УДК 004.056

Нарольський Т.М., здобувач,
Балацька В.С., д-р філ., ст. викладач,
Полотай О.І., к.т.н., доцент
Львівський державний університет безпеки життєдіяльності

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ РІВНЯ ДОВІРИ В ДЕЦЕНТРАЛІЗОВАНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ КСЗІ НА ОСНОВІ БЛОКЧЕЙН-ТЕХНОЛОГІЙ

Інформаційні системи, особливо ті, що функціонують у державному секторі, стикаються з проблемою втрати довіри до джерел та процесів обробки даних. Централізовані структури керування доступом, навіть за умови побудови комплексних систем захисту інформації (КСЗІ), залишаються вразливими до людського фактора, зловживань правами адміністратора та внутрішніх загроз.

В умовах децентралізації даних усе більшої актуальності набувають механізми математичного формалізування довіри, які дозволяють оцінювати поведінку кожного елемента системи не лише за його технічними параметрами, а й за історією взаємодій.

Метою дослідження є створення математичної моделі, яка дозволяє формалізувати процес формування довіри між вузлами в децентралізованій архітектурі КСЗІ. В основі запропонованої моделі лежить поєднання поведінкового аналізу, теорії графів та ймовірнісних функцій ризику. Такий підхід дає можливість системі автоматично виявляти аномалії, прогнозувати можливі загрози та реагувати ще до того, як вони реалізуються.

Для вузла *i* у момент часу *t* рівень довіри визначається функцією:

$$T_i t = \alpha P_i t + \beta H_i t + \gamma S_i t,$$

де $P_i(t)$ – ймовірність коректної поведінки; $H_i(t)$ – історичний показник дотримання політик безпеки; $S_i(t)$ – структурна взаємодія з іншими вузлами; α, β, γ – вагові коефіцієнти $(\alpha+\beta+\gamma=1\alpha + \beta + \gamma = 1\alpha+\beta+\gamma=1)$, що визначають вплив кожного параметра.

Якщо рівень довіри вузла падає нижче порогового значення Tcrit, система автоматично активує політику підвищеного контролю, багатофакторну аутентифікацію або перевірку транзакцій через смарт-контракт.

Для кількісного опису ризику використовується експоненціальна залежність: $R_i(t) = 1 - e^{(-\lambda(Tcrit - T_i(t)))}$, де λ – параметр чутливості системи. Зі зменшенням довіри ризик зростає нелінійно, що дозволяє більш точно реагувати на небезпечні зміни у поведінці користувачів.

Модель тестувалася в середовищі Python із використанням бібліотек *NetworkX* і *SymPy*. Для мережі з 50 вузлів при наявності 20 % зловмисних елементів середній рівень довіри зберігався вище 0,75, що свідчить про стійкість системи до внутрішніх аномалій. Алгоритмічна складність розрахунку матриці довіри становила $O(n^2)$, що є прийнятним для permissioned blockchain-мереж середнього масштабу.

Практична цінність запропонованого підходу полягає в тому, що він дозволяє перейти від статичних правил доступу до динамічної системи довіри, де кожна дія користувача впливає на його поточний статус у мережі. Такий механізм може бути реалізований на рівні permissioned blockchain (наприклад, Hyperledger Fabric, Quorum), де вузли виступають рівноправними учасниками з формалізованими математичними атрибутами довіри.

Використання блокчейн як реєстру довірчих взаємодій забезпечує прозорість і незмінність журналів подій, а математичне моделювання довіри – гнучкість і прогнозованість поведінки системи. У сукупності це створює основу для формування пояснюваної безпеки – коли кожне управлінське рішення (блокування, попередження, зміна прав доступу) може бути обґрунтоване формулою або моделлю.

Отже, запропонований підхід дозволяє поєднати переваги блокчейн-технологій із класичними методами оцінки ризику та забезпечення конфіденційності. Його застосування у КСЗІ державних реєстрів, освітніх або банківських систем дозволяє мінімізувати людський фактор, підвищити рівень довіри між користувачами та забезпечити відповідність міжнародним стандартам ISO/IEC 27001, ISO/IEC 27701 і GDPR.

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. 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

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