УДК 004.056
В. Пилипчук; **Н. Загородна, к. т. н., доц.**
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ІНТЕГРАЦІЯ ЦИФРОВОГО ПІДПИСУ У СИСТЕМАХ З НАСКРІЗНИМ ШИФРУВАННЯМ ПОВІДОМЛЕНЬ

UDC 004.056
V. Pylypchuk; N. Zagorodna, PhD., Assoc. Prof.

INTEGRATION OF DIGITAL SIGNATURE IN END-TO-END ENCRYPTED MESSAGING SYSTEMS

У сучасних системах захищеного обміну інформацією наскрізне шифрування є базовим механізмом забезпечення конфіденційності, оскільки лише відправник і отримувач володіють ключами для дешифрування повідомлень. Проте сам факт шифрування не усуває ризиків, пов'язаних із підміною відправника, компрометацією ключів або непомітним втручанням у процедури встановлення сеансу зв'язку. У таких сценаріях існує можливість перехоплення та модифікації даних без розкриття їх вмісту, що створює потребу в окремому механізмі підтвердження авторства й незмінності повідомлення.

Гарантування автентичності та цілісності забезпечується цифровим підписом. Його використання дозволяє підтвердити походження повідомлення, засвідчити відсутність змін під час передачі та знизити ймовірність атак «man-in-the-middle», фальсифікації змісту, повторного відправлення старих даних та прихованого втручання у процес початкового обміну ключами. Таким чином, цифровий підпис стає доповненням до шифрування, яке підвищує рівень гарантій безпеки понад ті, що надає сама криптографія шифрування.

Додавання цифрового підпису розширює функціональність E2EE-систем без зміни фундаментальної архітектури взаємодії, зберігаючи властивість незалежності від сервера та відсутності потреби в централізованих компонентах довіри. З урахуванням ротації ключів у сучасних протоколах обміну сформовано підхід, що поєднує цифровий підпис із механізмом довіри при першому використанні (TOFU), підтримкою історії змін ключів для контролю підміни та збереженням сумісності з forward secrecy. Така інтеграція дозволяє виявляти потенційні аномалії без розкриття ключової інформації та без порушення децентралізованої моделі взаємодії.

Реалізація цифрового підпису в системах із наскрізним шифруванням здатна підвищити рівень довіри між учасниками комунікації, посилити захист від сценаріїв підміни та покращити точність виявлення недостовірних повідомлень у зашифрованих каналах. Такий підхід робить цифровий підпис доцільним компонентом сучасних E2EE-рішень як у корпоративному, так і персональному обміні даними, де критичними є конфіденційність, автономність клієнта та доказовість джерела інформації.

Література

1. Menezes A., Van Oorschot P., Vanstone S. Handbook of Applied Cryptography. CRC Press, 2021.
2. Perrin T. The Signal Protocol: Technical Overview. Signal Foundation, 2022.
3. Bernstein D., Schwabe P. Ed25519: High-speed high-security signatures. Springer, 2017.