МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Дніпровський національний університет залізничного транспорту імені академіка В. Лазаряна

Кафедра «Електронні обчислювальні машини»

«ДО ЗАХИСТУ»

Завідувач кафедри
Жуковицький І.В.
(підпис) (ПІБ)
«____» _____ 20____р.

ДИПЛОМНА РОБОТА

на здобуття освітнього ступеня «магістр»

Галузь знань 12 Інформаційні технології
(шифр) (назва)

Спеціальність 125 Кібербезпека
(код) (повна назва)

Тема Дослідження та розробка системи захищеного обміну повідомленнями

Theme Research and development of secure messaging system

Керівник дипломного проекту _____ _____ Остапець Д.О.
(посада) (підпис) (ПІБ)

Консультант розділу з БЖД _____ _____ Музикін М. І.
(посада) (підпис) (ПІБ)

Нормоконтролер _____ _____ Шаповалов В. О.
(посада) (підпис) (ПІБ)

Студент групи КБ1921 _____ Зимін С.О.
(група) (підпис) (ПІБ)

Student Zymin Serhii
(family name)

Дніпро
2020

РЕФЕРАТ

Дипломна робота з теми «Дослідження та розробка системи захищеного обміну повідомленнями» складається з 6 розділів, 15 ілюстрацій, 3 таблиці, 20 літературних джерел та 3 додатків. Загальний обсяг дипломної роботи складає 62 сторінка.

Об'єкт дослідження — месенджер — система для обміну повідомленнями мережею Internet, та технології, які використовувались підчас передачі та зберіганні конфіденційних даних користувачів.

Мета кваліфікаційної роботи — розробка месенджеру — мобільного додатку, що забезпечує захист даних користувачів, і може вдало протидіяти спробам несанкціонованого доступу до листування абонентів шляхом використання шкідливого програмного забезпечення на пристрої , на якому розташований клієнт месенджера, підчас атаки типу «людина посередині» та фізичному захопленні пристрою абонента.

Використання подібного месенджеру може знизити рівень комфортності листування, але суттєво підвищить рівень інформаційної безпеки учасників обміну повідомленнями в ньому. Месенеджер рекомендовано до застосування частиною населення з підвищеними вимогами до конфіденційності інформації у їх професійному або особистому аспектах життя.

Економічна ефективність даної системи надзвичайно висока. Адже для функціонування месенджера достатньо постійно забезпечувати живленням одну серверну машину. Оскільки дані регулярно видаляються з усієї системи, питання заміни обладнання виникне тільки у разі несправності устаткування.

Ключові слова: МЕСЕНДЖЕР, ОБМІН ПОВІДОМЛЕННЯМИ, КРИПТОЗАХИСТ, АВТЕНТИФІКАЦІЯ, КОНФІДЕНЦІЙНІСТЬ, ІНФОРМАЦІЙНА БЕЗПЕКА, ЗАХИСТ ДАНИХ, WCF, C# , ANDROID.

ABSTRACT

Graduate work which dedicated to the theme which called "Research and development of secure messaging system" includes 6 parts, 15 illustrations, 3 tables, 20 literature sources and 3 applications. General volume of this work is 62 pages.

A research object is messenger – secure messaging system, and technologies of data transmition and saving confidential users data.

The goal of qualified work — development of messenger. Present messenger is a mobile application which provides high safety level of user's data. Also it must be able successfully opposite to hacker's attempts to made unauthorized intrusion by using spy software at the user's device, taking control server or user's one. Also it must be able to opposite to "man-in-middle"-type attacks.

Using of same messenger can debase comfortable of using this application, but one essentially boosts cyber security level of other members in a chat. App is recommended to use by people groups, which think that confidential is important fact in them life.

The cost-benefit of present messenger is very well? Because for successfully work of system enough to supply constantly only one server. Data is regular deletes from server. That is why crush case is single reason to spending money.

Keywords: MESSENGER, MESSAGING SYSTEM, CRYPTOSECURITY, AUTHENTIFICATION, CONFIDENTIAL, CYBER SECURITY, DATA PROTECTING, WCF, C#, ANDROID.

ВСТУП

Після зростання кількості кібератак у всьому світі надзвичайно гостро стоїть питання конфіденційності даних пересічних громадян, що через спілкування інтернет-мережею з іншими користувачами піддають загрозі несанкціонованого доступу дані, розголошення яких може мати дуже тяжкі наслідки як в фінансовому аспекті, так і нести загрозу життю людини або її здоров'ю.

У зв'язку з цим в даній дипломній роботі буде розроблена захищена система обміну повідомленнями. Метою даної системи – месенджера — є вирішення проблеми несанкціонованого доступу до інформації користувача, порушення її цілісності та конфіденційності.

1 ОГЛЯД ІСНУЮЧИХ СИСТЕМ ОБМІНУ ПОВІДОМЛЕННЯМИ

1.1 Загальні відомості

Сьогодні месенджер –це один з найпоширеніших інструментів швидкісного обміну інформацією. Месенджери дозволяють миттєво передавати текстову, фото-відео та аудіо інформацію та відслідковувати факт ознайомлення з нею.

У даному розділі буде проведений огляд трьох найпоширеніших месенджерів та здійснений аналіз їх можливостей та рівня інформаційного захисту.

Месенджер — програмний додаток для обміну інформацією текстового, аудіо та графічного формату в мережі Internet між двома або більше абонентами.

Клієнт — програмне забезпечення, яке знаходиться на пристрої абонента, призначене обробляти, зберігати дані отримані сервером та надсилати дані до сервера.

Сервер — апаратне забезпечення, яке призначене зберігати, отримувати, обробляти дані, надані клієнтом або іншим сервером, надсилати дані до клієнта або іншого сервера.

Автентифікація — процес підтвердження справжньості суб'єкта під час спроби отримати доступ до об'єкта з обмеженим доступом.

Ідентифікація — процес розпізнавання суб'єкта аобо груп суб'єктів серед інших суб'єктів за рахунок унікальної властивості суб'єкта, що розпізнається.

Авторизація — процес визначення повноважень суб'єкта щодо впливу на об'єкт.

Шифрування — процес оборотного перетворення інформації, а саме повне викривлення її змісту, об'єму та сенсу, з метою уникнення несанкціонованого доступу з боку зловмисника під час передачі даних між абонентами.

Дешифрування — процес перетворення інформації із зашифрованого виду у початковий з відновленням змісту, об'єму та сенсу інформації.

Ключ шифрування — публічні або секретні дані, що є необхідними даними під час шифрування інформації та її дешифрування.

Шифрограма — інформація у зашифрованому виді без можливості ознайомитися з її початковим змістом, уникаючи дешифрування.

Хеш — безповоротно перетворена електронна інформація із абсолютним спотворенням сенсу, обсягу та змісту у фіксований за довжиною блок даних, значення якого унікальне і буде повністю зміненим при зміні інформації перед її перетворенням.

Електронний цифровий підпис — хеш повідомлення підписаний публічним ключем асиметричної криптосистеми.

Конфіденційність — властивість даних, що передбачає певну міру секретності, недоступності, що дозволяє ознайомлення з даними лише тим суб'єктам, які мають на це право.

Цілісність — властивість даних, що передбачає відсутність будь-яких якісних перетворень, які змінюють зміст, сенс та об'єм інформації, а також факт її наявності.

Доступність — властивість даних, що передбачає можливість до зчитування, зміни, видалення, запису інформації або декількох з вище зазначених операцій.

1.2 Аналіз месенджера Telegram

1.2.1 Функціональність

Згідно офіційних даних сьогодні месенджер Telegram використовують більше 400 000 користувачів у всьому світі [1].

Компанія «Telegram», позиціонує свій додаток як месенджер, в якому всі персональні дані користувачів та їх листування є конфіденційними.

Месенджер Telegram надає своїм користувачам можливість швидкого обміну текстовими повідомленнями, зображеннями, аудіо-файлами, які включають голосові повідомлення, відео-записами, відео-повідомленнями, та іншими файлами, які не є виконуваними та не перевищують розмір у 2ГБ, а також трансляції або поштучної передачі інформації про місце знаходження клієнта за допомогою супутників GPS. Наявна функція інтернет-дзвінків з використанням або без відео-зв'язку між користувачами. Кожне повідомлення окрім свого змісту має час відправлення у клієнті відправника, час надходження у клієнті адресата та індикатор статусу повідомлення який визначає стадію передачі повідомлення до адресата:

- клієнт намагається встановити з сервером з'єднання та розпочати передачу повідомлення,
- повідомлення відправлене з клієнта відправника на сервер,
- повідомлення знаходиться на сервері та готове до відправки з сервера на клієнт отримувача,
- повідомлення надійшло до клієнта адресата,
- отримувач повідомлення повністю або частково ознайомлений з його змістом.

Будь-які повідомлення у приватному листуванні, з якими користувач має змогу ознайомитись, за бажанням користувача можуть бути технічно та візуально безслідно видаленими як локально, так і в клієнті співбесідника в односторонньому порядку.

Telegram надає можливість спілкування бесідами колом у декілька абонентів, та створення Telegram-каналів, адміністратор або користувачі-модератори уповноважені адміністрацією каналу, ведуть інформаційне сповіщення відвідувачів каналу. Кожне повідомлення за дозволом адміністратора каналу може мати можливість бути прокоментованим іншими відвідувачами ресурсу.

Месенджер також надає змогу створювати секретні бесіди, повідомлення абонентів в яких автоматично видаляються на усіх клієнтах учасників через визначений автором проміжок часу.

Telegram є одним з небагатьох месенджерів, що дозволяють створювати, та публікувати у каналах опитування декількох видів, редагувати надіслані повідомлення упродовж доби з моменту їх надходження до клієнта адресата.

1.2.2 Архітектура

Для зберігання даних Telegram використовує хмарні сховища та клієнти абонентів, що дозволяє зробити висновок, що архітектура месенджера є клієнт-серверною. Передача повідомлення від абонента А абоненту В відбувається за наступним алгоритмом:

1) Аліса створює повідомлення і натискає кнопку відповідальну за надсилання повідомлення.
2) Повідомлення зашифроване шифром довгострокового типу записується клієнтом Аліси до пам’яті пристрою.
3) Те ж повідомлення зашифроване шифром симетричного типу надсилається клієнтом Аліси до сервера у мережі Internet.
4) Після отримання шифрограми сервер надсилає сигнал її надходження до клієнта Аліси.
5) Сервер опитує клієнт Боба стосовно готовності прийняти повідомлення Аліси. Якщо клієнт під’єднаний до мережі Internet, то шифрограма передається мережею Internet до клієнта Боба. Якщо ні – клієнт Боба при відновленні зв’язку з Internet мережею опитує сервер стосовно наявності на сервері повідомлень призначених для нього. Для кожного повідомлення на сервері зберігається його хеш.

6) Після отримання шифрограми на клієнт Боба повідомлення дешифрується, і Боб має змогу ознайомитись з ним.
7) Дешифроване повідомлення шифрується клієнтом Боба шифром довгострокового типу і зберігається у пам’яті пристрою
8) До клієнта Аліси надходить підтвердження надходження повідомлення до клієнта Боба.

Після фактичного ознайомлення Боба з повідомленням до клієнта Аліси надходить підтвердження цього факту.

1.2.3 Захист даних

Захист відбувається за допомогою розробленого Telegram протокола MTProto. Передача повідомлень шифрується симетричним ключем за протоколом Діфі-Хелмана, що обчислюється за участі криптосистеми RSA. Для верифікації повідомлень використовується хеш-функція MD5. У склад протоколу MTProto входить протокол TLS версії 1.3 що забезпечує саму передачу повідомлень та додаткову безпеку підчас обміну повідомленнями. Схема встановлення з’єднання за протоколом TLS версії 1.3 наведена на рисунку 1.2.

Необхідно зауважити, що механізми передачі застраховані від атаки типу «людина посередині» тільки за рахунок перевірок на справжність сертифікатів, якими обмінюються клієнт і сервер підчас встановлення з’єднання. Якщо зловмиснику вдасться непомітно для механізмів перевірки сфальсифікувати сертифікати сервера, то вся система шифрування підчас передачі даних може бути скомпрометованою, а конфіденційність листування порушеною.

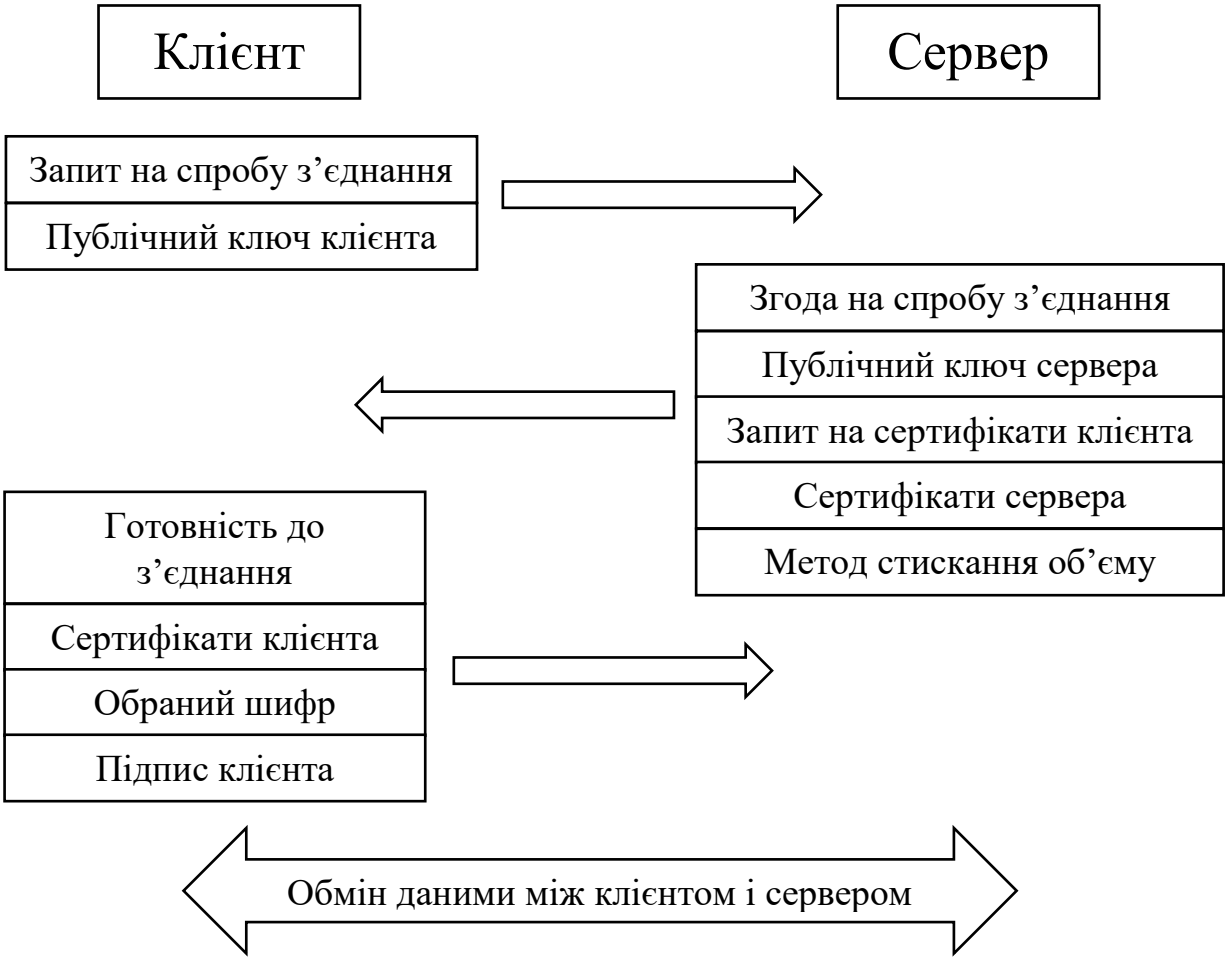

Рисунок 1.1 — Узагальнена схема з’єднання за протоколом TLS версії 1.3

Telegram реєструє користувачів у відповідній базі даних, яка знаходиться на сервері та дозволяє виконувати автентифікацію й ідентифікацію з будь-яких пристроїв, які підтримують можливість використання вище зазначеного додатку. Реєстрація відбувається за номером SIM-карти, що дозволяє ідентифікувати користувача, та OTP-пароля, який надходить на SIM-карту абонента в SMS-повідомленні, що є формою автентифікації. Також підтримується можливість автентифікації, підчас входу до свого акаунту, за довгостроковим паролем, який створюється користувачем.

