МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ
ІНЖЕНЕРНА АКАДЕМІЯ УКРАЇНИ
КИЇВОБЛСТАНДАРТМЕТРОЛОГІЯ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ
ЖИТОМИРСЬКА ПОЛІТЕХНІКА
WROCLAW UNIVERCITY OF SCIENCE AND TECHNOLOGY

ІНТЕГРОВАНІ ІНТЕЛЕКТУАЛЬНІ РОБОТОТЕХНІЧНІ КОМПЛЕКСИ (ІІРТК-2026)

ДЕВ'ЯТНАДЦЯТА МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

19-20 травня 2026 р.
Київ, Україна

ЗБІРКА ТЕЗ

Київ
2026

УДК 004

Відповідальний редактор: Шелуха О.О., к.т.н., доц. каф. комп’ютерної інтеженії та кібербезпеки, Державний університет «Житомирська Політехніка», м. Житомир.

Рекомендовано до друку вченою радою Аерокосмічного факультету Державного університету «Київський авіаційний інститут» (протокол № 4 від 18 травня 2026 р.).

Інтегровані інтелектуальні робототехнічні комплекси (ІІРТК-2026). Дев’ятнадцята міжнародна науково-практична конференція 19-20 травня 2026 р., Київ, Україна. К.: КАІ, 2026. 566 с. (збірка тез).

Містить результати наукових, експериментальних та теоретичних досліджень вчених, аспірантів та студентів.

Матеріали можуть бути корисними науковим співробітникам, інженерно-технічним працівникам, аспірантам та студентам, що спеціалізуються в галузі автоматизованих систем управління робототехнічних комплексів, інформаційних технологій та метрології.

УДК 004.056

Гібридний підхід до довгострокової перевірки електронних підписів

Охріменко А.О., к.т.н.
Маріупольський державний університет
a.okhrimenko@mu.edu.ua
Стокіпний О.Л., к.т.н.
Державний університет «Київський авіаційний інститут»
oleksandr.stokipnyi@kai.edu.ua

При переході на електронні документи виникає необхідність забезпечити їх автентичність та цілісність протягом багатьох років. Завдяки криптографічним методам гарантується автентичність підписанта (електронний підпис) та цілісність документа (гешування), проте довіра до електронного документу має зберігатись протягом усього необхідного часу його зберігання. Для забезпечення цього процесу необхідно застосовувати технологічні та організаційні методи. Довгострокова перевірка (Long-Term Validation, LTV) це набір методів та підходів, що направлені на забезпечення можливості перевірки електронних підписів через тривалий час після їх створення. Вона регулюється низкою міжнародних (ISO 14721, ISO 16363, IETF RFC 4998 та RFC 6283) та європейських стандартів (ETSI EN 319 102, ETSI EN 319 421, ETSI EN 319 422). Для забезпечення LTV повинні використовуватися спеціальні формати підписів Advanced Electronic Signature (CAdES, XAdES, PAdES), які визначають як зберігати підпис та пов'язані дані всередині файлу або окремо, позначки часу, метадані з додатковою інформацією про документ (коли, ким був підписаний, доданий до архіву, які операції проводились з ним), що підтверджують, що з моменту додавання до архіву вміст документу не модифікувався. Для більш тривалого зберігання необхідно використовувати спеціалізовані сервіси або набір процедур, які періодично оновлюються докази автентичності електронних документів з метою продовження довіри до них. До основних методів відносять повторний підпис, повторне створення позначки часу, засвідчення печаткою. Перспективним є використання блокчейну (забезпечує незмінність записів та можливість перевірки факту існування документа у певний момент часу за допомогою механізмів гешування та зчеплення блоків). Враховуючи зазначені методи пропонується гібридний підхід, що враховує рекомендації міжнародних і галузевих стандартів, перспективні напрямки і кращі практики:

1. Перед занесенням електронного документу до архіву має виконуватись перевірка електронного підпису. За необхідності, система має розширювати його до рівня LT чи LTA, придатного для довгострокового зберігання, шляхом збагачення додатковою інформацією, такою як сертифікати і статуси цих сертифікатів, позначки часу на момент додавання.
2. До документу додається електронний підпис в форматі LTA відповідальної особи (архіваріуса) та/або печатка установи для підтвердження прийняття електронного документу на архівне зберігання.

3. Метадані документу мають зберігатись у БД разом із самим документом, а геш-образ документу, геш-образ протоколу перевірки, протокол перевірки електронного підпису, тощо, зберігаються у окремій БД із зчепленими блоками на основі MAC.
4. Використовується приватний блокчейн з невеликою кількістю розподілених вузлів, де для кожного вузла використовується власний ключ MAC. Вузли блокчейну розгорнуто у кількох незалежних установах (юридичних компаніях, консалтингових компаніях, нотаріусів), які володіють власними ключами MAC та забезпечують незалежність і контроль цілісності власних вузлів блокчейну.
5. Для перевірки цілісності електронного документу і протоколу його перевірки, необхідно використовувати розподілений режим перевірки, що базується на консенсусі - результату перевірки отриманому від більшості вузлів. Щоб підробити дані, необхідно скомпрометувати більше половини вузлів блокчейну.
6. Регулярна та автоматична перевірка цілісності ланцюжків записів у БД блокчейну з занесенням результатів до самого блокчейну, дозволяє зменшити можливість підробки таких документів і прискорити отримання результату перевірки.
7. Виконується перевірка електронного підпису архіваріуса та/або печатки установи.
8. За розкладом, в автоматичному режимі, виконується додавання архівної позначки часу до електронного підпису архіваріуса та/або печатки установи з використанням підходів, які були описані раніше. Можливе використання алгоритмів підпису, що забезпечують або такий самий рівень захисту, або більший.
9. Забезпечення більшого рівня захисту можливе за рахунок використання алгоритмів підпису із більшою довжиною ключа і більшим розміром геш-образу, із більшим розміром MAC, чи взагалі, з використанням постквантових алгоритмів підпису. Допускається дублювання підписів, як з використанням класичного алгоритму підпису з більшою довжиною ключа, так і з постквантовим алгоритмом підпису.

Використання такої гібридної моделі поєднання класичного архіву з елементами блокчейну та приватного блокчейну з використанням MAC має підвищити довіру до даних протягом великого проміжку часу та надійність рішення в цілому.

Список використаних джерел

1. ETSI TS 119 511. Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques.
2. ETSI EN 319 102-1 V1.4.1 (2024-06). Electronic Signatures and Trust Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation.