Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

ННЦЗФН

Кафедра *інформаційно-мережної інженерії*
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти *перший (бакалаврський)*

Аналіз проблем безпеки в безкоштовних месенджерах

(тема)

Виконав:
здобувач *4* року навчання,
групи *ТРІМІз-21-1*

Артем Козлов
(власне ім'я, прізвище)

Спеціальність *172 Телекомунікації та радіотехніка*
(код і повна назва спеціальності)

Тип програми *освітньо-професійна*

Освітня програма *Інформаційно-мережна інженерія*
(повна назва освітньої програми)

Керівник *доц. к.т.н. Дарія Чеботарьова*
(посада, власне ім'я, прізвище)

Допускається до захисту

Завідувач кафедри ІМІ _____ *Валерій Безрук*
(підпис) (власне ім'я, прізвище)

2025 р.

Не містить відомостей, заборонених до відкритого публікування

Студент _____ *Артем Козлов*
(підпис) (власне ім'я, прізвище)

Керівник _____ *Дарія Чеботарьова*
(підпис) (власне ім'я, прізвище)

Харківський національний університет радіоелектроніки

ННЦЗФН

Кафедра *Інформаційно-мережної інженерії*
(повна назва)

Рівень вищої освіти *перший (бакалаврський)*

Спеціальність *172 Телекомунікації та радіотехніка*
(код і повна назва)

Тип програми *освітньо-професійна*

Освітня програма *Інформаційно-мережна інженерія*
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри ІМІ_____
(підпис)

"*25*" *червня* 2025р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві *Козлову Артему Володимировичу*
(прізвище, ім'я, по батькові)

1. Тема роботи *Аналіз проблем безпеки в безкоштовних месенджерах*

затверджена наказом університету від "*02*" *травня* 2025 р. №*63 Стз*

2. Термін подання здобувачем роботи до екзаменаційної комісії *20 червня 2025 р.*

3. Вихідні дані до роботи *розглянути принципи розвитку месенджерів, їх класифікацію, переваги та недоліки, виконати порівняння актуальних месенджерів; дослідити основні принципи функціонування месенджерів; проаналізувати основні проблеми безпеки в безкоштовних месенджерах; виконати детальний огляд засобів безпеки інформації в месенджерах, провести порівняльний аналіз месенджерів за показниками безпеки, визначити найбільш безпечний месенджер та запропонувати рекомендації для безпечного використання месенджерів.*

4. Перелік питань, що потрібно опрацювати в роботі

1. Аналіз сучасних месенжджерів

2. Основні принципи функціонування месенджерів

3. Проблеми безпеки в безкоштовних месенджерах

4. Засоби безпеки інформації в месенджерах

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) _____

Слайди у форматі Power Point (назва, мета та задачі роботи, сучасні месенджери, класифікація, переваги та недоліки месенджерів, порівняння найпопулярніших в Україні месенджерів, принцип дії та функції месенджерів, архітектура месенджерів, проблеми безпеки в безкоштовних месенджерах, ризики безпеки та загрози аналізу даних, основні засоби безпеки в месенджерах, порівняння месенджерів за показниками безпеки, рекомендації щодо безпечного використання месенджерів, висновки)

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Строк / термін виконання етапів роботи	Примітка
1	*Ознайомлення із завданням. Уточнення ТЗ.*	*05.05.25*	*Виконано*
2	*Підбір літератури за темою роботи.*	*05.05 - 10.05.25*	*Виконано*
3	*Виконання розділу 1*	*11.05 - 17.05.25*	*Виконано*
4	*Виконання розділу 2*	*18.05 – 24.05.25*	*Виконано*
5	*Виконання розділу 3*	*25.05 – 31.05.25*	*Виконано*
6	*Виконання розділу 4*	*01.06 - 14.06.25*	*Виконано*
7	*Оформлення пояснювальної записки,*		
	презентаційного матеріалу та підготовка		
	до захисту у ЕК	*15.06 - 20.06.25*	*Виконано*

Дата видачі завдання *05 травня 2025 р.*

Здобувач _____
(підпис)

Керівник роботи _____ *доц. Чеботарьова Д.В.*
(підпис) (посада, власне ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка: 72 с., 20 рис., 3 табл., 32 джерела, 1 додаток

Об'єкт дослідження – програми обміну миттєвими повідомленнями.

Мета роботи – дослідження проблем безпеки та засобів захисту месенджерів.

Результати – в роботі проаналізовано еволюцію, сучасний стан та основні тенденції розвитку месенджерів, розглянуто класифікацію месенджерів, їх переваги та недоліки, виконано порівняння актуальних месенджерів; досліджено основні принципи функціонування месенджерів; проаналізувано основні проблеми безпеки в безкоштовних месенджерах, ризики безпеки та загрози аналізу даних; виконано детальний огляд засобів безпеки інформації, що використовуються в месенджерах, проведено порівняльний аналіз месенджерів за показниками безпеки, визначено найбільш безпечний месенджер та запропоновано рекомендації для безпечного використання месенджерів, які допоможуть підвищити безпеку та знизити ризики можливих проблем.

МЕСЕНДЖЕР, МИТТЄВІ ПОВІДОМЛЕННЯ, ІНФОРМАЦІЯ, БЕЗПЕКА, ЗАХИСТ, ПРОТОКОЛ, ШИФРУВАННЯ, VIBER, FACEBOOK MESSENGER, TELEGRAM, WHATSAPP, SIGNAL.

THE ABSTRACT

Explanatory note: 72 p., 20 fig., 3 tabl., 32 sources, 1 app.

Object of research - instant messaging programs.

The purpose of the work is to study the security problems and means of protecting messengers.

Results - the work analyzes the evolution, current state and main trends in the development of messengers, considers the classification of messengers, their advantages and disadvantages, compares current messengers; investigates the basic principles of messenger functioning; analyzes the main security problems in free messengers, security risks and threats to data analysis; provides a detailed review of information security tools used in messengers, conducts a comparative analysis of messengers by security indicators, identifies the most secure messenger and offers recommendations for the safe use of messengers that will help increase security and reduce the risks of possible problems.

MESSENGER, INSTANT MESSAGING, INFORMATION, SECURITY, PROTECTION, PROTOCOL, ENCRYPTION, VIBER, FACEBOOK MESSENGER, TELEGRAM, WHATSAPP, SIGNAL.

ЗМІСТ

С.

ПЕРЕЛІК СКОРОЧЕНЬ

МП – миттєві повідомлення;

ПЗ – програмне забезпечення;

E2EE (End-to-End Encryption) – наскрізне шифрування;

FM (Facebook Messenger) – месенджер від Facebook;

HTML (HyperText Markup Language) – мова форматування гіпертекстових документів для перегляду вебсторінок;

HTTP (HyperText Transfer Protocol) – транспортний протокол для передачі гіпертекстових даних;

LDAP (Lightweight Directory Access Protocol) – полегшений протокол доступу до директорій / каталогів;

PFS (Perfect Forward Secrecy) - досконала пряма секретність;

SMTP (Simple Mail Transfer Protocol) – простий протокол передачі пошти;

TCP/IP (Transmission Control Protocol / Internet Protocol) – всесвітній мережний протокол;

XMPP (Extensible Messaging and Presence Protocol) – відкритий мережний протокол миттєвих повідомлень та інформації про присутність між користувачами в інтернеті;

ZKP (Zero-Knowledge Proof) – протокол доказу з нульовим розголошенням.

ВСТУП

Месенджери або програми обміну миттєвими повідомлення революціонізували спосіб спілкування між людьми, пропонуючи зручні та універсальні можливості зв'язку в режимі реального часу. Месенджери стали невід'ємною частиною повсякденного життя, від особистих чатів до професійної співпраці. Особливої актуальності месенджери набули останніми роками, оскільки події, що пов’язані з пандемією Covid-19 та війною,призвели до дистанційної форми праці та освіти. Тому віртуальне спілкування в наш час є важливішим ніж будь-коли.

Сьогодні багато компаній працюють онлайн, тому швидке, ефективне та результативне спілкування в режимі реального часу дуже важливе для компаній. Використання месенджерів в бізнесі та обмін миттєвими повідомленнями з клієнтами дозволяє компаніям залишатися успішними в довгостроковій перспективі.

Раніше розробники месенджерів основну увагу приділяли різним спеціальним можливостям додатків, цікавому та зручному інтерфейсу, але зараз (особливо в умовах війни в Україні) на перше місце виходить безпека месенджерів. Ризики безпеки та загрози аналізу даних, пов'язані з додатками обміну миттєвими повідомленнями, можуть мати серйозні наслідки. З цієї причини використання максимально безпечних месенджерів є життєво важливим.

Більшість користувачів в Україні використовують безкоштовні месенджери. Але саме безкоштовні месенджери мають приховані небезпеки, вони є привабливими цілями для кіберзлочинців через їх широке використання та часто ненайкращі заходи безпеки [1].

В епоху, коли витоки даних та порушення конфіденційності стають дедалі поширенішими, небезпеки безкоштовних месенджерів не можна ігнорувати, особливо підприємствам. Бізнес-компаніям покладатися на

споживчі додатки для комунікації не лише ризиковано, але й потенційно катастрофічно. Отже інвестування в надійне комунікаційне рішення корпоративного рівня є надзвичайно важливим [1]. Саме тому, безпека безкоштовних додатків обміну миттєвими повідомленнями потребує детального вивчення, аналізу та вжиття заходів.

Дана кваліфікаційна робота присвячена дослідженню проблем безпеки в безкоштовних месенджерах. Аналіз літератури за темою роботи [1 - 32] підтвердив актуальність та важливість цієї теми, тому ця кваліфікаційна робота є актуальною.

1 АНАЛІЗ СУЧАСНИХ МЕСЕНДЖЕРІВ

1.1 Еволюція та принципи розвитку месенджерів

Сучасний досвід обміну миттєвими повідомленнями є бездоганним та інтуїтивно інтегрує такі функції, як відео, фотографії, голосовий зв'язок, електронна комерція та ігри, зі звичайним обміном повідомленнями.

Миттєвий обмін повідомленнями пройшов довгий шлях з моменту своєї появи. Концепція миттєвого обміну повідомленнями стала поширеною в 1990-х роках, дозволяючи користувачам з усього світу спілкуватися в режимі реального часу.

Ранні месенджери, такі як ICQ та AOL Instant Messenger (AIM), проклали шлях для сучасних сервісів обміну миттєвими повідомленнями [2]. З появою смартфонів та розширенням інтернету, миттєвий обмін повідомленнями охопив складніші функції та ширшу базу користувачів і продовжує свій розвиток.

Еволюція месенджерів була досліджена за джерелами [2 - 6]. Результати огляду розвитку програм обміну миттєвими повідомленнями представлено в табл. 1.1.

Початком еволюції месенджерів вважається 1961 рік, коли інноваційна система сумісного розподілу часу (CTSS) Массачусетського технологічного інституту дозволила користувачам (до 30 осіб) увійти в систему та зв'язатися один з одним [3]. Важливою подією також став винахід систем електронних дошок оголошень (BBS) у 1978 році [3], що дозволило користувачам обмінюватися повідомленнями та файлами через публічні дошки оголошень.

Сучасні системи обміну миттєвими повідомленнями, створені після 2010 р., мають дуже багато різноманітних функцій. Вони підтримують широкий спектр мультимедіа (зображення, відео, голосові повідомлення тощо). Основні характеристики сучасного миттєвого обміну повідомленнями наведено на рис. 1.1.

Таблиця 1.1 – Еволюція месенджерів

№	Етап	Період	Зміст
1	Передумови	1960-ті	В 1961 р.Массачусетський технологічний інститут запустив інноваційну систему сумісного розподілу часу (CTSS), що дозволило започаткувати обмін миттєвими повідомленнями та створило можливість спілкуватися в режимі реального часу.
2	Ранні спроби	1970-1980-ті	В 1978 р. створено першу систему електронних дошок оголошень CBBS (Computerized Bulletin Board System) [3]. В 1988 р. поява інтернет-чату (IRC), що дозволив користувачам підключатися до мереж за допомогою клієнтського програмного забезпечення для спілкування в режимі реального часу.
3	Початок ери месенджерів	1990-ті	В 1996 р. компанія Mirabilis запускає ICQ, що дозволяв користувачам спілкуватися віч-на-віч або в групах, обмінюватися файлами та шукати інших користувачів. В 90-х з'являються перші великі конкуруючі платформи обміну миттєвими повідомленнями: ICQ, AIM, MSN та Yahoo Messenger. Зростання популярності миттєвих повідомлень (використовується текстове спілкування користувачів у режимі реального часу).

Продовження табл. 1.1

№	Етап	Період	Зміст
4	Зростання популярності мобільних повідомлень	2000-ні	Золота доба обміну миттєвими повідомленнями (поява обміну фотографіями, здійснення відеодзвінків та ігор). В 2003 р. з'явився сервіс Skype. В 2009 р. з'явився месенджер WhatsApp. Поява смартфонів призводить до популярності мобільних месенджерів.
5	Інтеграція із соціальними мережам	2010-ті	В 2010 р. з'явився месенджер Viber. В 2011 р. Facebook випустив окрему версію мобільного додатку під назвою Facebook Messenger. Платформи Facebook Messenger та Instagram Direct інтегрували обмін миттєвими повідомленнями із соціальними мережами, що покращило залучення користувачів. В 2013 р. з'явився месенджер Telegram.
6	Корпоративний обмін миттєвими повідомленнями	2020-ті	Такі інструменти, як Slack, Microsoft Teams та Zoom, революційно змінили комунікацію на робочих місцях, пропонуючи інтегровані рішення для професійної співпраці. В 2025 р. припинив роботу Skype на користь Microsoft Teams, при цьому Microsoft припиняє підтримку дзвінків на внутрішні або міжнародні номери [6].