1.3 Аналіз месенджера Viber

1.3.1 Функціональність

У 2010 році ізраїльська компанія «Viber Media S.à r.l.» створила однойменний месенджер, кількість користувачів якого сьогодні за офіціцйними даними компанії перевищує 1млрд [2].

Функціональність месенджера Viber за багатьма можливостями співпадає з функціональністю додатка Telegram. Але існують суттєві відмінності:

- Viber дозволяє користувачам здійснювати банківські операції через чат-ботів, в той час, коли чат-боти Telegram не мають такої можливості.
- Компанія «Viber Media S.à r.l.» стверджує, що після надсилання повідомлення адресату, копія повідомлення на сервері видаляється, і єдиним місцем знаходження повідомлень є клієнти абонентів, в той час коли Telegram певний час зберігає все листування і готовий надати можливість завантажити дані свого листування з серверу у випадку видалення відповідних файлів з файлової системи пристрою абонента.
- На відміну від Telegram, Viber підтримує тільки поштучне надсилання геолокаціїї клієнта, тому не підтримує можливість трансляціїї геолокації певний проміжок часу.
- Присутня функція надсилання секретного повідомлення з його автоматичним видаленням на усіх клієнтах учасників обміну інформацією через певний проміжок часу.
- Наявна функція видалення повідомлень на клієнті їх автора або додатково на клієнті співучасника розмови, відрізняється подальшою присутністю факту видалення повідомлень для обох сторін, ліквідація якої можлива тільки за повного видалення чату.

1.3.2 Архітектура

Архітектура месенджера Viber дуже схожа з відповідними параметрами Telegram. Але на відміну від Telegam, розробники Viber запевняють, що не зберігають листування користувачів у будь-якому вигляді на своїх серверах після досягнення повідомлення свого адресату. Тому після видалення месенджера одного й того ж

самого акаунту на всіх пристроях абонента, у разі повторного встановлення додатку, відновлюється інформація лише про факт участі абонента у бесідах. Зміст бесід, а також чати з абонентом повністю видаляються. З тої ж причини, у разі локального видалення одного або декількох надісланих абоненту файлів з файлової системи пристрою, втрачається можливість повернути зміст файлів шляхом повторного завантаження, навіть якщо співбесідник чату або бесіди має вище згадані дані в наявності на своєму пристрої. Але факт передачі файлів у такому випадку буде збережений. Viber надає змогу зберегти дані, у випадку видалення додатку та його повторного встановлення, за рахунок синхронізації з іншими клієнтами того ж акаунту на відповідних пристроях того ж самого абонента, або з використанням створених за бажанням користувача резервних копій листування, які у подальшому зберігаються на серверах компанії “Google”. Через дані обставини компанія «Viber Media S.à r.l.» попереджає, що не несе жодної відповідальності за конфіденційність даних користувача, у разі створення резервних копій листування.

1.3.3 Захист даних

Захист даних відбувається за допомогою розробленого компанією протоколуї. Шляхом експерименту за допомогою прослуховування трафіку підчас обміну інформацією через додаток було виявлено використання протоколу TCP, а також TLS версії 1.2, пакети якого не містили назви протоколу захисту.

Щоб здійснити реєстрацію користувача в месенджері, необхідно надати ім’я та прізвище, номер SIM-карти абонента та мати змогу надати можливість прийому підтверджуючого дзвінка ініційованого службами Viber за даним номером. Для вдалої автентифікації на додатковому пристрої абонента, клієнт з вже автентифікованим акаунтом на пристрої, що містить зареєстровану в базі даних SIM-карту, має зчитати QR-код виведений на екран пристрою, де відбувається спроба автентифікаціїї після вдалої ідентифікації акаунту.

Підвищує конфіденційність факт безповоротного видалення листування після видалення месенджера та повторного встановлення додатку. Можливість надсилати секретні повідомлення, що ліквідуються через заданий час на усіх клієнтах в усіх

абонентах листування, знижають ризик втрати або порушення конфіденційності передаваної інформації.

Секретні повідомлення із таймером самоліквідаціїї, зі слів розробників, захищаються наскрізним end-to-end шифруванням. Компанія запевняє, що не має доступу до ключів шифрування, через що ознайомлення з дешифрованою інформацією доступне тільки абонентам листування. Але варто зазначити, що шляхом експерименту був виявлений факт того, що шифрограми, які надсилають один одному абоненти, певний час зберігаються на серверах Viber.

1.4 Аналіз месенджера Signal

1.4.1 Функціональність

Месенджер Signal, створений у 2014 році, має повністю відкритий код та створений для високого рівня захисту даних користувачів, що певною мірою може завдати шкоди користувачу у зручності та функціональності додатку [3].

За функціоналом Signal схожий з месенджером Viber. Месенджер підтримує обмін файлами, даними геолокації, аудіо, відео інформацією та текстовими повідомленнями. Але нажаль додаток не підтримує створення відео-повідомлень. На відміну від вище наведених месенджерів, Signal має функцію заборони створення скріншотів підчас використання додатку користувачем, що знижує імовірність отримання даних користувача шляхом встановлення шпіонського програмного забезпечення та моніторингом клієнта на пристрої та супутнім збереженням зображень екрану в мить відображення конфіденційної інформації користувача у месенджері. В Signal наявна функція «інкогніто-клавіатура», що перешкоджає персоналізованому навчанню intelisense-системи клавіатури. У зворотному випадку подібне навчання призводить до збереження даних, що можуть бути використані підчас лінгвістичного аналізу повідомлень абонента з метою його ідентифікації, якщо конфіденційність даних подібного навчання буде порушена. Доступна функція ретрансляції інтернет-дзвінків крізь сервер Signal, що перешкоджає спробам

зловмисника дізнатись реальні IP-адреси абонентів. Цей захід знижує якість дзвінка, але підвищує рівень захисту від фізичних та юридичних осіб, що за законом України не мають права ознайомлюватись зі змістом розмови абонентів. Месенджер дозволяє увімкнути функцію відсутності індикації факта створення повідомлення для співбесідника абонентом перед надсиланням цього повідомлення. Але з активуванням даної функції, абонент втрачає доступ до такої ж самої індикації з боку співучасника листування. Signal надає можливість листування SMS повідомленнями та захисту наведеної інформації підчас зберігання на пристрої абонента. Також підтримується функція видалення повідомлень через визначений проміжок часу на усіх клієнтах співучасників діалогу.

1.4.2 Архітектура

Архітектура Signal з метою забезпечення мінімальної зручності листування включає сервер для прийома повідомлень від клієнтів відправників і доставки повідомлень адресатам. В цілому, архітектура Signal не має суттєвих відмінностей від вище згаданих месенджерів. Але розробники стверджують, що не зберігають на серверах Signal шифрограми листування після доставки повідомлень своїм адресатам. Наявна функція резервного копіювання даних, яка після створення не зберігається на сторонніх серверах або серверах розробників.

1.4.3 Захист даних

Месенджер Signal зберігає дані листування на пристрої абонента у вигляді шифрограм, створених за допомогою парольної фрази користувача та шифрів довгострокового типу. Месенджер регулярно вимагає введення парольної фрази користувача для доступу до листування у додатку.

Підчас передачі повідомлень месенджер використовує end-to-end шифрування, що є складовою протоколу Signal. Захист даних відбувається з використанням таких протоколів як Діфі-Хелмана для створення симетричних ключів шифрування, AES-256 , Curve25519 – шифр на еліптичних кривих де використовується крива Монтгомері для наскрізного шифрування, та HMAC-256 для хешування повідомлень.

Також, як і в попередніх месенджерах, присутня функція вимкнення попереднього перегляду змісту, до яких ведуть посилання на сторонні ресурси у листуванні, що також ускладнює фішингові атаки зловмисників.

Месенджер не наполягає на наданні абонентом дозволу до камери, мікрофону, телефонної книги, геопозиції пристрою для роботи додатку, що дозволяє уникнути використання потенційних каналів витоку інформації. Це дозволяє використовувати функціонал Signal для мінімального рівня зручності який потребує користувач, водночас із забезпеченням захищеності даних в усіх інших аспектах використання додатку. Таким чином є можливість регулювання балансу між функціональністю месенджера та захистом його даних.

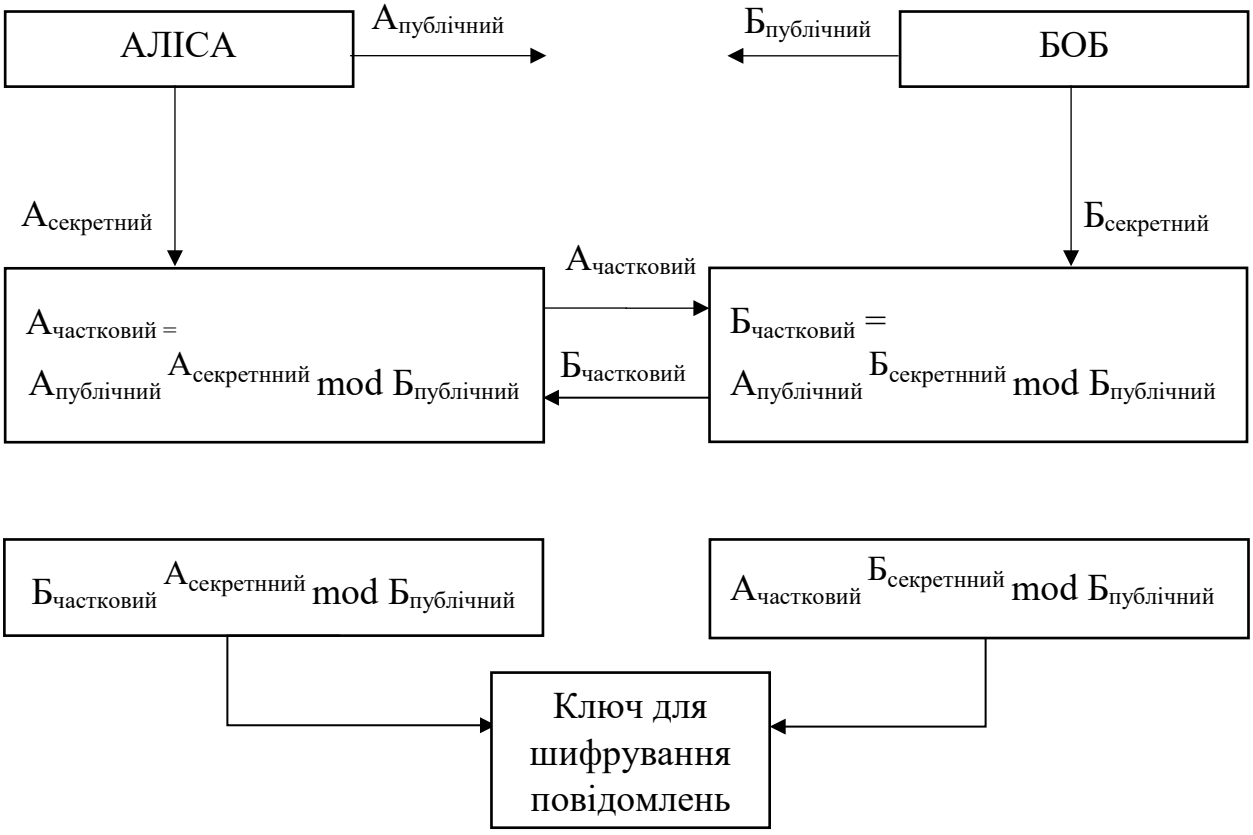

Рисунок 1.2 – Узагальнена схема створення симетричного ключа для шифрування повідомлення за алгоритмом Діфі-Хелмана.

1.5 Порівняльна характеристика властивостей месенджерів.

Підчас аналізу месенджерів була складена порівняльна таблиця. (Таблиця 1)

Таблиця 1 – Порівняння за функціональністю та захищеністю даних

Назва властивості додатку	Telegram	Viber	Signal
Резервне збереження даних	так	опціонально	опціонально
Десктопні версії	так	так	так
Наявність мобільних версій	так	так	так
Наскрізне шифрування	опціонально	опціонально	так
Видалення повідомлень за таймером	опціонально	опціонально	опціонально
Функція трансляції геолокації	так	ні	ні
Функція поштучної передачі геолокації	так	так	так
Шифрування даних підчас їх збереження на пристрої абонента	так	так	так
Чат-боти	так	так	ні
Вразливість до атаки «MIM»	так	так	так
Реєстрація за номером телефону	так	так	тка
Можливість одностороннього видалення повідомлень у всіх учасників бесіди	так	так	так
Приховування факту одностороннього видалення повідомлення	так	ні	ні
Використання парольної фрази	опціонально	ні	так
Використання OTP-паролей підчас автентифікації користувача	так	ні	так
Ретрансляція інтернет дзвінків	ні	ні	опціонально

1.5 Висновки за розділом

В результаті проведеного аналізу, було виявлено, що підчас використання месенджерів з'являється загроза порушення конфіденційності та цілісності користувацьких даних у випадку доступу зловмисника до пристрою абонента, на якому встановлений додаток. Також в разі виникнення несанкціонованого доступу до сервера, може бути скомпрометоване минуле та подальше листування користувачів. У таблиці 1 наведене порівняння можливостей месенджерів.

Signal є месенджером, де за допомогою опціонального використання функцій та дозволів додатку на використання вбудованого в пристрій обладнання та банків даних, користувач має можливість забезпечити рівень конфіденційності листування згідно його потреб. Але варто відзначити, що месенджер не може гарантовано протидіяти атакам типу «людина посередині», тому зберігається загроза порушення конфіденційності користувацьких даних у випадку доступу до сервера збоку зловмисника.

