection Regulation) – загальний регламент про захист даних.

HKDF (HMAC Key Derivation Function) – Функція отримання ключів HMAC.

HMAC (Hash-based Message Authentication Code) – код автентифікації повідомлень на основі хешу.

IGE (Infinite Garble Extension) – нескінченне розширення Garble.

ICQ (I Seek You) – є однією з перших систем миттєвого обміну повідомленнями.

IP (Internet Protocol) – Інтернет-протокол.

IPK – довготривалий ключ, який є ідентифікаційним і реєструється абонентом одноразово.

iOS – є операційною системою, розробленою компанією Apple Inc.

KDF (Key Derivation Function) – функція виведення ключів.

MITM (Man-in-the-Middle) – «людина посередині» - визначає атаку в контексті мережевої безпеки.

MK (Message Key) – ключ шифрування повідомлення.

MTProto (Mobile Protocol) – мобільний протокол.

OK – одноразові ключі.

OPK – відкритий ключ.

OS X – операційна система для комп'ютерів Macintosh.

OWS (Open Whisper Systems) – відкриті системи Whisper.

PKI – відкритий ключ.

PR (Relations Company) – компанія зі зв'язків з громадськістю.

QR (Quick Response) – швидке реагування.

RK (root key) – кореневий ключ.

RSA-2048 (Rivest-Shamir-Adleman) - (Рівест-Шамір-Адлеман) – криптографічний алгоритм.

SHA 256 (Secure Hash Algorithm) – безпечний алгоритм хешування.

SK – середньостроковий ключ.

SPK (SignIK) – середньостроковий відкритий ключ.

SMS (Short Message Service) – служба коротких повідомлень.

SSL (Secure Sockets Layer) – рівень захищених сокетів.

SS7 (Signaling System 7) – система сигналізації 7.

TLS (Transport Layer Security) – безпека на транспортному рівні.

VoIP (Voice over Internet Protocol) – Протокол передачі голосу через Інтернет.

Web – глобальна система взаємопов'язаних комп'ютерних мереж.

X3DH (Extended Triple Diffie-Hellman) – розширений потрійний Диффі-Хеллман.

ІК – індивідуальний код.

ОС – операційна система.

ПК – персональний комп’ютер.

СМС – короткі текстові повідомлення.

США – Сполучені Штати Америки.

ТОП – список найкращих елементів.

ВСТУП

Комунікації між людьми сьогодні досягли найвищого рівня технологічності. Прогрес в області комп'ютерних систем зробив можливим обмін повідомленнями за лічені секунди (або миттєво). Це дозволяє людям спілкуватися в режимі реального часу, перебуваючи навіть за сотні тисяч кілометрів один від одного. За допомогою системи миттєвих повідомлень можна обмінюватися не тільки текстовими посиланнями, але також зображеннями, звуковими сигналами та відеозаписами. Для такого роду комунікацій використовується спеціальна клієнтська програма, звана Instant Messenger [1].

Одна з головних відмінностей від SMS-повідомлень полягає в тому, що не потрібно платити за кожне надіслане повідомлення – через систему миттєвих повідомлень (месенджер), можливо надіслати скільки завгодно повідомлень і не заплатити за це жодної копійки.

Тому, всіх, без винятку, людей, які користуються інтернетом та месенджером, гостро турбує питання про безпеку їхніх особистих даних, телефонних дзвінків, відеодзвінків, текстових повідомлень та іншої інформації, яку пересилають. Ніхто не хоче, щоб їхнє особисте життя або трудова діяльність стала відома зловмисникам, різним силовим структурам, спецслужбам або широкої громадськості.

На сьогодні існує досить велика кількість месенджерів, які можна використовувати як на мобільних пристроях, так і на ПК. Усі вони відрізняються різним рівнем інформаційної безпеки.

Програма забезпечення безпеки інформаційних систем призначена для захисту інформації організації шляхом зниження ризику втрати конфіденційності, цілісності та доступності цієї інформації до прийнятного рівня.

Хороша програма забезпечення безпеки інформації включає два основні елементи: аналіз ризиків та управління ризиками.

На етапі аналізу ризиків до уваги береться реєстр усіх інформаційних систем. Визначають цінність кожної системи для організації та ступінь ризику, на який наражається організація. З іншого боку, управління ризиками включає вибір засобів контролю та заходів безпеки, які знижують схильність організації до ризику до прийнятного рівня. Щоб заходи зниження ризику були

ефективними, результативними і відображали здоровий глузд, вони повинні прийматися в межах інфраструктури безпеки, в яких заходи загальної безпеки доповнюються заходами комп'ютерної, адміністративної, кадрової та фізичної безпеки.

Управління ризиками стає проблемою вищого керівництва. Під час управління ризиками необхідно досягти балансу між важливістю інформації для організації, з одного боку, і вартістю кадрових, адміністративних і технічних заходів забезпечення безпеки, з іншого боку. Витрати на застосовані заходи забезпечення безпеки мають бути меншими, ніж потенційний збиток унаслідок втрати конфіденційності, цілісності та доступності інформації.

Багато офіційних методик аналізу ризиків, наявних на ринку, вимагають технічної експертизи в галузі інформаційних технологій і релевантних засобів контролю, а також наявності точних відомостей про прояви загроз, які можуть відбуватися поза межами досяжності багатьох аудиторських управлінь, принаймні спочатку. Тому завдання полягає в накопиченні з часом необхідної експертизи та ресурсів [2].

1 МЕСЕНДЖЕРИ. ВИКОРИСТАННЯ ТА АНАЛІЗ СИСТЕМ МИТТЄВИХ ПОВІДОМЛЕНЬ

1.1 Загальні відомості системи миттєвих повідомлень

Messenger - від англійської "кур'єр" чи "зв'язковий". Це програма створена для миттєвого обміну повідомленнями між користувачами. Їхня головна перевага перед звичайною електронною поштою, полягає саме в швидкості. Тут послання передається надшвидко, тоді як оновлення поштової скриньки відбувається раз на кілька хвилин. Говорячи про те, що таке месенджер, слід уточнювати важливу особливість – він є клієнтською програмою. Це означає, що програма самостійно працювати не може та для її використання необхідне підключення до сервера.

У перших версіях, адресат бачив повідомлення вже на момент його складання, що було не зовсім зручно, оскільки користувач міг зробити помилку, виправити її, відредагувати пропозицію, і це відображалося у вікні діалогу. Сьогодні текст з'являється на екрані співрозмовника після того, як він повністю відредагований і відправлений. Крім того, в сучасних версіях спілкування може відбуватися не лише за допомогою текстових повідомлень, а й шляхом здійснення інших дій, наприклад: обміну графічними, аудіо та відеофайлами, голосовим і навіть відео-зв'язком.

Майже кожна людина використовує як мінімум одну, а найчастіше одночасно кілька месенджерів. Необхідність у різних мережах обміну повідомленнями зумовлена тим, що між ними немає прямого зв'язку. Кожна з програм створена окремою групою розробників, має свої сервери та протоколи, особливості та правила використання.

Месенджери можна класифікувати за різними критеріями. Нижче наведені які бувають месенджери:

1. За типом використання

Особисте використання: це месенджери, які зазвичай використовуються для спілкування з друзями та сім’єю. Приклади включають WhatsApp, Telegram, Viber та Facebook Messenger.

Для бізнесу: це месенджери, які призначені для використання у робочих цілях. Приклади включають Slack, Microsoft Teams та Google Chat.

2. За рівнем безпеки

Стандартні месенджери: більшість месенджерів захищають спілкування користувача шляхом шифрування даних. Приклади включають WhatsApp, Telegram та Viber.

Месенджери з посиленою безпекою: деякі месенджери забезпечують додаткові рівні захисту, такі як шифрування та можливість спілкування “інкогніто”. Приклади включають Signal та Telegram (секретний чат).

3. По платформі

Мультиплатформні месенджери: ці месенджери доступні на різних платформах, таких як Android, iOS, Windows та Mac. Приклади включають WhatsApp, Telegram та Slack.

Месенджери для певної платформи: деякі месенджери працюють лише на певних платформах. Приклад – iMessage від Apple, який працює лише на пристроях Apple [3].

Розглянемо докладніше дев’ять найпопулярніших месенджерів, якими користуються українці у 2023 - 2024 роках.

1.2 Месенджер «Ватсап»

WhatsApp - американський безкоштовний сервіс обміну миттєвими повідомленнями та голосового зв'язку по IP, що належить компанії Meta. Він дає змогу користувачам надсилати текстові та голосові повідомлення, здійснювати голосові та відео-дзвінки, обмінюватися зображеннями, документами, місцезнаходженням користувача та іншим контентом.

Згідно зі статистикою 2023 року, програмою користується понад 2 000 000 000 користувачів. Донедавна їх кількість неухильно зростала, але потім з’явилася інформація про передачу особистих даних. Переважно, користувачі почали переходити до конкурентів, але більшість, розуміючи всі переваги програми, так само використовує її для спілкування і для роботи.

Розглянемо переваги месенджера:

- WhatsApp добре працює на всіх популярних операційних системах, включаючи Windows та Android;
- за потреби можна встановити на комп’ютер або ноутбук, і вже з них здійснювати дзвінки;
- синхронізація контактів із телефонної книги відбувається автоматично;

- можна створити корпоративний чат або групу інтересів;
- користувачі можуть налаштувати сповіщення та приватність;
- на день можна встановити статус;
- програма показує, коли співрозмовник востаннє був у мережі;
- цілком відсутня реклама.

Як будь-який створений додаток, месенджер має декілька недоліків:

- іноді некоректно працює відображення останнього відвідин;
- під час роботи WhatsApp на комп'ютері потрібно синхронізувати месенджер із телефоном;
- часом запізнюються повідомлення про нові повідомлення [3].

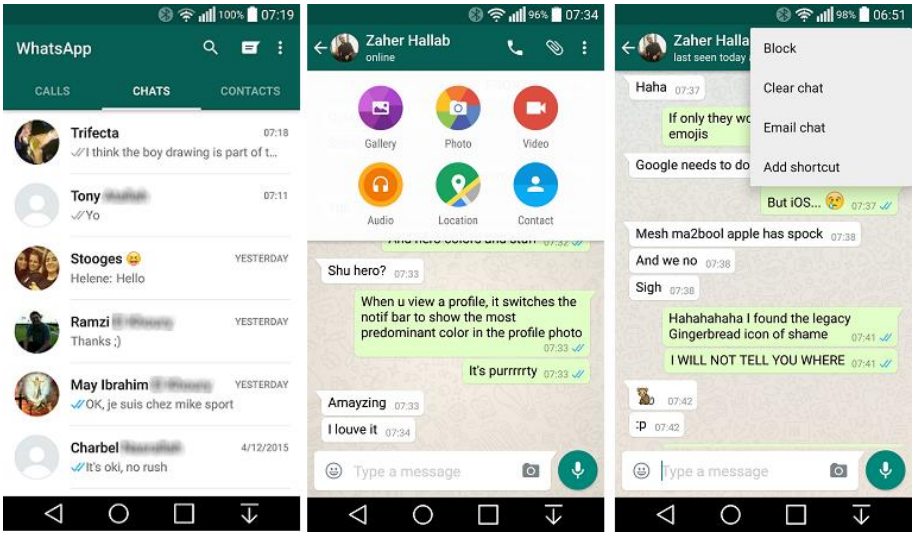

Рисунок 1.1 – Інтерфейс месенджеру WhatsApp

1.3 Месенджер «Вайбер»

Viber ("Вайбер") - додаток-месенджер, що дає змогу надсилати повідомлення, здійснювати відео- та голосові VoIP-дзвінки через Інтернет. Голосові виклики між користувачами зі встановленим Viber безкоштовні (оплачується тільки інтернет-трафік за тарифом оператора зв'язку). Viber має можливість надсилати текстові, голосові та відео-повідомлення, документи, зображення, відеозаписи та файли, а також працювати в автономному режимі.

За даними на 2023 рік, Viber використовували трохи більше 250 000 000 людей.

У ТОП-10 цей популярний додаток потрапив завдяки широкому набору функцій. Ось деякі з них:

- встановлення фотографій або іншого зображення на свій профіль;
- обмін текстовими та голосовими повідомленнями, звичайні та відео-дзвінки, передача файлів;
- можливість захищати листування паролем;
- синхронізація одного профілю Viber на кількох пристроях;
- можливість створювати бізнес-чати;
- можливість міняти тему оформлення.

На сьогоднішній день Viber перекладено 40 мовами, завдяки чому ним можуть користуватися жителі багатьох країн. Це один із важливих плюсів. Другий – через програму можна зателефонувати навіть на стаціонарні телефони. З мінусів: Viber зберігає всі листування у пам’яті телефону [3].