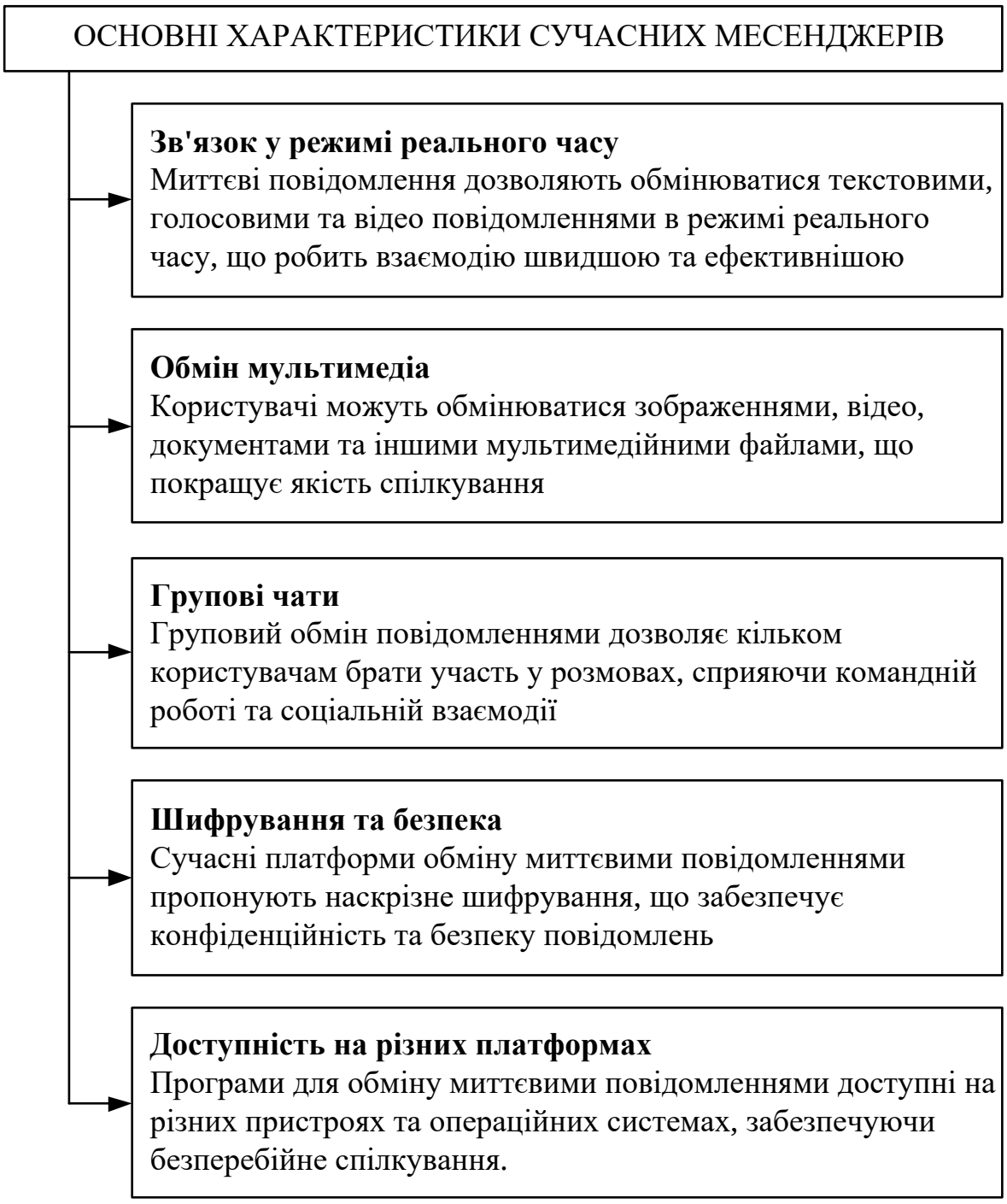
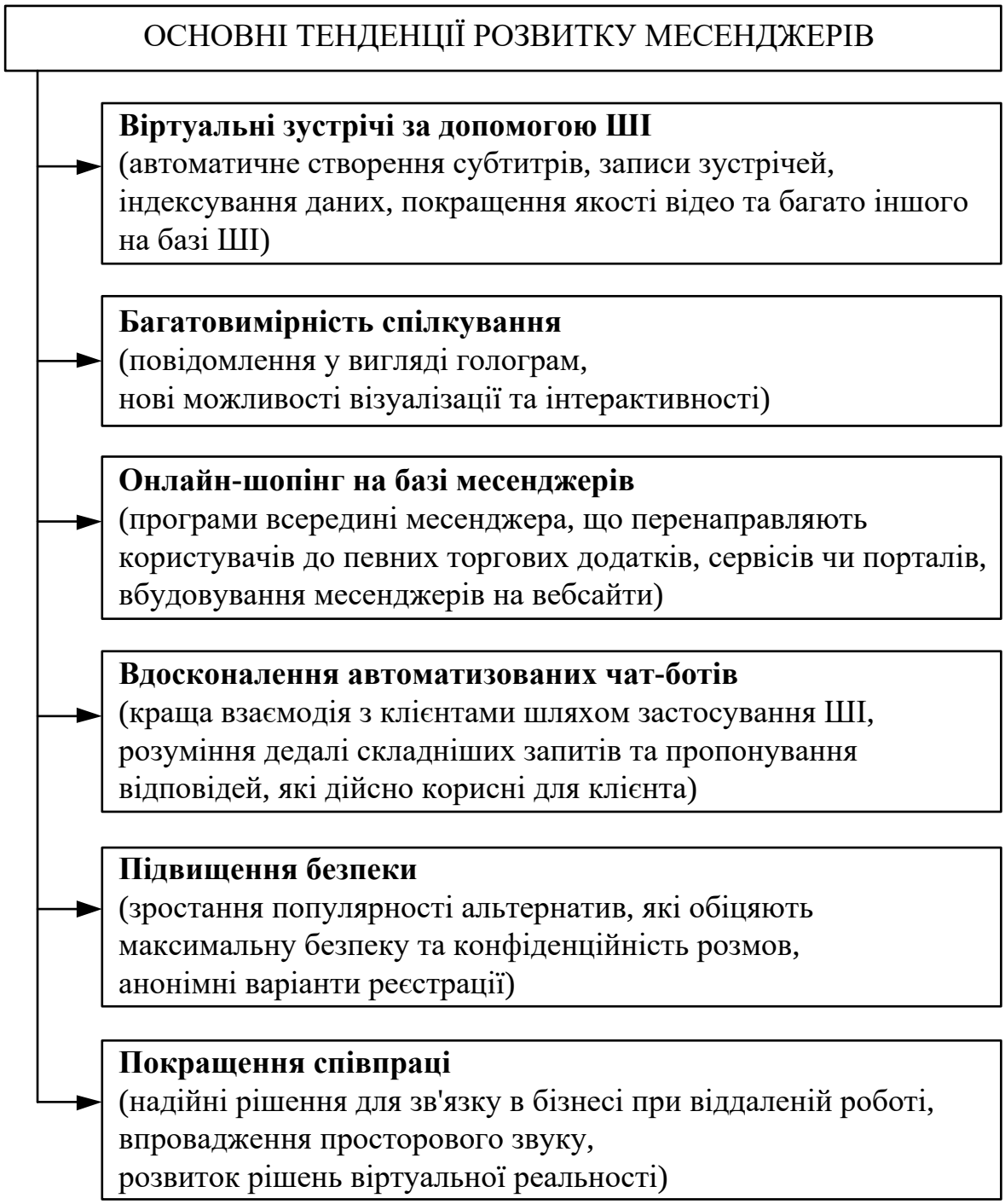


Рисунок 1.1 - Основні характеристики сучасних месенджерів

На основі інформації з джерел [3, 7, 8] були визначені та сформульовані основні тенденції сучасного розвитку месенджерів, що детально представлені на рис.1.2. Змагаючись за лідерство на ринку, месенджери продовжують додавати нові функції, щоб стати цікавішими та кориснішими.



Риснуок 1.2 – Основні тенденції розвитку месенджерів

Основні тенденції розвитку (рис. 1.2) показують, що месенджери збережуть зв'язок ще тіснийшим, ніж будь-коли. Месенджери продовжуватимуть відігравати дуже важливу роль у нашому житті, пропонуючи кращу допомогу з покупками, робочими завданнями та іншими повсякденними справами.

1.2 Класифікація месенджерів

Додатки для обміну миттєвими повідомленнями переживають сплеск популярності, постійно розвиваючись та доповнюючись новими функціями та можливостями. Ці універсальні інструменти бувають різних типів, кожен з яких розроблений для задоволення конкретних потреб та уподобань [9].

Існують різні класифікації месенджерів [9, 10] за різними типами ознак:

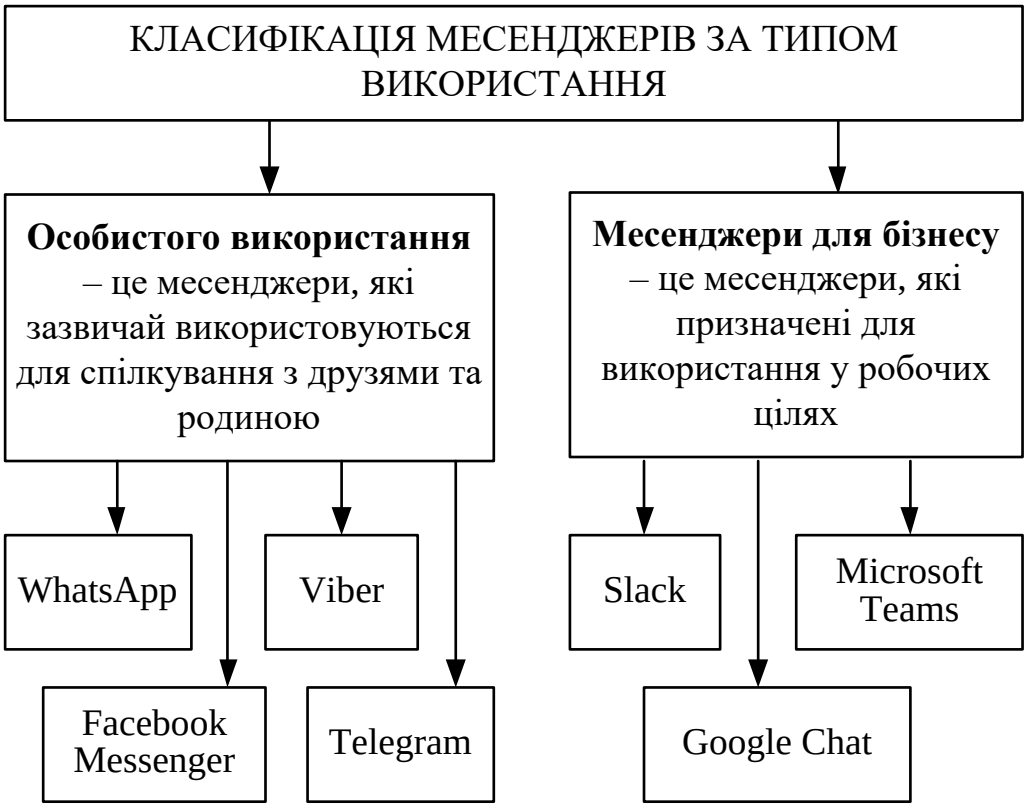
– за типом використання (рис.1.3);

– за вбудовуванням в інші програми (рис.1.4);