Месенджер Telegram є додатком, в якому дані користувачів захищаються системами шифрування, які можуть вдало протидіяти спробам порушення конфіденційності та цілісності інформації. Але суттєвим недоліком є те, що у разі спланованої атаки типу «людина посередині», зловмисники, маючи на озброєнні сфальсифіковані сертифікати сервера, які клієнт не в змозі відрізнити від справжніх, конфіденційність та цілісність даних опиняються під загрозою, а ключі криптосистем скомпрометованими. Теж саме відбудеться у випадку отримання зловмисником доступу до хмарного сховища, де зберігаються ключі та шифрограми листування користувачів, або до пристрою конкретного користувача месенджера.

Месенджер Viber може протидіяти спробам заволодіти даними при викраденні пристрою користувача з SIM-картою. Оскільки OTP-пароль з великою імовірністю може бути прочитаним у стані вімкненого екрану заблокованого гаджета, за умови вдалого парольного захисту сканер QR-коду з метою підтвердження справжньості об'єкта, який намагається увійти до акаунту, не зможе бути готовим до зчитування верифікуючого зображення.

Використання протоколу TLS версії 1.2 знижує рівень захисту на користь підтримки месенджером більшості операційних систем та їх версій. Резервні копії, підвищують інформаційний ризик, оскільки зберігаються на серверах компанії «Google» у не захищеному вигляді. А через клонування SIM-карти та видалення додатку на пристрої абонента або вимкнений стан пристрою, зловмисник може отримати повний доступ до листування користувача.

Також варто відзначити, що немає жодних офіційних підтверджень здібності систем захисту месенджера протистояти атакам типу «людина посередині», висока імовірність яких з’являється при використанні сервера у якості посередника.

2 ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ, ЗАСОБІВ ТА ПРОТОКОЛІВ ЗАХИСТУ В СИСТЕМАХ ОБМІНУ ПОВІДОМЛЕННЯМИ

2.1 Аналіз протоколів передачі даних

2.1.1 Протоколи TCP/IP

В залежності від потреб у використанні, існуючі протоколи передачі даних відрізняються за багатьма характеристиками. Серед них рівень сумісності роботи з іншими протоколами, швидкість передачі даних, рівень надійності передачі інформації, тощо[6].

TCP/IP — Transmission Control Protocol / Internet Protocol — сімейство протоколів TCP/IP (далі стек TCP/IP) призначених для передачі даних. Стек TCP/IP грає роль основи, у передачі даних, для використання криптографічних протоколів передачі.

Під час передачі, файли розбиваються на окремі частини – кадри. Кадри разом із відповідною службовою інформацією формують пакети, які є основною структурною одиницею у потоку передачі даних – трафіку.

Наступний алгоритм висвітлює основний принцип дії стеку TCP/IP під час передачі даних:

1) Клієнт, який хоче здійснити з’єднання із сервером, надсилає йому службове повідомлення зі стартовим номером послідовності пакетів ISN та синхронізуючим встановленим бітом SYN, а також портом клієнта, з якого надіслане повідомлення, та портом сервера, якому призначене дане повідомлення.
2) Сервер отримує від клієнта повідомлення, заносить до пам’яті номер послідовності і відповідає повідомленням яке містить встановлені біт SYN та біт підтвердження ACK з відповідним полем, яке містить номер ISN збільшений на одиницю. Сервер також генерує і надсилає свій номер послідовності байтів, що нумерує байти у повідомленнях та не дозволить переплутати байти підчас прийому з даними інших з’єднань.

3) Клієнт надсилає серверу повідомлення із встановленим бітом підтвердження ACK з відповідним полем, яке містить згенерований сервером номер послідовності збільшений на одиницю, та номер байту даних, який очікується на передачу до сервера.
4) Відбувається передача даних, які містять як сегменти даних, так і номери місця знаходження їх у файлах, а також номери послідовності пакетів підчас передачі.
5) Завершення з'єднання відбувається повідомленням сервера клієнту із встановленням біту завершення FIN та біту підтвердження ACK.
6) Клієнт теж повинен розірвати з'єднання, надіславши повідомлення із встановленим бітом ACK та FIN.

Переваги:

- швидкість передачі даних,
- поширюваність використання,
- контроль доставки пакета до адресата,
- впорядкування блоків даних за допомогою номерів послідовності

Недоліки:

- незахищеність даних підчас передачі,

2.1.2 Протокол TLS

TLS – Transport Layer Security – це протокол передачі даних, який передбачає асиметричне шифрування повідомлень з метою протидії спробам перехопити інформацію. Існує три версії протоколу: TLS 1.1, TLS 1.2, TLS 1.3 [6]. Нижче наведений механізм останньої версії, оскільки TLS 1.3 є попередніми TLS 1.2 та TLS 1.1, які мають додаткові функції та оптимізовані алгоритми роботи.

Принцип встановлення з'єднання схожий з принципом стеку TCP/IP, але є передача іншої інформації під час обміну, службовими повідомленнями, які ініціалізують з'єднання [7].

1) Клієнт, який хоче здійснити з'єднання із сервером, надсилає повідомлення, яке містить поля з наступною інформацією:

- версію протоколу TLS,

- 32 байти випадкових значень клієнта за для упередження підміни часу на вузлах мережі,
- ідентифікатор сесії, який дозволяє серверу та клієнту активувати раніше встановлені сесії,
- перелік шифрів, які підтримує клієнт, в якому порядок пунктів визначає пріоритет бажання клієнта використати визначений шифр (перший - найбажаніший),
- перелік методів стискання об’єму даних, які підтримує клієнт,
- дані декількох розширень протоколу TLS, які дозволяють використовувати нові технології шифрування та передачі даних, використання яких почалося пізніше ніж, затвердження протоколу TLS.

Кожне з полів перед змістом має значення своєї довжини.

2) У відповідь сервер або надсилає повідомлення про помилку з даними щодо неї, або відповідне службове повідомлення для встановлення з’єднання:
   - версію протоколу TLS,
   - 32 байти випадкових значень сервера,
   - ідентифікатор сесії,
   - обрана сервером сукупність шифрів з відповідного переліку клієнта,
   - обраний сервером метод стискання об’єму даних,
   - дані декількох розширень протоколу TLS.

   Підчас кожної сесії , окрім наведених параметрів, узгоджується алгоритм PRF для генерації сеансового ключа на основі даних, переданих клієнтом та сервером, алгоритм визначення MAC - коду автентифікації повідомлення, основний секретний ключ з 48 байтів, відомий обом легітимним учасникам обміну.

   Наступним передається сертифікат сервера, який містить публічний ключ сервера, та інші сертифікати підтверджуючі справжність першого.

   Далі передається повідомлення із серверними даними, які є частиною необхідної інформації для створення загального сеансового ключа. Повідомлення містить

параметри протоколу Діфі-Хелмана а також тимчасовий ключ RSA, підпис сервера за допомогою систем RSA або ECDSA на основі хеш-функцій MD5 та SHA-1.

Після цього надсилається повідомлення із запитом на сертифікат клієнта, яке містить перелік типів сертифікатів та криптосистем, який підтримує сервер, а також алгоритми підпису та хеш-функції.

Останнім у зазначеній черзі повідомлень на відповідь клієнту є дані, які надають підставу вважати, що сервер передав всю частину початкових ініціалізуючих даних.

3) Використовуючи отриманий від сервера публічний ключ, клієнт перевіряє справжність підпису повідомлення сервера. Клієнт надає серверу сертифікат, необхідний для автентифікації, згенерований власноруч 48-байтовий випадковий секретний ключ RSA, зашифрований публічним ключем клієнта, або згенерований клієнтом публічний ключ за алгоритмом Діфі-Хелмана. Клієнт підписує це повідомлення.

   Далі передається повідомлення підтвердження довіри серверу.

   Наступним повідомленням клієнт доводить до відома сервера, що шифр обрано, а всі наступні повідомлення будуть зашифровані відповідним домовленостям чином.

   Остання ініціалізуюча інформація збоку клієнта містить хеш від усіх попередніх повідомлень ініціалізації наявної сесії, щоб сервер мав змогу перевірити справжність ініціалізації. Це повідомлення передається вже у зашифрованому виді.

4) У випадку вдалої верифікації сервер надає клієнту свій сигнал, що подальший обмін буде захищений відповідним шифром і що ініціалізація завершена

5) Відбувається захищений обмін даними. Кожне повідомлення має шифрограму а також MAC код автентифікації повідомлення.

Недоліки:

- Ще не всі популярні браузери підтримують цю версію протокола.

Переваги:

- висока швидкість передачі даних

- підвищений рівень безпеки
- гнучкість до переходу на старіші версії протоколу у випадку відсутності змоги абонента підтримувати версію TLS 1.3;

порівняно легка конфігурація, що знижує імовірність виникнення вразливостей безпеки через помилку підчас налаштування

2.1.2 Протокол SSL

Протокол SSL — Secure Socket Layer — криптографічний протокол, який був розроблений у 1996 році для захищеного обміну інформацією.

Захист даних складається з двох процесів: автентифікації клієнта та шифрування передаваних даних.

SSL є незалежним від прикладного рівня протоколом, що є його перевагою. Даний протокол після автентифікації клієнта узгоджує алгоритм шифрування і ключ сесії передачі даних між сторонами — клієнтом і сервером. Шифрування даних залежно від налаштувань протоколу може відбуватись як симетрично, так і асиметрично. Алгоритм роботи протоколу SSL приведений нижче:

1) Клієнт надсилає серверу запит на з'єднання, який складається з інформації, чи потрібний новий майстер-ключ, переліку базових шифрів, які підтримує клієнт та запиту на сертифікат сервера. Якщо в новому майстер-ключі немає потреби, сторони переходять до наступного кроку. У зворотньому випадку клієнт здійснює запит на майстер-ключ сервера.
2) Сервер дає згоду на спробу з'єднання, надсилаючи у відповідь ідентифікаційний номер сесії, свій сертифікат та перелік шифрів, які підтримує сервер. Також у разі створення нового шифру, надсилає свій публічний ключ та запитує сертифікат клієнта.
3) Клієнт перевіряє сертифікат сервера і повідомляє сервер про результат перевірки, надсилає обраний алгоритм шифрування зі спільних з сервером шифрів, надсилає у випадку необхідності новий майстер-ключ, зашифрований публічним ключем сервера. А також надсилає свій сертифікат серверу.
4) Сервер перевіряє сертифікат клієнта і дає згоду на обмін повідомленнями.

5) Відбувається подальший захищений симетричним ключем обмін інформацією. Симетричні ключі створюються на основі майстер-ключа.

Переваги:

- протокол сумісний з багатьма пристроями та більшістю програмного забезпечення з можливістю передачі даних мережею,
- сумісність з технологією VPN.

Недоліки:

- обмежена підтримка сучасних веб-технологій,
- можлива легка підміна сертифікату.

2.1.3 Висновки

На підставі проведеного аналізу протоколом передачі даних у месенджері обрано TLS версії 1.3, оскільки даний протокол має найвищу сумісність з криптосистемами та порівняно високий рівень захисту сертифікацією від атак типу «людина посередині» [8]. У таблиці 2.1 представлене порівняння можливостей протоколів.

2.1.4 Порівняльна характеристика властивостей протоколів передачі даних

Підчас аналізу було складено таблицю порівняльних характеристик вище згаданих протоколів. (Таблиця 2)

Таблиця 2.1 — порівняльна характеристика протоколів передачі даних.

Властивість	SSL 3.0	TLS 1.3
Підтримка шифра Fortezza	так	ні
Основа для секретного ключа	Значення функції з використанням попереднього секретного ключа	Значення псевдовипадкової функції
Заходи щодо відсутності сертифіката	Попередження	Запит або надсилання додаткових автентифікуючих даних
Кількість симетричних шифрів, що підтримуються	5	6
Кількість асиметричних шифрів, що підтримуються	5	4
Імовірність вдалої підміни сертифіката	висока	мала

2.2 Аналіз шифрів використовуваних в месенджерах

2.2.1 Алгоритм RSA

RSA – асиметрична криптосистема, принцип дії якої полягає у розділенні великого числа на два простих множники. Цей шифр відноситься до довгострокового типу. Розглянемо приклад, де сервер є отримувачем, а клієнт – відправником [9].

1) Клієнт та сервер генерують пару секретних та відкритих ключів кожний за наступним алгоритмом:
   1) обираються два великі прості числа p і q,
   2) визначається число n за формулою $n=p\times q$
      та φ за формулою $\varphi = (p-1)(q-1)$,
   3) знаходиться число e, взаємно просте з φ та менше за φ,
   4) обчислюється число d, яке відповідає умовам $d\times e\equiv 1 \bmod \varphi$ та $d<\varphi$,

   Таким чином згенерований публічний ключ, який складають число e та n, а також секретний з чисел d та n. Шифрування відбувається представленням інформативного блоку даних та зведенням його у степінь e і подальшим діленням результату за модулем n. Отримане число і є частиною шифрограми, дешифрування якої полягає у подібному зведенні захищених даних у степінь d за модулем n.
2) Сервер та клієнт обмінюються своїми публічними ключами.
3) Клієнт шифрує публічним ключем сервера своє повідомлення.
4) Клієнт шифрує (ставить електронний цифровий підпис) хеш повідомлення своїм секретним ключем для того, щоб сервер мав змогу розшифрувати своїм секретним ключем підпис та порівняти хеш від клієнта з власноруч створеним хешем результату дешифрування.
5) Клієнт передає серверу шифрограму - захищені дані та підпис.
6) Сервер перевіряє повідомлення на відсутність порушення цілісності та фальсифікації даних.

На рисунку 2.1 зображена деталізована схема роботи алгоритму RSA.

