УДК 004.056.5
JEL C88, C89
DOI 10.32782/2617-5940.2.2025.11

Людмила Петренко
кандидат економічних наук, доцент,
доцент кафедри інформатики та системології,
Київський національний економічний університет імені Вадима Гетьмана
ORCID: https://orcid.org/0000-0002-4794-2566
E-mail: lpetrenko@kneu.edu.ua
Владислав Ніжегородцев
кандидат педагогічних наук, доцент,
доцент кафедри комп'ютерних та інформаційних технологій і систем,
Державний податковий університет
ORCID: https://orcid.org/0000-0001-9434-0564
E-mail: nizhegorodcev@ukr.net

ПРОГРАМНІ РІШЕННЯ ЩОДО ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ В ЕЛЕКТРОННИХ КОМУНІКАЦІЯХ

Анотація. *У статті досліджується проблема захисту інформації в контексті швидкого розвитку електронних комунікацій і зростаючих вимог до їх безпеки. Зазначено, що інтенсивне впровадження сучасних технологій в інформаційно-комунікаційні системи призводить до збільшення обсягів інформаційного обміну, що активізує потребу у високоефективних методах захисту. Стрімкий розвиток електронних комунікацій призводить до вирішення питань, пов'язаних з дотриманням конфіденційності даних. До ризиків конфіденційності та перехоплення даних найбільш часто відносять проблеми відсутності або слабкого наскрізного шифрування даних. Поєднуючи сучасні методи шифрування, технології регулярних оновлень, двофакторну аутентифікацію, є можливість підвищення рівня захисту та забезпечення конфіденційності цифрових комунікацій. Користуючись обміном голосовими повідомленнями в месенджерах порушується проблема забезпечення безпеки, що потребує застосування надійних методів і алгоритмів для захисту інформації під час передачі голосових і текстових повідомлень. Застосування технологій, зокрема криптографічних генераторів псевдовипадкових чисел, шифрування AES та бази даних Firebase, забезпечує ефективний підхід до створення надійного та непередбачуваного шифрування персональних даних. В роботі наведено порівняльну характеристику та оцінювання сучасних месенджерів з точки зору їх безпеки. Запропоновано застосування шифрування AES, яке забезпечує надійний захист даних і гарантує конфіденційність голосових повідомлень під час їх передавання. Висока надійність та ефективність шифрування AES надає можливість широкого застосування в захисті й забезпеченні конфіденційності даних, зокрема голосових повідомлень, що має особливе значення в сучасному цифровому середовищі.*

Ключові слова: *електронні комунікації, програмне забезпечення, месенджер, голосове повідомлення, шифрування, конфіденційність.*

Liudmyla Petrenko
PhD in Economics, Docent,
Associate Professor at the Department of Informatics and Systemsology,
Kyiv National Economic University named after Vadym Hetman
ORCID: https://orcid.org/0000-0002-4794-2566
E-mail: lpetrenko@kneu.edu.ua
Vladyslav Nizhegorodtsev
Ph.D in pedagogical sciences., Docent,
Associate Professor at the Department of Computer
and Information Technologies and Systems,
State Tax University
ORCID: https://orcid.org/0000-0001-9434-0564
E-mail: nizhegorodcev@ukr.net

SOFTWARE SOLUTIONS FOR ENSURING CONFIDENTIALITY IN ELECTRONIC COMMUNICATIONS

Abstract. *The article examines the issue of information security in the context of rapid development of electronic communications and growing security requirements. It is noted that the intensive introduction of modern technologies into information and communication systems leads to an increase in the volume of information exchange, which activates the need for highly effective protection methods. Electronic communications are developing rapidly, and therefore privacy issues are currently arising. The most common privacy and data interception risks include the absence or weakness of end-to-end data encryption. Thanks to a combination of modern encryption technologies, regular updates, and two-factor authentication, it is possible to significantly increase the level of protection and ensure confidentiality in digital communications. The exchange of voice messages in instant messengers raises the issue of security when using reliable methods and algorithms to ensure a high level of protection for information exchanged in the form of voice and text messages. The use of technologies such as cryptographic pseudorandom number generators, AES*

