МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МАРІУПОЛЬСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

АКТУАЛЬНІ ПРОБЛЕМИ НАУКИ ТА ОСВІТИ

Збірник матеріалів

XXVIII підсумкової науково-практичної конференції викладачів

24 лютого 2026

Київ 2026

УДК 061.3(063)

АКТУАЛЬНІ ПРОБЛЕМИ НАУКИ ТА ОСВІТИ: Збірник матеріалів XXVIII підсумкової науково-практичної конференції викладачів МДУ / За заг. ред. Т.В. МАРЕНИ, Київ: МДУ, 2026. с. 353

Рекомендовано до друку та поширення через мережу Інтернет вченою радою Маріупольського державного університету (протокол № 9 від 25 лютого 2026 року)

Збірник містить матеріали XXVIII підсумкової науково-практичної конференції викладачів МДУ, яка відбулася 24 лютого 2026 року в Маріупольському державному університеті.

У матеріалах висвітлені актуальні проблеми розвитку міжнародних відносин та зовнішньої політики, філософії та соціології, історії, економіки та менеджменту, права, екології, кібербезпеки, документознавства, культурології, журналістики, філології, літературознавства, методики викладання, педагогіки та психології.

Видання адресоване науковцям, викладачам, аспірантам та здобувачам вищої освіти, а також усім, хто цікавиться сучасними проблемами науки та освіти.

Редакція не несе відповідальності за авторський стиль тез, опублікованих у збірнику.

відмітити, що на сьогодні більшої популярності набирають методи глибинного навчання, які дозволяють поєднувати сигнатурні особливості та статистичні характеристики у певну глибинну мережу і проводити досконаліший аналіз аудіосигналів.

Література

1. Martyniuk H., Kozlovskiy V., Meleshko T., Sorokun A. Method of Finding Cover Signal for Audio Steganalysis Calibrated Methods. 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). 2021. Vol. 2. P. 1095–1100.

2. Мартинюк Г., Мартинюк І., Проценко Б. Аналіз сучасних методів стегоаналізу аудіосигналів. *Безпека інформації*. 2024, Т. 3 (30). С. 393-398

Охріменко Андрій,
кандидат технічних наук, старший викладач
кафедри системного аналізу та інформаційних технологій,
Маріупольський державний університет

КРИПТОГРАФІЧНА ЦІЛІСНІСТЬ І ДОВГОТРИВАЛА ВАЛІДАЦІЯ ПРИ АРХІВНОМУ ЗБЕРІГАННІ ЦИФРОВИХ ДАНИХ

В сучасному світі велика частка інформації існує виключно в цифровій формі, а її кількість постійно зростає. Це в свою чергу ставить нові задачі і виклики до довготривалого зберігання цифрової інформації. Все більшої ваги набирає фактор довіри до електронних документів. Довіра до цифрового документу ґрунтується на тому, що цілісність документу не порушена (він не модифікувався в процесі зберігання), документ автентичний (має встановленого автора) та створений в певний зафіксований час. При цьому важливим є те, щоб це все можна було перевірити навіть через десятки років.

Метою дослідження є аналіз існуючих криптографічних механізмів, що забезпечують довготривалу доказовість та цілісність електронних документів у процесі архівного зберігання.

Інформаційні системи для архівного зберігання цифрових даних зазвичай побудовані з використанням підходів викладених у:

1) концептуальній моделі Open Archival Information System (OAIS), яка стала міжнародним стандартом ISO 14721,

2) французькому стандарті електронного архівування NF Z42-013,

3) технічних настановах TR-03125 (TR-ESOR) від німецької BSI,

4) галузевих стандартах та рекомендаціях (наприклад, в сфері охорони здоров'я HSRAA «Guide to Archiving Electronic Records»),

5) рекомендаціях NIST та архівних установ, тощо.

До кожного документу, що вноситься до інформаційної системи архіву, можуть додаватись метадані для перевірки цілісності та автентичності даних (наприклад геш-суми, електронні підписи), дані про походження документу та його опис. В подальшому можуть виконуватись регулярні перевірки цілісності архівних даних (шляхом зіставлення геш-сум з еталонними значеннями), результати яких фіксуються в журналі для доведення незмінності документа впродовж усього часу його існування.

Проте електронні підписи, сертифікати, криптографічні алгоритми з часом втрачають актуальність. Сертифікати відкритих ключів електронного підпису мають обмежений термін дії. Через компрометацію ключів чи інші причини сертифікати можуть бути відкликані. Криптографічні алгоритми чи їх параметри з часом можуть стати слабкими. Без додаткових заходів, навіть підписаний документ може стати недійсним через кілька років. Тому архівне зберігання цифрових документів потребує довготривалої валідації підписів (Long-Term Validation), використання архівних міток часу, з подальшим періодичним оновленням (перепідпис, повторне отримання міток часу, тощо), використання криптографічно стійких алгоритмів. Таким чином, досягається підтримання довіри до архівних документів в часі.

Окрім того, існують технології ланцюгового гешування даних, наприклад, формування з групи файлів дерева Меркла впорядкованої структури гешів з однією архівною міткою часу. Цей підхід стандартизовано IETF у вигляді Evidence Record Syntax (ERS) в RFC 4998 (ASN.1) та RFC 6283 (XML) та дозволяє криптографічно довести існування даних у певний момент часу і підтримувати його валідність надалі [1]. У випадку зниження стійкості чи зламу алгоритмів, архівна система має своєчасно заново обчислити геші за новим алгоритмом і додати нову архівну позначку часу, таким чином зберігається достовірність та цілісність даних протягом десятиліть [2].