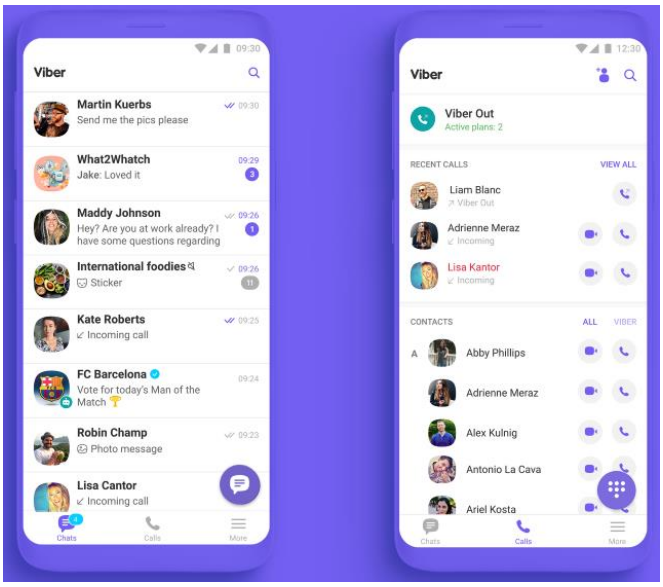

Рисунок 1.2 – Інтерфейс месенджеру Viber

1.4 Месенджер «Телеграм»

Telegram ("далеко" + "запис") – крос-платформна система миттєвого обміну повідомленнями (месенджер) із функціями обміну текстовими, голосовими та відео-повідомленнями, а також стікерами, фотографіями та файлами багатьох форматів. Також можна здійснювати аудіо- та відео-дзвінки, влаштовувати трансляції в каналах і групах, організовувати конференції, багатокористувацькі

групи і канали. Клієнтські додатки Telegram доступні для Android, iOS, Windows, macOS і GNU/Linux [4].

У червні 2022 року увійшов до п'ятірки найзавантажуваніших застосунків, а кількість його постійних користувачів перевищила 700 мільйонів. За словами засновника сервісу Павла Дурова, на початок 2023 року Telegram став другим месенджером у світі за популярністю, поступившись лише WhatsApp.

Незважаючи на високу надійність протоколу шифрування, проблема з безпекою все ж таки існує. Якщо хакер підбере до нього ключ, він отримає доступ і до листування, і до особистої інформації про користувачів. [3]

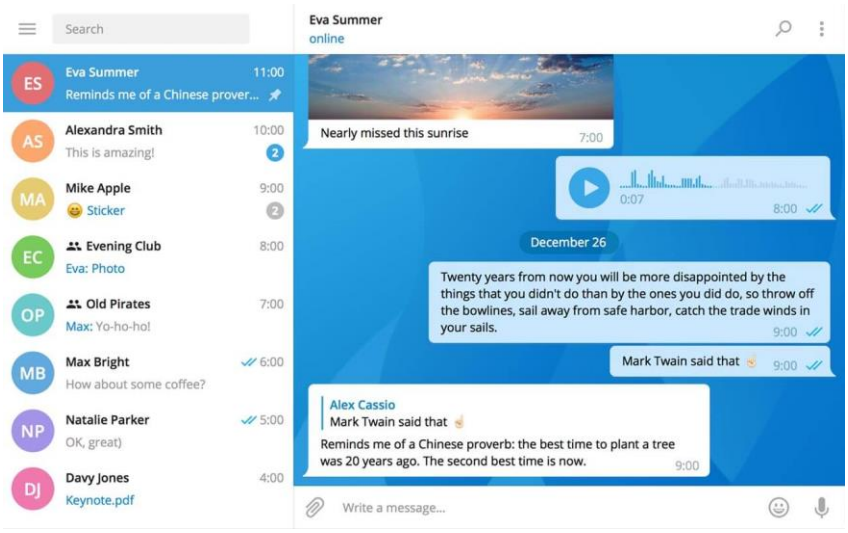

Рисунок 1.3 – Інтерфейс месенджеру Telegram

1.5 Месенджер «Трима»

Threema - швейцарський розробник і провідний постачальник безпечних і конфіденційних рішень для обміну миттєвими повідомленнями.

Рішення Threema корпоративного класу Threema - це безпечний бізнес-месенджер, що відповідає вимогам GDPR. Платформа надає компаніям і організаціям набір безпечних комунікацій у вигляді застосунку для обміну повідомленнями, який відповідає найвищим вимогам безпеки, оскільки зв'язок завжди зашифрований. Сьогодні розробками компанії для внутрішніх і зовнішніх комунікацій користуються два мільйони користувачів із 7 000 компаній, державних установ, шкіл та організацій по всьому світу.

Основні переваги Threema:

- Гарантована конфіденційність: Threema розроблено таким чином, щоб генерувати якомога менше даних на серверах.
- Повна анонімність: Немає необхідності надавати особисту інформацію (наприклад, номер телефону або адресу електронної пошти).
- Відкритий вихідний код: Щоб забезпечити повну прозорість, додатки Threema мають відкритий вихідний код. Будь-яка достатньо обізнана людина може самостійно перевірити безпеку Threema.
- Необов'язкова синхронізація контактів: Для використання Threema необов'язково надавати доступ до адресної книги.
- Комплексне шифрування: У Threema все спілкування наскрізь зашифроване - не тільки текстові повідомлення, голосові та відео-дзвінки, а й групові чати, медіа-файли і навіть повідомлення про статус.
- Багатий функціонал: Threema є універсальною та багатофункціональною платформою [5].

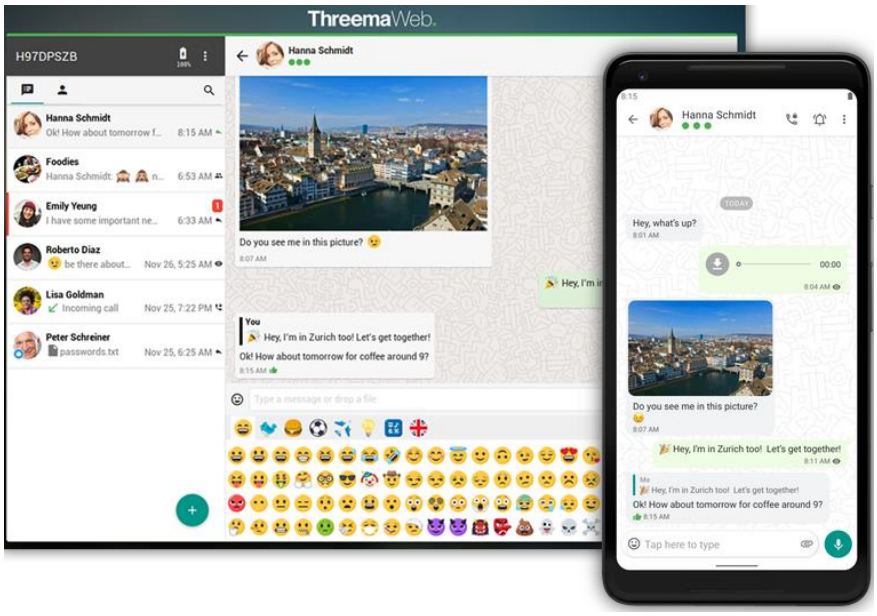

Рисунок 1.4 – Інтерфейс месенджеру Threema

1.6 Месенджер «Дискорд»

Спочатку цей месенджер створювався для геймерів. Однак зараз його використовують і просто для спілкування, і для робочих цілей. У 2022 році в ньому було зареєстровано понад 300 000 000 людей.

Тут можна здійснювати дзвінки, надсилати файли, створювати конференції. Приємний бонус – програма сумісна практично з усіма ОС.

З особливостей Discord можна виділити такі:

- не перевантажує пристрій одночасно з іншими програмами. оскільки програма цілеспрямовано створювалася для гравців, розробники подбали про її оптимізацію. результат – вона використовує зовсім небагато системних ресурсів;
- користувачі мають можливість змінювати нік та його оформлення для різних чатів;
- Discord не містить реклами та абсолютно безкоштовний;
- геймерам достатньо натиснути лише одну клавішу, щоб почати розмову, завдяки чому можна не відволікатися від ігрового процесу;
- не обов’язково встановлювати програму на пристрої. можна скористатися нею через браузер.

Серед недоліків можна виділити — проблеми із серверами, причина яких — перевантаження [3].

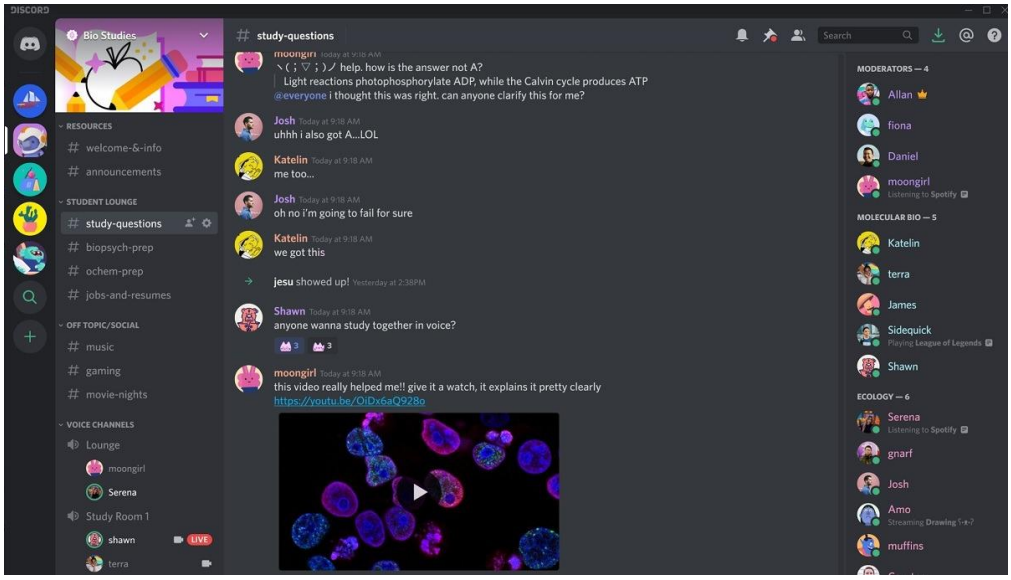

Рисунок 1.5 – Інтерфейс месенджеру Discord

1.7 Месенджер «Сигнал»

Цей месенджер схожий на Telegram і теж вважається одним із найбезпечніших. Справа в тому, що розробники впровадили в нього свою

систему шифрування повідомлень, дзвінків та файлів. Вона настільки надійна, що доступ до цих даних не можуть отримати навіть сервери, що їх передають. Такий захист стоїть і на групових чатах. А під час відеодзвінків, які здійснюються захищеними каналами, від співрозмовника можна приховувати свій IP.

Користувачам доступне надсилання повідомлень, стікерів, медіа-файлів. Можна виставляти таймер на їхнє видалення. Також є можливість надсилання одноразових повідомлень. Це означає, що система автоматично видалить їх одразу після того, як адресат перегляне [3].

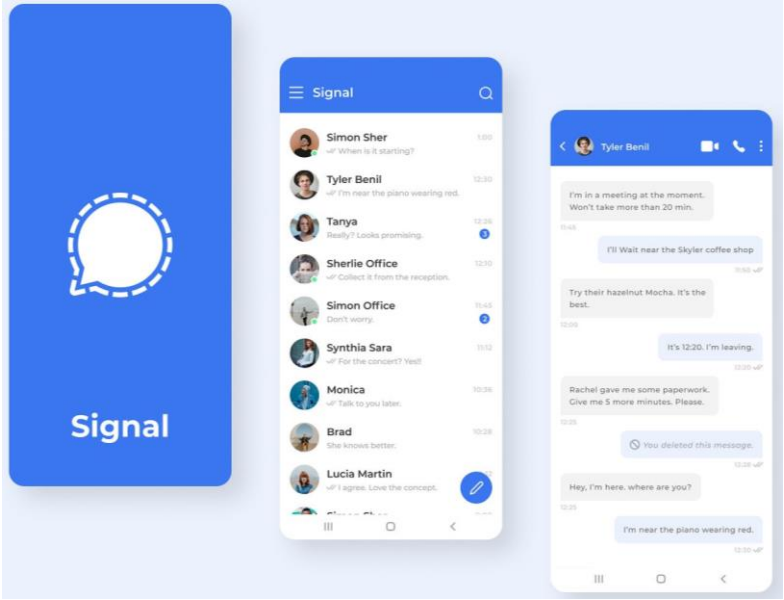

Рисунок 1.6 – Інтерфейс месенджеру Signal

1.8 Месенджер «Фейсбук»

Facebook - це соціальна мережа, де користувачі можуть публікувати коментарі, ділитися фотографіями та посиланнями на новини або інший цікавий контент в Інтернеті, спілкуватися в чаті та переглядати короткі відео.