encryption, and Firebase Database is an effective approach to encrypting reliable and unpredictable personal data. The paper provides a comparative description and evaluation of modern messengers in terms of their security. It proposes the use of AES encryption, which provides a high level of data protection, ensuring the confidentiality of voice messages during transmission. Due to its reliability and efficiency, AES is widely used to ensure data privacy and security, including voice communications, which is critical in today's digital world.

Keywords: *electronic communications, software, messenger, voice messaging, encryption, confidentiality.*

Вступ. Протягом останніх кількох років зберігається інтенсивне зростання кіберзагроз, яке відображається у масовому державному та корпоративному секторах: фейкові новини, фальсифікації з метою надання допомоги від держави, зламані акаунти месенджерів та сторінок соціальних мереж, тощо.

Часті випадки витоків даних підкреслюють нагальну потребу в надійних програмних рішеннях, а архітектура сучасних комунікаційних систем вимагає інтеграції технологій, які не лише забезпечують функціональність, але й закладають основи «приватності за дизайном».

В умовах військового конфлікту проти України формується безпрецедентний рівень вразливості особистих, корпоративних та державних даних. Конфіденційність в електронних комунікаціях виступає як не просто бажаний атрибут, а критична необхідність, що гарантує захист інформації від несанкціонованого доступу, перехоплення чи розкриття.

Літературний огляд. Серед досліджень сталої роботи комунікаційних мереж та захисту інфраструктури в умовах кібернетичних загроз можна виділити роботи Д. Дубова, Є. Кильчицького, А. Коваленко, Г. Колченко, О. Климчука, О. Резнікова, Н. Слободян, О. Суходолі, Р. Шикаса.

Методологія. Метою дослідження є вивчення можливостей використання програмних моделей, що ґрунтуються на надійних методах і алгоритмах, для забезпечення високого рівня конфіденційності та захисту голосових повідомлень під час їх передавання в месенджерах.

У дослідженні проведено аналіз найпопулярніших месенджерів, здійснено їх порівняльну характеристику, розглянуто технології, що використовуються під час їх розроблення, а також застосовано шифрування AES для захисту даних, що забезпечує конфіденційність голосових повідомлень під час їх передавання та зберігання.

Основна частина. Цифрова епоха радикально трансформувала способи комунікації, зробивши обмін інформацією миттєвим та глобальним. Електронні комунікації – від електронної пошти та месенджерів до відеоконференцій стали основою сучасного суспільства та економіки. Основою забезпечення конфіденційності в електронних комунікаціях стають криптографічні методи та архітектурні підходи, які реалізовані програмно.

Найкраще програмне забезпечення для конфіденційності передачі даних стає незахищеним, якщо користувачі не вміють ним користуватися або не розуміють його переваг: людський фактор повстає найбільшою слабкістю в інформаційному секторі.

Впровадження новітніх технологій в управлінні та передачі баз даних мають забезпечуватися програмним забезпеченням, яке повинно бути максимально інтуїтивно зрозумілими та простими у використанні, щоб забезпечення конфіденційності було стандартним, а не додатковим кроком. Потрібні інновації в інтерфейсах, які роблять складні криптографічні процеси невидимими для пересічного користувача.

Слід підкреслити, що Україна має впровадити загальноєвропейські стандарти щодо захисту основоположних прав людини в цифровому просторі та забезпечити створення безпечного цифрового середовища для своїх громадян.

У березні 2021 року була ухвалена Національна стратегія у сфері прав людини, метою якої є утвердження пріоритету прав і свобод людини як ключового чинника у формуванні та реалізації державної політики, діяльності органів державної влади й місцевого самоврядування, а також у веденні господарської діяльності.

