УДК 004.056.5

**М. В. Березюк**

# ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ МЕСЕНДЖЕРІВ З ВИКОРИСТАННЯМ НАСКРІЗНОГО ШИФРУВАННЯ, ГОЛОСОВОЇ БІОМЕТРІЇ ТА АУДІОСТЕГАНОГРАФІЇ

Вінницький національний технічний університет

**Анотація**

*У роботі запропоновано підхід до підвищення захищеності месенджерів шляхом поєднання наскрізного шифрування, голосової біометричної автентифікації та аудіостеганографії. Такий підхід дозволяє захистити зміст повідомлень, посилити контроль доступу користувачів і приховати факт передавання конфіденційної інформації у голосових повідомленнях.*

**Ключові слова:** месенджер, наскрізне шифрування, голосова біометрія, аудіостеганографія, захист інформації.

**Abstract**

*The paper proposes an approach to improving the security of messengers by combining end-to-end encryption, voice biometric authentication, and audio steganography. This approach protects message content, strengthens user access control, and hides the fact of transmitting confidential information in voice messages.*

**Keywords:** messenger, end-to-end encryption, voice biometrics, audio steganography, information security.

## Вступ

Месенджери є одним із найпоширеніших засобів щоденного обміну інформацією. Через них передаються текстові повідомлення, файли, зображення, голосові повідомлення та інші дані, які можуть мати конфіденційний характер. У зв’язку з цим важливим завданням є підвищення рівня захищеності таких систем від перехоплення повідомлень, несанкціонованого доступу до облікового запису та витоку приватної інформації [1].

Застосування лише одного механізму захисту не завжди забезпечує достатній рівень безпеки. Тому доцільним є використання комплексного підходу, який поєднує криптографічний захист повідомлень, біометричну перевірку користувача та приховану передачу окремих даних у аудіосигналі. Такий підхід дозволяє розглядати захист месенджера не як окрему функцію, а як сукупність взаємопов’язаних механізмів, що доповнюють один одного.

## Результати дослідження

Запропонований підхід передбачає використання наскрізного шифрування, за якого повідомлення шифруються на пристрої відправника та розшифровуються лише на пристрої отримувача. У такій моделі сервер виконує переважно функцію передавання зашифрованих даних і не має доступу до відкритого змісту повідомлень. Це дозволяє знизити ризик розкриття інформації навіть у разі компрометації серверної частини або перехоплення мережевого трафіку [2].

Для реалізації захищеного обміну повідомленнями доцільно застосовувати гібридний підхід до шифрування. Він передбачає використання асиметричних алгоритмів для безпечного обміну ключами та симетричних алгоритмів для швидкого шифрування основного вмісту повідомлень [3]. Такий спосіб дозволяє поєднати високий рівень криптографічної стійкості з достатньою швидкодією, що є важливим для роботи месенджера в режимі реального часу.

Для посилення контролю доступу до месенджера пропонується використовувати голосову біометрію. Під час реєстрації формується еталонний голосовий профіль користувача, а під час входу до системи поточний голосовий зразок порівнюється з ним. У разі достатнього збігу користувач отримує доступ до облікового запису, а в разі невідповідності доступ блокується. Це ускладнює використання месенджера сторонніми особами навіть за умови отримання ними пароля [4].

Використання голосової біометрії є доцільним саме для месенджерів, оскільки робота з голосовими повідомленнями вже є природною функцією таких систем. Тому додавання голосової

автентифікації не потребує суттєвої зміни способу взаємодії користувача з додатком. Водночас такий механізм створює додатковий рівень захисту, оскільки голосові характеристики користувача складніше підробити, ніж звичайний пароль або PIN-код.

Додатковим елементом захисту є аудіостеганографія, яка дозволяє приховувати службову або конфіденційну інформацію у голосових повідомленнях. На відміну від шифрування, яке приховує зміст повідомлення, стеганографія приховує сам факт наявності додаткових даних. Для цього може використовуватися метод фазового кодування, що забезпечує незначний вплив на якість звуку та робить приховану інформацію менш помітною для стороннього аналізу [5-6].

Застосування аудіостеганографії у месенджері може бути корисним для прихованої передачі додаткових службових даних, ідентифікаторів, ключової інформації або коротких конфіденційних повідомлень. При цьому голосове повідомлення зберігає звичайний вигляд для користувача та не викликає підозри під час передавання [6]. Це підвищує рівень прихованості інформаційного обміну та доповнює криптографічний захист.

Поєднання цих механізмів формує багаторівневий захист месенджера. Наскрізне шифрування забезпечує конфіденційність повідомлень, голосова біометрія підвищує надійність автентифікації, а аудіостеганографія створює додатковий рівень прихованості під час передавання даних. У результаті запропонований підхід дозволяє підвищити стійкість месенджера до перехоплення трафіку, несанкціонованого доступу та аналізу переданих повідомлень.

## Висновок

У роботі запропоновано підхід до підвищення захищеності месенджерів, що базується на комплексному використанні наскрізного шифрування, голосової біометрії та аудіостеганографії. Такий підхід дозволяє зменшити ризики перехоплення повідомлень, несанкціонованого доступу до облікового запису та виявлення прихованої інформації у голосових повідомленнях.

Практичне значення запропонованого підходу полягає у можливості його застосування під час створення захищених систем обміну повідомленнями. Подальше удосконалення може бути пов’язане з оптимізацією криптографічних операцій, підвищенням точності голосової автентифікації та дослідженням стійкості аудіостеганографічних методів до обробки звуку.

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ


1. SoK: Secure Messaging. *IEEE Xplore*. URL: https://ieeexplore.ieee.org/document/7163029.
2. A Formal Security Analysis of the Signal Messaging Protocol. *IEEE Xplore*. URL: https://ieeexplore.ieee.org/document/7961996.
3. What is End-to-End Encryption (E2EE) and How Does it Work?. *Splashtop Inc.* URL: https://www.splashtop.com/blog/what-is-end-to-end-encryption.
4. Kinnunen T., Li H. An overview of text-independent speaker recognition: From features to supervectors. *Speech Communication*. 2010. Т. 52, № 1. С. 12–40. URL: https://doi.org/10.1016/j.specom.2009.08.009.
5. Techniques for data hiding / W. Bender et al. *IBM Systems Journal*. 1996. Vol. 35, no. 3.4. P. 313–336. URL: https://doi.org/10.1147/sj.353.0313.
6. Comparative study of digital audio steganography techniques / F. Djebbar et al. *EURASIP Journal on Audio, Speech, and Music Processing*. 2012. Vol. 2012, no. 1. URL: https://doi.org/10.1186/1687-4722-2012-25.



***Березюк Максим Віталійович*** – студент групи 2КІТС-22б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: berezukmaksim045@gmail.com

**Науковий керівник: Карпінець Василь Васильович** – кандидат технічних наук, доцент, завідувач кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: karpinets@vntu.edu.ua

***Bereziuk Maksym Vitaliiovych*** – student of group 2KITS-22B, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: berezukmaksim045@gmail.com.

***Supervisor: Karpinets Vasyl Vasylovych*** – Candidate of Technical Sciences, Associate Professor, Head of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: karpinets@vntu.edu.ua.