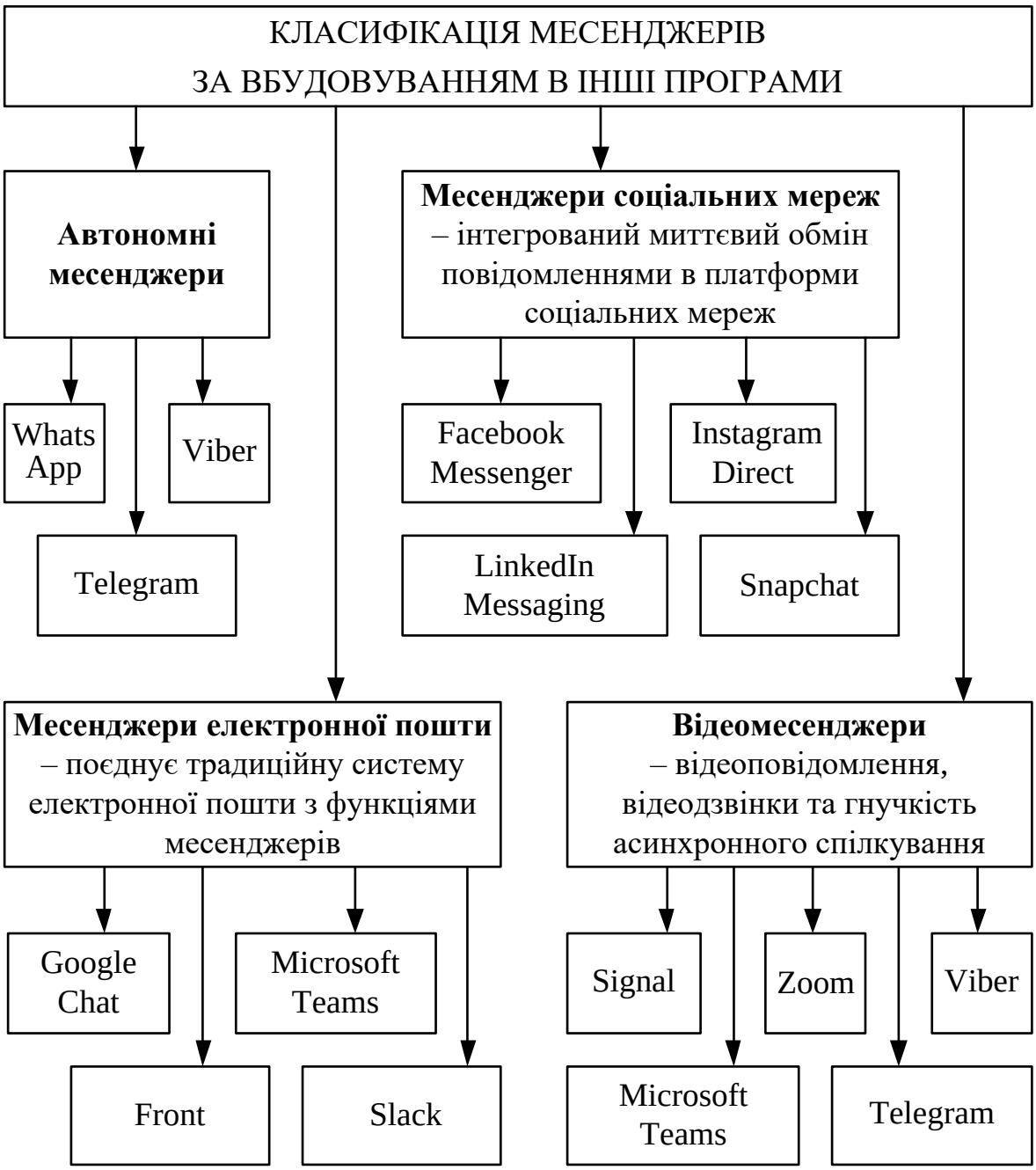
– за платформою (рис.1.5);

– за вартістю (рис.1.6);

– за рівнем безпеки (рис.1.7).

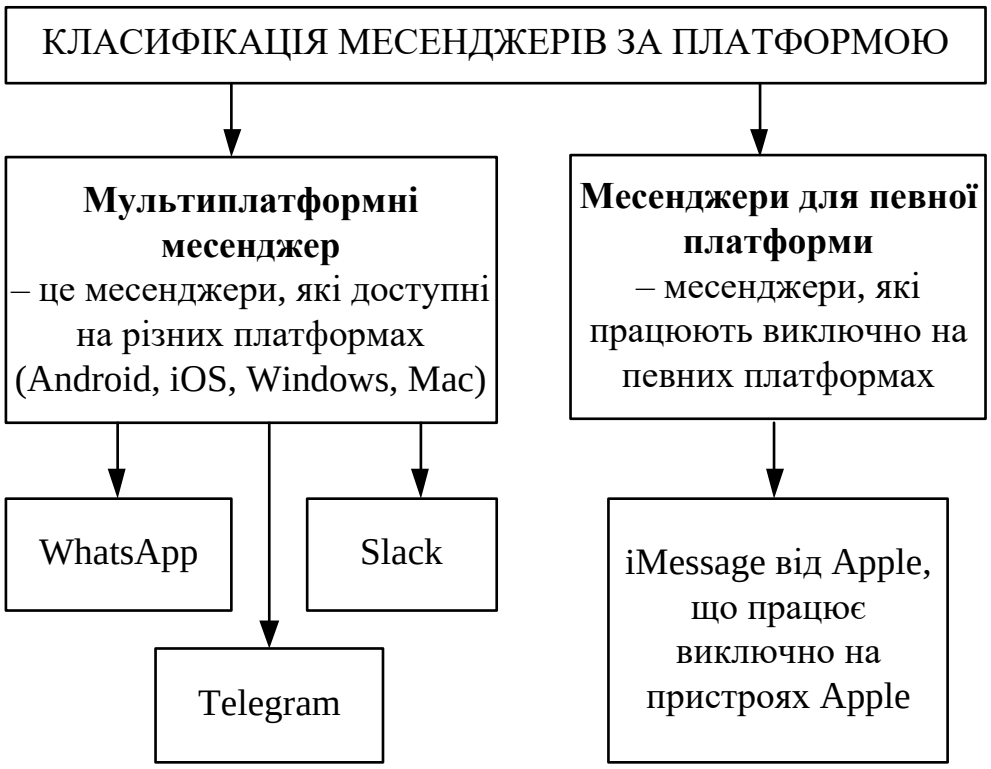


Риснуок 1.3 – Класифікація месенджерів за типом використання

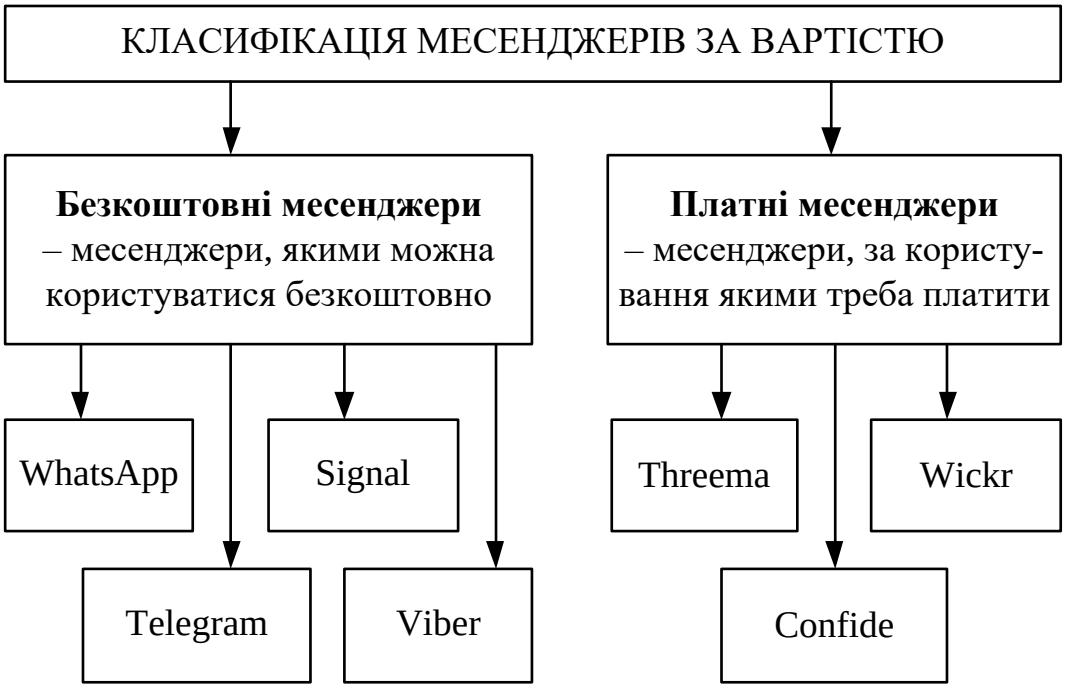


Риснуок 1.4 – Класифікація месенджерів за вбудовуванням в інші програми

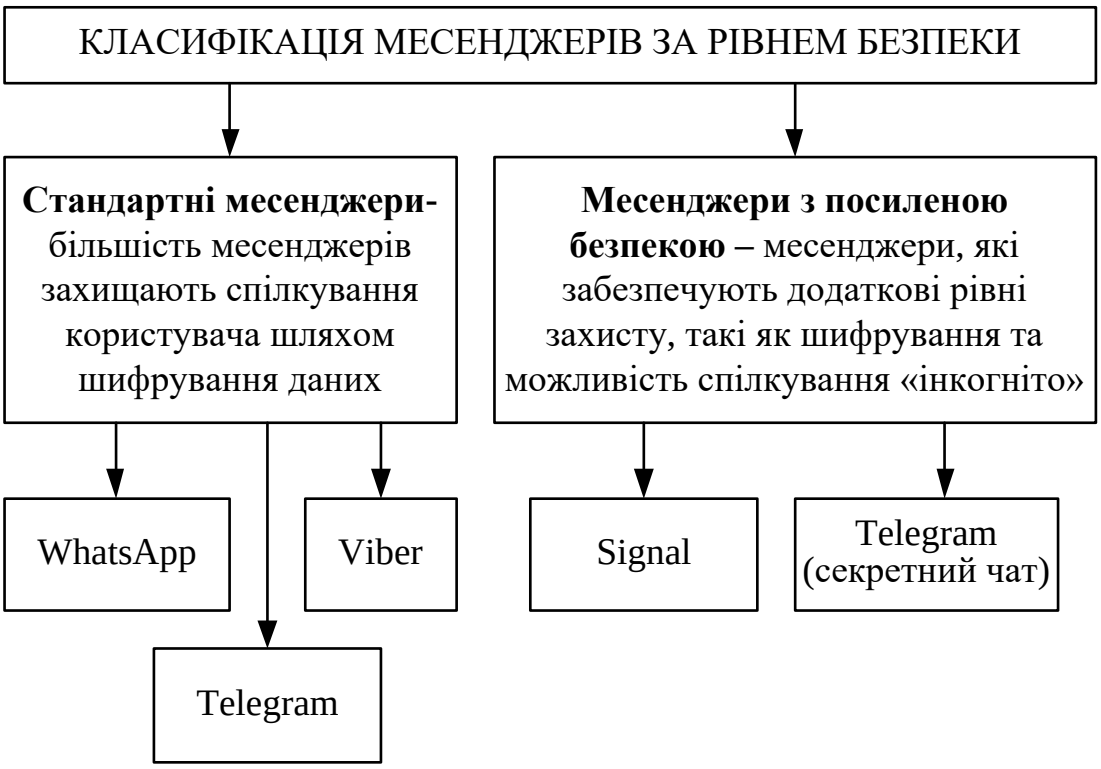
З рис. 1.4 видно, що програми для обміну миттєвими повідомленнями можуть бути автономними, або вбудованими в інші програми для забезпечення різноманітних функцій. Інтегровані платформи розширюють функціонал месенджерів та надають функції, які дозволяють компаніям взаємодіяти з клієнтами в режимі реального часу, підвищуючи залученість клієнтів та надаючи їм миттєву допомогу.



Риснуок 1.5 – Класифікація месенджерів за платформою



Риснуок 1.6 – Класифікація месенджерів за вартістю



Риснуок 1.7 – Класифікація месенджерів за рівнем безпеки

Як видно з рис. 1.3 – 1.7, на сучасному ринку програм обміну миттєвими повідомленнями існує велике різноманіття месенджерів, які здатні вдовольнити всі потреби сучасних користувачів.

1.3 Переваги та недоліки сучасних месенджерів

На основі інформації з джерел [2, 9, 11] були сформульовані основні переваги та недоліки сучасних програм миттєвого обміну повідомленнями, які представлені на рис.1.8.

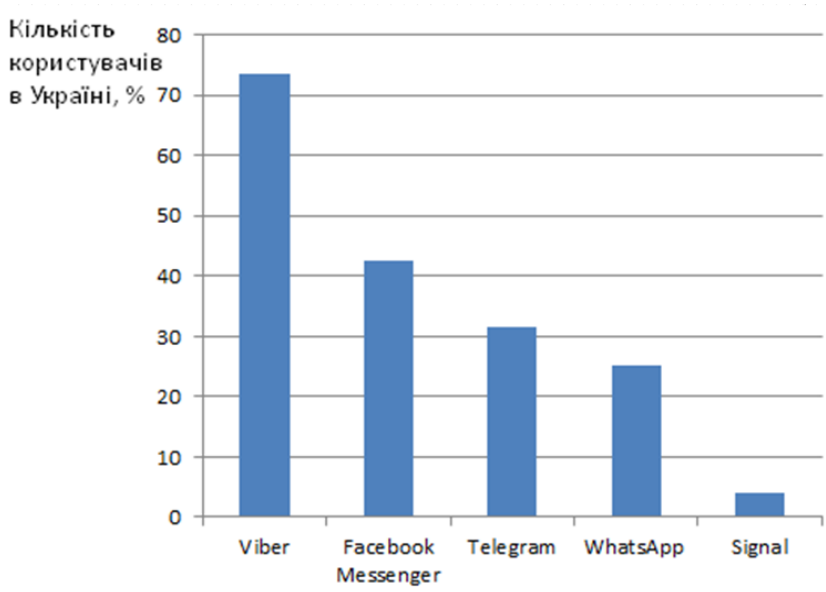
До найважливіших переваг месенджерів відносять можливість спілкуватися в режимі реального часу з іншими користувачами або групою користувачів, здатність виконувати багато завдань одночасно з комунікацією в месенджері, зручність, ефективність, доступність, простота використання та багато інших.