Зокрема, положення Національної стратегії вказують на невідповідність українського законодавства у сфері захисту персональних даних європейським стандартам, а також на відсутність ефективного інституційного механізму незалежного контролю за дотриманням права на захист таких даних [1].

Централізовані способи обміну повідомленнями часто виявляються недостатньо масштабованими при зростанні обсягів трафіку чи кількості повідомлень і можуть потребувати повної модернізації інфраструктури для роботи за умов підвищеного навантаження. Це зумовлено складністю передавання даних про стан з'єднання та потребою у встановленні сеансу зв'язку. Таке обмеження не становить суттєвої проблеми для бізнесів, що не розширюються та мають стабільний обсяг трафіку, адже централізовані методи часто забезпечують вищу якість обслуговування завдяки пріоритезації повідомлень і стабільній доступності сервісу [2].

Електронні комунікації розвиваються надзвичайно швидкими темпами, що призводить до появи проблем, пов'язаних із забезпеченням конфіденційності. На ранніх етапах розвитку цифрових комунікацій передавання даних здійснювалося переважно через автовідповідачі та електронну пошту, проте сьогодні основним засобом спілкування стали месенджери – програми для обміну миттєвими повідомленнями на мобільних пристроях і персональних комп'ютерах. Месенджери стали безумовним лідером в спілкуванні між людьми. Попри певні відмінності у своїх характеристиках, усі месенджери залишаються ключовими інструментами сучасної комунікації та нетворкінгу. Їх об'єднують спільні риси: безкоштовне використання, підтримка передачі даних різних форматів (зображень, анімацій, аудіо, відео, документів тощо), створення груп і синхронізація між різними пристроями.

У 2025 році популярність месенджерів не зменшується – навпаки, з'являються нові гравці, а старі сервіси пропонують ще більше можливостей. За останніми даними з відкритих джерел, у 2025 році світовий рейтинг месенджерів виглядає так [3]: WhatsApp – 2,8 млрд користувачів; Facebook Messenger – 1,1 млрд користувачів; WeChat – 1,3 млрд користувачів; Telegram –

900 млн користувачів; Snapchat – 750 млн активних користувачів на місяць.

Український ринок має свою специфіку. Згідно з актуальним дослідженням компанії InMind за перше півріччя 2025 року, ситуація виглядає так:

1. Viber – 45%
2. Telegram – 35%
3. Facebook Messenger – 10%
4. WhatsApp – 7%
5. Signal – 3%

Майже кожна людина використовує як мінімум один, а найчастіше одночасно кілька месенджерів. Необхідність у різних мережах обміну повідомленнями зумовлена тим, що між ними немає прямого зв'язку. Кожен месенджер розроблений окремою командою фахівців, має власні сервери й протоколи, а також характеризується індивідуальними особливостями та правилами користування. Месенджери підлягають класифікації за різними критеріями [4].

За типом використання:

– особисте використання – месенджери, що переважно застосовуються для спілкування з родиною та друзями, зокрема WhatsApp, Telegram, Viber і Facebook Messenger;

– для бізнесу – месенджери, розроблені для професійного спілкування та роботи в команді, такі як Slack, Microsoft Teams і Google Chat;

За рівнем безпеки:

– стандартні месенджери – більшість із них забезпечують захист користувацького спілкування за допомогою шифрування даних, зокрема WhatsApp, Telegram і Viber;

– месенджери з підвищеним рівнем безпеки – окремі сервіси надають додаткові засоби захисту, зокрема наскрізне шифрування та режим спілкування «інкогніто», як-от Signal і секретні чати в Telegram.

За платформою:

– мультиплатформні месенджери – програми, що доступні на кількох операційних системах, зокрема Android, iOS, Windows і macOS, як-от WhatsApp, Telegram та Slack;

– месенджери для окремих платформ – це програми, що функціонують виключно в межах певної операційної системи, наприклад iMessage від Apple, доступний лише на пристроях цієї компанії.

