УДК 004.056

Ланчевич А.І., здобувач
Балацька В.С., д. філ., ст. викладач
Полотай О.І., к.т.н., доцент
Львівський державний університет безпеки життєдіяльності

АРХІТЕКТУРА ІНТЕГРАЦІЇ БЛОКЧЕЙН-ТЕХНОЛОГІЇ У ПІДСИСТЕМУ АУДИТУ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Підсистема аудиту є складовою комплексних систем захисту інформації (КСЗІ), що забезпечує реєстрацію подій інформаційної безпеки, контроль адміністративних дій та формування доказової бази під час розслідування інцидентів. Типовою проблемою є відсутність криптографічно підтвердженої незмінності аудиторських артефактів у разі використання централізованих сховищ журналів (лог-сервери, SIEM), що зумовлює ризики ретроспективної модифікації або видалення записів, зокрема за сценаріїв внутрішніх загроз або компрометації привілейованих облікових записів.

Для підвищення доказовості аудиторських даних запропоновано архітектуру інтеграції permissioned blockchain у підсистему аудиту КСЗІ у форматі реєстру доказів (evidence ledger). Архітектура базується на розмежуванні on-chain/off-chain рівнів зберігання: первинні журнали подій і результати кореляції зберігаються у SIEM (off-chain), тоді як у блокчейн-мережі фіксуються лише криптографічні «якорі» пакетів журналів (Merkle-root або хеш пакета) разом із метаданими. Такий підхід мінімізує обсяг on-chain даних і зменшує накладні витрати, одночасно забезпечуючи можливість незалежної перевірки цілісності й послідовності фіксації аудиторських артефактів.

Архітектурна модель включає: (1) джерела подій (сервери, мережеві пристрої, засоби захисту, прикладні сервіси); (2) модуль збору та нормалізації журналів; (3) сховище журналів/SIEM для зберігання повних подій і виконання кореляції; (4) шлюз доказів (Evidence Gateway), який виконує пакетування подій за часовим інтервалом або кількістю записів, формує Merkle-дерево та обчислює корінь R, накладає електронний підпис і формує метадані пакета; (5) permissioned blockchain-мережу для реєстрації доказів; (6) модуль верифікації для підтвердження цілісності журналів під час аудиту або розслідування.

Формування доказу для пакета Bt= {e1, e2, …, en} реалізується послідовністю: нормалізація подій ei; обчислення листів hi= H(ei) та кореня R = MerkleRoot(h1hn); формування структури доказу

P = ⟨ID, tstart, tend, n, R, prevR, src, Sig⟩, де *prevR* – попередній корінь для зв’язування пакетів у безперервний ланцюжок, *Sig* – підпис Evidence Gateway. Запис *P* у блокчейн забезпечує виявлення будь-якої зміни off-chain журналів через розбіжність контрольних значень. Використання *prevR* підвищує стійкість до сценаріїв «вирізання» фрагментів журналів та ретроспективних підмін, оскільки порушується ланцюгова узгодженість пакетів.

Запропонований підхід забезпечує властивості tamper-evidence для аудиторських артефактів, підвищує рівень довіри до результатів функціонування підсистеми аудиту КСЗІ та створює механізм доказовості під час перевірок відповідності й цифрової криміналістики. Розмежування on-chain/off-chain рівнів і пакетування подій дозволяють масштабувати рішення без критичного впливу на продуктивність SIEM і мережевої інфраструктури. Перспективним напрямом подальших досліджень є обґрунтування параметрів пакетування (часове вікно, розмір пакета), оцінювання накладних витрат і формалізація моделі довіри між учасниками permissioned blockchain у контексті КСЗІ.

Список використаних джерел

1. Балацька В. С., Опірський І. Р. Забезпечення конфіденційності персональних даних і підтримки кібербезпеки за допомогою блокчейну. Кібербезпека: освіта, наука, техніка. 2023. № 4(20). С. 6–19. DOI: https://doi.org/10.28925/2663-4023.2023.20.619

2. Балацька В., Дмитрів Н. Міжорганізаційний обмін конфіденційними персональними даними на основі дозвільного блокчейн. Кібербезпека: освіта, наука, техніка. 2025. № 2(29). С. 178–193. DOI: https://doi.org/10.28925/2663-4023.2025.29.875

3. Балацька В., Ткачук Р., Маслова Н. Еволюція КСЗІ та інтеграція блокчейн-технологій у кіберзахисті державних інформаційних систем України. Кібербезпека: освіта, наука, техніка. 2025. № 2(30). С. 316–332. DOI: https://doi.org/10.28925/2663-4023.2025.30.975

4. Балацька В. С., Івануса А. І., Пановик У. М. Метод інтеграції політик інформаційної безпеки, стандартів та протоколів у процес побудови комплексної системи захисту інформації в організації. Кібербезпека: освіта, наука, техніка. 2025. № 3(31). С. 283–297. DOI: https://doi.org/10.28925/2663-4023.2025.31.1021

5. Balatska V., Opirskyy I. Blockchain as a tool for transparency and protection of government registries. Ukrainian Scientific Journal of Information Security. 2024. Vol. 30, Issue 2. P. 221–230. DOI: https://doi.org/10.18372/2225-5036.30.19211