Риснуок 1.8 – Переваги та недоліки сучасних месенджерів

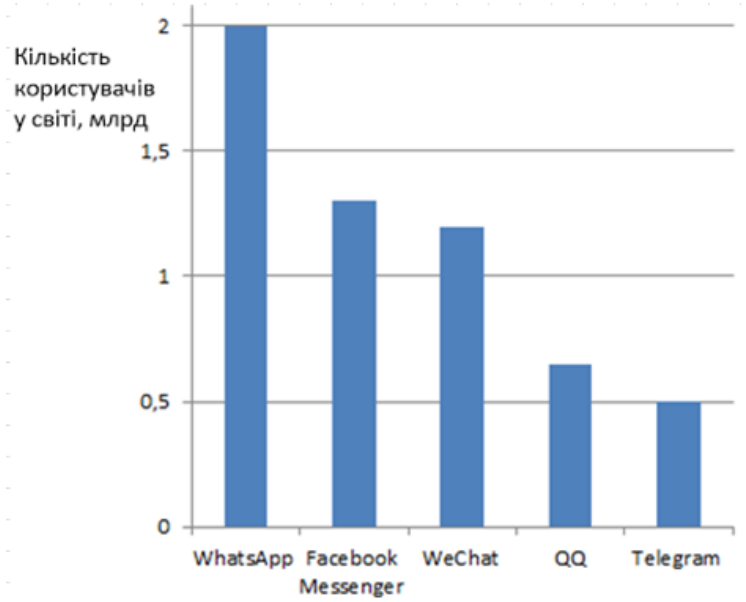
Серед недоліків месенджерів найважливішим є проблеми конфіденційності та безпеки. Існує кілька ризиків, яких слід остерігатися під час використання миттєвих повідомлень та текстових повідомлень на робочому місці: віруси та інші шкідливі програми, крадіжка особистих даних, витік конфеденційних даних, спам у миттєвих повідомленнях та інші.

1.4 Огляд найпопулярніших месенджерів

Статистика [10, 12 – 15] свідчить про те, що п’ятірка лідерів на ринку месенджерів в Україні та світі суттєво відрізняється. Найбільш популярні месенджери в Україні та світі представлені на рис.1.9.



(а)



(б)

Риснуок 1.9 – Найбільш популярні месенджери в Україні (а) та світі (б)

Основну увагу в цій роботі зосереджено на дослідженні месенджерів, які є найбільш популярними саме в Україні. Згідно з діаграмою, що представлена на рис. 1.9 (а) такими месенджерами в Україні є Viber [16], Facebook Messenger [17], Telegram [18], WhatsApp [19] та Signal [20].

Результати порівняння основних характеристик популярних в Україні безкоштовних месенджерів наведено в табл. 1.2.

Viber – найбільш популярний месенджер в Україні, яким користуються понад 73 % українців [12]. Viber є безкоштовним та безпечним месенджером, створений в Ізраілі в 2010 р. Viber дозволяє обмінюватися текстовими, голосовими та відео повідомленнями, проводити голосові та відеодзвінки, транслювати екран під час відеодзвінка, створювати канали, спільноти та групи, видаляти та редагувати повідомлення, надсилати секретні зникомі повідомлення, що мають таймер самознищення, використовувати невидимий режим, анонімні та приховані чати, крім того чати Viber синхронізуються на всіх пристроях користувача [16].

Viber пропонує кілька зручних функцій безпеки. Безкоштовний додаток для зашифрованого чату позначає чати кольором, щоб позначити рівень їхнього захисту: сірий колір означає зашифроване спілкування з довіреним контактом, а червоний – проблему з ключем шифрування. Щоб приховати повідомлення на спільному пристрої, Viber надає приховані чати з PIN-кодом та можливістю самознищення [15].

Facebook Messenger (або просто Messenger) — це безкоштовний мобільний додаток, запущений в 2011 р. розробниками Facebook та інтегрований з сайтом соціальної мережі Facebook. Facebook Messenger побудований на основі відкритого протоколу MQTT та використовується для обміну миттєвими повідомленнями, фотографіями, відео, аудіозаписами та створення групових чатів [17]. Крім користувачів Facebook месенджером можуть також користуватися і ті, хто не є зареєстрованим в соціальній мережі (просто за номером телефону та іменем).

Таблиця 1.2 – Порівняння найпопулярніших в Україні месенджерів

№	Месен-джер	Переваги	Недоліки	Наскрізне шифру-вання	Підтри-муване ПЗ
1	Viber	- безкоштовний; - пропонує наскрізне шифрування; - необмежені голосові та відео дзвінки іншим користувачам Viber; - інтерфейс простий для користувачів з будь-яким досвідом	- для реєстрації потрібен номер телефону; - періодично низька якість звуку через нестабільне з'єднання; - ліміт для спільного доступу до файлів – 200 МБ	для всіх повідом-лень та дзвінків (як особис-тих, так і групових)	Android, iOS, Windows, macOS, Linux
2	FM	- безкоштовний; - зручний для користувачів соціальних мереж, - широка мережа користувачів; - інтеграція з іншими платформами Meta; - секретні чати з наскрізним шифруванням; - простий та інтуїтивно зрозумілий	- відсутність автоматичного резервного копіювання чатів; - залежність від мобільного номера; - недостатня конфіденційність: - відсутність деяких функцій, присутніх у конкурентів (наприклад відеодзвінки для великої групи та ін.)	існує можли-вість створити приват-ний чат, який шифрує повідом-лення	Android, iOS, Windows, macOS

Продовження табл. 1.2

№	Месен-джер	Переваги	Недоліки	Наскрізне шифру-вання	Підтри-муване ПЗ
3	Tele-gram	- безкоштовний; - потужні функції соціальних мереж; - програма розподілу доходів від реклами для власників каналів; - корисні функції та чат-боти для бізнес-користувачів; - дозволяє користувачам видаляти обидві сторони розмов віч-на-віч	- наскрізне шифрування обмежується секретними чатами та відео/голосовим зв'язком; - для налаштування потрібен номер телефону; - збір даних; - потрібен доступ до списку контактів; - нефункціональні швидкі відповіді під час тестування	тільки для деяких режимів	Android, iOS, Linux, macOS, Windows
4	Whats App	- найбільша база користувачів; - безкоштовний; - самознищувані повідомлення та зображення; - відео- та голосові дзвінки	- для реєстрації потрібен номер телефону; - на Android потрібен доступ до списку контактів; - деякі люди можуть не довіряти Meta у захисті своєї конфіденційності	для всіх неділових повідом-лень	Android, iOS, macOS, Windows

Продовження табл. 1.2

№	Месен-джер	Переваги	Недоліки	Наскрізне шифру-вання	Підтри-муване ПЗ
5	Signal	- безкоштовний; - високий рівень конфіденційності; - належить некомерційній організації; - групові та приватні текстові повідомлення; - конференції, аудіо та відео дзвінки; - мінімальний збір даних; - відкритий вихідний код [20]; - відсутність реклами тощо	- для реєстрації потрібен номер телефону; - менше функцій в порівнянні з іншими месенджерами; - не підтримує двофакторну автентифікацію; - нижча популярність (менша кількість користувачів)	для всіх повідом-лень за замовчу-ванням	Android, iOS, Linux, macOS, Windows

Telegram – це швидкий, безкоштовний, безпечний та простий у використанні месенджер, що був запущений в 2013 р. Telegram – це хмарний додаток, що використовує безшовну синхронізацію, саме тому користувачі можуть користуватися програмою Telegram на всіх своїх пристроях одночасно, оскільки повідомлення легко синхронізуються між будь-якою кількістю користувацьких пристроїв (смартфони, планшети, ноутбуки, комп’ютери тощо). Telegram входить до п’ятірки найбільш затребуваних додатків у світі (рис.1.9б) та має близько мільярда активних користувачів [18]. Додаток

Telegram дає можливість надсилати повідомлення, фотографії, відео та файли різних типів (розміром до 2 Гб), створювати групи до 200000 людей, канали для трансляції на необмежену аудиторію. Ви можете писати своїм телефонним контактам і знаходити людей за їхнім іменем користувача. Також Telegram підтримує наскрізно зашифровані голосові дзвінки, голосові чати та відеовиклики для великої кількості учасників [18].

WhatsApp – найпопулярніший месенджер в світі. В Україні він на 4 місці за популярністю, але в світі ним користується понад 2,7 млрд користувачів [15]. WhatsApp був створений у 2009 р. WhatsApp був першим мобільним сервісом приватних повідомлень, який набрав критичну масу користувачів. Він безкоштовний, дозволяє проводити відео та голосові дзвінки, використовувати самознищувані повідомлення та зображення, має простий у використанні інтерфейс та цікаві функції, але для виконання основних функцій, таких як спілкування в чаті чи здійснення дзвінків, додаток вимагає доступу до конфіденційних даних на телефоні користувача [13].

Signal – це поширений у світі додаток для справді приватного обміну повідомленнями. Криптографічні технології забезпечують додаткові рівні конфіденційності, окрім самого додатка Signal. З моменту запуску в 2013 році протокол Signal використовує технологію наскрізного шифрування (E2EE), що стала фактичним стандартом для приватного спілкування, захищаючи вміст мільярдів розмов у WhatsApp, Google Messages та багатьох інших. Signal також продовжує інвестувати в дослідження та розробки з метою розширення конфіденційності зв'язку. Це зобов'язання для розробників Signal лежить в основі нещодавньої роботи з додавання рівня квантового опору до протоколу Signal та попередньої роботи над технологіями захисту метаданих, які допомагають захистити особисті дані, такі як список контактів, членство в групах, ім'я профілю та іншу особисту інформацію. Основна зосередженість на збереженні приватності спілкування є однією з причин, чому розробники Signal працюють відкрито, роблячи код відкритим для перевірки [20].

2 ОСНОВНІ ПРИНЦИПИ ФУНКЦІОНУВАННЯ МЕСЕНДЖЕРІВ

2.1 Принцип дії месенджерів

Месенджери створені для покращення як ділового, так і особистого спілкування. Миттєві повідомлення можна використовувати для індивідуального та групового спілкування. Для обміну миттєвими повідомленнями користувачі-відправники та користувачі-одержувачі повинні мати підключення до інтернету та встановлений додаток для обміну миттєвими повідомленнями на своїх пристроях (смартфон, комп'ютер, ноутбук, планшет тощо).

Інструменти обміну миттєвими повідомленнями залежать від кількох складних протоколів, таких як XMPP (Extensible Messaging and Presence Protocol), та стандартів шифрування, таких як TLS (Transport Layer Security), щоб забезпечити безпеку, шифрування та успішну доставку повідомлень, забезпечуючи конфіденційність [9].

Процес обміну миттєвими повідомленнями містить в собі 8 основних кроків (рис. 2.1).

На першому кроці потрібно завантажити та встановити клієнтську програму для обміну миттєвими повідомленнями на особистий клієнтський пристрій. Далі, використовуючи власний протокол, програма для обміну миттєвими повідомленнями підключиться до сервера.

Другий крок – це реєстрація. Після успішного підключення програми месенджера до сервера користувачу буде запропоновано ввести ім'я користувача та пароль для реєстрації. Для подальших відвідувань користувачу потрібно буде використовувати ці облікові дані. Після підтвердження даних для входу користувач миттєво ввійде в систему.

Рисунок 2.1 – Процес основних етапів роботи месенджера

Крок 3 – це збір даних та синхронізація контактів. Програма для обміну миттєвими повідомленнями збирає необхідну інформацію, таку як загальна кількість портів, список контактів, IP-адреса користувацького пристрою тощо, і надішле її на сервер. Після відкриття месенджера з'явиться список контактів у самій програмі.

Крок 4 – це синхронізація контактів на стороні сервера. Сервер створює тимчасовий файл для зберігання інформації про кожне підключення та списку контактів, а також перевірить, хто з контактів користувача зараз у системі. Сервер надсилає клієнту повідомлення з контактною інформацією зареєстрованого користувача та надає доступ до контактної інформації онлайн-контактам [9].

Крок 5 – це надсилання повідомлень. Для початку спілкування користувач у списку контактів співрозмовника, відкривається вікно для введення повідомлення. Після введення натиснення кнопки «надіслати» одразу відправить повідомлення одержувачу.

Крок 6 – це шифрування повідомлень та обробка сервером. Після набору повідомлення та натискання кнопки «надіслати», це конкретне повідомлення шифрується та надсилається на сервер служби обміну миттєвими повідомленнями для подальшої обробки.

Крок 7 – це маршрутизація та доставка повідомлення одержувачам. На цьому етапі сервер миттєвих повідомлень перевіряє доступність одержувача та направляє повідомлення. Якщо одержувач онлайн, повідомлення надсилається безпосередньо на його пристрій. Там повідомлення розшифровується та відображається у месенджері [9].

Останній восьмий крок – це розширення розмови та перегляд повідомлень. Одержувач може відповісти на повідомлення таким самим чином. Під час або після розмови співрозмовники можуть переглядати попередні повідомлення та відповідати на поточні. Після завершення розмови можна закрити вікно повідомлення і вийти з режиму онлайн або вийти з програми.