Зростання зручності та швидкості обміну голосовими повідомленнями в месенджерах актуалізує проблему забезпечення безпеки, що вимагає застосування надійних методів і алгоритмів для досягнення високого рівня конфіденційності та захисту інформації під час обміну голосовими й текстовими повідомленнями. Порівняно зі звичними способами спілкування, зокрема телефонними дзвінками та SMS, месенджери довели свою ефективність і зручність як сучасні та практичні засоби комунікації.

Сучасні та доступні технології в сфері розпізнавання голосу значно підвищили можливості й зручність перекладу голосових повідомлень. Поширення штучного інтелекту відкриває нові можливості та загрози. З одного боку, ШІ може посилити конфіденційність за допомогою автоматизованого виявлення аномалій та захисту від атак, а з іншого боку: величезні обсяги даних, можуть становити нову загрозу, якщо не будуть належним чином регулюватися і захищатися.

Безпека використання обміну голосовими повідомленнями (або войсами) має кілька важливих аспектів, які стосуються як технологічної конфіденційності, так і особистої безпеки та вразливості до шахрайства. Найбільші загрози стосуються того, як повідомлення зберігаються, передаються та хто може отримати до них доступ.

До ризиків конфіденційності та перехоплення даних найбільш часто відносять проблеми відсутності або слабкого наскрізного шифрування даних. На відміну від тексту, голосові повідомлення часто містять фонові шуми або інтонації, які можуть ненавмисно розкрити ваше місцезнаходження, оточення або емоційний стан, що може бути використано для соціальної інженерії чи стеження.

Голосова імітація, діпфейки, фейкові сповіщення про «пропущену голосову пошту», посиланням на шкідливий сайт або використання записаного голосу як приманки для подальшого шахрайства найбільш часто використання набувають останнього часу у діях зловмисників.

Офлайн-повідомлення – не зберігаються на центральному сервері, але дають змогу надсилати повідомлення користувачам, які перебувають поза мережею. Повідомлення залишатимуться збереженими локально на вашому пристрої до моменту, коли одержувач підключиться до мережі, після чого вони будуть успішно доставлені.

Це становить значну перевагу централізованих месенджерів, у яких повідомлення, надіслані користувачам, що перебувають офлайн, не зберігаються на центральному сервері, а залишаються локально на пристроях до моменту підключення одержувача або успішної доставки [5].

Інформаційна безпека є одним із ключових чинників під час вибору месенджера для спілкування: порівняння WhatsApp, Viber, Telegram і Facebook Messenger свідчить, що всі вони забезпечують певний рівень захисту, однак відрізняються використовуваними функціями та методами шифрування.

WhatsApp, Viber і Telegram застосовують наскрізне шифрування, яке забезпечує високий рівень конфіденційності повідомлень. Натомість Facebook Messenger використовує лише часткове шифрування, що зумовлює певні обмеження в безпеці.

Втім, усі месенджери спрямовані на захист персональних даних користувачів і запобігання кібератакам. Водночас слід враховувати, що рівень їхньої безпеки може змінюватися з часом. Тому, вибір месенджера слід здійснювати не лише з огляду на його функціональні можливості, а й на рівень кібербезпеки, щоб гарантувати захищеність і конфіденційність усіх комунікацій (табл. 1).