Facebook розпочав свою діяльність у лютому 2004 року як шкільна соціальна мережа Гарвардського університету. Її створили Марк Цукерберг та Едвард Саверін, обидва студенти коледжу. Лише у 2006 році Facebook став доступним для всіх, кому виповнилося 13 років, і почав стрімко розвиватися, випередивши MySpace і ставши найпопулярнішою соціальною мережею у світі.

Успіх Facebook можна пояснити його здатністю приваблювати як людей, так і бізнес, а також його здатністю взаємодіяти з сайтами в Інтернеті, надаючи єдиний логін, який працює на декількох сайтах.

Ось кілька функцій, які роблять Facebook таким популярним:

- Facebook дозволяє вам вести список друзів і вибирати налаштування конфіденційності, щоб визначити, хто може бачити вміст вашого профілю.
- Facebook дозволяє завантажувати фотографії та вести фотоальбоми, якими можна ділитися з друзями.
- Facebook підтримує інтерактивний онлайн-чат і можливість коментувати сторінки профілів ваших друзів, щоб підтримувати зв'язок, ділитися інформацією або просто сказати "привіт".
- Facebook підтримує сторінки груп, фан-сторінки та бізнес-сторінки, що дозволяє компаніям використовувати Facebook як інструмент для маркетингу в соціальних мережах [6].

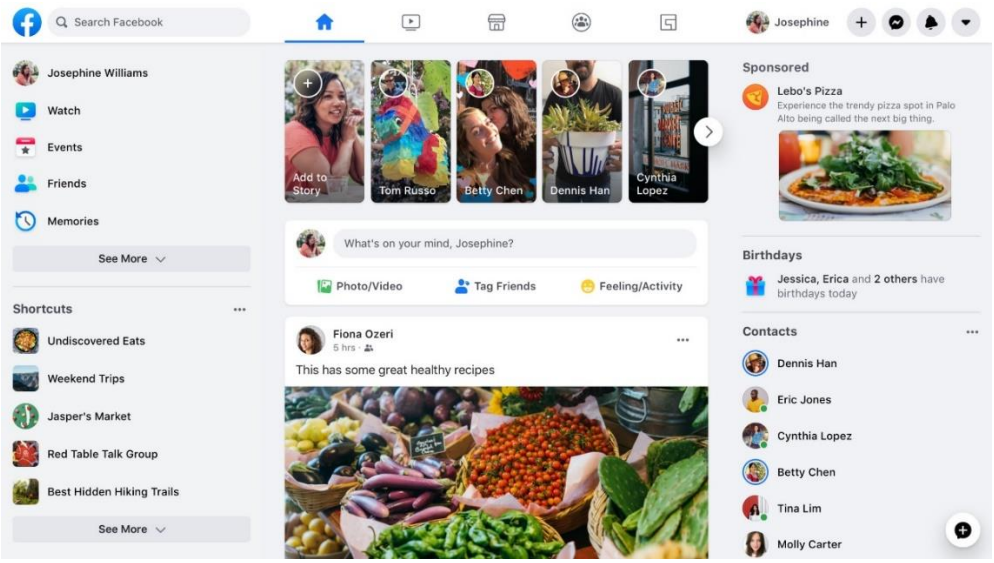

Рисунок 1.7 – Інтерфейс месенджеру Facebook

1.9 Месенджер «Вайр»

Wire - це месенджер для миттєвого обміну інформацією через наскрізне шифрування, створений компанією Wire Swiss для iOS, Android, OS X, Windows, GNU/Linux. Wire пропонує три різновиди власної продукції: Wire Pro — для

спільного обміну інформацією між бізнесом; Wire Enterprise — має ті самі можливості, що й Wire Pro, але з додатковими функціями для великих організацій; Wire Red — «безпечний спосіб спілкування в умовах кризи».

У Wire, як і в багатьох інших месенджерах, користувачі можуть обмінюватися текстовими повідомленнями, картинками, музикою і відео, також дзвонити один одному по VoIP — в тому числі й в групах. Виробник намагається відрізнятися від інших месенджерів тим, що представляє зміст повідомлень максимально просто, без пояснень, і має більший захист даних, ніж інші месенджери. Wire доступний у вигляді додатку для мобільних пристроїв і настільних комп'ютерів або може використовуватися через веб-браузер; для реєстрації не потрібен номер телефону, користувач може також зареєструватися за допомогою адреси електронної пошти [7].

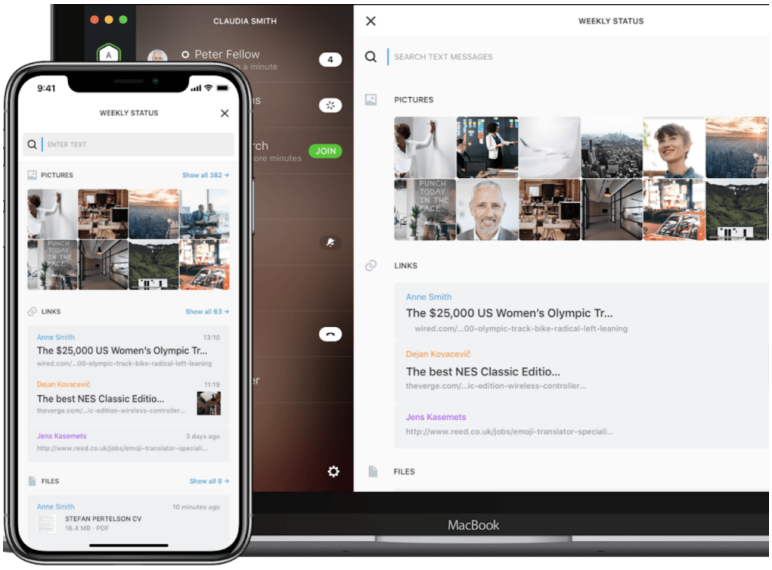

Рисунок 1.8 – Інтерфейс месенджеру Wire

1.10 Месенджер «Вікр Мі»

Wickr Me - додаток для листувань. Цей застосунок очолює рейтинг найбезпечніших месенджерів і має низку переваг.

Плюси:

- Для реєстрації в ньому не потрібне введення особистих даних (телефон, пошта). Ви реєструєтеся тільки за логіном і паролем. Знаходите співрозмовника теж тільки за логіном. Ви можете в разі небезпеки

вийти/видалити застосунок - і без вашої допомоги ніхто не зможе, як в інших застосунках, переактивувати його СМС-кою на номер телефону.

- Є можливість персонального подвійного налаштування чатів. Ви можете встановити таймер авто-видалення повідомлення після його прочитання. Друге - термін життя самого повідомлення. У цьому налаштуванні ви можете задати авто-видалення після закінчення часу незалежно від того, прочитав його ваш співрозмовник чи ні. Зручності цих функцій очевидні.

Мінуси

- Мінус у тому, що іноді можна проґавити повідомлення - і воно автоматично видалиться. Так ви ризикуєте проґавити щось важливе, але тут просто потрібно бути уважнішим.
- Погана якість зв'язку під час дзвінків, незручно відправляти файли і медіа [8].

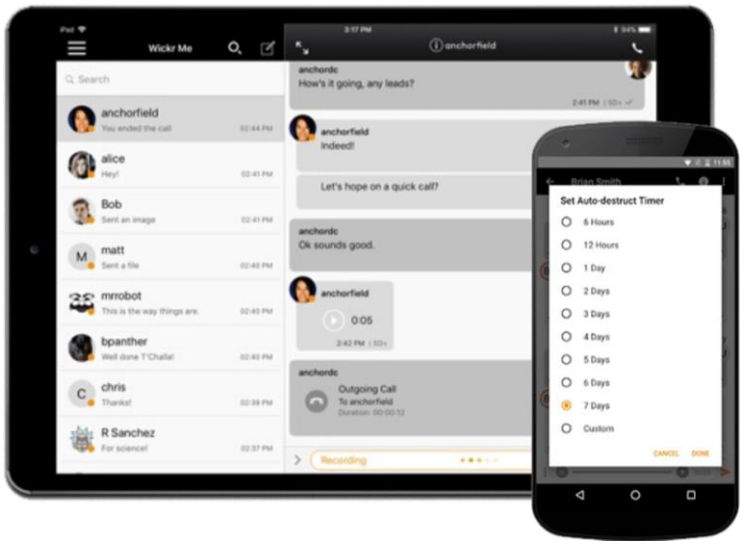

Рисунок 1.9 – Інтерфейс месенджеру Wickr Me

Висновок з розділу: у першому розділі було розглянуто загальні відомості системи миттєвих повідомлень та розібрано дев’ять найпопулярніших месенджерів якими користуються українці у 2023 році, а також дізналися, що месенджер є неодмінним атрибутом сучасного суспільства, який дозволяє вибудовувати комунікації та спілкуватися легко, швидко та часто безкоштовно. Месенджери активно витісняють SMS як самостійний спосіб зв'язку. Вибір зручних та багатофункціональних мереж миттєвого обміну повідомленнями з кожним роком стає дедалі ширшим.

2 БЕЗПЕКА МЕСЕНДЖЕРІВ

Масове розповсюдження та зріст функціональності мобільних пристроїв, розвиток мобільних ОС та безліч наданих ними засобів комунікації в умовах відносної обмеженості апаратних ресурсів, гостро становить питання безпеки. Нижче будуть більш детально розглянуті проблеми та методи забезпечення безпеки месенджерів, тісно пов'язаних із загальними питаннями забезпечення інформаційної безпеки мобільних платформ.

Найбільшу частину, у справжній час, отримали месенджери WhatsApp, Viber, Telegram, Facebook Messenger Wickr Me, Threema, Wire та інші. В Україні, віддають перевагу першим чотирьом продуктам із цього списку, крім того особиста переписка проводиться в рамках соціальних мереж, таких як ВКонтакті та Facebook, які також мають попит. При цьому, кожен абонент користується трьома різноманітними системами обміну повідомлень [9].

Загальний ріст уваги до проблем безпеки, наряді з загостренням конкуренції серед месенджерів, яке виникає на фоні скандалів, які зв'язані з продажем користувацьких даних компанією Facebook та блокуванням месенджера Telegram, використане розробником останнього для просування ідеї о захищеності своєї системи, змушує розробників впроваджувати додаткові засоби захисту, такі як end-to-end шифрування переданих даних.

Поряд з месенджерами, які початково розроблялися та позиціонувалися як захищені (Signal, Threema, Wire, Wickr Me), в 2016 році увімкнено повне шифрування повідомлень, голосових дзвінків та файлів, які пересилаються в месенджерах WhatsApp та Viber, в ICQ почали шифруватися не тільки текстові повідомлення, але аудіо та відео, а в Facebook Messenger з'явились «таємні» чати. В 2018 році систему кінцевого шифрування чатів та дзвінків в рамках «особистої бесіди» ввів Skype, а «ВКонтакті» для iOS та Android запустив шифрування голосових та відеодзвінків.

«Таємні» чати підтримуються також і в Telegram, однак в звичайному режимі хмарних чатів, який використовується за замовчуванням, дані «видно» серверам Telegram у відкритому вигляді. При цьому PR-компанія месенджера будувалася на запевненнях його господарів, що ніякі спецслужби не зможуть прочитати особисті повідомлення, та проводилася для англомовних аудиторії під лозунгом «Taking back our right to privacy» («повернемо собі право на

приватність»). За заявами Павла Дурова, «з самого першого дня ми не передали урядам та третім особам ні байту приватних даних». Таким чином, захищеність месенджера Telegram забезпечується скоріш не технічними заходами, а політикою компанії. Однак, в серпні 2018 року Telegram був вимушений внести зміни в політику конфіденційності месенджера в рамках нового європейського закону про захист персональних даних GDPR (General Data Protection Regulation), що додав пункт про можливість розкриття IP-адреси та номеру телефону абонента на підставі судового рішення, яке підтверджує, що абонента підозрюють в тероризмі.

Це відображає ще одну тенденцію в забезпеченні безпечності месенджерів, обумовлену підсиленням регулювання зі сторони держави, яке прагне, за можливістю, деанонімізувати комунікації на випадок необхідності їх контролю. В цьому ряді стоїть також повідомлення, яке з'явилося в серпні 2018 року про відмову WhatsApp від технології, яка використовується в справжній час кінцевого шифрування.

Месенджери використовують власні протоколи передачі даних, при цьому шифрування повідомлень зазвичай виконується на прикладному рівні, потім зашифровані дані вбудовуються в транспортний протокол. В якості транспортного протоколу, як правило (не обов'язково), використовуються SSL/TLS, де-факто, який став стандартом для всіх захищених web-комунікацій. Разом з тим, реалізація останнього на мобільних платформах буває далека від досконалості [9].