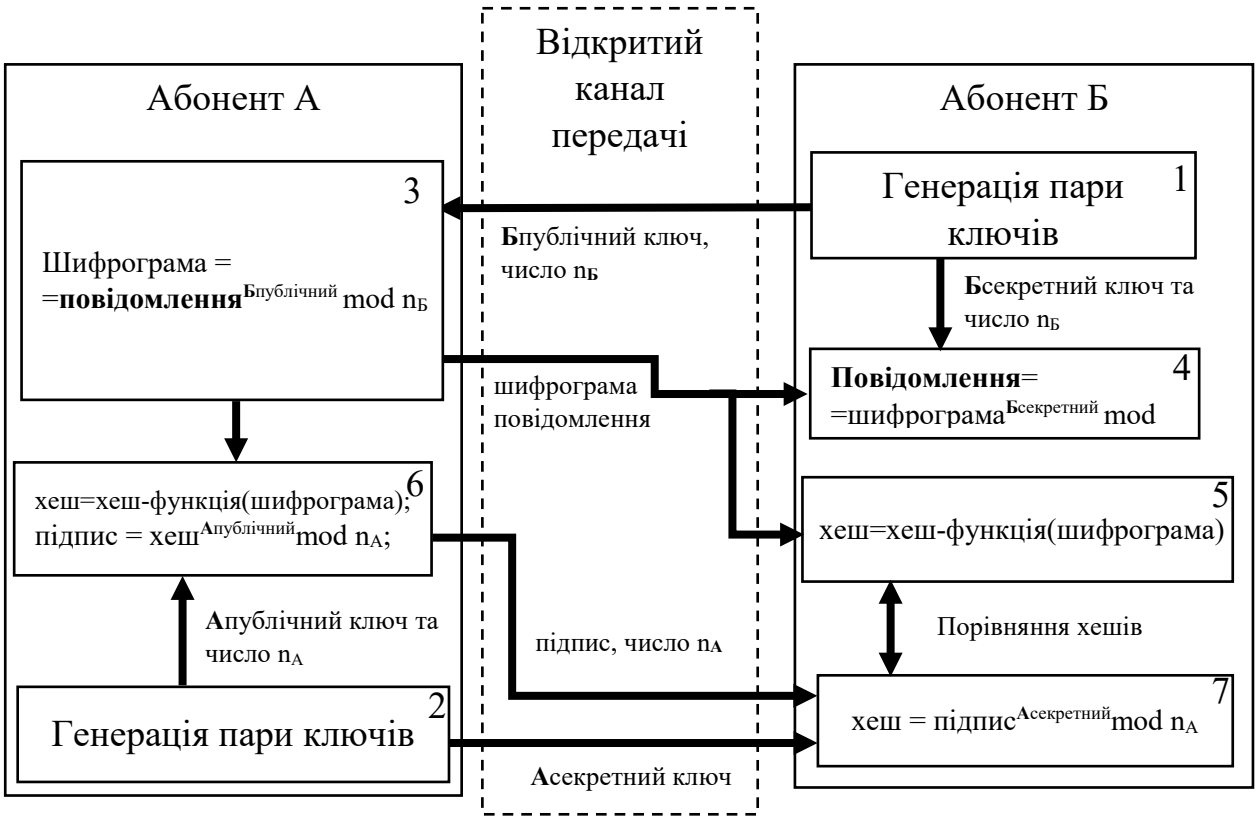

Рисунок 2.2 — Схема роботи алгоритму RSA.

Недоліки:

- процес шифрування займає багато часу порівняно з іншими криптосистемами;
- для максимального зниження ризику кожної передачі даних ключі мають замінюватись новими, що займає багато часу;
- криптосистема не може протидіяти нападу типу «людина посередині»
- потреба у генерації великої кількості ключів у випадку збільшення кількості учасників обміну даними.

Переваги:

- система є одною з найефективніших проти атаки перебором за умови великої довжини ключів;
- будь-яку зміну змісту повідомлення або його фальсифікацію буде викрито, якщо попередити іншими засобами атаку «людина посередині»
- Одна пара ключів може використовуватись декілька разів, не даючи певний час зловмисникові шансу на компроментацію ключів шляхом перебору [11].

2.2.2 Алгоритм Діфі-Хелмана

Криптосистема Діфі-Хелмана — асиметричний шифр, принцип роботи якого заснований на частковому обміні ключами з метою створення єдиного симетричного ключа для шифрування повідомлень [10].

1) Клієнт та сервер генерують пару секретних та відкритих ключів кожний за алгоритмом RSA.
2) Сервер та клієнт обмінюються своїми публічними ключами.
3) Клієнт обчислює свій частковий ключ за фомулою:
   $КлючКлієнта_{частковий} = (КлючКлієнта_{публічний})^{КлючКлієнтаСекретний} \bmod \bmod КлючСервера_{публічний}$.
4) Сервер також обчислює свій частковий ключ:
   $КлючСервера_{частковий} = (КлючКлієнта_{публічний})^{КлючСервераСекретний} \bmod \bmod КлючСервера_{публічний}$.
5) Клієнт та сервер обчислюють повні ключі для шифрування:
   $Повний_{Клієнта} = (КлючСервера_{частковий})^{КлючКлієнтаСекретний} \bmod \bmod КлючСервера_{публічний}$.
   $Повний_{Сервера} = (КлючКлієнта_{частковий})^{КлючСервераСекретний} \bmod \bmod КлючСервера_{публічний}$.
6) Отримані повні ключі однакові і можуть за допомогою симетричних шифрів шифрувати повідомлення та розшифровувати.

Недоліки:

- захист від атаки типу «людина посередині» відсутній,

Переваги:

- швидка операція шифрування даних,
- будь-яка кількість учасників обміну даними може вдало і з малими витратами обчислювальних та часових ресурсів вести шифрування.

2.2.3 Висновки

За результатами проведеного аналізу, усі наведені криптосистеми були обрані автором для подальшого використання в додатку та задіяні у додатку. Алгоритм RSA шифрує дані для довгострокового зберігання на пристрої. Криптосистема Діфі-Хелмана призначена до шифрування обміну повідомленнями.

2.3 Аналіз хеш-функцій

2.3.1 Хеш-функція MD5

MD5 —хеш-функція, яка перетворює блок даних на 128 біт хешу. Алгоритм її дії наступний:

1) В кінець блоку вхідних даних дописується один байт із значенням 0x80 і доповнюють нульовими бітами поки довжина повідомлення не зможе бути порівняна з виразом 448 mod 512.
2) Далі у повідомлення додають 64 біти із значенням довжини вхідного блоку даних.
3) Створюється буфер з 4 слів розміром по 32 біти кожний з наступними 16-річними значеннями:

   слово A: 01 23 45 67,

   слово B: 89 ab cd ef,

   слово C: fe dc ba 98,

   слово D: 76 54 32 10.

   Дані слова призначені для збору хеша.
4) Ініціалізуються 4 логічні функції для зміни значень вхідних 32 біт на інші значення вихідних 32 біт на основі використання побітової арифметики:

   F(X,Y,Z) = XY v not(X) Z,

   G(X,Y,Z) = XZ v Y not(Z),

   H(X,Y,Z) = X xor Y xor Z,

   I(X,Y,Z) = Y xor (X v not(Z)).

Після цього хеш підсилюють 64 слова довжиною 32 біти, які містять псевдовипадкове значення залежне від формули: $2^{32} \times |\sin(i)|$, де і вимірюється в радіанах та означає номер рядка.

5) Кожний 512-бітний блок вхідних даних підлягає 4 етапам обчислення по 16 раундів кожний. Через це 512 біт розбиваються на масив 32-бітних слів розміром 16 елементів. Розпочинаються 4 етапи по 16 раундів наступних дій:
   a) На початку етапу створюються тимчасові 32-бітні змінні: AA, BB, CC, DD та відбувається заміна значень:

      AA=A;

      BB=B;

      CC=C;

      DD=D.
   b) Відбуваються 16 раундів наступних дій:
      1) A = B + ((A + F(B,C,D) + X[k] + T[i]) <<< s), де A, B, C, D — 32-бітні регістри, F(B,C,D) — одна з логічних функцій, X[k] — k-й елемент 16-бітного блоку, T[i] — і-й елемент таблиці із синусоїдальними значеннями, <<< s — побітова операція циклічного зсуву ліворуч на s бітів.
      2) A = D;

         D = C;

         C = B;

         B = B + (F <<< s[i]);
   c) В кінці кожного етапу сумується результат:

      A = AA + A;

      B = BB + B;

      C = CC + C;

      D = DD + D.
6) Побайтовий вивід значень регістрів ABCD і буде хешем MD5.

Недоліки:

- існує відносно легкий спосіб для зламу хеш-функції за допомогою так званих райдужних таблиць [12],
- завелика імовірність колізії – одного хешу за різними значеннями вхідних даних.

Переваги:

- порівняно з іншими функціями вища продуктивність.
- добре підходить для вияву фальсифікацій або порушення цілісності даних підчас миттєвого обміну повідомленнями.

2.3.2 Хеш-функція SHA-256

SHA-256 —хеш-функція, яка перетворює блок даних на 256 біт хешу. На сьогоднішній день не існує алгоритму принципового зламу даної хеш-функції. Алгоритм її дії наступний:

1) В кінець блоку вхідних даних дописується один байт із значенням 0x80 і доповнюють нульовими бітами поки довжина повідомлення не зможе бути порівняна з виразом 448 mod 512.
2) Далі у повідомлення додають 64 біти із значенням довжини вхідного блоку даних.
3) Створюється 8 32-бітних констант з перших значень після цілої частини квадратних коренів перших 8 простих чисел.
4) Створюється масив k[i] з 64 32-бітних констант з перших значень після цілої частини квадратних коренів перших 64 простих чисел.
5) Кожний 512-бітний блок вхідних даних підлягає обчисленню по 16 раундів кожний. Через це 512 біт розбиваються на масив 32-бітних слів розміром 16 елементів. Додаємо до цього масиву ще 48 слів заповнених нулями. Таким чином створений масив на 64 32-бітні елементи w[i], де i — номер елемента масиву.
6) Виконується цикл з наступними діями:

a) усі нульові елементи, починаючи з 16-го до 63-го слова підлягають обробці за наступною формулою:

w[i]=w[i-16]+((w[i-15]>>>7) xor (w[i-15]>>18) xor (w[i-15]>>3))+

+w[i-7]+((w[i-2]>>>17) xor (w[i-2]>>>19) xor (w[i-2]>>>10));

b) Ініціалізуються змінні a, b, c, d, e, f, g, h та набувають значення 8 32-бітних констант створених раніше.

c) Далі відбувається цикл стискання на 64 ітерації:

h=g;

g=f;

f=e;

e=d+h+((e>>>6) xor (e>>>11) xor (e>>>25))+((e and f) xor (not(e) and g))+k[i]+w[i];

d=c;

c=b;

b=a

a=e-d+((a>>>2) xor (a>>>13) xor (a>>>22))+

+((a and b) xor (a and c) xor(b and c));

d) Модифікуємо константні 8 значень хешу:

h0 = h0 + a;

h1 = h1 + b;

h2 = h2 + c;

h3 = h3 + d;

h4 = h4 + e;

h5 = h5 + f;

h6 = h6 + g;

h7 = h7 + h;

7) Побайтовий вивід модифікованих значень і є хешем.

Недоліки:

- все ще існує імовірність колізій.

Переваги:

- висока стійкість до зламу,
- висока продуктивність.

2.3.4 Висновки

В результаті аналізу було виявлено, що SHA-256 має більш високу стійкість до атак перебором, меншу імовірність колізій, ніж її аналог MD5. Порівняння характеристик даних хеш-функцій наведене у таблиці 2.3.

Таблиця 2.3 — Порівняння властивостей хеш-функцій.

Властивість	MD5	SHA-256
Довжина хешу	128 біт	256 біт
Розмір блоку обробки	512 біт	512 біт
Кількість логічних примітивів	4	3
Число додаткових констант	64	4
Імовірність виникнення колізій	висока	мала

2.4 Висновки за розділом

Підчас огляду існуючих технологій передачі даних та їх захисту, було вирішено у якості протоколу передачі даних обрати TLS версії 1.3, застосувати для захисту даних криптосистеми RSA і Діфі-Хелмана. Також в якості хеш-функції було обрано SHA-256.

3 ОРГАНІЗАЦІЯ СИСТЕМИ ТА ІНФОРМАЦІЙНА СТРУКТУРА

3.1 Архітектура обміну даними між абонентами

Обмін повідомленнями між двома абонентами здійснюється за участі трьох сторін:[13]

- клієнта абонента А,
- клієнта абонента Б,
- серверу.

Сервер виконує роль посередника підчас передачі ключів для абонентів за алгоритмом Діфі-Хелмана, а також тимчасового сховища даних підчас обміну повідомленнями. Схема клієнт-серверної архітектури додатку наведена на рисунку 3.1.

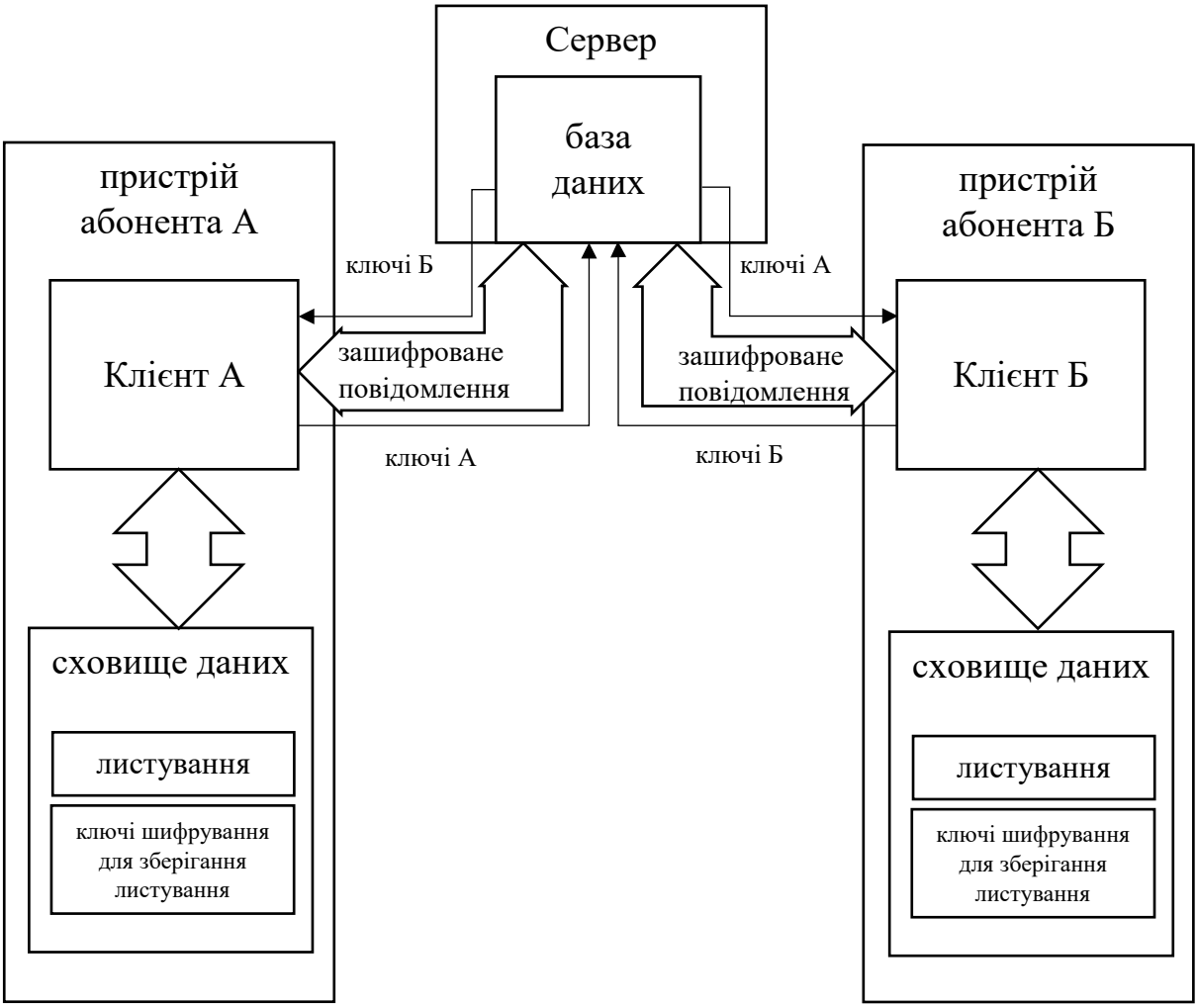

Рисунок 3.1 — Архітектура розроблюваної системи

Всі отримані та надіслані абонентом повідомлення протягом доби зберігаються на сервері. Листування, яке зберігається клієнтом на пристрої абонента може бути видалене за бажанням цього абонента або збережене стільки, скільки в цьому має потребу абонент. Зберігання наявного в клієнті листування відбувається у зашифрованому виді.