Оцінка показника безпеки на основі технічної документації, наявності наскрізного шифрування, прозорості коду, інцидентів витоків даних наведена на рис. 1:

Налаштування профілю користувача в сучасному месенджері дає змогу змінювати особисті дані – ім'я, статус, фотографію профілю – а також керувати параметрами конфіденційності та сповіщень за допомогою Firebase Realtime Database. Завдяки цим компонентам і технологіям месенджер отримує повну функціональність із пріоритетом на безпеку та комфорт користувачів. Усі дані також синхронізуються між усіма пристро-

Таблиця 1

Порівняльний аналіз месенджерів з позиції забезпечення безпеки

Параметр	WhatsApp	Telegram	Facebook Messenger	Viber
Шифрування під час передачі	End-to-End Encryption (E2EE)	Client-Server Encryption (основне E2EE), E2EE (секретні чати)	Client-Server Encryption (опціонально E2EE)	End-to-End Encryption (E2EE)
Шифрування повідомлень на сервері	Ні	Так, окрім клієнтських секретних чатів	Так, серверно-клієнтське шифрування	Ні
Шифрування резервних копій	Опціонально E2EE	Ні	Ні	Ні
Аутентифікація користувачів	SMS/Call	SMS/Call, Bot Authentication	Facebook Account	SMS/Call
Самознищувані повідомлення	Так	Так	Ні	Так
Верифікація контактів	Так (код безпеки)	Так (шифрувальний ключ)	Ні	Так (код безпеки)
Захист від зломів	Двофакторна аутентифікація (2FA)	Двофакторна аутентифікація (2FA)	Двофакторна аутентифікація (2FA)	Двофакторна аутентифікація (2FA)
Збір метаданих	Так	Мінімальний збір даних	Так	Мінімальний збір даних
Доступ до контактів	Так	Опціонально (можна відключити)	Так	Так
Сховище на сервері	Зберігання зашифрованих медіа	Зберігання повідомлень (не секретних чатів)	Зберігання зашифрованих медіа	Зберігання зашифрованих медіа
Політика конфіденційності	Приналежність до Facebook, обмін даними	Прозора політика, власні сервери	Приналежність до Facebook, обмін даними	Приналежність до Rakuten, прозора політика

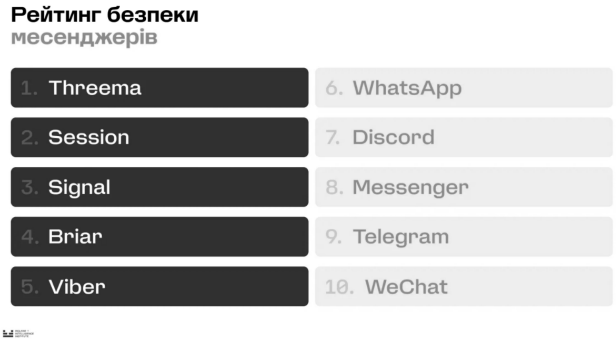

Рис. 1. Оцінка рівня захисту популярних месенджерів

Джерело: [6]

ями. База даних реального часу забезпечує миттєву синхронізацію даних між користувачами та сервером, що робить її особливо ефективною для месенджерів, де критично важлива оперативність оновлень.

Клієнтська частина месенджера є ключовим елементом взаємодії користувача з додатком, забезпечуючи зручний інтерфейс для перегляду повідомлень, управління контактами та виконання інших функцій.

Клієнтська частина сучасних месенджерів зазвичай розробляється мовою Kotlin для Android і Swift для iOS або іншими мовами програмування, взаємодіючи із серверною частиною для обміну даними, забезпечуючи синхронізацію між користувачами. Застосування HTTP-запитів і WebSocket-з'єднань для встановлення зв'язку з сервером забезпечує двосторонню взаємодію в реальному часі, що має вирішальне значення для оперативної доставки повідомлень.

Безпека та автентифікація в месенджерах мають ключове значення для захисту персональних даних користувачів, адже передбачають перевірку їхньої особи, встановлення захищеного каналу зв'язку між клієнтом і сервером, а також реалізацію заходів, спрямованих на запобігання несанкціонованому доступу до інформації.

Месенджери застосовують власні протоколи передачі даних, причому шифрування повідомлень зазвичай здійснюється на прикладному рівні, після чого зашифрована інформація інтегрується. Як транспортний протокол зазвичай (хоча й не обов'язково) застосовують SSL/TLS, який фактично став стандартом для захищених web-комунікацій. Водночас його реалізація на мобільних платформах нерідко залишається недосконалою.

