УДК 004.056

М. Ю. Маричев
Г. В. Крайнічук (Шелепало)

АНАЛІЗ СУЧАСНИХ КРИПТОГРАФІЧНИХ СХЕМ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ

Вінницький національний технічний університет

Анотація. *У роботі досліджено сучасні криптографічні схеми електронного цифрового підпису. Розглянуто принципи функціонування класичних і вдосконалених схем підпису, зокрема порогових, кільцевих, групових та делегованих підписів. Проаналізовано їх переваги, недоліки та перспективи використання у сфері кібербезпеки та електронного документообігу*.

Ключові слова: електронний цифровий підпис, пороговий підпис, кільцевий підпис, груповий підпис, делегований підпис, кібербезпека.

Abstract. *The paper examines modern cryptographic schemes of electronic digital signatures. Threshold, ring, group and delegated signatures are analyzed together with their security properties and application prospects in cybersecurity systems*.

Keywords: electronic digital signature, threshold signature, ring signature, group signature, delegated signature, cybersecurity.

Вступ

Стрімкий розвиток цифрових технологій, електронного урядування та дистанційної взаємодії користувачів вимагає надійних механізмів підтвердження справжності електронних документів. Одним із ключових інструментів забезпечення довіри в інформаційних системах є електронний цифровий підпис. Його використання дозволяє підтвердити особу підписувача, гарантувати цілісність даних та запобігти відмові від факту підписання документа.

В умовах постійного зростання кількості кіберзагроз традиційні схеми електронного підпису вже не завжди здатні задовольнити сучасні вимоги щодо анонімності, масштабованості та колективного управління ключами. Саме тому активно розвиваються нові криптографічні механізми, орієнтовані на підвищення рівня безпеки та розширення функціональних можливостей цифрових підписів.

Результати дослідження

Використання Електронний цифровий підпису(ЕЦП) дозволяє підтвердити особу автора документа, забезпечити цілісність переданих даних та запобігти несанкціонованим змінам інформації. Найбільш поширеними класичними алгоритмами цифрового підпису - RSA, DSA та ECDSA.

Одним із перспективних напрямів розвитку є порогові підписи. Їх особливість полягає в тому, що секретний ключ не зберігається в одного користувача, а розподіляється між кількома учасниками. Для створення підпису необхідна участь певної кількості сторін, визначеної заздалегідь. Такий підхід значно підвищує рівень безпеки, оскільки компрометація одного учасника не призводить до втрати всього ключа. Порогові підписи активно використовуються в корпоративних системах, хмарних сервісах та блокчейн-платформах. Одним із сучасних прикладів є схема FROST, яка поєднує високу швидкодію та надійність.

Важливе місце серед сучасних криптографічних механізмів займають кільцеві підписи. Вони забезпечують анонімність користувача під час підписання повідомлення. Перевірка такого підпису підтверджує, що документ був підписаний одним із членів певної групи, проте визначити конкретного автора немож-

ливо. Завдяки цій властивості кільцеві підписи застосовуються в системах, де особливого значення набуває захист конфіденційності користувачів, зокрема в деяких криптовалютах та анонімних мережах обміну даними.

Групові підписи поєднують переваги анонімності та контролю. Для зовнішніх користувачів особа підписувача залишається прихованою, однак спеціальний адміністратор групи має можливість встановити автора підпису в разі необхідності. Такий механізм корисний для корпоративних мереж, електронних систем голосування та державних інформаційних ресурсів, де важливо зберігати баланс між конфіденційністю та відповідальністю користувачів.

Окрему категорію становлять делеговані підписи, що дозволяють власнику ключа тимчасово передавати право підписання документів іншій особі без розкриття секретної інформації.

Очікується, що розвиток квантових комп'ютерів може знизити рівень безпеки традиційних алгоритмів асиметричної криптографії у майбутньому. У зв'язку з цим науковці активно працюють над новими методами підпису, які залишатимуться стійкими навіть за наявності потужних квантових обчислювальних систем.

Висновки

Проведений аналіз показав, що сучасні криптографічні схеми електронного цифрового підпису значно розширюють можливості класичних алгоритмів. Порогові підписи забезпечують колективний контроль над ключами, кільцеві та групові підписи підвищують рівень конфіденційності, а делеговані підписи спрощують управління повноваженнями. Подальший розвиток технологій цифрового підпису пов’язаний із впровадженням постквантових алгоритмів та підвищенням рівня кібербезпеки інформаційних систем.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 01.12.2022 № 2801-IX. URL: https://zakon.rada.gov.ua/laws/show/2155-19 (дата звернення: 05.06.2026).
2. Про електронний цифровий підпис : Закон України від 22.05.2003 № 852-IV. URL: https://zakon.rada.gov.ua/laws/show/852-15 (дата звернення: 05.06.2026).
3. Struck P., Weishäupl M. *A Framework for Advanced Signature Notions*. 2025. URL: https://eprint.iacr.org/2025/960 (дата звернення: 05.06.2026).
4. *Digital Signature Standard (DSS)*. FIPS PUB 186-5. Gaithersburg : National Institute of Standards and Technology, 2023. URL: https://doi.org/10.6028/NIST.FIPS.186-5 (дата звернення: 05.06.2026).
5. Rivest R. L., Shamir A., Adleman L. *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems* // Communications of the ACM. 1978. Vol. 21, № 2. P. 120-126. URL: https://doi.org/10.1145/359340.359342 (дата звернення: 05.06.2026).
6. Komlo C., Goldberg I. *FROST: Flexible Round-Optimized Schnorr Threshold Signatures*. 2020. URL: https://eprint.iacr.org/2020/852 (дата звернення: 05.06.2026).
7. Shamir A. *How to Share a Secret* // Communications of the ACM. 1979. Vol. 22, № 11. P. 612-613. URL: https://doi.org/10.1145/359168.359176 (дата звернення: 05.06.2026).
8. Bender A., Katz J., Morselli R. *Ring Signatures*. 2006. URL: https://ia.cr/2005/304 (дата звернення: 05.06.2026).
9. Manulis M. *Group Signatures: Authentication with Privacy*. Bonn : Federal Office for Information Security (BSI), 2012. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/GruPA/GruPA.html (дата звернення: 05.06.2026).
10. Backes M., Meiser S., Schröder D. *Delegatable Functional Signatures*. 2013. URL: https://eprint.iacr.org/2013/408 (дата звернення: 05.06.2026).

Маричев Микита Юрійович — студент групи 2БС-24Б, кафедра захисту інформації, Вінницький національний технічний університет marychevmukuta@gmail.com

Крайнічук (Шелепало) Галина Василівна — доцент кафедри захисту інформації, кандидат фізико-математичних наук, Вінницький національний технічний університет. hv.shelepalo@vntu.edu.ua

Marchyev Mykyta Yuriiovych — student of group 2BS-24B, Vinnytsia National Technical University. marychevmukuta@gmail.com

Krainchuk (Shelepalo) Halyna Vasylivna — Associate Professor, Vinnytsia National Technical University. hv.shelepalo@vntu.edu.ua