# Механізми забезпечення незмінності журналів аудиту як основа достовірності цифрових доказів

***Валерій Настопиров***

заступник начальника Управління інформаційних технологій — начальник відділу забезпечення захисту інформації та розвитку інформаційних систем, Антимонопольний комітет України, м. Київ, Україна, ORCID: https://orcid.org/0009-0006-3603-401X, e-mail: nastopyrov@amcu.gov.ua

*Розглянуто важливість забезпечення незмінності журналів аудиту в умовах глобальної цифровізації та кіберзагроз 2026 року. Проаналізовано ризики, пов'язані з APT-атаками, внутрішнім фродом і технічними збоями, що можуть компрометувати цифрові докази. Обґрунтовано перехід до систем на основі цільових профілів захисту та впровадження криптографічних механізмів гарантування цілісності даних.*

***Ключові слова:*** *журнали аудиту; цифрові докази; кібербезпека; цілісність даних; криптографічне хешування; судова експертиза.*

# Mechanisms for Ensuring the Immutability of Audit Logs as a Basis for the Reliability of Digital Evidence

***Valerii Nastopyrov***

*The article examines the importance of ensuring the immutability of audit logs in the context of global digitalization and cyber threats in 2026. The author analyzes the risks associated with APT attacks, internal fraud, and technical failures that can compromise digital evidence. The paper emphasizes the transition from formal security systems to systems based on target security profiles. Key technical mechanisms such as cryptographic hashing (SHA-256), "write-once" principles, and physical isolation of logs are proposed to ensure data integrity and procedural economy in legal proceedings.*

***Keywords:*** *audit logs; digital evidence; cyber security; data integrity; cryptographic hashing; forensic examination.*

Процеси глобальної цифровізації та цифрової трансформації у державній сфері в Україні призвели до того, що інформаційні системи (далі — *ІС*) стали не просто інструментом автоматизації, а первинним джерелом юридично значущої інформації. У 2026 році підрозділи із захисту інформації та кібербезпеки в державних інституціях, окрім забезпечення захисту від підвищеної кількості різноманітних видів атак на інформаційні системи, також забезпечувати надійний і сучасний захист для нових систем автоматизації. Судова експертиза все частіше стикається з необхідністю аналізу об'єктів, які існують винятково в цифровому середовищі, а через динамічний розвиток цієї сфери доволі часто це комбінація з різноманітних рішень [1]. За таких умов основним викликом стає забезпечення достовірності даних з носіїв інформації інформаційних систем такого типу. Якщо неможливо гарантувати, що інформацію в базі даних не модифікували після моменту її створення, вона втрачає статус належного доказу. Саме тому механізми забезпечення незмінності журналів аудиту потребують особливої уваги й пильності як у сфері кібербезпеки, так і в криміналістиці.

Надійність державних інформаційних систем сьогодні безпосередньо залежить від того, наскільки добре вони захищені від різних типів атак і чи актуалізували підготовку сценаріїв до ймовірних ризиків. Оскільки держава активно цифровізує процеси, дані із цих систем стають головними доказами в судах. Саме тому важливо гарантувати, що ці дані не були змінені. Основним елементом тут є незмінність журналів аудиту (логів) — записів про те, хто та що робив у системі.

За умови постійних зовнішніх кіберзагрозах та актів гібридної агресії, у контексті воєнного стану особливої актуальності набувають цілеспрямовані атаки (APT-атаки) з боку суб'єктів іноземної технічної розвідки та хактивістів [2]. Основною метою таких дій є не лише дестабілізація роботи державних реєстрів, а й латентна підміна критичних даних. За відсутності реалізованих механізмів незмінності журналів аудиту подібне втручання може залишатися невиявленим протягом тривалого часу, що може призве-

сти до прийняття юридично хибного рішення на основі скомпрометованих доказів. Наявні також адміністративні й операційні ризики, до яких належать загрози, пов'язані з антропогенним чинником — зокрема, можливим зловживання привілейованим доступом з боку персоналу (адміністраторів систем і баз даних) [3]. Можливість несанкціонованої модифікації записів особами, які мають легітимний доступ до інфраструктури, створює умови для внутрішнього фроду й корупційних виявів. Науковий підхід до захисту логів передбачає нівелювання можливості «саморедагування» дій адміністратора, що є критичним для забезпечення невідворотності відповідальності та прозорості державного управління. Окрім навмисних утручань, можуть мати місце системно-техногенні дефекти й апаратні збої. На достовірність цифрової інформації можуть вплинути чинники ненавмисного викривлення записів, оскільки помилки в конфігурації складних архітектурних рішень або критичні збої програмного забезпечення чи деградація апаратних компонентів можуть спричинити порушення цілісності даних. У цьому аспекті захищений журнал подій стає еталонною точкою відновлення, що дає змогу чітко розмежувати технічний збій і навмисну деструктивну дію під час проведення криміналістичного дослідження.