Голосові повідомлення в розглянутих месенджерах підтримують функції запису, надсилання, відтворення, зберігання та шифрування, що дає змогу забезпечити конфіденційність даних користувачів. Голосові повідомлення мають значне значення для конфіденційного обміну інформацією, оскільки забезпечують зручний і ефективний формат спілкування. Вони дають змогу користувачам передавати повідомлення швидко й емоційно, зберігаючи індивідуальний тон і відтінки голосу.

Однією з основних характеристик голосових повідомлень є їхня конфіденційність. У них може міститися особиста, конфіденційна чи важлива інформація, яку користувачі не прагнуть розкривати широкому колу осіб. Конфіденційність голосових повідомлень гарантується завдяки захищеному обміну між відправником і отримувачем, а також застосуванню шифрування та додаткових заходів безпеки.

Крім того, голосові повідомлення можуть використовуватися для підтвердження особи або автентифікації користувачів у системах безпеки, адже голос виступає унікальним біометричним ідентифікатором,

що робить його дієвим інструментом перевірки особистості.

Застосування криптографічних методів шифрування – зокрема генераторів псевдовипадкових чисел і алгоритму AES – у поєднанні з надійними сервісами зберігання даних, такими як Firebase Database, забезпечує високий рівень конфіденційності голосових повідомлень.

Симетричний алгоритм шифрування AES (Advanced Encryption Standard) передбачає використання одного й того самого ключа для шифрування та розшифрування даних, тобто відправник і отримувач мають володіти спільним секретним ключем.

Безпека голосових повідомлень гарантується завдяки структурі AES та використанню складних математичних операцій. Цей алгоритм вважається надзвичайно надійним, оскільки наразі не існує практичних способів його зламу за умови застосування довгих ключів. Алгоритм AES має широке застосування в різноманітних програмах і системах – від захисту конфіденційних даних у державних установах, фінансових організаціях та на підприємствах до використання в побутових пристроях.

Завдяки високій надійності та ефективності AES широко застосовується для гарантування конфіденційності й захисту даних, зокрема голосових повідомлень, що має особливе значення в сучасному цифровому середовищі.

Попри високий рівень захисту, відомі випадки зламів голосових повідомлень у месенджерах свідчать про необхідність постійного вдосконалення систем безпеки та кіберзахисту. Поєднання сучасних технологій шифрування, регулярних оновлень, двофакторної автентифікації та підвищення обізнаності користувачів дає змогу суттєво зміцнити захист і гарантувати конфіденційність цифрових комунікацій. Захист конфіденційності голосових повідомлень і надалі є одним із ключових завдань у сучасному цифровому просторі. Застосування технологій, зокрема криптографічних генераторів псевдовипадкових чисел, шифрування AES і бази даних Firebase, забезпечує ефективний підхід до створення надійного та непередбачуваного шифрування персональних даних.

Реалізація шифрування голосових повідомлень у середовищі Swift для iOS із застосуванням генератора псевдовипадкових чисел для створення ключів AES передбачає розшифрування голосових даних, завантажених із Firebase, із використанням згенерованого AES-ключа (рис. 2).

Шифрування даних відіграє вирішальну роль у забезпеченні безпеки інформації, особливо в галузі комунікацій. Інтеграція алгоритму AES дає змогу ефективно захищати дані від несанкціонованого доступу, підвищуючи надійність обміну повідомленнями. Використання платформи Firebase для зберігання даних забезпечує зручне та безпечне керування зашифрованими повідомленнями, створюючи додатковий рівень захисту.