Для захисту передаваємих даних месенджери, як правило, використовують end-to-end (E2E, кінцеве або наскрізне) шифрування. Це означає, що криптографічні ключі генеруються та зберігаються на кінцевому пристрої (пристрої користувача), а не на серверах системи миттєвих повідомлень. Тому ніхто, окрім адресату, навіть сервер системи, не зможе прочитати вміст зашифрованих повідомлень. З іншого боку, листування буде не доступне також самому абоненту, якщо він перейде на другій пристрій. Тому синхронізація пристроїв або відновлення у випадку втрати пристрою (тобто отримання доступу до архіву листування) разом з використанням кінцевого шифрування неможливо без депонування особистого ключа поза пристроєм.

Оскільки кінцеве шифрування реалізується на верхніх рівнях мережевої архітектури, адресні дані повинні бути доступні в незашифрованому виді в проміжних вузлах (тобто, на серверах системи). А це означає, що методані

комунікацій користувачів (хто кому дзвонив або писав, та коли) залишаються відкритими.

Багато месенджерів в даний час реалізують кінцеве шифрування на основі протоколу Signal, розробленого некомерційною організацією Open Whisper Systems (OWS) для однойменного месенджера. Протокол ретельно документований та має бібліотеки, що його реалізують, з відкритим вихідним кодом на мовах Java, C++ та JavaScript. На сьогоднішній день протокол Signal використовується месенджерами WhatsApp, GoogleAllo, Facebook Messenger та Skype. Реалізація шифрування Viber використовує концепцію протоколу Signal, але інші криптографічні алгоритми. За заявами розробників Wire, протокол, який використовується в цьому месенджері шифрування Proteus, також базується на протоколі Signal.

Протокол використовує криптографію з відкритим ключем на еліптичної кривої Curve25519 або Curve448 для цифрових підписів, узгодження ключів на основі модифікації протоколу Діффі-Хеллмана, шифрування повідомлень за допомогою симетричного алгоритму AES-256 у режимі CBC та перевірку цілісності за допомогою коду автентифікації HMAC-SHA256. Крім того, для зміни ключів шифрування протягом сеансу зв'язку використовується функція диверсифікації ключа (KDF, Key Derivation Function) на основі HMAC-SHA256 та HMAC-SHA512 (HKDF). Усі використовувані протоколом криптографічні примітиви добре відомі та рекомендовані для застосування у системах захисту інформації.

Основні особливості протоколу Signal обумовлені тим, що друга сторона комунікацій може бути недоступна (перебувати в автономному режимі, оф-лайн) в момент відправлення повідомлення. Тому стандартні протоколи аутентифікації та обміну ключами (AKE, Authenticated Key Exchange) не можуть бути безпосередньо застосовані. Наприклад, у класичному протоколі Діффі-Хеллмана (DH) в формуванні загального секретного ключа беруть участь обидві сторони, оскільки значення ключа обчислюється на основі секретних ключів обох абонентів. При цьому абоненти відкрито обмінюються значеннями, які можна трактувати як відкриті ключі криптосистеми DH.

Для вирішення проблеми автономності однієї із сторін Signal реалізує асинхронний протокол передачі X3DH, вимагаючи попереднього відправлення на проміжний сервер партії попередньо обчислених значень (відкритих ключів). Така відправка проводиться під час реєстрації або пізніше (рис. 2.1). Коли

абонент бажає надіслати повідомлення, він отримує необхідні для виконання AKE-подібного протоколу значення одержувача з проміжного сервера (який діє тільки як буфер) та обчислює ключ шифрування повідомлення.

Рисунок 2.1 - Перший етап протоколу Signal – реєстрація ключової інформації користувачів

На етапі реєстрації, до початку обміну повідомленнями, кожен абонент формує 3 типи ключів асиметричної схеми: довготривалий ключ IK (для підпису), середньостроковий попередній ключ SK та набір одноразових попередніх OK ключів. При цьому на сервер надсилаються лише відповідні їм відкриті ключі IPK, SPK, OPK та підпис (SignIK(SPK) – середньостроковий відкритий ключ SPK підписується довгостроковим ключем IK абонента).

Абонент може періодично (наприклад, раз на тиждень або раз на місяць) оновлювати свій середньостроковий відкритий ключ SPK з підписом, а також у будь-який час завантажувати новий набір попередніх одноразових відкритих ключів OPK (наприклад, коли сервер інформує Боба про те, що їхній запас на сервері знизився). Довготривалий ключ IPK є ідентифікаційним і реєструється абонентом одноразово.

Нехай абонент A хоче розпочати сеанс зв'язку з абонентом B (рис. 2.2). Абонент A запитує у сервера та отримує пакет ключів абонента B, а потім обчислює секретний ключ SK з кількох значень протоколу DH, отримані на основі значень ідентифікаційних ключів обох абонентів IPK_A, IPK_B, середньострокового відкритого ключа одержувача SPK_B та короткострокового відкритого ключа EPK_A із знову згенерованої відправником пари ключів асиметричного шифрування:

$$DH_1 = DH(IK_A, SPK_B),$$
$$DH_2 = DH(EPK_A, IK_B),$$
$$DH_3 = DH(EPK_A, SPK_B),$$

$$DH_4 = DH(EPK_A, OPK_B),$$
$$SK = KDF\ (DH_1 \| DH_2 \| DH_3 \| DH_4).$$

Якщо на сервері вичерпано запас одноразових попередніх ключів OPK_B, значення DH_4 опускається.

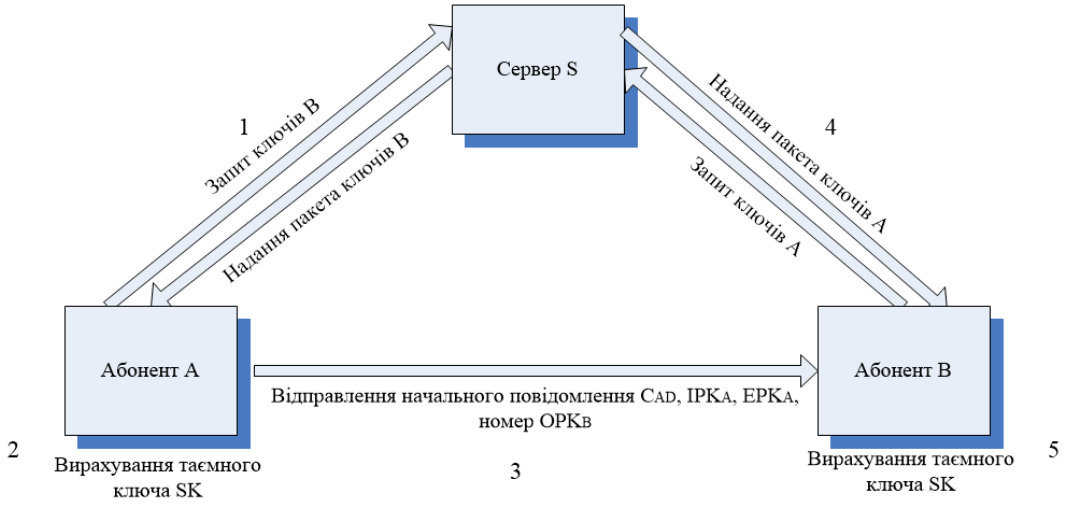

Рисунок 2.2 - Другий етап протоколу Signal – встановлення сеансу зв'язку

SK служить основою для формування ланцюжка ключів шифрування повідомлень. Коли ключ шифрування створено, абонент A шифрує симетричним алгоритмом своє ідентифікаційне повідомлення AD, складене із значень ідентифікаційних ключів відправника та одержувача, а також будь-якої додаткової ідентифікаційної інформації – імен абонентів, сертифікатів тощо.

Потім A відправляє одержувачу B криптограму C_{AD}, свій ідентифікаційний ключ IPK_A, короткостроковий відкритий ключ EPK_A, та інформацію про те, який із попередніх ключів OPK_B був використано для отримання ключа шифрування повідомлення.

Отримавши всю цю інформацію, абонент B зможе сформувати ключ SK для розшифрування повідомлення. Якщо повідомлення розшифровано вдало та ідентифікаційна інформація коректна, B продовжує використовувати ланцюжок ключів, отриманих із SK, для шифрування свого повідомлення.

Використані одноразові ключі OPK_B видаляються сервером, а відповідні їм OK_B – абонент B.

Слід зазначити, що якщо взаємодія абонентів із сервером S і один з одним відбувається в недовіреному середовищі, то можлива реалізація загрози "людина посередині" (MITM, the man in the middle), що дозволяє порушнику підміняти ключі при передачі та видавати себе за будь-яку зі сторін комунікації. Як правило, дана проблема вирішується за допомогою цифрової сертифікації та розгортання інфраструктури відкритих ключів PKI, проте протоколом Signal вони не описуються, а проміжний сервер не відіграє ролі центру сертифікації.

Захист від реалізації атак «людина посередині» покликана забезпечити використання на нижньому рівні захищеного транспортного протоколу (SSL/TLS), проте практично його реалізації у мобільних додатках найчастіше вразливі для цього типу атак. Крім того, використання SSL/TLS зберігає можливість реалізації MITM атак на самому сервері (наприклад, у разі контролю з боку спецслужб та адміністраторів системи).

Для підтвердження справжності другої сторони абоненти можуть порівнювати отриманий ідентифікаційний ключ IK через деякий автентифікований канал. Наприклад, вони можуть порівнювати відбитки цифрового підпису вручну або шляхом сканування QR-коду. Методи створення такого автентифікованого каналу виходять за межі опис протоколу Signal. Перевірка справжності сторін за зовнішнім каналу може проводитись до або після процедури погодження ключа, однак, як зазначено в [9] у більшості реалізацій така перевірка може бути здійснена лише після обміну повідомленнями.

Ще більш гостро стоїть проблема підтвердження справжності сервера розподілу ключів S під час реєстрації, не визначений у специфікації протоколу Signal. Без забезпечення довіри до сервера існує можливість підміни особистості будь-якого абонента. Таким чином, вирішення питання взаємної автентифікації сервера та клієнта лягає на конкретну реалізацію месенджера. Як правило, при установці додаток месенджера прив'язується до конкретного телефонного номеру, і клієнт автентифікується за допомогою одноразових SMS-паролей. Автентифікація сервера може проводитись на нижньому рівні за допомогою цифрових сертифікатів (як у браузерах), або за допомогою перевірки відбитків відкритого ключа, дані які можуть бути «захистами» в клієнтському додатку (як це зроблено, наприклад, в Telegram).

Для зниження негативного ефекту від можливої компрометації ключів використовується оригінальний Double Ratchet алгоритм, описує зміну

короткострокового ключа асиметричної схеми EK/EPK з кожним повідомленням у відповідь і зміну симетричних ключів у породжуваному ним ключовому ланцюжку (для шифрування кожного повідомлення використовується свій ключ). Узгоджене за допомогою DH значення секретного ключа SK є основою для отримання відправного ключа ланцюжка (RK, root key), ключа ланцюжка (CK, chaining key) та ключа шифрування повідомлення (MK, message key). Ключ ланцюжка CKj+1 виходять із попереднього CKj за допомогою конструкції HMAC.

Алгоритм формування ланцюжка ключів симетричного шифрування за одного з абонентів (абонента 1) показаний на рис.2.3.

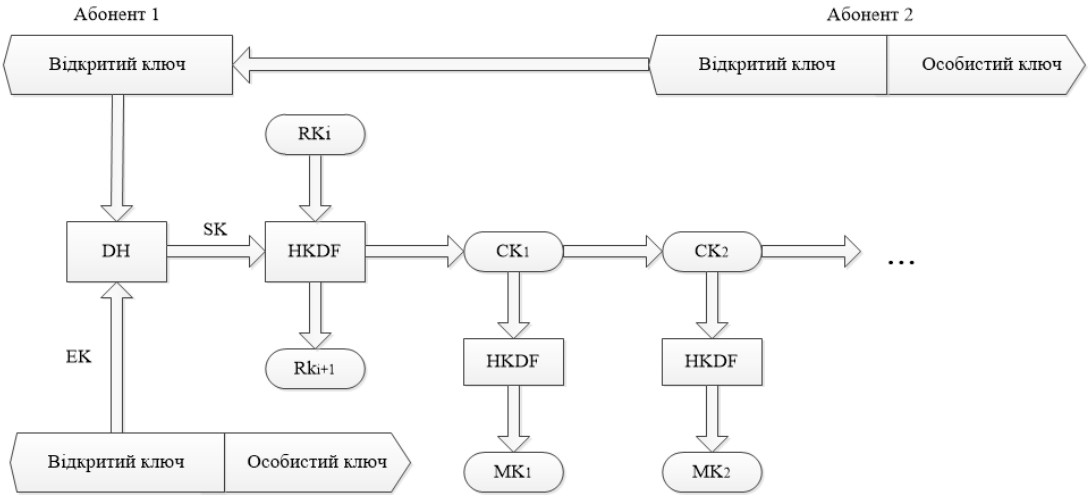

Рисунок 2.3 - Формування ланцюжків ключів шифрування повідомлень

Коли абонент розшифровує отримане повідомлення, він використовує для формування ланцюжка своє старе значення особистого ключа та надіслане йому значення відкритого ключа іншого абонента. В результаті ключі розшифрування збігатимуться з ключами, використаними для шифрування.