2.2 Архітектура програм обміну миттєвими повідомленнями

Миттєвий обмін повідомленнями забезпечує цілісність зв'язку завдяки численним механізмам автентифікації та з'єднанням Secure Sockets Layer (SSL). Інтеграція з Portal Server та Access Manager забезпечує додаткові функції

безпеки, політику доступу на основі служб, керування користувачами та безпечний віддалений доступ [21].

Месенджери будуються за клієнт-серверною архітектурою та містять такі основні компоненти: клієнт, сервер, мультиплексор, протоколи доступу, зв’язку та передачі, служба управління доступом, API тощо.

Ресурси миттєвого обміну повідомленнями (клієнт) - це набір файлів, що складають клієнтську програму, за допомогою якої кінцеві користувачі можуть ініціювати, складати та відповідати на повідомлення. Зазвичай користувачі також використовують клієнт для участі в конференціях. Клієнт також називається Sun Java System Instant Messenger [21].

Сервер миттєвих повідомлень - це система електронної доставки повідомлень, яка підтримує доставку миттєвих повідомлень з однієї системи до іншої. Сервер надає інформацію про присутність клієнтам Instant Messenger, дозволяє кінцевим користувачам встановлювати сеанси та забезпечує дотримання політик.

Мультиплексор миттєвих повідомлень - це компонент масштабованості, який об'єднує з'єднання месенджерів. Для підтримки великих розгортань з тисячами одночасних з'єднань, месенджер використовує мультиплексор з'єднань для покращення масштабованості сервера. Цей компонент відкриває одне з'єднання із сервером миттєвих повідомлень. Можна встановлювати мультиплексор поза брандмауером, залишаючи сервер всередині брандмауера, щоб захистити його від несанкціонованого зовнішнього доступу.

Протоколи доступу, зв’язку та передачі - це протоколи, такі як LDAP, HTTP, TCP/IP та SMTP.

Служба управління доступом (Access Manager) - це служба, що керує доступом за допомогою SDK Access Manager, щоб забезпечити підтримку керованих політик та можливостей єдиного входу [21].

API миттєвих повідомлень дозволяє створювати власні клієнти миттєвих повідомлень.

Архітектуру програмного забезпечення для обміну миттєвими повідомленнями показано на рис. 2.2.

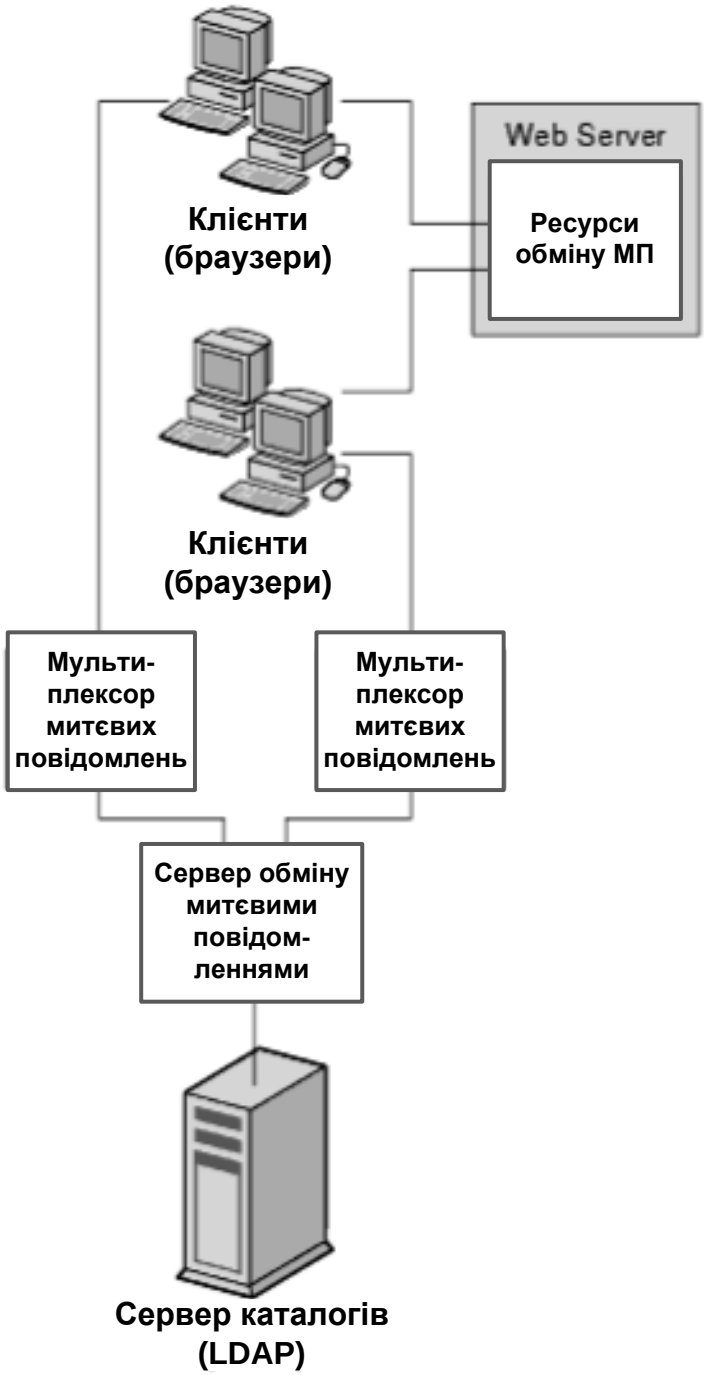


Рисунок 2.2 - Архітектура програмного забезпечення для обміну миттєвими повідомленнями

Сервер миттєвих повідомлень виконує такі завдання, як керування привілеями та безпекою миттєвих повідомлень, дозволяючи клієнтам миттєвих повідомлень спілкуватися один з одним, надсилаючи сповіщення, ініціюючи чат та публікуючи повідомлення в доступних новинних каналах. Сервер миттєвих повідомлень також обробляє архівування, сповіщення календаря та сповіщення електронною поштою офлайн.

Сервер миттєвих повідомлень маршрутизує, передає та доставляє миттєві повідомлення для месенджера.

Компонент мультиплексора миттєвих повідомлень з'єднує кілька з'єднань миттєвих повідомлень в одне TCP-з'єднання, яке потім підключається до сервера миттєвих повідомлень. Мультиплексор зчитує дані з миттєвих повідомлень і записує їх на сервер. Кколи сервер надсилає дані до миттєвих повідомлень, мультиплексор зчитує дані та записує їх у відповідне з'єднання. Мультиплексор не виконує жодної автентифікації кінцевого користувача та не аналізує протокол клієнт-сервер. Кожен мультиплексор підключений тільки до одного сервера миттєвих повідомлень.

Як приклад на рис. 2.3 показана технічна архітектура месенджеру Facebook Messenger (FM). Вся система складається з кількох слабо пов'язаних модулів, що працюють разом один з одним, таких як веб-рівень, інтерфейс користувача, реєстратор чату, модуль присутності користувачів та кластер каналів [22].

Інтерфейс користувача написаний на JavaScript, а для рендерингу на стороні сервера використовується частина PHP.

Веб-рівень обробляє звичайні веб-запити, обслуговує автентифікацію користувачів, налаштування конфіденційності друзів, історію чату, оновлення, зроблені друзями, та бізнес-логіку інших функцій платформи.

Модуль присутності користувача надає інформацію про онлайн-доступність контактів або друзів користувача. Він написаний на C++ та є модулем системи, який найчастіше пінгується. Модуль агрегує онлайн-інформацію користувачів у пам'яті та надсилає її клієнту за запитом.

Рисунок 2.3 – Технічна архітектура системи миттєвих повідомлень Facebook Messenger

Сервери каналів займаються чергою повідомлень та їх доставкою. Функціональність написана за допомогою Erlang. Erlang — це мова паралельного функціонального програмування, яка використовується для написання масштабованих та високодоступних систем реального часу [22].

Реєстрація метаданих чату та іншої інформації здійснюється за допомогою модуля реєстрації чату. Він написаний на C++ та реєструє інформацію між завантаженнями сторінок інтерфейсу користувача.

2.3 Протоколи доступу та зв’язку, що використовуються в месенджерах

Миттєвий обмін повідомленнями побудовано на власних інтернет-технологіях, тому можна підтримувати єдину архітектуру всередині та зовні певної організації, навіть під час співпраці з клієнтами та партнерами. Крім того, немає потреби прив'язки до власної системи. Усі ключові компоненти

месенджерів базуються на перевірених відкритих інтернет протоколах, зокрема: LDAP, HTML, HTTP, SMTP, TCP/IP, XMPP тощо.

Протокол LDAP (Lightweight Directory Access Protocol) забезпечує доступ до інформації з каталогу компанії, що дозволяє створювати точну та безпечну систему миттєвого обміну повідомленнями.

HTML (HyperText Markup Language) – це мова форматування для забезпечення доступу клієнта через веббраузер.

HTTP (HyperText Transfer Protocol) – це транспортний протокол для надання клієнту доступу через веббраузер.

SMTP (Simple Mail Transfer Protocol) – це простий протокол передачі пошти для надійної доставки миттєвих повідомлень через поштові повідомлення інтернету.

TCP/IP (Transmission Control Protocol / Internet Protocol) – це перевірений всесвітній мережний протокол.

XMPP (Extensible Messaging and Presence Protocol) – це розширюваний протокол повідомлень та присутності для взаємодії з публічними мережами через шлюзи з відкритим кодом.

Для форматування миттєвих повідомлень використовується протокол XMPP. Самі тіла повідомлень можуть бути опрацьовані в HTML.

В месенджерах інформація та налаштування користувача отримуються з каталогу LDAP. Цей каталог може бути або виділеним для використання системою миттєвих повідомлень, або спільним для інших компонентів, таких як Access Manager або Portal Server. Дані користувача зазвичай отримуються за допомогою функцій пошуку LDAP. Розгортання миттєвих повідомлень, які використовують Access Manager та Portal Server, використовують один і той самий сервер LDAP [21].

Зв'язок між сервером та клієнтом-сервером в месенджерах відбувається через TCP/IP.

Месенджер використовує протокол SMTP для надсилання повідомлень користувачам, які не працюють в мережі.

Браузери використовують HTTP для отримання файлів ресурсів Instant Messenger з веб-сервера. Після отримання браузер зчитує HTML-код та відображає вміст файлів [21].

Instant Messaging 7 – це клієнт-серверне рішення XMPP/Jabber, здатне взаємодіяти з XMPP-сумісними серверами, клієнтами та шлюзами. Шлюзи доступні у спільноті відкритого коду для забезпечення зв'язку між Jabber та AOL, Yahoo та іншими системами миттєвого обміну повідомленнями [21].

2.4 Функціональні можливості месенджерів

Кожен додаток для обміну миттєвими повідомленнями має свою конкурентну перевагу. Однак більшість месенджерів мають певний набір стандартних та розширених функцій (рис. 2.4).

Дві основні функції характеризують месенджер як такий [3], це:

- текстове спілкування в режимі реального часу (повідомлення надсилаються та отримуються миттєво),

- індикатори присутності (можливість перевірити доступність будь-кого зі списку контактів).

Розширені функції [3, 9] – це свідчення еволюції месенджерів протягом багатьох років – від простого обміну текстовими повідомленнями до набагато просунутіших функцій: голосові та відеодзвінки, спільний доступ до файлів, спільний доступ до екрана, індикатори набору тексту, групові чати та багато іншого. Наприклад, індикатори набору тексту відображають у режимі реального часу, коли один користувач активно друкує повідомлення; ця функція додає рівень інтерактивності та очікування до розмови, повідомляючи користувачам, що вони скоро отримають відповідь.

Всі ці функції обміну миттєвими повідомленнями дозволяють користувачам підключатися з різних місць, організовувати зустрічі та співпрацювати з колегами або друзями в різних географічних регіонах, сприяючи зміцненню стосунків та спрощенню віддаленої роботи.