Хоча проведення експертиз у державному секторі здійснюють на безоплатній основі, ігнорування зазначених вище загроз призводить до значних утрат державного ресурсу. У разі якщо цілісність логів порушено, проведення комп'ютерно-технічної експертизи стає надмірно ресурсномістким. Це може зумовлювати: надмірні часові витрати, неефективне користування кадровим капіталом і зростання навантаження на експертні установи. Замість автоматизованої перевірки цілісності, експерти змушені виконувати трудомістку роботу з відновлення ланцюжків подій ручними методами, що розтягує строки досудового розслідування. Тож висококваліфіковані державні фахівці також витрачають робочий час на доведення очевидних фактів, які могли б бути підтверджені автоматично за наявності імутабельних логів, водночас накопичення черг на проведення складних досліджень гальмує роботу всієї системи правосуддя.

Отже, упровадження превентивних механізмів захисту (за принципом *Security by Design*) є кроком до оптимізації державних процесів. Це дає змогу забезпечити «процесуальну економію» — мінімізувати зусилля та час держави на з'ясування істини в судовому процесі.

Особлива небезпека полягає в тому, що кваліфікований зловмисник після вчинення маніпуляцій з даними намагається видалити або відредагувати «цифрові сліди» у журналах аудиту (*log*-файлах). Без надійного захисту цих журналів проведення ретроспективного аналізу інциденту стає технічно неможливим, що нівелює зусилля правоохоронних органів і судових експертів [1].

Для створення системи, якій можна довіряти, необхідно відійти від традиційних методів збереження логів на користь сучасних засобів захисту інформації, що відповідають актуальним цільовим профілям безпеки [4]. Провідними елементами такої системи є криптографічне закріплення через хешування: застосування стійких алгоритмів (*SHA-256* або аналогічних) дає змогу створювати унікальні контрольні суми для кожного запису. Формування ланцюжків хешів, де кожен наступний запис містить відбиток попереднього, унеможливлює непомітне видалення або заміну будь-якого рядка в минулому. Потрібно впровадження на рівні системного коду й налаштувань сховищ принципу, за якого дозволено лише операцію запису та суворо заборонено операції видалення або редагування вже наявних секторів даних. У фізичній і логічній ізоляції важливою є реалізація миттєвого дублювання журналів на виокремлений сервер, розміщений в іншому сегменті мережі з окремою системою авторизації. Це гарантує, що навіть у разі повної компрометації прав адміністратора з розширеним доступом в основній системі, він не зможе вплинути на архів логів у захищеному сховищі. Із позицій економіки, захист інформації — це не лише витратна частина бюджету, а й стратегічне управління активами та ризиками. Упровадження

автоматизованого контролю цілісності логів є значно дешевшим, аніж вартість розслідування одного масштабного інциденту, включно з орендою спеціалізованого обладнання, простоями в роботі державних сервісів та оплатою праці висококваліфікованих експертів. Довіра громадян і бізнесу до державних реєстрів має прямий грошовий еквівалент у вигляді інвестиційної привабливості й ефективності надання державних послуг. Будь-який скандал, пов'язаний із сумнівністю даних у реєстрах, спричиняє падіння довіри, що потребує значних витрат на відновлення іміджу та додаткові аудити. Якщо цілісність журналу аудиту підтверджено автоматично на основі криптографічних доказів, судовому експертові не потрібно проводити трудомісткі процедури з відновлення ланцюжка подій. Це прискорює розгляд справ і зменшує навантаження на бюджетні установи. Сучасний підхід до побудови систем захисту інформації в Україні відходить від формального КСЗІ до розробки систем на основі цільових профілів захисту [4]. Це дає змогу створювати гнучкі механізми авторизації, де кожен крок користувача жорстко прив'язаний до його ідентифікатора та фіксується в журналі аудиту із застосуванням кваліфікованого електронного підпису (КЕП). Захищена в такий спосіб система відповідає вимогам законодавства 2026 року й автоматично наділяє свої дані статусом належного цифрового доказу.

Уважаю за потрібне зазначити, що незмінність журналів аудиту — це вузька, але фундаментна ланка в ланцюзі забезпечення правосуддя в цифровому просторі. Інвестиції в незмінність даних є економічно обґрунтованими, оскільки вони трансформують інформаційну систему з пасивного сховища в надійне джерело юридично значущих фактів. Розвиток авторизованих систем із вбудованими механізмами контролю цілісності є безальтернативним шляхом розвитку для будь-якого державного органа, що прагне забезпечити стійкість до сучасних гібридних загроз [2].

### *Перелік джерел посилання*

1. Про затвердження Положення про державну експертизу у сфері технічного захисту інформації : наказ Адмін. Держспецзв'язку від 16.05.2007 р. № 93 (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/z0820-07 (дата звернення: 11.04.2026).
2. Аналітичний звіт про стан виконання Плану реалізації Стратегії кібербезпеки України за 2025 рік (основна частина) / Держспецзв'язку. Київ, 2026. 27 с. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=73801 (дата звернення: 13.04.2026).
3. Підсумковий звіт з кібербезпеки за II півріччя 2025 року. Тенденції атак, вразливості та ключові ризики для Підприємства / ДП «НАІС». 23 с. URL: https://nais.gov.ua/files/general/2026/03/24/20260324182225-93.pdf (дата звернення: 12.04.2026).
4. Міжнародні стандарти та правова регламентація цифрових (електронних) доказів у кримінальному аналізі : наук.-метод. рек. Харків, 2025. 36 с. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/10ad6bf2-b7d4-45d1-9923-34e9acc0d785/content (дата звернення: 14.04.2026).