

## ШИФРУВАННЯ ІНФОРМАЦІЇ В ПОПУЛЯРНИХ ІНТЕРНЕТ МЕСЕНДЖЕРАХ

*канд. економ. наук, доц. С.В. Мілевський, д-р техн. наук, проф.  
С.П. Євсєєв, канд. економ. наук, доц. С.С. Погасій, Національний  
технічний університет "Харківський політехнічний інститут",  
м. Харків*

В умовах стрімкого зростання використання новітніх технологій в сфері комунікації, переважна більшість населення світу активно використовує в повсякденному житті та професійній діяльності для передачі інформації велику кількість різноманітних месенджерів. Це суттєво підвищує актуальність захисту інформації в таких засобах обміну та передачі, особливо в умовах виникнення гібридних загроз останнім часом. Основним елементом захисту, звичайно, є шифрування.

Найбільш популярні месенджери використовують такі протоколи: Telegram [1] – MTProto (комбінація AES в режимі IGE та протокола Діффі-Хелмана); Viber [2] – наскрізне End-to-end шифрування. Кожен з клієнтів використовує пару ключів: публічний та приватний. Алгоритм шифрування 256-bit Curve-25519; WhatsApp [3] – наскрізне шифрування з використанням libaxolotl (Signal Protocol) Double Ratchet algorithm; Signal [4] – протокол Signal (поєднує в собі Double Ratchet Algorithm, prekeys та розширений протокол потрібного обміну ключами Діффі-Хелмана (3-DH) та використовує Curve25519, AES-256 та HMAC-SHA256 в якості примітивів).

Таким чином, наявні протоколи не можуть забезпечити достатньо високий рівень безпеки, особливо якщо зловмисники мають потужні технічні можливості. Ця проблема постане ще гостріше найближчим часом із використанням квантових комп'ютерів. Тому в сучасних умовах відповідний ступінь захищеності можливо забезпечити із застосуванням постквантових крипто-кодових конструкцій Мак-Еліса та Нідеррайтера на алгеброгеометричних кодах.

**Список літератури:** 1. Технічні питання Telegram <https://tigrm.ru/techfaq>. 2. Viber encryption overview. <https://www.viber.com/app/uploads/viber-encryption-overview.pdf>. 3. Безпека та конфіденційність WhatsApp. <https://faq.whatsapp.com/general/security-and-privacy/end-to-end-encryption> 4. Ermoshina K. End-to-End Encrypted Messaging Protocols: An Overview / K. Ermoshina, F. Musiani, H. Halpin // Internet Science. INSCI 2016. Lecture Notes in Computer Science, vol 9934. Springer, Cham. [https://doi.org/10.1007/978-3-319-45982-0\\_22](https://doi.org/10.1007/978-3-319-45982-0_22).