Якщо ж абонент хоче надіслати повідомлення у відповідь, він формує нову пару короткочасних ключів EK/EPK асиметричної схеми, та використовує її для формування нового ланцюжка, а відкритий ключ EPK нової пари відсилає разом із зашифрованим повідомленням.

Якщо ж абонент хоче надіслати наступне повідомлення, не отримавши відповідь на попереднє, він використовує наступний ключ шифрування повідомлення з поточного ланцюжка, не оновлюючи асиметричні ключі схеми.

Таким чином, симетричні ключі у ланцюжках виводяться KDF на основі нових значень DH на кожному етапі, тому кожне оновлення потребує знання свіжої інформації. Тому навіть якщо якийсь середньостроковий чи короткостроковий ключ був скомпрометований, він незабаром буде замінений новим, невідомим порушнику значенням.

Такий підхід дозволяє забезпечити специфічні властивості безпеки, такі як пряма секретність (forward secrecy) та безпека після компрометації, або посткомпрометаційна таємність (post-compromise security, post-compromise secrecy) [9].

Використання односпрямованих хеш-функцій (або HMAC) для формування ланцюжка ключів $x \rightarrow H(x) \rightarrow H(H(x)) \rightarrow \ldots$ дозволяє забезпечити властивість прямої секретності. Ця властивість означає, що якщо скомпрометовано поточний ключ, попередні значення ключів неможливо знайти. Це означає, що навіть у разі компрометації поточного ключа, порушник не зможе розшифрувати та прочитати повідомлення, надіслані раніше.

Використання для породження ланцюжків оновлюються узгоджених значень DH забезпечує властивість безпеки після компрометації (post-compromise security). Ця властивість дозволяє гарантувати безпеку протоколу навіть у разі, якщо секрети однією із сторін раніше були скомпрометовані (рис. 2.4). Можна сказати, що гарантія прямої таємності захищає сеанси від компрометації, що відбулася у наступні моменти часу, а посткомпрометаційна секретність захищає сеанси від компрометації, що сталася раніше.

Рисунок 2.4 - Сценарії атак, які розглядаються в рамках майбутньої секретності та посткомпрометаційної секретності

Алгоритм Double Ratchet дозволяє врахувати недоставлені повідомлення за рахунок включення до кожного заголовка повідомлення його номера у

ланцюжку відправки та довжину попереднього ланцюжка відправки. Це дозволяє одержувачу перейти до відповідного ключа повідомлення при збереженні значень пропущених ключів на випадок, якщо пропущені повідомлення надійдуть пізніше. Разом з тим, збереження застарілих ключів дещо послаблює забезпечуване алгоритмом Double Ratchet - властивість прямої секретності. X_3DH також має властивість майбутньої секретності.

Авторами дослідження, що спиралися у тому числі і на аналіз коду протоколу Signal, не було знайдено суттєвих недоліків з погляду застосування криптографії (за умови створення автентифікованого каналу обміну даними між абонентами та з сервером). Помилки коду протоколу, пов'язані з порушенням граничних значень у протоколі (наприклад, використання нульових значень ключа), а також загальні класи помилок програмного забезпечення.

Реалізації месенджерів містять поряд із кодом бібліотек протоколу Signal значний обсяг стороннього коду. Разом з тим, кожне застосування протоколу має особливості, що може істотно позначитися на надійності кінцевого шифрування. При цьому аналіз більшості реалізацій утруднений у зв'язку із закритістю їх коду (WhatsApp, Viber, Skype, Wickr, Threema). Наприклад, відомі проблеми з реалізацією протоколу в системі WhatsApp, яке дозволяє серверу примусово змінювати ключі користувача, що в свою чергу може призвести до розкриття недоставлених повідомлень. Подібна вразливість відсутня у месенджері Signal. Недосконалий і захист групових чатів WhatsApp, незважаючи на використання наскрізного шифрування [9].

Крім того, протокол Signal був надалі доповнений алгоритмом керування сеансами користувачів для забезпечення синхронізації листування на різних пристроях, управління паралельними сеансами та відновлення з резервних копій. В цьому підпротоколі повноваження сервера суттєво розширено, а компрометація хоча одного пристрою ставить під загрозу безпека усієї комунікації. Документація до алгоритму управління сеансами лише вказує на те, що зв'язок між пристроями та серверами має бути зашифрована та автентифікована, як і раніше, не обумовлюючи способів вирішення цих задач.

Додатково джерелом проблем безпеки може бути некоректна реалізація процедур, які не мають прямого відношення до протоколу. Так, наприклад, клієнтська частина месенджера Signal в процесі міграції від розширення для Chrome до повноцінного десктопного клієнта експортує повідомлення користувача в незашифровані текстові файли При цьому жодних попереджень

не виводиться, а створені файли залишаються на диску навіть після завершення апгрейду [9].

На відміну від вже згаданого WhatsApp, месенджер Telegram використовує власний протокол MTProto, безпека якого, попри заяви розробників, є спірним питанням. Telegram позиціонується як система з відкритим кодом, проте в вільному доступі відсутній вихідний код серверної частини, крім того, використовувані рішення не настільки докладно документовані, як у Signal.

Протокол визначає 3 рівні: високорівневий шар, визначальний взаємодія програми з API, криптографічний шар та компонент доставки, відповідальний за вибір способу передачі повідомлень (транспортного протоколу).

Криптопротокол MTProto за час свого існування зазнав кількох змін, і в даний час використовує асиметричну криптосистему RSA-2048, узгодження ключа Діффі-Хеллмана, симетричне шифрування за допомогою алгоритму AES-256 режимі IGE та хеш-функцію SHA-256.

На початковому етапі здійснюється автентифікація клієнта на основі обміну випадковими значеннями та реєстрація сформованого їм відкритого ключа асиметричної пари на сервері (рис. 2.5).

Автентифікація пристрою клієнта здійснюється за допомогою надсилання SMS-код на телефонний номер, вказаний при реєстрації. Якщо надалі користувач здійснить вхід з іншого пристрою, йому буде знову надіслано SMS-код.

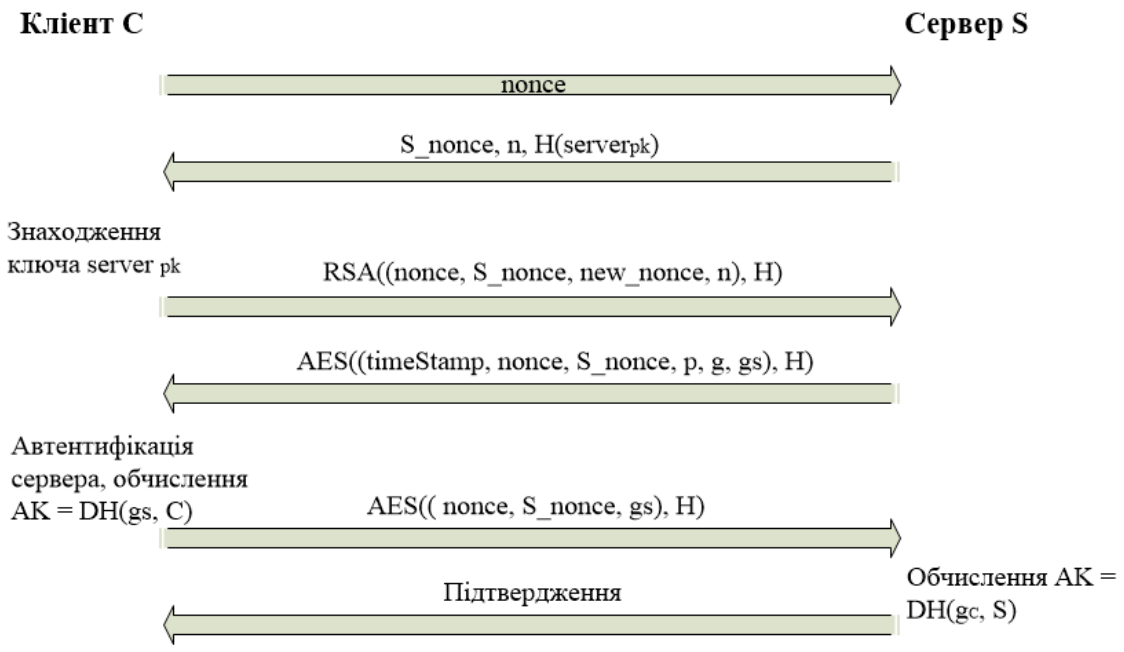

Рисунок 2.5 - Реєстрація клієнта у протоколі MTProto

1. Клієнт C надсилає запит на сервер S із випадковим рядком nonce.

2. S відправляє у відповідь іншу випадкову послідовність S_nonce, ціле число n (64 біта) та відбиток відкритого RSA-ключа сервера.

3. Клієнт C розкладає n на два прості числа p і q, p < q, і вибирає з набору публічних ключів сервера, що зберігається на пристрої, відкритий ключ serverpk, який має відповідати відбитку, що прийшов з сервера.

4. C вибирає інший випадковий рядок new_nonce, що відрізняється від попередніх рядків nonce та S_nonce. Цей рядок у відкритому вигляді не передавалась. Потім клієнт збирає набір із трьох випадкових рядків, чисел n, p та q, обчислює його хеш H і шифрує все це за алгоритмом RSA за допомогою ключа serverpk та відправляє на сервер S.

5. У відповідь сервер S передає свою мітку часу, значення nonce та S_nonce (що дозволяє клієнту аутентифікувати сервер), а також параметри криптосистеми Діффі-Хеллмана g, p і свій відкритий DH ключ gS і хеш вмісту. Отриманий пакет доповнюється випадковими значеннями і передається у зашифрованому вигляді. Для шифрування використовується алгоритм AES-256 на тимчасовому ключі та з вектором ініціалізації, отриманим на основі S_nonce та new_nonce (рис. 2.6).

6. Клієнт перевіряє надіслані значення, а потім вибирає секретне число C та обчислює за допомогою криптосистеми Діффі-Хеллмана загальний секретний ключ AK = DH(gS, C) та свій відкритий ключ gC. Потім gC значення nonce і S_nonce і хеш всього пакета шифруються AES і надсилаються на сервер S.

7. Отримані значення S достатні для формування сервером загального таємного ключа AK. Якщо всі надіслані клієнтом значення правильні, сервер посилає відповідь з підтвердженням (або з відмовою в іншому випадку).

Загальний секретний ключ AK тепер може використовуватись для шифрування обміну даними між клієнтом і сервером при використання хмарних чатів (без кінцевого шифрування).

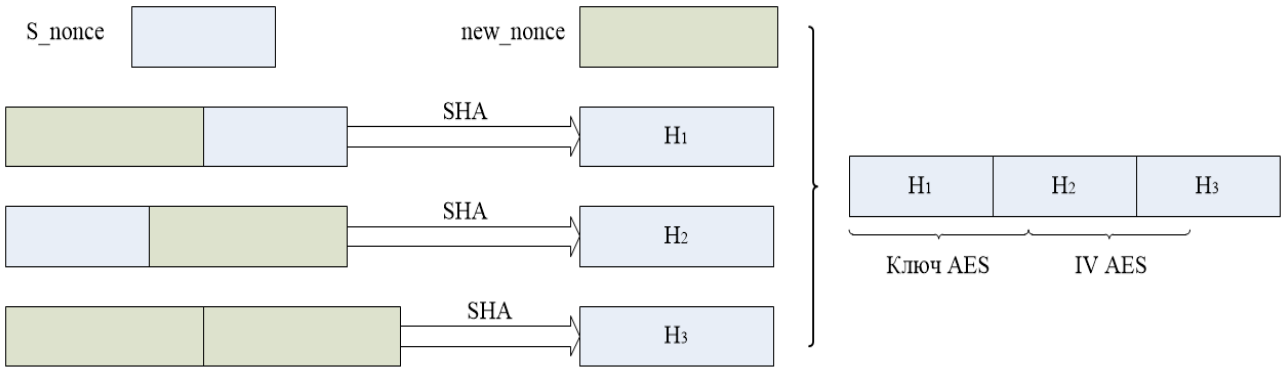

Рисунок 2.6 - Формування тимчасового ключа та вектора ініціалізації шифру AES під час реєстрації MTProto

Кінцеве шифрування в режимі секретних чатів виконується наступним чином. При ініціалізації секретного чату користувачі A і B виконують стандартний протокол Діффі-Хеллмана узгодження загального ключа AK без попередньої автентифікації сторін. Узгодження загального ключа періодично проводиться наново. Як уже зазначалося, оскільки узгодження ключа здійснюється без автентифікації каналу, це уможливлює реалізацію класичної атаки "людина посередині". Користувачам пропонується перед обміном повідомленнями проводити візуальну звірку відбитків AK як графічного коду.