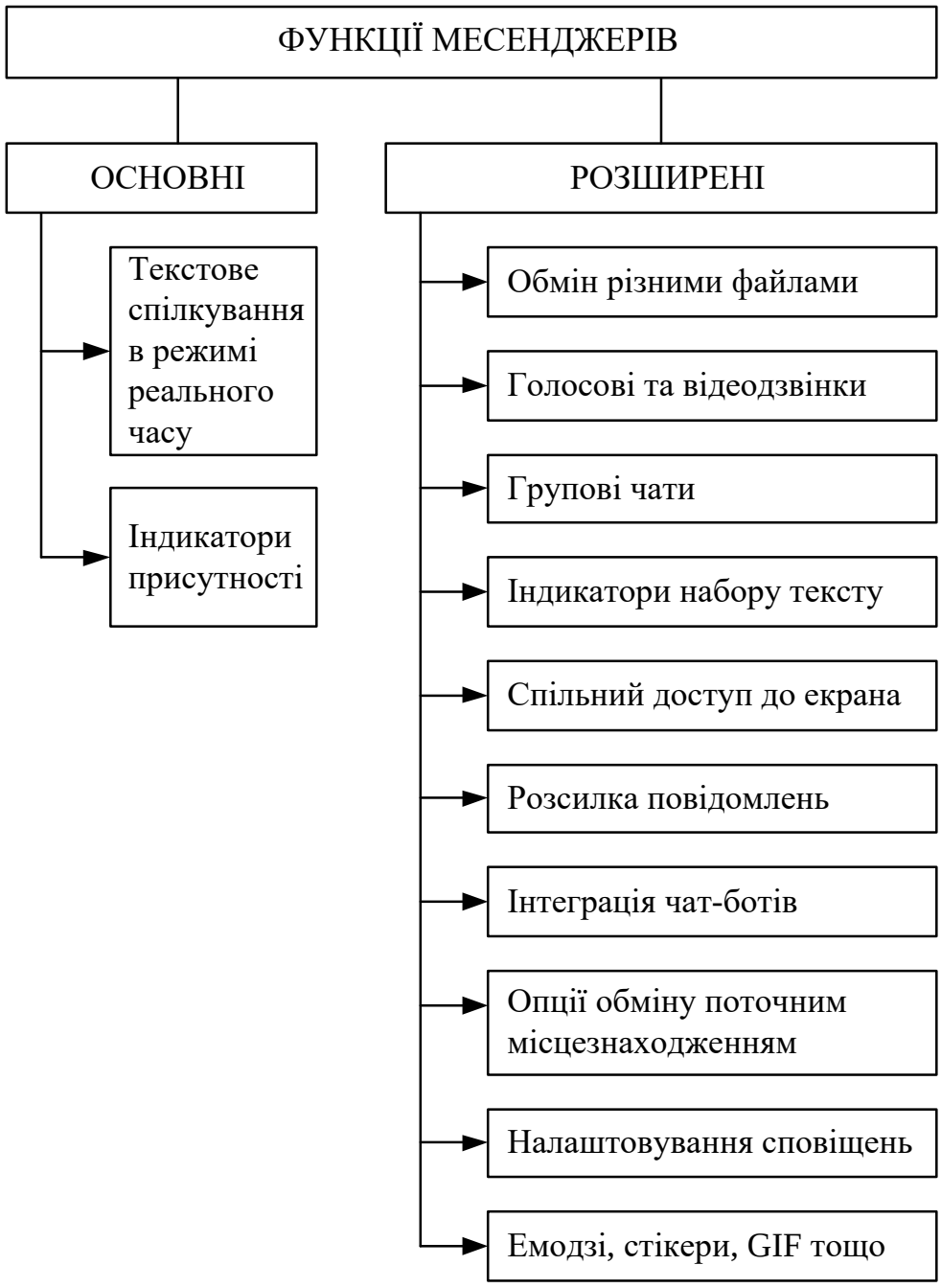


Рисунок 2.4 – Функції месенджерів

Багато месенджерів сьогодні мають розширені функції чату, безпеки та співпраці, які допомагають безперебійно керувати бізнес-операціями та робочими процесами команди, використовувати платформи обміну миттєвими повідомленнями для організації командних зустрічей, мозкових штурмів та обміну швидкими оновленнями, покращуючи співпрацю.

3 ПРОБЛЕМИ БЕЗПЕКИ В БЕЗКОШТОВНИХ МЕСЕНДЖЕРАХ

3.1 Основні проблеми безпеки в месенджерах

Програми для обміну миттєвими повідомленнями, в тому числі і мобільні додатки, набувають дедалі більшої популярності. Сьогодні месенджерами користуються мільярди користувачів і при використанні месенджерів через інтернет передаються дуже великі обсяги даних, що можуть викликати інтерес зловмисників. Метадані та особиста інформація збираються та зберігаються щодня, поки споживачі шукають захисту від стеження або атак хакерів.

Сучасні споживачі стали більше усвідомлювати конфіденційність в інтернеті, небезпеку цифрового збору даних та крадіжки особистої інформації. Діяльність стеження зростає в усьому світі, і занепокоєння серед користувачів щодо цього значно зросло у всьому світі. Дослідження показують, що користувачі турбуються про захист конфіденційності на своїх смартфонах та виступають проти додатків, які збирають їхні контакти [23]. Саме тому питання безпеки інформації, що передається через месенджери, особливо безкоштовні, є надзвичайно важливими та потребують уваги.

Існує багато доступних додатків, деякі з них є лідерами за популярністю, доступністю платформи або функціями. З точки зору безпеки, важливо розрізняти достатньо безпечні месенджери від менш безпечних та надійних. Важливо розуміти, які месенджери функціонують на основі вбудованих функцій безпеки і конфіденційності, розташування та подальшого доступу до збережених даних.

Зловмисники постійно використовують різні проблеми безпеки та конфіденційності для зламу популярних месенджерів. Тому є необхідність визначити можливі проблеми безпеки месенджерів та застосовувати засоби захисту від цих проблем.

Основні проблеми безпеки в месенджерах пов’язані з персональними даними, що індивідуальні для кожної людини. Користувачі повинні визначити, яка саме інформація потребує захисту. Це може варіюватися від повідомлень, контенту та ідентифікаційних даних до метаданих та місцезнаходження, часто охоплюючи всі ці аспекти. Кожна потенційна загроза створює власні труднощі, тому важливо враховувати різні фактори [24].

Основні проблеми безпеки в месенджерах представлені на рис. 3.1. Кожна можлива небезпека пов’язана з унікальними перешкодами, які необхідно подолати, що підкреслює важливість врахування різних аспектів.

Рисунок 3.1 – Основні проблеми безпеки в месенджерах

Несанкціонований доступ до даних месенджера може багато чого розкрити. Це включає перехоплення повідомлень, перегляд минулих чатів та отримання хмарних даних. Він також містить непомітне проникнення. Такий сценарій створює умови для різноманітних неочікуваних та руйнівних подій. Наслідки можуть включати шантаж, допомогу особі, яка себе видає за іншу особу, або зловмисні дії шахраїв.

Розкриття інформації про місцезнаходження користувача або його номер телефону можуть бути використані зловмисниками. Вони можуть відстежувати місцезнаходження та використовувати звички переміщень користувача для планування нападу або продажу цієї інформації [25].

Месенджери можуть містити різні вразливості, що можуть призвести не тільки до розкриття конфіденційної інформації. Сумнівний додаток із сумнівного джерела несе небезпеку. Невідомі завантаження запрошують хакерів, спричиняючи хаос на пристрої користувача. Один клік може поставити під загрозу дані користувача, розкриваючи особисту інформацію кіберзлочинцям. Хоча обліковий запис може не містити важливої інформації, його все одно можна використовувати для DDoS-атак, розсилки спаму, обміну шкідливими посиланнями тощо.

Деякі месенджери не шифрують повідомлення та файли, що зберігаються в хмарі. Якщо хакеру вдасться зламати хмарну інфраструктуру , це може призвести до розкриття конфіденційних даних [24].

Наслідки цих проблем можуть включати шантаж, дозвіл комусь маскуватися під довірений контакт або накопичення інформації, призначеної для складних шахрайств, створених за допомогою тактик соціальної інженерії.

3.2 Ризики безпеки в безкоштовних месенджерах

Безкоштовні месенджери є привабливими цілями для кіберзлочинців через їх широке використання та часто неадекватні заходи безпеки. Ці додатки можуть наражати користувачів на різні ризики безпеки (рис. 3.2).

Рисунок 3.2 – Ризики безпеки в безкоштовних месенджерах

Основна проблема використання месенджерів для бізнесу полягає в відсутності контролю організацій над платформою, тобто вони не можуть регулювати спілкування співробітників. Така відсутність нагляду може призвести до неконтрольованого обміну конфіденційною інформацією за межами цільових одержувачів, що збільшує ризики витоку даних та недотримання галузевих норм.

Популярні платформи обміну повідомленнями є поширеними векторами розповсюдження шкідливого програмного забезпечення через свою відкриту природу, дозволяючи будь-кому спілкуватися з будь-ким. Такий підхід означає, що користувачі не можуть запобігти зв’язку хакерів через ці програми, що може зробити їх вразливими до отримання шкідливого програмного забезпечення, компрометації їхніх пристроїв та крадіжки їхньої інформації. Кіберзлочинці часто маскують шкідливі посилання або вкладення в повідомлення, які після відкриття можуть встановлювати шкідливе програмне забезпечення, яке фіксує натискання клавіш, отримує доступ до файлів або навіть контролює весь пристрій [1].

Погані механізми автентифікації можуть дозволити неавторизованим особам отримати доступ до облікових записів, що призведе до витоків даних. Слабкі паролі, відсутність багатофакторної автентифікації та недостатні методи шифрування полегшують зловмисникам доступ. Потрапивши всередину, вони можуть викрасти конфіденційну інформацію, видавати себе за інших користувачів або поширювати дезінформацію, що потенційно може завдати значної фінансової шкоди та завдати репутаційної шкоди.

3.3 Загрози аналізу даних в безкоштовних месенджерах

Одна з найпідступніших небезпек безкоштовних месенджерів – це аналіз даних (рис. 3.3). Ці платформи часто збирають та аналізують дані користувачів для монетизації своїх послуг, що створює значні проблеми для конфіденційності.

Безкоштовні месенджери часто збирають розмови користувачів, метадані та особисту інформацію. Ці зібрані дані часто продаються третім сторонам, таким як рекламодавці або брокери даних, часто без явної згоди користувача. Така практика викликає значні проблеми з конфіденційністю, оскільки користувачі можуть не повністю усвідомлювати, якою мірою збираються та поширюються їхні особисті дані.

Рисунок 3.3 - Загрози аналізу даних в безкоштовних месенджерах

Дані, зібрані від користувачів, використовуються для створення детальних профілів користувачів, які потім використовуються для цільової реклами. Ці профілі можуть містити інформацію про ваші інтереси, поведінку та вподобання, що дозволяє рекламодавцям показувати високоперсоналізовану рекламу. Хоча деяким це може здаватися корисним, багатьом користувачам це може здаватися нав'язливим, оскільки часто показує, скільки додаток знає про них. Таке порушення конфіденційності може призвести до втрати довіри до

платформи, оскільки користувачі стають дедалі більше стурбованими тим, як використовується їхня інформація [1].

Дані, що передаються третім сторонам за допомогою месенджерів, можуть бути продані, передані або спричинити витік. Щойно дані виходять з-під контролю застосунку, стає складно контролювати, як вони використовуються, що призводить до потенційного зловживання. Такий неконтрольований обмін даними може призвести до того, що конфіденційна інформація стане доступною зловмисникам або буде використана таким чином, як користувач ніколи не планував, наприклад, для крадіжки особистих даних, фінансового шахрайства або небажаного просування. Відсутність прозорості та контролю над цим обміном даними ще більше підриває довіру користувачів і може мати серйозні наслідки для особистої конфіденційності та безпеки.

4 ЗАСОБИ БЕЗПЕКИ ІНФОРМАЦІЇ В МЕСЕНДЖЕРАХ

4.1 Захист інформації в месенджерах

Оскільки споживачі вимагають кращої безпеки та конфіденційності в месенджерах, компанії-розробники програмного забезпечення намагаються вирішити ці проблеми та впроваджують різноманітні засоби безпеки. Основні засоби безпеки в месенджерах наведені на рис. 4.1.

Рисунок 4.1 – Основні засоби безпеки в месенджерах

Всі ці засоби (рис. 4.1) дозволяють користувачам та/або підприємствам будь-якого типу уникнути можливого порушення конфіденційності чи даних. Але найбільш ефективним є застосування комплексних заходів безпеки, що включають в себе надійні методи шифрування, надійні методи автентифікації, гнучке розгортання, суворі політики зберігання даних, постійне оновлення протоколів безпеки та інші засоби.

4.1.1 Шифрування в месенджерах

Наскрізне шифрування E2EE (рис. 4.2) - це найбільш надійний спосіб шифрування в системах миттєвих повідомлень. Наскрізне шифрування означає, що повідомлення шифруються під час передачі, і жодна копія не зберігається незашифрованою на серверах постачальників послуг. Ніхто, окрім людей, які спілкуються, не може переглядати ці повідомлення; жодна третя сторона, навіть уряд чи розробники цих месенджерів. Зв'язок передається за допомогою секретного коду, а не звичайного тексту [23].

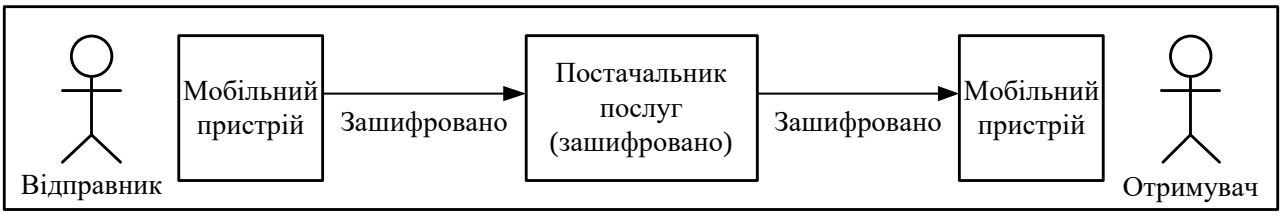


Рисунок 4.2 – Наскрізне шифрування

При E2EE дані або повідомлення шифруються на пристрої, з якого вони створюються та надсилаються, а потім зберігаються в зашифрованому стані, доки не досягнуть цільових одержувачів, де дані потім розшифровуються. Таким чином, дані захищені протягом усього часу передачі. Треті сторони або неавторизовані користувачі не зможуть прочитати повідомлення, навіть якщо його перехоплено. E2EE працює над забезпеченням безпеки зв'язку та даних.

