БЛОКЧЕЙН ЯК ІНСТРУМЕНТ ПІДВИЩЕННЯ СТІЙКОСТІ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ ДО ІНСАЙДЕРСЬКИХ ЗАГРОЗ

Валерія БАЛАЦЬКА

Василь ПОБЕРЕЖНИК

У сучасних умовах цифрової трансформації державних органів та активного розвитку електронних сервісів особливого значення набуває питання захисту персональних даних та забезпечення довіри до державних інформаційних систем. Традиційні комплексні системи захисту інформації (КСЗІ), що ґрунтуються на криптографічному захисті, ідентифікації та контролі доступу, демонструють обмежені можливості у протидії інсайдерським загрозам. Центральним слабким місцем залишаються журнали подій, які, попри використання криптографічних механізмів, можуть піддаватися маніпуляціям з боку адміністраторів, що істотно знижує їхню доказову цінність у разі проведення аудитів чи розслідування інцидентів.

Для подолання цієї вразливості запропоновано інтеграцію технологій дозвільного-блокчейн (Hyperledger Fabric) у КСЗІ як інструменту децентралізованого журналювання та незалежної верифікації транзакцій. Такий підхід забезпечує незмінність даних, колективний контроль послідовності подій та унеможливлює приховане редагування чи видалення записів. Додаткове використання Zero Knowledge Proofs (ZKP) дозволяє підтверджувати достовірність транзакцій без розкриття чутливої інформації, що є особливо важливим для захисту персональних даних і відповідає вимогам міжнародних нормативів, зокрема GDPR.

Експериментальне моделювання було реалізовано у віртуалізованому середовищі VMware, де на базі Hyperledger Fabric створено кілька вузлів, що імітували роботу органів державної влади. Кожен вузол мав власну базу даних і функціонував як незалежний учасник мережі. Використання механізму консенсусу Raft забезпечило досягнення згоди між усіма вузлами без істотних затримок, а середній час підтвердження транзакцій склав 1–1,2 секунди, що є прийнятним для більшості адміністративних процедур. Усі події, пов'язані з доступом до даних (створення, модифікація, вилучення записів, запити довідок), автоматично фіксувалися у блокчейн як хешовані транзакції з цифровими підписами. Це унеможливлювало їх непомітне редагування навіть адміністраторами з найвищими привілеями.

Результати експерименту показали підвищення надійності журналювання на 25–30 % у порівнянні з централізованими системами, ско-

рочення часу виявлення інсайдерських загроз майже на 40 % та суттєве зниження ризику маніпуляцій із журналами подій. Додатково було інтегровано модуль поведінкової аналітики на основі алгоритмів машинного навчання (Isolation Forest, Autoencoder), який автоматично аналізував активність користувачів. У разі відхилення від типової поведінки формувалася транзакція, що записувалася у блокчейн, створюючи незмінну доказову базу для подальшого аудиту.

Аналіз отриманих результатів свідчить, що поєднання класичних механізмів КСЗІ з блокчейн-технологіями та машинним навчанням створює гібридну архітектуру захисту, здатну забезпечити якісно новий рівень стійкості державних інформаційних систем. Така архітектура підвищує ефективність реагування на інциденти, зменшує залежність від адміністраторів і відкриває можливості для незалежного аудиту в режимі реального часу.

У довгостроковій перспективі запропонований підхід може бути масштабований для впровадження у національних цифрових платформах, таких як “Дія”, а також у міжвідомчих системах обміну даними. Це дозволить створити єдиний простір довіри в українському електронному врядуванні, підвищити захищеність критичної інформаційної інфраструктури та відповідність міжнародним стандартам кібербезпеки (ISO/IEC 27001, ISO/IEC 27701). Таким чином, інтеграція блокчейн у КСЗІ виступає дієвим інструментом підвищення рівня інформаційної безпеки, довіри та прозорості функціонування державних інформаційних систем.