Саме шифрування повідомлень користувача здійснюється за схемою, представленою на рис. 2.7 (заливкою тут відмічені секретні параметри шифрування). Додаткова інформація, що додається до повідомленню при шифруванні, включає вихідний та вхідний номер повідомлення, випадкові значення солі та доповнення, загальну довжину та інші значення. У процедурі шифрування, що використовується в хмарних чатах, додається до повідомлення додаткова інформація, яка кілько відрізняється, а загальна структура процедури шифрування залишається незмінною.

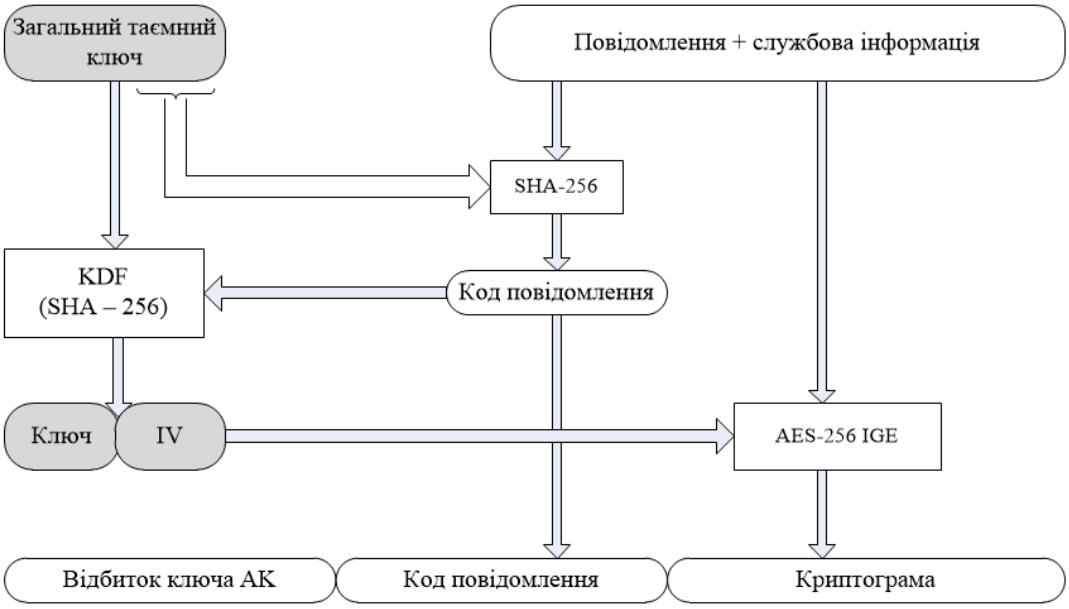

Рисунок 2.7 - Загальна схема шифрування повідомлень у MTProto

На основі інформації, що шифрується (тобто самого повідомлення з доданою до нього додатковою інформацією) та частини загального секретного ключа розраховується код повідомлення, що служить для перевірки цілісності, а також дозволяє сформувати різні ключі шифрування для різних повідомлень. Код повідомлення надсилається разом із криптограмою у відкритому вигляді. Для виведення ключів шифрування використовується функція на основі SHA-256, побудована за принципом, подібним до KDF.

Оскільки відбиток загального секретного ключа надсилається з кожним повідомленням, при використанні кінцевого шифрування абонент у будь-який момент може переконатися у справжності другий сторони комунікації за допомогою звірки графічних кодів, однак це доведеться робити вручну.

Слід зазначити, що повідомлення про виявлення вразливостей Telegram з'являються регулярно, і не менш регулярно вони спростовуються власниками месенджера, які заявляють про його виняткової безпеки.

Знання особливостей кінцевого шифрування дозволяє дійти розуміння існуючих обмежень та можливих проблем безпеки. Так, основною проблемою є реалізація автентифікації сторін комунікації. Єдиним справді надійним способом зв'язування відкритого ключа з абонентом та забезпечення аутентифікації сторони при децентралізованому (без участі сервера) розподіл ключів в асиметричних схемах є використання цифрової сертифікації. Останнє

неможливо поза інфраструктурою відкритого ключа (PKI). Вимушена відмова від використання цифрових сертифікатів призводить до перекладання вирішення проблеми аутентифікації сторін спілкування на самих абонентів, які мають здійснювати звіряння відбитків відкритих ключів або їх графічних уявлень щоразу, коли проводиться процедура узгодження загального ключа (на початку сеансу та у разі його зміни надалі). Це не найзручніший варіант автентифікації, оскільки:

- для зниження ймовірності розкриття шифру ключ може змінюватися досить часто;

- не всі реалізації месенджерів здійснюють повідомлення користувачів про зміну ключа;

- користувач повинен бути достатньо поінформований, щоб усвідомлювати необхідність звіряння ключів, і мати хорошу дисципліною, щоб виробляти її регулярно;

- якщо звірка проводиться візуально (як у Telegram) велика можливість помилки для зовні «схожих» графічних кодів.

Ще одна серйозна проблема пов'язана із синхронізацією листування для різних пристроїв під час використання кінцевого шифрування. Системи обміну повідомленнями вирішують цю проблему по-різному. Наприклад, Telegram і Skype відмовилися від синхронізації листування для секретних чатів (листування буде доступне тільки на тому пристрої, на якому розпочато); синхронізація виконується тільки для звичайних хмарних чатів, які не використовують кінцевого шифрування. Інші системи підтримують можливість синхронізації і при використання кінцевого шифрування, наприклад протокол Signal містить відповідний алгоритм. Однак залишаються питання до реалізації цієї функції. Наприклад, Signal (як і багато інших месенджери) дозволяє відкрити паралельну сесію (і отримати повний доступ до листування) на іншому пристрої, просто відсканувавши QR-код, що дає простір для зловживань навіть при короткочасний доступ порушника до пристрою. Для синхронізації листування на різних пристроях WhatsApp та Viber підтримують механізм відновлення повідомлень з хмари, які зберігаються у ньому у незашифрованому вигляді [9]. Таким чином, з'являється ще одне можливе джерело інформації про листування, захищеність якого забезпечується засобами, відмінними від наскрізного шифрування. Незважаючи на те, що створення резервних копій, як правило,

може бути відключено у додатку, вони можуть створюватися автоматично також самим пристроєм, і не завжди контролюються користувачем.

Ще одна проблема – можливість збирання метаінформації про контактах та діях абонентів самою системою обміну повідомленнями чи третіми особами (проблема захисту соціального графа). Увага до цього питання було залучено під час скандалу, пов'язаного з компанією Facebook, яка займалася широкомасштабним збором та продажем інформації про користувачів. Як правило, можливість такого збору обумовлюється в користувальницькій угоді месенджера. Наприклад, в угоді користувача WhatsApp – продукту, що належить компанії Facebook, зазначено, що месенджер збирає інформацію про діяльність абонентів (наприклад, як абоненти використовують послуги, як взаємодіють з іншими користувачами за допомогою сервісів системи тощо), журнали веб-сайту, інформацію про конкретний пристрій під час встановлення, доступу або використання сервісу системи (такі як модель телефону, його операційна система та інформація з браузера, IP-адреси та мобільної мережі, включаючи номер телефону). Водночас розробники месенджера Signal стверджують, що сервер системи зберігає лише номер телефону, вказаний абонентом при реєстрації, та дату останнього входу в систему (з точністю до дня). З іншого боку, як зазначалося вище, при використанні кінцевого шифрування адресна інформація передається у відкритому вигляді та може бути доступна порушнику.

Як видно, саме собою використання кінцевого шифрування не є гарантією безумовної захищеності, як це уявляють численні публікації, зводячи питання безпеки до того, чи включено в месенджері кінцеве шифрування за замовчуванням або ні (див. Додаток В).

Запропоновані такі критерії для оцінки безпеки месенджерів та проведено аналіз кількох найбільш відомих систем:

- ступінь централізації управління та архітектури системи (можливість роботи без підтримки серверної частини системи, можливість прямих peer-to-peer з'єднань абонентів без участі сервера);

- можливість анонімної реєстрації та використання;

- підтримка кінцевого шифрування;

- підтримка синхронізації секретних чатів;

-повідомлення про необхідність перевірки відбитків ключів співрозмовників у секретних чатах;

- заборона скріншотів у режимі секретного чату;

- підтримка групових секретних чатів;

-повідомлення про необхідність перевірки відбитків ключів співрозмовників у групових секретних чатах;

- захист соціального графа.

Вкажемо, не розкриваючи докладно, ще ряд моментів, які можуть служити джерелом проблем безпеки під час використання систем обміну повідомленнями на мобільних платформах.

Критичним з погляду безпеки є отримання порушником фізичного доступу до пристрою, у зв'язку з цим постають питання про надійність видалення інформації (старих повідомлень), створення локальних резервних копій листування (автоматично збереження повідомлень на пристрої) та захист локального сховища.

Обліковий запис користувача, що створюється системою, як правило, прив'язується до номера телефону, на який під час реєстрації або під час входу з іншого пристрою надсилається код підтвердження за допомогою SMS. Відома вразливість у протоколі стільникового зв'язку SS7 дозволяє здійснювати перехоплення SMS-повідомлень, як наслідок, порушник може зайти в обліковий запис абонента, знаючи лише номер його телефону. Останнє дозволяє, як мінімум, відправляти повідомлення від імені абонента, а в ряді випадків і отримати доступ до його листування.

Отримання несанкціонованого доступу до користувача даних з іншої програми або за допомогою шкідливого коду. Ця загроза має досить загальний характер, проте вона особливо актуальна для мобільних платформ, операційні системи яких мають обмежену модель безпеки.

Використання небезпечних клієнтів. Якщо абонент завантажує клієнтське програмне забезпечення не з офіційного магазину, а пряме посилання, велика ймовірність використання підробленого клієнта з неконтрольованими можливостями [9].

Висновок за розділом: таким чином, наявність криптографічних функцій є важливим, але далеко не єдиним фактором забезпечення безпеки мобільних систем, та месенджерів зокрема.

3 ПОРІВНЯЛЬНИЙ АНАЛІЗ ФУНКЦІЙ БЕЗПЕКИ ТА ПРИВАТНОСТІ МЕСЕНДЖЕРІВ

В цьому розділі буде проведено аналіз функцій безпеки та приватності найпопулярніших месенджерів, якими користуються українці у 2023- 2024 рр.

При створенні таблиць будуть використовуватися дані, які вдалося знайти в офіційних джерелах і підтвердити. Якщо інформація за будь-яким критерієм на поточний момент відсутня або ніяк не може бути перевірена, то в комірці пишеться – "немає відомостей". Якщо функція підтверджується, але є певні нюанси або особливості, що впливають на рівень безпеки або приватності, то прописується коментар у відповідній комірці.

При створенні таблиці порівняльного аналізу були перевірені такі критерії безпеки та приватності месенджерів:

1. Наскрізне шифрування - це коли дзвінки, повідомлення, фотографії та всі інші дані всередині чату доступні тільки двом співрозмовникам, без можливого потрапляння в треті руки. Поки повідомлення проходить весь шлях від одного користувача до іншого, воно перебуває в зашифрованому вигляді, тому його ніхто не може побачити, крім співрозмовника [10].

2. Збір даних та метаданих. Метадані, які кожен з нас генерує своїми діями в мережі, схожі з цифровим відбитком особистості. Месенджери також збирають метадані, які можуть описувати нашу особистість досить докладно. По суті це - всі дані, крім змісту безпосередньо повідомлення: наприклад, із ким із нашого списку контактів ми розмовляємо, як довго і як часто (відправник, одержувач, час надсилання, час прочитання). Це такий собі запис нашої активності. Також може збиратися інформація про використовуваний пристрій, IP-адресу, номер мобільного тощо [11].

3. Відкритий вихідний код додатка для обміну миттєвими повідомленнями дає змогу здійснювати комплексний аудит безпеки. Аматори, ентузіасти, експерти можуть зробити збірку додатка, дослідити його роботу і привернути увагу до слабких місць, до вразливостей як у серверній, так і в клієнтській частинах коду. З іншого боку, вільний доступ до коду дещо підвищує ризик того, що інформацію про виявлену вразливість можна використовувати зі злим наміром, доки її не буде закрито або хтось інший зі спільноти не зверне увагу на слабке місце [12].

4. Передавання даних третім особам. Третіми особами можуть виступати спецслужби, органи громадського порядку, урядові структури. Адміністрація одних месенджерів активно співпрацює з третіми особами, а інші принципово відмовляються передавати особисті дані [13].

5. Шифрування бекапів у хмарі. Далеко не всі месенджери застосовують шифрування для зберігання листування і файлів у хмарі. Успішна атака зловмисника на хмарну інфраструктуру може призвести до витоку конфіденційної інформації. Так само як і у випадку зі збором даних, інформація про те, чи дійсно бекап шифрується, є у відкритому доступі далеко не за всіма месенджерами [14].