Він доступний для читання лише між передбачуваним відправником та одержувачем. Навіть постачальник послуг чи сервер не можуть прочитати зашифровані повідомлення [26].

Наскрізне шифрування зазвичай працює з використанням асиметричної криптографії, що включає відкритий ключ та закритий ключ для шифрування та дешифрування. Відкритий ключ генерується довіреним центром сертифікації та є загальнодоступним. Відкриті ключі зберігаються на сервері та використовуються для розшифрування повідомлень. Однак закритий ключ зберігається безпосередньо на пристрої одержувача. Тільки унікальний та секретний закритий ключ може розшифрувати повідомлення, надіслане з відповідним відкритим ключем. Відкритий ключ використовується для блокування повідомлення, тоді як закритий ключ служить для його розблокування. Оскільки доступ до закритого ключа має лише адресат, повідомлення не може бути розшифроване ніким іншим.

Наскрізне шифрування вважається надзвичайно безпечним. Навіть якщо хакери перехоплять повідомлення, вони не зможуть його прочитати без закритого ключа, який мають лише відправник та одержувач.

Іншим типом шифрування, що використовується, є шифрування під час передачі (рис. 4.3). Це означає, що повідомлення шифрується між користувачем і постачальником послуг, але зберігається у вигляді відкритого тексту на сервері. Це створює ризик, оскільки збережені повідомлення можуть бути прочитані постачальником послуг або іншими третіми сторонами, які отримують доступ до сервера [23].

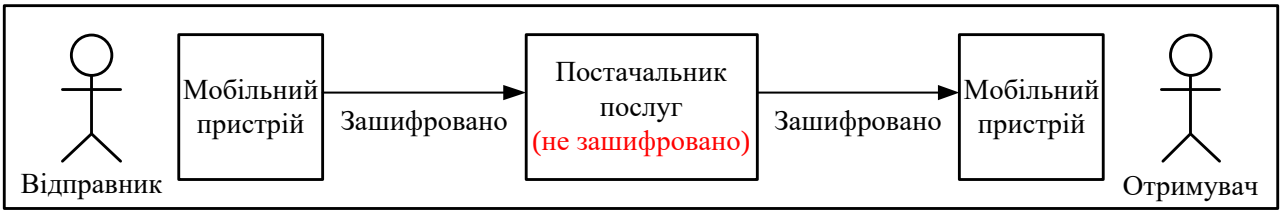


Рисунок 4.3 – Шифрування під час передачі

Адекватний рівень наскрізного шифрування має бути стандартним для сучасних месенджерів і функцією безпеки за замовчуванням, яка має бути включена в месенджери. Більшість месенджерів (навіть безкоштовних) сьогодні забезпечують наскрізне шифрування.

Деякі месенджери (наприклад Signal, WhatsApp, Facebook Messenger тощо) використовують протокол наскрізного шифрування Signal, що був розроблений некомерційною організацією для однойменного месенджера Signal. Цей протокол шифрування детально документований та має бібліотеки з відкритим вихідним кодом на мовах Java, JavaScript та C++.

Деякі месенджери використовують шифрування, що базується на протоколі Signal. Наприклад месенджер Viber використовує для шифрування концепцію протоколу Signal, але інші криптографічні алгоритми.

Деякі месенджери (наприклад Telegram) пропонують наскрізне шифрування, але воно не ввімкнено за замовчуванням. Telegram пропонує цю функцію як опцію «секретного чату». Якщо вона не ввімкнена, використовується шифрування під час передачі.

4.1.2 Надійна автентифікація

Одним із найважливіших аспектів безпеки є автентифікація, яка вважається першою лінією захисту, але традиційні (централізовані) механізми автентифікації не можуть забезпечити безпечне з'єднання, оскільки вони мають слабкі місця, проблему конфіденційності та єдину точку відмови. Крім того, механізми розподілу дають збій, коли ключі розподілені в центральній структурі, і тому не можна забезпечити з'єднання. Найбезпечнішим рішенням для цього є використання централізованої автентифікації, яка містить набір функцій, включаючи прозорість та стабільність. При застосуванні централізованої автентифікації було виявлено, що вона ефективна в процесі комунікації та приблизно на 70% краща та в десять разів швидша, ніж центральний процес автентифікації [27].

Підтримка багатофакторної автентифікації (MFA) слугує важливим додатковим рівнем безпеки. Цей додатковий захист може ефективно запобігти несанкціонованому доступу.

Двофакторна автентифікація (2FA) панує в цифровій безпеці, встановлюючи новий стандарт захисту. Цей широко поширений захист є скрізь в інтернеті, від гігантів соціальних мереж до банківських додатків. 2FA додає важливий другий рівень перевірки, балансуючи між надійною безпекою та зручністю для користувача. 2FA має багато методів автентифікації, від біометрії до одноразових кодів, що ідеально підходять для месенджерів. 2FA запобігає несанкціонованому доступу, але не перевантажує користувача. Вона може захистити облікові записи користувачів від сучасних кіберзагроз [25]. Функції мобільної безпеки, такі як 2FA, також відіграють ключову роль у захисті персональних даних, що зберігаються на смартфонах, на які часто спрямовані атаки хакерів.

Також використовується інтерактивний криптографічний протокол ZKP (Zero-Knowledge Proof) - протокол доказу з нульовим розголошенням. Він дозволяє користувачеві довести, що він знає певну приватну та конфіденційну інформацію, не розкриваючи її. Наприклад, користувач може підтвердити свою особу, не розкриваючи її [27]. Вся робота з ним буде зашифрована і алгоритми доказу нульового розголошення не дозволяють передачу будь-яких даних. Ключі або конфіденційні матеріали не шифруються. Файли та ключі завжди шифруються, і ніхто не може прочитати конфіденційні повідомлення, а клієнти мають засоби зв'язку один з одним та з сервером. Це свідчить про те, що захист працює належним чином, і таким чином досягається повна довіра без витоку інформації [27].

4.1.3 Відкритий вихідний код

Відкритий вихідний код означає, що додаток відкритий для зовнішньої відповідальності та аудиту експертами, що може бути корисним способом

привернути увагу до будь-яких слабких місць або вразливостей у коді [28].

Месенджер з відкритим вихідним кодом надає перевагу ретельних оцінок безпеки. Цей метод дозволяє як початківцям, так і експертам допомагати додатку. Вони можуть протестувати його роботу та знайти недоліки безпеки на сервері та клієнті. Відкритість дозволяє проводити перевірки. Хоча існує ризик, що зловмисники можуть скористатися будь-якими вразливостями, перш ніж спільнота їх виправить. Відкритий вихідний код не гарантує безпеку даних користувачів, однак він допомагає покращити її.

Чим популярніший месенджер, тим більша ймовірність того, що люди переглядають код, готові повідомити про проблеми. Той простий факт, що є люди, які бажають і можуть працювати з таким відкритим вихідним кодом, означає, що помилки, ймовірно, будуть виправлені швидше, а будь-хто, хто спробує зробити щось підступне в коді, буде публічно викритий [29].

4.1.4 Додаткові засоби безпеки

Кожен месенджер може включати функцію самовидалення повідомлень, що може бути за замовчуванням або активована за вибором користувача. Також користувач може налаштовувати час демонстрації повідомлень до їх зникнення. У будь-якому випадку опція ввімкнення або вимкнення зникнення повідомлень у налаштуваннях є нважливою для безпеки. Автоматичне видалення повідомлень не повинно залишати слідів. Під час активації цієї функції краще не використовувати сервер або хмарне сховище. Як тільки повідомлення зникають для користувача, вони повинні зникати всюди.

В деяких месенджерах можливе однорангове спілкування. У конфігурації peer-to-peer повідомлення доставляються безпосередньо на пристрій одержувача без залучення будь-яких посередників. Проте, ця стратегія має свої недоліки. Вона може розкривати імена користувачів та тривалість їхньої взаємодії, що дещо знижує анонімність та конфіденційність [25].

Важливою є також відповідність нормативним вимогам. Компанії

повинні дотримуватися низки правил захисту даних, таких як DORA, SEC, GDPR, HIPAA та інші. Месенджери розроблені для забезпечення відповідності цим правилам, пропонують розширені функції безпеки, контроль даних та конфігурації відповідності. Ці системи дозволяють підприємствам застосовувати політики обробки даних, забезпечувати шифрування комунікацій та надавати необхідні інструменти для демонстрації відповідності під час аудитів [1].

Для підвищення безпеки також можуть використовуватися такі додаткові функції [24]:

- функція для створення PIN-коду або парольної фрази для входу до важливих зон безпеки або приватних розмов;

- функція автоматичного блокування програм, яка активується, коли користувач більше не знаходиться поруч зі своїм пристроєм;

- шифрування резервних копій повідомлень та файлів, що зберігаються в хмарі;

- можливість автоматичного видалення прив’язаного пристрою, раніше підключеного до облікового запису.

4.2 Порівняння забезпечення безпеки в різних месенджерах

В даній роботі було виконано порівняння п’яти безкоштовних та найбільш популярних в Україні меседжерів за характеристиками безпеки на основі детального аналізу різних сучасних джерел [1 – 3, 9 – 29]. Результати порівняння наведено в табл. 4.1. При порівнянні месенджерів були проаналізовані найбільш важливі показники (функції) безпеки месенджерів, зокрема ті, що були розглянуті в п. 4.1 даної роботи.

Варто зазначити, що розробники месенджерів постійно оновлюють додатки, додають нові функції, що вдосконалюють їхню безпеку. І тому існує потреба порівняння месенджерів за показниками безпеки, оскільки порівняльні аналізи минулих років втрачають свою актуальність.

Таблиця 4.1 – Порівняння меседжерів за показниками безпеки

№	Показник	Viber	FM	Telegram	Whats App	Signal
1	Наскрізне шифрування за замовчуванням	+	–	–	+	+
2	Можливість наскрізного шифрування	+	+	+	+	+
3	Шифрування під час передачі	+	+	+	+	+
4	Приватний ключ недоступний постачальнику	+	–	+	+	–
5	Видалення з серверу	+	–	–	–	–
6	Самознищення повідомлень	+	+	+	–	+
7	Відкритий вихідний код (сервер і клієнт)	–	–	–	–	+
8	Блокування паролем	+	–	+	+	+
9	Підтвердження SMS / Email	–	–	–	+	–
10	Виявлення знімків екрану	–	–	–	–	–
11	Двоетапна верифікація	–	+	+	+	+
12	Віддалений вихід із системи	–	–	+	–	–
13	Дистанційне стирання повідомлень	–	–	–	+	–
14	Самоліквідація облікового запису	–	–	+	–	–

Продовження табл. 4.1

№	Показник	Viber	FM	Telegram	Whats App	Signal
15	Відсутність збору месенджером особистих даних користувачів	–	–	–	–	+
16	Генерація та зберігання ключа на пристрої	+	+	+	+	+
17	Шифрування метаданих	–	–	–	–	+
18	Наявність прямої секретності ключів (PFS)	+	+	–	+	+
19	Створення контакту без передачі даних на сервер	+	–	–	–	–
20	Відсутність зберігання переписок користувачів на сервері	–	–	–	–	+
21	Інформування про оновлення ключа шифрування співрозмовника	+	–	–	–	+
22	Відсутність передавання особистих даних користувачів державним органам	+	–	–	–	+
23	Заборона резервного копіювання на ПК або в хмару	–	–	–	–	+
	Результати	12 з 23	6 з 23	9 з 23	10 з 23	15 з 23

Більшість додатків, перелічених в табл. 4.1, забезпечують наскрізне шифрування – це Viber, Signal, WhatsApp. Facebook Messenger використовує наскрізне шифрування тільки при виборі користувачем захищеного чату. Telegram за замовчуванням використовує шифрування під час передачі, хоча він пропонує наскрізне шифрування, але тільки для деяких чатів і за окремим налаштуванням. Важливо те, що наскрізне шифрування за замовчуванням також шифрується під час передачі. Тому у всіх розглянутих месенджерів таке шифрування присутнє. Існує багато месенджерів, які не забезпечують наскрізного шифрування (Hangouts, WeChat, Slack тощо), що робить їх менш безпечними та менш надійними. Але в нашій країні вони не розповсюджені.

Другим важливим питанням після шифрування, є питання про те, чи доступний постачальник послуг до закритого ключа. Telegram та WhatsApp стверджують, що не можуть отримати закритий ключ. Щодо решти додатків з табл. 4.1 інформації не знайдено.

Viber – єдиний додаток з розглянутих, який стверджує, що видаляє повідомлення користувачів із сервера. Повідомлення зберігається в оперативній пам'яті сервера. Після того, як одержувач отримав повідомлення, воно видаляється з оперативної пам'яті.

Telegram, Viber та Signal мають функцію, яка дозволяє повідомленням самознищуватися або зникати через певний проміжок часу як для пристроїв відправника, так і для пристроїв одержувачів. Facebook запускає таймер самознищення для повідомлень, який дозволяє користувачам встановлювати таймер, після якого повідомлення автоматично зникатимуть [23].