Процес створення ключа AES включає шифрування голосового повідомлення, збереження зашифрованих даних у Firebase Storage, подальше завантаження цих даних із хмарного сховища та їх розшифрування. Застосування шифрування AES забезпечує надійний захист інформації, гарантує конфіденційність голосових повідомлень під час їх передачі та зберігання.

```swift
import Firebase
import FirebaseStorage
import CryptoSwift

// Генерація ключа AES
let aesKey = generateAESKey()

// Шифрування голосового повідомлення
let voiceMessageData = ... // Ваше голосове повідомлення у вигляді Data
do {
    let encryptedMessage = try encryptVoiceMessage(key: aesKey, voiceMessage:  voiceMessageData)

    // Завантаження зашифрованого повідомлення у Firebase Storage
    uploadEncryptedVoiceMessage(encryptedMessage: encryptedMessage) { url in
        guard let downloadURL = url else {
            print("Failed to upload encrypted message")
            return
        }

        print("Encrypted message uploaded to: \(downloadURL)")

        // Завантаження зашифрованого повідомлення з Firebase Storage
        downloadEncryptedVoiceMessage(from: downloadURL) { data in
            guard let encryptedData = data else {
                print("Failed to download encrypted message")
                return
            }

            // Дешифрування голосового повідомлення
            do {
                let decryptedMessage = try decryptVoiceMessage(key: aesKey, encryptedMessage: encryptedData)
                print("Decrypted message: \(decryptedMessage)")
            } catch {
                print("Failed to decrypt message: \(error.localizedDescription)")
            }
        }
    }
} catch {
    print("Failed to encrypt message: \(error.localizedDescription)")
}
```

Рис. 2. Програмна реалізація шифрування голосових повідомлень для IOS на Swift

Сучасний захист даних від несанкціонованого доступу вимагає комплексних програмних рішень, які охоплюють як базові, так і просунуті технології. Найефективнішим є наскрізне шифрування, яке гарантує, що лише кінцеві користувачі можуть прочитати повідомлення. Програмні інструменти, такі як VPN та Tor, використовуються для анонімізації та приховування метаданих, захищаючи місцезнаходження та активність користувачів. Для бізнесу ключовими можуть стати системи DLP (Data Loss Prevention), що запобігають витокам, та платформи управління конфіденційністю (OneTrust), які автоматизують дотримання регуляторних вимог.

Голосові повідомлення легко пересилаються, що робить контроль над конфіденційною інформацією практично неможливим. Крім того, фонові шуми можуть ненавмисно розкрити місцезнаходження або оточення відправника.

Безпека електронних комунікацій вимагає багатошарового підходу, який повинен мати лише технічні рішення, а й вимагає цифрової грамотності користувачів.

Висновки. Месенджери – це не просто чат, а інструмент комунікації, бізнесу, новин, сервісу. Українські користувачі продовжують обирати знайомі бренди, але водночас активно досліджують нові можливості, цінуючи зручність, безпеку та багатофункціональність. Програмні рішення щодо забезпечення конфіденційності в електронних комунікаціях еволюціонують від простих інструментів шифрування до складних, багатошарових екосистем. Архітектурні концепції відіграють важливу роль у розподілі функцій та взаємодії між компонентами, забезпечуючи ефективну організацію клієнтської частини месенджера на основі сучасних архітектурних підходів.

Конфіденційність передачі інформації вимагає невпинної адаптації у сучасних системах програмного забезпечення з метою не лише забезпечувати зв'язок, але й гарантувати, що цей зв'язок залишається приватним, надійним і підконтрольним самим користувачам. Необхідним є системний підхід до захисту конфіденційності даних, що повинен включати правове регулювання, впровадження сучасних технологій для захисту інформації, підвищення рівня медіаграмотності серед населення.