3.2 Спосіб збереження листування у додатку і автентифікація

Сервер протягом доби зберігає повідомлення у вигляді шифрограм, які надсилають абоненти.

Клієнт підчас автентифікації отримує від користувача пароль.
Клієнт отримує хеш цього пароля від функції SHA-256. Даний хеш є секретом допоміжного шифру AES-256, який симетрично розшифровує пару довгострокових асиметричних ключів, і зашифровує їх, якщо користувач вийде з додатку. Асиметричні ключі відповідно розшифровують та зашифровують файл листування абонента.

Файл листування абонента має зберігатись на пристрої в захищеному вигляді. AES-256 шифрує асиметричні ключі, щоб запобігти порушенню конфіденційності листування у випадку заволодіння пристрою зловмисником, оскільки головним секретом є хеш від паролю, який не має потреби зберігати на пристрої.

З даної причини перевірка правильності паролю не відбувається, оскільки неправильний пароль не дасть змогу дешифрувати асиметричні ключі дешифруючі листування (рисунок 3.2).

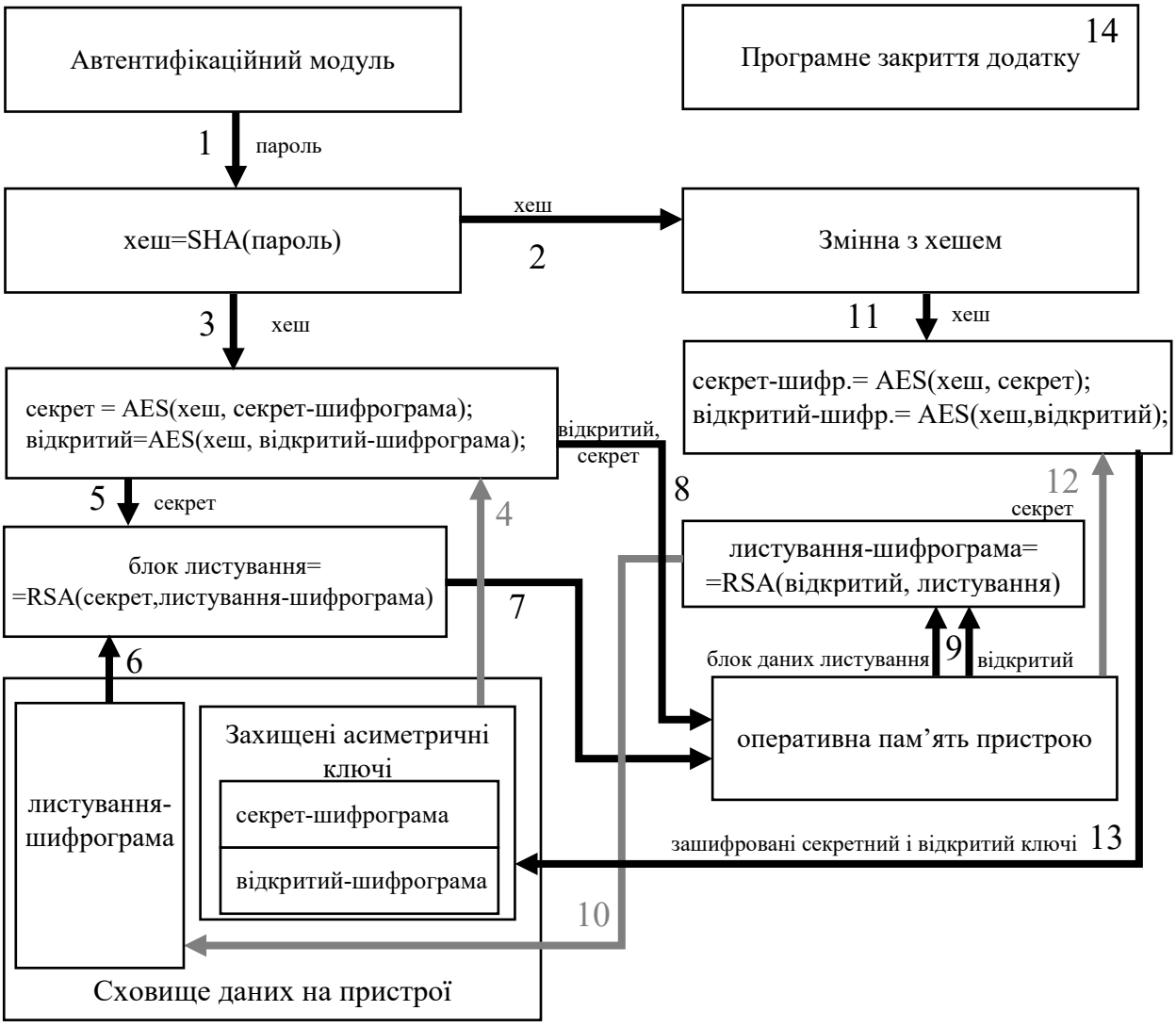

Рисунок 3.2 — Цикл шифрування і дешифрування даних у додатку

3.3 Інтерфейс клієнта

Месенджер дозволяє обмін повідомленнями між двома абонентами. Кожне повідомлення окрім свого змісту містить час відправлення. Інтерфейс додатку складається з поля для введення повідомлень, кнопки «Connect», яка відповідає за під’єднання до чату, поля для ведення паролю, поля для введення ніку, області, де відображене листування, кнопки «Send» відповідальної за надсилання повідомлення а також кнопки нової генерації ключів «Keys!» для зберігання листування (рисунок 3.3)

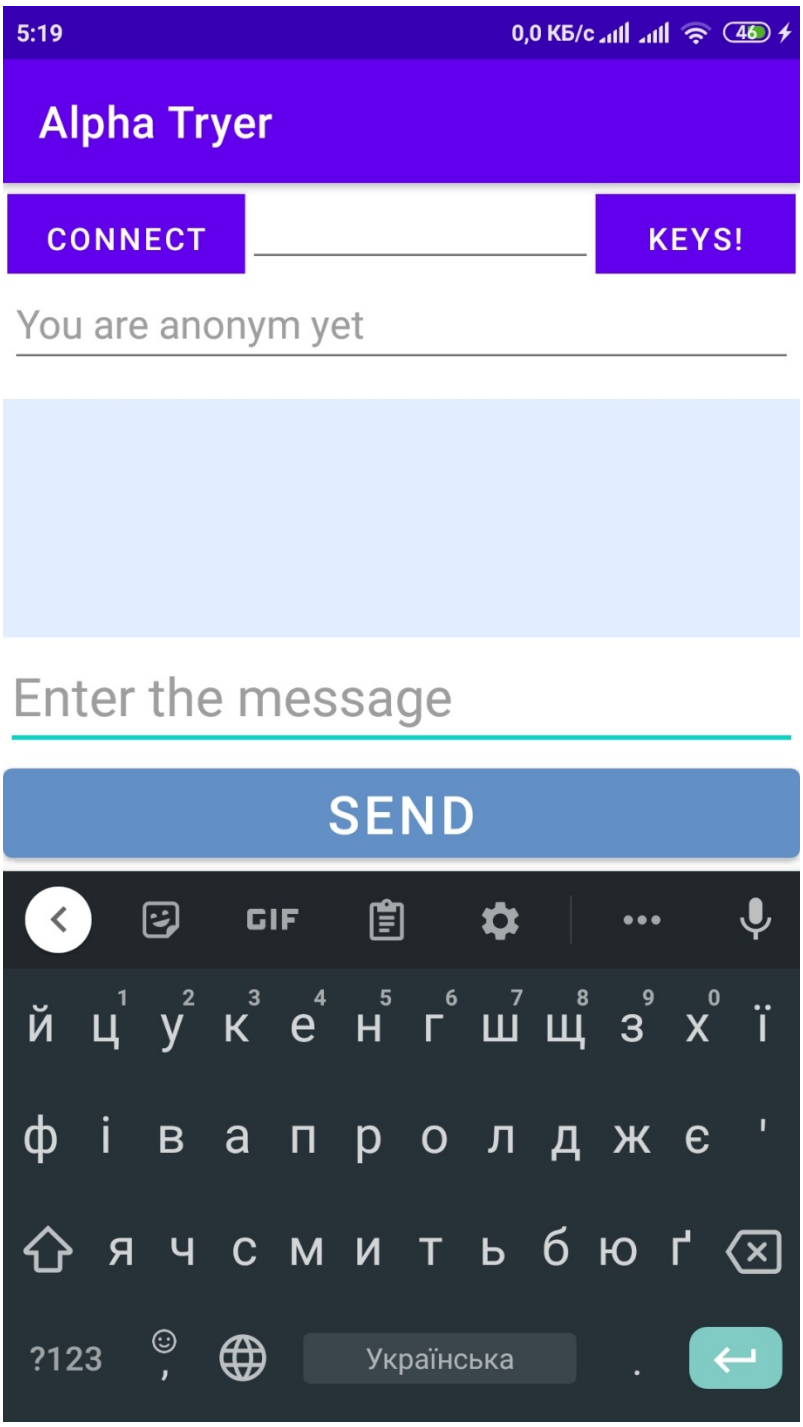

Рисунок 3.2 — Інтерфейс додатку

3.4 Висновки за розділом

В даному розділі була представлена структура додатку, його параметри передачі, збереження даних, шифрування у випадку передачі та загальна архітектура месенджера. Також висвітлений дружній інтерфейс для користувача.

4 РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ СИСТЕМИ

4.1 Вибір засобів реалізації месенджера

Для створення месенджера було обрано інтегровану середу розробки Visual Studio 2019. Приводом для цього слугували :

- зрозумілий дружній графічний інтерфейс;
- велика кількість таких допоміжних інструментів як intelliSense-система, система оптимізованого пошуку помилок в програмному коді та інших опцій;
- Додатково встановлений модуль Xamarin дозволив розробити додаток орієнтований на використання пристроями на базі операційної системи Android.
- Месенджер складають дві головні частини: сервер і клієнт.

Мовою програмування додатку було обрано C#, враховуючи сумісність з мовою з боку ОС Android [14].

4.2 Розробка алгоритмів програмного забезпечння клієнтської частини

Робота додатку, що розробляється має наступні функції:

- автентифікація абонента,
- створення текстового повідомлення,
- шифрування та дешифрування листування асиметричним криптоалгоритмом для зберігання на пристрої та виведенні в клієнт,
- передача та прийом повідомлень у захищеному вигляді.
- отримування текстового повідомлення від учасника бесіди в чаті,
- надсилання повідомлення іншому абоненту в чаті,
- додавання великої кількості співучасників розмови в чаті,
- заміна наявних довгострокових ключів для листування новими,
- термінове видалення листування з серверу та клієнта,
- режим анонімного обміну повідомленнями,

Автентифікація абонента відбувається за рахунок паролю користувача, який він повинен ввести підчас входу у додаток. Абонент вводить на панелі керування у поле пароль і натискає кнопку «Connect». Пароль, зчитується та стає вхідним значенням до хеш-функції SHA-256. Отриманий хеш є секретом для алгоритму AES-256, що дозволяє дешифрувати ключі RSA, щоб секретним ключем розшифрувати файл листування та відобразити його зміст у додатку. Відкритий ключ на час сеансу використання додатку зберігається в оперативній пам’яті пристрою. Листування відображається в клієнті. Блок-схема на рисунку 4.1 ілюструє даний алгоритм.

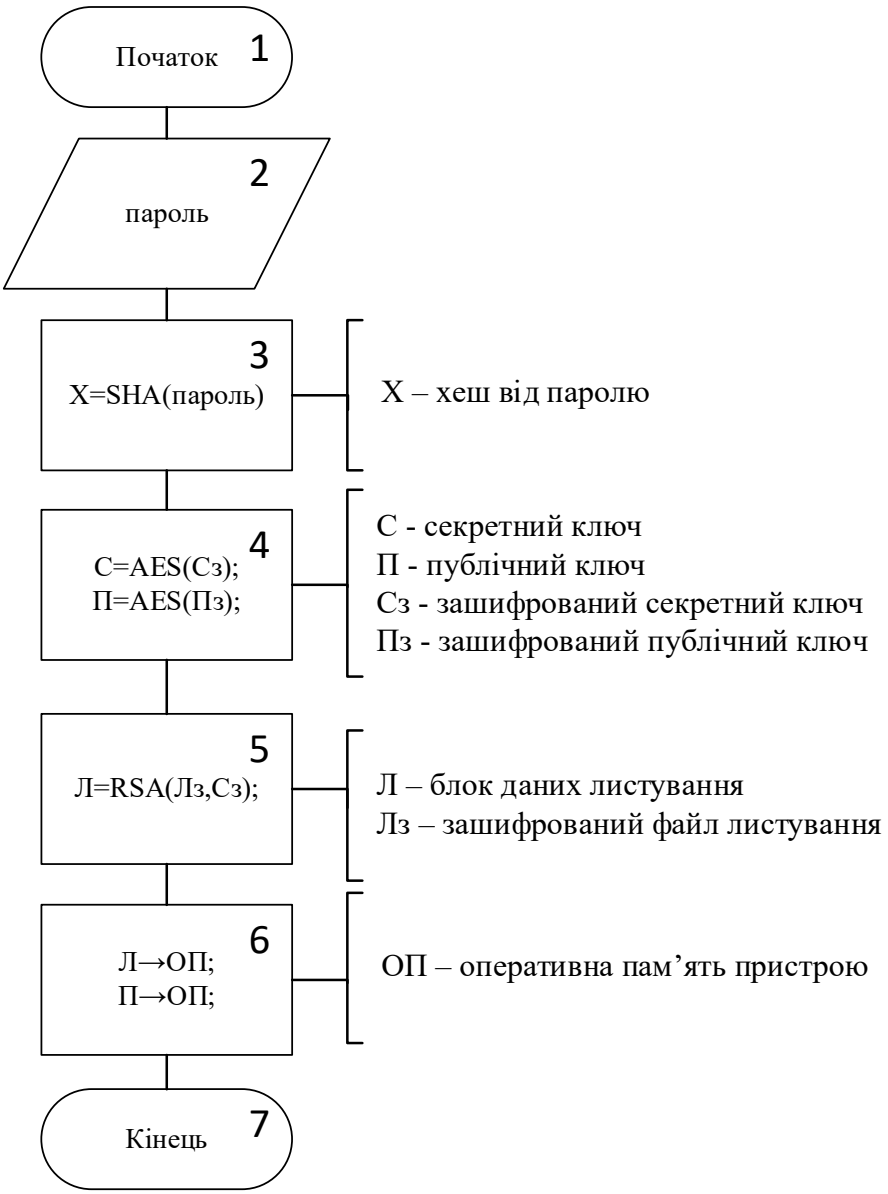

Рисунок 4.1 – Блок-схема алгоритму автентифікації та дешифрації листування.