Signal має політику повністю відкритого коду. Будь-хто може перевірити вихідний код, протокол та API. Telegram має частково відкритий код.

Signal, Telegram, Viber та WhatsApp мають блокування за допомогою пароля в додатку чату, яке потрібно ввести перед використанням додатка. Після реєстрації нового користувача WhatsApp надсилає код підтвердження через SMS, який потрібен перед завершенням встановлення.

Більшість месенджерів пропонують функцію двоетапної перевірки, коли для входу в додаток потрібно використовувати як SMS-код, так і пароль. Додаток Telegram також дозволяє налаштувати адресу електронної пошти для відновлення, якщо користувач забуде пароль.

Функція віддаленого виходу пропонується лише месенджером Telegram. Більшість додатків дозволяють входити в додаток з кількох пристроїв. За допомогою цієї функції можна вийти з усіх пристроїв з поточного пристрою.

Ще однією функцією є самознищення облікового запису. Тільки Telegram пропонує цю функцію. Якщо обліковий запис був неактивним протягом певного періоду, за замовчуванням шість місяців, він автоматично самознищиться, а всі повідомлення та медіафайли, пов’язані з обліковим записом, будуть видалені.

У всіх розглянутих додатках, крім Telegram, є функція досконалої прямої секретності PFS (Perfect forward secrecy), яка є особливістю специфічних протоколів узгодження ключів.

Відсутність резервного копіювання на ПК або в хмару присутня тільки у месенджера Signal.

В цілому в результаті порівняння п’яти найпопулярніших в Україні месенджерів за 23 показниками безпеки, можна наступний зробити висновок. Найбільш безпечним месенджером є Signal, оскільки він має 15 з 23 функцій безпеки. Найменш захищеним месенджером є Facebook Messenger, оскільки він має лише 6 з 23 функцій безпеки.

4.3 Рекомендації щодо захисту інформації в безкоштовних месенджерах

Окрім вбудованих у месенджери функцій безпеки, також важливими є поведінка та поводження користувачів, які також несуть відповідальність за безпеку інформації та конфіденційність даних. Існують певні правила, яких варто дотримуватися для під час використання систем миттєвого обміну повідомленнями для особистих цілей , а особливо в бізнесі.

В даній роботі на основі аналізу різних джерел [9, 29 – 32] були сформульовані найбільш важливі рекомендації щодо безпечного використання месенджерів (рис. 4.4).

Рисунок 4.4 – Рекомендації щодо безпечного використання месенджерів

При використанні месенджерів ніколи не варто передавати паролі, банківські реквізити чи дані кредитних карток у чаті, голосових та відеодзвінках, навіть якщо це зашифровано від початку до кінця.

Погана практика - встановлення одного пароля для кількох облікових записів. Якщо один обліковий запис зламано, всі інші облікові записи також стають вразливими. Безпечно створювати окремі, унікальні паролі для кожного з облікових записів.

Часто посилання з невідомих або ненадійних джерел можуть призвести до фішингових вебсайтів, призначених для крадіжки особистої інформації або завантаження шкідливого ПЗ на пристрій користувача. Навіть якщо повідомлення здається надійним, завжди необхідно перевіряти джерело та переконуватися, що вебсайт безпечний, перш ніж натискати на будь-які посилання.

Ніколи не можна завантажувати вкладення від незнайомих контактів, оскільки вони можуть містити шкідливе ПЗ, яке може пошкодити пристрій, викрасти інформацію або поставити під загрозу безпеку. Завантажувати вкладення можна тільки з перевірених джерел, але ї їх варто сканувати на наявність шкідливого ПЗ перед відкриттям.

Що стосується використання месенджерів в бізнесі, то компаніям слід розглянути більш безпечні та відповідні засоби комунікації, розроблені спеціально для корпоративного використання. Ці інструменти пропонують кращий контроль, моніторинг та функції безпеки, гарантуючи, що ділове спілкування залишається захищеним та відповідає відповідним нормам. Компаніям слід бути обережними та шукати альтернативні рішення, які надають пріоритет безпеці, відповідності та цілісності даних. Роблячи це, вони захистять свою діяльність, репутацію та прибуток від численних ризиків, пов’язаних з використанням додатків для обміну миттєвими повідомленнями в бізнес-цілях.

ВИСНОВКИ

Програми для обміну миттєвими повідомленнями користуються великим попитом. Оскільки смартфони та хмарні технології стають все більш поширеними, а обсяг переданих даних стрімко зростає, зростає і потреба в безпечному спілкуванні.

Оскільки технологія миттєвого обміну повідомленнями використовується так широко (як на особистому, так і на професійному рівні), вкрай важливо вживати заходів для захисту даних, що передаються в месенджерах, особливо враховуючи, що уряди, кіберзлочинці та навіть великі технологічні компанії зацікавлені в тому, щоб отримати до них доступ.

В роботі було розглянуто та проаналізовано ряд питань, що стосуються функціонування та проблем безпеки месенджерів.

В першому розділі проаналізовано еволюцію, сучасний стан та основні тенденції розвитку месенджерів. Розглянуто класифікацію месенджерів, переваги та недоліки сучасних додатків обміну миттєвими повідомленнями. Виконано огляд та порівняння найпопулярніших месенджерів.

В другому розділі досліджені основні принципи функціонування месенджерів, зокрема принцип дії, технічна та програмна архітектура, протоколи зв’язку та функціональні можливості месенджерів.

В тертьому розділі проаналізовані основні проблеми безпеки в безкоштовних месенджерах, ризики безпеки та загрози аналізу даних.

В четвертому розділі виконано детальний огляд засобів безпеки інформації, що використовуються в месенджерах. Проведено порівняльний аналіз найбільш використовуваних в Україні месенджерів за 23 характеристиками безпеки. Порівняння функцій безпеки різних месенджерів показало, що Signal є найбезпечнішим безкоштовним додатком. На другому місті за безпекою опинився месенджер Viber. А найгіршим серед розглянутих виявився Facebook Messenger. Серед всіх розглянутих месенджерів Signal, хоча

і входить в п’ятірку найбільш популярних, але має найменшу кількість користувачів в Україні. Враховуючи воєнний стан в нашій країні та часті кібератаки з боку ворога, а також високі показники безпеки месенджеру Signal, українцям слід звернути увагу на цю систему обміну миттєвими повідомленнями.

Також в даній роботі були сформульовані та запропоновані рекомендації для безпечного використання месенджерів, які допоможуть підвищити безпеку та знизити ризики можливих проблем.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Heron N. The Hidden Dangers of Free Messaging Apps: Security Risks and Data Mining Threats. *Salt Communications*. 07.10.2024. URL: https://saltcommunications.com/news/the-hidden-dangers-of-free-messaging-apps-security-risks-and-data-mining-threats/.

2. Vinura P. The Evolution and Impact of Instant Messaging in Modern Communication. *Linked in.* 22.07.2024. URL: https://www.linkedin.com/pulse/evolution-impact-instant-messaging-modern-punu-vinura-op9wf.

3. Chekanov S. What Is Instant Messaging (Definition, How It Works, and Examples). *Brosix Inc. Instant messaging*. 08.07.2024. URL: https://www.brosix.com/blog/what-is-instant-messaging/.

4. Desjardins J. The Evolution of Instant Messaging. *Visual Capitalist. Technology*. 17.11.2016. URL: https://www.visualcapitalist.com/evolution-instant-messaging/.

5. A history of Instant Messaging and Chat. *MAIZE. Jakala*. 23.04.2020. URL: https://www.maize.io/cultural-factory/lizshemaria-historyof-instant-messaging/.

6. Warren T. Microsoft is shutting down Skype in favor of Teams. *The Verge. News.* 28.02.2025. URL: https://www.theverge.com/news/621353/microsoft-skype-shutting-down-retirement-may-2025.

7. Instant Messaging App Market Size, Share, Growth, Trends, Global Industry Analysis, By Type (Mobile Version, Desktop Version, Web Version), By Application (Personal, Enterprise and Others), Regional Insights and Forecast From 2025 To 2033. *Business Research.* 05.05.2025. URL: https://www.businessresearchinsights.com/market-reports/instant-messaging-app-market-101595.

8. Chat app development trends that will shape the industry in 2025. *RST Software.* 15.05.2025. URL: https://www.rst.software/blog/chat-app-development-trends-that-will-shape-the-industry-in-2025.

9. What is Instant Messaging & How Does IM Work with Examples. *REVE Chat. 03*.09.2024. URL: https://www.revechat.com/blog/instant-messaging/#the-future-of-instant-messaging.

10. Рикова В. ТОП-10 месенджерів для повідомлень та дзвінків у 2025 р.. *Vlada Rykova*. 07.11.2024. URL: https://vlada-rykova.com/top-messendzherov/.

11. Duncan C. Advantages And Disadvantages Of Instant Messaging. *DeskAlerts. Internal Communication Tools.* 02.09.2024. URL: https://www.alert-software.com/blog/pros-and-cons-of-instant-messaging-for-business.

12. Топ-10 популярних месенджерів світу та України у 2024 році. *SiteCat.* URL: https://sitecat.net/review/top-10-popular-messengers/.

13. Key K. The Best Private Messaging Apps for 2025. *PCMag.* 05.02.2025. URL: https://www.pcmag.com/picks/best-secure-messaging-apps.

14. Connell A. 10 Most Popular Messaging Apps In 2025 (Data + Trends). *Adam Connell*. 30.01.2025. URL: https://adamconnell.me/popular-messaging-apps/.

15. Chekanov S. The 10 Best Encrypted Messaging Apps in 2025 (Private and Team Messengers). *Brosix Inc. Instant messaging.* 16.06.2024. URL: https://www.brosix.com/blog/encrypted-messaging-apps/.

16. Офіційний сайт Viber. *Viber Media*. 22.05.2025. URL: https://www.viber.com/ua/.

17. A place for meaningful conversations. *Meta*. 22.05.2025. URL: https://www.messenger.com/.

18. Офіційний сайт Telegram. Telegram. 22.05.2025. URL: https://telegram.org/.

19. Офіційний сайт WhatsApp. *WhatsApp LLC.* 22.05.2025. URL: https://www.whatsapp.com/.

20. Whittaker M., Lund J. Privacy is Priceless, but Signal is Expensive. *Signal*. 16.11.2023. URL: https://signal.org/blog/signal-is-expensive/.

21. Introduction to Instant Messaging Software. *Sun Microsystems. Java*. URL: https://docs.oracle.com/cd/E19396-01/819-0063/im-intro.html (дата звернення: 22.05.2025).

22. Shivang. Facebook Real-time Chat Architecture Scaling With Over Multi-Billion Messages Daily. *Scaleyourapp. Architecture, Distributed Systems, Real World Architecture.* URL: https://scaleyourapp.com/facebook-real-time-chat-architecture-scaling-with-over-multi-billion-messages-daily/ (дата звернення: 23.05.2025).

23. Botha J., Van 't Wout C., Leenen L. A Comparison of Chat Applications in Terms of Security and Privacy. *Proceedings of the 18th European Conference on CyberWarfare and Security.* University of Coimbra, Portugal, 2019. P.55.

24. Balaban D. Security Factors To Consider When Choosing A Messaging App. *Forbes.* 18.02.2024. URL: https://www.forbes.com/sites/davidbalaban/2024/02/18/security-factors-to-consider-when-choosing-a-messaging-app/.

25. Dasa A. Essential Security Measures for Messaging Apps. *Troop Messenger.* 29.08.2024. URL: https://www.troopmessenger.com/blogs/security-measures-for-messaging-apps.

26. End-to-End Encryption (E2EE): Definition & Examples. *Okta. Security.* 09.01.2024. URL: https://www.okta.com/identity-101/end-to-end-encryption/.

27. Almhanawi A. R., Nema B. M. Instant Messaging Security: A Comprehensive Review of Behavior Patterns, Methodologies, and Security Protocols. *Journal of Al-Qadisiyah for Computer Science and Mathematics.* 2024. Vol. 16 (1). P. 117 – 123.

28. Messaging app security: Which are the best apps for privacy? *Kaspersky Lab.* URL: https://www.kaspersky.com/resource-center/preemptive-safety/messaging-app-security (дата звернення: 27.05.2025).

29. Mann B. Best Secure and Encrypted Messaging Apps in 2025. *Cyber Insider.* 17.01.2025. URL: https://cyberinsider.com/secure-encrypted-messaging-apps/.

30. Security and Behaviour When Chatting Online. *Federal Office for Information Security.* URL: https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Chat-Messenger/Chats/chats.html (дата звернення: 30.05.2025).

31. Security and Privacy in Instant Messaging. Why is it important for your company or institution? *Tecno Soluciones*. URL: https://tecnosoluciones.com/security-and-privacy-in-instant-messaging-why-is-it-important-for-your-company-or-institution/?lang=en (дата звернення: 30.05.2025).

32. Eve. The Hidden Dangers of Using Instant Messaging Apps for Business Communication. *YOPLA*. 23.06.2024. URL: https://www.yopla.co.uk/blog/the-hidden-dangers-of-using-instant-messaging-apps-for-business-communication.