Список використаних джерел:

1. Національна стратегія у сфері прав людини : Указ Президента України від 24 березня 2021 року. № 119/2021. URL: https://zakon.rada.gov.ua/laws/show/119/2021#Text (дата звернення: 26.09.2025).
2. Gerar Maral, Michel Bousquet, Zhili Sun. Satellite communications systems Systems, techniques and technology. Sixth edition. John Wiley & Sons Ltd. 2020. P. 437. URL: https://books.google.com/bookshl=en&lr=&id=kdjIDwAAQBAJ&oi=fnd&pg=PR15&dq=Most+communications+satellites+used+today+operate+as+centralised+messengers.&ots=FPARYMgolC&sig=PSk2-l5mz_O8LigWM6NEDuBDdPM (дата звернення: 26.09.2025).
3. Популярні месенджери для спілкування – топ в Україні URL: https://sitecat.net/review/top-10-popular-messengers/ (дата звернення: 26.09.2025).
4. Рейтинг месенджерів 2025 року: оцінюємо безпеку, конфіденційність та функціонал URL: https://www.molfarinstitute/rejtyng-mesendzheriv-2025-roku-oczinyuyemo-bezpeku-konfidenczijnist-funkczional/ (дата звернення: 27.09.2025).
5. K. Jefferys, M. Shishmarev, S. Harman. Session: End-To-End Encrypted Conversations With Minimal Metadata Leakage – arXiv preprint arXiv. 2024 – arxiv.org. URL: https://arxiv.org/pdf/2002.04609 (дата звернення: 27.09.2025).
6. ТОП-10 месенджерів для повідомлень та дзвінків у 2023 р. Владислава Рикова. 7 Листопада 2023 р. URL: https://vlada-rykova.com/ua/top-messendzherov/#i (дата звернення: 27.09.2025).

References:

1. Natsionalna stratehiia u sferi prav liudyny : Ukaz Prezydenta Ukrainy vid 24 bereznia 2021 roku. № 119/2021 [National Strategy on Human Rights: Decree of the President of Ukraine dated March 24, 2021. No. 119/2021]. Available at: https://zakon.rada.gov.ua/laws/show/119/2021#Text.pdf (accessed 26.09.2025). (in Ukrainian)
2. Gerar Maral, Michel Bousquet, Zhili Sun. Satellite communications systems Systems, techniques and technology. Sixth edition. John Wiley & Sons Ltd. (2020). P. 437. Available at: https://books.google.com/bookshl=en&lr=&id=kdjIDwAAQBAJ&oi=fnd&pg=PR15&dq=Most+communications+satellites+used+today+operate+as+centralised+messengers.&ots=FPARYMgolC&sig=PSk2-l5mz_O8LigWM6NEDuBDdPM (accessed 26.09.2025).
3. Populiarni mesendzhery dlia spilkuvannia – top v Ukraini [Popular messengers for communication – top in Ukraine] Available at: https://sitecat.net/review/top-10-popular-messengers/ (accessed 26.09.2025). (in Ukrainian)
4. Reitynh mesendzheriv 2025 roku: otsiniuiemo bezpeku, konfidentsiinist ta funktsional [2025 messenger rating: evaluating security, privacy, and functionality] Available at: https://www.molfarinstitute/rejtyng-mesendzheriv-2025-roku-oczinyuyemo-bezpeku-konfidenczijnist-funkczional/ (accessed 27.09.2025). (in Ukrainian)
5. K. Jefferys, M. Shishmarev, S. Harman. Session: End-To-End Encrypted Conversations With Minimal Metadata Leakage – arXiv preprint arXiv. (2024). Available at: https://arxiv.org/pdf/2002.04609 (accessed 27.09.2025).
6. TOP-10 mesendzheriv dlia povidomlen ta dzvinkiv u 2023 r. Vladyslava Rykova. 7 Lystopada 2023r. [Top 10 messengers for messaging and calls in 2023. Vladislav Rykov. November 7, 2023.] Available at: https://vlada-rykova.com/ua/top-messendzherov/#i (accessed 27.09.2025). (in Ukrainian)

Стаття надійшла: 08.10.2025
Стаття прийнята: 28.10.2025
Стаття опублікована: 27.11.2025