Концепція Long-Term Validation електронного підпису дозволяє підтвердити дійсність електронного підпису навіть через багато років після його накладання. Загальний підхід довготривалої валідації полягає у тому, що під час або одразу після підписання документа

збирається вся необхідна інформація для валідації (ланцюжок сертифікатів, OCSP відповіді про статус всіх сертифікатів в підписі, позначки часу підпису та даних) і вкладається в структуру підпису. Якщо підпис зроблено у форматах CadES-X Long, XadES-X-L або PadES-LTV, то документ вже містить необхідний набір даних для перевірки підпису в довгостроковому періоді.

В Україні нормативна база щодо довготривалого зберігання електронних даних активно формується та узгоджується з європейською, прийняті стандарти форматів підписів, дано визначення довгострокового КЕП, діють галузеві вимоги (НБУ, державні органи) щодо захищеного зберігання електронних документів. Наприкінці 2023 року Кабінет Міністрів затвердив вимоги до форматів удосконалених електронних підписів та печаток, що використовуються у наданні е-послуг. Згідно з ними, в Україні впроваджуються базові формати підписів ETSI – XML, CMS, PDF (XadES, CadES, PadES) на рівнях B-B, B-T, B-LT, B-LTA [3]. Це фактично імплементація європейських стандартів ETSI TS 119 102 та профілів Baseline, де рівень LT передбачає включення в підпис усіх необхідних даних для довготривалої валідації, а LTA – додаткова архівна мітка часу.

Також, для довготривалого зберігання використовуються технології розподіленого реєстру (DLT), зокрема, блокчейн, що використовується як інструмент забезпечення автентичності цифрових записів. Транзакції в блокчейн містять геш кожного архівного документу та захищені від несанкціонованого виправлення, тому що для підробки запису, потрібно одночасно скомпрометувати більшість вузлів мережі, що практично неможливо у публічних блокчейнах з консенсусом. Існує й інший підхід, коли використовуються приватні корпоративні блокчейни або геш-ланцюжки в середині архівних систем. Тобто технологія геш-ланцюжків лежить і в основі традиційних архівних доказів (ERS), і в блокчейні, різниця лише в ступені розподіленості і довіри до зовнішньої мережі.

Аналіз світових, європейських та українських практик довготривалого зберігання цифрових даних показує, що Україна активно переймає досвід впровадження передових рішень та адаптує нормативну базу до європейської. Провідні країни світу і ЄС вже мають усталені стандарти й технології для забезпечення криптографічної цілісності архівів, підтримання довгострокової валідності електронних підписів та експериментують із блокчейн для підвищення прозорості й довіри.

Література

1. Schwalm S., Korte U., Hühnlein D. Standards for the Preservation of Evidence and Trust for Electronic Records. *Archiving Conference*. 2014. Vol. 11. DOI: 10.2352/issn.2168-3204.2014.11.1.art00003.

2. Can I still prove the validity of a signature after ten years? URL: https://trustservices.Swisscom.com/en/support/help-center/can-i-still-proof-the-validity-of-a-signature-after-10-years (дата звернення: 16.12.2025)

3. Про затвердження вимог до форматів удосконалених електронних підписів та печаток, які використовуються для надання електронних публічних послуг, та вимог до створення та перевірки удосконалених електронних підписів та печаток, що базуються на кваліфікованих сертифікатах відкритих ключів: постанова Кабінету Міністрів України від 12 грудня 2023 р. № 1298.

Анжеліка Стахова,
кандидат технічних наук, доцент,
доцент кафедри системного аналізу та інформаційних технологій
Маріупольський державний університет

МЕТОД МОНТЕ-КАРЛО ДЛЯ АНАЛІЗУ ПОХИБОК СПЕКТРАЛЬНИХ ВИМІРЮВАНЬ У ЦИФРОВИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

У сучасних цифрових інформаційних системах значна частина даних формується на основі вимірювання аналогових сигналів із подальшим аналого-цифровим перетворенням та цифровою обробкою. Аналого-цифрові перетворювачі (АЦП) є ключовою ланкою таких систем, а їхні неідеальності безпосередньо впливають на точність аналізу даних [1]. Одним із фундаментальних джерел похибок є шум квантування, зумовлений кінцевою розрядністю АЦП, який особливо критично проявляється під час спектрального аналізу сигналів [2, 3].

У задачах аналізу даних, пов’язаних зі спектральною обробкою (FFT), важливими є не лише амплітудні, а й фазові характеристики окремих спектральних складових. Похибки, викликані шумом квантування, можуть призводити до спотворення спектра, появи додаткових гармонік та зниження достовірності оцінок параметрів сигналу [5, 6]. Тому актуальним є завдання кількісної оцінки впливу квантування на результати спектральних вимірювань із використанням сучасних методів числового аналізу.

У даній роботі розглянуто застосування методу Монте-Карло для аналізу похибок спектральних вимірювань, спричинених шумом квантування АЦП. Метод Монте-Карло широко застосовується для статистичного аналізу похибок у цифровій обробці сигналів і дозволяє враховувати випадкові параметри, зокрема початкову фазу сигналу, що є типовим