Після автентифікації у додатку користувач має змогу надсилати та отримувати повідомлення від інших учасників чату.

За натисканням кнопки «Send» повідомлення надсилається на сервер, а з серверу до усіх інших клієнтів співучасників чату. Кожне з повідомлень, окрім свого змісту, має свій часовий-код та псевдонім автора повідомлення, який за бажанням вводиться у відповідне текстове поле. Передбачена передача повідомлень в анонімному режимі. Приклад бесіди на рисунку 4.2.

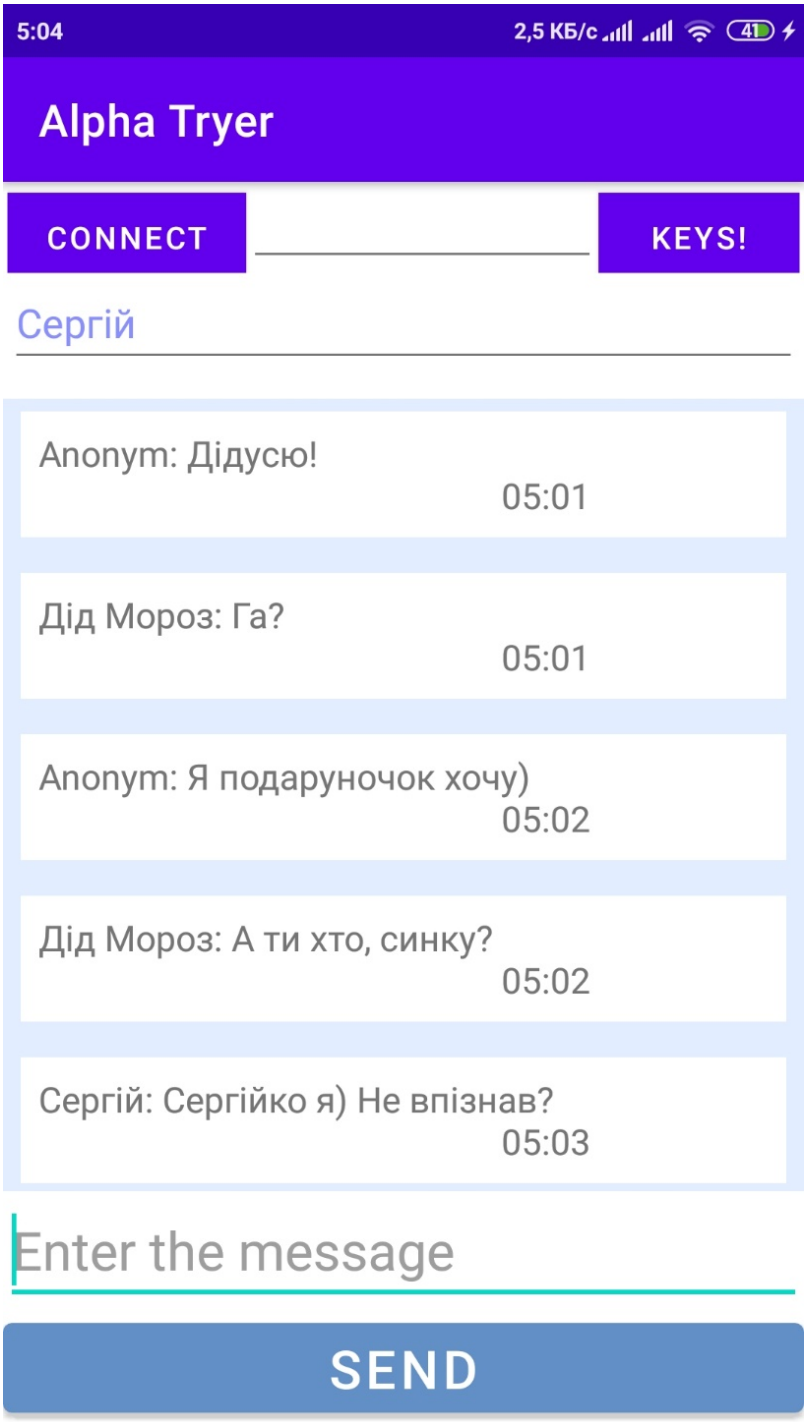

Рисунок 4.2 – Ілюстрація бесіди в чаті.

У випадку компрометації листування через несанкціонований візуальний доступ до екрану, або тимчасове заволодіння пристроєм з клієнтом у стані пройденої автентифікації користувача, абонент може відновивши доступ до пристрою, або скориставшись пристроєм інших співучасників чату, натиснути кнопку з надписом «Keys!». Після чого автоматично згенеруються нові довгострокові ключі RSA з відповідним повідомленням, а листування буде у повному обсязі безповоротно видалене як на клієнті, так і на сервері. Клієнти інших учасників у такому випадку також повністю втратять листування чату, як тільки під'єднаються до мережі Internet, автоматично синхронізуючи свої дані з базою даних серверу. Стан додатку після даної операції зображений на рисунку 4.3.

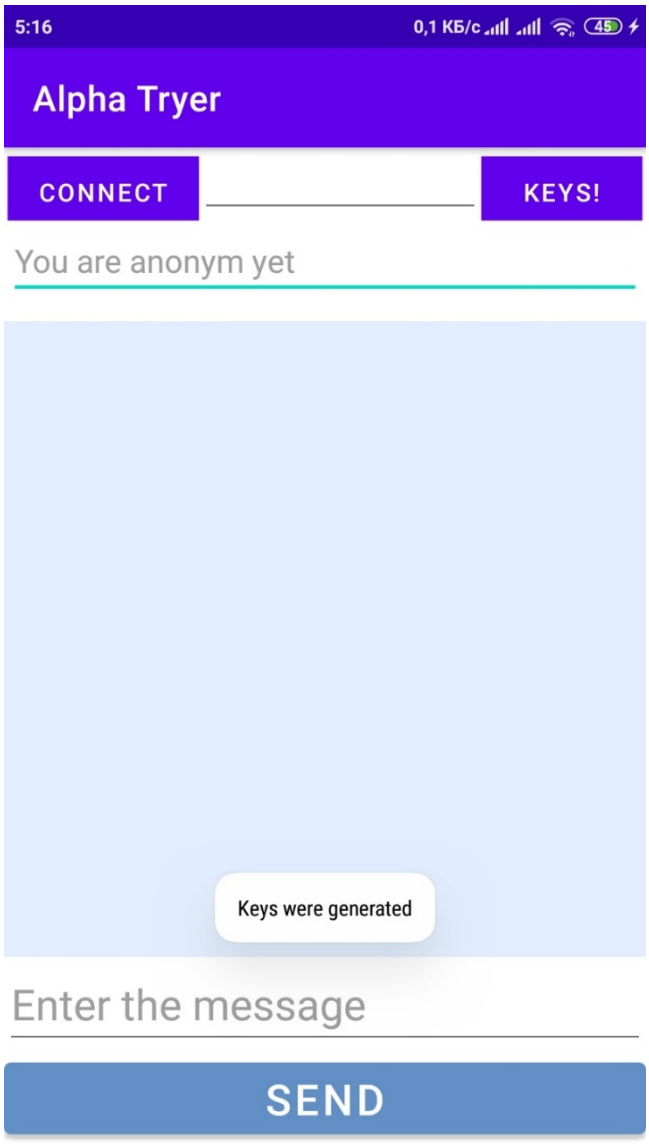

Рисунок 4.3 – Стан додатку після генерації нових довгострокових ключів.

Після сеансу обміну повідомленнями абонент може вийти з додатку. При цьому листування шифрується публічним ключем RSA, що зберігається протягом сеансу в оперативній пам’яті пристрою. Після даної операції шифрограма листування зберігається у постійній пам’яті . Хеш паролю, який теж зберігався в оперативній пам’яті пристрою, використовується як секрет для шифрування секретного та публічного асиметричних ключів, що надалі зберігається у постійній пам’яті пристрою. Блок-схема цього алгоритму наведена на рисунку 4.4.

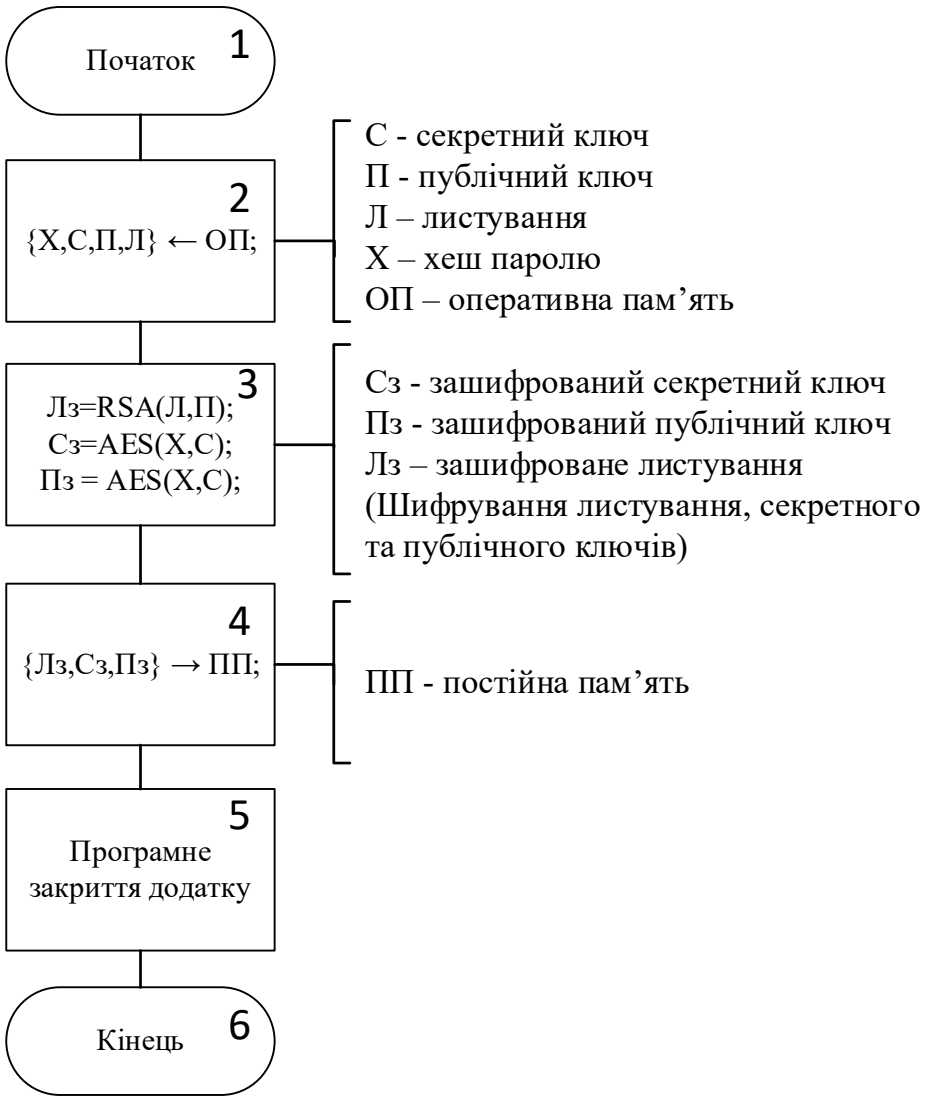

Рисунок 4.4 – Блок-схема алгоритму підчас виходу з додатку.

4.3 Розробка алгоритмів програмного забезпечення серверної частини месенджера.

За основу зв’язку між сервером та клієнтом було прийнято рішення обрати використання фреймворку від компанії WCF – Windows Communication Foundation. Головним аргументом у виборі технології стала гнучкість налаштування протоколів передачі даних [15].

Сервер передає та отримує повідомлення від користувача іншим користувачам чату. Окрім цього сервер відповідальний за генерацію та розподілення ключів шифрування обміну повідомленнями за алгоритмом Діфі-Хелмана, в якому шифрування повідомлень відбувається симетричним спільним ключем клієнтів. Блок-схема роботи алгоритму підчас обміну повідомленнями між клієнтами А та Б представлена на рисунку 4.5.

Також слід зауважити, що кожні сім днів ключі шифрування обміну повідомленнями оновлюються з метою протидії атакам перебором. Від атаки типу «людина посередині» дані захищає дані сертифікація протоколу TLS версії 1.3.

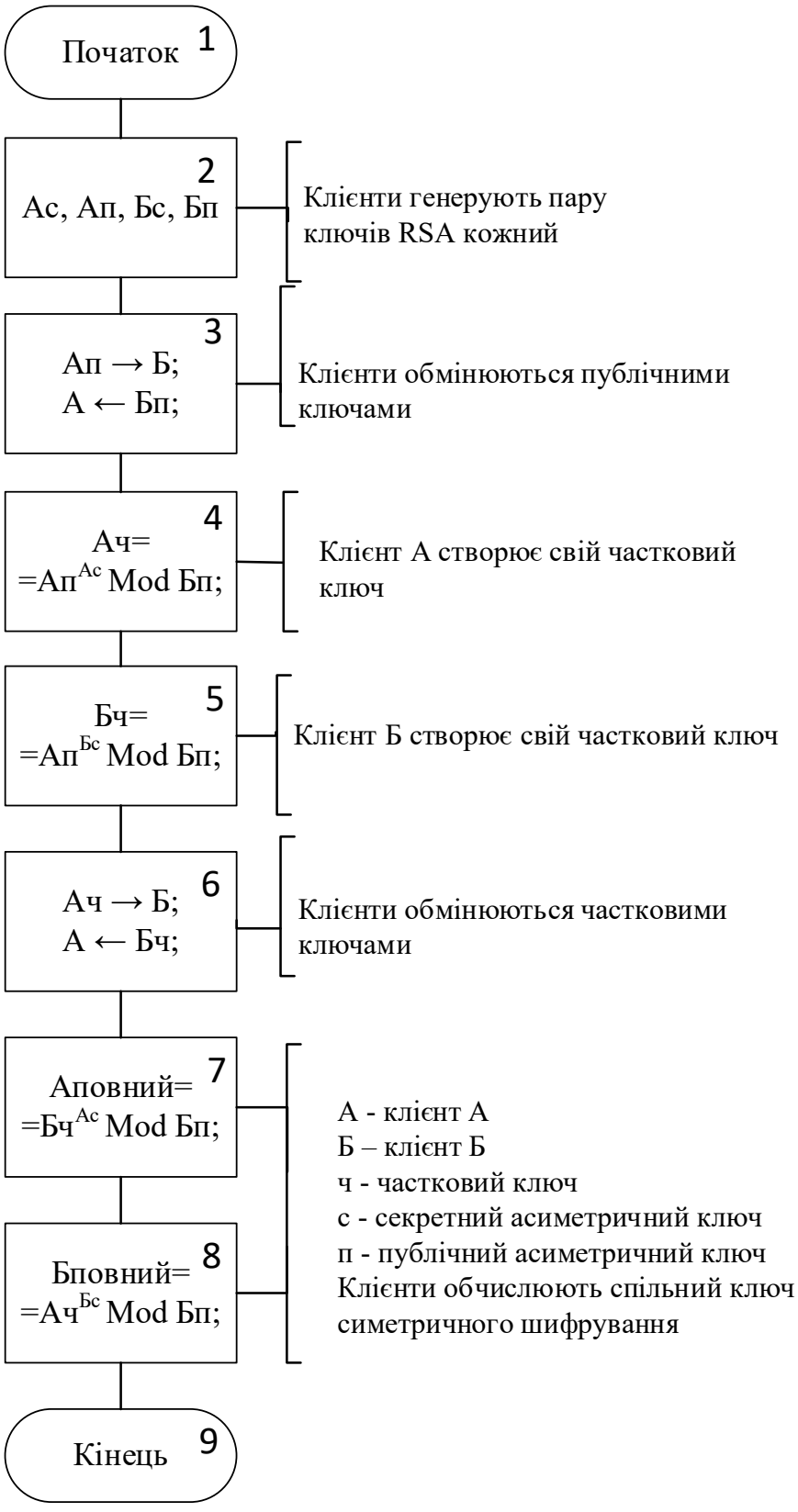

Рисунок 4.5 — Блок-схема алгоритму шифрування даних.