6. Підтримка однорангового з'єднання. Однорангове, або пірингове (peer-to-peer), з'єднання виключає участь третьої сторони. Відправлені повідомлення надходять безпосередньо на пристрій адресата. Важливо зауважити, що таке з'єднання вільно дає змогу побачити, з ким і як довго воно встановлене, що, природно, впливає на анонімність і знижує рівень конфіденційності [15].

7. Інформація під час реєстрації. При створенні облікового запису в месенджері, наприклад, часто потрібно вказати номер мобільного телефону, який вкрай тісно пов'язаний з нашою реальною особистістю. Безпека даних може бути не порушена, але анонімність значно знижується. Що більше даних потрібно під час реєстрації, то нижча анонімність. Це може бути вимога адреси електронної пошти, додаток може запросити доступ до контактів або до вхідних SMS-повідомлень для верифікації. Підтвердження реєстрації може бути реалізовано через дзвінок на ваш номер [16].

Серед багатьох систем обміну повідомленнями, було обрано 9 найпопулярніших месенджерів в Україні на 2023 рік: Viber, WhatsApp, Signal, Discord, Telegram, Facebook Messenger, Wickr Me, Threema, Wire.

Для того аби оцінити безпеку даних користувача в тому чи іншому месенджері, визначимо ключові критерії безпеки, приватність та анонімність. Після цього буде можливо звести дані в таблицю, побачити загальну картину і зробити висновки.

Таблиця 3.1 - Порівняльний аналіз функцій безпеки месенджерів

	1	2	3	4	5	6	7	8	9
Месенджери / Критерій безпеки	Viber	WhatsApp	Signal	Discord	Telegram	Facebook Messenger	Wickr Me	Threema	Wire
Підтримка наскрізного шифрування за замовчуванням	Так	Так	Так	Ні (потрібно самостійно почати захищений чат)	Ні (потрібно самостійно почати захищений чат)	Ні (потрібно самостійно почати захищений чат)	Так	Так	Так
Підтримка наскрізного шифрування для дзвінків / відеодзвінків	Так	Так	Так	Ні	Так	Так	Так	Так	Так
Відсутність збору особистих даних користувача з боку адміністрації месенджера	Ні (контент користувача, місце розташування, ідентифікатори, покупки, контактна інформація, контакти)	Ні (контент, покупки, фінанси, місце розташування, контактна інформація, контакти, ідентифікатори)	Так	Ні (контент, ідентифікатори, контактна інформація, дзвінки, історія тощо)	Ні (контактна інформація, контакти, ідентифікатори)	Ні (контент, здоров'я і фітнес, покупки, фінанси, місце розташування, контакти, історія пошуку, історія переглядів, ідентифікатори)	Так	Так	Так
Повністю відкритий вихідний код (як серверної, так і клієнтської частин)	Ні	Ні	Так	Ні	Ні	Ні	Ні	Ні	Так

Продовження таблиці 3.1

	1	2	3	4	5	6	7	8	9
Можливість самостійно перевірити відбиток відкритого ключа	Так	Так	Так	Ні	Ні	Так	Так	Так	Так
Повідомлення в разі оновлення ключа шифрування співрозмовника	Так	Ні	Так	Ні	Ні	Ні	Так	Так	Ні
Додаток генерує і зберігає ключ безпосередньо на пристрої	Так	Так	Так	Так	Так	Так	Так	Так	Так
Хешує персональну інформацію (номер, список контактів тощо)	Ні	Ні	Ні	Так	Так	Ні	Так	Так	Ні
Підтримка PFS (Perfect Forward Secrecy)	Так	Так	Так	Ні	Ні	Так	Так	Ні	Так
Застосовуються надійні криптографічні алгоритми	Так (Curve25519 256 / Salsa20 128 / HMAC-SHA256)	Так (Curve25519 / AES-256 / HMAC-SHA256)	Так (Curve2551 9 / AES-256 / HMAC-SHA256)	Ні (RSA-1536 & 2048 / AES-256 / SHA-1)	Так (RSA 2048 / AES-256 / SHA-256)	Так (Curve25519 / AES-256 / HMAC-SHA256)	Так (ECDH512 / AES-256 / HMAC-SHA256)	Так (Curve25 519 256 / XSalsa2 0 256 / Poly130 5-AES 128)	Так (Curve255 19 / ChaCha20 / HMAC-SHA256)

Продовження таблиці 3.1

	1	2	3	4	5	6	7	8	9
Шифрування метаданих (відправник, одержувач, прочитано, доставлено, час відправлення, час прочитання тощо)	Ні	Ні	Так	Ні	Ні	Ні	Так	Так	Ні
Додавання контакту без передавання даних на сервер	Так	Ні	Ні	Ні	Ні	Ні	Ні	Так	Ні
Зберігання користувацьких даних із месенджера на пристрої в зашифрованому стані	Ні	Ні	Так (якщо активована парольна фраза)	Ні	Так (хмарне зберігання, але локальний кеш зашифрований)	Ні	Так	Так	Так
Підтримка двофакторної аутентифікації	Ні	Так	Так	Ні	Так	Так	Так	Так	Так
Шифрування бекапа листування в хмарі	Ні	Ні	Бекап зберігається тільки на пристрої в зашифрованому вигляді	Так	Так	Ні	Так (дані зберігаються на пристрої і в хмарі в зашифрованому вигляді і мають TTL: 30 днів для хмари)	Так	Бекап зберігається тільки на пристрої в зашифрованому вигляді
Проведено аудит вихідного коду та аналіз безпеки ентузіастами	Ні	Ні	Так (жовтень 2014)	Ні	Так (листопад 2015)	Ні	Так (серпень 2014)	Так (жовтень 2020)	Так (березень 2018)

Продовження таблиці 3.1

	1	2	3	4	5	6	7	8	9
Захист листування від прочитання адміністрацією месенджера	Так	Так	Так	Так (якщо активовано чат із наскрізним шифруванням, за замовчуванням вимкнений)	Так (якщо активовано чат із наскрізним шифруванням, за замовчуванням вимкнений)	Так (якщо активовано чат із наскрізним шифруванням, за замовчуванням вимкнений)	Так	Так	Так
Вхід за PIN-кодом / парольною фразою	Ні	Ні	Так	Ні	Так	Так (системний пароль)	Так	Так	Так
Підтримка альтернативного способу входу (за відбитком пальця, обличчя тощо)	Ні	Ні	Так	Ні	Так	Так	Так	Так	Так
Відсутність зберігання листування на сервері	Ні	Ні	Так	Ні	Ні	Ні	Ні	Ні	Так
Відсутність передачі особистих даних користувача державним органам безпеки	Так	Ні	Так	Ні	Ні	Ні	Так	Так	Так

Таблиця 3.2 - Порівняльний аналіз функцій приватності месенджерів

	1	2	3	4	5	6	7	8	9
Месенджер / Функція приватності	Viber	Whats App	Signal	Discord	Telegram	Facebook Messenger	Wickr Me	Threema	Wire
Можливість анонімної реєстрації	Ні	Ні	Ні	Ні	Ні	Ні	Так	Так	Ні
Можливість повного видалення акаунта із системи	Так	Ні	Так	Ні (акаунт прив'язаний до екосистеми Microsoft)	Так	Ні (акаунт прив'язаний до Facebook)	Ні	Так	Так
Можливість приховати дані профілю від усіх	Так	Так	Так	Ні	Так	Так (інтегрований профіль Facebook)	Так (у профілі тільки нікнейм)	Ні	Ні
Можливість приховати від усіх час останнього візиту	Так	Так	Так (час останнього візиту не фіксується)	Ні	Так	Так	Так (час останнього візиту не фіксується)	Так (час останнього візиту не фіксується)	Так (час останнього візиту не фіксується)
Можливість заборони пересилання повідомлень	Ні	Ні	Ні	Ні	Так	Ні	Так (опції пересилання повідомлень немає)	Так (опції пересилання повідомлень немає)	Ні
Підтримка видалення листування з пристрою і з сервера	Так	Так	Так	Так	Так	Так	Так	Так	Так

Продовження таблиці 3.2

	1	2	3	4	5	6	7	8	9
Можливість відключити сповіщення про доставку та прочитання повідомлення	Ні	Ні	Так	Так	Ні	Ні	Так (повідомлення про доставку та прочитання відсутні)	Так	Так
Можливість відключити попередній перегляд повідомлення на екрані сповіщень	Так	Так	Так	Ні	Так	Так	Так	Так	Так
Можливість відключити автоматичний попередній перегляд посилань	Ні	Ні	Так	Так	Так (тільки в секретному чаті)	Ні	Так	Так (прев'ю посилань не відбувається)	Так
Можливість відключити опцію "співрозмовник друкує повідомлення"	Ні	Ні	Так	Ні	Ні	Ні	Так (не використовується в додатку)	Так	Ні
Можливість видалення повідомлення для всіх учасників чату	Так	Так	Так	Так (у секретному чаті не підтримується)	Так	Так (якщо не було скарги на чат)	Так	Так	Так
Повідомлення учасників чату про зроблений скріншот листування	Ні	Ні	Ні	Ні	Так (тільки в секретному чаті)	Ні	Так	Так	Ні
Можливість приховати поточний статус (онлайн / офлайн) від усіх	Так	Так	Так (статус не фіксується)	Ні	Так	Так	Так	Так (статус не фіксується в додатку)	Так (статус не фіксується в додатку)

Таблиця 3.3 - Підтримка функцій безпеки та приватності популярних месенджерів

Месенджер / Функція чи критерій	Viber	WhatsApp	Signal	Discord	Telegram	Facebook Messenger	Wickr Me	Threema	Wire
Загальний бал безпеки та приватності	2	-10	46	-40	14	-8	52	50	31
Так (зелений: +2 бали; блакитний: +1 бал)	+36	+30	+56	+16	+40	+30	+60	+60	+49
Ні (жовтий: -2 бали)	-34	-40	-10	-56	-26	-38	-8	-10	-18
Особливості (білий: 0 балів)	0	0	1	0	0	0	0	0	1

Як видно з порівняльної таблиці, жоден месенджер не зібрав у собі всі розглянуті функції приватності та безпеки. Відокремити можна тільки один із трьох більш-менш виразно найкращих - це месенджер Wickr Me.

Месенджер завжди залишатиметься вкрай індивідуалізованим. Якщо один застосунок зручно, приємно і звично використовувати для особистих потреб спілкування, то інший може абсолютно не влаштовувати. Саме з цієї причини нам завжди доводиться використовувати не один месенджер, щоб підтримувати зв'язок з усіма контактами з нашого оточення.

За даними таблиць можна поділити аналізовані месенджери на такі категорії:

1. Небезпечні:
   - Discord;
   - WhatsApp;
   - Facebook Messenger.
2. Золота середина:
   - Telegram;
   - Wire;
   - Viber.
3. Найбезпечніші:
   - Signal;
   - Wickr Me;
   - Threema.

Signal - у плані безпеки та функціональності дуже гарний, проте є недолік, який вельми серйозно впливає на конфіденційність: не підтримується анонімна реєстрація, тому доведеться довірити свій номер мобільного телефону адміністрації месенджера [17].

Wickr Me підтримує анонімну реєстрацію. З особливостей - дані листування в зашифрованому вигляді зберігаються на сервері 30 днів. Також знадобиться почекати 24 години для того, щоб акаунт був видалений із системи. Але в іншому на сьогоднішній день це - найкращий вибір, що поєднує в собі належну безпеку і конфіденційність [18].

Threema - безпечний, але платний месенджер. Зберігає листування на сервері, має повністю анонімну реєстрацію. Має відкритий код і пропонує всі функції, які можна очікувати від найсучаснішого месенджера. Додаток також дозволяє здійснювати наскрізне шифрування голосу, відео та групових дзвінків [19].

Висновки за розділом: у третьому розділі було розроблено таблиці порівняльного аналізу функцій безпеки месенджерів, порівняльного аналізу функцій приватності месенджерів та таблицю підтримки функцій безпеки та приватності популярних месенджерів; поділено месенджери за категоріями виходячи з даних у таблицях та виявлено три найбезпечніших месенджери.

4 ПОРІВНЯННЯ ТА РОЗРАХУНОК ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ МЕСЕНДЖЕРІВ МЕТОДОМ АНАЛІЗУ ІЄРАРХІЇ

4.1 Заповнення таблиці відповідності

Спочатку проведемо порівняння месенджерів, проставимо відповідні оцінки та заповнимо у вигляді таблиці А.1 (див. Додаток А)

Для вирішення багатокритеріальної задачі, застосуємо метод аналізу ієрархії. Ідея цього метода полягає в розбитті однієї великої проблеми на декілька простих частин для подальшого аналізу.

Таким чином система дає результат, який може мати вигляд матриці пріоритетів, ці елементи матриці *W_ij* є інтенсивностним проявом елементом ієрархії відносно між собою елементів *i* та *j*.