4.4 Висновки за розділом

У даному розділі були висвітлені механізми роботи додатку, що забезпечують функціонування обміну повідомленнями в месенджері та захисту даних підчас їх зберігання та передачі відкритими каналами.

5 МЕТОДИКА ВИКОРИСТАННЯ СИСТЕМИ

5.1 Інструкція з використання системи

Для того, щоб скористатись месенджером, користувачу необхідно увійти у додаток на своєму пристрої . У вікні, що з’явилося потрібно натиснути на поле 1, що відповідає введенню пароля користувача (рисунок 5.1) та ввести пароль.

Після цього спробувати під’єднатися — натиснути кнопку 2 з надписом «Connect» .

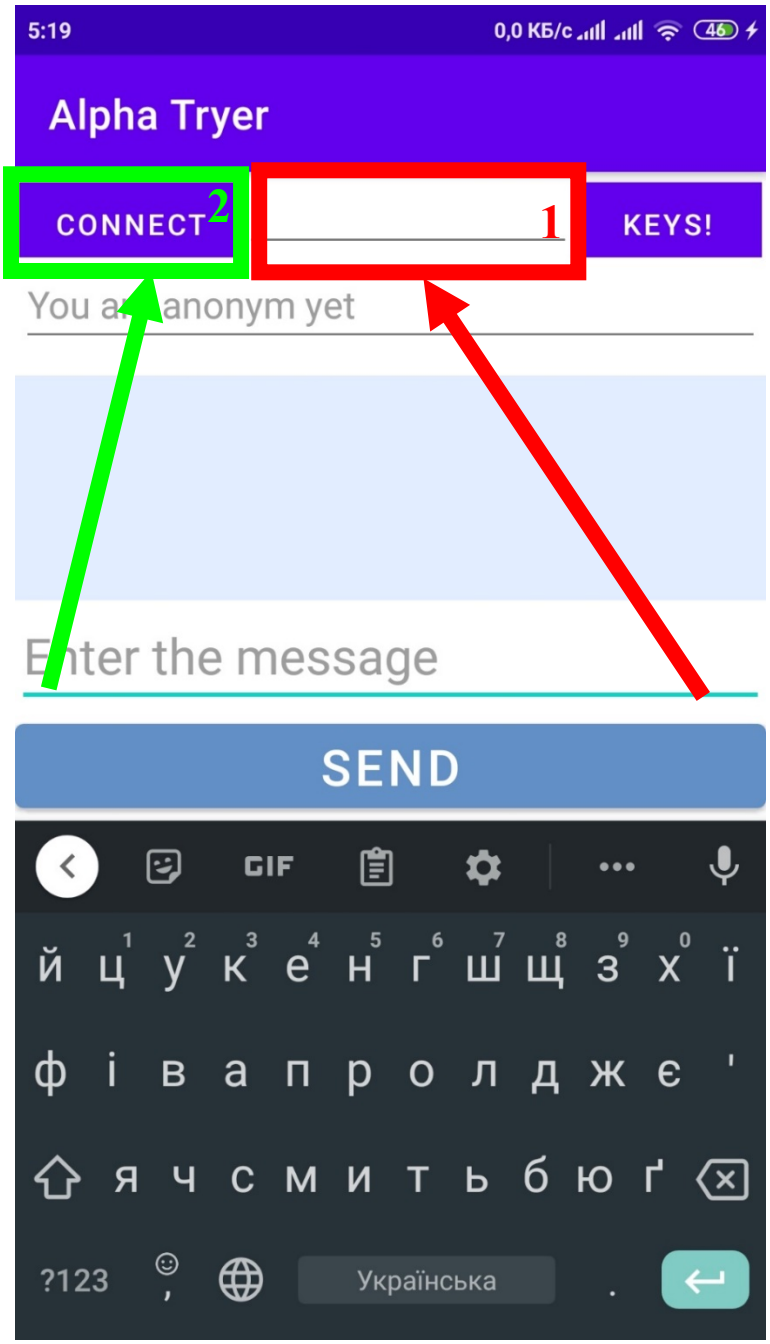

Рисунок 5.1 — Процедура автентифікації

Якщо пароль користувача був введений правильно, автентифікація здійснилася вдало і на екрані буде відображене листування в чаті — рисунок 5.2. Для того, щоб встановити псевдонім і продовжити листування, потрібно натиснути на поле 3для введення псевдоніму і надрукувати за допомогою клавіатури. Якщо поле лишатиметься незаповненим — месенджер буде діяти в режимі інкогніто і замість псевдоніму у повідомленнях буде надпис «Anonym» Після цього необхідно натиснути на поле 4, щоб створити повідомлення.

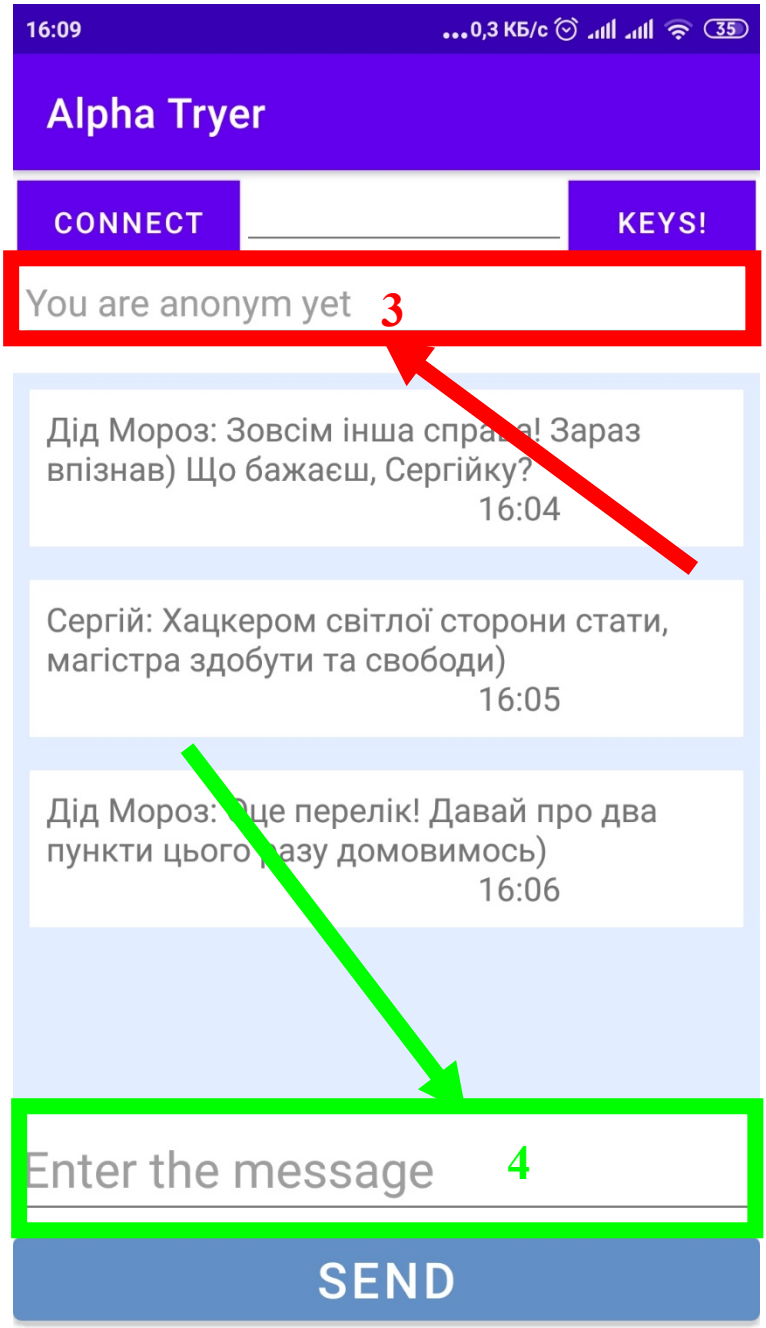

Рисунок 5.2 — Відображення листування

Для того, щоб створене повідомлення надіслати іншим учасникам чату потрібно натиснути на кнопку 5 з надписом «Send», що вказана на рисунку 5.3

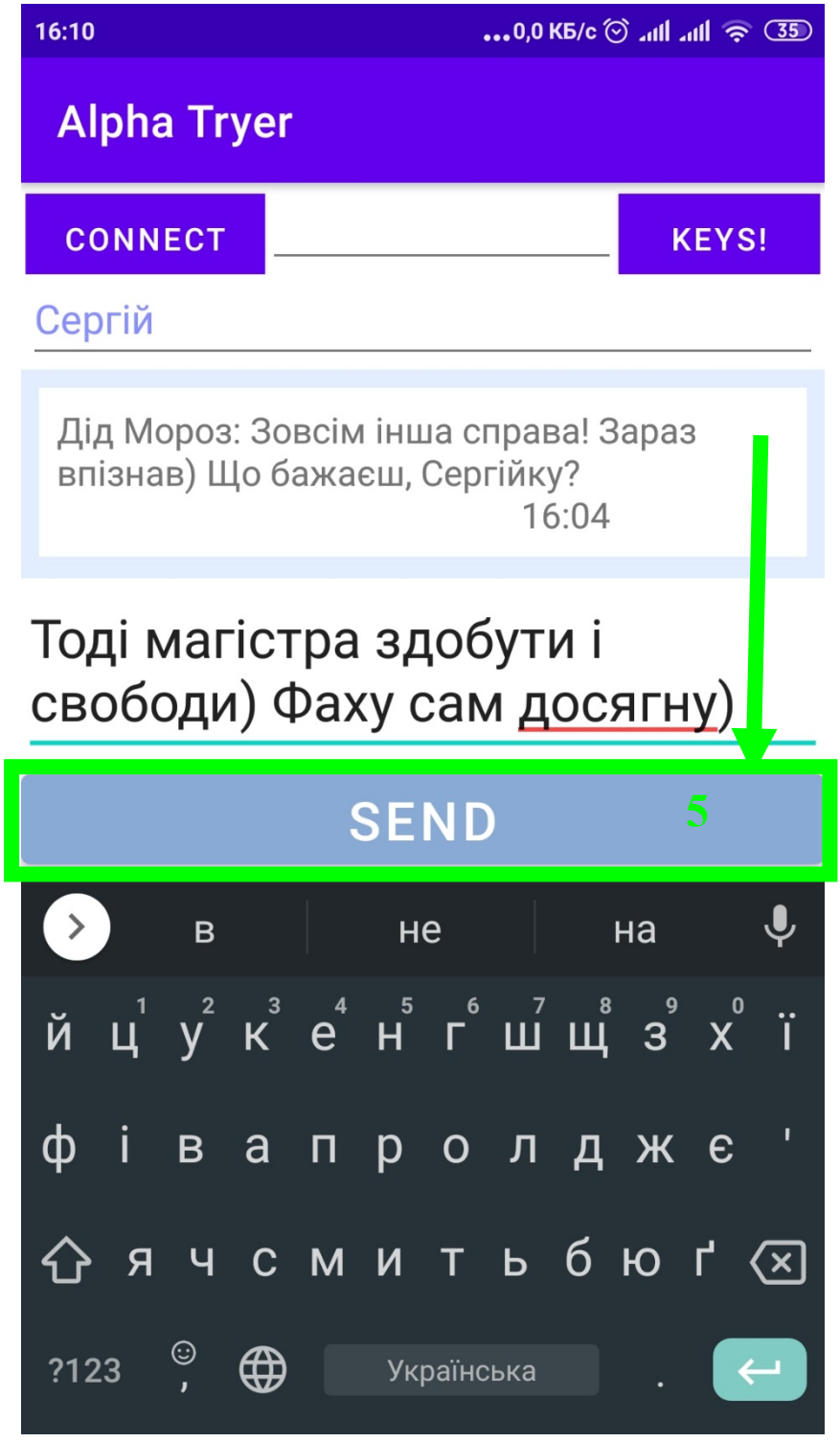

Рисунок 5.3 – Створення та відправлення повідомлення

У випадку загрози витоку інформації або підтвердженого факту цієї події рекомендовано кнопкою 6 з написом «Keys!» видалити в усіх учасників чату все листування та перезапустити систему захисту. (Рисунок 5.4)

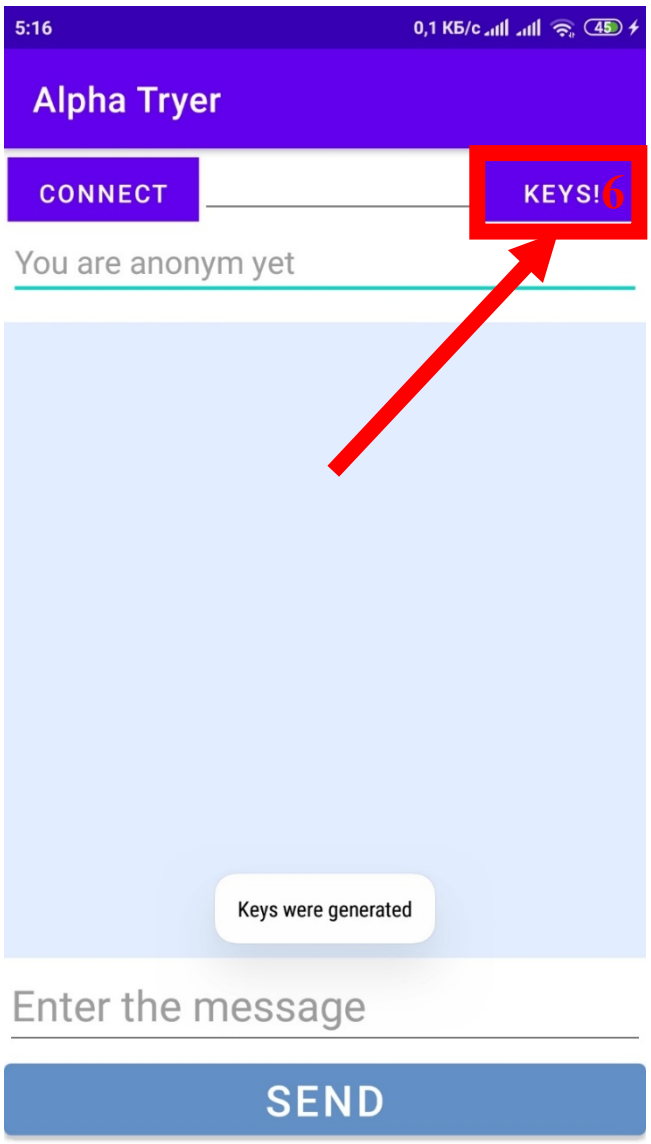

Рисунок 5.4 — Перезапуск системи захисту даних

5.2 Висновки за розділом

У даному розділі був проведений інструктаж щодо використання месенджеру, та здійснена перевірка його справності. Всі функції працюють у штатному режимі.

6 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

6.1 Вимоги безпеки при виконанні робіт на робочому місці.

Розділ описаний згідно затверджених Міністерством юстиції України «Вимог щодо безпеки та захисту здоров'я працівників підчас роботи з екранними пристроями» (далі — Вимоги) №207 від 14.02.2018 за № [508/31960], які було зареєстровано 25.04.2018 року [16]

Усі положення даного розділу покликані забезпечити мінімально необхідний рівень комфорту та безпеки працівників з метою зниження ризику порушення стану здоров'я або абсолютного уникнення наслідків чинників, які негативно впливають на здоров'я та життя співробітника програміста-розробника під час виконання своїх службових обов'язків.

Згідно Вимог робочі місця програмістів-розробників мають бути розроблені з урахуванням можливості здійснити рухи або зміну положення тіла.

Гранично допустимий рівень випромінювання від екранних пристроїв не може бути перевищеним. Маються на увазі супутні в роботі приладів та пристроїв вібрація, шум, перевищення або зниження комфортної температури для роботи, чинники забруднення, стан працездатності, поведінки, що не підвладні здатності адаптації програміста-розробника.

Робоче місце програміста-розробника повинно мати відповідний до Вимог рівень ергономіки, відповідати антропологічним та психофізіологічним нормам а також характеру службових обов'язків.

Робоче місце програміста-розробника з екранним пристроєм має бути достатньо освітленим і мати відповідний рівень контрасту між екраном та довкіллям за витримкою «Гігієнічні вимоги до організації роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» [17], що є частиною «Державних санітарних правил і норм роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» №7 затверджених Головним державним санітарним лікарем України від 10 грудня 1998 р. (ДСанПІН [3.3.2.007-98]) [18].

Мікроклімат у виробничих приміщенннях з робочими місцями програмістів-розробників з екранними пристроями має постійно відповідати вимогам

«Санітарних норм мікроклімату виробничих приміщень» ДСН [3.3.6.042-99] [19] що було затверджено постановою Головного державного санітарного лікаря України від 01 грудня 1999 року №42.

Стіл на робочому місці або поверхня повинні мати низьку відбивну здатність, достатньо ергономічні розміри та мати гнучкість при розміщенні клавіатури, екрана, документів, обладнання, тощо.

Крісло на робочому місці повинне бути стійким та дозволяти програмісту-розробнику займати зручне положення.

Сидіння повинне мати здатність до регулювання висоти та нахилу.

Має бути передбачена підніжка для тих, якщо це необхідно для зручності.

Щодня початок роботи має супроводжуватись очищенням екрану пристрою від пилу та бруду.

Разом із закінченням роботи пристрій має бути вимкнений та знеструмлений.

У випадку аварії пристрій підлягає терміновому знеструмленню.

Не допускається підчас роботи програміста-розробника, на його робочому місці здійснювати технічне обслуговування, технічне налагодження або зміни у конструкції, у склад якої входить екранний пристрій.

Забороняється взаємодія з екранними пристроями підчас роботи програміста-розробника, якщо виникають нестабільне зображення на екрані, нехарактерна поведінка та інші виведення з ладу.

Екранні пристрої не повинні викликати ризик для програміста-розробника.

Електромагнітне випромінювання видимої частини спектру має бути відповідати незначному впливу на безпеку життя та здоров’я програміста-розробника.

Символи повинні мати достатню чіткість та інтервали, а між рядками належну дистанцію.

Не допускається миготіння зображення чи інші прояви нестабільності.

Контрастність та яскравість символів повинна мати здатність до регулювання.

Екрани повинні володіти здатністю нахилу та повороту, якщо це необхідно програмісту-розробнику. Можливе використання підставки або регулюючого столу для розміщення екрану.

Підчас вибору клавіатури слід надавати перевагу клавіатурі, що може відкидатися або відділена від екрану для зручного положення тіла програміста-розробника та уникнення втоми рук або їх частин.

Не допускається віддзеркалювання на поверхні клавіатури. Через це поверхня клавіатури має бути матовою. Положення клавіш на клавіатурі має відповідати достатньому рівню ергономіки програміста-розробника.

Обладнання не має виділяти тепло в такій кількості, що може порушити комфортний мікроклімат на робочому місці програміста-розробника.

Розробка робочого місця програміста-розробника має супроводжуватись добиранням програмного забезпечення і обладнання, що вирішує відповідні завдання, має простоту керування програмістом-розробником, або відповідає рівню знань програміста-розробника.

6.2 Шкідливі виробничі фактори на робочому місці

На робочому місці програміста-розробника може відбуватись вплив наступних шкідливих чинників з відповідними наслідками:

- підвищений рівень шуму вентиляторів , процесорів, аудіоплат, тощо може спровокувати часткову або повну втрату слуху, погіршити психологічний стан програміста-розробника та стан його здоров’я в цілому;
- підвищене значення напруги в електричному колі у випадку замикання може спричинити значні втрати здоров’я програміста-розробника або призвести до летального випадку;
- підвищений рівень електромагнітного випромінювання пристроїв може спричинити хронічний головний біль;
- підвищена напруженість електричного поля та підвищена вологість повітря можуть спричинити удари струму;

- блисткість екранів та несприятливий здоровому стану зорового апарату програміста-розробника розподіл яскравості може сприяти частковій втраті зору або його погіршення;
- підвищена і знижена температура повітря може призвести до зниження імунітету програміста-розробника, його переохолодження, теплового удару або інших захворювань;
- надмірна запиленість та загазованість повітря може спричинити хронічні захворювання дихальної системи та призвести до інших проявів погіршення стану програміста-розробника;
- підвищена і знижена вологість повітря може призвести до суттєвого погіршення стану здоров'я програміста-розробника та викликати хронічні захворювання дихальної системи;
- недостатня освітленість робочого міста програміста-розробника може призвести до погіршення функціонування зорового апарату.

Усі вище зазначені шкідливі чинники можуть знизити тривалість життя програміста-розробника підчас виконання своїх службових обов'язків.

Відповідно до [20] був проведений аналіз робочого місця автора на відповідність параметрам шуму, вібрації, мікроклімату та іншим умовам праці програміста-розробника.

Згідно встановлених за цією постановою норм величини температури повітря, його вологості та швидкості руху задовольняє за значенням категорії робіт «Легка 1а». Фактичні значення наведені нижче:

- температура повітря 23°С при нормі 22-24°С;
- відносна вологість 57 при нормі 60-40% ;
- швидкість руху 0,1, що відповідає нормам.

Вище зазначені значення відповідають нормам на холодний період року. Перепад температури повітря в межах робочої зони не повинен перевищувати 3°

Мікроклімат робочого місця автора відповідає межам допустимих значень категорії робіт «Легка 1а» — температурі, швидкості руху повітря, відносної вологості повітря в робочій зоні виробничих приміщень. Фактичні значення наведені нижче:

- температура повітря на постійному робочому місті програміста-розробника 23°С при нормі 21-25°С;
- температура повітря на непостійному робочому місті програміста-розробника 21°С при нормі 18-26°С;

Вище зазначені значення відповідають нормам на холодний період року. Внутрішні поверхні приміщень, де розташоване робоче місце програміста-розробника мають такі ж самі значення, що відповідають нормам.

Інтенсивність теплового опромінення належна та не перевищує гранично допустиме значення у 70 Вт/м^2 при опроміненні тіла за площею 30%, шо відповідає нормі у 25 – 50%.

Робоче крісло має здатність регулювати висоту та нахил. Робоча поверхня достатня за розміром та відповідає критеріям ергономіки. Екран встановленої на стіл ЕОМ має здатність нахилу для зручного користування пристроєм. Яскравість та контрастність екрану знаходиться у допустимих значеннях. Екран знаходиться у чистому вигляді. Робоче місце достатньо освітлене. Отже висновок полягає у повній відповідності робочого місця програміста-розробника нормам чинного законодавства.

6.3 Дії працівників в надзвичайних ситуаціях

Згідно наказу Державної служби України з надзвичайних ситуацій , «Про затвердження Методичних рекомендацій щодо підготовки населення до дій в умовах загрози або вчинення терористичного акту» затвердженого від 23.03.2015 № [167][19] у разі терористичної загрози працівникам рекомендовано діяти відповідно вказівок, наведених нижче.

У разі захоплення в наручники рекомендується:

- не провокувати терористів на прояви насилля, утриматись від різких руків звуків, тощо;
- не чинити опір терористам, якщо ті озброєні;
- не дивитися терористам в очі;
- бути уважним і запам’ятовувати всі прикмети злочинців та підозрілі дії не видаючи цього факту нападникам;
- підчас стрільби тої ж миті впасти на підлогу та закрити руками потилицю.

У випадку перебування в приміщенні, де відбувається терористичний акт:

- уникати контактів з терористами;
- повідомити як можна непомітніше на лінії 102 про злочинців, знайти укриття та повідомити місце свого знаходження;
- не наближатись до вікон і дверей сховати документи, які засвідчують особу;
- чітко виконувати накази правоохоронців;
- у разі наявності засобів фото і відео фіксації здійснити приховану фіксацію дій терористів, якщо є можливість — передати матеріали на непублічні файлові сховища і видалити факт створення фіксації на своєму пристрої;
- у випадку перестрілки пересуватись по кімнатах в разі необхідності повзком.

ВИСНОВКИ

У даній дипломній роботі була розроблена система захищеного обміну повідомленнями на базі операційної системи Android. Рівень захисту даних відповідає моделі ситуації, що припускає існування на пристрої абонента шкідливого шпіонського програмного забезпечення, можливого перехоплення повідомлення зловмисником між сервером та клієнтом. А також частково передбачений захист, на випадок несанкціонованого доступу до даних сервера. А саме невідкладне видалення даних з серверу та усіх пристроїв учасників чату. За рахунок можливості змінювати псевдонім підчас листування користувачі мають змогу передавати інформацію використовуючи принципи стеганографії [20].

Перевірка месенджеру на працездатність жодних несправностей не виявила. Мессенджер рекомендовано до використання користувачам, які гостро потребують підвищеного рівня конфіденційності інформації у своїх професійних та особистих аспектах життя.

Розроблену систему рекомендовано до використанні у навчальному процесі як демонстраційного комплексу для захищеного елементарного інформаційного зв’язку абонентів на базі клієнт-серверної архітектури.

ПЕРЕЛІК ПОСИЛАНЬ

1. Новини Telegram [Електронний ресурс] – Режим доступу: https://tlgrm.ru/blog
2. Блог Viber [Електронний ресурс] – Режим доступу: https://www.viber.com/ru/blog/
3. Блог Signal [Електронний ресурс] – Режим доступу: https://signal.org/blog/
4. Transport Layer Security (TLS) Protocol Version 1.2 [Електронний ресурс] T. Dierks Independent E. Rescorla RTFM, Inc. August 2008The – Режим доступу: https://tools.ietf.org/html/rfc5246
5. Defense Advanced Research Projects Agency Information Processing Techniques Office 1400 Wilson Boulevard Arlington, Virginia 22209 TRANSMISSION CONTROL PROTOCOL DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION [Електронний ресурс] by Information Sciences Institute University of Southern California 4676 Admiralty Way Marina del Rey, California 90291 – Режим доступу: https://tools.ietf.org/html/rfc793
6. DecoderConfigurationGuide [Електронний ресурс] / RSANetWitness®Platform11.5 – Режим доступу: https://community.rsa.com/servlet/JiveServlet/downloadBody/113797-102-6-418752/rsa_nw_11.5_decoder_config_guide.pdf
7. Грингард С.Г85 интернет вещей : Будущее уже здесь [Електронний ресурс] / Сэмюэл Грингард : Пер. с англ. — м. : издательская группа «Точка», Альпина Паблишер, 2017. — 224 с
8. D.Eastlake 3rd Motorola Labs T.Hansen AT&T Labs July 2006 – Режим доступу: https://tools.ietf.org/html/rfc4634
9. КАСЭ. Таненбаум, Д. Уэзеролл "Компьютерные сети" 5-е изд. (2016)
10. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы : Учеб. пособие для вузов / Олифер В.Г., Олифер Н.А. - СПб. : Питер, 2000. - 672 с.
11. Д.Куроуз, К. Росс "Компьютерные сети. Нисходящий подход" / Джеймс Ф. Куроуз, Кит В. Рос – Из-во «Эксмо» 2016 – 912 с
12. Васильцов, І. В. Атаки спеціального виду на криптопристрої та методи боротьби з ними : Монографія / І. В. Васильцов. - Кременець : Видав. центр КОГПІ, 2009. - 264 с.

13. Корниенко, А. А Средства защиты информации на железнодорожном транспорте (криптографические методы и средства) : учеб. пособие для вузов ж.-д. трансп. / А. А. Корниенко, М. А. Еремеев, С. Е. Ададуров ; ред. А. А. Корниенко. - М. : Маршрут, 2006. - 253 с. :
14. Информационная безопасность в каналах телекоммуникаций : Учеб. пособиедля вузов / #v922. - 2-е изд. - Х. : Регион-информ - Транспорт Украины, 2000. - 216 с. -
15. Рихтер, Дж. Программирование серверных приложений Microsoft для Windows 2000. Мастер-класс / Дж. Рихтер, Дж. Кларк . - СПб. ; М. : Питер - Изд-во-торговый дом "Русская Редакция", 2001. - 592 с.
16. НПАОП 0.00-7.15-18 «Вимоги щодо безпеки та захисту здоров’я працівників підчас роботи з екранними пристроями» від 14.02.2018 № 508/31960.
17. ДСанПІН 3.3.2.007-98 «Гігієнічні вимоги до організації роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» №7 від 10.12.1998.
18. ДСанПІН 3.3.2.007-98 «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин», № 7 від 10.12.1998.
19. ДСН 3.3.6.042-99 «Санітарні норми мікроклімату виробничих приміщень» від 01.12.1999 №42, постанова затверджена Головним державним санітарним лікарем України.
20. Наказ ДСНС України «Методичні рекомендації
щодо підготовки населення до дій в умовах загрози або вчинення терористичного акту» № 167 від 23.03.2015
21. Зимін С.О. Дослідження та розробка системи захищеного обміну повідомленнями / С.О. Зимін // XIV Міжнародна науково-практична конференція. – 2020.