Для того щоб провести розрахунок порівняння між месенджерами застосуємо перехід зі шкали оцінювання «Відсутня – Задовільно – Відмінно» до числової шкали оцінювання, наведеної на рисунку 4.1.

Відсутнє	1
Задовільно	3
Відмінно	5

Рисунок 4.1 - Конвертація шкали оцінювання «Відсутня – Задовільно – Відмінно»

Для того щоб було зрозуміло, що означає кожна оцінка в таблиці Б.1 буде наведено опис критеріїв оцінки та відповідна одиниця оцінювання (див. Додаток Б)

4.2 Розрахунок за методом аналізу ієрархії

Для того, щоб провести розрахунок та структурувати інформацію, зробимо таблицю у вигляді матриці (рисунок 4.2).

$$\begin{pmatrix} 5 & 3 & 3 & 5 & 1 & 3 & 1 & 5 & 5 \\ 3 & 3 & 3 & 5 & 1 & 3 & 3 & 5 & 5 \\ 1 & 1 & 5 & 5 & 3 & 5 & 1 & 3 & 3 \\ 5 & 1 & 3 & 5 & 5 & 5 & 3 & 5 & 3 \\ 5 & 5 & 5 & 3 & 5 & 1 & 1 & 5 & 3 \\ 3 & 3 & 5 & 5 & 3 & 5 & 3 & 1 & 3 \\ 1 & 1 & 5 & 5 & 1 & 5 & 5 & 1 & 1 \\ 5 & 1 & 5 & 3 & 5 & 5 & 3 & 5 & 3 \\ 5 & 1 & 3 & 3 & 1 & 3 & 1 & 3 & 1 \\ 5 & 5 & 5 & 5 & 5 & 5 & 3 & 5 & 3 \\ 1 & 1 & 1 & 5 & 1 & 1 & 1 & 3 & 1 \\ 1 & 5 & 3 & 3 & 5 & 3 & 1 & 5 & 1 \\ 5 & 1 & 3 & 5 & 5 & 5 & 1 & 1 & 3 \end{pmatrix}$$

Рисунок 4.2 – Матричне подання таблиці порівняння

Після побудови матриці, пріоритет кожного окремого об’єкту в ієрархії визначається оцінкою відповідного йому нормованого головного власного вектора даної матриці. Точне визначення власного вектору матриці пріоритетів досить складне, тому на практиці пропонується застосувати один з наступних способів:

1. Скласти усі елементи кожної строки та нормалізувати діленням кожної суми на суму всіх добутків елементів строк матриці. Перший елемент результуючого вектора буде пріоритетом першого об’єкту, другий – другого об’єкту і т.д.

2. Скласти елементи кожного стовпця та отримати зворотні величини цих сум. Нормалізувати їх так, щоб сума дорівнювала одиниці, поділив кожну зворотну величину на суму всіх зворотних величин.

3. Поділити елементи кожного стовпця на суму елементів даного стовпця (нормалізувати стовпець), потім скласти елементи кожної отриманої строки та поділити цю суму на число елементів строки.

4. Визначити середнє геометричне значення кожної строки та нормалізувати отримані числа.

5. Піднести матрицю до довільно великих ступенів, обчислювати суму елементів строк та нормалізувати отримані суми [20].

Використаємо перший спосіб, тобто складемо усі елементи кожної строки та нормалізуємо діленням кожної суми на суму всіх добутків елементів строк матриці:

$$V_i = \frac{\sqrt[n]{\prod_{j=1}^{N} W_{ij}}}{\sum_{i=1}^{N} \sqrt[n]{\prod_{j=1}^{N} kj}}; \quad (4.1)$$

де $\prod_{j=1}^{N} W_{ij}$ – добуток всіх елементів строк;

$\sum_{i=1}^{N} \sqrt[n]{\prod_{j=1}^{N} kj}$– загальної сума коренів n-ного ступеня від всіх добутків кожної зі строк матриці ймовірностей;

n – кількість елементів у строчці [20].

Розрахуємо загальну суму всіх добутків кожної строки матриці ймовірностей:

$$\sum_{i=1}^{N} \sqrt[n]{\prod_{j=1}^{N} kj} = \sqrt[13]{703\,125} + \sqrt[13]{3\,375} + \sqrt[13]{11\,390\,625} + \sqrt[13]{158\,203\,125} + \sqrt[13]{140\,625} + \sqrt[13]{6\,328\,125} + \sqrt[13]{1\,215} + \sqrt[13]{2\,109\,375} + \sqrt[13]{54\,675} = 25.379.$$

За формулою (4.1) були отримані наступні значення ймовірностей вищенаведених атак:

$$V_1 = \frac{\sqrt[13]{703\,125}}{25.379} = 0.111;$$

$$V_2 = \frac{\sqrt[13]{3\,375}}{25.379} = 0.074;$$

$$V_3 = \frac{\sqrt[13]{11\,390\,625}}{25.379} = 0.138;$$

$$V_4 = \frac{\sqrt[13]{1215}}{25.379} = 0.068;$$

$$V_5 = \frac{\sqrt[13]{140\,625}}{25.379} = 0.098;$$

$$V_6 = \frac{\sqrt[13]{6\ 328\ 125}}{25.379} = 0.131;$$

$$V_7 = \frac{\sqrt[13]{158203125}}{25.379} = 0.168;$$

$$V_8 = \frac{\sqrt[13]{2\ 109\ 375}}{25.379} = 0.121;$$

$$V_9 = \frac{\sqrt[13]{54\ 675}}{25.379} = 0.091.$$

Отримані результати занесемо в таблицю 4.3 у порядку зменшення.

Таблиця 4.3 – Результати розрахунків оцінок можливостей кожного з месенджерів

Месенджер		Відносна оцінка
1	Wickr Me	0.168
2	Signal	0.138
3	Facebook Messenger	0.131
4	Threema	0.121
5	Viber	0.111
6	Telegram	0.098
7	Wire	0.091
8	WhatsApp	0.074
9	Discord	0.068

Висновки з розділу: З отриманих результатів бачимо, що Wickr Me має найбільшу перевагу з представлених програм, вона славиться своєю приватністю та захищеністю даних, дозволяє зашифровувати передачу повідомлень, а також дозволяє користувачам реєструватися без використання особистого номера телефону або адреси електронної пошти, є можливість контролю над тим, які дані і дозволи надаються іншим користувачам та можливість використання месенджера на різних платформах (iOS, Android, Windows, тощо).

ВИСНОВКИ

Месенджери активно витісняють (і досить успішно) SMS як самостійний спосіб зв'язку. Вибір зручних та багатофункціональних мереж миттєвого обміну повідомленнями з кожним роком стає дедалі ширшим [21].

Для того, аби виявити найбезпечніший месенджер у 2023 році, яким без зайвих побоювань, будуть користуватися всі українці, в дипломній роботі був проведений аналіз систем миттєвих повідомлень; розглянуті загальні відомості системи миттєвих повідомлень кожного месенджера; було розглянуто безпеку месенджерів; проведено порівняльний аналіз функцій безпеки та приватності месенджерів та створено порівняльні таблиці разом з таблицею підтримки функцій безпеки та приватності популярних месенджерів; проведено розрахунок забезпечення безпеки месенджерів методом аналізу ієрархії та зроблено висновок, який з месенджерів є найкращим та найбезпечнішим.

Найефективніший месенджер із погляду безпеки особистих даних і забезпечення приватності на поточний момент, очолює Wickr Me.

Як видно з рисунку В.1 (див. Додаток В), кожен месенджер має свої переваги та недоліки. Ідеального застосунку з погляду абсолютної безпеки й анонімності обміну миттєвими повідомленнями на поточний момент не представлено, але Threema, Signal та Wickr Me цілком можуть бути використовувані українцями в 2023 – 2024 рр і надалі.

Під час побудови моделі загроз насамперед важливо визначити для себе особисто: від кого вибудовується захист і що саме ми захищаємо? Наскільки критичною є ситуація? Чи ми обираємо захищений месенджер заради модних тенденцій?

Неможливо забезпечити високу анонімність без шкоди для інших функцій. Наприклад, швидкість доставки повідомлення в безпечнішому месенджері значно знижується, є обмеження на розмір файлу, що надсилається, тощо. Доводиться приносити в жертву зручність користування і час заради підвищення пріоритетів безпеки.

При виборі месенджера для повсякденного спілкування пересвідченому користувачеві, буде оптимально поєднувати розумний баланс між зручністю і безпекою. [21]

ПЕРЕЛІК ПОСИЛАНЬ

1. Що таке месенджери та якими вони бувають. Месенджери – що це таке. Месенджер: що це. [Електронний документ] - Режим доступу: https://crashbox.ru/boot-disk/chto-takoe-messendzhery-i-kakimi-oni-byvayut-messendzhery---chto-eto/

2. Комплекс навчально-методичного забезпечення навчальної дисципліни "Безпека інфокомунікаційних мереж" підготовки бакалавра спеціальності 172 - Телекомунікації та радіотехніка [Електронний ресурс]: освітні програми "Інформаційно-мережна інженерія", "Телекомунікації" / ХНУРЕ; розроб. В. А. Золотарьов. – Харків, 2021. – 470 с.

3. ТОП-10 месенджерів для повідомлень та дзвінків у 2023 р. Владислава Рикова. 7 Листопада 2023р. [Електронний документ] - Режим доступу: https://vlada-rykova.com/ua/top-messendzherov/#i

4. Telegram. [Електронний документ] - Режим доступу: https://uk.wikipedia.org/wiki/Telegram

5. Компанія Threema. [Електронний документ] - Режим доступу: https://iitd.com.ua/threema/

6. Что такое Facebook? До Деніел Нейшнс. Оновлено 19 вересня 2023 р. [Електронний документ] - Режим доступу: https://www.lifewire.com/what-is-facebook-3486391

7. Wire (програмне забезпечення). [Електронний документ] - Режим доступу: https://uk.wikipedia.org/wiki/Wire

8. Безопасность данных во время войны – на личном опыте в оккупации. Пособие Константина Рыженко. [Електронний документ] - Режим доступу: https://irrp.org.ua/bezopasnost-dann%D1%8Bh-vo-vremya-vojn%D1%8B-na-lychnom-op%D1%8Bte-v-okkupaczyy-posobye-konstantyna-r%D1%8Bzhenko/#a003

9. Інформаційна безпека цифрового простору: колективна монографія /під ред. О. В. Стельмашонок, І. М. Васильєвої. - СПб.: Вид-во СПбДЕУ, 2019. (155 с.) - С. 20–36.

10. Наскрізне шифрування: що це і де застосовується? 13.12.2023. [Електронний документ] - Режим доступу: https://foxminded.ua/naskrizne-shyfruvannia-tse/

11. Метадані. Oct 28, 2022. [Електронний документ] - Режим доступу: https://ukrayinska.libretexts.org

12. Що таке відкрите джерело? Арнуд Енгельфітрі 15 березня 2011р. [Електронний документ] - Режим доступу: https://uk.itpedia.nl/2011/03/15/wat-is-open-source/

13. Повідомлення про обробку персональних даних. [Електронний документ] - Режим доступу: https://www.womensaid.net/povidomlennya-pro-obrobku-personalnih-danih/

14. Що таке "бекап" і для чого він потрібен? Лужна Софія -26.08.2023. [Електронний документ] - Режим доступу: https://itechua.com/articles/230192

15. Що таке Mesh-система: 9 переваг та 2 недоліки комірчастої домашньої мережі. 28.01.2022. [Електронний документ] - Режим доступу: https://www.moyo.ua/ua/news/chto_takoe_mesh_sistema_9_preimushchestv_i_2_nedostatka_yacheistoy_domashney_seti.html

16. Щодо захисту персональних даних в умовах воєнного стану. [Електронний документ] - Режим доступу: https://ombudsman.gov.ua/storage/app/media.pdf

17. Що таке Signal та чи варто ним користуватись? Yuri Svitlyk - 22/01/2021. [Електронний документ] - Режим доступу: https://root-nation.com/ua/articles-ua/services-ua/ua-signal-chi-varto-koristuvatis/

18. Wickr Me. 31 грудня 2023 року. [Електронний документ] - Режим доступу: https://neolurk.org/wiki/Wickr_Me

19. Threema. The Secure Messenger. [Електронний документ] - Режим доступу: https://play.google.com/store/apps/details?id=ch.threema.app&hl=uk

20. Метод аналізу ієрархій. [Електронний документ] - Режим доступу: https://dss.tg.ck.ua/ahp-help

21. Популярні інтернет месенджери. Що таке Messenger та як ними користуватися? Огляд кращих програм для спілкування на iOs та Android. 14.06.2019. [Електронний документ] - Режим доступу: https://bumotors.ru/uk/popular-internet-messengers-what-is-messenger-and-how-do-i-use-it.html